Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 7, číslo 5/2005 **15. květen 2005**

5/2005

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

Obsah : **str.**

Příloha : zpráva vysílaná radioamatérskou stanicí GB2HQ - nedele_30m.wav

A. Výzva k rozluštění textu zašifrovaného Enigmou

Pavel Vondruška, ČESKÝ TELECOM, a.s.,
(pavel.vondruska@crypto-world.info)

Během minulého víkendu (7.5.-8.5.) si mohli radioamatéři otestovat, jak před 60-ti lety vypadala práce jejich kolegů – profesionálů v armádních službách. V éteru se ozval signál radiové stanice GB2HQ, která v morseovce odvysílala text zašifrovaný Enigmou. Pro zájemce je nahrávka tohoto vysílání uvedena jako příloha k tomuto e-zinu nebo si ji můžete stáhnout z adresy http://crypto-world.info/casop7/nedele_30m.wav .

Nyní předávám slovo jednomu z našich stálých čtenářů. E-zin odebírá prakticky od samého začátku a úspěšně se zúčastnil námi pořádaných podzimních luštitelských soutěží. Přikládám jeho e-mail (mírně „cenzurovaný“), ve kterém mne upozornil na toto vysílání a ve **kterém žádá o pomoc při vyluštění zachyceného textu** .

---------- Original Message ----------
From: "OK1DF" <ok1df@qsl.net>
Date: Tue, 10 May 2005 14:25:44 +0100

Vážený pane magistře,
dovoluji si nahlásit, že jsem rozšířil počet zemí, kde jsou čtenáři Crypto-Worldu, o zemi určitě ještě "neobsazenou" a to je Alžírsko, kde ….. (mimochodem, vína tu mají také kvalitní).

Obracím se na Vás s prosbou:

Minulý víkend vysílala anglická radioamatérská stanice GB2HQ zprávu zašifrovanou Enigmou. Přikládám nahrávku, ale bohužel je v telegrafní abecedě, ale i tak - pro zajímavost.

Blíže viz: http://www.princ7.demon.co.uk/enigma.htm

Bohužel, nebo asi schválně, text je dlouhý pouhých 20 znaků.

A to je samozřejmě **výzva k luštění**. Prohledal jsem Internet, ale bohužel vzhledem k místním podmínkám připojení (dial up - stále se rozpadává), je to náročné. Našel jsem jeden program, ten však bohužel luští Enigmu jen do roku 1938, tj. výběr jen ze tří rotorů.

Proto se dovoluji na Vás obrátit, zda nevíte o nějakých programech na luštění Enigmy ???

Radiogram, který je na stránkách uveden jako příklad (v FAQ), mně stále vychází jako řada Q, tedy 20x Q.

Děkuji a se srdečným pozdravem
…..

Zdravím a děkuji!

---------- Original Message ----------

From: "OK1DF" <ok1df@qsl.net>

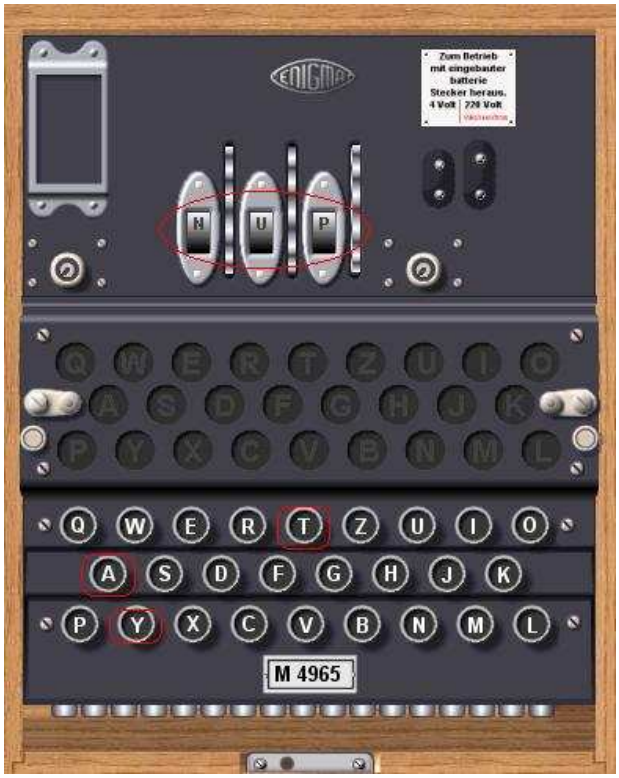
Teprve nyní jsem si uvědomil, že jsem Vám neposlal to nejdůležitější - text radiogramu.

Tedy:

QRX
QTC QTC = SPECIAL ENIGMA STN =
NW QTC =

CQ CQ CQ DE GB2HQ GB2HQ GB2HQ
= ENIGMA MESSAGE =

1200 20 NUP AYT =
ZCSIU ECZCD YOEFX NGRDP = RPT =
ZCSIU ECZCD YOEFX NGRDP +



Význam jednotlivých Q-kódů a zkratek:
CQ = všeobecná výzva
DE = zde, tady
STN = stanice

QRX = zavolám Vás později (nebo možno doplnit časovým údajem = QRX 10.00, zavolám Vás v 10.00)
QTC = mám pro Vás telegram (QTC 3 = tři tlg)
NW = nyní
RPT = opakuji
+ = konec zprávy
GB2HQ = volací znak anglické radioamatérské organizace (HQ = HeadQuarter)

Děkuji za pomoc!!!

Věřím, že mezi čtenáři je řada těch, které také zajímá, co vlastně stanice GB2HQ v zašifrované podobě odvysílala**. Pokud se vám podaří text rozšifrovat – prosím o jeho zaslání kolegovi do Alžíru (ok1df@qsl.net). Pomoci mu můžete i nalezením vhodného programu na luštění** (nikoliv pouhý simulátor)**.**

Pokud jde o výborný simulátor Enigmy – pak doporučuji ADVANCED ENIGMA SIMULATOR SOFTWARE PROGRAM: (2500KB) od Dirka Rijmenantse http://w1tp.com/enigma/#Enigma

Současně prozradím, že ti, kteří se této výzvě budou věnovat, získají i určitý náskok v chystané podzimní soutěži 2005.

B. Přehledová zpráva o významných publikacích a projektech na téma poskytování anonymity, klasifikace a měřitelnost informačního soukromí (privacy), část 1.

Mgr. Marek Kumpošt , Fakulta informatiky, MU, Brno
(xkumpost@fi.muni.cz **)**

Tato zpráva má za cíl prezentovat dosavadní průzkum v dané oblasti a seznam významných publikací a projektů na dané téma, které jsem pročetl během prvního semestru Ph.D. studia na Fakultě Informatiky.

Zpráva je strukturována tak, že ke každé odkázané literatuře je připojen krátký text shrnující problematiku popisovanou v daném článku. V seznamu referencí uvádím veškerou literaturu, tedy případně i tu, která nebude v textu odkázána.

Vzhledem k rozsahu původní zprávy je nezbytné její publikování v několika samostatných částech. V této úvodní části se zaměříme na publikace související s terminologií používanou ve světe anonymizačních systémů, články věnované mixovacím systémům, mixovacím sítím a Onion Routingu.

