KONFERENCIA ANYAG

SZÉCHENYI ISTVÁN EGYETEM

GYŐR

2004. ÁPRILIS 5-7.

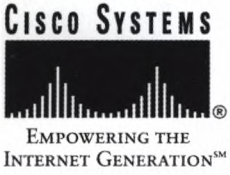
NETWORK SHOP 2004

A NETWORKSHOP 2004

KONFERENCIA RENDEZŐJE:

NEMZETI INFORMÁCIÓS INFRASTRUKTÚRA FEJLESZTÉSI PROGRAM
HUNGARNET EGYESÜLET

A KONFERENCIA KIEMELT TÁMOGATÓJA:



CISCO SYSTEMS MAGYARORSZÁG KFT.

TOVÁBBI TÁMOGATÓK:

HEWLETT PACKARD MAGYARORSZÁG KFT.

IBM MAGYARORSZÁGI KFT.

MATÁV RT.

MICROSOFT MAGYARORSZÁG KFT.

SIEMENS RT.

SUN MICROSYSTEMS KFT.

SYNERGON INFORMATIKA RT.

SZÉCHENYI ISTVÁN EGYETEM, GYŐR

Nemzeti Információs Infrastruktúra Fejlesztési Program
(NIIF Program)

NETWORKSHOP 2004 KONFERENCIA

GYŐR
SZÉCHENYI ISTVÁN EGYETEM
2004. ÁPRILIS 5-7.

TUTORIÁLOK
2004. ÁPRILIS 4.

http://nws.iif.hu
http://www.iif.hu/rendezvenyek/networkshop
http://www.conftours.mtesz.hu/nws2004

PROGRAM

A konferencia helyszíne:
SZÉCHENYI ISTVÁN EGYETEM
9026 Győr, Egyetem tér 1.
Telefon: + 36 96 503-400
http://www.gyor.hu

NEMZETI INFORMÁCIÓS INFRASTRUKTÚRA FEJLESZTÉSI IRODA

Felelős kiadó: Nagy Miklós igazgató
Szerkesztő: Fulajtár Pál
Nyomás: Tiszszo Nyomda, Budapest

Kivonatok

NAGYSEBESSÉGŰ HAZAI ÉS NEMZETKÖZI INTERNET, HÁLÓZATI TECHNOLÓGIÁK ÉS FEJLESZTÉSEK

Az NIIF IPv6 projekt

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda
Kovács András <akov@niif.hu>
NIIF Iroda
Máray Tamás <maray@niif.hu>
NIIF Iroda

Az Előadás NIIF IPv6-os hálózatának jelenlegi topológiáját, az elvégzett kísérleteket és az elért eredményeket mutatja be. A 2003-as és 2004-es év folyamán erre az IPv6-os natív infrastruktúrára építve elkezdődött a dual stack IPv6-os szolgáltatásokat tesztelése, valamint IPv6 alkalmazások (videokonferencia, multimédia játékok) tesztelése. Kitérünk arra, hogy milyen nehézségekkel kellett szembe néznünk a dual-stack IPv4-IPv6 infrastruktúra kialakításakor. Áttekintjük azt is, hogy jelenleg a világban és elsősorban az Európai Unióban milyen stádiumban vannak az IPv6 szolgáltatások és milyen hatások mozgatják az IPv6 szolgáltatások bevezetését.

IP hálózatok minőségmenedzselése

Zsiga Árpád <arpad.zsiga@siemens.com>
Siemens Rt.
Újvári Tibor <tibor.ujvari@siemens.com>
Siemens Rt.

Az előadás az IP hálózatok minőségvizsgálati módszereit tekinti át és mutat néhány mérési eredményt. A mért eredmények a Siemens-Rt. által fejlesztett, NetCheck IP minőségmenedzselő rendszerrel készültek.

Áttekintjük a hálózatminősítés aktív és passzív méréseken alapuló megoldásait, az SNMP protokoll felhasználását, a mérendő QoS paraméterek körét.

Az SLA minősítés előnyeit igyekszünk kiemelni, összehasonlítva a menedzselt és nem menedzselt hálózaton a fenntartási tevékenységeket, és megmutatjuk a NetCheck által generált SLA alarm elvét. A menedzselt hálózaton SLA minősítést végző eszköz dolgozik, előjelző és trend analízis riasztással. Az SLA (Service Level Agreement) minősítés egy időbeni és minőségi rendelkezésre állás vizsgálatát, dokumentálását és segítését jelenti.

Bemutatjuk a hálózat minőségmenedzselése során alkalmazott analíziseket és az ezek alapján képzett performance analízis riasztásokat. A performance analízis minőségi osztályok szerinti eloszlásfüggvényt képez a hálózat működéséről.

A mérőrendszer adatgyűjtő, mérésvezérlő, feldolgozó és WEB alapú megjelenítő elemekből áll. Az adatgyűjtő elemek SNMP és FLOW adatokat fogadnak és tárolnak. A mérésvezérlő konfigurálja az adatgyűjtő és adatküldő elemeket. WEB felületen keresztül érhetők el a mérési eredmények és a mérésvezérlés. Kisebb hálózatoknál egy gépben is lehet a teljes rendszer, nagyobb hálózatoknál pedig a mérésvezérlő és az adatgyűjtő elemeket elosztva telepítjük.

A mérések konfigurálásánál azt kell megadni, mit, hol és mikor mérünk. A méréseket mérési csoportokban adjuk meg és hajtjuk végre. A mérési csoportban azonos időzítéssel hajtjuk végre a csoporthoz rendelt méréseket a csoporthoz rendelt hálózati elemeken . A mérések a méréshez rendelt paraméterek lekérdezéséből és feldolgozásából állnak. A feldolgozás a lemért forrásadatok között megadott matematikai összefüggések (analízis képlet) szerint történik. A riasztások felügyeleti PC-n, mail vagy SMS formátumban is kiadhatóak.

Az ismertetésre kerülő rendszer alkalmas folyamatos minőségmenedzselésre vagy audit jellegű minőségvizsgálatok elvégzésére.

A Siemens NetCheck ALAPSZOLGÁLTATÁS keretében a Siemens Telepíti és Konfigurálja, majd a felhasználó teljeskörűen használja a NetCheck mérőrendszert.

A Siemens NetCheck Üzemeltetés szolgáltatás keretében a Siemens TREND ANALÍZIS vizsgálatot végez a hálózat minőségi paraméterein, és előjelzi az SLA-ban definiált minőségi előírásoktól való eltérést, valamint a hálózat minőségfelügyeleti riasztásait kezeli.

A Siemens NetCheck HÁLÓZATMONITOROZÁS szolgáltatás keretében a Siemens mérési időszakonként RIPORTOT készít a hálózatról, és jelzi a hálózat minőségi problémáit, illetve javaslatot tesz a hibák kiküszöbölésére.

A Siemens NetCheck AUDIT szolgáltatás keretében a Siemens AUDITÁLJA a hálózatot, melynek során teljeskörű minőségdiagnosztikát végez. Méri, elemzi, regisztrálja a hálózat minőségi működését, az eszközök kihasználtságát, illetve javaslatot tesz a hibák kiküszöbölésére és az erőforrás allokáció módosítására.

A NetCheck szolgáltatási kör bővülni fog a közeljövőben a voip specifikus mérések terén. Itt a jelenleg is meglévő voip specifikus QoS minősítés mellett, az aktív teszt és az eszköz specifikus hívásrekord rögzítés felé lépünk.

Az előadás második részében a felhasználási lehetőségeket riport részleteket mutatunk.

Mobil multicast protokollok vizsgálata IPv6 hálózatokban

Kovácsházi Zsolt <kz365@hszk.bme.hu>
BME

Kis Zoltán Lajos <kz345@hszk.bme.hu>
BME

Kersch Péter <kpeti@sch.bme.hu>
BME

Simon Csaba <simon@david.tmit.bme.hu>
BME

Az Internet alapú műsorszórás, telefon- és videokonferenciák és sok más alkalmazás alapja a multicast, aminek segítségével jelentős sávszélesség megtakarítás érhető el az unicast alkalmazásokkal szemben. A mobil eszközök és alkalmazások térhódításával természetes igényként

jelentkezik, hogy a multicast alkalmazásokat mobil környezetben is használni lehessen.
A Mobil IPv6 azonban csak az unicast forgalom mobilitásával foglalkozik. Kutatói körökben a mobil multicast támogatására két különböző megközelítés terjedt el: a kétirányú alagutazás (*bidirectional tunelling*) és a távoli feliratkozás (*remote subscription*).
A kétirányú alagutazás során a mobil állomás az otthoni ügynökének segítségével csatlakozik multicast csoportokhoz. Hátránya, hogy az otthoni ügynök sok állomás esetén szűk keresztmetszetet jelenthet, illetve, hogy az alagutazás miatt nem használja ki a többesadás nyújtotta sávszélesség-takarékos útvonalválasztást.
A távoli feliratkozásnál a mobil állomás az idegen hálózat helyi multicast útválasztóján keresztül csatlakozik egy multicast csoporthoz, mint az adott hálózat fix állomásai. Itt az új ágak kiépülésének ideje alatt csomagvesztés, ezáltal szolgáltatás kiesés jelentkezhet.

A két protokoll hátrányainak kiküszöbölésére számos javaslat született, ezek közül a távoli feliratkozás módszernek egy olyan továbbfejlesztését ismertetjük, amely lehetővé teszi a multicast adatfolyamok zökkenőmentes hívásátadását. A módszer két pontban fejleszti tovább a távoli feliratkozás koncepcióját: gyorsítja a fa kiépítését az MLD időzítők megkerülésével, valamint hívásátadáskor alagutak kiépítésével megszünteti a csomagkiesést. Ennek implementálásaként jött létre protokollunk, az ***MMCAST.*** A tervezése során olyan architektúrát használtunk, melyben a multicast útválasztóknak nem kell ismerniük a protokollt.

A hívásátadást a mobil állomások kezdeményezik. A létrehozott GUI segítségével ez történhet mind automatikusan, mind manuálisan. Amennyiben szükséges a jelenlegi és az új bázisállomás között egy alagutat épít ki, amelyen az új bázisállomás megkapja a szükséges folyamokat mindaddig, míg ki nem épülnek hozzá a multicast fák.

Egyik méréssorozatunk a WLAN → WLAN hívásátadások paramétereinek mérése. Eredményeink mutatják, hogy sikerült zökkenőmentes hívásátadást: az átadás során nem történt csomagvesztés, és az átadás közben csak minimálisan nőtt meg a csomagkésleltetés.

A másik méréssorozatban WLAN → GPRS, ill. GPRS → WLAN technológiák közti hívásátadásokat vizsgáltunk. Leszámítva a GPRS technológiából adódó megnövekedett késleltetést a sávszélességének megfelelő adatfolyamokkal itt is sikerült a „zökkenőmentes" hívásátadás megvalósítása.

A mérési eredmények bebizonyítják, hogy az implementált protokoll a zökkenőmentes hívásátadással pontosan a jobb minőségű és megbízhatóbb szolgáltatások bevezetését teszi lehetővé, a sávszélesség takarékos kihasználása mellett.

Nemzetközi kitekintés

Bálint Lajos, PhD. <h48bal@helka.iif.hu>
NIIF Iroda

Az előadás az NIIF Program széles nemzetközi kapcsolatrendszerét vizsgálja röviden. Kiemelten foglalkozik a GEANT fejlesztése kapcsán lezáruló GN1 projekttel és vázolja a GN1 folytatásaként ez évben beinduló GN2 projekt előkészítésének helyzetét. A TERENA tevékenységének bemutatása kapcsán a nemrég zárult SERENATE projekt eredményeinek ismertetésére koncentrál. Szól a nemzetközi kapcsolatrendszer néhány további fontos eleméről, az ismertetések fő szempontjaként minden esetben a nemzetközi konnektivitás és a nemzetközi együttműködés eredményeit és lehetőségei tartva szem előtt. Az előadás fő célja egyrészt az, hogy felhívja a hallgatóság figyelmét a legfontosabb nemzetközi szervezetekben végzett munkákra, valamint azokra a lehetőségekre, melyek gyümölcsöző és elismert nemzetközi kapcsolataink továbbfejlesztésében rendelkezésünkre állnak, másrészt annak bemutatása, hogy a szervezeti kapcsolatok hogyan biztosítják a magyar oktatási intézmények, kutatóhelyek és közgyűjtemények

számára, hogy egyenjogú partnerekként részesülhessenek mindazokból az előnyökből, melyek a nyugat-európai országok hasonló intézményei számára rendelkezésre állnak.

Nagysebességű TCP protokollok

Telbisz Ferenc <telbisz@sunserv.kfki.hu>
KFKI RMKI SzHK és MATÁV ÖKI-FI

Németh Vilmos <nemeth@ttt-atm.ttt.bme.hu>
Egyetemközi Távközlési és Informatikai Központ

Molnár Sándor dr. <molnar@tmit.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

Szabó Róbert dr. <robert.szabo@tmit.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

Az Internet hálózat működése és stabilitása jelentős mértékben a Transmission Control Protocol-ba (TCP) épített forgalomszabályozáson (flow control) és torlódásvezérlésen (congestion control) nyugszik. A közel két évtizede kidolgozott protokoll jól viselkedik alacsony sebességeknél, megszokott hálózati alkalmazások esetén, és garantálja az adatok megbízható szállítását a végpontok között heterogén hálózatokban, de nem nyújt hatékony adatátvitelt, ha nagymennyiségű (terabájt, petabájt) adatot kívánunk továbbítani nagy távolságra gigabites összeköttetéseken.

Ezért néhány neves egyetem és kutatóintézet hozzáfogott a TCP protokoll új generációjának a kidolgozásához. Mivel a TCP protokoll gyenge sávszélesség kihasználását a torlódásvezérlési algoritmusban alkalmazott korlátok és a csomagvesztést követő erős visszaszabályozás okozza, ezért az Internet szállítási protokolljának hiányosságait a forgalom- és torlódásvezérlés módosításával próbálják kiküszöbölni. Ezen munkák során több javaslat született, amelyekből a TCP protokoll új verziója születhet meg. Ezek az új TCP protokollok a jelenlegi IP szolgáltatásra épülnek. A közelmúltban végzett kísérletek azt mutatták, hogy az új TCP verziók lényegesen nagyobb átviteli sebességet tesznek lehetővé.

A jelenleg használatos TCP protokoll módosítása és alkalmazása számos elméleti és gyakorlati kérdést vet fel. Ezért az Egyetemközi Távközlési és Informatikai központ (ETIK), a BME Távközlési és Médiainformatikai Tanszékével, valamint a MATÁV PKI-val együttműködve kutatásokat kezdett a nagy sebességű TCP protokollok működésének és viselkedésének a tanulmányozására. A kutatások kiterjednek többek között: a különböző TCP protokollok teljesítményének és együttműködésének a vizsgálatára, forgalmi modellezésére, nagy sebességű TCP protokoll fejlesztésére és kísérleti környezetben való vizsgálatára.

Az előadás keretében áttekintjük a nagy sebességű TCP protokoll fejlesztésének legújabb irányait. Az előadás összehasonlítja a különböző TCP megoldásokat, ezenkívül bemutatja az ezen a területen elindult hazai kutatások céljait és eredményeit.

IPv6 technológia alkalmazása a szélessávú hozzáférési hálózatokban

Szabó Gábor <szabo.gabor@siemens.com>
Siemens Rt.

IPv6 technológia alkalmazása a szélessávú hozzáférési hálózatokban

Az Internet alkalmazásának egyik – sokáig csak futurisztikus jövőképekben megfogalmazott – lehetősége a háztartási hálózatok („home networking") területe. A háztartási hálózatok a jelenlegi otthoni Internet felhasználáshoz képest (felhasználó otthoni PC-ről éri el az Internetet) új jellemzőkkel rendelkeznek: kibővül a hálózati eszközök köre (set-top box-ok, háztartási eszközök, érzékelők, kamerák), a kommunikáció iránya (háztartáson belül, távolról a háztartási hálózat felé). A szélessávú (egyúttal állandó) hálózati hozzáférés, a vezeték nélküli hálózati technológiák rohamos bővülése napjainkra reális közelségbe hozza a háztartási hálózatok elterjedését, mely komoly kihívást jelent a jelenlegi IPv4 alapú Internet számára és az IPv6 technológia alkalmazásának a 3G mobil eszközök mellett a másik fő hajtóerejévé válhat.
Az előadás bemutatja az IPv6 háztartási hálózatokban történő alkalmazásának előnyeit, elemzi a háztartási IPv6 alhálózat szélessávú Internet hozzáférésének lehetséges műszaki megoldásait, illetve áttekinti, hogy az alkalmazott hálózati protokollok és eszközök hol tartanak az IPv6 implementáció folyamatában.

Felhordó hálózat rekonstrukciója az ELTE Lágymányosi épületében

Borosnyay Csaba <borosnyay.csaba@elte.hu>
ELTE Információtechnológiai Központ

Az ELTE lágymányosi tömbje három épületből áll, a legidősebb 1992-ben, a legfiatalabb 2001-ben került átadásra. A három épület informatikai infrastruktúrája jól tükrözi az elmúlt 12 év trendjeit illetve a hálózattervezési elvek változásait.

Az épületek közül leginkább a két idősebb szorult felújításra. Költség- illetve eszközoptimálási megfontolások alapján a Természettudományi kar 1998-ban átadott „Északi" épületének felhordóhálózatán végeztük el az első rekonstrukciót. A hálózat alapját képező kábelezés megfelel a CAT5E szabványnak, így az aktív eszközök cseréjére, illetve a kábelrendezők átkábelezésére redukálódott a feladat.

A felhasználókat ellátó mintegy 1300 aktív végpontot az épület hat kábelrendezőjéből szolgáljuk ki. Az épület átadása óta üzemelő moduláris rendszerű DECHUB típusú switcheket négy helyen moduláris rendszerű Catalyst switchekkel váltottuk fel, míg a fennmaradó két kábelrendezőben desktop switchekkel oldottuk meg a feladatot.

Az eszközök lecserélésével egyidejűleg az épületgerinc meghajtását is korszerűsítettük. Az eredeti koncepcióban szereplő ATM alapú meghajtás helyett korszerűbb és előremutatóbb GigabitEthernet alapú meghajtást építettünk ki.

A beépített aktív eszközök segítségével jelentősen javult a szolgáltatás minősége a felhasználók irányába, és egy lépéssel közelebb kerültünk egy, az egész ELTE-re kiterjedő homogén rendszerhez kialakításához.

Az intézményi hálózathoz való hozzáférés szabályozása

Budai Károly <karoly_budai@hu.ibm.com>
IBM Magyarországi Kft.

Az utóbbi időben igen széles körben elterjedt a vezeték nélküli hálózati szegmensek alkalmazása. Így többek között felbukkantak szinte az összes egyetemi épületegyüttesi (Campus) hálózatban is. E megoldás megjelenése – a technológia rohamos elterjedése következtében – kihívást jelent az intézményi hálózatok hozzáférés-szabályozása számára.
Az előadás célja, hogy áttekintse mindazon elterjedtebb módszereket, melyek e körülmények között megoldást nyújtanak a hálózatok védelmére, a hozzáférés minél finomabb szabályozására. Különös hangsúllyal kívánja vizsgálni azokat az eszközöket, melyek egységesen képesek kezelni a vezetékes és vezeték nélküli hálózatos infrastruktúrát.

A HBONE 2003. évi fejlesztési eredményei

Farkas István <istvan@sztaki.hu>
MTA SZTAKI

A HBONE hálózatában 2003-ban jelentős fejlesztéseket hajtott végre az NIIF Program.
Az előadás összefoglalja a legfontosabb műszaki eredményeket, bemutatja a felhordó hálózati technológiák jelenlegi helyzetét, koncentrálva a budapesti bővítésekre. (10 Gbit/s kapcsolatok, nemzetközi, gerinc és intézményi irányokba.)
Az előadás áttekinti az NIIF behívó rendszerének aktuális állapotát, illetve a csatlakozott intézmények jelenlegi státuszát.
Az előadás bemutatja, hogy a HBONE miképpen támogatja egy sor projekt megvalósítását: pl. IPv6, IP telefónia, videokonferencia, clustergrid, névtár.

A HBONE végponti telepítések tanulságai és kalandjai az elmúlt 3 évben

Szabó Szabolcs <szesz@sztaki.hu>
MTA SZTAKI

Bangó György <bango@sztaki.hu>
MTA SZTAKI

Jurányi Rudolf <juranyi@sztaki.hu>
MTA SZTAKI

Kovács Attila <attis@sztaki.hu>
MTA SZTAKI

A projekt 2001 második felében indult útjára. Ekkorra az NIIF-hez kapcsolódó bérelt vonalas (64kbps – 512kbps) intézmények végponti eszközei (általában pc alapú Multigate routerek ill. COMX kartyás linux-os pc-k) egyre többször mondták fel a szolgálatot, megérettek a cserére. Az eszközök cseréjét az is indokolta, hogy az elavuló félben lévő eszközök konfigurálása nehézkes volt, menedzsment szempontjából sok kívánnivalót hagytak maguk után. Az NIIF felügyelt végponti szolgáltatást akart nyújtani a végfelhasználó intézményeknek, ehhez viszont korszerű, követett, felügyelhető végponti eszközökre volt szükség. A régi eszközök kiváltását a Cisco

Systems 805-ös sorozatú routerével oldottuk meg, mely már konfigurálás és menedzsment szempontjából is beváltotta a hozzá fűzött reményeket.
Az elmúlt 3 évben az "elavult routerek cseréje" projekt kinőtte magát, s fokozatosan újabb projektek kapcsolódtak hozzá.
Az első ilyen nagyobb feladat volt az MTA tagintézményeiben bevezetésre kerülő bérszámfejtési rendszer kapcsán felmerült korszerűsítés, mely során kb. 45 tagintézményben került sor router cserére. Itt Cisco 805 és 1751-es routereket telepítettünk.
Ezután az IKB által kiírt pályázaton nyertes iskolák, könyvtárak ill. múzeumok, közgyűjtemények végponti eszközeinek korszerűsítése következett. Ennek keretében kb. 250 intézményben jártunk. Itt már vegyes volt a kép a tekintetben, hogy milyen eszköz került a végpontra. Bérelt vonal esetében a már jól bevált Cisco 805 és 1751 típusú routereket alkalmaztuk, ISDN ill. dial-up esetében modemeket használtunk.
Ezzel párhuzamosan, mivel az ADSL technológia már egyre több területen elérhetővé vált, az újonnan kapcsolódó intézmények ill. a már meglévő bérelt vonali kapcsolatok kiváltása esetében ADSL kapcsolatok kerültek kiépítésre. Itt kb. 150 helyszínre szállítottunk ki Cisco 806-os routereket.
A negyedik nagyobb feladat volt a Fővárosi Szabó Ervin Könyvtár fiókjainak bekötése. Itt bérelt vonal és ADSL kapcsolatok kerültek kiépítésre. Itt kb. 35 Cisco 805, 806 és 1720-as routert telepítettünk.
Előadásomban a 3 év alatt szerzett tapasztalatainkat ill. keserédes pillanataikat szeretném felvázolni, valamint a jövőben tervezett telepítésekről és ADSL bekötésekről szeretnék beszélni.

Központi felhasználó kezelés egyetemi környezetben

Mogyorósi János <janos.mogyorosi@bkae.hu>
Budapesti Közgazdaságtudományi és Államigazgatási

Adatbiztonsági alapelvek

- Nincs azonosítatlan felhasználó, nincs tisztázatlan felelőssel működő PC
- Publikus és védett szolgáltatások szétválasztása – Security Policy
- Szolgáltatás menedzsment automatizálása

Üzemeltetési szempontok

- Nagytömegű automatikus felhasználó kezelés
- Felhasználóknak biztosított saját Webes menedzsment felület
- Többszintű ügyfélszolgálati rendszer

Központi szolgáltatások

- Automatikus címlista szolgáltatás, Közös - Átmeneti / Saját Háttértár
- Windows rooming Profil, Terminal Szerver Profil, Group Policy
- Email, Dinamikus Levelező listák, Telnet / FTP / Saját WEB
- Betárcsázás

Rendszer architektúra, műszaki megoldások

- Automatikus Neptun XML interface
- Java / Web felhasználói felület
- Központi Oracle adatbázis
- Többszintű Applikációs szerver, Messages Broker
- LDAP, Active Directory, TACACS autentikációs adatbázisok

Tapasztalatok

Fejlesztés további irányai

Elektronikus információs és nyilvántartási rendszer a Doktori Iskolák fiatal kutatói részére

Adamkó Attila <adamkoa@inf.unideb.hu>
Debreceni Egyetem

A tudományos életben mindig fontos szerepet töltenek be a pályájukat még csak most kezdő, de érdeklődő és új ötletekkel rendelkező fiatal kutatók.

A képzésüket, a kutatásaikat a Doktori Iskolák és a témavezető(i)k segítik, támogatják. Ugyanakkor viszonylag kevés információval rendelkezünk arról, hogy az egyes Doktori Iskolákban milyen tudományos munka folyik, a doktoranduszok milyen kutatási területeken tevékenykednek.

Az általunk kifejlesztett és jelenleg még fejlesztés alatt álló információs rendszer fő célja, hogy ezeket az "alapvető" adatokat az Interneten keresztül elérhetővé tegye a szélesebb nyilvánosság számára is.

A rendszer leglényegesebb eleme egy olyan internetes eszközökkel kezelhető adatbázis, amely összegyűjti és tartalmazza a Doktori Iskolákhoz kapcsolódó adatokat, híreket mind helyi, mind országos szinten (DOSZ, www.phd.hu, OM, pályázati lehetőségek), továbbá lehetőséget nyújt arra,

hogy hozzáférjünk a tudományos dokumentumokhoz (cikkekhez, publikációkhoz).

Az előadásban ennek az elektronikus nyilvántartási és információs rendszernek a bemutatása mellett kitérünk a fejlesztés közben alkalmazott modellek, technológiák, programok (szerver - kliens, session management, webes kezelőfelület, XHTML, XML, SQL, perl, DBI, PostgreSQL, Apache) ismertetésére, valamint együttműködésük és a központi fejlesztésű NEPTUN rendszerrel való kapcsolatuk felvázolására is.

Vastag kliensek menedzsmentje Tivoli környezetben

Orosz Péter <oroszp@delfin.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

A Debreceni Egyetem informatikai központjában működő homogén géppark csatlakoztatása az országos cluster GRID projekthez a kivitelezés fázisába került. Az egyetem több campusán elhelyezkedő 160 azonos hardver és szoftver konfigurációjú munkaállomásból a DISZK épületében üzemelő hallgatói gépterembe 40 darab került, amely jó lehetőséget biztosítnak az üzemelés hatékony megszervezésére. Kettős funkciót ellátva nappal, nyitvatartási időben a munkaállomások a hallgatókat szolgálják ki, míg az éjszakai üzemmódban az országos GRID hálózathoz csatlakoznak a gépek. A nappali üzem menedzselését a rendszergazdák gyakran csak a helyszínen tudták elvégezni, ami a kapusok között időigényes utazás miatt csak nehézkesen biztosítható. Szükségessé vált a kliensek nappali üzemmódjának központosított menedzselése. Vékony kliensek felügyelete számára számos programcsalád kapható a piacon, amelyek teljesen más algoritmus alapján teszik lehetővé úgy a géphasználatot, mint a felügyeletet.

Feltevődik a kérdés, amely az üzemeltetési munka során komoly változásokat jelenthet: vastag kliensek esetén léteznek-e olyan komplex szoftvercsomagok, amelyek lehetővé teszik a centralizált menedzsmentet? A válasz: igen. Erre a célra számos szoftvercég (HP, Enterasys, IBM, SUN) kínál megoldásokat. A DISZK ezek közül az IBM Tivoli termékcsaláddal került kapcsolatba. Jelenleg a programcsomag tesztelésében a DISZK épületében működő gépterem munkaállomásai vesznek részt. A kisérletezés során a szoftvercsomag alábbi moduljai kerültek installálásra: Tivoli Infrastructure (framework), Remote Control, Configuration Manager. Ezek használatával többek között a szoftverek disztribúciója, illetve a vállalat szintű hardver és szoftver leltárak elkészítése nagymértékben automatizálható. SQL alapú háttéradatbázis segíti a rendszeren belüli folyamatok követését, nyilvántartását. Ezen túlmenően a rendszer távoli segítségnyújtást biztosít, használatával a rendszergazdák elkerülhetik az utazást igénylő helyszíni problémamegoldást.

Az előadás a tesztüzem alatt szerzett tapasztalatokat ismerteti, részletesen kitérve az egyes Tivoli modulok lehetőségeire, technikai megoldásaira, működésükre heterogén szoftverkör-nyezetben. A bemutatásra kerülő tapasztalatok segítséget nyújtanak más intézmények számára is a rendszer-menedzsment hatékonyságának növelésében.

A Neptun rendszer erőforrás használatának elemzése

Faragó Zsuzsa <zsuzsa@delfin.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

A 14 kar illetve kar szintű intézményből álló Debreceni Egyetemen szükségessé vált egy korszerű

hallgatói nyilvántartó és információs rendszer bevezetése. Több más felsőfokú oktatási intézményhez hasonlóan egyetemünk is a Neptun Egységes Felsőoktatási Tanulmányi Rendszer bevezetése mellett foglalt állást. Az Informatikai Szolgáltató Központra hárult az a feladat, hogy az alkalmazás működésének hardver és operációs rendszer szintű feltételeit biztosítsa, és kidolgozza az üzemeltetési környezet informatikai elemeit. A Windows 2000 szerver platformmal rendelkező négy darab terminál- és egy darab adatbázis szerver Oracle Kliens és MS Sql Server modulokat futtat.

A rendszer felhasználásából adódó időben inhomogén, de trenddel rendelkező terhelés az üzemeltetésért felelős rendszergazdák számára egy, a folyamattal párhuzamos, intenzív odafigyelést feltételez. Mivel intézményünknél a Neptunt 26.000 hallagató és 3.500 oktató nap mint nap használja, a rendszer a telefonhoz hasonlóan nagyon nagy megbízhatósági színvonallal és rendelkezésre állási jellemzővel kell rendelkezzen. Emiatt a DISZK a többi kritikus alkalmazáshoz hasonlóan folyamatosan figyeli és elemzi a saját Neptun rendszerének előforrás használatát. Ehhez tartozik nemcsak a szerverek CPU és hálózati interfészének folyamatos monitorozása, hanem a védelmi funkciót ellátó Neptun tűzfal elemei által érzékelt támadási típusok és azok gyakoriságának nyomon követése, valamint a gerinchálózati eszközök segítségével történő forgalommérések is. Az SNMP protokoll segítségével lekérdezett MIB változókat MRTG programmal rendszerezzük és ábrázoljuk. A begyűjtött állapotinformációk idősorait statisztikai eszközökkel dolgozzuk fel, amiből az erőforrások időszakos terhelésére vonatkozóan intelligens következtetéseket vonunk le.

Az előadás a kiépített szerverfarm és a hálózati elemek erőforrásainak használatát részletezi, amely alapján a szükséges fejlesztési lépések és azok időszerűsége, valamint az üzemeletetési technikák bevezetése prognosztizálhatóvá válik. Az elemzés során felgyült gyakorlati tapasztalatot megosztjuk másokkal is, így a hasonló alkalmazást üzemeletető egyetemek, főiskolák számára a saját Neptun rendszerük napi üzemeltetési munkájának optimalizálása egyszerűbbé tehető.

Nagy egyesített azonosító rendszer - bevezetés és az első tapasztalatok

Ecsedi Kornél <ecsedi@unideb.hu>
Debreceni Egyetem

Jelen munka az elmúlt évi Networkshop konferencián elhangzott "Neptun - LDAP - PAM" címû elõadás folytatása. A kiinduló probléma lényegében az volt, hogy a központi szervereken hogyan lehetne minél egyszerûbben rendet teremteni a felhasználói (leginkább hallgatói) azonosítók között. A feladat nem lebecsülendõ, lévén szó tízezres nagyságrendû felhasználó számról. Az alapötlet szerint össze kell valahogy kapcsolni a login neveket a hallgatói nyilvántartással (esetünkben a Neptunnal), és meg kell találni a módját, hogy a felhasználók a lehetõ legegyszerûbben, mindenféle papírmunka nélkül jussanak hozzá azonosítóikhoz. A nyilvántartások összekapcsolását egy OpenLDAP alapú adatbázissal terveztük megoldani, a felhasználói felületet pedig egy PHP-ban írt webes felülettel kívántuk biztosítani. Mára mindez megvalósult, s bár van még mit csiszolni a rendszeren, úgy tûnik, hogy mûködõképes a dolog. Az LDAP azonosítóknak ráadásul az a kellemes tulajdonsága is megvan, hogy sok rendszeren közvetlenül login névként is használhatók, azaz nem kell a helyi gépen létrehozni semmit, hogy biztosítsuk a bejelentkezést: elegendõ a kapcsolat az LDAP szerverrel. Az elõadás a megvalósítás részleteirõl ad képet, valamint a kezdeti tapasztalatokról fog beszámolni.

Koncepció és informatikai fejlesztés a KFRTKF-n

Cserhátiné Vecsei Ildikó dr. <vecsei@kfrtkf.hu>
Kölcsey Ferenc Református Tanítóképző Főiskola

Egy felsőoktatási intézmény életében mindig fontos szerepet játszik a rövid és hosszú távú koncepciók kidolgozása és elfogadtatása, no meg a végrehajtása. Külön érdemes odafigyelni arra, hogy az informatikai fejlesztések terén miként alakul ez.

Azokról a lényeges elemekről szeretnék előadásomban szólni, ami az elképzelések sarkalatos pontjait érinti. Ilyenek pl.: a belső hálózat bővítése, szerverek funkciói, szolgáltatások reformja, számítógépes kultúra terjesztése, új információs központ kialakítása, digitális tananyag fejlesztésének tárgyi és személyi feltételeinek megteremtése, korszerűsítések, szoftverek legalizációja, stb.

A felsoroltakból is látszik, hogy ez nem egy tanszékhez kapcsolódó munkafolyamat, hanem közös tervek, ötletek összegyúrását jelenti intézményi vezetői jóváhagyással és a megfelelő pénzügyi források felkutatásával együtt.

KÖNYVTÁRAK, LEVÉLTÁRAK, MÚZEUMOK, TARTALOMSZOLGÁLTATÓK

Kép vagy térkép

Plihal Katalin <kplihal@oszk.hu>
Országos Széchenyi Könyvtár

Az interneten elérhető térképek, főleg a régiek, a felhasználó számára csak képek. Mit kell ez alatt érteni?
- A térkép méretarányát a felhasználó a saját képernyőjén meghatározni nem tudja.
- A térképhez tartozó mutatókat közvetlenül használni nem tudja.
- A térképlapok nagy mérete miatt a felhasználó csak részeket tud abból egyszerre megtekinteni.

Miért alakult ez így? Minden területen megnőtt az online publikációk iránti igény. A fenti igény kielégítése legkönnyebben szkennelt térképekkel lehetséges, így valójában raszteres térképek uralják a hálózatot. E térképek csak böngészésre alkalmasak. A hagyományos böngészők alapértelmezésként csak néhány képformátum megjelenését támogatják (GIF, JPG, PNG). Ha azonban nemcsak böngészni szeretnénk a régi térképeket, hanem akár intaraktívan is hozzáférni kívánnánk tartalmukhoz, akkor az komoly költséget jelentene e térképek szolgáltatói számára. Ezért azt gondoljuk, hogy képszerű térképek a világhálón még hosszú ideig megtalálhatók lesznek.

Az országos régi könyves adatbázis fejlesztési problémái

Hegyi Ádám <hegyi@mek.oszk.hu>
OSZK - SZTE BTK Könyvtártudományi Tanszék

2003. szeptemberében kezdődött el az OSZK-ban az országos régi könyv adatbázis tervezése. Mostani előadásomban az azóta elért eredményekről szeretnék beszámolni.

Első lépésben egy országos felmérés alapján szereztünk pontos információkat arról, hogy a különböző gyűjteményekben hogyan építhető ki egy központi számítógépes adatszolgáltatásban való részvétel. Ez alapján sikerült képet kanunk arról, hogy ma Magyarországon milyen könyvtári feltárások készültek 1850 előtt nyomtatott könyvekről, illetve hogyan használják fel a számítógép adta lehetőségeket ezekhez a könyvtári munkafolyamatokhoz (pl.: MARC-ban való címleírás, digitális archiválás, stb.)

Ezzel párhuzamosan elkészült egy technikai terv. Így a technikai célok és a felmérés ismeretében készül el hamarosan a teljes projekt megvalósíthatósági terve.

Jelenleg tesztelés céljából az adatbázis építésében a következő könyvtárak vesznek részt:

Debreceni Egyetem. Egyetemi és Nemzeti Könyvtár
ELTE Egyetemi Könyvtár
Dunamelléki Református Egyházkerület Ráday Gyűjteménye. Könyvtár
Országos Széchényi Könyvtár
Szegedi Tudományegyetem Egyetemi Könyvtár

Ez az adatbázis XML-ben tárolja az egyes rekordokat. Ehhez tarozik egy keresőfelület,

amely interneten keresztül érhető el, valamint egy szerkesztő felület. A szerkesztő felületen lehet az egyes rekordokat felvinni és javítani. Ehhez szintén interneten keresztül lehet hozzáférni.

Egyelőre még nincs kidolgozva az, hogy az egyes tagkönyvtárak hogyan adják át a számítógépes állományaikat a közös katalógus számára. Ezt az után szeretnénk eldönteni, miután a tesztelés lezárult.
Az adatbázis ténylegesen akkortól fog működni, amikor egy kész megvalósíthatósági tanulmányra alapozva elindul a részt vevő gyűjtemények közötti együttműködés létrehozása.

A Magyar Elektronikus Könyvtár metaadat- szolgáltatása, az adatbázis kereshetővé tételének kérdései egy integrált könyvtári rendszer, a KisTéka webes felületének alkalmazása kapcsán

Simon András <simon@lib.bkae.hu>
BKÁE EKK

Góczán Andrea <goczan@oszk.hu>
OSZK MEK osztály

A 2004-ben fennállásának 10. évfordulóját ünneplő Magyar Elektronikus Könyvtár (MEK), közel két éves fejlesztőmunka után 2003. július elsején nyitotta meg új szolgáltatását, a MEK2.1-t. A mind tartalmában, mind külsejében "megszépült", szolgáltatásaiban kibővült könyvtár megújulását az az elvárás sürgette, melyet Internetes körökben "nyíltság"-nak és "összekapcsolhatóság"-nak hívnak, azaz: a MEK legyen nyitott más tartalomszolgáltatások felé, legyen alkalmas arra, hogy metaadatai más könyvtári adatbázisokba integrálhatóak
legyenek. Ennek alapja egy olyan bibliográfiai adatstruktúra és adatbázis kialakítása volt, amely kompatibilis egyrészt a könyvtári címleíró szabványokkal (MARC), másrészt az Interneten használatos szabványokkal (pl. Dublin Core). Előadásomban ismertetem a MEK bibliográfiai adatstruktúrájának kialakítását; a különböző szabványokkal való megfeleltetés problémáit, a továbbiakban pedig példákkal illusztrálom az integrálás lehetséges változatait, és konkrét megvalósulásait a MEK-ben.
Az integrációra példa a Kistéka könyvtári rendszer alkalmazása a MEK adatállományának keresésére. A Kistéka web alapú könyvtári rendszer kereső felülete is alkalmazkodik a ma már a világhálón megszokott feltételekhez és elvárásokhoz. A kisméretű könyvtárak, melyek számára a Kistéka készült, különösen nagy hasznát látják a Magyar Elektronikus Könyvtár gyűjteményének, ezért különösen fontos számukra, hogy ezt az állományt saját keresőfelületükről közvetlenül is elérhessék. A Kistéka messzemenően alkalmas a MEK adatainak szolgáltatására. MARC alapú rendszer lévén könnyen fogadja a MEK adatait, és a katalógusban megtalált tételek teljes szövegéhez is azonnal átléphet az olvasó a Kistéka keresőfelületéről. A Kistéka nem helyhez kötött rendszer, a forgalmazó központjában, a SZTAKI egyik szerverén karbantartott Kistéka MEK adatbázist minden érintett könyvtár azonnal, naprakészen érheti el, akár országhatárokon túlról is.

Elosztott könyvtári rendszerek megvalósítása a Z39.50 és az OAI protokoll használatával

Tóth Kornél <tothk@sztaki.hu>
MTA SZTAKI

Elöljáróban vázlatosan áttekintjük a könyvtárgépesítés főbb állomásait, különös tekintettel a könyvtári hálózatok kialakulására. Ezután rátérünk a hazai közös katalógusok ismertetésére és a Z39.50 protokoll

rövid bemutatására, amely a közös katalógusok technológiai hátterét biztosítja. A Z39.50 alkalmazásának két konkrét esetét is bemutatjuk az MTA SZTAKI által fejlesztett és forgalmazott *HunTéka* és *KisTéka* könyvtári rendszereken. Amint az a címből is látható, az előadás időbeli folyamatot szeretne megragadni, ezért a továbbiakban a közeli és távolabbi lehetőségeket tekintjük át: hogyan lehetne a könyvtári rendszerek online katalógusait még magasabb szinten integrálni. Az integráció lehetséges szintjei: könyvtári rendszerek együttműködése; könyvtári rendszerek együttműködése más közgyűjteményi -- levéltári, múzeumi -- rendszerekkel; közgyűjteményi rendszerek együttműködése az Interneten más, nem közgyűjteményi információs rendszerekkel. A jövőbeli magasabb szintű és szélesebb körű integráció elérésének egyik lehetséges -- véleményünk szerint legjobb -- útja az OAI (Open Archives Initiative) és a DC (Dublin Core) protokoll bevezetése a közgyűjteményi rendszerekbe. Ennek megvalósítása érdekében jelenleg az MTA SZTAKI is komoly erőfeszítéseket tesz részben azzal, hogy OAI alapú szolgáltatást nyújtó szervert helyez üzembe, másrészt azáltal, hogy az általa forgalmazott könyvtári rendszereket felkészíti az ehhez való kapcsolódásra.

