NEWS

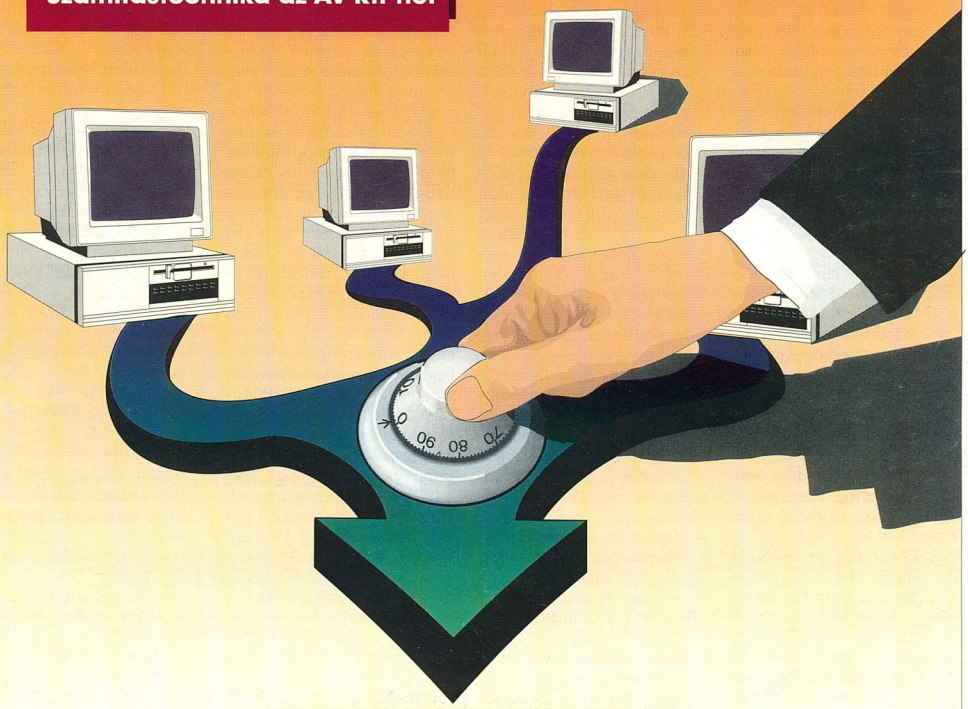
MONTANA

18. szám

1994. október

Csoportmunka –
Lotus Notes

BanyanVines és a
Gigantikus Adatbázis –
Számítástechnika az ÁV Rt.-nél



Secure Data Networking-
Adatvédelem hálózatokon

Csoportmunka

Az amerikai Lotus cég terméke a Notes (Megjegyzések) nevű program, amely a cégek informatikai feladainak megoldását hivatott segíteni. Mióta csak kitalálták az ellenfelek két dolgot tehetnek: vagy megveszik, vagy csinálnak egy hasonlót. A hasonlók többsége gyenge eresztésnek bizonyult. Mi tette ilyen gyorsan népszerűvé ezt a programot?

Minden cég szeretné ha a házon belüli információáramlás egyszerűen szervezhető és követhető lenne. Számítógépes munkánál ehhez olyan felhasználói felület is kell, amely minden szinten lehetőleg egységes. Ha ez egyszerű lenne, már régen kitalálták volna. De nem találták ki. Eddig.

Kezdjük talán az alapoktól: Mi is az információ ? Formális definíció helyett álljon itt egy pragmatikus megfogalmazás: információ mindaz, aminek ismerete a cég hatékony működése szempontjából fontos. Persze más információ kell a kereskedőnek, mint a projektvezetőnek.

A kérdés az, hogy a különböző információkat lehet-e egységes elvek alapján kezelni - rögzíteni, megjeleníteni, feldolgozni, továbbítani, csoportosítani, törölni - és lehet-e az információ-kezelést és annak eredményét egységes felülettel megvalósítani ill. megmutatni. A Notes. válasza az, hogy igen, lehet.

Kettős feladat

Az első probléma az információk ábrázolásának formai különbözősége. A műszaki információknál azok szöveges, táblázatos, képes megjelenítése is fontos. A gazdasági információk kezelésénél a táblázatos és grafikonos ábrázolás a legmegfelelőbb. Az egységes felhasználói felületnek mindazt tudnia kell, ami a vezetői, kereskedői, karbantartói, mérnöki munkához kell.

A következő probléma a hozzáférés. Van aki csak el akar olvasni valamit, másra nincs joga és felhatalmazása, van aki egy termék vagy szerződés élettörténetét szeretné megnézni. Van aki bevihet új információkat, van aki már meglevő, rögzített információt javíthat is, és van aki törölhet is a mások által bevitt információkból.

Az irodai és termelésirányítási munka analízise során elemezték, milyen jellegű információáramlás történik egy szervezetben. Az információ keletkezésének, mozgatásának, elévülésének elemzése alapján négy tipikus, különböző jellegű információ-tárolást és szétosztást csoportosítottak.

– *Követés*
Objektív és szubjektív adatok gyűjtésével jellemezhető, ahol az információhalmaz állandóan nő. Többnyire több munkatárs is közreműködik az információ gyűjtésében. Példa: szervízszolgálat, a bejövő hívások és azok tartalmának rögzítése.

– *Hirdetés*
Legtöbbször statikus információ, amely sokszor időkritikus (értékét rövid időn belül elveszíti) és sok ember számára kell elérhetővé tenni. Példa : leendő esemény vagy valamilyen eredmény ismertetése.

– *Referencia*
Hasonlít a hirdetésre, amennyiben sok ember használja, de jellemzője hogy tartalmát hivatkozásként használják. Maga a dokumentum időben változhat. Példa: referencia kézikönyv, szótár, telefonkönyv, publikációk jegyzéke.

– *Megbeszélés (diszkusszió)*
Vélemények, azokra adott válaszok, ellenvélemények gyűjtése és rendelkezésre bocsátása. Példa: ötletbörze.

Ezek tehát jellegzetes információkezelési típusok. Érdemes megfigyelni, hogy ezek a típusok minden cégnél ill. hivatali egységnél megfigyelhetők, függetlenül a mérettől. Emellett a felhasználó szabadon csinálhat más jellegű adatbázist is a Lotus Notes segítségével. Mivel a legjobb a testreszabott alkalmazás, ebben az értelemben a Lotus Notes az integrátor szerepét tölti be. A felhasználó megtervezi a célnak leginkább megfelelő adatbázisokat, azokat a Notes könnyen kezelhető módon megvalósítja.

