Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 2/2004 **16. únor 2004**

2/2004

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Opožděný úvodník

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Slovo *opožděný* může mít v češtině ve spojení s podstatným jménem dva zcela odlišné významy – jeden ve smyslu *časovém,* druhý ve smyslu *vývojovém (duševně zaostalý apod.)*. Tento úvodník by měl mít (snaha autora) blíže k významu časovému; pokud sklouzne ke druhému významu - nebyl to úmysl a autor se za to předem omlouvá.

Tento úvodník měl být původně součástí minulého čísla a měl zahájit šestý ročník vydávání e-zinu Crypto-World.

Časopis byl od září1999 do konce roku 2003 rozesílán registrovaným odběratelům e-mailem. Od května roku 2000 šlo starší čísla stáhnout z domovské stránky časopisu. Tato stránka byla od ledna roku 2000 do konce března 2003 na adrese http://mujweb.cz/veda/gcucmp/ . Na této stránce jsem během jejího trvání zaznamenal přes sedmnáct tisíc přístupů.

Uvedu zde malou statistiku počtu registrovaných odběratelů:

Rok	1999	2000	2001	2002	2003
Odběratelů*	25	190	320	367	470

* počet registrovaných odběratelů k 31.12.příslušného roku

Mimo možnosti stáhnout e-ziny z domácí stránky bylo možné je získat na CD s materiály z různých konferencí, např. Security 2000, Security 2001, Mikuláška kryptobesídka 2002, 2003. Crypto-World byl zveřejněn i na CD, které bylo přílohou časopisu CHIP 5/2003.

Pro potřeby e-zinu Crypto-World byla na jaře loňského roku českým informačním serverem CZECHIA poskytnuta doména http://crypto-world.info. Obsah byl ze „staré“ adresy přesunut na novou doménu 10.4.2003. Mimo „důstojnějšího jména“ skýtá tento web i možnosti, které na staré stránce nebyly k dispozici (např. PHP, MySQL). Přepracování celé stránky se ujal můj syn, který alespoň částečně změnil starý a již dávno nevyhovující vzhled domácí stránky Crypto-Worldu. Během roku tak byly vylepšeny osobní stránky hlavních protagonistů e-zinu Pinkavy a Vondrušky, modul registrace, změnil se k lepšímu design vstupní stránky (navržen a realizován druhým synem), informací a stránky s uloženými staršími čísly Crypto-Worldu.

Na nové stránce byla loni na podzim otevřena i sekce *Soutěž 2003*, kde bylo umožněno soutěžícím on-line otestovat, zda jejich řešení jsou správná. Poněkud lehčí úlohy, snadný způsob hodnocení a především možnost neustále sledovat aktuální stav soutěže přilákal (oproti minulým létům) velký počet soutěžících. O výsledcích soutěže a jejím průběhu jsem psal v čísle 12/2003, a tak zde uvedu pouze jednoduchou statistiku minulých soutěží.

Legenda	**2000**	**2001**	**2003**
Počet všech řešitelů	18	15	107
Vyřešilo alespoň jednu úlohu	17	13	53
Vyřešilo všechny úlohy	4	3	11

Jako doprovodný obrázek soutěží v luštění přikládám fotografii, kterou mi zaslal František P. (volací znak: OK1DF). Fotografii jsem vybral ze souboru, který nazval luštitelky. Snímky pořídil letos na podzim a zachytil své dcery při řešení úlohy na transpozici. Uznejte sami – to se mu pak luští! S nadsázkou mne napadlo, že by se tou domácí manufakturou (na jiných fotografiích luští ještě i jeho manželka) dalo vysvětlit, proč v předchozích ročnících 2000 a 2001 patřil mezi těch pár soutěžících, kteří vyřešili všechny úlohy.

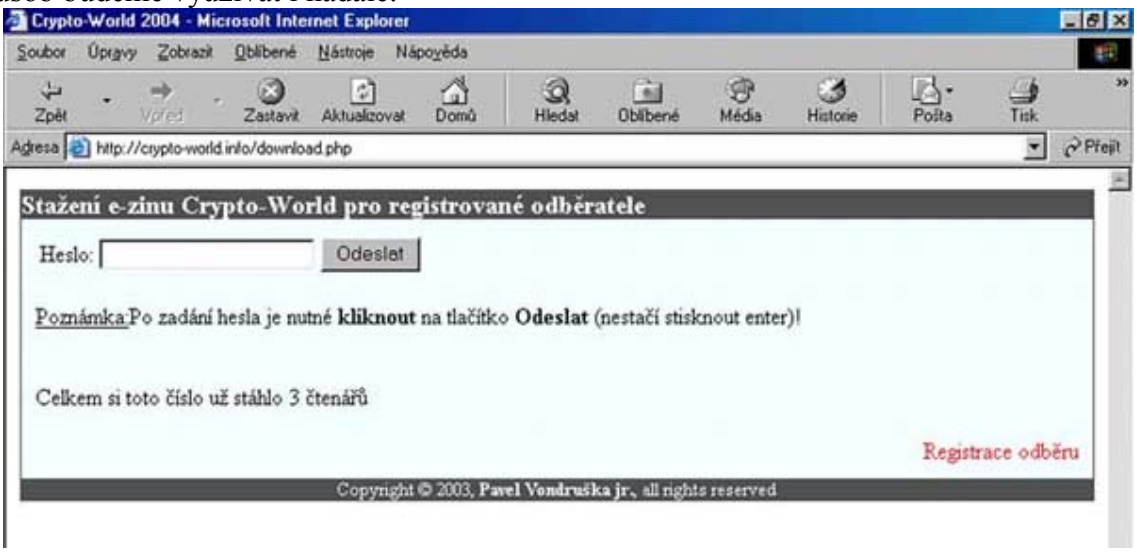
Vraťme se k přestavbě domácí www stránky e-zinu. Během ledna 2004 byla otevřena dosud poslední sekce *Novinky –News*. Rozhodnutí zprovoznit tuto sekci, padlo téměř ze dne na den ve druhé polovině ledna, a proto jsem vás dosud nestačil na ni upozornit.

Samotnou realizaci umožnil

a) slib kolegů Tomáše Rosy a Jaroslava Pinkavy, že budou (každý podle svého zájmu a zaměření) do systému novinek společně se mnou pravidelně přispívat
b) a téměř okamžité vytvoření „systému“ pro vkládání novinek přes web autorizovanými osobami, které připravil můj syn.

Každá novinka se skládá z *předmětu*, který ji charakterizuje nebo vysvětluje, *linky* (odkaz na původní zdroj) a *komentáře* (může se jednat o náš vlastní komentář nebo je použit blíže specifikující text z původního zdroje). Novinky odkazují na původní anglicky psané články nebo dokumenty a dále na články a zdroje v českém a slovenském jazyce. Nemáme ambici každý den zveřejnit jednu novinku – tedy hledat za každou cenu nějakou událost, ale zveřejňovat především opravdu důležité nebo zajímavé zdroje, události apod. Co můžete najít v těchto novinkách? Jednak to můžete zjistit přímo na naší www stránce, nebo se stačí jednoduše podívat v tomto čísle do části **Letem šifrovým světem**, kde místo obvyklých komentovaných zpráv ze světa přetiskuji seznam všech zveřejněných novinek od 23.1.2004 do 13.2.2004.

