Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 4/2003 **15. duben 2003**

4/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(420 e-mail výtisků)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Úvodní komentář

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.
http://crypto-world.info/vondruska/

Vážení čtenáři,

Dovolte, abych vám poděkoval za váš stálý a dlouhotrvající zájem o náš e-zin. Počet registrovaných odběratelů neustále roste. Poprvé jsme překonali počet 420 ! Při průměrné velikosti e-zinu cca 600 kB to však znamená rozeslat každý měsíc přibližně 250 MB dat. Chtěl bych vás poprosit o jistou spolupráci v udržování aktuální databáze odběratelů. Rozesílání dat na adresy, které již neexistují, nebo jsou nedostupné, nebo existují, ale byly majitelem opuštěny a jsou z tohoto důvodu neustále přeplněné (např. adresy na post.cz, volny.cz…), nebo nastavené politiky příjemce nedovolují hromadné rozesílání - je zbytečné a jen námi provozovanou službu zpomaluje. V současné době mám nastaven systém tak, že pokud je adresa 3x za sebou nedostupná (z libovolného důvodu!), je automaticky vyjmuta z mailing-listu. Pokud se tak stane a Vy máte stále zájem o rozesílání, prosím o pochopení tohoto opatření a novou registraci…

Od srpna 2002 do dnešního dne bylo takto ze seznamu vypuštěno 67 adres. Prosím tedy nejen o zaregistrování, ale i oznámení v případě, že e-zin již nechcete odebírat. Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán (především pokud žádáte z jiné adresy než která byla registrována ☺).

Prosím také o oznámení změny v případě, že měníte zaměstnání nebo svoji osobní e-mailovou schránku. Zasílání na opuštěné schránky zbytečně systém zatěžuje. Děkuji za pochopení a spolupráci.

Možná, že jste již někteří z vás zaregistrovali stěhování domovské stránky Crypto-Worldu ze staré adresy http://www.mujweb.cz/veda/gcucmp/ na adresu novou. Na staré adrese sídlil e-zin od prosince roku 1999 a nastřádalo se zde úctihodné množství dat (celkem 60 MB). Jako každé stěhování i toto bylo trochu nostalgicky spojeno se vzpomínkami. Nicméně jsem uznal, že je potřeba najít „důstojnější doménu“, a tak vás nyní zvu na návštěvu domény nové http://crypto-world.info/ , kde ode dneška (13.4.2003) Crypto-World sídlí. Tuto doménu mi pro potřeby e-zinu Crypto-World poskytl zdarma český informační server **CZECHIA** (http://www.czechia.com). Touto cestou jejím pracovníkům upřímně děkuji.

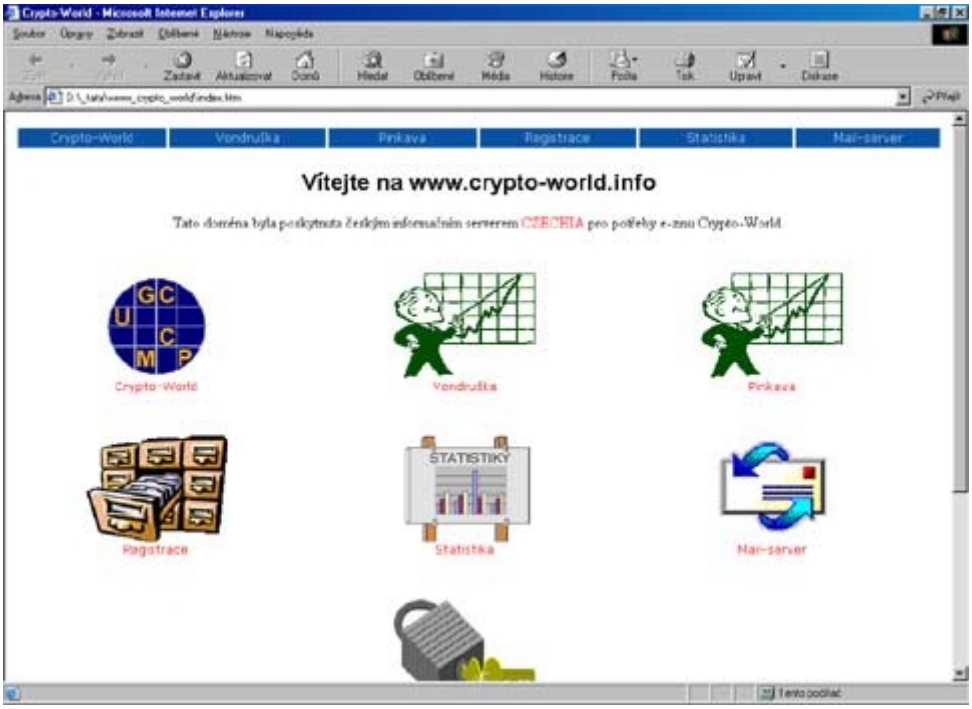
Na nové adrese zatím příliš nového nenajdete. Prakticky jsem pouze stihl přestěhovat stará data, opravit řadu nefungujících odkazů (z důvodu, že na novém serveru je potřeba dodržovat „velká“ a „malá písmena“ v odkazech) a provést pár drobných změn.

Z hlavní stránky (její náhled je uveden na následující straně) lze volat osobní stránky hlavních autorů Crypto-Worldu (Vondruška , Pinkava). Tyto sekce lze volat také samostatně jako: http://crypto-world.info/vondruska/ , http://crypto-world.info/pinkava/ .

Zpřístupnil jsem velice podrobné volání statistických informací o serveru a jeho návštěvnících (http://crypto-world.info/stats/).

Z hlavní stránky se lze také přímo zaregistrovat k odběru e-zinu (http://crypto-world.info/dotaz/dotaz2.html/) .

Majitelé poštovních schránek *@crypto-world.info si zde také mohou přes www rozhraní vyzvednout svoji poštu.



Jako člen výboru BITIS jsem sem přestěhoval i domácí stránku tohoto sdružení. (BITIS - Sdružení pro bezpečnost informačních technologií a informačních systémů) http://crypto-world.info/bitis/ .

Uvědomuji si, že za přepracování by stála i poněkud archaická stránka samotného Crypto-Worldu, plná nelogických otevírání oken a odkazů na články a konference, které již bohužel neplatí. Omlouvám se, ale síly mi již nestačily, a tak snad někdy v létě dojde na důkladnou revizi….

Co však již teď mohu slíbit, je obnovení tradičních podzimních soutěží. V tomto roce se bude soutěž skládat z většího množství lehkých úloh, které se budou zabývat nejen kryptologií, ale budou zde i úlohy na hacking, logické úlohy, bude nutné cracknout programy, scripty apod. Na letošní podzimní soutěž se již teď důkladně připravuji a v šuplíku mám několik zajímavých úkolů…

Nezapomeňte tedy, že ode dneška je nová domovská adresa vašeho oblíbeného e-zinu:

http://crypto-world.info/ (alias http://cryptowolrd.info)

Závěrem mi dovolte, abych vám popřál hezké prožití velikonočních svátků a bohatou pomlázku.

