Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 78/2004 **2. srpna 2004**

78/2004

Připravil : Mgr.Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(548 registrovaných odběratelů)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Soutěž v luštění 2004
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

HISTORIE SOUTĚŽE

Vážení čtenáři, 15.9.2004 zahajujeme již tradiční podzimní soutěž o ceny v luštění jednoduchých šifrových textů. Obdobné soutěže pořádal náš e-zin v letech 2000, 2001 a 2003. V roce 2000 byly úlohy zaměřeny na klasické šifrové systémy. V roce 2001 soutěž pokračovala řešením "modernějších" systémů. Soutěž v roce 2003 byla z hlediska předložených úloh mnohem jednodušší než v předchozích letech. Skládala se z řešení devíti úloh od hříček, přes jednoduché šifry až opět po klasické šifrové systémy (jednoduchá záměna, transpozice, periodické heslo).

Pokud se chcete podívat na tyto starší úlohy, najdete je zde:
Soutěž 2000: http://crypto-world.info/index2.php?vyber=soutez
Soutěž 2001: http://crypto-world.info/index2.php?vyber=soutez2
Soutěž 2003: http://crypto-world.info/soutez2003/index.php

V roce 2003 se do soutěže zaregistrovalo rekordních 107 řešitelů, z nichž však pouze 32 splnilo podmínky pro zařazení do losování o ceny; všech 9 úloh vyřešilo celkem 11 soutěžících.

V letošním ročníku plánuji, pokud jde o typ úloh, navázat na rok 2003 a opět vám předložit výběr jednoduchých úloh od jednoduchých hříček (připomínajících skautský tábor) až po klasické šifrové systémy. Pokud se chcete teoreticky na soutěž připravit a podívat se na postupy řešení jednotlivých klasických šifrových systémů, doporučujeme se seznámit se staršími články otištěnými v Crypto-Worldu v roce 2000. V těchto článcích byly jednotlivé klasické systémy podrobně představeny a čtenář zde nalezne i doporučený postup luštění. Doporučuji se podívat i na řešení loňských úloh, kterým je věnované celé číslo e-zinu 12/2003.

Pokud se chcete seznámit s metodami luštění ještě podrobněji, doporučuji doprovodné texty k prvním lekcím přednášky Úvod do klasických a moderních metod šifrování ALG082. Kurs probíhal pod odborným vedením doc. RNDr. J.Tůmy, DrSc. na Katedře algebry MFF UK Praha v zimním semestru 2004 (http://adela.karlin.mff.cuni.cz/~tuma/ciphers.html).

Steganografie, Crypto-World 9/2000, str.2-5
Jednoduchá záměna, Crypto-World 10/2000, str. 2-4
Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
Substituce složitá - periodické heslo, srovnaná abeceda , Crypto-World 11/2000, str. 4-10
Řešení úloh ročníku 2003, Crypto-World 12/2003, celé číslo

PRAVIDLA

Soutěž začne 15.9.2004 a skončí 6.prosince 2004 ve 22.00 hod. Zúčastnit soutěže se může každý odběratel e-zinu Crypto-World. Registrace probíhá přes web. Vstup na tuto stránku soutěže bude přes domovskou stránku Crypto-Worldu – ikona Soutěž 2004.

Při registraci řešitel zadá kód, který mu bude zaslán společně s kódy pro stažení e-zinu Crypto-World 9/2004 (15.9.2004). Potom zadá svůj login, autentizační heslo pro opětovné přihlášení a e-mail. Tento e-mail se dále nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný.

Na této stránce budou postupně ve třech kolech zveřejňovány soutěžní úlohy. Za vyřešení úlohy budou připsány soutěžícímu podle její obtížnosti 1 až 4 body. Registrovaný řešitel bude zadávat své odpovědi přes www rozhraní. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne. Na stránce bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku vidět nejen počet dosažených bodů, ale i pořadí úloh, ve kterém je soutěžící vyřešil.

Pro určení celkového pořadí je rozhodující celkový počet dosažených bodů za vyřešené úlohy a to 6.prosince 2004 ve 22.00 hod. Při rovnosti počtu vyřešených úloh je rozhodující, kdo dříve tento počet docílil. První tři řešitelé získají automaticky cenu. Další tři ceny se vylosují mezi řešitele, kteří dosáhnou nejméně deseti bodů.

CENY

Pro první tři řešitele je připravena láhev whisky (značka bude upřesněna po dodání sponzorem soutěže) se soupravou dvou skleniček na whisky (historická replika inspirovaná renesančním sklem).

Cenu dostanou ještě další tři luštitelé, ti budou vylosováni z těch, kteří dosáhnou alespoň deseti bodů. V tomto případě je připravena láhev stejné značky whisky s jednou skleničkou.

Ceny do soutěže věnovali sponzoři soutěže:

- firma Dignita , s.r.o., http://www.dignita.cz
- Qobchod - Internetový obchod se sklem, http://www.qobchod.cz/

ÚLOHY

Pokud máte zájem, můžete se na soutěž trochu rozcvičit a pokusit se vyřešit tři následující cvičné úlohy. Obtížnost těchto úloh odpovídá úkolům v prvním kole a za každé správné řešení úlohy byste získali po jednom bodu.

Cvičná úloha č.1

B AB BAB B BBB BAAA BABB BB BBB AAAA ABAA BABB AAAB BABB ABBA AB BAA AB B AAA BBB AAB B A BBAA BA AA AAB ABAA BBB AAAA BABB ABA A AAA A BA AA BB ABBB A AAA ABAA BBB AAAB BBB BB BBB ABA AAA A

Cvičná úloha č.2

QYXKA REJOL SEHUK TAPZO PONAS POTEJ EZLED IVDEN HIKAN IJHCY BTOBE NYPEL SMESJ

Cvičná úloha č.3

P aV ElP A CRY Pzin LpAV EL PAV worl vElp AvTG pavE LpXC eLPa vE Lgv vE L cry ELP avE L u AVel Pa ve lpA vElp AVE ezin ElPA vEl p ave l Pa ve LP aQWE p ave lPav ZIN aveL PAV EL PAV eLp ave b

Správné řešení cvičných úloh najdete v části Letem šifrovým světem na straně dvacet tři.

Přeji hodně zábavy a potěšení z luštění soutěžních úloh 2004 !

B. Hackeři, Crackeři, Rhybáři a Lamy
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Tento článek si klade za cíl připomenout některé pojmy, které jsou často širokou veřejností spojovány především s tematikou současné počítačové kriminality. Po přečtení některých článků lze totiž zjistit, že pojmy jako hacker a cracker jsou prezentovány ne vždy správně a někdy se zaměňují. Jejich výklad se velmi často nezakládá na pravdě a v některých pramenech se tyto výrazy ztotožňují. Souhlasíte snad se spojením hacker a Kevin Mitnick (viz nedávná zpráva v televizi „Největší hacker všech dob Kevin Mitnick navštívil Prahu)? Pro větší zmatek v pojmech se v poslední době začalo používat nové „české“ slovo rhybaření (jak již asi většina ví, nejde o překlep). Článek je tedy jen jakousi rekapitulací nebo ještě lépe inventurou těchto pojmů. Téma je široké a vydalo by spíše na celou studii a materiálu tohoto typu lze pro zájemce o širší pohled nalézt na Internetu opravdu spoustu. V omezeném prostoru se proto budeme zabývat jen těmi nejzákladnějšími pojmy.

Hackeři podle Policie České republiky

Začnu téměř „oficiální policejní definicí“ Doc. Ing. Ivo Látala, CSc**.,** z Policejní akademie České republiky.

„Hackeři (průnikáři) - osoby, které pronikají do ochraňovaných systémů, přičemž jejich cílem je prokázat své vlastní schopnosti, kvality, aniž by měly zájem získat informace nebo systém narušit. Hlavní je překonávat ochranné bariéry, což považují za zábavu, dobrodružství, provázené "sportovním nadšením", aniž by očekávaly osobní veřejné uznání. Stačí jim, jestliže se o jejich činu hovoří. Snad by vyhovovalo srovnání se žháři, kteří mají požitek z pozorování ohně, nebo se dokonce podílejí na jeho likvidaci. Hackerství je jejich koníčkem, u počítačů vysedávají po dlouhý čas a získaná data nebo programy využívají spíše pro svoji potřebu nebo pro přátele.“

Citace je převzata z přílohy časopisu POLICISTA č. 3/1998 - Počítačová (informační) kriminalita a úloha policisty při jejím řešení
http://www.mvcr.cz/casopisy/policista/prilohy/pc_krimi.html .

