NEWS

MONTANA

19. szám 1994. november

- Adatvédelem hálózatokon 2.
- Ügyviteli rendszerváltás -Scala for Windows
- 400 csapás Compaq módra - Contura 400-as sorozat

Ügyviteli rendszerváltás

Ugye Ön is volt már úgy, hogy bár tetszett egy ruha, mégsem vette meg, mert nem tudta egyértelműen megállapítani, jó-e a mérete? Akkor képzeljünk el egy külföldi befektetőt, akinek a magyar mérlegadatokból kellene eldöntenie, megéri-e a privatizálni kínált "áru" az érte kért pénzt! Tapasztalt vállalati pénzügyeseknek is rémálomszerű feladatot jelent sokszor, ha a cég mérlegét, gazdasági mutatóit a hazaitól eltérő szisztéma szerint kell kidolgozniuk. Márpedig éppen most, amikor a privatizáció felgyorsítása és minél több külföldi befektető becsalogatása a hivatalosan meghirdetett cél, egyre gyakoribb és természetes igény ez az érdeklődőktől. Az egyértelmű és gyors válasz lehetőségét kínálja a Scala, amelynek most jelent meg windows-os változata.

Külön melengeti szívünket, hogy az új programot teljes egészében Magyarországon fejlesztették és még az év vége előtt világszerte 80 országban kezdik meg az értékesítését. 18 szakember több, mint egy évi fejlesztőmunkájának eredménye már a bevezetés pillanatától 30 nyelven kapható.

Országról országra

Ez a soknyelvűség nem véletlen, hanem a Scala nemzetközi sikerének egyik alapja. Az eredeti programot az angoltól a kínain át a magyarig már több mint 30 nyelvre fordították le. Ez azt jelenti, hogy minden ügyfélnél meghatározhatjuk, milyen nyelven küldjünk neki számlát, milyen nyelven levelezzünk vagy milyen valutában számoljunk el.

A nyelv értése azonban nem okvetlenül járna együtt a helyi szabályozók ismeretével, márpedig azok nélkül ugye.... A Scala ezt úgy küszöböli ki, hogy valójában minden országban ugyanaz a Scala verzió használatos. A helyi Scala irodának kell számontartania és követnie az adott ország jogszabályainak, adózási és könyvelési előírásainak a változását, majd beépítenie azokat az ország moduljába. Így azok bekerülnek a rendszerbe, a felhasználónál pedig az adott országkód megadásával a program automatikusan átáll a helyi szabályozórendszer használatára. Ezt különösen azok a cégek tudják értékelni, amelyeknek vagy szerteágazó nemzetközi hálózatuk, vagy hasonló ügyfélkörük van. Nem véletlen, hogy a Scala vevői között találjuk az AT&T-t, a SAS-t, a Tetra Pak-ot, vagy hazánkban a Magyar Televíziót és a Pannon GSM-et.

DOS és Windows

Az ilyen nagyságrendű cégek persze kevés dologtól irtóznak jobban, mint ha valaki előáll egy olyan ötlettel, hogy holnaptól egészen más rendszer szerint kell könyvelniük, számlázniuk. A Scala ez ellen kétféle megoldást is kínál. Egyrészt modulrendszerű és apránként is megvalósítható az átállás. Ma a rendszer 18, egymással integrált modult tartalmaz, benne a Főkönyvet, a Bejövő és Kimenő Számlakönyvet, de a Bérszámfejtést vagy a Készletnyilvántartást is.

Azok pedig, akik már használják a rendszert, gond nélkül működtethetik tovább a Windows alatti változattal együtt.

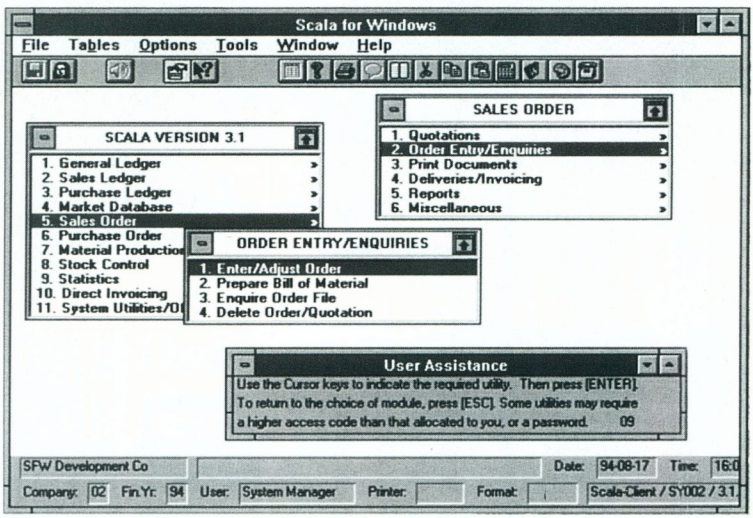
Információcsere

Megőrizve a hagyományos scala-s szolgáltatásokat kiegészítették a Windows egyszerű kezelhetőségével. A BTrieve filekezelő rendszer révén más programokban, például Lotus 1-2-3-ban, vagy Excel-ben készült állományokat is felhasználhat. Másik újdonság a Jelentéskészítő, amelyben a felhasználó a grafikus környezetnek hála a kinyomtatás előtt megtekintheti az elkészített jelentés képét. A felhasználó munkáját segíti az általa kialakítható eszközsor és természetesen a jobb windows-os alkalmazásoktól megszokott széleskörű Help is.

