DECROS NEWS

ČERVEN 2000 ČÍSLO 2/2000

Úvodník

Na začátku mi dovolte, abych poděkoval Vám všem, kteří jste se na nás přišli podívat na výstavu CeBIT 2000 v Hannoveru či InfoSecurity 2000 v Londýně. Jistě se mnou budete souhlasit, že všechny firmy "finišují" ve velkém závodě o elektronický podpis a levnější čipovou kartu.

Z mého pohledu se však daleko zajímavější závod běží v České republice. Doslova před pár dny začal platit zákon o ochraně osobních údajů, dolní sněmovnou parlamentu prošel zákon o elektronickém podpisu, problém informatiky dostal na starosti nový ministr, Úřad pro státní informační systém má nového ředitele a navíc probíhá jednání o "Akčním plánu", který by měl využít všech těchto změn a popostrčit naši státní správu o řádný kus dopředu.

Je to opravdu strhující finiš, při kterém se leckterým divákům až tají dech. Jiní však svírají v dlaních své prsty a doufají, že neztratíme v posledních metrech dech. Příprava, realizace a ověření všech projektů, na jejichž konci bude pružná elektronická státní správa, vyžadují nejen velmi vysoké know-how, závratné finanční prostředky, ale i změnu uvažování a pohledu jak samotných pracovníků státní správy, tak i doslova celé společnosti.

Nejsem objektivním soudcem, abych odhadl, jak bude společnost akceptovat tento nový systém styku se státní správou. Na jedné straně je bezpochyby nutnost takový systém zavést, na straně druhé jde o zjednodušení práce pro počítačově gramotné občany, na další straně tohoto mnohoúhelníku je to právě naopak malá počítačová gramotnost u většiny obyvatelstva a v neposlední řadě pak velké riziko zneužití takového systému. Sami si jistě doplníte ještě řadu dalších stran, ale bez ohledu na skutečnost, zda tento mnohoúhelník má tři či tisíc stran, jsme již velmi blízko, i když nás ten největší kus práce teprve čeká.

Jiří Mifek
jiri.mifek@decros.cz

Bezpečné kryptografické nástroje pro třetí tisíciletí

Blíží se třetí tisíciletí. Nejsem přítelem zveličování věcí jen proto, že se píše rok 2000. Shodou okolností ale právě v této době dochází ke skutečně radikálním změnám v oblasti šifrování. Tyto změny nejsou tedy významné zrovna tím, že se dějí na konci tisíciletí, ale tím, že jejich význam je opravdu historický a zlomový z hlediska dějin kryptologie. Završují překotný vývoj v oblasti kryptografie a počítačové bezpečnosti vůbec, který započal v sedmdesátých letech. Je téměř jisté, že vyústí do stavu, kdy budeme mít k dispozici bezpečné kryptografické nástroje, posvěcené dokonce úředními místy. Máme na mysli nové americké standardy, které byly a jsou pro vývoj v této oblasti základní. Co bylo a je v dnes pro kryptologii určující?

DES - první standard

Pokusme se zamyslet nad historickými mezníky v kryptologii. Je nutné si uvědomit, že hlavní boom kryptologie nastal s větším využíváním počítačů a zejména s rozvojem počítačových sítí. To první přineslo nutnost šifrovacího standardu. USA poprvé v roce 1977 formálně přijaly veřejný standard pro ochranu dat (Data Encryption Standard, DES). Snahu o vznik DES lze datovat k počátku let sedmdesátých, proto o ní hovořím jako o prvním mezníku. Přestože DES nebyl určen pro ochranu utajovaných, ale "jen" citlivých vládních dat, stal se nejen americkým, ale i světovým šifrovacím komerčním standardem, který převažuje dodnes.

Asymetrická kryptografie

Druhým mezníkem byl objev kryptografie s veřejným klíčem (Diffie-Hellman, 1976), který byl motivován právě řešením klíčového hospodářství ve vznikajících počítačových sítích. Následoval vznik RSA (1978), který se stal dominujícím asymetrickým kryptosystémem pro následujících 20 let. Bylo to zejména díky tomu, že jde o systém s veřejným klíčem, který může být použit jak pro přenos resp. výměnu klíčů (key exchange), tak pro digitální podpis. Záhy poté začaly být společností RSA publikovány standardy a formáty dat využívající tuto asymetrickou šifru. S tím souvisí i vznik hašovacích funkcí Message Digest MD2,4 a 5, užitečných pro digitální podpisy a další kryptografické účely. Hašovací funkce byly tím dalším prvkem, který rozhýbal kryptografii. Nejpodstatnější bylo opět vyhlášení oficiálního standardu s názvem "Secure Hash Algorithm" americkým standardizačním úřadem v roce 1993 a jeho aktualizace na SHA-1 v roce 1995. Tento počin odsunul do pozadí funkce MD, u nichž byly také později nalezeny určité slabiny. Dnes jsou proto na ústupu. "Státem posvěcený standard" ovlivnil i přijetí standardu pro digitální podpis DSS (Digital Signature Standard), využívající algoritmus DSA (Digital Signature Algorithm). Razítko kvality od státu způsobilo, že společně s SHA-1 začal vytlačovat do té doby kralující komerční kombinaci MD a RSA. Pokud budeme pokračovat jen v linii asymetrických systémů, další zlom nastal v roce 2000, kdy americký standardizační úřad NIST uznal platnost - a tím i de facto "zrovnoprávnění" - algoritmů DSA, ECDSA a RSA pro digitální podpis (FIPS PUB 186-2). Jde o velké rozhodnutí, které má hned

Obsah

několik důsledků. Za prvé se zavádí a ihned zrovnoprávňuje technika eliptických křivek (ECC, Elliptic Curve Cryptography), konkrétně algoritmus DSA realizovaný na eliptických křivkách (to je ona zkratka ECDSA). Za druhé se s DSA a ECDSA zrovnoprávňuje digitální podpis pomocí RSA.

To je ústupek algoritmu RSA, na který se čekalo 20 let. Možná je tomu proto, že se za tu dobu ukázal dost silný, možná i proto, že 20.9. tohoto roku vyprší patent na RSA a státní správa tak nebude moci být nařčena, že podporuje komerční algoritmy. V každém případě tak NIST mimoděk zrovnoprávnil i sílu algoritmu RSA pro účely šifrování, neboli pro účely výměny klíčů. To je trochu něco jiného než jen digitální podpis. Nicméně i v této oblasti výměny klíčů pomocí kryptosystémů s veřejným klíčem je už zaveden Diffie-Hellmanův algoritmus (také s prošlým patentem) i vládní systém KEA (Key Exchange Algorithm) podporující symetrický algoritmus Skipjack) - takže, co se týká algoritmů pro výměnu klíčů, máme také už z čeho vybírat. Pro tyto účely zbývá už jen potvrdit i techniku eliptických křivek a v této oblasti bude na dlouhou dobu vystaráno. Vraťme se ale ještě zpět k tomu, čím jsme začali, tj. k symetrickým algoritmům.

Symetrické algoritmy

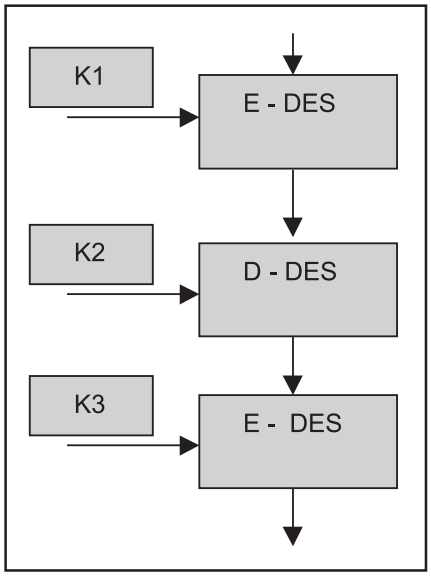
Od té doby, co začalo být jasné, že je DES již neudržitelný, začal NIST s veřejnou soutěží na nový symetrický standard. Jmenuje se Advanced Encryption Standard a příslušný algoritmus Advanced Encryption Algorithm (AEA). Jak už to bývá zvykem, nikdo mu ale AEA neříká a je to prostě algoritmus AES. Jeho vstupní podmínky byly vskutku grandiózní: 128-mibitová bloková šifra s povinně podporovanými klíči o délkách 128, 192 a 256 bitů. Taková bloková šifra nejenže nenechává nikoho na pochybách, že délka klíče je více než dostačující i v té nejmenší možné velikosti 128 bitů, ale zejména blok délky 128 bitů znemožňuje i různé další útoky (například tzv. "time-memory trade-off"). Navíc, v současné době všichni kandidáti (Rijndael, Serpent, Twofish, RC6, MARS), z nichž bude vybrán jeden nebo dva v létě tohoto roku za AES, mají velmi dobré kryptografické vlastnosti a vypadají opravdu skvěle. V každém případě letos budeme mít nový blokový algoritmus, který nahradí stařičký luštitelný DES. Tato náhrada nebude mít žádnou berličku. Je to volba, která - pokud nedojde k zásadnímu průlomu v oblasti kryptoanalýzy - může vydržet klidně i sto let nebo věčně. Prakticky totiž (pokud se nenajde analytická slabost) lidstvo není schopno útočit na AES hrubou silou. Připomeňme, že útok hrubou silou byl úspěšný na DES z úvodu krátkého 56 bitového klíče. Tato vrátka tam byla zabudována na žádost americké tajné služby NSA, která je zodpovědná za luštění. Dnes je to ale právě NSA, která pomáhá tvořit nové bezpečné standardy, neboť stála například u vzniku DSA a publikovala své dříve utajované algoritmy Skipjack a KEA. AES, který by měl být oficiálně přijat v příštím roce, tak završí soutěž mezi algoritmy, která se rozvíjela v posledních 20-ti letech. Není pochyb o tom, že se stane novým hitem a převládajícím světovým šifrovacím standardem. V této oblasti nebude co řešit.