Hackeři podle slovníku

Termín hacker se používá různě: jako označení uživatele, který se snaží proniknout do cizích systémů, případně počítačového podvodníka nebo piráta. Anglicko-český slovník na Seznamu (http://www.seznam.cz) vám nabídne tento překlad slova hacker: uživatel, který se ze svého počítače nabourává do cizích systémů. Slovní základ hack pak lze (podle tohoto slovníku) přeložit 33 různými způsoby (doporučuji vyhledat). Některé dost dobře vystihují to, co hacker dělá nebo to, o co se pokouší (rozsekat, rozřezat, otesávat, opracovávat, zaseknout, udělat zářez), jiné jsou docela „mimo“ (taxík, nájemná drožka, jet na koni). Není bez zajímavosti, že slovo hack se používá také jako hanlivé označení pro novináře.

Hackeři podle hackerů

Jaký je tedy obecně používaný význam slova hacker? Koho tím můžeme označit? Na základě informací dostupných na Internetu se dá sestavit takovýto profil hackera: *„Jedná se o velmi dobře znalostmi vybaveného uživatele (zpravidla získanými samostudiem), který nachází uspokojení v objevování skrytých detailů v informačních a telekomunikačních systémech, především jejich zabezpečení a zranitelnosti. Hacker miluje praktické, rychlé, ale*

promyšlené programování (ale nikoliv „průhledné“). Hackeři jsou lidé velmi kreativního myšlení. Hackeři najdou uplatnění v pozicích jako jsou systémový administrátor, správce sítí, programátor, designér. Nelze je „použít“ pro stereotypní práce (např. k nudnému zadávání dat do počítače).“

To vše ale z takového jedince ještě hackera nedělá. Pro opravdové hackery je dále typické jejich sociální chování, používaný jazyk, uznávání morálních hodnot vlastní hackerské komunity a samozřejmě provádění samotného hackingu.

Sociální chování hackerů

Hackeři jsou spíše uzavření, nevynikají komunikativností, nejsou vhodní pro kolektivní práci. V pracovním kolektivu nebývají příliš oblíbení. Zaměstnavatel pro jejich výbornou znalost technologií trpí některé jejich výstřelky a dá se říci, že jsou na své pozici stabilizováni, nepočítá se ovšem s nimi na pozice vedoucích či manažerů. Hacker neuznává nadřazené autority, systémem nadřízenosti a podřízenosti v zaměstnání pohrdá. Hackeři rádi hrají počítačové hry, oblékají se především s ohledem na své pohodlí (nikoliv požadavky firmy).

Pokud se v této komunitě objeví dívka, pak nikdy nepoužívá nápadný make up nebo jej nepoužívá vůbec. Peníze pro hackery neznamenají na žebříčku hodnot tolik, jako respekt ostatních (zejména opět hackerů), obdiv, uznání a porozumění (opět především v rámci své komunity). Mívají v oblibě méně běžná (často orientální) jídla, pijí obrovské množství čaje (existují výjimky pijící kávu). Typický je pro ně speciální způsob zápisu textů a používání vlastního žargonu (viz dále warez a odkaz na slovník). Běžná u nich bývá obliba černého humoru.

Morální hodnoty hackerské komunity

Hackeři věří ve svobodu jedince a jsou ochotni pomoci jiným (na základě svého vlastního rozhodnutí). Elektronický svět je pro ně výzva a je zaplněn problémy, které čekají na pokoření (vyřešení). Hacker žádný problém neřeší dvakrát - jednou vyřešený problém již pro něj není zajímavou výzvou. Sdílení informací a know-how pro vyřešení problémů je nedílnou součástí hackerské komunity a přispět vlastním know-how je morální povinností pravého hackera. Svět hackerů je založen na reputaci. Nový člen komunity získá svoji pozici v této komunitě až poté, co projeví své schopnosti, ale také svoji ochotu podílet se na ideálech komunity hackerů. Hacker nebere, ale dává. Věnuje svůj čas, svoji kreativitu a výsledek svých znalostí ve prospěch vyřešení problémů.

Hacking

Činnosti, které pravý hacker provádí a kterými získává uznání a respekt, jsou:

- získání a zpřístupnění zdrojového kódu programů
- odhalení slabin informačního systému a zpřístupnění příslušných informací
- publikování užitečných informací na Internetu
- pomoc při administraci a provozu diskuzních skupin, seznamů mailů, archivů atd.
- pomoc při testování nových programů (tzv. beta verzí)
- propagace hackerské kultury

Pro lepší pochopení myšlení hackerů doporučuji si přečíst Interview s hackerem, které najdete v e-zinu Crypto-World 10/2001 (http://crypto-world.info/index2.php?vyber=casop3).

V tomto článku zpovídám českého hackera s přezdívkou EB#L@ (jeho jméno se ještě jednou v tomto článku objeví).

Nevěříte, že jsou hackeři takoví ?

Na podporu výše uvedených tvrzení (speciálně na podporu teze o pomoci hackerů s testováním nových programů) uvádím zprávu z chystané 12-té hackerské konference Defcon, která se konala v Las Vegas 30. 7. - 1.8. 2004. Téma konference bylo Bezpečnost elektronických voleb a hackeři slíbili zdarma otestovat předložené systémy.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/65272096?-2622

Něco vám zde v popisu činnosti a aktivit hackerů stále chybí? Samozřejmě, že čekáte na napadání www stránek a na jejich neoprávněnou změnu. Z článků na Internetu (např. Stránky lidovců napadl hacker, Stránky ministerstva vnitra napadl hacker, České noviny napadli hackeři,…) se přece zdá, že je to hlavní činnost hackerů.

Možná se budete divit, ale toto praví hackeři nedělají. Tedy většinou … a pokud to dělají, pak již to nejsou hackeři podle naší výše uvedené definice. Podle důvodu, proč stránky byly napadeny, se jednalo buď o samuraje, crekery nebo hacktivismus.

Takže hackeři opravdu nenapadají www stránky? Pokud jste se rozhodli při čtení předchozí části být hackery a teď váháte (být hackerem a nehackovat ….), nebojte se, hackeři přece jen stránky hackují. Jejich motivace je však typicky pro ně vlastní – buď řeší nějakou výzvu (na můj web se nedostanete …) nebo si vzájemně testují své schopnosti. Chcete tedy také legálně hackovat? Prosím vstupte do FHZ (Free Hacking Zone) a „udělejte si“ pro radost a bez problémů se zákonem nějaký ten server:

http://www.hackerslab.org/
http://www.cyberarmy.com/ ,
http://www.roothack.org/ , …

Samuraj

Pokud se útočník naboural do systému a následně vysvětlí správci, např. pomocí e-mailu ze superuživatelského accountu, jak k nabourání došlo a jak má správce tuto díru "záplatovat", říká se mu zpravidla v hackerské komunitě samuraj.

Hacktivismus

Politicky motivované napadání internetových stránek se nazývá hacktivismus. V posledních letech se stále více a více rozvíjí. Je pravděpodobné, že mimo jednotlivce a organizované skupiny se do této činnosti zapojují i profesionálové ze speciálních služeb. Např. na Blízkém východě pravděpodobně izraelské tajné služby opakovaně napadli webové stránky fundamentalistického hnutí Hizballáh, na stránkách Hamasu tak bylo např. umístěno tvrdé porno. Také webové servery izraelského Parlamentu a ministerstva zahraničí byly opakovaně napadeny.

Dalším příkladem je zmizení katarské televize al-Džazíra (http://www.aljazeera.net/) z Internetu během války v zálivu (26.3.2003). Její webové stránky údajně napadla skupina počítačových pirátů podepsaná jako "patrioti, jednotky domobrany a kyber svobody". Místo zpravodajství zde umístila tato skupina výzvu "Ať zní svoboda" napsanou přes vlajku Spojených států oříznutou do tvaru zmíněné země. V dolní části stránky pak byl umístěn

slogan "Bůh žehnej našim vojenským jednotkám!!!" (detaily viz můj článek z roku 2003 E-válka v zálivu (a okolí?), http://www.root.cz/clanek/1593).

A co Česká republika, provádí se zde hacktivismus? Ale ano, samozřejmě, že ano. Snadno např. na Internetu vyhledáte, jak vypadaly po útoku stránky KSČM, které byly napadeny během voleb, ale nebyl to jediný cíl, útočníci pozměnili i stránky jiných politických stran. Stránky lidovců napadl např. 12.6.2002 hacker EB#L@ (náš „známý“ z dříve uvedeného interview). Že se jednalo v tomto případě o typický hacktivismus, potvrdil sám útočník v e-mailu zaslaném administrátorovi serveru, ve kterém napsal: „Chtěl jsem zkrátka vyjádřit svůj politický názor...“.˝
http://zpravy.idnes.cz/vedatech.asp?r=vedatech&c=A020612_103111_vedatech_has&l=1&t=A020612_103111_vedatech_has&r2=vedatech

Obr.1 – Hacktivismus po česku (EB#L@ , stránka Čs. strany lidové).