Terminologie

Definice nejpoužívanějších pojmů z oblasti informačního soukromí uvádí [PK01]. Ve svém článku definuje pojmy *anonymita*, *nespojitelnost*, *nesledovatelnost* a *pseudonymita* a rozebírá různé pohledy a přístupy při definování těchto pojmů (pohled Společných kritérií vs. pohled mixovacích systémů). V dalších částech textu pak uvádí základní vztahy a vzájemné souvislosti mezi těmito pojmy. Zbývající část dokumentu detailně pojednává o pseudonymitě a vztahu pseudonymity k nespojitelnosti. Na základě tohoto rozboru pak autor definuje některé další pojmy a termíny.

Terminologii z oblasti Onion Routingu se věnuje článek [Cla03]. V příspěvku autor navrhuje nový formální zápis struktury zvané Onion. Návrh nového zápisu vzešel z debaty na konferenci PET2003. V úvodu článku autor uvádí, jak by měla notace pojmu vypadat a jaké vlastnosti by měla splňovat, co se formálního zápisu týče. Nově navrhovaný zápis má tvar: $|R_0, T\#K_a|R_1, *, A\#K_1$ a čteme jej: paket šifrovaný veřejným klíčem K_1 obsahující náhodnou hodnotu R_1, adresa A dalšího routeru a paket pro tento router, zašifrovaný jeho veřejným klíčem a obsahující náhodnou hodnotu R_0 a výslednou zprávu T. Hvězdička se používá k označení vnějších slupek. Paket, který neobsahuje hvězdičku, je výsledek poslední dešifrovací operace. Jednou z výhod uvedeného zápisu je skutečnost, že není třeba hlídat uzávorkování. Autor v článku dále ještě mírně upravuje navrhovanou notaci. V závěru jsou uvedeny zápisky s diskuze, která při navrhování nové notace proběhla.

Dobrý článek se základními informacemi z oblasti anonymizačních systémů (definice pojmů, základní rozdělení, různé systémy pro zajištění anonymity, měřitelnost apod.) poskytuje publikace [Wri04]. Jedná se o teze disertační práce.

Články věnované mixům

[Cha81] je dokument s prvotním návrhem MIX systémů. Jedná se o publikaci Davida L. Chauma z roku 1981 a ve svém příspěvku popisuje systém založený na kryptografii s veřejným klíčem použitelný pro posílání anonymních zpráv, tzn. takových zpráv, u kterých není zpětně možné zjistit jejich původce nebo příjemce. Systém dále umožňuje i utajení vlastního obsahu přenášených zpráv, takže útočník nejen, že nezjistí, kdo s kým aktuálně komunikuje, ale ani nemá možnost získat čitelná data. V příspěvku jsou dále uvedeny některé další aplikace uvedeného návrhu, jako jsou například elektronické volby nebo použití pseudonymů. Systém MIX je zde prezentován jako obranný mechanismus před tzv. útokem analýzou provozu, kdy se útočník snaží získat identifikační údaje pouhým sledováním provozu v síti.

[BFK01] se zabývá problematikou WEB-mixů. Prezentuje architekturu MIX-based systému pro anonymní (a real-time) přístup na Internet. Navrhovaný systém by měl zabránit útokům analýzou provozu a útokům záplavou (flooding attacks). Ochrana před druhým typem útoků spočívá v autentizaci založené na autentizačních lístcích (ticket-based authentication). Systém podporuje generování falešného provozu v situacích, kdy jsou uživatelé neaktivní. V systému existuje mechanizmus informující uživatele o aktuální míře poskytované anonymity. Adresa webových stránek tohoto projektu je: http://www.inf.tu-dresden.de/hf2/anon/. V článku jsou také rozebrány různé další typy útoků na navrhovaný systém.

[DP04a] se věnuje analýze mixů a falešného provozu, což jsou základní stavební kameny pro systémy poskytující anonymitu. Cílem článku je spojit veškeré otázky týkající se analýzy a návrhu mixovacích sítí. V článku jsou diskutovány různé typy mixovacích systémů, dále pak topologie mixovacích sítí a politiky falešného provozu. Autoři prezentují klady a zápory návrhu mixů a politik falešného provozu. V závěru článku jsou uvedeny problémy pro další výzkum v oblasti, která je v článku představena.

[DP04b] v článku studují míru anonymity, kterou poskytuje obecný mixovací systém, který do sítě posílá falešné zprávy. V článku je uvedeno, jak počítat anonymitu poskytnutou jak příjemci, tak odesílateli zprávy. Je prezentován postup vyhodnocení anonymity nejprve v případě, že se falešný provoz v síti negeneruje a poté je anonymita vyhodnocena za předpokladu, že v síti existuje i tento falešný provoz. Výsledky jsou porovnány a komentovány. Dále jsou diskutovány dva možné přístupy, jak do sítě vkládat falešný provoz a tyto dvě metody jsou porovnány (falešná zpráva je buď ponechána v paměti mixu a zpracována jako každá jiná příchozí zpráva a nebo je ihned po vygenerování odeslána dále do sítě). V závěru článku je demonstrována praktická analýza systému, na který je veden útok.

Porovnáním dvou konkrétních přístupů k mixovací strategii je věnována publikace [DSD04]. Autoři zde provádějí porovnání systému Mixminion a systému Reliable, kde druhý jmenovaný je zástupcem tzv. stop-and-go mixovací technologie. V úvodu článku jsou oba dva typy stručně popsány a jsou diskutovány rozdíly z hlediska funkcionality. Dále je představena metodika použitá pro porovnání zmiňovaných systémů a je uveden model útočníka. Následuje stručný popis simulátoru, který byl použit pro testování. Další část je věnována diskuzi k výsledkům simulací (jsou zde uvedeny různé grafy pro ilustraci rozdílů). Závěrečná část je věnována rozboru dalších faktorů ovlivňujících anonymitu poskytovanou systémem (stručně je popsáno poměrně velké množství různých aspektů). V příloze dokumentu je uvedena metodika použitá pro vyhodnocení výsledků simulace.

[KEB98] je článek věnovaný novému typu mixovacího systému, tzv. continuous nebo stop-and-go mixů (do češtiny by se tento název mohl přeložit jako průběhové mixy). Důvodem pro zavedení tohoto přístupu při mixování je fakt, že v otevřených systémech není zajištěna verifikace identity, čehož by útočník mohl zneužít a získat citlivá data od poctivých uživatelů systému. Dále je prezentován termín pravděpodobnostní anonymity (probabilistic anonymity). V úvodu článku autoři diskutují systémy, které byly v té době dostupné, a zdůrazňují skutečnost, že v těchto systémech je prováděna verifikace identity, což ovšem v prostředí Internetu nemusí být vždy možné. Následuje rozbor dostupných technik pro poskytování anonymity a jsou diskutovány jejich nevýhody a nedostatky. Následuje definice pojmu pravděpodobnostní bezpečnost (probabilistic security). V další části se již autoři věnují popisu nového návrhu mixovacího systému, diskutují jeho bezpečnost, odolnost (nebo prevenci) proti *n*-1 útoku a věnují se také určování velikosti anonymitní množiny.

Článek [MD04] se věnuje konkrétnímu mixovacímu systému - systému Mixminion [MIX]. Jedná se o systém navržený Georgem Danezisem [Dan04] pro anonymní posílání emailových zpráv. V článku jsou diskutovány důvody pro nasazení silného anonymizačního systému do komerční sféry, jmenovitě pak finančního sektoru. Dále krátce pojednává o původním návrhu Davida Chauma [Cha81] a zbytek článku je pak již věnován systému Mixminion. Jsou zde diskutovány jeho výhody a poskytovaná funkcionalita. Na závěr jsou pak diskutovány některé vybrané oblasti pro budoucí vývoj v oblasti těchto systémů.