Háromszoros forgalom

A Scala Hungary Kft. idén várhatóan megháromszorozza eladásait a tavalyi évhez képest. Véleményük szerint ennek az az alapja, hogy egyre több cég ismeri fel egy nemzetközi piacon elfogadott ügyviteli program használatának szükségességét. Mivel pedig Magyarország minden gondunk ellenére még mindig stabil politikai és gazdasági hátteret nyújt, az itteni vegyesvállalatok számára az Ablaksoft Kft. közreműködésével kifejlesztett Scala for Windows ideális megoldás.

Lapzártakor érkezett a hír, hogy ügyviteli rendszere korszerűsítése érdekében az egyik vezető számítógépgyártó, az ICL magyarországi leányvállalata is a Scala lépcsőzetes bevezetése mellett döntött.



A Notes még nálunk is gyorsabb volt

Bár igyekszünk mindig a legfrissebb újdonságokkal megismertetni olvasóinkat, a szerkesztési és nyomdai átfutás időnként nem képes versenyezni a számítástechnika fejlődési ütemével. Így volt ez legutóbbi számunk esetében is, amikor a megjelenés idejére a Lotus Notes-ról szóló cikkünk néhány információja már el is avult.

A Notes szerver programja a 3.11, 3.12 és 4.0 Novell verziókon is képes futni, sőt maximum 5 felhasználóra korlátozva a sima Windows 3.1-en is. Várhatóan még az idén megkezdik az SCO UNIX és AIX 3.1.5 operációs rendszerekre tesztelt szerverprogramok árusítását is.

Rántott csirke Tornádóval

Ezt a szokatlan menüt az Santa Cruz Operation (SCO) állította össze az elmúlt hetekben. A cég, amely az IDC felmérése szerint a UNIX-os operációs rendszerek vezető szállítója – 1993-ban például az eladott UNIX operációs rendszerek 37%-a az SCO terméke volt, – a közelmúltban két teljesen eltérő megrendelőt vehetett fel megrendelői listájára.

Az egyik a Kentucky Fried Chicken, amely az SCO Open Server rendszerét választotta az éttermeket kiszolgáló informatikai rendszer alapjául. A másik a RAF, az Angol Királyi Légierő, amely 8000(!) Open Server-t rendelt meg a vadászgépek karbantartási-ellátási munkáinak felügyeletét végző informatikai rendszerhez, amelyben több, mint 30 ezer felhasználó dolgozik.

Ez a két megrendelés is bizonyítja az SCO UNIX nyitottságát és az alkalmazók igényeihez való maximális alkalmazkodóképességét. A Montana 1991. nyara óta forgalmazza ezt az operációs rendszert mint az SCO magyarországi master reseller-e és az utóbbi időben a felhasználók nálunk is egyre növekvő érdeklődést mutatnak iránta.

3Com újdonságok

A 3Com szeptember végén egy csokor új terméket jelentett be. Az FMS hubok új családja, az FMS II. már 8 elem stackelését teszi lehtővé az eddigi négy helyett. A szintén most piacra dobott, hozzá illeszthető LinkSwitch modul 6 Ethernet és 1 FDDI portot tartalmaz. Ez az Ethernet switch modul 10 Mbit/sec dedikált sávszélességet biztosít mind a hat Ethernet portra, jelentősen növelve ezzel a kliens-szerver alkalmazások hatékonyságát.

A NetBuilder router család is új tagokkal bővült. Nemcsak új Remote Office routereket jelentettek be mind a hagyományos, mind a boundary routingot használók számára, de a családhoz tartozó szoftver legújabb, 7.1 verzióját is megjelentették. Ez elsősorban a boundary routing-ot használók számára tartalmaz előnyös újdonságokat.

A Kedves Olvasó

most valószínűleg először a naptárhoz kap meglepetésében: hogy lehet ez, november és Montana News? Hát igen, ennek két oka is van. Egyrészt nem akartuk Olvasóinkat megfosztani az évi hat találkozási alkalomtól, márpedig a nyári uborkaszezon miatt kicsit hosszabbra nyúlt a szünet és ezt be szeretnénk pótolni. Másrészt mint a mellettünk lévő rövidhír is mutatja, most olyan gyorsan jönnek a minket érintő újdonságokról szóló hírek, hogy nem akartuk őket két hónapig tartogatni.

Körülöttünk közben zajlik az élet. Amikor az adatvédelemről, rejtjelezésről szóló sorozatunkat múlt hónapban elindítottuk még nem gondoltuk, hogy a fél ország azt fogja mára találgatni, ki kit és kinek az utasítására hallgatott le. A másik fele pedig azon csodálkozik, hogy Friderikusz Sándornak újbóli megjelenése alkalmából sikerült egy gyanútlan utcai járókelőt másfél óra alatt útnak indítania Hawaii-ra, firss útlevéllel, amerikai vízummal és szalmakalappal. Jellemző technikai fejlettségünkre, hogy az nem jutott eszükbe, milyen jó útiélményeket írhatna mondjuk egy Contura 400 notebookon. Na mindegy, ha mindenki Fridije ilyen tempóban gyűjti a nemzetközi szponzorokat és fogadja a nemzetközi sztárokat, akkor hamarosan ő is rá fog szorulni a Scala for Windows szolgáltatásaira. A program egyébként akár magába a show-ba is bekerülhetne: 80 országban járt, 30 nyelven beszél, nagyon látványos – mi kell még?

