NEWS

MONTANA

20. szám 1994. december

A kapcsolat elemei – 3Com újdonságok

Kerberos és társai – Secure Data Networking 3.

Reszkessetek betörők! – Egységes hálózat a bűnüldözésben

A 3Com új termékei

A 3Com Corporation a hálózati eszközök egyik legismertebb fejlesztője és gyártója. Több tízezer 3Com hálózat működik világszerte kormányhivatalokban, egyetemeken, a hadiipar, és a gazdaság különböző területein. A hálózati eszköz gyártók közül a 3Com Corporation rendelkezik a legszélesebb termékskálával az ún. Global Data Networking megvalósításához.

A hálózati aktív elemek homogenitása sok előnyt hordoz: nem kell az elemek különbözőségéből adódó inkompatibilitással foglalkozni, az eszközöket egységes szoftverfelületen lehet programozni, mely a rendszergazdák életét jelentősen megkönnyíti. Nagyon fontos szempont, hogy az egységes hálózatmenedzsment az eszközök összes paraméterét képes kezelni, míg az inhomogén rendszerekben a szabványos felület használatával a gyártóspecifikus plusz adatok esetleg nem kezelhetők. A 3Com routerek – mint ezt több egymástól független cég (Computerworld, Corporate Computing, Communications Week) által elvégzett tesztsorozat is bizonyítja – a legjobbak és tavaly az Év Internetworking Terméke kitüntető címet kapták.

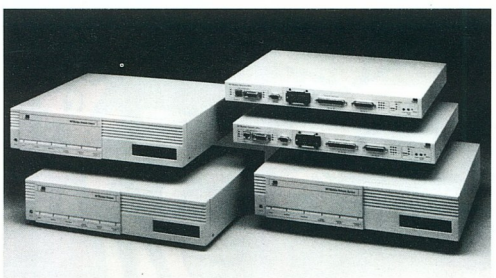
NetBuilder II Bridge/ Router újdonságok

A multiprotokoll routolást végző NetBuilder II router 70.000 pps teljesítménye a közeljövőben kb. 250.000 pps-re növelhető. Ehhez a routert meg lehet tartani, csak a nagyobb sebességet igénylő modult kell cserélni.

Hamarosan megjelenik a 3 portos HSS modul RS-232 interface-el (V.35 interface-el már jelenleg is elérhető). Egy ilyen modul 3 WAN csatlakozási lehetőséget biztosít, így megtriplázza az egy router által kiszolgálható WAN kapcsolatok számát. (Így a 8 modulhelyes ház max. 24 WAN, a 4 modulhelyes max. 12 WAN kapcsolatot képes fogadni.) A modul felhasználása jelentősen csökkenti az egy WAN csatlakozás kialakításának költségét.

SuperStack rendszer

A 3Com a 90-es évek elején kezdte meg tornyozható (angolul stack) hub-család kialakítását, amelyekben a hub-ok ún. hub expansion kábellel egymáshoz csatlakoztathatók. A különböző hálózati közeget támogató, bevált és olcsó LinkBuilder FMS (Flexible Media Stack) hubok mellet megjelent a bridge és menedzsment modullal bővíthető LinkBuilder FMS II család, mely lehetővé teszi 12 és 24 portos 10BASE-T, egy 6 portos fiber modul és a 10 portos koaxos modul elhelyezését egy menedzselhető stackben. Az így összkepcsolt 4, sőt a LinkBuilder FMS II családnál már 8 hub egy logikai repeater-ként vehető figyelembe a hálózattervezésnél. A SuperStack hibatűrő képessége redundáns tápegységgel növelhető.



A SuperStack építőelemei:

NetBuilder Remote Office 221 és Remote Office 201 Boundary Router

A NetBuilder Remote Office 221 mind önálló egységként, mind a 3Com SuperStack elemeként üzemelhet, míg a Remote Office 201 standalone boundary router. Az egyszerű plug-and-play telepítésű boundary routerek közepes és kis telephelyek költségtakarékos kiszolgálását teszi lehetővé 1 LAN és 1 WAN kapacitásával. A boundary routing architektúrából adódóan a router a központi oldalon NetBuilder II bridge/router-hez kapcsolódik, így minden olyan hálózati protokollt támogat, melyet a NetBuilder II bridge/router.

A biztonság és az elérhetőség növelése érdekében automatikus kapcsolt backup WAN porttal rendelkezik. A dinamikus sávszélességhasználat (bandwidth-on-demand) lehetővé teszi, hogy a WAN oldali kommunikációs csatorna túlterheltsége esetén a router a backup WAN portján is összeköttetést létesítsen, melyet a forgalmi csúcs megszűnésével automatikusan megszüntet. Ezek mellett, a router a kapcsolt vonalon megvalósítandó WAN összeköttetéseket egy új, költségtakarékos dial-on-demand opcióval támogatja: azaz csak akkor építi fel a kapcsolatot, ha adatot kell rajta továbbítania, ezt követően lebontja. A WAN csatlakozás költség kímélését szolgálja az is, hogy az IPX forgalomra különböző szűrési feltételeket lehet beállítani.

WAN oldalon bérelt összeköttetések esetén a PPP protokollt, kapcsolt összeköttetések esetén a dial, a frame relay és az X.25 protokollok használatát támogatja. A pont-pont (PPP) összeköttetéseken teljes adattömörítést támogat; a csomagok fejrészét is tömöríti, nem csak az adatrészt. A router a beállított konfigurációt flash PROM-ban tárolja.

NetBuilder Remote Office 222 Router

A Remote Office 222 router a közepestől az egészen nagy telephelyek költségtakarékos kiszolgálását teszi lehetővé. Mind önálló üzemmódban, mind a 3Com SuperStack rendszerében üzemelhet. A Remote Office Router család e tagja un. access router-ként hagyományos routolást végez TCP/IP, IPX és XNS protokollokra. Egyéb jellemzői megegyeznek a NetBuilder Remote Office 221 routerével.

