Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 8, číslo 3/2006 **15. březen 2006**

3/2006

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1082 registrovaných odběratelů)

Obsah :

A. Klíče a hesla (doporučení pro začátečníky)

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

Jaká mají být hesla a klíče šifrového systému?

Částečně na tuto otázku odpovídá ve své knize *Vojenská kryptografie* holandský kryptolog Auguste Kerckhoffs (1835–1903). V jedné ze zásad, které zde stanoví, se požaduje na dobrém šifrovém systému toto:

Vyzrazení systému nesmí mít nepříjemné následky pro dopisovatele.

Jinými slovy: u dobrých šifrových systémů není třeba utajovat systém, ale klíč. Proto jsou vytváření klíče a jeho kvalita tak důležité. Pokud bude např. klíč krátký a útočník má možnost klíče testovat, může se stát, že má dostatek času, aby otestoval všechny klíče. Luštění se tedy změní na hledání správného klíče. A tak zpráva zašifrovaná kvalitním šifrovým systémem může být odhalena jen proto, že odesílatel zvolí nevhodný klíč (krátký, lehce uhodnutelný - předpovídatelný)…

V kvalitním šifrovém systému musí proto platit, že jeho složitost (odolnost proti luštění) musí být dostatečně velká, aby útočník nemohl šifru rozluštit v rozumném (dosažitelném) čase. Současně se musí dbát na to, aby byla složitost odpovídající otestování všech možných klíčů dostatečně velká, a to tak, aby nebylo možné všechny klíče v dosažitelném čase otestovat a tím šifru „prolomit“. Jako typický příklad si připomeňme historii prvého všeobecného používaného šifrového standardu algoritmu DES, který musel být v devadesátých letech minulého století pro svoji krátkou délku klíče nahrazen modifikaci 3DES a později novým šifrovým standardem AES. Co totiž nedokázali kryptologové svými analytickými útoky, docílil časem rozvoj síly výpočetní techniky. Algoritmus používal velikost klíče "pouze" 56 bitů a v roce 1998 bylo zkonstruováno zařízení (DES Cracker), které dokázalo vyzkoušet všechny možné klíče algoritmu DES do 9 dní.

Jaký musí být tedy klíč? Již jsme řekli, že musí být dostatečně dlouhý, aby nebylo možné otestovat všechny možné klíče. Dostatečně dlouhý klíč je relativní pojem, a proto se bude doporučená délka klíče měnit podle aktuálního výkonu výpočetní techniky. V současné době se pro symetrické algoritmy považuje za dostatečnou délka klíče 80 bitů, ale doporučuje se 128 bitů a více. Předpokládá se, že jde o dostatečnou rezervu, neboť v současnosti jsou teoreticky dosažitelné testy klíčů délky do 64 bitů.

Délka klíče sama o sobě však nestačí… Klíč musí být nejen dostatečně dlouhý, ale i „náhodný“ a „nepředvídatelný“. Nesmí tedy existovat vodítko, které by tomu, kdo se snaží zprávu vyluštit hledáním klíčů, umožňovalo z množství všech možností vytipovat jen jakýsi okruh (podmnožinu) možných hesel, a ta následně otestovat.

Vytvořit náhodné heslo je poměrně složitý problém. Potřebujete k tomu buď fyzikální generátor náhodných čísel (např. založený na výsledcích házení kostkou nebo mincemi nebo na fyzikálních jevech jako radioaktivní rozpad, analýza tepelného šumu připojeného rezistoru …) nebo lze vyrobit nějaký software, který na základě dodaného vstupu (náhodné inicializace) produkuje posloupnost, která se jeví při statistických testech jako náhodná (v takovém případě říkáme, že výsledkem je pseudonáhodná posloupnost). Nicméně jen statistické testy výstupu nestačí k tomu, abychom mohli říci – toto je ten pravý a vhodný klíč.

Např. posloupnost :
14159 26535 89793 23846 26433 83279 50288 41971 69399 37510 58209 74944 59230 … se jeví v běžných statistických testech jako náhodná, ale jako klíč není vhodná. Proč ? Jedná se totiž o začátek rozvoje Ludolfova čísla neboli „pí“, kde jsme pouze na začátku vypustili číslo 3 (tedy 3,14159 26…). Uvedené číslo má náhodné charakteristiky, ale je „předvídatelné“, tj. útočník by mohl jeho použití jako klíče (za jistých okolností) uhodnout.

U moderních symetrických systémů je klíčové hospodářství velmi komplikovanou záležitostí. Do klíčového hospodářství patří řada aspektů, jako je výběr požadavků na klíče, tvorba klíče, testy vhodnosti klíče, vyloučení slabých klíčů, bezpečné předání klíčů druhé straně, využití vhodného média, bezpečné balení, vhodný transport, způsob přechodu na záložní klíče, plány výměny klíčů, postup při kompromitaci klíče atd. atd.

Poznámka: Slabým klíčem může být např. klíč, který při šifrování otevřeného textu v daném šifrovém systému vede zase na původní otevřený text. Při jednoduché záměně by byla takovou slabou převodovou tabulkou např. záměna písmena A za A, B za B atd. Pokud vše provádíte automaticky a převodové tabulky také automaticky generujete, může se stát, že taková tabulka vznikne, a proto ji musíte předem vyloučit. Takové slabé klíče existují i v mnohem dokonalejších šifrových systémech, např. jsou známy i v algoritmu DES.

Závěrem této části si zopakujme, že klíče musí být vždy dostatečně dlouhé, náhodné a vhodné (nesmí být např. „uhodnutelné“, nesmí se opakovat, nesmí být slabé atd.).

V tomto doporučení jsme se vědomě odchýlili od jedné z dalších zásad z již citované knihy Auguste Kerckhoffa *Vojenská kryptografie*. Tato zásada stanoví: *Klíč musí být takový, aby se dal zapamatovat bez písemných poznámek a musí být snadno měnitelný.*

Hesla

S výše uvedenou zásadou Augusta Kerckhoffa, věnovanou vytváření klíčů, jsme se neztotožnili, protože jsme popisovali vytváření klíčů pro moderní šifrové systémy, které musí odolat těm nejsložitějším kryptoanalytickým útokům a využití nejmodernější výpočetní techniky a její obrovské síle. V době Augusta Kerckhoffa byla situace přece jen výrazně odlišná. Kerckhoff se zabýval především polními vojenskými šiframi, které byly ruční a byly masově nasazeny a klíčové hospodářství z tohoto důvodu muselo být velmi jednoduché. Výpočetní technika dnešního typu samozřejmě ještě neexistovala, takže možnosti kryptologa byly z hlediska využití útoku založeném na testování klíčů omezené. Důležité tehdy bylo především to, aby vojáci vytvářeli klíče k šifrám kvalitní, dostatečně dlouhé, ale současně si je zapamatovali a nemuseli si je někde zaznamenávat, což by mohlo vést k jejich vyzrazení. Podmínky při práci s těmito klíči připomínaly dnešní situaci, kdy zadáváte přístupová hesla k různým systémům a aplikacím. Na jedné straně by to měla být hesla odolná útoku hrubou silou (dostatečně dlouhá a dostatečně „náhodná“), na druhou stranu si je musíte zapamatovat, abyste si je nemuseli zaznamenávat, což může jednak vést k jejich kompromitaci a jednak k tomu, že když je potřebujete, nejste schopni se k záznamu dostat a heslo použít.