B. E-válka v zálivu (a okolí…)

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.
http://crypto-world.info/vondruska/

Od vydání Crypto-Worldu 3/2003 do dnešního dne (13.4), kdy připravuji další číslo, se toho ve světě hodně stalo a změnilo. Začala např. válka v Iráku a zdá se, že vlastně také již skončila (alespoň britská letadlová loď „balí“ a pluje domů).

Jaká to vlastně byla válka? Během svého studia na gymnáziu jsem se učil v hodinách občanské nauky, že války se dělí na obranné a útočné, později jsem se na vysoké škole v hodinách marxismu-leninismu dozvěděl, že jsou války spravedlivé a nespravedlivé, nyní jsem se v televizi dozvěděl, že se jedná o válku preventivní. Tato válka měla být podle prohlášení amerických generálů a politiků *jako žádná jiná před ní*. Ve válce bylo použito nejmodernějších zbraní, nejmodernější naváděcí a telekomunikační techniky, široce byla využita mediální propaganda. Vnější projevy této války jsou však dost podobné válkám minulým – rozbombardovaná města, tisíce mrtvých vojáků, stovky mrtvých civilistů, nemocnice plné zraněných nevinných lidí, nedostatek potravin, léků, zničená a rozvrácená země…. V čem tedy byla tato válka tak jiná? Hodnocení nechám na povolanějších. Já se ve svém článku soustředím pouze na tři malé detaily z této války, momenty, které souvisí s tím, co jsem nazval v nadpise e-válkou.

I. e-propaganda - Ganda worm

Krátce po zahájení války v Iráku varoval v časopise Computer Times Charles Cousins, marketingový ředitel pro Asii společnosti Sophos (se sídlem v Británii), která se specializuje na antivirové programy, před virem nazývaným Ganda worm (W32/Ganda-A). Virus proniká na počítače uživatelů pod pláštíkem ankety o válce v Iráku, láká uživatele PC např. na americké družicové snímky iráckého bojiště a obrazovými montážemi prezidenta George W. Bushe, které lze použít jako spořiče obrazovky. Vzhledem k zájmu o konflikt existuje velké riziko jeho šíření, uvedl Cousin. Allan Bell z kalifornské společnosti Network Associates zaměřené na ochranu obchodní elektronické korespondence, nevyloučil irácký původ viru. Řekl : "Irák a další méně rozvinuté země mají rovněž vysoce zkušené programátory schopné vytvářet složité viry“.

Nechávám na čtenářích, aby se sami pokusili nalézt odpověď na starou právnickou otázku „Quo bonum ?“ (komu prospěšné).

Nabízím i možnost ztotožnit se s jednou z těchto tezí:

- iráčtí hackeři se snažili poškodit data běžných uživatelů na počítačích „koalice“ a bojovali tak v řadách Saddama Husajna
- snahou výrobce viru je rozsévat nenávist proti Iráčanům (pokud vám irácký vir smaže data z disku, bude pro vás přijatelnější potrestání „viníka“)
- poněkud absurdní může být domněnka, že by mohlo jít o nepřímé potrestání těch, kteří se zajímají o válku v Iráku a dychtí po datech, která by mohla hypoteticky diskreditovat koalici
- ???

Pro někoho může být výše uvedený příběh naprostou banalitu, maličkostí, která snad s válkou nemá nic společného, ale může se stát, že někdo jiný (nebo třeba některá bezpečnostní složka) vyhodnotí takovou událost jinak, např. jako signál, že e-válka začala.

II. e-propaganda a e-boj : al-Džazíra

Druhý příběh je příběhem propagandy, který je ukončen ne-li e-bojem, pak určitě e-útokem.

Katarská televize al-Džazíra byla během války zdrojem informací a pohledů z druhé strany konfliktu – arabského světa. Vysílala nejen propagandistické šoty, ale často také odvysílala zprávu, která do té doby nebyla v ostatních médiích zveřejněna. Během války se stalo pravidlem, že teprve po zveřejnění jejích záběrů zničených civilních cílů byly tyto zásahy přiznány anglo-americkou koalicí. Fotografie mrtvých Iráčanů a plačících dětí, které byly dostupné na webovské stránce této televize, přejala média celého světa. Záběry válčících stran z přístavu Umm-Kasr této televize dva dny poté, co byl oznámeno dobytí přístavu, mohlo být jistě spojencům také nepříjemné. Ostatně několikanásobné ohlášení válečného úspěchu dobytí tohoto přístavu spojenci zavdalo příčinu ke vtipu, který byl rozesílán e-mailem i v Čechách:

„Anglo-americká koalice oznámila dobytí města Umm-Kasr. Je to už čtvrtý Umm-Kasr dobytý od začátku války.“

Je jasné, že ze strategického hlediska bylo potřeba takovýto zdroj informací umlčet. A tak se stalo, že katarská televize al-Džazíra zmizela ve středu 26.3.2003 z Internetu (http://www.aljazeera.net). Její webové stránky údajně napadla skupina počítačových pirátů podepsaná jako "patrioti, jednotky domobrany a kyber svobody". V hackerském světě je tato skupina zcela neznámá a jednalo se o její první „úder“. 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!!!“.

III. e-boj : Racal Jaguar V

Poslední příběh je již příběhem o konkrétním e-boji. Boji, který (pokud je to pravdou) rozhodl válku v Iráku. Z historie je jasné, že pravou skutečnost se nedozvíme příliš brzy a budeme muset čekat na otevření vojenských archívů 10 (20,50) let. Obdobně jako informace o

prolomení Enigmy (šifrovací stroj německého wermachtu) za druhé světové války byla dostupná až po desítkách let a některé detaily byly zveřejněny až po 40 letech.

Příběh začíná v roce 1985, kdy Saddam Husajn nakupuje od firmy Racal na ukázku první kus šifrovací radiové stanice **Racal Jaguar V.**

Jedná se o vojenský bezpečný radiový systém, toto zařízení obsahuje dva základní bezpečnostní mechanismy: šifrování hovorů (scramble) a neustálou změnu frekvence (určenou klíčem), frekvence se mění 200x za vteřinu a útočníkovi se tím výrazně ztěžuje zachycení přenášené zprávy. Testy na irácké straně pravděpodobně dopadly dobře a v roce 1989 kupuje Irák od svých britských spojenců nejprve 13 kusů těchto zařízení a koncem téhož roku dalších 2000 kusů (v hodnotě 52 milionů US dolarů). Připomeňme, že tehdy byl režim Saddama Husajna bezvýhradně podporován americkou a britskou vládou ve svém boji proti Iránu a nebyl důvod v bezpečnost těchto zařízení nevěřit. Toto dřívější spojenectví připomíná jeden velice trpký vtip, který doputoval do mé e-mail schránky (tyto e-maily a vtipy samozřejmě patří také do kategorie e-propaganda):

- *Pane prezidente Bushi, máte důkazy, že Irák má zbraně hromadného ničení?*
- *Ano, máme schované stvrzenky o zaplacení.*

V případě šifrovacího zařízení Jaguár V si neschovali Britové jen stvrzenky, ale jak uvidíme dále, pravděpodobně ještě něco více…

Příběh pokračuje začátkem dubna 2003. Americká vláda připravuje veřejné mínění na dlouhé boje, které čekají spojenecká vojska při obléhání Bagdádu. Vstup do Bagdádu je očekáván s napětím, veřejnost očekává prudké a nemilosrdné boje. Američané se bojí o své chlapce, kteří budou krvácet v ulicích města.