NetBuilder Remote Office 227 Router

A SuperStack rendszer harmadik s egyben legtöbbet tudó router tagja a Remote Office 227, mely külön routerként is működhet TCP/IP, IPX, XNS, AppleTalk, DECNet és VINES protokollokra.

LinkBuilder FMS TR

A SuperStack rendszerben 12-260 Token Ring felhasználó csatlakoztatása válik lehetővé.

LinkSwitch

A LinkSwitch munkacsoport átkapcsoló hub 6 ethernet hálózat között végez nagy teljesítményű "kacsolást". FDDI portján akár közvetlen nagy sebességgű csatlakozást biztosíthat FDDI interface-szel rendelkező szerver felé, vagy nagy sebességű gerinchálózat kialakítását teszi lehetővé.

LinkConverter 200

Az eszköz SDLC-LLC2 konverzióval lehetővé teszi SNA forgalom routolt WAN hálózatba való integrálását.

Redundáns Tápegység

A redundáns tépegység

(Folytatás a 7 . oldalon)

Reszkessetek betörők!!!

Igen reszkessetek, mert ha minden az elképzelések szerint halad, jövő év elejére kifejlesztésre kerül egy olyan "bűnügyi kommunikációs adatnyilvántartó és áramoltató" rendszer modellje, mely megoldja a bűnüldöző szervek között az adatok oda-vissza áramoltatását, illetve bizonyos funkcionális rendszerek közös hozzáférhetőségét. A mintarendszer alapját képezi egy egységes, integrált országos rendszernek.

Mindez nem fantáziálás, a nagy információs rendszer alapköveit már akkor elhelyezték, amikor a rendőrségi információs rendszer országos kiépítése érdekében tendert írt ki az ORFK. Hamarosan meghatározták az ügyészségi információs rendszer fejlesztési irányait is. A bűnüldözési társszervek — az Országos Rendőrfőkapitányság, valamint a Vám- és Pénzügyőrség Országos Parancsnoksága — illetékeseivel hónapok óta folytattak előkészítő tárgyalásokat, ahol kirajzolódott, hogy a bűnüldözés az a terület, amelynél a jogszabályok is lehetővé teszik és határozott előnyökkel is jár a három rendszer összekapcsolódása.

A fejlesztési feladatokhoz egy 16 munkaállomásból felépülő, UNIX alapú hálózat telepítésére írtak ki meghívásos, zártkörű tendert, amelyre négy rendszerintegrátor ajánlatát kérték be. A tendergyőztes MONTANA egyelőre egy fejlesztői és egy (a rendszer funkcióit ügyészségi oldalon demonstráló) mintarendszer telepítésére kapott megbízást.

Novemberben installálták is a Legfőbb Ügyészség Számítóközpontjában azt a hálózatot, amellyel a mintarendszer, majd később a kiépítendő országos rendszer alkalmazói szoftvereit fejlesztik.

Mint *Pusztainé Dr. Jakab Róza* osztályvezető ügyész elmondta, határozott és letisztult elképzeléseik vannak mind a fejlesztendő rendszer formai és tartalmi elemeiről, mind az informatikai hálózatok kapcsolódási pontjaival szemben támasztott elvárásokról.

A három rendszer kapcsolatának leggyorsabban használható előnye, hogy az egyes bűnesetekről készült dokumentumok (elkövető neve, bűncselekményi adatok, bűnüldöző szervek intézkedései, stb.) azonnal hozzáférhetők a jogosultak számára. Az előre elkészített számítógépes iratminták alkalmazása jelentősen csökkentheti az un. formai munkára fordított időt, többet hagyva a szakmai tevékenységre. A folyamatosan felépülő, részben a korábbi bűnügyek adataival feltöltött adatbázisok révén pedig mindhárom bűnüldöző szerv nemcsak meggyorsíthatja, de pontosabbá, egyszerűbbé is teheti munkáját. Egy betöréses lopás felderítésekor például az "elkövetés módja" adatbázis áttekintésével behatárolható lehet, hogy kik azok, akikre az aktuális esethez hasonló vagy azonos módszer használata jellemző.

Áttekinthetőség, gyorsaság, precízség: ezt kapjuk az informatikai rendszertől, s állandó kapcsolatot tarthatunk fenn a bűnüldözési társszervekkel — foglalta össze Pusztainé Dr. Jakab Róza.

A Budakörnyéki Városi Ügyészségen építi ki a mintarendszert a MONTANA, mely hálózaton azokat a szoftvereket futtatják majd, amelyek a már működő fejlesztői rendszeren készültek. Ugyanekkor helyezik üzembe a Budaörsi Rendőrfőkapitányság informatikai rendszerét. A két szerv között az adatforgalom vezetékes hálózaton folyik, míg a Vám- és Pénzügyőrség Pest megyei Nyomozó Hivatalával modemeken keresztül cserélnek majd adatokat.

A mintarendszer O.1 verziója átadásának határideje február 28. Márciustól tehát egyelőre Budaörsön , a saját bűnügyi információs rendszerükre építkezve egységes, integrált kommunikációs rendszert használ majd a három bűnüldöző szerv.

A Kedves Olvasó

is bizonyára szomorúan tapasztalta az utóbbi években, hogy a csendes kis utcák földszinti balkonjait egyre több helyen csúfítják el ronda rácsok, hogy a lakótelepeken mekkora tülekedés folyik a lámpák alatti éjszakai parkolóhelyért, hogy a postaládákban rendre kis szórólapok bukkannak fel a lakatosok jobbnál jobb hevederzár ajánlataival. Mi pedig tárcsázzuk, érdeklődünk és hívjuk őket, mert félünk és a félelemre megvan minden okunk.