Kandidáti na AES a výsledky neformálního hlasování účastníků poslední konference o AES o vítězi		
Algoritmus	Počet hlasů pro "měl by být vybrán jako AES"	Počet hlasů pro "neměl by být vybrán pro AES"
Rijndael	86	10
Serpent	59	7
Twofish	31	21
RC6	23	37
MARS	13	83

Tab.: Kandidáti na AES

Generátory náhodných čísel a hašovací funkce

Mezi další techniky, které jsou potřeba při návrhu bezpečnostně-kryptografických aplikací, patří bezesporu i generátory náhodných čísel (RNG). Zde se postupem času standardizovaly určité postupy (generátory náhodných čísel od společnosti RSA nebo rodina generátorů Yarrow a pod.), které umožňují konstruovat solidní softwarové generátory. V této oblasti je ale také k dispozici standard (FIPS-PUB 140-1) a jeho aktualizace se připravuje. Dále je zde tendence montovat čipy s kvalitními generátory přímo na základní desky osobních počítačů. Lze tedy předpokládat, že s náhodnými generátory, které potřebujeme k činnosti jak symetrických, tak asymetrických šifer, nebude v brzké době problém. U hašovacích funkcí se ještě zmiňme, že lze očekávat vznik SHA-2, která bude mít výstup 256 bitů pro kompatibilitu s AES. Současná SHA-1 má výstupní kód o délce 160 bitů. Jedná se víceméně o kosmetickou úpravu, ale pro komplexnost to bude jistě velmi užitečné. Pro pořádek je ještě vhodné se zmínit o alternativě k SHA-1, kterou je také poměrně často používaná hašovací funkce RIPEMD-160. Suma sumárum v hašovacích funkcích a RNG bude také vystaráno.



Obr.: TripleDES - dočasná renesance DES

Ještě pár zajímavostí

Nebude na škodu si uvést ještě pár historických a faktických poznámek. Zdálo se, že DES je mrtvý, protože pro všechny pochybovače byl nakonec konstruován DES-cracker, stroj, který garantuje vyluštění neznámého klíče k DES do 9-ti dnů. Není tomu ale tak. Pro zesílení DES byl kdysi navržen algoritmus TripleDES, který spočívá v trojím šifrování DES se dvěma nebo třemi různými klíči. Původních 56 bitů se tak rozrůstá na zcela postačujících 112 nebo 168 bitů. TripleDES je, až na pár relativně nevýznamných maličkostí, dobrou a bezpečnou šifrou, která se používá všude tam, kde nevadí její pomalost, ale je potřeba použít schválený a ověřený algoritmus.

Je také zajímavé, že trendem posledních 20-ti let bylo používat publikované algoritmy. Přesto jeden z nejpoužívanějších - RC4 - byl nepublikován až do doby, kdy ho disassembloval jeden hacker. Další zajímavostí je, že v roce 1997 byl publikován algoritmus CAST, který byl jako jediný publikovaný komerční algoritmus schválen nějakou vládou pro ochranu utajovaných dat ve státní správě. Jedná se o kanadskou vládu a informace stupně "designated", tedy v naší terminologii "vyhrazené". Snad ještě poslední zajímavost k šifře RC4. Ač se jedná o proudovou šifru, používá se zcela nestandardně bez inicializačního vektoru a klíč se generuje náhodně na každé použití. Jinými slovy, svět se neřídí podle schémat, ale podle něčeho úplně jiného. Například je dobrým bontonem říkat, že asymetrická kryptografie je vhodná na distribuci klíčů ve velkých systémech s mnoha uživateli. Přitom nejrozsáhlejšími systémy na světě se stamiliony uživatelů jsou právě systémy, které k distribuci symetrických klíčů nepoužívají

asymetrickou kryptografii! Je pravděpodobné, že jste účastníky několika takových systémů. Jsou to především mobilní telefony GSM a bankovní karty nebo tokeny nejrůznějších typů. Naproti tomu módní PKI (public key infrastructure) je ještě z uživatelského hlediska v plenkách. Tím neříkám, že to není velmi užitečný a perspektivní nástroj, ale spíše, že si na něj budeme muset ještě chvíli počkat. Souvisí to i s legislativním rámcem pro systémy s veřejným klíčem a digitálními podpisy. Na úrovni Evropské Unie je přijata sjednocující direktiva pro národní zákony tohoto typu. Ač se o tom mluví, zákon o elektronickém podpisu v naší republice ještě není přijat. Až bude přijat , bude to velký pokrok, ale je jisté, že státní správa i soukromý sektor budou muset projít značnými porodními bolestmi při jeho zavádění. Pokud ale vláda neposkytne k jeho provádění jinou podporu, může to dopadnout jako s ustavením našeho Národního bezpečnostního úřadu. Zákonem byl sice zřízen a byly mu naloženy úkoly, ale bez výrazné materiální podpory, aby je mohl plnit. A to nemám na mysli jen medializované bezpečnostní prověrky, nýbrž úkoly technicko-odborného rázu.

luštící stroj na DES, velká událost roku 1998

"Politické" události

O "politických" událostech bych se nezmiňoval, kdyby jejich význam nebyl tak velký. Připomenu první z nich, kterou bylo sestrojení DES-crackeru v roce 1998.

Jeho jednoduchost, schopnosti, dostupnost a cena dávají nejen za pravdu Martinu Hellmanovi a všem, kdo už při vzniku DES poukazovali na možnost útoku hrubou silou na DES, ale dávají nám do rukou nástroje a data pro výpočet bezpečných délek klíčů.

Z důvodu této slabosti DES vznikala v osmdesátých a devadesátých letech řada algoritmů, které se snažily vytvářet náhradní standardy místo DES. Mezi vážné kandidáty se dostaly algoritmy IDEA, Blowfish a jiné. Vznikly i neamerické národní standardy. V roce 1989 tak vznikla ruská obdoba DES - algoritmus GOST, kanadský CAST a řada dalších komerčních algoritmů (například japonský FEAL, který byl totálně rozbit). V této době také vznikl český algoritmus WinCros a dokonce i první český šifrovací čip (SIC 5000). Tato soutěž, jak jsem již uvedl, prakticky končí vydáním AES.

Nejdůležitější politickou událostí je bezesporu uvolnění amerických vývozních restrikcí na silnou kryptografii. Jak jistě víte, ještě donedávna se v Evropě používal jiný software než v USA (například od Microsoftu, Lotusu, Novellu aj.). Americké firmy musely vyrábět dvojí software díky tomu, že do ostatního světa nemohly vyvážet silné kryptografické nástroje. A tak se ve světě vesele šifrovalo americkým exportním softwarem se 40bitovými klíči. Tlak průmyslu a rozvoj mobilních počítačů, telefonů a počítačových sítí vůbec, přiměl americkou vládu, aby změnila studenoválečnické zákony na normální. A tak se v posledním roce tisíciletí situace stává po 50-ti letech přijatelnější. Restrikce nejsou ještě zcela uvolněny ve všech oblastech, například pro export pro vládní použití stále platí různé obstrukce a omezení, ale oproti minulosti se jedná již o "detaily".

Trocha věšteb na závěr

Pokud se zamyslíme nad vývojem kryptologie v posledních 30-ti letech, jeho vyvrcholení je opravdu pozitivní. Velmi brzo budeme mít k dispozici algoritmy, které budou státně posvěcené - půjde tedy o oficiální standardy, které budou bezpečné a budou pokrývat drtivou většinu potřeb pro tvorbu bezpečných aplikací. Jinými slovy, vývojářské firmy čekají šťastné časy, kdy se nebudou muset starat o to, co je bezpečnější, ale o to, co je pro uživatele potřebnější a jak to udělat pro něho co nejpříjemnější. Doba, kdy soutěžily mezi sebou algoritmy, pomalu odchází. A to je dobře.

Vlastimil Klíma
vlastimil.klima@decros.cz

Poznámka

O mnoha věcech jsme na malém prostoru nemohli psát podrobněji. Těm z Vás, kteří se zastavili nad nějakým pojmem nebo zkratkou, mohu doporučit archiv publikací na http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm. Pokud si otevřete "komentovaný seznamu publikací", můžete v něm podle názvů nebo hledáním klíčových slov nalézt to, co Vás zajímá. Příslušné články si je možné přečíst on-line nebo si je stáhnout v elektronické formě pro svoji potřebu.

CeBIT 2000

Největší světový veletrh informačních technologií CeBIT proběhl v letošním roce už koncem února; tedy o měsíc dříve, než bývá zvykem. Důvodem je ten fakt, že německý Hannover v tomto roce hostí světovou výstavu EXPO. Přípravy na tuto mimořádnou událost byly patrné na každém kroku. Venkovní reklama, výstavba nových hal, lanovky a zejména parkovišť na výstavišti svědčily o velkoleposti připravované show. Bohužel se také odrazily v organizaci veletrhu CeBIT.

Hned první dva dny došlo k něčemu, co je možné s klidem nazvat dopravní kolaps. Ti, kteří to pocítili na vlastní kůži, jistě vědí, o čem mluvíme. Doslova hodiny strávené v dopravní zácpě, která se posouvá "šnečím tempem" k dalšímu parkovišti, které je opět označené nápisem "Obsazeno", jistě nejsou nic příjemného a k celkové pohodě, tolik důležité pro hladký průběh výstavy, nepřispějí. Abychom nebyli nespravedliví, toto byla jedna z mála věcí, kterou bylo možné jinak zcela perfektní organizaci vytknout. Kdypak se takové profesionality služeb asi dočkáme u nás v Čechách.

Ale zpět k výstavě samotné. Malá statistika pro začátek: počet hal se rovná číslu 26, návštěvníků letos přišlo na 700 000. Na Cebitu2000 vystavovalo celkem 7 802 vystavovatelů, z toho bylo 13 firem českých. DECROS vystavoval opět v hale 23, která je zaměřena na bezpečnost a Smart Cards. Hlavní hitem letošního CeBITu byly bezesporu Windows 2000 a vše s nimi spojené. Společnost DECROS nemohla samozřejmě zůstat pozadu… Kromě prodejních verzí Protectu pro Windows TM se na naší expozici objevily i horké novinky. Vedle Beta verze Protectu pro Windows s novým modulem digitálního podpisu, která je k dispozici i pro aktuální verzi Windows2000, to byl také DECROS Crypto Service Provider pro Microsoft Crypto API. Novou zajímavou vlastností je také WCD - šifrovaný archiv a technologie šifrování on-line X off-line.