Szabad forráskódú preprint archivum XML alapon, magyar nyelven

Csirmaz László <csirmaz@ceu.hu>
Közép Európai Egyetem

Egyetemeken, főiskolákon és egyéb felsőoktatási intézményekben egyre fontosabb feladat az oktatók és hallgatók kéziratainak -- preprintek, szakdolgozatok, diplomamunkák -- megfelelő archiválása és naprakész publikációs listák készítése. Erre a célra több elektronikus archiváló rendszer létezik. A gazdag választékból egyetemünk az angliában fejlesztett, GNU licensz alapú szabad forráskódú EPRINTS szoftvert választotta. Az előadásban az EPRINTS felépítését, filozófiáját, használati módját szeretném ismertetni. Mivel az archiválás, a tudományos publikációk közkinccsé tétele minden intézmény mindennapi gondjai közé tartozik, szeretném felhívni a figyelmet egy -- véleményem szerint -- kiváló eszközre, mely sokat segíthet a megoldásban. Az EPRINTS-et világszerte több mint száz intézmény használja, köztük a Kalifoniai Műszaki Egyetem (CalTech), a Carnegie Mellon számos tanszéke, a Weitzman Intézet is; az angliai egyetemek könyvtárainak szövetsége által javasolt szoftver. Az EPRINTS egy úgynevezett ön-archiváló rendszer, melyben a szerzők saját maguk töltik fel a dokumentumokat, és adják meg a dokumentuhoz tartozó bibliográfiai adatokat. EPRINTS támogatja a Nyílt Archivum Kezdeményezést (OAI, Open Archive Initiative), melynek keretében az archivumban elhelyezett dokumentumok könnyen és gyorsan bekerülhetnek a tudományos élet vérkeringésébe; a dokumentumok kulcsszavak, témakör, kivonat alapján kereshetők. Ugyanakkor lehetőség van arra, hogy a teljes dokumentum csak korlátozottan legyen elérhető; ezzel a rendszer elébe megy néhány kiadó gyakorlatának, mely copyright-ra hivatkozva megtiltja a szerzőnek hogy a művét teljes terjedelmében interneten hozzáférhetővé tegye. Az EPRINTS minden funkciója -- a kezdeti konfigurálástól eltekintve --web-es felületen érhető el. Külön érdekessége, hogy a megjelenítés nyelve választható; így ugyanaz a tartalom akár magyar, akár angol, olasz, vagy német nyelvű lapon is megtekinthető. Más tekintetben is rugalmas; könnyen és jól alakítható a speciális helyi igényekhez, mind külalakban, mind tartalomban. A rendszer a felhasználók több csoportját különbözteti meg. Az archivum nyilvános része bárki által elérhető és kereshető. Az előfizetők rendszeres időközönként elektronikus levelet kapnak amennyiben az archivum általuk megszabott feltételnek elget tevő dokumentummal gyarapodik. Szerzők gyarapíthatják az archivum anyagát; az általuk felvitt anyag végül a szerkesztők jóváhagyása után lesz mások számára is hozzáférhető. Előfizető bárki lehet; a szerzői jogot az előfizetők e-mail címük alapján automatikusan kapják meg. A szerkesztők jogait az archivum adminisztrátora állítja be. A különleges joggal bírók az általuk választott felhasználói névvel és jelszóval azonosítják magukat. Egy új dokumentum felvitele a típus megadásával kezdődik: ez lehet könyv, könyv fejezet, gyűjtemény, konferencia előadás, tudományos cikk, újságcikk, kézirat, diplomamunka, stb. A típustól függően kell további bibliográfiai adatokat megadni; könyv esetén a szerzőt, kiadót, kiadás évét; fejezet esetén a tartalmazó könyv adatait, stb. Ezután kerül sor magának a dokumentumak a felvitelére. Ez tipikusan WORD, PDF, postscipt, HTML vagy egyszerű szöveges formátumú; ugyanazt a dokumentumot

egyszerre több formátumban is fel lehet vinni. Utolsó lépésként a szerzõ felhatalmazza a rendszert, hogy a teljes anyagot a megfelelõ szerkesztõ jóváhagyása után közkinccsé tegye. Az EPRINTS különbözõ XML állományok és perl rutinok segítségével konfigurálható. A használható dokumentum típusok, az azokhoz tartozó bibiográfiai adatok, kötelezõen kitöltendõ mezõk; felhasználói csoportok, jogosultságok mind itt definiálandók. Például a könyvfejezet definíciójának egy részlete:

```
<metadatatypes>
 <dataset name="eprint">
  ....
  <type name="bookchapter">
   <field name="authors" required="yes" />
   <field name="title"  required="yes" />
   <field name="ispublished" required="yes" />
   ....
  </type>
 </dataset>
</metadatatypes>
```

Az egyes dokumentumtípusok megjelenítése (mely mezõket milyen formátumban, milyen magyarázó szöveggel) minden támogatott nyelven külön megadható és finoman hangolható. A könyvfejezet megjelenítése angolul:

```
<ep:citation type="eprint_bookchapter">
  <b>@authors@</b>:
  <i>@title</i>, in
  <ep:ifset name="editors">@editors@ (Eds.)</ep:ifset>
  <ep:ifset name="chapter">, chapter @chapter@</ep:ifset>
</ep:citation>
```

Míg ugyanez magyarul például így néz ki:

```
<ep:citation type="eprint_bookchapter">
  <b>@authors@</b>:
  <i>@title</i>,
  <ep:ifset name="editors">Szerkeszti @editors@</ep:ifset>
  <ep:ifset name="chapter">, @chapter@ fejezet</ep:ifset>
</ep:citation>
```

A természettudományokban (fõleg a matematikában) szokás a kivonatban (absztrakt) TeX formulákat használni, EPRINTS ezt is támogatja: az elõforduló formulákatat helyettesítõ képeket automatikusan generálja. Az EPRINTS legfrissebb verziója ezen kívül támogatja a teljes szövegre való keresést is.

Az EPRINTS üzemeltetéséhez egy web kiszolgáló, perl interpreter, és a MySQL adatbázis kezelõ rendszer szükséges. A kezdeti beállítások után annyi felügyeletet igényel, mint egy átlagos web kiszolgáló.

Digitális tartalom bővítés és távmunka bevezetése a Veszprémi Egyetemi Könyvtárban

Vizi Szilárd <vizisz@freemail.hu>
Veszprémi Egyetemi Könyvtár

Egyházy Tiborné, dr <hazitibo@almos.vein.hu>
Veszprémi Egyetemi Könyvtár

Tóth Gábor <tothgab@almos.vein.hu>
Veszprémi Egyetemi Könyvtár

Az utóbbi években az informatikai technológia robbanásszerű fejlődésének lehettünk tanúi. Az elektronikus hálózatok lehetővé teszik a hagyományos ismeretszerzési módszerek átültetését az Internetre, amely gyors hozzáférést, szelektív válogatást tesz lehetővé. A mai világban az információnak vitathatatlanul kulcsszerepe van. Nélkülözhetetlen a tudományos kutatásban, a fejlesztési munkában, a mindennapi élet számos területén. Az egyén állandóan szembekerül a folyamatosan gyarapodó információk tömegével, amelyek különböző úton jutnak el hozzá: nyomtatott, online, CD-ROM formában és az Interneten és tömegkommunikációs eszközökön keresztül.

A hazai könyvtáraknak a hagyományos, eddig ismert szolgáltatásaikon túl központi szerepet kell vállalniuk az ilyen elektronikus információk továbbításában, közreadásában. Éppen ezért egyre nagyobb jelentőséggel bír az, hogy a könyvtárak egymás állományait, információ és dokumentum szolgáltatók szolgáltatásait hálózaton elérjék és olvasóik számára rendelkezésre bocsássák.

A VESZPRÉMI EGYETEM KÖZPONTI KÖNYVTÁRa egyik fő feladatának tekinti azt, hogy az egyetem hallgatóinak, oktatóinak, kutatóinak a hálózaton elérhető információk sokaságában kielégítő eligazodást tudjon nyújtani. Az egyetem könyvtára a kor kihívásaihoz igazodva bővítette szolgáltatásait az alábbi területeken:

- digitális tananyagok, jegyzetek, kiadványok online szolgáltatása,
- elektronikus adatbázisok elérésének megkönnyítése SFX és MetaLib rendszerek alkalmazásával,
- távmunka bevezetése a könyvtári feldolgozásban.

Könyvtárunkban az olvasók ezentúl egyes kiadványokat, jegyzeteket elektronikus formátumban is elérhetik, ezzel az olvasó még a kölcsönzés előtt beletekinthet a műbe, szabadon kereshet benne és eldöntheti, hogy tényleg erre a műre van-e szüksége akár könyv, akár nyomtatott vagy elektronikus formátumban. Az elektronikus változatokban a szabad keresés eshetősége, és az a lehetőség, hogy igény szerint – „on-demand" – dönthetünk arról, hogy a könyvet vagy csak annak egyes oldalait, fejezeteit milyen formátumban szeretnénk megszerezni a könyvtári szolgáltatások új színvonalát jelenti.

A szakirodalom kiszolgálására számos, elszórtan elhelyezkedő adatbázis található. Ezen adatbázisok elérhetőségének, az általuk szolgáltatott témakörök megjegyzése, illetve kezelésének elsajátítása az átlagos érdeklődőt hamar eltántorítja az irodalom felkutatásában. A felhasználók részére olyan fejlett programrendszereket (SFX és MetaLib) vezettünk be, amelyek a végfelhasználókat olyan eszközökkel (kereső programokkal) látja el, amelyek rendezett módon és egységes – kereső – felületen képesek több adatbázisban párhuzamosan keresni és a találatokat megjeleníteni, ezáltal megkönnyítve a teljes tartalom felkutatását.

A távmunka – telework, distance work – bevezetésével a könyvtári feldolgozás tervezhetőbbé, gyorsabbá válik, az internet segítségével bárhonnan be lehet segíteni a feldolgozásba egy egységes felületen keresztül.

HUNMARC rekordok előállításának nehézségei "hagyományos" rendszerekből

Lengyel Mónika <lmoni@sztaki.hu>
MTA SZTAKI

A könyvtári együttműködések (MOKKA) és az elavult könyvtári rendszerek cseréjének egyik sarkalatos pontja a rekordok lehető legteljesebb, veszteségmentes áttöltése. A napjainkban kifejlesztett könyvtári rendszerek egyik lényeges ismérve a bibliográfiai adatok MARC struktúrájú feldolgozásának követelménye, együttműködésekben való részvétel feltétele pedig a (HUN)MARC formátumú rekordcsere (export / import) képessége.

A (HUN)MARC szerkezet leképezése többnyire a hagyományos, MARC rekordstruktúrát nélkülöző rendszerek számára sem okoz gondot. A probléma inkább az ezekben foglalt adattartalom mennyiségi és minőségi vonatkozásaiban keresendő. A kérdés legtöbbször az:

- Lehet-e, s ha igen, miből a „hiányzó" kötelező adatokat előállítani;
- Hogyan lehet a bevitelből eredő helytelen eltéréseket egységesíteni;
- Felül lehet-e kerekedni a használt rendszer korlátoltságából eredő kényszer megoldásokon (eddig összezárt adatok szétválogatása, „rossz" helyre bevitt adatok felismerése és átirányítása);
- Besorolási rekordok léte esetén megoldható- e minden esetben a bibliográfiai rekordokhoz történő egyértelmű kapcsolódás.

A rekordokban keletkező tartalmi hibák gyorsabb felderítésének egyik eszköze lehet a TINLIB –HUNTÉKA konverziók során alkalmazott HUNMARC struktúrájú XML formátum bevezetése.

A felmerülő nehézségek illusztrációját elsősorban a TINLIB-HUNTÉKA konverziók során, illetve a MOKKÁ-hoz csatlakozó TINLIB-es könyvtárak exportjánál előfordult problémák szolgáltatták, de ezek természetesen más rendszerekből származó (ISIS, TEXTÁR, SZIRÉN, SRLIB, DRLIB) (HUN)MARC rekordokra is általánosíthatóak.

Tartalomalapú képkinyerés képarchívumokból – egy lehetséges megoldás

Veréb Krisztián <sparrow@inf.unideb.hu>
Debreceni Egyetem, Informatikai Intézet

Egyik ismerősöm mutatott egy számot nekem, amely nagyon megtetszett. Láttam, ahogy fogja a CD-t, kiveszi a tokjából, majd beteszi a meghajtóba. Nem igazán figyeltem, mit mondott, ki volt az előadó, a dallamot jegyeztem meg csak, és a borító külsejét. Nos ezek után, pár héttel később pont egy CD-boltban jártam, és eszembe ötlött, meg kellene a CD-t venni. Na igen, de az eladóknak nem tudtam semmilyen lényeges információval szolgálni az előadót vagy albumcímet illetően. Mindössze a zenei stílust tudtam behatárolni, és a borítót ismertem volna fel, ha látom. El is kezdtem keresni, de lehetetlen feladatnak tűnt a több ezer CD átnézése. Ha akkor, egy olyan adatbázissal rendelkeztem volna, amely képes a CD-borítók valamilyen módon történő felvázolása után esetleg némi szöveges segítséggel elnavigálni a keresett CD előadójához, akkor perceken belül végezhettem volna, és nem kellett volna órákon át bolyonganom a CD-borítókkal megtöltött polcok közötti végeláthatatlan folyosókon.

A fenti problémát megoldó képarchívumhoz, és a belőle képeket kinyerő visszakereső algoritmusokhoz szükséges alapok és megközelítési módok az NWS 2003 keretében Pécsett tartott *Tartalomalapú képkinyerés képarchívumokból – van ilyen?* című előadásomban már bemutatásra kerültek. Ez az előadás, mintegy annak folytatásaként, az ott megismert technikákat próbálja bemutatni egy létező, leimplementált zenei CD-k borítóit és egyéb járulékos információit tartalmazó összetett archívumon keresztül.

Az adatbázis lehetővé teszi a CD-k közötti szöveges kereséseket, illetve a képek alapján történő kereséseket. (Ehhez az Oracle9*i* *inter*Media lehetőségeit használja fel.) Egy sajátfejlesztésű

technika segítségével pedig lehetővé teszi, hogy részképeken alapuló bonyolult kérdéseket is feltehessünk. Egy előre elvégzett hierarchikus osztályozásnak köszönhetően, mely a borítók által ábrázolt motívumokat osztályozza, a szemantikus indexelés nagyságrendekkel felgyorsítja a keresést az elvégzendő illesztések számának csökkentésével. Az így kapott „keresőmotor" tehát nem más, mint a már korábban említett előadásomban bemutatott technikák működő változatainak egy adott cél érdekében összeszerelt egysége.

Az előadásban a rendszer technikai paramétereinek és működésének bemutatásán túl számos példát hozok a rendszer képességeinek bemutatására, és összehasonlítom azt más létező, rendszerekkel is.

A WebKat.hu a magyar internetkatalógus és tématérképe

Ignéczi Lilla <lilla@neumann-haz.hu>
Neumann Kht.

Boros Andrea <andreab@neumann-haz.hu>
Neumann Kht.

Nagyon megtisztelõ számunkra, hogy a 2004-es év Networkshop elõadásai között bemutathatjuk a Neumann János Digitális Könyvtár és Multimédia Központ (Neumann-ház) legrégibb szolgáltatását, a www.webkat.hu címen elérhetõ internetes katalógust.
Ebben a katalógusban a magyar internetforrásokat gyûjtjük össze. Ez egy teljes szövegû adatbázis, melyben a dokumentumok szinte minden válfaja megtalálható: képek, dolgozatok, tanulmányok, folyóiratok, hanganyagok, e-könyvek, fotók, festmények, grafikák stb.

A WebKat.hu 1998 óta épül, a munkát könyvtárosok végzik, az internetforrások erõs szûrõn mennek keresztül, a meglévõ anyagokat pedig analítikusan feltárjuk.

Sokakban felmerül, még a szakmában is, hogy kell-e, lehet-e, érdemes-e egyáltalán katalogizálni az internetet... Hangokat hallani, amelyek azt kérdezik, minek kifinomult, elsõ látásra bonyolultnak tûnõ rendszereket alkalmazni, amikor a mind népszerûbb és egyszerûen

használható keresõmotorok, sokkal nagyobb anyagot és gyorsabban dolgoznak fel, a felhasználó pedig, nagyságrendekkel nagyobb találatok özönében bóklászhat.

Nem feladatunk, hogy ezen a fórumon válaszoljunk erre a kérdésre, de talán nem lesz haszon nélkül való, ha elmondjuk az elmúlt hat esztendõ tapasztalatait, amelyet a magyar internet feltérképezése közben szereztünk.

A tezaurusztól a tématérképig - a WebKat.hu tématérképe

A magyar internetkatalógushoz 1999-ben egy tezaurusz létrehozását tartottuk ideálisnak. 2000 októberében a létrehozott, tezauruszokhoz hasonló, ETO-alapú tartalmi feltárásra képes rendszerrel megkezdõdött a feldolgozás. 2002 tavaszán koncepcióváltásra volt szükség: míg 1999-ben egy tezaurusz létrehozása volt a cél, addig a feldolgozás során szerzett tapasztalatok és az OLIB tezauruszkezelõ és -szerkesztõ moduljának korlátai miatt megkérdõjelezõdött - tezaurusz-e az a rendszer, melyben minimális reláció létrehozásra és tükrözésére van csak mód. A teljes felülvizsgálat eredményeként tartalmi feltöltésre és strukturális átrendezésre került sor - ezzel kiemeltük a 9 legfelsõbb szintû kategóriát.
Ez a munka alapja és egyben elõkészítése volt a 2003-as fejlesztésünknek, melyet a nemzetközi tendenciák és a felhasználói igények sürgettek: a tárgyszó-rendszerünkbõl létrehoztunk egy

vizuálisan jól áttekinthetõ, bejárható tématérképet. A fejlesztést alternatív lehetõségként ajánljuk honlapunkon a felhasználóknak, mellette megtartottuk a témák szerinti keresés lehetõségét is.

10 éves a Magyar Elektronikus Könyvtár
Múlt, jelen, jövő

Moldován István <moldovan@oszk.hu>
Országos Széchényi Könyvtár

1994-ben indult meg az Információs Infrastruktúra Fejlesztési Program támogatásával a Magyar Elektronikus Könyvtár, amely mára a hazai Internet egyik legnagyobb elektronikus szövegarchívumává, legnépszerűbb szolgáltatássá nőtte ki magát. Az előadás egy rövid vázlatos áttekintést ad a MEK kezdeteitől, az 1994-es Gopher időktől a MEK 2.0 beindulásán át a tervezett jövőig. Az előadás főbb területei:

- *Gyarapodás*: önkéntes szövegrögzítés, digitalizálási programok, UNESCO irányelv;
- *Metaadatok*: az ASCII MEK fejléctől a MARC-ig és a Dublin Core-ig.
- *Elektronikus formátumok*: az ékezet nélküli ASCII szövegektől az XML-ig és a UNICODE-ig és az e-book-ig;
- *Digitális könyvtár*: a Gopher-től és az anonymous FTP-től a Z39.50-ig és az OAI szabványig. MEK tükörszerverek;
- *Elektronikus dokumentumok:* könyvek, kották, festmények, hangok. A folyóiratok és az Elektronikus Periodika Archívum.
- *Nyíltság, könyvtári tájékoztatás:* MEK-L, Vendégkönyv és tájékoztatás, a MIT-HOL-tól a LibInfo-ig.

Az információszolgáltatástól a tartalomszolgáltatásig - a Libinfo jelene és jövője

Tóth Ferenc Tibor <ftoth@oszk.hu>
OSZK

Iványi Kristóf <ivanyik@oszk.hu>
OSZK

A magyar könyvtárak közös internetes tájékoztató szolgáltatása, a *LibInfo* 2003 júniusában – a NKÖM anyagi támogatásával – új honlappal jelentkezett, mely nemcsak grafikai változásokat foglal magában, hanem az eddig bevált keretek figyelembevételével kialakított gyökeresen új működési rendszert is, azaz tényleges verzió-váltásról is beszélhetünk. A változás alapvetően két dolgot jelent: áttérést a teljesen *web* alapú, közvetlenül az interneten történő válaszadásra, másrészt adatbázis alapú szolgáltatási hátteret, mellyel a *LibInfo on-line* forrástájékoztatással, tematikus, feldolgozott linkgyűjteményével, archivált, katalogizált weboldalakkal hozzájárulhat az internet tartalommal való feltöltéséhez. Megteremtettük annak technikai lehetőségeit is, hogy az információ- és tartalomszolgáltatáson túlmenően a *LibInfo* a jövőben a dokumentumszolgáltatás rendszerébe is bekapcsolódhasson.
A *LibInfo* működésének ezen alapelvei összhangban állnak az Országos Széchényi Könyvtár – mint a szolgáltatás moderátorának és koordinátorának – jelenlegi stratégiai terveivel.
Előadásunkban az új rendszer működését mutatjuk be, és felvázoljuk további fejlesztési terveinket is.

Képek - metaadatok

Káldos János <kaldos@oszk.hu>
Országos Széchényi Könyvtár

A digitálizálási projektekben és a mindennapi élet digitalizálási mûveleteiben tömegesen keletkeznek olyan digitális állóképek, amelyek valamilyen kultúrális értékrõl készült másolatok (nyomtatvány, kódex, kézirat, újság stb.) A közgyûjtemények alapvetõ feladata, hogy anyagaik megóvása, illetve az információ széleskörû terjesztése érdekében a digitalizált értékeiket szolgáltassák. A tömeges szolgáltatásban megoldandó azonban az egyes digitális dokumentumok, képsorozatok azonosítás, menedzselése és megjelenítése. Ezeket segítik az álloképekre vonatkozó metaadatok illetve ezek szabványosítási kisérletei és ajánlásai (NISO Z39-87, EXIF, XMP, MIX stb.) továbbá az egyes közgyûjtemények gyakorlata. Az elõadás bemutat néhányat külföldi és belföldi példát, továbbá felvázolja az Országos Széchényi Könyvtár elképzelését a tömeges digitális képkezelésre.

ZING: A Z39.50 új generációja

Horváth Ádám <adam@oszk.hu>
Országos Széchényi Könyvtár

A Z39.50 szabvány közel 20 éves múltra tekint vissza. Hatalmas intellektuális vagyon halmozódott fel benne. A Z39.50 protokollt széleskörûen használják, további fejlõdésének azonban gátat szab viszonylagos bonyolultsága és az a tény, hogy a jelenleg használatos webes technikáktól eltérõ megoldásokon alapul. A ZING "Z39.50-International: Next Generation" több ajánlásnak a közös neve, melyek célja, hogy könnyebbé tegyék a használatát, telepítését, és más rendszerekbe való beépítését, miközben a Z39.50-ben testet öltött eredmények sem vesznek kárba.
Az Országos Széchényi Könyvtár ITEM pályázat keretében hozzálátott egy ZING kliens kifejlesztéséhez. Elõadásomban az eddig elért eredményeket és az SRW "Search/Retrieve Web Service" valamint a CQL "Common Query Language" ajánlásokat szeretném ismertetni.

Egységes szolgáltatási környezet : a könyvtári portálok kialakítása

Pataki Gábor <gabor@oszk.hu>
Országos Széchényi Könyvtár

Bánki Zsolt <bazso@oszk.hu>
Országos Széchényi Könyvtár

Az információtechnológiai eszközpark - ma már közhelyszerû - folyamatos változása új feladatok elé állítja az emberi tudáskincs közvetítésével foglalkozó intézményeket, különösen a könyvtárakat.

Ezek a változások ún. információs szigetek képzõdését vonják maguk után. Ebben a szigetvilágban a felhasználó könnyen és gyakran eltéved. Az információközvetítéssel foglalkozó intézmények, könyvtárak feladata ezeknek a szigeteknek koherens rendszerré szervezése.
Jelenleg rendszerint külön szolgáltatás a könyvtári honlap, az OPAC és az offline elektronikus dokumentumok elérhetõsége, illetve a digitális források használtatása.

Az elõadás az integrációt szolgáló eszközöknek az alkalmazását szeretné bemutatni az OSZK munkájában, illetve ezeknek kutatását, tesztelését, fejlesztését.
Az új információs interface-k lényege, hogy a heterogén használati lehetõségeket egyetlen,

személyre szabott, differenciált, biztonságos rendszerbe szervezve segítse az eligazodást a különböző felhasználási céloknak megfelelően, funkcionálisan megkülönböztetve a könyvtárban személyesen megjelenő és a forrásokat távolról elérő felhasználót. A két felhasználói kör igényeinek megfelelően egyesítenie kell magában a honlap, az olvasói professzionális munkaállomás, és a Z39.50 gateway funkcióját.
A rendszerbe szervezés előnyei a felhasználó számára a releváns információk könnyebb megtalálása, a rendszerbe intergált eszközök közvetlen használata, valamint a belső munkatársak kapacitásának, és a munkafolyamatokba épített technológiai eszközöknek magas hatékonyságú kihasználása.

Elektronikus folyóiratok archiválása és nyilvántartása: EPA 2.0

Csáki Zoltán <csaki@mek.oszk.hu>
OSZK MEK

Az Elektronikus Periodika Archívum / Adatbázis (EPA) digitális időszaki kiadványokat kezelő archívum és lelőhely-nyilvántartó rendszer, mely egyrészt a Magyar Elektronikus Könyvtár (MEK) időszaki kiadványokat tároló különgyűjteménye, másrészt a MEK által működtetett országos internetes lelőhely-adatbázis.

Az archívum

Az EPA kiadványokat archivál, biztos hozzáférést, szükséges tárhelyet, infrastruktúrát biztosít, felhasználói-felületet épít, teljes szövegű keresést biztosít. Az archivált kiadványoknak javított, formailag egységesített kiadásváltozatai készülnek az archiválás során.

Az adatbázis

A lelőhely-adatbázis az elektronikus időszaki kiadványok adatainak szabályos bibliográfiai jellegű feltárását és leírását, valamint a lelőhelyadatok leírását tartalmazza azok rendszeres ellenőrzése mellett.
Az adatbázisban egyszerű és összetett keresés végezhető. Az adatokat szabályos csereformátumban (HUNMARC, DC-XML) szolgáltatja a további rendszerszintű felhasználás céljából (Z39.50).

EPA felhasználói felület

Bemutatjuk a kiadványok EPA-ban való megjelenési módjait (segédlapok, cédula- és adatformátumok, felhasználót orientáló források), fontosabb archívumainkat, virtuális könyvtári szolgáltatásunkat.

Az EPA harmadik szintje

A jövőben kilátás van az EPA tervezett harmadik szintjének kiépítésére, mely különösen az IKER adatbázis lezárása után jelentős hiányt pótol a tájékoztatásban: online kiadványok cikkszintű feltárása és a szövegek XML-alapú feldolgozása. Tervezett együttműködés a MATARKA szolgáltatással.

Metaadatsémák nyilvántartása szemantikus web alapon

Fülöp Csaba <csabi@dsd.sztaki.hu>
MTA SZTAKI

Kovács László <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

Micsik András <micsik@dsd.sztaki.hu>
MTA SZTAKI

A szemantikus web elgondolás alapfeltétele a hálózaton elérhető adatok és metaadatok szemantikai összekapcsolhatósága. Ennek az egyik legkézenfekvőbb módja a digitális könyvtárakban, archívumokban és adatbázisokban használt metaadatsémák összehangolása. Az ezzel kapcsolatos egységesítési, szabványosítási törekvések egyre ígéretesebbek. Kialakulóban van egy RDF alapú séma leíró rendszer, amely alkalmas a metaadatsémák pontos definiálására, és lehetővé teszi a már meglévő sémaelemekből történő építkezést, a sémák újrafelhasználását.

Az MTA SZTAKI Elosztott Rendszerek Osztálya figyelemmel követi ennek a területnek a fejlődését, és szeretné a külföldi eredményeket Magyarországon is hasznosítani, terjeszteni. Terveink között szerepel egy nyílt Internetes szolgáltatás megvalósítása, amely nyilvántartásba veszi az országban használt metaadatsémákat, és lehetővé teszi azok különböző szempontú böngészését, a sémák közti kapcsolatok áttekintését. A szolgáltatás segítséget nyújtana az új sémák összeállításához is, amelyhez a mások által már definiált sémaelemek is felhasználhatók. Egy ilyen szolgáltatás megteremti a lehetőséget a metaadatsémák áttekintésére és újrafelhasználására, amely által a használatban lévő sémák egységesebbé, kezelhetőbbé válnak, illetve elkerülhető lesz mások munkájának megismétlése. A metaadatsémák megosztása és összehangolása országos érdek, hiszen ezáltal válhat gazdaságosabbá az adatok kezelése és hatékonyabbá az adathozzáférés.

HEKTÁR: Hazai elektronikus könyvtári rendszerek összekapcsolása

Kiss Gergő <gege@dsd.sztaki.hu>
MTA SZTAKI

Kovács László <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

Micsik András <micsik@dsd.sztaki.hu>
MTA SZTAKI

Moldován István <moldovan@oszk.hu>
OSZK

A HEKTÁR nevű futó ITEM projekt keretén belül az MTA SZTAKI Elosztott Rendszerek Osztálya és az Országos Széchenyi Könyvtár az Open Archives Initiative (OAI) ajánlásainak alkalmazásával különböző digitális könyvtári rendszereket kapcsol össze. Az OAI két alapvető fogalma az adatszolgáltató (data provider) és a szolgáltatási pont (service provider). Az adatszolgáltató egy szabványos protokollon keresztül lekérdezhetővé teszi metaadatállományát a külvilág számára. A szolgáltatási pontok ezt a protokollt felhasználva a kiválasztott adatszolgáltatók számára értéknövelt és egységesített szolgáltatásokat valósítanak meg.

A projekt során az MTA SZTAKI nyílt forráskódú referencia-implementációt készít az OAI

metaadat begyűjtő protokollra (OAI-PMH), amelyet a Magyar Elektronikus Könyvtár (MEK) gyűjteményeihez illesztünk hozzá. Ezenkívül egy szolgáltatási pont is megvalósul, amely összegyűjti a hazai elérhető metaadatokat, és közösített szolgáltatásokat nyújt az összekapcsolt könyvtárak tartalmára vonatkozóan. Az OAI alkalmazása megkönnyíti különböző telephelyek, könyvtárak összekapcsolását, egyszerűvé teszi újfajta közös szolgáltatások bevezetését, és nem utolsó sorban az alkalmazókat bekapcsolja a dinamikusan növekvő nemzetközi OAI közösségbe is. Az OAI kulcsszerepet játszik az NDA (Nemzeti Digitális Adattár) kezdeményezésben is. Ezért érezzük fontosnak az OAI és a kapcsolódó technológiák (pl. Dublin Core) elterjedését Magyarországon, melyet e projekttel is szeretnénk elősegíteni.

Szabványosítási lehetőségek az ODR-ben

Dávid Boglárka <bdavid@lib.unideb.hu>
Debreceni Egyetem Egyetemi és Nemzeti Könyvtár

Molnár Sándor Gábor <molnarsg@lib.unideb.hu>
Debrecen Egyetem Egyetemi és Nemzeti Könyvtár

A 2003. október 1-jén indult új ODR (Országos Dokumentum-ellátási Rendszer) felület és a Debreceni Egyetemi és Nemzeti Könyvtár könyvtárközi kölcsönzési nyilvántartás sikeresen működik; a kérések száma jelentősen megnőtt. A következő fejlesztési lépéseket mindenképpen érdemes a meglévő könyvtári/informatikai szabványokkal összhangban tervezni .Az előadás megvizsgálja, hogy az egyes szabványok/előírások (pl. Z39.50, ISO ILL 10160, 10161-1 10161-2) az ODR és a könyvtárközi kölcsönzés mely területein lehetnek használhatóak, elősegítendő a könyvtárak jobb együttműködését és a jövőbeni egységes fejlesztést.

A MOKKA technikai háttere - on-line rekordfeltöltés

Balázs László <lbalazs@lib.unideb.hu>
Debreceni Egyetem Egyetemi és Nemzeti Könyvtár

A Corvina integrált könyvtári rendszer adottságai kitűnően illeszkednek a MOKKA jelenleg alkalmazott technikájához, ahhoz a közös katalógus rendszerhez, ahol a katalogizálás a helyi szinten történik. A rekordokat on-line lehet beküldeni egy java program segítségével. A beérkező rekordokat a rendszer ellenőrzi és ha minden feltételnek megfelelnek, akkor betölti az adatbázisba. A betöltésekről naplófájl készül, amit a rekord felküldője ellenőrizhet. Az előadásból megtudhatjuk, miért utasítja vissza a rendszer egyes rekordok betöltését, és hova kerülnek, ha a feltételeknek megfelelnek, de mégsem találjuk őket a katalógusban, miért nem tanácsos egyszerre több százezer rekordot feltölteni, és miért kell először az authority rekordot küldeni. Végül a jelenleg folyó fejlesztési munkákról is tájékozódhatunk.

Digitális archivumok

Dicse Jenő <dicse.jeno@synergon.hu>
Synergon Informatika Rt.

A szervezetek működésük folyamán jelentős mennyiségű információt termelnek, illetve fogadnak be más helyekről. Ez az információtömeg a legkülönfélébb módon tárolódik: papíron,

számítástechnikai adathordozón, magnószalagon, stb., s ezeken belül is számtalan formátumban. Minden bizonnyal többféle nyilvántartási rendszer is létezik vagy létezett ezek kezelésére. Az ezekben való eligazodás, maguknak az adathordozóknak a kezelése, a különféle keresési igények kiszolgálása gyakran nehéz feladat. A korszerű módszereket ötvöző digitális archívumok nagyobbrészt megoldják ezeket a problémákat, s az információtömeget jól hasznosítható adatvagyonná alakítják. Tehát nem csak egyszerűen egy új rendszerező, tároló eszközt jelentenek, hanem sokszor egy új bevételi forrás valós alapjaként érdemes tekinteni rájuk.

Egységes Múzeumi Nyilvántartási Rendszer projekt

Veres Gábor <gabor.veres@nkom.gov.hu>
NKÖM

Molnár László <lmolnar@freesoft.hu>
Freesoft Kft

A jogszabályok (20/2002 (X. 4) NKÖM miniszteri rendelet és az ahhoz kapcsolódó „Tájékoztató a muzeális intézmények számítógépes rendszereinek informatikai követelményeiről") változása 2003.01.01-től lehetővé teszi a muzeális intézmények számára az elektronikus nyilvántartások vezetését, megfelelő feltételek teljesülése esetén.
E feltételek szigorú követelményeket támasztanak az alkalmazott rendszerrel, az ügyviteli folyamatokkal és a szabályozással szemben.
A számítógépes nyilvántartások elterjedésének segítésére a minisztérium elhatározta egy – a jogszabályoknak minden tekintetben megfelelő – számítógépes rendszer elkészíttetését, melyet elkészülte után minden magyarországi muzeális intézmény térítésmentesen megkaphat.

A fejlesztési folyamat magában foglalja számítógépes rendszer kifejlesztését minden szakterület számára, a bevezetést 4 pilot helyszín 2-2 gyűjteményében, valamint jogszabálykövetést és Helpdesk szolgáltatást minimálisan 5 évig.

A fejlesztési és implementálási szakasz befejezése 2004. március végén várható, az előadás a projekt eredményeit, illetve a szoftver bevezetésének feltételeit foglalja össze, illetve röviden bemutatja az elkészült szoftvert.

A szegedi új egyetemi könyvtár informatikai rendszere

Bakonyi Géza dr. <bakonyi@bibl.u-szeged.hu>
SZTE EGyetemi Könyvtár

Sándor Ákos <akos@bibl.u-szeged.hu>
SZTE Egyetemi Könyvtár

Az SZTE Egyetemi Könyvtár 2004. nyarán költözik új épületbe. Az épületben, amelynek alapterülete több mint 24 m^2, a könyvtáron kívül konferenciaközpont is helyet kap. A könyvtár alapterülete több mint 14 m^2. A raktári szárny hat, az olvasói terek szárnya 4 szintes (a két olvasói tér galériás). A várható napi látogatók száma 4 és 5 ezer között lesz. Az épületben induláskor kb. 500 PC kap helyet, amelyből közel 400 az olvasók rendelkezésére áll. Az épületben 1260 végpont került kialakításra. A számokból is következik, hogy az épület informatikai infrastruktúrája igen gondos tervezést és kivetelezést igényelt. Ráadásul ebben a kifejezetten funkcionális épületben nem a hagyományos könyvtári szolgáltatásokon van a hangsúly, hanem a modern, komplex (azaz a

hagyományos és számítástechnikai eszközökön, Interneten alapuló) könyvtári szolgáltatásokon. Az előadás ezt a tervezési és kivitelezési munkát foglalja össze röviden.

E-learning alapú kurzusok oktatási tapasztalatai a Közép Európai Egyetemen

Balogh Anikó <balogha@ceu.hu>
CEU

A 2003-2004-es tanévben elkezdődött az e-learning alapú oktatás az egyetem Számítástechnikai és Statisztikai Központjában. A népszerű weboldalkészítés kezdőknek tanfolyam anyagát öntöttem html formátumba. Hosszas mérlegelés után a WebCT keretrendszerre esett a választás.

A diákok és a dolgozók körében nagy volt az érdeklődés a tanfolyam iránt, kb. 130-an jelezték részvételi szándékukat, ezért négy csoportra bontva indult a kurzus kb. 30 fő/csoport részvételével.

Előadásomban a következőkről szeretnék szólni:

- a diákok felkészültsége, e-tanulási készségük
- a keretrendszer jellegzetességei
- a tananyag
- feladatok beküldése, ellenőrzése, osztályzása
- a diákok „követése"
- segítségnyújtás, visszajelzés lehetőségei
- tanár-diák, diák-diák kommunikáció, fórum, valós idejű csevegés

Végezetül áttekintem a további irányokat a tananyagfejlesztésben, és az e-learning alapú kurzusok kiterjesztését, alkalmazásaiknak lehetőségét más tanszékekkel együttműködve.

E- learning tananyagok hatékonyságának vizsgálata az informatikus könyvtáros szakon

Forgó Sándor Ph.D <forgos@ektf.hu>
EKF
Hauser Zoltán Ph.D <hauserz@ektf.hu>
EKF
Kis-Tóth Lajos Ph.D <ktoth@ektf.hu>
EKF

A 2000/2001. évtől MÉDIAINFORMATIKA INTÉZET felvállalta az *informatikus könyvtáros* képzés akkreditációs eljárásba való alávetését, melyet a MAB elfogadott.

Az online tananyagaink (WEB-es felületen bármilyen böngészővel megtekinthetők), hálózati kommunikációra optimalizált állományok, alkalmasak akár online vizsgáztatásra is. A fejlesztőmunka fázisai közül a minőségi követelményeket emeltem ki. A tananyag tervezése során az első fázis, az hogy megalkossuk a minőségbiztosításhoz szükséges alapelemeket.

A távoktatásnak felnőtt és nyitott képzési szempontból arra, a kérdésre próbál felelni: hogyan

tudnánk olyan tananyagot és szolgáltatásokat nyújtani, amelyben a hallgatók tértől és időtől függetlenül hatékonyan sajátíthassák el a tananyagot. Az e-learninggel kombinált (blended) képzésünk hatékony képzési forma napjainkban, de az alkalmazott szervezeti forma vajon megfelel-e minden elvárásnak. Melyek az erősségeink, és hol kell még javítanunk az oktatás technológiájában.

Tekintettel arra, hogy egy eLearning rendszernek sok követelménynek – integrálhatóság, szerver kliens feltételek, biztonságosság, adatok nyomon követése, információszolgáltatási és kommunikációs lehetőségek, adminisztráció, statisztika, hallgatói környezet, – kell megfelelnie, elkezdtük a minőségbiztosítási elvek kidolgozását. Ennek egyik mérföldköve volt egy reprezentatív kérdőíves vizsgálat, amelynek szempontjai az alábbiak voltak.

1. Általános szociológiai jellemzők
2. Számítógépes, hálózati érintettsége
3. Pályaválasztási motívumok
4. Időmérleg
5. Tanulási szokások
6. Tantárgyi értékorientáció
7. Minőségbiztosítási kérdések
   - Információ a kurzusról. (*Információ és tájékoztatás biztosít*ása, bemutatás).
   - Kommunikáció. (Aszinkron együttműködés, szinkron együttműködés, visszacsatolás).
   - Design. (Struktúra, forma).
   - Adminisztráció. (*Általános jellemzők*).
   - Tartalom közzététele (Tartalom, pedagógiai elvek didaktikai módszerek érvényesülése, pszichológiai-ergonómiai elvek, médiális (műfaji) közlési elvárásoknak való megfelelés).
   - Központi adatbázis (Hallgatókra vonatkozó adatok gyűjtése, dokumentációgyűjtés, iktatás).
   - Navigáció (Általános elvárások, kiegészítők).
   - Hallgatói támogatás (Elérhetőség, hozzáférés, személyes testreszabottság).
   - Technikai követelmények. (Böngésző, op. rendszer) (*Kliens platform – standard*).
   - Értékelés, visszacsatolások minőségbiztosítás (*Tartalom, felépítés, használhatóság*)
8. Szubjektív észrevételek, vélemények.

Az előadásban tanulást támogató vegyes (blended) típusú oktatás tapasztalatai kerülnek felvázolásra.

Authoware és WebCT használata a távoktatási anyagok fejlesztésében és közzétételében

Szabó Bálint <balint@ektf.hu>
Eszterházy Károly Főiskola

Authoware és WebCT használata a távoktatási anyagok fejlesztésében és közzétételében

Előadásomban az Eszterházy Károly Főiskola Informatikus könyvtáros, távoktatásos formában megvalósuló képzés informatikai infrastruktúráját, és az azzal kapcsolatos tapasztalatokat mutatom be.

Az Eszterházy Károly Főiskola távoktatási infrastruktúrájának ismertetése:

- Képzési célok
- Hardver, és szoftver feltételek
- Tananyagfejlesztés a gyakorlatban
- Humán erőforrások

A WebCT távoktatási keretrendszer:

- A WebCT lehetőségei az adminisztráció, kommunikáció, és oktatási folyamat területén.
- A WebCT testreszabhatósága
- Kapcsolat a távoktatási szabványokkal.
- A WebCT nemzetközi elfogadottsága, helye a távoktatási keretrendszerek között
- Tapasztalatok a WebCT alkalmazásában

A Macromedia Authoware tananyag fejlesztőrendszer:

- Az Authoware tananyagainak felépítése, összetevői
- Magas fokú interaktivitás az Authoware anyagokban (navigációs lehetőségek, tesztek, öntesztek…)
- Multimédia elemek, médiaszinkronizáció
- Kapcsolat külső állományokkal, szabványok alkalmazása (Learning Standards)
- Tananyagok publikálása

Keretrendszer, és tananyagfejlesztő rendszer együttes használata:

- Macromédia Authoware tananyagok közzététele a WebCT segítségével.