Ebben a nagy zajlásban mi pedig egy kicsit megváltoztunk. Ahogy az a cikkekből is látszik, szeretnénk a jövőben a technikai újdonságok ismertetése mellett, megvalósult rendszereket és a létrehozásukhoz vezető utat is bemutatni, megkönnyítve ezzel egy kicsit azok dolgát, akik ma állnak hasonló döntések előtt. Reméljük, hogy ez az új tartalom a jövőben sokaknak segít abban, hogy új reklámunk szlogenjének megfelelően "Nyerjen velünk!"

Négyszáz csapás Compaq módra

A Compaq – versenytársai legnagyobb bánatára – lassan eljut oda, hogy különlegesebb hírnek számít, ha mondjuk egy negyedévig nem jelent be újdonságot, mint az, ha bejelent valamit.

A felhasználók persze azért még mindig inkább a bejelentéseket várják, általában nem is hiába. Most a Contura 400 sorozattal a hordozható gépek frontján dobott új erőket csatasorba az európai piacon vezető notebook-gyártó.

Olyan gépet csinálni, ami ma a legkorszerűbb viszonylag egyszerű (már ha valaki egyáltalán tud gépet csinálni). Olyat viszont ami mondjuk még egy év múlva is az lesz, már sokkal nehezebb. A Compaq azonban a sikernek ezt a nehezebb, ám kétségtelenül tartósabb útját választotta a korábban is népszerű Contura sorozat megújított tagjaival.

Jövőre is korszerű

Egy korszrű notebook még ma sem filléres beruházás, érthető tehát, ha birtokosa nem szeretné néhány hónap múltán technikatörténeti emlékként kezelni. A Contura 400 tulajdonosainak nem fog fájni a feje amiatt, hogy hogyan kövessék a technikai fejlődést. Jelenleg 486DX2/40 Mhz SL processzor ketyeg valamennyi gépben és háromféle képernyővel (monokróm vagy színes STN, illetve színes TFT) kerülnek forgalomba. Ha valaki a vásárláskor még nem mérte fel pontosan az igényeit, vagy csak nem volt pénze a legnagyobb teljesítményű 400CX modellre, a későbbiekben a processzort de még a képernyőt is kicserélheti korszerűbbre.

A merevlemez és a memória egyszerűen cserélhető, csak egy-egy borító panelt kell leemelni és máris behelyezhetjük az új egységet.

Gondoltak a fejlesztők a felhasználók ergonómiai igényeire is. Úgy tűnik, vége az ET korszaknak, amikor a notebookok billentyűzetét csak a kis űrlény vékony ujjaival lehetett gond nélkül használni. A Contura 400 szabványos 101/102 gombos billentyűzetet kínál az előírt 0,85 mm-es billentyűközzel, a megszokott funkció- és kurzorbillentyűkkel. A nagy, 19 mm-es követőgolyó a beépített tenyértámasz közepén helyezkedik el, a kényelmes kéztartást pedig a billentyűzet dönthetősége segíti.

Elemi követelmények

A nagyteljesítményű processzor és kijelző persze fokozott követelményeket támaszt a gép energiaforrásával szemben is. A monokróm kijelzős változat 6, az színes modellek 5,5 órányi üzemet bírnak ki újratöltés nélkül. Eltűntek a speciális, egy-egy típushoz kifejlesztett akkuk, az áramforrás szabványos, újratölthető Duracell notebook elem. Ez azt is jelenti, hogy ha valahol véletlenül sürgősen szükségünk van új tápegységre, akkor elég csak egy nagyobb elektronikai boltot felkeresnünk.

Persze a Contura 400 maga is mindent megtesz azért, hogy minél tovább használhassuk. A gépek megfelenek az EPA EnergyStar követelményeinek, és 7 napig tárolják készenléti állapotban az adatokat. A felhasználó is kezdeményezheti a hibernálást, de biztonsági okból a gép maga is megteszi ezt. A billentyűzet felett lévő, kicsit az autók műszerfalára emlékeztető kijelző egyébként folyamatosan tájékoztat a telep állapotáról. Természetesen hálózati adapter is tartozik a géphez és külön autós adapter is rendelhető hozzá azoknak, akik gépkocsijukban is használni akarják mobil irodájukat.

Dokk ahoy!

Amikor pedig visszatérnek állandó irodájukba, a már megszokott Compaq dokkoló bázisba csatlakoztatva igazi asztali géppé alakíthatják kézi kedvencüket. A helyi sínes integrált grafikus vezérlő képes akár egyszerre is támogatni a belső és a külső monitort, ez utóbbit 1024 x 768 felbontásig.

A modellek rendelhetők integrált Ethernet csatolóval is, amelyeknél a soros és kiterjesztett párhuzamos portok RJ-45 és BNC csatlakozókkal is kiegészülnek.

A PCMCIA bővítésekhez két II. típusú, együttesen is használható slot található a gépen, ezek egy III. típusú bővítőhelyként is használhatók.

