Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 5/2009 **17.květen 2009**

5/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1315 registrovaných odběratelů)

Obsah :

Příloha: Call for Papers Mikulášská kryptobesídka 2009 - CFP_MKB2009.pdf

A. O bezpečnosti objevování sousedů (SEND + CGA)

Pavel Vondruška (pavel.vondruska@crypto-world.info)

V počítačových systémech je jedním ze známých bezpečnostních problémů mechanismus pro objevování sousedů. Např. lze odpovědět na výzvu sousedovi, která byla určena jinému stroji, lze se vydávat za stroj, který již v síti není k dispozici apod. Mezi možné útoky na mechanismus hledání sousedů lze zařadit i některé prvky automatické konfigurace.

V souvislosti s nasazením protokolu IPv6 do praxe, byl v květnu 2004 publikován dokument RFC 3756: *IPv6 Neighbor Discovery (ND) Trust Models and Threats* http://www.ietf.org/rfc/rfc3756.txt , který podrobně analyzuje známé bezpečnostní problémy objevování sousedů.

Jako reakce na tyto známé problémy vznikl koncept bezpečného objevování sousedů (**SE**cure **N**eighbor **D**iscovery - SEND), který rozšiřuje mechanismus ND popsaný v RFC 2461: *Neighbor Discovery* (ND). Byl publikován v březnu 2005 jako de facto standard RFC 3971: *SEcure Neighbor Discovery* (SEND) http://www.rfc-editor.org/rfc/rfc3971.txt. Bezpečnostním cílem v IPv6 bylo zavést a poskytnout dostatečnou úroveň zabezpečení vyměňovaných zpráv. Návrh počítal s uplatněním standardních bezpečnostních prvků zabudovaných v IPsec. Bohužel se ukázalo, že toto není reálné, protože stanice pro inicializaci bezpečnostních mechanismů by potřebovala příliš mnoho informací. Proto byl zaveden výše odkazovaný koncept SEND, který není tak náročný a minimalizuje nároky na zúčastněné.

Koncept, který se zde pokusíme přiblížit, prochází v současné době přísnou bezpečnostní kontrolou. Výsledky kontoly jsou zpřístupňovány v podobě draftů v rámci k tomu pověřené pracovní skupiny CSI Working Group. Problematika je řešena ve dvou různých dokumentech, které byly zveřejněny letos v březnu. Prvý se zabývá bezpečnostní samotného protokolu a jmenuje se *SEND Hash Threat Analysis* (draft-ietf-csi-hash-threat-03.txt, autorů Ana Kukec, Suresh Krishnan, Sheng Jiang). Druhý řeší otázku bezpečnosti z pohledu proxy serverů, které SEND zpracovávají *Securing Neighbor Discovery Proxy Problem Statement* (draft-ietf-csi-sndp-prob-01.txt, autorů Greg Daley, Jean-Michel Combes, Suresh Krishnan).

SEND

Každá zpráva související s objevováním sousedů se digitálně podepíše (RSASignature). Předává se otisk veřejného klíče (Key Hash), jenž příjemci slouží k identifikaci klíče pro ověření podpisu a pak samozřejmě vlastní digitální podpis (Digital signature) a případně vycpávka, která zajišťuje, že velikost předávaných datových struktur je konstantní. Algoritmem RSA jsou podepsány zdrojová a cílová adresa a celá zpráva ležící před podpisem (první řádek ICMP, Typ, Kód, celá základní hlavička objevování sousedů a všechny volby před podpisem).

Při přijetí se podepsaná zpráva ověřuje. K tomu je potřeba veřejný klíč, který je identifikován předaným otiskem. Ten může dorazit ve volbě CGA (Cryptographically Generated Addresses) této zprávy (detaily viz dále) nebo jej přijímací stroj mohl získat již dříve. Pokud je zpráva ověřena, je považována za důvěryhodnou a je přijata, pokud ověření nelze provést nebo skončí chybou, není zpráva považována za bezpečnou a její osud záleží na konfiguraci příjemce. Je-li nastaven na přijetí jen bezpečných zpráv, bude zahozena. V opačném případě ji přijme a zachází s ní, jako se zprávami, které bezpečnostní prvky nemají. V RFC pro protokol SEND se požaduje, aby počítač v defaultním nastavení, přijal bezpečné i „nebezpečné“ zprávy. Toto se vyžaduje zejména z důvodu kompatibility, aby byla možná komunikace po dobu, než bude SEND plně implementován. Vyžaduje se, aby správce měl konfigurační nástroj, který umožňuje nastavit zákaz příjmu (ignorování) nebezpečných zpráv (tedy zákaz ohlašovaných zpráv sousedů, které nejsou podepsány nebo jsou s neplatným podpisem).

