Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 6/2003 **16. červen 2003**

6/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(440 e-mail výtisků)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Nebezpečí internetových řešení
Ing. Miloš Kuchař, IT-COM, s.r.o.

Úvod

O bezpečnosti Internetu se hovoří snad od jeho počátku. Média či specializované firmy nás tu a tam informují o nových, rychle se šířících virech nebo o útocích hackerů, kterým se podařilo pozměnit obsah WWW serveru té či oné organizace. Mnoho lidí z IT pokládá rovnítko mezi bezpečnost internetových aplikací a pojem SSL. Takže pokud se zákazník svého dodavatele ptá na bezpečnost, diskuse s dodavatelem internetového řešení se obvykle točí kolem firewallů nebo kolem autentizace mezi klientem a serverem a šifrování spojení právě prostřednictvím SSL. Tyto prostředky samozřejmě bezpečnosti pomohou, ale bohužel nejsou všelékem. Jakých triků tedy mohou útočníci využít, na co si dávat pozor a jak se útokům bránit?

Internetové útoky

Útoky můžeme rozdělit do několika základních skupin podle jejich charakteristik:

- ***Útok na dostupnost*** – cílem útočníka je službu www serveru shodit, zamezit, aby uživatelé mohli daný systém používat. Formou útoku může být například přetížení serveru takovým způsobem, aby došlo ke zpomalení nebo úplnému zahlcení.
- ***Útok na důvěrnost*** – útočník se snaží dostat k informacím, které mu nejsou určeny, například do e-mailové schránky někoho jiného, apod. Útok má pak například formu odchytávání paketů odcházejících od oběti, nebo dokonce pokus o rozlomení šifrovaných zpráv.
- ***Útok na integritu*** – útočník se snaží změnit obsah serveru a umístit zde neautorizované informace. Klasickým příkladem je pozměnění vizáže stránek tak, aby došlo k poškození dobrého jména majitele stránek.
- ***Převzetí identity*** – cílem je obvykle začít se v systému vydávat za někoho jiného. Zajímavým příkladem je pokus přihlásit se k bankovnímu účtu někoho jiného a provádět "za něj" finanční transakce. Útok může být realizován například prostřednictvím trojského koně.

Většina ostatních útoků je nejčastěji kombinací předchozích možností.

Útoky je rovněž možné rozdělit podle jejich cílového zaměření. V zásadě existují tři možnosti: útok na server, útok na data během přenosu mezi serverem a klientem a útok na klientskou stanici.

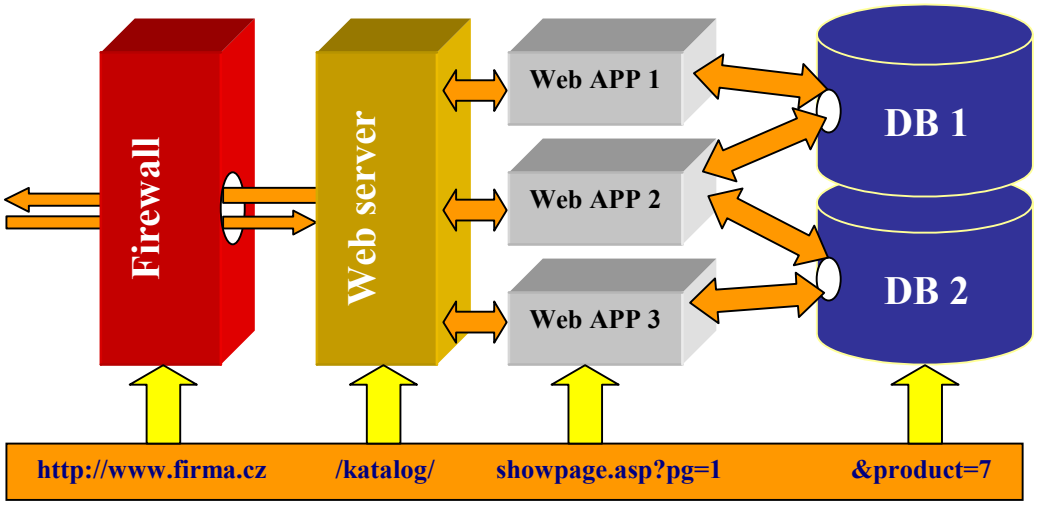
Hackerské techniky útoků na servery

Typické internetové serverové prostředí můžeme charakterizovat následovně: klasickým modelem zabezpečení internetových aplikací je předřazení firewallu. WWW server je pak provozován v tzv. demilitarizované zóně. WWW server žádá provedení příslušných

akcí po aplikacích v pozadí, které jsou napojeny na databáze obsahující všechny cenné informace. Popišme si některé jednoduché principy útoků možné na základě této architektury.