Dokumentum mindenhol

Dokumentum: ez a Notes kulcsszava és egyben alapegysége is. Minden információ dokumentumként jelenik meg, még a Lotus Notes működésével kapcsolatos, operációs rendszer szintű üzenetek is. Ennek ellenére nem okos dolog az egész programot dokumentumkezelő rendszerként felfogni. Ez egy egységes felületű információkezelő rendszer, ahol az információk dokumentumokban vannak letéve.

A cégen belüli információ keletkezése mindig köthető egy dokumentumhoz. Hibabejelentés, munkaerőfelvétel, fizetésemelés, szabadságkérés, megbízás, árurendelés, stratégiai terv elkészítése, egy megbeszélés eredménye – ez mind megadható, vagy leírható egy dokumentummal. Persze a felhasználónak is az a legjobb, ha csak egy jól megszerkesztett formanyomtatványt kell kitölteni. Még jobb, ha az állandóan ismétlődő, vagy már előre ismert adatokat a program maga tölti ki. A programhoz számtalan "űrlaptípust" kapunk, de természetesen magunk is készíthetünk újakat.

Nem minden információ jelenik meg külön dokumentumban. Egy termék árának változása egy dokumentum egy elemének változtatását jelenti. Ekkor a kérdés az, ki hozhat létre ill. módosíthat egy dokumentumon.

A jognak asztalánál

A dokumentumokat célszerű csoportosítani, nem pedig az összes keletkező dokumentumot egyetlen helyre lepakolni. A csoportosításkor ún. adatbázisokat hozunk létre. Ezek az adatbázisok adatvédelem szempontjából külön életet élnek.

Ha már készülnek dokumentumok, természetes dolog hogy szabályozva legyen ki és hogyan olvashatja, módosíthatja, terjesztheti, másolhatja azokat.

Maga a Notes a következő lehetőségeket adja, mit csinálhat egy Notes felhasználó:

– nem láthat, nem szerkesztheti semmit (nincs hozzáférés)
– nem láthat semmit: létrehozhat egy adott tipusú dokumentumot, de azt a létrehozás után már nem láthatja (szavazólap)
– dokumentumokat olvashat (olvasó)
– olvashatja a dokumentumokat, ő maga létrehozhat újakat is. Az általa létrehozott dokumentumokat később is átszerkesztheti. (szerző)
– olvashatja a dokumentumokat, szerkesztheti is azokat (szerkesztő)
– olvashatja a dokumentumokat, szerkesztheti azokat, változtathatja az adatbázis felépítését (adatbázis tervező)
– teljes jogosultság (manager)

Az itt megadott általános hozzáférés tipus mellet vannak még finomságok. Ilyen például, hogy minden dokumentumhoz egyedi hozzáférési lista is megadható. Ekkor az egyedi listán megadott jogok felülirják a dokumentumtípushoz tartozó általános jogokat.

(folytatás a 4. oldalon)

Professzionális programfejlesztés WINDOWS környezetben

A Montana csoporthoz tartozó IDEON Szoftver Kft és a Montana Consulting Kft közös rendezésében augusztus 22-24 között került sor első ízben ezen rendezvényünkre.

Az előzményekhez tartozik, hogy az előadóval,aki a freiburgi Management Academy munkatársa, az idei CEBIT-en kerültünk kapcsolatba. Az általa kifejlesztett eljárás a példákon keresztül a Clipper felhasználókat célozta meg. Ennek ellenére, illetve emellett bárki, aki Windows programozással szeretne foglalkozni, minden nehézség nélkül be tudott illeszkedni a tanfolyam menetébe.

A szervezőket elsősorban az ragadta meg, hogy Magyarországon sok Clipper alkalmazás létezik, amelyeket a számítástechnika fejlődésével valamely irányba modernizálni kell. Így jutottunk arra a gondolatra, hogy a piaci elvárásokat és a Management Academy által kifejlesztett és kínált lehetőséget összekapcsoljuk.

Az első napon workshop-ot tartottunk, ahol gyakorlatilag a módszer ismertetésére került sor. Néhány kulcsszó az anyagból

- Mivel fejlesszünk Windows alkalmazásokat ? (C, C++, Visual Basic, Visual Object, Clipper)
- A Windows felület fejlesztési eszközei
- Portabilitás
- Memoriakezelés
- Clip4WIN

Teljességében a tanfolyamon szereplő témaköröket nem lehet felsorolni, mivel a résztvevők saját maguk kérdéseikkel is bővíthették, alakíthatták az előadás tematikáját.

A workshop-ot követő kétnapos szemináriumon a tanfolyami anyag mellé az átállítást megkönnyítő programokat is kaptak a résztvevők . A teljesség igénye nélkül pár téma a tanfolyam anyagából:

- a Windows alapkoncepciója
- modális és nem modális technika
- ablakok felépítése
- egér , billentyűzet
- fejlesztési környezetek

A hallgatók érdeklődésére jellemző, hogy a meghírdetett tanfolyami időn túl is kérdésekkel ostromolták az előadót.

A jó hangulatú előadások után úgy döntöttünk, hogy ismét megrendezzük október 19-én a workshop-ot, 20-án 21-én a kétnapos szemináriumot, melyet november 14-19 egy háromnapos továbbképzés követ.

Rendezvényeinkre minden érdeklődőt szívesen várunk.

Géresi János Monatana Consulting

Jankó Mihály IDEON Szoftver

A Kedves Olvasóval

ezúton szeretnénk tudatni, hogy újságunk visszatért nyári szabadságáról. Reméljük a nyájas olvasónak sikerült egy kellemes vízparton átvészelni a még Aigner Szilárd által sem ismert hőséget. Míg nálunk a Steindl Imre utcában felforrt az aszfalt, honatyáink más bosszantáson törték a fejület. Hiába menekültünk a hűsítő habok, árnyas fák felé, egy idő után mégis elért bennünket a rettegett hír, hogy már megint alábbhagyott a Ft értéke, okozva ezzel lázas számolgatást, hogy mennyivel is kell már megint drágábbnak lenni.

Volt akit mindez hidegen hagyott és visszatért inkább az iskolapadba, hogy elfeledje azt a régi jó Clippert és most már az időközben oly divatossá vált Windows környezetben programozzon. A nagy sikerre való tekintettel Jankó Misiék (Ideon Szoftver Kft.) októberben új osztályt indítanak a Montana Consulting-gal karöltve.