Crackeři

Dalším důvodem napadání informačních systémů je „kriminální činnost“. Napadení stránky je spojeno buď se snahou získat některá zde uložená data, nebo s úmyslnou a plánovanou destrukcí zde uvedených dat nebo se snahou o neoprávněné pozměnění dat. Takovéto útoky provádí crackeři.

Crack znamená rozbít, rozlousknout. Cracking je tedy činnost, kdy dojde k narušení informačního systému zvenčí. Cracker zpravidla nepracuje sám, ale ve skupinách. Členové bývají ve skupině děleni na hierarchicky odlišené pozice a každý má na starosti konkrétní činnost. Skupina tak může mít např. svého prezidenta, webmastera, dodavatele, kurýra,

testera, manažera, mluvčího apod. Skupiny bývají tematicky specializované na herní oblasti, weby a na aplikace. Soutěživost mezi skupinami je poměrně vysoká a předhánějí a trumfují se ve svých aktivitách. Své úspěchy pečlivě dokumentují a zpravidla i zpřístupňují na Internetu. Crakeři se sami často považují za hackery. Z toho, co jsem již napsal, je však zřejmé, že jimi nejsou. Jejich znalosti informačních systémů, internetových protokolů a programování nejsou na tak vysoké úrovni jako u hackerů. Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali. K úpravě komerčních programů crackeři používají a testují známé triky. Cracknuté programy umožňují dále nelegální cestou šířit (viz warez).

Policejní definice (z již citované přílohy časopisu POLICISTA) je ke crackerům ještě „přísnější“ :
Crackeři, což jsou spíš patogenní osobnosti, jimž se nejedná jen o překonání ochranných překážek, ale po průniku různým způsobem nabourávají informační systémy, získávají data, aniž by snad měli zájem je využít pro svůj prospěch. Potěšení mají spíše z destrukce systému.

Definice se liší proti běžnému chápání v tom, že crackeři mají ve skutečnosti velice často zájem *využít úspěch pro svůj prospěch* (šíření nelegálního software atd.) a mají potěšení z překonání ochranných překážek. Jen malá část skutečných crackerů vyhovuje policejní definici – tedy tomu, že motorem jejich akcí je pouze potěšení ničit. Nicméně jsou takoví a lze o nich tvrdit, že se pohybují ve své činnosti na hranici mezi crackery a hackery (viz samuraj).

Příkladem takové skupiny na hranici mezi hackery a crackery může být známá velice aktivní Česko-slovenská skupina Binary Division, která se specializovala na pozměňování webů. V roce 2000 napadla například weby ISDN, stránky slovenského HZDS a web českého ministerstva vnitra. Její útoky ochromily i služby freemailových serverů Post v Česku i na Slovensku, členové skupiny napadli i České noviny a řadu dalších serverů.

Na stránce http://hysteria.sk/hacked/ najdete zadokumentováno napadnutí některých serverů hacknutých touto skupinou. Na napadených stránkách zpravidla zanechávali tyto pro ně typické vzkazy:
no czert, no dastych, 100% binary division
0% CzERT, 0% Dastych, 100% You have new mail, 100% binary.division

Pro pochopení vzkazu mladšími čtenáři připomenu, že major Dastych měl na starosti boj proti počítačové kriminalitě na Ministerstvu vnitra ČR.

Warez

Speciální podskupinou crackerů je skupina warez d00dz (dud - falešný), která se zabývá překonáním ochrany proti kopírování, úpravou komerčních programů, luštěním ochranných kódů a následnou distribucí nelegálního, copyrightem chráněného software. Jednotlivé skupiny soutěží o prvenství v překonání překážek, kterými jsou hry, programy, CD atd. chráněny. Typické pro tyto skupiny je vytváření vnitřního hierarchického uspořádání a dělba úloh jednotlivých členů.

Skupiny *warez* si vytvořily svůj vlastní jazyk, lépe řečeno slang.
Typické je zejména:

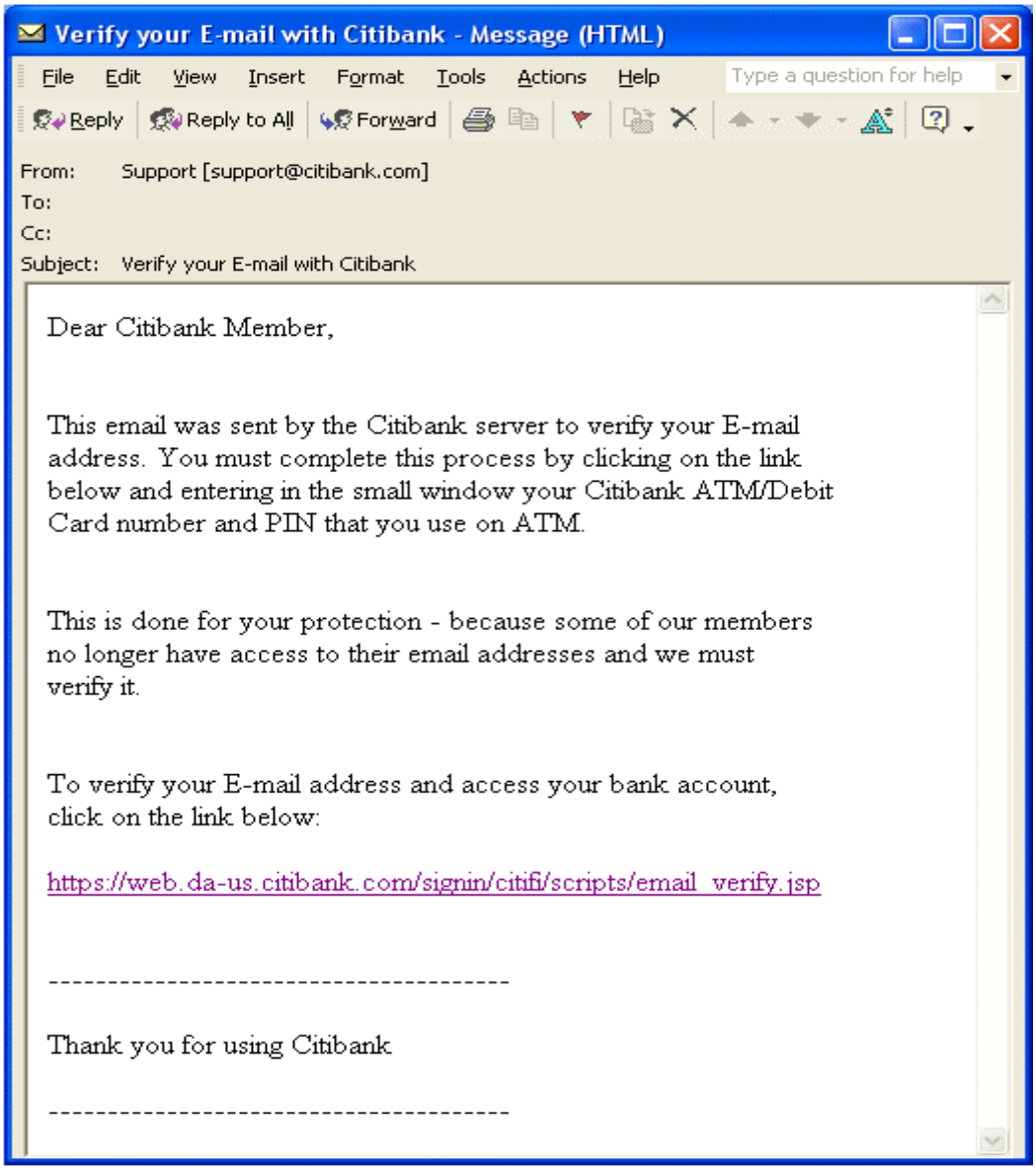
- náhrada písmene S za $: Compu$erve, Micro$oft
- systematické nahrazení písmene `s` označujícího množné číslo písmenem `z` (passwordz, passez, utilz, MP3z, distroz, pornz, sitez, gamez, crackz, serialz, downloadz, FTPz, ...)
- použití zdůrazňující předpony k (snad jako kilo) (k-cool velice chladnokrevný, k-awesome – hrozně děsivý, k-korun - drahý)
- nahrazení o-0 (c00l, l0zer, b00t, d00d …)

- vzájemná záměna ph a f : (phone => fone, freak => phreak)
- používání znaků #!$ při doplňování textů ("Hey Paul!#!$#$!#!$").
- využívání fonetického čtení/zápisu (You are => u R , For You => 4U…)
- nadměrné používání VELKÝCH PÍSMEN
- používání jednoduchých obrázků v tzv. “znakové grafice“ nebo “ASCII grafice” (některé ukázky viz závěr článku)
- pro českou komunitu je typické nepoužívání diakritiky a používání anglických (i méně obvyklých) zkratek.