Poslední změna, o které se zde zmíním, je změna v distribuci e-zinu registrovaným čtenářům a to zasílání kódu ke stažení místo celého e-zinu. Nestačil jsem vám tuto změnu včas oznámit a připravit vás na ni. Z celkového počtu 490 registrovaných odběratelů si prvé číslo stáhlo 376 čtenářů. Vaše písemná odezva však byla jednoznačně kladná, a tak tento způsob budeme využívat i nadále.



Důvody, které mne ke změně v rozesílání vedly, jsem uvedl v e-mailu, který doprovázel rozeslání lednového kódu ke stažení. Důvodů byla opravdu celá řada – zejména:
- zátěž mého poštovního serveru (rozesílání až 0,5 GB dat)
- nastavení politiky, kdy e-mail nesmí obsahovat přílohu větší než stanovená délka (např. 500 kB)
- omezení kapacity některých vašich poštovních schránek
- nastavená bezpečnostní politika hlídající obsah příloh (např. nesmí být ani v zazipovaném souboru exe soubor, který je někdy součástí přílohy)
- vaše možnost opakovaně stáhnout e-zin (např. při jeho poškození, ztrátě apod.)
- některé poštovní servery detekovaly mnou rozesílané informace jako SPAM a do mé schránky se vracely „velké“ soubory

Nově zavedený způsob spočívá v oznámení registrovaným uživatelům, že e-zin vyšel a v uvedení aktuální linky, na které je možné si jej stáhnout. Při pokusu o stažení musíte vložit přidělené zaslané autentizační heslo (platné pouze pro toto konkrétní číslo)!

Při stažení lednového čísla se stalo, že během prvních deseti minut se pokusilo stáhnout e-zin kolem 100 čtenářů. Tím se stalo, že linka byla zahlcena a někteří z vás se na ni nemohli připojit nebo stažení skončilo chybou (projevila se až při pokusu rozzipovat stažený e-zin). Prosím vás proto o trpělivost při stažení e-zinu a v případě neúspěchu o opakování pokusu např. až po dalších deseti minutách.

Závěrem tohoto *Opožděného úvodníku* mi dovolte vám poděkovat za váš dlouhodobý čtenářský zájem, podporu a za zaslané připomínky a podněty.

Současně si vás dovolím touto cestou vybídnout k zasílání prací k otištění v našem e-zinu a podělit se tak o své myšlenky a názory s touto e-komunitou. Budete vřele vítáni! Text prosím zašlete na moji adresu nebo adresu kolegy Jaroslava Pinkavy.

V letošním roce se mi podařilo zajistit mnohadílný a předpokládám, že čtenářsky vysoce zajímavý seriál zkušeného a známého autora Tondy Beneše. Blíže vám tento seriál představí v tomto e-zinu sám a to v úvodu prvého dílu, který nazval „Jak jsem pochopil ochranu informace“.

A. Jak jsem pochopil ochranu informace

Mgr. Antonín Beneš, PhD., KSI MFF UK Praha

Na MFF UK běží od roku 1995 úvodní kurz do problematiky informační bezpečnosti - přednáška "Ochrana informace". Za těch bezmála deset let si přednášku přišlo poslechnout hodně chytrých a hloubavých duší a jejich zhusta velmi netypické dotazy mne donutily celou věc si rozmyslet z mnoha různých, často na pohled absurdních úhlů.

Aby se přednáška nezvrhla v bezduché opisování tabule, a abych věděl, co říkat, vznikly k prvnímu přednesení problematiky handouty, pomocí kterých jsem se danou problematikou probíral. Ty jsem se pak po léta snažil přitesávat, doplňovat a přerovnávat, aby odrážely aktuální pochopení problematiky. Na počátku letošního roku jsem pak dostal od Pavla Vondrušky nabídku, ať ty své rozumy přepíšu do smysluplného textu a uveřejním v jeho Crypto-Worldu. Když budu mít štěstí, jednou z toho budou skripta. Proto jsem také souhlasil, že budu psát.

Tak taková je geneze následujícího textu a teď již k té bezpečnosti.

Tři pojmy do začátku

Když si hned na počátku definujeme nejdůležitější pojmy, budeme si lépe rozumět a bude hned i jasné, „vo co go".

Informačním systémem(IS) rozumíme soubor technických prostředků, softwaru a jeho konfigurací, záznamových medií, postupů, dat a personálu, který daná organizace používá ke správě svých informací. Informační systém ne nutně musí využívat počítačů a mnohé z dalších úvah můžeme vztáhnout na jakýkoliv systém zpracování informací. Přesto v drtivé většině případů základem IS jsou počítače, což zohledním.

Korektní stav IS odpovídá situaci, kdy systém je schopen v definovaném rozsahu poskytovat zajišťovat všechny požadované vlastnosti zpracovávaných informaci, či poskytovaných služeb, například

- utajení	- nepopiratelnost	- autenticita
- dostupnost	- včasnost	- anonymita
- integrita	- současnost	- pseudonymita ...

Uvedený výčet není v žádném případě vyčerpávající, nebo reprezentativní. Výběr služeb, které od toho svého informačního systému bude vlastník požadovat je vždy individuální a může se v čase měnit. Jak ještě ukážu dále, některé ze služeb požaduje vlastník pro svoji vnitřní potřebu, udržovat jiné mu ukládá zákon, nebo jiné normy. Pokud vám je nekterý z pojmů neznámý nevadí, časem to napravím.

Naopak *Bezpečnostní incident* je stav, kdy došlo k porušení alespoň jedné z požadovaných vlastností. Zde stojí za upozornění, že bezpečnostní incident vzniká bez přímé účasti poškozené strany, která jej nemusí včas, či vůbec detekovat, natož být schopna na jeho výskyt reagovat.

Pravidla hry

Homo administrator je člověk jako každý jiný – chce mít svůj klid. Ten má, když všechno funguje tak, jak má, tj. nemá žádný bezpečnostní incident. K tomuto účelu buduje

spoustu mechanismů – tzv. *bezpečnostních protiopatření*, jejichž smyslem je zabránění vzniku incidentu s cílem, aby opatření byla dokonalá a tudíž incidenty nevznikaly. Je nasnadě, že tohoto stavu se dobrat nelze. Popíšu dva přírodní zákony, které mu v tom efektivně brání:

Základní princip ochrany výpočetních systémů.
O peníze jde až v první řadě.

Poněkud to rozeberu:
→ Chráněné objekty mají svoji cenu, pro kterou jsou chráněny. Cena může být různá pro majitele a útočníka.
→ Ochrana není, ani přibližně, zadarmo.
Vaše bezpečnostní opatření budou vždy kompromisem mezi tím, co byste chtěli a tím, co si můžete dovolit.

Princip nejsnazšího průniku.
Je třeba očekávat, že útočník použije libovolný způsob průniku.

Nemusí to být nejzřejmější metoda a útok nemusí být veden proti nejsilnějšímu místu ochrany výpočetního systému. Jinými slovy – útočník se chová nezodpovědně. Útočí když to nečekáme na místa, kde jej nečekáme a ještě ke všemu namísto aby lámal vaše technické zábrany, používá nečestné metody, jako podplácení, vydírání a násilí, nebo se prostě vetře.

Shrnuto bezpečnost je souboj mezi zdroji (čtěte penězi, znalostmi, důvtipem, ..) útočníka a zdroji provozovatele systému. Kdo jich má víc, vítězí. Jako vždy v životě, svoji roli zde má i štěstí.

O co se hraje

Před tím, než se dostaneme k tomu, co je ve skutečnosti cílem hry, ještě několik poučných pojmů.