A Montana Kriptológia munkatársainak pedig úgy érezzük, kifejezetten jót tesz a meleg. Egy háromrészes sorozat teljes anyagával tértek meg a jól megérdemelt vakációról. Reméljük, hogy a folytatásokban kitanult titkolódzást segítségükkel mindenki sikeresen fogja használni.

Szóval sokaknak munkával telt a szabadsáég. És hogy vége csak abból veszik észre, hogy újra és egyre nagyobb körben keringhetnek a szomszédos háztömbök körül, mire rálelnek egy darabkára a kincset érő aszfaltból. Mert hogy az bezzeg nem inflálódik...

NEWS
MONTANA

Kiadja a Montana Marketing Kft.
1054 Budapest, Steindl Imre u. 6. Tel:269-5564 Fax:269-5573
Felelős kiadó: Kövér Hedvig, a Montana Marketing Kft. ügyvezetője
Szerkesztő: Lesták Zsuzsa
Megjelenik kéthavonta 10.000 példányban
1994 Montana Marketing Kft.
Nyomás: Ságvári Nyomda
Felelős vezető: Szilágyi Tamás

(folytatás a 2. oldalról)

Minél nagyobb a cég, annál nehezebb kezelni az információkat. Adatkarbantartási segítség az, hogy a hozzáférési jogok szempontjából azonos személyeket csoportokba lehet osztani, és az adatbázishoz tartozó jogok kiosztásánál elég a csoportra vonatkozó jogokat megadni.

Mit gondolnak, a Notesben a felhasználói csoportok létrehozása hogyan történik? Szerintem sejtik a választ: létrehozunk egy új dokumentumot aminek típusa csoportleírás. Ebben fel kell sorolni az adott csoporthoz tartozó személyek neveit. Ennyi. Amikor a személyek változnak, a nevek felsorolását változtatjuk, amikor meg akarjuk szüntetni a csoportot, csak ezt a dokumentumot kell törölni.

És ha azt mondom: gömbcsukló?

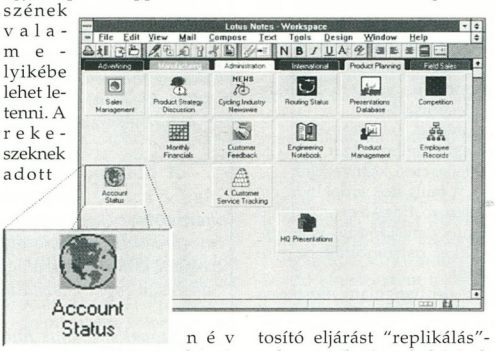
Főleg műszaki információk keresésénél nagy segítség a szó alapján történő keresés. Ennek lényege az, hogy azokat a dokumentumokat keressük egyszerre egy vagy több adatbázisban, amelyekben egy vagy több adott szó vagy kifejezés előfordul.

Ebben a teljes szóra történő keresésben nagyon jó a Notes - a piacon kapható legjobb szöveges visszakeresőt vette meg a Lotus. A Verity – amely cég a nagykapacitású, gyors dokumentumvisszakereső rendszerek (Topic) fejlesztésében élen jár – átadta a Lotusnak szókereső programjának legujabb változatát.

Erre a kereső programra jellemző, hogy a dokumentumokat a találati eredmény alapján sorrendbe szedi. A lista elején szerepelnek azok a dokumentumok, amelyekben az adott szó vagy kifejezés gyakrabban szerepel. A dokumentumok kiválasztásánál logikai operátorokat is lehet használni.

A teljes szövegkeresés a szavakat ragozott alakjukban is megtalálja. Bár az eredeti program természetesen csak angolul tud, Magyarországon magyar menüvel és magyar szótókereső eljárással is forgalmazzuk a programot. Az újabb dokumentumok érkezése miatt azokat az index-állományokat, amelyek segítik a gyors szókeresést, úrja kell építeni. Ezen index-állományok építése bármikor történhet, az nem zavarja vagy korlátozza a lekérdezés használatát.

A felhasználói felület igen egyszerű és könnyen kezelhető. Az adatbázisokat egy-egy képi szimbólum, ún. ikon jelzi. Az adatbázis tervezője maga tervezheti meg ezeket az ikonokat. Az adatbázisoknak nevet lehet adni, ekkor nem kényszerülünk DOS-os filenév konvenciók betartására. Az adatbázisokat egy elképzelt mappa hat rekeszének valamelyikébe lehet letenni. A rekeszeknek adott



név bármikor változtatható. Az adatbázisok is egy egérkattintással és húzással áttehetők egyik rekeszből a másikba.

Az adatbázis jelölő ikonra duplán kattintva kinyílik az adatbázis. A Lotus Notes nagyon nagy előnye, hogy az a felület, ahogyan egy adatbázist kezel a felhasználó, minden adatbázisra ugyanaz, és az információ mindig abban a formában jelenik meg, ahogyan azt a rendszerbe bevitték. Nem szerénytelenség azt mondani, hogy a program általános használata tíz perc alatt megtanulható.

Háttér kérdések

Az adatbázisokat tervezőjük összekapcsolhatja. Ekkor az egyik adatbázis használata közben lekérdezhetünk egy másik adatbázist is. A lekérdezés közbeni a felhasználó akár észre sem veszi, hogy a kérdésére adott válasz közben egy másik adatbázist is használtunk. Nem a Noteshoz tartozó adatbázist is használhatunk, igaz, ehhez egy külön programot kell megvenni.

Azonos források

A Lotus Notes-ot úgy tervezték meg, hogy a mobil felhasználó is hatékonyan tudja használni. A centrális adatbázis helyett a felhasználók több, célszerűen elhelyezett, ugyanolyan tartalmú adatbázist használhatnak. Az adatbázisok azonosságát biztosító eljárást "replikálás"-nak nevezik. Az adatbázisok kiegyenlítése mögött az a felismerés áll, hogy egy fizikailag nagy területen elhelyezkedő, pl. nemzetközi cég alkalmazottjai csak akkor tudnak hatékonyan egymással kommunikálni, ha mindenki ugyanazon adatbázisból dolgozik. Az azonnal továbbítandó információt mail-en, a pár órás vagy napos késést megengedő információt az adatbázison keresztül kell továbbítani.

A fizikailag több példányban létező adatbázisok között szükség szerint indítható a kiegyenlítés. Mindenki az adatbázisnak hozzá legközelebb eső példányát használja. A replikálás legtöbbször éjjel, telefonvonalon keresztül történik, ehhez a Lotus Notes egy beépített mail funkciót is tartalmaz.