Správci systémů a aplikací vám často předepisují určitou politiku, kterou musíte při zadání hesla splnit. Např. se předepisuje délka hesla, hlídá se současné použití malých a velkých písmen a případně využití číslic či dalších speciálních znaků. Jste upozorněni, že v hesle by

nemělo být obsaženo vaše jméno, jména vašich známých, jste nuceni hesla pravidelně obměňovat apod. I přes tato doporučení a kontrolu je běžné, že hesla nejsou kvalitní a jsou nejslabším článkem daného systému. Připočteme-li k tomu neprofesionální chování uživatelů jako např. prozrazení hesla sekretářce, heslo napsané na papírku nad monitorem, použití stejného hesla ke všem systémům, ponechání defaultního (předdefinovaného) hesla, při vynucené změně jen nepatrné a odvoditelné pozměnění (např. doplnění číslice za heslem), neopatrné zadávání hesla před svědky apod., je pak právě „heslo“ tou vstupní branou, kterou hacker projde do jinak bezpečného systému či aplikace.

Jak tedy správně postupovat při vytváření vhodného hesla?

Jedna z nejstarších rad, která se k tomuto tématu vztahuje, je v knize Řeka Aineia Taktika *Obrana opevněných míst* ze 4. st. př. n. l., kde autor radí římským vojákům vydávat hesla do stráže snadná pro zapamatování a svým významem co možná nejbližší zamýšlené akci. Je vidět, že bylo v tomto případě preferováno hledisko „pamatovatelnosti“ oproti hledisku kvality hesla. Důležité také je, že v případě hádání hesla před strážní hlídkou se útok hrubou silou (zkoušení různých hesel) použít nedá. To bychom asi dopadli velmi špatně. Kvalita hesla je tedy přímo závislá i na okolnostech použití. Obdobně se dá proto v případě bankovní čipové karty použít PIN (heslo) pouze v délce 4 číslic – služba je totiž po stanoveném počtu pokusů odmítnuta a karta zablokována.

Existuje řada různých systémů a situací, které vyžadují zadání hesla, a podle konkrétní situace je nutné klást důraz na různé aspekty hesla. V současné době se při stanovení obecných požadavků na profesionální heslové systémy vychází nejčastěji z dokumentu *Příručka pro řízení správy hesel* (Password Management Guidelines), který byl vydán již před dvaceti lety v USA (Department of Defense, April 1985).

Oblíbené pro vytváření přístupových hesel k softwarovým aplikacím je také využívání doporučení firmy Microsoft uvedené v dokumentu Windows 2000 Hardening guide (Chapter 5 - Security Configuration), které stanoví následující požadavky na přístupová hesla

Pamatování historie hesel	24 dny
Maximální délka trvání hesla	70 dnů
Minimální délka trvání hesla	2 dny
Minimální délka hesla	8 znaků
Požadavek na složitost	alespoň 3 znaky ze skupin: - velká - malá písmena - číslice - speciální znaky (nealfanumerické znaky)

http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/05sconfg.mspx

Obecně však stačí, když si zapamatujeme následující zásady pro běžné užívání hesel:

- délka hesla nejméně 8 znaků (znaky, pokud je to možné, vybírat z celé typové nabídky, tj. využívat velká a malá písmena, číslice, speciální znaky)
- heslo má být uživatelem snadno zapamatovatelné, má se dát snadno a rychle napsat, ale nelze je nepovolanou osobou uhádnout
- heslo nikdy nikomu neprozraďte
- heslo nikdy nikam nezapisujte a neukládejte

- pro různé systémy používejte různá hesla
- heslo měňte (přibližně za čtvrt až půl roku).

Mimo druhé zásady jsou ostatní doporučení pochopitelná a uživatelem (pokud chce) realizovatelná. Druhá zásada … *heslo má být uživatelem snadno zapamatovatelné, ale nelze je uhádnout*…, se však již zajišťuje podstatně hůře.

Tvorba hesla

Existuje spousta doporučení a návodů, jak tvořit vhodná hesla. Patří mezi ně např. doporučení používat slova, která nejsou ve slovníku daného jazyka a nelze je tedy při „slovníkovém útoku“ uhodnout. Taková slova mohou být různé novotvary, termíny z vědecko-fantastických knížek, slova z dětského žvatlání apod. Obecně se však takováto slova ještě stále nepovažují za příliš bezpečná. Pokud je chcete přesto použít, měli byste je doplnit o nějakou tu hvězdičku, číslici apod. Jindy se doporučuje vyjít např. z data pro nás důležité události (kterou však útočník nezná resp. se k němu nemůže dostat, tedy vaše datum narození není to „pravé“) a toto datum podle nějakého jednoduchého vzorce upravit (přičíst konstantu, místo číslice uvádět její doplněk do deseti atd.) a samozřejmě doplnit nějaké to „písmenko“. Mnoho studií považuje za jednu z vhodných a dostačujících metod spojení dvou kratších slov s číslicí nebo speciálním znakem.

Přes všechny tyto výše uvedené návody doporučuji pro zodpovědnou tvorbu hesla (tedy vždy tehdy, kdy vám záleží jak na kvalitě hesla, tak na tom, abyste heslo nezapomněli) jako nejvhodnější *metodu motivu a výpočtu hesla*. **Motiv** vám umožní si základ hesla v případě potřeby připomenout a výpočet pak z tohoto základu zajistí vytvoření silného hesla. Vzniklé heslo pak zdánlivě vypadá jako náhodné a může být poměrně odolné.

Motivem by mělo být něco, co je vám blízké, takže pokud si na něj vzpomenete, musí se vám díky němu jednoznačně vybavit příslušný základ hesla. Výpočet hesla pak musí být postup, který je jednoduchý a jednoznačný a také si jej samozřejmě bezpečně zapamatujete.

Vše si ukážeme na několika příkladech.

Pokud se zajímáte o šachy, pak můžete např. používat heslo: SpE2E4Jf3Jc6Sb5. To odvodíte v případě potřeby tak, že si vzpomenete na motiv „šachy“ a základem hesla je pak vaše

oblíbené zahájení - Španělská hra. Odvození hesla spočívá v tom, že se zadá zkratka názvu zahájení a zápis úvodních tahů tohoto zahájení v klasické šachové notaci. Vstup do jiného systému může pak být zase začátek jiného zahájení.

Jiné heslo může být odvozeno z motivu vaši oblíbené písně. Výpočet může být založen na využití prvních písmen jednotlivých slov. Příklad: motiv Mrazík - Ivanova píseň „Před naší za naší, cesta má ať nepráší, hej“ a odvozené heslo : Pnzncmanh. Můžeme ještě heslo vylepšit tím, že si stanovíme silnější pravidlo pro jeho výpočet např. tak, že budeme střídat malá a velká písmena a na závěr doplníme číslo, které vyjadřuje počet slov vybrané ukázky z písně. Po této úpravě dostanete heslo: PnZnCmAnH11.