Článek [DS03b] se zabývá systémem pro vyjádření mixovací strategie mixovacího systému. Autoři uvádějí, že na mixování lze pohlížet jako na funkci z množiny vstupních zpráv do množiny výstupních zpráv. Dále je uvedeno, jak vyjádřit existující mixovací strategie s ohledem na navržený systém, a autoři také uvádějí návrh několika dalších přístupů pro mixování. Poznamenávají, že tyto návrhy nelze vyjádřit ve smyslu pool mixů. Návrh nového mixu, tzv. binomial mix, je pool mix s časovou podmínkou, který si „hází“ mincí a uvažuje pravděpodobnostní funkci závisející na množství zpráv v mixu v čase odeslání zpráv. V úvodu článku jsou porovnány různé mixovací strategie a jsou diskutovány jejich výhody a nevýhody. Následně je uveden pojem *obecného mixu*, jakožto funkce. Ve zbývající části je pak uveden a diskutován nově navrhovaný mixovací systém, je diskutována odolnost proti vybraným útokům a některé negativní aspekty tohoto přístupu. V závěru autoři shrnují problematiku a diskutují směry dalšího výzkumu.

Články věnované mixovacím sítím

Článek [BPS01] se zabývá detailním porovnáním různých přístupů při volbě cesty v mixovacích sítích. Porovnává fixní mixovací cesty v kaskádových sítích a libovolné mixovací cesty v mixovacích sítích bez omezení. Prezentují výhody a nevýhody jmenovaných přístupů a diskutují možné útoky na tyto dva typy mixovacích sítí. Dále je v příspěvku rozebrán vliv útoků na míru poskytované anonymity a významnost útoků s ohledem na vybrané existující systémy (Mixmaster, Crowds, Freedom).

Mixovacím sítím se také věnuje [Dan03]. Ve svém příspěvku prezentuje návrh nového přístupu pro budování mixovací sítě, který je založen na tzv. sparse expander grafech. V článku popisuje návrh tohoto přístupu a jeho výhody. V další části příspěvku je diskutován systém pro porovnání různých mechanizmů pro budování mixovacích sítích (plně propojená síť, kaskádová síť, síť založená na expander grafech). Následně je prezentována analýza anonymity v kaskádových sítích, ochrana proti útoku průnikem. V další sekci je porovnání

všech prezentovaných topologií. V závěru je, pro ilustrování navrhovaného přístupu, uveden příklad sítě využívající této topologie a je provedena její analýza. Také je prezentována odolnost vůči útokům průnikem a analýzou provozu.

Zajímavý přístup v oblasti kaskádových mixovacích sítí prezentuje [DS02]. Ve svém příspěvku popisuje protokol pro kaskádové sítě s využitím reputace. Cílem je zvýšit spolehlivost sítě. Mixy periodicky generují společné náhodné semínko (seed), které je, společně s jejich reputací, použito pro konfiguraci sítě. Uzly v síti posílají testovací zprávy a monitorují tak své kaskády. Existují mechanizmy umožňující přesvědčit poctivé uživatele sítě, že daná kaskáda se nechová správně a zřejmě je vůči ní veden útok. V důsledku toho, že každý uzel může oznámit poškození své kaskády, není nutná existence centrálního důvěryhodného svědka. Také je prezentována odolnost vůči útokům průnikem a analýzou provozu. V článku je dále uveden popis reputačního systému pro ohodnocování uzlů a vlastní konfigurace kaskády. V závěru jsou uvedeny některé možné útoky na tento protokol. Jiným článkem na téma reputační systémy a mixovací sítě je [DFHM01], využitím reputace v P2P sítích se zabývá např. [DMS03].

Články věnované Onion Routingu

Problematice tzv. cibulového směrování (Onion Routing) se věnuje [RSG99] v příspěvku s názvem *Anonymous Connections and Onion Routing*. Jedná se o technologii pro zajištění anonymity v prostředích, kde je nutný real-time přenos dat a nejsou přípustné latence, které jsou typické pro mixovací systémy. Onion Routing poskytuje obousměrné anonymní propojení pro různé aplikace. V původním návrhu byly podporovány ty aplikace, pro které byla napsána speciální proxy fungující jako most mezi zvolenou aplikací a Onion Routing sítí. Příkladem takových aplikací je třeba běžné brouzdání na Internet, ftp přenos dat, ssh spojení, VPN sítě apod. V příspěvku je detailně popisována technologie Onion Routingu, definice útočníka a rozbor možných útoků, popis vlastní implementace a seznam typických využití. Analýze bezpečnosti Onion Routing systému se věnují autoři článku [STRL01].

[DMS04] představuje nový systém v oblasti Onion Routingu, totiž TOR (The Onion Router). Jedná se o vylepšenou implementaci původního návrhu, který je popisován v [RSG99]. Použití systému a jeho základní vlastnosti jsou stejné jako v původním návrhu, přibyla však řada nových vlastností a vylepšení na základě nových požadavků na funkcionalitu tohoto typu systému. V článku jsou detailně probrány všechny nově přidané funkce a jsou diskutovány jejich výhody a důvody pro implementaci v systému TOR. Dále je uveden návrh systému (struktura paketů, ustanovení komunikačních cest apod.). V závěrečné části jsou rozebrány některé typické útoky na tento typ systému a je zde prezentována obrana, kterou proti těmto útokům poskytuje nově navržený systém.

V příštím čísle Crypto-Worldu se zaměříme na mixovací sítě, peer-to-peer systémy, měření anonymity, některé teoretické aspekty anonymizačních systémů a útoky na systémy pro poskytování anonymity.

Použitá literatura:

[BFK01] O. Berthold, H. Federrath, and S. Köpsell. Web MIXes: A System for Anonymous and Unobservable Internet Access. *Anonymity 2000*, LNCS 2009, pages 115-129. Springer-Verlag, 2001.

[BPS01] O. Berthold, A. Pfitzmann, and R. Standtke. The Disadvantages of Free MIX Routes and How to Overcome Them. *Anonymity 2000*, LNCS 2009, pages 30-45. Springer-Verlag, 2001.

[Cha81] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communication of the ACM*, Volume 4, number 2, February 1981.

[Cla03] R. Clayton. Improving Onion Notation. *Privacy Enhancing Technologies Workshop (PET 2003)*, LNCS 2137, pages 245-267. Springer-Verlag, 2003.

[Dan03] G. Danezis. Mix-Networks with Restricted Routes. *Privacy Enhancing Technologies Workshop (PET 2003)*, LNCS 2760, pages 1-17. Springer-Verlag, 2003.

[Dan04] G. Danezis. *Designing and attacking anonymous communication systems*. PhD thesis, University of Cambrigde, Computer Laboratory, January, 2004.

[DFHM01] R. Dingledine, Michael J. Freedman, D. Hopwood, and D. Molnar. A Reputation System to Increase MIX-net Reliability. *Information Hiding Workshop (IH 2001)*, LNCS 2137, pages 126-141. Springer-Verlag, 2001.

[DMS03] R. Dingledine, N. Mathewson, and P. Syverson. Reputation in P2P Anonymity Systems. *Workshop on Economics of Peer-to-Peer Systems*, June, 2003.