Útok skrze URL

Prostřednictvím URL bývá nepřímo ovládáno mnohem více systémů v pozadí. Například URL http://www.firma.cz/katalog/showpage.asp?pg=1&product=7 může hackerovi prozradit následující údaje o struktuře systému v pozadí:



Útočník prostřednictvím testu může zjistit, že proměnná ***pg*** nabývá určitých hodnot pro mazání záznamů, a hodnota ***product*** nabývá určitých hodnot pro identifikaci jednotlivých položek zboží. Pokud server pro dané sezení neověřuje autenticitu uživatele pokaždé, tak po jednom přihlášení může docházet k nekontrolovaným akcím, které nejsou vyvolány prostřednictvím uživatelského rozhraní, ale pomocí změn v URL. Další možností takovéhoto útoku je například získání neoprávněných údajů. Uživatelský interface nabízí pouze informace, které uživateli náležejí, ale pouhou důmyslnou změnou v URL mohu docílit získání dalších informací, které mu nejsou určeny.

Ochrana proti takovémuto útoku je pouze v dobrém návrhu aplikace, tj. v ověřování práv uživatele před každou žádostí přicházející ze strany klienta.

Ověřování vstupních dat

Další oblastí, která může být použita jako nástroj pro útok na WWW server ze strany Internetu, je nedůsledné ošetření vstupních dat, což může otevřít možnost úspěšných útoků založených na:

- *Buffer overflow* – přetečení plánovaného prostoru pro vstupní data – tento typ útoku může způsobit například zhroucení aplikačního serveru. Představme si situaci, kdy pro vstupní pole jméno je programátorem plánováno 20 znaků. Útočník však ve vstupním poli pošle na server text s délkou 2000 znaků. Pokud aplikace na straně

serveru na tuto eventualitu není připravena, může dojít k chybě, v krajním případě i ke zhroucení aplikace.

- Chybových hlášeních serveru prozrazujících další informace – například názvy připojení k databázi, apod. Cílem útočníka pak může být navození nečekaných událostí, které vyzradí další potřebné informace pro realizaci útoku. Další zajímavou skutečností je zotavení programu po chybě – tj. zda aplikace bude schopná pokračovat v chodu i po jejím "zahnání do kouta". Zda například správně vrací alokovanou paměť a všechny ostatní zdroje. Pokud ne, může mnohonásobné opakování simulace chybového stavu vést ke zhroucení serveru.
- Pozměňování hodnot skrytých polí ve formulářích – jedná se o pole, která slouží například pro uchování jednoznačné identifikace uživatele, apod. Stejná situace je s cookies na straně klienta, kam se na mohou ukládat informace důležité pro identifikaci uživatele.
- Vkládání dat ze vstupních formulářů SQL dotazů které jsou odesílány na databázový server. Znalost SQL a vhodného přidání složitější podmínky do vstupního pole umožní získat odpověď na dotazy, které programátor rozhodně nezamýšlel. Příkladem je příkaz typu "SELECT * FROM table WHERE table.id=%promenna%;". Představme si situaci, kdy za %promenna% je doplněn např. řetězec "1 OR 1=1" a ne prostá číselná hodnota jak předpokládal autor programu. Čitatelé znalí SQL zajisté tuší, co to způsobí – výraz za WHERE se vždy vyhodnotí jako pravda (protože 1=1), a útočník získá obsah celé tabulky a ne jen jemu určené řádky.
- Spouštění vzdálených procedur – jedná se v podstatě o stejný trik jako v případě doplňování SQL příkazů. Vhodnou interpretací vstupních polí nebo URL můžeme modifikovat parametry, které jsou použity při spouštění uložených procedur nad databází.

Z důvodu ochrany by měla být všechna vstupní pole na straně serveru kontrolována minimálně na následující parametry:

- Typ vkládaných dat
- Povolený rozsah
- Velikost vkládaných dat
- Metaznaky a skripty

Všechny testy by měly být prováděny na serveru. Kontroly parametrů na straně klienta, například pomocí JavaScriptu, mohou být útočníkem snadno vypnuty.

Získávání souborů nesouvisejících se samotnou aplikací

Další hackerskou technikou je pokus o získání "nadbytečných" souborů z WWW serveru, které mohou další útok usnadnit. Dobrým příkladem je například existence adresáře "reports" obsahujícího statistiky přístupů nebo různých ZIP souborů se zálohami obsahu serveru. Pokud se tyto záložní soubory dostanou do rukou útočníka, obvykle se z nich dozví mnoho zajímavého. Za nebezpečné lze považovat i příklady skriptů a dokumentaci, která bývá instalována spolu s WWW serverem. Je znám například útok založený na příkladech ASP skriptů přikládaných k IIS serveru.

Protiopatření je velmi jednoduché - udržovat na WWW serveru pouze ty soubory, které jsou nezbytně nutné a pečlivě kontrolovat nastavení práv k nim.

Útok pomocí trojského koně

Představme si například internetové aplikace, které využívají autentizaci prostřednictvím uživatelských certifikátů. V tomto případě soukromé části šifrovacích klíčů mohou být uloženy buď na pevném disku lokálního počítače nebo na čipové kartě či jiném autentizačním prostředku. V obou případech soukromá část klíče dále může mít nastaven příznak, který umožňuje jeho exportování. Toho bývá využíváno pro zálohování nebo pro přenos klíčového páru na jiný počítač.