Stalo se však něco zcela neočekávaného. V pondělí 7.4.2003 Fred Swan, velitel amerického neviditelného bombardéru, který se právě nachází nad pouští v západním Iráku, dostává rozkaz zničit cíl. Nadiktovány jsou mu souřadnice a pak je z velitelské věže doplněn rozkaz, který upřesňuje cíl a význam jeho mise: „ Kill Saddam Hussein“. Osobně sice nevěřím, že by o konkrétním cílu mise věděla kontrola na naváděcí věži, ale převzal jsem toto tvrzení z „Pentagon reporters“, kterému to v telefonickém interwiev tvrdil přímo sám Fred Swan.

Dvanáct minut po tomto rozkazu jsou shozeny čtyři speciální dvě tuny liber vážící bomby z výšky 6000 metrů na restauraci ve čtvrti Mansour, kde se měl Saddam nacházet.

Bomby byly naváděny pomocí satelitu a cíl zasáhly naprosto přesně. Na místě zůstal jen kráter o velikosti 60 stop.

Zatím stále není jasné, zda byl Saddam při útoku skutečně zabit. Britské zdroje se domnívají, že ne, CIA oznámila úspěšný zásah, ale později nebyl potvrzen. V každém případě byl účinek naprosto ohromující, obrana Bagdádu se zhroutila. Následující den vjíždí americké tanky téměř bez odporu do města a do konce týdne je jasné, že je konec války. Zbývají jen drobné, z vojenského hlediska již bezvýznamné cíle. V ulicích se přestalo bojovat, ale začíná se rabovat, a také začíná vyřizování účtů, vytváří se domobrana. Američané nezasahují, neboť vítězové se nechtějí vměšovat do vnitřních záležitostí irácého lidu.

Vraťme se k tomu, jak se vlastně Američané dozvěděli místo schůzky Saddama Husajna se svými nejbližšími. Na setkání měla být údajně projednávána obrana Bagdádu a případně odchod do exilu. Zpočátku se objevilo tvrzení, že informace byla získáno na základě rozluštění komunikace nejvyššího iráckého velení. Později již bylo jen oznámeno, že informace byla získána ze tří nezávislých důvěryhodných zdrojů.

Snažil jsem se proto získat další detaily k možnému luštění irácké komunikace. První vyhledávání googlem (Saddam AND jaguar) dopadlo nečekaně dobře – 8000 odkazů. Bohužel odkazy se týkaly nákupů aut značky Jaguár bývalým diktátorem. Teprve hledání Saddam AND jaguar AND code je úspěšné a vrací články, které potvrzují, že při určení místa výskytu Saddama bylo využito zpráv předávaných šifrovým systémem Racal Jaguar V:
http://www.guardian.co.uk/Iraq/Story/0,2763,932739,00.html ,
http://www.cipherwar.com/lists/politech/msg00905.html
http://www.nypost.com/news/worldnews/72979.htm.

Prolomení komunikace se podle těchto zdrojů podařilo Britům a informace o možném luštění byla předána Američanům krátce před začátkem války. K dispozici jsou zde dvě hlavní hypotézy. První tvrdí, že šifrování bylo zastaralé a šlo prolomit, druhá tvrdí, že dodaná zařízení byla Brity modifikována a nebyla bezpečná již v roce 1989. Prvou hypotézu vyslovuje Steven Aftergood (a senior intelligence technology researcher at the Federation of American Scientists). Tvrdí, že technologie byla dvacet let stará a není tedy divu, že šlo použité kryptologické algoritmy prolomit. Druhá hypotéza vyplývá z tvrzení některých vojenských bezpečnostních expertů (např. Rupert Pengelly), kteří tvrdí, že britská vláda by koncem devadesátých let nevydala exportní povolení na vývoz bezpečného šifrovacího zařízení, kdyby si nebyla jista, že toto zařízení je možné prolomit (např. speciální „vývozní úpravou“ – tzv. zadní vrátka).

Skutečná válka, která probíhala za přispění e-války, prakticky skončila. Americký úspěch v závěrečných bojích, kdy jakoby mávnutím kouzelného proutku se zhroutila obrana Bagdádu, umožnila úspěšná e-válka - zachycení důležité zprávy a její následné vyluštění (hypotéza I.) nebo včasné dešifrování (hypotéza II.).

A e-propaganda? Je zřejmé, že koalice si po celou dobu války uvědomovala její veliký vliv a snažila se jej využít ve svůj prospěch. I po válce bude dále využívána. Příkladem může být okamžitá realizace spojeneckého televizního vysílání v Iráku. K irácképu národu tento čtvrtek v televizním přenosu promluvili i představitelé vítězné koalice.

Celý článek zakončím posledním vtipem ze série e-propagandy (tentokráte pacifistického hnutí), která byla rozesílána minulý týden po českém Internetu:
„Po ukončení bojů bude Irák rozdělen na zóny. Budou to zóny Natural, Natural plus a Diesel.“

C. Začátek roku 2003 protokolu SSL nepřeje….

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.
http://crypto-world.info/vondruska/

Jako kdyby se kryptologové domluvili na společném termínu publikování svých prací, které ukazují na slabosti a problémy v protokolu SSL. V únoru a březnu tak byly krátce za sebou publikovány tři útoky, každý založený na zcela odlišném principu.

I. Jako první se v únoru objevila práce švýcarského týmu prof. Vaudenaye, jeho útok je založen na doplňování CBC módu (http://lasecwww.epfl.ch/memo_ssl.shtml).

II. Začátkem března byla zveřejněna práce od týmu Boneh-Brumley ze Stanfordu. Ten využil dnes již klasický útok postranním kanálem - timing-attack
(http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf).

III. Třetí místo a pomyslnou bronzovou medaili (kdybychom měřili pořadí publikování) získal český tým Klíma-Pokorný-Rosa. Jejich útok na SSL vedený postranním kanálem se řadí mezi útoky zvané - bad version oracle. Práce je dostupná v archívu IACR (http://eprint.iacr.org/2003/052/) .

Pokud bychom hodnotili předchozí tři útoky nikoliv dnem zveřejnění, ale závažností daného útoku, pak pomyslné zlato získá bezesporu český tým.

K hodnocení jejich úspěchu si dovolím ocitovat slova předního světového kryptologa Davida Wagnera (University of California Berkeley):

.....But then, the recent Klima-Pokorny-Rosa paper shows how even just a tiny crack can lead to subtle, totally unexpected attacks. Who would have thought that SSL's version rollback check (two bytes in the input to the modular exponentiation) could enable such a devastating attack? Not me. .....

