Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 8, číslo 5/2006 **15. květen 2006**

5/2006

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1112 registrovaných odběratelů)

Obsah : str.

A. Hledá se náhrada za kolizní funkce …

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

Hašovací funkce, u níž byla nalezena kolize, ztrácí obecně smysl, neboť hypotéza o tom, že se chová jako náhodné orákulum, byla (prakticky) vyvrácena.
Z tohoto důvodu by neměla být používána v aplikacích, které principiálně vyžadují bezkoliznost. Mezi takovéto využití hašovacích funkcí patří např. vytváření časových razítek a digitálních podpisů (resp. chcete-li zaručených elektronických podpisů), neboť tam kolize znamená, že je možné předložit dvě různé zprávy s tímtéž platným digitálním podpisem (elektronickým), ověřitelným pro obě zprávy.

Po té, co byla hašovací funkce MD5 naprosto deklasována útokem, který trvá pouze vteřiny (viz Vlastimil Klíma [1], [2], [3]), a hašovací funkce SHA-1 byla teoreticky prolomena (Akashi Satoh [4]), se samozřejmě začala hledat opatření pro minimalizaci rizik. Jsou možné v zásadě tři odlišné přístupy: za prvé - tyto funkce zakázat a nahradit je zcela jinými, které považujeme za bezpečné, za druhé - stávající funkce částečně modifikovat tak, aby byly odolné proti současným útokům vycházejícím z práce prof. Wangové ([5]). Třetí přístup nazveme „salámovou metodou“ - tvářit se, že se nic neděje.
Je pravdou, že prvé dvě metody se z hlediska běžného uživatele těžko uplatňují, jeho aplikace nemají volbu silnějších hašovacích funkcí (jako např. SHA-224, SHA-256, SHA-384, SHA-512 ..) a také nejsou připraveny na modifikaci stávajících funkcí. Navíc vyměnit funkci za jinou „nestandardní“ sebou nese velký problém s kompatibilitou. U systémů, které nepotřebují „všeobecnou“ kompatibilitu (jsou vyvíjeny a provozovány pro konkrétní účel bez ohledu na okolní vazby – lokální archivace, lokální komunikace spec. zařízení), to nemusí být zásadní problém. U obecně používaných aplikací je podmínkou k běžnému využití, aby se upravené funkce rychle připravil standard a nový identifikátor pro takto upravené a nově zavedené hašovací funkce.

Proto mne nepřekvapily dotazy čtenářů Klímova článku [3], kde se někteří čtenáři snažili navrhnout jednoduché řešení, které by okamžitě pomohlo. Např. tam, kde je to možné, používat otisky podle dvou hašovacích funkcí. Viz. *Bedo* a odpověď čtenáře *jaja* .

Datum: *27. 3. 10:33*
Vložil: *bedo* *(neregistrovaný)*
Titulek: **praktické problémy?**
1. Kolízie MD5 spomínané v článku znamenajú, že k súboru s nejakou MD5 viem nájsť iný s rovnakou MD5, ktorý bude obsahovať mnou dodané data?

2. Pokiaľ má súbor viac hašov ako napr. MD5 a SHA1, existuje nejaká možnosť podvrhnutia iného, pričom všetky haše budú sediet?

Datum: *27. 3. 12:23*
Vložil: *jaja* *(neregistrovaný)*
Titulek: **Re: praktické problémy?**
1) Ne, ale dokazu najit 2 "soubory", ktere maji stejny MD5 hash
2) Zatim se toho neni treba bat.

Překvapující je odpověď Vlastimila Klímy v této diskusi. Běžný čtenář by si mohl odvodit, že použití dvou hašů nepomůže, neboť se bezpečnost výrazně nezvýší.

Datum: *27. 3. 23:08*
Vložil: *Vlastimil Klíma* *<v (tečka) klima (zavináč) volny (tečka) cz>*
Titulek: **Re: praktické problémy?**

1. ne, ale pracuje se na tom
2. ano, je to jen o málo složitější (podrobnosti jsou zrovna v článku ve Sdělovací technice č.4). Něco vyjímám:

   Dvě hašovací funkce
   K nalezení kolize funkce MD5 || SHA1 potřebujeme pouze 2^80 zpráv, které mají stejnou MD5 haš. Mezi nimi nalezneme pak dvě, které mají i stejnou SHA1, čili kolizi celé MD5 || SHA1. Trikem Jouxové získáme těch 2^80 zpráv pouze se složitostí POUZE 80 krát složitost nalezení jedné kolize MD5 (teď jednu kolizi umím na notebooku, na kterém píšu, jsem připojen na internet a běží mi test kolizí, za 30 sekund - trochu jsem původní program vylepšil). Získání těch 80 na sebe navazujících zpráv je teda za 2400 sekund. Zbývá je zkombinovat do 2^80 zpráv a zhašovat pomocí SHA-1. Čili je to až na tu hodinu práce navíc úplně stejné jako kdybychom vzali 2^80 libovolných zpráv a hledali v nich kolizi SHA-1. Poznamenávám, že tento dotaz jsem dostal i od pracovníka jedné velké certifikační autority.
   …

Myslím si, že je vhodné tuto odpověď okomentovat. Dal bych do uvozovek „o málo složitější“. Nejde o tu hodinu práce navíc spojené s MD5, ale o to, že se musí hledat kolize SHA-1 mezi množinou zpráv 2^80. Složitost tohoto hledání je tedy shodná se složitostí hledání kolize SHA-1 v době, kdy se věřilo, že je kryptograficky bezpečná. Jinými slovy - využití dalšího otisku pomocí MD5 vrátilo bezpečnost na původní hodnotu 2^80. Podle mne je tedy tato kombinace jakýmsi východiskem, jak jednoduše na krátkou dobu zvýšit odolnost proti kolizím na přijatelnou míru. Obě funkce jsou sice slabé (jsou kryptograficky prolomeny), ale praktické nalezení společné kolize je ještě složitým výpočetním problémem, který (za současného stavu) nelze realizovat.