Již jsme řekli, že mechanismus SEND má proti standardním bezpečnostním mechanismům IPv6 (IPsec) výhodu ve své jednoduchosti a zejména minimální režii. Zejména odpadá výměna veřejného klíče. K tomu zde slouží jedna zpráva obsahující rozšíření CGA. To, co je zde uvedeno jako výhoda daného protokolu, je současně i nevýhodou mechanismu SEND. Je totiž velmi těsně s CGA spjat a neumožňuje zabezpečit obecné IPv6 adresy, ale jen CGA adresy.

SEND mimo zmíněných voleb RSA a CGA ještě obsahuje další dvě volby a to časovou značku (Timestamp) a unikát tj. „přenos náhodných dat“ (Nonce). Obě jsou relativně jednoduché a slouží jako ochrana proti možnému opakování starší platné zprávy.

Tyto prostředky slouží jako vhodná obrana proti většině známých problémů při objevování sousedů. Jak se však ukazuje, nechrání proti podvodným směrovačům. Tyto tzv.

„lžisměrovače“ si mohou vytvořit CGA adresu a posílat podepsané korektní zprávy, v níž se prohlásí za směrovače a pokud se dostanou do směrovacích tabulek, stáhnou na sebe celý datový provoz. I zde existuje řešení, které bylo do SEND implementováno. Je to tzv. certifikace směrovačů a vytváření tzv. certifikační cesty. Certifikační autority, které koncový počítač (stroj) důvěřuje, vystavují směrovačům certifikáty, které prokazují, že jde o směrovač a případně jaké prefixy má oprávnění ohlašovat. Certifikáty nejsou vkládány přímo do zpráv ohlašujících jednotlivé prefixy. Klientovi totiž stačí ověřit směrovač pouze jednou a jednalo by se proto o zbytečnou zátěž komunikace. Klient důvěřuje (po ověření!) směrovači až do vypršení certifikátu. SEND za tím účelem zavedl dvojici zpráv ICMP 148 (Žádost o certifikační cestu) a ICMP typ 140 (Ohlášení certifikační cesty). Když klient dostane ohlášení od směrovače, kterému zatím nedůvěřuje, pošle Žádost o certifikační cestu. Směrovač po přijetí výzvy odpoví Ohlášením certifikační cesty. V této zprávě je zahrnuta sada certifikátů, které klientovi umožní ověřit jeho důvěryhodnost.

V RFC 3971 je mimo výše uvedených technik (CGA adresy, digitální podpisy, certifikace směrovačů) zavedeno i několik implicitních opatření proti DoS útokům.

Zbývá doplnit informace k CGA adresám.

CGA adresy

Kryptograficky generované adresy jsou definované v RFC 3972: Cryptographically Generated Addresses (březen 2005, http://www.ietf.org/rfc/rfc3972.txt). Cílem je, aby se nemohl za vlastníka adresy prohlásit kdokoliv. Využívá se k tomu jednosměrnost hashovacích funkcí a vlastnictví soukromého/veřejného klíče.