[DMS04] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. *13th USENIX Security Symposium*, August, 2004.

[DP04a] C. Díaz and B. Preneel. Taxonomy of Mixes and Dummy Traffic. *Information Security Management, Education and Privacy. IFIP 18th World Computer Congress TC11 19th International Information Security Workshops*, August, 2004.

[DP04b] C. Díaz and B. Preneel. Reasoning About The Anonymity Provided By Pool Mixes That Generate Dummy Traffic. *Information Hiding Workshop (IH 2004)*, LNCS 3200, pages 309-325. Springer-Verlag, 2004.

[DS02] R. Dingledine and P. Syverson. Reliable MIX Cascade Networks through Reputation. *Financial Cryptography (FC'02)*, LNCS 2357. Springer-Verlag, 2002.

[DS03b] C. Díaz and A. Serjantov. Generalising Mixes. *Privacy Enhancing Technologies Workshop (PET 2003)*, LNCS 2760, pages 18-31. Springer-Verlag, 2003.

[DSD04] C. Díaz, L. Sassman, and E. Dewitte. Comparison Between Two Practical Mix Designs. *ESORICS 2004*, LNCS 3193, pages 141-159. Springer-Verlag, 2004.

[KEB98] D. Kesdogan, J. Egner, and R. Büschkes. Stop-and-go MIXes: Providing Probabilistic Anonymity in an Open System. *Information Hiding Workshop (IH 1998)*, LNCS 1525, pages 83-98. Springer-Verlag, 1998.

[MD04] N. Mathewson and R. Dingledine. Mixminion: Strong Anonymity for Financial Cryptography. *FC 2004*, LNCS 3110, pages 227-232. Springer-Verlag, 2004.

[MIX] *Mixminion: A Type III Anonymous Remailer - project development page*. http://www.mixminion.net.

[PK01] A. Pfitzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. *Anonymity 2000*, LNCS 2009, pages 1-9. Springer-Verlag, 2001.

[RSG99] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection*, 1999.

[STRL01] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr. Towards an Analysis of Onion Routing Security. *Anonymity 2000*, LNCS 2009, pages 96-114. Springer-Verlag, 2001.

[Wri04] J. Wright. Designing Anonymity: A Formal Basis for Identity Hidding. Technical report, Department of Computer Science, University of York, Heslington, York, June, 2004.

C. Kryptografie a normy
Formáty elektronických podpisů - část 4.
(dokument ETSI TS 101 7733 - Electronic Signature Formats)

Jaroslav Pinkava, PVT a.s. (jaroslav.pinkava@pvt.cz)

1. Úvod

V prvních dvou částech tohoto článku (Crypto-World 11/2004 a Crypto-World 1/2005) byly popsány jednotlivé formáty elektronického podpisu dle dokumentu ETSI [1] TS 101 733. Jednalo se postupně o formáty - základní (BES, EPES), s časovým razítkem (ES-T), tzv. rozšířené formáty (ES-X) atd. Posledním formátem byl archivační formát elektronického podpisu ES-A. Minulé pokračování bylo věnováno definicím souvisejících atributů (kapitola 5. a 6 dokumentu ETSI TS 101 733). Zbývající část dokumentu tvoří přílohy. První z nich - příloha A - popisuje ASN.1 syntaxi podpisových formátů. Příloha B dává přehled atributů, které musí být obsaženy v různých formátech rozšířených elektronických podpisů a také příklady validace podpisů v těchto rozšířených formátech.

2. Validační data a rozšířené formáty

Z předešlého vyplývá, že elektronický podpis ve formátu ES-X Long vzniká tehdy, jestliže jsou k formátu ES-C přidány hodnoty certifikátů a revokační informace. Tento formát je užitečný v těch situacích, kdy ověřující strana nemá přímý přístup k následujícím informacím:
- certifikát podepsané strany;
- všechny certifikáty CA, které leží na úplné certifikační cestě;
- celou informaci o souvisejícím revokačním statutu, na kterou je odkazováno v ES-C.

V některých situacích přitom mohou k podpisům být vytvářeny a přidávány další časové značky jako přidané atributy. Např. časová značka přes všechny validační data obsažená v ES-C (to je formát ES-X Type 1) anebo přes jednotlivé odkazy používané pro úplnou validaci (formát ES-X Type 2).
Pokud jsou využívány kombinace předešlých formátů, hovoříme o formátech ES X-Long Type 1 a ES X-Long Type 2.

2.1. Formát ES X-Long

Skládá se z následujícího:
- BES či EPES ;
- atribut complete-certificate-references;
- atribut complete-revocation-references.

Požadovány jsou také následující atributy (pokud ES není označeno časovým markerem):
- atribut signature-time-stamp

a pokud nejsou úplné hodnoty certifikátů a revokačních informací již zahrnuty v BES či EPES:
- atribut certificate-values;
- atribut revocation-values.

V případě, že jsou používány atributové certifikáty, pak mohou být přítomny:
- atribut attribute-certificate-references;
- atribut attribute-revocation-references.

2.2. Formát ES-X Type 1

Skládá se z následujího:
- BES či EPES ;
- atribut complete-certificate-references;
- atribut complete-revocation-references.
- atribut ES-C-Timestamp

Požadovány jsou také následující atributy (pokud ES není označeno časovým markerem):
- atribut signature-time-stamp.

V případě, že jsou používány atributové certifikáty, pak mohou být přítomny:
- atribut attribute-certificate-references;
- atribut attribute-revocation-references.

Mohou být přítomny také další nepodepsané atributy, ale nejsou vyžadovány.

2.3. Formát ES-X Type 2

Skládá se z následujícího:
- BES či EPES ;
- atribut complete-certificate-references;
- atribut complete-revocation-references;
- atribut time-stamped-certs-crls-references.

Požadovány jsou také následující atributy (pokud ES není označeno časovým markerem):
- atribut signature-time-stamp.

V případě, že jsou používány atributové certifikáty, pak mohou být přítomny:
- atribut attribute-certificate-references;
- atribut attribute-revocation-references.

Mohou být přítomny také další nepodepsané atributy, ale nejsou vyžadovány.

2.4. Formát ES-X Long Type 1 a ES-X Long Type 2

Skládá se z následujícího:
- BES či EPES ;
- atribut complete-certificate-references;
- atribut complete-revocation-references;
- atribut time-stamped-certs-crls-references.

Požadovány jsou také následující atributy (pokud ES není označeno časovým markerem):
- atribut signature-time-stamp

a pokud nejsou úplné hodnoty certifikátů a revokačních informací již zahrnuty v BES či EPES:
- atribut certificate-values;
- atribut revocation-values.

V případě, že jsou používány atributové certifikáty, pak mohou být přítomny:
- atribut attribute-certificate-references;
- atribut attribute-revocation-references.

Je také požadován jeden z následujících atributů:
- atribut ES-C-Timestamp;
- atribut time-stamped-certscrls-references.

Mohou být přítomny také další nepodepsané atributy, ale nejsou vyžadovány.

2.4. Rozšíření vztahující se k časovým značkám

Každé zařazení atributu Time-stamp může obsahovat (jako nepodepsané atributy v SignedData) následující atributy (vztažené k TSU):

- atribut complete-certificate-references;
- atribut complete-revocation-references;
- atribut certificate-values;
- atribut revocation-values.