Harsányi László

SECURE DATA NETWORKING
2. rész

A kereskedelemben kapható információvédelmi termékek a következő formában állnak rendelkezésre:

- **hardver eszközök:** mint a PC- be helyezhető kártyák alkalmas firmwarekkel; vonaltitkosító egységek; chipkártyák és a hozzájuk tartozó interfacek; PIN pad-ek; tamperproof modulok; és algoritmusok megvalósítására szolgáló integrált áramkörök (pl. DES-chip).
- **szoftver csomagok:** a végfelhasználók rendszerébe ágyazva, vagy az operációs rendszerbe, esetleg a szoftverek device driverébe beépítve. Ezek a csomagok tipikusan a kulcsgenerálás, a biztonsági management szolgáltatások, és a rendszerek hozzáférhetőségének hitelesítése terén alkalmazhatók elsősorban.
- **kiegészítő egységek:** amelyek nem kifejezetten biztonsági eszközök, de kiválóan alkalmazhatók biztonsági rendszerekben, mint a csak olvasható és optikai memóriák, vagy archiváló eszközök.
- **rendszerek:** amelyek integrálják a fentieket egy vagy több biztonsági szolgáltatás ellátása és a támadók azonosítása érdekében.

Kommunikációs rejtjelzők

A kommunikációs rejtjelzők a végrendszerek között cserélt adatok bizalmasságáról gondoskodnak. Az alapkonfiguráció az 1.ábra bérelt pont-pont konfigurációja. Az "A"-ban levő rejtjelző az összes "A"-ból "B"-be küldött adatra hat, "B"-ben a megoldó visszafejti az adatot; vice versa az ellentétes irányban.

A kapcsolat lehet aszinkron, ekkor a rejtjelzés karakterenként történik. Ha a kapcsolat szinkron, a rejtjelzés lehet folyamatos egy duplex csatornán, vagy esetleg blokkonkénti egy duplex vagy félduplex csatornán.

Ha a blokkonkénti rejtjelzést használjuk, a rejtjelzőnek képesnek kell lennie arra, hogy felismerje a blokkok kezdetét és végét; figyelembe véve a használt kommunikációs protokollt, vagy az ellenőrző rendszer explicit parancsát.

A két rejtjelző egység között egy saját protokollt alkalmaznak, a következők vezérlésére:

- a rejtjelző és a megoldó eljárások szinkronizálása;
- a használt rejtjelző/megoldó kulcsok invokációja.

A leggyakoribb kulcskezelő eljárásmód, hogy mindegyik rejtjelző/megoldó egység saját tamperbiztos területén tárolja a rejtjelzett mesterkulcsok biztonsági listáját, amit előre letöltöttek az egységekbe. A kulcsok tápfeszültség-kiesés ellen is védve vannak. Minden kommunikációs kapcsolat számára a kulcsok egyikét kiválasztják. Ezt vagy közvetlenül kapcsolatkulcsként, vagy a kapcsolatkulcs megoldására, vagy egy véletlenszámmal együtt a kapcsolatkulcs kiszámítására használják.

A leggyakrabban használt rejtjelző algoritmusok a szimmetrikus algoritmusok, mint a DES, de saját algoritmusokat is sokszor használnak.

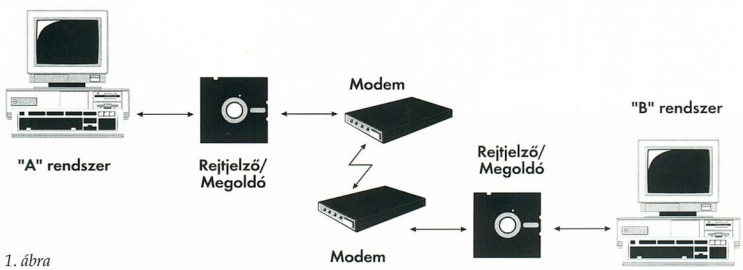
Az 1.ábra alapkonfigurációjának számos változata van. Például a rejtjelzőt beépíthetik a modembe vagy a host rendszerbe (pl. mint egy PC- be helyezhető kártya).

A rejtjelzők lehetnek protokollérzékenyek is, és csak az adatblokkokon vagy a frameken operálnak, például a BSC, HDLC és SDLC, vagy az X.25 adatcsomagok esetén. Ez történhet egy független rejtjelzőegységben vagy egy kombinált rejtjelző és protokoll egységben. A protokollérzékeny megközelítés lehetővé teszi a hibadetektálást és hibajavítást a rejtjelzett szövegen.

Az X.25 esetén, a protokoll- és a rejtjelző egységet általában önálló rejtjelző berendezésként (esetenként pl. PC-be helyezhető kártyaként) alkalmazzák. Ez esetben csak az X.25 adatcsomagjainak tartalmát rejtjelzik.

Magasabb szintű kommunikáció esetén a rejtjelzést a protokollfüggő szoftvercsomagok vagy alkalmazások hajtják végre. A rejtjelző/megoldó szoftver termékek rendelkezésre állnak a leggyakoribb operációs rendszerek alatti működésre. Ezek a szoftverek azokat a funkciókat teljesítik, mint az alcsonyszintű rejtjelzők. Előnyük, hogy a szinkronizálás esetükben nem gond, viszont a szoftverekben levő kulcsok biztonsága problémás. Egy gyakori megoldási mód, hogy a szoftvercsomagokat egy tamperbiztos társprocesszoros kártyával védik, amit egy alkalmas szoftver hív meg végrehajtáskor. A kulcsokat (és a kódot) biztonságosan elszigetelik a szoftver többi részétől, például úgy, hogy a kulcsokat védett formában önálló floppy-lemezeken, vagy chip-kártyán tárolják.