Moodle - egy ingyenes, sokoldalú LMS rendszer használata a felsőoktatásban

Vágvölgyi Csaba <vagvolgy@kfrtkf.hu>
Kölcsey Ferenc Református Tanítóképző Főiskola

Az e-learning technológiák terjedésével egyre nagyobb az igény az olyan keretrendszerekre, amelyek alkalmasak az elektronikus információk tárolására, a tananyaghoz való hozzáférés szabályozására, és a tanulással kapcsolatos folyamatok nyomon követésére. A felsőoktatásban használatos keretrendszerek esetében talán a legnehezebb feladat a nagyszámú felhasználó authentikációjának megvalósítása. A Moodle (www.moodle.org) egy ingyenes és nyílt forráskódú LMS (Learning Management System) keretrendszer, amely több módon is beilleszthető a meglévő hallgatói és oktatói nyilvántartásunkba. Képes a felhasználók azonosítására akár az általánosan elterjedt LDAP protokoll segítségével, akár más módszerekkel, így lehetővé válik a meglévő címtárak, vagy az intézményben működő tanulmányi rendszerek adatbázisának felhasználása is.

Szabványok, keretrendszerek, technológiák

Papp Gyula <pappgy@kfrtkf.hu>
Kölcsey Ferenc Református Tanítóképző Főiskola

Az eLearning alkalmazások elterjedése a felsőoktatásban immáron elérhető közelségbe került. A közeljövőben jelentős méreteket ölthet az elektronikus tananyagfejlesztés. De melyek azok a körülmények, amelyek meghatározzák a fejlesztés fő vonalát, s milyen környezetet kell kialakítaniuk az intézményeknek? Milyen együttműködési lehetőségek kínálkoznak?
Előadásomban egy ideális jövőkép technológiai oldalát szeretném felvázolni. Dilemmákat, trendeket, lehetőségeket, melyek meghatározhatják a jövő felsőoktatásának arculatát.

KOPI Online Plágiumkereső és Információs Portál

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI

Pataki Máté <Mate.Pataki@sztaki.hu>
MTA SZTAKI

Tóth Zoltán <Zoltan.Toth@sztaki.hu>
MTA SZTAKI

A projekt célja egy olyan plágiumkereső szolgáltatás kifejlesztése, amely segíti a digitális könyvtárakat dokumentumaik védelmében, valamint a tanárokat és professzorokat másolt munkák vagy publikációk megtalálásában. Ezeken a szolgáltatásokon kívül még megismerteti az oldalra látogatókat az ide vonatkozó jogszabályokkal és rendeletekkel, valamint lehetőséget biztosít különböző témákban való beszélgetésre is.

Ilyen szolgáltatás jelenleg nem áll a magyar internetező közösség rendelkezésre, külföldi változatai is igen korlátozottak, mind számukat, mind szolgáltatásaikat tekintve. Ezért is érezzük időszerűnek egy magyar plágiumkereső portál létrehozását, amely elősegítené az internetes publikálások és a digitális könyvtárak elterjedését azáltal, hogy visszaszorítja a dokumentumokról készült illegális másolatokat. Amennyiben a szolgáltatás elindul, nem lesz értelme egy digitális forrásban megjelent dokumentumot lemásolni és sajátként eladni, lévén percek alatt kiderül, hogy honnét lett átvéve a dokumentum egésze, vagy egyes részei.

A projekthez tovább kell fejleszteni a szöveg-összehasonlító algoritmusokat, adatbázis szerkezeteket kell kifejleszteni és nagy adatbázisokra optimalizálni. Magyarország nemsokára csatlakozik az Európai Unióhoz, ezért kiemelkedő jelentőségű a többnyelvűség is. Minden algoritmust nyelvfüggetlenül fogunk kialakítani, hogy bármilyen nyelvű szöveges állományban tudjon keresni a rendszer.

BIZTOSTŰ – Iránymutató az IT biztonság területén

Endrődi Csilla <csilla@mit.bme.hu>
BME MIT

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME

A **Biztostű** internetes oktató tananyag, amely a Budapesti Műszaki és Gazdaságtudományi Egyetem és az Eötvös Loránd Tudományegyetem tanárainak és hallgatóinak segítségével, az Informatikai és Hírközlési Minisztérium, az Oktatási Minisztérium és a Search-Lab Kft. támogatásával jött létre.

A projekt célja egy olyan informatikai biztonsággal foglalkozó portál kialakítása volt, amely a jelenleg elérhető hasonló tartalmú oldalaktól eltérően kevésbé a termékfüggő konkrétumokra, hanem sokkal inkább a szemléletformálásra, a biztonsági látásmód kialakítására, ökölszabályok felismerésére és rögzítésére valamint ennek eredményeként a tudatosság, a biztonságérzet és a bizalom megerősítésére koncentrál. Hitünk szerint a biztonság témáját nem lehet pusztán tárgyi tudásként kezelni. A hosszútávon érvényes örökigazságok nélkül, a megfelelő szemlélet hiányában nem lehet tudatos, bizalmat teremtő biztonsági megoldásokat készíteni, illetve alkalmazni. Mivel jelenleg még sem az alsó-, sem a közép-, sem a felsőoktatásban – nem is beszélve a tanulmányaikat

már befejezett korosztályokról – nem található meg hasonló, játékokkal, interaktív módszerekkel támogatott biztonsági szemlélet kialakítását célzó oktatási forma, így ebben a minőségében a **Biztostű** egy hiánypótló szerepet tölt be.

A honlap tartalmának összeállítása során több éves szakmai oktatási tapasztalatra, illetve már elkészült anyagok, tantárgy tematikák, jegyzetek, hallgatói munkák és videón rögzített előadások forrásaira támaszkodhattunk. A portál kialakítása során – a jelenleg elérhető nyomtatott irodalmak lehetőségein jelentősen túlmutató – webes technológiák minél szélesebb palettáját igyekeztünk felhasználni. Így a **Biztostű** oldalain a „klasszikus" hierarchikusan szervezett oktatóanyagon kívül az „önmagukat ajánló" ökölszabályok, az interaktív játékok, valamint videofelvételek és ezeket kiegészítő előadás fóliák is megtalálhatóak. Mindezekkel igyekeztünk igazán színessé varázsolni az oldalt – hogy így az audiovizuális hatások és a „játszva tanulás" élménye még jobban elmélyítsék a megszerzett ismeretanyagot. A multimédiás anyagok elérhetőek a vakok és gyengénlátók, valamint siketek számára is hozzáférhető változatban.

A **Biztostű** legnagyobb terjedelmű részét a tematikus, rendezett *oktatóanyag* teszi ki, amely az IT biztonságtechnika széles területét fogja át. A feldolgozott témaköröket igyekeztünk különböző mélységekben tárgyalni, így az érdeklődők a megértést szolgáló lazább bevezetők elolvasásával, míg a haladók az anyagok „testre szabott" kifejtése, a precíz, definíció szintű meghatározások, specifikációk révén megtalálhatják az érdeklődési szintjüknek megfelelő szintű hasznos ismeretanyagot. Az oktatóanyag bejárását segítik az oldalak alján található, „haladási irányt" megadó linkek. Ezeken kívül egy adott témánál a szövegen belül a kapcsolódó témakörökhöz is találhatóak ugrási pontok.
A legfontosabb biztonságtechnikai irányelveket az *ökölszabályok* laza láncolata tartalmazza. Ezekben jól érthető és emlékezetes példákon keresztül igyekszünk megértetni és tudatosítani a helyes szemléletet, amelyeket a megértést segítő leírások, továbbá az egyes konkrét területek kifejtései egészítenek ki.
A honlapon található, néhány fontos ökölszabály vagy összefüggés bemutatására komponált *játék* révén saját élményeket szerezhetünk az adott témával kapcsolatban, ami az ismeretanyag rögzülését intenzívebbé teszi.
A tananyagot *multimédia anyagok* – videón rögzített, feliratozott előadások – színesítik, amelyek mindegyikéhez tartozik kiegészítő anyag fólia, html vagy pdf formátumban.
Az érdeklődők számára igyekeztünk további fogódzókat is adni az ismeretszerzéshez. A *további anyagok* között megtalálhatóak a linkek a BME és az ELTE kapcsolódó tantárgyainak oldalaira, elérhető innen néhány színvonalas hallgatói munka, valamint számos hasznosnak tartott szakirodalom.
Az anyagok tanulmányozása közben lehetőségünk van arra is, hogy az aktuálisan olvasott oldal elhagyása nélkül „segítséget kérjünk" egy-egy *fogalom magyarázatára* vonatkozóan egy külön ablakban.
A honlapon található anyagok kulcsszó alapján *kereshetőek* is.

Nem titkolt célunk volt egy olyan honlap kialakítása, amely az informatikai biztonság iránt érdeklődők számára *hosszútávon is kiindulópontként* szolgálhat. A **Biztostű** a szemlélet elsajátítása mellett egyszersmind egy olyan – idővel bővülő – tudásbázist jelent, ahol a leglényegesebb algoritmusok, specifikációk, módszertanok, technikák megfelelően rendszerezetten megtalálhatóak, és így egy adott témával kapcsolatban a részletek és az átfogó ismeretek is egyszerűen megszerezhetők. Reméljük, hogy látogatóink – mind a fiatalok, diákok, mind a későbbi korosztályok – a konkrét gyakorlati esetekben is visszatérnek majd ezen alapokhoz, így rendszerünk mintapéldája lehet az életfogytig tartó tanulást szolgáló tartalmaknak.

Elektronikus önkormányzati ügyintézés

Kecskés Zsuzsa <kecskes@sztaki.hu>
MTA SZTAKI

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI

Zöld Krisztina <zold@sztaki.hu>
MTA SZTAKI

Az MTA SZTAKI *"Az információs társadalom igényorientált eszközei és rendszerei"* című NKFP projekt keretében az e-közigazgatás bevezetésének, kiépítésének lépéseit, az e-demokrácia minél szélesebb körű elterjesztésének lehetőségeit kutatja. A projekt feladatköre multidiszciplináris jellegű: a célok sikeres megvalósításához az egyes szakterületeket kiválóan ismerő közigazgatási szakemberek, szakjogászok, ügyvitelszervezési, pénzügyi és informatikai szakemberek, szociológusok együttgondolkodására, együttműködésére van szükség.

A projekt résztvevői a következő területeken szeretnének előrelépést elérni:

- a közigazgatással történő kapcsolattartás (ügyintézés, hatósági ügyek stb.) megkönnyítése az állampolgár számára,
- a front-office tevékenység (ügyfélkapcsolat) "ügyfélbarát" jellegének erősítése a mesterséges intelligencia, döntéstámogatás eszközeinek felhasználásával,
- a közigazgatás működésének átláthatóbbá tétele az állampolgárok számára,
- a közigazgatási folyamatok újragondolása (folyamatok, szervezetek, jogszabályok),
- back-office tevékenység (saját belső adminisztráció) szakszerűségének támogatása.

Az előadás a prototípus rendszer megvalósításáról fog szólni, melynek keretében Kaposvár Megyei Jogú Város Polgármesteri Hivatalában front-office és back-office rendszer kerül kialakításra, valamint megtörténik ezek összekapcsolása. Az ügyfélnek lehetősége nyílik tényleges e-ügyintézésre, hiszen egy interaktív portálon keresztül kezdeményezheti építéshatósági ügyeinek lebonyolítását. Az építéshatósági ügyintézők szintén elektronikus felületen képesek kezelni a beérkezett kérelmeket egészen az ügy lezárásáig.

ORACLE iLearning – az eLearning bevezetése a katonai felsőoktatásba

Vörös Miklós <mvoros@zmne.hu>
Zrínyi Miklós Nemzetvédelmi Egyetem

Az információs és kommunikációs technológia (IKT) korszerű eszközei lehetővé teszik, de meg is követelik a tanítási-tanulási környezet átalakítását, a korszerű információs és kommunikációs eszközök ismeretét, használatát. Uralkodóvá válik az egész életen át tartó tanulás, a hagyományos oktatást egyre több helyen felváltja a tanulásmenedzselés, a hagyományos oktatási intézményeket pedig a nyitott tanulás és a művelődés virtuális környezetei. Az USA védelmi minisztériuma által kezdeményezett Advanced Distributed Learning (ADL) projekt a legkorszerűbb technológiai eszközök és tartalomfejlesztési eljárások, szabványok felhasználásával olyan web-alapú tanulási környezetet kíván kialakítani, melyben a tananyag egy világméretű elosztott tudásbázisból a tanuló személyére szabottan kerül kialakításra.

A Magyar Honvédség (MH) korszerűsítése során a technikai és szervezeti átalakulást, a professzionalista haderőre való áttérést integráció, specializáció és várhatóan létszámcsökkenés kíséri, szakmák tűnhetnek el, és újak jelenhetnek meg. Jelentős lehet a tudás amortizációja, ezért megnő a rendszeres, azonnal alkalmazható és számon kérhető ismereteket nyújtó (tovább)képzések szerepe. A honvédségi karrier-modell (haladás fölfelé, vagy kilépés a civil életbe) szintén az át- és továbbképzések iránti igény ugrásszerű növekedéséhez vezet, mely -tekintettel a résztvevők nagy számára és a képzési formák sokszínűségére- a hagyományos oktatási formában nem valósítható meg.
A szervezeti változások és az IKT rohamos fejlődése következtében átalakul a képzés eszközrendszere, módszertana és didaktikája:

- a képzésre fordítható költségek és az oktatók terhelhetőségének korlátjai, a helyettesítés nehézségei miatt jelentősen csökkenhet az összevonások, a hosszú idejű beiskolázások aránya: megnő az önképzés szerepe;
- a tovább- és átképzések nagy száma és sokfélesége megköveteli egy mobil és rugalmas továbbképzési rendszer kialakítását;
- az önálló ismeretszerzés iránti igény megköveteli a korszerű információhordozók és oktatástechnikai eszközök, valamint a távoktatásban alkalmazható, hálózaton keresztül is elérhető tananyagok kidolgozását és alkalmazását;
- az önállóan tanulók segítése érdekében elengedhetetlen egy tutori/mentori hálózat kiépítése.

A távoktatás és az eLearning katonai felsőoktatásba történő bevezetését nehezíti, hogy rövid időn belül tömeges (a tanulók számát és tanfolyamok sokféleségét egyaránt értve ez alatt) oktatási igény jelenik meg úgy, hogy a leendő tanulók és oktatók zöme még nem vett részt távoktatási formában. A feladat ezért nem csak egy egységes távoktatási rendszer kialakítását jelenti, hanem tevőleges részvételt az egész honvédség állományának felkészítésében a távoktatási formában történő ismeretszerzés elsajátítására, az MH távoktatási rendszerének kialakításában, működtetésében. Tanulástámogatási rendszerként az ORACLE iLearning megoldása kerül bevezetésre, mely harmonizál a Magyar Honvédségben a személyzeti és a pénzügyi területen használt többi ORACLE programmal.

Térinformatikai támogatás a kistérségi erőforrás-gazdálkodásban

Pázmányi Sándor MSc <spazmanyi@hbmo.hu>
Hajdú-Bihar Megyei Önk. Informatikai Központ

Nem csak az Európai Uniós csatlakozás, hanem a gazdasági versenyképesség, a térségek között dúló egyre ébredő verseny is arra késztet bennünket, hogy emberi, természeti adottságainkkal, szervezeteinkkel, infrastruktúránkkal hatékonyan gazdálkodjunk.

A rendszerváltás idején az emberek önszerveződési alapjoga megelőzte a hatékonyság követelményeit, így jöhetett létre az Európai összehasonlításban is magas önkormányzati szám (≈ 3260) település – differenciálatlan hatásköri feltételekkel.

A kistérségi együttműködés részben ezt is hivatott megoldani. Az együttműködés, közös feladatellátás alapvető feltétele az együttgondolkodás, ami viszont átgondolt struktúrájú információgyűjtést, rendszerezést és felhasználást feltételez.

Hajdú-Bihar Megyei területi és helyi, valamint Szabocs-Szatmár-Bereg megyei erőforrástérkép tapasztalatok alapján dolgoztunk ki egy módszert, rendszert mely testre szabva képes Európai színvonalon megfelelni ennek a feladatnak.

A kistérségek helyzetének, pozíciójának erősítése a közigazgatásban valamint a közelgő Európai

Únió-hoz való csatlakozás generálta elvárások kézenfekvővé tették egy olyan informatikai rendszer kialakítását mely újszerű szemlélettel és eszközrendszerrel segíti a kistérségek megváltozott információ gyűjtési, elemzési, rendszerezési és adatszolgáltató igényeinek kiszolgálását.

A Kistérségi-Erőforrástérkép egy térinformációs adatbázis és felhasználói szoftver együttese, mely biztosítja az adott területre rendelkezésre álló valamennyi szabványos formátumú térképi adat és hozzájuk kapcsolódó leíró, táblázatos információ egy közös, "magyarul beszélő", egyszerűen kezelhető és megtanulható felületen történő kezelését.
A kistérségi területi döntéstámogatási rendszer az alkalmazott információtechnológia olyan ága, mely a térbeli információk gyűjtését, feldolgozását és kezelését végzi. Az adatok gyűjtése és feldolgozása, és ezek hatékonysága alapvető a döntéshozatali stratégia egésze szempontjából. Ezen információk pontossága és megbízhatósága kihat az erőforrás-allokációval foglalkozó döntéstámogatási rendszerek, és az ez alapján hozott döntések megbízhatóságára is.

A projekt keretében a megye, a kistérségek, a statisztikai körzetek és a települések négyszintű digitális térképi alapú rendszerét valósult meg, az alulról építkező, nyitott, szabványos rendszerek elvárásainak eleget téve.

Tudásalapú közigazgatási rendszerek

Pajna Sándor MSc <spajna@hbmo.hu>
Hajdú-Bihar Megyei Önk. Informatikai Központ

WorkFlow v3.2-*Elektronikus ügyintézést támogató szoftver rendszerünk*

A problémafelvetés
Nyilvánvaló, hogy a hagyományos papír alapú kommunikációt egyre inkább felváltja az elektronikus – számítógépes kommunikáció. Ennek a robbanásszerű fejlődésnek az eredménye, hogy megszűnnek a tér-idő korlátok, vagyis az állampolgár a nap 24 órájában elérheti a hivatalt. Tény, hogy naponta több ezer mobiltelefont értékesítenek, és legalább ennyi informatikai eszköz kerül a gyártóktól a felhasználókhoz. Az alapfelvetés azonnal adódik, miért nem használjuk ki ennek a hatalmas informatikai robbanásnak az előnyét, és miért nem fordítjuk ezt az állampolgár és az ő ügyét intéző hivatal felé. Egy olyan komplex rendszerre lenne szükség, ami a hivatal belső munkáját is maximális mértékben támogatja, valamint létrehozza a virtuális hivatal fogalmát, melyben az állampolgár kihasználva az internet lehetőségeit indíthat ügyeket, lekérdezheti azok állapotát, kérdéseket tehet fel az ügyintézőnek stb.
A megoldás
Ezekre a kérdésekre ad egyértelmű választ az általunk készített WorkFlow szoftver rendszer. Ebben a hivatal a saját belső felépítésének reprezentálása után az internet segítségével nyitottá válik az állampolgár számára, leküzdve ezzel a távolsági és a helyhez kötöttségi akadályokat. Természetesen miután az állampolgár felvette a kapcsolatot a hivatallal, ezután lehetősége nyílik arra, hogy interneten keresztül beküldje az ő egyedi ügyét, melyet a hivatal elektronikus formában kap meg és így kezel továbbra is. Az ügyintéző az előre definiált elektronikus ügymenet modell alapjait figyelembe véve elintézi a beküldött ügyet, majd az ügy lezárása után tájékoztatja az állampolgárt, szintén elektronikusan a hivatal döntéséről. Természetesen nem minden állampolgár tudja igénybe venni az elektronikus ügyintézés adta előnyöket, rendszerünk erre is megoldást ad. Képes kezelni a hagyományos papír, illetve az elektronikus dokumentum környezetet is, vagyis ha az ügyintézőnek ki kell nyomtatnia az elkészült határozatot, alá kell írnia, és postáznia kell, akkor arra is lehetőséget kínál a szoftver.
Ezeket figyelembe véve, az elektronikus dokumentum menete, kezelése, tárolása sokkal átláthatóbb, gyorsabb és gördülékenyebb lesz, segítve a pontos hivatali ügyintézést. Az általunk ajánlott

rendszer tehát rendelkezik azzal az előnnyel, hogy képes működni mindkét környezetben, tehát támogatja a papír alapú ügyintézési modellt az ahhoz tartozó dokumentumokkal, szakmai eljárásokkal, munkafolyamtokkal, valamint segíti és megoldja a teljesen elektronizált – papírmentes – hivatal működési mechanizmusát is.

Az alkalmazás

A rendszer alkalmazásának egyik fő jellemzője a költségtakarékosság. Redszerünk egyenszilárd, tudásalapú, tehát az ügyintéző minden lépésben támogatva van a rendelkezésére álló dokumentumokkal, szakmai eljárásokkal, jogleírásokkal. Alapeljárásként kezeli az Államigazgatási Eljárást, melyet kiegészít a speciális szakmai eljárásokkal. Amennyiben a rendszer ASP környezetben kerül bevezetésre abban az esetben a legkisebb településen is elérhető ugyanaz a szolgáltatási minőség mint egy nagyobb lélekszámú nagyvárosban. Tehát nem szükséges nagy beruházásokat végrehajtani annak érekében, hogy az ott élő állampolgárok elérjék a nekik nyújtott szolgáltatásokat a lehető legjobb minőségben.

A rendszer éles beüzemelése folyamatban.

Tájékozódás a weben

K. Princz Mária <pmaria@delfin.unideb.hu>
Debreceni Egyetem MFK

Az Internet használata egyre inkább tért hódít a mindennapi életben, s különösen igaz ez az oktatás területén.

Hatalmas mennyiségű információ érhető el a weben keresztül, de vajon megtaláljuk–e mindig a számunkra éppen szükségeset? Milyen keresési stratégiákat követhetünk? Hogyan növelhetjük az esélyét a minél relevánsabb információ fellelésének?

A weben lévő információ keresésekor néhány jól bevált módszert követhetünk: a jónak vélt URL cím beírása, keresőszoftverek vagy tematikus keresők alkalmazása.

A felhasználók mintegy háromnegyed része keresőszoftvereket használ az információk fellelése érdekében, de ezen szoftverek a webnek csak töredékét indexelik. Mi van a nagyobbik résszel, a láthatatlan webbel? Kereshető, s ha igen, hogyan?

Az előadás számadatokat ismertet a web megoszlásáról, a felhasználók szokásairól, illetve a webes keresők tanítása során szerzett tapasztalatokat, a hallgatók által leggyakoribb hibákat ismerteti.

ÚJ ALKALMAZÁSOK, ALKALMAZÁSFEJLESZTÉSI TECHNOLÓGIÁK

NIIF Videokonferencia projekt: hol tartunk?

Kovács András <akov@niif.hu>
NIIF Iroda

Máray Tamás <maray@niif.hu>
NIIF Iroda

Mészáros Mihály <misi@niif.hu>
NIIF Iroda

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda

Az előadás célja, hogy az NIIF videokonferencia projekt keretében végrehajtott munkát, a projekt állását illetve a tervezett jövőt bemutassa az akadémiai közösségnek. Szó lesz a projekt elején lebonyolított közbeszerzési eljárásról, amelyben az NIIF professzionális videokonferencia végberendezéseket és egy nagyteljesítményű videokonferencia szervert vásárolt az akadémiai intézmények számára. Az előadásban részletesen beszámolunk az NIIF videokonferencia szolgáltatás műszaki hátteréről és lehetőségeiről. Elsőként a szolgáltatást alkotó hálózati elemekről és azok kapcsolódásáról lesz szó. Bemutatjuk a videokonferencia hívásokat irányító Gatekeeper-hálózatot, majd a központi videokonferencia szerver műszaki paramétereit és lehetőségeit illetve a kapcsolódó értéknövelt szolgáltatásokat. Végül ismertetjük a videokonferencia hálózat menedzsment eszközeit és eljárásait.

Többpontos videokonferencia

Mészáros Mihály <misi@niif.hu>
NIIF Iroda

Mint a videokonferencia neve is mutatja konferencia, virtuális találkozó. Amely nem csak két helyszín (pont-pont) összekötésére alkalmas, hanem többpontos konferencia létrehozására is. A többpontos H.323 alapú videokonferenciának elengedhetetlen feltétele egy olyan berendezés, amely képes a hangot és képet valós időben összekeverni. Ezt az eszközt H.323 terminológiában MCU-nak, azaz Multipoint Control Unit-nak, hívjuk. Előadásomban beszélni szeretnék a többpontos videokonferencia szolgáltatás előnyeiről. Eddigi tapasztalataim alapján szeretném megvizsgálni, bemutatni a következő három MCU-t. Felvázolva ezek képességeit, illetve a bennük rejlő lehetőségeket.
Az MCU-k a következőek: Az első az www.openh323.org által fejlesztett szoftveres MCU, az OpenMCU, a második a Polycom ViewStationFX végberendezésekbe épített kis teljesítményű hardveres MCU. Végül be szeretném mutatni, a legnagyobb tudású legtöbb többlet szolgáltatást adó, dedikált Polycom Accord MGC-100 típusú videószervert.

Grafikus keretrendszer komponensalapú webalkalmazások fejlesztéséhez

Székely István <iszekely@inf.unideb.hu>
Debreceni Egyetem, Informatikai Intézet

Az utóbbi néhány évben az Internet óriási fejlődésen ment keresztül, olyannyira, hogy már használata mindennapossá vált. Ekkora mértékű elterjedése az alkalmazásokra is hatással vol Egyre több alkalmazás választja "platformjának" az Internetet. Az alkalmazások ezen csoportjá webalkalmazásoknak nevezték el.

A programozók és alkalmazásfejlesztők felismerték, hogy a programok ipari méretekben val előállítása csak megfelelő módszertanok és eszközök alkalmazásával lehetséges. Az eszközök egyi fajtáját az integrált fejlesztői környezetek jelentik, amelyek manapság kivétel nélkül grafiku felhasználói felülettel rendelkeznek.

Előadásban egy általam készített fejlesztőeszközt szeretnék bemutatni, ami maga is eg webalkalmazás. Segítségével grafikus felületen készíthetők webalkalmazások. A keretrendszere belül komponensekkel dolgozhatunk, az egyes weblapokat ezekből kell felépíteni. A komponenseket egy szerver szolgáltatja, ami egy XML állományból olvassa be a rendelkezésre áll komponensek listáját az összes olyan információval együtt, ami a grafikus módban val szerkesztéshez szükséges. Ide tartoznak például a komponensek jellemzői, amiket a komponense megjelenítéséhez meg kell adni.

Az elkészült lapok leírása visszakerül a szerverre, ami gondoskodik a tárolásról. Éppen ezé szerkesztés közben kétirányú kommunikációra van szükség a keretrendszer és a komponensszerve között. A lapok leírása szintén XML formátumban kerül tárolásra, hogy később tovább szerkesztésre is legyen lehetőség. Ebben a formában viszont a lapok közvetlenül nem használható webalkalmazásokban. Gondoskodni kell az XML lapok JSP lapokká való alakításáról, amiket Java technológiával dolgozó alkalmazásszerverek már képesek használni. A JSP lapok feladata végeredmény előállítása a komponensek által szolgáltatott adatok alapján.

Minden komponens mögött egy vagy több Java osztály áll. A komponensek implementációja a MVC mintát követi. A komponensek fő osztálya az MVC modell kontrollerének funkcióját tölti be Ehhez társulhat még két osztály a modell és a megjelenítés megvalósításához.
Előadásomban bemutatom, hogy a fent ismertetett elvekre építve hogyan történhet egy alkalmazás elkészítése és a végleges JSP lapok előállítása.

Java alapú hordozható kliens vakok számára hálózati szolgáltatások elérésére

Juhász Zoltán, PhD <juhasz@irt.vein.hu>
Veszprémi Egyetem, Információs Rendszerek Tanszék

Arató András, PhD <arato@sunserv.kfki.hu>
KFKI RMKI Beszéd- és Rehabilitáció-technológiai O.

Az informatikai ipar, lenyűgöző fejlődése ellenére, a mai napig nem képes általánosan, bárki által használható rendszereket készíteni. Ez különösen igaz a tömegtermelésre kifejlesztett személyi számítógépekre és programjaikra. A „szabványos" kezelőeszközök és felhasználói interfészek olyan metafórákat, mentális modelleket és fizikai kialakításokat használnak, mely a felhasználók egészségeges többségének képességeit veszi alapul. Különösen hátrányos helyzetbe kerültekmára a vakok és gyengénlátók, mivel a grafikus felületek egyeduralkodóvá válása miatt a viszonylag egyszerű programok is csak rendkívüli erőfeszítések árán használhatók.
Cikkünkben ismertetünk egy alternatív – kéziszámítógépre épülő – megoldást, mely kimondottan a vakok igényeinek megfelelő kezelőfelülettel rendelkezik, kisméretű, olcsó és hordozható, ám mindezek ellenére lehetővé teszi a Braille gépelést és támogatja a tipikus számítástechnikai feladatok elvégzését (levélírás, olvasás, jegyzetelés, levelezés, számolás, internet elérés). A cikk

részletesen tárgyalja a kifejlesztett rendszer architektúráját, a szoftver felépítését és működését, valamint a hálózati szolgáltatás-elérés támogatására alkalmazott módszereket.

Komponensek együttműködése webalkalmazás környezetben

Jónás Richárd <richard.jonas@tsoft.hu>
Debreceni Egyetem

Napjainkban az élet valamennyi szereplőjének előnye származik abból, ha az Interneten tud közölni és fogadni információkat, majd ezen információkat jól szervezetten képes felhasználni. Ehhez elengedhetetlen egy szoftverinfrastruktúra kidolgozása, amelyet ma a webalkalmazások valósítanak meg. Ebből fakadóan a webalkalmazások gyors és rövid életciklusokkal rendelkező szoftverfejlesztési folyamata elengedhetetlen ahhoz, hogy időben reagáljunk a követelményekre.

A webalkalmazások ilyen fejlesztését támogatja a komponensalapú szoftverfejlesztés, amelynek számos ága van. Egyesek a komponensek általános reprezentációjával foglalkoznak, mások a komponensek felhasználásával elért üzleti profitot tartják szem előtt, emellett léteznek a módosíthatóságra kihegyezett komponensarchitektúrák, stb.

Cikkemben egy általam készített, előzőleg már bemutatott komponenstechnológia vizsgálatát végzem el, különböző aspektusokból. Ilyenek a biztonsági, nyomkövetési, fejlesztési aspektusok, amelyek már jól ismertek az aspektusorientált programozás világából, továbbá megvizsgáljuk, hogy hogyan lehet a komponensek együttműködését, kommunikációját aspektusorientáltan megfogalmazni, és ezekből milyen előnyeink származnak.

Aspektusorientált nyelvek XML reprezentációja

Kincses Róbert <kincsesr@tsoft.hu>
Debreceni Egyetem

A szoftverfejlesztése néhány jól körülhatárolható paradigma elveinek használatán alapszik. Napjaink legismertebb és legtöbbet használt programozási elvei az Eljárás-orientált programozás és az Objektum-orientált programozás (OOP). Az OOP elveit megvalósító nyelvek használata jelentős tért nyert a kereskedelmi használatra szánt szoftverek készítésekor.

Az OOP előrelépést jelent a procedurális megközelítéshez képest. Segítségével ugyanis könnyebben modellezhetőek le a valós élet rendszerei, valamint egy jól megtervezett és kivitelezett OO program jól karbantartható és könnyen továbbfejleszthető. Azonban léteznek olyan problémák, amelyeket nehéz elegánsan modellezni OO technikák segítségével, ezek például valamilyen módon a program egészét érintik. Egy létező program módosításakor könnyen felléphetnek ilyen típusú problémák és gyakran az ilyen problémák megoldására készülő konkrét programkód „szétszóródik". Az ilyen programkódot nehéz karbantartani és fejleszteni.

Erre a jelenségre kerestek és találtak egy megoldást a XEROX Palo Altoi Kutatási Központjának munkatársai. Ezeket az objektumok határain átívelő, a programot független helyeken befolyásoló döntéseket, tényezőket elnevezték *aspektus*nak, és az aspektusokkal operáló programozási paradigmát pedig Aspektus Orientált Programozásnak (AOP). A megoldás életképességét mutatja, hogy azóta többféle implementáció, keretrendszer (framework) is megjelent.

Az előadás témája egy olyan XML nyelv bemutatása, mely lehetővé teszi létező aspektus orientált nyelvek elemeinek reprezentálását. Elsőként egy konkrét nyelv alapján elkészíthető XML dokumentumok kerülnek bemutatásra, valamint megvizsgáljuk ennek felhasználhatóságát is konkrét példákon keresztül: hogyan készíthető futtatható programkód az XML dokumentumból, milyen más célokra lehet felhasználni az XML dokumentumot, nyújt-e kiemelkedő előnyt az XML formában történő leírás, például a kód automatikus feldolgozása során (transzformálás).

A továbbiakban azt is megvizsgáljuk, hogy egy aspektus orientált nyelv mely részeit érdemes és

lehetséges XML segítségével leírni. Amennyiben az XML nyelv teljesen függetlenné válik az adott AOP nyelv szintaktikájától (azaz minden nyelvi elemnek megfeleltetünk XML elemeket), akkor lehetővé válik annak vizsgálata, vajon lehetséges-e több konkrét nyelv eszközeit valamilyen közös XML nyelv segítségével leírni, valamint azt, hogy milyen előnyökkel vagy hátrányokkal szolgál ez az egységes reprezentáció.

Videokonferencia rendszerek minőségi garancia jellemzőinek elemzése

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Karsay Andrea <kandrea@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Napjainkban az Interneten továbbított különféle multimédiás szolgáltatásokra egyre nagyobb szerep hárul. A videotovábbító megoldások palettája egyre szélesebbé válik: az egyszerűbb szoftveres alkalmazásoktól a videó megfigyelő rendszereken, az off-line, illetve valós idejű-jellegű streaming videon keresztül a bonyolultabb videokonferencia alkalmazásokig. A "best effort" típusú átviteli technikák feleti valósidejű jellegű alkalmazások gyors terjedése szükségessé teszi a hálózati erőforrás igényének pontosabb behatárolását ahhoz, hogy a felhasználói oldalon megfelelő minőségű szolgáltatást kapjunk. Ennek megállapítása nem egyszerű feladat, hiszen a minimális sávszélesség igényen túl ez magába foglalja a protokoll adatelemek továbbításának különféle minőségi garanciáit is.

A hálózattal szemben támasztott igények meghatározásához különböző multimédiás alkalmazások tesztkörnyezetben való futtatását végezzük. Ehhez különféle paraméterekkel (keretméret, sávszélesség, simítás, stb.) rendelkező valós videó forgalmakat generálunk és a tesztkörnyezet megfelelő pontjain protokoll analizátor segítségével méréseket végzünk. Az így nyert számszerű adatok, illetve a videoműsor minőségére vonatkozó szubjektív tapasztalatok birtokában tervezzük meghatározni a H.323 protokollra épülő különféle multimédiás alkalmazások hálózati igényeit.

Előadásunk célja, hogy a tesztkörnyezetben nyert tapasztalatok alapján ajánlásokat tegyünk a működő hálózat azon kapcsolódási pontjaira és azok jellemzőire vonatkozóan, amelyeken legcélszerűbb elhelyezni a különféle multimédiás szolgáltatásokat nyújtó eszközöket. Az ismeretésre kerülő eredmények felhasználhatók lesznek az intézményi hálózat későbbi fejlesztésének meghatározása vonatkozóan abból a célból, hogy a választott eszközök, megoldások alkalmasak legyenek a multimédiás alkalmazások által támasztott minőségi igények kiszolgálására is.

Webhez Kapcsolódó Szabványosítás Magyarországon

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI, W3C Magyar Iroda

Vásárhelyi Nóra <vnora@sztaki.hu>
MTA SZTAKI, W3C Magyar Iroda

A World Wide Web Consortium (W3C) a World Wide Web technológiai ajánlásait és szabványait kidolgozó nemzetközi szervezet. 1994 októberében jött létre azzal a céllal, hogy

elősegítse a Web-ben rejlő lehetőségek minél teljesebb kihasználását olyan informatikai szabványok, ajánlások kidolgozásával, amelyek előremozdítják a Web fejlődését, és garantálják annak széleskörű felhasználhatóságát.

Az Internet globális hálózati rendszer elterjedését nagyban befolyásolta a World Wide Web Consortium tevékenysége, kutatásai-fejlesztései. Ma a köznapi ember, amúgy helytelenül, az Internetet a Web-bel azonosítja, ami megmutatja a Web-technológiák kulcsszerepét az Internetes technológiák területén. A World Wide Web rendszer az emberi kommunikáció új formáit teremtette meg, és új lehetőségeket nyújt a tudás, a multimédia információ globális megosztására.
A W3C Magyar Iroda a World Wide Web Consortium Magyarországon működő helyi szervezete, aktívan részt vesz a magyar webes szabványok kidolgozásában, terjesztésében, megismertetésében. Célja az, hogy a magyarországi intézményekkel (egyetemekkel, főiskolákkal, kormányzati szervekkel, kutató-fejlesztő intézetekkel, civil szervezetekkel) és cégekkel megismertesse a Konzorcium fejlesztéseit (szabványait, specifikációit, irányelveit, szoftvereit), s folyamatos tájékoztatást adjon róluk. Ma a W3C több mint 40 szakmai területen végez fejlesztéseket.

Videokonferencia a gyakorlatban

Giese Piroska dr <giese@rmki.kfki.hu>
KFKI RMKI

A KFKI Részecske- és Magfizikai Kutatóintézet (KFKI RMKI) kutatói nemzetközi együttműködésben folytatott kisérletekben vesznek részt. A közös munkát elősegítő folyamatos eszmecserén, a szemináriumokon és előadásokon való részvétel a videokonferencia rendszeres használatát teszi szükségessé.

Az előadásban röviden szó lesz az általunk használt IP alapú, VRVS (Virtual Rooms VideoConferencing System) és H.323 videokonferencia rendszerekről, és videokonferenciákon szerzett tapasztalatainkról. Szó lesz azon "szabályokról", melyek betartása alapvető a sikeres konferencia lebonyolításához, továbbá röviden ismertetésre kerülnek azon a szoftver/hardver eszközök, melyeket a nemzetközi konferenciák rendezése esetén kiegészítő eszközként használunk.

Végezetül néhány szóban beszámolok a 2003 decemberében, a mintegy 200 helyszín részvételével Robert Dixon (Ohio State University) és az OARNET (Ohio Academic Research Network) szervezésében megrendezésre került "Megaconference V" H.323 alapú világkonferenciáról..

Modellinformációk szabványos cseréje

Papp Ágnes <agi@delfin.unideb.hu>
Debreceni Egyetem

Az alkalmazások sokszor bonyolult adatszerkezeteket kezelnek. Számtalan alkalmazásfejlesztő eszköz létezik, amelyek ha elérhetővé kívánják tenni egymás számára az adataikat, konverziót kell végrehajtani. Az UML egy széles körben elismert, objektum orientált szemléletű alkalmazások elemzése/tervezése során használt módszer. Egy alkalmazás-független adatcsere formátum lehetővé teszi a modellek megosztását a fejlesztők és fejlesztőeszközök között.

Az OMG specifikációi egy négyrétegű architektúrában foglalják össze az adattárolási és modellezési irányelveket. Az első réteg a meta-meta modell, amely metamodell szinten definiálja az UML nyelvet. A második réteg a metamodell, amely az elsőre épülve leírja az UML szintaxisát. A harmadik rétegben a modellező nyelv használatával létrehozott modellek találhatók, míg a negyedik rétegben a modellek segítségével létrehozott adatok, objektumok vannak.

Az XML alkalmas formátumnak bizonyult az Interneten történő adattovábbításra. Az XML alapú XMI szabvány pedig lehetővé teszi, hogy különböző típusú alkalmazások között szabványos módon történjen az adatok, illetve modellek cseréje.

A Modell Vezérelt Architektúra (Model Driven Architecture) egy új alkalmazásfejlesztési megközelítés. Az MDA specifikáció egy platform-független UML modellből (PIM) és egy vagy több platform specifikus modellből (PSM) áll. Ily módon egy alkalmazási rendszer teljes modelljét csak egyszer kell megalkotni. Az MDA szintén kihasználja az XMI által nyújtott előnyöket, amikor PIM-XML összerendelést definiál.

Élő webes alkalmazások rendszerfelügyeletének automatizálása cím- és tartalomteszteléssel

Ercsényi Gábor <gercsenyi@allied-visions.de>
Allied Visions GmbH

Élő webes alkalmazások rendszer-felügyeletének automatizálása cím- és tartalomteszteléssel

Napjainkban egyre nagyobb jelentőséggel bírnak az Internet segítségével egész nap folyamatosan elérhető alkalmazások. Ezen cikk egy olyan felügyelő rendszert mutat be, amely rendszeresen tájékoztat a tesztelendő alkalmazások elérhetőségéről, és ezen túlmenően azok kielégítő vagy hibás működéséről az általuk generált tartalom ellenőrzésének segítségével. Az alkalmazás alapvető célja, hogy a webszolgáltatásokhoz igényelt manuális tesztelésekhez szükséges idő megfelelő konfiguráció mellett nagyságrendekkel rövidüljön.

Ennek lényege, hogy egy XML adatbázisban tároljuk a tesztelendő web-alkalmazások címeit valamint egyéb, a teszteléssel magával kapcsolatos adatokat.

Az alkalmazás HTTP kérésekkel kérdezi le a megadott URL-ek állapotát, méghozzá úgy, hogy webböngészőhöz hasonló módon HTTP-klienskent viselkedik. Összeállít egy kérést a megfelelő adatokkal, majd azt elküldi a HTTP szervernek. Az pedig adott állapotától függően reagál. Ez eredményezhet sikeres választ vagy jelenthet valamilyen ismert hibaüzenetet, illetve természetesen előfordulhat, hogy a szerver valamilyen ismeretlen oknál fogva nem is válaszol megadott időn belül.