Amikor egy alkalmazott telefonon keresztül akarja a Notes programot használni, azonosítása jelszóval történik. Amennyiben nem szeretnénk, hogy ilyenkor lehallgatható és interpretálható formában menjen adat a vonalon, a teljes dokumentumot vagy annak megfelelő mezőjét rejtjelezni kell. Erre a Notes, beépített rejtjelzőt kínál.

A Lotus Notes kompatibilis a többi Lotus termékkel, de nem minden Microsoft termék minden verziójával. Ezt nagyon jó OLE lehetőségeivel egyenlíti ki.

Nem olcsó, de jó

Mindenkinek lehetnek saját gépen levő lokális adatbázisai és használhatja az egyik központi gépen levő adatbázisokat. A központi és a személyi gépeket összekapcsoló hálózati szoftver lehet Novell, Banyan VINES, vagy TCP/IP. A központi gépeken többtaszkos - többfelhasználós operációs rendszer fut. Jelenleg OS/2 2.1 és Solaris 2.2 lehet, de kisszámú felhasználó esetén Windows is lehet.

A Lotus Notes minden eszközt megad, hogy minden cég a számára legmegfelelőbb struktúrába tegye le az adatait. Minden felhasználó a tartalomtól függetlenül egységes felületen keresztül keresi vissza és hozza létre az információkat.

Ami terjed az vagy olcsó, vagy jó. A Lotus Notes terjed. Hogy miért? Szerintem mert jó. Előnye a könnyű kezelhetőség, az egységes információkezelés és a megoldott adatvédelem.Hátránya a magas egyszeri beruházási költség és a nem széleskörű kompatibilitás.

A Lotus Notes mégis jó beruházás, mert csak néhány embert kell megtanítani a saját adatbázisok tervezésére, a többséget nem kell több hetes oktatásban részesíteni. Az adatbázisok utólag is egyszerűen módosíthatók.

Varga György

SECURE DATA NETWORKING

Korábbi cikkeinkben a kriptográfiát különböző elméleti szempontok alapján tárgyaltuk, amibôl látni lehetett, hogy a biztonsági szolgáltatások hogyan alakíthatók ki eltérő mechanizmusokból és eljárásokból. A szolgáltatásokhoz menedzsmentre van szükség , és ha igény van a különböző számítógéprendszerek közötti kapcsolatra is , akkor szükséges a szabványosítás is.

Újabb három részes sorozatunkban néhány olyan valóságos biztonsági rendszert és terméket mutatunk be, amelyek a korábban ismertetett elképzeléseket, elméleteket és szabványokat foglalják magukba.

Nem kíséreljük meg, hogy a bemutatás átfogó legyen, inkább tipikus rendszerek (melyek banki és pénzügyi tranzakciók biztonságos végrehajtását végzik) és a biztonsági termékek hardverek, szoftverek gyakoribb fajtáinak ismertetesére szorítkozunk.

E rendszerek felépítői, operátorai és felhasználói gyakran érzik úgy, hogy nehezen kezelhető termékkel dolgoznak. A felhasználóknak például egy szakaszon belül három-négy alkalommal kell biztonságosan belépniük a PC-jükbe, (egy LAN-ba, távoli hostba), a biztonsági adminisztrátoroknak pedig nyomon kell követniük, ki kell adniuk és vissza kell vonniuk titkos információk összetett sorait. Ilyenek például a kulcsok, hitelesítő attribútumok és képességek, valamint működtetni és fenntartani számos igen eltérő biztonsági eszközt és terméket.

Ez vezetett ahhoz, hogy létrehozzák a kívánt "biztonsági architektúrát", amelybe az összes egyéni szolgáltatás, termék és management funkció beilleszthető.

Talán már évekkel ezelőtt meg kellett volna egyezni egy ilyen architektúrában, mielőtt az egyéni termékek és szabványok feltűntek volna, de az igazság az, hogy biztonsági architektúrák létrehozásánál az igazán jelentős fejlődés nemzetközi szinten is csak a késő 1980-as évekre tehető. Sorozatunk utolsó része áttekint majd néhány architektúrát.

Hitelesség, bizalmasság

A bankok és a gazdasági intézmények a biztonsági szolgáltatások fontos felhasználói. Ezek a szolgáltatások általában – néhány különleges kivételtől eltekintve – nem túl bonyolultak és a kommunikációt illetően inkább a hitelességre vonatkoznak, mint a bizalmasságra.

Egy bank belső hálózatán belül például a tipikus hálózatok a központi iroda számítógépközpontjához kapcsolják a fiókirodákat, itt gyakran nincs szükség biztonsági szolgáltatásokra. A forgalom hiteles és bizalmas természete feltételezi, hogy ez a hálózat bérelt vonalain is biztosítva van. Ámbár a bankoknak, akik állandó (PVC), vagy kapcsolt virtuális áramköröket (SVC) használnak zárt felhasználói csoporton, de egyébként nyilvános csomagkapcsolt hálózaton belül, óvatosabbnak kellene lenniük nemcsak a tranzakciók védelmét illetően, hanem a távoli küldői és címzetti hely azonosításánál is. Ebből a célból a bankon belüli hálózatoknál is a különböző bankok közötti átutalásoknál használt biztonsági szolgáltatásokat lenne célszerű alkalmazni.

ISO 8730

A bankok közötti átutalások esetében általában az ANSI X9.17/ISO8730 szabvány szerint történik a hitelesítés, amely a szimmetrikus kulcsú (pl. DES) kriptológián alapszik és ANSI X9.17/ISO 8732 kulcselosztási mechanizmusra épül. A kulcselosztási vagy a kulcstovábbítási központ működtetését az egyes bankok átruházhatják valamelyik erre kijelölt, és kölcsönösen elfogadott nemzeti vagy nemzetközi szolgáltató központnak.