Félnivalója persze akad a különböző állami és önkormányzati hivataloknak, bankoknak, kisebb-nagyobb cégeknek, vállalkozásoknak is. Nekik ráadásul nem csak az úgynevezett hagyományőrző, pajszerral dolgozó betörőktől kell rettegniük, hanem a számítógépes hálózatok adatbázisainak fosztogatóitól is. Az adatbázisokat ugyanis köztudottan éppen úgy fel lehet törni, mint a sötétben parkoló autókat vagy a cilinderzáras lakásokat, ezért biztonságos védelmük ma már legalább olyan fontos feladat, mint azoknak az előfeltételeknek a megteremtése, melyek az adatok betáplálását és gyors, az igényeknek megfelelő formában történő előhívhatóságát teszik lehetővé.

A Montana Holdingon belül működő különböző Kft-k mind a két kihívásnak igyekeznek elébe menni. Az adatvédelem legmodernebb technikáinak telepítésével "kriptológusaink" foglalkoznak, a számítógépes hálózatok telepítésére kiírt különböző tendereken pedig cégünk évek óta igen eredményesen szerepel. Az a feladat, melynek megoldására most teljesítünk megbízásokat, egyszerre jelent rendszerépítést és adatvédelmet: a Montana ugyanis részt vesz annak az országos integrált informatikai hálózatnak a kiépítésében, amely lehetővé teszi a rendőrkapitányságok, a vám- és pénzügyőrségek, valamint az ügyészségek informatikai rendszereinek összekapcsolódását. A kapcsolat elsőként Pest megyében jön majd létre a jövő év vége felé, de minden remény megvan arra, hogy néhány éven belül az ország legtávolabbi pontjai is csatlakozhassanak e hatalmas informatikai hálózathoz. Akkor pedig, ha a rácsokat és a hevederzárakat nem is dobhatjuk nyugodt szívvel a fölöslegessé vált kacatok lomtárába, de a mainál majd minden esetre jóval nyugodtabban alhatunk.

SECURE DATA NETWORKING 3.

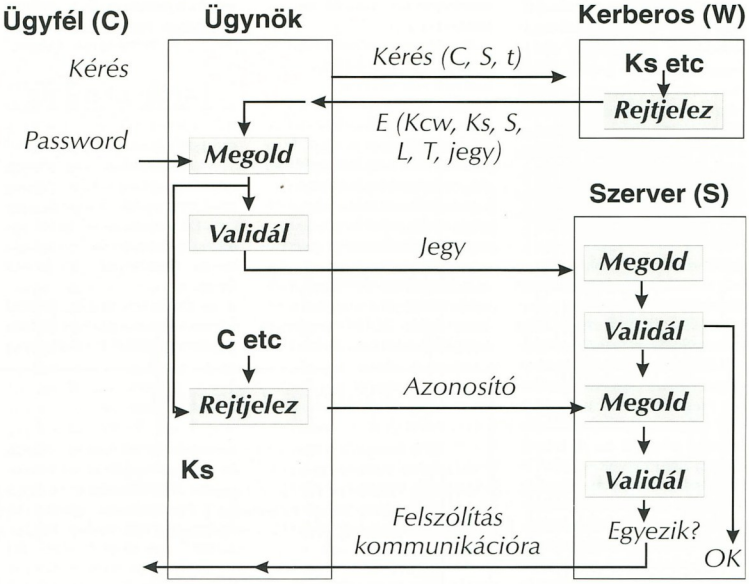
A biztonsági architektúra egy olyan teljes rendszert próbál meg biztosítani, amely segítségével számos biztonsági szolgáltatás (bizalmasság, integritás, hitelesítés, letagadhatatlanság, stb.) egységesen használható; például eljárások és erőforrások megosztásával, vagy a szolgáltatások egymás számára elérhetővé tételével. Ez az architektúra sok esetben alkalmazható: helyi vagy távoli terminállal használt hostalapú rendszer; hálózaton keresztül egymással együttműködő, vagy egymást helyettesítő (pl. directory service agent) alkalmazások; LAN alapú rendszerek és LAN-ok közötti kapcsolatok osztott szolgáltatásokkal, mint pl. fileszerverek; kommunikációs gateway-ek, bridgeek vagy router-ek.

A biztonsági architektúrák fogalma alatt a gyakorlatban általában a kulcs kiosztás és más engedélyezések, azonosítások, személyeket és rendszereket felhatalmazó attribútumok használatát értjük. Az egyéni biztonsági szerverek specifikus eljárásai és mechanizmusai - még a szimmetrikus vagy aszimmetrikus kulcsú kriptológia alkalmazása is - gyakran nyitottak vagy opcionálisak. A következőkben néhány architektúrát ismertetünk.

Kerberos

A Kerberost a Massachusetts Institute of Technology fejlesztette ki, és mint a neve is sejteti, ez egy watchdog szolgáltatás, amely a számítógépes rendszerekhez való hozzáférést ellenőrzi. A védett rendszerhez a Kerberos engedélyével lehet hozzáférni. Ha a jelentkezést jóváhagyták, a Kerberos kiad egy „jegyet" a jelentkezőnek, ezzel válik lehetővé számára a védett rendszer használata. Az 1.ábrán látható rendszer a következő lépésekkel írható le.

1. A (C) ügyfél igénybe kívánja venni az (S) szolgáltatást. C egy közvetítőt-ügynököt (pl munkaállomást, vagy PC-t) használ. C a Kerberos watchdog (W) -tól jegyet kér S-hez a C és S azonosítója, és az aktuális időpont (t) elküldésével.