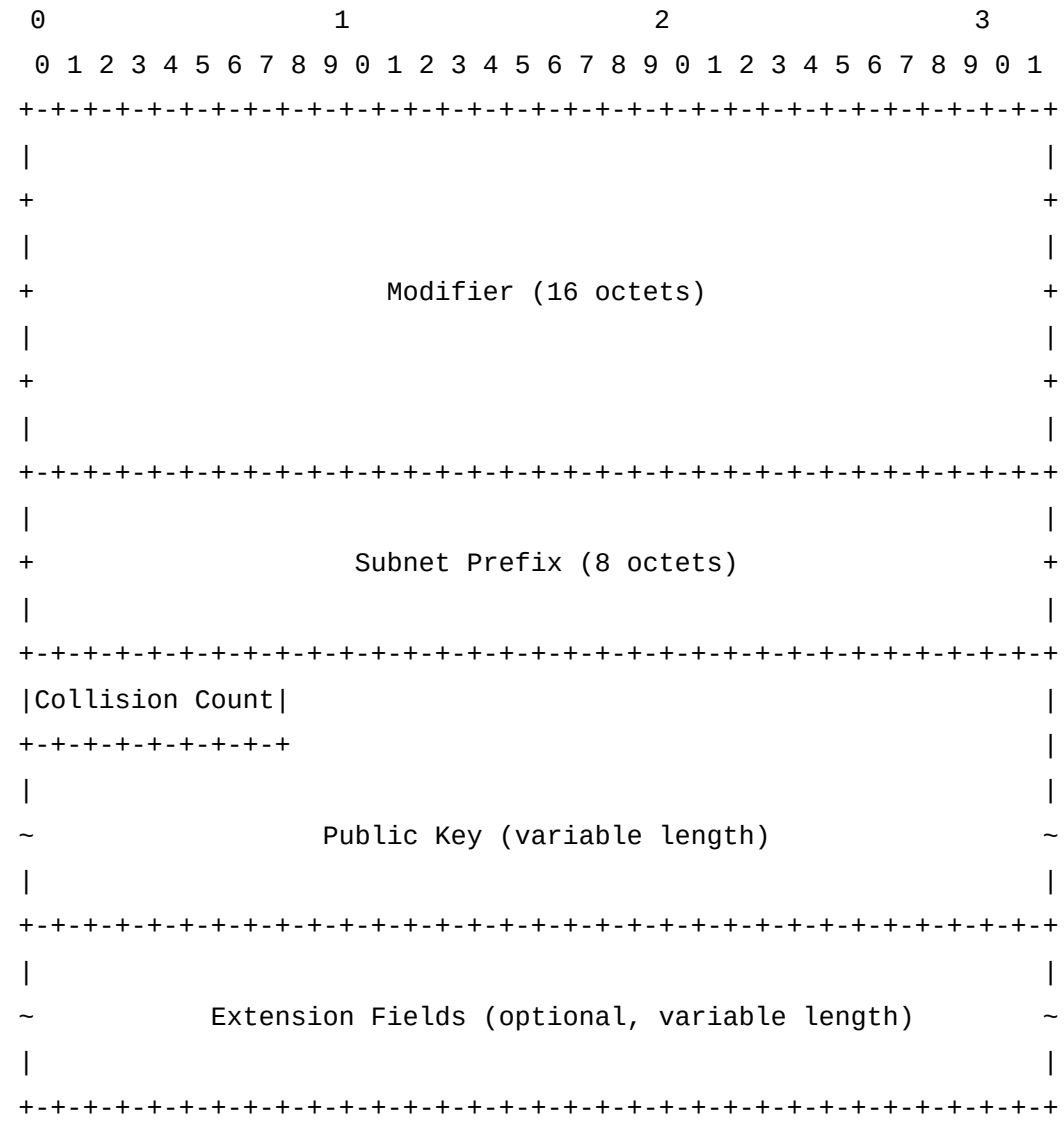
Výpočet datové struktury CGA je následující:

0) Zvolí se bezpečnostní parametr Sec. Jeho velikost je 3 bity a může nabývat všech hodnot od 0-8.

1) vypočte se (pseudo)náhodné číslo tzv. modifikátor délky 128 bitů.

2) Vypočte se hodnota Hash2. Tato hodnota je SHA-1 otisk zřetězení modifikátoru // 9 nulových bajtů // veřejného klíče // rozšiřujících položek. Z tohoto otisku se vezme 112 bitů (od leva).

3) Nyní se porovná 16xSec nejlevějších bitů Hash2 s nulou. Jestliže je hodnota nulová, pokračuje se bodem 4. Obsahuje-li nenulovou hodnotu, zvětší se modifikátor o jedničku a krok 2 se opakuje. Pokud je parametr Sec=0, pak se pochopitelně tento krok vynechá.



(obr. převzatý z RFC 3972).

4) Nastaví se 8-bitové počítadlo kolizí na nulu

5) Nyní se zleva doprava zřetězí modifikátor // prefix podsítě // počítadlo kolizí // veřejný klíč // rozšiřující položky. Vypočte se pomocí SHA-1 otisk tohoto řetězce a vezme se 64 levých bitů. Výsledek se označí jako Hash1.