Mohou být přítomny také další nepodepsané atributy, ale nejsou vyžadovány.

2.5. Formát ES-A

Dříve než se stanou slabými použité algoritmy (resp. klíče či jiná kryptografická data), měla by být podepsaná data, ES-C a další informace (např. ES-X) opatřena časovým razítkem. A to pokud možno takovým, které používá silnější kryptografický algoritmus (či delší klíč) než původní časová značka. To se může dít opakovaně a tedy ES-A může obsahovat více časových značek (včleněných v sobě).
ES-A se skládá z následujícího:

- BES či EPES;
- atribut complete-certificate-references;
- atribut complete-revocation-references;
- atribut time-stamped-certs-crls-references.

Požadovány jsou také následující atributy (pokud ES není označeno časovým markerem):

- atribut signature-time-stamp.

V případě, že jsou používány atributové certifikáty, pak mohou být přítomny:

- atribut attribute-certificate-references;
- atribut attribute-revocation-references.

Pokud nejsou úplné hodnoty certifikátů a revokačních informací již zahrnuty v BES či EPES:

- atribut certificate-values;
- atribut revocation-values.

Je také požadován jeden z následujících atributů:

- atribut ES-C-Timestamp;
- atribut time-stamped-certscrls-references.

Je vyžadován:

- atribut archive-time-stamp

(může být přítomen vícekrát a to i od různých TSU).
Mohou být přítomny také další nepodepsané atributy, ale nejsou vyžadovány. Ve vztahu k archivní časové značce zde mohou být obsaženy atributy:

- atribut TSU complete-certificate-references;
- atribut TSU complete-revocation-references;
- atribut TSU certificate-values;
- atribut TSU revocation-values.

V příloze B je dále uveden příklad posloupnosti probíhající validace.

3. Popis některých použitých koncepcí (příloha C)

Podpisová politika:

Podpisovou politikou chápou autoři množinu pravidel pro vytváření a ověřování elektronického podpisu, v rámci kterých lze určit, zda je el. podpis platný. Pokud tuto politiku vztáhneme k příslušným legislativním (smluvním) podmínkám, lze říci, zda daná politika příslušné, z nich vyplývající požadavky splňuje. Podpisová politika může být např. vydána stranou, která se spoléhá na el. podpisy a je volena podepisující se stranou pro daný účel, nebo může být vydána obchodní organizací pro používání členstvem této obchodní organizace. Jak podepisující se strana, tak i ověřující strana používají tutéž podpisovou politiku.

Podpisová politika musí být dostupná v čitelné a srozumitelné (pro uživatele) podobě a za účelem elektronického zpracování musí být také definovaná v počítačově zpracovatelném tvaru.

Podpisová politika zahrnuje:

- pravidla, která se používají pro technickou validaci konkrétního podpisu;
- pravidla, která vyplývají z přijetí Certifikační Politiky aplikované na el. podpis (např. pravidla pro ochranu soukromého podpisového klíče);
- pravidla, která se vztahují k prostředí, které používá podepisující se strana (např. dohodnutá čtečka karet) ve spojení s čipovou kartou.

Podepisovaná informace:

Informace, která je podepisována, může být definována např. jako zpráva v obálce MIME a odsud je pak odvozován formát obsahu (tak, aby byl obsah správně zobrazen).

Komponenty elektronického podpisu:

Pokud dvě nezávislé strany chtějí vyhodnotit elektronický podpis, je důležité, aby vždy dospěly k témuž výsledku. Tuto podmínku lze splnit používáním zevrubné podpisové politiky takové, která zajišťuje konzistenci validace elektronického podpisu. Zde jsou mj. popsány následující komponenty:

K1. Odkaz na podpisovou politiku
K2. Indikace typu sdělení
K3. Identifikace certifikátu podepisující stranou
K4. Atributy rolí (nárokovaných, certifikovaných)
K5. Lokace podepisující strany
K6. Čas podpisu
K7. Formát obsahu
K8. Křížové reference obsahu

Obdobně je nutné se zabývat (při ověřování) následujícími komponentami.

Komponenty validačních dat:

L1. Informace o revokačním statutu
L2. Informace obsažená v CRL
L3. Informace z OCSP
L4. Certifikační cesta

L5. Časové značky zajišťující dlouhodobou platnost podpisů
L6. Časové značky zajišťující dlouhodobou platnost podpisů před možnou kompromitací klíče CA
L7. Časové značky pro archivaci podpisu
L8. Odkazy na další data
L9. Kompromitace klíče TSA

Poznámka: V materiálu jsou jednotlivé komponenty podrobněji rozebírány (z hlediska jejich nezbytných vlastností).

Vícenásobné podpisy:

Některé elektronické podpisy jsou platné pouze tehdy, pokud souvisí s dalšími podpisy. Příkladem je smlouva dvou stran. Pořadí podpisů přitom může či nemusí být důležité.
Existují přitom dvě základní kategorie:

- nezávislé podpisy;
- včleněné podpisy.

4. Ostatní přílohy

Již jen stručně. Příloha D popisuje požadované vlastnosti operačních protokolů pro komunikaci s poskytovatelem časových razítek. Příloha E se zabývá ochranou soukromého (podpisového) klíče. Informativní příloha F dává příklad strukturovaného obsahu zprávy (dle MIME - RFC 2045, resp. S/MIME).

Příloha G. poukazuje na vztah mezi podpisy, které jsou vytvářeny na základě daného dokumentu ETSI a požadavky Evropského parlamentu a Evropské komise (Směrnice EU, normy EESSI).

Příloha H odkazuje na existující API (Application Programming Interface) pro manipulaci se strukturami, které jsou popisovány v daném dokumentu. Jedno z nich definovalo IETF a druhé OMG (Object Management Group).
Příloha I popisuje odkazy na používané kryptografické algoritmy. Jednak hashovací algoritmy - SHA-1, MD5, ale také širší třídy popsané v normách ISO/IEC 10118 a dalších dokumentech. Jednak jsou zde odkazy na podpisové algoritmy - DSA (FIPS PUB.186), RSA (RFC 2437, RFC 3370) a také je zde odkaz na dokumenty IEEE P1363 resp. normy ISO, které obsahují širší škály algoritmů.

Příloha J se zabývá problematikou přidělování jmen subjektem prostřednictvím registrační autority - tak, aby byla zajištěna jejich jednoznačnost. Konečně příloha K obsahuje přehled bibliografie.

5. Literatura

[1] ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
[2] RFC 3126, Electronic Signature Formats for long term electronic signatures

D. Jak psát specifikaci bezpečnosti produktu nebo systému

Pavel Vondruška, ČESKÝ TELECOM, a.s.,
(pavel.vondruska@crypto-world.info)

1. Specifikace bezpečnosti - úvod

Specifikace bezpečnosti produktu nebo systému (dále pro systém a produkt zavedeme zkratku SP) by měla poskytnout všem jeho uživatelům základ pro jejich uživatelská rozhodnutí a je podkladem pro subjektivní (uživatel) či objektivní hodnocení (hodnotitel).

Doporučuje se, aby při psaní specifikace bezpečnosti bylo použito cizí odborné asistence, tj. aby ji nepsal dodavatel či vývojář. Vývojář může spolupracovat na vytváření specifikace pro následnou implementaci, ale neměl by ji její vytváření řídit či kompletovat.