Možná se i někteří z Vás zúčastnili opravdové české párty s pravým českým Budvarem. Návštěvnost byla skutečně velká. Kromě našich partnerů a zákazníků se zde objevila i konkurence! Vzhledem k pozitivním ohlasům jsme se museli zavázat, že akci na příštím CeBITu zopakujeme. A tak si i Vás dovolujeme pozvat na příští CeBIT na prezentaci nových produktů i dobré pivo.

Denisa Mylbachrová
denisa.mylbachrova@decros.cz

Úsvit technologie čipových karet

Již delší dobu se hovoří o čipových kartách jako o novém standardu. Komu by se to nelíbilo - elegantní řešení pro bankovní styk, osobní identifikaci a řada dalších informací uložených bezpečně v kartě velikosti vizitky uložené v peněžence.

Pokud bych měl poukázat na hit letošní CeBITové show, tak bezpochyby budu volit čipové karty. Desítky firem s nabídkou potisku či vlastní tiskárny, aplikací a nadstaveb pro čipové karty se snažily každého návštěvníka přesvědčit, že už je to tu - doba čipové karty. Je tomu opravdu tak? Podívejme se na několik zajímavých zpráv z této oblasti a odpovězme si sami.

MasterCard a čipové karty [1]

MasterCard International uvedl na trh MasterCard M/Chip Select pro MULTOS™ verze 2. Nová verze byla navržena tak, aby splnila všechny potřeby, které významné světové finanční instituce požadovaly. První M/Chip aplikace, které umožňovaly vydávat karty jako jsou MasterCard, Maestro a Cirrus postavené na čipové kartě, byly představeny v roce 1998 a nabízely kreditní/debetní služby postavené na EMV standardu ([2],[3]). V té době ohlásilo 25 členů MasterCard implementaci těchto karet na čipové kartě v U.S., Japonsku, Jižní Africe, UK, Korei, Brazílii, Argentině, Mexiku a Libanonu. MasterCard spolupracoval se svou odběratelskou základnou, aby následně vytvořil M/Chip dostupný v řadě provedení. Ku příkladu si zákazníci mohou koupit předkompilované aplikace od MC nebo si je mohou sami naprogramovat v případě, že dodrží specifikace a doporučení MC. MasterCard nabídl provedení M/Chip pro platformu MULTOS a současně pro na platformě nezávislé verze k jednoduchým aplikačním kartám jako je například M/Chip Lite.

Nová verze nyní nabízí rozsáhlou kontrolu nad uskutečněnými transakcemi. Ty mohou být sledovány pomocí vestavěného počítače, který zajistí sledování uskutečněných transakcí i v Off-line režimu. Díky této vlastnosti může programátor karty například nadefinovat hodnotu, po kolika transakcích musí být připojena on-line. Taktéž byla implementována lepší kontrola při možném zneužití karty. Vydavatel karty může v případě podezření na její zneužití prakticky v momentě vyslat zprávu do všech hostujících systémů pro její zablokování. Je vestavěna lepší kontrola nad oblastmi obchodu, kde může být karta využívána - vydavatel karty může definovat oblasti možného použití karty, např. pro jaký typ transakcí je její použití povoleno.

Je rozšířena bezpečnost pro e-platby - M/Chip je plně kompatibilní s novou Chip Electronic Commerce (CEC) specifikací vyvinutou EMVC organizací, která zajišťuje a zastřešuje standardy pro čipové karty a která byla založena roku 1999 společnostmi Europay International, MasterCard International a Visa International. CEC specifikace popisuje, jakým způsobem může být EMV čipová karta použita pro bezpečné platby přes Internet, čím rozšiřuje EMV standard o rychle se rozvíjející virtuální svět.

Microsoft a čipové karty

Internetový časopis Nando Media [4] uveřejnil prohlášení Billa Gatese, novodobého vizionáře, coby jeho postoj k používaní technologií čipových karet.

LAS VEGAS (Květen 9, 2000 17:49) - Bill Gates (ředitel Microsoft Corp.) pobídl ostatní firmy, aby co nejdříve přijaly technologii autentizace čipovou kartou místo používání hesel. "Nejslabší stránkou bezpečnosti používání hesel je právě jejich používání", řekl vizionář Gates na konferenci Interop 2000. Zákazníci, kteří chtějí nakupovat zboží po internetu nebo platit účty "online", obvykle využívají heslo pro registraci do těchto sítí. Tento systém však není bezpečný, protože právě tyto společnosti heslo obvykle prozradí v případě, že se po telefonu někdo jiný vydává za zákazníka, který právě toto heslo zapomněl. Minulý rok zaznamenala FTC (Federal Trade Commission) na 18 tisíc stížností na zneužití platební karty při platbách na aukcích nebo při nákupu software a hardware. SEC (Securities and Exchange Commission) dostává okolo 200 až 300 stížností denně, což je pravděpodobně současný denní stav zneužití platebních karet na Internetu.

Gates dále řekl, že Internet se potřebuje oprostit od používání hesel a přejít k používání bezpečných čipových karet, kde jsou data chráněna na vestavěném čipu a je taktéž možné vysledovat, jak a kde byla případně použita. Současně může taková karta sloužit k uložení osobních dat, případně souborů. V případě osobního počítače může být čipová karta vložena do malého snímače (čtečka čipové karty) a poté jakákoli Internetová síť dokáže identifikovat uživatelovu identitu (pozn.: nejprve je samozřejmě třeba něco takového nastavit).

Čipové karty (pozn.: technologie původem z Francie) jsou používány v Evropě, části Asie a Latinské Ameriky, ale ve Spojených státech se dosud ve větší míře neuchytily. Zde jsou lidé zvyklí používat k placení více kreditní nebo bankovní karty. Společnosti jako je právě Microsoft aktivně pracují na vývoji multifunkčních čipových karet. Vizionář v závěru svého proslovu vyzval průmysl na spolupráci a nasazení čipových karet, aby zajistil nejen na Internetu tak potřebnou bezpečnost. Také naše firma sleduje veškeré aktivity, které se kolem čipových karet odehrávají a přichází se svojí "rodinkou karet DECROS PKI" viz. článek na jiném místě tohoto čísla DN.

"Windows for Smart Card" nebo "Smart Card for Windows" [7]

Hovoří-li vizionář o přínosné aktivitě své firmy na vývoji multifunkčních čipových karet, myslí tím, že také firma Microsoft vycítila prostor a díky svému monopolu na trhu operačních systémů vytvořila návrh specifikace čipové karty s vnitřním operačním systémem Microsoftu, který "padne na míru" tomuto operačnímu systému. Tento OS (na řadě míst označovaný jako SCW) je nezávislý na hardware čipu čipové karty na rozdíl od ostatních výrobců, kteří vytvářeli OS karty jako svůj firemní standard. Microsoft navíc umožňuje v tomto SCW nejen vytvářet soubory a adresáře a ty chránit pomocí PINu, ale i nahrávat a spouštět aplikace. Celý systém pro programování této karty se pak instaluje k Microsoft Developer Studiu, jazyk použitý pro programování SCW je překvapivě Visual Basic a souborový systém FAT.

Škodolibý uživatel v tuto chvíli poznamená, zda bude ve chvíli uvedení také dostupná utilita pro defragmentaci FAT systému této karty. Naopak bystrý uživatel jistě vzápětí poznamená, že tato poznámka je nesmysl. Věděli byste proč?

Napište mi e-mail a jednoho z Vás, který napíše správnou odpověď, a druhého, který napíše nejzajímavější sci-fi, odměním. (Do subjektu e-mailu napište Windows for Smart Card story.)

Radoslav Půr
radoslav.pur@decros.cz

Zdroje použité pro tento článek:

[1] MasterCard SmartCard:
http://www.mastercard.com/ourcards/smartcard/ aragorn
[2] Errata for EMV '96: ICC Specifications for Payment Systems:
http://www.mastercard.com/emv/emvspecs03.html
[3] EMV '96 Specifications (Version 3.1.1):
http://www.visa.com/nt/chip/download.html
[4] http://www.nandotimes.com/noframes/business/story/0,2469,500202240-500279774-501491622-0,00.html
[5] E-Konference: C I P H E R T E X T - Cryptography, Security & Privacy
[6] E-Konference: CRYPTO-GRAM by Bruce Schneier - a free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography
[7] Windows for Smart Card
http://www.microsoft.com/WINDOWS2000/library/howitworks/security/smart.asp

Nová rodina na obzoru - čipové karty DECROS Card

Kousek plastu ve velikosti vizitky jistě nadchnul každého nového majitele, ať se jednalo o kartu opravňující ho ke vstupu do určitého objektu, platební kartu s přístupem k vlastním úsporám či kartu s magnetickým proužkem umožňující vjezd na firemní parkoviště. Ale za poslední roky se tyto plastové kousky nějak rozmnožily. Jednoduše řečeno, kartičky se nám hromadí všem v peněženkách (navzdory obecnému povědomí, že to není zrovna nejbezpečnější místo), jako by se nám tam sami rozmnožovaly.

Asi to nikdy nebude tak jednoduché, abychom měli pouze jeden kousek plastu, který bychom používali celý svůj život. Bylo by to hezké, to ano, a to nejen proto, že bychom konečně dokázali peněženku zavřít a zapnout. V předcházejícím článku se můžeme dočíst o čipových kartách, které by mohli nahradit ledacos a přitom shromáždit a sdružit na sobě a v sobě řadu informací, které obsahují jiné plastové karty dnešní doby.