Sikeres válasz esetén a rendszer az adott HTML tartalmat elemzi. Ennek során megpróbálja felkutatni mindazon tartalom-részleteket, amik elvártak a teljes HTML tartalomban, valamint megkeresi azon tartalom-szegmenseket, amik hibás működésre utalnak. Megvizsgálja azt is, hogy találhatók-e hiper-hivatkozások a szövegben, amiken további elemzést végez rekurzívan.

Az alkalmazások által létrehozott tartalom felügyeletének bonyolultságát többek közt az is okozza, hogy a tesztelendő webszolgáltatások alkalmazásai session-ökkel operálnak. Egyes alkalmazások által szolgáltatott tartalom tesztelését például csak az alkalmazásokba történő sikeres bejelentkezés esetén kezdhetjük meg.

A rendszer a tesztelés eredményéről jelentést készít, amit jelentésállományba ment. Ez lehet szintén XML formátumú a további hatékony feldolgozást elősegítve. A jelentést az alkalmazás elektronikus levélben is képes továbbítani a kívánt címzettekhez.

NIIF központi elosztott szolgáltatói platform

Bajnok Kristóf <kristof.bajnok@sztaki.hu>
MTA-Sztaki

Az NIIF központi szolgáltatásait több éven keresztül a helka.iif.hu gép látta el. 2002-re bebizonyosodott, hogy a növekvő teljesítmény- és rendelkezésre állás-követelményeket már nem lehet egyetlen kiszolgálóval megvalósítani, ezért valamilyen elosztott rendszerre volt szükség. Komoly megkötést jelentett, hogy változatos hardver (x86, SPARC) és szoftver (Solaris, Linux és egyéb operációs rendszerek) környezetet, valamint számos meglévő alkalmazást kellett támogatni. Több alternatíva vizsgálata után a Linux Virtual Server (LVS) alkalmazása mellett döntöttünk.
A helka → klaszter migráció során az alábbi változtatások voltak talán a leglényegesebbek:
- Solaris operációs rendszer helyett (RedHat) Linux alkalmazása
- PMDF levelezőszerver helyett a nyílt forrású Qmail használata
- Osztott háttértár-alrendszer és párhuzamos fájlrendszer (GPFS) használata
- Rendszerszintű felhasználók helyett:
  - Szolgáltatások a központi LDAP névtárat használják az autentikációhoz és az autorizációhoz
  - Interaktív bejelentkezés nem engedélyezett, a felhasználók nem kerülnek a lokális felhasználó-adatbázisba

Ez utóbbi változtatás számos megoldandó problémát teremtett, hiszen az alkalmazásokat általában nem készítik fel arra, hogy virtuális felhasználókkal működjenek. Az előadás során részletesen ismertetésre kerül a megvalósított rendszer struktúrája, az osztott háttértár használata, valamint az egyes alkalmazások névtárhoz történő illesztésének módja.

Nagy kommunikációs igényű elosztott alkalmazások dinamikus elhelyezése a hálózaton

Goldschmidt Balázs <balage@inf.bme.hu>
Budapesti Mûszaki és Gazdaságtudományi Egyetem

László Zoltán dr. <laszlo@iit.bme.hu>
Budapesti Mûszaki és Gazdaságtudományi Egyetem

Az internet robbanásszerû terjedésének köszönhetõen gyorsan nõ az igény az online tartalomszolgáltatásra: a hagyományos tartalomhordozók (CD, DVD, VC) helyébe egyre inkább a "letöltés" lép. Az olyan alkalmazásokban, ahol a felhasználó valós idejû követelményeinek kielégítését korlátozza az erõforrások szûkössége, az adaptáció különösen fontossá válik. Ilyen alkalmazásnak tekinthetõk az elosztott multimédia - különösen a mozgóképet kezelõ - rendszerek. A szerzõk részvételével korábban kidolgozott és megvalósított rugalmas architektúrájú rendszer képes a hálózaton új szerver számítógépek lefoglalására, majd programok és adatok ezekre igény szerint történõ átküldésére. A megfelelõ hosztok keresése alapvetõen NP-nehéz kombinatorikus optimalizálási feladat. A probléma közel optimális megoldására a szerzõk több algoritmust vizsgáltak és valósítottak meg. A legígéretesebbnek a részecske-raj (particle swarm) algoritmusnak egy, a szerzõk által kidolgozott és paraméterezett változata tûnik. Az evolúciós algoritmusok családjába tartozó particle swarm-ban részecskék egy halmazát használjuk fel valamely probléma megoldására. Minden részecske egy konkrét, de nem feltétlenül optimális megoldási javaslatot ír le. A részecskék a sajátjuknál kisebb költségû megoldást adó szomszédaik javaslatából vesznek át részleteket, és ezekkel kombinálják sajátjukat. Az algoritmus addig tart, amíg minden részecske megoldásának ugyanakkora nem lesz a költsége.
Az algoritmus eredeti változatában a javaslatok kombinálása csak bináris és valós (rendezhetõ) értékekre volt definiálva. A szerzõk által kidolgozott algoritmusban olyan halmazok elemein is

lehetséges a kombináció, amelyeken semmilyen rendezés nincs értelmezve. Az elvégzett mérések és szimulációk igazolták, hogy a javasolt algoritmus futási ideje és az általa szolgáltatott megoldások lényegesen jobbak, mint a többi vizsgált algoritmusé.

A smart kártyától az integrációig

Zsemlye Tamás <tamas.zsemlye@sun.com>
Sun Microsystems Kft.

A Java szoftverplatform rendkívül interaktív, dinamikus, biztonságos alkalmazások elõállítására, futtatására alkalmas hálózatba kapcsolt számítógéprendszereken. Valójában az különbözteti meg a többitõl, hogy más platformok fölött van, és a szoftvert bájtkódokra fordítja le, amelyek nem a fizikai géphez kötöttek, hanem gépi utasítások virtuális számítógéphez.
A Java Platform lehetőséget nyújt elosztott alkalmazások fejlesztéséhez nemcsak a hagyományos számítástechnikai környezetre, hanem akár különböző beágyazott rendszerekre is. Az elosztott alkalmazás komplex, összetett architectúrán valósulhat meg a SmartCard eszköztől a nagy teljesítményű szerver rendszerek integrációs platformjáig..

A vakok információszerzésének lehetőségei a rendelkezésre álló eszközök tükrében

Várhelyi Eszter <eszter.varhelyi@bne.hu>
Andrássy Gyula Német Nyelvű Egyetem Könyvtára

Az információs társadalom megléte még jobban kitágította a valamely fogyatékkal élő emberek és az úgymond „átlag" emberek közötti szakadékot. A technika gyors ütemben történő fejlődése nem volt minden esetben tekintettel a hátrányos helyzetüekre, akik ily módon lemaradtak a rendelkezésre álló eszközök használatában. A múlt év azonban elindított valamiféle változást e tekintetben, hiszen mint tudjuk a Fogyatékkal Élők Európai Évévé minősítették 2003-at. A kezdet adott, már csak azon kell munkálkodnunk, minekünk könyvtárosoknak, hogy folytatás is legyen.

Ahhoz, hogy a fogyatékkal élők számára (jelen esetben a vakok) használható megoldásokkal tudjunk szolgálni az információszerzés területén, tisztáznunk kell magát a fogalmat és annak következményeit.
A fogyatékosság mint jelenség nem önmagában létező, hanem valaminek az eredményeként létrejövő folyamat, aminek következtében az érintett személynek súlyos hátrányokkal kell szembenéznie.
A felmerülő nehézségek megszüntetésének egyik legfontosabb eszköze az esélyegyenlőség megteremtése.
Az esélyek biztosításának egyik fontos területe a könyvárak mint a szellemi szabadság kapui. Segédeszköz az integrációs folyamatban.
A végső cél, hogy olyan központokat hozzunk létre, melyekben a nem látók a látókkal együtt elégíthessék ki információs igényeiket az általuk ismert és használt eszközökkel.
A rendelkezésre álló eszközök: Braille-könyvek
Hangoskönyvek
Számítógép
Hangsúlyt a számítógéphasználatra illetve a digitalizálásra helyezem. Az általam végzett felmérések alapján egyre kevesebben használják a pont írást. Ennek oka kettős lehet: fizikai és lelki. A „beszélő számítógép" elterjedése azt a tendenciát hozta magával, hogy egyre többen akarják megtanulni és alkalmazni a számítógépet a fiatalok körében és kevesebb hangsúlyt helyeznek a

hagyományos eszközök használatára. A géphasználat épp azokat a hibákat igyekszik kiküszöbölni, melyek egy hangzó illetve egy Braille dokumentumnál felmerülhetnek. (időigényes előállítás, gyors elhasználódás, nehéz kezelhetőség ,stb..)
A hiányosságok kiküszöbölésére különböző alternatívák adottak: digitalizálás, internet használat, olvasógépek, hibrid hangoskönyvek, a vakok számára használható „Széchenyi Könyvtár" létrehozása.
A modern technikában rejlő rehabilitációs lehetőségek tehát adottak, csak ezeket ki kell aknázni. Fontos cél lenne olyan Windows-os felület megalkotása is, melyet a látássérültek is minden nehézség nélkül használni tudják. Jelenleg a vakok jelentős százaléka a DOS- os felületet veszi igénybe a számítógéphasználat során, mivel a Windows nem vakbarát felépítésü.(Olyan utasításokat ad mint pl: kattint ide). A linux rendszerben rejlő lehetőségek kiaknázása is fontos lenne. Ehhez a rendszerhez is készíteni kellene kompatibilis képernyőolvasókat, főleg az Uhu Linuxhoz, mely magyar nyelvű és kezelése könnyebb mint a Windows-é. Az is tény, hogy kevés olyan honlap van mely a vakok által használható lenne és ügyelne a vakbarát honlapok kritériumaira.
Meglátásom szerint a Magyar Elektronikus Könyvtár pont egy ilyen hidat képez, hiszen honlapját a látássérültek által is használhatóvá tette. (Új felület)
Összefoglalómban több célt, jövőbeni lehetőséget vázoltam fel, melynek megvalosulása nagyobb lehetőséget adna arra, hogy az a bizonyos szakadék kisebbé váljon és a látássérültek ugyanolyan eséllyel vegyenek részt az információs társadalomban, mint a látók.
Végezetül egy idézettel zárnám írásomat:
„ A vakság igazi problémája nem a látás hiánya. Az igazi probléma a meg-nem értés és a létező információk elérésének hiánya.(www.nfb.org)

Szervezeti portálok – egészen másként és a dokumentum-menedzsment jelentősége a szervezeti folyamatokban

Dicse Jenő <dicse.jeno@synergon.hu>
Synergon Informatika Rt.

A szervezeti folyamatok igen összetetté váltak, s ezek integrált informatikai támogatást igényelnének. A mai általános gyakorlat szerint azonban a különböző munkatársak, különböző rendszerekből különböző információkat látnak egy adott ügyről, s a megfelelő intézkedéshez az ezektől a kollégáktól kapott információrészeket valakinek „össze kell rakni". Az is gyakori, hogy egy dolgozó egymaga kénytelen megtanulni a sokféle rendszer kezelését, s közöttük kapcsolgatva maga „vadássza össze" a szükséges adatokat. Mindezen túl, a napi munkavégzéshez szükséges sok apró, de nélkülözhetetlen információ megosztása és elérése sincs megfelelően támogatva a legtöbb informatikai rendszerben. Ez az állapot meglehetősen nehézkes, s az embereket szükségtelenül terhelő munkafolyamatokat eredményeznek, sok idő, energia megy el felesleges dolgokra. Az ilyen indokolatlan költségek eltüntetésének, a csoportmunka hatékony támogatásának modern eszköze a szervezeti portál.

A dokumentum-menedzsment jelentősége a szervezeti folyamatokban

A szervezeti információáramlás egyik alapvető eleme a dokumentum. A dokumentumok és ezen belül az információk tárolása, átalakítása és felhasználása általában kritikus jelentőségű, ennek ellenére a legtöbb szervezetben ez informatikai oldalról nincs rendesen megoldva. A sok felesleges nyomtatás, a formailag és tartalmilag hibás dokumentumok, a nagyfokú redundancia, az emberi mulasztások és a nem megfelelő rendszerezés jelentős összegeket emésztenek fel, teljesen szükségtelenül. Egy jól átgondolt dokumentum-menedzsment rendszer bevezetésével jelentős mértékben lehet optimalizálni a napi működést, lényegesen csökkentve annak költségeit.

Csoportos üzenetszórás optimalizálása klaszter rendszerekben

Juhász Sándor <juhasz.sandor@aut.bme.hu>
BME, AAIT

Csikvári András <csiki@mail.datanet.hu>
BME, AAIT

A klaszterek, bár jelentős vetélytársai a hagyományos szuperszámítógépeknek, a kommunikációs alrendszerek sebessége területén még lemaradásban vannak, mivel a klaszterek csomópontjainak összekapcsolásánál használt általános célú kommunikációs elemek kisebb sávszélességet biztosítanak a drágább, speciálisan egy adott feladatra kifejlesztett társaiknál. Cikkünk a klaszter kommunikáció egy részterületével, a csoportos kommunikációs primitívek működésének gyorsításával foglalkozik. A különálló számítógépekből felépített klaszter rendszerekben a csomópontok együttműködésének megkönnyítésére különféle üzenetkezelő könyvtárak (pl. PVM, MPI) állnak rendelkezésre, melyek az üzenetküldés és fogadás mellett összetett csoport kommunikációs elemeket (ún. kommunikációs primitíveket) is biztosítanak a felettük működő programok számára. A kommunikációs primitívek hatékonyságát jelentősen befolyásolja a kommunikációs topológia (egy-több, fa, több-több), a szinkron vagy aszinkron végrehajtás, de akár a kommunikációs megoldás szimmetriája is.

Cikkünkben az üzenetszórás (*broadcast*) primitív különféle klaszterekben gyakran használt implementációit vizsgáljuk meg alaposabban, majd bemutatunk egy, a hagyományostól lényegesen eltérő új algoritmust, mely az üzenetek részekre bontásával és szimmetria kialakításával tovább növeli a kommunikáció teljesítményét. Az újfajta algoritmus egy egy-mindenkinek (*broadcast*) típusú üzenetszórás primitívet definiál, mely az eddig ismert, különféle architektúrákban (lánc, hiperkocka, fa) megvalósítható $O(n)$, $O(dn^{1/d})$, $O(\log_b n)$ komplexitású megoldásokkal szemben a klaszter architektúrában szoftveresen biztosítja a résztvevő csomópontok számától elvileg független, $O(1)$ komplexitást, melyet eddig csak hardver támogatással lehetett elérni.

A fent bemutatott megoldás alkalmazhatóságát mérésekkel illusztráljuk, melyek során az összehasonlítási alapot a számunkra elérhető leggyorsabb üzenetkezelő könyvtár implementáció (MPICH) saját üzenetszórás primitívje szolgáltatja. A cikkben leírt eredmények közvetlenül felhasználhatók a csoport kommunikációs primitívek teljesítményének növelésére, így közvetve hozzájárulnak a klaszter környezetben futó elosztott algoritmusok futási idejének javításhoz is.

Párhuzamos kommunikáló Java programok futtatása a JGrid rendszerben

Póta Szabolcs <pota@irt.vein.hu>
Veszprémi Egyetem, Információs Rendszerek Tanszék

Juhász Zoltán dr. <juhasz@irt.vein.hu>
Veszprémi Egyetem, Információs Rendszerek Tanszék

A globális méretű számítási Grid rendszerek kialakulásának egyik legfőbb műszaki akadálya a Grid programfuttató rendszerek együttműködésének hiánya. Nagy számításigényű alkalmazások végrehajtása csak több elosztott erőforrás igénybevételével lehetséges, emiatt egy Grid rendszernek

biztosítania kell a Grid alkalmazás különböző helyeken futó komponenseinek egyidejű végrehajtását. A jelenleg használt, számítási kapacitást kínáló, futtató környezetek a kötegelt (batch) feldolgozást részesítik előnyben, melyek működési elvükből adódóan csekély garanciát tudnak nyújtani a beküldött feladat végrehajtásának adott időpontban történő megkezdésére. Mivel ezek a rendszerek zártak, tipikusan klaszter architektúrákon üzemelnek, több ilyen rendszer összehangolása rendkívül nehéz feladat. A Grid futtatáshoz olyan futtató környezetek és globális ütemezési mechanizmusok szükségesek, melyek képesek garantálni a földrajzilag elosztott, de párhuzamosan futó komponensek egyidejű futtatását, valamint párhuzamos feladatok esetén támogatják a különböző helyekre kiosztott komponensek közötti kommunikációt.

A cikk részletesen ismerteti a JGrid projket keretélben kifejlesztett futtatási környezetet, mely megoldást nyújt a fent vázolt problémára. A JGrid rendszerben lehetséges földrajzilag elosztott számítási erőforrásokra kihelyezett párhuzamos Java programok egyidejű és azonnali futtatása. Ez a számítási erőforrásokon alkalmazott időosztásos ütemezésnek köszönhető, mely az interaktív, ill. kommunikáló feladatok végrehajtása során előnyös. Ezen felül, a rendszer egy magasszintű kommunikációs modellt is nyújt a programfejlesztők számára, amely lehetővé teszi a futó feladatok közötti kommunikáció egyszerű távoli metódushívásokkal történő megvalósítását, továbbá a feladat vezérlését is. Az említett mechanizmusok működését egy párhuzamos képfeldolgozó alkalmazást illusztrálja, melyben a számításokat logikai rácshálózatba rendezett kommunikáló Java folyamatok végzik.

Globális szolgáltatás-felfedezés a JGrid rendszerben

Kuntner Krisztián <kuntner@irt.vein.hu>
Veszprémi Egyetem

Juhász Zoltán Phd. <juhasz@irt.vein.hu>
Veszprémi Egyetem

Ahogy a Grid egyre ismertebbé és elfogadottabbá válik, úgy hallani egyre többet az egész világot behálózó, szolgáltatások millióit magába foglaló Grid rendszerekről. A milliós nagyságrendű komponensből álló rendszerek működése azonban alapvetően különbözik a néhány gépes környezetektől. A szoftver-hardver hibák miatt a szolgáltatások tetszőleges időben hagyják el a Gridet, illetve kapcsolódnak ahhoz; nincs realitása továbbá az URL vagy IP cím alapú keresésnek. A globális Grid rendszerek alapvető jellemzője kell hogy legyen tehát a gépfüggetlen, magasszintű szolgáltatás felfedezés képessége ahol a felhasználók milliónyi szolgáltatás közül hatékonyan tudják kiválasztani a számukra legmegfelelőbbeket. A cikk, a szolgáltatás felfedezés ismert módszereinek áttekintése után, ismerteti a JGrid projekt keretében kifejlesztett globális felfedező rendszer architektúráját és működését. Bemutatja a JGrid szolgáltatások leírásának módját, valamint a kliens-oldali felfedező módszereket. Ismerteti a hierarchikus felfedező-rendszer komponenseit, a komponensek szerepét és azok kapcsolatát. A cikk kitér a hibatűrés és skálázhatóság kérdéseinek vizsgálatára is, majd végezetül – kísérleti eredmények alapján – becslést ad a rendszer várható teljesítményére a szolgáltatások illetve a kliensek számának függvényében.

A JGrid rendszer biztonsági architektúrája

Magyaródi Márk <magyarodi@irt.vein.hu>
Veszprémi Egyetem

Juhász Zoltán Phd. <juhasz@irt.vein.hu>
Veszprémi Egyetem

A JGrid rendszer egy Java és Jini alapú szolgáltatás-orientált számítási Grid implementáció, amely több millió szolgáltatás és felhasználó támogatását tűzte ki célul, A Grid rendszerek kutatásának és fejlesztésének egyik legaktuálisabb kérdése a biztonság. A JGrid rendszer a Jini technológiára épül, implementációja a nemrég megjelent Jini 2.0-ás verzióját használja, mely magas funkcionalitású biztonsági architektúrát tartalmaz. A JGrid első, Jini 1.0 verzióra épülő, prototípusa nem volt biztonságos, viszont alkalmas volt egy támadásanalízis elvégzésére, mely hasznos tapasztalatokat nyújtott az új verzió biztonsági rendszerének megtervezéséhez. A cikk ismerteti ezeket a biztonsági hiányosságokat, valamint azokat az biztonsági igényeket, melyeket a szolgáltatók és felhasználók megkövetelnek a rendszerrel szemben. Megmutatjuk, hogy a Jini biztonsági architektúrája milyen megoldásokat biztosít a Jini és Grid rendszerekben előforduló támadásokra és fenyegetésekre., illetve melyek azok problémák, amik további fejlesztéseket igényelnek. Példák segítségével részletesen ismertetjük a futtató gépen belüli, és a Grid erőforrások együttműködése között jelentkező problémákat, azok megoldásait, valamint kitérünk a hálózat biztonság adminisztrációja során használt tűzfalak kezelésének kérdéseire is. A JGrid rendszer biztonsági architektúrája tehát kiterjeszti a Jini új biztonsági rendszerét, hogy nagyfokú biztonságot és védelmet nyújtson a Grid rendszerekben előforduló támadások ellen.

Klaszter alapú, nagysebességű adatgyűjtés és real-time feldolgozás

Molnár Gergely <gemolnar@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Emri Miklós <emri@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Molnár József <jmolnar@atomki.hu>
MTA ATOMKI

Balkay László <balkay@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Ecsedi Kornél <ecsedi@unideb.hu>
Debreceni Egyetem Informatikai Szolgáltató Központ

Trón Lajos <tron@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Gál Zoltán <zgal@unideb.hu>
Debreceni Egyetem Informatikai Szolgáltató Központ

A Debreceni Egyetem Orvos- és Egészségtudományi Centrumának PET Centruma, a Debreceni Egyetem Informatikai Szolgáltató Központja, valamint a Magyar Tudományos Akadémia Atommagkutató Intézete közös fejlesztésbe kezdett, melynek során részfeladatként kialakított egy speciális klasztert párhuzamosított nagysebességű adatgyûjtés és jelfeldolgozás céljára. A klaszter

PC/104-es típusú beágyazott gépekbõl, mint adatgyûjtõ kliensekbõl és nagy számolási sebességû elõfeldolgozó szerverekbõl áll. A klaszter mûködését megvizsgáltuk többféle adatátviteli sebességû switch használatával is. Operációs rendszerként hálózatról boot-oló Debian Linuxot alkalmaztunk, az adattovábbításra pedig szabványos MPI/LAM implementációt. Munkánk során tanulmányoztuk a klaszter optimális kihasználási lehetõségét, terhelhetõségét különbözõ adatgyûjtési feladatokat modellezõ szoftverek használatával.

A CERN LHC-Grid rendszerének telepítése az RMKI-ban

Debreczeni Gergely <Gergely.Debreczeni@cern.ch>
KFKI-RMKI

Hajdu Csaba <hajdu@sunserv.kfki.hu>
KFKI RMKI

Kulyassa Robert <qji@rmki.kfki.hu>
KFKI RMKI

A Genf közelében található CERN részecskefizikai kutatóintézetben most épül a világ legnagyobb részecskegyorsítója az LHC (Large Hadron Collider). A gyorsító elõreláthatólag 2007-ben fog mûködésbe lépni és segítségével a fizika legalapvetõbb kérdéseit próbálja majd megválaszolni a világ számos egyetemén és kutatóintézetében dolgozó mintegy 6000 ember. A kísérletek elvégzéséhez szükséges számítási kapacitás minden eddiginél nagyobb lesz. Évenként 12-14 PetaByte adatot kell majd feldolgozni ami kb. ekvivalens 20 millió CD tárolókapacitásával. Ha ezt napjaink leggyorsabb személyi számítógépeivel szeretnénk elvégezni , 70.000 darabra lenne szükségünk. Az LCG (LHC Computing Grid) feladata, hogy megoldást nyújtson erre a nem kis kihívást jelentõ problémára.

A KFKI-RMKI (KFKI Részecske és Magfizikai Kutató Intézet) munkatársai üzembe helyeztek egy regionális LCG központot, amely a sikeres kvalifikáció és tesztelés után teljes kapacitásával mûködésbe lépett. Elõadásunk során az LCG szerkezetének és mûködésének legfontosabb és legérdekesebb tulajdonságait fogjuk bemutatni.

A deklaratív nyelvek szerepe a szuperszámítástechnikában és az SchML projekt

Békés András György <bekesa@sch.bme.hu>
BME

Az egyre könnyebben elérhető cluster és grid rendszerek programozása nagy szakértelmet igénylő feladat. Sok eszköz segíti a párhuzamos programok írását, de a programozónak továbbra is gondosan meg kell terveznie a párhuzamosan futó részek közötti információáramlást és szinkronizációt.

A deklaratív programozási nyelveken írt programokat bizonyos tulajdonságaik miatt alapvetően könnyebb párhuzamosan végrehajtani, mint a hagyományos, imperatív programokat. Sok olyan nyelvet, nyelvi kiterjesztést fejlesztettek ki, amely a párhuzamos programozást olyannyira leegyszerűsíti, hogy a programozónak csak a párhuzamosan futó részeket kell kijelölnie.

Egy program implicit párhuzamos végrehajtása azt jelenti, hogy a programozónak egyáltalán nem kell foglalkoznia azzal, hogy a programot potenciálisan több processzor fogja végrehajtani. A BME-n futó SchML projekt egy funkcionális nyelv clustereken történő implicit párhuzamos

végrehajtását tűzte ki célul. Előadásomban bemutatok néhány párhuzamos programozást támogató deklaratív nyelvet és ezek alkalmazhatóságát cluster-rendszereken. Bemutatom továbbá az SchML rendszer főbb tulajdonságait, összehasonlítva az előzőleg ismertetett más rendszerekkel.

A Magyar Szuperszámítógép Grid tapasztalatainak bemutatása

Patvarczki József <patvarcz@sztaki.hu>
MTA SZTAKI,Párhuzamos és Elosztott rendszerek Laboratórium

Ez a cikk a Magyar Szuperszámítógép Grid (SzuperGrid) aktuális állapotát mutatja be, leírva a SzuperGrid felépítését, a konzorciumban résztvevő intézmények hálózati infrastruktúráját, valamint a rendelkezésre álló szoftver lehetőségeket. Az összekapcsolt klaszterek és szuperszámítógépek lehetővé teszik egy elosztott, nagy teljesítményű és nagy számítási kapacitású erőforrás magyarországi létrehozását.

Részletesen foglalkozik a szekvenciális, MPI és PVM alkalmazások végrehajtási lehetőségeivel Condor, Globus és Condor-G környezetekben. Mélyebben érinti a felhasználói lehetőségek teszt eredményeit, vizuálisan is megjelenítve azokat.

Továbbá, tartalmaz egy nagyon hasznos megoldást a PVM típusú programok Globus környezetben történő végrehajtásához Condor lokális menedzsert alkalmazva.

Egy Monte-Carlo Szimulációs Program Lineáris Gyorsítása a P-GRADE Fejlesztő Eszközzel

Hermann Gábor <ghermann@sztaki.hu>
MTA SZTAKI

A P-GRADE az MTA SZTAKI-ban kidolgozott általános tervező, futtató, megfigyelö, és átirányító keretrendszer, amivel párhuzamos programokat lehet létrehozni és működtetni számítógép klaszterekben és a Griden. A P-GRADE különösen alkalmas arra, hogy kivételesen rövid fejlesztési idő alatt lehessen segítségével egyrészt új párhuzamos programokat írni, tesztelni és futtatni, másrészt már meglévő C-ben vagy FORTRAN-ban megirt és bevizsgált programokat párhuzamosítani. A jelen dolgozat bemutatja, hogyan lehet párhuzamosítani oly módon egy soros programot, hogy annak végrehajtási sebessége az alkalmazott processzorokkal arányosan nőjön. Továbbá, a demonstráció tárgyául szolgáló jól strukturált, fotonok eloszlását kristálydetektoron Monte-Carlo módszerrel szimuláló FORTRAN program kapcsán megtárgyaljuk a processzek processzorokra való leképezésének hatásait. Végül bemutatjuk a P-GRADE vizuális monitorának hatékonyságát a fejlesztés minőségének növelésére.

A Magyar ClusterGrid infrastruktúra projekt

Stefán Péter <stefan@niif.hu>
NIIF Iroda

A cikk, illetve az előadás a Magyar ClusterGrid infrastruktúra projekt legfőbb struktúrális jellemzőit foglalja össze, illetve rámutrat arra, hogy az hogyan illeszkedik a réteges felépítésű grid

modellbe. A réteges felépítés legfontosabb előnye az, hogy minden réteg elrejti az alatta lévő részleteket, ugyanakkor jól definiált szolgáltatást nyújt a magasabb rétegek számára.

A ClusterGrid infrastruktúra modell hat különböző réteget különít el:

A Fizikai Réteg, vagy hardver réteg, a grid hardver építőelemeinek legfőbb szerepét, azok lehetséges funkcióit, leírását foglalja össze. Ezek az elemek lehetnek a számítási csomópontok, helyi kiszolgálók, belépési pontok, számítási feladat átjárók.

A Kapcsolati Rétegben valósul meg az előző rétegben említett hardver elemek teljesítményhatékony összekapcsolása. E réteg szoros kapcsolatban áll a számítógép-hálózatoknál megszokott adatkapcsolati réteggel, és intenzíven használja az ott bevált technikákat, mint például a 802.1q, illetve a 802.1x.

A lokálisan összekapcsolt erőforrások globális, hálózati szintű kiterjesztését végzi a Hálózati Réteg. Itt a biztonságos implementáció, illetve a hatékony kommunikáció egyaránt kiemelt szempont. E réteg felhasználja a privát hálózatok kialakítási lehetőségeit, mint például az MPLS, vagy az IPSec alapú privát hálózat.

Az Erőforrás Réteg legfontosabb feladata, hogy az egyedi erőforrásokat egyetlen absztrakt erőforrássá formálja. Ez a cluster. E réteg legfontosabb feladatai a megfelelő file rendszer kialakítása, a párhuzamos kommunikációs elemek kimunkálása, erőforrás foglalás és ütemezés.

A Grid Réteg legfontosabb feladata, hogy egy egységes felületet biztosítson a különböző cluster-ek, illetve különböző felépítésű grid rendszerek számára. A legfontosabb feladat a számítási feladat (job) fogalmának megfelelő specifikálása, illetve a rajta elvégzett műveletek definiálása (job transfer, job execution, stb.). Ebben a rétegben kell foglalkozni azzal is, hogy hogyan történik a felhasználók autentikációja, illetve hogyan történik a feladatok azonosítása.

A Felhasználói Rétegben kerül megvalósítása minden olyan alap, illetve kiegészítő fukció, mely a felhasználók közvetlen, vagy közvetett feladatait támogatja. Például szoftverek fejlesztésére alkalmas eszközök, hibakeresésre, hibajavításra alkalmas eszközök, felügyeleti eszközök.

Az előadásban szó lesz a projektben elért legújabb minőségi és mennyiségi eredményekről egyaránt.

Az NIIF VOIP rendszerének üzemeltetési tapasztalatai

Fehér Ede <ede@niif.hu>
NIIF Iroda

Tirpák Miklós <mtirpak@sztaki.hu>
MTA SZTAKI

Az NIIF Program keretében 2002. tavaszán kezdődött meg a HBONE infrastruktúrájára épülő VoIP (Voice over IP) rendszer kiépítése, amelynek első fázisa 2003. év végén zárult le. Az intézményi fejlesztések, a központi infrastruktúra kialakítása és a kihívást lehetővé tevő távközlési szolgáltatók közbeszerzésen történő kiválasztása után megkezdődött a rendszer éles üzeme. Az első körben csatlakozó 35 intézménnyel 2003. júliusától kezdődtek meg a szerződéskötések, a bekötések átvételi tesztélései és a rendszer éles üzemi támogatása.

Az intézményekkel megkötött szerződés tartalmazza azon szolgáltatási szint egyezményt, amely a hazai piacon elérhető VoIP szolgáltatásokhoz hasonló értékeket tartalmaz a rendszer rendelkezésre-állására és a hangminőséget meghatározó hálózati paraméterekre (késleltetés, csomagvesztés). A belső hívások dinamikusan növekvő forgalma mellett a nyilvános telefonhálózatokba irányuló hívások (külső hívás) lebonyolítására egyre több nagy intézmény veszi igénybe az NIIF VoIP hálózatát, így a rendszer rendelkezésre-állása és minősége egyre kritikusabbá vált. A megnövekedett igényeknek való megfelelés érdekében egy sor adminisztratív és műszaki feladatok elvégzése vált szükségessé:

- Formális, tesztforgatókönyv alapján elvégzett átadás-átvételi folyamat elvégzése az intézményi alközpontok bekötése után, amellyel feltárhatóak a leggyakoribb hibaforrások (pl. zajos ISDN vonal)
- A hangminőség eseti és folyamatos mérhetőségének és a jelzésrendszer (SIP, H.323) analizálásának megoldása professzionális mérőeszközökkel.
- Folyamatos, on-line adatgyűjtés, az adatok elemzése, statisztikák készítése.
- A központi kiszolgáló infrastruktúra – SIP szerver, SIP-H.323 gateway, PSTN felé kiépített vonalak, gateway-ek – redundáns megvalósítása.
- QoS beállítások kipróbálása és implementálása a telített vonalak esetén.
- Nemzetközi és hazai VoIP rendszerekkel peering kialakítása.
- Tesztlabor kiépítése, az új technológiák és eszközök kipróbálására.

Az előadás összefoglalja az NIIF VoIP rendszerének üzemeltetése során szerzett tapasztalatokat, és bemutatja azon eszközöket, megoldásokat, amelyek alkalmazásával az intézményi igényeknek megfelelő szolgáltatás nyújtható.

Elektronikus pályáztatás és bíráltatás -- kísérletek és tapasztalatok

Hanák Péter dr. <hanak.peter@om.hu>
Nemzeti Kutatási és Technológiai Hivatal

Simonkay Sándor <simonkay.sandor@om.hu>
Nemzeti Kutatási és Technológiai Hivatal

Magyarországon az utóbbi évtizedben megsokszorozódott a pályázatok és pályázók száma. Ma már szinte minden pályázó és bíráló elektronikus

formában tölti ki az ûrlapokat, állítja elõ a pályamûveket és bírálatokat-- majd mindent gondosan kinyomtat. A pályáztatók, tisztelet a kivételnek, a papíron beérkezõ pályamûvek és bírálatok fontosnak vélt adatait sok-sok munkával (és hibával!) ismét begépelik, hogy azután – számítógépek segítségével -- kimutatásokat, jelentéseket készítsenek belõlük. Újabban egyre több szó esik elektonikus kormányzati szolgáltatásokról, de eddig még aránytalanul kevés eredmény született.

Az Országos Mûszaki Fejlesztési Bizottság Hivatala 1997-ben hirdette meg az IKTA pályázatot információs és kommunikációs technológiai alkalmazások fejesztésének támogatására. A pályázatot gondozó osztály munkatársai számára kezdettõl fogva nyilvánvaló követelmény volt, hogy a teljes pályázati folyamatban -- a pályázatok kiírásától a pályamûvek fogadásán és elbíráltatásán át a támogatott projektek szakmai beszámolóinak és pénzügyi elszámolásainak kezeléséig -- informatikai eszközökkel kell egyszerûsíteni a munkánkat. Az évek során az IKTA ûrlaprendszerét vette át és fejlesztette tovább a Nemzeti Kutatási és Fejlesztési Programok informatikai rendszere, majd 2002-tõl használni kezdtük a többi mûszaki-fejlesztési pályázatnál is. 2003-ban a pályázati ûrlapokat már elektronikus levélben kellett beküldeni, amelyeket számítógép fogadott és dolgozott fel.

Sajnos, különféle nehézségek és akadályok miatt a megálmodott rendszernek csak egyes elemei készültek el, és többször újra kellett kezdeni a munkát. Ennek ellenére az eltelt 7 év mégsem szakmai tanulság nélkül való. A pályázatok száma az uniós csatlakozással csak növekedni fog, az adminisztrációs terhek pedig csak úgy tehetõk elviselhetõvé, ha az automatizálható feladatokat a számítógépre bízzuk. Úgy gondoljuk, hogy a pályáztatás és a bíráltatás elektronikus támogatásával hét év alatt szerzett tapasztalatainkat mások is hasznosítani tudják, ezért érdemes ezekrõl szót ejteni a Networkshop 2004 konferencián.

IP telefon szolgáltatás az Interneten I.

Szendrői József <szendroi.jozsef@synergon.hu>
Synergon Informatika Rt.

Az előadás során betekintést nyerhetünk a végponttól-végpontig terjedő, tisztán IP hálózaton megvalósított telefon szolgáltatás működésébe. Alkalmazási példákon keresztül mutatjuk meg a hálózat funkcionális elemeit, valamint az érintett protokollokat, szükséges hardver és szoftver részegységeket.

IP telefon szolgáltatás az Interneten II.

Láday Zoltán <zladay@deverto.com>
Deverto Rendszertechnika Kft.

Az előadás második részében ismertetésre kerül egy hívásvezérlő alkalmazás, mely a klasszikus szolgáltatói telefonközpont funkcionalitást emeli át az IP telefon környezetbe.
Az előadáshoz kapcsolódó technikai demonstráció a Synergon standon, a konferencia teljes időtartama alatt megtekinthető.

HÁLÓZATBIZTONSÁG, HÁLÓZATMANAGEMENT, ELEKTRONIKUS HITELESÍTÉS

Wireless LAN a Műegyetemen

Jákó András <goya@eik.bme.hu>
BME EISZK

A vezeték nélküli helyi hálózatok a médium alapvető tulajdonságaiból adódóan más biztonsági jellemzőkkel bírnak, mint a vezetékes átviteli közeget használó hálózati technológiák. Ez szükségessé teszi a vezetékes hálózatoknál megszokottakon túl egyéb biztonsági mechanizmusok alkalmazását is. A jól használható kiegészítő biztonsági mechanizmusok erősen függnek az alkalmazási környezettől.
Ez az esettanulmány bemutatja a Műegyetem vezeték nélküli hálózatán alkalmazott biztonsági mechanizmusokat, illetve azok kiválasztásának okát.

Az NIIF CSIRT projektje

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda

Németh Ervin <nemethe@niif.hu>
NIIF Iroda

Az NIIF CSIRT projektjében az elmúlt évben elkezdtük kezelni a hálózatbiztonsági kérdéseket az NIIF/HUNGARNET hálózatán. Rendszeressé váltak a biztonsági bejelentések és az incidensek kezelése a regionális központok biztonságért felelős személyeivel. A NIIF/HUNGARNET hálózati infrastruktúra biztonságosabbá tételére lépéseket tettünk a HBONE projekttel együtt. Ehhez kapcsolódó feladatként megjelent a hálózattal kapcsolatos információk összegyűjtése és terjesztése.

Az előadás keretében bemutatásra kerülnek az NIIF CSIRT projekt eddig elért eredményei, tapasztalatok, a rövid és hosszú távú tervek, és az, hogy az együttműködések eredményeként milyen szolgáltatások indulhatnak el.

Hitelesítés elektronikus aláírással e-SZALESZ

Szőllősi Loránd <lorro@lorro.wigner.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

Gyímesi Csaba <ympy@freemail.hu>
BME Távközlési és Médiainformatikai Tanszék

Juhász András <juhand@axelero.hu>
BME Távközlési és Médiainformatikai Tanszék

Marosits Tamás <marosits@tmit.bme.hu>
BME TMIT

Bevezetés

Az elektronikus aláírás a részletesen kidolgozott matematikai alapok mentén viszonylag könnyen implementálható valamely magas szintű programozási nyelvben. Elfogadásának jogi szabályozási keretei is adottak mind hazánkban, mind az Európai Unióban. Mégsem terjedt még el igazán széles körben használata, ennek elsősorban biztonságtechnikai okai vannak. Az sem elhanyagolható szempont továbbá, hogy egy ilyen, az egész országra kiterjedő rendszer meglehetősen nagy beruházást és adminisztratív munkát jelent. Vajon a jelenlegi megoldások képesek-e megfelelő biztonságot nyújtani?

Célok

A tanszéken 2002 szeptembere óta folyó kutatási és fejlesztési munkánk célja feltárni és megszűntetni ezeket az akadályokat. Ennek érdekében hardveres aláíró/ellenőrző eszköz implementációjába fogtunk bele, a hozzá tartozó hitelesítő szerverekkel és protokollokkal együtt. Az eszköz új ötleteket tartalmaz, melyek közül a legfontosabb talán, hogy LCD kijelzővel és saját billentyűzettel rendelkezik, így olyan biztonsági fokot jelent, amit egy smart card képtelen nyújtani. (Smart card esetén a felhasználó meg kell bízzon a leolvasó terminálban; esetünkben ez szükségtelen.) Egy ilyen eszköz létrehozása nem csak programozási munkát jelent, hanem elvi szintű optimalizálási feladatokat is a hardverben rendelkezésre álló tár korlátozott volta miatt. Ezeken kívül alapos átgondolást igényel a kommunikációs protokollok és az egyes aláírási funkciók folyamatainak kialakítása (a matematikai alapokon túl).

Eredmények

Ezt az aláírás létrehozó eszközt *e-SZALESZ*-nek neveztük el, mint "elektronikus SZövegkijelzős ALáíró ESZköz". A prototípust már elkészítettük, jelenleg a továbbfejlesztése folyik.
A hitelesítő eszköz mellett – a működéshez elengedhetetlen – szerveralkalmazást is fejlesztünk, melynek feladatai között található a kulcsosztás, -visszavonás és a hitelesség frissítése. Az általunk javasolt kétszerveres megoldás viszonylag rövid kulcsok esetén is megfelelő biztonságot képes nyújtani. Ezen kívül nincs szükség központi kulcstárra! Az újrahitelesítés kevés többletmunkát igényel a felhasználóktól, viszont lehetővé teszi az off-line aláírást, és általa mindenki maga határozhatja meg a sebezhetőségi ablakának méretét. A VIP változattal lehetőség nyílik a partner hitelességének tetszőlegesen pontos ellenőrzésére is.