Zde je vhodné připomenout, že se rozlišuje mezi ***kryptografickým prolomením, teoretickým a praktickým prolomením.*** Zatímco hašovací funkce MD5 byla již prolomena teoreticky „dávno“, pak kryptograficky a prakticky až v létě 2004 ([6]). Kryptografickým prolomením se u hašovací funkce myslí, že byl nalezen způsob vyhledání kolize s nižší složitostí než je vypočtená odolnost na základě předpokladu, že se hašovací funkce chová jako náhodné orákulum (tj. pro otisk délky d je kryptografická odolnost 2^d). Teoretické prolomení hašovací funkce znamená, že existuje takový algoritmus a taková výpočetní síla, která umožní nalézt kolizi v rozumném čase. Např. u hašovací funkce MD5 bylo zřejmé, že útok se složitostí 2^64 je možné realizovat pomocí distribuovaného útoku např. za pomoci dobrovolníků, kteří dají k dispozici svoji výpočetní kapacitu (projekt MD5CRK, [7]). Cílem bylo najít kolizi MD5 hrubou silou a přesvědčit tak architekty, aby od ní konečně ustoupili. Po uveřejnění příspěvku Wangové byl projekt zastaven.
Praktické prolomení hašovací funkce je pak nalezení kolize této funkce. V případě MD5 byla první kolize publikována v již zmíněné prezentaci prof. Wangové [6].

Podívejme se jaká je současná situace v této oblasti u hašovací funkce **SHA-1**. Funkce již byla **kryptograficky prolomena**, neboť byl nalezen postup hledání kolizí se složitostí nižší než 2^80. Postup byl popsán začátkem roku 2005 ve zprávě, kterou publikoval čínský kolektiv kryptologů Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu ([8]). Hlavní výsledek zprávy se týká právě SHA-1, kde pro nalezení kolize podle nich stačí 2^69 operací.
Množství operací 2^69 je však stále ještě vysoké, a tak mnoho lidí a institucí nadále obhajovalo SHA-1 jako použitelnou a to pro velkou teoretickou a praktickou náročnost prolomení.

Ovšem již v létě 2005 na rump session konference Crypto bylo oznámeno, že paní prof. Xiaoyun Wang nalezla urychlení útoku na SHA-1 z původní složitosti 2^69 na 2^63 ([9]).. To již je složitost výpočtu, který by mohl být dosažitelný distribuovaným výpočtem na internetu tak, jak jsme toho byli svědky i u jiných kryptoanalytických útoků.
Krátce na to v září 2005 byla **SHA-1 teoreticky prolomena**. Akashi Satoh publikoval práci, která obsahuje návrh hardware, který by nalezl kolize podle postupu Wangové se složitostí 2^69. Navrhuje se architektura LSI na bázi 0.13-µm CMOS. Na základě toho byla vypočítána rychlost, velikost a spotřeba HW. Za 10 milionů dolarů lze tak teoreticky sestavit zákaznický hardwarový systém, který by sestával z 303 PC, každý s 16 deskami (na každé je 32 jader SHA-1), pracujícími paralelně. Útok by trval 127 dní.
Takže již zbývá poslední krok – zveřejnění, informace, že **SHA-1 byla prakticky prolomena**! Tj. nalezení kolizí tohoto standardu. Jak píše Vlastimil Klíma, zatím kolize nalezeny nejsou, ale již se na tom pracuje …

Pod dojmem právě zopakovaného bouřlivého vývoje bezpečnosti hašovacích funkcí bylo v březnu tohoto roku zveřejněno stanovisku NIST k dalšímu používání hashovacích funkcí ([10]). Toto stanovisko pohřbívá funkci SHA-1. Přesněji pro digitální podpis, časová razítka a další aplikace, kde je podstatná bezkoliznost, již její využití nedoporučuje a má být co nejdříve nahrazeno hašovací funkcí z rodiny SHA-2 (SHA-224, SHA-256, SHA-384 a SHA-512). Její použití je v této oblasti po roce 2010 dokonce zakázáno. SHA-1 se bude moci využívat jen pro výpočet HMAC, derivaci klíče (KDF) a jako náhodný generátor (RNG).

Obdobně NSA ([11]) v září 2005 ve schválené sadě algoritmů pro ochranu utajovaných dat stupně SECRET a TOP SECRET (tzv. sadě B) funkci SHA-1 již pochopitelně neuvádí a povoluje pouze algoritmus SHA-256 a SHA-384, podle standardu FIPS 180-2.

Blížíme se k závěru. Vhodným vodítkem, jak postupovat, je samozřejmě stanovisko NIST nebo NSA a na základě toho začít přecházet na bezpečnější hašovací funkce třídy SHA-2. Tam, kde to není prozatím možné (tato sada není implementována), lze dočasně využívat zdvojení hašů MD5 || SHA1.

Vědci samozřejmě hledají další možná řešení. Jsou připraveny metody, jak s využitím současných HW zařízení nebo SW balíků, které realizují funkce MD5 nebo SHA-1, zabránit současným kolizním útokům drobnou vnitřní změnou některých služebních funkcí (SHAInit, SHAUpdate, SHAFinal, MD5Init, MD5Update, MD5Final) ([12]). Testují se i hašovací funkce s více inicializačními hodnotami nebo můžeme z jednoho 512-bitového bloku m (u SHA-1, ale i u MD5), který máme zpracovat, vytvořit a zpracovat bloky dva (například m || C(m), kde C bude nějaký kontrolní kód bloku m). (Klíma v diskusi ke článku [3]). Další opatření tohoto typu byla navržena na kryptologických konferencích, kde se řešily problémy hašovacích funkcí ([13], [14], [15]).

Literatura

[1] Vlastimil Klima: Tunnels in Hash Functions: MD5 Collisions Within a Minute (extended abstract), IACR ePrint archive Report 2006/105 , http://eprint.iacr.org/2006/105.pdf, 18 March, 2006,
v češtině na http://cryptography.hyperlink.cz/2006/tunely.pdf,
zdrojové kódy na http://cryptography.hyperlink.cz/2006/web_version_1.zip

[2] Klima, V.: Kolize MD5 do minuty aneb co v odborných zprávách nenajdete, Crypto-World 4/2006

[3] Klíma, V.: Tunely v hašovacích funkcích: kolize MD5 do minuty
http://www.root.cz/clanky/tunely-v-hasovacich-funkcich-kolize-md5-do-minuty/

[4] Akashi Satoh: Hardware Architecture and Cost Estimates for Breaking SHA-1, ISC 2005, Singapore, September 20-23, 2005, LNCS 3650, pp. 259-273, 2005

[5] X. Wang and H. Yu: How to Break MD5 and Other Hash Functions., Eurocrypt'05, Springer-Verlag, LNCS, Vol. 3494, pp. 19–35. Springer, 2005.