Skutečnost, že platební kartou v podobě Smart Card (jak je ten kousek plastu s programovatelným čipem nazýván odbornou veřejností) budeme moci bezpečněji obchodovat přes Internet a že se více eliminuje nebezpečí zneužití našich finančních prostředků, bezpochyby nadchne spousty lidí. Ale o přednostech Smart Card se nehovoří pouze ve finanční sféře, ale také ve sféře informačních technologií, které především se budeme dále věnovat.

Předmět pro přihlášení?

V roce 1996 uvedla společnost DECROS identifikační a autentizační modul nazvaný dGINA, kterým podle údajů společnosti Microsoft získala prvenství při náhradě standardního modulu GINA v operačním systému Windows NT. Hlavní význam modulu dGINA tkvěl v možnosti přihlásit se do systému a sítí fyzickým předmětem, Touch Memory 1990A. V současné verzi modulu dGINA se přímo ve fyzickém bezpečnostním předmětu uchovává přihlašovací informace uživatele (jméno, heslo a popřípadě doménu). Myšlenka se ukázala jako správná, a tak se tato filozofie rozšířila i na další předměty jako například Touch Memory či Security Box a také na další Windows systémy, jako Windows 95, Windows 98 a v poslední řadě i Windows 2000.

Výhody, které s sebou nese použití fyzického předmětu, vyplývají především ze skutečnosti, že si uživatel (neboli vlastník předmětu) nemusí pamatovat heslo do operačního systému.

To znamená, že heslo uživatele:

- se nedá odkoukat případným útočníkem z klávesnice
- může být dostatečně dlouhé a nezapamatovatelné (tedy bezpečné)
- nemůže ani sám uživatel sdělit nikomu jinému, ať k dobrým či nekalým účelům, bez toho, aniž by jej učinil vlastníkem předmětu
- se nemusí tak často měnit, protože riziko jeho vyzrazení není veliké
- může použít pouze vlastník předmětu (heslo uživatele totiž nemusí znát ani správce systému či sítě, pokud zadávání hesel pověří organizace jinou důvěryhodnou osobu).

Přitom všem získává přístup k předmětu pouze jeho vlastník (uživatel), který jediný má právo znát přístupové heslo k předmětu (u platebních karet nazvané PIN). Protože si uživatel svůj předmět nosí s sebou, například na svazku klíčů, nemusí mít přístupové heslo k předmětu tak složitou hodnotu jako heslo do systému.

Smart Card a Protect

Aplikační nadstavba Protect, jejíž součástí je identifikační a autentizační modul, nabízela pro nekomerční použití od roku 1998

podporu i první Smart Card podporované společností DECROS, zvané BrainCard.

BrainCard umožňuje uchování nejenom jména, hesla a domény uživatele, ale dále pro aplikaci Protect nabízí možnost uchování až 9-ti šifrovacích klíčů. Samozřejmostí je, že i tento kousek plastu dokáže Protect využít pro všechny systémy Windows.

Čipová realita a společnost DECROS

Komerční použití čipových karet ale společnost DECROS vázala na kvalitní zázemí Smart Card v podobě kvalitních čteček, standardů a vývojových nástrojů.

Ke komerčnímu uvedení přispěl jak standard PC/SC, který je dnes plně podporován SAPI (rozhraní Security API společnosti DECROS), ale také zkušenosti s desítkami výrobců čteček.

Tak světlo světa spatřila nová rodinka Smart Card, nazvaná DECROS Card, která od března 2000 nabízí své služby. Do této rodinky patří DECROS Card MEMORY, DECROS Card PKI a DECROS Card DUAL.

DECROS Card MEMORY je základním modelem kontaktní čipové karty. Jedná se o plnohodnotného nástupce čipové karty BrainCard, který nabízí bezpečné uchování jména, hesla a domény uživatele a dále pak až 9-ti šifrovacích klíčů. Tento model je využíván pro standardní použití v organizaci i pro svou nízkou cenu.

Naproti tomu je kontaktní čipová karta DECROS Card PKI poznamenána nejnovějšími technologiemi, které se v oblasti Smart Card vyskytují. Ucelená řada bezpečnostních funkcí tohoto výjimečného kousku plastu nabízí od bezpečného uchování přihlašovacích informací uživatele (jako u DECROS Card MEMORY) a až 31-ti šifrovacích klíčů pro aplikaci Protect, ucho-

I LOVE YOU

Letošní jaro má hořkou příchuť emailových virů. První předzvěstí byla loňská MELISSA, následovaná letošním veleúspěšným ILOVEYOU a jejich následovníky.

Co je příčinou vzniku a úspěchu těchto virů a jak se jim bránit, je obsahem právě tohoto článku. Nejprve se podíváme na společné charakteristiky těchto virů a příčiny jejich úspěchu.

Emailoví červi

Základními společnými rysy obou virů je šíření prostřednictvím elektronické pošty, přístup k emailovým adresářům uživatele a využití nepozornosti uživatele pro jejich aktivaci.

Tyto rysy nejsou v dějinách počítačových sítí ničím ojedinělým. Již v prosinci 1987 se objevil emailový červ CHRISTMAS TREE [1][2], který dokázal ochromit mainframy IBM v síti BITNET a v interní síti IBM VNET.

Pro hromadné rozšíření emailových červů je potřebné zajistit homogenní prostředí, ve kterém pracuje velké množství uživatelů. Čím více uživatelů, tím větší škody může nadělat.

V roce 1987 byl tímto prostředím svět mainframů IBM v síti BITNET. CHRISTMAS TREE, napsaný ve skriptovacím jazyce REXX, se posílal jako příloha vánočního blahopřání a na terminál uživatele nakreslil vánoční stromeček. Mezi tím prošel standardními soubory, ve kterých měl uživatel uloženy emailové adresy a na všechny se rozeslal. Během jednoho dne, stejně jako o 13 let později ILOVEYOU, se dokázal rozšířit po celé síti BITNET a dostal se i do interní sítě IBM VNET. Svým nekontrolovaným šířením přetížil poštovní systémy tak, že bylo nutné jednotlivé počítače izolovat od sítě.

V roce 1999 je tímto prostředím svět osobních počítačů s operačním systémem Microsoft Windows 95/98/NT. Prakticky všichni uživatelé používají stejný operační systém, který se konečně dočkal plnohodnotného skriptovacího jazyka. Navíc téměř všichni používají stejný kancelářský balík programů. Tato situace si přímo říká o zneužití. První velkou pohromou byla MELISSA [3]. Virus vytvořený jako makro ve Visual Basicu, uložený v dokumentu Word97. Maskovala se jako důležitá zpráva a vybízela uživatele k otevření připojeného souboru. Při jeho otevření musel uživatel souhlasit s provedením makra (pokud již neměl tuto volbu vypnutou). Uživatelé většinou souhlasili. MELISSA infikovala šablonu NORMAL.DAT a rozeslala se na 50 emailových adres z každé složky v kontaktech Outlooku. Při splnění určitých podmínek přidávala do právě zpracovávaných dokumentů text. Existuje řada modifikací, které tyto vlastnosti modifikují.

Jednoznačným hitem letošního jara se stal emailový červ ILOVEYOU [4], který byl vytvořen jako skript ve Visual Basicu pro Windows Scripting Host. Skript se maskoval jako milostný dopis a vybízel uživatele, aby si přečetl přiložený textový soubor. Při jeho otevření musel uživatel souhlasit se spuštěním programu, což zhusta učinil. ILOVEYOU se rozeslal na všechny emailové adresy, které nalezl v kontaktech Outlooku, a uložil se do systémových adresářů Windows. Provedl i další operace: při dalším spuštění Internet Exploreru se stáhnul a spustil trojský kůň, který odchytával hesla, která odesílal na emailovou adresu mailme@super.net.ph. Dále se pokusil šířit pomocí programu mIRC a poškodit nebo přejmenovat soubory s příponami .vbs .vbe .js .jse .css .wsh .sct .hta .jpg .jpeg .mp2 .mp3.

Od vypuštění ILOVEYOU uběhla velmi krátká doba a za ní se objevilo velké množství jeho mutací, což bylo zapříčiněno jeho extrémní jednoduchostí - pro vytvoření podobného viru vám stačí NOTEPAD. Objevily se i nové mutace MELISSY a také se vrátila řada starých známých, jako jsou například HAPPY, PRETTYPARK a spousta dalších [5], o kterých jsem se nezmiňoval, ale jejichž princip šíření je stejný.

Jak se bránit

Jaké závěry lze z těchto událostí odvodit? Tvorba emailových červů je stále snazší, vznikají stále dokonalejší techniky maskování a rychlost jejich šíření je ohromná - vznik pandemie se počítá na hodiny. Také chování uživatelů je stále stejné - i když přijde na první pohled podezřelý email (kdo uvěří, že Vás miluje Váš zákazník), uživatelé i přes varování emailového programu přiložený virus spustí.

Vzhledem k rychlosti a masivnosti šíření emailových červů je prvním obranným mechanizmem v řadě školení uživatelů o používání elektronické pošty. Uživatelé musí vědět, že podezřele vypadající emaily s přílohou, které obdrží i od svých partnerů (často v angličtině, ačkoliv partner je Čech jako poleno) musí vhodným způsobem prověřit. Dalším poznávacím znamením je vícenásobný výskyt téže zprávy, který přišel z různých míst.

Protože maskovací schopnosti emailových červů rostou a uživatelé nejsou neomylní a zapomínají, je nutné se schránit aktivně. Nejvhodnějším způsobem je použít antivirovou ochranu, která Vás zabezpečí proti všem již známým emailovým červům a i proti řadě jejich nově vzniklým mutacím.

Protože všechny emailové programy musí před spuštěním viru přiloženého k emailu uložit soubor s virem na disk, může být jako antivirová ochrana použit jakýkoliv antivirový program běžící na stanicích s online kontrolou ukládaných souborů. Aby byla zajištěna pravidelná aktualizace, musí antivirový program podporovat centrální distribuci virových vzorů.

Velmi užitečný doplněk je centrální antivirová ochrana prováděná na úrovni emailového serveru. Antivirové programy jsou dnes k dispozici pro většinu emailových systémů.