Irodalomjegyzék

Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996
Ronald L. Rivest, Adi Shamir, Len Adelman: On Digital Signatures and Public Key Cryptosystems, MIT Laboratory for Computer Science Technical Memorandum 82 (1977).
PIC18FXX2 Microcontroller Data Sheet, Microchip,
http://www.microchip.com/download/lit/pline/picmicro/families/18fxx2/39564b.pdf

A hálózati vírusvédelem és a szolgáltatásmegtagadásos támadások elleni védekezés problémái és kapcsolatai

Bencsáth Boldizsár <boldi@crysys.hit.bme.hu>
Budapesti Műszaki Egyetem Híradástechnikai Tanszék

A hálózati vírusvédelem és a szolgáltatásmegtagadásos támadások elleni védekezés problémái és kapcsolatai

Előadásomat a problémakör és a javasolt, ismert megoldások rövid bemutatásával kívánom kezdeni. Be kívánom mutatni, hogy a hálózati vírusvédelmet jelenleg milyen eszközökkel szokásos és érdemes elvégezni: kliens oldali védelem, levelező szerver / relay szerver védelme kiemelve a nyílt forráskódú megoldásokat (pl. linux, amavis, mailscanner, clamav, unix víruskeresők és „mail gateway" védelmi szoftverek), tartalomszűrési lehetőségek (web forgalom szűrése), fájlhozzáférés-védelem vírusvédelemmel kombinálva (pl. RSBAC malware scan). Hasonló módon röviden ismertetni kívánom a DDoS (elosztott szolgáltatás-megtagadásos támadás) támadások különböző fajtáit (protokoll hiba, hálózati túltöltés, szerver-leterhelés) és az azok elleni védekezési alapvető védekezési módszereket (hibajavítás, tűzfalas védelem, anomália alapú szűrés (SYN védelem, stb.), forgalomanalízis alapú lehetőségek). A DDoS támadások kapcsán meg kívánom említeni az aktuális támadások főbb fajtáit, gyakorlatát (spam elleni védekező szolgáltatások támadása, Ebay, SCO stb. támadások, zombie hálózatok).
A tömör bevezető után be kívánom mutatni a vírusvédelmi rendszerek főbb problémáit a DDoS támadások szemszögéből: A vírusvédelem teljesítményigényét, az elárasztás lehetőségeit, a vírus-visszajelzések által okozható és okozott károkat. A problémák vázolása után a védekezési lehetőségek kiterjesztését kívánom bemutatni az általunk vizsgált egyik megoldási lehetőséget: A vírusvédelmi rendszer kombinálását a forgalmi analízis technikájával a DoS támadások ellen. A megoldás a beérkező levelek egyszerű statisztikai analízisével teremti meg annak lehetőségét, hogy a vírusvédelmi szerver ellen a DDoS támadások lehetőségét lecsökkentsük. A módszer felhasználható még az ismeretlen vírusok elleni védekezésben is a korai járvány-detekció érdekében. A javasolt megoldás alátámasztásaként ismertetem jelenlegi mintaimplementációnk felépítését.

Kriptográfiai algoritmusok implementációfüggő támadása

Endrődi Csilla <endrodi@mit.bme.hu>
BME MIT

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME MIT

Egy biztonságkritikus informatikai rendszert rendkívül sok ponton, sokféle módszerrel lehet megtámadni. Ráadásul a támadók lehetőségei és a támadási módszerek időről időre fejlődnek, így a megfelelő biztonsági szint fenntartásához a rendszerek tervezőinek, üzemeltetőinek is folyamatosan fejlődniük, illetve fejleszteniük kell. A megfelelő megoldások, a hatásos védelmi intézkedések kiválasztásához *kulcsfontosságú, hogy ismerjük a lehetséges támadási módszereket és azok hatékonysági jellemzőit.*
A támadások irányulhatnak például az adatbiztonsági szolgáltatások „lelkét adó" kriptográfiai algoritmusok ellen. Ekkor a támadó olyan matematikai összefüggéseket, algoritmusokat keres, amelyekkel például a titkos kulcs nélkül is megfejthető egy titkosított üzenet, digitálisan aláírható egy dokumentum, vagy esetleg maga a kulcs is kinyerhető. A gyakorlatban éppen ezért csak olyan kriptográfiai algoritmusok használata elfogadott, amelyek kellően jól teszteltek, kipróbáltak ilyen szempontból, így – bár nem lehetetlen, de – nagyon nehéz új, még ki nem védett törő módszert

találni ellenük. Jelenleg nagy bizonyossággal állíthatjuk, hogy egy kriptográfiát használó informatikai rendszernek – amelyet az előírásoknak megfelelően implementáltak – *nem a (matematikai értelemben vett) kriptográfiai algoritmus a leggyengébb pontja.*
Egy másik, érdekes támadási lehetőség a *side-channel attack* néven ismert módszer. Itt az algoritmus működése során fellépő különböző mellékhatásokat, kísérő jelenségeket, működési jellemzőket (pl. idő, áramfelvétel, elektromágneses kisugárzás) mérik, és ezen többlet információk felhasználásával próbálnak meg következtetni a titkos információra. Az ilyen támadásokkal szemben többek között *az RSA, a Diffie-Hellman, a DSA és az RC5 bizonyos implementációi is kiszolgáltatottak.*
Az *időmérés alapú támadás* (timing attack) esetében az egyes – titkos kulcs felhasználásával végzett – műveletek végrehajtási idejei alapján következtetnek magára a titkos kulcsra. Ennek alapja, hogy az egyes műveletek végrehajtási idejei a használt *kulcstól*, az aktuális *üzenettől*, illetve esetleg *más tényezőktől* függően különböznek. Ez a függés az algoritmust megvalósító, *futtatásra kerülő kód* és a *futtatási környezet* pontos ismeretében feltérképezhető, és bizonyos algoritmusoknál módszer adható arra, hogy a mért idők és az aktuális üzenetek ismeretében következtetni tudjunk a használt kulcsra. Fontos kiemelni, hogy az ilyen támadások sikeres végrehajtásához elegendő, ha a támadó passzívan *le tudja hallgatni* a csatornát (elegendő az üzenetek megfigyelése, nem szükséges, hogy ő maga is küldhessen üzenetet); azonban szükség van az algoritmus részletekbe menő ismeretére.
Az idő alapú támadások leggyakoribb célpontja a *moduláris szorzás* művelet, amelyet a gyakorlatban sokszor valósítanak meg a *Montgomery algoritmus* segítségével. Ennek sajátossága, hogy az operandusok értékétől függetlenül mindig ugyanannyi ideig tart, kivéve azt az egyetlen esetet, amikor az eredmény több lenne a modulusnál, és ezért szükség van egy végső kivonásra (redukciós lépésre). Ugyan a *moduláris hatványozást* a kódban többnyire nem a moduláris szorzással ismétlésével, hanem valamely *gyorshatványozó algoritmussal* valósítják meg, a támadás ezekre a módszerekre is átültethető.
Természetesen ma már léteznek olyan moduláris szorzó algoritmusok, amelyek kivédik ezt a támadási lehetőséget; ennek ellenére sok, főleg korábban készült implementációban találkozhatunk még az eredeti Montgomery algoritmussal. A timing attack ellen való védekezésnek létezik olyan módszere is, amely az alap algoritmus megváltoztatása nélkül nyújt védelmet, igaz, az algoritmus hatékonyságának (gyorsaságának) rovására. Ilyen például a *Ron Rivest-féle blinding*, amelynek alapja, hogy az aktuális üzeneten a kriptográfiai művelet elvégzése előtt egy transzformációt hajt végre, majd a kapott eredményen végrehajtja a transzformáció ellentettjét. Ezzel a művelet eredménye matematikai értelemben nem változik, azonban a passzív lehallgató nem tudja megállapítani, hogy milyen bitsorozaton került végrehajtásra a kriptográfiai művelet, ami pedig az ilyen jellegű időalapú támadás alapfeltétele lenne. Ezt a védelmi megoldást már több kriptográfiai implementáció is tartalmazza opcionálisan, sajnos azonban – felmérések szerint – a gyakorlatban többnyire nem alkalmazzák.

Az előadásban bemutatásra kerülnek az időalapú támadás működésének részletei, valamint egy választott RSA implementáció esetében működő timing attack módszereket is bemutatunk. Ezen módszerekből kiindulva felvázoljuk egy újabb megközelítést alkalmazó időalapú támadás alapötletét. Végezetül ismertetésre kerülnek a védelmi megoldások.

Decentralizáltan adminisztrálható, biztonságos email szolgáltatás felépítése nyílt forráskódú elemekből

Tornóci László, Dr. <torlasz@xenia.sote.hu>
Semmelweis Egyetem, Kórélettani Intézet

2001-ben munkahelyemen, a Semmelweis Egyetem Nagyvárad téri tömbjében nyilvánvalóvá vált, hogy az addig használt Netware/IPX alapú Mercury/pmail rendszer helyett egy új, korszerű email

szolgáltatást kell kiépíteni. Tervezéskor a következő célokat tűztem ki:

- a rendszer nyílt forráskódú komponensekből álljon
- nagyfokú üzembiztonság (RAID, user kvóták)
- a mailboxokhoz ne tartozzék valódi user-id
- kódolatlan jelszavak ne kerüljenek ki a hálózatra
- egységes elérés és kliens konfiguráció az Internet bármely pontjáról
- elérhetőség webmail felületen keresztül vagy IMAP klienssel
- decentralizált (szervezeti egységenkénti) adminisztrálhatóság
- SPAM és vírusszűrés
- magyar és angol nyelvű verzió
- skálázhatóság, további fejleszthetőség

A rendelkezésre álló nyílt forráskódú eszközök és a megfelelő internetes fórumok alapos tanulmányozása után a rendszert a következő főbb komponensekből építettem meg: Linux (RH 8), postfix MTA, cyrus-imapd, mysql, apache httpd, IMP (webmail interface), amavisd-new (virus/spam detection). A rendszer igyekszik kihasználni a postfix ill. a cyrus-imapd előnyös tulajdonságait (pl. rugalmas address mapping ill. shared folders).

Az adminisztrációhoz szükséges web felületet perlben írtam meg, a kód és a HTML részek teljes elkülönítésével, így a felület stílusa, megjelenése könnyen megváltoztatható.

A felhasználók és a rendszer között minden adatforgalom SSL csatornákon történik. Ha IMAP kliensből szeretnénk SMTP/TLS-sel levelet küldeni, akkor ez csak csak a felhasználó sikeres authentikációját követően lehetséges.

A rendszer 2003 decembere óta rendkívül megbízhatóan működik. Sem a levélforgalom, sem a felhasználók száma nem túl magas (kb. 400), de a rendszer elvileg jól skálázható. Egy lényeges jelenlegi limitáció azonban, hogy egyetlen névtér van.

Az előadás teljes anyaga, a rendszer felépítéséhez szükséges részletes útmutató, valamit a perl adminisztrációs felület a http://xenia.sote.hu/~torlasz/networkshop/ címen lesz elérhető.

RSA implementáció végrehajtási idő alapú támadása

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME Méréstechnika és Információs Rendszerek Tsz.

Endrődi Csilla <endrodi@mit.bme.hu>
BME Méréstechnika és Információs Rendszerek Tsz.

Még a matematikai szempontból alaposan megvizsgált és megfelelőnek tartott kriptográfiai algoritmusok – mint például az RSA – alkalmazása sem jelent önmagában feltétlen garanciát a kriptográfiai modul által megvalósított biztonsági szintet illetően. Sok esetben a modul *implementációs sajátosságait* kihasználva jut sikerre egy támadó. Ide tartozik például annak kihasználása, hogy a gyakorlatban megvalósított algoritmusok a működésük során *mérhető fizikai jellemzőkkel bírnak* – például egy smartcard az algoritmus végrehajtása során *áramot vesz fel* és *energiát fogyaszt*, a művelet minden esetben valamennyi *időt vesz igénybe* stb. Ezeket az „egyéb hatásokat" figyelve és mérve olyan másodlagos információkhoz juthat a támadó, amelyek megkönnyíthetik a titkos kulcs meghatározását. Ezeket a technikákat összefoglaló néven *side channel attack*-nek nevezik.
Az időmérésen alapuló támadás a *timing attack*, amelynek sikeres, gyakorlati alkalmazására –

bizonyos kriptográfiai algoritmus implementációk esetén – már vannak példák. Ezekkel már néhány tízezer megfigyelés alapján jó eséllyel *ki lehet találni a titkos kulcsot kivárható időn belül.* A támadó algoritmus végrehajtási ideje – konkrét megvalósítástól függően – mindössze lineárisan vagy négyzetesen függ a kulcs méretétől, így ezek a módszerek *érdemi törésnek minősülnek.*
A működő timing attackek alaposabb vizsgálatához létrehoztunk egy újabb idő alapú támadási változatot. Modellünk három lényeges pontban tér el az eddigi módszerektől, amelyek mind a pontosabb mérést és nyomonkövethetőséget, tisztább összefüggéseket és következtetések levonását segítik.
(1) Az időalapú támadás esetében a titkos kulcs meghatározásához felhasznált információhalmaz az adott kiindulási *adatok* (üzenetek) és a rajtuk elvégzett kriptográfiai művelet *végrehajtási idejei.* A támadás gyakorlati megvalósításának egyik kritikus pontja maga az időmérés, mivel egyrészről a mérésünk pontatlanságával, másrészről a legkülönfélébb zajokkal is számolni kell. A mi módszerünkben az eddig vizsgált fizikai idő helyett áttértünk *logikai időre,* vagyis az egyes végrehajtandó utasításokhoz mi magunk rendelünk egy bizonyos „költséget", amelyeket aztán zajmentesen összegezünk. A módszer alkalmazásának természetesen előfeltétele a kód részletes ismerete és a megfelelő költségértékek meghatározása. Ezek tetszőleges értékekre beállíthatóak, így tetszés szerinti „teszteset" kipróbálható illetve bármely létező implementáció működése szimulálható. Utóbbihoz a valóságos értékeket kell beállítanunk, amit a *hangolás* folyamatának nevezünk.
(2) A logikai idők alkalmazásának és az egyes műveletek költségértékekkel való ellátásának másik nagy előnye, hogy így nem csak az összesített időigényt tudjuk mérni – mint ahogyan az eddigi módszerekben – hanem képesek vagyunk az algoritmus *egyetlen iterációját* önmagában vizsgálni. Ez azért lényeges, mert a kulcsfejtő algoritmus az egyes iterációk végrehajtási idejének különbözőségén alapszik, azoktól függően határoz meg minden lépésben egy újabb kulcsbitet. Amennyiben csak az üzenetekhez tartozó teljes végrehajtási idők állnak rendelkezésre, az adott iterációs lépés és a teljes végrehajtási idő között csak statisztikai összefüggés áll fenn.
(3) A mérési pontatlanságokat valamint a statisztikai tulajdonságok alapján, valószínűségi alapon hozott esetleges téves döntéseket az egyik publikált módszernél egy speciális hibajelző képesség kompenzálja. Ennek segítségével pár lépésen belül felismerhető, ha a törés során egy kulcsbit hibásan került meghatározásra, így visszalépéssel és újra próbálkozással a tévedés javítható. Azonban ez a megoldás sem vezet mindig célba, ráadásul futási ideje nem becsülhető előre. A mi módszerünkben nem a hibadetektálás és visszalépés módszerét alkalmaztuk, hanem ellenkezőleg, egy előretekintő módszert választottunk. Minden lépésben előre meghatározott számú *kulcsjelöltet* tartunk számon. Így a törő algoritmus sikerességéhez nem feltétlenül szükséges, hogy minden lépésben jó döntést hozzunk, elegendő, hogy a keresett kulcs a szabályaink szerint megválasztott kulcsjelöltek között maradjon. A kulcsjelöltek konstans száma révén nem következik be exponenciális robbanás a keresési térben, a törő algoritmus futási ideje is előre becsülhető. Módszerünk lehetővé teszi, hogy adott hangolás és titkos kulcs esetén meghatározzuk, hogy mekkora jelöltszám elegendő a sikeres töréshez.
A továbbfejlesztett idő alapú támadási módszer elméletileg alkalmas minden olyan algoritmus vizsgálatára, amelynek a titkos kulccsal végzett művelete a kulcs bitjeitől egyenként függő elágazást tartalmaz (a legtöbb moduláris gyorshatványozó módszer ilyen). Modellünk számos továbbfejlesztési lehetőséget tartalmaz.

Az előadásban a kifejlesztett időalapú támadási módszert egy konkrét algoritmus, az RSA esetében mutatjuk be, valamint bemutatjuk a segítségével elért eredményeket. A tárgyalt módszer elméleti hátterével kapcsolatban további információkat tartalmaz „Kriptográfiai algoritmusok implementációfüggő támadása" című cikkünk.

Hiteles üzenet küldése rosszindulatú terminálról

Berta István Zsolt <istvan.berta@crysys.hit.bme.hu>
BME, Híradástechnikai Tanszék

Bencsáth Boldizsár <boldi@crysys.hu>
BME, Híradástechnikai Tanszék

Előadásunkban a hiteles üzenetküldés problémakörével foglalkozunk. A felhasználó egy távoli félnek kíván hiteles üzeneteket küldeni. Hogy a hálózaton kommunikálhasson, egy terminálra van szüksége. A hitelesség biztosítása végett az üzeneteket a terminál különféle kriptográfiai protokollok (MAC, digitális aláírás) segítségével hitelesíti.

Nem minden terminál tekinthető biztonságosnak. Ha feltételezhető, hogy egy támadó a terminált irányítása alá vonhatja, akkor a terminál által „hitelesített" üzenet nem tekinthető hitelesnek. Meglepően sok terminál tartozik ebbe a kategóriába.

A smart cardok (chipkártyák) biztonságos mikroszámítógépek, amelyek jelentős kriptográfiai teljesítményre képesek. Hordozhatóságuk, biztonságos architektúrájuk és kriptográfiai erejük miatt gyakran tekintik őket a fenti probléma megoldásának. Könnyen megmutatható, hogy – felhasználói felületük nem lévén – a smart cardok csakis a terminálon keresztül képesek a felhasználóval kommunikálni, így a felhasználó-chipkártya kapcsolat továbbra is ki van téve man-in-the-middle támadásoknak.

Az általunk modellezett felhasználó átlagos emberi lény, a smart cardon kívül nem áll rendelkezésére kriptográfiai számítások elvégzésére alkalmas eszköz, így pusztán saját korlátos memóriájára és számításigényére hagyatkozhat. Megvizsgáljuk, hogy a fenti felhasználó milyen kriptográfiai védelem biztosítására képes, és e védelem megfelelhet-e a hitelesség irodalomból ismert kritériumainak.

Előadásunk első részében áttekintjük a szakirodalomból ismert megoldásokat, protokollokat, melyek a felhasználó segítségére lehetnek nem biztonságos vagy rosszindulatú terminálokkal szemben.

Előadásunk második részében bemutatjuk saját megoldásunkat, amely egyrészt megvalósítható a ma létező chipkártyákkal is, másrészt nem igényli, hogy a felhasználó bonyolult számításokat végezzen.

Igaz, a chipkártya nem képes meggyőződni róla, hogy az üzenet valóban a felhasználótól származik, ennek ellenére segítségére lehet az embernek a hitelesítésben. Ez lehetséges, ha a felhasználó ún. biometriai üzenetet küld, amely összekapcsolja az ő személyazonosságát az üzenet tartalmával. Biometriai üzenet lehet például egy hang- vagy videófelvétel. Egy ilyen üzenetet manipulálni nehéz feladat, több erőforrást és esetleg emberi beavatkozást is igényel. A chipkártyának – ezt meggátolandó – azt kell biztosítania, hogy a támadónak ne legyen ideje, lehetősége egy bonyolult támadást kivitelezni.

A chipkártya segítségével ún. biztonságos időkapu alakítható ki, amely igazolja, hogy az üzenet elküldése egy bizonyos időintervallumon belül történt. Ezáltal jelentősen korlátozható az az időtartam, amelyet a támadó az üzenet hamisítására fordíthat, így a felhasználó egyszerűbb hitelesítési módszerekkel is nagy biztonságot érhet el.

A GeneSyS projekt - Generikus rendszerfelügyeleti middleware

Pataki Balázs <pataki@dsd.sztaki.hu>
MTA SZTAKI

Kovács László dr. <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

A GeneSyS projekt az Európai Unió 5. keretprogramja által finanszírozott "Információs Társadalom" projekt (IST-2001-34162), mely 2002 márciusában kezdõdött, 2.5 évig tart, 2.6 millió eurós költségvetéssel 4 partner részvételével (EADS Space Transport, NAVUS, Stuttgarti egyetem HLRS laborja, MTA SZTAKI - DSD) mûködik.

A GeneSyS projekt célja, hogy megtervezésre kerüljön és megvalósuljon egy újfajta, elosztott rendszereket kiszolgálni képes rendszerfelügyeleti middleware. Célunk volt, hogy:

- az elkészült rendszer ne csak alacsony szintû eszközök (hálózati elemek, rendszer közeli programok, stb.) vezérlését és monitorozását legyen képes kezelni, hanem magasabb szintû alkalmazásokra, üzleti logikákra is alkalmazható legyen
- a rendszerfelügyelet a passzív monitorozás mellett az applikációk vezérlésére is kiterjedjen.
- a rendszerfelügyelet alkalmazható legyen többféle elosztott rendszerben és alkalmazásban, vagyis nyitottnak és generikusnak kell lennie.

Az elkészült middleware-t ipari partnerekkel együttmûködve próbáljuk ki különbözõ valós és küldetés kritikus alkalmazásban. A Konzorcium célja, hogy a GeneSyS koncepciót minél szélesebb körben tegye ismertté, és hogy a javasolt generikus architektúrából ipari szabvány/ajánlás váljék. További cél, hogy az elkészült prototípus ingyenesen és forráskóddal együtt, szabadon hozzáférheto legyen.

A Projekt jelenleg túl van az elsõ fázisán, melynek eredményeképpen megszületetet a GeneSyS V1 prototípus, amely ingyenesen, szabadon forráskóddal együtt hozzáférhetõ a SourceForge.net-en keresztül.

A GeneSyS projekt a következõ fázisában az alap architektúra kiterjesztésével és intelligens ágensek alkalmazásával válik teljes értkû és kommercilizálásra alkalmas rendszerfelügyeleti alkalmazássá.

Mondd, Te kit választanál? Vírusvédelmi rendszerek minősítése és tesztelése

Leitold Ferenc Dr. <fleitold@veszprog.hu>
Veszprémi Egyetem

Kárpáti Nikoletta <niki@veszprog.hu>
Veszprog Kft.

A szoftvertesztelők, a minőségbiztosítással foglalkozó szakemberek a programjaikat a lehetőségekhez képest a legváltozatosabb környezetekben, nagyon sok bemeneti paraméter mellett tesztelik. Anti-vírus termékek esetén ez még nehezebb és bonyolultabb feladat, hiszen a termék állandóan változik, a fejlesztők újabb és újabb eljárásokat építenek bele. Az antivírus szoftverek általában néhány ezer vírusfelismerő és vírusmentesítő algoritmust tartalmaznak, melyeket sok vírusmintával és természetesen vírusmentes file-okkal is kell tesztelni.

A CheckVir projekt alapvető célja, hogy antivírus fejlesztőktől függetlenül teszteljen antivírus szoftvereket és megoldásokat, segítve a felhasználókat és az antivírus fejlesztő cégeket egyaránt. A projekt során 2002. áprilisától kezdődően havonta végezzük el a vírusvédelmi szoftverek tesztelését változó platformon, folyamatosan megújuló vírusmintákkal. A CheckVir projekt keretében **2004. januártól** kezdődően elkezdtük a vírusvédelmi rendszerek minősítését. A meghatározott feltételeknek megfelelő antivírus rendszerek havonta részesülnek a címben, mely azt bizonyítja, hogy az antivírus rendszerek a legelterjedtebb vírusok ellen sikeresen képesek felvenni a harcot. A minősítési eljáráson minden, a CheckVir projekt keretében tesztelt antivírus termék részt vesz.

A minősítés során két szintet különböztetünk meg:

1. **Standard Level:** csak a vírusok keresésére vonatkozó információkat vizsgáljuk. A vírusvédelmi rendszernek valamennyi teszteléshez használt vírus minden példányát azonosítani kell.
2. **Advanced Level:** a vírusok keresését és irtását is vizsgáljuk. A vírusvédelmi rendszernek a Standard Level feltételén túlmenően az alábbi feltételeknek kell megfelelnie:
   - A vírus kódját a fertőzött objektumból el kell távolítani, minden olyan vírus esetén, amelyiknél ez elvileg megtehető.
   - A visszaállított objektumnak továbbra is teljes értékűnek kell lennie a használhatóság szempontjából.
   - Bármilyen információvesztés megengedett, amennyiben a vírusvédelmi program erről a felhasználót tájékoztatja. Ide értendő például az az eset is, ha az antivírus egy makróvírus eltávolítása során törli a dokumentum többi makróját, és erről a felhasználót informálja.

A tesztelés során vizsgáljuk az antivírus rendszerek manuális indítású **(on-demand)**, valamint a folyamatosan figyelő védelem **(on-access)** víruskeresési képességét.

Az előadás keretében a projekt eddigi, mintegy kétéves tevékenységét szeretnénk összefoglalni, kiemelve az utóbbi hónapok minősítési eredményeit.

Biztonságos elektronikus aláírás megbizhatatlan környezetben

Leitold Ferenc Dr. <fleitold@veszprog.hu>
Veszprémi Egyetem, Információs rendszer Tanszék

Az elektronikus aláírás gyakorlati alkalmazásának biztonságát az alábbiak garantálják:

3. Nyilvános kulcsú algoritmusok (pl. RSA), mely matematikai hátterével gondoskodik róla, hogy belátható időn belül ne lehessen az elektronikus aláírást a titkos kulcs nélkül előállítani, a titkosított üzenetet ne lehessen visszaállítani.

4. Az elektronikus aláírásról szóló törvény biztosítja a titkos kulcs felhasználóhoz rendelését, illetve azt is, hogy ellenőrizhető legyen, hogy az aláírás érvényes volt az aláírás létrehozásakor.

5. Az elektronikus aláírásról szóló törvény alapján a kijelölt tanúsító szervezetek minősítik az aláírás létrehozó eszközöket.

A felsoroltak közül a leggyengébb láncszem az aláírás létrehozó eszközök biztonsága, különösen, ha ez egy más célra is használt számítógéphez csatlakozik. Mekkora ez a kockázat? Milyen módszerekkel és eszközökkel tehetjük biztonságosabbá az elektronikus aláírás használatát? Előadásomban ezeket a kérdéseket szeretném körüljárni, konkrét példákkal bemutatni.

C6500 firewall modul: történetek a biztonsághoz vezető út kanyarjairól

Horváth Gábor <hg@ludens.elte.hu>
ELTE ITK

Kiss Bence <bence@noc.elte.hu>
ELTE ITK

- Történeti parabola a transzparens gerinchálózattól az intranet kialakításáig és védelméig. Hol védjünk, hogyan védjünk és mit? Szeretnék-e a userek, hogy megvédjük őket és hogyan szeretnék? Mi [nem] történik, ha a userek védik meg magukat?
- Mivel védjünk? Miért pont C6500 firewall service modul? Hogyan építsük be? Lehetséges konfigurációk és elemzésük. Mi a legegyszerűbb működő, de L3-ban redundáns konfiguráció? [És miért nem működik?] [Hogyan lehet működőképessé tenni?] A peering forgalom routing-ja AS-en belül és AS-ek között, redundáns konfigurációban, a firewall-on keresztül.
- Tapasztalatok. Rutintalanok vagyunk vagy béta-teszterek? A feature lista mellékhatásai. Végül néhány szép diagram az FWSM által megfogott támadásokról.

IBM BladeCenter - Menedzsment, nem csak menedzsereknek

Varga Zsolt <zsolt_varga@hu.ibm.com>
IBM Magyarország Kft.

Már sok szervezet hozzálátott a szerverek központosított adatközpontokba való összevonásához; a fizikai eszközök, az alkalmazások és az adatok összevonásával céljuk, hogy a vállalatban szétszórt kis szerverek kezelésével együtt járó terheket és költségeket csökkentsék.

A blade szerverek olyan rackre optimalizált szerverek, amelyekkel az említett problémák nagy része kiküszöbölhetõ, és az 1 és 2 egység méretû szerverek alternatívájának tekinthetõk. A blade szerverek széles kínálatában egyaránt megtalálhatók nagy sûrûségû, kis feszültségû, kis teljesítményû szerverek, nagy teljesítményû, kisebb sûrûséget nyújtó szerverek és egyedi, testreszabott rackmegoldások is – amelyek már a blade rendszerekre jellemzõ egyes funkciókat is biztosítanak.

A blade szerverek úgy lettek megtervezve, hogy kis méretben óriási horizontális skálázhatóságot biztosítsanak, egyetlen házba többféle kártya is behelyezhetõ legyen,az kicsitõl a nagy teljesítményû és magas rendelkezésre állású processzorokig a processzorok széles skálája használható legyen, a javítás gyorsan és könnyen elvégezhetõ legyen, a felügyelet fejlett az üzembe helyezés pedig egyszerû legyen, emellett a rendszer jelentõs költségmegtakarítást nyújtson – kezdetben és hosszabb távon is.

Kémprogramok és az ellenük való védekezés

Krausz Tamás dr. <kuka@delfin.unideb.hu>
Debreceni Egyetem

Kémprogramnak tekintünk bármely olyan programot, ami az internet kapcsolatot tudtunk vagy kifejezett engedélyünk nélkül a háttérben használja. Az internet háttércsatornáinak használatát meg kell előzze egy teljes és valódi leírása ezen csatornák használatának, követve ezt egy világos egyértelmű beleegyező nyilatkozatnak e használatról. Bármely szoftver, melyekből a fenti elemek egyike is hiányzik, az vétkes információszerzésben és jogosan hívjuk kémprogramnak.

Az eredeti definícióhoz képest a fogalom bővült és némileg jelentést váltott. A kémprogram ma egy érzelmileg töltött szó és mást jelent különböző embereknek. Néha ez reklámprogram, böngésző objektum segítő, gengszter program vagy trójai, de mindesetben a szó olyan szoftverre utal, amelyet a felhasználó nem szándékozott telepíteni a gépére, nem kívánja a működését és nehezen tud megszabadulni tőle.

Kriptográfiai algoritmus implementációk időalapú támadása

Endrődi Csilla <endrodi@mit.bme.hu>
BME MIT

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME MIT

Még a matematikai szempontból alaposan megvizsgált és megfelelőnek tartott kriptográfiai algoritmusok – mint például az RSA – alkalmazása sem jelent önmagában feltétlen garanciát a kriptográfiai modul által megvalósított biztonsági szintet illetően. Sok esetben a modul *implementációs sajátosságait* kihasználva jut sikerre egy támadó. Ide tartozik például annak kihasználása, hogy a gyakorlatban megvalósított algoritmusok a működésük során *mérhető fizikai jellemzőkkel bírnak* – például egy smartcard az algoritmus végrehajtása során *áramot vesz fel* és *energiát fogyaszt*, a művelet minden esetben valamennyi *időt vesz igénybe* stb. Ezeket az „egyéb hatásokat" figyelve és mérve olyan másodlagos információkhoz juthat a támadó, amelyek megkönnyíthetik a titkos kulcs meghatározását. Ezeket a technikákat összefoglaló néven *side channel attack*-nek nevezik.

Az időmérésen alapuló támadás a *timing attack*, amelynek sikeres, gyakorlati alkalmazására – bizonyos kriptográfiai algoritmus implementációk esetén – már vannak példák. Ezekkel már néhány tízezer megfigyelés alapján jó eséllyel *ki lehet találni a titkos kulcsot kivárható időn belül.* A támadó algoritmus végrehajtási ideje – konkrét megvalósítástól függően – mindössze lineárisan vagy négyzetesen függ a kulcs méretétől, így ezek a módszerek *érdemi törésnek minősülnek.*

A működő timing attackek alaposabb vizsgálatához létrehoztunk egy újabb idő alapú támadási változatot. Modellünk három lényeges pontban tér el az eddigi módszerektől, amelyek mind a pontosabb mérést és nyomonkövethetőséget, tisztább összefüggéseket és következtetések levonását segítik.

(1) Az időalapú támadás esetében a titkos kulcs meghatározásához felhasznált információhalmaz az adott kiindulási *adatok* (üzenetek) és a rajtuk elvégzett kriptográfiai művelet *végrehajtási idejei.* A támadás gyakorlati megvalósításának egyik kritikus pontja maga az időmérés, mivel egyrészről a mérésünk pontatlanságával, másrészről a legkülönfélébb zajokkal is számolni kell. A mi módszerünkben az eddig vizsgált fizikai idő helyett áttértünk *logikai időre*, vagyis az egyes

végrehajtandó utasításokhoz mi magunk rendelünk egy bizonyos „költséget", amelyeket aztán zajmentesen összegezünk. A módszer alkalmazásának természetesen előfeltétele a kód részletes ismerete és a megfelelő költségértékek meghatározása. Ezek tetszőleges értékekre beállíthatóak, így tetszés szerinti „teszteset" kipróbálható illetve bármely létező implementáció működése szimulálható. Utóbbihoz a valóságos értékeket kell beállítanunk, amit a *hangolás* folyamatának nevezünk.

(2) A logikai idők alkalmazásának és az egyes műveletek költségértékekkel való ellátásának másik nagy előnye, hogy így nem csak az összesített időigényt tudjuk mérni – mint ahogyan az eddigi módszerekben – hanem képesek vagyunk az algoritmus *egyetlen iterációját* önmagában vizsgálni. Ez azért lényeges, mert a kulcsfejtő algoritmus az egyes iterációk végrehajtási idejének különbözőségén alapszik, azoktól függően határoz meg minden lépésben egy újabb kulcsbitet. Amennyiben csak az üzenetekhez tartozó teljes végrehajtási idők állnak rendelkezésre, az adott iterációs lépés és a teljes végrehajtási idő között csak statisztikai összefüggés áll fenn.

(3) A mérési pontatlanságokat valamint a statisztikai tulajdonságok alapján, valószínűségi alapon hozott esetleges téves döntéseket az egyik publikált módszernél egy speciális hibajelző képesség kompenzálja. Ennek segítségével pár lépésen belül felismerhető, ha a törés során egy kulcsbit hibásan került meghatározásra, így visszalépéssel és újra próbálkozással a tévedés javítható. Azonban ez a megoldás sem vezet mindig célba, ráadásul futási ideje nem becsülhető előre. A mi módszerünkben nem a hibadetektálás és visszalépés módszerét alkalmaztuk, hanem ellenkezőleg, egy előretekintő módszert választottunk. Minden lépésben előre meghatározott számú *kulcsjelöltet* tartunk számon. Így a törő algoritmus sikerességéhez nem feltétlenül szükséges, hogy minden lépésben jó döntést hozzunk, elegendő, hogy a keresett kulcs a szabályaink szerint megválasztott kulcsjelöltek között maradjon. A kulcsjelöltek konstans száma révén nem következik be exponenciális robbanás a keresési térben, a törő algoritmus futási ideje is előre becsülhető. Módszerünk lehetővé teszi, hogy adott hangolás és titkos kulcs esetén meghatározzuk, hogy mekkora jelöltszám elegendő a sikeres töréshez.

A továbbfejlesztett idő alapú támadási módszer elméletileg alkalmas minden olyan algoritmus vizsgálatára, amelynek a titkos kulccsal végzett művelete a kulcs bitjeitől egyenként függő elágazást tartalmaz (a legtöbb moduláris gyorshatványozó módszer ilyen). Modellünk számos továbbfejlesztési lehetőséget tartalmaz.

Az előadásban a kifejlesztett időalapú támadási módszert egy konkrét algoritmus, az RSA esetében mutatjuk be, valamint bemutatjuk a segítségével elért eredményeket. A tárgyalt módszer elméleti hátterével kapcsolatban további információkat tartalmaz „Kriptográfiai algoritmusok implementációfüggő támadása" című cikkünk.

Helyi hálózatok biztonsági kérdései

Ács György <gacs@cisco.com>
Cisco Systems Magyarország Kft.

Az előadáson bemutatom, hogy a helyi hálózatokon milyen biztonsági sérülékenységek fordulnak elő, és hogyan lehet ellenük védekezni. A helyi hálózatokban használt hálózati berendezések, eszközök (ethernet kapcsolók, rádiós hozzáférési pontok) biztonsági szolgáltatásaival is foglalkozik az előadás. Az előadás segít megvédeni a hálózatok eme igen fontos részét. Bemutatjuk a Cisco Systems által kifejlesztett új, önmagát védő hálózatbiztonsági megközelítést.

A Spam jogi szabályozása

Dósa Imre dr. <dosa@jak.ppke.hu>
ONYF

1. A kéretlen reklámlevelek meghatározása a hatályos magyar jogi szabályozásban
2 .A reklám jelleg meghatározása
3.Az opt-in módszer alkalmazásának gyakorlata
4.A jogkövetkezmények
5.A védelmi intézkedések törvényessége
6.Csatlakozási újdonság

A Spam-ek – szabatos jogi szakkifejezéssel: kéretlen reklámlevelek – nem kevés bosszúságot, feladatot adnak mind az Internet felhasználóinak, mind a szolgáltatóknak. Az előadás a Spam elleni küzdelem jogi hátterének alapjait tekinti át.
A kéretlen reklámlevelek a hazai szabályozásának alapját az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény teremtette meg. A jogalkalmazás során fontos, hogy a levél taralma mikor minősíthető reklámcélúnak. Erre a kérdésre a gazdasági reklámtevékenységről szóló 1997. évi LVIII. törvény szabályai adnak választ. A törvények értelmezésével sajátos gyakorlat kialakulásának lehetünk tanúi. A reklámozók gyakran önkényesen értelmezik a reklám fogadása iránti szándék kifejeződését. A felhasználók is értelmezik a jogot. Számukra a védelmi intézkedések hatékonysága és törvényessége fontos. A szabályozási újdonságok felvillantása sem mellőzhető: az uniós csatlakozástól hatályos a „szabályozott szakmák" joganyaga.

Jogi felelősség az Internet szolgáltatásaiban

Dósa Imre dr. <dosa@jak.ppke.hu>
ONYF

1. A joghatóság problémái
2. Hárompólusú jogviszony
    a. Szerződéses kötelezettségek
    b. Szabályzatok, általános szerződési feltételek
    c. Szolgáltató felelőssége harmadik személyek tevékenységéért
3. Felelősség a tartalomszolgáltatásért
    a. A tartalom ura
    b. Fellépés a szolgáltató nevében
    c. E-mail tartalom vizsgálata, szűrése
4. A szolgáltató együttműködési kötelezettsége
5. Büntetőjog

Az előadás az Internet szolgáltatás nyújtása kapcsán kialakuló – általában hárompólusú – jogviszony felelősségi alakzatait igyekszik körbejárni. A szerződéses kötelezettségekből adódó felelősségek, a szolgáltatás minőségének harmadik személyektől való függése, az általános szerződési feltételek, belső szabályozások szerepe sajátos belső felelősségi viszonyokra vezet. Példaként elegendő olyan vírusos e-mail károkozására utalni, amely komoly károkat okozhat, a címzett felelőssége pedig alig mutatható ki.

A tartalomszolgáltatásért való felelősség kérdései is bonyolultak. Nyilvánvalóan kerülendő a szolgáltatói cenzúra, de hasonlóan nyilvánvaló a sérelmet szenvedettek kiszolgáltatottságának csökkentése is. A felelősségek meghatározása során személyiségvédelmi és adatvédelmi szempontokra is figyelemmel kell lenni. A felelősségi alakzatok szélsőséges eseteiben a büntetőjog védőernyőjét is ki kell terjeszteni.

MIT NYÚJTUNK AZ AKADÉMIAI KÖZÖSSÉGNEK? SZPONZOROK PLENÁRIS FÓRUMA

A nyilvános, intézményi és otthoni kommunikációs alkalmazások egységesítésének legújabb koncepciója

Szüllő Zsolt <zsolt.szullo@siemens.com>
Siemens Rt.

A koncepció lényege
Az első generációs IP megoldásoknál (1gIP) az alközponti beszéd és adathálózatot IP alapú közös hálózattá vonjuk össze. A hálózat méretei általában behatároltak. (LAN, campus). A 2gIP megoldás egyrészt kiterjeszti a hálózat lehetséges méreteit (WAN) függetlenül az átviteli közegtől, hálózati szolgáltatásokat képes nyújtani (Centrex), továbbá biztosítja a felhasználók multimédiás elérhetőségét függetlenül az éppen aktuális access megoldástól és hálózattól (mobil, vagy vezetékes szélessávú csatlakozás).
A LifeWorks koncepció Hosted HiPath megoldásainak lényege, hogy elősegítse a mobil munkavégzés hatékonyságát, a kommunikációs rendszer (HiPath kommunikációs alközpont) szolgáltatásait a vállalati környezeten túl elérhetővé tegye nyilvános hálózati szinten is, a Surpass hiQ–n keresztül a nyilvános felhasználó számára is. A szolgáltatások menedzselhetősége azt biztosítja, hogy ezzel a vállalati kommunikációs funkciók nemcsak a vállalat, hanem nyilvános hozzáférésen is elérhetők. A felhasználó nyílt interfészen keresztül képes szolgáltatásait saját igényei szerint testre szabni.
Összefoglalva: a Hosted HiPath megoldásai egyesítik tehát a vállalati hálózat PBX előnyeit a nyilvános hálózat Centrex szolgáltatás kényelmével. A Siemens Hosted HiPath koncepciójának lényege hogy elősegítse a munkavégzés hatékonyságát azáltal, hogy a vállalati környezetben használt kommunikációs szolgáltatásokat a vállalati környezeten túl elérhetővé tegye nyilvános szinten is.

A Cisco Hálózati Akadémia Program aktualitásai

Mátrai Balázs <bmatrai@cisco.com>
Cisco Systems Magyarország Kft.

A Programban a közismert hálózati tananyagok (CCNA vizsgára felkészítő 1-4 szemeszterek, CCNP vizsgára felkészítő 5-8 szemeszterek) mellett számos új, széles sálán mozgó informatikai tananyag jelent meg az elmúlt időszakban. Ezen új tananyagok közül vannak, amelyek szorosan kötődnek a hálózati témakörhöz (**Hang és adatkábelezés, Vezeték-nélküli hálózatok, Security**), azonban vannak olyanok is, amelyek más IT területekre terjed ki (**JAVA és UNIX alapok a SUN Microsystems-től, IT Alapok a HP-től**). Az előadásban áttekintjük a Program legújabb fejleményeit, különös tekintettel ezen, a Cisco Hálózati Akadémia Programban nemrég megjelent legújabb tananyagokra, tartalmi és oktatás-metodológiai szempontból egyaránt.