Poslední příklad, který si uvedeme, může být založen na motivu čísla domu a odvození hesla bude založeno např. na úkonu dělení. V tomto případě by mohl proces vytvoření hesla vypadat nějak takto: motiv – číslo domu, základ pro výpočet hesla číslo domu, kde bydlí teta (2084), výpočet hesla bude založen na dělitelnosti číslem 3. Heslo pak dostaneme tak, že nejprve spočteme 2084 : 3 = 694,6666…. . Pokud lze použít pouze číselné heslo (např. PIN) bude heslem sekvence 6946 a v případě hesla, kde lze použít i jiné znaky, lze využít např. zápis *Sest94,6 atd.*

V těchto případech musíte svůj „motiv“ a základy hesel opravdu úzkostlivě tajit a samozřejmě si pamatovat přesný způsob odvození hesla. Způsob výpočtu hesla ze základu hesla, které nám motiv připomene, se nedoporučuje často měnit. Motiv by měl být natolik nosný, aby vám byl schopen dobře připomenout několik základů hesel.

Klíčové fráze

V některých návodech k autentizaci heslem se dočtete, že je doporučováno použití tzv. ověřovací věty – **klíčové fráze** (passphrase). Termín zavedl v roce 1982 S. N. Porter pro velmi dlouhé znakové heslo, tím může být např. dlouhá věta, ale může to být také shluk různých nesouvisejících slov. Ani tato metoda však není dokonalá, a to zejména ze dvou důvodů. Řada systémů neumožňuje zadávat dlouhé heslo, ale třeba jen heslo délky 8-15 znaků a v tomto případě je tato metoda nepoužitelná a svádí k použití pouze začátku ověřovací věty, což by se ovšem mohlo ukázat jako velmi slabé heslo, které by nebylo odolné při slovníkovém útoku. Druhý důvod je, že zadání klíčové fráze z klávesnice není bez problémů, zápis trvá dlouho a hrozí nebezpečí přepsání nebo vynechání písmene, neboť většina systémů při zapisování hesla neumožňuje sledovat, co píšete.

Tak co, už máte jasno, jak vytvořit svá silná a přitom jednoduchá hesla pro různá použití?

B. Poznámky k internetovému podvodu zaměřenému na klienty české Citibank

Ondřej Suchý, LOGIOS s.r.o., (ondrej.suchy@logios.cz)

Úvod

Počátkem března se v Čechách objevil první tvrdý pokus o vylákání identifikačních údajů k účtům českých klientů Citibank.

Přestože byl podvod poměrně dobře popsán jak v mainstreamových, tak ve specializovaných médiích, pokusím se shrnout dostupné informace a doplnit ještě několik aktuálních poznámek. Domnívám se totiž, že podobných podvodů bude přibývat a je užitečné mít informace pohromadě.

Tento článek je upravenou a rozšířenou verzí krátké zprávy, která vyšla na webu firmy LOGIOS (viz [1]).

Co je to Phishing?

Čtenářům Crypto-World snad netřeba vysvětlovat, ale pro úplnost: Phishing (z angl. „fishing“, rybaření) je podvod, při kterém se počítačoví piráti snaží od důvěřivých uživatelů získat citlivé údaje, například přístup k elektronickému bankovnictví. Obvykle k tomu využívají lživé výzvy zaslané elektronickou poštou, často odkazující na falešné webové stránky s formulářem pro zadání údajů, imitující prezentaci skutečné instituce.

Kdo provozuje Phishing?

Výzkumy projektu Honeynet (blíže [2]) ukázaly, že „phishingem“ se zabývají organizované gangy s vazbami na státy východní Evropy (např. Rumunsko) a Rusko. Úlohy v takových organizacích bývají rozdělené: někdo získává e-mailové adresy potenciálních obětí a rozesílá podvodné výzvy, jiní lidé programují falešné stránky a pravděpodobně jiní lidé zajišťují převody a výběr peněz.

Jedná se o první český Phishing?

Aktuální případ Citibank je prvním útokem svého druhu v českém jazyce. Nicméně čeští uživatelé Internetu byli v minulosti často adresáty podobných výzev v jiných jazycích, převážně v angličtině.

Jak reagovali adresáti výzev?

Uvádím některé zajímavé reakce. Vyjma první, stoprocentně autentické, jsou převzaty z diskusních fór a článků, kde nebylo možno ověřit jejich pravdivost:

„*Já účet v Citibank nemám, ale nemohl si ho tam někdo založit na moje jméno?*“ (osobní sdělení)

„*Bohužel jsem naletěla, poslala jsem číslo karty i PIN (ovšem ne u Citibank, ale u KB)*“ (diskusní fórum na VIRY.CZ, viz [3])

„*Sousedovi přišlo divné, že ho kontaktovali ze CityBank, když má peníze v České spořitelně. Soused je ukázněný, když na něm někdo něco chce, tak to udělá. … Pečlivě vyplnil číslo karty a PIN*“ (článek na blogu Zina, viz [4])

„*Hned jsem se poradil s kolegy v kanceláři. Byli zajedno, že když mi někdo posílá peníze, měl bych ten mail určitě otevřít, kliknout na odkaz a vyplnit tam všechno co vím.*“ (komentáře k článku tamtéž)

„*Proč v Citibank nikdo nebere telefony, když si chci ověřit, zda mi tohle vůbec bylo odesláno?*“ (komentáře k článku na Novinkách, viz [10])

„*Napsal jsem o tom do CitiCZ, ale nezajímá je to, odpověď = 0*” (tamtéž)

Uživatelé nebyli schopni správně odhalit podvodnou podstatu výzvy, psané česky. Na anglicky psaný spam (a anglicky psané phishing podvody, které běžně českým uživatelům chodí a které zřejmě řadí do stejné kategorie jako spam) si lidé již nejspíš zvykli a nepřikládají jim velkou pozornost. Na tento e-mail reagovali. To je znepokojivé - stačí útok správně propracovat a vybočit z řady.

Za povšimnutí také stojí informace, že někteří dezorientovaní uživatelé vyplňovali přihlašovací údaje z jiných bank! Proto je důležité, aby i jiné banky, než jen Citibank, využily mediální pozornosti a co nejdřív zodpovědně a nepřehlédnutelně informovaly své klienty.

A poslední dvě reakce jsou rovněž zajímavé. Tito klienti se včas nedostali ke správným informacím. Netvrdím, že je chyba na straně Citibank, oni se také nemuseli ozvat na ty správné kontakty, ale i z toho by si banka měla vzít ponaučení.

Je pachatelem Čech?

Nejspíš ne. Hovořilo by proti tomu několik indicií:

(1) Některé jazykové konstrukce použité v podvodném dopisu jsou velmi kostrbaté („*Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank online a dále postupujte podle předloženého návodu*“). Poznámka: kromě této zvláštní stylistiky je však jazyková úroveň zbytku textu překvapivě dobrá. Jízlivá poznámka: v počítačovém světě nemusí být podobné vyjadřování výjimkou, ale prozatím předpokládejme, že text nepsal Čech.

(2) Zpráva je ve špatném kódování. Je použito UTF-8, které není dobře zadáno do hlavičky mailu. Velké části příjemců se zpráva zobrazila se špatnou diakritikou („rozsypaný čaj“). Znalec místních internetových reálií by určitě věděl, jak psát český mail, a navíc má možnost si zobrazení otestovat.