Informační systém je tvořen souborem tzv. *aktiv*. Jejich společným cílem je poskytovat vám služby v požadované kvalitě. Mezi aktiva patří mimo jiné:

- záznamová media
- počítače
- tiskárny
- programy
- konfigurace
- vlastní informace
- sklad spisů
- napájení
- komunikační linky
- administrátoři
- uživatelé
- zálohy
- provozní prostory
- ...

Jako obvykle seznam není vyčerpávající a svůj soupis aktiv si každý musí provést sám. Aktiva vám umožňují dosahovat služeb, o kterých jsem psal na počátku. A o to hrajete vy, jakožto majitelé, provozovatelé, nebo správci informačního systému.

Váš útočník to vidí z druhé strany. Zkoumá, jak by si na váš účet polepšil, nebo alespoň jak vám by uškodil, přesně podle českého ... aby tak sousedovi chcíplo prase. Začne tím, že hledá expozici.

Expozice je místo potenciálního poškození některého z aktiv, které alespoň potenciálně povede k poškození některé ze služeb IS. Tradičně si pod tímto pojmem

představujeme naše tuze důvěrná data, ale někdy jde jen o pěkně vypadající myš, která se kolemjdoucím moc líbí - zkuste ovládat takové Corel Draw bez myši.

Zranitelností rozumíme nedostatek bezpečnostního systému, může být použit k poškození nebo zcizení informací. Data o novém výrobku jsou z pohledu útočníka expozicí, když si naplánuji, že je budu svým pobočkám posílat nešifrované majlem, je to zjevná zranitelnost.

A teď se konečně podívejte za hranice vlastního IS. Dobrý bezpečák je paranoidní, a všude kolem by měl vidět samé *hrozby* tj. skutečnosti, které potenciálně mohou být původci bezpečnostního incidentu. Laik si tady představí špióna a v poslední době i teroristu, realita nás učí, že zdaleka nejstrašnější hrozbou jsou vlastní uživatelé. Kromě nich sem patří ještě:

- povodně a záplavy
- požáry
- zloději
- rozvědky
- konkurence
- hackeři
- vandalové
- nešikové s bagrem
- viry a červi
- závady techniky
- výpadky napájení
- teplota
- vlhkost
- vibrace
- ...

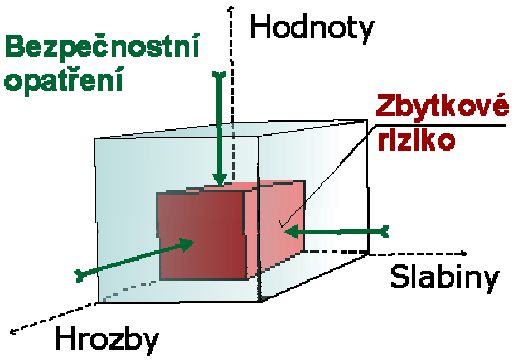
Pokud vás napadlo ještě něco, patří to sem nepochybně také. Nemělo by vás překvapit, že seznam relevantních hrozeb si pro ten svůj IS musí každý sestavit sám. Někdy se tomu učeně říká *model ohrožení*.

Cíl hry

Vaším cílem překvapivě není zbavit se útočníka. Ne proto, že to nejde, ani pro to, že by vás to mohlo připravit o práci, ale prostě proto, že se to nevyplatí. Proč?

Kolem vašeho IS krouží spousta různých hrozeb. Když se některá z nich naplní, tj. vznikne bezpečnostní incident. V jeho rámci utrpíte škodu, jejímuž finančnímu vyjádření se říká *dopad*. Patrně se vám nestávají každý den všechny myslitelné incidenty, každá hrozba pouze představuje určité ohrožení, které se naplní tu s větší, tu s menší pravděpodobností. Pokaždé, když se naplní vás to ale přijde na částku odpovídající dopadu. Rozsah hrozeb spolu s pravděpodobností jejich realizace vám udávají celkovou míru *rizika*. Riziko vztažené k určitému období, zpravidla to bývá fiskální rok, je označováno jako *očekávaná ztráta*.

A tak budujete stále lepší a lepší bezpečnostní protiopatření a snažíte se, aby dopady hrozeb na váš IS byly co nejmenší a děláte všechno proto, aby se k nule přiblížila pravděpodobnost, že někdo zdolá vaši obranu a způsobí vám incident. Bohužel, podobně jako tisíc zedníků nepostaví dům za jediný den, ani stálé zvyšování výdajů na bezpečnost nepřináší donekonečna lineární snižování rizika, potažmo očekávané ztráty.



Vaším cílem tedy je najít místo, kde se bezpečnostní opatření přestávají vyplácet, to jest kdy další investice do bezpečnosti již nejsou vyváženy nejméně stejně velkým poklesem očekávané ztráty. V tomto bodě jste dosáhli optimálního stavu bezpečnosti, další utápění prostředků v nových bezpečnostních opatřeních je ekonomický nesmysl.

Všimněte si, že jsme zcela nevyloučili riziko incidentu – nějaký kousek tu ještě zbyl. Tomu se říká *zbytkové riziko*, a nezbývá, než se s ním naučit žít. Celou věc dokumentuje můj oblíbený obrázek.

Nelze říci, že jde o nějakou předem danou veličinu. Dvě stejné organizace pracující v identickém prostředí mohou mít za stejných podmínek různě velké zbytkové riziko. Důvodem je efektivita použití prostředků na aplikaci bezpečnostních protiopatření. Pokud se to dělá špatně, lze „docílit“ vyššího zbytkového rizika při numericky rentabilním vynaložení větších prostředků. Jak na to, bude obsahem celého navazujícího povídání.

Z uvedených úvah ještě vyplývá, že stav, kdy vám někdo nebo něco prostřelilo bezpečnostní opatření, je nutno brát jako další z provozních režimů IS. Opatrně volte den, kdy tohle sladké tajemství svěříte šéfovi.

Že takhle nikdo nepřemýšlí? Ale zálohujete data na svém PC, že. Protože vás napadlo, že je lepší tu a tam se smířit s tím, že uhyne disk a přijdete o pár dnů práce, než si kupovat plně redundantní pole a stavět geografický cluster.

Jak na to

Teď už byste měli rozumět tomu, o co v bezpečnosti jde, takže toho nechám a budu se zabývat otázkou, jak se dělá taková bezpečnost. Budeme se tím zabývat ještě později, ale je dobré říci si všechny kroky na jednom místě.

Požadavky na bezpečnost

Je řada důvodů, proč vytvářet bezpečnostní opatření:

- zákonné požadavky
- obecné standardy
- resortní normy
- ochrana obchodního tajemství
- dosažení provozní kontinuity
- požadavky protistrany
- zajištění konkurenčních výhod atd.

Zhruba v tomto pořadí byste si je měli projít a ujasnit si, které jsou pro vás relevantní a jak váš IS vyhovuje jejich požadavkům.

Vezmu to po pořádku. Už i do naší vlasti dorazily zákony, které nám ukládají chránit různé informace – třeba osobní data, utajované skutečnosti atd. Podobně je tomu s různými druhy norem. Spoustu těchto věcí má políčeno EU v nejrůznějších oborech. Až si budete chtít na zahrádce založit chemičku, jadernou elektrárnu, nebo třeba jen sanatorium, vězte, že soupis toho, jak má vypadat váš IS nebude brát konce.