Költséghatékony sávszélesség növelés a Matáv IP hálózatában

Czinkóczky András <czinkoczky.andras@ln.matav.hu>
Matáv Rt. PKI Távközlésfejlesztési Intézet

A sávszélesség növekedése iránti igény a közeljövő egyik műszaki kihívása. A technológia fejlődése ma már lehetőséget nyújt a megfelelő sebességű hálózat kialakítására, azonban maga a sávszélesség rendelkezésre állása önmagában nem jelent üzleti lehetőségeket. Ehhez új értéknövelt szolgáltatások bevezetésére van szükség, amelyek kiegészülnek új tartalmakkal és személyre szabott szolgáltatásokkal. Ennek kapcsán az IP hálózatokban az adatátvitel mellett megjelenik a beszéd és multimédia tartalom is (triple play), és az igény szerinti sávszélesség biztosításával a hálózati erőforrások kihasználtsága optimalizálható. Az IP hálózat alkalmas a szolgáltatások integrálására, ez a lehetőség fogalmazódik meg a szolgáltatóknál és gyártóknál napjainkban előtérbe kerülő NGN elképzelésekben.

A távközlési szolgáltatók egyik problémája a gyors változások kezelése. Kérdés, hogy melyek azok az alkalmazható technológiák, amelyekkel a szolgáltatók képesek lehetnek a folyamatosan növekvő sávszélesség igényeket kielégíteni. Persze mindezt a kapacitások megfelelő kihasználtságával, biztonságos és költséghatékonyan kiépíthető hálózaton szeretnék megvalósítani. Az előadásban ezt a kérdéskört vizsgáljuk, bemutatva a Matáv Rt. IP maghálózatában alkalmazott technológiákat és a benne rejlő lehetőségeket.

A Gigabit Ethernet technológiának fontos szerepe van a Matáv IP hálózatának kialakításában. Ennek alkalmazásával nagy sávszélesség biztosítható fajlagosan olcsón, különösen akkor, ha a routerek összekapcsolására kapcsolt Ethernet technológiát alkalmazunk. A Gigabit Ethernet átvitel az áthidalandó távolságtól függően többféle médiumon megvalósítható (pl. sötét szál, WDM, SDH), így akár helyi hálózati, akár gerinchálózati technológiaként alkalmazható. A közeljövőben a hozzáférési hálózatba is bekerülve, a Gigabit Ethernet technológia fokozatosan át fogja venni az ATM jelenlegi szerepét az ADSL előfizetők forgalmának aggregálásában is. Ezzel lehetővé válik a nagyobb sávszélesség nyújtása a hozzáférési hálózatban is.
A processzor technológia fejlődésével a 2.rétegbeli kapcsolók számára ma már a korábbi évekénél erősebb vezérlők használatával az Ethernet kapcsolók IP és MPLS képességekkel ruházhatók fel, lehetőséget adva arra, hogy a 2.rétegbeli kapcsolt hálózat jelentős költségmegtakarítás mellett MPLS hálózattá legyen alakítható. Ez a képesség lehetővé teszi a hálózat könnyebb tervezhetőségét és üzemeltethetőségét a forgalom lebonyolító képesség növekedése mellett. Az IP/MPLS képesség bevezetésével és pont-pont VLAN-ok kialakításával a hálózati hurkok elkerülhetők és a hálózat hibaesetekben való konvergenciája is gyorsabbá válik. A forgalom jövőbeli folyamatos növekedésére való felkészülés, a sávszélesség növelése a maghálózatban a 10 Gigabit Ethernet interfészek bevezetésével hatékonyan megoldható.

Kérdés továbbá az is, hogy az IP hálózat teljesíteni tudja-e majd az egyes alkalmazások által kívánt minőségi követelményeket, pl. a megfelelően kicsi késleltetést vagy csomagvesztést, garantált sávszélességet. A túlméretezéssel megvalósított „mindent egyforma minőségben" nyújtás helyett egyre inkább előtérbe kerül az eszközökben a ma már egyszerűen megvalósítható szolgáltatás differenciálás lehetősége. Az IP-hez hasonlóan az Ethernet hálózatrészekben is bevezethető a DiffServ architektúra, továbbá az Ethernet pont-multipont jellegét tekintve, illeszkedve a multicast-hoz, lehetővé teszi a TV műsorszórás bevezetését is.

GRID

Vitéz Gábor - Stefán Péter <vitezg@niif.hu, stefan@niif.hu>
NIIF Iroda

A gyakorlat legfontosabb célja a Magyar Clustergrid infrastruktúra szerkezetének, egy cluster telepítés folyamatának, valamint a felhasználói támogatás alapelveinek bemutatása.

1. ClusterGrid bevezetés
1.1. Az általános felépítés, a projekt története
1.2. Cluster erõforrások, a számítógépes laborok kettõs célja
1.3. A rétegezett modell
1.3.1. Fiziaki réteg
1.3.2. Kapcsolati réteg
1.3.3. Hálózati kapcsolati réteg
1.3.4. Operációs rendszer réteg
1.3.5. Erõforrás réteg
1.3.6. Grid réteg
1.3.7. Alkalmazási és feladat réteg

2. Egy cluster telepítése
2.1. Szerver konfiguráció
2.1.1. A szerver alap-funkciói
2.1.2. A grid erõforrás bróker
2.2. PC konfiguráció
2.3. Hálózati konfiguráció
2.4. A telepítés folyamata

3. A grid használata
3.1. Felhasználói és feladat azonosítás
3.2. A felhasználói körfolyamat
3.2.1. Szoftverfejlesztés
3.2.2. Párhuzamosítás
3.2.3. Portolás és fordítás
3.2.4. File átvitel
3.2.5. Feladatkezelés
3.3. A "jobdir" feladat-formátum
3.4. Hibakeresés

4. Jövõbeli elképzelések és kitûzött célok

IPv6

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda

1. IPv6 háttere és szükségessége
2. IPv6 alapvetõ tulajdonságai
3. IPv6 a felhasználó szemszögébõl
3.1. IPv6 Neighbor Discovery protocol (környezet felmérõ protokoll)
3.2. IPv6 host konfiguráció
4. IPv6 a hálózati rendszergazda szemszögébõl
4.1. IPv6 címigénylés
4.2. IPv6 DNS konfiguráció
4.3. IPv6 szerver konfiguráció
5. IPv6-os áttérés és IPv4-IPv6 együttmûködés
6. További referenciák az IPv6-al kapcsolatosan

Videokonferencia - Streaming

Kovács András <akov@niif.hu>
NIIF Iroda

Mi a videokonferencia?

- Videokonferencia történelem
- Videokonferencia definíció
- Videokonferencia vs. streaming: melyiket válasszam? Mi köze egymáshoz a két technológiának?

H.323 alapok:

- H.323 protokoll műszaki háttere
- H.323 hálózati elemek
- A hálózati elemek kommunikációja

Videokonferencia végberendezésekről általában:

- Legfontosabb végberendezés típusok
- Végberendezések műszaki paraméterei

NIIF videokonferencia szolgáltatás:

- Mi történt eddig?
- Gatekeeper hálózat, zónák, GDS kapcsolat
- MCU szolgáltatás
- További tervek a 2004-es évre
- Hálózatbiztonsági kérdések (H.323 és firewall)
- Etikett, elhelyezés, környezet

Streaming:

- NIIF Streaming szolgáltatás

Video on Demand archívum és E-learning

PKI, névtár és hitelesítés

Magyar Zsuzsanna <magyarzs@sztaki.hu>
MTA SZTAKI

Bajnok Kristóf <bajnokk@sztaki.hu>
MTA-Sztaki

Évezredek óta foglalkoztatja az embereket, hogy milyen módon lehet bizalmas információt átvinni az egyik helyről a másikra úgy, hogy illetéktelenek semmilyen módon ne férhessenek hozzá. A történelmi áttekintés helyett azonban a tutoriál során a jelenkor követelményeivel és technológiai lehetőségeivel fogunk foglalkozni.
Bevezetésképpen összehasonlítjuk a különböző titkosítási eljárások (szimmetrikus és aszimmetrikus kriptográfia) előnyeit és hátrányait, és azokat a problémákat, amelyek megoldása megbízható harmadik fél közreműködését igényli.
A Publikus Kulcsú Infrastruktúra (PKI) részleteit számos különböző szabvány írja le: X.509, PKCS, stb. Az ezekkel történő közelebbi ismerkedéshez az OpenSSL programcsomag segítségét vesszük igénybe.
Az előadás második részében a PKI elméleti és gyakorlati részletei kerülnek ismertetésre. Szó lesz a névtárról, amely lényeges eleme az infrastruktúrának, hiszen a legtöbb PKI megoldás feltételezi egy elérhető névtár szolgáltatás működését. Az LDAP azonban nem csak a tanúsítványok tárolását teszi lehetővé, de ezen alapulhat a tanúsítványok hitelességének és érvényességének ellenőrzése is.
A harmadik részben tanúsítvány alapú autentikációval (ezen belül is a kliens-oldali autentikációval), valamint az autorizációval foglalkozunk. Bemutatjuk az IETF PKI munkacsoportjának (PKIX) Privilege Management Infrastructure modelljét, valamint a névtárból történő, tanúsítvány-alapú autentikációt és autorizációt.

Spanning Tree Protocol

Jákó András <goya@eik.bme.hu>
BME EISZK

A legtöbb Ethernet hálózaton, így szinte minden lokális hálózaton működik a Spanning Tree Protocol. Ennek ellenére a hálózatok adminisztrátorai általában igen keveset tudnak róla. Legtöbbjük számára a Spanning Tree Protocol egy olyan dolog, ami „van, és magától működik". Az ismeretek hiánya viszont azt eredményezi, amit sajnos számos példa is igazol világszerte, hogy gyakran ugyan működik a hálózat, de – a nem ismert lehetőségek kihasználásának hiányában – nem olyan jól, mint ahogy működhetne. Más esetekben pedig – a Spanning Tree Protocol helytelen használatából adódóan – súlyos hibák keletkeznek, és ezek következtében a hálózat működésképtelenné válik, néha teljesen össze is omlik.
Az előadás ezeket a hiányosságokat próbálja pótolni: részletesen ismerteti az Ethernet hálózatokon használatos Spanning Tree algoritmus és protokoll működését, valamint használatának módját. Szó lesz benne az Ethernet bridge-ek és switchek működéséről; az IEEE 802.1d szabványában leírt Spanning Tree protokollról; annak bizonyos nem szabványos, de több gyártó által implementált kiegészítéseiről; valamint az újabb, szabványos kiegészítésekről, nevezetesen a 802.1w (Rapid Reconfiguration) és a 802.1s (Multiple Spanning Trees) dokumentumokban leírt módszerekről.

Netfilter alapú tűzfalak elméletben és gyakorlatban

Kadlecsik József <kadlec@sunserv.kfki.hu>
KFKI RMKI SZHK

A tutorial betekintést nyújt a Linux 2.4/2.6-os kernel netfilter alrendszerének szerkezetébe és működésébe. Áttekintjük a legfontosabb csomag-egyezési feltételeket és cselekvéseket, amelyekkel a csomagok kiválaszthatók és a sorsuk meghatározható, valamint a gyakran előforduló szűrési, címfordítási és csomag-módosítási eseteket. Kitérünk a patch-o-matic-ot leváltó patch-o-matic-ng és updates rendszerekre valamint az aktív fejlesztési irányokra. Röviden bemutatunk néhány szabály-generátor rendszert.

Abstracts

HIGH SPEED NATIONAL AND INTERNATIONAL INTERNET, NETWORK TECHNOLOGIES AND DEVELOPMENTS

NIIF IPv6 project

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda

Kovács András <akov@niif.hu>
NIIF Iroda

Máray Tamás <maray@niif.hu>
NIIF Iroda

We are planning to present the topology of the NIIF IPv6 network, our experiments and results. In the year of 2003 and beginning of 2004 based on the results gained from the separate but native IPv6 network infrastructure, we started to build the dual-stack IPv4-IPv6 network with the HBONE project together. To attract the users we tested several IPv6 applications including videoconferencing and multimedia gaming. We will explain the challenges we faced when we started to build the dual-stack IPv6-IPv4 network. The presentation will also cover the IPv6 services in the World and in Europe and the motivations behind the IPv6 services.

Quality management of IP networks

Zsiga Árpád <arpad.zsiga@siemens.com>
Siemens Rt.

Újvári Tibor <tibor.ujvari@siemens.com>
Siemens Rt.

This paper describes measuring methods of IP network quality, and presents some results. The results are measured by NetCheck quality management system, developed by Siemens Rt.
We discuss the active and passive methods of the network quality management, the SNMP protocol and the measured QoS parameters.
We show the advantages of the managed network, compare the service activity at managed and unmanaged networks and show the NetCheck generated SLA alarms.
This presentation discusses the QoS measuring methods for IP networks and illustrates them showing some measuring examples.
The QoS measuring techniques are based on active and passive measurements, and often all the two methods are based on the SNMP control. The device of the measurements may be separated measuring equipment or the network element device itself.
The configuration data is collected by an automatic network discovery algorithm, which maintains the element list, the IP addresses, interfaces with actual working status, the routing table contents, and the working software versions.
The quality parameters are collected continuously, stored, analysed, and by the analysis' results alarms are generated. The alarms can be ordered to a single quality parameter, or to the availability of the quality parameter group listed in the Service Level Agreement. The trend alarm is generated if the SLA account overflow is predictable.
The paper presents some measuring examples from the most important cases of the network management. The examples have been measured with the NetCheck measuring tool developed by Siemens Rt.

The presented tool is available to serve as continuous network quality management tool or network quality audit tool for a time interval.
At the Siemens NetCheck Basic service Siemens makes first installation and configuration, and the customer has unlimited access right to use it.
The Siemens NetCheck Network Operation service gives trend analysing reports periodically and performance alarms when the measured network parameters are not acceptable.
The Siemens NetCheck Network Monitoring service gives performance reports periodically and error analysis and advice to avoid network degradation.
The Siemens NetCheck audit is an overall network quality status report and advice to repair the problems.
In the last part we present some interesting parts of NetCheck reports.

Enhancement for mobile multicast protocols in IPv6 networks

Kovácsházi Zsolt <kz365@hszk.bme.hu>
BME

Kis Zoltán Lajos <kz345@hszk.bme.hu>
BME

Kersch Péter <kpeti@sch.bme.hu>
BME

Simon Csaba <simon@david.tmit.bme.hu>
BME

Internet based broadcasting, phone- and videoconferences and many other applications are based on multicasting that let us preserve a notable amount of bandwidth compared to unicast applications. As mobile equipment and applications gain momentum, the need of multicast applications in mobile environment raises. Mobile IPv6 emerged as a widely accepted solution for mobility support in IPv6 networks. However, Mobile IPv6 deals with unicast traffic only.
In research communities mainly two different approaches are proposed for multicast: *bidirectional tunnelling*, and *remote subscription*. In *bidirectional tunnelling* a mobile host joins every multicast group via its home agent using IPv6 tunneling. Thus, the home agent can become a bottleneck. Also bandwidth-usage and routing will not be optimal, because tunnelling is based on unicast.
In *remote subscription* the mobile host uses the multicast routers of the foreign network, just like any fix hosts of that network. This makes bandwidth and routing optimal, however it requires the reconstruction of the multicast tree. Therefore the time between entering a new network, and the multicast data reaching the mobile host is too much for a seamless handover. Due to the optimal resource usage, we have chosen the remote subscription approach as the basis of our further research.

There are numerous proposals to deal with the disadvantages of these multicast approaches, relying on the fast handover schemes developed for unicast mobility. We introduce an enhancement of the remote subscription approach, that makes seamless handover of multicast data flows possible. This method makes the tree build faster by by-passing MLD timers, and it utilises temporary tunnels to deal with packet losses. Our extension is transparent to the multicast routers in the network, thus maintains network scalability and lowers the costs of deployment.

Handovers are initiated by mobile hosts. In our implementation this can be done both manually (using a GUI) and automatically based on the best signal to noise ratio of the access points. During handovers a temporary tunnel will be built up between the previous and new access points to provide the necessary data flows till the new multicast branches are created.

We measured the parameters of WLAN to WLAN handovers. Our results show that there were no

packet losses, and packet-delay rose only by the acceptable propagation delay caused by the tunnel during handovers.

We also measured inter-technology handovers, both WLAN to GPRS and GPRS to WLAN. Not taking the low bandwidth and high packet-delay caused by the GPRS network into count, we managed to make handovers 'seamless' here as well.

Our results prove that the implemented protocol makes seamless handovers possible. Thus it helps create better quality and more reliable services possible, while conserving bandwidth.

International outlook

Bálint Lajos, PhD. <h48bal@helka.iif.hu>
NIIF Iroda

The broad range of international relations of the NIIF Program is briefly investigated by the contribution. Special emphasis is put on GN1, the project devoted to the development of the GEANT network, and to GN2, the new project taking over from late 2004 the activities started within the frameworks of the GN1 to be closed before the end of this year. As far as the activities of TERENA are concerned, the presentation concentrates at the final results of the recently completed SERENATE project. Several further important elements of the international co-operation are also mentioned by keeping throughout in mind the results and opportunities in the field of international connectivity and multi-NREN collaboration as key aspects of the investigation. The main goal of the contribution is, on one hand, to draw the attention of the audience to the most important achievements within the relevant international organisations, and to the possibilities of further improving our fruitful and acknowledged international relations. Another aim of the presentation is to demonstrate how all these relations help the Hungarian academic and research institutions and individuals in enjoying all those benefits available for their scientific and education partners worldwide.

High Speed TCP protocols

Telbisz Ferenc <telbisz@sunserv.kfki.hu>
KFKI RMKI SzHK és MATÁV ŐKI-FI

Németh Vilmos <nemeth@ttt-atm.ttt.bme.hu>
Egyetemközi Távközlési és Informatikai Központ

Molnár Sándor dr. <molnar@tmit.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

Szabó Róbert dr. <robert.szabo@tmit.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

The operation and stability of Internet is highly depending on the flow control and congestion control of the Transmission Control Protocol (TCP). The protocol developed more than two decades ago is performing well at relatively slow speed with the generally used applications and it guarantees the reliable end-to-end transport of data in heterogeneous networks. Lately it turned out; however, that the traditional TCP protocol is not efficient at gigabit speeds if a large quantity of data should be transported to great distances.

Therefore a couple of Universities and Research Institutes started different projects for developing a new version of the TCP protocol. As the poor utilisation of the bandwidth by the TCP protocol is due to the limitations of the congestion control algorithm and to the strong feedback in case of packet loss, the new protocols want to eliminate the deficiencies of the TCP protocol by new congestion control algorithms. During these works several suggestions were made which may result in a new version of the TCP protocol still based on the unmodified present IP service. The experiments demonstrated the reality of reaching much higher speeds with the new versions.

A number of theoretical and practical questions are connected to the modification of the present well-known TCP protocol. Therefore the *Inter-University Centre for Telecommunications and Informatics* (ETIK) in co-operation with the *BUTE Department of Telecommunications and Media Informatics* and with the *MATÁV PKI-FI* started a project for studying the high-speed TCP protocols. The studies will investigate the throughput and interworking of the different TCP protocols, the modelling of their operation and traffic, development and implementations of these protocols as well as their investigation in experimental environment.
The presentation overviews the most recent directions in the development of high speed TCP protocols, it will compare the different solutions furthermore the goals and results of the Hungarian research in this area will also be presented.

Application of IPv6 in broadband access

Szabó Gábor <szabo.gabor@siemens.com>
Siemens Rt.

One of the possible Internet applications – which were often only a part of futuristic visions – is the home networking. This application will change the way people use Internet at home: the type of networked devices (set-top boxes, home appliances, sensors, cameras) and the direction of communication (within the home, from remote side to the home) will be extended. Broadband (and always-on) network access solutions and different wireless technologies enable home networking to turn to reality. Home networks are serious challenges for the present IPv4-based Internet and should be a strong driving force (together with 3G mobile devices) for IPv6 deployment.
The presentation explains the advantages of using IPv6 in home networks, demonstrates the different technical solutions to connect the home IPv6 island via broadband access to the public Internet and finally gives an overview of IPv6 implementation status of networking protocols and equipment.

LAN reconstruction at the Lágymányos campus of ELTE

Borosnyay Csaba <borosnyay.csaba@elte.hu>
ELTE Információtechnológiai Központ

The Lágymányos campus has three buildings, the oldest one was built in 1992 and the youngest one was finished in 2001. The LAN infrastructure of these buildings shows all trends and changes of network design conceptions of the last 12 years.

For the optimal usage of equipment, and under pressure of cost effectiveness we started the reconstruction in the "Northern" building built in 1998. The LAN is based on a cabling which suit the requirements of the CAT5E standard, so the task was reduced to changing of the aggregator switches and re-cabling the closets.

We aggregate approximately 1300 endpoints in six closets in the building. All of these closets had a modular system DECHUB switch. In four closets we changed these switches to, also modular

system, Catalyst switches and in the other two closets to desktop Catalyst switches.

At the same time, we modernised the backbone of the building too. The original concept was an ATM based system that we changed to a most scalable Gigabit Ethernet system.

With the help of the new switches we can give better services for the users and we took the first step towards a homogeneous network system in the entire university.

Control of Access to Enterprise Networks

Budai Károly <karoly_budai@hu.ibm.com>
IBM Magyarországi Kft.

Recently, the application of wireless network segments begun to spread widely. Among others, they exist in almost every university campus. The appearance of this solution is continuously challenging the access control of enterprise networks – mainly because it has become popular rapidly.

The purpose of this presentation is to give an overview of the most frequently used methods, which are able to provide as sophisticated control as possible for the protection of the networks in this new environment. It intends to give great emphasis to the investigation of tools, which are able to handle universally both the wired and the wireless network infrastructure.

INFORMATION SYSTEMS, INTRANET SERVICES

Central User Management in Campus Environment

Mogyorósi János <janos.mogyorosi@bkae.hu>
Budapesti Közgazdaságtudományi és Államigazgatási

Security Issues

- There is no user without authentication; there is no PC without responsible person
- PPP – Partitioning of Public and Protected applications
- Automation of Service Deployment

Management Issues

- Mass User Management
- Self management Interface for Users
- Multilayer Operator Interfaces

Central Services

- Managing of Address Book services, Dynamic Mail lists
- Common / Temporary Disk spaces, and Rooming User Disk spaces
- Maintenance of Windows Rooming Profiles, Terminal Servers, and Group Policy
- Managing Emails, Dynamic Mail Lists, Telnet / Ftp / Web access, Dialing services

System Architecture

- Campus Management XML Interface
- Java / Web User Interfaces
- Central Oracle User Database

- Multilayer application architecture, Message Broker
- Output: LDAP, Active Directory. TACACS, authentication databases

Managing experiences

Next steps of development

Electronic informational and registry system for the Doctor School's young researchers

Adamkó Attila <adamkoa@inf.unideb.hu>
Debreceni Egyetem

The young researchers, who are really interested people and possess a lot of new ideas and inspirations, have always taken a prominent part in the scientific life on their careers. Doctoral schools and project leaders help them in their postgraduate studies and researches. However, we have less information about what kind of scientific researches really go on in doctoral schools and what fields of research are these young entrants involved in.

Our purpose with the development of this information system is to make the basic information available to a wider public even via the Internet. The main objective of the development is to create an Internet accessible database containing information about doctoral schools, at both regional and national level (DOSZ, OM- Ministry of Education, www.phd.hu, competition possibilities, etc.), moreover, to provide a possibility of obtaining scientific documents (articles, publications, etc.).

In my lecture I would like to present this electronic information and registry system including the models, technologies, systems and tools (cf. sever-client, session management, web-based admin surface, XHTML, XML, SQL, perl, DBI, PostgreSQL, Apache) used during the development and their cooperation and relationship with NEPTUN system as well.

Management of thick clients in Tivoli environment

Orosz Péter <oroszp@delfin.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

The integration of the solid computer park working in the Service Center for Informatics of University of Debrecen reached the phase of implementation in the nation-wide cluster GRID project. The 160 workstations with identical hardware and software configuration were installed at different campuses of the University. These workstations have dual functions, daytime they serve the students, while night-time they connect to the nation-wide GRID network. For the management of daytime operation administrators often go on the spot, and it takes a lot of time to travel between campuses witch is quite difficult to ensure. A centralised management of the daytime operation of the clients is needed. Several software packages are on the market for thin clients that allow to use as well as to manage the clients in a totally different way.

Question is raised, which may mean serious changes in the operational work: Is there any complex software pack for thick clients ensuring centralised management? The answer is yes.

Several software companies (HP, Enterasys, IBM, SUN) provide software solutions for this purpose. From the mentioned solutions Service Center for Informatics became acquainted with IBM Tivoli management software. Currently 40 workstations in the centre were joined in the test operation. For experimental purpose three modules of Tivoli were installed previously: Tivoli Infrastructure (framework), Remote Control,

Configuration Manager. Using these modules, a high level of automation can be reached in software distribution and enterprise-level hardware and software inventories. SQL based relational databases help tracking and registering the system processes. Furthermore, the package ensures time-saving remote assistance for clients, so administrators can easily avoid on-the-spot problem solutions.

The discourse reviews the experiences gained during the test operation, details the possibilities, technical solutions, operation of each Tivoli module, the latter in heterogeneous environment. The presented experiences give assistance to other institutes in enhancement of the efficiency of system management.

Analysis of resource utilisation of the Neptun system

Faragó Zsuzsa <zsuzsa@delfin.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

At the University of Debrecen with 14 faculties and faculty-level institutes an up-to-date information system for student registration was needed to be introduced. Similarly to other high-level educational institutes, our university took a stand on deploying the student registry system named Neptun. The Service Centre for IT is responsible to provide operational conditions on hardware and operating system level, and to develop hardware and software elements of the operational environment. Oracle Client and MS Sql Server are running on four terminal servers and one database server, all of them based on Windows 2000 Server operating system.

The inhomogeneous but trend-characterised system load coming from the utilisation makes a rigorous, intensive monitoring task necessary. Because of the high number of day by day users, 26 thousand students and 35 hundred teachers, the Neptun system must have a very high confidence level and continuous availability similar to telephone service. Therefore the Service Center of Informatics continuously monitors and analyses the resource utilisation of the registry system: the CPU and network interfaces, furthermore, attacks against the Neptun firewall and the results of the traffic measurements of the backbone devices. MIB variables are evaluated by SNMP protocol, then ordered and processed by MRTG Management software. The sampled set of status information is processed with different sophisticated statistical tools.

The lecture discusses the usage level of the installed server-farm and the load of the network device resources. This helps to foretell the required development steps and their actualities and also to introduce the high performance operational techniques. We share the experiences gained during the analysis and give aid to other universities and colleges to simplify the optimisation of the daily operational processes of their local Neptun systems.

Conceptual and IT developments of the KFRTKF

Cserhátiné Vecsei Ildikó dr. <vecsei@kfrtkf.hu>
Kölcsey Ferenc Református Tanítóképző Főiskola

In the life of any institute of higher education it is always important to work out, to get across and, last but not least, to attain short and long term concepts. It is especially interesting to monitor what is happening in the field of IT developments.

In this presentation I would like to express on those important components, which touch the cardinal points of the above mentioned concepts. These are for instance: expansion of internal networks, distribution of the functions of different servers, fundamental changes in the services,

spreading out the culture of information technology, development of new inquiry centres, bringing up the physical and personal conditions for the development of new digital type curricula, software legalisation, etc.

From this list, it is clear that these concepts can not be assigned to a single department, but it should be a result of a collective thinking, planning and brain storming. Moreover the affirmation of the leaders of the institute and the quest for the possible financial sources are also indispensable.

LIBRARIES, ARCHIVES, MUSEUMS, CONTENT PROVIDERS

Information system in the new University Library of Szeged

Bakonyi Géza dr. <bakonyi@bibl.u-szeged.hu>
SZTE EGyetemi Könyvtár

Sándor Ákos <akos@bibl.u-szeged.hu>
SZTE Egyetemi Könyvtár

The University Library of Szeged moves to a new building in the summer of 2004. Besides the library the building, the area of which is more then 24 thousand square metres, it will house a conference centre, too. The area of the library is more then 14 thousand square metres. The wing of the stockrooms has six floors and the wing of the reading rooms has four floors (the 2 reading areas have galleries). Presumably, the number of visitors will be 4-5 thousand per day. The Library will begin to operate with nearly 500 PCs from among which 400 will serve patrons. There will be 1260 end points in the building. It comes from these numbers that the infrastructure of the information systems requires a very thorough planning and execution. Moreover, in this emphatically functional building the stress is not on the traditional library services but on the modern and complex services that are based both on traditional and automated tools, and on the Internet. The lecture will give a brief overview of the planning and implementing operations.

Image or map

Plihal Katalin <kplihal@oszk.hu>
Országos Széchenyi Könyvtár

Maps, especially old ones accessible on the Internet, are only displayed as images for users. What does this really mean?

- Determination of the map's scale cannot be done on the user's screen
- Direct index use belonging to a map is also impossible
- Due to the large size of a map, a user can consult only a small part of it at a time

What stands behind this? In all fields of information services the claim for online publications have been growing. The easiest way to meet this claim was to scan maps. This procedure resulted in predomination of raster maps on the Internet. These maps can, however, be only viewed. By default, the traditional browsers support only some image file formats (GIF, JPG, PNG). For more than viewing an old map, but also using its content interactively, it would need considerable

expenses for the hosts of the maps.
For this reason, we have the opinion that picture-like maps will be found on the World Wide Web for a fairly long time.

Problems in Constructing the Hungarian Hand Press Book Database

Hegyi Ádám <hegyi@mek.oszk.hu>
OSZK - SZTE BTK Könyvtártudományi Tanszék

In September 2003, the plans for a Hungarian Hand Press Book Database were outlined. In this presentation I am going to talk about the achievements we have made since.

Our first step was to acquire data through a nation-wide survey on how the participation in a central computer-based information system can be organised. Based on this survey we were able to assess what kind of bibliographical descriptions of books printed before 1850 exist, as well as to what extent computer technology has been made use of (such as MARC formats, digital archiving, etc.)

Parallel to this, a technical plan was also drawn up. Thus, being conscious of both our technical aims and the present state of affairs, a feasibility study can be completed at last.

For testing purposes the following libraries have joined the project:

University of Debrecen. University and National Library
The University Library of Eötvös Loránd University
The Ráday Library of the Danubian District of the Hungarian Reformed Church
Hungarian National Library
University of Szeged. University Library

Records are kept in XML format. A search screen belongs to the database as well as a data-entry sheet. Records can be entered and updated through the data entry sheet. Access to this is also Internet based.

We have no plans as of yet how each member library will transfer their own computerised data to the shared catalogue. This is to be decided after the testing period.

The database will actually come into existence only after - based on the feasibility study - the co-operation between the collections starts to develop.

Metadata service of Hungarian Electronic Library

Simon András <simon@lib.bkae.hu>
BKÁE EKK

Góczán Andrea <goczan@oszk.hu>
OSZK MEK osztály

The in 2004 ten years old Hungarian Electronic Library after two years of innovation has it's new service, the MEK2.1. Both the database and it's interface was developed, to become open to other systems, so it's metadata can be integrated into the services of other libraries. This solution was based on a bibliographic and data structure which compatible to the librarian cataloguing (MARC) and in the Internet used (Dublin Core) standards.
The using of Kistéka library automation system for MEK data search, is a good example for integration. The WEB based search interface of Kistéka fits well the environment of the Internet. The full text database of the Hungarian Electronic Library is especially useful to the Kistéka users,

the libraries of small collection , so it is very important them to be able to reach the MEK throughout their own OPAC interface.The Kistéka software is appropriate for MEK data service. As a MARC based system can adopt the data from the MEK easily, and the users can get to the full text records by the links built in the Kistéka database. The Kistéka is open for remote use and administration, so the MEK Kistéka is running on the server of the distributor, the MTA SZTAKI, it is updated daily, and can be used from everywhere, even from abroad.

Development of Distributed Library Systems by using Z39.50 and OAI protocols

Tóth Kornél <tothk@sztaki.hu>
MTA SZTAKI

First we will survey the main steps of the history of library automation. The focus will be on the development of library networks. After this, the most important Hungarian Union Catalogues will be reviewed and a short introduction will be given into the Z39.50 protocol, which is the technical basis of the present union catalogues. The practical application of the protocol in library systems will be shown as well. The demonstrated library systems will be *HunTéka* and *KisTéka* developed by MTA SZTAKI. As you can learn from the title, the main point of this lecture is to apprehend a temporal progress, so we will try to describe the future prospects of integration: how could be the libraries' online catalogues integrated on a higher level. The possible levels of the integration are:
Interoperability of online library systems;
Interoperability of online library systems and other public collections, like museums and archives;
Interoperability of public collections and other data sources found anywhere on the Web.
In our opinion the most effective way to achieve a higher level of integration is the adoption of OAI (Open Archives Initiative) and DC (Dublin Core) protocols in the systems used by public collections. MTA SZTAKI wants to help public collections to reach this goal in two ways: on the one hand an OAI server has been installed, on the other hand we prepare our library systems to be able to connect to this OAI server.

EPrints: an XML Preprint Archive in Hungarian

Csirmaz László <csirmaz@ceu.hu>
Közép Európai Egyetem

Keeping papers, manuscripts and preprints up-to-date, and producing publication lists on a short date is an important task universities and higher educational institutions face. Among several preprint archiving systems available, CEU has chosen the free GNU EPrints. EPrints is developed at the University of Southampton, UK. In the lecture, I will discuss its philosophy, structure, and usage. EPrints can be a useful tool in the dissemination of scientific works.

The problems of producing HUNMARC format from the content of items of non MARC based databases – HUNMARC records of XML format

Lengyel Monika <lmoni@sztaki.hu>
MTA SZTAKI

One of the most serious problems of the shared cataloguing systems as well as the changing of the library's older automation system to a new one is, the database migration, without mistakes and

data losses. The library automation systems developed for a few years should mainly be based on MARC format, and have to be able to take part shared cataloguing projects, so they have to export and import their items in MARC format too.

Most of the not MARC-based systems can create a (HUN)MARC data structure for record export. The problems are usually caused by the quality of the content of the database and the too large amount of the items. So the main questions are:

- How and from what can be the missing obligatory data produced?
- How an authority database can be built from a non-authority one, which was created non-authorised, and includes several mistyped items?
- How the faults caused by the insufficiency of the former system and the mistakes of the librarians can be corrected? (The data elements stored in the same data field should be separated, the wrongly recorded ones should be recognised and corrected.)
- Can the authority records exactly be joined to the bibliographic records?

To correct the bugs of the content of the records, there is a useful device for TINLIB – HUNTÉKA migration, the HUNMARC based XML format.
Most of the experiences of this paper are based on the experience of the cases of the TINLIB – HUNTÉKA migrations, and the problems of the HUNMARC export made for the MOKKA from the databases of Tinlib using libraries, but problems and their solutions are can be extrapolated to migrations from other systems (ISIS, TEXTÁR, SZIRÉN, SRLIB, DRLIB) too.

Content-based image retrieval from image archives – a possible solution

Veréb Krisztián <sparrow@inf.unideb.hu>
Debreceni Egyetem, Informatikai Intézet

A friend of mine has shown me a song in the last few weeks, which I liked a lot. A saw her takes the CD out of the box and put into the hi-fi system. I didn't really pay attention on what she told me about the singer. I only memorised the melody itself and the look of the cover. A couple of weeks later I was in a CD-shop and it occurred to me that I should buy that CD. At this point I realised that I haven't got any important information concerning the author or the title of the album. All I could determine was the category (genre). Had I seen the cover, I may have been able to recognise it. I started to look for it but it seemed an impossible task to scan more than five thousand CDs. Having a database system being able to find the singer of the CD based on describing the cover, I could have finished in a few minutes. I shouldn't have been roaming for hours among the never-ending corridors of the shelves full of CD covers.

The bases and the approaches needed to reach the archive with image retrieval algorithms – solving the above-mentioned problems – were already shown in may presentation *„Content-based image retrieval from image archives – where are we?"* in NWS 2003, Pécs. This presentation – continuing the previously mentioned one – is trying to introduce the applied techniques through an implemented existing complex archive containing covers of musical CDs and extra information.

The database enables textual search among CDs and the query based on images as well. (Using the features of the Oracle9*i* *inter*Media.) A self-developed technique makes it possible to ask complex questions based on image parts. The used pre-classification (as a semantic index) grouping the motives of the CD covers accelerates the searching by reducing the number of the comparisons to be executed. The „engine" given this way is an assembled unit of the operating versions of the retrieval techniques mentioned in NWS 2003.
Beyond the technical parameters and the operation of the system, I give a number of examples in my presentation, showing the abilities of the system and compare them to other existing systems as well.

The topic map of WebKat.hu

Ignéczi Lilla <lilla@neumann-haz.hu>
Neumann Kht.

Boros Andrea <andreab@neumann-haz.hu>
Neumann Kht.

In 1999 we decided to create and integrate a new thesaurus into our existing web catalogue. In October 2000 we started to process materials using this new thesaurus-like module which was based on the UDC system.

In the spring of 2002 we realised that we need to change our approach: while the main aim in 1999 was to create a new thesaurus, the experience of processing materials using the system brought a lot of experience, and we found that the OLIB thesaurus module has many limitations. We had to find an answer to the question: can we call our scheme a thesaurus at all when we can create only a few, limited relations between the items? As a result of a full investigation we rearranged the whole structure of our scheme: we highlighted the 9 top-level categories.

This work laid the basis for and served at the same time as a preparation for starting in 2003 another development project which ad been urged by international trends and user needs: We created a new visual interface for our thesaurus, a topic map. We offer this topic map on our homepage as an alternative interface to our catalogue, but we kept the old thematic search functions as well.

From information service to content providing – the present and future of Libinfo

Tóth Ferenc Tibor <ftoth@oszk.hu>
OSZK

Iványi Kristóf <ivanyik@oszk.hu>
OSZK

Libinfo, the joint information service of Hungarian libraries, launched its new homepage in June 2003 (with financial backing from the Ministry of Cultural Heritage), which introduced, along with graphical changes, a completely new version of operation built on the framework of the previous system. The new version comprises of two essential changes: primarily, a switch to an entirely web based operation, whereby the process of providing answers is conducted through the Internet, and secondly, a new system of database service, which enables Libinfo to contribute to Internet content through its on-line reference service, its catalogued link collection and its indexed archive of Internet web pages. The upgraded version also provides Libinfo the means to participate more and more in the digital document providing network. These features conform to the strategic plans of the National Széchényi Library, which acts as moderator and co-ordinator to the service.
Our presentation aims to introduce the new system of operation and to outline our plans for future development.

ZING: The new generation of Z39.50

Horváth Ádám <adam@oszk.hu>
Országos Széchényi Könyvtár

ZING, "Z39.50-International: Next Generation", covers a number of initiatives by Z39.50 implementers to make the intellectual/semantic content of Z39.50 more broadly available and to make Z39.50 more attractive to information providers, developers, vendors, and users, by lowering the barriers to implementation while preserving the existing intellectual contributions of Z39.50 that have accumulated over nearly 20 years.
The National Széchényi Library within the framework of ITEM has started to develop a ZING client. In my paper I would like to present our results as well as the SRW "Search/Retrieve Web Service" and CQL "Common Query Language" initiatives of ZING.

Unified environment for services: developing library portals

Pataki Gábor <gabor@oszk.hu>
Országos Széchényi Könyvtár

Bánki Zsolt <bazso@oszk.hu>
Országos Széchényi Könyvtár

The continuous changing of the means of information technology (which may sound trite today) is a challenge for the institutions conveying human knowledge, especially for libraries.

These changes trigger the formation of information islands. It is easy for the user to get lost in this archipelago. It is the task of the institutions and libraries involved in information exchange to organize these islands into a coherent system.
Currently the usual case is that the library homepage, the OPAC and access to electronic documents are separate services, and so is the use of digital resources. Our paper aims to demonstrate the application of tools serving integration in the activities of the NSZL, including research, test and development.

The main point of the new information interfaces is that they organize the heterogeneous possibilities of usage into a unique, customized, structured and safe system, thus helping orientation according to the different objectives of applications, functionally differentiating between the user appearing in the library and the user accessing the resources through the web. It has to incorporate the functions of the homepage, the readers' terminal and the Z39.50 gateway, satisfying the demands of the two groups of users.
The advantages of this approach for the user are: easier access to the relevant information, the immediate access to the means integrated into the system and the highly efficient usage of the capacity of the staff and the available technological equipment.

Developing Electronic Periodical Archives and Database in the Hungarian National Library's Hungarian Electronic Library Department: EPA 2.0

Csáki Zoltán <csaki@mek.oszk.hu>
OSZK MEK

The Electronic Periodical Archives and Database (EPA) is an online service which archives all the Hungarian-related e-periodicals having significance in the field of academic research and culture

and are available to the public. EPA provides long-term access, storage, infrastructure, user interface and full text search.
Furthermore EPA includes a bibliographical database which collects metadata of all the Hungarian-related online and offline e-periodicals. The database is searchable online in a simple and detailed way (advanced search) and provides metadata in HUNMARC and DC format.
Future plans include a database of articles based on the archived sources processed with the help of XML technology. At the same time we are planning to co-operate with the MATARKA service (Hungarian table of contents service) to link our full text articles to their tables of contents.

Sharing Metadata Schemas on the Basis of the Semantic Web

Fülöp Csaba <csabi@dsd.sztaki.hu>
MTA SZTAKI

Kovács László <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

Micsik András <micsik@dsd.sztaki.hu>
MTA SZTAKI

The ability to semantically relate various data and metadata is a basic criterion of the Semantic Web concept. The most obvious and most urgent subtask in this area is to share and align metadata schemas used in digital libraries, collections and databases. As a result of international research activities, an RDF based framework is evolving which provides a common metadata schema definition format and the possibility to reuse existing schemas and schema elements.