Pár poznámek k dalším indiciím:

(3) Zdrojové adresy, ze kterých byl e-mail poslán, jsou umístěny v zahraničí. To však nemusí nutně na zahraničního podvodníka ukazovat. Ani pro českého pachatele by nemusel být problém získat pro rozesílání napadená PC z cizích zemí.

(4) Adresy, na kterých byl umístěn podvodný web, jsou též zahraniční. To má stejně spornou vypovídací hodnotu jako předchozí bod.

Také proto, že podobné útoky jsou v zahraničí běžné, se domnívám, že šlo o zahraniční pachatele, kteří zkouší své operace rozšířit i do dalších lokalit.

Kdo byl adresátem výzvy?

Výzva přišla na e-mailové adresy velkého počtu uživatelů české národní domény. Podvodníci pravděpodobně zakoupili část spammerské databáze.

Poznámka: dle příspěvku P. Součka (viz [5] – diskusní fórum na Živě.cz, (ostatně toto fórum je plné i dalších zajímavých informací) výzva přišla jednak na adresy zjevně ze spammerské databáze, jednak na automaticky generované neplatné adresy. Nemyslím si však, že by tyto cíle naslepo zkoušeli sami phishingoví podvodníci. Spíš si spammer, který jim adresy prodal, zkouší přilepšit a do nabízené databáze sem tam něco „přigeneruje“. Že by se podvodníci stali obětí podvodníčka?

Proběhly podobné útoky i jinde než v ČR?

Zejména v Polsku je internetová kriminalita tohoto typu poměrně rozšířená. Polsko též drží smutný rekord, kdy pomocí trojského koně kdosi odchytil přihlašovací údaje k účtu, z něhož poté odčerpal 1 milion zlotých, tedy přes 7 milionů korun.

Aktuálně má polská Citibank velký problém, kdy někdo „vycucl“ peníze z několika stovek účtů. Zatím mi není znám mechanismus útoku.

Citibank také řeší vážný incident (viz [9]), kdy prý vinou třetí strany, která zpracovává data o platebních kartách, unikly informace o PIN kódech velkého množství klientů. Klientům z USA, kteří se v Kanadě, Velké Británii a Rusku pokusí vybrat hotovost, bankomat transakci zamítne. Helpdesk jim obvykle nepomůže (a mlží) a klienti jsou ponecháni v zahraničí bez hotovosti.

Nicméně výše uvedené problémy zřejmě s „českým“ útokem přímo nesouvisí, zřejmě se bude jednat o izolované incidenty.

Je možné podvodníky odhalit?

Velmi obtížně. Jedná se o mezinárodně operující gangy a jejich odhalení by vyžadovalo velmi úzkou spolupráci vyšetřovatelů z mnoha zemí. Technické odhalení by mohlo teoreticky proběhnout pomocí tří stop:

(1) Trasováním internetových adres použitých k rozeslání e-mailových výzev,
(2) Identifikací majitele internetové adresy, na které byly umístěny podvodné stránky,
(3) Identifikací osoby převádějící nebo vybírající peníze z účtů obětí.

S tím však pachatelé pravděpodobně počítají:

(1) Adresy, ze kterých jsou e-maily odesílány, jsou pravděpodobně umístěny na serverech nic netušících obětí, kterým pachatelé „hacknuli“ počítače. Pokus provedený před rokem odborníky LOGIOS ukázal, že stačí dva dny, aby byl nezabezpečený počítač napaden a zneužit k podobným bankovním podvodům.

(2) Falešné webové stránky byly pravděpodobně umístěny také na počítači nic netušící oběti. A internetová doména byla registrována na člověka jménem Travis Godfrey, který skutečně žije v Utahu v USA (*Google našel, že osoba tohoto jména ze stejného města se před časem umístila na 356. místě běhu na 5. kilometrů*). Nemyslím si, že by chudák pan Godfrey byl do podvodu zapojen, spíš je další oběti stejného gangu. Jeho identifikační údaje (a možná i jeho peníze) byly zneužity k registraci domény. Nezapomeňme, že podle předchozích indicií se jedná o mezinárodní gang, který tuto činnost nejspíš neprovádí poprvé a má již pravděpodobně přístup k cizím údajům a penězům.

(3) Pachatelé mohou k výběru peněz použít „bílé koně“ nebo peníze převádět do zahraničí. Analýza projektu Honeynet (viz [2]) upozorňuje na nabídky ve

špatné angličtině a němčině, které osobám z Evropy nabízí 10% provize z částek, které pomohou převést „ze zahraničí“ do Ruska.

Je za úspěšně realizovaný podvod odpovědná banka nebo zákazník?

Pravděpodobně by podvod byl k tíži klienta. Smluvní podmínky obvykle obsahují ustanovení, které uživateli zakazuje sdělovat své přihlašovací údaje někomu dalšímu. Přestože si uživatel nebyl vědom, že se jedná o podvod, svévolně sdělil údaje někomu cizímu. Jinými slovy: máte smůlu.

Závěr

Podvodné gangy se evidentně rozhlížejí po nových „trzích“. Domnívám se, že se podobné výzvy jistě budou opakovat. Z toho, jak uživatelé překvapivě pozitivně reagovali, je jasné, že půjde o vážný problém. Zvlášť pokud pachatelé opraví chyby narušující věrohodnost výzvy (například špatné kódování).

Z toho vyplývá celá řada poučení:

Doporučení pro banky

České banky by měly spustit informační kampaň, například formou dopisu každému klientovi, opakovaných e-mailů a viditelného upozornění na webových prezentacích. Je nutné uživatele upozornit, že podobné podvody existují, a vysvětlit, jak je rozeznat a jak se bránit.

Protože z reakcí uživatelů Internetu je patrné, že údaje vyplnili i klienti jiných bank, do informování by se měly pustit i ostatní české banky - nejen exponovaná Citibank. Co nejdřív, dokud mediální pozornost ještě úplně nevychladla.

Aby byly schopny včas a správně reagovat a vyhnuly se improvizaci, měly by bankovní ústavy předem vypracovat plány na zvládnutí situace, kdy se klienti banky stanou adresáty podobných podvodů.

Doporučení pro IT manažery firem

Opatření ve firmách by měla směřovat hlavně do dvou směrů: Zajištění bezpečnosti systémů, aby někdo nezneužil servery k rozesílání výzev nebo umístění falešných stránek a společnost se tak nechtěně nestala mezičlánkem útoku. A informování uživatelů, pracujících s firemními účty, o podobných podvodech a způsobu, jak jim čelit.

Doporučení pro běžné uživatele

Hlavní doporučení zní: buďte si vědomi, že podobné útoky existují a mohou se přihodit i vám. V případě pochybností volejte banku, ale použijte číslo z tištěných materiálů banky nebo z telefonního seznamu. Telefonní číslo uvedené ve falešné e-mailové výzvě nebo na stránkách, kam vás zpráva odkáže, může vést k podvodníkovi.

Vyberte si takovou banku, která používá dodatečné metody autorizace, například přes SMS, čipovou kartou nebo kalkulátorem. Nedůvěřujte bance, ve které stačí pro převod peněz znát jméno a heslo.