[6] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu: Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, rump session, CRYPTO 2004, *Cryptology ePrint Archive*, Report 2004/199, first version (August 16, 2004), second version (August 17, 2004), http://eprint.iacr.org/2004/199.pdf

[7] Projekt MD5CRK, 2004, http://www.md5crk.com/

[8] Xiaoyun Wang, Hongbo Yu: Collision search Attacks on SHA1, published February 13,2005 on http://www.financialcryptography.com/mt/archives/000357.html

[9] http://www.iacr.org/conferences/crypto2005/program.html

[10] http://csrc.nist.gov/CryptoToolkit/tkhash.html

[11] http://www.nsa.gov/ia/industry/crypto_suite_b.cfm?MenuID=10.2.7

[12] Charanjit S. Jutla and Anindya C. Patthak : Is SHA-1 conceptually sound?, 7.10.2005, Cryptology ePrint Archive: Report 2005/350, http://eprint.iacr.org/2005/350

[13] Cryptographic Hash Workshop, NIST, USA, Oct. 31 - Nov. 1, 2005, http://www.csrc.nist.gov/pki/HashWorkshop/program.htm

[14] Conference on Hash Functions (Ecrypt), June 23-24, 2005, Przegorzaly (Krakow), Poland, http://www.ecrypt.eu.org/stvl/hfw/

[15] WEWoRC 2005, Western European Workshop on Research in Cryptology, Leuven-everlee, Belgium, July 5-7, 2005,
http://www.cosic.esat.kuleuven.be/WeWorc/allAbstracts.pdf

B. Bezpečnost IP Telefonie nad protokolem SIP

Ing. Jan Růžička (jan.ruzicka@cesnet.cz), CESNET, z. s. p. o.
Ing. Miroslav Vozňák, Ph.D. (miroslav.voznak@vsb.cz), CESNET, z. s. p. o.

Drtivá většina bezpečnostních problémů VoIP vzniká z faktu, že IP telefonie pracuje na otevřených systémech, využívá stávající IP sítě, standardní prvky a známé operační systémy. To znamená, že základním nebezpečím jsou všechny známé problémy z oblasti IP.

Nejdříve musíme konstatovat, že pokud někdo dokáže útočit na část IP sítě, tak může útočit na VoIP. Dále je třeba si uvědomit, že bezpečnostní riziko je vyšší u protokolu UDP než u TCP a VoIP je převažující měrou postavena na UDP. IP telefonie patří mezi aplikace, na které se útočí snadněji a dostupnost služby je závislá na dostupnosti IP infrastruktury. Určitě si dokážeme představit jednoduchý útok typu DoS, kdy nemusí nakonec jít ani o konkrétní útok na některý z centrálních logických prvků VoIP, jehož výsledkem je snížená dostupnost VoIP služeb. Útokům nahrává i fakt, že komunikace probíhá v reálném čase, což vyřazuje některé metody robustnosti a ochrany založené na odloženém zpracovaní požadavku, jak je tomu například u elektronické pošty.

Nepřehlédnutelným rizikem VoIP jsou také odposlechy. Pokud se daří zachytit RTP pakety na trase, tak jejich uložení do formátu wav zvládne i Ethereal, a to je jeden z největších problému IP telefonie. Mohli bychom říci, že byl, protože od května roku 2004 je specifikován SRTP (Secure Real Time Protocol) v RFC 3711, který umožňuje šifrovaný přenos, ale implementace v klientech ještě není dostatečně rozšířená. Zajímavou aktivitou poslední doby je také ZRTP Phila Zimmermanna [4].

Další úrovní problému je získání citlivých informací z odchycené VoIP signalizace a její následné zneužití. Autentizace šifrovaným heslem při přihlášení by měla tedy být samozřejmostí. Ze zachycených dat lze však také vyčíst údaje o účastnících spojení, a to nejen údaje, kdo a jak dlouho například volal, ale i odkud je dotyčný aktuálně přihlášen. Ze získaných údajů útočník třeba zjistí, že uživatel s konkrétním číslem přešel se svým WiFi telefonem ulici, protože je přihlášen z jiného přístupového bodu. Proto je potřebné v otevřených sítích šifrovat i signalizaci.

Z pohledu používaných protokolů s VoIP můžeme říci, že nejrozšířenější jsou ITU-T H.323 a IETF SIP, pro rozsáhlé sítě s velkým počtem řízených hlasových bran je vhodný protokol MGCP nebo velmi podobný a z MGCP vycházející MEGACO/H.248. Kromě těchto rozšířených a standardizovaných protokolů je spousta dalších více či méně oblíbených protokolů, za zmínku určitě stojí protokol IAX2 z open-source řešení Asterisk, který by měl být v polovině 2006 dotažen do RFC. Protokol SIP v současnosti hodně nabírá na síle. Již několik let pozorujeme vzrůstající zájem o tento protokol nejen ve výzkumné a vzdělávací sféře, ale i v komerčním světě. Můžeme si všimnout, že většina VoIP operátorů v České republice ho ve svých nasazeních používá, a proto je většina následujících kapitol zaměřena konkrétně na protokol SIP.

1. Autentizace

SIP (Session Initiation Protocol) je protokolem pro navázání, modifikaci a ukončení spojení. Základ je popsán v RFC 3261, na něž navazuje mnoho rozšíření, například pro IM a prezenci. Principy a problémy popsané dále samozřejmě platí i pro tato rozšíření. SIP vyšel z HTTP

protokolu, je tedy narozdíl od H.323 textový. Textová podstata dává protokolu lepší čitelnost a rozšiřitelnost, kterou však také může využít potencionální pozorovatel nebo útočník.
Základním prvkem bezpečnosti je autentizace, která v SIPu vzhledem tomu, že ideovým rodičem je protokol HTTP, používá schéma HTTP Digest. Ve starší verzi standardu (RFC 2543) bylo uváděno i HTTP Basic, které již ovšem podle RFC 3261 nesmí být používáno, tj. vyžadováno ani přijímáno.