Specifikace bezpečnosti je rozsáhlý, podrobný dokument (nebo sada několika dokumentů), který definuje zejména:
a) bezpečnostní cíle produktu nebo systému (SP),
b) protiopatření, zabudovaná do SP, za účelem eliminace hrozeb.
c) poskytuje bezpečnostní požadavky a záruky, kladené na SP, popsané na vysoké rovni abstrakce.

Specifikace bezpečnosti musí jednoznačně definovat schopnosti SP a jeho možné způsoby použití. Specifikace bezpečnosti se zpravidla zabývá procedurální, funkční a technickou problematikou. Na základě požadavků může také zahrnovat jiná hlediska, jako je například podpora dodavatele nebo vývojáře.

2. Obsah specifikace bezpečnosti

Aby specifikace bezpečnosti splnila svoji úlohu (zejména v případě použití jako podkladu pro hodnocení SP) musí:
a) podrobně uvést bezpečnostní požadavky na SP,
b) definovat protiopatření, která mají zabránit identifikovaným hrozbám.

Pro naplnění těchto podmínek se požaduje, aby:
a) bezpečnostní požadavky byly pokryty bezpečnostní politikou (v případě systému) nebo popisem produktu (pro produkt),
b) byly vytvořeny a popsány funkce, které odpovídají bezpečnostní požadavkům (tyto funkce se nazývají *funkce prosazující bezpečnost*),
c) v případě, že pro splnění bezpečnostních požadavků jsou potřebné speciální technické přístupy (například algoritmus pro šifrování hesel), tyto přístupy byly uvedeny v seznamu požadovaných bezpečnostních mechanismů,
d) byla definována minimální síla mechanismů a to zpravidla ve stupnici *základní*, *střední* a *vysoká*,
e) pokud je podkladem pro hodnocení, musí být specifikována cílová úroveň hodnocení a standard, který má být použit (ITSEC, CC, ...).

V závislosti na cílové úrovni hodnocení musí být funkce prosazující bezpečnost specifikovány požadovaným způsobem tj. neformálně, poloformálně nebo formálně.

3. Analýza rizik

U každého SP musíme volit kompromis mezi potřebou chránit aktiva a cenou této ochrany (sem patří pořizovací náklady, náklady na audit, podporu, lidské zdroje, provozní a technické náklady). Tyto kompromisy jsou voleny s ohledem na výsledky procesu analýzy rizik. Výsledek nám slouží ke specifikaci funkcí prosazujících bezpečnost daného SP.

Proces konstrukce SP je však ovlivněn nejen zvolnými funkcemi prosazujícími bezpečnost, ale i jinými omezeními SP (například zákony, nařízeními, technologií, naším know-how, tradicí, oblíbeností, výběrem dodavatele atd.).

Analýza rizik zjišťuje hrozby, které ohrožují aktiva, která má chránit popisovaný SP. Pro každou hrozbu musí být zjištěna pravděpodobnost ohrožení aktiv touto hrozbou.
Analýza rizik musí být provedena se provádí jako jedna z prvních činností při vývoji SP.

Proces analýzy rizik ovlivňuje vytváření specifikace bezpečnosti, neboť spojuje aktiva, hrozby a protiopatření do formy, která je použitelná ve specifikaci bezpečnosti.

Analýza rizik se skládá z posloupnosti činností, které jsou prováděny se specifikacemi a požadavky.
Tyto činnosti jsou následující:
a) analýza problému (která se zabývá prostředím a požadavky),
b) identifikace volitelných možností (která se zabývá aktivy, hrozbami a omezeními),
c) ohodnocením jednotlivých řešení (které berou v úvahu přívětivost řešení, vhodnost a cenu protiopatření),
d) vypracování zprávy.

Různé varianty tohoto procesu jsou popsány ve standardních metodologiích (například CRAMM, MARION, MELISA, Acertus, viz např. http://www.riskworld.com/SOFTWARE/). Tyto metodologie jsou zejména užitečné při vytváření knihoven prostředků, hrozeb a tříd protiopatření.

Pokud není použita žádná metodologie, je vhodné použít alespoň některé vhodné generické specifikace. Vhodnými příklady mohou v takovém případě být modely bezpečnosti otevřených systémů ISO nebo např. předdefinované třídy funkčnosti kritérií ITSEC apod..

4. Systémová bezpečnostní politika nebo Popis produktu

4.1 Obecné požadavky

Specifikace bezpečnosti obsahuje na svém začátku soupis informací o hrozbách, cílech a prostředí v němž SP bude nasazen nebo již pracuje. V případě systému tvoří tyto informace *systémovou bezpečnostní politiku*. V případě produktu tvoří *popis produktu*.
Systémová bezpečnostní politika (dále jen SBP) nebo popis produktu definuje, kdo může manipulovat s prostředky, službami. funkcemi a zařízeními SP.
Vytvoření SBP nebo popisu produktu pro zabudování do specifikace bezpečnosti může být obtížné a to zejména proto, že SBP nebo popis produktu musí definovat chráněná aktiva a pravidla pro práci s těmito aktivy a to bez ohledu na implementaci SP!

4.2 Předpokládané provozní prostředí

Provozní charakteristiky SP jsou získány pomocí analýzy rizik, studia SP a studia prostředí, ve kterém bude SP provozován.. Tyto provozní charakteristiky určují vztah mezi SP a jeho provozním prostředím a proto musí být popsány ve specifikaci bezpečnosti.
Tato část specifikace bezpečnosti musí definovat:
a) účel a hranice SP,

b) jaké informace bude SP zpracovávat a jak je bude zpracovávat,
c) osoby, které budou používat SP(tj. uživatele, operátory, správce, rozdělení do jednotlivých rolí atd.),
d) zařízení, potřebná pro podporu činnosti SP,
e) umístění a topologii SP, včetně fyzických bezpečnostních opatření,
f) provozní režimy a provozní procedury,
g) provozující organizaci a její procedury.

4.3 Bezpečnostní cíle

Prvním krokem v procesu vytváření SBP nebo popisu produktu by měla být definice bezpečnostních cílů. Ty zpravidla popisují následovně:

a) Seznam aktiv organizace, vyžadujících ochranu, zajištěnou prostřednictvím SP nebo jiných systémů nebo fyzickými opatřeními.
b) Informaci jaká konkrétní aktiva (resp. jejich „části“) jsou pomocí SP zpracovávaná, popis souvisejících procesů a povinnosti a role jednotlivých privilegovaných i obyčejných uživatelů.
c) Prostředky SP, a soupis definovaných externích specifikací. Tyto prostředky mohou být fyzické prostředky (například zařízení nebo přístroje) nebo abstraktní prostředky (například konfigurace, procesy, algoritmy, programy).

Častou chybou při psaní specifikace bezpečnosti je, že se odkazuje na míru bezpečnosti poskytovanou bezpečnostními cíli (například stupeň utajení dat v případě důvěrnosti) , které byly získány během analýzy rizik. Pokud má specifikace bezpečnosti sloužit hodnocení bezpečnosti je potřeba se soustředit *na míru záruky*, která může být získána z implementace funkcí prosazujících bezpečnost.

Při využití bezpečnostních cílů jsou proto možné dva přístupy:
a) data a prostředky jsou analyzovány postupně vzhledem ke všem bezpečnostním cílům,
b) prostředky a data se vztahem k témuž bezpečnostnímu cíli jsou posuzovány společně.