CAI InoculateIT

Pro sítě založené na Novell NetWare a Microsoft Windows NT dodává DECROS řešení založené na antivirovém programu CAI InoculateIT [6].

CAI InoculateIT je distribuovaná antivirová ochrana počítačové sítě obsahující online antivirovou ochranu serverů Novell NetWare a Microsoft Windows NT/2000, stanic Macintosh, Microsoft DOS a Windows 3.x/95/98/NT/2000, centrální správu, automatickou distribuci virových vzorů a propracovaný systém alarmů [7].

InoculateIT obdržel certifikát ICSA [8] potvrzující kvalitu a úspěšnost detekce a odstranění virů v offline i online režimu. InoculateIT používá heuristické metody analýzy virových vzorů, které mu umožňují detekovat dosud neznámé viry - týká se zejména makrovirů. InoculateIT automaticky rozpozná a zkontroluje i běžné typy archivů jako jsou .zip, .arj a .cab.

V počítačové síti umožňuje InoculateIT izolovat uživatele pracujícího se zavirovanými soubory od sítě a tím výrazně omezit možnosti šíření viru.

Centrální správa umožňuje konfigurovat InoculateIT na všech serverech a stanicích v síti. Servery i stanice mohou být zařazeny do skupin, které mohou být spravovány jako celek. Centrální správa umožňuje spustit antivirovou kontrolu na dálku.

Při automatické aktualizaci virových vzorů si hlavní server stáhne novou databázi virových vzorů z Internetu. Podle nastavení v centrální správě se potom aktualizovaná virová databáze distribuuje na ostatní servery a stanice.

Při objevení viru umožňuje InoculateIT provést řadu operací: upozornění, zakázaný přístup, vyléčení, smazání, přesun zavirovaného souboru do vyhrazeného adresáře. Každý výskyt viru je zaznamenán v centrální databázi a správce může být upozorněn pomocí výzvy, pageru nebo elektronické pošty. Informace o výskytu viru může být vytištěna na síťové tiskárně. Pomocí SNMP události může být informace o výskytu viru předána do systému pro správu sítě.

InoculateIT je možné integrovat do emailových serverů Microsoft Exchange a Lotus Notes. Veškeré příchozí emaily a připojené soubory jsou kontrolovány na přítomnost virů. Možnosti detekce a akcí při výskytu viru jsou shodné s kontrolou souborů.

InoculateIT je možné integrovat s CAI ARCserve, který provede antivirovou kontrolu všech souborů při zálohování souborů na pásku i při obnovování souborů z pásky.

Dále lze začlenit InoculateIT do systému správy sítě TNG Unicenter. Centrální správu InoculateIT je potom možné provádět z přímo prostředí TNG Unicenter.

Antivirus pro sendmail

Udává se, že více než 50 % všech emailů na Internetu je doručeno pomocí email serveru sendmail na Unixu. Unix se sendmailem také bývá velmi často součástí firewallu mezi interní sítí a Internetem.

Společnost DECROS proto vyvinula rozšíření sendmailu [9], které umožňuje zkontrolovat každý procházející email. Celé řešení je zaměřeno na efektivitu. Každý email, který je přijat, je nezávisle na počtu příjemců zkontrolován pouze jednou. Pokud je email zařazen do fronty pro pozdější doručení, kontrola se již neprovádí. Pokud je antivirus nefunkční, jsou přijaté emaily zařazeny do fronty a po zprovoznění antiviru je provedena dodatečná kontrola a emaily jsou doručeny.

Primárně je použit antivirus AvpDaemon firmy KasperskyLab [10] pracující na platformě i386 pod operačními systémy Linux, FreeBSD a BSDI. Lze však použít i jiné antivirové programy pracující na ostatních platformách podporovaných sendmailem.

V rámci produktu Firewall FreeBSD [11] poskytuje firma DECROS svým zákazníkům toto řešení, včetně automatické denní aktualizace virových vzorů, jako i komerční technickou podporu.

Petr Řehoř
petr.rehor@decros.cz

Odkazy

[1] WAN Security & Viruses
http://www.ja.net/CERT/Barron/
WAN_Security_and_Viruses.html
[2] The Risks Digest 1987
http://www.eu.veg.org/Risks/index.5.html
[3] Viruslist: MELISA
http://www.viruslist.com/eng/viruslist.asp?id=3773
&key=00001000060000900078
[4] Viruslist: ILOVEYOU
http://www.viruslist.com/eng/viruslist.asp?id=4010
&key=00001000130000100015
[5] Viruslist: Internet E-Mail Worms
http://www.viruslist.com/eng/viruslist.asp?id=3111
&key=000010001300001&f_page=0
[6] CAI InoculateIT
http://www.cai.com/products/inoculateit.htm
[7] CAI InoculateIT: Vlastnosti
http://www.cai.com/products/fdb/inoculateit.htm
[8] ICSA: Certified Antivirus Products
http://www.icsa.net/html/communities/antivirus/
certification/certified_products/certprod.shtml
[9] Antivirus pro sendmail
http://www.decros.cz/~reho/ check_virus
[10] Kaspersky Lab: AvpDaemon pro Unix
http://www.avp.ru/eng/products
[11] DECROS: Firewall FreeBSD
http://www.decros.cz/net/firewall.htm

...pokračování ze strany 5.

vání i certifikátů a dalších informací pro jiné aplikace. Velikost 8kB vnitřní paměti dnes nabízí využití v oblastech, o kterých se nám do nedávna mohlo pouze snít.

Čipová karta DECROS Card DUAL obsahuje dvě části, dotykovou a bezdotykovou. Dotyková (neboli kontaktní) část je plně identická s DECROS Card PKI. Bezdotyková část (nazývaná také bezkontaktní) je zatavena v plastovém pouzdře a umožňuje plné využití pro další potřeby uživatele prostřednictvím standardního protokolu MIFARE. Využití nachází bezkontaktní čipové karty v oblastech identifikačních systémů:

- v docházkových systémech
- přístupových systémech
- systémech fyzické bezpečnosti
- různých garážových a parkovacích systémech
- stravenkových systémech
- a v řadě dalších.

Příjemná skutečnost pro DECROS Card DUAL je cena, která je překvapivě téměř shodná s cenou DECROS Card PKI.

Čipová realita v budoucnosti?

Již v dnešní době jsou klienti, kteří používají produkty firmy DECROS společně se Smart Card a samozřejmě se nabízí i efektivní využití těchto předmětů dále (jako například u DECROS Card DUAL). Lze samozřejmě očekávat další posuny v této oblasti tak, jak to již naznačil předcházející článek (na straně 4), v podobě multiplatformních karet apod. To, zda lidé ustoupí od hromady plastových kartiček k jedné Smart Card ukáže až budoucnost. Vybavuje se mi obrázek z jedné parodie agenta 007. Agent 007 si při platbě v hotelu vyjme z kapsy u bundy velký svazek plastových karet, od platebních až po karty do nejrůznějších klubů, a když tu "harmoniku" pustí, tak se konec karet dotýká země. A on chudák začne mezi těmi plasty hledat tu správnou, kterou by použil. Věřím, že by i on rád používal pouze jednu.

A nebo ne?

Josef Dvořák
josef.dvorak@decros.cz

Kompatibilita filtrovacích driverů

2. část

Obecně rozšířeným názorem je, že mít na počítači nainstalovaný antivirový program je vcelku dobrá věc. Pokud tento antivir navíc vyhledává viry při přístupu k jednotlivým souborům, nemusíme se ve většině případů virů obávat. Co se ale stane, když si nainstalujeme antiviry dva?

Vyhledávání virů při přístupu je realizováno na Windows NT pomocí filtrovacích driveru. Problémy, které mohou nastat, závisí nejen na zručnosti a znalostech jednotlivých programátorů, ale i na způsobu, jakým je implementována funkčnost příslušného software. Různým způsobům implementace funkčnosti a možným konfliktům byla věnována předchozí část článku. Tato část článku je věnována vlastnímu řešení těchto konfliktů.

Řešení konfliktů

Je smutnou skutečností, že i když se autoři antivirů musí zabývat problémem kompatibility jednotlivých částí svých systémů, řeší tento problém takovým způsobem, že tato řešení nemohou využít další filtrovací drivery. Zároveň on-line detekce virů představuje nejčastěji se vyskytující filtrovací driver, což má za následek nepsané pravidlo, že každý další filtrovací driver musí být kompatibilní s antiviry (a dalšími nejrozšířenějšími programy). Toto pravidlo se ale nezmiňuje o konkrétních antivirech, a tak je instalace jakéhokoliv systému obsahujícího filtrovací driver vždy malým dobrodružstvím. Míra rizika je pak nepřímo úměrná rozšířenosti příslušného systému. Zároveň se pravidlo vzájemné kompatibility filtrovacích driverů nevztahuje na antiviry, a tak je instalace dvou různých antivirů na počítač nepřiměřeným pokoušením štěstí.

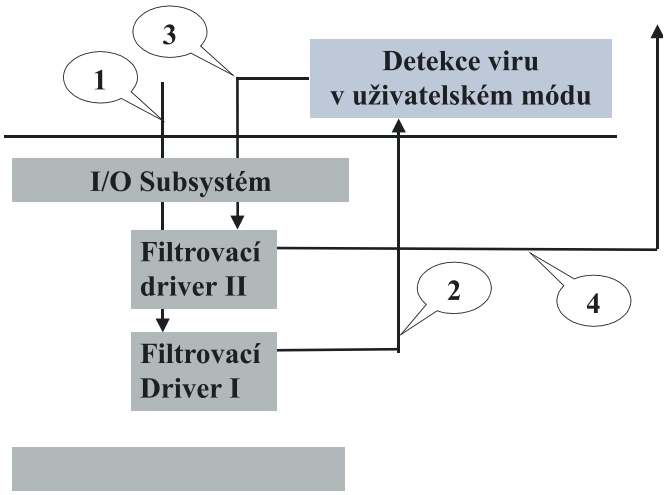
To, jaká část funkčnosti zůstane po instalaci dvou různých filtrovacích driverů zachována, závisí z velké části na způsobu, jakým jsou ve filtrovacích driverech řešeny očekávané konflikty. V současnosti existuje několik používaných metod, jak problémy kompatibility řešit.