Végül meg kell még említenünk, hogy a nyers adatokon dolgozó rejtjelző használható bármilyen digitális adatfolyamon, például digitalizált hang esetén. Létezik digitális telefon, amely olyan modern kompressziós technikákat használ, mint a CELP (kód-gerjesztett lineáris predikció), a két végponton elhelyezett rejtjelző/megoldó berendezéssel kiegészítve.



1. ábra

Filebiztosító termékek

A filebiztosító termékek általában a következő követelmények egyikének vagy mindkettőjének megvalósítására használhatók:

- a file-ok bizalmassága rejtjelzéssel;
- a file-ok integritása, ellenőrző összeggel.

Filevédelem érdekében minden felhasználónak kívánatos a saját kulcsát használni. A kulcsok potenciálisan nagyon hosszú életűek is lehetnek, ha a file-okat hosszú ideig kell tárolni. A file titkosítása és újraolvasása között több hónap is eltelhet, és

(folytatás a 6. oldalon)

ezalatt a file tulajdonosa megváltoztathatja a kulcsát. Így a felhasználó azonosítása után a felhasználó megfelelő kulcsát is ki kell választani.

A felhasználói kulcsok tipikusan egy szimmetrikus személyi kulcson alapulnak, amit minden használatkor egy megnövekedett offset-tel (számláló) módosítanak. Ha a számlálóértéket elraktározták a file-ban, a rejtjelzéskor használt kulcs később visszaállítható.

A felhasználó egyéni alapkulcsait biztonságosan kell tárolni valahol. Ezt megtehetik egy tamperbiztos interface-kártyán vagy társprocesszoron. Egy másik, gyakran használt módszer, hogy a felhasználók kulcsát hordozható kártyán tartják.

Egy felhasználó file-jának bizalmasságát rejtjelzéssel, az integritást pedig integritásellenőrző vagy manipuláció felderítést ellenőrző (MDC) hozzáfűzésével biztosítják. Az integritásellenőrzőt minden védendő file végéhez csatolják akkor, amikor a filet eltárolják. Általában dátumot, időt és egyéb információt csatolnak az adatfile-hoz és azokat belefoglalják az ellenőrzésbe. Az integritásellenőrzőt újragenerálják és összehasonlítják a tárolt értékkel akkor, amikor elolvassák a file-t.

A file-okat természetesen egyaránt védhetik integritás-ellenőrzővel és rejtjelzéssel.

Azokban a rendszerekben, amelyek az egyéni felhasználók file-jainak védelméről gondoskodnak, ugyanolyan mechanizmussal oldják meg a rendszert alkotó file-ok védelmét is.

A felhasználó azonosítására szolgáló termékek

Sok termék létezik a felhasználó azonosítására. Ha a felhasználó a helyi rendszerhez tartozik az azonosítására megszokott az alábbi adatok megadása:

- jelszó vagy személyi azonosító szám (PIN);
- a személyes chipkártyáján tárolt titkos adat.

A jelszót vagy a PIN- kódot a klaviatúrán kell begépelni, míg a titkos információt a chipkártyaolvasó olvassa be. Ezt a két adatot felhasználva egy one-way függvény inputjaként, két összehasonlítandó értéket kapunk. Ha az értékek megegyeznek, akkor a felhasználót biztonságosan sikerült azonosítani.

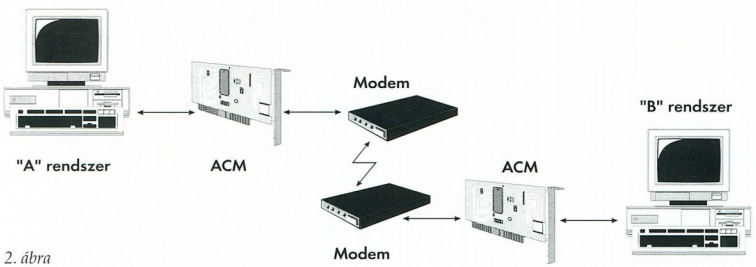
Sok más személyi azonosító rendszer létezik. Például egy rendszer alkalmassá tehető arra, hogy olyan távoli unintelligens terminálokat irányítson, amelyek valaminek az ismeretén (PIN, jelszó) és birtoklásán alapulnak.

Ebben az esetben a " birtokolt valami " nem egy chipkártya (hiszen itt nincs chipkártyaolvasó), hanem egy kis mobil eszköz, amely a felhasználó azonosítására szolgáló titkos információt hordoz. Amikor az eszközt a képernyő felé tartják, válaszol a host által küldött adatra, amely függ a felhasználó feltételezett azonosítójától és az időtől. Az eszköz válaszul megjelenít egy login kódot. Ez a kód mind a három inputtól függ: tehát a feltételezett azonosítótól, az időtől, továbbá az eszközben lévő titkos azonosítótól.