V rámci komunikace se ještě rozlišuje autentizace mezi uživateli (User-to-User) a mezi proxy serverem a uživatelem (Proxy-to-User). S prvním případem se setkáme nejčastěji u registrace. Registrační server je koncovým příjemcem požadavku, proto je použita metoda User-to-User. Komunikace probíhá následovně (viz obr. 1.), pokud nejsou potřebné údaje ve zprávě vyplněny, cílový klient posílá odpověď 401 Unauthorized a hlavička WWW-Authenticate obsahuje výzvu. Zdroj pak zopakuje požadavek s ověřovacími údaji odpovídajícími výzvě v hlavičce Authorization (obr. 2.).

```
SIP/2.0 401 Unauthorized.
Via: SIP/2.0/UDP 1.2.3.4:49252;branch=z9hG4bK.6afb7404;rport=49253.
From: sip:user@cesnet.cz;tag=6c2c90b8.
To: sip:user@cesnet.cz;tag=c10ed4fff3e6fb17efd0bfbdcce87ce2.c76e.
Call-ID: 1814859960@1.2.3.4.
CSeq: 1 REGISTER.
WWW-Authenticate: Digest realm="cesnet.cz",
      nonce="43eeaeb76e6eec559d737d4f4018dc659c5d282a".
Server: Sip EXpress router (0.9.5-pre1 (i386/linux)).
Content-Length: 0.


REGISTER sip:cesnet.cz SIP/2.0.
Authorization: Digest username="user", uri="sip:cesnet.cz", algorithm=MD5,
      realm="cesnet.cz", nonce="43eeaeb76e6eec559d737d4f4018dc659c5d282a",
      response="9e83c39e8a7262901
Via: SIP/2.0/UDP 1.2.3.4:49252;branch=z9hG4bK.32f02bf2;rport.
From: sip:user@cesnet.cz;tag=6c2c90b8.
To: sip:user@cesnet.cz.
Call-ID: 1814859960@1.2.3.4.
CSeq: 2 REGISTER.
Content-Length: 0.
Max-Forwards: 70.
Expires: 15.
Contact: sip:user@1.2.3.4:49252.
```

Obr. 1. : Autentizace při registraci.

V případě, že proxy server potřebuje před zpracováním požadavku uživatele ověřit, žádá o to v odpovědi 407 Proxy Authentication Required a v hlavičce Proxy-Authenticate je obsažena výzva. Klient doplní do požadavku hlavičku Proxy-Authorization s patřičnými údaji.

```
INVITE sip:mamut@iptel.org SIP/2.0.
Max-Forwards: 10.
Record-Route: <sip:5.6.7.8;ftag=5DAA94E7;lr=on>.
Via: SIP/2.0/UDP 5.6.7.8;branch=z9hG4bK0a5d.90580ee2.0.
Via: SIP/2.0/UDP 1.2.3.4:5062;branch=z9hG4bK2E1FD348.
CSeq: 262 INVITE.
To: <sip:mamut@iptel.org>.
Proxy-Authorization: Digest username="bbb", realm="ces.net",
nonce="43788e90381194d66364fced4dc7097828391e81",
uri="sip:mamut@iptel.org", cnonce="abcdefghi", nc=00000001,
response="ed4adec8
Content-Type: application/sdp.
From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.
Call-ID: 379332994@1.2.3.4.
Subject: sip:bbb@ces.net.
Content-Length: 234.
```

```
User-Agent: kphone/4.2.
Contact: "Franta Vomacka" <sip:bbb@1.2.3.4:5062;transport=udp>.
.
v=0.
o=username 0 0 IN IP4 1.2.3.4.
s=The Funky Flow.
c=IN IP4 1.2.3.4.
t=0 0.
m=audio 33728 RTP/AVP 0 97.
a=rtpmap:0 PCMU/8000.
a=rtpmap:97 iLBC/8000.
```

Obr. 2. : Příklad ověření ve zprávě INVITE.

2. Utajení a integrita

Autentizace však zprávu samotnou nijak nechrání. Jak se tedy stavět k integritě a utajení obsahu zprávy? Nabízí se například použití S/MIME v těle zprávy. Obsahem těla, který je specifikován hlavičkou Content-Type, může být kromě obvyklého SDP (viz obr. 2.) pro požadavky jako například INVITE také elektronický podpis hlaviček. Příjemce je pak schopen ověřit, zda nedošlo po cestě ke změně zprávy. Je nutno podotknout, že některé hlavičky (například Request URI, Route, Via, Max-Forwards) mění během cesty svůj obsah, je proto účelné podepisovat pouze neměnné části jako hlavičky To, From, Cseq, Call-ID, Contact a případně další hlavičky mající význam pouze pro koncové body. I když i s hlavičkou Contact se může vyskytnout problém při průchodu přes NAT, když je třeba změnit inzerovanou privátní IP adresu za veřejnou často až na proxy serveru.

Utajení informací v signalizaci můžeme zajistit také S/MIME šifrováním. Například vložené SDP můžeme zašifrovat, aby případný posluchač nebyl schopen okamžitě určit zdroje, cíle a kodeky použité při transportu médií. Zároveň tím však můžeme narazit na omezení funkcionality v určitých případech, jakými je použití některých hraničních elementů (IP2IPgw) nebo výskyty privátních IP adres v SDP.

Je dokonce možné využít systému tunelování, kdy je v těle obalující zprávy obsažena celá originální SIP zpráva včetně těla, kterou je možno jen podepsat nebo i zašifrovat. Tímto postupem lze například také zamaskovat identitu volajícího, jež je obsažena pouze ve vnořené zprávě, ale velikost přenášených zpráv nepříjemně roste. Uvedené mechanismy jsou poněkud komplikované, avšak jejich výhodou je dosažení integrity a utajení mezi koncovými prvky (End-to-End).

Další možností zabezpečení je použití šifrovaného komunikačního kanálu, jakým je například TLS. Při navazování spojení by měla být ověřena platnost certifikátu a pak sestaven šifrovaný kanál, čímž je zajištěno utajení zpráv protokolu. Při použití TLS není zaručeno šifrované spojení mezi koncovými body, ale pouze do příštího skoku (Hop-By-Hop), a nelze s jistotou vynutit, že další prvky na cestě použijí také TLS. Samozřejmě TLS nevylučuje možnost využít předtím popsaných mechanismů S/MIME.

V reálném nasazení je do signalizace hovoru zapojeno obvykle okolo čtyř prvků – volající a volaný klient (pomineme-li větvení) a proxy server domény každého z nich. Z hlediska zabezpečení je vhodné, aby alespoň první skok, který je obvykle nebo dokonce vždy veden k domácímu proxy serveru, probíhal po šifrovaném kanále, protože narušení registrace má vážný důsledek na používaní služby (krádež identity a přesměrování) a u ostatních zpráv mohou být uplatňovány politiky přidávající hlavičky na základě ověřené identity v doméně. Zároveň však udržování dlouhodobých spojení TLS pro každého klienta znamená vysoké

nároky na systémové prostředky serveru. Reálný výskyt TLS podpory zatím není u klientů velký, ale situace se začíná zlepšovat, z čehož vyplývá potěšující skutečnost, že si implementátoři uvědomují potřebu bezpečnosti. Výskyt S/MIME v implementacích je však ještě řidší než je tomu u TLS.