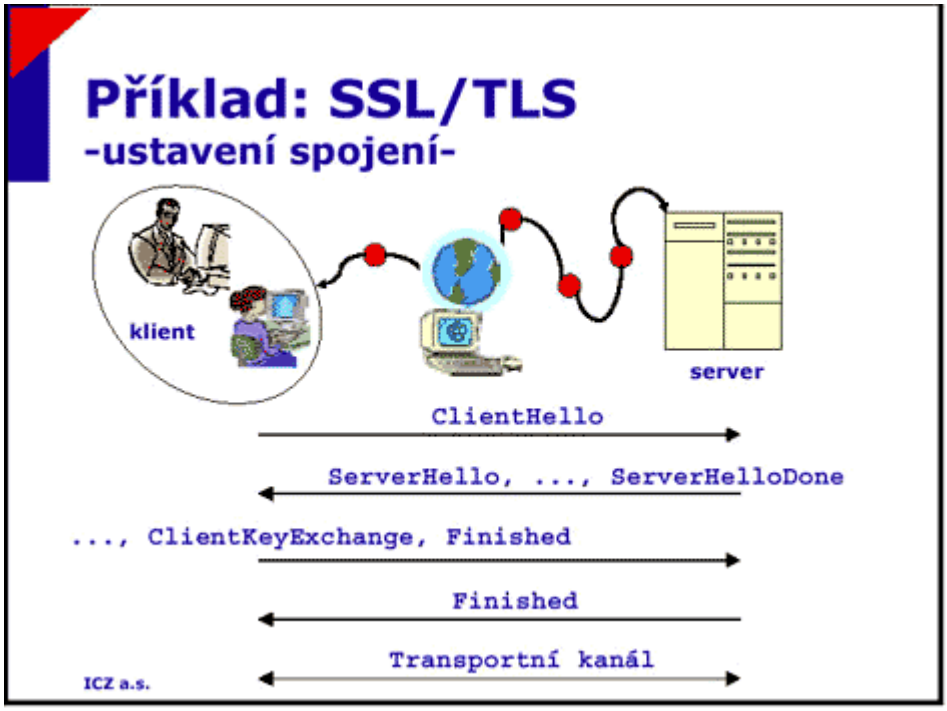
Česká média tento výsledek příliš nekomentovala a ani firma ICZ nezahájila vlastní mediální kampaň k tomuto bezesporu cennému výsledku. Jistě se při této příležitosti vkrádá vzpomínka na rok 2001, kdy byl ze „stejné kuchyně“ zveřejněn útok na „elektronický podpis“ (uložení klíčů pro PGP). Pokud jde o mne, nelíbila se mi bombastická kampaň v roce 2001 a nelíbil se mi obsah článků řady tehdejších periodik, kde se veřejnost dozvěděla pouze to, že zaváděný elektronický podpis byl rozbit a je nebezpečný a bude vést k odložení možnosti podávat daňová přiznání apod… ale nyní s odstupem času si uvědomuji, že byl ve veřejnosti vyvolán zájem o tuto oblast a že tento zájem je pro obor potřeba. Proto mne trochu mrzí, že letošní (podle mě důležitější výsledek) trochu zapadl a snažím se alespoň touto cestou jej připomenout.

Útok na SSL/TLS – Klima-Pokorny-Rosa (bad version oracle)

Dne 18.3.2003 zveřejnila firma ICZ a.s. tiskovou zprávu „Čeští kryptologové objevují slabinu v šifrované internetové komunikaci a navrhují její řešení“ (http://www.icz.cz/onas/tisk14.html). Nalezená slabina umožňuje realizovat úspěšný útok, zaměřený na protokoly SSL/TLS (Secure Sockets Layer a Transport Layer Security) . Útok na uvedené protokoly, popsaný týmem českých kryptologů (RNDr. Vlastimil Klíma, Ing. Tomáš

Rosa, Ing.Ondřej Pokorný) umožňuje tuto ochranu zcela prolomit a rozšifrovat chráněnou komunikaci.

Útočník na základě zachycené zašifrované transakce postupně sestavuje podle matematického algoritmu vlastní výzvy, které pak zasílá serveru. Na každou takovou výzvu server reaguje, čímž útočníkovi poskytuje tzv. postranní informaci. Z těchto informací získá útočník hodnotu hlavního symetrického klíče daného spojení (tzv. premaster-secret). Poté jednoduše dešifruje zachycenou komunikaci.



Doprovodný obrázek je z přednášky ing.T.Rosy na MFF UK 9.4.2003

Typický internetový server, který používá 1024bitovou šifru RSA, podlehne útoku v polovině případů po méně než 13.34 milionech výzev. V testovacím prostředí bylo dosaženo rychlosti zpracování 67.7 výzev za vteřinu. Každý druhý útok by tedy měl být úspěšný cca do 55 hodin.

Útok se dá zařadit mezi útoky postranním kanálem. Po technické stránce se jedná o využití Bleichenbacherova útoku na PKCS# 1, verzi 1.5. V SSL je zavedena ochrana proti tomuto útoku . Práce českých kryptologů je cenná právě v nápadu, jak modifikovat dotazy tak, aby z odpovědí serveru na předkládané zprávy dostali informace, které vedou na základě Bleichenbacherova útoku k známému prolomení šifry RSA. Další cenný výsledek byla modifikace útoku tak, aby bylo možné použít menší počet nutných dotazů a tím bylo dosaženo času útoku, který je v praxi reálný. Závěr práce se pak zabývá vypracováním detailní metodiky k odstranění možnosti takovéhoto útoku. Technické podrobnosti lze nalézt ve výzkumné kryptologické zprávě na adrese http://eprint.iacr.org/2003/052/ .

D. Eliptická kryptografie a kvantové počítače

Jaroslav Pinkava, PVT a.s.
http://crypto-world.info/pinkava/

Je dnes již všeobecně známou skutečností, že potenciál kvantových počítačů (v případě, že se podaří překonat existující technologické překážky) umožňuje pro řadu matematicky náročných problémů konstruovat algoritmy, které dokáží řešit tyto problémy s výrazně nižší výpočetní složitostí. Například úloha faktorizace velkých čísel je pomocí klasických výpočetních postupů řešitelná pouze algoritmy jejichž složitost je v nejlepším případě subexponenciální (metoda Number Field Sieve pracuje zhruba s výpočetní složitostí $O(\exp(c \log^{1/3} n))$. Oproti tomu Shor v [2] nalezl algoritmus pro kvantový počítač, který řeší daný problém v polynomiálním čase.

Při srovnatelné úrovni bezpečnosti (viz [7], též článek autora NIST – dokument Key Management – Crypto-World 02/2003) je potřebná délka klíče pro kryptografické algoritmy založené na eliptických křivkách (ECC) výrazně nižší než je délka klíče pro algoritmy založené na úloze faktorizace resp. klasického diskrétního logaritmu (RSA, DSA). Nejlepší algoritmy pro řešení eliptického diskrétního algoritmu (Pollardova ρ-metoda) pracují s exponenciální složitostí. Připomeňme, že například v současné době pro více méně obvykle používanou úroveň bezpečnosti, která odpovídá 128 bitové délce klíče pro symetrickou šifru, je adekvátní délkou klíče pro algoritmus RSA – 3072 bitů, zatímco pro eliptické algoritmy to je pouze 256 bitů.

Z těchto důvodů je určitě zajímavé podívat se na otázku, jak obstojí eliptické křivky proti kvantovým počítačům. Článek [1] autorů Proos, Zalka (Waterloo University - mimochodem zde na univerzitě pracuje známá silná pracovní skupina zabývající se problematikou eliptické kryptografie – Menezes, Teske, Vanstone a další - svou úlohu zde sehrává i napojení na blízkou firmu Certicom) si položil za cíl provést odpovídající analýzu.