A felhasználó most be tud lépni ezzel a kóddal, amelyet összehasonlítanak a számítógép által generált engedélyezési értékkel. Az összehasonlítás hibát mutat, ha a felhasználó valaki más eszközét használja. A belépőkód csak egy adott időtartamra érvényes, ezáltal megakadályozva egy későbbi jogtalan felhasználást.

Termékek a rendszerek közötti hozzáférési jogok ellenőrzésére

Ha a kommunikációban résztvevő mindkét fél megfelelő számítási képességgel rendelkezik, akkor kölcsönös azonosítási protokollok hajthatók végre, amire egy humán felhasználó, vagy egyszerű terminál nem lenne képes.A tipikus elrendezés a 2.ábrán látható.



2. ábra

A hozzáférést vezérlő modul (ACM) lehet önálló egység, vagy a rendszerbe integrált kártya. A modul feladata biztonságosan azonosítani minden kommunikációban résztvevő tagot.

Két oka van, hogy a legtöbb esetben az ACM megközelítést használják az egyszerűbben implementálható szoftver megoldások helyett:

1. A kulcsok a berendezés tamperbiztos területén tárolhatók.
2. A szabványos kommunikációs szoftverek használata A és B között nem kívánatos.

Az ACM - ACM azonosításra tipikusan egy vagy több, mindkét ACM-ben titkosan tárolt szimmetrikus titkos kulcsot használnak. A megfelelő kulcs kiválasztása azután történik, hogy a kommunikációt kezdeményező közli az azonosítóját. A hitelesítési eljárás a következő:

1. ACM **A** generálja az RA véletlen számot és elküldi az ACM **B**-nek
2. ACM **B** XOR-olja az RA-t az aktuális titkos kulccsal K-val, kiszámolja az f(RA+K)-t, ahol f() egy one-way függvény, és elküldi **A**-nak
3. **A** kiszámolja az f(RA+K)-t és összehasonlítja a **B**-től vett értékkel. Ha egyezik, akkor **A** azonosítja, hogy **B** K-t birtokolja.
4. Ezután **B** hitelesíti **A**-t az RB hasonló módon történő elküldésével

Egy másik megközelítés esetében **A** és **B** egyaránt az f(T+K)-t számolja ki, ahol T az aktuális idő. A kapott érték egy (nagy) decimális szám, aminek páros számjegyeit **A** elküldi **B**-nek, míg a páratlanokat **B** elküldi **A**-nak. Ha a vett számjegyek egyeznek a kiszámoltakkal, akkor a küldő hiteles.

Security Management termékek

A Security Management (továbbiakban SM) funkciói az alábbiak:

- Kulcsmanagement (KM).
- Beloggolás.
- Ellenőrzés.

Néhány termék esetén a kulcsgenerálás és a kulcsok letöltése még a szállítás előtt megtörténik. Sokkal elfogadhatóbb megoldás, ha a vásárló maga képes a felhasználói kulcsok menedzselésére. Ezt általában egy saját PC-n futó védett szoftver valósítja meg. A szoftvert titkosított formában egy ellenőrző összeggel ellátott file-ban tárolják. Csak betöltés esetén oldják meg, és futni csak akkor fut, ha a rendszer azonosító amivel indították, megfelelő.

A KM felhasználói kulcsokat generál, és azokat letölti vagy magába a rejtjelző egységbe, vagy egy kulcshordozóra (pl. chipkártyára).

Olyan rendszerekben, ahol a kulcsokat PIN segítségével

Váltás év közben

lehet aktiválni, a KM feladata a megfelelő PIN-ek generálása és rejtjelzett formában történő letöltése. Ez a későbbiekben a felhasználó azonosítására is szolgál.

Általában a KM nem tárolja a felhasználói PIN-t, ha mégis akkor kizárólag rejtjelzett formában.

Néhány KM RSA algoritmust használ, azaz nyilvános és titkos kulcsokat generál és oszt ki. Ezek a rendszerek igazolási listákat tartalmaznak (pl. alá tudják írni a kiadott nyilvános kulcsokat).

Tipikus PC-s biztonsági termékek

Egy PC-s környezetben alkalmazható biztonsági termék az előzőekben említett eszközök nagy részét, de nem feltétlenül mindet tartalmazza. Például egy olyan információvédelmi eszköz amely egy beépített chipkártya-vezérlővel rendelkező biztonsági társprocesszoros egységet tartalmaz, a következőket támogatja:

- a rejtjelző egység jogosulatlan felhasználóval szembeni fizikai és logikai védelmét
- a chipkártya tartalmának fizikai és logikai védelmét
- felhasználó azonosítást és hitelesítést
- a felhasználói file-ok ellenőrző összeggel történő szelektív hitelesítését
- a felhasználói file-ok szelektív védelmét rejtjelzéssel;
- rendszer file-ok hitelesítését
- rendszer file-ok rejtjelzését
- biztonságos beloggolást és a biztonsági események archiválását
- hitelesítési eljárásokat távoli hostok hozzáférése esetén
- offline kulcsmanagement rendszert

Sorozatunk következő, befejező részében röviden bemutatunk néhány olyan populáris biztonsági architekturát, mint a "KERBEROS" vagy a "SESAME".