1.ábra

2. W válaszol, azaz elküldi a C és S által használandó egyszeri kulcsot (K_s), S azonosítóját és a jegy érvényességi idejét (L). Továbbá visszaküldi (t)-t, és magát a jegyet. Mindent DES-sel rejtjelez a K_{cw} kulcsot használva; ez egy szimmetrikus titkos kulcs, melyen a Kerberos és az ügyfél osztoznak. A jegy hasonló információkat tartalmaz, K_{sw}-vel rejtjelezve, ahol ez utóbbi olyan szimmetrikus kulcs, amelyen a Kerberos és a használandó szolgáltatás osztoznak. A jegy = E (K_{sw}; (K_s, C, S, time, C címe, L)), így csak S tudja olvasni a jegyet. C címét (azaz az ügynök hálózati címét) a W határozza meg a kapcsolat létesítésekor, és csak S használhatja visszahívásra, az ügyfél táblázatának verifikálására ...

3. C-nek meg kell oldania W válaszát, amit csak a K_{cw} ismeretében tehet meg. A felhasználó megadja a jelszavát (P), amiből egy one-way függvény segítségével kiszámítható a K_{cw} kulcs; K_{cw}=f(P). Így a C ügynök - ami publikus területen lévő munkaállomás is lehetnem kell, hogy tárolja a K_{cw} kulcsot, csak egyszer kell generálnia, ha szüksége van rá, és a kapcsolat után azonnal megsemmisíti. W válaszának megoldása után a C ügynök ellenőrzi az S és t helyességét (azaz azt, hogy a válasz és így a jegy is nem ismétlése-e egy korábbi kérésre érkezett válasznak). C természetesen bízik abban, hogy W jó jegyet küldött. C ügynöke tudja, hogy a válasz W-től jött, hiszen meg tudja azt oldani.

4. C ügynöke kapcsolatot létesít S-sel és elküldi a jegyet. S megoldja, és érvényesíti (idő, L) azt, hiszen neki szánták, és C egyes adatait is tartalmazza. Így tudja, hogy a Kerberos kezeskedik C-ért. S természetesen nem tudja, hogy C ügynöke küldte a jegyet. Lehetett egy csaló is, aki a hálózaton elfogott egy jegyet és most megismételte azt.

5. Annak érdekében, hogy S megállapíthassa, hogy a jegy tényleg C-től és C ügynökétől érkezett, az ügynök küld egy azonosítót = E (K_s;(C, C címe,t)). S megoldja ezt a jegy kapcsolatkulcsát használva, és megvizsgálja (t ellenőrzésével, valamint C és C címének a jegyen lévő értékkel történő összehasonlításával), hogy az azonosító C-től származik-e. C címe összehasonlítható a C és S közötti kapcsolat létesítésekor kapott forráscímmel pl X.25 csomagkapcsolt hálózat esetén. Ettől a ponttól kezdve a kapcsolat végéig a C és ügynö-

ke egyazon személyként kezelhetők.

6. S és C most már biztonságosan kommunikálhat a K_s kulcs segítségével rejtjelezve vagy üzeneteket hitelesítve. C azért bízik abban, hogy S hiteles, és nem egy csaló, mert bízik W-ben. S a K_s-t csak W-től kaphatta meg K_{sw}-vel rejtjelezve; és K_s-t csak az S és a C birtokolja. Így a kölcsönös hitelesítésnek még egy indirekt módja is létezik.

Elképzelhető, hogy C több különböző szerverhez is szeretne hozzáférni amíg az ügynököt használja, és esetleg több kapcsolatot kíván egyidejűleg aktívan fenntartani. A jegy egyszerű mechanizmusa (az L érvényességi idővel) egyértelműen lehetővé teszi ezt, hiszen C újra be tudja mutatni a még érvényes jegyet, vagy újraérvényesíttetni azt, ha akarja. Ezt C a Kerberos jegy engedélyező segítségével egyszerűen megteheti. Ebben az esetben az inicializáló hozzáférést a Kerberoshoz úgy tekinthetjük, mint a kulcs kiosztó szervízhez történő fordulást, ami az ügyfélnek jegyet és egyszeri kulcsot ad a jegy engedélyezőhöz.

Ha az ügyfél a Kerberos jegy engedélyezőhöz jegyért vagy más szolgáltatásért többször kíván hozzáférni a jegy érvényességi ideje alatt, megteheti, a jelszó (P) megadása nem szükséges minden alkalommal.

A Kerberos célja, hogy biztosítsa, hogy a szerveren futó alkalmazás meg legyen győződve a hozzáforduló ügyfél azonosságáról, még abban az esetben is, ha az ügyfél egy olyan nembiztonságos terminálon dolgozik, mint pl. egy nyilvános munkaállomás.

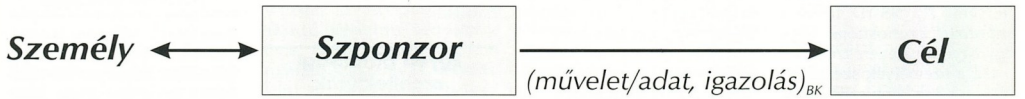
A Kerberos nem specifikál hitelesítő attribútumokat, bár a szerver megállapíthatja ezeket az ügyfél azonosítójából.

A Kerberos nem szabja meg, hogy K_s-t hogyan használjuk hitelesítés után, bár alkalmas lenne adat eredet hitelesítési és integritási szolgáltatások támogatására. Így a Kerberos mint architektúra egy tökéletesen hitelesített interaktív kapcsolat létrehozásának első lépésére korlátozódik. Alapja a szimmetrikus kulcsú DES.

SESAME

A SESAME (**S**ecure **E**uropean **S**ystem for **A**pplication in a **M**ultivendor **E**nvironment) olyan európai project, amelynek célja az ECMA (**E**uropean **C**omputer **M**anufacturers' **A**ssociation) TR/46 és 128 nevű projectek részleteinek kidolgozása és kereskedelmi forgalmú termékek létrehozása.