3. Útoky

Samozřejmě jako u jakékoliv komunikace je i zde nebezpečí zachycení a pozměnění zpráv, kterému brání techniky popsané v předchozích odstavcích. Důsledkem pozměnění zprávy může být například přesměrování všech hovorů účastníka nebo pozměnění či ukončení i probíhajícího hovoru, které je u SIP protokolu vzhledem k textové povaze poměrně jednoduché. Pak tu jsou také útoky, které omezují či zcela znemožňují využití služby (DoS) a znepříjemňují život uživatele SPIT (Spam over IP telephony). Ochrana před takovou komunikací je v IP telefonii o to těžší, že jde o komunikaci v reálném čase a tak hovor nelze odložit do fronty a analyzovat jej. Ochranu lze spatřovat v první řadě v ověřování, které však zvláště ve své jednodušší podobě omezuje otevřenost služby. V případě SPITu je náročnost na prostředky, které musí mít spammer k dispozici, vyšší než u klasického SPAMu, protože odesílatel musí mít nepoměrně vyšší dostupné komunikační pásmo, silnější hardware i více času k realizace jednotkového SPITu. Uvedené nároky spolu s doposud nepoměrně nižším počtem potenciálních odběratelů než u elektronické pošty jsou zřejmě důvod, proč nás zatím SPIT neobtěžuje, což v žádném případě neznamená, že není třeba se připravit.

I DoS má v IP telefonii rychlejší průběh a složitější obranu než například u elektronické pošty. Rozezvonit všechny telefony ve firmě vyžaduje výrazně menší objem zpráv než zahltit schránky poštovního serveru. Navíc je tu i efekt zvonícího aparátu, který bezprostředně vyrušuje v práci, či nemožnost si zavolat nebo se dovolat ve srovnání s tím, že mail dorazí třeba o půl hodiny později. Zde je možností, opět kromě ověřování, pokusit se hlídat frekvenci zpráv z určitého místa. Účinnost této metody je však značně snížena možností distribuovaného útoku. Zatím se však s takovými útoky nesetkáváme, což je pravděpodobně dáno rozšířením IP telefonie a způsobem jejího nasazení na místech pro útok zajímavých (uzavřené ostrůvky). Opět to ovšem neznamená, že není třeba se obávat.

4. Mezidoménová důvěra

Současná nasazení IP telefonie jsou často ještě uzavřenými ostrůvky. Přitom teprve mezidoménová komunikace umožňuje lépe využít potenciál IP telefonie. Postavit uzavřený ostrůvek, kdy i mobilní nebo vzdálení klienti jsou připojováni například pomocí VPN, není nic složitého. Zrovna tak komunikaci mezi doménami lze uzavřít do připravených VPN kanálů a podobně, ale míra nutné administrace z obou stran je poměrně vysoká a řešení se často špatně škáluje. Jsme-li v situaci, kdy subjektů, které bude třeba propojit, bude třeba padesát nebo také tisíc, je třeba volit jiné řešení. A především chceme operativně navazovat hovory do vzdálených domén bez toho, aby musela spojení s každou novou doménou předcházet i několikahodinová práce týmu techniků na obou stranách. K tomu samozřejmě i následný monitoring takových spojení.

Celý problém vzniku spojení se dá shrnout do dvou bodů: nalezení cíle a navázání komunikace. Oboje však musí být navíc podloženu důvěrou. Jedním řešením je vybudování hierarchie prvků, které mohou, ale nemusí využívat tentýž komunikační protokol. Praktickým příkladem je GDS (Global Dialing Scheme), což je hierarchie H.323 gatekeeperů, které umožňují spojení široké světové výzkumné a vzdělávací komunity. Existuje několik tzv.

světových gatekeeperů, na něž jsou navázány národní a pod nimi jsou gatekeepery jednotlivých institucí. Nevýhodou tohoto systému je přímá vazba na protokol H.323, která neumožňuje systém použít i pro SIP. Samotný prvek důvěry není příliš silný, protože je založen pouze na konfigurovaných vazbách mezi prvky. Problémem hierarchie jako takové je závislost na dostupnosti vyšších prvků, jejichž výpadek má vážné důsledky na funkčnost celých podstromů.

Jinou možností je směřovat k federativnímu systému, který lze chápat jako nadstavbu distribuovaného AAI. V současné době je tento sytém již používán pro webové aplikace a asi nejčastější uplatnění nachází při přístupu ke knihovnickým zdrojům, ale principielně lze použít i pro další aplikace jako jsou gridy nebo právě telefonie. Proces může pro případ telefonie fungovat následovně. Subjekty, například instituce, se dohodnou na vzájemné důvěře tj. důvěryhodnému způsobu a formě předávaní ověřené identity. Samozřejmě čím více subjektů najde společnou řeč, tím lépe. Klient se přihlásí ke svému domovskému serveru a volá následně do jiné instituce z federace. Požadavek prochází přes jeho domovský server, kde je ověřen a autentizační hlavičky domácí domény jsou nahrazeny definovanou externí identitou, která říká, že volající byl ověřen a má povolení domácí instituce takové spojení realizovat. Příjemce takového požadavku ověří platnost vložené identity (elektronický podpis) a spojení povolí. Systém samozřejmě může být ještě prohlouben uplatněním lokálních politik a brát v potaz další dohodnuté atributy identity jako například funkci volajícího (student, učitel). Z pohledu SIPu můžeme najít základ takového přístupu v IETF draftu sip-identity [2], který využívá PKI infrastrukturu a prosté podepisování vybraných hlaviček. Dalším mechanismem může být využít vkládání SAML položky, jak navrhuje draft tschofenig-sip-saml [3].

5. DNS

Systém IP telefonie úzce závisí na sytému DNS jako většina dnešních IP systémů. IP telefonie však stále častěji využívá i pokročilejších záznamů, než jen překlad jména na IP adresu jako například SRV záznamy pro lokalizaci serverů obsluhujících příslušné domény a ENUM. A opět důvěryhodnost těchto záznamů má důležitý význam. Například podaří-li se podvrhnout SRV záznam, budou požadavky směrovány na zcela jiný stroj a celá doména nebude korektně dostupná. Stejně tak je tomu samozřejmě u A záznamů serverů, příklad má však ilustrovat existenci dalších citlivých bodů. Některé negativní účinky přesměrování lze omezit například pomocí oboustranného ověřování při sestavení TLS spojení.