Kovács Tamás

A Topp Group ma Magyarországon az egyik legnagyobb felhasználója a Scala-nak. 1994-ben vezették be, méghozzá év közepén. Mivel egy ilyen célú programcsomagról mindennél többet mond a tényleges üzemeltető véleménye, megkértük Peter Nielsent a Topp Group igazgatóját, hogy ossza meg tapasztalatait olvasóinkkal.

– Nem jelentett-e gondot az év közbeni átállás?

Kereskedelmi erőfeszítéseink hatására forgalmunk olyan mértékben emelkedett, hogy a régi számlázó programmal, illetve manuális adatfeldolgozással nem lehetett biztosítani a naprakészséget. Dönteni kellett, hogy a probléma megoldását az adminisztrációs létszám megnövelésével és egy komplett szoftver csomag megvásárlásával, vagy egy külső könyvelő cég megbízásával oldjuk meg.

Az évközbeni bevezetés mellett szólt, hogy közel azonos feladatot jelentett az éves adatmennyiség manuális feldolgozása, mint a Scalára történő átállás és az új módszerrel történő adatbevitel.

Egyszeres adatbevitel

A Scala legnagyobb előnye, hogy egyszeres adatbevitel mellett, az adminisztrációs feladatok elvégzésén túl szinte korlátlan lehetőséget biztosít a folyamatok részletes ellenőrzésére, kimutatások készítésére.

Az évközbeni bevezetést mindenképpen javasoljuk, mert bár az átmeneti időszakban mindkét módszerrel kell a könyvelést végezni, ellenben ha a bevezetés időpontja január elseje, még az előző év lezárása is növelné a terhelést.

Lényeges azonban, hogy az új módszerrel történő feldolgozás kezdetének időpontjáig a felhasználók teljes képzése befejeződjék, mert ez alapvető feltétele a pontos, gyors adatbevitelnek.

– Volt-e szükség különleges szervezési intézkedésekre ahhoz, hogy ilyen rövid idő alatt történjen meg a a bevezetés? Végül is 2 hónap alatt feldolgozták nyolc hónap anyagát.

A Scala bevezetési időpontját az határozta meg, hogy a Scala által megkívánt folyamatokhoz ki kellett alakítsuk a megfelelő szervezeti felépítést. Újból kellett szabályozni az információáramlás folyamatát, meg kellett tervezni az új bizonylatokat, rögzíteni kellett az egyes munkakörökben dolgozók hatáskörét, felelősségét, a feldolgozások és továbbítások határidejét, melyeket új munkaköri leírásokban rögzítettünk.

Mindenki képben volt

Nagy segítséget jelentett, hogy a bevezetés során a cég vezetése a teljes folyamatot megismerte, tevékenyen részt vett benne. Így nem okozott problémát az azonnali, ám átgondolt döntések meghozatala. Az alkalmazottak betanítása és felkészítése az új rendszer használatára munkaidő után történt.

– Milyen segítséget nyújt ma a program a munkájában?

A Scala naprakész és teljeskörű információt biztosít a forgalom, a készletek és a pénzügyi helyzet állapotáról, a likviditásról és a profitról. Teljeskörű tervezést tesz lehetővé, valamint biztosítja a mindenre kiterjedő ellenőrzést is.

Megtérülő befektetés

A program rugalmassága többféle elemzési, illetve statisztika készítési lehetőséget biztosít a különböző folyamatoknál (árképzés, költségelemzés. A program gondoskodik róla, hogy az adatokhoz illetéktelenek ne férhessenek hozzá.

A probléma célszerű megoldása érdekében szükség volt erre a befektetésre, és egy korszerű megoldásra, melynek segítségével hosszútávon tudunk eleget tenni a követelményeknek. Ezek a költségek hosszabb távon tekintve alacsonyabbak mint a létszámnövelés, vagy egy külső cég megbízása.

További előnyt jelent a naprakészség, valamint az, hogy a rendszer magasszintű segítséget nyújt a cég vezetéséhez és a marketinghez.

– A telepítés és a betanítás során milyen segítséget kapott az installáló szervezettől? Mi volt nagyobb segítség, a dokumentáció, vagy az oktatás?

A Montana Informatika Kft. biztosította és installálta a Scala Hungary Kft. által javasolt hardver berendezéseket. Az alkalmazottak betanítása a Montana Marketing Kft. szakembereinek segítségével történt tanfolyamok, illetve konzultációk keretében.