A SESAME-ban a személy szponzora (vagy felhasználói ügynök) az „igazolások"-at kommunikációs csatornán, vagy hálózaton keresztül küldi el a cél-alkalmazásokhoz (továbbiakban cél), hogy a hozzáférési jogot a személy (felhasználó) megkapja. Az igazolás olyan információkat tartalmaz a személyről, mint az azonosítója és személyi attribútumok, amelyeket egy bizalommal felruházott igazolás kibocsátó pecsétel le, vagy ír alá. Az igazolást hozzácsatolják a többi adathoz és/vagy parancsokhoz és egy alap-kulccsal lepecsételik, mielőtt a szponzor elküldi. Az alap-kulcsot egy kulcselosztó szolgálat (KDS) állítja elő ehhez a személy-cél kapcsolathoz, ezáltal, ha a célpont sikeresen hitelesíti az igazolást (és más adatokat), akkor biztos, hogy az igazolásban azonosított személytől, és a személynek attól a szponzorától jött, amelyre a személy az alap-kulcsot rábízta.



BK = Alap-kulcs
$( )_{BK}$ = BK által lepecsételve

2.ábra

Kétféle igazolás létezik: hitelesítő igazolás (AUC) és személyi attribútumok igazolása (PAC). Az AUC-t egy hitelesítő szerver (AS) állítja ki egy sikeres partnerhitelesítés után. Az AUC egy meghatározott időtartamig érvényes, alapvetően a személy azonosítóját és a szponzor adatait tartalmazza, és a szerver aláírja vagy lepecsételi. Az AUC célja, hogy engedélyezze a személy számára a PAC megszerzését egy személyi attribútum kiadó szervertől (PAS).

A PAC-t a PAS aláírja, és alapvető információként az egyén személyi attribútumait tartalmazza („hozzáférhet a titkos információkhoz", „a 19-es csoporton belül dolgozik", ...). A PAC tartalmaz más információt is: érvényességi időt és a személy azonosítóját. Az AUC és PAC tartalmazzák a saját azonosítójukat, ami hitelesítőként használható ellenőrzéskor. Az érvényességi-idő ellenőrzés nemcsak az idő érvényességét ellenőrzi, hanem egy „fehasználás számlálót" is tartalmaz, ami az egyes célok számára lehetővé teszi ugyanazon igazolás ismételt felhasználásának a visszautasítását. Az igazolásrendszer egyszerű vázlata a 3.ábrán látható.

Az AS és PAS a 3.ábrán külön szerverként szerepel. Egy másik lehetséges megoldás az AS és PAS kombinálása. A szponzor sikeres hitelesítése esetén a szerver (az AUC elhagyásával) közvetlenül a PAC-ot állítja ki.

A SESAME szélesebb területet céloz meg, mint a Kerberos. Ennek illusztrálására két példát mutatunk be: egyéni attribútum és helyettesítés.

Személyi attribútumot használhat a felhasználó/személy és az alkalmazás is. Eltérően a Kerberos-tól, a PAC nem engedélyez hozzáférést a speciális célhoz; helyette megállapítja a személy kategóriáját, intézményi tagságát, szervezeti pozícióját, aláírási jogát stb. Ezek a cél számára lehetővé teszik, hogy eldöntse, ezek az attribútumok illenek-e a sajátjaihoz; ez meghatározhatja a különböző kategóriájú személyek számára a célszervíz elérhetőségi idejét, és az aláírás elfogadásának számos típusát. Ez a megközelítés nagyon rugalmas.

A SESAME biztosítja a helyettesítés vagy „delegálás" lehetőségét. A cél tevékenykedhet megbízottként és használhatja az igazolást további célok eléréséhez a személy vagy szponzora számára. Ez elosztott hálózatok esetén alapkövetelmény. Az első cél továbbadja a következőnek a személy igazolását, hiszen a végső cél is szeretné tudni a személy attribútumait. Az igazolások továbbadása azonban számos csalásra ad lehetőséget. A cél működhet a saját érdekében valaki mást helyettesítve, felhasználva az igazolás valódi tulajdonosának aláírását és jogait.

Normál SESAME igazolások nem használhatók helyettesítésre, mivel tartalmaznak egy „SS-ID"-t, amit a cél csak abban az esetben tud elfogadni, ha az a szponzor-cél alap-

(folytatás a 6. oldalon)

(folytatás az 5. oldalról)

kulccsal van rejtjelezve. Ha a cél helyettesíteni szeretné a személyt, akkor a cél-cél kapcsolathoz új alapkulcsot kell kérnie a KDS-től, így az új SS-ID nem egyezhet meg az eredetivel. Az SS-ID lehet a szponzor azonosítója, vagy egy egyedi véletlen szám is.

Ha a személyek szeretnék, hogy a célok képviseljék őket, akkor a SESAME ezt mégis megengedi. Ez a célok egy úgynevezett „megbízható csoportján" belül lehetséges, a célok a csoporton belül képviselhetik egymást, de azon kívül nem. A mechanizmus tartalmaz az igazolásban egy megbízható csoportazonosítót és egy „védelmi értéket". A védelmi érték a kezdetben kizárólag a személy által ismert kontroll értékből kapható meg egy one-way függvény segítségével. A személy, ha szeretné, hogy helyettesítsék, ezt a kontroll értéket küldi el rejtjelezve a célnak, aki azt megoldva és a one-way függvényt használva meghatározza és érvényesíti a védelmi értéket. A második és további célok akkor tudnak elfogadni igazolásokat, ha azok a helyes kontroll értékkel vannak kombinálva.

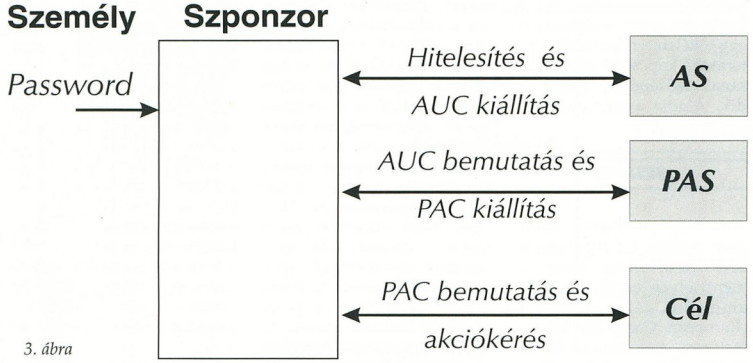
Architektúrák összehasonlítása

Érdemes lehet összehasonlítani a Kerberost, a SESAME-t és az X.509 aszimmetrikus kriptográfiai megközelítést.