6) Nyní se z hodnoty Hash1 vytvoří identifikátor rozhraní a to tak, že tři jeho nejlevější bity jsou nahrazeny hodnotou Sec a do bitu 6 a 7 se uloží příznaky rozhraní („u“ 0/1 globální/lokální, „g“ 0/1 individuální/skupinový).

7) Pokračuje se zřetězením 64 bitů prefixu sítě a 64 bitů identifikátoru rozhraní. Tato hodnota délky 128 bitů je IPv6 adresa (dle RFC 3513).

8) Pokud je požadována detekce duplicit adres (dle RFC 3971), provede se tento krok. Je-li detekována, zvýší se počítadlo kolizí a opakuje se postup od kroku 5. Po třetí kolizi je ohlášena chyba a proces je zastaven.

9) Z vypočtených hodnot se sestaví datová struktura, která je výstupem z algoritmu CGA.

CGA je navržena tak, aby pravost adresy šla rychle a snadno z doprovodné datové struktury ověřit. Vzhledem k vlastnostem hashovací funkce SHA-1 nelze vytvořit k již existující adrese vyhovující datovou strukturu s jiným veřejným klíčem. Případný útočník může pouze zkopírovat informace, které poskytuje skutečný vlastník soukromého klíče a adresy. Útočník tedy nemůže případné datové struktury, které se k CGA váží, podepisovat. CGA tedy poskytuje důvěryhodné propojení mezi adresou a veřejným klíčem.

Literatura

[1] RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models and Threats

[2] RFC 2461: Neighbor Discovery (ND).

[3] RFC 3971: SEcure Neighbor Discovery (SEND)

[4] SeND Hash Threat Analysis, draft-ietf-csi-hash-threat-03.txt

[5] Securing Neighbor Discovery Proxy Problem Statement, draft-ietf-csi-sndp-prob-01.txt

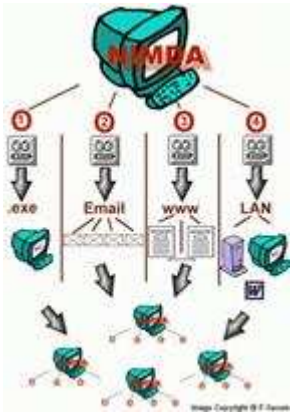
[6] RFC 3972: Cryptographically Generated Addresses

[7] RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture

[8] Satrapa, P.: Internetový protokol verze 6, Edice CZ.NIC, 2008

B. SIM karta mobilu ako bezpečné zariadenie pre vytváranie zaručeného elektronického podpisu (ZEP)

Ing. Peter Rybár, NBÚ SR, (peterryb@gmail.com)

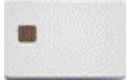


Pred niekoľkými rokmi počítače pripojené k internetu alebo počítačovým sieťam boli záležitosťou skupiny nadšencov a nad otázkou ich bezpečnosti sa nikto nepozastavoval, až kým sa pripojené počítače nezačali zneužívať podvodníkmi, proti ktorým je v súčasnosti nevyhnutné použiť rôzne antivírusové či firewall programy. V súčasnej dobe je v rovnakej pozícii použitie elektronických dokumentov, ktoré sú nechránené pred manipuláciou pri komunikácii v obchodnom či administratívnom styku, čo v najbližšom čase môže tvrdo zasiahnuť firmy, banky či štátne inštitúcie. Najlepšou ochranou pre prenášané elektronické dokumenty je zabezpečiť ich proti zmene elektronickým podpisom a ak je potrebné aj jednoznačné preukázanie identity fyzickej osoby, ktorá elektronický dokument proti zmene zabezpečila, potom je namieste použitie zaručeného elektronického podpisu (ZEP).

Pre vytvorenie ZEP z elektronického dokumentu je potrebné certifikované bezpečné zariadenie, ktoré obsahuje podpisový kľúč (súkromný kľúč), pomocou ktorého ZEP v certifikovanej aplikácii pre vytváranie ZEP vytvoríme.

Na overenie ZEP, čiže overenie či elektronický dokument nebol sfalšovaný, používame kvalifikovaný certifikát. Kvalifikovaný certifikát obsahuje overovací kľúč (verejný kľúč) a údaje identifikujúce fyzickú osobu, ktorá vlastní podpisový kľúč.