Autoři tedy implementovali Shorův kvantový algoritmus pro diskrétní logaritmus na speciální případ grupy eliptické křivky (konkrétně se jedná o křivky v prvočíselném tělese, ale v zásadě jsou výsledky přenositelné i na druhý důležitý případ – eliptické křivky v binárních tělesech). Ukázali, že k rozbití kryptografického klíče 160 bitové eliptické křivky je zapotřebí využít kvantový počítač, který má zhruba 1000 qubitů. Přitom pro faktorizaci 1024 modulu algoritmu RSA je zapotřebí 2000 qubitů. Poslední číslo vyplývá z práce [8], kde autor ukázal, že pro optimalizované implementace Shorova algoritmu je zapotřebí 2n qubitů (n je délka čísla, které faktorizujeme).

Hlavním problémem, se kterým se autoři článku potýkali, byla otázka implementace rozšířeného Eukleidova algoritmu, ten je zapotřebí pro výpočet inverze v multiplikativní grupě.

V postupech, které jsou v článku uvedeny, nebyla zvažována paralelizace výpočtů – zde mohou ležet další cesty k optimalizaci algoritmu.

Podstatou Shorova algoritmu je vlastně úloha nalezení řádu prvku a konečné grupy G. Problém eliptického diskrétního logaritmu lze formulovat následovně.

Mějme eliptickou křivku E nad tělesem GF(p), kde p je velké prvočíslo. Základem logaritmu je bod P na eliptické křivce E, řádem bodu P je jiné velké prvočíslo q, tj. $qP = 0$,

kde O je bod křivky ležící v nekonečnu. Úloha diskrétního logaritmu na eliptické křivce pro dané *d* je pak úloha nalezení jiného bodu Q na eliptické křivce E a to takového, že Q = dP. Autoři v článku pak ukazují, jak lze převést úlohu diskrétního logaritmu (řešenou kvantovým algoritmem) na posloupnost posuvů v grupě. Ukazují pak, jak (kvantově) realizovat rozšířený Eukleidův algoritmus, tak aby jeho jednotlivé části byly reversibilní (což je podstatnou a nezbytnou součástí každého kvantového algoritmu).

Následující tabulka dává porovnání složitosti kvantového algoritmu pro faktorizaci a kvantového algoritmu pro výpočet eliptického diskrétního logaritmu. Je zde uváděn jak počet nezbytných qubitů, tak i "pracovní" výpočetní složitost algoritmů, zde uvedený parametr čas znamená vlastně počet součtů "1-qubitů".

	Faktorizace (RSA)			**Eliptický diskrétní logaritmus** (ECC)	
n	počet qubitů	čas	n	počet qubitů	čas
512	1024	$0{,}54 \cdot 10^9$	110	700	$0{,}5 \cdot 10^9$
1024	2048	$4{,}3 \cdot 10^9$	163	1000	$1{,}6 \cdot 10^9$
2048	4096	$34 \cdot 10^9$	224	1300	$4{,}0 \cdot 10^9$
3072	6144	$120 \cdot 10^9$	256	1500	$6{,}0 \cdot 10^9$
15360	30720	$1{,}5 \cdot 10^{13}$	512	2800	$50 \cdot 10^9$

Kryptografické algoritmy versus kvantové počítače - zatím stále je to jen hra ve smyslu co by bylo kdyby. Postupy jsou známé a pro malé počty qubitů již byly implementovány. Z teoretického hlediska nejsou známy žádné skutečnosti, které by ukazovaly na nereálnost konstrukce kvantových počítačů i s vyšším počtem qubitů, tedy i takovým počtem qubitů, který je dostatečný pro výše popsané algoritmy. Praxe v realizaci kvantových počítačů však zatím neslaví takové úspěchy jako teorie.

Literatura

[1] Proos, John; Zalka Christof: Shor´s discrete logarithm quantum algorithm for eliptic curves, University of Waterloo 2003
[2] Shor, P.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Press, pp.124-134, Nov. 1994, quant-ph/9508027
[3] Zalka, Ch.: Fast versions of Shor´s quantum factoring algorithm, quant-ph/9806084
[4] FIPS 186-2, http://csrc.nist.gov/encryption/dss/fr000215.html
[5] Josza, R.: Quantum algorithms and the Fourier Transform, Proc. R.Soc.Lond. A, 1998, 454, pp.323-337, také quant-ph/9707033
[6] Josza, R.: Quantum factoring, discrete logarithms, and the hidden subgroup problem, Computing in Science and Engineering March/April 2001
[7] Key Management Guideline, http://csrc.nist.gov/CryptoToolkit/tkkeymgmgt.html
[8] Beauregard, S.: Circuit for Shor´s algorithm using 2n + 3 qubits, quant-ph/0205095

Poznámka:
reference quant-ph... je odkazem na archív Quantum Physics:
http://xxx.lanl.gov/archive/quant-ph .

E. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 11. Archivace elektronických dokumentů

Jaroslav Pinkava, PVT a.s.
http://crypto-world.info/pinkava/

1. Úvod

V minulých pokračováních seriálu byla řeč o existenci čtyř protokolů, které se zabývají problematikou ověřování (validation) certifikátů. Byly popsány vlastnosti protokolu OCSP (online Certificate Status Protocol), dále protokolu CSVP (Simple Certificate Validation Protokol) a protokolu CVP (Certificate Validation Protocol). Zbývá popsat protokol v rámci DVCS (Data Validation and Certification Server Protocols). Tento protokol [1] vznikl v rámci pracovní skupiny PKIX, výsledné rfc.3029 však bylo zařazeno do kategorie experimentálních a není tedy běžnou internetovou normou. Na jeho vzniku se podíleli pracovníci firem Entrust (C.Adams a R.Zuccherato), Baltimore (M. Zolotarev) a P. Sylvester z EdelWeb SA.

Posledně jmenovaný je hlavním zpracovatelem projektu **OpenEvidence** (http://www.openevidence.org) v rámci 5. rámcového programu IST (Information Society Technologies - http://www.cordis.lu/ist/). Cílem tohoto projektu je příprava technologie, která umožní - v podmínkách splňujících odpovídající legislativní požadavky - zajišťovat dlouhodobou platnost elektronických dokumentů, zajišťovat a rozpoznávat platnost elektronických podpisů resp. časových značek. Je bohužel smutnou pravdou, že ač důležitost problematiky je již dlouho rozpoznána, probíhá odpovídající vytváření normativních dokumentů velice pomalu a neodpovídá praktickým potřebám. Projekt OpenEvidence si klade za cíl provést kombinací technologií popsaných v rfc.3029 a rfc.3161 [5], přitom pro vytváření časových značek mají být používána tzv. linkovací schémata (linking schemes – viz [13]). Výstupem projektu je otevřený software (Open source) – klientská i serverová část.