A jegy/igazolás a következő szándékokat szolgálja.

A Kerberosban a jegy engedélyezi egy felhasználó (ügyfél) hozzáférését egy alkalmazáshoz (szerverhez). Ez tartalmazza a kapcsolatkulcsot. Általában minden kapcsolat számára új jegy szükséges. A jegyek nem nyilvánosak.

A SESAME- ban az igazolás azonosítja a felhasználó (egyén) attribútumait. A SESAME igazolások hosszabb életűek és szélesebb hatáskörűek lehetnek, mint a Kerberos jegyek, de valójában rövid idejűek (egy kapcsolatra vonatkoznak) és nem a nyilvánosság számára elérhetőnek szánják.



3. ábra

Az X.509-ben az igazolások a felhasználó nyilvános kulcsa érvényességének a nyilvánosság számára elérhető bizonyítékai.

Egy alkalmazásba (szerver/célpont) történő belépés biztonsága a következők szerint biztosított:

A Kerberosban az ügyfelet a jegy tulajdonosaként azonosítják egy kapcsolatkulccsal rejtjelzett igazolás segítségével. A következő parancsok hasonlóképpen rejtjelezhetőek, vagy a kapcsolat feltételezett integritására hagyatkozhatnak.

A SESAME- ban az egyént az engedélyezés rejtjelzése által az engedélyezés tulajdonosaként úgy azonosítják, hogy az igazolást és a hozzáférési parancsokat egy alapkulccsal rejtjelzik. Az alapkulcsot egy meglehetősen komplex eljárással hozzák létre és az SS-ID-hez csatolják.

Az X.509-ben a parancsokat a felhasználó a titkos kulcsával írhatja alá. Alternatívaként: csak a belépési kérelmet írják alá, és a rákövetkező parancsok a kapcsolat feltételezett integritására hagyatkozhatnak.

Egyéb biztonsági architektúrák

A Kerberos, a SESAME és az X.509 fontossága abban nyilvánul meg, hogy ezek egy szabványosított biztonsági architektúra fejlesztéséhez járulnak hozzá. Egy ilyen architektúra lehetővé teszi, hogy a különböző gyártóktól származó különböző rendszerek az OSI elvei szerint biztonságosan érintkezhessenek.

A Kerberosnak jelentős hatása van az elosztott számítástechnikai környezet (DCE) biztonsági szempontjaira. Léteznek javaslatok a jelenlegi DCE biztonsági tulajdonságainak kiterjesztésére, mely ötleteket és eljárásokat tartalmazna a SESAME-ból. Az X.509, amely még nyilvánvalóbban az aszimmetrikus kulcsú rejtjelzésen alapul, szintén közreműködő. Ebben az összefüggésben érdekes az, hogy a Digital Equipment-nél a nyilvános kulcsú igazolásokon alapuló javaslatokat részesítették előnyben.

Más szabadalmaztatott biztonsági architektúra is létezik, úgy, mint speciális csoportokra vagy intézményekre kifejlesztett architektúrák. Például az IBM-nek van egy olyan átfogó egyszerű kriptográfiai architektúrája, amely nagyrészt a DES algoritmuson alapul, és tartalmazza a bizalmasság valamint a hitelesség szokásos funkcióit.

Ez az architektúra számos rendszerben került implementálásra, software komponenseket éppúgy tartalmaz (standard kriptográfiai alkalmazói programozható interface (API)), mint hardware komponenseket (az IBM 4753 biztonsági hálózati processzor, a 4754 biztonsági interface-egység, a 4755 kriptografikus adaptor és az IBM személyi biztonsági kártya). Az IBM mostanában javasolt egy új, a Kerberoshoz kapcsolodó architektúrát „Krypto Knight" néven. Más gyártóknak is vannak hasonló termékeik, amelyeket beépíthetnek a saját architektúráikba.

Végül egy speciális felhasználói csoport számára kifejlesztett architektúra példájaként megemlíthetjük a NATO OSI biztonsági architektúrát (NOSA), amely az OSI hétrétegű modell biztonsági feltételeit határozza meg, és a hozzá kapcsolódó US OSD „plus" programot, amely nyilvános kulcsú rejtjelzésen alapul.

Rönkös Judit

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

Nyomás: Ságvári Nyomda Felelős vezető: Szilágyi Tamás

(folytatás a 2. oldalról)

maximum 4, egy stackben levő eszköz tartalék tápegységeként működik.

Mobil felhasználók kapcsolt vonalon

Az AccessBuilder Remote Access Server az egyik legújabb eszköz, mely lehetővé teszi a WAN hálózat elérését kapcsolt vagy bérelt vonalon, modemen, ISDN terminál adapteren vagy kapcsolt 56 DSU-n keresztül távoli egyedi PC-k felhasználói számára, vagy mobil PC-k felhasználói számára, illetve alkalmas két LAN összekapcsolására is, akár több párhuzamos, alacsony sebességű vonalon is.

Maximum 16 aszinkron, egyenként 115,2 Kbps sebességű dial-up portot, vagy maximum 2 szinkron 2,048 Mbps portot képes kezelni. LAN oldalon Ethernet vagy Token Ring hálózatra kapcsolódhat.

Amennyiben a hálózat fejlődése további dial-up lehetőséget kíván, a feladat egyszerűen megoldható egy újabb AccessBuilder üzembe helyezésével.

Az eszköz az IP és IPX forgalom routolására képes, míg az AppleTalk, DECnet, XNS, NetBIOS, VINES és egyéb IEEE 802.3 protokollokat bridge-eli.