Až se prokoušete tím, co musíte, přijde řada na to, co potřebujete. Nikdo se nechce s konkurencí dělit o své plány do budoucna, nikdo nechce, aby ho nefungující IS odřízl od světa v okamžiku, kdy horečka na burze vrcholí. Pokud se rozhodnete stát dodavatelem leckteré státní instituce, nebo velké firmy, budete muset ukázat, že je na vás spoleh i po stránce správy svěřených informací a třeba vytvářeného software. A v neposlední řadě vaší

konkurenci vezme dech, když se budete moci prokázat uznávaným certifikátem na svůj výtvor – což se zpravidla neobejde bez poctivé aplikace nejrůznějších bezpečnostních mechanismů.

Okruh možných řešení

Poté, co zjistíte čeho chcete docílit, je na čase položit si otázku, jak to udělat. V tomto směru vám může pomoci celá řada technických norem a certifikátů, ve kterých se dočtete, jaké přesně mechanismy potřebujete. Certifikáty potom jsou pro vás indikací, že daný produkt zmíněné požadavky splňuje. Jiné normy vám zase mohou říci, jak a o čem máte přemýšlet, aby výsledek byl dobrý.

Plán

V každém případě potřebujete plán – potřebujete *bezpečnostní politiku*. To je podle situace popsaný pivní tácek (jste-li třichlapová firma) nebo dvě či tři knihovny papírů, jste-li nadnárodní korporace. V bezpečnostní politice si naplánujete, jak budete řešit všechny oblasti bezpečnosti, kdo je za co zodpovědný a jak to budete implementovat a provozovat.

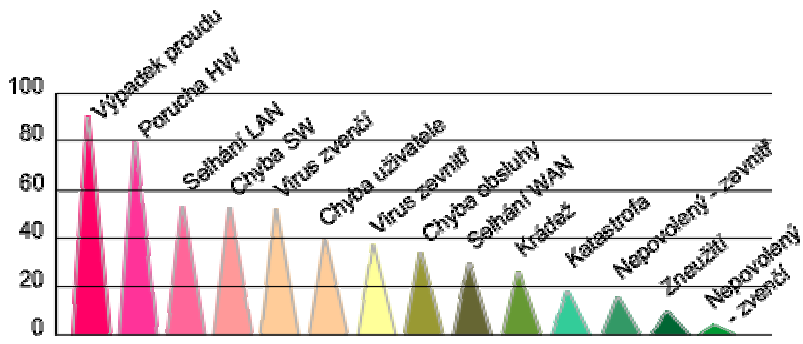
Realizace a provoz

Poté, co napíšete bezpečnostní politiku, přesouváte se z šedivé teorie do veselého prostřed praktické realizace, následně provozu, monitorování, aplikace změn, verifikace, auditu atd. atp.

Krok stranou

Zdá se vám, že se v tom nemožně babrám? Že jsem to celé zatemnil jenom abych si připadal chytře? Činím tak zcela záměrně. Mým cílem je ukázat vám, že bezpečnost je naprosto netriviální propletenec povětšinou velmi triviálních záležitostí. Trocha té učené rétoriky patří k věci, jen je třeba nepozbývat selský rozum. Až vám konzultant začne vykládat o perimetrických bezpečnostních opatřeních, musíte si pod tím představit babu s pendrekem na vrátnici a půl třetího metru vysoký plot kolem fabriky. Na druhou stranu když se to udělá diletantsky, tak dříve či později přijde řada i na vás. Viděl jsem organizaci, kde dopad bezpečnostního incidentu v krátké době dosáhl několikanásobku ceny celého jejich informačního systému.

Za domácí úkol si můžete podumat o obrázku, který jsem namaloval před zhruba dvěma lety podle průzkumu který činil Národní Bezpečnostní Úřad ve spolupráci s časopisem DSM a společnosti PriceWaterhouseCoopers.



Ukazuje žebříček čtrnácti nejčastějších bezpečnostních incidentů ve středních a větších firmách v Česku. Všimněte si, že daleko větší bestie než hacker, který se příliš neumístil, je vlastní uživatel a že oba dohromady jsou jen slabým odvarem problémů, který dokáží způsobit rozvodné závody případně ve spolupráci s matičkou přírodou. Tabulka říká, kolik procent dotázaných uvedený incident zažilo v posledním roce. Z následných průzkumů stejných autorů vyplývá, že tabulka je stále aktuální.

B. Kryptografie a normy - Digitální certifikáty

Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158)

Část 2.

Jaroslav Pinkava, PVT a.s.

Úvod

Dokument ETSI 102158 (lit. [1]) obsahuje specifikace základních požadavků politiky na prováděcí směrnice atributových autorit vydávající atributové certifikáty, které lze používat pro podporu kvalifikovaných elektronických podpisů a jsou tedy dostupné pro používání veřejností a jsou přiřazovány ke kvalifikovaným certifikátům podporujíce tak certifikační politiku "QCP public + SSCD". V první části tohoto článku (Crypto-World 01/2004) byly popsané základní definice, o které se tento normativní dokument opírá (atributový certifikát, atributová autorita, ...), popsána filozofie funkčností atributové autority (rozčlenění celkového modelu na dílčí služby). Dále byla zmíněna existence dvou typů atributových certifikačních politik (z hlediska popisu v tomto dokumentu) a diskutována problematika závazků a odpovědností (klienta, subjektů, spoléhajících se stran a samotné atributové autority). V druhé části článku budou popsány požadavky, které se týkají atributové certifikační prováděcí směrnice.

Atributová certifikační prováděcí směrnice (ACPS)

Atributová autorita provádí vlastně několik typů služeb tak, jak byly popsány v předchozí části. V AA musí být implementovány kontroly, které se týkají jak těchto jednotlivých služeb, tak i činnosti AA jako celku. Cílem je samozřejmě dosažení požadované bezpečnosti služeb AA, resp. dosažení konkrétních bezpečnostních cílů.

Atributová autorita musí zajistit demonstraci spolehlivosti, která je nezbytná pro provádění atributových certifikačních služeb. Konkrétně:

- AA musí mít prováděcí směrnici pro naplnění požadavků každé atributové certifikační politiky, kterou podporuje;
- v ACPS musí být identifikovány závazky všech externích organizací, které podporují služby AA včetně aplikovatelných politika praktik;
- AA musí svoji ACPS poskytnout klientům a spoléhajícím se stranám, to se týká také další dokumentace, která je nezbytná pro dosažení souhlasu s každou atributovou certifikační politikou;
- AA musí seznámit všechny klienty, subjekty a potenciální spoléhající se strany s podmínkami a okolnostmi, které se týkají používání atributových certifikátů;
- AA musí mít odpovědný management, který má finální pravomoce a odpovědnost za schválení ACPS;
- Management AA odpovídá za zjištění, že praktiky jsou správně implementovány;
- AA musí definovat auditní procesy vzhledem k certifikační praxi včetně odpovědností za podporu ACPS;

- AA vydává informace ohledně chystaných úprav ACPS a po jejich schválení managementem zajistí, že revidovaná ACPS bude okamžitě dostupná všem zúčastněným stranám;
- AA musí v ACPS specifikovat podrobnosti příslušných informací a praktik, za kterých proběhne verifikace jí certifikovaných atributů a to včetně zdrojů informací, které jsou použity pro uznání atributu;
- AA musí v ACPS specifikovat dobu platnosti atributové certifikace;
- AA musí v ACPS specifikovat zda podporuje či nepodporuje revokaci (odvolání) atributů. V případě podpory této revokace musí být zde specifikovány příslušné postupy.
- AA musí v ACPS specifikovat zda atributy mohou být požadovány v jediném atributovém certifikátu, či zda pouze ve spojení s dalšími atributy. Pokud je požadováno, aby jediný AC obsahoval více atributů, je nezbytné, aby zde byly specifikovány požadované postupy;
- AA musí specifikovat v ACPS zda a jak může subjekt informovat AA, že chce delegovat jeden či více svých atributů na jiný subjekt.