The Department of Distributed Systems of MTA SZTAKI tries to introduce these results in Hungary. We are planning to implement an open web service for the registration of metadata schemas used in Hungary. This service could provide an overview of the registered schemas and their interconnections. It could also support the creation of new schemas using elements also from existing schemas. Such service could facilitate the reuse and standardization of metadata schemas, which is of public utility, as it can make data management and data retrieval more economical.

HEKTÁR: Interconnecting Hungarian Digital Libraries

Kiss Gergő <gege@dsd.sztaki.hu>
MTA SZTAKI

Kovács László <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

Micsik András <micsik@dsd.sztaki.hu>
MTA SZTAKI

Moldován István <moldovan@oszk.hu>
OSZK

HEKTÁR is a current project funded by ITEM with the participation of the Department of Distributed Systems of MTA SZTAKI and the National Széchenyi Library. The project aims at interconnecting several digital libraries based on the recommendations of the Open Archives

Initiative (OAI). OAI defines two basic terms: the data provider and the service provider. A data provider exposes its metadata to the public through the OAI-PMH protocol. A service provider uses metadata harvested via the OAI-PMH protocol as a basis for building value-added services.

Within this project MTA SZTAKI will implement an open source reference implementation for the OAI-PMH protocol, and will apply this software for the Hungarian Electronic Library (MEK) as data provider. We will also implement and operate an example for a service provider. There are numerous technical advantages of using OAI, and additionally it places data providers on a much wider global scope as the member of the dynamically growing OAI community. Therefore, we try to spread the use of OAI and accompanying technologies (e.g. Dublin Core) among Hungarian digital libraries.

Examining standardisation possibilities in NDSS

Dávid Boglárka <bdavid@lib.unideb.hu>
Debreceni Egyetem Egyetemi és Nemzeti Könyvtár

Molnár Sándor Gábor <molnarsg@lib.unideb.hu>
Debrecen Egyetem Egyetemi és Nemzeti Könyvtár

The new ODR (NDSS – National Document Supply System) and the ILL records of the University and National Library of Debrecen launched on October 1st, 2003 have been working successfully: the number of requests handled has grown significantly. The next development steps should be taken in accordance with the existing library and computer standards. The presentation examines in what areas of the NDSS and ILL could different standards and rules (e.g. Z39.50; ISO/ILL 10160, 10161-1, 10161-2) be used contributing to better co-operation of libraries and common development in the future.

The technical background of MOKKA – record upload

Balázs László <lbalazs@lib.unideb.hu>
Debreceni Egyetem Egyetemi és Nemzeti Könyvtár

The Corvina integrated library system functions are excellent for the MOKKA system, especially for the union catalogue model where cataloguing is performed at the local catalogue level. The record upload is an on-line process completed by a Java program. The uploaded records are checked by the system and, if they are found ok, uploaded to the catalogue. All the processes are logged and the logs are supervised by the record sender. The presentation is about the reasons why the system denies the upload of some records, the location of the missing records, why hundred thousands of records don't upload, and why the authority records should upload first. Last but not least we can hear about the new developments of the project.

Digital archives

Dicse Jenő <dicse.jeno@synergon.hu>
Synergon Informatika Rt.

Organisations produce lots of information as part of their work and get plenty of them from others.

This vast information set is stored in different places: on paper, on PC-s, tapes and so on, and in different formats within these places. Surely there are – or there were – several registry systems for handling this problem. The navigation within these systems, the maintenance of storage and satisfying the search criteria are hard tasks to fulfil. Modern digital archives mostly solve these problems, transforming the information-flow to an easily usable data wealth. Digital archives not only mean a new kind of structuring, ordering and storing system. In many times it worth considering them as a new, real revenue source.

Unified museum filing system project (MNyR)

Veres Gábor <gabor.veres@nkom.gov.hu>
NKÖM

Molnár László <lmolnar@freesoft.hu>
Freesoft Kft

The change of the Ministry Order No. 20/2002 (X. 4) and related „Information on the IT requirements of the museological institutes computer systems" made it possible for the Hungarian Museums to use IT systems as their official filing system providing they apply the required security regulations.
These regulations set strict requirements towards the systems, administrative procedures and regulations applied.
To help the museums use the new opportunity, the Ministry decided to develop the Integrated Filing System for Museums, a software which indulges each museological area's special needs. After completion of the system, all Hungarian museums will have the right to use the it free of charge.
The project includes development of the software, installation and testing in 4 pilot museums, and other services (eg. Helpdesk) for at least 5 years. The development and implementation period will end in March-April 2004.
The presentation covers the project, conditions of the software rollout and a brief demonstration of the software itself

EDUCATIONAL NETWORK APPLICATIONS, E-LEARNING

Teaching Experience of E-learning Based Courses at the Central European University

Balogh Anikó <balogha@ceu.hu>
CEU

E-learning based teaching started in the academic year of 2003/2004 in the Computer & Statistics Center of the university. After weighing the pros and contras, the center has chosen the online WebCT framework to present the material of the popular Webpage Creation course to the students.

There was a big interest towards the course among the students and staff. About 130 people signed up for the course so the course started in four groups, with about 30 participants per group.

In my presentation I would like to talk about the following topics:

- The students' previous IT experience, their e-learning abilities
- Specialities of the framework
- Course material
- Sending, checking and grading the assignments
- Following the students' work
- Help and feedback possibilities
- Teacher-student, student-student communication, real time chat

Finally I am going to give an overview of the future perspectives in course material development and the possibilities of cooperation with other departments within the university.

Examination the effectiveness of e-learning curriculums of special librarian profession

Forgó Sándor Ph.D <forgos@ektf.hu>
EKF

Hauser Zoltán Ph.D <hauserz@ektf.hu>
EKF

Kis-Tóth Lajos Ph.D <ktoth@ektf.hu>
EKF

As of 2000/2001 The INSTITUTE OF MEDIA INFORMATICS at the Eszterházy Károly College applied for the accreditation of the *informatics expert-librarian* training program at the Hungarian Accreditation Committee. This distance learning scheme approved by the Hungarian Accreditation Committee is fully adapted to the credit system, and as a result of the project such educational course materials were elaborated which are available for dissemination both in printed and electronic form. The educational materials are on-line based (accessible on a WEB surface by any browser function), optimalized for network-based communication and are even suitable for administering on-line examinations. Our presentation focuses on the quality requirements of the developmental process as the first stage of curriculum development efforts is the elaboration of the basic concepts of quality assurance criteria.

As e-learning programs emphasize individual learning, the teacher's most important task is to provide personalized learning assistance and guidance in addition to functioning as a tutor in the learning process. Our blended learning system is an effective training form, however, in addition to the provision of adequate conditions for knowledge acquisition, students must be provided feedback concerning their efforts and the degree of the level of knowledge acquisition has to be monitored as well.

Since an e-learning system has to meet numerous requirements--integration capability, server client conditions (hardware, and software, orgware, courseware), safety, data monitoring, information provision and communication options, administrative concerns, statistical considerations, and learner environment--the Institute of Media Informatics launched the elaboration of quality assurance principles. One of the important steps of it the representative survey form with following standpoints:

1. General sociological profile
2. Role of computer network
3. Motives of choice of profession
4. Time balance
5. Learning habits
6. Value orientation of subjects
7. Questions of quality assurance

a. Information provision on the course *(Information and orientation* (1), the introduction of the course (2)
b. Communication (*A synchronized (3) and synchronized cooperation (4), feedback systems (5),*
c. Design (*Structure (6), Form (7)*
d. Administration (*General features* (8)
e. The content (*The content of educational materials (9), the prevalence of pedagogical and didactic principles (10), psychological-ergonomical principles (11), meeting media communication (device -based) requirements (12),*
f. Central data base (*The gathering of student data (13), the compilation and filing of documents (14)*
g. Navigation, (*General expectations (15), accessory or supplementary inform. (16)*
h. Learner support (*availability, accessibility (17), customisation to individual needs (18)*
i. Technical requirements, (browser, op systems,) (*Client platform – standard (19)*)
j. Evaluation, feedback, quality assurance, (*Content, structure, usability* (20))

Subjective comments, opinions.

Standards, technologies and framework systems

Papp Gyula <pappgy@kfrtkf.hu>
Kölcsey Ferenc Református Tanítóképző Főiskola

E-Learning applications come into general use in higher education. Development of electronic curricula will be significant in immediate future. But which are those circumstances, which determine the development of the main line? What kinds of environments want to shape for the institutions? What sort of possibilities for collaboration are available between institutions? I wish to make a rough draft of the frame of the future, which determines the educational face of the higher education in the future.

KOPI Online Plagiarism Search and Information Portal

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI

Pataki Máté <Mate.Pataki@sztaki.hu>
MTA SZTAKI

Tóth Zoltán <Zoltan.Toth@sztaki.hu>
MTA SZTAKI

The goal of the project is to develop an online plagiarism-search portal, which helps both

digital libraries to protect their documents and teachers, professors to find copied work or publications. The portal would also give information about the Hungarian laws belonging to this special field, and would include a discussion forum as well.

Such a service is not available for the Hungarian net community yet, and the foreign services are also limited in number and functionality. This portal will foster Internet publications and spreading of digital libraries by beating back the illegal copies. It has no sense to copy a digital document if within minutes the copy of the whole or part can be detected.

For the project the text-comparing algorithms, the database structures and queries need to be researched and developed, especially the runtime system needs to be optimized for big databases. As Hungary is about to join the European Union an other important aspect is multilingualism. All algorithms need to be implemented language independent to support the search in texts written in any language.

BIZTOSTŰ – Guide to IT security

Endrődi Csilla <csilla@mit.bme.hu>
BME MIT

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME

The **Biztostű** is an educational material on the Internet developed by teachers and students of the Budapest University of Technology and Economics (BUTE) and the Eötvös Loránd Univesity (ELTE) with the support of the Ministry of Informatics and Communications, the Ministry of Education and the Search-Lab Kft.

The goal of our project was to create an IT security related portal, which focuses not on product-specific information, but on forming the sense of view, conducing to the recognition and learning of the basic rules, and through these, ameliorates the consciousness, secure and confidence feeling about IT security. We believe that security cannot be handled simply as pure material knowledge; without the application of basic rules and the proper approach, conscious and confidence-making security solutions cannot be developed. As still there isn't an educational form like this – which contains games and other interactive methods in order to support the deep learning –, **Biztostű** plays a lack filling role.

For the compilation of the content, we built on the educational experience of many years, already created materials, lecture scripts, student works and sources of presentation videos. For the design of the portal we tried to use the widest palette of the technical possibilities. Besides the classical hierarchical tutorial materials you can find the "itself -suggesting" basic rules, the interactive games, and a lot of videos with slides. This way we we tried to use the audiovisual tools and the techniques of "learning through playing" to make the study as effective as possible. The multimedia material can be accessed for blind and deaf people as well.

- The largest part of the **Biztostű** is the thematically ordered educational material, which covers a wide domain of the IT security. The captions are presented in multiple levels of depth to allow the beginners to understand the introductions and the advanced readers to find precise definitions and the exact specifications. The links at the bottom of the pages support easy navigation and the links inside the texts allow jumps to the details of mentioned topics.
- The most important basics of security are represented by a loosely coupled chain of rules.

These contain easy to understand and interesting examples to teach the proper point of view. These are extended by the descriptions of the several categories

- There are games on the web site designed for some of the basic rules to provide personal experience, which make learning more intensive.
- To all the multimedia materials containing subscribed videos of presentations belong extending material in the form of slides, html or pdf files.
- We provide links for further information on the Internet for those, who want to read more information. These contain links to lectures of the BUTE and ELTE, some work of students and many useful literatures.
- While reading a specific topic, we have the possibility to get the description of an expression using the thesaurus.
- All the materials on the web site can be searched through keywords.

Our aim was to make a web site for the people interested in IT security, which could be used later as a starting point as well. **Biztostű** is not only a tutorial portal, but an extending knowledge base about the most important algorithms, specifications, methods and techniques, where the basics and the details of several topics can be found. We hope, that the students and other users will return here time to time. This way our system can be an example of materials supporting life long learning.

Towards E-Administration

Kecskés Zsuzsa <kecskes@sztaki.hu>
MTA SZTAKI

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI

Zöld Krisztina <zold@sztaki.hu>
MTA SZTAKI

The "Demand Driven Information Tools" project explores the steps of introducing and establishing e-administration and the opportunities of disseminating e-democracy in a wider circle. The scope of duties in the project is multidisciplinary; successfully reaching the predetermined targets needs the co-operation of administrative specialists, jurists, administration-reengineering specialists, financial and computer specialists and sociologists.

The participants of the project try to make an advance in the next areas:

- facilitating the office routine to citizens
- strengthening front-office activity (client contact) in a "client-friendly" way by using the tools of artificial intelligence and decision support
- making the work of administration more transparent for citizens
- reconsideration of administration processes (processes, organisations, laws)
- making back-office activity (own internal administration) more professional
- examining the solvability of administrative and law problems in the above mentioned areas

The presentation will be about the realisation of the prototype, which will be an integrated front- and back-office system of the Kaposvár Local Government. The citizens of Kaposvár will have the opportunity to use a real e-government site on the interactive portal.

ORACLE iLEARNING – eLEARNING IN THE HUNGARIAN ARMY

Vörös Miklós <mvoros@zmne.hu>
Zrínyi Miklós Nemzetvédelmi Egyetem

The means of information and communication technology (ICT) are widely used in our lives. They make possible and, at the same time, they require the transformation of teaching and learning environment, and the use of modern tools of information and communication. The new paradigm of education assisted by ICT is efficiency, that is, the time- and cost-factors of providing an individual with instantly marketable knowledge. This article aims to survey changes in the teaching and learning process, possibilities of acquiring knowledge based on ICT, and give an account on distance education to be introduced in Hungarian military higher education.

Modernisation of the Hungarian Defence Forces and transition to the all-volunteer force require permanent update of personnel knowledge and skills. Due to financial limitations, concentration of teaching staff and infrastructure, and demand for specialised military-professional knowledge, the proportion of conventional resident courses is expected to decrease significantly, while demand for organised conversion and follow-on training will highly increase. Conventional education is unable to meet that challenge, so it is inevitable for the Hungarian Home Defence Forces to introduce and spread new educational methods, means and media. The distance learning system based on Oracle iLearning Learning Management System has proved to be efficient in a national and international environment alike. Its relevance, quality, well-balanced content, high cost effectiveness, and the possibility of flexible learning at home cater for acquiring and permanent updating of necessary knowledge and skills, and helps to transform learning from being a necessity to becoming integral part of the way of life, becoming routine activity for everyone.

GIS (Geographic Information System) support provided to resource management by special-purpose districts

Pázmányi Sándor MSc <spazmanyi@hbmo.hu>
Hajdú-Bihar Megyei Önk. Informatikai Központ

In addition to Hungary's accession to the European Union, also the need to enhance our economic competitiveness and the fierce competition that developed among the regions for increasing their share from the scarce resources have encouraged us to manage with our human and natural resources and the available organizations and infrastructure in a prudent manner.

At the time of political and economic restructuring, the elementary right granted to people to organize their life at their discretion preceded the importance of efficiency requirements, leading to the creation of a relatively high number of municipalities (approx. 3260) vested with an undifferentiated scope of authority.

Cooperation of special-purpose districts is expected to resolve also this problem. Cooperation and common completion of tasks requires sharing of agreed views which, in turn, assumes the existence of carefully structured collection, classification and utilization of information.

Based on local and regional experiences available in the County of Hajdú-Bihar and the resource maps received from the County of Szabolcs-Szatmár-Bereg, we developed a system and methodology capable of meeting this task (after some customization), in compliance with the respective EU standards.

The need to strengthen the special-purpose districts' position in the public administration system and the pre-accession expectations clearly required the development of an information system

whose innovative nature and set of tools can assist in meeting the increasingly sophisticated requirements imposed by the special-purpose districts, in terms of collection, analysis and classification of information and the supply of adequate data.

The Resource Map of Special-Purpose Districts is a combination of a GIS database and a user software which allows for the comfort of handling of all the standardized mapping data and the related tabulated information over a common surface that can be easily managed and understood furthermore offers the special advantage of being specified in the Hungarian language.

The system designed to support decision-making in the special-purpose districts represents a branch of applied information technology dedicated to the collection, processing and management of spatial information. The method and efficiency of data collection and processing is crucial for the viability of the decision making strategy. The accuracy and reliability of this set of information influences also the reliability of both the systems dedicated to supporting the decision-making processes related to resource allocation and the decisions themselves.

The project implements a system based on a four-level set of digital maps (county, special-purpose districts, statistically identified regions and settlements), meeting the expectations applicable to the open and standardized systems structured according to the bottom-to-top principle.

Knowledge based public administration systems

Pajna Sándor MSc <spajna@hbmo.hu>
Hajdú-Bihar Megyei Önk. Informatikai Központ

WorkFlow v3.2 – A software system we developed to support electronic administration

The problem to be solved:

Electronic IT-based communication has clearly tended to substitute for the traditional paper-based communication. The extremely fast development has obliterated any limit in terms of both time and space; in other words, the citizens can get access to the authorities 24 hours a day. Each day, thousands of cellular phones are sold and manufacturers supply at least as much new IT-based devices to the users. The key question is whether we are able to exploit all of the potential benefits and advantages offered by this rapid expansion by assisting the citizens and the offices of public administration in improving their communication. We need a complex system capable of making the back-office tasks performed in the offices easier and of creating the "virtual office" where the citizens can utilise the Internet to initiate cases or file requests, can follow up such cases, can put questions to the administrators, etc.

The solution

These questions are unambiguously answered by our WorkFlow system. Within this system and after having familiarised with its internal structure, the citizen can approach the office via the Internet, forgetting any former obstacles previously imposed by geographic distance and location. After having established contact with the office, the citizen can submit his specific problem or request via the Internet and the office receives and processes the issue as an electronic file. In compliance with predefined electronic procedures, the administrator settles the problem and, after having closed the file, sends an electronic message to the citizen to inform him about the decision made by the office. Since not every citizen has access to the Internet or can make use of the resulting advantages, our system was designed to manage such situations, as well. It can operate in both the traditional paper-based and the electronic environment, i.e. the software can be instructed to print the decision to be signed and mailed by the administrator.

All these capabilities make the processing, managing and filing of electronic documents a faster,

smoother and more transparent process, which also enhances the accuracy of the completion of public administration, tasks. Accordingly, our system offers a dual benefit since it is capable of operating in both environments; in other words, it supports the managing of the paper-based administrative model including all the documents, professional processes and workflow that pertain to it while assisting and facilitating also the operative mechanisms characteristic of the fully electronic (i.e. paper-free) offices.

The application

Cost efficiency is one of the key features of the system's application. The fact that our knowledge-based system is consistently structured means that the administrator is effectively supported by the available documents, procedural rules and legislative background in completing either and all steps of the official procedures. The fundamental principles stipulated in the Public Administration Procedures are supplemented by special capabilities of this trade. Introduction of the system in an ASP environment would facilitate the provision of administrative services of identical quality in both the smallest remote villages and in large cities. Accordingly, the provision of best quality services to citizens living in either corner of the country does not require unaffordable investments.

Commissioning is in the process.

Orientation on the Web

K. Princz Mária <pmaria@delfin.unideb.hu>
Debreceni Egyetem MFK

There is a lot of information on he Web, but can we find the necessary piece every time? What kind of strategies can we follow? What is worth paying attention to?

There are some strategies that we can use: guessing the URL, subject directories, search engines.

Search engines are important tools for searching information on the web, but there is a large part of the web, which is hidden for general search engines. How can we search in this part?

In this paper, we present some statistics about web, review users' behaviours and tell experiences on how students do searches.

NEW APPLICATIONS AND APPLICATION DEVELOPMENT TECHNOLOGIES

NIIF Videoconference project: where are we?

Kovács András <akov@niif.hu>
NIIF Iroda

Máray Tamás <maray@niif.hu>
NIIF Iroda

Mészáros Mihály <misi@niif.hu>
NIIF Iroda

Mohácsi János < mohacsi@niif.hu>
NIIF Iroda

The main aim of this lecture is to introduce the work that has been done in the NIIF Videoconference project, the current state of the project and the possible future to the academic community. We're going to describe the public procurement procedure by NIIF to buy professional videoconference endpoints and a high capacity videoconference server for the academic institutions. The technical background and capabilities of the NIIF videoconference service will be detailed. First the network equipment and their interconnection will be introduced. We're going to present the gatekeeper network that does the routing of videoconference calls and the technical parameters, capabilities and value-added services of the central videoconference server unit. At the end, the management tools and procedures of the NIIF videoconference network will be presented.

NIIF multipoint videoconference service

Mészáros Mihály <misi@niif.hu>
NIIF Iroda

In my presentation I will introduce the NIIF multipoint videoconference service. I will provide a comparison of three possible MCU solutions.

- OpenMCU – www.openh323.org
- ViewStationFX -Polycom
- Accord MGC100 - Polycom

At the end I will emphasize (give details about) the booking system of the NIIF videoconference project.

A graphical framework to develop component-based web applications

Székely István <iszekely@inf.unideb.hu>
Debreceni Egyetem, Informatikai Intézet

In recent years the Internet passed through large growth. Today its use is an ordinary thing. Its world-wide spreading affected the development of applications. More and more applications have the choice to use the Internet as their platform. These applications are known as 'web applications'.

Programmers and software engineers recognised they can produce applications in industrial size only if they use suitable methodologies and tools. One kind of tools are integrated development environments. Today these have graphical user interfaces without exception.

In my presentation I would like to present a development tool I made. It is a web application itself. By the aid of this tool we can create web applications on a graphical user interface. Within the framework we can work with components. The individual web pages will be built from the components. The components are provided by a so-called component server, which reads the list of available components from an XML file along with all the information that is necessary to build our pages visually. For example the configuration includes the properties of the components we have to provide in order to display them.

The finished pages are then sent back to the server, which takes care of their storage. For this we need a two-way communication between the server and the framework while constructing the pages. The description of the pages will be stored in XML files so we can edit them later. This form of the pages cannot be directly used in web-applications. So we have to attend to convert the XML files into JSP pages, which can be used by Java-technology based application servers. It is the task of the JSP pages to produce the resulting HTML pages based on the data provided by the components.

Every component is made up of one or more Java classes (at least one Java class). The implementation follows the MVC design pattern. The main class of the components serves as the controller in the MVC pattern. Two additional classes can be associated with a component to accomplish the functions of the model and the view.

In my presentation I will explain how we can create a web application and produce the final JSP pages based on the above-described principles.

A Java-based mobile client for the blind to access network services

Juhász Zoltán, PhD <juhasz@irt.vein.hu>
Veszprémi Egyetem

Arató András, PhD <arato@sunserv.kfki.hu>
KFKI RMKI Beszéd- és Rehabilitáció-technológiai O.

The computing industry, despite its unprecedented development process, is still not in the position to provide universal usability, i.e. create devices and computer programmes that can be used by users with various disabilities. The de facto standards and metaphors used in today's commodity personal computers and various programs are based on the abilities of the healthy majority of the user population. The current technology trends are especially unsuited for blind people. The universal acceptance of the point-and-click graphical user interfaces makes using even the simplest program a very demanding task for them.

In our paper we describe an alternative, mobile PDA-based solution that was purposefully designed with the requirements of blind people in mind. It is a cheap, small and portable computer that enables users to carry out everyday tasks (word processing, letter and book reading, email sending and receiving) and access internet services for information and entertainment. In the paper, we describe in detail the architecture of the system and the developed software, as well as the methods used in order to use remote services.

Component collaboration in Web application environment

Jónás Richárd <richard.jonas@tsoft.hu>
Debreceni Egyetem

Nowadays everyone can benefit by sending and receiving information over the Internet, and use them in all walks of life. To establish a communication in a way like that, one has to work out a software infrastructure that is capable of performing those tasks. The main part of the infrastructure is a Web application in software engineering aspect, so Web applications have a short lifecycle with frequent loop-backs.

Component-based software development supports all steps of the development process of such Web applications. There are several component technologies: certain technologies deal with the generic representation of components, others keep business profit in view, there are component technologies for extreme programming, etc.

In this paper I will analyse my own recently introduced component technology from security, debug and developmental aspects, which are well known from the field of aspect oriented programming. Then I will investigate how we can capture the collaboration and the communication of components in aspect oriented way, and what are the benefits of such an approach.

Aspect Oriented Languages represented using XML

Kincses Róbert <kincsesr@tsoft.hu>
Debreceni Egyetem

The software development involves using the concepts of a small number of paradigms. Nowadays, the best-known and mostly used programming principles are the Procedural Oriented Programming and the Object Oriented Programming (OOP). The languages implementing the concepts of OOP are widely used in the creation of software for commercial purposes.

The OOP means improvement compared to the procedural approach. With the help of the OOP, real life systems can be modelled easier. Besides that, a well designed and implemented OO program is well maintainable and can be easily developed further. However, there are problems, which are hard to model in an elegant way, when using OO techniques. Some examples of these kinds of problems are those which affect the whole program. Such problems easily arise when an existing program is being modified. The program code made to solve these problems is usually scattered over the whole system.

The staff of XEROX PARC has searched for a solution and they have found one. These inter-object decisions, which are influencing the whole program, are called *aspect*s. The paradigm that operates with aspect is called Aspect Oriented Programming. This is a successful solution. There are several implementations (languages and frameworks) of the concepts.

The presentation will be focused on an XML language, which makes possible to represent the elements of an AOP language as XML elements. Firstly, certain XML documents will be discussed that are representing elements of a specific language. Afterwards, we will examine the usability of this idea through some example: how is it possible to create executable code from an XML document? What other purposes this XML is appropriate for? Does it provide any significant advantage in automatic code transformation, etc?

Further, we will consider which parts of an AOP language are worthy to represent using XML. If the XML language is independent of the syntax of the AOP language (that is, XML elements have been assigned to every language element), then we can examine if it is possible to represent constructs of several different languages using one XML language and if this uniform representation provides any advantage or disadvantage.

Examination of the quality warranty parameters of videoconference systems

Gál Zoltán <zgal@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

Karsay Andrea <kandrea@cis.unideb.hu>
Debreceni Egyetem, Informatikai Szolgáltató Közp.

The role of the multimedia services transmitted over the Internet is raising nowadays. The portfolio of the video transmission solutions is rapidly increasing from the basic software applications through the monitoring systems and the off-line/real-time streaming videos to the most sophisticated videoconference applications. Applications using best effort method are getting widespread quickly, therefore a growing need exists to determine the necessary network resources more accurately than ever and to provide adequate quality of service at end user. This resource quantity and quality determination is not an easy task, because beside the calculation of the minimal bandwidth needs to be set different quality of service parameters of the protocol data unit transmissions.

To determine necessary network resources we run multimedia applications in test environments. Real video streams are generated having different frame size, bandwidth, shaping and other parameters and samples are collected at the proper points of the test environment with Tekelec protocol analyser. We plan to determine the necessary network resources of different multimedia applications based on protocol H.323. These parameters are set according to the subjective experiences about the quality of the video streams and the numeric results obtained from the measurements.

The aim of this paper is to determine a set of connection points of the running network being most suitable to serve multimedia applications and to give recommendations of the numeric parameters of these locations. Concluded results can be used for further development of the institutional local area network. The mechanisms and solutions presented according to these results will satisfy the quality needs of high performance multimedia applications, too.

Web standardization in Hungary

Kovács László dr. <Laszlo.Kovacs@sztaki.hu>
MTA SZTAKI

Vásárhelyi Nóra <vnora@sztaki.hu>
MTA SZTAKI

The World Wide Web Consortium (W3C) is an international organization that develops technological recommendations and standards for the World Wide Web. It was created in October 1994 to lead the World Wide Web to its full potential by developing common standards and recommendations that promote its evolution and ensure its interoperability.

The spread of the Internet as a global network system was influenced by the activity, researches and developments of the World Wide Web Consortium. Nowadays, an average person regards the Web and the Internet to be the same, which shows the importance of web technologies in the area of Internet technologies. The World Wide Web system has created new forms of human communication and provides new possibilities of global distributing of knowledge and multimedia information.

The W3C Hungarian Office is the local organization of the World Wide Web Consortium in Hungary. It takes an active part in creating, spreading and familiarizing the Hungarian web standards. Its mission is to familiarize the Hungarian institutes (universities, colleges, government bodies, R&D institutes, civil organizations) and companies with the developments of the Consortium, like standards, specifications, guidelines, software), and to inform about them continually. The W3C today makes developments in more than 40 areas.

Videoconference in practice

Giese Piroska dr <giese@rmki.kfki.hu>
KFKI RMKI

The success of the experimental physics collaborations depends on the frequent and regular information exchange across several countries.
In the presentation a short overview of the used teleconferencing tools, the H.323/VRVS (*Virtual Rooms VideoConferencing System*), and some useful hints will be given.

In order to achieve a good quality of conference, it is necessary to keep some basic regulations. In the presentation some of the regulations and the additional software/hardware tools we are using at the international conferences will be presented.

Last but not least, a short report of the H.323 based worldwide "**Megaconference V**" organised by Robert Dixon (Ohio State University) and OARNET with 187 registered institutions from 28 countries held in December 2003 will be given.

Standardised interchange of model-information

Papp Ágnes <agi@delfin.unideb.hu>
Debreceni Egyetem

Application systems usually maintain difficult data structures. There are several application development tools but data conversion is needed when they want to make their data accessible for each other. UML has been widely accepted as an object oriented analysis and design method. An application-neutral interchange format allows UML models to be interoperable between development tools and developers.

Specifications by OMG summarise principles of data storing and modelling in a four level architecture. The first level is the meta-meta model that defines UML at metamodel level. The second level is the metamodel that describes the UML syntax. In the third level there are the models created by the users, and in the fourth level there are the object instances or records.
XML is an appropriate format for transferring data via the Internet. The XML based XMI standard allows for different types of applications to interchange their data or models in a standardised way.

There is a new way of developing applications, the Model Driven Architecture. The MDA specification consists of a platform-independent UML based model (PIM), and one or more platform-specific models (PSM). With MDA, an application system is modelled once and only once. The MDA also will take advantage of XMI when it defines the mapping from PIM to XML.

Automatisation of live web-applications' system verification by address and content test

Ercsényi Gábor <gercsenyi@allied-visions.de>
Allied Visions GmbH

Nowadays' applications that can be accessed via Internet 24 hours a day are getting more and more important. This paper introduces a system that regularly informs the users about the availability of the applications to be tested, plus it reports if the run of them is satisfying or erroneous. This information is received by verification of the content generated by the applications.

An XML database contains the addresses of the web-applications to be tested and additional data about the testing process itself. The verification of the content generated by these applications is complex because these applications use sessions. [It can occur that it is possible to test the content provided by these applications only after a successful login.] The system mounts a report about the test results that is saved into a file and sent to given e-mail addresses.

NIIF Central Services Cluster Architecture

Bajnok Kristóf <kristof.bajnok@sztaki.hu>
MTA-Sztaki

Central services in NIIF have been supplied by a single machine named helka.iif.hu for many years. As of the year 2002 it became clear, that increasing performance and availability demands could not be satisfied with a single monolithic architecture, thus development had to address some cluster-based solution.
A challenge was to support various hardware (x86, SPARC) and software (Solaris, Linux and other OS'es) architectures as well as a great number of existing applications. After inspecting many Load Balancing and High Availability solutions, Linux Virtual Server (LVS) was chosen.
Migrating services from 'helka' to the new cluster, the following changes were probably the most important:

- (RedHat) Linux instead of Solaris OS
- Use of Open Source Qmail MTA instead of PMDF
- Storage Area Network (SAN) and global parallel filesystem (GPFS)
- Instead of system-level users:
- Applications use NIIF Directory Services for authentication and authorisation
- Interactive login is no longer supported

The last change resulted in several questions to solve, as applications are usually unprepared for virtual user environment. In the presentation, structure of the implemented architecture, usage of the SAN and adaptation of applications to the Directory are examined in detail.

Dynamic placement of distributed application with significant communication demands

Goldschmidt Balázs <balage@inf.bme.hu>
Budapesti Mûszaki és Gazdaságtudományi Egyetem

László Zoltán dr. <laszlo@iit.bme.hu>
Budapesti Mûszaki és Gazdaságtudományi Egyetem

Due to the high speed expansion of the Internet, on-line content service demands are increasing; common content bearers (CD, DVD, VC) are going to be replaced by "downloading". Adaptation bears key importance in applications where lack of resources limit satisfaction of real-time user requirements. Distributed multimeda systems - especially the systems handling moving pictures - belong to these kind of applications.
A system developed with the participation of the authors is able to deploy applications to new host computers. Finding the good candidate hosts is, however, an NP-hard problem. To give a near optimal solution, the authors have examined and implemented several algorithms. The most promising is a modified version of the particle swarm algorithm, that belonging to the family of evolutionary algorithms. In it, problems are solved by employing a set of particles, each describing a possible, but not necessarily optimal, solution. They take over solution-details from their neighbours that have less costy solutions, and combine these details with their our proposed solutions. The algorithm runs until all particles' solutions have the same cost.
In its original form, the algorithm only supported combination of binary or real (ordered) values. The version elaborated by the authors allows combination of elements of such sets, upon which no ordering is defined. The measurements and simulations proved, that the runtime and the solutions given by the algorithm is significantly better than that of the previously considered algorithms.

From SmartCard to Integration platform

Zsemlye Tamas <tamas.zsemlye@sun.com>
Sun Microsystems Kft.

The computer world currently has many platforms, among them Microsoft Windows, Macintosh, OS/2, UNIX® software must be compiled separately to run on each platform. The binary file for an application that runs on one platform cannot run on another platform, because the binary file is platform-specific. The Java Platform is a software platform for delivering and running highly interactive, dynamic applications on networked computer systems. But what sets the Java Platform apart is that it sits on top of these other platforms, and executes bytecodes, which are not specific to any physical machine, but are machine instructions for a virtual machine.
The Java Platform enable to write distributed application not only on traditional computing device. The application can run from embedded device, like SmartCard to high server environment.

Chances of information-retrieval for the blind

Várhelyi Eszter <eszter.varhelyi@bne.hu>
Andrássy Gyula Német Nyelvű Egyetem Könyvtára

The existence of the information-based society enlarged even more the gap between average and handicapped people. The fast pace of technical development often disregarded the handicapped who, as a result, are lagging behind in the use of the instruments at our disposal. But last year some

kind of a change began in this respect, because – as you know – 2003 was declared to be the year of the handicapped in Europe. Now librarians only have to strive to maintain what has already been launched.
To provide solutions of information retrieval for the handicapped (in this case for the blind) that can really be used by them we have to define the notion itself and its consequences.
Being handicapped as a notion does not exist in itself, it is the result of something, and as a consequence the person affected has to face severe disadvantages.
A most important way of abolishing these difficulties is creating equal chances for the handicapped. In this respect libraries play a very important part because they represent intellectual freedom and help the handicapped to integrate in society.
Our main target is to establish centres where the blind can satisfy their needs of information-retrieval together with those able to see, with the help of instruments they know and are able to use. These are: Braille-books
Sound books
Computers
I focus on the use of computers and digitalisation. According to my own survey less and less people are using the dot-script. This might have two reasons: physical and psychic. The spread of "talking computers" makes more and more young people want to learn how to use them and they put less stress on the use of traditional instruments. Computers try to eliminate the drawbacks of sound and Braille-documents (time-consuming production, short life span, difficult to handle etc.). We have several possibilities to eliminate them: digitalisation, use of the Internet, reading systems, hybrid sound books and establishing a "National Library" for the blind.
Given the possibilities of rehabilitation by modern technique, we just have to make use of them. An important target is to achieve a Windows-interface, which even those who cannot see properly can use easily. Nowadays many blind people use DOS' interface when working with a computer, because Windows is not really blind-friendly. (It gives you instructions like 'click here'.) It would also be important to make the most of the possibilities inherent in the Linux system. Compatible screen readers should also be made to this system, especially to the Uhu Linux, which is Hungarian-based and easier to handle than Windows. Also there are only few websites that can be visited by the blind.
In my opinion the Hungarian Electronic Library is a bridge because its website was made accessible for blind users as well (new interface).
In my summary I sketched several targets and possibilities. Their realisation would contribute to minimising the gap between the healthy and the handicapped so that they can participate in the information-based society with equal chances.
I should like to finish my essay with a quotation:
"The real problem of being blind is not the lack of the ability to see. It is rather the lack of understanding and of information-retrieval. (www.nfb.org)"

Organisation portals – quite in another way The importance of document-management in organisational processes

Dicse Jenő <dicse.jeno@synergon.hu>
Synergon Informatika Rt.

Organisation portals – quite in another way

Nowadays, the processes in the organisations are more complex than before, and they would need an integrated IT support. The general practice is today: different contributors can access different information in different systems about a same matter. For example, if anybody needs to make a decision, he/she should collect this information from his/her colleagues, or he/she should be an expert of all different systems (and he/she should have access rights too). Moreover, the sharing and

accessing of many small, but essential pieces of information (which are needed for everyday work) has no powerful support in most IT systems. This situation results in rather clumsy workflows, which burden the employees needlessly, so it is a waste of time and money. The organisation portal is the modern solution for supporting the collaboration, integrating the applications and information services and eliminating these unjustified costs.

The importance of document-management in organisational processes

The document is one basic element of organisational information flow. Storage, transformation and usage of documents and information within documents is critical, after all they are not supported from IT side. Lots of unnecessary prints, inadequate documents regarding their content and face, high redundancy, human malpractices and inadequate systemisation mop up considerable amount of money totally needlessly. Implementing a well-designed document management system can increase efficiency of daily operation, and remarkably decrease its costs.

SUPERCOMPUTING, GRID

The Hungarian ClusterGrid infrastructure project

Stefán Péter <stefan@niif.hu>
NIIF Iroda

The paper and the presentation describe the key characteristics of the Hungarian ClusterGrid infrastructure, and shows how it fits into the layered grid infrastructure model. The layered layout is of great importance, since each layer provides a certain amount of abstraction to the upper layers.

In the ClusterGrid infrastructure model there are six layers need to be distinguished:

The Physical Layer or the hardware layer concentrates on the roles, and the potential functions of the different grid elements which can be resources (compute nodes and local masters), access points (entries), grid-level service providers (service nodes) and job gateways.

The Link Layer focuses on the local computer network interconnection of the different resources. Layer-2 tools and protocols, such as 802.1q encapsulation or 802.1x authentication are applied.

Global network connection of individual clusters is carried out via the Networking Layer. Providing efficient links as well as considering reasonable security issues are equally important. Private networking techniques such as IPSec or MPLS can be extensively used.

Resource Layer is used for integrating separate nodes into a single large computational unit. This layer concentrates on appropriate use file systems (NFS, XFS, or global file systems), parallelization, resource allocation and scheduling as well.

The Grid Layer gives a uniform interface between differently structured and build grid systems. One of the most important issues here is the job definition, and the job exchange mechanism, i.e. to transfer one job from one system into another one. This layer is responsible for user authentication and job identification.

User jobs and applications, such as job and resource monitoring appear on the Application Layer.

In the presentation up-to-date configuration issues as well as computer node statistics will be given.

Optimisation of Group Broadcasting in Cluster Systems

Juhász Sándor <juhasz.sandor@aut.bme.hu>
BME, AAIT

Csikvári András <csiki@mail.datanet.hu>
BME, AAIT

Being built up out of standard personal computers and being connected with standard communication networks, clusters provide a cheaper alternative for solving high-demanding computational problems, and in the same time their modularity allows an easier implementation of fault tolerance and scalability compared to the traditional super computers. Despite of their numerous advantages cluster systems have not fully replaced the other solutions (SMP, NUMA, MMP and vector supercomputers) providing –without exception– a more expensive computational power, because clusters also suffer of two significant drawbacks compared to the traditional solutions. The first is related to the relative slowness of their communication, while the other lies in their programming paradigm being significantly different from the traditional methods. There is a continuous and active research effort directed to eliminate these disadvantages. Our paper deals with a sub-domain of the cluster communication, namely the acceleration of the group communication primitives in such environments.

The general-purpose communication components usually offer a smaller throughput than the ones designed specially for a specific hardware environment; that is why the communication planning and modelling plays a more critical role in algorithm design in the cluster systems. In cluster systems composed of separate computers, the cooperation of the nodes must be organised over the commodity network medium. To ease this task the various message passing libraries (e.g. PVM, MPI) implement some group communication functions (so-called communication primitives) as well, and offer them for the application built on the library. These communication primitives are built from basic communication elements for sending and receiving messages, and their efficiency is significantly influenced by the topology (one-many, tree, many-many), the synchronous or the asynchronous nature, and even by the symmetry of the communication.

As the nodes connected with active network devices (switching hub) can also be considered as a virtual crossbar system, the effect of the various topologies and of the different communication solutions can be examined without making hardware changes. In this paper the effects of the different solutions are presented through the different implementations of the broadcast primitive, and two algorithms deferring significantly from the traditional methods will also be introduced. These algorithms seek to enhance the performance by dividing the messages into smaller parts and by improving the symmetry of the communication. The new algorithm defines a broadcast primitive that provides –instead of the well-known solutions in other architectures (chain, hypercube, tree) having a complexity of $O(n)$, $O(dn^{1/d})$, $O(\log_b n)$– a method of $O(1)$ complexity, meaning an execution time theoretically independent of the number of the communicating nodes in the cluster system.

The usability of above mentioned solutions is demonstrated by experimental results, where we use the implementation of the broadcast primitive in the best known communication library as a base of the comparison. The results presented in this paper can directly improve the performance of the message passing libraries in cluster environments, and also help to increase, to predict and to tune the performance of distributed algorithms.

Execution of parallel communicating Java tasks in the JGrid system

Póta Szabolcs <pota@irt.vein.hu>
Veszprémi Egyetem

Juhász Zoltán dr. <juhasz@irt.vein.hu>
Veszprémi Egyetem

One of the main technical obstacles in the conformation of global Grid computing systems is the lack of cooperation among program execution environments. Execution of computation-bound applications is often only possible with the utilisation of many distributed resources. Therefore, a Grid system must assure that Grid application components allocated to geographically different sites can run concurrently. Today's mainstream execution environments, however, prefer batch processing, thus can give very little guarantees about the exact start time of the allocated tasks' execution. Since these systems are closed, typically operating on cluster architectures, synchronising them is a hard task. Grid execution needs such execution frameworks and global scheduling mechanisms that are capable to guarantee the concurrent execution of geographically distributed tasks running in parallel, and are capable to provide means of communication among the components allocated to different sites.