Phreakři / Phrackeři

Skupiny *phreaks* (ph=phone, freaks=podivíni) a *phrackers* (ph=phone a crackers) jsou další subkulturou crackerů a jejich činnosti jsou zaměřeny na vnikání do telekomunikačních systémů a obecněji na krádež telefonní služby (napichování služby, hovory na účet někoho jiného nebo telekomunikační firmy) a na sběr a využívání ukradených telefonních informací (čísla tel. karet, domácí tel. čísla, apod.). Hackeři se od této skupiny distancují.

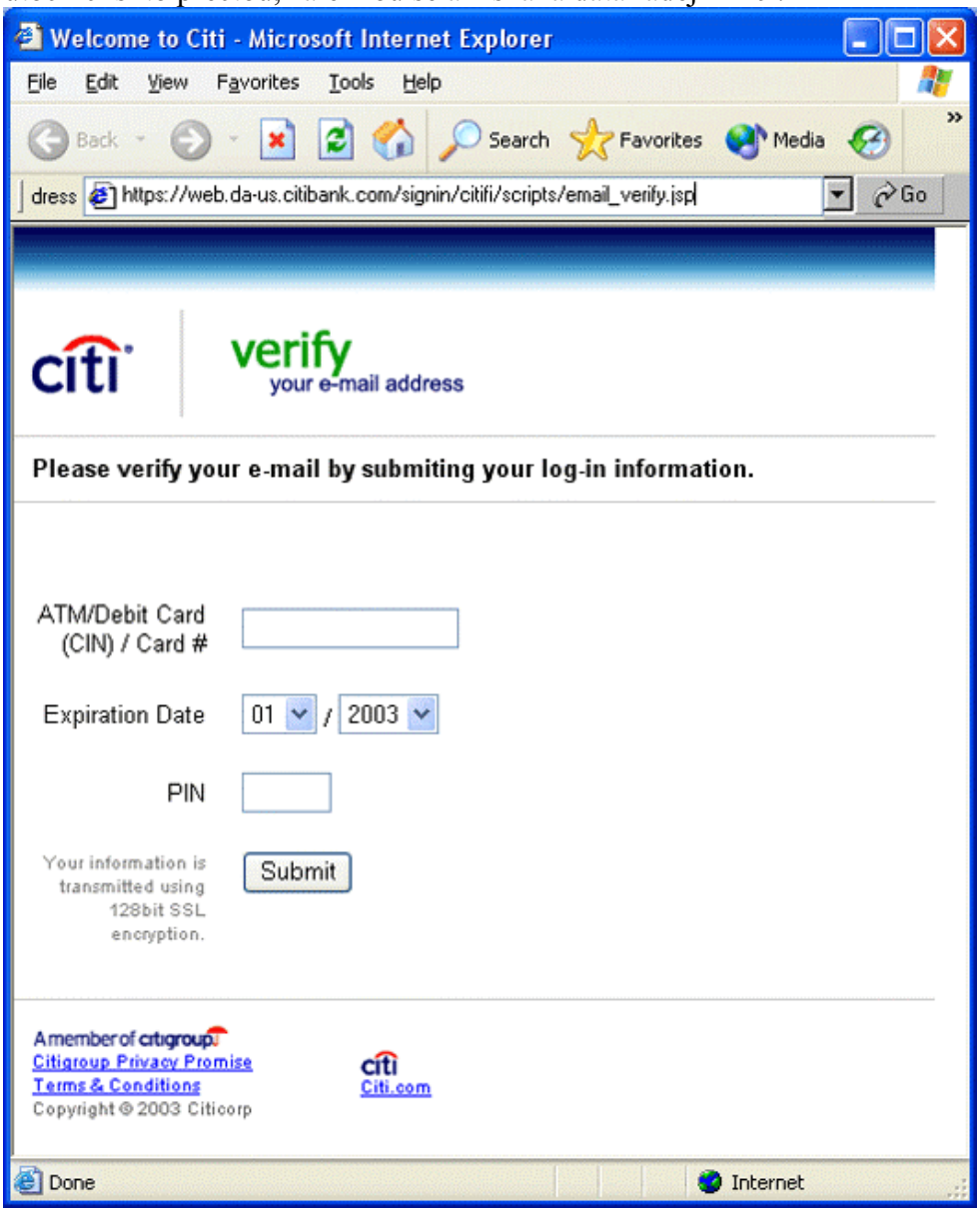
Stránky jedné ze slovenských skupin najdete http://hysteria.sk/phreak/ .



Obr. 2 - Rhybářský e-mail

Rhybáři a rhybaření (Phishing)

Phishing historicky navazuje na aktivity phracekrů, těžiště jejich zájmu nejsou čísla telefonních karet, ale krádež obecnějších privátních citlivých informací patřících jedinci. Těmito údaji mohou být především údaje o platební kartě (nejběžnější objekt zájmu) nebo krádež přístupového jména a hesla, s jejichž pomocí lze na dálku manipulovat s bankovním kontem. Hlavním metodou phishingu je sociální inženýrství a vzhledem k tomu proti němu vlastně neexistuje dobře fungující automatická ochrana. Nejčastěji je prováděn pomocí e-mailů (ale i pomocí falešných webových stránek), které vypadají naprosto legitimně a mají snahu vypadat oficiálně – správná adresa odesílatele (na první pohled), veškeré formální náležitosti jsou také splněny, a obsah, který vás žádá např. o potvrzení nebo doplnění vašich bankovních údajů…. Pokud však odpovíte a do e-mailu vložíte svá data – jste chyceni do sítě rhybářů. Obraně proti phishingu je v současné době věnována značná pozornost. Dokonce současný americký prezident Bush zařadil boj proti němu do svého volebního programu a slibuje podepsat návrh zákona určující mj. relativně přísný způsob potrestání pro každého, kdo vlastní cizí přihlašovací údaje s cílem způsobit trestný čin. Předpokládá zřejmě, že útočníci si to přečtou, zaleknou se a získaná data raději zničí.



Obr. 3 – Link z předchozího rhybářského e-mailu – Račte vyplnit ☺ !

Američané (ale samozřejmě i my ostatní) si musí zatím pomoci sami. Lze například využívat službu proti-rhybářského serveru, který provozuje skupina APWG (Anti-Phishing Working Group). Na tomto serveru naleznete řadu zajímavých informací, rad a můžete zde nalézt i archív e-mailů, které do této oblasti patří
http://www.antiphishing.org/phishing_archive.htm

Další desítky příkladů rhybářských e-mailů najdete na mailfrontieru:
http://www.mailfrontier.com/threats/advisories/threat_index.html (odtud byl také převzat náš příklad na obrázku č.2 a č.3).

Lamy

Možná se vám stalo, že vás již někdo nazval lamou. Lamou rozumíme člověka, který je v nějakém určitém oboru nešikovný, začínající, vše kazící. Lama je počeštěná verze anglického výrazu lammer (resp. *lamer*). Původ označení *lammer / lamer* pravděpodobně vznikl ve skateboardovém slangu jako synonymum pro *luser* (pochází z loser = ztracená existence, poražený). Slovo lame má pak tyto významy: chromý, kulhavý, nepřesvědčivý, neuspokojivý, zchromit, zmrzačit..., ale v počítačovém slangu označuje především osobu, která získává ze serverů data, ale nikdy žádné nenahrává a nikomu neposkytuje. Lammerem je v komunitě pohrdáno, je protikladným označením k pojmu **elita** nebo **guru** (komunitou uznávaný expert pro konkrétní oblast např. VMS, Linux, grafiku, ….). Lamou jsou nazýváni také lidé, kteří se až moc často ptají na různé triviálnosti.

Obr. 4 – Lama (fotomontáž Petr Vondruška)

V češtině má však slovo lama především význam pojmenování zvířete podobného velbloudu. Oba významy se proto začaly v řeči naší mladé generace prolínat. A tak mohly vzniknout nádherné věty: *Já jsem ale lama obecná. Ty jsi jak lama vikuňa.*

Objevují se i výrazy odvozené jako např. výraz "lamaismus", což je synonymum pro skutečně lamerský způsob života, myšlení apod. nebo "lamerka", což sice může být příslušnice ženského pohlaví, která nic neumí, ale dá se tím s úspěchem nazvat i nějaký starý, již nevyhovující hardware (zvuková karta, grafická karta, síťová karta apod.)