A stále platí pravidla pro obecnou bezpečnost na Internetu: neinstalovat neznámé programy, nenavštěvovat nedůvěryhodné stránky, používat aktualizovaný antivirus a osobní firewall, ale to se již opakujeme.

Doporučení pro média

Publicita. Média by měla podobným útokům věnovat velkou pozornost, aby každý uživatel elektronického bankovnictví o podvodech věděl. Velmi dobře o problému informovala televize Nova. Nezatěžovala přílišnými podrobnostmi, ale uvedla to nejpodstatnější. Ve způsobu, jak podstatné informace „ergonomicky" dostat k těm nejobyčejnějším uživatelům, se od ní můžeme učit.

Zdroje informací

[1] Suchý O.: *Analýza phishing podvodu zaměřeného na klienty Citibank,* http://www.logios.cz/a/citibank-cesky-phishing-analyza/66

[2] Honeynet Project: *Know your Enemy: Phishing*, http://www.honeynet.org/papers/phishing/

[3] VIRY.CZ: *První český Phishing se stal realitou! - komentáře k článku*, http://www.viry.cz/go.php?od=0&perstranka=15&p=viry&t=listkomentare&k=novinka&id=2468

[4] Zina Blog: *Největší pes a phishing*, http://zina.blog.cz/0603/nejvetsi-pes-a-phishing

[5] Živě.cz: *Kdo se skrývá za prvním českým phishingem? – komentáře k článku*, http://zive.cz/h/Viryabezpecnost/F.asp?ARI=128484&HID=1&CAI=

[6] WebSEC: *Citibank – phishing*, http://websec.blog.lupa.cz/0603/citibank-phising-20060303

[7] WebSEC: *zdrojový text podvodného e-mailu*, http://websec.cz/phishing/citi-20060303/mail.txt

[8] Symantec: *Symantec Internet Security Threat Report, Trends for January 05 – June 05*, Symantec 2005

[9] Appelbaum J.: *Citibank - "We don't care about you!"*, záznam v blogu http://ioerror.livejournal.com/301520.html

[10] Novinky: *Citibank varuje své klienty před podvodnými e-maily – komentáře k článku*, http://cgi.novinky.cz/discussion.py?action=showDiscussion&server=novinky&discussionId=77358&articleId=79087

[11] Novotný P.: *Deníček („kterak známý bavič Petr Novotný reagoval na podvodný mail")*, http://www.petr-novotny.cz/denicek/4.3.2006/cist.aspx

C. NIST (National Institute of Standards and Technology - USA) a kryptografie, část 2.

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

1. Úvod

Jak již bylo řečeno v první části, na stránkách NIST se můžeme seznámit s klíčovými dokumenty důležitými pro implementace IT bezpečnosti (a konkrétně i kryptografie) ve vládních organizacích USA. V prosinci 2005 (tedy relativně nedávno) se objevila nová verze dokumentu uvedeného v názvu této části, tedy příručky pro implementace kryptografie [1]. Pro naše účely (přehledu o dokumentech NIST) je jako výchozí dokument proto vhodná ze dvou důvodů - jednak obsahuje ucelený pohled na problematiku a jednak jsou v ní i odraženy momenty aktuální situace. Současné vydání SP 800-21 nahrazuje příručku z roku 1999, je její přepracovanou verzí. Ještě je třeba upozornit, že doporučení a normy NIST jsou závazné pro federální systémy USA, ale nevztahují se na systémy národní bezpečnosti.

Samotný dokument je rozdělen do 6 kapitol a 5 příloh. Po úvodní kapitole následují:

2. Normy a příručky
3. Kryptografické metody
4. Obecné problémy implementací
5. Hodnocení
6. Volba kryptografických postupů

Přílohy obsahují doplňkové informace (akronymy, termíny a definice, odkazy, legislativa, další související publikace SP a FIPS).

Kromě dokumentů FIPS a NIST SP jsou v příručce citovány i odkazy na výstupy dalších normalizačních institucí – ANSI (American National Standards Institute), ISO (International Organization for Standardization), IETF (Internet Engineering Task Force), IEEE (Institute of Electrical and Electronics Engineers). Úvodní kapitola také ve stručnosti říká, komu je příručka určena, kterých problémů se týká, a obsahuje stručný popis možných využití kryptografických postupů.

2. Normy a příručky

V této kapitole najdeme především odkazy na odpovídající legislativu USA a s tím související vysvětlení, která zdůvodňují závaznost postupů obsažených v dokumentech NIST. Normy NISTu jsou určeny pro orgány federální vlády, avšak velice často jsou používány a požadovány i soukromou sférou.

Jaké užitky mohou plynout z využívání norem:

- *interoperabilita* (produkty vyvíjené dle konkrétní normy mohou být použity k ustavení interoperabilty s jinými produkty, které byly vyvíjeny dle téže normy);
- *bezpečnost* (normy mohou být použity k tomu, aby jejich prostřednictvím byla nastavena schválená bezpečnostní úroveň);

- *kvalita produktu* (která vlastnost musí být implementována, vyvinuté testy ověřují správnou funkčnost);
- *všeobecně používaný způsob reference* (např. FIPS 140-2 je používána jako obecně užívaný způsob reference tím, že definuje 4 úrovně bezpečnosti pro každý z jedenácti bezpečnostních atributů);
- *úspora nákladů* (je definována jediná obecně uznávaná specifikace, není třeba něco obdobného vyvíjet v jednotlivých organizacích).

Dokumenty FIPS mají závazný charakter, zatímco například dokumenty SP (Special Publication) mají charakter doporučení.

3. Kryptografické metody

Tuto část dokumentu lze mj. číst i jako příjemný úvod do kryptografie (tedy bez popisu matematických algoritmů). Jsou zde shrnuty základní objekty kryptografie, popsány jejich vlastnosti a vzájemné vztahy. Rozlišeny jsou tři základní typy kryptografických algoritmů:

- kryptografické hashovací funkce nevyžadující klíče
- symetrické algoritmy
- asymetrické algoritmy

a odděleně jsou uvedeny generátory náhodných čísel.

K tomu, aby kryptografie fungovala, musí být na správném místě klíče. Musí být "ustaveny" a to buď ručně (důvěryhodným kurýrem či osobním setkáním) anebo elektronicky. Ale i při elektronické metodě je vyžadováno použití ruční metody pro instalaci prvního klíče (na tomto základě fungují i certifikační autority).

Algoritmy pro hashovací funkce (schválené pro používání federální vládou) jsou popsány v dokumentu FIPS 180-2, Secure Hash Standard (http://csrc.nist.gov/publications/fips/fips180-2/fips180-2change1.pdf) a jsou to hashovací funkce SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. V dokumentu je také (aktuálně) poznamenáno, že vzhledem k novým útokům na SHA-1 není tento algoritmus doporučován k použití v nových implementacích.

Mezi doporučované symetrické algoritmy, které dokument zmiňuje, patří TDEA (Triple Data Encryption Algorithm) a AES (Advanced Encryption Standard). TDEA vychází z algoritmu DES, který byl dříve používán jako americká vládní norma pro šifrování, dnes již nemá dostatečnou kryptografickou odolnost. Algoritmus TDEA je popsán v NIST SP-67, jeho použití pro vládní orgány bude podporováno pouze do roku 2030 (viz NIST SP 800-57).