A hálózati szervereket és adatokat az illetéktelen behatolástól az AccessBuilder 6 szintű védelmi rendszere óvja. (Jelszó védelem, automatikus visszahívás, kódolás, stb.) Az illetéktelen behatolási kísérleteket az AccessBuilder naplózza és jelenti a menedzsment állomásnak.

Transcend Management

A 3Com Corporation moduláris, un. Transcend Management rendszere *egységes, grafikus felületen* lehetővé teszi a hálózat menedzselését, – beleértve az eszközök konfigurálását, a hibaanalízist, a naplózást – a PC-kben lévő 3Com hálózati csatolóktól, a LAN-ok HUB-jain keresztül a WAN-hálózatig. Az un. Remote Network Monitoring (RMON) költséges analizátorok használata nélkül lehetővé teszi a gyors hibafeltárást. Automatikus discovery, topology mapping, event logging, és performance monitoring funkciókkal rendelkezik.

A Transcend management rendszer moduljai a IBM NetView/6000, a SunNet, a HP OpenView, az MS Windows, az OS/2, később a Novell NMS rendszerek alatt működnek.

Transcend Network Management For Windows

A már korábban megjelentetett, Windows környezetre készült, LinkBuilder FMS készülékek menedzselésére képes program továbbfejlesztéseként megjelent a Transcend WorkGroup Manager for Windows program, illetve már jelenleg is elérhető az igazán figyelemre méltó Transcend Enterprise Manager for Windows programcsomag.

Transcend WorkGroup Manager for Windows

Ez az első olyan Windows-os munkacsoportok (nem nagyhálózatok) számára készült SNMP menedzsment alkalmazás, amely lehetővé teszi mind a hub-ok portjainak mindpedig az adaptereknek egy rendszerben történő figyelését. Ez a port-to-adapter adatkapcsolat lehetővé teszi a gyorsabb hibakeresést. Képes önállóan megkeresni az összes SNMP eszközt a hálózatban, és ezeket grafikus képernyőn jeleníti meg. Az eszköz állapota a képernyőről a kódolt színek használatának köszönhetően azonnal leolvasható.

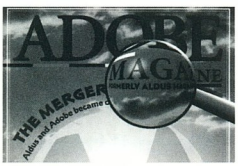
Transcend Enterprise Manager for Windows

Ez a program az előzőtől eltérően kezeli az összes átviteli rendszert egy vállalati hálózati infrasruktúrában. (workgroup, backbone, WAN). Kezeli az összes 3Com Ethernet adaptert, az Ethernet és Token Ring hubokat, a NETBuilder II-t, és már az egyik legújabb terméket, a NETBuilder Remote Office-t is.

A program teljesen SNMP kompatibilis, így képes kezelni más gyártók SNMP eszközeit is. A discovery során felismeri az összes 3Com eszközt, a NetWare, VINES, és LAN Manager szervereket, illetve a NetWare vagy az NDIS kompatibilis adaptereket.

dr. Zsótér Antal,
Gínál Gabriella

A + A = A



Nem ez a cím nem valamilyen betűrejtvény, hanem annak a ténynek a rövid összefoglalása, hogy a DTP két nagyhatalma, az Adobe és az Aldus nyár óta egy cég és a két névből hamarosan valószínűleg csak egy, az Adobe marad meg. A termékek ugyan egyelőre még a régi nevükön futnak, de például az egykori Aldus Magazine képen látható új számának fejléce már Adobe-ra változott és csak egy kisbetűs felirat utal a korábbi névre.

Az Aldusnak az egyesülésbe bevitt "gyerekei" közül egyelőre a PageMaker sorsa tűnik a legbiztosabbnak (ilyen program eddig teljesen hiányzott az Adobe palettájáról), így most néhány olyan kiegészítő alkalmazást szeretnénk bemutatni, amelyek az eddiginél is könnyebbé tehetik a vele való munkát.

Már elválik

Először is lássuk a már régen várt magyar elválasztó programot. A MorphoLogic fejlesztői szokásukhoz híven most is magasra tették a mércét, ezúttal olyan magasra, hogy a PageMaker nem is tudja mindig átugrani. A "Helyesel" gond nélkül telepíthető, gyorsan és szinte észrevétlenül dolgozik, szóval ideális lenne, ha... Ha a PageMaker is tudná, amit ő tud. Mert bár a szoftver algoritmusa képes lenne a hosszú kettős mássalhangzók (ssz, nny, stb.) betűbetoldásos elválasztására, ezt a PageMaker még nem tudja fogadni. Az Aldus fejlesztői ígérik, hogy a következő változat már miránk, szegény magyarokra is tekintettel lesz. A Mac-eseknek rossz hír, hogy az elválasztó program az ő gépükre egyelőre nem kapható