Citace některých lamerů najdete na nedávno otevřené stránce http://www.lamer.cz/ . Za všechny zde uvedené výroky alespoň jeden :

Lamer je prostě ten, kdo si myslí, že ssh klíč může být ukryt pod rohožkou …

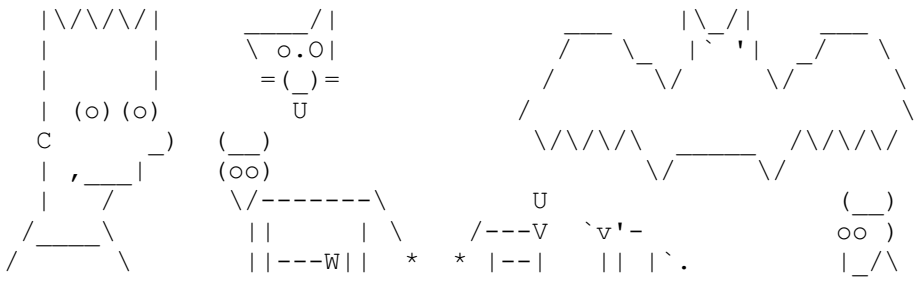
Ale pozor - lamou můžou některé výše uvedené skupiny nazývat všechny ostatní, kteří nejsou přímo v jejich komunitě, a to bez ohledu na skutečné schopnosti takto označených.

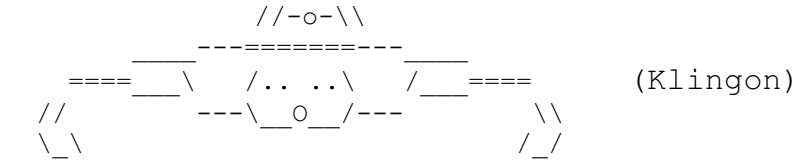
Hackerem snadno a rychle (rada pro lamy)

Jak je vidět, stát se hackerem není jednoduché. Chcete-li se však cítit hackerem mezi lamami, doporučuji místo studia informačních systémů začít především osvojením si slovníku hackerů. Psát a mluvit jako hackeři – to řadu lam oslní a vybuduje vám pověst hackera, guru apod. Pokud jde o kvalitní hackerský výkladový slovník, pak asi nejznámější a nejcitovanější je od Erica S. Raymonda - The New Hacker's Dictionary. Slovníků se prodalo již více jak jeden milión kusů (!) a za USD 28 si jej můžete pořídit v prestižním nakladatelství The MIT Press (http://www-mitpress.mit.edu).

Pokud nechcete za slovník platit, můžete si stáhnout sice méně prestižní, ale také rozsáhlý a pro výše uvedený účel bohatě vyhovující slovník z adresy http://www.catb.org/esr/jargon/html/go01.html nebo méně přehledný od již zmíněného Erica Raymonda: =JARGON FILE, VERSION 4.2.3, 23 NOV 2000 = http://jargon.exobit.org/jargon.html .

Chcete-li být považováni za hackera, můžete také začít vkládat do rozesílaných e-mailů grafické ASCII obrázky, jako např.





Závěr

Jak je z výše uvedeného textu patrné, není jednoduché se vyznat ve spletité síti hackerských vztahů, jejich skupin a na nich parazitujících a navazujících undergroundových a víceméně zločinných skupin. Nejčastější chybou médií je nesprávné a nespravedlivé použití pojmu hacker na všechny, kteří způsobují lidem a počítačovým firmám různé druhy ztrát (finanční, prestižní, …). Snad tento článek přispěje k částečnému pochopení rozdílů mezi těmito komunitami a k používání přesnějšího označení a zařazení příslušného jedince ke správné skupině.

C. Přehledy v oblasti IT bezpečnosti za poslední rok
Jaroslav Pinkava, PVT a.s.

Čtenář Crypto-Worldu, který sleduje i novinky uváděné na jeho webových stránkách, měl možnost se seznámit s řadou dokumentů, které se zabývají celkovou situací v IT bezpečnosti a to z různých hledisek. V následujícím přehledu uvedeme nejdůležitější momenty, které se v těchto přehledech objevily tak, aby čtenář měl možnost dát si tyto výsledky do těch souvislostí, které právě jej zajímají. Týká se to postupně šesti citovaných zpráv (viz literatura), které byly zveřejněny v průběhu posledních měsíců. Zprávy pocházejí od organizací různého typu (státních i soukromých) a každá umisťuje své těžiště do trochu jiné polohy, tj. rozsah i zaměření jednotlivých zpráv nejsou samozřejmě srovnatelné. Přesto ve svém souhrnu poskytují velice zajímavý a informačně bohatý pohled.

Článek je psán formou určité rešerše. Přitom v komentářích je např. vynecháván popis struktury respondentů (odstavce 1. a 2.) a vzhledem k rozsahu článku samozřejmě celá řada dalších podrobností. Problematika informační bezpečnosti dnes zahrnuje velice širokou škálu okruhů a získat v ní určitý celkový přehled není už vůbec jednoduchou záležitostí.

1. CSI - Computer Security Institute - San Francisco

Každoroční zprávu připravuje CSI ve spolupráci s FBI (kanceláře San Franciso). Zpráva byla zveřejněna v květnu 2004.

Klíčové závěry:

- Klesá neoprávněné používání počítačových systémů (podle velikosti finančních ztrát v dolarech, ztrát, které vznikly ne základě bezpečnostních průniků).
- Oproti loňskému roku nejdražší počítačová kriminalita vzniká odepřením služby (tato situace vzniká například v momentu, kdy určité webové stránky jsou mimo provoz v důsledku virové hrozby nebo jsou to přímo tzv. DOS = Denial of Service útoky, které jsou často směrovány na konkrétní organizaci prostřednictvím zahlcení webovského či poštovního serveru atd.).
- Procento organizací, které hlásí počítačové narušení zákonů za uplynulý rok kleslo. Hlavním důvodem jsou obavy z negativní publicity.
- Většina organizací provádí nějakou formou hodnocení svých nákladů na bezpečnost, přitom 55 procent z nich používá návratnost investic, 28 procent používá interní index návratnosti (IRR - Internal Rate of Return) a 25 procent používá přidanou hodnotu (NPV - Net Present Value).
- Přes 80 procent organizací provádí bezpečnostní audity.
- Většina organizací neprovádí outsourcing příslušných aktivit v oblasti počítačové bezpečnosti. U těch organizací, které takovýto outsourcing provádí, je procento takovýchto aktivit nízké.
- Podstatná většina organizací považuje školení zvyšující bezpečnostní povědomí za důležitá, ačkoliv průměrný respondent (ze všech odvětví) si myslí, že organizace neinvestuje v tomto směru dostatečně.

Zajímavý je pohled na členění procenta organizací dle rozpočtu (IT) na bezpečnost.

- více než 10 % rozpočtu dává na bezpečnost 8 % organizací;
- 6 až 10 % dává 15 % organizací;

- 1 až 5 % rozpočtu dává 46 % organizací;
- méně než 1 % dává 16 % organizací;
- neuvádí 14 % organizací.

Ekonomický pohled na bezpečnost se uplatňuje stále tvrději. Příslušní bezpečnostní manažeři musí velice pečlivě zdůvodňovat svůj rozpočet a to čistě z ekonomického hlediska. Zajímavý je také pohled na rozčlenění používaných bezpečnostních technologií:

Biometrie:	11 %
Systémy PKI:	30 %
Čipové karty či jiné tokeny (jednorázová hesla):	35 %
Šifrování souborů:	42 %
Systémy prevence průniků:	45 %
Účty, logování heslem:	56 %
Šifrování dat během přenosu:	64 %
Detekce průniků:	68 %
Serverová kontrola přístupů:	71 %
Firewally:	98 %
Antivirový software:	99 %

2. Australian High Tech Crime Centre

Dokument **Australian Computer Crime and Security Survey** poskytuje obdobný pohled jako výše uvedený materiál CSI - vychází z obdobné koncepce doplněné některými dalšími otázkami. To vše samozřejmě při pohledu na praxi v Austrálii. Zpráva byla zveřejněna v dubnu 2004 a týká se trendů posledních 12 měsíců.