Přímé volání souborového driveru

Ke konfliktu dvou filtrovacích driverů dojde, pokud driver, který je v řetězci jako první (Filtrovací Driver II), serializuje požadavky na otevření souboru a driver, který je zařazený jako druhý (Filtrovací Driver I), soubor rekurzivně otevře (viz obrázek). Je zřejmé, že pokud nebude Filtrovací Driver II volán, nedojde ani ke konfliktu. Vstupní body pro vlastní souborový systém jsou známy, a tak v podstatě nic nebrání programátorovi filtrovacího driveru implementovat tímto způsobem nekonfliktní chování. Drobnou nepříjemností je, že pokud nebude Filtrovací Driver I volán, neuplatní ani svojí funkčnost. Pokud by byl Filtrovací Driver I šifrovacím driverem, byla by ztráta funkčnosti zřejmá na první pohled, pokud se ale bude jednat o detekci virů při přístupu, bude prvotní informací o nefunkčnosti celého systému zavirovaný počítač a i v tomto případě bude uživatel spíše zvažovat kvalitu antiviru a ne dalších instalovaných programů. Toto řešení je implementováno např. u Quarterdeck CleanSweep (verze 3.0) a i u dalších méně rozšířených systémů.

Rozpoznávání jmen procesů

Tento způsob řešení, který je v současnosti nejrozšířenější, vychází z předpokladu, že je rekurzivní otevření souboru prováděno pouze několika málo programy, jejichž jména jsou přesně známa. K nejčastěji užívaným jménům patří jména nejrozšířenějších antivirů. Řešení má jednu velkou výhodu - pokud se vyskytne konflikt, je jej autor filtrovacího driveru schopen odstranit během několika hodin a tím prokázat dostatečný um. Stačí nalézt jméno konfliktního programu a to doplnit do seznamu. Nevýhodou řešení je omezená kompatibilita. Není patrně v lidských silách opatřit a otestovat veškeré systémy, které používají rekurzivní otevření souboru. Nejrozsáhlejší seznam (http://www.microsoft.com/ddk/IFSkit/testing.htm) obsahuje pouze zlomek produktů, které využívají filtrovací drivery.



Další nevýhodou je omezení funkčnosti. Představme si, že Filtrovací Driver I je šifrovací driver. Pokud propouští požadavky detektoru virů bez jakéhokoliv zpracování, dostává detektor virů požadavky zašifrované a v zašifrovaných datech se viry hledají velmi těžko. Tak mohou být viry skryté v zašifrovaných datech rezistentní vůči detekci při přístupu.

Přímé volání filtrovacího driveru

Oba předchozí případy řešily situaci, kdy filtrovací driver chce být kompatibilní s dalším driverem, který provádí rekurzivní otevření souboru. Driver provádějící rekurzivní otevření souboru se pak o kompatibilitu s čímkoliv dalším nestará. Obdobný způsob řešení kompatibility je akceptovatelný pouze u produktů, které byly již uvedeny na trh a jsou dostatečně rozšířené. Pokud produkt dostatečně rozšířený není a zároveň provádí rekurzivní otevření souboru, musí jeho autor řešit otázku, jak soubor otevřít, aniž by si této operace další filtrovací drivery povšimly. Častým řešením je otevření souboru v módu jádra. Tím je dosaženo kompatibility s většinou existujících filtrovacích driverů. Uživatel pak může jenom doufat, že právě on si nenainstaloval driver, který u otevíraných souborů nerozlišuje mód operace při otevření souboru.

Drobným nepříjemnostem spojeným s existencí filtrovacího driveru, který nerozlišuje módy operace, se lze vyhnout poněkud obecnějším řešením. Jednou z možností je "komolit" jména otevíraných souborů, tj. modifikovat jméno před otevřením souboru a ve filtrovacím driveru tomuto jménu vrátit jeho původní podobu. Další možností je využít vlastností prostoru jmen jádra a vytvořit ve filtrovacím driveru sadu vstupních bodů určených právě pro rekurzivní otevírání souborů. Pokud např. zaregistrujeme jméno vstupního bodu (Device Object-u) jako "\\DosDevice\\AA:" a otevřeme soubor "\\DosDevice\\AA:\\mysoubor.txt", je volán příslušný vstupní bod filtrovacího driveru se jménem "\\mysoubor.txt". Volání lze pak dále poměrně jednoduše přesměrovat na souborový systém reprezentující svazek "A:". Vstupní body filtrovacího driveru v tomto případě nereprezentují souborový systém, a tak

...pokračování na další straně

Irský velvyslanec na vernisáži ve firmě DECROS aneb Co mají Češi a Irové společného

Ve čtvrtek 4.5.2000 proběhlo v budově společnosti DECROS slavnostní otevření výstavy prací dvou irských umělců Paula Gribbina a Damiana Keenana, kterou zahájil velvyslanec Irska v České republice pan Michael Collins.

Proč právě irské umění?

Celý nápad vznikl na základě dlouhodobé spolupráce mezi Paulem Gribbinem a firmou DECROS. Paul pracuje pro DECROS coby externí grafik. S tvorbou Damiana Keenana jsme se setkali také prostřednictvím Paula, který je jeho spolužákem z univerzity. Paul Gribbin se narodil v Irsku a do Čech se dostal díky své manželce, která odsud pochází.

V rámci své tvorby se věnuje zejména malbě a ilustraci. Velkou inspirací jsou pro něho například české pohádky. Na výstavě v DECROSU je možné nalézt několik druhů jeho tvorby - k vidění tu jsou obrazy inspirované keltskou tématikou a rodným Irskem, dále obrázky s nádechem mystična až pohádkovna a konečně se zde objevují i klasické akty.

Damian Keenan je rovněž Ir, ale pro změnu se oženil do sousedního Německa.

Jeho práce jsou kombinací počítačové grafiky a kresby zároveň. Ačkoliv se vesměs jedná o počítačové abstrakce, keltský vliv je patrný i zde.

Slavnostní otevření proběhlo ve čtvrtek 4. května 2000, v sídle společnosti DECROS. Byli jsme potěšeni, že jsme mezi hosty mohli přivítat primátora Českých Budějovic pana Miroslava Tettera, ředitelku Okresní hospodářské komory paní Ivu Škopovou, ředitelku British Council paní Renatu de Quincey a mnoho dalších.

Svou návštěvou DECROS také poctil velvyslanec Irska v České republice pan Michael Collins, který přijel na přání autorů výstavu zahájit. Kromě výstavy samotné navštívil během dne také představitele města, univerzity a Budějovického Budvaru. Během výstavy poskytnul několik interview místním novinářům, které zaujala jeho srdečná zahajovací řeč, ve které se mimo jiné zmínil o příbuznosti obou národů. Podle pana Collinse spolu Češi a Irové dobře vycházejí díky společným keltským kořenům. Pan Collins působí v České republice teprve 9 měsíců a jeho návštěva v Českých Budějovicích byla v historii města vůbec první návštěvou vysoce postaveného představitele Irska. Podle jeho slov by do Českých Budějovic znovu rád zavítal v rámci rodinného výletu. Na závěr tento zástupce země, která je často díky závratnému ekonomickému růstu nazývaná "Keltským tygrem", popřál Čechům hodně zdaru a rychlý vstup do EU.

Denisa Mylbachrová
denisa.mylbachrova@decros.cz

nejsou filtrovány žádným dalším filtrovacím driverem.

Závěrem

Při hledání příčin vzájemné nekompatibility filtrovacích driverů jsem popsal pouze obsluhu jediné služby - otevření souboru. Jedná se o nejčastější, ne však jedinou službu, u které konflikty nastávají. Další konfliktní službou ve vztahu k antivirům je např. přejmenování nebo zavření souboru. Způsob řešení těchto konfliktních situací je obdobný jako u otevření souboru. Konflikty filtrovacích driverů se projevují v lepším případě zamrznutím systému. Tyto konflikty lze eliminovat postupným odstraněním nainstalovaného software.

Tento postup nezaručuje, že bude odhalen viník daného problému (u problémů s kompatibilitou je viníků většinou více), ale zaručuje návrat k funkčnímu systému. Horším případem je omezení funkčnosti některých částí systému. Pokud tato omezení nejsou známa a není s nimi uvažováno při analýze možných rizik, mohou vést k vážnému ohrožení bezpečnosti celého systému.

Miloslav Mařík
miloslav.marik@decros.cz

Information Security Summit - IS2

IS2 s podtitulem "Finanční služby ve virtuálním prostředí " proběhnul ve dnech 30.-31.5.2000 v Míčovně Pražského hradu. Jednalo se o první ročník mezinárodní konference, která byla zaměřena na oblast informační bezpečnosti. Nápad zorganizovat podobnou akci, vznikl v řadách redakce časopisu Data Security Management. Podle slov jedné z organizátorek Mgr. Vlaďky Kaplanové byla už delší dobu v České republice znát absence podobné akce, a tak se rozhodla tento nedostatek napravit.