Životní cyklus správy atributů

Při vstupní registrace subjektu a atributu musí AA zajistit:

- že subjekt je oprávněným držitelem certifikátu veřejného klíče (CVK), na který se atributový certifikát (AC) odkazuje (to lze například učinit elektronickým podpisem učiněným v přítomnosti AA);
- subjekty, klienti a osoby autorizované klientem jsou informováni ohledně procedur pro odvolání jednoho či více atributů obsažených v stávajícím AC (v rámci podpisu smlouvy, elektronickou cestou;
- AA musí ověřit, že práva subjektu pro naplnění atributu jsou zaznamenána (registrována);
- AA musí odpovídajícími prostředky ověřit totožnost subjektu ať již přímo či nepřímo. Poskytnutý důkaz může mít buď papírovou či elektronickou podobu a musí obsahovat jméno a příjmení, datum a místo narození a také jiné atributy, které mohou být použity pro odlišení dané osoby od osob s týmž jménem;
- subjekt a klient musí poskytnout fyzickou adresu či jiný atribut, který popisuje cestu, jak lze s ním navázat kontakt;
- AA musí zaznamenat všechnu informaci, která je použita k ověření totožnosti subjektu a také PKC a to včetně referenčního čísla dokumentu, který byl pro verifikaci použit a také jakákoliv omezení jeho platnosti;
- AA musí klienta informovat o cestách, s jejichž pomocí subjekt může získat atributové certifikáty garantované atributovou autoritou;

AA musí uchovávat smlouvu (může být v elektronické podobě) podepsanou klientem, která obsahuje:

- dohodu na klientových závazcích;
- souhlas klienta a subjektu s uchováváním (atributovou autoritou) záznamu informace, která byla použita při registraci a při libovolné následné revokaci a postupem, jakým bude tato informace předána třetím stranám (za stejných

podmínek, které tato politika vyžaduje v případě, že AA ukončuje svoji činnost);
- zda a za jakých podmínek požaduje klient souhlas subjektu se zveřejněním atributových certifikátů;
- potvrzení toho, že informace poskytnuté při registraci jsou správné;
- souhlas subjektu s libovolnou relevantní okolností, včetně odpovídající souhlasu ve vztahu k legislativě o ochraně dat a osobních údajů;

AA musí dále zajistit, že:

- výše definované záznamy budou uchovávány po to časové období, o kterém byli klient a subjekt informováni a tak dlouho, jak je nezbytné z hlediska prokazování certifikaci během soudního řízení;
- požadavky národní legislativy, které se vztahují k ochraně dat jsou v rámci registračního procesu dodržovány;
- důvěrnost a integrita registračních dat je chráněna speciální cestou (při jejich výměně s klientem, subjektem či uvnitř organizačních složek AA).
- v případě, že jsou použity vnější registrační služby, musí AA ověřit, že registrační data jsou přenesena rozpoznaným poskytovatelem registračních služeb, jehož totožnost byla autentizována.
- subjekt a klienti mají dostatečné informace o prostředcích k revokaci jednoho či více atributů a AC obsahující revokované atributy.
- atributy subjektu jsou správně verifikovány.

Při registraci atributů musí AA:

- ověřit, že v čase registrace atributu je daná osoba oprávněna k tomuto atributu. Ověření musí být provedeno odpovídajícími prostředky a v souladu s národní legislativou;
- zaznamenat všechnu informaci, která byla použita pro ověření atributů subjektu;
- zajistit souhlas subjektu k vydání AC;
- zaznamenat všechnu informaci, která demonstruje, že subjekt souhlasí se získáním atributového certifikátu prostřednictvím této služby.

V další části materiálu jsou rozebírány podmínky pro obnovu atributů. AA musí být samozřejmě ujištěna o oprávněnosti požadavku na obnovu a dodržení všech dříve stanovených podmínek. Atributová autorita musí zajistit dostupnost všech podmínek a omezení ve směru ke klientům, subjektům a spoléhajícím se stranám. Tito musí mít přístup k atributové certifikační politice a/nebo atributové certifikační prováděcí směrnici a stejně tak ke všem aplikovatelným okolnostem a podmínkám, které se týkají poskytování a používání atributových certifikátů, konkrétně jsou seznámeni s:

- identifikátorem podporované certifikační politiky (se kterou je vyhlašována shoda);
- zřetelným popisem významu každého typu podporovaného atributu;
- seznamem dokumentů, které musí subjekt poskytnout při prokazování svého práva na registraci atributu a s procedurami, které AA používá pro verifikaci tohoto práva;
- jak je každý atribut vyjádřen (reprezentován) v AC (řetězec znaků resp. OID);

- jakýmikoliv omezeními, která se týkají jejich používání;
- závazky klienta a subjektu;
- se způsobem, kterým jsou AC poskytováni;
- jak je pojednáno s revokací atributů a AC (pokud vůbec);
- informací jak, ověřovat AC, včetně informací, které se vztahují k ověřování revokačního statutu AC (v případě, že je tato služba poskytována) tak, aby se spoléhající strana mohla opřít o AC věrohodnou cestou;
- s omezeními závazků, které jsou AA definovány;
- s obdobím, během kterého jsou registrační informace resp. logy událostí uchovávány;
- s procedurami pro řešení stížností a sporů;
- s aplikovatelnou národní legislativou;
- zda je AA certifikována na shodu s identifikovanou atributovou certifikační politikou a pomocí jakého schématu;

Ve vztahu k akviziční službě atributová autorita se musí ujistit o náležité oprávněnosti požadavku registrovaného subjektu na vydání atributového certifikátu, konkrétně:

- AA musí vydat atributový certifikát obsahující náležité informace (specifikováno v příloze A dokumentu)
- AA musí vydat AC pouze legitimnímu držiteli certifikátu veřejného klíče;
- přitom atributy mohou být poskytovány jako jediný AC či jako více AC;

Atributové certifikáty mohou být k uživatelům distribuovány prostřednictvím služby pro šíření a takováto jejich dostupnost musí být pouze taková, jaká je definována souhlasem klienta.

AA musí zajistit bezpečné postupy pro vydávání atributových certifikátů, konkrétně:

- služba pro generování AC musí generovat AC, obsahující minimálně pole popsaná v příloze A. Profily atributových certifikátů musí být obsaženy v ACP a /nebo ACPS;
- služba pro generování AC musí zajistit, že jsou akceptovány pouze takové požadavky na AC, jejichž původem je organizace AA a které jsou v souladu s procedurami AA.

V případě, že je poskytována služba revokace či pozastavení AC, musí AA zajistit adekvátní cesty pro naplnění autorizovaných a ověřených požadavků na odvolání.

Poznámka: Následující pokračování bude věnováno "interním" problematikám atributové autority (životní cyklus podpisového klíče AA, administrativní a řídící procedury AA, spolehlivost organizace).

Literatura

[1] Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates (ETSI TS 102 158, V.1.1), http://portal.etsi.org/esi/el-sign.asp
[2] rfc3281: An Internet Attribute Certificate Profile for Authorization
[3] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002
[4] J. Pinkava: Politika pro vydávání atributových certifikátů - požadavky, část 1+2, Crypto-World 10,11/2003

C. Archivace elektronických dokumentů
Část 3.
Jaroslav Pinkava, PVT, a.s.

1. Úvod

V listopadovém článku (lit. [1] v rámci informace o zahájení činnosti pracovní skupiny IETF: Long-Term Archive and Notary Services (ltans) (lit.[2]) jsme se zmínili o souvisejících aktivitách v rámci projektu ArchiSig (http://www.archisig.de/index.html).