Jako **klíčové** uvádí australská zpráva následující momenty:

- Větší počet organizací se potýká s následky elektronických útoků (49 % v roce 2004 oproti 42 % v roce 2003).
- Většina útoků pocházela z vnějšího prostředí (mimo organizaci), 88 % proti 36 % z vnitřního prostředí (v roce 2003 ale bylo z vnějšího prostředí 91 % útoků).
- Nejčastější formou elektronických útoků byly viry, červy a trojské koně. Byly největší příčinou finančních ztrát a celkem se na ztrátách podílely 45 %.
- Další nejčastější příčinou finančních ztrát byly krádeže laptopů a zneužití přístupu do počítačové sítě či zdrojů počítačové sítě.
- Průměrné roční ztráty, které vznikly díky elektronickým útokům, počítačové kriminalitě či neoprávněným přístupům vzrostly oproti předchozímu roku o 20 %.
- Procentuálně hlásí CNII (národní informační infrastruktura) v průměru větší procento elektronických útoků (50 %) a s tím souvisejících ztrát oproti organizacím mimo CNII (42 %).
- Připravenost organizací k ochraně svých IT systémů se zlepšila v následujících třech faktorech - používání informačních bezpečnostních politik, směrnic a postupů; využívání bezpečnostních norem či příruček; větší počet organizací zaměstnává zkušený, školený a kvalifikovaný či certifikovaný personál.
- Avšak oproti roku 2003 uvádí menší procento organizací (5 % oproti 11 % v minulých letech), že se dostatečně vypořádaly se všemi aspekty počítačové bezpečnosti.

- Potřeba většího chápání či podpory aspektů bezpečnosti IT starším managementem byla důležitá pro 45 % respondentů.
- Jako dva nejčastěji uváděné faktory, které umožnily škodlivé elektronické útoky jsou neošetřené slabiny softwaru (patche) a neodpovídající úroveň proškolení personálu ve vztahu k bezpečnostním praktikám.
- Největší výzvou jsou a nejvíce problémů způsobily organizacím respondentů změny názorů a chování uživatelů ve vztahu k novým hrozbám a zranitelnostem.
- Důsledkem je nedostatečná připravenost organizací respondentů k ochraně svých systémů, jejichž zranitelnost vzniká díky frekventovanějším a různorodějším hrozbám a útokům.

Ve zprávě je uvedeno následující členění z hlediska používaných bezpečnostních technologií (uvedeme čísla vztahující se k roku 2004).

Biometrie	5 %
integrita souborů	25 %
čipové karty, jednorázové tokeny	33 %
digitální ID, certifikáty	46 %
šifrování souborů	47 %
systémy k detekci průniků	53 %
vícenásobně používaná hesla	53 %
šifrovaný login, relace	58 %
VPN	74 %
fyzická bezpečnost	94 %
kontrola přístupu	95 %
firewall	95 %
antivirový software	100 %

3. NIST - National Institute for Standard Technology - USA

Ve zprávě je uvedeno, že je zpracována za rok 2003, zveřejněna byla v červnu 2004. Cíl má tato zpráva odlišný od výše uvedených dvou zpráv - záměrem je především podat informaci o činnosti divize NIST - Computer Security Division. Výsledky této činnosti se objevují v celé řadě organizačních modelů a také jimi byla publikace některých norem a příruček (pro vládní organizace v USA). Pro čtenáře je materiál zajímavý uceleným přístupem k řešení otázek bezpečnosti IT a to z celé řady hledisek - volba vhodných organizačních struktur pro podporu navržených opatření (mj. prostředky certifikace a akreditace, prostředky kontroly atd.), dále volba programů v oblasti bezpečnosti (např. vládní program pro čipové karty, program pro hodnocení kryptografických modulů - CMVP, Cryptographic Standard Toolkit) a samozřejmě cílenou publikací standardizačních dokumentů.

V následující tabulce je dán přehled materiálů, které vznikly díky programům NIST:

SPECIAL PUBLICATIONS
SP 800-43 System Administration Guidance for Windows 2000 Professional November 2002
SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices November 2002
SP 800-49 Federal S/MIME V3 Client Profile November 2002
SP 800-55 Security Metrics Guide for Information Technology Systems July2003
SP 800-59 Guideline for Identifying an Information System as a National Security System August 2003

DRAFT NIST SPECIAL PUBLICATIONS
SP 800-35 Guide to Information Technology Security Services October 2002
SP 800-36 Guide to Selecting Information Technology Security Products October 2002
SP 800-37 Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems October 2002, June 2003
SP 800-38B Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode October 2002
SP 800-38C Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality September 2003
SP 800-50 Building an Information Technology Security Awareness and Training Program May 2002
SP 800-56 Recommendation on Key Establishment Schemes January 2003
SP 800-57 Recommendation on Key Management January 2003
SP 800-61 Computer Security Incident Handling Guide September 2003
SP 800-64 Security Considerations in the Information System Development Life Cycle (originally was SP 800-4A) October 2002

DRAFT FEDERAL INFORMATION PROCESSING STANDARDS
FIPS 199 Standards for Security Categorization of Federal Information and Information Systems May 2003
NIST INTERAGENCY REPORTS
NIST IR 7046 A Framework for Multi-Mode Authentication: Overview and Implementation Guide August 2003
NIST IR 7030 Picture Password: A Visual Login Technique for Mobile Devices July 2003
NIST IR 6887 Government Smart Card Interoperability Specification (GSC-IS), v2.1 July 2003
NIST IR 7007 An Overview of Issues in Testing Intrusion Detection Systems June 2003
NIST IR 6981 Policy Expression and Enforcement for Handheld Devices May 2003
NIST IR 6985 COTS Security Protection Profile - Operating Systems (CSPP-OS) (Worked Example Applying Guidance of NISTIR-6462, CSPP) April 2003

INFORMATION TECHNOLOGY LABORATORY BULLETINS WRITTEN BY THE CSD
October 2002 Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
November 2002 Security For Telecommuting And Broadband Communications
December 2002 Security of Public Web Servers
January 2003 Security Of Electronic Mail
February 2003 Secure Interconnections for Information Technology Systems
March 2003 Security For Wireless Networks And Devices
June 2003 ASSET: Security Assessment Tool For Federal Agencies
July 2003 Testing Intrusion Detection Systems
August 2003 IT Security Metrics

Přehled publikací však nedává úplný pohled na aktivity divize CSD. V rámci daného článku není samozřejmě možné se jednotlivými problematikami detailně zabývat, proto ještě bude uveden výčet okruhů problematik, kterými se CSD zabývá a které jsou ve zprávě obsaženy.

A. Organizační struktury:
- The Information Security and Privacy Advisory Board (ISPAB)
- The Federal Information Systems Security Educators' Association (FISSEA)
- The Computer Security Resource Center (CSRC)
- The Small Business Administration (SBA)
- The Federal Computer Security Program Managers' Forum (Forum)

B. Security Management and Guidance:
- SECURITY CERTIFICATION AND ACCREDITATION (C & A) PROJECT
- SENSITIVITY STANDARDS AND GUIDELINES
- SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS
- PRACTICES, CHECKLISTS, & IMPLEMENTATION GUIDES
- COMPUTER SECURITY EXPERT ASSIST TEAM

- AUTOMATED SECURITY SELFEVALUATION TOOL – ASSET

C. Security testing and Metrics
- National Voluntary Accreditation Laboratory Accreditation Program
- Cryptographic Module Validation Program

D. Security Research and Emerging Technologies
- WINDOWS 2000 PROFESSIONAL SYSTEMS ADMINISTRATION GUIDANCE
- IT SECURITY CHECKLISTS FOR COMMERCIAL IT PRODUCTS
- MULTI-CARD TECHNOLOGY
- GOVERNMENT SMART CARD PROGRAM
- MOBILE AGENT SECURITY
- MOBILE DEVICE SECURITY
- WIRELESS SECURITY STANDARDS
- ICAT Metabase
- INTERNET PROTOCOL SECURITY (IPsec)
- AUTHORIZATION MANAGEMENT AND ADVANCED ACCESS CONTROL MODELS
- VOICE OVER INTERNET PROTOCOL (VoIP) SECURITY ISSUES
- AUTOMATED SECURITY TESTING
- CRITICAL INFRASTRUCTURE PROTECTION GRANTS PROGRAM
- SCALABLE QUANTUM INFORMATION NETWORK

E. Cryptographic Standards and Applications
- CRYPTOGRAPHIC STANDARDS TOOLKIT
- BIOMETRIC TECHNOLOGIES
- KEY MANAGEMENT
- MODES OF OPERATION FOR BLOCK CIPHER ALGORITHMS
- E-AUTHENTICATION
- E-GOV IDENTITY MANAGEMENT INFRASTRUCTURE
- SECURING E-GOV APPLICATIONS WITH CRYPTOGRAPHY

Přitom každá z uvedených problematik by si zasloužila samostatný článek.