Celá akce se konala pod záštitou společností CACIO, ISACA a ČILA. Mezi partnery summitu samozřejmě patřila i společnost DECROS. Delegáti nás mohli navštívit v "zimní zahradě", kde jsme sdíleli společný slunečník s ICZ. Se svými příspěvky vystoupilo 11 přednášejících. Jmenujme například RNDr. Evu Rackovou z KPMG, RNDr. Ing. Zdeňka Kaplana z DSM, z těch zahraničních potom R. Boswor - Daviese z Unisys, Velké Británie, L. Strouse z De Nederlandsche Bank, Nizozemí, a mnoho dalších. Aktuální témata byla zahrnuta do příspěvků s tituly jako např. "Řízení bezpečnosti na top manažerské úrovni", "Trendy informační

bezpečnosti", "Bezpečnost jako soutěživá výhoda", "Návratnost investic do informační bezpečnosti", "Penetrační testování" či "Bezpečnostní vzdělávání". Více informací můžete nalézt na www.dsm.tate.cz

A celkový dojem? Jak už to bývá, některé přednášky byly hodnoceny velice kladně, jiné již méně. Summit byl zaměřen na konkrétní cílovou skupinu - bezpečnostní manažery - a zde svůj účel nepochybně splnil. Z této události jsem si odnášela jak z pozice vystavovatele, tak i návštěvníka velmi dobrý dojem a každému, kdo se bezpečnostním managementem zabývá, doporučuji navštívit její příští ročník.

Denisa Mylbachrová
denisa.mylbachrova@decros.cz

Elektronická pošta na serveru NetWare
zajímavá jednoduchá, rychlá a levná alternativa

Používá Vaše organizace síť se servery NetWare 4.11 nebo 5? Chtěli byste na těchto serverech rozběhnout jednoduchý a spolehlivý systém pro elektronickou poštu a přitom se Vám zdá GroupWise příliš komplikovaný nebo příliš drahý?

Jistě, můžete použít také freeware řešení - poštovní server Mecury, u něhož však neexistuje oficiální podpora ani záruka plné funkčnosti a kompatibility. Pokud si přejete vytvořit skutečně efektivní a jednoduchý systém elektronické pošty s nativní podporou NetWare, je zde nový produkt, který svými vlastnostmi i cenou stojí mezi těmito extrémy: Novell Internet Messaging System 2.1 (NIMS 2.1).

Původ NIMS

Tento systém elektronické pošty má svůj původ ve firmě Netscape. Později byl v rámci spolupráce mezi společnostmi Netscape a Novell původní Netscape Messaging System portován na servery NetWare a upraven pro využití adresářových služeb NDS. Nyní je vyvíjen a podporován čistě v rámci firmy Novell. NIMS 2.1 je koncipován modulárně - jeho jednotlivé funkce zajišťují specializované softwarové moduly (agenti). Díky této koncepci vyniká NIMS 2.1 svou jednoduchostí a snadnou rozšiřitelností. Mezi jeho další výhody patří snadná konfigurace a správa, plná integrace s prostředím NetWare a adresářovými službami NDS, bohaté bezpečnostní funkce a široká podpora standardů Internetu. Cena je kalkulována podle počtu uživatelů a pohybuje se okolo 700,- Kč na jednoho uživatele, což je skoro 7x méně než cena systému GroupWise 5.5.

Instalace NIMS 2.1 je pro běžného správce serveru NetWare jednoduchou záležitostí - produkt se instaluje na konzole serveru v prostředí utility Install resp. NWConfig. V rámci instalace jsou také kopírovány potřebné plug-iny pro integraci správy systému NIMS 2.1 do utility NWAdmin. Prvotní nastavení parametrů systému NIMS 2.1 včetně určení, kteří agenti v systému poběží, je asi nejsnazší provést právě pomocí utility NWAdmin. Stejné nastavení (v poněkud neobvyklé podobě) se dá provést také přes webové rozhraní systému, nazývané WebAdmin. Tento modul je však třeba nejprve na serveru spustit - je to samostatná součást systému a spouští se zvláštním příkazem nezávisle na ostatních agentech NIMS 2.1.

Po instalaci systému NIMS 2.1 je každému uživateli NDS založena poštovní schránka. Jednotlivým kontejnerům ve stromě NDS je možné přiřadit vlastní poštovní doménu a adresář serveru, ve kterém budou zřízeny poštovní schránky uživatelů z tohoto kontejneru. Jednotlivé organizační jednotky stromu NDS mohou být realizovány v poštovním systému NIMS 2.1 jako samostatné poštovní domény nebo mohou být sloučeny do jedné poštovní domény. NIMS 2.1 podporuje také NDS skupiny, organizační role a NDS aliasy. Při testování různých konfigurací systému NIMS 2.1 jsme si ověřili, že například pro společnosti s několika pobočkami v jednom NDS stromu, která má jednu poštovní doménu, lze vytvořit distribuovanou konfiguraci, kdy je na každé pobočce umístěn poštovní server doručující elektronickou poštu uživatelům v dané pobočce.

Nástroje NIMS

NIMS 2.1 je vybaven několika silnými nástroji určenými pro zabezpečení systému proti zneužití a proti zasílání nevyžádané pošty (spamu). Administrátor i jednotliví uživatelé mohou zakázat příjem nevyžádané pošty z určitých adres. Můžete využít mnoho vlastností - včetně Realtime Blackhole Listu (RBL) a reverzních DNS dotazů, možnosti zablokování IP adres, e-mailových adres a domén a SMTP autentikace - k vyloučení příjmu nevyžádaných zpráv z nežádoucích poštovních domén a e-mailových adres libovolného poštovního serveru. Užitečnou funkcí je anti-relaying - mechanismus, který brání neautorizovaným uživatelům posílat zprávy pomocí tohoto systému. Můžete dokonce zakázat použití určitých SMTP příkazů, čímž ztížíte hackerům získání přístupu k Vašemu systému.

Jedním ze zajímavých agentů systému NIMS 2.1 je WebMail, který realizuje webové rozhraní systému. Uživatelé mohou díky němu přistupovat ke svým zprávám z jakéhokoli standardního web browseru. K realizaci web rozhraní není třeba, aby byl na NetWare serveru nejdříve instalován webserver - tato funkce je zcela autonomní. Další užitečnou funkcí je Mail Proxy. Ta umožňuje uživatelům, aby si nastavili automatické stahování pošty z jiných (externích) systémů elektronické pošty do svých lokálních schránek. Samozřejmostí je možnost nastavení aliasů pro uživatelské účty.

Příhodné jsou také možnosti uživatelského nastavení systému. Uživatelé si mohou sami bez pomoci administrátora systému nastavit základní vlastnosti svého účtu - změnit heslo, nastavit pravidla pro automatické odpovídání nebo předávání zpráv, změnit jazykovou preferenci, barvy prostředí webmailové schránky apod.

K dalším funkcím NIMS 2.1 patří možnost nastavení administrativních restrikcí - zavedení kvót na velikost poštovních schránek uživatelů, možnost potlačení zacyklování zpráv pomocí zákazu předávání zpráv doručených z cizích účtů pomocí Proxy agenta, omezení počtu uživatelsky nastavitelných voleb, evidence všech pokusů o spam do logu a nastavení maximálního povoleného počtu adresátů v odchozích zprávách.

Požadavky na systém

Mezi jediné požadavky na server patří minimálně 128 MB paměti a dostatečná kapacita disku, která samozřejmě souvisí s počtem uživatelů. Systém, který server využívá, samozřejmě musí být NetWare® 5 nebo NetWare 4.11, ale o tom jsem již psal v úvodu. Na straně klienta lze použít libovolný POP3 nebo IMAP4 klienta, jejichž nejznámější představitele naleznete v tabulce.

Pokud Vás oslovily tyto informace a uvažujete o vlastním vyzkoušení, pak neváhejte. Jak se zdá z posledních zpráv z vývojové dílny Novellu, tak Novell Internet Messaging Systém bude mít od 15.června 2000 svého nástupce v podobě vylepšené verze 2.5, která bude dostupná i pro platformy LINUX a SOLARIS. Až bude k dispozici, jistě Vás budeme informovat.

Martin Štrobl
martin.strobl@decros.cz

Nejznámìjší POP3 a IMAP4 klienti
Netscape Navigator
Netscape Communicator
Internet Explorer
Outlook
Outlook Express
Eudora
Pegasus Mail

Podporované standardy

NIMS 2.1 podporuje tyto internetové standardy:
- Post Office Protocol 3 (POP3)
- Internet Mail Access Protocol 4 (IMAP4)
- Lightweight Directory Access Protocol (LDAP)
- Secure Sockets Layer (SSL 3.0)
- Multipurpose Internet Mail Extensions (MIME)

Přehled základních produktů firmy DECROS

Kompletní přehled je možné nalézt na internetové stránce http://www.decros.cz

Pokud byste uvítali informace o produktech firmy DECROS v tištěné podobě, kontaktujte nás. Rádi vám je zašleme.