Bezpečnostní cíle, vyjadřující **dostupnost**, jsou popsány pomocí pojmů stav, oprávnění, doba provedení služby, doba odezvy a priorita.

Bezpečnostní cíle, vyjadřující **integritu**, jsou vyjádřeny některým z následujících způsobů:
a) splnění standardů a specifikací,
b) splnění počátečního stavu nebo podmínky,
c) pravidla pro použití kontrolovatelných procesů, zajišťující konzistenci a koherenci.

Bezpečnostní cíle, vyjadřující **důvěrnost**, by měly vysvětlit použití všech prostředků a ne pouze vyjmenovat zranitelná místa, která by měla být odstraněna (jako je například prozrazení nepovolané sobě, náhrada obsahu nebo manipulace s cílem poškodit vlastníka dat).

Autor by se měl snažit vypracovat tuto část specifikace bezpečnosti co možná nejúplnější, protože bezpečnostní cíle tvoří základ pro hodnocení (ať už subjektivní nebo jako podklad pro hodnotitele).

4.4 Hrozby

Dalším krokem při vypracovávání SBP nebo popisu produktu je určení předpokládaných hrozeb, t.j. akcí, které by mohly ohrozit splnění bezpečnostních cílů.

Stejně jako bezpečnostní cíle, i hrozby musí být uvažovány již během specifikace SP. Hrozby se vztahují k externímu popisu SP. Ohodnocení hrozeb je však mnohem obtížnější než určení bezpečnostních cílů, protože nikdy nelze vzít v úvahu všechny možné způsoby útoku (např. proto, že některé typy útoků nejsou v době popisu SP známi...)

Během ohodnocení hrozeb mohou být užitečné metody analýzy rizik. Tyto metody mohou poskytnout generický seznam útoků, který může být snadno aplikován na konkrétní SP. Tento seznam může být vodítkem pro ohodnocení hrozeb, které může být prováděno na základě možných událostí nebo na základě bezpečnostních cílů.

Autor specifikace bezpečnosti je zodpovědný za přesnost a úplnost bezpečnostních cílů a hrozeb. Hodnotitel nemá za úkol kontrolovat úplnost těchto informací (!, má za to, že takto má být SP navržen a je to úplné a správné zadání pro SP), hodnotitel pouze kontroluje jejich přesnost a konzistenci!

4.5 Systémová bezpečnostní politika (SBP)

V případě hodnocení systému je známo skutečné provozní prostředí a lze určit hrozby pro systém. V úvahu mohou být vzata i existující protiopatření (které mohou být kombinací elektronických, fyzických, procedurálních a personálních opatření). Tyto informace jsou poskytovány prostřednictvím systémové bezpečnostní politiky.

Každá organizace má typicky několik bezpečnostních politik. Zpravidla na každé úrovni řízení organizace existuje bezpečnostní politika, související s touto úrovní. Například IT systém organizace má obvykle bezpečnostní politiku, která specifikuje pravidla pro práci s informacemi, zpracovávanými systémem a komponentami systému.

Na každé nižší úrovni řízení organizace se musí zjemňovat bezpečnostní politika. Například mechanismy ochrany citlivých informací by neměly být v bezpečnostní politice organizace, ale měly by být postupně rozpracovávány v bezpečnostních politikách nižší úrovně a v jejich funkcích prosazujících bezpečnost .

Systémová bezpečnostní politika definuje zákony, pravidla a praktiky, které určují, jak jsou systémem spravovány chráněné a citlivé informace a jiné prostředky. Na rozdíl od technické bezpečnostní politiky zahrnuje i fyzické, personální a procedurální opatření.
Technická bezpečnostní politika definuje pravidla, která řídí zpracování chráněných a citlivých informací a využití prostředků v samotném systému (zejména IT).

Bezpečnostní politika představuje spojení mezi bezpečnostními požadavky, stanovenými ve fázích "hrozeb" a "cílů" a mezi funkcemi prosazujícími bezpečnost, definovanými později ve specifikaci bezpečnosti. Z hlediska organizace musí být informace obsažená v bezpečnostní politice dostačující k vytvoření specifikace pro implementaci. Aby tato informace mohla tvořit specifikaci požadavků na SP, je nutno ji dále zjemnit. Toto zjemnění je cílem posledního kroku při vytváření bezpečnostní politiky.

Bezpečnostní cíle a předpokládané hrozby napovídají, jakými pravidly se budou řídit uživatelé SP.

Tato pravidla stanoví:
a) která možnost je pro konkrétní aktivum *povinná, povolena nebo zakázaná,*
b) která role *může, musí nebo nesmí* provést konkrétní operaci.

Tato pravidla reprezentují odezvu organizace na bezpečnostní požadavky a vycházejí z:
a) obecných bezpečnostních pravidel,
b) organizační doktríny,
c) předpisové základny organizace
d) speciálně pro tyto případy navržených plánů.

Splněny musí být také následující obecné bezpečnostní principy:
a) oddělení rolí/uživatelů, které má za cíl omezit možnost útoku vzniklého přecházením privilegií od uživatele k uživateli a které také souvisí s odstraňováním uživatelů ze systému a má za úkol zamezit kompletu (v různých variantách dohody osob v jednotlivých rolí),
b) snadnost použití, která má za úkol předcházet omylům, které by mohly vést ke zranitelným místům,
c) implicitní ochrana, která má za cíl poskytnou maximální úroveň ochrany bez aktivního zásahu,
d) odstranění výjimek, které má za úkol učinit model bezpečnosti snadno pochopitelným,
e) pravidlo nejmenšího oprávnění, které minimalizuje rizika tím, že požaduje, aby přiřazená úroveň oprávnění (uživatele, role, procesu) byla právě postačující pro provádění jeho činnosti.
Vypracovaná bezpečnostní politika musí být vnitřně konzistentní a musí zachycovat všechny bezpečnostní cíle a všechny hrozby.

Je vhodné, aby pravidla bezpečnostní politiky byla rozdělena do dvou podmnožin:
a) na netechnická opatření, která se skládají z fyzických, personálních a procedurálních opatření, kterým podléhá provozní prostředí SP (systémová bezpečnostní politika),
b) na technická opatření, která tvoří bezpečnostní požadavky pro specifikaci funkcí prosazujících bezpečnost (technická bezpečnostní politika).

4.6 Popis produktu

Skutečné provozní prostředí produktu není známé, protože produkt může být použit v různých systémech a v různých provozních prostředích. Specifikace bezpečnosti proto může pouze definovat předpokládaný způsob použití, může vyslovit předpoklady o provozním prostředí a o hrozbách, kterým produkt odolává.

V případě produktu je specifikace bezpečnosti tvořena informacemi o SP, poskytnutými prodejcem produktu (resp. jeho vývojářem) za účelem poskytnout potenciálnímu zákazníkovi dostatek informací k tomu, aby se mohl rozhodnout, zda bude produkt splňovat jeho bezpečnostní cíle. Tyto informace jsou poskytnuty ve formě popisu produktu.

Produkt může být vytvořen tak, aby mohl být provozován v různých konfiguracích. Pro tyto produkty může být žádoucí provést jejich hodnocení ve všech konfiguracích a hodnotitel se musí se sponzorem dohodnout na hodnocených konfiguracích. Tyto konfigurace musí být dokumentovány ve specifikaci bezpečnosti (příkladem je FIPS a non-FIPS mód u krypografických produktů hodnocených podle FIPS 140-2).