4. Deloitte

Zpracovaný přehled "Global Security Survey" je teprve druhým v pořadí (první byl v roce 2003), firma však hodlá pokračovat v založené tradici a zpracovávat obdobné přehledy každoročně. Totiž důležitost informační bezpečnosti je podle Deloitte rostoucím faktorem, který se stává kritickým z celé řady hledisek.

Cílem přehledu je napomoci účastníkům (kteří zpracovali podklady pro přehled) vyhodnotit stav informační bezpečnosti jejich organizace v širších souvislostech, ve vztahu k srovnatelným finančním institucím ve světě, jak se tento stav mění v průběhu let atd.
Přehled je zpracován ve spolupráci s finančními institucemi, jejichž činnost zasahuje do následujících geografických regionů: Severní Amerika, Evropa, Blízký Východ, Afrika (EMEA), pacifická Asie (APAC), latinská a střední Amerika (LACRO).

Klíčové závěry přehledu jsou formulovány v následujících deseti bodech.

1) Velikost instituce není rozhodujícím faktorem. Vnímání bezpečnosti probíhá napříč celým spektrem institucí všech velikostí. Většina chápe správu rizik jako klíčovou otázku své obchodní činnosti. Větší finanční instituce však k informační bezpečnosti přistupují z pochopitelných důvodů profesionálněji. Outsourcing bezpečnostních funkcí lze také očekávat spíše u větších finančních institucí. Z hlediska personální struktury z přehledu vyplývá, že instituce se snaží dodržovat

poměr jeden bezpečnostní profesionál na 650 uživatelů (v loňském roce to bylo na 1000 uživatelů).

2) Ve vztahu k legislativním a regulačním požadavkům provádí globální finanční instituce politiku, která má za cíl co nejlepší přizpůsobení se bezpečnostním normám a používání lepších praktických postupů. Většina finančních institucí se snaží demonstrovat úspěšnou implementaci kontrolních mechanizmů bezpečnosti ve vztahu k příslušným regulacím a zákaznickým požadavkům. Velká pozornost je věnována implementacím požadavků, které vyplývají z normy ISO 17799 a samozřejmě požadavků legislativy (Sarbanes-Oxley, European Data Protection Directive, Gramm-Leach-Billey Act).

3) Vytvoření programů pro hodnocení efektivnosti bezpečnostních opatření ve vztahu k zaměstnancům napomáhá při identifikaci a ochraně organizace. Rostoucí povědomí zaměstnanců ve vztahu k ochraně dat a k bezpečnostním cílům je nezbytnou složkou pro naplnění regulačních a legislativních požadavků.

4) Souběžně s naplněním požadavků nové legislativy a regulačních opatření a s cílem minimalizace nákladů je hodnota IT aktiv strategickou prioritou mnoha finančních institucí. Efektivnost postupů pro správu aktiv spolu s obchodními strategickými záměry vytváří vhodný základ pro úspěch na trhu a růst produktivity.

5) Přesun aktivit do oblastí s nižšími náklady na pracovní sílu a nižšími náklady na výrobní prostředky je zatím ve vztahu k bezpečnosti a důvěrnosti málo hodnoceným faktorem. Většina finančních institucí se v tomto směru potýká s problémem nalezení a získání kvalifikovaného personálu s dostatečnými zkušenostmi a kompetencemi v oblasti bezpečnosti.

6) Z hlediska soutěže trhu (při náhlých změnách situace) je na finanční instituce kladen i požadavek určité strategické flexibility. 11. září 2001 bylo v tomto směru určitým testem.Aby finanční instituce byly schopné vytvářet přizpůsobivé strategie, musí mít dobře zhodnoceny otázky rizik, ale být i schopny rychlých změn. Souvisí s tím i například geografické rozmístění pracovišť, řídícího a kritického personálu atd.

7) Zatímco bezpečnostní politiky vychází v převážné míře z požadavků odpovídajících legislativ, je nezbytné, aby v instituci existovaly bezpečnostní strategie obsahující potřebná výhledová hlediska. Cílem je připravit se na nezbytné budoucí adaptace, které vyplynou z možných změn - technologických, regulačních a konkurenčních.

8) Proces správy slabých míst (vulnerabilty management) začíná nabývat reálných rozměrů. Instituce se začínají více zabývat možnými bezpečnostními trhlinami, je to i díky rostoucímu počtu červů a virů v posledním roce. Je v této souvislosti poukazováno i zjištěnou skutečnost, že organizace, které mají implementovánu správu slabých míst signalizují o 90 % méně úspěšných útoků než organizace, které investovaly pouze do systému na detekci průniků.

9) Konsolidace finančních služeb je v některých situacích brána jako prvořadá nezbytná záležitost, ale o bezpečnosti se pak uvažuje často až mnohem později.

10) Bezpečnost se přesouvá z "válečné" místnosti do místnosti "řídící" (board). Tedy přestává být chápána jako mimořádný prostředek a stává se běžným postupem pracovního myšlení. Budoucí svět bud pravděpodobně více prosperující nikoliv však více bezpečný.

K některým uváděným číslům:

Celkem 83 % respondentů uvádí, že jejich systém byl v uplynulém roce nějakým způsobem kompromitován. Přitom 21 % hlásí vnější útok (v roce 2003 to bylo 16 %), dále 13 % hlásí útok zevnitř (v roce 2003 to bylo 10 %) a 49 % hlásí útoky z obou zdrojů (oproti 13 % v roce 2003).

5. Verisign

Verisign zveřejňuje své "Internet Security Intelligence Briefing" čtvrtletně. Cílem je podat informace o trendech ve vztahu k Internetu - nárůst, využívání, bezpečnost a podvody. Orientuje se na tzv. kritické služby infrastruktury Internetu. Jimi jsou - DNS (Domain Name systém), SSL digitální certifikáty, řízení bezpečnostních služeb (Managed Security Services) - to je např. monitoring a správa firewallů, systémů pro detekci průniků a další síťové služby - konečně sem jsou zahrnovány služby vztahující se k ochraně plateb a ochranám před podvody (Payments and Fraud Protection Services). Poslední taková zprava byla zveřejněna v červenci 2004.

V popisu hrozeb a existujících trendů je zejména poukázáno na rostoucí počet útoků prostřednictvím multivektorových červů. Tito červi simultánně využívají různé slabiny a mají delší životnost než obvyklí červi. Jiným trendem je rychlé využití oznámených slabin, velice rychle se objeví software, který tyto slabiny využije. Je tedy nezbytné, aby instituce aplikovaly patche dodavatelů pokud možno co nejrychleji.

E-mailové šíření červů je stále velice populární (zmiňovány jsou Novarg, MyDoom, Lovegate, Netsky). Autoři červů používají stále rafinovanější triky k tomu, aby donutili příjemce mailů otevřít přílohu mailu. Pro podniky je však stále velkým problémem "den-nula", tj. den, kdy započne šíření červa a kdy ještě neexistuje jeho podchycení antivirovým softwarem. Také jeden ze současných trendů v mailech - otevírání zadních vrátek, které později umožní vstup červu (třeba i od jiného autora) do daného počítače. Nebezpečí spočívá také v tom, že celé části zdrojových kódů škodlivých červů jsou veřejně přístupné a poměrně snadno upravitelné. Hacker pak lehce nachází jejich nová využití.

V následující tabulce jsou uvedeny nejčastější útoky v 1. a 2. čtvrtletí 2004.

1.čtvrtletí 2004

1 POP3 Authorization overflow attempt
2 Microsoft Windows ASN.1 Library buffer overflow
3 RPC mountd UDP export request
4 HTTP Client URL Argument Overflow Attack
5 WEB-PHP content-disposition memchr overflow
6 SMTP Content-Transfer-Encoding overflow attempt
7 Mail message contains suspicious ZIP file
8 WWW General cgi-bin Attack
9 Shell interpreters used to execute commands on Web servers
10 TCP port scan has been detected

2. čtvrtletí 2004

1 Telnet Server 2000 rexec password overflow attempt
2 DDOS shaft synflood
3 ASN.1 BER Length Overflow Heap Corruption
4 ICMP Ping Flood

5	SYN Flood
6	RPC DCOM overflow attempt
7	RPC portmap request NFS UDP
8	PCT Client_Hello overflow attempt
9	MS-SQL version overflow attempt
10	RPC mountd UDP export request

Roste počet útoků na jedno zařízení. Červencová zpráva se dále podrobně zabývá novým trendem "Phishing" - viz článek Pavla Vondrušky v tomto čísle Crypto-Worldu. Dále je konstatován stálý růst v obchodování prostřednictvím Internetu. Zajímavá je tabulka zachycující situaci v podvodných transakcích (procento rizikových transakcí) a které země jsou "nejnebezpečnější".