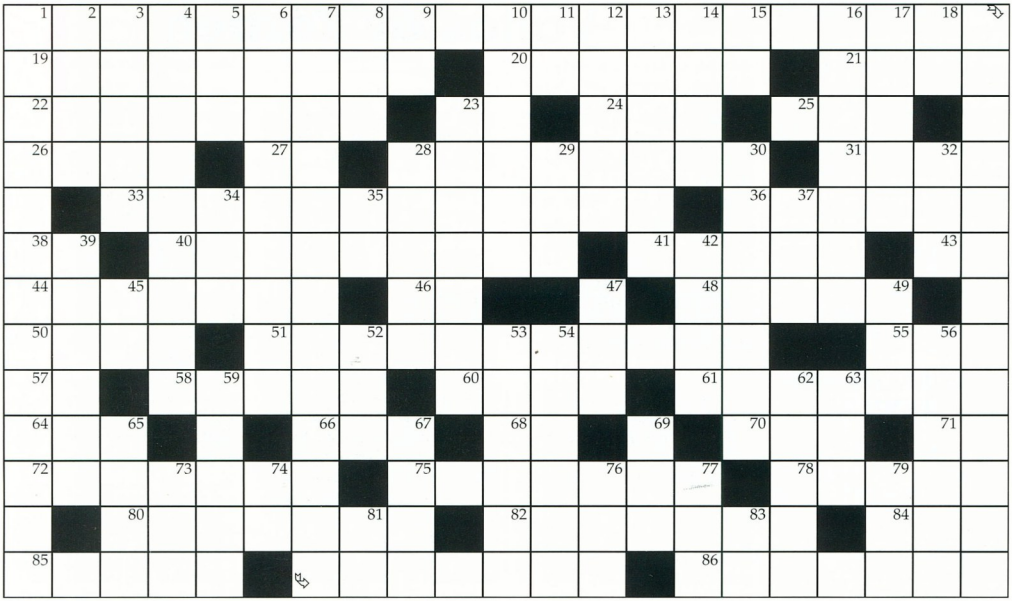
Az írásos dokumentáció viszonylag kevés segítséget nyújtott, a gyors bevezetést leginkább a próbaállományon történt gyakorlás és tesztelés tette lehetővé.

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: MESTERPRINT Kft.
Felelős vezető:
Szilágyi Tamás

REJTVÉNY



Súlyom kicsi,
Eszem sok,
Mondd meg nékem,
Ki vagyok?

A választ a vízszintes 1., valamint a függőleges 7. sorokban rejtettük el.

Vízszintes:

1. A megfejtendő válasz első sora, zárt betűk: E, C, A, C, U. 19. A kis Edit rí. 20. Növényi zsiradék. 21. ... d' Orsay, fordítva. 22. Orvosi vények. 23. Kicsinyítő képző. 24. Nemzetközi kamionjelzés. 25. ... right. 26. Egyesült Nemzetek Szervezete. 27. Kutya. 28. Hajnal. 31. Római államférfi. 33. Magyar színésznő. 36. "A" padon. 38. Irodalmi hetilap, rövidítve. 40. Mesebeli állam, a Hajnal birodalmának ellentéte. 41. Felöltöm. 43. Múlt idő jele. 44. Csinosabbat. 46. Lekvár. 48. Fényforrás. 50. Kugli. 51. Németország budapesti nagykövete a második világháború idején. 55. Izgalom jele az arcon. 57. Rangjelző szócska. 58. Alkohol. 60. Bessenyei György egyik drámájának címszereplője. 61. Tekeré. 64. Északi szarvasfajta. 66.Zalaegerszegi Torna Egylet. 68. Deciliter. 70. Kínai vallási és filozófiai tanítás. 71. Tamási Áron. 72. Kattog. 75. Kikapcsol. 78. Német germanista, a német nyelv szófejtő szótárának szerzője, Friedrich (1856-1926). 80. Nyakmelegítő befejeződése. 82. Francia kapcsolat. 84. Oszlopfajta. 85. Ritka női név. 86. Zajos.

Függőleges:

1. Menekülttáboráról hírhedtté vált község. 2. Paradicsom. 3. Így bíztatták Nagy Feróékat. 4. Ritka keresztnevet viselő férfi tolvaj. 5. Magyar Kommunista Párt. 6. Esetlen "e" dromedár. 7. A megfejtendő válasz befejező része, zárt betűk: P, G. 8. Birtokos kérdőnévmás, fordítva. 9. Néma por! 10. Tiltás Ernának. 11. Lap is van ilyen. 12. Műdalok. 13. Ottragad. 14. Bács-Kiskun megyei község. 15. Ittrium, jód. 16. Olaj Társ., angolul. 17. Kis disznó. 18. Pályaudvar. 23. ..., ki azzal. 28. Bevizelt. 29. Közúti Igazgatóság. 30. Pokrócot. 33. Község Esztergom közelében. 34. Üres zseb! 35. Páros nyár!. 37. Régi kacat. 39. Teniszcsillag (Mónika). 42. Héber betű kiejtve. 45. Kő is van ilyen. 47. Ragadozó madár. 49. Az egyik szülő. 52. Mutatónévmás. 53. Piócaszerű gyűrűsféreg. 54. 1000 x 1000. 56. Ott Magóg ellentéte. 59. Szótlan közepe. 62. Tenni. 63. A futball öröme. 65. Amerikai űrhajózási hivatal. 67. Filozófiai iskolájáról híres dél-itáliai város. 69. Római hetes. 73. Edény. 74. Véd. 76. Házikó. 77. Termelő Szövetkezet. 79. Férfinév. 81. gévé! 83. Fűszer fordítva.

A megfejtés beküldendő a Montana Marketing Kft. címére:

1361 Budapest, Pf. 501. Beküldési határidő: 1994. december 31.

A helyes megfejtők között ajándékcsomagokat sorsolunk ki, melyeket postán küldünk el.

A júniusi szám helyes megfejtése:

Villámgyorsan, nagy biztonsággal képes banki átutalásokat lebonyolítani.

A helyes megfejtők közül ajándékcsomagot nyertek:

Gellér Miklós, Győr-Szentiván, Keresztesi Bence, Budapest, Moharos László, Velence, Pusztai Endre, Kállósemjén, Sütő Gábor, Budapest.

Gratulálunk!