Az ISO 8730 szabványnak megfelelően, a bankok közötti átutalásoknál meghatározott elhatárolt mezők léteznek, melyeket meglétük esetén a hitelesített üzenetnek mindig tartalmaznia kell. Ezek:

- A dátum, amikor az üzenet hitelesítô kódjának (MAC) kiszámítása történt. Ezt DMC-nek nevezzük és a QD- és - DQ azonosítók határolják.
- A címzett által használt hitelesítő kulcs azonosítója (IDA), a QK- és KQ-határolóval.
- Az üzenetazonosító (MID), amely a küldő által előállított, a dátumtól (DMC) és a kulcstól (IDA) függő egyedi szám. Ez nyújt védelmet ismétlés vagy elvesztés ellen és határolója QX- és -XQ. (A DMC és MID mezőknek mindig jelen kell lenniük.)
- Jellemző részek az üzenet szövegében, úgymint a tranzakció összege, valutanem, hitelezô és tartozó felek azonosítója, haszonélvező fél és az érvényesség dátuma. Ezeket a szövegrészeket explicit határolja a QT- és TQ, ha a MAC-ba foglalás céljára kivonatolunk, de ha a teljes üzenetet hitelesíteni kell, akkor erre nincs szükség és ezek is lehetnek implicit módon körülhatároltak.
- Végül, maga a MAC, - amely nyolc hexadecimális digitből áll egy helyközzel a közepén, és amely a kimenet baloldali 32 bitje CBC módú DES algoritmus esetén - QM- és -MQ határolóval.

Öt opció

Az ISO 8730 öt opciót támogat az átalakítandó adat feldolgozásakor:

1. A MAC létrehozására a teljes üzenetet bináris számrendszerben módosítás nélkül dolgozzák fel, vagy esetleg az üzenetnek csak részeit, de ez a küldő és a fogadó közötti kölcsönös megállapodás kérdése lehet.
2. A teljes szöveget dolgozzák fel, szerkesztetlenül.
3. Csak a kiválasztott szövegmezők kerülnek a MAC-ba, szerkesztetlenül. A mezők az explicit QT- és -TQ határolók segítségével azonosíthatók, vagy esetleg implicit módon egy szabványos üzenet felépítésében elfoglalt pozíciójuk alapján határozhatók meg.
4. A teljes szöveg elkészített, megszerkesztett. A szerkesztés a kocsi vissza/soremelés, a fölöslegesen betöltött nullák, stb. törléséből áll. A cél azon karakterek eltávolítása, amely csak pazarolja az átviteli időt és/vagy átviteli problémákat idéz elő olyan médiák használatánál, mint pl. a telex.
5. A kiválasztott szövegmezők elkészítettek, megszerkesztettek.

A 2.-tól az 5. opcióig az üzenetet szövegként kezelik. A kód hétbites, a nyolcadik a paritás bit, a kisbetűket nagybetű helyettesíti, stb. Ebben a módosított formában dolgozzák fel a szöveget a MAC előállításához (jegyezzük meg, hogy maga a szöveg nem változott, csak amely a MAC kiszámításának alapját képezi).

Az ISO 8730 és elődje, az X9.9 viszonylag régi szabványok és széles körben, különösen közvetlen bérelt vonali

összeköttetéseken, bankpénztárak között használják.

SWIFT

A The Society for Worldwide Interbank Financial Telecommunications (SWIFT) kb. 3000 intézetnek nyújt X.25 alapú csomagkapcsolt szolgáltatást pénzátutalásokhoz.

Ez a szolgáltatás már sok éve létezik és biztonságát a következő funkciók garantálják:

- Trunkvonali rejtjelzés
- Hálózati hozzáférésvédelem login- kódok segítségével
- Opcionális rejtjelzés a felhasználótól a hálózat felé irányuló bérelt kapcsolatokban

Ezen az infrastruktúrán végpontok közötti pénzügyi tranzakciók bonyolíthatók le különböző protokollok szerint, különböző biztonsági szolgáltatásokkal (pl. a tranzakciók hitelesítése).

A SWIFT felhasználók általában SWIFT által támogatott termékeket futtatnak számítógép alapú termináljaikon és ezek a termékek a működtető személy biztonsági azonosítását kívánják meg.

A SWIFT nemrégiben javította hálózatának alapvető biztonsági jellemzőit, a User Security Enhancement (USE)-et kínálva:

- biztonságos kulcscserét a SWIFT-en keresztül
- chipkártyás hozzáférésellenőrzést a SWIFT-hez.

A biztonságos kulcscsere kétoldali kulcsgenerálást, rejtjelzést és cserét jelent. Ennek alapja egy temperbiztos kiegészítő hardvermodul, amely a kulcscserét 4 fokozatban hajtja végre:

1. a csere inicializálása,
2. a biztonsági azonosító vétele a válaszolótól,
3. a (rejtjelzett és aláírt) kulcsok átvitele, és
4. a kulcsok visszaküldése és ellenőrzése (sok banki alkalmazásban két kulcsra van szükség, hogy lehetővé tegye a kettős aláírást – például az operátor és a biztonsági manager számára).

A biztonsági hardvermodul chipkártya-olvasót támogat. A chipkártya dolgozza fel SWIFT-be való loggoláshoz használt kódokat, amiket egy vagy két PIN aktivál, melyet az operátor és/vagy a biztonsági manager ad meg.

Példaként említhetjük a SWIFT value added termékere a bankok közötti filetranszfert (IFT). Az IFT X.400-on keresztül működik és a filetranszfer tárolását és több irányba történő továbbítását teszi lehetővé. Maga a SWIFT X.400-as szolgáltatás X.25 infrastruktúrán alapul és az alábbi szolgáltatásokhoz tervezték:

- Tömeges (bulk) kifizetés (nyugdíjak, osztalékok, fizetések)
- Hitelfelszólítások, analízisek, hitelesítések
- Biztonsági nyilatkozatok
- Kockázat managelési információk.

A felhasználói oldalon a csomag aktivizálásához kétszintű jelszóra van szükség. A felhasználói hely és a hálózat alapú IFT szolgáltatás között biztonsági hozzáférési ellenőrzés működik. A filetranszfer a pIFT protokollt használja az X.400-as üzeneteken belül.

A pIFT protokoll

A pIFT -nek biztonsági fejléce van, mely egy *token*-t tartalmaz (a CCITT X.509 szerint) az átvitel biztonsági adataival. A szolgáltatás biztonsági elemei a pIFT tartalmi integritás, pIFT tartalmi bizalmasság és az üzenet eredetének hitelesítése, melyekhez különböző algoritmusokat - szimmetrikus vagy aszimmetrikus - használhatunk.

A token-t a küldő generálja, és ez tartalmazza az algoritmus azonosítót is. Ezek végpontok közötti biztonsági funkciók és az algoritmusok vagy kulcsok bilaterális vagy multilaterális egyezmény alapján határozhatók meg magától a SWIFT-től függetlenül.

A SWIFT EDI termékeket is kifejleszt az alapinfrastruktúrán és X.400-on történő futtatásra. Tehát várható, hogy az EDIFACT-tal definiált üzenetek lépnek a meglévő SWIFT-hez tervezett tranzakciók, üzenetek helyére.