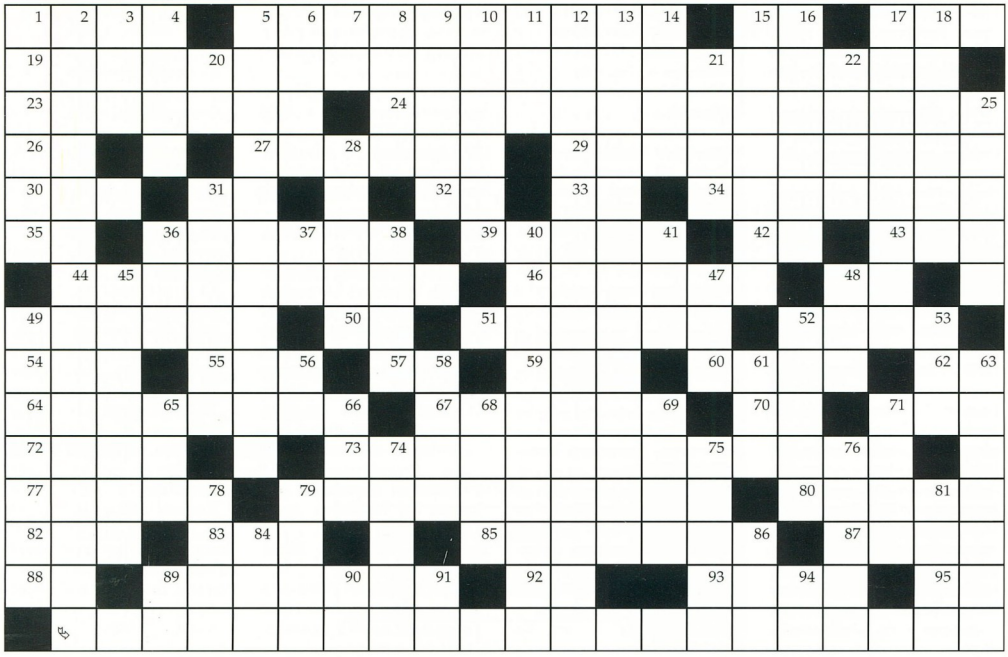
Végy egy adatbázist...

Ha van egy adatbázisunk, akkor annak tördelése eddig a PageMakerrel elég nehéz feladat volt, mivel nem volt olyan egyszerűen működő tördelési lehetőség, amellyel az adatbázis mezőneveihez lehetett volna formázási utasításokat rendelni. Most viszont megjelent az Info Publisher Database Addition, amellyel egyszerűen készíthetők katalógusok, árlisták. A program egy táblázatkezelőhöz hasonló grafikus felületet kínál a felhasználónak és a kész, formázott adatbázist közvetlenül helyezi át a PageMakerbe.

Igazodj!

Nagyon hiányzott a programból egy igazítási modul, amellyel az egyes elemeket lehetett volna egymáshoz képest elrendezni. A Zephyr SmartAlign programja a Corel felhasználóknak megszokott lehetőségeket nyújtja, még további szolgáltatásokkal kibővítve.

REJTVÉNY



Honnan kapta a nevét a Kerberos biztonsági architektúra? A választ a függőleges 2., a vízszintes 19. és a függőleges 12. sorokban rejtettük el.

Vízszintes

1. Savanyítószer. 19. A megfejtendő második része. 23. Fenséges németül. 24. Indulásra készen. 26. Ottlik Iskolájának sokatmondó mássalhangzói. 27. Becézett Nándort. 29. Előkelő léte. 30. Három spanyol autó. 31 A Balaton ilyen. 32. Magyarország rövidítve. 33. Jim eleje! 34. Selypes édesanya!. 35. Röntgensugár! 36. Ínycsiklandó. 39. Híres magyar grafikus (Endre). 42. Állatlak. 43. ...ferbivaly. 44. Kiruccanásaim. 46. Ritka férfinév. 48 Lötty. 49. Becézett női név. 50 Néma Séd!. 51. Elélendül. 52. Ravasz fickó. 54. Művészet. 55. Vigyázója. 57. A volt Szovjetunió volt autóinak volt jele. 59. "A" súly. 60. FordítGATT!. 62. Bíró Ferenc. 64. Több bizánci császár neve. 67. Mozdulatlanul. 70. Francia arany. 71. Csatorna is, ivólé is van ilyen. 72. Disznó háza. 73. Oszkár végzett vele. 77. Na itt ellentéte. 79. Édesapa lángesze. 80. Csípte. 82. Gézsé! 83. Német vörös. 85. Amerikai színész, rendező (Anthony). 87. ...itikum (csiszolt kőkorszak). 88 Zeusz tehene, fordítva. 89. Felvidéki városból való. 92. Nem férfi. 93. Nem azon. 95. Japán játék.

Függőleges

1. Átmeneti. 2. A megfejtendő első része, zárt betűk: S, Z, K, S, E, R. 3. Kevert hej! 4. Kemény fá ... i a fejszéjét, fordítva. 5. Argentína fővárosa. 6. Tűzhányó. 7. Kettős mássalhangzó. 8. Angol hosszmérték. 9. ... kedvezőek, olcsó vagyok. 10. Cafrangos. 11. Romániai folyó. 12. A megfejtendő harmadik része. 13. Szigetcsoport. 14. Becézett Izabellát, fordítva. 15. Műanyag kötőelem. 16. Kirúgja a labdát. 17. Ikon. 18. Vau-vauzna. 20. Körülbelül. 21. Becézett limonádé. 22. Osztrák szecessziós építész (Adolf). 25. Angol katonai kantin. 28. Daloskedvű. 31. Tout jeune kiejtve. 36. Gyomnövény. 37. Dupla mássalhangzó. 38. A 20. század pestise. 40 Dalmáciai ebédajánlat. 41. Buddhizmus is van ilyen. 45. Fekete István gyermekhőse. 47. Locomotív GT. 48. Függ. 52. Ide terelik a marhákat. 53. Hal is van ilyen. 56. Kötőszó. 58. Új Magyar Zenei Egyesület. 61. Magyar származású szobrász (Amerigo) 63. Nem tárgy és nem személy. 65. ... Roid. 66. Testtartás fordítva. 68. Keverve lepi! 69. Becézett Ilona fordítva. 71. Angol feleség. 74. Népies fiatal fickó. 75. "Te" asszony. 76. Kanta. 78. Királyi szék. 79. Apa. 81. Afrikai állam. 84. ... korban éltem én e Földön. 86. Népies szív. 89. A nagy varázsló, fordítva. 90. Ebben a funkcióban felülír a Word. 91. Szintén. 94. Indulatszó.

A megfejtés beküldendő a Montana Marketing Kft. címére: 1361 Budapest, Pf. 501. Beküldési határidő: 1995. január 31. A helyes megfejtők között ajándékcsomagokat sorsolunk ki.

Viszontlátásra 1995-ben!