Podpisový kľúč pre ZEP musí byť uložený na bezpečnom zariadení, čo v súčasnosti znamená čip čipovej karty alebo USB token. K vytvoreniu ZEP (teda použitiu podpisového kľúča) musíme mať počítač, kde je nainštalovaný špeciálny komunikačný program pre spomenuté bezpečné zariadenie, ak ide o čipovú kartu tak aj špeciálne zariadenieako je čítačka čipových kariet, a samozrejme aplikáciu pre vytváranie ZEP. A tu nastáva hlavný problém. Na to aby sme dokázali vytvoriť ZEP potrebujeme toho príliš veľa, čo odradí veľa ľudí od ochrany elektronických dokumentov zaručeným



elektronickým podpisom a radšej riskujú, že dokument, ktorý bol odoslaný, môže byť počas prenosu sfalšovaný.

A dá sa to spraviť aj inak? Jednoduchšie, bezpečnejšie a s možnosťou využitia pre širokú verejnosť napríklad v elektronickom obchode, bankových službách, či portáloch pre občanov poskytovaných štátom?

Určite áno, a to práve pomocou SIM karty, ktorá je súčasťou mobilného telefónu. Technické detaily riešenia sú popísané v NBÚ štandarde „**SIM mobilného zariadenia na elektronické podpisovanie cez bezpečné WEB/WAP alebo PKCS#11 rozhranie**“ http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html .

Zjednodušene povedané, podpisový kľúč je uložený na SIM karte, certifikovanej pre vytváranie ZEP spolu s certifikovanou aplikáciou, ktorá celé podpisovanie riadi. Mobilný telefón pritom zabezpečuje pre túto SIM aplikáciu len niektoré činnosti ako: zobrazovanie informácií na displeji telefónu, prijímanie a odosielanie SMS správ a zadávanie kódov či PIN údajov pri podpisovaní.

Ak chce niekto podpísať elektronický dokument pomocou SIM v mobile, potom si:

- Vloží elektronický dokument do podpisovej aplikácie na svojom počítači alebo nahrá elektronický dokument na web portál, cez ktorý je podpisová aplikácia prístupná pre každého.
- Vloží do podpisovej aplikácie súbor so svojím DiGiID, alebo zadá URL na svoje DiGiID, ktoré obsahuje ním podpísaný zoznam jeho certifikátov a certifikátov, ktorým on dôveruje. Aplikácia sa potom na základe údajov z DiGiID sama automaticky nakonfiguruje a je pripravená nielen na podpisovanie ale aj na overovanie ZEP (Pri súčasných aplikáciách pre ZEP je práve správne konfigurovanie aplikácií pre ZEP pomerne náročný proces a teda najväčší strašiak).
- Podpisová aplikácia vyčíta z DiGiID telefónne číslo, na ktoré má odoslať žiadosť o podpísanie elektronického dokumentu.

- Aby sa zabránilo prijatiu falošnej požiadavky na mobil, podpisová aplikácia vygeneruje „Prístupový kód“, ktorý zobrazí podpisovateľovi. Prístupový kód môže obsahovať náhodné číslo spojené s aktuálnym časom.
- Podpisová aplikácia vyčíta z DiGiID kľúč na zašifrovanie prístupového kódu spolu s údajmi, ktoré je potrebné podpísať a údajmi identifikujúcimi podpisový kľúč.
- Podpisová aplikácia odošle SMS na mobil.
- Mobil vloží SMS do SIM aplikácie, ktorá odšifruje SMS a požiada zadanie prístupového kódu, aby si overila, či neprijala falošnú žiadosť.
- Ak podpisovateľ zadá na mobile správny prístupový kód, je požiadaný zadať podpisový PIN na vytvorenie podpisu.
- Po zadaní podpisového PIN je cez mobil odoslaná SMS s digitálnym podpisom do podpisovej aplikácie na počítač podpisovateľa alebo na web portál, kde sa vytvorí výsledný ZEP z elektronického dokumentu.
- Podpisovateľ si uloží výsledný ZEP a podpísaný elektronický dokument alebo ho môže opäť vložiť do aplikácie pre ZEP a požiadať o jeho overenie.

Ako z predchádzajúcich krokov vyplýva, podpisovanie elektronických dokumentov pomocou SIM aplikácie pre ZEP **je jednoduché**, **bezpečné** a podpisovateľovi postačuje bežný mobil a pripojenie na internet.