Podívejme se nyní na ně trochu podrobněji. Projekt Archisig běžel v rámci většího souboru (celkem sedmi) projektů VERNET – "Secure and reliable transactions in open communication networks" a byl rozvržen na období od července roku 201 do září roku 2003. Byl financován v rámci grantu spolkového ministerstva hospodářství a práce a podílely se na něm celá řada partnerských organizací: medicínské centrum Heidelberské univerzity, Fraunhofer institut, univerzita v Kasselu, firma SECUDE a řada dalších německých výzkumných pracovišť.

Výsledkem projektu je jednak určitý prototyp celkového řešení – a dále několik dokumentů, k jejichž obsahu se nyní obrátíme.

2. Východiska projektu

Při startu projektu bylo zformulováno následujících deset podmínek.

P1. Použit bude jednoznačně interpretovatelný dlouhodobě stabilní a standardizovaný formát uživatelských dat.
P2. Použit bude jednoznačně interpretovatelný dlouhodobě stabilní a standardizovaný formát podpisových dat.
P3. Bude vzat zřetel na bezpečnostní vlastnosti kryptografických algoritmů.
P4. Budou použity elektronické podpisy mající dostatečně vysokou úroveň bezpečnosti.
P5. Údaje požadované pro verifikaci budou archivovány v podobě umožňující jejich rychlé použití.
P6. Včasná a prokazatelná obnova podpisů.
P7. Provozuschopné technické komponenty.
P8. Bezpečné převody elektronicky podepsaných dokumentů (po převodu musí zůstat jak uživatelská tak i podpisová data v ověřitelné podobě).
P9. Musí být vzat zřetel na otázky záruky ochrany dat a problematiky utajení.
P10. Redundantně bude řešena otázka zvýšené bezpečnosti pro ukládání a obnovu elektronicky podepsaných dokumentů (ochrana proti výskytu chyb).

3. Elektronický podpis a zdravotnická dokumentace

V populárněji formulovaném materiálu [5] se autoři zabývají možnostmi použití konceptů založených na kryptografických metodách pro převod papírové dokumentace nemocného do elektronické podoby. Jedná se jak o jejich využití pro šifrovou ochranu (k zajištěná jejich důvěrnosti a utajení), tak i využití elektronických podpisů pro zabezpečení neporušenosti dat a jejich autentizaci. Článek dále popisuje požadavky a možná řešení uživatelsky orientovaného PKI z hlediska použití elektronických podpisů pro zdravotnickou dokumentaci a v návaznosti na německý zákon o elektronickém podpisu.

V rámci prací byla provedena analýza existující papírové zdravotnické dokumentace (v různých odděleních Zdravotního centra heidelberské univerzity a na jejím základě byl

vytvořen adekvátní model PKI. Bylo zvoleno odpovídající vybavení HW a SW komponentami. Jako úložiště pro soukromé podpisové klíče byly zvoleny čipové karty konkrétního typu. V rámci dvouměsíčního pilotního projektu byly podepisována všechna výstupní dokumentace elektronicky. Dle následných šetření (různých typů – dotazníky, pozorování, interview, statistické metody) autoři tvrdí, že byla prokázána jak užitečnost elektronických podpisů, tak i jejich akceptace z hlediska uživatelů.

Zvolený model PKI, aby vyhověl podmínkám legislativy pro elektronický podpis se opíral o pojem "akreditovaný elektronický podpis", tj. bylo doporučeno, aby příslušný poskytovatel certifikačních služeb byl akreditován. Analyzovaný model PKI doporučuje jak využití časových značek, tak i použití atributových certifikátů (prokazování potřebné zdravotnické kvalifikace).

Ve další části článku se autoři zabývají implementací nezbytných modelů dle doporučení z evropských normativních dokumentů (CEN/ISSS) a v závěru článku pozitivně hodnotí efektivnost používání elektronického podpisu pro zdravotní dokumentaci. Samotnou archivací el. dokumentů se však již hlouběji nezabývají.

Trochu hlouběji jsou tyto otázky analyzovány v materiálu [6]. Autoři zde konstatují, že z hlediska dlouhodobého pohledu může docházet k ztrátě prokazovací hodnoty elektronicky podepsaných dokumentů a to v důsledku v čase se snižující bezpečnosti kryptografických algoritmů. Autoři se odkazují na dokumenty ETSI (lit. [8],[9]), které na problematiku dlouhodobého uchovávání elektronicky podepsaných dokumentů berou zřetel.

Samotný koncept projektu ArchiSig pro zachování dlouhodobé prokazatelnosti elektronicky podepsaných dokumentů se opírá o pojem centrálního archivačního systému (služby), která generuje "obnovené" elektronické podpisy v podobě časových značek a zajišťuje takto jejich dlouhodobou platnost. Podstatou navrženého modelu je využívání hashů pro strom dokumentů a časovou značkou je vždy opatřen pouze kořen tohoto stromu.

Za tímto účelem byl v rámci projektu navržen i určitý dokument normativního typu – v podobě draftu (lit.[7]). Jeho obsah stojí určitě za samostatný výklad a bude proto předmětem následujícího článku.

V závěrečné poznámce je možné tlumočit víru autorů, že jimi zvolená cesta je vhodná pro archivaci elektronicky podepsaných dokumentů z dlouhodobého hlediska, přičemž zde uvažují o vhodnosti pro časová období v délce 30 až 40 let.

Literatura

[1] Jaroslav Pinkava: Archivace elektronických dokumentů, Crypto-World 11/2003
[2] webovská stránka ltans: http://ltans.edelweb.fr/ .
[3] Long-term Archive Service Requirements draft-ietf-ltans-reqs-01.txt
[4] Projekt ArchiSig: http://www.archisig.de/index.html
[5] Brandner, R.; van der Haak, M.; Hartmann, M.; Haux, R.; Schmücker, P. (2002): The Electronic Signature of Medical Documents - Integration and Evaluation of a Public Key Infrastructure in Hospitals. Methods of Information in Medicine 41, 321 - 330.
[6] Brandner, R.; Pordesch, U. (2002): Long-Term Conservation of Provability of Electronically Signed Documents. Tagungsband ISSE 2002 - Information Security Solutions Europe: The Independent European Conference for IT Security vom 02. bis 04. Oktober 2002 in Paris.
[7] Archive Time-Stamps Syntax (ATS), draft-brandner-etal-ats-00.txt - Archive Time-Stamps Syntax (ATS)
[8] ETSI 101 733, Electronic Signature Formats, http://portal.etsi.org/esi/el-sign.asp
[9] ETSi 101 903, XML Advanced Electronic Signatures, http://portal.etsi.org/esi/el-sign.asp

D. IFIP a bezpečnost IS

RNDr. Dagmar Brechlerová, Česká zemědělská univerzita, Praha

IFIP (International Federation for Information Processing) je nevládní nezisková organizace, která zastřešuje národní organizace pracující na poli informačních procesů. IFIP byl ustaven v lednu roku 1960. Dnes se jedná o velmi rozsáhlou organizaci, která má různé typy členství. V roce 2002 měl IFIP 48 řádných členů, 3 korespondenční členy, 11 přidružených mezinárodních organizací jako je např. CEPIS (Council of European Professional Informatics Societies), FACE, ICCC a další.