This paper describes in detail the execution framework developed in the JGrid project that provides solution to the above mentioned problems. The JGrid system provides facilities to assure the concurrent and immediate execution of parallel Java tasks allocated to geographically distributed computing resources. This is due to the time slice scheduling strategy used on the JGrid computing resources, which is mostly beneficial for interactive and communicating tasks. In addition, the system provides a high level communication model to program developers that enable communication and task control via remote method invocations. A parallel image processing application illustrates the above mentioned mechanisms, where the computation is carried out by Java tasks arranged into a logical mesh topology.

Global service discovery in the JGrid system

Kuntner Krisztián <kuntner@irt.vein.hu>
Veszprémi Egyetem

Juhász Zoltán Phd. <juhasz@irt.vein.hu>
Veszprémi Egyetem

As the Grid receives more and more attention by the general public, so we hear more and more about proposed Grid systems that will encompass the entire world and connect millions of services together. The operation of systems consisting of large number of components, however, is very different from the operation of small distributed systems. Due to software and hardware failures, services may leave and join the system unpredictably at any time; moreover, performing search based on URL or IP address is not feasible. A fundamental property of global Grid systems should be the capability of machine-independent high-level service discovery, where users can efficiently select from millions of services the most suitable for their needs.

After giving an overview of the known methods of service discovery, the paper presents the architecture and operation of the service discovery system developed in the JGrid project. It illustrates how services participating in the system can be described, and explains the methods used by clients to discover services. The paper outlines the components of a hierarchical discovery system, the role of its components and their relationships. The paper also discusses the issues of scalability and fault tolerance and, in conclusion, gives an estimation of the expected performance based on experimental results as a function of the number of connected services and clients.

The security architecture of the JGrid system

Magyaródi Márk <magyarodi@irt.vein.hu>
Veszprémi Egyetem

Juhász Zoltán Phd. <juhasz@irt.vein.hu>
Veszprémi Egyetem

The JGrid system is a service-oriented computational Grid infrastructure based on Java and Jini, which aims to support millions of services and users. One of the most crucial problems in Grid system research and development is security. The JGrid system is based on Jini technology; its implementation uses the recently released Jini version 2.0, which provides a flexible security architecture with wide-ranging functionality. The first prototype release of JGrid – based on the earlier Jini version 1.0 – was not secure, but it was eligible for performing threat analysis, which provided useful experience for the design of the security system of the new version. The article reviews these potential security weaknesses together with security requirements that are demanded by the service providers and users of the system. We show the solutions provided by the Jini security architecture for threats and attacks in Jini and Grid systems, as well as potential problems that require further improvements. With the help of examples we describe in detail the problems appearing inside the executing machine and between the co-operating Grid resources, and their solutions. In addition, we also discuss the issues arising in the presence of firewalls used by the secure network administration. The security architecture of the JGrid system thus extends the new security system of the Jini to achieve high level security and protection against attacks occurring in Grid systems.

Cluster based data recording and real time processing

Molnár Gergely <gemolnar@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Emri Miklós <emri@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Molnár József <jmolnar@atomki.hu>
MTA ATOMKI

Balkay László <balkay@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Ecsedi Kornél <ecsedi@unideb.hu>
Debreceni Egyetem Informatikai Szolgáltató Központ

Trón Lajos <tron@pet.dote.hu>
Debreceni Egyetem OEC PET Centrum

Gál Zoltán <zgal@unideb.hu>
Debreceni Egyetem Informatikai Szolgáltató Központ

A complex software development project was started to work out a multiprocessor-technology-based software developing environment for medical image processing and high-speed data acquisition for tomographic devices by a consortium (PET Center and the Service Center for Informatics of University of Debrecen, and the Institute of Nuclear Research). The first task was

obtaining, building and testing the clusters and three research and development projects – parallel procession of high speed digital signals coming from a detector systems used in nuclear medicine; adaptation of 2D/3D iterative image reconstruction and correction algorithms for multiprocessor environment; development of real-time, interactive 3D graphical diagnostic test programs, with special regard to segmentation and image fusion based multi-modal visualization – are in progress. In the framework of this software development project a special computer cluster was set up for parallel high-speed data acquisition and digital signal processing. In the course of our work we studied the optimal usage possibility and applicability of this cluster using software simulation and real data acquisition based on a positron emission tomographic detector system.

Implementation of the CERN LHC-Grid at the RMKI

Debreczeni Gergely <Gergely.Debreczeni@cern.ch>
KFKI-RMKI

Hajdu Csaba <hajdu@sunserv.kfki.hu>
KFKI RMKI

Kulyassa Robert <qji@rmki.kfki.hu>
KFKI RMKI

The world's largest and most powerful particle accelerator, the Large Hadron Collider (LHC), is being constructed at CERN, the European Organization for Nuclear Research, near Geneva on the border between France
and Switzerland. The accelerator will start operation in 2007 and will be used to answer the most fundamental
questions of science by some 6,000 people from universities and laboratories all around the world. The
computational requirements of the experiments that will use the LHC are enormous: 12-14 PetaBytes of data will
be generated each year, the equivalent of more than 20 million CDs. Analysing this will require the equivalent
of 70,000 of today's fastest PC processors. The aim of the LCG (LHC Computing Grid) project is to find a solution to this
challenging problem.
In KFKI-RMKI (KFKI Research Institute for Particle and Nuclear Physics) as in one of the collabrating institute
we set up a regional LCG center which - after successfuly passed on the qualification and testing procedure -
entered in the production phase. We focus on the presentation of the most important features of this - in each of it's meanings - world-wide computing grid.

Declarative languages in the supercomputing. The SchML project

Békés András György <bekesa@sch.bme.hu>
BME

Programming of the more and more easily available cluster and grid systems needs high proficiency. There are several tools to simplify the creation of parallel programs, but the

programmer still has to carefully design the information flow and synchronisation amongst the parallel parts.

Programs written in declarative languages are generally easier to execute in parallel, compared to traditional, imperative programs. Several languages and language extensions are developed, which simplify parallel programming to such level, where the programmer only has to mark the parallel parts.

The implicit parallel execution of a program means that the programmer does not have to care about the fact that the program will possibly be executed on multiple processors. The goal of the SchML project is the implicit parallel execution of a functional language on computer clusters. In my presentation, I will briefly describe a few declarative languages that support parallel programming, and the applicability of these systems on clusters. I will also introduce the main characteristics of SchML, and compare it to the formerly described other systems.

Introduction of the Hungarian Supercomputing Grid experiments

Patvarczki József <patvarcz@sztaki.hu>
MTA SZTAKI,Párhuzamos és Elosztott rendszerek lab.

This paper presents the actual state of the Hungarian Supercomputing Grid testbed (H-SuperGrid), describes the current infrastructure of the project and the members' hardware and middleware constructions. The interconnected members of this testbed give a good practicability to create a distributed computing resource and a high-performance and high-throughput computational Grid in Hungary.

Especially, this paper deals with the execution possibilities for the sequential, MPI (Message Passing Interface) and PVM (Parallel Virtual Machine) applications under certain run-time environments like Condor, Globus and Condor-G. Perscribes the test results of the various user facilities and illustrates the capabilities of the testbed.

Furthermore, it contains a useful solution for the execution of PVM jobs under Globus by the help of the Condor jobmanager.

Linear acceleration of a Monte-Carlo simulation

Hermann Gábor <ghermann@sztaki.hu>
MTA SZTAKI

P-Grade as a general programming and development framework for creating running, monitoring and migrating of parallel programs for clusters and for the Grid has been developed in the Laboratory of Parallel and Distributed Systems of the MTA SZTAKI. It is highly appropriate to create, to test, and to launch new parallel programs written in C and FORTRAN and to accelerate tested serial programs by parallelisation in an extremely short development cycle. The current paper demonstrates haw to parallelise a serial program to gain scalable linear speedup. The effect of the mapping of processes to the processors will be discussed on the example of a well-structured Monte-Carlo simulation program written in FORTRAN investigating the distribution of photons scattering on crystal detector. The usability of P-GRADE's visual monitoring facility in the enhancing the quality of the development is demonstrated.

Electronic proposal and evaluation processing -- experiments and experiences

Hanák Péter dr. <hanak.peter@om.hu>
Nemzeti Kutatási és Technológiai Hivatal

Simonkay Sándor <simonkay.sandor@om.hu>
Nemzeti Kutatási és Technológiai Hivatal

In the last decade, the number of calls for proposals and proposers has multiplied in Hungary. Nowadays almost all proposers and evaluators fill in the forms, prepare project proposals and evaluations in electronic form -- and then carefully print everything. The agencies (with respect to the exception!) retype the presumably important data from the documents received in print -- working hard and making errors -- in order to make statements and reports on their computers. Recently, there has been more and more talk about electronic government services, however, the results are relatively shy.

The Office of the National Board for Technological Development (OMFB) announced the first call for proposals for information and communication technology developments (IKTA) in 1997. It has always been evident for the officers of the department responsible for IKTA that the whole process -- starting from the announcement of the calls through the reception and evaluation of the proposals to the handling of written deliverables and financial reports -- had to be made simpler by using computers and programs. Since then, the electronic forms developed for IKTA have also been used in the information system of the National Research and Development Programmes, and since 2002 identical electronic forms have been used with all the calls for proposals announced by the Research and Development Division of the Ministry of Education (the successor of OMFB). In 2003, the electronic forms had to be sent already as email attachments and were received and processed (almost) automatically, in contrast to previous years where the forms were submitted on floppies or CDs.

Unfortunately, due to various difficulties and obstacles, only components of the envisaged system have been implemented and several times the development had to be restarted from the beginning. Nonetheless, these seven years have been full of illuminating lessons. The number of calls for proposals will only increase when Hungary joins the European Union, and the administrative burdens can only be made bearable if the tasks that can be automated will be automated, i.e. solved by computers. We believe that others, too, can utilise our 7-year experience with computer aided processing of proposals and evaluations and this is a good enough reason for a talk at the Networkshop 2004 conference.

IP telephone service on the Internet I.

Szendrői József <szendroi.jozsef@synergon.hu>
Synergon Informatika Rt.

This presentation will cover the end-to-end native IP based telephone services. We will show the application possibilities of the network elements regarding affected protocols, hardware and software requirements.

IP telephone service on the Internet II.

Láday Zoltán <zladay@deverto.com>
Deverto Rendszertechnika Kft.

In the second part of this presentation we will introduce a Call Agent application which moves the classical central office telephone exchange functionality into the IP telephone network.

The technical demonstration of this IP telephone service can be viewed at the demo desk of Synergon.

NETWORK SECURITY, NETWORK MANAGEMENT, AUTHENTICATION

Wireless LAN at the Budapest University of Technology and Economics

Jákó András <goya@eik.bme.hu>
BME EISZK

Wireless LANs' security requirements are very different compared to wired LANs, because of the fundamental properties of the wireless medium. This mandates the usage of more security measures than those we are used to on wired networks. The group of suitable complementary security mechanisms depends on the application environment.
This case study describes the applied WLAN security measures at the Budapest University of Technology and Economics, as well as the reasons behind the choices.

The NIIF CSIRT project

Mohácsi János <mohacsi@niif.hu>
NIIF Iroda

Németh Ervin <nemethe@niif.hu>
NIIF Iroda

In the last year NIIF CSIRT project we started to handle the security incidents regularly in network of NIIF/HUNGARNET. We also are announcing serious vulnerabilities, wildly spreading viruses. We initiated the cooperation in security incident prevention, and avoidance to be in sync with the European level network service of NIIF/HUNGARNET. We cooperated with the HBONE project to improve handling and preventing security problems of HUNGARNET network. We would like to help users of HBONE collecting informations and best current practices on secure network computing.
In the presentations we will show the latest result of the project, our experiences, our strategy in NIIF CSIRT and background of the project.

Digital Signature Applications TeDiES

Szőllősi Loránd <lorro@lorro.wigner.bme.hu>
BME Távközlési és Médiainformatikai Tanszék

Gyímesi Csaba <ympy@freemail.hu>
BME Távközlési és Médiainformatikai Tanszék

Juhász András <juhand@axelero.hu>
BME Távközlési és Médiainformatikai Tanszék

Marosits Tamás <marosits@tmit.bme.hu>
BME TMIT

Intoduction:

It is easy to implement digital signature using any high level programming language based on the well-known mathematical background. Although digital signature has been accepted by law in the European Union and even in Hungary since many years, it is not widely used yet. The main reasons for this are mostly of security issues and therefore the lack of confidence from the people, and also the huge cost of the deployment and maintenance of a system covering the public administration of a country. If we would have tools or applications using digital signature, which could increase the convenience of their user without having any considerable financial risk, than would the acceptance of digital signature be better. Are today's systems capable of supporting the security needed?

Goals

The main goal of the research and development of our team – who have worked since September, 2002 – to explore and overcome these obstacles. To achieve our goal, we started the implementation of a hardware signer device, simultaneously developing authentication servers and communication protocols to support our device. This tool contains some of our new ideas, from which the most important would be that it has an LCD display and buttons, which give it much higher level of security than one could achieve using a smart card. (In case of a smart card, the user must trust the card reader terminal, which is unneeded in our case.) The creation of such device consists not only of programming, but also optimization of procedures because of limited memory in the hardware. Moreover, the communication protocols and the flow of operations and functions in creating and verifying a signature demand thorough considerations.

Achievements

We named our signer/verifier tool the TeDiES, as in Text Displaying Electronic Signer. The prototype of TeDiES is ready and working, further development is on its way.

Along with the device, we are also developing server applications necessary for the operation of such tool. The functions include key generation and withdrawal, and certificate revalidation. Our two-server solution provides acceptable security even with smaller key sizes. Also there is no need for a central key storage! Revalidation of certificates demands little work from users, but provides off-line signing and lets the user specify his own security window. With VIP version, one can even check the partner's validity with optional precision.

Bibliography

- Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996
- Ronald L. Rivest, Adi Shamir, Len Adelman: On Digital Signatures and Public Key Cryptosystems, MIT Laboratory for Computer Science Technical Memorandum 82 (1977).

PIC18FXX2 Microcontroller Data Sheet, Microchip,
http://www.microchip.com/download/lit/pline/picmicro/families/18fxx2/39564b.pdf

The problems and connections of network virus protection and the protection against denial of service attacks

Bencsáth Boldizsár <boldi@crysys.hit.bme.hu>
Budapesti Műszaki Egyetem Híradástechnikai Tanszék

First I will provide some introduction into the problems and solutions in both the network virus protection and the protection against Distributed Denial of Service (DDoS) attacks. I will show the usual and most workable methods in the area of virus protection: client-side virus protection, mail server / relay server protection (with the priority of open source tools) (e.g. linux, amavis, mailscanner, clamav, unix virus scanners, "mail gateway" protection software), content-filtering tools (filtering web traffic), extended file access control systems (RSBAC malware scan module). I will also introduce the problem area of DDoS protection: Different types of DDoS attacks (protocol fault ("magic packet"), network bandwidth overflow, server resource consumption). I will also show the most usable techniques for the protection (error correction, firewalls, anomaly detection (SYN flood protection, etc.), protection based on network analysis) and will provide some data about the recent major attacks (Ebay, SCO, anti-spam rbl providers, zombie networks). After the introduction I will show the possible DDoS problems of the network virus protection: The resource consumption of the virus protection, the possibility of flooding, the dangers of virus reports and e-mail alerts. After defining the problems I'll show our proposed solutions: A virus protection system combined with the technique of network analysis to protect the system against DoS attacks. The incoming mails will be examined by the network analysis engine and therefore it makes possible to filter out DDoS attacks against the virus protection system. Our proposed solution might be useful against unknown (not detectable) viruses and in the area of early epidemic protection. To support our method I'll show the details of the structure of our pilot implementation.

Building a safe email service with decentralised administration from open source components

Tornóci László, Dr. <torlasz@xenia.sote.hu>
Semmelweis Egyetem, Kórélettani Intézet

It became clear at my workplace in the Nagyvárad tér building of the Semmelweis University in 2001, that we need to replace our Netware/IPX based Mercury/pmail system with a new, modern email service. In the planning stage I had the following goals:

- open source components
- very reliable service (RAID, user quotas)
- mailboxes should have no real user id's
- passwords should not get out to the network unencrypted
- uniform access and configuration from anywhere on the Internet
- access though webmail interface or with an IMAP client
- decentralised administration (by departments)
- SPAM and virus filtering
- Hungarian and English versions
- scalability, possibility to develop further features

After carefully studying the available open source components and the proper Internet forums, I built the system from the following main components: Linux (RH 8), postfix MTA, cyrus-imapd, mysql, apache httpd, IMP (webmail interface), amavisd-new (virus/spam detection). The system attempts to make a good use of the advantages of postfix and cyrus-imapd (e.g.: flexible address mapping and shared folders).

The administrative web interface was witten in perl. The code is completely separated from the HTML source, so the style and appearance of the interface is easy to change.

All data exchange between the users and the server is through SSL channels. Sending an email from an IMAP client through SMTP/TLS is possible only after a successful user authentication.

We have been using this system very successfully since December 2003.

Neither the traffic, nor the number of users is high (cca. 400) at our site, but the system should scale well. An important current limitation is, however, that there is a single, flat namespace.

A detailed guide describing how to set the system up, and the perl administrative interface will be available at this address: http://xenia.sote.hu/~torlasz/networkshop/ .

Execution Time Based Attack of RSA Implementation

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME Méréstechnika és Információs Rendszerek Tsz.

Endrődi Csilla <endrodi@mit.bme.hu>
BME Méréstechnika és Információs Rendszerek Tsz.

Even the use of precisely examined cryptographic algorithms – like RSA – doesn't always guarantee the security level of the used method in connection with the used implementation. An attacker may often use the specialities of the implementation to achieve success. The physical form of systems have parameters like energy consumption (for example in the case of Smart Cards), running time etc., which can be measured while the cryptographic algorithm is running. In this way, they provide additional, "secondary" information about the secret keys and other secure data. This type of attacks is called "side channel attack".

The side channel attack based on time measurement is called timing attack, which already has published successful cases. Through this method the secret key can already be extracted with some 10.000 measurements in acceptable time. As the running time of these methods is linear or quadratic to the size of the key, these endeavours are very important.

For the more precise examination of the working timing attacks, we introduced a new side channel attack based on time measurement. Our model has three basic differences to the already published ones, which allow more precise measurements and execution tracing, and this way clearer connections and conclusions.

(1) The information set used by timing attack consists of the starting data and the time consumption of the cryptographic operation applied. The time measurement is a critical point because of the noises of the data and the measurements. In our method, we substituted the physical time with logical time. We assign the logical time needed by the operations ourselves. These values can then be summarised without any noise. An important precondition of the use is the knowledge of the source code and the correct logical time assignments. As these values can be set without restrictions, any test situation can be examined and any existing implementations can be simulated. The phase in which we set these parameters of the simulation is called the alignment process.

(2) Application of logical times has another advantage: in contrast to the previous methods we

can measure not only the total time usage of the algorithm, but the one of a single iteration as well. This is important, because the key cracking algorithm is based on the time consumption differences in the single iterations. The attacking method calculates the next bit of the key from these time differences. Without the knowledge of single iterations' time need, we can only use statistical methods.

(3) In one of the published methods, the false decisions (caused by noisy measurements and wrong probabilistic choices) are corrected with an "error correction property", as a false choice in the previous few bits can easily be recognised, and then corrected. But this possibility isn't always right either and the running time of the attack cannot be predicted (as we cannot see how many mistakes we will have to correct). In our method, we use a forward looking approach. We don't look for possible errors, but make key candidates. We do not have to choose the right bit every time. We only have to have the right choice always be amongst the candidates. As the number of the candidates is constant, there is no exponential explosion and the running time of the method can be previously approximated. The method allows us to calculate the number of candidates needed for the success.

The advanced timing attack is theoretically suitable to examine all algorithms, which contain a junction depending on the single bits of the secret key one after each other (most of the fast modular exponentiation methods satisfy this constraint). Our model has many further interesting possibilities to enhance.

In the presentation we will show the developed method for the case of RSA and the results we got. In connection with the theoretical background, further information can be found in our article "Implementation-dependent Attack of Cryptography Algorithms".

Sending authentic messages from malicious terminals

Berta István Zsolt <istvan.berta@crysys.hit.bme.hu>
BME, Híradástechnikai Tanszék

Bencsáth Boldizsár <boldi@crysys.hu>
BME, Híradástechnikai Tanszék

The user wishes to communicate with a remote partner over an insecure network. Since the user is a human being, a terminal is needed to gain access to the network. Various cryptographic algorithms running on the terminal may provide authenticity and/or secrecy for the user's messages.

In this paper the problem of sending authentic messages from insecure or untrusted terminals is analysed. In this case attackers are able to gain total control over the terminal, so the user must consider the terminal as a potential attacker.

Smart cards are often considered the ultimate tool for secure messaging from untrusted terminals. Although they are secure tamper-resistant microcomputers with strong cryptographic powers, their lack of user interface enables man-in-the middle attack from the terminal.

This paper analyses the usability of smart cards for the above problem, and investigates various possibilities for authentic communication between the user and the smart card. Since the user is a human being with limited memory and little computational power, it is questionable that authentic communication is possible between the above two parties in practice.

In the first part of my lecture, I review various solutions and protocols (e.g. visual cryptography, human computer cryptography, protocols for authenticating terminals, etc.) from literature that can aid the user in an untrusted terminal environment.

In the second part of my lecture, I propose a solution that can be implemented with smart cards that exist today and does not need the user to perform cryptographic operations.

Although the smart card cannot decide if the message came from the user or from malicious software running on the terminal, but can still aid the user in authenticating the message. This is possible if the user sends a so-called biometric message. A biometric message could be a video or

voice message. Such a message is very hard to manipulate, it may even require human interaction. In order to prevent the attack, the smart card should ensure that the attacker has no possibility, no time to perform such a complicated attack.
The smart card can be used as a secure time that can guarantee that the message was sent in a certain time frame. This way, the time the attacker has to manipulate the message can be severely limited so even simple algorithmic authenticators can provide strong security.

The GeneSyS project - Generic Systems Supervision Middleware

Pataki Balázs <pataki@dsd.sztaki.hu>
MTA SZTAKI

Kovács László dr. <laszlo.kovacs@sztaki.hu>
MTA SZTAKI

GeneSyS is a European Union project (IST-2001-34162) co-funded by the Commission of the European Communities (5th Framework). EADS Launch Vehicles of France is the project Coordinator, with University of Stuttgart (Germany), MTA SZTAKI (Hungary) and NAVUS GmbH (Germany) as participants. GeneSyS started in March 2002 with planned completion in September 2004.

The top-level objectives of the GeneSyS project are:
1. To specify and develop an open, generic, modular and comprehensive supervision concept,
2. To integrate and validate this supervision structure within various industrial contexts,
3. To achieve the adoption of the GeneSyS concepts by all stakeholders (internal and external to the consortium), and to ensure that the vision of the proposed generic structure will become a new emerging standard.

The first objective is aimed at specifying and developing a new supervision middleware for distributed systems and applications, as the need for a global and generic supervision solution has arisen among various industries in different domains such as space, maritime, medical, automotive and e-business ones. In fact, present solutions are mainly focusing on the supervision of low levels of a distributed system, i.e. hardware and network availability and monitoring. But these systems are becoming more and more complex and therefore, they need to be supervised in a new way:

- The supervision shall implement the control and monitoring not only of low level but also of higher levels (i.e. application, QoS, GroupWare) of the distributed system.
-The global supervision shall range from a passive monitoring of the resources to an active control of the applications running over these distributed systems.
-The supervision shall be applicable to a various set of different distributed systems and applications; i.e. it must be generic and open.

The second objective is to achieve a validation of the deployment and the use of the supervision solution, with an assessment of the benefits of a GeneSyS-based distributed application in an international, tool- & network-heterogeneous system environment. Relevant and realistic scenarios based on real user-cases of the industry support the validation process.

The GeneSyS project is now over its first phase resulting GeneSyS V1 that is available as free and open source from SourceForge.net.

The next phase of the Project concentrates on adding more intelligence to the system with the use of intelligent software agents that will make it not only a successful research project but also a product ready for commercialisation.

CERTIFICATION AND TESTING OF ANTIVIRUS PRODUCTS

Leitold Ferenc Dr. <fleitold@veszprog.hu>
Veszprémi Egyetem

Kárpáti Nikoletta <niki@veszprog.hu>
Veszprog Kft.

Software testers and quality engineers have to test their programs in as many various environments as it is possible with a lot of input combinations. In the case of anti-virus products this task is more difficult because the product changes continuously, newer and newer procedures are being built in them. Anti-virus software usually include several thousands of detection and disinfecting algorithms, which should be tested on a great number of virus samples and of course on non-virus files as well.

The main purpose of CheckVir project is to provide independent anti-virus testing for users and for anti-virus developing companies. Antivirus software testing was started from April 2002 and from then the testing procedure had been executed monthly on different platforms using various virus sets.

During the CheckVir anti-virus testing project, the anti-virus certification program is going to start from **January 2004**. All of anti-virus products that are tested during the CheckVir anti-virus project are participating in the certification process, too.

There are two different levels of certification:

1. **Standard Level**: Only the virus searching capability will be examined. The AV software products have to find all of the tested virus samples
2. **Advanced Level**: Virus searching and killing capability will be examined. Anti-virus products have to accomplish the conditions of Standard Level and the followings as well:
    - •The code of virus has to be removed from the infected object in the case of all virus where it can be done theoretically
    - • The repaired object must still be usable.
    - •Loss of information during the removing process is allowed, but the user should be informed before it. For example during the remove of a macro virus from the document the AV can remove all of the macros from the document but the user should be informed before this action.

During the certification process both **on-demand** and **on-access** scanning are tested.

In this paper, the results of the CheckVir project are summarised and the certification project is highlighted as well.

SAFETY DIGITAL SIGNATURE IN AMBIGUOUS ENVIRONMENT

Leitold Ferenc Dr. <fleitold@veszprog.hu>
Veszprémi Egyetem

The safety of the usage of digital signature is certified by the followings:

- Public Key Infrastructure (e.g. RSA algorithm).
- The Hungarian law about digital signature certifies the mapping the secret key and

the person who uses it. It also certifies that the digital signature was valid when it was created.

- Devices for creating digital signature are certified by organisations assigned by the law of digital signature.

The biggest problem of the mentioned things is the third even if a computer – which is used for other purposes – is used for creating digital signature. How big is the risk of this problem? How can be increased the safety of the usage of digital signature? What kind of methods and tools should be used for this purpose? During the presentation of this paper I would like to present some security problems, samples related to the usage of digital signature.

IBM BladeCenter - Management, not only for managers

Varga Zsolt <zsolt_varga@hu.ibm.com>
IBM Magyarország Kft.

Many organisations have begun consolidating servers into centralised data centres, looking to use physical, application or data consolidation as a means of reducing the challenges and costs associated with administering many small servers scattered across the enterprise.

A blade server is a type of rack-optimised server that eliminates many of these complications, thus providing an effective alternative to 1U and 2U servers. There is a range of blade server designs-from ultradense, low-voltage, lesser-performing servers to high-performance, lowerdensity servers to proprietary, customised rack solutions-that include some blade features.

By design, IBM BladeCenter can offer the benefits of tremendous horizontal scalability in a small space, the versatility to mix and match types of blades within a single chassis, a performance spectrum ranging from low cost to high performance/high availability, with quick and easy serviceability, enhanced manageability and simplified deployment, and significant cost savings-both upfront and long-term.

INTERNET INTRUDERS

Krausz Tamás dr. <kuka@delfin.unideb.hu>
Debreceni Egyetem

Spyware programs are any software which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission. Silent background use of an Internet "backchannel" connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use. Any software communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed: Spyware.

Today, the word has broadened and shifted in meaning. "Spyware" is an emotionally charged word, and often means different things to different people. Sometimes the term is used to mean Adware, or Browser Helper Object or Hijacker or Trojan, but in all cases, the user of the word is referring to software that they did not intend to introduce to their machine, do not want, and are having trouble removing.

Execution Time Based Attack of RSA Implementation

Endrődi Csilla <endrodi@mit.bme.hu>
BME MIT

Csorba Kristóf <kristof@impulzus.sch.bme.hu>
BME MIT

Even the use of precisely examined cryptographic algorithms – like RSA – doesn't always guarantee the security level of the used method in connection with the used implementation. An attacker may often use the specialities of the implementation to achieve success. The physical form of systems have parameters like energy consumption (for example in the case of Smart Cards), running time etc., which can be measured while the cryptographic algorithm is running. In this way, they provide additional, "secondary" information about the secret keys and other secure data. This type of attacks is called "side channel attack".

The side channel attack based on time measurement is called timing attack, which already has published successful cases. Through this method the secret key can already be extracted with some 10.000 measurements in acceptable time. As the running time of these methods is linear or quadratic to the size of the key, these endeavors are very important.

For the more precise examination of the working timing attacks, we introduced a new side channel attack based on time measurement. Our model has three basic differences to the already published ones, which allow more precise measurements and execution tracing, and this way clearer connections and conclusions.

(1) The information set used by timing attack consists of the starting data and the time consumption of the cryptographic operation applied. The time measurement is a critical point because of the noises of the data and the measurements. In our method, we substituted the physical time with logical time. We assign the logical time needed by the operations ourselves. These values can then be summarized without any noise. An important precondition of the use is the knowledge of the source code and the correct logical time assignments. As these values can be set without restrictions, any test situation can be examined and any existing implementations can be simulated. The phase in which we set these parameters of the simulation is called the alignment process.

(2) Application of logical times has another advantage: in contrast to the previous methods we can measure not only the total time usage of the algorithm, but the one of a single iteration as well. This is important, because the key cracking algorithm is based on the time consumption differences in the single iterations. The attacking method calculates the next bit of the key from this time differences. Without the knowledge of single iterations' time need, we can only use statistical methods.

(3) In one of the published methods, the false decisions (caused by noisy measurements and wrong probabilistic choices) are corrected with an "error correction property", as a false choice in the previous few bits can easily be recognized, and then corrected. But this possibility isn't always right either and the running time of the attack cannot be predicted (as we cannot see, how many mistakes we will have to correct). In our method, we use a forward looking approach. We don't look for possible errors, but make key candidates. We do not have to choose the right bit every time. We only have to have the right choice always be amongst the candidates. As the number of the candidates is constant, there is no exponential explosion and the running time of the method can be previously approximated. The method allows us to calculate the number of candidates needed for the success.

The advanced timing attack is theoretically suitable to examine all algorithms, which contain a junction depending on the single bits of the secret key one after each other (most of the fast modular exponentiation methods satisfy this constraint). Our model has many further interesting possibilities to enhance.

In the presentation we will show the developed method for the case of RSA and the results we got. In connection with the theoretical background, further information can be found in our article "Implementation-dependent Attack of Cryptography Algorithms".

Security questions of local area networks

Ács György <gacs@cisco.com>
Cisco Systems Magyarország Kft.

I will present the security vulnerabilities and mitigation techniques in local area networks. The presentation deals with security features of local area network devices; i.e. ethernet switches and wireless access points. The presentation helps to defend this very important network area. There will be introduced the Cisco-developed new, self-defending network security approach.

Anti-Spam rules in the Hungarian law system

Dósa Imre dr. <dosa@jak.ppke.hu>
ONYF

Legal definition of the Spam in the Hungarian law.

- The advertisement characteristics of the spam
- Practice of the opt-in procedure
- Legal consequences
- Lawful protecting steps
- News at the EU integration

The Spam irritate the Internet users. The lecture is a review of the Hungarian legal rules, focusing on the e-commerce law and the law of the advertising.

HOW WE ARE SUPPORTING THE ACADEMIC SOCIETY? SPONSORS FORUM

Reference model at Mannheim University: lunch and control la carte

Szüllő Zsolt <zsolt.szullo@siemens.com>
Siemens Rt.

The past several years have marked the rise of mobile technologies and the first generation of Internet Protocol-based communications (1gIP), with a much needed focus on IP-enabling voice and real-time communication infrastructures – both public and private. Today, we forge ahead with a new generation of technology that leverages the IP infrastructure to provide entirely new ways to construct relationships among all of our communications resources; to bring new intelligence and applications into the picture; and to create more efficient and powerful ways to communicate.

The Hosted HiPath solutions of Siemens' LifeWorks concept describes the new intelligent intersections between public and private communication services in this, the second generation of IP-based communications (2gIP). As part of its next-generation network strategy, Siemens creates a second generation IP fabric that tightly weaves together all of the tools that we use to communicate, both at work and in our private lives, enabling businesses and individuals to tailor solutions that balance accessibility and intrusion; flexibility and complexity; information and intelligence

GRID

Vitéz Gábor - Stefán Péter <vitezg@niif.hu, stefan@niif.hu>
NIIF Iroda

The tutorial aims at surveying key features of the Hungarian ClusterGrid infrastructure, and gives brief introduction into the cluster installation process and user support activity.

1. ClusterGrid introduction
1.1. The general view, project history
1.2. The cluster resources, dual purpose computer labs
1.3. The layered structure model
1.3.1. Physical layer
1.3.2. Link layer
1.3.3. Network fabric layer
1.3.4. Operating system layer
1.3.5. Resource layer
1.3.6. Grid layer
1.3.7. Application and job layer

2. Cluster installation
2.1. Server configuration
2.1.1. Fundamental server functionality
2.1.2. The grid resource broker
2.2. PC configuration
2.3. Network configuration
2.4. The installation process

3. Using the grid
3.1. User authentication and job identification
3.2. The "user process" cycle
3.2.1. Software development
3.2.2. Parallelization
3.2.3. Porting and compilation
3.2.4. File transfer
3.2.5. Job handling
3.3. The "jobdir" job format
3.4. Debugging

4. Future prospects and goals

Videoconference tutorial details

Kovács András <akov@niif.hu>
NIIF Iroda

What is videoconferencing? Videoconference history

- Definition of videoconference
- Videoconference vs. streaming: which should I choose? How is related each technology to the other?
- H.323 basics:
- H.323 protocol technical background
- H.323 network elements
- Communication of network elements
- Videoconference endpoints in general
- Endpoint types
- Technical parameters
- NIIF videoconference service
- What has happened so far?
- Gatekeeper network, zones, GDS connection
- MCU service
- Plans for year 2004
- Network security considerations Etiquette, placement, environment Streaming
- NIIF streaming service

Video on Demand archive and E-learning

PKI, Directory Services and Authentication

Magyar Zsuzsanna <magyarzs@sztaki.hu>
MTA SZTAKI

Bajnok Kristóf <bajnokk@sztaki.hu>
MTA-Sztaki

Transferring information secure from place A to B is something that has been concerning scientists for thousands of years. However, instead of historic review, the tutorial will be dealing with requirements and technology of today.

As an introduction, pros and contras of different cryptographic procedures (symmetric and asymmetric cryptography) are examined as well as questions, which require application of trusted third party. Details of the Public Key Infrastructure is described by many different standards: X.509, PKCS, etc. To demonstrate the function of each, an open source tool, OpenSSL is used.

In the second part, both theoretical and practical details of PKI are examined. Directory Service is an important component of PKI as most of the solutions presume an available LDAP Directory. LDAP, however is not only a database to store certificates, while validation of the certificates may be based on Directory attributes.

Client-side certificate-based authentication and authorization are the topics of the third part. Privilege Management Infrastructure of IETF X.509 (PKIX) Working Group is one solution to authorization problems. Another approach may be to use LDAP bind operation for authentication and authorization.

Spanning Tree Protocol

Jákó András <goya@eik.bme.hu>
BME EISZK

Most Ethernet networks and therefore almost every local area network runs Spanning Tree Protocol. However, network administrators usually know very little about it. For most of them Spanning Tree Protocol is something that "just works". As many examples show worldwide, the lack of knowledge often leads to networks operating in a suboptimal way. In other cases misuse of the Spanning Tree Protocol causes severe network failures, or even worse, some LANs collapse completely.

This tutorial tries to fill these gaps. It gives a comprehensive description of the Spanning Tree Algorithm and Protocol, its operation, and also tells the proper way to use it. The tutorial will cover the operation of transparent Ethernet bridges and switches; the Spanning Tree Protocol as specified by the IEEE 802.1d standard; some non standards based but often implemented extensions of 802.1d STP; and the new extensions to the standard, specified in the 802.1w (Rapid Reconfiguration) and the 802.1s (Multiple Spanning Trees) documents.

Szerzők/Authors

Tartalomjegyzék / Table of contents

Mibe kerül Önnek, ha meghibásodik a számítógép hálózata?

Előzze meg!

Ebben segít Önnek a Siemens Netcheck®

A Siemens Netcheck® cégének költség és erőforrás megtakarítást eredményez, amely a hálózat meghibásodásából, leállásából, az adatok sérüléséből, a partnerek nem megfelelő szinten történő kiszolgállásából származhat.

SIEMENS

Innovációk világhálózata

FELKÉSZÜLT?

A küszöbön álló Európai Uniós csatlakozás, a hallgatói létszám várható csökkenése, továbbá a kétszintű felsőoktatási rendszer bevezetése eddig nem tapasztalt kihívásokat, ugyanakkor új lehetőségeket is jelent a hazai felsőoktatás számára.

Az intézmények az oktatási-kutatási színvonal folyamatos emelése mellett az **informatikai infrastruktúra és szolgáltatások révén is megkülönböztethetik** magukat az élesedő versenyben.

- A XXI. század campusán a hallgatók és az oktatók a **802.11g/b szabványú vezeték nélküli hálózat**nak köszönhetően biztonságos módon, bárhol, bármikor hozzáférhetnek az internethez és az intézményi hálózathoz.
- A **Cisco IP telefónia** által kínált mellék-mobilitás teljeskörű mellékhordozhatóságot tesz lehetővé, valamennyi felsőoktatási intézményre kiterjedően. Az oktatók így azonosítójuk segítségével bármely készülékről úgy telefonálhatnak, mintha az saját mellékük lenne, és a készüléken saját beállításaikat is megtalálják.
- A hallgatók az interneten és a **Cisco IP alapú Contact Center**en keresztül gyorsan és hatékonyan intézhetik tanulmányi ügyeiket.
- A felhasználók otthonról az **IPSec VPN** technológia alkalmazásával biztonságosan kapcsolódhatnak az intézményi hálózatokhoz, **távoktatási** programokon vehetnek részt.
- A hálózathoz való hozzáférés - valamint azon belül a megfelelő VLAN-hoz való hozzárendelés - intelligensen szabályozható a **802.1x protokoll** alkalmazásával.

A CISCO SYSTEMS HÁLÓZATI MEGOLDÁSAI SEGÍTENEK ÖNNEK A XXI. SZÁZAD HÁLÓZATI INFRASTRUKTÚRÁJÁNAK MEGVALÓSÍTÁSÁBAN. KÉRJÜK KERESSE FEL A NETWORKSHOP 2004 HELYSZÍNÉN TALÁLHATÓ CISCO BEMUTATÓT, AHOL RÉSZLETESEBB TÁJÉKOZTATÓVAL VÁRJUK.

A CISCO MEGOLDÁSAIRÓL A WWW.CISCO.COM/HU WEBOLDALON OLVASHAT.
TOVÁBBI INFORMÁCIÓVAL GÁSPÁR IMRE ÁLL RENDELKEZÉSÉRE A (06-1) 225 4660-AS TELEFONSZÁMON.

CISCO SYSTEMS

THIS IS THE POWER OF THE NETWORK. NOW.


A csapat
létszáma:
egy fő
Egy fő-rendszerintegrátorral minden egyszerűbb
A Matáv egyedüli infokommunikációs fővállalkozóként fogja össze a legjobb informatikai partnereket személyre szabott üzleti megoldásaihoz.
Bízza ránk a csapatépítést!
A Matáv tagvállalataival – Axelero, BCN, Cardnet, CompArgo, MatávCom, SafeCom, X-Byte – és partnereivel kidolgozott komplex üzleti megoldásai választ adnak Önnek mind informatikai, mind távközlési igényeire, az összehangolt elemek pedig hatékonyan támogatják cége üzletmenetét.
matáv
a szavakon túl
www.matav.hu

SYNERGON

A Synergon Informatika Rt., mint vezető hazai IT megoldásszállító és a hálózatintegrátor piac legnagyobb szereplője – ahogy minden évben, idén is – a Networkshop támogatója. A rendezvény szervezője, a NIIF és a Synergon aktív szerepet kíván játszani a VoIP technológia elterjesztésében az információ-technológia nyújtotta társadalmi és gazdasági előnyök kiaknázása érdekében.

Az eseményen programjaink kiemelkedő szakmai értéket képviselnek:
- a **„Digitális archívumok"** előadás során megismerhetik a legkülönfélébb módon tárolt információtömeg korszerű és hatékony kezelését, felhasználását.
- **„Szervezeti portálok – egészen másként"** előadás keretén belül bemutatjuk a csoportmunka hatékony támogatásának e modern eszközét, valamint azt, hogy egy jól átgondolt dokumentummenedzsment-rendszer bevezetésével hogyan optimalizálható a napi működés, lényegesen csökkentve annak költségeit.
- az **„IP telefon szolgáltatás az Interneten I."** előadás során betekintést nyerhetnek a végponttól-végpontig terjedő, tisztán IP hálózaton megvalósított telefonszolgáltatás működésébe. Alkalmazási példákon keresztül mutatjuk meg a hálózat funkcionális elemeit, valamint az érintett protokollokat, szükséges hardver és szoftver részegységeket.
- az **„IP telefon szolgáltatás az Interneten II."** előadáson ismertetésre kerül egy hívásvezérlő alkalmazás, mely a klasszikus szolgáltatói telefonközpont funkcionalitást emeli át az IP telefon környezetbe.

Az előadáshoz kapcsolódó technikai demonstráció a Synergon standon, a konferencia teljes időtartama alatt megtekinthető.

Nyerje meg fődíjunkat, egy digitális fényképezőgépet vagy nyerjen egyet egyéb értékes ajándékaink közül!

Minden látogató, aki a regisztrációs csomagban található Synergon kérdőívet kitölti és leadja a Synergon standján vagy a Synergon bármelyik szekció előadásán részt vesz, tombolát kap és részt vesz sorsolásunkon. További részletek a Synergon standján.

Synergon Informatika Rt.
1047 Budapest, Baross u. 91-95. tel.: 399-5500 fax: 399-5599
e-mail: info@synergon.hu www.synergon.hu

J E G Y Z E T E K

J E G Y Z E T E K