2. Protokol DVCS

Dokument rfc.3029 popisuje vlastnosti severu DVC (Data Validation and Certification Server) a protokoly používané pro komunikaci s tímto serverem. DVC server je chápán jako důvěryhodná třetí strana, která může být využívána pro vytváření služeb, kde je vyžadována nepopiratelnost (non-repudiation services). Server vytváří určitá potvrzení (ve vztahu k platnosti elektronicky podepsaných dokumentů, certifikátů veřejných klíčů, resp. existencí určitých dat), tato potvrzení nazývá ověřovacími certifikáty (Data Validation Certificates). Tyto certifikáty pak lze použít pro konstrukci příslušných důkazů (platnost a nepopiratelnost elektronických podpisů, lze ověřit, že příslušný uživatel vlastní určitá data, lze ověřit platnost a revokační statut certifikátu veřejného klíče atd.). U uložených dat přítomnost DV certifikátu prokazuje, že příslušný digitálně podepsaný dokument či certifikát veřejného klíče byly platné v čase, který je obsažen v DV certifikátu.

V materiálu jsou definovány 4 typy ověřovacích a certifikačních služeb:
- certifikace vlastnictví (possession) dat (cpd);
- certifikace tvrzení o vlastnictví dat (ccpd);
- ověření platnosti digitálně podepsaného dokumentu (vsd);
- ověření platnosti certifikátu veřejného klíče (vkpc).

Přitom DVC server musí podporovat nějakou podmnožinu těchto služeb a výstupem každé služby je vydání DV certifikátu.

Samotná transakce s DVC serverem začíná přípravou klientské žádosti, tato žádost vždy obsahuje data, jejichž platnost, vlastnictví či správnost je ověřována. Je zvolen vhodný transportní mechanismus (je vhodné využívat mechanismy umožňující zajistit důvěrnost transakce, autentizaci DVC serveru např. pomocí TLS či CMS nebo pomocí šifrování S/MIME).

Server DVC po obdržení žádosti ověří její platnost a provede odpovídající ověřovací postupy. Následně (v případě shody) provede vygenerování DV certifikátu a pošle odpověď, která obsahuje tento certifikát.

Zbývající část rfc obsahuje syntaxi ASN 1 výše popsaných objektů a zpráv.

3. Protokol TAP

V souvislosti s výběrem vhodného ověřovacího protokolu byl diskutován i protokol DVCS. Byl přitom podroben poměrně důrazné kritice. Faktickou příčinou kritiky byla skutečnost, že problematika ověřování platnosti certifikátů (včetně souvisejících otázek) za poslední dva roky značně pokročila. To se však nedalo říci o DVCS problematice, která ustrnula na stavu z počátku roku 2001.

Toto mj. vedlo k návrhu nového protokolu Trusted Archive Protocol (draft-ietf-pkix-tap-00.txt - [2]). Autory protokolu jsou C. Wallace (CygnaCom Solution – dceřiná společnost Entrustu) a S.Chokhani (Orion Security – konzultační firma).

Dokument popisuje službu důvěryhodné archivní autority (TAA – Trusted Archive Authority), která má za cíl vytvořit podporu dlouhodobé nepopiratelnosti pomocí bezpečného uložení (kryptograficky obnovované) informace. Tato služba (TAA) zajišťuje dlouhodobé uchovávání dat pomocí obnovy časových značek. Definuje důvěryhodný archivní protokol (TAP - trusted archive protocol), který umožňuje interakci s TAA.

Entity, které příspívají do archivu se nazývají přispěvatelé; entity, které data naopak vyžadují přístup k datům, či vyžadují odstranění určitých dat, se nazývají žadatelé.

Objekty archivačního procesu jsou v rámci dokumentu členěny následovně:
- archivovaná data - data, která jsou přispěvatelem zasílána TAA;
- archivní známka – objekt generovaný TAA po obdržení dat od přispěvatele a akceptaci jejich archivace. Je zasílána zpět k přispěvateli a lze ji použít k žádosti o vyhledání či odstranění archivovaných dat a asociovaných informací kryptografického charakteru. Známky obsahují : přispěvatelovo DN, časovou značku, datum a čas, kdy

příspěvek TAA obdržela a (nepovinně) vyhledávací informace. Přispěvatel musí ověřit obsah této známky (pro ověření správnosti složení uložených informací v TAA);
- archivní záznam, obsahuje kryptografickou obnovu historie, kterou provádí TAA. Prvotní archivní záznam – to je časová značka, která byla spočtena pro data získaná od přispěvatele. Formát časové značky je definován v rfc.3161. Při každé obnově nově získaný archivní záznam obsahuje předešlou verzi tohoto archivního záznamu a novou časovou značku. Při ověření archivního záznamu je toto ukončeno v momentu, kdy je ověřena původní časová značka.
- archivní soubor (package), to je složený objekt, který minimálně obsahuje archivní známku, archivní záznam a archivovaná data. Může obsahovat další kryptografické informace.

TAA potenciálně může archivovat data v libovolném formátu, je však také možné, že na typ archivovaných dat je kladeno nějaké omezení. Data přispěvatelů mohou obsahovat veškerou potřebnou kryptografickou informaci, mohou obsahovat pouze její část, resp. nemusí obsahovat žádnou.

V rámci protokolu TAP vystupují následující čtyři typy entit : TAA, TSA, klient-přispěvatel a klient-žadatel.
TAA musí zabezpečovat následující služby:
- uchovávání archivovaných dat;
- generování archivních známek (včetně vyžádání časové značky pro archivovaná data);
- periodickou obnovu archivních záznamů;
- uchovávání svěřených kryptografických informací pro verifikaci archivního záznamu (kořen důvěry, certifikáty, CRL, odpovědi protokolu OCSP, certifikáty serveru OCSP atd.);
- přijetí archivního souboru a jeho odstranění;

TAA dále může provádět další nepovinné služby jako např.:
- uchovávání historických kořenů důvěry;
- sběr a ověřování informací ve vztahu k PKI;
- ověřování kryptografických zpráv;

Draft protokolu se opírá (stejně jako rfc.3126 – formáty dlouhodobě platných elektronických podpisů, [4]) o syntaxi CMS (rfc.3369, [3]) a protokol pro časové značky (rfc.3161, [5]). Definuje
- protokol pro přenos dat mezi TAA a klienty;
- objekty, které lze používat k archivaci a uchovávání libovolné kryptografické služby, jako je digitální podpis a k archivaci libovolných nekryptografických dat;

Protokol TAP používá přístup opírající se o obnovu časových značek a tak značně snižuje nároky na stupeň důvěry k TAA vzhledem k integritě archivovaných dat. Jinými slovy, případné modifikace dat v archivních záznamech TAA mohou být detekovány.

TAA se nemusí zabývat archivovanými daty (z hlediska obsahu) a lze ji využít k archivaci jak kryptografických tak i nekryptografických dat. Kryptografická data mohou být buď podepsána či šifrována anebo jsou současně šifrována a podepsána.

Pro podporu dlouhodobého uchovávání elektronických podpisů může přispěvatelem zasílaný soubor obsahovat všechny certifikáty, revokační informace (odpovědi CRL a OCSP)

a také kořen důvěry tak, aby byla usnadněna následná verifikace v libovolném budoucím čase a to bez potřeby obracet se k službám či skladům nebo k jiným zdrojům informací o certifikátech a revokacích.

Pokud pak žadatel používá jiný důvěryhodný zdroj pro kořen důvěry k ověření podpisu a časových značek, pak není nutné opírat důvěru v integritu dat o důvěru v TAA. Autorita časových značek však musí být důvěryhodnou institucí v každém případě.