ENUM umožňuje překlad telefonního čísla na identifikátory dalších služeb, jako je IP telefonie, e-mail, web, atd. Systém může výrazně zjednodušit úkol nalezení cesty k volanému a zjednodušit administraci směrovacích údajů. Jednoduchost je však zároveň vzhledem k využití DNS také jeho slabinou. Číslice telefonního čísla tvoří strom, stejně jako běžné záznamy, avšak jedno pole zde vždy obsahuje pouze jedinou číslici. Tento fakt výrazně zjednodušuje prohledání celého takového stromu a následné volání s vysokou jistotou existence volaného. Výsledkem je opět důraz na ochranu ve směrovacích prvcích IP telefonních sítí, tedy například doplněním o mezidoménovou autentizaci.

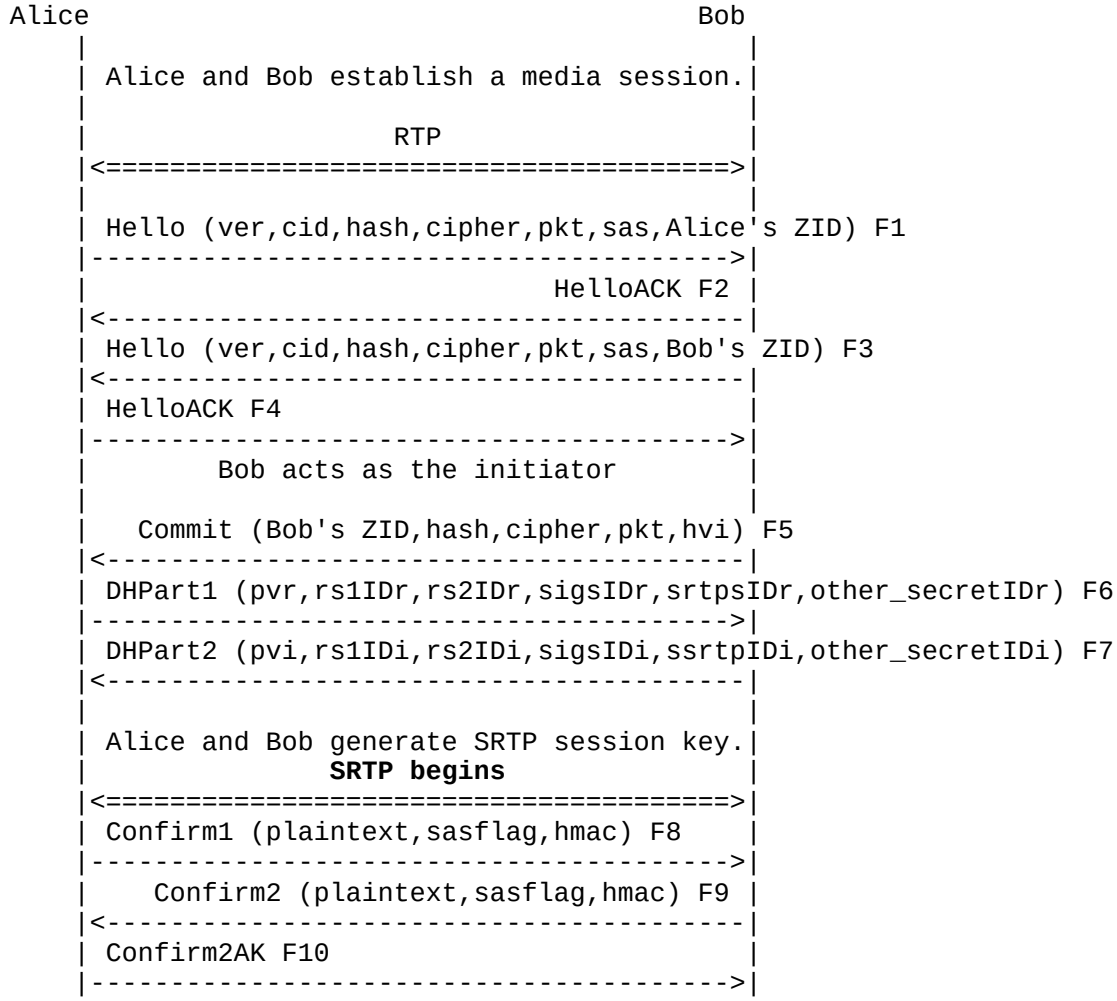
Prostředkem obrany proti podvrženým DNS záznamům obecně by měl být DNSSec, jehož masové nasazení je zatím stále v nedohlednu, a proto nezbývá než používat prosté DNS, ale každý by si měl být vědom možné hrozby

6. Závěr

Úkolem článku bylo seznámit čtenáře se základními bezpečnostními postupy, které se vztahují k použití protokolu SIP v IP telefonii a především upozornit na problematická místa, která mohou ovlivnit kvalitu služby. Uživatel by si měl být vědom bezpečnostních omezení a technik k jejich potlačení. Protože v současném stavu všech služeb, nejen IP telefonie, jedině poučený a obezřetný uživatel může vyžadovat a dosáhnout co možná nejbezpečnější komunikace, samozřejmě v poměru k důležitosti přenášeného obsahu.

Literatura

[1] RFC 3261
[2] http://www.ietf.org/internet-drafts/draft-ietf-sip-identity-06.txt
[3] http://www.ietf.org/internet-drafts/draft-tschofenig-sip-saml-05.txt
[4] http://www.ietf.org/internet-drafts/draft-zimmermann-avt-zrtp-01.txt



Ustanovení SRTP session užitím ZRTP (draft-zimmermann-avt-zrtp-01,March 5, 2006)

C. NIST (National Institute of Standards and Technology - USA) a kryptografie.
Recommendation on Key Management – část 1.

Jaroslav Pinkava, CA Czechia, (Jaroslav.Pinkava@zoner.cz)

1. Úvod

Cílem této informace je dát určitý přehled o dalším z důležitých dokumentů NIST, které se vztahují ke kryptografii. Tentokráte to je materiál Recommendation on Key Management, který byl vydán jako Special Publication SP 800-57 v srpnu 2005 (patří tedy mezi relativně novější). Dokument je rozdělen do tří částí. První část obsahuje celkový přehled a doporučení pro nejlepší praktické postupy ve vztahu k práci s kryptografickými klíči. Druhá část je věnována otázkám souvisejícím s definicí politik a bezpečnostních plánů, tj. především otázkám správy kryptografických klíčů. Konečně třetí část (zatím nevyšla) má obsahovat popis kryptografických vlastností současných systémů.