V súčasnosti používané technológie pre mobilné podpisovanie využívajú rôzne postupy, ktorých bezpečnosť je veľmi nízka, pričom túto nízku bezpečnosť prevádzkovatelia ospravedlňujú malým počtom podvodov a veľkými nákladmi na prechod na iné bezpečnejšie technológie.

Ďalšou nevýhodou v súčasnosti používaných jednorazových hesiel a GRID kariet je obmedzenie komunikácie iba medzi dvoma subjektmi vlastniacimi rovnaké zariadenia. Ak klient chce použiť rovnakú technológiu aj s niekým iným, tak s každým ďalším klientom alebo poskytovateľom služieb si musí vymeniť ďalšie rovnaké zariadenia či podpisové kľúčenky.

Podpisovanie pomocou SIM obsahujúceho aplikáciu podľa NBÚ štandardu tieto nedostatky odstraňuje, keďže sa pri komunikácii používa kvalifikovaný certifikát, ktorý je verejný a zabezpečuje jednoznačnú identitu podpisovateľa podpísaných elektronických

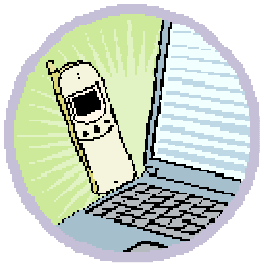
dokumentov pre všetkých overovateľov a tým umožňuje nezávislú komunikáciu s ľubovoľným počtom subjektov bez potreby osobnej alebo zmluvnej vzájomnej výmeny autentifikačných údajov.

Jediné, čo je potrebné zabezpečiť, aby bolo možné podpisovanie v SIM, je certifikovaná SIM aplikácia, ktorú musia mobilní operátori do SIM vložiť a nakonfigurovať so správnymi údajmi. K tomu bude potrebná návšteva mobilného operátora, ktorý vymení aktuálnu SIM za novú SIM a vykoná administratívne úkony pre korektné nastavenie SIM, čo pozostáva z vygenerovania podpisového a overovacieho kľúča, šifrovacieho párového kľúča, vydania certifikátov na kľúče a vydania a podpísania DiGiID súboru. Tieto úkony zaberú operátorovi len niekoľko minút a pre užívateľa sa budú javiť ako bežné úkony, na ktoré je už zvyknutý pri vydávaní SIM karty pre mobilný telefón.

A potom už používateľ mobilu môže začať elektronicky podpisovať neobmedzene veľké množstvo elektronických dokumentov pre neobmedzene veľké množstvo služieb a účelov.

Napríklad, pri zmene bydliska cez verejný portál pre komunikáciu so štátnou správou bude postup nasledovný:

- na web portáli vyplní potrebné údaje na zmenu trvalého bydliska,
- na web portál priloží svoj DiGiID súbor pomocou cesty na súbor alebo URL adresy,
- web portál mu zobrazí nový prístupový kód a odošle SMS na jeho mobil,
- na mobile po prijatí SMS zadá prístupový kód, ktorý mu predtým zobrazil web portál
- na mobile zadá svoj podpisový PIN, čím vytvorí podpis, ktorý sa odošle v SMS na web portál,
- web portál vytvorí z prijatej SMS a údajov z DiGiID výsledný ZEP a ponúkne mu po zrealizovaní zmeny trvalého bydliska aj uloženie tohoto ZEP podpisu a podpísaných údajov.
- A je to.



C. Mikulášská kryptobesídka , Call for Papers

3. – 4. prosinec 2009, Praha , http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka se koná letos již podeváté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *3. prosince 2009* a (b) půldne prezentací příspěvků a diskusí v pátek *4. prosince 2009*. Pro workshop jsou domluveny zvané příspěvky:

- Kenny Paterson (Royal Holloway, UK): *Cryptography and secure channels*.
- Paul Leyland (Cepia Technologies, ČR): *Use of Graphics Processing Units in cryptography*.
- Otokar Grošek (Slovak University of Technology): *Latin squares and cryptography.*
- Vlastimil Klíma (nezávislý kryptolog, ČR): *Hašovací funkce SHA-3, BMW a EDON-R.*.
- Pavel Vondruška (Telefónica O2 Czech Republic): *Vývoj kryptografických zařízení v ČS(S)R.*