Požadavky jak přispěvatelů tak i žadatelů mohou být buď podepsány, mohou být ale i neautentizovány či autentizovány jinými prostředky (např. klientská autentizace pomocí SSL/TLS). Požadavky na odstranění části archivu musí být autentizovány. Zprávy TAA jsou vždy podepsány (CMS SignedData – rfc.3369). Odpovědi TAA musí být vždy podepsány a nesmí obsahovat jakýkoliv jiný podpis (kromě podpisu samotné TAA). V odpovědích musí být obsažen certifikát TAA serveru. Mohou zde být i další certifikáty a případná CRL.

Materiál v dalším definuje formáty žádostí (přispěvatelovy, žadatelovy), formáty odpovědí a jejich ASN.1 syntaxi.

Podpisy všech odpovědí TAA musí být ověřovány, přitom postupy se mírně liší v závislosti na druhu prováděné transakce. V dokumentu je dále popsáno využití http jako přenosového protokolu. Žádný konkrétní typ přenosového protokol není však stanoven jako povinný.

V páté kapitole se autoři zabývají některými možnými přístupy ke kontrole archivu. Kontroly obvykle probíhají na základě klientského požadavku (jsou součástí žádosti).

Vzhledem k tomu, že se vlastně jedná teprve o "nultou" verzi draftu, jsou zde některé další momenty práce TAA zatím spíše jen naznačeny. To se týká například problematiky autorizace (kdo a jak má právo používat služeb TAA), nezbytných "bezpečnostních" vlastností TAA – potřebných k tomu, aby TAA mohla fungovat jako důvěryhodná strana (zpracování dokumentace, využívání kontrolních prostředků, fyzické prostředky vhodné pro archivaci, atd.).

4. Transakce v rámci TAP.

(symbolem N jsou označeny nepovinné transakce)

T1. Zaslání požadavku

T11. Přispěvatelova žádost - jméno přispěvatele, data k archivaci,
politika (N), kontroly archivu (N)
T12. Zpracování žádosti v TAA – autentizace a autorizace (N), zpracování případně vyžádaných kontrol archivu, získání časové značky pro archivovaná data, vytvoření archivní známky a archivního záznamu, uložení archivovaných dat, vygenerování odpovědi, která obsahuje archivní známku (popř. i odpovědi o proběhlé kontrole archivu), podpis a zaslání odpovědi;
T13. Odpověď přispěvatelovi – status odpovědi, archivní známka, kontrola archivu (N)
T14. Zpracování odpovědi klientem – ověření podpisu TAA na odpovědi, ověření časové značky z archivní známky, uložení archivní známky pro budoucí použití

T2. Vyhledávání

T21. Požadavek klienta - jméno klienta, archivní známka (resp. informace pro zahájení vyhledávání), kontrola archivu (N);
T22. Zpracování žádosti v TAA – autentizace a autorizace (N), zpracování případně vyžádaných kontrol archivu, získání archivních záznamů a archivovaných dat; vytvoření archivního souboru (obsahuje archivovaná data, archivní známku a archivní záznam), generování odpovědi obsahující archivní soubor, resp. odpověď ke kontrole archivu (N), podpis a zaslání odpovědi;
T23. Odpověď klientovi – statut, archivní soubor, kontrola archivu (N);
T24. Zpracování odpovědi klientem – ověření podpisu TAA na odpovědi, ověření archivního záznamu (včetně všech časových značek).

T3. Odstranění z archivu

T31. Požadavek na odstranění – jméno žadatele, archivní známka (resp. informace pro zahájení vyhledávání), kontrola archivu (N);
T32. Zpracování žádosti v TAA – autentizace a autorizace (N), zpracování případně vyžádaných kontrol archivu, odstranění archivních záznamů a dat, generování odpovědi, která obsahuje archivní známku a případnou odpověď ke kontrole archivu, podpis a zaslání odpovědi;
T33. Odpověď žadateli – statut, archivní soubor, kontrola archivu (N);
T34. Zpracování odpovědi žadatelem – ověření podpisu TAA na odpovědi.

5. Další poznámky

Obecnou situací v oblasti archivace elektronických dokumentů (i v návaznosti na Směrnici EU o elektronickém podpisu) se zabývá článek [7]. Kromě legislativních otázek upozorňuje na některé existující analýzy problematiky ([8], [9], [10]). Mimo jiné je zde také poukazováno na jeden zásadní problém při archivaci, kdy autentizace dokumentu je vázána na elektronický podpis. V takovém případě je integrita dokumentu vázána až na úroveň hodnot jednotlivých bitů. Pokud je vhodné provést transformaci dokumentu (například převod z jednoho formátu na jiný) nelze toto provést bez narušení takto fixované integrity dokumentu. Uchování elektronického podpisu je přitom v některých situacích nezbytné zejména z hlediska nepopiratelnosti. Problém je v některém stupni řešen pro dokumenty ve formátu XML (tzv. metoda kanonizace- [11]). Podmínkami, které musí splňovat řešení archivace elektronických dokumentů se zabývá studie EESSI – Trusted Archival Services (například výběr vhodných formátů dokumentů, nezbytná návaznost na PKI). Autoři doporučují decentralizovaný model archivace a provádí některá doporučení pro budoucí legislativu pro archivaci elektronických dokumentů v členských státech EU – mj. doporučují urychlené vypracování vhodných norem.

V současné době však proces vytváření norem pro archivaci elektronicky ukládání dat probíhá spíše na okraji zájmu architektů bezpečnosti internetu. Momentálně se velice diskutuje o tom, zda výše komentovaný draft (k protokolu TAP) má být vůbec součástí prací skupiny pkix, spíše se objevují názory doporučující přesun problematiky jinam, například nechat vzniknout skupinu typu pkixapp (aplikace pkix), která by se zabývala těmito a dalšími

otázkami. Podle komentátorů totiž problematika zas až tak bezprostředně nesouvisí s otázkami certifikátů, normou X.509 atd.

Na druhou stranu (viz např. [6]) problematika archivace elektronických dat patří k těm, jejichž vyřešení praxe potřebuje. Z hlediska dlouhodobého pohledu vyřešení této otázky je zcela nezbytné. Množství informací, se kterými lidstvo pracuje, narůstá značnou rychlostí. Pokud nenajdeme vhodné cesty k ukládání těchto informací (a to dlouhodobě), hrozí nebezpečí, že některé nám již známé informace se k budoucím generacím ani nedostanou.

6. Literatura

[1] Adams, C.; Sylvester, P.; Zolotarev, M.; Zuccherat, R.:Data Validation and Certification Server Protocol, rfc.3029, February 2001

[2] Trusted Archive Protocol (TAP), draft-ietf-pkix-tap-00.txt, February 2003

[3] CMS, rfc.3369, August 2002

[4] Pinkas, D., Ross, J., and N. Pope, "Electronic Signature Formats for Long Term Electronic Signatures", rfc. 3126, September 2001.

[5] Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", rfc.3161, August 2001.