Podrobněji - obsah první části je věnován následujícímu:

- definuje ty bezpečnostní služby, které mohou být poskytovány a typy klíčů, které jsou využívány v kryptografických postupech;
- poskytuje základní informace, které se vztahují ke kryptografickým algoritmům (využívajícím kryptografické klíče);
- je provedena klasifikace různých typů klíčů a dalších kryptografických informací ve vztahu k jejich funkcím, jsou specifikovány ochrany pro každý z těchto typů informací a identifikovány metody pro poskytnutí těchto ochran;
- jsou identifikovány stavy, ve kterých se kryptografický klíč může nacházet v průběhu svého životního cyklu;
- je identifikována množina funkcí týkajících se správy klíčů;
- je diskutována celá řada otázek, které se týkají klíčového materiálu (použití klíčů, délka doby platnosti klíče, validace parametrů domény, validace veřejného klíče, odpovědnosti, audit, funkčnost systému pro správu klíčů a průvodce kryptografickými algoritmy a volbou velikostí klíčů).

Názvy jednotlivých kapitol první části:

kapitola 1. úvod
kapitola 2. terminologický slovník
kapitola 3. bezpečnostní služby
kapitola 4. kryptografické algoritmy
kapitola 5. příručka pro celkovou (obecnou) správu klíčů
kapitola 6. požadavky na ochranu kryptografických informací
kapitola 7. stavy klíčů a přechody mezi těmito stavy
kapitola 8. fáze a funkce správy klíčů
kapitola 9. odpovědnosti, audit a obnova
kapitola 10. specifikace správy klíčů pro kryptografická zařízení a aplikace

(příloha A se zabývá integritou a autentizačními mechanizmy, příloha B pak problematikou rozkrytí klíčů - key recovery)
Tato části přehledu je věnována stručnému shrnutí prvních čtyř kapitol první části materiálu.

2. Celkově

V roce 1977 NIST opublikoval Data Encryption Standard (DES) a od té doby NIST opublikoval celou řadu dalších materiálů, které se vztahují jak k popisu samotných kryptografických algoritmů (hashovací funkce, asymetrické algoritmy, AES), tak i k doporučením pro postupy při jejich využívání. Základní doporučení obsahuje příručka SP800-21 (viz Crypto-World 3/2006)a dokument SP 800-57 slouží pro prohloubení těchto doporučení.
Ke kapitole 2 – obsahuje dvanáctistránkový přehled používaných termínů a akronymů, pokud si čtenář není jistý významem některého termínu a potřebuje upřesnění, zde najde oporu.

3. Bezpečnostní služby

Prostřednictvím kryptografických postupů lze zajistit řadu základních služeb vztahujících se jak k bezpečnosti informací a dat tak i bezpečnosti samotných kryptografických klíčových materiálů.
S1. Důvěrnost (confidentiality) – tato vlastnost zajišťuje, aby informace nebyly prozrazeny neoprávněné straně (používá se také termín utajení jako synonymum této vlastnosti). Důvěrnost dosahujeme zašifrováním chráněných informací, informace jsou pak dostupné pouze oprávněným stranám (tyto umí informace dešifrovat).
S2. Integrita dat – tato vlastnost zajišťuje, že data nejsou neautorizovaně změněna (po jejich vytvoření, odeslání či uložení). Touto neautorizovanou změnou je chápáno jakékoliv vložení dalších dat, či naopak odstranění některých dat nebo jejich pozměnění.
Za tímto účelem jsou používány takové kryptografické mechanizmy jako MAC (message authentication codes) a digitální podpisy. Lze takto detekovat i náhodné modifikace (např. někdy vzniklé během přenosu dat) a to s dostatečně vysokou pravděpodobností.
S3. Autentizace – to je služba, kteá je používána s cílem ustavit původ informace. Autentizační služba tedy umožňuje verifikovat totožnost uživatele či systém, který vytvořil danou informaci (např. transakci či zprávu). Autentizace je obvykle zajišťována prostřednictvím digitálních podpisů či pomocí MAC, také některé techniky pro dohodu na klíči (key agreement) poskytují autentizaci.
S4. Autorizace – služba souvisí s oficiálním povolením (sankcí) provádět některé bezpečnostní funkce či aktivity. Obvykle je autorizace vázána na autentizační proces. Po proběhlé autentizaci role entity, má tato všechna oprávnění, která jsou s danou rolí asociována.
S5. Nepopiratelnost – touto službou je zajišťována integrita a původ dat pro ověření třetí stranou a to tak, že entita, která je původcem dat, nemůže toto následně popírat. Pro zajištění této funkce je obvykle používán digitální podpis (na základě použití soukromého klíče, který je znám pouze entitě, která tento digitální vytváří).
S6. Podpůrné služby – jsou to služby jako např. ustavení klíčů, generování náhodných čísel atd.
S7. Kombinace služeb – to je obvyklá praktická situace, neboť nevystačíme s využíváním jen jediného postupu. Proto je třeba navrhnout systém ochran (bezpečnostních služeb v této terminologii) vhodným způsobem tak, aby odrážel všechny požadované bezpečnostní vlastnosti. Příkladem zde mohou sloužit třeba postupy implementované pro praxi certifikační autority. Činnost CA vytváří poměrně složitý systém, existuje zde nezbytnost ochran pro komunikace mezi CA, RA a uživateli, pracuje se zde s řadou kryptografických klíčů atd.

4. Kryptografické algoritmy

V kapitole 4. dokumentu jsou rozebírány tři následující základní typy kryptografických algoritmů – hashovací funkce, symetrické algoritmy a asymetrické algoritmy. Zpracovaná kapitola vychází samozřejmě z algoritmů doporučených NIST (resp. schválených v dokumentech FIPS). Jaké jsou zde tedy popsány funkce kryptografických algoritmů?