Prodejce produktu by měl být schopen prohlásit, že produkt je schopen chránit určité aktivum nebo několik aktiv, které existují v předpokládaném provozním prostředí. Prodejce by měl být navíc schopen identifikovat některé hrozby (vyskytující se v předpokládaném provozním prostředí), jimž je produkt schopen čelit. Prodejce by měl mít v případě potřeby možnost konzultovat otázky vhodnosti konkrétního nasazení produktu s výrobcem (vývojářem).

5. Funkce prosazující bezpečnost

Funkce prosazující bezpečnost (dále jen FPB) jsou, na nejvyšší úrovni abstrakce, *vyjádřením funkčnosti*, která je požadována *pro splnění bezpečnostních cílů*. FPB musí poskytnout neměnný a nepřekonatelný aparát, který zcela splňuje požadavky, formulované v systémové bezpečnostní politice.

Prvním krokem při specifikaci FPB je formulace FPB pro každé pravidlo bezpečnostní politiky, čímž vznikne přímá korespondence mezi pravidly a jednotlivými FPB. Jelikož tyto FPB přímo implementují bezpečnostní politiku, jsou nazývány *provozní FPB*. Mimo tyto FPB mohou být formulovány další FPB, které zajišťují funkce, které pomáhají provozním FPB. Tyto FPB se nazývají *podpůrné FPB.*

Provozní FPB mohou být rozděleny do následujících čtyř skupin:
a) Preventivní funkce, které mají za úkol zabránit potenciálnímu útoku minimalizací aktiv (například mezi dvěma relacemi uživatele jsou smazána citlivá data).
b) Detekční funkce, které detekují a sledují útok.
c) Omezovací funkce, které řídí přístup k citlivým prostředkům. Tyto funkce mohou provádět rozdělení do skupin, prosazovat masky přístupových práv nebo bránit v přístupu k dočasným datům. Mezi omezovací funkce patří často i kryptografické mechanismy.
d) Zotavovací funkce, které provádějí bezpečné zotavení SP po poruše nebo útoku.
Jakmile jsou provozní FPB formulovány, autor specifikace bezpečnosti určí, zda jsou potřebné nějaké podpůrné FPB. Tyto FPB zajišťují, že provozní FPB pracují vždy správně a že je nelze obejít. Podpůrné FPB zajišťují ochranu pouze části citlivých prostředků, například samotných FPB. Určení podpůrných FPB je iterační proces, který končí v okamžiku, kdy jsou chráněny všechny FPB (včetně samotných podpůrných FPB).
Tento iterační proces je vhodný pro tvůrce specifikace bezpečnosti.

Některá kritéria hodnocení bezpečnosti (např. ITSEC) nedělají rozdíl mezi provozními a podpůrnými FPB. Namísto toho doporučují, aby FPB byly klasifikovány podle následujících generických záhlaví:
a) identifikace a autentizace,
b) řízení přístupu,
c) účtovatelnost,
d) audit,
e) opakované užití,
f) přesnost,
g) spolehlivost služeb,
h) výměna dat.

Tato klasifikace FPB byla navržena a je vhodná zejména proto, aby umožnila porovnání mezi různými SP. Pokud se plánuje hodnocení hodnotitelem, je nutné tuto část psát dle požadavků konkrétního standardu hodnocení a dále respektovat doplňující pokyny a požadavky hodnotitele.

FPB musí být popsány na takové úrovni detailnosti, která umožní prokázat jejich korespondenci s bezpečnostní politikou.

6. Požadované bezpečnostní mechanismy

Specifikace bezpečnosti může předepsat nebo stanovit použití konkrétních bezpečnostních mechanismů (tj. zařízení, algoritmů nebo procedur), použitých při implementaci některých FPB. Mezi tyto mechanismy zpravidla patří:
a) algoritmy, jako například šifrovací algoritmy, kryptografické rozptylovací funkce, kódy pro opravu chyb a algoritmy pro generování hesel,
b) mechanismy identifikace a autentizace, jako například biometrická zařízení (rozpoznávání hlasu, otisky prstů), PKI apod.

Analýza, prováděná během specifikace bezpečnostních požadavků, může tyto mechanismy prohlásit za povinné.

Autor specifikace bezpečnosti by se však měl vyvarovat nadbytečné specifikace těch bezpečnostních mechanismů, u kterých je definován zároveň bezpečnostní cíl i prostředky, použité k jeho dosažení.

Až doposud specifikace bezpečnosti specifikovala FPB abstraktním způsobem, bez odkazu na implementační mechanismy. V praxi je každá FPB realizována jedním nebo více mechanismy, z nichž každý může patřit do několika FPB.

Při specifikaci bezpečnostních mechanismů musí autor uvážit, zda jsou mechanismy relevantní pro bezpečnost a zda tedy mají být uvedeny ve specifikaci bezpečnosti.

Principiálně by specifikace bezpečnostních mechanismů měla být omezena pouze na pokrytí bezpečnostních požadavků. Z těchto požadavků může plynout použití konkrétní techniky, algoritmu, komponenty nebo vývojové metody. Může z nich dokonce plynout i nezbytnost použití konkrétního produktu nebo vývojáře.

7. Požadovaná kategorie minimální síly mechanismů

Mechanismem rozumíme logický obvod nebo algoritmus, který implementuje určitou funkci prosazující bezpečnost nebo funkci relevantní pro bezpečnost.

Některé mechanismy mají přirozené slabiny, které mohou být útočníkem překonány za použití jistých prostředků, speciálního vybavení nebo využitím vhodné příležitosti. Příkladem může být systém autentizace, který může být překonán pomocí postupného zkoušení všech možných hesel nebo totalizace klíčů pro symetrický šifrový algoritmus.

V závislosti na síle útoku, které jsou tyto mechanismy schopny odolat, by měly být mechanismy kategorizovány jako *základní, střední nebo vysoké*.

Ve specifikaci bezpečnosti musí být uvedena kategorie ***nejslabšího kritického mechanismu SP.***

8. Úroveň hodnocení (volba)

Specifikace bezpečnosti, která je psána pro účely hodnocen,í musí také specifikovat standard podle, kterého má být SP hodnocen a cílovou úroveň hodnocení SP, který má být dosažen (např. CC/ISO 15408 EAL1,2, 3…., ITSEC E1, E2, E3 ….).

Při přípravě SP a volba úrovně hodnocení, nesmíme zapomenout, že se vždy jedná o kompromis mezi tím, co je žádoucí (tj. co největší míra záruky) a tím, co je možné (náklady, čas, počet osob do důvěryhodných rolí,...).

Pokud se rozhodne, že bude SP hodnocen hodnotitelem (tj. uživateli SP nestačí pro subjektivní ohodnocení bezpečnosti dodat specifikaci bezpečnosti, tj. nestačí mu tato subjektivní míra záruky na základě vytvoření detailní specifikace bezpečnosti) je nutné vzít do úvahy nejen náklady na hodnocení, ale i ostatní s tím spojené náklady, jako jsou náklady na výrobu a na distribuci potřebných podkladů, komunikaci s vývojářem a případně vytvoření dalších nezávislých posudků.

Méně obvyklé zkratky:
SP – systém nebo produkt
SBP – systémová bezpečnostní politika
FPB – funkce prosazující bezpečnost

E. O čem jsme psali v květnu 2000 – 2004

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

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@pvt.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/