Top Countries By Percentage of Fraudulent Transactions

Cameroon	100.00%
Nigeria	95.79%
Indonesia	92.81%
Slovenia	92.02%
Brunei Darussalam	90.74%
Israel	90.48%
Kenya	90.05%
Lebanon	89.50%
Romania	88.68%

Pro nás je zajímavé, že na čelních místech se zde vyskytuje např. Slovinsko, Izrael či Rumunsko.

6. ATT

Zpráva společnosti AT&T: "Network Security: managing the risk and opportunity" (zpracovaná ve spolupráci s Economist Intelligence Unit) jako jediná v článku není pravidelně vydávana. Přesto obsahuje řadu zajímavých informací, zabývá se především bezpečností sítí a jejími klíčovými momenty. Některé údaje jsou uvedeny v následujících tabulkách.

Otázka: Jaké tři hrozby považujete za nejpodstatnější pro Vaši firmu dnes (a za dva roky)?

Odpovědi:

Viruses and worms	87 (92)
Hackers	53 (50)
Accidental damage	33 (40)
Spam	31 (36)
Internal sabotage	25 (27)
Power outages	14 (19)
Denial of service attacks	19 (17)
Competitor espionage	17 (12)
Terrorist attacks	15 (9)
Natural disasters	8 (8)
Other	2 (1)

Jaké procento Vašeho IT rozpočtu je věnováno na bezpečnost?

rok 2002	9 %
rok 2003	11 %
rok 2004	13 %

Jaké bezpečnostní chyby jste udělali v posledním roce?

- otevření přílohy e-mailu od neznáme osoby	78 %
- zvolení svého jména či data narození jako bezpečné heslo pro vstup do firemní sítě	29 %
- vstup do firemní sítě na veřejném místě a zapomenutí se odlogovat	17 %
- sdílení firemního hesla s někým mimo firmu	9 %

7. Shrnutí

Celkově - čím více máme informací, čím je větší přehled o konkrétních případech a o důsledcích narušení počítačové bezpečnosti, čím organizace efektivněji řeší otázky počítačové bezpečnosti, tím je pravděpodobnější dosažení žádoucí IT bezpečnosti. Rozšiřující se znalostní báze opírající se o obdobně zpracované přehledy je v tomto směru vysoce efektivním nástrojem.

8. Literatura:

[1] 2004 CSI/FBI Computer Crime And Security Survey, by Lawrence.Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, May 2004
http://www.gocsi.com/forms/fbi/pdf.jhtml

[2] Australian Computer Crime and Security Survey, 2004
http://www.auscert.org.au/download.html?f=114

[3] NIST - Computer Security Division - 2003 Annual Report
http://csrc.ncsl.nist.gov/publications/nistir/IR7111-CSDAnnualReport.pdf

[4] Deloitte's 2004 Global Security Survey,
http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_SecuritySurvey2004_051704.pdf

[5] Verisign Internet Security Intelligence Briefing, July 2004
http://www.verisign.com/static/006583.pdf

[6] AT&T. Network Security: managing the risk and opportunity
http://www.business.att.com/emea/english/whitepaper

D. Letem šifrovým světem

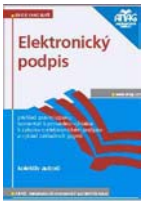
Průběžně můžete sledovat novinky a zajímavosti ze světa kryptografie, informační bezpečnosti a příslušných standardů na http://www.crypto-world.info/news/index.php Novinky v tomto měsíci pro vás již tradičně vybrali : Vlastimil Klíma, Jaroslav Pinkava, Tomáš Rosa, Libor Tvrdík a Pavel Vondruška.

Kryptologické osobní stránky

22.7.2004 byly na stránky Crypto-Worldu přidány odkazy na osobní stránky kolegů Vlastimila Klímy a Tomáše Rosy. Vlastík Klíma k tomu za sebe i kolegu Tomáše Rosu dodává, že na nich naleznete téměř všechny jimi vydané publikace a to v elektronické podobě, prezentace, přednášky apod. Mezi nejnovějšími také například seriál "Kryptologie pro praxi", vycházející přes rok ve Sdělovací technice. Pokud by Vás zaujala nějaká dřívější práce a nenaleznete ji tam, postačí si o ni autorům napsat!
Ing.Tomáš Rosa: http://crypto.hyperlink.cz/
RNDr. Vlastimil Klíma : http://cryptography.hyperlink.cz/

Kniha Elektronický podpis uvolněna k volnému stažení

Po dohodě s nakladatelstvím ANAG si mohou návštěvníci naší www stránky stáhnout kompletní knihu autorů Bosáková, Vondruška, Kučerová, Peca: Elektronický podpis - přehled



právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů. Kniha vyšla v březnu roku 2002 v nakladatelství ANAG. Je potřeba si uvědomit, že od vydání knihy došlo již celkem ke třem novelám zákona o elektronickém podpisu č.227/2000 Sb. Aktuální citace je *Zákon č.227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb., č.517/2002 Sb. a č. 440/2004 Sb.* (http://www.crypto-world.info/pravo/podpis/z_227_2000.pdf).

Tyto změny je potřeba vzít do úvahy při používání knihy. Výše uvedené novely se týkají zejména kapitoly 2. Kapitoly 3 až 8 zůstávají (až na drobné změny) zatím stále platné.
Knihu (525 kB) lze stáhnout zde http://crypto-world.info/kniha/elektronicky_podpis.pdf
Na stránce http://crypto-world.info/kniha/ dále naleznete opravu strany 106, link na nakladatelství a recenze knihy.

Záhadná páska z Prahy

Doprovodný materiál (forografie pásky) http://crypto-world.info/paska/

Záhadná páska z Prahy , 1. díl - Nález uschované pásky

Pro „staré“ čtenáře Crypto-Worldu připomínka článku z roku 2001 – nyní však doplněno a rozšířeno a především ve třetím díle je odhalen zdroj textu, který v článku z roku 2001 uveden není. Pro ostatní čtenáře populárně zpracovaný příběh nálezu atypické pásky. Máte tak zde možnost se seznámit s odhalováním s ní spojené záhady. Ve třech dílech můžete sledovat krok za krokem postup odhalování textu, který je uložen na pásce. Páska byla nalezena při opravě

Dětského domu v Praze. Zúčastníte se i hledání zařízení na kterém byly takovéto pásky vytvářeny a dozvíte se k čemu vlastně sloužily. V první části se dozvíte o nálezu pásky a o neúspěšném testování jedné z možných hypotéz řešení ....
Zveřejněno: iDnes, Technet : 21.7.2004
http://technet.idnes.cz/hw/zahadna_paska040721.html
http://crypto-world.info/paska/cast1.pdf (pro zájemce dávající přednos pdf formátu)

Záhadná páska z Prahy , 2. díl - Rozluštění textu

Pokračování odhalování záhady spojené s páskou, která byla nalezena při opravě Dětského domu v Praze. V tomto díle je popsáno, jak byl získán text, který je na pásce zakódován ....
Zveřejněno: iDnes, Technet : 22.7.2004
http://technet.idnes.cz/hw/zahadna_paska2_040722.html
http://crypto-world.info/paska/cast2.pdf (pro zájemce dávající přednos pdf formátu)

Záhadná páska z Prahy , 3. díl - Zařízení

Poslední část, krátkého seriálu, který je věnován odhalování záhady spojené s páskou, která byla nalezena při opravě Dětského domu v Praze. V tomto díle je popis zařízení na kterém se také pásky používaly a další detaily k textu, který je na pásce...
Zveřejněno: iDnes, Technet : 23.7.2004
http://technet.idnes.cz/hw/zahadna_paska040723.html
http://crypto-world.info/paska/cast3.pdf (pro zájemce dávající přednos pdf formátu)

Řešení cvičných úloh ze strany tři:

Cvičná úloha č.1 :	MORSE	(Morseovka, tečka: A, čárka : B)
Cvičná úloha č.2 :	RAXYQ	(text psán pozpátku)
Cvičná úloha č.3 :	MORSE	(Morseovka, tečka : malé písmeno, čárka: velké písmeno)

O čem jsme psali v létě 2000 - 2003

Crypto-World 78/2000

Příloha :
10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha :
priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě)

Crypto-World 78/2002

Crypto-World 7-8/2003

Příloha: "zábavná steganografie" (steganografie.doc)

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze **jméno a příjmení, titul**, pracoviště (není podmínkou) a **e-mail adresu** určenou k zasílání kódů ke stažení sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Spojení

Adresa pro běžnou komunikaci, zasílání příspěvků k otištění, informace
pavel.vondruska@crypto-world.info
pavel.vondruska@ct.cz