Algoritmus AES je specifikován v dokumentu FIPS 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). Souvisejícím dokumentem, ve kterém jsou popsány módy operací blokových šifer (postupy konkrétního používání algoritmů symetrických blokových šifer), je dokument Recommendation for Block Cipher Modes of Operation (NIST SP 800-3A). Dokument NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Authentication Mode definuje módy pro výpočet MAC a dokument SP 800-38C definuje mód pro provádění obou operací (šifrování a výpočet MAC) souběžně.

Asymetrické algoritmy (algoritmy, které používají pro šifrování a dešifrování dva odlišné klíče) mohou být v praxi využívány pro několik různých účelů. Primárním využitím je zabezpečení integrity zpráv, autentizace a nepopiratelnosti (používáno při vytváření digitálních podpisů), ale také jsou používány při ustavení klíčů.

Dokument FIPS 186-3 (draft tohoto dokumentu se nyní právě objevil – http://csrc.nist.gov/publications/drafts.html#fips186-3 – nahradí dokument FIPS 186-2), Digital Signature Standard (DSS) specifikuje postupy pro generování a verifikaci digitálních podpisů (opřené o použití asymetrické kryptografie). V dokumentu jsou specifikovány tři algoritmy pro digitální podpis: RSA, DSA a ECDSA.

Významnou změnou pro algoritmus DSA (oproti FIPS 186-2) jsou nově doporučované hodnoty pro velikosti parametrů. DSA - namísto pouze L=1024, N=160 se objevují až hodnoty L=3072, N=256, kde L je velikost použitého základního prvočísla p, N je velikost druhého použitého prvočísla q, což je prvočíselný dělitel p-1.

Co se týká RSA, tak tato norma specifikuje tři možné volby pro délku modulu n (součin dvou prvočísel, n = pq). Jsou to hodnoty 1024, 2048 a 3072 bitů. Certifikační autority by měly používat pouze poslední dvě hodnoty. Původní doporučení pro délku klíče algoritmu RSA se opírala o ANSI X9.31 (256 – 1024 bitů).

Co se týká eliptických křivek, tak dokument umožňuje využití tří typů eliptických křivek – křivky nad prvočíselnými tělesy, křivky nad binárními tělesy a tzv. Koblitzovy křivky.
Zůstaly zachovány doporučené křivky z dokumentu FIPS 186-2.

Speciální pozornost je třeba věnovat také následujícím třem otázkám:

- problematice ustavení klíčů, zde je odkazováno na dokument NIST SP-56, Recommendation on Key Establishment Schemes;
- generování náhodných čísel (odkaz na popis ve FIPS 186-3);
- správě klíčů, které je věnován dokument NIST SP 800-57, Recommendation for Key Management - rozsáhlý dokument, skládá se ze tří částí:
    1. General Guidance,
    2. Best Practices for Key Management Organizations a
    3. Application-Special Key Management Guidance.

Samostatný okruh otázek vytváří problematika PKI (bezpečnostní infrastruktura, ve které jsou vytvářeny a spravovány digitální certifikáty).

4. Obecné problémy implementací

S těmito otázkami souvisí celá řada problémů, které jsou hlouběji rozebírány v jiných dokumentech NISTu. Zde je poukázáno pouze na některé otázky, kterými se implementátoři kryptografie musí zabývat:

- použití HW či SW metod
- použití symetrické či asymetrické kryptografie
- obecné problémy správy klíčů

5. Hodnocení

V popisovaném modelu se testování bezpečnosti (v návaznosti na používání kryptografických postupů) dotýká čtyř základních vrstev:

- kryptografický algoritmus (FIPS 197)
- kryptografický modul (FIPS 140-2)
- produkt (Common Criteria Evaluation and Validation Scheme)
- aplikace, systém (Certification and Accreditation, SP 800-37)

V závorkách jsou uvedeny dokumenty, kde jsou příslušné postupy blíže specifikovány.

K programu CMVP (Cryptographic Module Validation Program) byly podstatné informace obsaženy v minulé části (Crypto-World 2/2006). K dalším podrobnostem se lze odkázat na citovaný dokument [1].

6. Volba kryptografických postupů

Obecně lze říci, že proces, při kterém jsou vybírány kryptografické mechanizmy, je podobný procesům výběru libovolných mechanizmů IT. Lze se tedy i zde odkázat na model životního cyklu pro vývoj informačního systému. V dokumentu jsou v návaznosti na to pak identifikovány některé specifické otázky související s implementacemi kryptografie (poměrně podrobně).

7. Literatura:

[1] SP 800-21-1 Second Edition, Guideline for Implementing Cryptography in the Federal Government, December 2005 (http://csrc.ncsl.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf)

D. Elektronické volby v ČR?

RNDr. Jaroslav Hrubý, CSc., FzÚ AV ČR, (hrubyj@prf.upol.cz)

1. Úvod

Vize realizace elektronických voleb v ČR je i v roce 2006 stále vzdálena realitě, i když v současnosti již má částečnou oporu v legislativě. Doposud však chybí politická vůle zákonně akceptovat formu elektronických voleb na úroveň formy klasického volebního procesu, tak jak jej známe.

Částečnou oporou v legislativě se myslí akceptace novel dále zmíněných zákonů, které by již umožnily důvěryhodnou realizaci voleb

Jedná se především o vládní návrh novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy, z roku 2004, která byla zpracována v návaznosti na nové požadavky vyvolané v praxi při dosavadní aplikaci zákona a dalším rozvojem informačních a komunikačních technologií, zejména postupným zaváděním služeb e-governmentu. Tato novela zpřesňuje povinnosti orgánů veřejné správy v souvislosti se správou a provozem informačních systémů veřejné správy a dává jakýsi legislativní základ pro budování informačních systémů. Druhým novelizovaným zákonem je zákon o elektronickém podpisu č. 227/2000 Sb. (a o změně některých dalších zákonů, jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb.) a rychlost jeho uvedení do života v celém spektru aplikací , včetně jeho dopadu na státní správu ČR.

Tyto novelizace by neměly být podceňovány a zákony by měl být uváděn co nejrychleji do praxe ruku v ruce s úpravou legislativy a to v celé šíři aplikací, kde se vůle občana stvrzuje podpisem.

V současnosti již v ČR existují tři akreditované certifikační autority a řada občanů je vlastníkem zaručeného elektronického podpisu. Novelizace zákona o elektronickém podpisu včetně zavedení kvalifikovaného časového razítka otevírá cestu k informační společnosti a jeho správná implementace do naší státní správy a také do všech ostatních oblastí naší činnosti, v níž hrál dosud stvrzovací roli klasický podpis jedince, je nezbytná pro naše přibližování k Evropské Unii (EU).

Jednou z možných aplikací, kterým tyto zákony otevírají cestu, jsou elektronické volby (e-volby). Tato aplikace je nesmírně významná, protože umožňuje realizovat tzv. on-line demokracii, tedy vztah realizovaný elektronicky mezi občanem na straně jedné a státní správou a politickými autoritami na druhé straně.

Se vstupem do 21. století je více než kdykoliv předtím jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů u státní správy, zavést elektronické peníze a v neposlední řadě vytvořit infrastrukturu pro takovéto praktické použití elektronického podpisu, jako jednoho se základních kamenů elektronické společnosti.

Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, kulturního a vědeckého je potřeba respektovat daný stav v EU. V případě

základních zákonů a právních norem v oblasti informačních technologií a systémů jsme (pokud to míníme s naším vstupem do EU vážně) rovněž povinni slaďovat naše zákony a normy s těmi platnými v EU, jelikož tyto dávají základ universálnosti použití, a hlavně garantovat bezpečnost všech aplikací, které stojí nad informační infrastrukturou .

V ČR je podstatným nástrojem k prosazování záměrů této iniciativy státní informační politika a v jejím rámci budovaná komunikační infrastruktura veřejné správy, což v současnosti patří do kompetence Ministerstva informatiky. Hlavním motorem by měly být finanční úspory, dosažené při její správné realizaci ve všech oblastech elektronizace u nás.

V tomto příspěvku se budeme zabývat vizí e-voleb v ČR a to z pohledu roku 2006. Dovolujeme si poznamenat, že se nejedená o pouhou nerealizovatelnou vizi, ale tento projekt je již dříve realizován pro státní správu ve Švýcarku. V ČR se jedná zatím o vizi, jelikož chybí potřebná legislativa, která by v rámci rozvoje e-governmentu takovýto způsob voleb, byť i jako doplňkovou možnost, připouštěla.

Projekt e-voleb navazuje na problematiku spojenou s aktivitami EU v oblasti elektronického podpisu a e-governmentu a realizuje nejenom on-line demokracii, která je vyjádřena kvalitní elektronickou komunikací občana se státní správou a politickými autoritami, ale tato aplikace také realizuje i obrácenou vazbu, tedy poskytování služeb státu občanům.

Zodpovědným orgánem za tuto zcela novou oblast je Ministerstvo informatiky, které by s Ministerstvem vnitra, Statistickým úřadem popř. jinými státními orgány mohlo učinit kroky k přípravě vytvoření potřebné legislativy pro realizaci e-voleb v ČR.

Kroky mohou být postupné, prokazující užitečnost realizace e-voleb popřípadě elektronického hlasování s využitím Internetu.

Některé firmy jsou již nyní schopny realizovat dílčí modely formou pilotních projektů, jako byl např. pilotního projektu pro hlasování parlamentu (i když tento model je jistou modifikací e-voleb) s možností budoucího rozšíření pro všechny druhy voleb realizovaných v ČR, pokud tak bude v příslušné legislativě toto umožněno.

Výhody realizování e-voleb přes Internet v ČR, jako doplňkové metody klasického způsobu voleb, jsou zejména následující:

- umožnění dostupného hlasování našim spoluobčanům žijícím trvale v zahraničí
- výrazné snížení nákladů na realizaci voleb / referenda (tisk a distribuce hlasovacích lístků)
- rychlost získání konečných volebních výsledků a možnost předpovědi výsledků s vysokou přesností (opět s minimálními náklady)
- mobilita voličstva (možnost hlasování občana s jiného místa než je jeho volební okrsek)
- jednoznačná identifikace garantující volbu pouze právoplatných voličů
- autentizace garantující voličovu identitu
- bezpečnost garantující tajnost hlasovacího (elektronického) lístku
- zpětná nezjistitelnost výběru kandidáta voličem
- nezpochybnitelnost volebního aktu, volič nemůže volit dvakrát resp. nemůže změnit svůj výsledek.

Projekt e-voleb by mohl vhodně navázat na druhou část projektu KI ISVS (Komunikační infrastruktura informačního systému veřejné správy), část GOVNET2, který je prezentován v materiálu [1].

Projekt e-voleb by vycházel z aplikace Směrnice evropské unie 1999/93/ES [2] a českého právního předpisu zákona o elektronickém podpisu č. 227/2000 Sb. a jeho pozdějších úprav. Tento projekt by mohl být významnou službou portálu veřejné správy a akceleroval by využívání PKI i pro jiné aplikace v rámci e-governmentu.

2. Bezpečnost a důvěryhodnost elektronických voleb

Ideální protokol garantující bezpečnost elektronických voleb by měl minimálně garantovat následující požadavky:

1. **Pouze autorizovaní voliči smí volit**
2. **Každý z nich smí volit pouze jednou**
3. **Nikdo nesmí zjistit, jak který volič volil**
4. **Nikdo nemůže provést duplikaci kterékoliv voličova hlasu**
5. **Nikdo nemůže změnit voličovu volbu bez toho, aby tato změna byla objevena**
6. **Každý volič musí mít jistotu, že byl jeho hlas započítán v konečném sčítání**

K těmto základním požadavkům lze přidávat další jako např.

7. **Každý může zjistit, kolik oprávněných voličů volilo apod.**

Např. při hlasování v parlamentu je naopak zájem znát, jak který poslanec volil, a proto bod 3. lze vypustit.

Samotná volba protokolu je poměrně složitá otázka související s autentizací a autorizací voličů, včetně identifikačního schématu, kteří jej po zašifrování svého hlasu veřejným klíčem Centrální volební komise (CVK) bezpečným způsobem musí zaslat do CVK. Zde musí proběhnout dešifrování a další nikým neovlivnitelné zpracování voličova hlasu, a to při garantování bezpečnosti a splnění výše uvedených požadavků.
Toto lze v současnosti řešit různými typy protokolů s modifikací podpisu (tzv. podpis naslepo), více volebních komisí apod., což je pro zájemce popsáno např. v knize B. Schneiera „Aplikovaná Kryptologie“ [3].

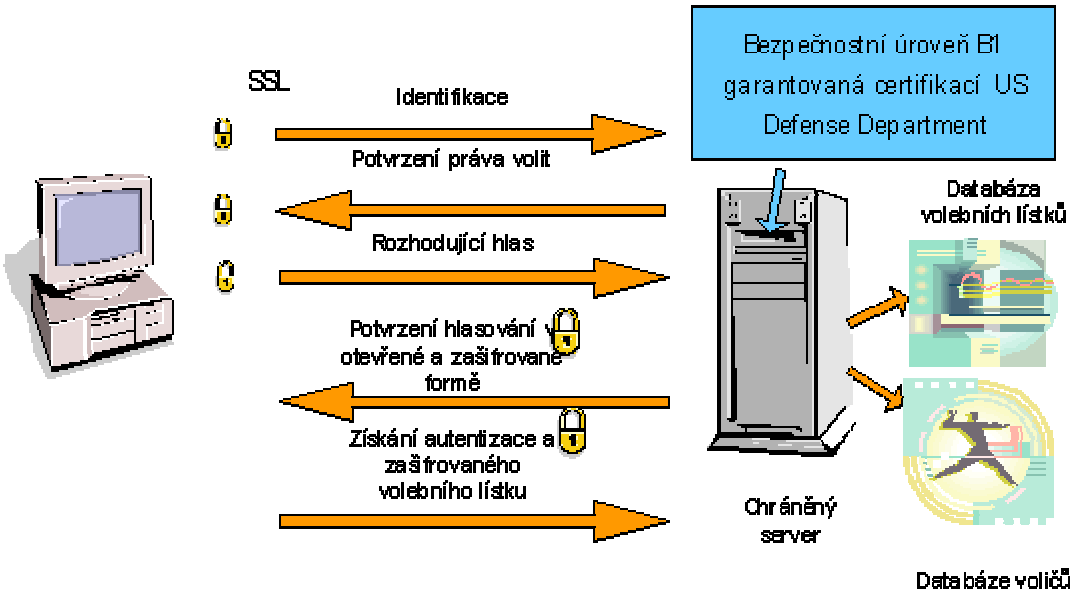
Zde se zaměříme pouze na nástin konkrétního zpracování problematiky e-voleb, tak jak je projekt e-voleb realizován ve Švýcarsku [4].
Tento projekt e-voleb je založen na následující ekvivalenci poštovních voleb a e-voleb:

Poštovní volby	**E-volby**
Registrace voličů	Elektronická registrace voličů
Volební obálka s hlasovacím lístkem	Balík šifrovacích dat s hlasovacími daty
Podpis voličů	Balík dat s identifikačními kódy
Dopis s volební obálkou, kde je uložen hlasovací lístek	Zašifrovaný balík dat s identifikačními kódy
Urna (box) s volebními obálkami s hlasovacími lístky	Elektronický box se zašifrovanými hlasovacími lístky

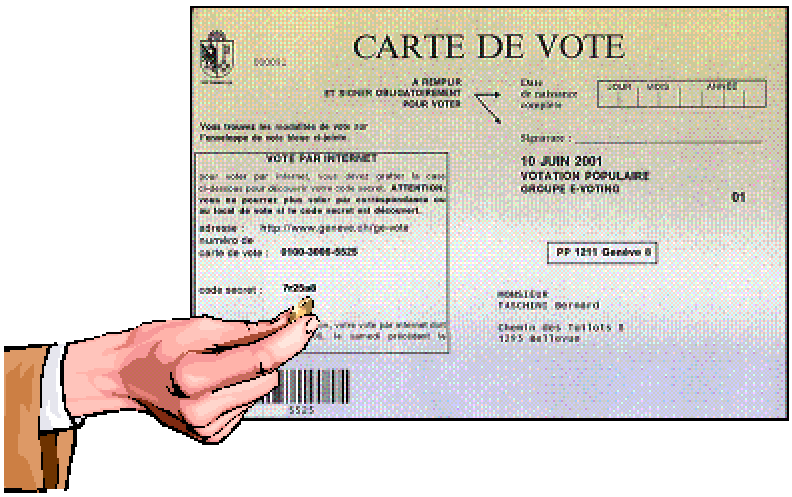
Analýza komplexního zabezpečení e-voleb je provedena z následujících hledisek:

- z hledisek politických a veřejných
- z hlediska zákonů, právních předpisů a norem
- z finančních hledisek
- z hledisek organizace a procesů
- z technických hledisek
- z hledisek užitečnosti e-voleb.

Politické a veřejné aspekty spočívají ve vysvětlení politickým subjektům a občanům, že e-volby jsou pouze alternativou ke klasickému způsobu voleb, která všem přináší řadu výhod, a to s cílem dosažení politické dohody o přijetí způsobu e-voleb. Politickým stranám je přitom garantována optimální bezpečnost, rychlost získání výsledků, zpětná kontrola a zapojení jejich potenciálních oprávněných voličů, nemohoucích se jich v den voleb osobně zúčastnit, ale majících přístup k Internetu.
Absolutní bezpečnost samozřejmě neexistuje, ale v současnosti lze dosáhnout i vyšší úrovně bezpečnosti, než při klasickém způsobu voleb, a navíc eliminovat negativní případy, jako např. nesrovnalosti při sčítání hlasů při prezidentských volbách v USA ve státě Florida.
V současnosti jsou zvažovány i možnosti realizace kvantových protokolů na realizaci elektronických voleb, které mohou eliminovat i v budoucnu případné útoky na PKI pomocí kvantového výpočtu [5].
Zákonné a právní předpisy bylo nutné ve Švýcarsku zvládnout úpravou legislativy. To by bylo samozřejmě také prvním a nezbytným krokem pro realizaci e-voleb v ČR. Elektronické databáze voličů by naopak mohly vznikat již nyní v rámci rozpracování projektu KI ISVS. Bezpečnostní IT normy aplikované ve Švýcarsku tj. X 509 certifikát a šifrování 128 bitovým klíčem v protokolu SSL/TLS přes spojení http na Internetu jsou již běžně akceptovány také u nás.
Financování e-voleb je levnější než financování voleb klasických při zachování vyváženosti mezi stupněm požadované bezpečnosti a mírou investovaných prostředků do zabezpečení e-voleb. Toto je garantováno kvalitně provedenou analýzou rizik.
Provázanost technologických a organizačních procesů je obzvláště silná. To lze nahlédnout z následující obrázku schématicky znázorňujícího průběh e-voleb:



Úroveň bezpečnosti by u nás mohla být EAL 4 dle ISO/IEC 15408, která je vyhláškou stanovena pro IS akreditovaného poskytovatele certifikačních služeb, vydávajícího kvalifikované certifikáty, namísto úrovně B1 dle US normy.
Ve Švýcarsku např. proces identifikace probíhá nejenom zadáním „passwordu“, ale také dvěma doplňujícími otázkami. Jak konkrétně vypadá hlasovací lístek s udáním klíče, je patrné z následujícího obrázku:



E-volby ve Švýcarsku garantují bezpečnou identifikaci, autentizaci, utajenost volby oprávněného voliče, právní neodmítnutelnost a všechny další aspekty uvedené na začátku této kapitoly v bodech 1.-7. Podrobnosti o nich lze získat na Internetu http://e-gov.admin.ch/vote/.

3. Závěr

Přínosem by již nyní byly značné finanční úspory při komplexním pojetí všech možných aplikací KI ISVS a především v řešení aplikace chytrých karet pro PKI (SC PKI), které budou v EU bezpečným podepisovacím prostředkem.
I když Švýcarsko je první vlašťovkou a i v EU se legislativa teprve dotváří, je nutné brát tuto výzvu vážně.
Věřím, že kryptologická komunita může sehrát význačnou roli v prosazení vědomí o volební „e-demokracii“ v ČR.

Literatura

[1] Metodika využívání komunikační infrastruktury veřejné správy, ÚVIS, duben-květen (2002).
[2] The Directive 1999/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 1999/93/EC, dále dokumenty ETSI, http://www.etsi.org/SEC/el- sign.htm ,viz. také http://www.uoou.cz .
[3] Bruce Schneier, Applied Cryptography, ISBN 0-471-12845-7, John Wiley&Sons.Inc.(1996), p.125.
[4] Frank Zimmermann, HP Consulting& Integration, IST 2002 Conference, Kopenhagen, November 2002.
[5] S. Dolev, I. Pitowski, B.Tamir, e-print xxx.lanl.gov, quant-ph 0602087 (2006).

E. O čem jsme psali v březnu 1999 – 2005

Crypto-World 3/2001

Crypto-World 3/2002

Crypto-World 3/2003

Crypto-World 3/2004

Crypto-World 3/2005

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:

http://crypto-world.info

2. Registrace / zrušení registrace

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

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a **e-mail adresu**, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf

NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška

Webmaster Pavel Vondruška, jr.

4. Spojení (abecedně)

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