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2009*. Pro

podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2009 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pro sborník workshopu pak musí být dodán do *19. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2009
Oznámení o přijetí/odmítnutí:	30. října 2009
Příspěvky pro sborník:	19. listopadu 2009
Konání MKB 2008:	3. – 4. prosince 2009

Programový výbor

Jan Bouda, FI MU, Brno, ČR
Petr Hanáček, FIT VUT v Brně, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Štefan Porubský, ÚI AV ČR, Praha, ČR
Zdeněk Říha, FI MU, Brno, ČR
Luděk Smolík, Siegen, SRN
Jiří Tůma, MFF UK, Praha, ČR
Jozef Vyskoč, VaF, Rovinka, SR

Mediální parneři

D. Akademie CZ.NIC nabízí vysoce specializované kurzy o internetových technologiích

Akademie CZ.NIC je dalším z projektů sdružení CZ.NIC, správce české domény nejvyšší úrovně. Výukové centrum, které se pod tímto názvem skrývá, nabízí zájemcům možnost odborného vzdělávání v oblasti internetu a internetových technologií. Současné kurzy jsou určené všem, kteří se chtějí dozvědět více o DNS, DNSSEC, ENUM a PKI (k těmto tématům budou postupně přibývat další), vyzkoušet si přednášenou látku v praxi a podělit se o své zkušenosti s lektory.

Výukové centrum otevřelo sdružení na začátku dubna 2009. Od prvního dne tohoto měsíce nabízí Akademie CZ.NIC specializované kurzy zaměřené na internetové technologie. Ty probíhají v prostorách, které jsou na taková, vysoce technická školení vybavené. Zájemci o kurzy se mohou přihlásit na internetových stránkách www.nic.cz/akademie, kde najdou kromě rozvrhu kurzů také další informace, například o lektorech jednotlivých kurzů. Toto centrum je výjimečné tím, že nabízí školení, která v nabídce jiných podobných škol v České republice nejsou.

V Akademii CZ.NIC je v tuto chvíli možné absolvovat čtyři kurzy, v nichž se jako přednášející střídají jak zaměstnanci CZ.NIC, tak odborníci z praxe. V případě DNS a DNSSEC je to Ondřej Surý, technický ředitel sdružení. Kurzy na téma ENUM vede Lukáš Macura ze Slezské univerzity v Opavě a Petr Hruška z CZ.NIC. Školení týkající se problematiky PKI má na starosti Pavel Vondruška, vysokoškolský pedagog a odborník na infrastrukturu veřejných klíčů. Nabídka kurzů se bude do budoucna rozrůstat. V plánu jsou například školení na téma IPv6, směrování, BGP, PostgreSQL a další.

První, testovací kurzy se uskutečnily v Akademii CZ.NIC už na konci loňského roku. Tato setkání ale nebyla veřejná. Zaměstnanci sdružení připravili tato školení pouze pro své členy a registrátory a to proto, aby zjistili, jaký by o ně mohl být zájem; zároveň si chtěli jednotlivé kurzy vyzkoušet před známým publikem. Podle počtů posluchačů, kteří se těchto setkání zúčastnili, je evidentní, že jsou v České republice zájemci a takto odborná témata.

Všechny kurzy jsou určené především pro techniky, kteří ve svých společnostech spravují DNS, starají se o bezpečnost dat, odpovídají za telekomunikační systémy nebo dohlíží na jiné síťové systémy. Zajímavé ale mohou být i pro všechny ostatní, kteří mají o tyto technologie zájem a chtějí se o nich dozvědět více.

Více informací o Akademii CZ.NIC, o termínech kurzů najdou zájemci na internetové adrese www.nic.cz/akademie.

O sdružení CZ.NIC, z. s. p. o.

Zájmové sdružení právnických osob CZ.NIC bylo založeno předními poskytovateli internetových služeb v roce 1998 a nyní má již 60 členů. Hlavní činností sdružení je provozování registru doménových jmen .CZ a 0.2.4.e164.arpa (ENUM), zabezpečování provozu domény nejvyšší úrovně CZ a osvěta v oblasti doménových jmen. V současné době se sdružení intenzivně věnuje rozšiřování systému DNSSEC, rozvoji systému správy domén a podpoře nových technologií a projektů prospěšných pro internetovou infrastrukturu v České republice. CZ.NIC je členem sdružení EURid, spravující evropskou domény EU, a dalších obdobně zaměřených mezinárodních společností (CENTR, ccNSO a další). Více informací o sdružení CZ.NIC najdou zájemci na internetové adrese www.nic.cz.