[6] O. Macek, M. Wanner: Bude minulost záhadou schovanou v počítačových pamětech, Hospodářské noviny 8.4.2003, příloha Digital, str.2

[7] Dumortier, Jos; Van den Eynde: Electronic Signatures and Trusted Archival Services, 2003

[8] Blanchette, J. P.: Dematerializing Written Proof: French Evidence Law, Cryptography and the Global Politics of Authenticity, Doctoral dissertation 2001,

[9] InterPARES Authenticity Task Force, http://www.interpares.org/documents/atf draft final report.pdf

[10] DAVID-project, http://www.antwerpen.be/david

[11] Canonical XML, W3C Recommendation, http://www.w3C.org/TR/2001/REC-xml-c14n-20010315

[12] Trusted Archival Services, European Commission, August 2000, 37

[13] Haber, Stuart A.; Stornetta, Wakefield Scott: Stuart: How to Time-stamp a Digital Document, *Journal of Cryptology*, 3(2):99–111, 1991.

F. Letem šifrovým světem

Mobilní telefon s vestavěným utajovačem TopSec GSM

Dne 5. března 2003 byl Národním bezpečnostním úřadem (http://www.nbu.cz/) vydán certifikát kryptografického prostředku na mobilní telefon s vestavěným utajovačem dodávaný na trh pod označením TopSec GSM (číslo certifikátu K20036). Certifikát je vydán na stupeň utajení "Vyhrazené".

Samotné šifrování se v telefonu provádí pomocí vlastní symetrické proudové šifry s délkou klíče 128 bitů. Dohoda na klíči k této šifře (nastavení generátoru náhodných čísel) je založena na výměně metodou Diffie-Hellman. Délka asymetrického číselného vektoru použitého pro ustanovení šifrovacího symetrického klíče je 1024 bitů. Jednotlivé telefony mohou být organizovány do uzavřených skupin, ve kterých obdrží každý přístroj svůj vlastní certifikát, autentizace účastníků před zahájením utajené komunikace je v tomto případě prováděna na principu RSA (modifikovaná metoda Diffie - Hellmann).

Výrobcem tohoto prostředku je německá společnost Rohde & Schwarz SIT GmbH se sídlem v Berlíně. Další informace k zařízení lze nalézt na www.sit.rohde-schwarz.com nebo je můžete získat e-mailem (část informací je k dispozici i česky) na adrese Jan.Wagner@RSCZ.rohde-schwarz.com .

SIM karty lze klonovat za sedm minut

Doba potřebná k naklonování SIM karty se výrazně zkrátila. Umožňuje to další zlepšení původního útoku z roku 1998, který dovoluje klonovat SIM karty s původním algoritmem A38. Publikovaný diferenční útok umožnil naklonování karty přibližně za osm až dvanáct hodin. V laboratoři IBM vznikl nový vylepšený útok. Podle sdělení zástupců této firmy dokáží nalézt klíč během sedmi minut.

Klonování SIM karet se tak může stát významným problémem pro mobilní operátory. Umožňuje totiž podvodníkům vytvořit klonovanou SIM kartu a na ni protelefonovat vysoké finanční částky. Podvodné hovory mohou být realizovány prostřednictvím sítí roamingových partnerů, takže jsou pro operátora v reálném čase prakticky nezjistitelné. To je pravděpodobně také důvod, proč Český mobil od roku 2002 začal prodávat karty s jiným autentizačním algoritmem. Tyto bezpečné Oskarovy karty se poznají podle toho, že druhá číslice zleva v jejich identifikačním čísle je dvojka.

Daňová přiznání s elektronickým podpisem

Ministerstvo financí - ÚFDŘ uvedlo do provozu 12.3.2003 program, který umožňuje podávat v elektronické podobě se **zaručeným elektronickým podpisem** po Internetu tato podání pro finanční úřady:

a) Daňové přiznání k silniční dani,
b) Daňové přiznání k dani z nemovitostí,
c) Daňové přiznání k dani z přidané hodnoty,
d) Oznámení o nezdaněných vyplacených částkách fyzickým osobám dle § 34 odst. 5, 8, 9 a 14 zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

Program je umístěn na adrese http://adis.mfcr.cz/adis/jepo/index.html a je na něj přímý odkaz z hlavní internetové stránky Ministerstva financí.

Pro podepsání podání lze použít jen zaručený elektronický podpis založený na **kvalifikovaném certifikátu**, který musí obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná (§ 11 zákona č. 227/2000 Sb., o elektronickém podpisu), a proto při žádosti o vystavení certifikátu **je současně nutné požádat o uvedení bezvýznamového identifikátoru vytvářeného MPSV**, který bude používán i pro daňovou správu.

Pozvánka

ČESKÁ TECHNIKA
spolek absolventů a přátel ČVUT v Praze
Rektorát ČVUT v Praze,
Zikova 4, 166 36, Praha 6

BITIS
sdružení pro bezpečnost informačních technologií a informačních systémů
http://crypto-world.info/bitis/
Katedra telekomunikační techniky
FEL ČVUT,Technická 2, 166 36, Praha 6

organizují pro členy, přátele a hosty přednášku s názvem

CESTY K UNITÁRNÍ TEORII Z POHLEDU ASTROFYZIKY ,
kterou přednese **RNDr. Jiří Grygar, CSc**.

Přednáška se uskuteční : **16.dubna 2003** od 18.00 hod. na FEL ČVUT, Technická 2, Praha 6 ve velké posluchárně č. 209-211 (2. patro).

Za přípravný výbor zve členy BITIS, spolku ČESKÁ TECHNIKA a další zájemce
Doc. Ing. Jiří Přibyl, CSc.,
předseda BITIS a místopředseda ČESKÉ TECHNIKY

Pozvánka na semináře: Broadband Visions 2003, Enterprise

Vážení přátelé,

dovolte mi, abych Vás touto formou informoval a zároveň pozval na dva odborné semináře, které se uskuteční v druhé polovině měsíce dubna.

První akcí je **seminář „Broadband Visions 2003“**, který pořádá časopis TECHNOLOGIES & PROSPERITY **17.4.2003 v hotelu Olšanka.** Jedná se o 3. ročník našich jarních "širokopásmových" setkání s cílem diskutovat aktuality z oblasti širokopásmových sítí, služeb a aplikací. Účast na akci je zdarma. Program a přihlášku si můžete stáhnout na http://www.tapmag.cz v sekci semináře, přímý link: http://www.tapmag.cz/image/tap/semin/Seminar_Broadband.pdf .

Druhou akcí je **seminář** „**Enterprise Content Management**“ pořádaný společností Efcon. Časopis TECHNOLOGIES & PROSPERITY je mediálním partnerem této akce. Akce proběhne **24.4.2003 v Kongresovém centru Praha.**

Na tomto semináři zazní zhodnocení současných i budoucích směrů rozvoje řešení pro správu dokumentu a obsahu, zkušenosti uživatelů s výběrem a nasazením těchto řešení. Zvláštní pozornost bude věnována integraci s informačním systémem SAP.
Účast na akci je rovněž zdarma. Program a přihlášku si můžete stáhnout na
http://www.tapmag.cz/image/tap/semin/ECM_Efcon.pdf
Další informace jsou k dispozici na stránkách pořadatele na http://www.efcon.cz

Jiří Sochor
WIRELESSCOM, s.r.o.
zástupce šéfredaktora T&P pro projekty
Domažlická 5, 130 00 Praha 3
tel. 233000500
j.sochor@wirelesscom.cz

O čem jsme psali v dubnu 2000 - 2002

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

G. 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 (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (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 sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@post.cz
pavel.vondruska@ct.cz