Česká republika je jedním ze řádných členů IFIPu, příslušná národní organizace je zde Česká společnost pro kybernetiku a informatiku.

Hlavním cílem IFIPu je podporovat rozvoj informačních procesů, prosazovat je ve vědě a technologiích, pomoci rozvíjet mezinárodní spolupráci a vzdělávání v informačních procesech. Zvláštní pozornost je věnována rozvojovým zemím, tak aby dosáhly použitím aplikací IT optimálního užitku. Dalším cílem je zavést vysoké etické standardy mezi profesionály pracujícími v IT, poskytnout forum pro diskusi o sociálních aspektech užití IT a zabývat se také ochranou lidí při nevhodném užití IT, což se zejména dnes stává reálným nebezpečím a souvisí právě s bezpečností IS. IFIP chce poskytnout styčný prostor pro kontakt mezi akademickou, průmyslovou a státní sférou. Dalším je mezinárodní aspekt vývoje a aplikací vzhledem s ohledem na vývoj mezinárodních standardů. IFIP chce přispět k formulaci programů vzdělávacích a tréninkových metod pro uživatele IT, praktiky v IT i pro širokou veřejnost.

Generální shromáždění všech IFIP členů je zodpovědné za IFIP strategii, aktivity a finance, schází se každoročně, volí presidenta, 4 vicepresidenty, finanční správu, sekretáře a 8 zplnomocněnců, kteří tvoří IFIP Koncil. Sekretariát IFIPu je v Rakousku, veškeré další informace možno najít na http://www.ifip.or.at .

IFIP má 12 technických výborů, 80 pracovních skupin, a ročně zorganizuje více než 70 mezinárodních akcí. Např. v roce 2002 to bylo 84 kongresů a konferencí, řada vydaných IFIP publikací apod. Hlavní náplní činnosti IFIPu jsou konference, malé pracovní konference, semináře a tutoriály, elektronické konference.

Technické výbory (TC) v podobě pracovních skupin mají více než 2000 členů z celého světa, zastoupení České republiky je ale celkově bohužel zcela minimální.

Každé 2 roky se koná kongres IFIPU. 17. kongres byl v Montrealu, Kanada, 25. až 30. srpen 2002 a další je plánován na srpen 2004, Francie - Toulouse. Kongres je organizován tak, že se jedná o řadu souběžně probíhajících konferencí.

Bezpečnosti se věnuje speciální technický výbor a to TC 11, jeho název je Bezpečnost a ochrana v informačních systémech. (Security and Protection in Information Processing Systems). Některé pracovní skupiny spadající do této oblasti jsou spojené s jinými pracovními skupinami z jiných TC.

Pod technickým výborem 11 je celkem 7 pracovních skupin, které vyvíjejí různě bohatou činnost.

11.1. Management informační bezpečnosti
11.2. Bezpečnost malých systémů
11.3. Bezpečnost dat a aplikací
11.4. Bezpečnost sítí
11.5 Integrita a řízení systémů
11.7 + 9.6 IT : Právo a zneužití IT
11.8 Výuka informační bezpečnosti

Vedením TC je 11 je v současné době pověřen pan L. Strous, Holandsko, De Nederlandsche Bank, a dále prof. Dr. K. Rannenberg, Německo, Goethe University Frankfurt, Mobile Commerce and Multilateral Security. Oba se již několikrát účastnili různých akcí v České republice.

Autorka tohoto textu zastupuje od roku 2003 Českou republiku v celé skupině 11, jsem tedy národním delegátem pro TC 11. Toto místo nebylo již řadu let obsazeno a na konec jsem o zastupování byla požádána právě panem L. Strousem, který je, jak již bylo uvedeno, nyní předsedou celé TC 11 a s kterým jsem se setkala na několika akcích IFIPu. Slovensko je již řadu let zastupováno panem J. Vyskočem. Obecně nutno říci, že bohužel účast z České republiky v jednotlivých pracovních skupinách TC 11 je mizivá.

V roce 2002 jsem v Praze organizovala pracovní schůzku skupiny 11.7., jejímž jsem již řadu let členem.

Velká společná akce TC 11 byla 18. IFIP mezinárodní konference o informační bezpečnosti v květnu 2003 v Athénách, které jsem se aktivně zúčastnila, sborník je zájemcům k dispozici u mne.

V roce 2004 bude ve Francii v Toulouse 18. kongres IFIPu (http://www.wcc2004.org/), jeho součástí bude 19. IFIP Mezinárodní konference o informační bezpečnosti. (SEC 2004). Na tuto konferenci jsou právě v současné době přijímány příspěvky. Témata konference jsou např. autentizace, autorizace a kontrola přístupu, bezpečnostní modely a architektury, analýza rizik a management rizik, internet a www bezpečnost, detekce útoků, bezpečnostní politiky, bezpečný e- government, ochrana dat atd. Konečné datum pro abstrakty příspěvků bylo 9. 2. 2004 , konečné datum pro celé příspěvky 16. 2 . 2004. Všechny další informace je možno najít na http://www.wcc2004.org/sec/ . Další konferencí o bezpečnosti v rámci IFIPu , na kterou jsou nyní přijímány příspěvky, je 18th IFIP WG 11.3 Working Conference on Data and Application Security (http://seclab.dti.unimi.it/~ifip113/2004/). Řada dalších akcí je na stránce TC 11 http://www.ifip.tu-graz.ac.at/TC11/CONF/index.htm.

Jako zástupce České republiky v organizaci IFIP TC 11 bych všechny čtenáře ráda k účasti ať pasivní tak aktivní pozvala. Jde o možnost seznámit se s děním ve světové bezpečnostní komunitě, ke které bohužel doma nemáme příliš příležitostí. Členství v IFIPu je bezplatné.

Navíc účast na podobných akcích umožňuje získat kontakty např. na projekty v rámci 6. rámcového programu a dalších podobných aktivit. Moje osobní zkušenost je taková, že když jsem se kdykoliv obrátila kvůli nějakým informacím na kohokoliv z adresáře IFIPu, dostala jsem odpověď velmi rychlou a kvalitní.

E. Letem šifrovým světem

Ukázka z nově otevřené sekce stránky http://crypto-world.info . Sekce je v provozu od 23.1.2004. Novinky pro Vás pravidelně vybírají a doplňují:

TR - Tomáš Rosa, **JP** - Jaroslav Pinkava, **PV** - Pavel Vondruška

14.02. 2004	Novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy	http://www.micr.cz/scripts/detail.php?id	13.2.2004, Ministerstvo informatiky připravilo návrh novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Návrh bude zaslán v příštím týdnu do meziresortního připomínkového řízení. Text návrhu novely zákona včetně textů novelizovaných zákonů v platném znění s vyznačením navrhovaných změn a doplnění je vystaven na webu MI k veřejné diskusi.	**PV**
13.02. 2004	Shawna McAlearney: Microsoft ASN flaw may be biggest defect ever found	http://searchsecurity.techtarget.com/ori	Experts are concerned about a recently announced Windows vulnerability, which affects multiple versions of the operating system. The flaw can be exploited in a variety of ways to remotely attack systems.	**PV**
12.02. 2004	FIPS 199 Standards for Security Categorization of Federal Information and Information Systems	http://csrc.nist.gov/publications/fips/f	důležitá norma pro bezpečnostní kategorizaci (federálních - USA) informací a informačních systémů schválena	**JP**
11.02. 2004	CBC v SSL/TLS - vybrané bezpečnostní aspekty	http://www.openssl.org/~bodo/tls-cbc.txt	Text, který je pravidelně aktualizován dvorním kryptologem OpenSSL, shrnuje známé útoky na modus CBC ve schématu AtE (Authenticate then Encrypt), které jsou relevantní vůči SSL/TLS. Je všeobecně známo, že schémata CBC/AtE jsou náchylná k aktivním útokům, přičemž velmi záleží na konkrétní aplikaci, zda a kde se tato zranitelnost projeví. Uvedený dokument stručně, avšak inspirativně popisuje možné zranitelnosti CBC/AtE v SSL/TLS. Je z něho mj. dobře vidět, že bezpečnost SSL/TLS	**TR**