ETEBAC 5

A pénzügyi tranzakciók egyre növekvő területei lesznek azok a nagy filetranszferek, melyek nemcsak a pénzintézetek között, hanem közöttük és nagy ügyfeleik között bonyolódnak. Példa erre a cégtől az alkalmazottak számlája felé irányuló filetranszfer, mely a fizetéseiket utalja át. Az ezen a területen levő szolgáltatásokra nézzük meg az ETEBAC 5 -öt, a biztonsági filetranszfer protokollt, melyet a francia bankrendszerekkel történő használatra a *Comité Francais d' Organisation et de Normalisation Bancaires* (CFONB) tervezett.

Az ETEBAC 5 a filetranszferrel kapcsolatban két szintet ismer fel: a felhasználói bankszintet, amellyel a főnökök cserélik és fogadják/visszautasítják a pénzügyi biztonsági file-ok tartalmát; és az ügyfél operátor – bankoperátor szintet amely csak a fizikai filetranszfer biztonságával foglalkozik és nem a file-ok tartalmával. Ez a két szint különböző kriptográfiai kulcsot használ. A filetranszfereket mindig az ügyfél kezdeményezi, de az ezt követő transzfer(ek) bármilyen irányúak lehetnek (ügyféltől a bank felé, vagy fordítva).

Az ETEBAC 5 a FTAM-en alapuló PEsIT nevű filetranszfer-protokollt használja (de nem csupán erre korlátozott). Ez egy X.25 protokoll szerinti csomagkapcsolt hálózaton, vagy egy X.25-ös vonalon keresztül működik. A banknak bérelt vonali X.25 -ös kapcsolata lesz a hálózattal. Az ügyfélnek bérelt X.25-ös vagy X.32-es (tárcsázható X.25) vagy egy X.28/X.29 aszinkron bérelt vagy tárcsázható kapcsolata lehet a hálózathoz. Az ETEBAC 5 aszimmetrikus és szimmetrikus rejtjelzést használ, nevezetesen az RSA-t és a DES-t (vagy DES-CBC-t).

Az ETEBAC 5 által kínált biztonsági szolgáltatások a következők:

- Reciprok (kölcsönös) hitelesítés a bank és az ügyfél (operátorok) között a kapcsolat felépítésekor. A hitelesítés aszimmetrikus kulcspárokat használ a kapcsolat mindkét végén.
- Adatintegritás normál módú DES-CBC szerinti MAC (ISO8730) segítségével. A MAC kulcsát a küldő generálja és átküldi a címzetthez.
- Kölcsönös letagadhatatlanság. A file-ok integritás ellenőrzéseit (a MAC-eket) a főnökök titkos kulcsaikkal digitálisan aláírják (egyúttal ellenőrizve az operátorét), ezáltal garantálva és felelősséggel elfogadva a tranzakció tartalmát.
- (opcionális) átvitel titkosítás, szimmetrikus kulcsú rejtjelzést (DES-CBC) alkalmazva a küldő által generált kulccsal. Ez utóbbit a címzett nyilvános kulcsával rejtjelezve viszik át .

Az ETEBAC 5 egy X.509-hez hasonló security management-et használ.

Problémakezelés

Az ETEBAC 5 eredetileg a TeleTrust T projecthez és később az X.509-hez kifejlesztett legtöbb ismert eljárást alkalmazza. Teljes részletességben ezt a CFONB specifikáció tartalmazza. Olyan különbözó szituációkat is kezel, mint például:

- A file-ba integrált /PeSIT/ változatot használják-e, ahol a biztonsági paraméterek a fejlécekbe vannak beépítve, vagy a filefüggetlen változatot, ahol a paraméterek külön "file"-ban vannak?
- Van-e operátori szint, vagy a transzfer közvetlenül a főnökök között történik?
- Biztonságos háromutas handshake reciprok hitelesítés, vagy egyszerű, az igazolások cseréjén alapuló hitelesítés van-e?
- A bizalmasság garantálására rejtjelzés van-e vagy

nincs ?
- Az átvitt file kétszeresen van-e aláírva vagy sem ?
- Milyen irányú a file-transzfer ?

Az ETEBAC 5 sok egyebet tartalmaz, hogy igen rugalmas szolgáltatást tegyen lehetôvé. Például nemcsak a file tartalmát (MAC-ben tömörítve) lehet aláírni, hanem a file azonosítójának a MAC-jét is, igy egy biztonsági file-nak a referenciái is biztonságossá tehetôk. A ETEBAC 5 az elsô olyan nagyobb szabvány, mely az RSA nyilvános kulcsú kriptográfiát alkalmazza .

Automata pénzek

Egy másik pénzügyi terület, ahol a biztonság kritikus tényezô, a kiskereskedelmi fogyasztói készpénz tranzakciók. Közismert példa erre a bankautomata (ATM) , melyen keresztül két kriptográfiai eljárás történik a hitelesítés és titkosítás.

Az elsôrendû követelmény a készpénzfelvevô személyének a hitelesítése és számlájának készpénzfelvétel és fedezet szerinti megterhelése. A hitelesítés az ügyfél alábbi adatai szerint történik:
- Az ügyfélkártya azonosítója, a bankszámla száma és esetleg további részletek a lehetôségektôl függôen – melyek vagy egy mágneses csíkon, vagy ha chipkártyáról van szó, a memóriában tárolva kódolva találhatók.
- Személyi azonosítószám (PIN), melyet az ügyfél ad meg a PIN Pad-en anélkül, hogy az megfigyelhetô lenne. Csak a kártya tulajdonosa ismeri a PIN-t és ez jelenti a védelmet a kártyát eltulajdonító ellen.

Az ATM-nél hitelesíteni kell, hogy a beadott PIN megfelel-e a kártyának. Ezt rendszerint, de nem mindig, központilag végzik, úgy, hogy a PIN nincs az ATM-nél (ahol elképzelhetô, hogy ellopják) és úgy, hogy más kívánalmak (pl. a fedezet rendelkezésre állásának igazolása) kezelhetôk. Mivel ATM-ek tipikusan bankfiókokban találhatók, az ATM és a központi host közti kapcsolat része lehet a bank meglévô hálózatának, és igy a telekommunikációs költségek minimalizálhatók.