Produkt	Popis	Verze
Protect pro Windows 98/95	Rozšíření Windows 98 nebo Windows 95 o ochranné a bezpečnostní funkce, kvalitní transparentní šifrování šiframi WinCros, Wincros II a CAST, bezpečný přenos dat po internetu a preventivní antivirovou ochranu. Protect 98/95 chrání soubory před smazáním či modifikací.	2.6.11
Protect Plus (IR-15) pro Windows 98/95	Kombinace Protect pro Windows 98/95 s bezdrátovým elektronickým zařízením, zvaným Security Box Infrared, které komunikuje s IrDA portem počítače. Security Box plní identifikační a autentizační funkci a dále v něm lze bezpečně uložit až 15 (nebo 63) šifrovacích klíčů pro dvě bezpečnostní úrovně. Přístup ke klíčům je chráněn heslem (PIN), které zadává uživatel. Security Box navíc umožňuje uzamykání a odemykání stanice.	
Protect Plus (RS-15) pro Windows 98/95	Kombinace Protect pro Windows 98/95 s elektronickým zařízením, zvaným Security Box. Security Box plní identifikační a autentizační funkce, dále v něm lze bezpečně uložit až 6 šifrovacích klíčů pro dvě bezpečnostní úrovně. Přístup ke klíčům je chráněn heslem (PIN), které zadává uživatel.	
Protect pro Windows NT	Rozšíření Windows NT 4.0 o možnost šifrování dat na úrovni souborového systému a další ochranné funkce.	2.6.13
Protect Plus (IR-15) pro Windows NT	Kombinace Protect pro Windows NT s bezdrátovým elektronickým zařízením, zvaným Security Box Infrared. Součástí je modul pro identifikaci předmětem do Windows NT. Security Box je možno použít pro bezpečné přihlašování, odemykání stanice a úschovu šifrovacích klíčů.	
Protect Plus (RS-15) pro Windows NT	Kombinace Protect pro Windows NT s elektronickým zařízením, zvaným Security Box. Součástí je modul pro identifikaci předmětem do Windows NT. Security Box je možno použít pro bezpečné přihlašování a úschovu šifrovacích klíčů.	
SBXadmin	Aplikace umožňující centrální vzdálenou správu obsahu bezpečnostních předmětů typu Security Box.	2.0.50
Security Card Y2k	Hardwarový adaptér řešící problém BIOSu u starších počítačů při přechodu na rok 2000.	1.0.04
Security Card Lite	Základní bezpečnostní adaptér určený především pro ty, kteří si chtějí Security Card nejprve vyzkoušet a potom se teprve rozhodnout pro optimální model. Pracuje ve všech OS.	2.2.08
Security Card Economy	Bezpečnostní adaptér pro běžné nasazení. Vhodný pro menší firmy nebo domácí počítač. Umožňuje ochranu přístupu pro tři uživatele, nastavení práv přístupu k diskům, zákaz bootování z diskety, ochranu zavádění operačního systému a další ochranné funkce.	
Security Card Economy/C	Stejná jako Security Card Economy, navíc umožňuje transparentní automatické šifrování logických disků. (aplikace WinCoder)	
Security Card Stat	Karta určená pro nasazení ve velkých organizacích. Kromě většího počtu uživatelů (8) má více bezpečnostních funkcí a poskytuje spolehlivou evidenci průběhu práce s počítačem.	
Security Card Stat/C	Stejná jako SC Stat, navíc umožňuje transparentní a automatické šifrování logických disků. (aplikace WinCoder)	
Security Card 98	Bezpečnostní karta pro běžné nasazení. Vhodný pro menší firmy nebo domácí počítač. Součástí karty je Protect pro Windows 98/95 umožňující šifrování souborů a adresářů. Karta umožňuje mimo jiné bezpečné uložení až šesti šifrovacích klíčů programu Protect pro Windows 95/98.	
Security Card 98 Stat	Karta určená pro nasazení ve velkých organizacích. Kromě většího počtu uživatelů (8) má více bezpečnostních funkcí a poskytuje spolehlivou evidenci průběhu práce s počítačem. Součástí karty je Protect pro Windows 98/95, umožňující šifrování souborů a adresářů. Karta umožňuje mimo jiné bezpečné uložení až šestnácti šifrovacích klíčů programu Protect pro Windows 95/98.	
Security Card WiNT	Bezpečnostní karta, která rozšiřuje bezpečnostní funkce vlastní systému Windows NT zejména o statistiku provozu a ochranu zavádění operačního systému. Součástí karty je identifikační a autentizační modul dGINA , který umožňuje přihlašování uživatele do Windows NT pomocí bezpečnostních předmětů (Touch Memory, Security Box, Security Card, BrainCard). Šifrování je zajištěno aplikací Protect pro Windows NT.	
Security Card WiNT/C	Rozšíření vlastností Security Card WiNT o možnost šifrování souborů, adresářů a úschovu šifrovacích klíčů. Součástí karty je identifikační a autentizační modul dGINA , který umožňuje přihlašování uživatele do Windows NT pomocí bezpečnostních předmětů (Touch Memory, Security Box, Security Card, BrainCard). Šifrování je zajištěno aplikací Protect pro Windows NT.	

Poznámka: Všechny uvedené modely Security Card jsou ve verzi s centrální správou. (firmware verze 2.x).
Čísla verzí jsou aktuální ke dni 10. červnu 2000 a jsou zde uvedeny především pro orientaci.

Infosecurity Europe 2000 v Londýně

V letošním roce patřil DECROS ke dvěma společnostem, které na Inforsecurity v Londýně reprezentovaly Českou republiku. Ve středu zájmu návštěvníků stánku firmy DECROS byla nejen nejnovější verze (těsně před uvolněním) Protectu pro Windows s novým modulem digitálního podpisu, jež je k dispozici i pro aktuální verzi Windows2000, ale i DECROS Crypto Service Provider pro Microsoft Crypto API.

Již pátý ročník výstavy Infosecurity se konal mezi 11. - 13. dubnem 2000 v londýnské Olympii. Oficiální název letošního ročníku zněl "Infosecurity Europe". Jak jsem se dozvěděla od organizátorů, přídomek Europe zvolili v souvislosti s narůstajícím zájmem takzvaných "zaoceánských" (Overseas) návštěvníků i vystavovatelů. Zatímco v prvním roce výstavy byli téměř všichni výhradně britské národnosti, letos pocházela bezmála pětina návštěvníků i vystavovatelů z jiných zemí.

Jak už samotný název napovídá, jedná se o úzce specializovanou výstavu zaměřenou na oblast informační bezpečnosti. Pokud Vás zajímá konkrétní oblast, hledáte-li optimální řešení a nechcete trávit svůj drahocenný čas putováním po halách

obrovského výstaviště, je pro Vás výstava typu Infosecurity ideální příležitostí pro uspokojení Vašich potřeb. Pořadatel, společnost Reed Exhibition Companies, si tento trend velice dobře uvědomuje, a proto se rozhodla pořádat lokální výstavy ve Francii, Německu, Belgii, Jižní Africe a Asii.

Ale zpět k samotné Infosecurity Europe 2000. Jak jsem již zmínila na začátku, výstava se každoročně koná v National Hall, v Olympii, Kensingtonu v Londýně. Jedná se skutečně "pouze" o jednu halu. Záměrně jsem použila uvozovek u slova pouze, protože naplnit halu 160-ti společnostmi ze stejné branže je jistě úctyhodný výkon. Výstava pro organizátory neznamená pouze prodej plochy a výstavbu stánků, ale také spoustu souvisejících marketingových aktivit. Po celé tři dny trvání výstavy je možné navštívit asi 50 seminářů, které jsou opravdu velice kvalitní a zajímavé. Pokud chcete vést obchodní jednání mimo stánek nebo si jen chvíli odpočinout od všeho ruchu, je možné využít služeb speciální restaurace pro vystavovatele. Další výhodou se stalo vstupné, které bylo pro všechny návštěvníky zdarma. Pokud Vám bylo více než 18 let a svolili jste se k vyplnění registračního formuláře, pak Vám brány výstaviště byly otevřeny.

A žhavá novinka na závěr? Nevím si rady. K vidění bylo vše a vše si našlo svého zákazníka. V hojném počtu bylo slyšet dotazy na stále módní PKI (Public Key Infrastructure) a samozřejmě se letos do středu zájmu dostala i bezpečnostní řešení pro Windows2000.

Pokud byste chtěli získat více informací o této výstavě, naleznete je na http://www.infosec.co.uk.

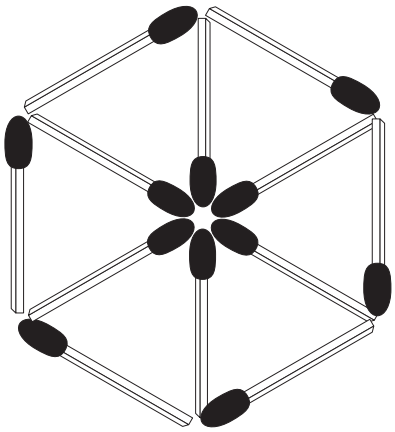
Denisa Mylbachrová
denisa.mylbachrova@decros.cz

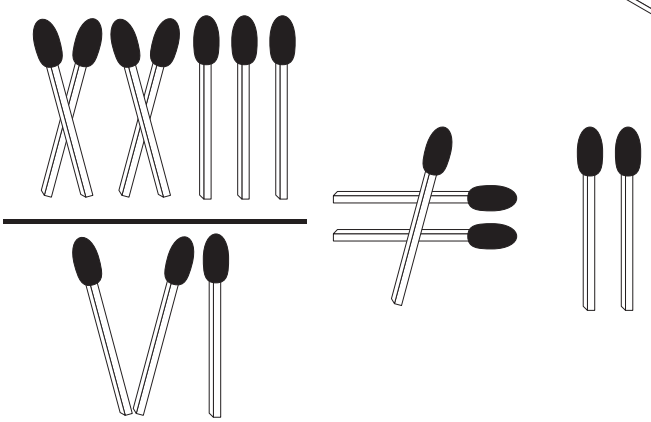
Hádanky pro volné chvíle

Opět jsme si pro vás připravili rébusy ze sirek.

V horním obrazci ze 12-ti zápalek přemístěte 3 zápalky tak, aby vzniklo 6 shodných rovnoběžníků.

Ve druhém obrazci přemístěte 2 zápalky tak, aby se změnila nerovnost rovnice na rovnost.





(Nápověda: V řešení se vyskytuje Ludolfovo číslo.
Nápověda 2: Tím se nemyslí 3,14)

V příštím čísle

vás seznámíme s novými vlastnostmi Protectu 3.0 a Security Card 3.0, budeme se zabývat zákonem 148 a jeho uvedením do praxe, nezapomeneme ani na další infrormace o projektu Třebíč a samozřejmě nebude chybět ani pozvánka na INVEX 2000 do Brna. Příští číslo DECROS News vyjde začátkem října. Do té doby nashledanou.

DECROS NEWS

Informační bulletin pro zákazníky, partnery firmy DECROS a zájemce o informační bezpečnost.
Šéfredaktor: Josef Dvořák
Vydává: DECROS s.r.o., J.Š.Baara 40,
370 01 České Budějovice, tel.: 038-7312808,
fax: 038-7311480, http://www.decros.cz,
e-mail: dn@decros.cz, Vyšlo v červnu 2000, zdarma

Podávání novinových zásilek povoleno Českou poštou, s.p., ředitelství odštěpného závodu Jižní Čechy v Českých Budějovicích, j.zn.: P-2901/99 ze dne 24. května 1999.
Registrační číslo: MK ČR 8230
Sazba a grafická úprava: © Martin Klíma, 2000