Hashovací funkce – resp. kryptografická hashovací funkce vytváří relativně malý otisk (hodnotu hashe) z velkého (možná) vstupu a to tak, že obrácený postup je vlastně nereálný (tj. vytvořit na základě daného otisku zprávu tak, aby odpovídala tomuto otisku, hashi). Doporučené hashovací funkce jsou popsány v dokumentu FIPS 180-2, hashovací funkce s klíčem (HMAC) pak ve FIPS 198 (The Keyed-Hash Message Authentication Code - HMAC). Známé problémy s hashovací funkcí SHA-1 našly svůj odraz v posledním stanovisku NIST (http://csrc.nist.gov/CryptoToolkit/tkhash.html) z března tohoto roku.

Symetrické algoritmy – prostřednictvím šifrování dat zajišťujeme jejich důvěrnost (utajení). Schválenými algoritmy (NIST) jsou AES a TDEA. Každý z těchto algoritmů operuje s blokem dat otevřeného textu, ze kterého algoritmickým postupem vytváří (s využitím klíče) blok šifrového textu.

AES – tento algoritmus patřící k moderním zástupcům kryptografických postupů je popsán v dokumentu FIPS 197 (http://csrc.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf). Pracuje s 128 bitovými bloky a může používat klíče o dílce 128, 192 a 256 bitů.

TDEA – algoritmus je popsán v SP 800-67. Vychází z původního algoritmu DES, který byl modifikován a to následovně. Na 64-bitový blok dat je postupně použit algoritmus DES třikrát po sobě. Podle doporučení pro federální aplikace (USA) by měl být v každé z těchto tří fází použit jiný 56-bitový klíč.

Operační módy blokových šifer – to je vcelku samostatná problematika. Dnes v rámci doporučení NIST existuje celá škála těchto módů, jejich popis obsahuje publikace SP 800-38A (Recommendation for Block Cipher Modes of Operation - Methods and Techniques) a je třeba zmínit i nedávno doplněné módy - CMAC, CCM a GCM. Popis těchto je obsažen v publikacích SP 800-38B, SP 800-38C a SP 800-38D.

MAC (message authentication codes) slouží jak k zajištění autentizace dat, tak i k zajištění jejich integrity. MAC vytvářené využitím algoritmů pro blokové šifry popisuje SP 800-38. V dokumentu FIPS 198 je popsáno vytváření MAC opírající se o využití hashovací funkce.

Podpisové algoritmy – jejich prostřednictvím jsou zabezpečeny následující služby – autentizace, integrita a nepopiratelnost. Používají se v návaznosti na operace provedené prostřednictvím hashovacích funkcí - spočtený otisk zprávy, hash je podepsán (zašifrován) soukromým klíčem podpisového asymetrického algoritmu. Federální doporučení se vztahují k těmto třem podpisovým algoritmům – DSA, RSA a ECDSA.

DSA – tento podpisový algoritmus je nyní nově specifikován (FIPS 186-3) pro použití větších délek klíčů. Umožňuje práci s klíči v délkách 1024, 2048 a 3072 bitů, digitálním podpisem jsou pak bloky dat v délce 320, 448 a 512 bitů.

RSA – algoritmus specifikovaný v ANSI X9.31 a PKCS 1 byl pro potřeby vytváření digitálních podpisů popsán ve FIPS 186-3. V současnosti je rovněž tak předpokládána práce s většími délkami klíčů.

ECDSA – obdobně také tento algoritmus specifikovaný v ANSI X9.62 je pro digitální podpisy popsán ve FIPS 186-3. Pracuje s kratšími délkami klíčů než předchozí dva algoritmy (lze uplatnit obecné pravidlo, které říká, že pro asymetrickou eliptickou kryptografii je třeba používat klíče dvojnásobné délky – ve vztahu k požadované délce klíčů pro symetrickou kryptografii.

Schémata pro ustavení klíčů – východiskem zde je popis obsažený v dokumentu SP 800-56A (Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography – tento dokument pochází z března 2006). Existují dva základná typy těchto postupů – přenos klíče (key transport) a dohoda na klíči (key agreement).

Protokoly pro ustavení klíčů – oproti předešlým schématům pro ustavení klíčů obsahují tyto protokoly navíc informace, které se vztahují k vlastním zprávám - jejich toku a formátu.

Generování náhodných čísel – existují v zásadě dva typy GNČ, deterministické a nedeterministické. V dokumentu FIPS 186-3 je popsán deterministický GNČ, který lze použít pro kryptografické aplikace.

5. Shrnutí a literatura:

Příští pokračování se bude zabývat (v návaznosti na obsah SP 800-57) otázkami, které souvisí se samotnou správou klíčů, životním cyklem kryptografického klíče atd.

[1] NIST Special Publication SP 800-57 Recommendation on Key Management, Part 1 (http://csrc.ncsl.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf)

D. Compar Call for Papers - Mikulášská kryptobesídka

BUSLab

7. – 8. prosinec 2006, Praha

http://mkb.buslab.org

TRUSTED NETWORK SOLUTIONS

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos pošesté. 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 z (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *7. prosince 2006* a (b) půldne prezentací příspěvků a diskusí v pátek *8. prosince 2006*. Součástí workshopu budou opět zvané přednášky. Předběžně jsou domluveni následující řečníci:

- **Alex Biryukov** (University of Luxembourg)
- **Riccard Focardi** (Universitá Ca' Foscari di Venezia)

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 příspěvků (5-15 stran A4) připravené pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím vyplňte při registraci v našem konferenčním systému.
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 PDF, nebo PS přes registrační stránky MKB2006 a to nejpozději do 2. října 2006.
Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do 23. *října*. Upravený příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *20. listopadu*.

Zasílání příspěvků

Letos opět používáme konferenční systém.
Pro odevzdání příspěvku je třeba se zaregistrovat na ConfTool MKB2006
Na stejném místě je možné odevzdat příspěvek.

Důležité termíny

Podání návrhů příspěvků:	2.října 2006
Oznámení o přijetí/odmítnutí:	23. října 2006
Příspěvky pro sborník:	20. listopadu 2006
Konání MKB 2005:	7. – 8. prosince 2006

Programový výbor

Dan Cvrček, FIT VUT v Brně – předseda
Antonín Beneš, SAP ČR
Vašek Matyáš, FI MU Brno
Daniel Olejár, FMFI UK Bratislava
Tomáš Rosa, eBanka
Zdeněk Říha, FI MU Brno
Martin Stanek, FMFI UK Bratislava
Jan Staudek FI MU Brno
Pavel Vondruška, ČESKÝ TELECOM, a.s

E. O čem jsme psali v květnu 1999 – 2005

Crypto-World 5/2000

+ příloha : J.Hrubý , soubor QNG.PS

Crypto-World 5/2001

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

F. 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/