Azonban a felhasználók PIN-jeit tilos nyíltan átvinni egy hálózaton, ezért azokat rejtjelezik (rendszerint közvetlenül a PIN Pad-ben), majd hozzákapcsolják a kártya és a tranzakció azon részleteihez, melyeket a hosthoz küldünk, ahol a PIN-ek megoldása és a hitelesítés megtörténik. Általában egy szimmetrikus kulcsot használnak ATM-enként, melynek a párja a hostban van.

Néhány esetben az ATM hajtja végre a PIN hitelesítését, ebben az esetben az ATM a PIN-t csak rejtjelzett formában tárolja egyirányú függvényt használva. Néha különbözô bankok használhatják ugyanazokat az ATM-eket. Ebben az esetben az anyabank oldja meg és rejtjelzi a PIN-t (vagy az egész tranzakciót) és azután juttatja tovább az ügyfél saját bankjához hitelesítés céljából.

Debit- és hitelkártyák

Hasonló alkalmazás a hitelkártya, mellyel tulajdonosa fizet az üzletben vásárláskor. A vásárlás részleteit az üzlet alkalmazottja beírja a megfelelô billentyűzettel, a felhasználó hitelkártyáját a terminál beolvassa (a billentyűzet és a kártyaolvasó terminál összevonható egy normál pénztárgéppel), és a felhasználó beadja (titkosan) a PIN-jét a PIN Pad-be. A PIN rejtjelzésre kerül és a tranzakció többi részéhez csatolva a hálózaton keresztül további feldolgozás céljából továbbítják. Ha pozitív válasz érkezik vissza a host-tól, a vásárlás megtörténik, egyébként visszautasítják.

A hitelesítô host-tal történô kommunikációhoz value-added hálózatokat lehet használni. A fôfunkció a tranzakció elküldése a megfelelô bankhoz. Ilyen hálózatok nemcsak az ügyfél számlájának a terhelését tartalmazhatják, hanem az eladást végzô kereskedô számlájának hitelezését is. Az is gyakori, hogy egy bizonyos érték alatti eladásnál nem online hitelesítenek, hanem több ilyen tranzakciót összevonnak és késôbb viszik át a megfelelô host-okhoz, ezáltal csökkentve a kereskedô telekommunikációs költségeit. Ebben az esetben általában a kereskedô vállalja a kockázatot.

A hitelkártya hitelesítése egy ezzel kapcsolatos másik pénzügyi alkalmazás. Itt arról van szó, hogy azt kell biztosítani, hogy a kártya érvényes és nem lopott. Ezt is megvalósíthatjuk online módon a terminál - amely beolvassa a kártyát - és a hitelesítô host között, vagy egymásutáni összegyűjtéssel, ha a hitel összege bizonyos érték alatti.

Mostanában tömörített formában viszik be a a "hot card file"-t (a visszavont hitelkártya file-ja) a terminálba rendszeres aktualizálással. A hitelkártya terminálok rendszerint képesek a "data capture" funkcióra is, melynél a tranzakciók adatait összegyűjtik és a kártya kibocsátóhoz elektronikus feldolgozásra továbbítják papíron való dokumentálás helyett. A hitelkártyákat általában PIN nélkül használják vásárláskor.

Sorozatunknak a következô számban megjelenô második részében a "SECURE DATA NETWORKING" legelterjedtebb biztonsági hardvereit és szoftvereit ismertetjük.

Kondákor Tibor

Az első IP router Windows NT-hez

Az Eicon Technology volt a leggyorsabb, amikor piacra dobta az elsô, Windows NT környezetben mûködô WAN hálózatokhoz kifejlesztett IP routert.

Ez a lépés tovább erôsíti a Microsoft és az Eicon közötti jó kapcsolatokat. A cég már korábban is szállított WAN termékeket a Windows NT-hez és további fejlesztéseket is tervez ehhez a környezethez. Az új IP router iroda-iroda közti kapcsolatot tesz lehetôvé a Windows NT TCP/IP LAN-jain, ISDN, Frame Relay, X.25 vagy bérelt vonalas PPP protokoll szerint. Természetesen teljes mértékben kompatibilis a legnagyobb gyártók (Wellfleet, Cisco, IBM) által szállított gerinc-routerekkel is.

Az IP Router for Windows NT PC alapú termék, amely könnyedén beilleszthetô a helyi irodákba.

Nagyteljesítményû adattömörítô képessége és az átviteli sávszélesség maximális kihasználása révén az átviteli költségek terén jelentôs megtakarítás érhetô el. A termék interoperabilitása és megfelelése a gerinc-routerekkel biztosítja, hogy a helyi irodák probléma mentesen csatlakozzanak a cég hálózatára.

Könnyedén adaptálható a késôbbi fejlesztésekhez, így a cégeknek a jövôben sem kell további költségeket hardver felújításokat vagy cseréket eszközölniük, nem úgy, mint a speciális hardver megoldásoknál. A Rover Group-nál, akik az IP router for Windows NT egyik béta tesztelôi voltak különösen meg voltak elégedve azzal, hogy az új termék a nagy sebességet megbízhatósággal párosította.

A következô sorozat már egy SNMP alapú Windows 3.1 alatt futó hálózat-menedzselô konzolt is tartalmaz, ingyenesen. Az eddig helyszíni kiszállást igénylô konfigurálási és upgrade problémák ezentúl a távolból is elháríthatók lesznek, csökkentve ezzel a mûködési és betanítási költségeket.

A routernek a várható új "Daytona" Windows-hoz illetve a Digital Alpha chipjéhez illeszkedô változatainak kidolgozása folyamatban van.

A Banyan Vines legyőzi a Gigantikus Adatbázist

Irigylésre méltó helyzet, amikor egy beruházó minden indokolt vásárlásában olyan minőségű eszközöket választhat, amelyek garantálják a hibátlan működéshez szükséges hátteret. 1992-ben ilyen lehetőséget kapott az akkor alakuló Állami Vagyonkezelő Részvénytársaság, s az a rendszergazda vesse rájuk az első Stoned-vírust, aki hasonló helyzetben nem használta volna ki a ritkán adódó lehetőséget.

Tény, hogy az ÁV Rt. olyan rendszert épített fel, amely valóban párját ritkítja. Mind a hardverek, mind a szoftverek közül az igényeiknek leginkább megfelelőt választották, s végül olyan, 180 Compaq munkaállomást magában foglaló hálózatot építettek ki, amely képes a számítógépes kommunikációs lánc külső folytatására is.