E. O2 a PMDP představují Plzeňskou kartu v mobilu

Společnost Telefónica O2 Czech Republic a Plzeňské městské dopravní podniky, a.s. (PMDP) představují unikátní řešení městské multifunkční čipové karty - Plzeňské karty, integrované v mobilním telefonu.

V současné době Plzeňská karta slouží obyvatelům západočeské metropole nejen jako jízdenka pro místní i integrovanou veřejnou dopravu, ale lze ji použít například také pro bezhotovostní úhrady zboží/služeb u smluvních partnerů, zakoupení vstupenek na kulturní akce, jako průkaz do Knihovny města Plzně nebo identifikátor ve stravovacích a přístupových systémech. Plzeňská karta v mobilním telefonu je založena na technologii NFC (Near Field Communications). Používání uvedeného řešení je identické s užíváním standardní Plzeňské karty - bezkontaktní čipové karty založené na technologii MIFARE™, kterou vyvinula společnost NXP Semiconductors.

Plzeňská karta se poprvé představila v roce 2004 a od té doby si jí pořídilo téměř dvě stě tisíc obyvatel z celé ČR (zhruba tři čtvrtiny držitelů jsou z Plzeňského kraje). V roce 2008 začaly na projektu Plzeňské karty spolupracovat společnosti Telefónica O2 a NXP, které se společně s PMDP rozhodly integrovat celou kartu a její funkce do **mobilního telefonu**. Pro majitele to bude znamenat nejenom zvýšení komfortu, ale především možnost využívat další funkce, jako je například kontrola zůstatku elektronické peněženky v mobilním telefonu nebo možnost jejího on-line dobíjení.

Dne 1. 4. 2009 byl spuštěn pilotní provoz první fáze projektu Plzeňské karty v mobilním telefonu s technologií NFC, která je založena na využívání služeb souvisejících s elektronickou peněženkou (nákup přestupních jízdenek ve vozech MHD). Cíl pilotního provozu spočívá v ověření výše uvedené technologie v reálném provozu systému Plzeňské karty. Do pilotního provozu bylo zapojeno 50 účastníků a potrvá do 30. 6. 2009. Další fáze vývoje bude od poloviny léta do konce roku 2009 zaměřena na využití elektronické peněženky v mobilním telefonu i mimo dopravu - platby za zboží/služby u smluvních partnerů (restaurace, sportovní centra, kina). Zároveň bude připravováno i spuštění Plzeňské karty v mobilním telefonu s technologií NFC do produktivního provozu. V rámci dalšího vývoje je uvažováno také o implementaci vzdálené správy mobilní Plzeňské karty. To znamená vzdálené dobíjení elektronické peněženky, doručování a validace předplatných kupónů prostřednictvím NFC mobilního telefonu.

Pro využívání funkce Plzeňské karty v telefonu musí mít uživatel přístroj, který tuto technologii podporuje. V současné době se jedná o telefony Nokia 6131 NFC a Nokia 6212, jejich nabídka se ale bude do budoucna rozšiřovat. Technicky je celé řešení postaveno na platformě MIFARE4Mobile™a jedná se o její první implementaci na světě. Hlavní výhodou je zde využití mobilního telefonu, do kterého je zabudován SmartMX čip. Do něj je nahrána aplikace elektronické peněženky Plzeňské karty, která zobrazuje na displeji telefonu okamžitý zůstatek v peněžence a informace o posledních 4 provedených transakcích (nákupech přestupních jízdenek ve vozech MHD). Funkce aplikace je možno dále rozšiřovat ve vazbě na to, jak poroste možnost využití Plzeňské karty v mobilním telefonu.

F. O čem jsme psali v květnu 2000 – 2008

Crypto-World 5/2000

Crypto-World 5/2000

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 5/2002

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

Crypto-World 5/2003

Crypto-World 5/2004

Crypto-World 5/2005

Příloha : zpráva vysílaná radioamatérskou stanicí GB2HQ - nedele_30m.wav

Crypto-World 5/2006

Crypto-World 5/2007

Crypto-World 5/2008

Příloha:
1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf
2) Příloha k článku „Príklad útoku na podpisovaný dokument … “ : priklad.bmp

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
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 elektronický 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. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/