			je třeba analyzovat vždy v kontextu celého systému, ve kterém je tento protokol použit. Jinak se lze dočkat poměrně nemilých překvapení...	
11.02. 2004	Microsoft warns consumers about major Windows security flaws (10 2004 11:18AM)	http://securityfocus.com/news/8003	! Microsoft urged consumers to apply the repairing patch immediately if they were using Windows NT, Windows 2000 or Windows XP versions of its software, or its Windows NT Server, Server 2000 and Server 2003 software commonly found in corporations.	**PV**
08.02. 2004	Britain spied on UN allies over war vote	http://observer.guardian.co.uk/politics/	Security Council members 'illegally targeted' by GCHQ after plea from US security agency (špionáž proti Radě Bezpečnosti OSN)	**PV**
07.02. 2004	Slovenská CA EVPÚ byla akreditovaná NBÚ v soulade se zkonem o elektronickém podpise č. 215/2002	http://www.caevpu.sk/akred.html	Předpokládaný termín zahájení poskytování akreditovaných certifikačných služeb je 11. 02. 2004	**PV**
06.02. 2004	SNARF attack and Bluetooth	http://www.bluestumbler.org/	Máte Nokii 6310? - čtěte!	**JP**
06.02. 2004	Entrust Announces Advanced Security for Adobe® Acrobat®6.0 Software	http://www.entrust.com/news/2004/archive	Entrust, Inc. announced enhancements to the Entrust Entelligence™ Verification Plug-in to make use of digital signatures and encryption capabilities with Adobe Acrobat 6.0 software	**JP**
06.02. 2004	Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004)	http://islab.oregonstate.edu/ches/	Cambridge (Boston), USA, August 11-13, 2004, submissions must be received by March 2, 2004,	**JP**
06.02. 2004	1st European PKI Workshop Research and Applications	http://www.aegean.gr/EuroPKI2004/	submission of papers till 15 February 2004	**JP**
05.02. 2004	RFC 3675 on .sex Considered Dangerous	ftp://ftp.rfc-editor.org/in-notes/rfc367	Diskutována je velice zajímavá myšlenka vytvořit novou doménu .sex. V případě potřeby by bylo jednoduché ji zablokovat. Konstatuje se, že z technického hlediska není	**PV**

			probémem ji vytvořit (blokovat). Účinnost opatření by byla dána pouze při změně legislativy tak, aby byl "obscéní" obsah v národních doménách zakázán.	
04.02. 2004	Voynich Manuscript	http://www.world-mysteries.com/sar_13.ht	Vynikající přehledový článek věnovaný této záhadě. Obsahuje základní data, přehled teorií a řadu odkazů.	**PV**
03.02. 2004	Necudný útok na Turinguv test "živé inteligence"	http://groups.google.com/groups?dq=&hl=c	Trivialní, leč přesto zajímavá a usměvná finta ukazující, jak mohou správci pornografických stránek mimoděk využívat "zbytkové" inteligence svých právě nalogovanch uživatelů k útoku zaměřenému na obejití ochran proti SPAMu na bázi obecného Turingova rozlišovacího testu.	**TR**
03.02. 2004	NIST-Recommendation for Common Criteria Assurance Packages	http://www.cryptome.org/cca.zip	první veřejný draft - ekonomicky efektivní strategie pro naplnění požadavků EAL v CC	**JP**
02.02. 2004	Jak se v Čechách využívají e-agendy?	http://www.lupa.cz/clanek.php3?show=3185	Zajímavý článek J.Peterky s podrobným rozborem využití čistě elektronické cesty v některých agendách...	**PV**
01.02. 2004	How to Hack an Election	http://cryptome.org/hack-vote.htm	článek z New York Times (January 31), včetně zprávy o závažných slabinách volebního zařízení - AccuVote-TS Voting System	**PV**
30.01. 2004	draft NIST Special Publication 800-63, Recommendation for Electronic Authentication.	http://csrc.ncsl.nist.gov/publications/d	draft obsahuje doporučení pro vzdálenou autentizaci v počítačové síti ve Federálním (USA) IT-systému.	**JP**
28.01. 2004	NIST Special Publication 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)	http://csrc.ncsl.nist.gov/publications/d	DRAFT předložen k diskuzi 21.1.2004	**JP**

28.01. 2004	NIST Special Publication 800-30 Rev A, Risk Management Guide for Information Technology Systems	http://csrc.ncsl.nist.gov/publications/d	DRAFT předložen k diskuzi 21.1.2004	**JP**
28.01. 2004	NIST Statistical Test Suite for Randomness-corrections	http://eprint.iacr.org/2004/018.pdf	Autoři ukazují, že dva z testů (diskrétní Fourierova transformace a Lempel-Ziv) obsahují chybná nastavení a uvádí nezbytné korekce.	**JP**
27.01. 2004	Aktualní epidemie červa Mydoom (alias Shimgapi, Novarg, Mimail.R, Shimg)	http://www.aec.cz/WebNET/Main/Default.as	Červ šířící se pomocí e-mailu a P2P sítě Kazaa. První exempláře nového červa Mydoom se v našich končinách objevily v brzkých ranních hodinách 27. ledna 2004...	**PV**
26.01. 2004	Security Zdroje leden 2004 (Doseděl Tomáš, Connect)	http://connect.cpress.cz/Bezpecnost/ar.a	info o našem e-zinu	**PV**
25.01. 2004	Bill Gates v Praze	http://www.microsoft.com/cze/presspass/b	V úterý 27. ledna 2004 navštíví Prahu Bill Gates ....(a vše co stím souvisí :-))	**PV**
24.01. 2004	Infiltration of files seen as extensive / Senate panel's GOP staff pried on Democrats	http://www.boston.com/news/nation/articl	Major hack attack on the U.S. Senate	**PV**
23.01. 2004	Code that can't be cracked	http://www.thestar.com/NASApp/cs/Content	využití ECC	**JP**
23.01. 2004	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	ftp://ftp.rfc-editor.org/in-notes/rfc366	RFC 3664, leden	**PV**
23.01. 2004	sci.crypt Sandbox - Home	http://sandbox.emboss.co.nz/	zajímavá iniciativa, hodnocení zaslaných šifrovacích algoritmů	**TR**
23.01. 2004	USAF Wants To Find Steganographic Content	http://slashdot.org/article.pl?sid=04/01	U.S. Air Force vypisuje grant na systém vyhledavání skrytých informací	**PV**

VIII. O čem jsme psali v lednu 2000 - 2003

Crypto-World 2/2000

Crypto-World 2/2001

Crypto-World 2/2002

Příloha: Program pro naše čtenáře : "Hašák ver. 0.9" (viz. letem šifrovým světem) hasak.

Crypto-World 2/2003

Příloha : Crypto_p2.pdf

Přehled dokumentů ETSI, které se zabývají elektronickým podpisem (ETSI - European Telecommunication Standards Institute) 10 stran

F. Závěrečné informace

1. Sešit

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

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

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

3. Spojení

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