Az igényesen kiépített rendszer létjogosultságát indokolja, hogy az ÁV Rt. feladatkörébe a tartósan állami kézben lévő vállalatok felügyelete tartozik. Jelenleg közel 170 vállalatról kell naprakész adatokat tudniuk, ami magában foglalja a vezetőség tagjainak személyi adataitól kezdve a részletes vállalati mérlegen keresztül a állóés forgóeszközök nyilvántartását — s ezek az adatok alig elképzelhető méretű adatbázist képeznek.

A csillag topológiájú, csavart-érpáras kábellel Ethernet hálózatba kötött rendszer központja egy SynOptics 3000 típusú hálózati koncentrátor. Az adatbázis szerver egy Hewlett Packard 9000/800 G40-es nagyszámítógép, amelyet 64 megabájt RAM-mal és 8 gigabájt háttértárral helyeztek üzembe. A kommunikációs szerverek (X.25-ös adatvonalon tartják a külső kapcsolatokat, többek között az MTI Economic News érhető el) két Intel 486-os alapú Compaq SystemPro, ezek 2 gigabájtos merevlemezzel és 16 MB-os operatív tárral rendelkeznek. A HP nagyszámítógépén UNIX operációs rendszer fut, míg a Compaq szerverek a Banyan Vines 5.50-es hálózati operációs rendszerét használják.

Három dedikált szerver is segíti az ÁV Rt. munkáját. Egyikük az öt lemez olvasására alkalmas CD-ROM meghajtóval tart kapcsolatot, a másik szerver a részvénytársaság telefax-forgalmát hivatott megoldani — a legizgalmasabb feladatkört azonban a kihelyezett PC-kel és munkaállomásokkal kommunikáló szerver kapta. Az Állami Vagyonkezelő Rt. munkatársai ugyanis szükség esetén ideiglenesen kitelepülnek egy-egy vizsgált vállalathoz, s ilyenkor a helyszínről férhetnek hozzá a harmadik dedikált szerveren keresztül a központi adatbázishoz, meghatározott hozzáférési jogosultsággal kérhetnek le adatokat, illetve módosíthatják azokat.

Házon belül nem kevesebb mint 180 Compaq PC kapcsolódik a hálózathoz. Ezek kiépítése már az adott feladatkörökhöz igazodik, operatív táruk 4-8, háttértárolójuk pedig 120-240 megabájtos. A PC-s munkahelyeken egységesen Windows-os felületekkel találkoznak az ÁV Rt. munkatársai, s mindenhol a Microsoft irodai szoftvereit (Word, Excel, MS-Mail, vagy MS-Office, illetve a vezetők részére MS-Schedule, MS-Poject) használják.

Az eddig bemutatott minőségi hardver-halmaz, és a fejlett szolgáltatásokat nyújtó Banyan Vines hálózati operációs rendszer csak a lehetőségét teremti meg annak, hogy a 2000 állami vállalat, és 3000 vezető adatait tartalmazó gigászi adatbázis a felhasználók igényei szerinti szempontok szerint átjárható, lekérdezhető legyen.

A hardver "felélesztését", pontosabban az ÁV Rt. elvárásainak megfelelő alkalmazásokat az informatikai igazgatóság vezetésével létrehozott, főként az IQSOFT fejlesztőiből álló munkacsoport készítette el. Mint *Németh Péter*, az ÁV Rt. informatikai igazgatója és *Tóth Miklós* informatikai munkatárs elmondta, igen erőteljes tempóban történt a fejlesztés, alig három havonként készültek el egy-egy alkalmazással. Eddig öt modul készült el, s ezeket a folyamatos oktatás eredményeként ma már minden munkahelyen használják is.

Az Oracle relációs adatbáziskezelő rendszerhez Gupta SQL Windows fejlesztői környezetben készültek az alkalmazások. Ha valaki látja ezeket az alkalmazói felületeket bizonyára elfogadja a "felhasználó-barát" jelzőt. Valószínűleg a Windows-logika korábbi elsajátítása is nagyban hozzásegítette az új székházban dolgozókat ahhoz, hogy az alkalmazások kezelését gyorsan elsajátíthassák.

Az *iktató-ügykezelő* rendszer a HyperMedia Systems Doktár moduljaira épül, míg a *céginformációs rendszer* (ebben a vállalatok pénzügyi mérlegei találhatók, s akár havi bontásban is lekérdezhetők), a *külső és belső humánpolitikai rendszer* (ezekben a vállalati vezetők, felügyelőbizottsági tagok, illetve az adott posztokra delegálható személyek adatai találhatók), illetve a *tanácsadói információs rendszer* teljes mértékben a Gupta fejlesztői környezetében készült.

A végeredmény: bármilyen alapinformáció mellé keressük a kiegészítő vagy háttérinformációkat, az átjárható alkalmazásokkal másodpercek alatt eredményt kaphatunk. Ha a humánpolitikai rendszerben megkérdezzük, hogy X. Y. kicsoda, néhány képernyőváltás után minden hivatalos adatát megismerhetjük, bepillanthatunk vállalatának számviteli adataiba, és megtudhatjuk milyen a cég megítélése privatizációs szempontból? Talán nem árt megismételni: 2000 vállalat és 3000 vezető adatairól van szó, s szinte "real-time" információ-lekérdezésről.

A rendszer megbízhatóságát a híres Compaq-minőségen túl a hálózati operációs rendszer is garantálja. Az informatikai igazgatóságon gyakorlati szempontok szerint minősítették a Banyan Vines alkalmazhatóságát: legfontosabbnak tartották, hogy LAN/WAN környezetben egyaránt minden igényt kielégítően működik, egyszerűen biztosította az induláskor telepített és a később rendszerbe állított szervergépek összekapcsolhatóságát.

Ugyanakkor az új, vagy kitelepített munkaállomásokat is egyszerűen lehet a rendszerhez kapcsolni és a hozzáférési jogok átdefiniálása sem jelent gondot. Az általánosságban jól hangzó "megbízhatóságot" azzal támasztották alá, hogy a Banyan Vines egyszerűen menedzselhető és adminisztrálható, ami úgy fordítható, hogy hozzáértő rendszergazdák számára teljesen flexibilis operációs rendszerről van szó, amit a felhasználó mindenkori igényeinek megfelelően lehet átkonfigurálni.

Ha igaz, hogy egy rendszer kiépítését a működőképességen és az említett megbízhatóságon túl az is minősíti, hogy mekkora létszám kell az üzemeltetéséhez, akkor az ÁV Rt.-nél igazán korszerűre sikeredett az informatika kiépítése: az informatikai igazgatóságon összesen hárman dolgoznak. Akik talán használhatnák az Állami Adatbáziskezelő címet is.