Z důvodů minimalizace ceny řešení se autoři internetových aplikací obvykle spokojí s méně bezpečným uložením klíčů na pevném disku a bohužel i s nastaveným příznakem umožňujícím export soukromé části klíče. Tento stav je však bezpečnostní dírou umožňující útok pomocí trojského koně. Ten může mít řadu podob. Může to být spustitelný soubor připojený k e-mailu odeslaný "jakoby" od kolegy z firmy. Není třeba zdůrazňovat, že chudák kolega o takovémto e-mailu nemá ani potuchy. Příjemce e-mailu připojený soubor důvěřivě spustí a nevědomky si tak nainstaluje trojského koně na svůj lokální počítač. Ten se zde "zahnízdí" a čeká na okamžik, kdy se uživatel bude připojovat k dané Internetové aplikaci a na klávesnici napíše přístupové heslo k soukromé části klíče. To si trojský kůň zaznamená a spolu s vyexportovaným soukromým klíčem odešle útočníkovi někam do Internetu. Útočník tak má k dispozici soukromou část klíče a heslo k ní, což postačuje k získání identity oprávněného uživatele. Po provedení těchto akcí se trojský kůň odinstaluje a zamete po sobě stopy.

Pokud systémy nepoužívají pro autentizaci uživatelů certifikáty, je situace ještě jednodušší. Úkolem trojského koně je pak z klávesnice "odchytit" přístupové heslo a to odeslat útočníkovi.

Důležitou skutečností je, že trojský kůň není virus. Mezi zásadní rozdíly patří, že se neumí samovolně šířit a je obvykle naprogramován zcela jednoúčelově k cílenému útoku na jednu konkrétní osobu/jeden konkrétní počítač. Z těchto důvodů jej ve většině případů antivirové programy nerozpoznají a neohlásí jeho přítomnost.

Další důležitou skutečností je, že útok přes klientské počítače je mnohem jednodušší než útok na lépe opevněný server, který je na druhé straně spojení. Proto jeho realizace může být pro útočníka zajímavější.

Organizace provozující on-line internetové služby obvykle ve smlouvách předem deklarují, že nenesou odpovědnost za škody spojené prozrazením přístupového hesla, atp. V lepším případě umožňují několik alternativ pro autentizaci – od "levné", která ukládá soukromé části klíčů na disk a potencionálně sebou nese riziko nasazení trojského koně, až po dražší, které využívají bezpečnější autentizační prostředky. Uživatel takovéto služby by však měl být správně seznámen s bezpečnostními riziky spojenými s jednotlivými možnostmi. Obecně lze říci, že takovéto vyvinění poskytovatele služby je poměrně krátkozraké, protože v případě, že se najde útočník, který se na danou službu zaměří, může to poškodit dobré jméno firmy a důvěru v celou provozovanou službu.

Reverse engeneering (metody zpětného inženýrství)

Metoda zpětného inženýrství je dalším způsobem jak získat cenné informace o provozovaném internetovém řešení. Ačkoli je prováděna na stanici klienta, ve výsledku vede k útoku na server. Vždy se všeobecně mínilo, že tento typ útoku je po technické stránce velmi náročný a proto jeho pravděpodobnost je velmi malá. Není to však úplně pravda. Společným prvkem celé řady appletů spouštěných na straně klienta je právě skutečnost, že byly vyvíjeny v programovacím jazyce JAVA a byly překompilovány do tvaru JAR – většinou z důvodu možnosti použití v multiplatformním prostředí. Specielně pro tento jazyk existuje celá řada nástrojů umožňujících zpětný překlad JAR souborů do celkem dobře čitelného zdrojového tvaru.

Studium takto získaných zdrojových textů může útočníkovi prozradit důležité skutečnosti a napomoci tak v cíleném útoku. JAR soubor navíc může obsahovat i konfigurační soubory, které jsou pro útočníka snadno modifikovatelné. Klasickým problémem je možnost nastavení různých ”ladících režimů” dané aplikace, která obvykle vyřazuje některé bezpečnostní mechanismy.

Částečným řešením jsou tzv. *Obfuscátory* – programy, které se snaží zamíchat se symboly použitelnými při dekompilaci. Jiným, bohužel také pouze částečným řešením, je digitální podpis kódu appletu. Ten program chrání před jeho modifikací. Kontrola je však bohužel prováděna pouze na straně klienta – tj. tam, kde je přítomen útočník.

Závěr

Jak je vidět, slabiny internetových projektů mohou být založené na celé řadě faktorů a neexistuje jednoduchý a univerzální návod, jak před nimi chránit. Obecně platí, že bezpečnost IT je oblastí úzce specializovanou a měla by být řešena odborníky. Tato skutečnost platí i u zakázkově vyvíjených systémů, kterými internetové systémy obvykle jsou. Jak je z předchozích odstavců patrné, kvalitní analýza bezpečnosti výsledného řešení je základem pro dlouhodobě bezpečné řešení.

V každém případě je ale nutné sledovat novinky zejména z oblasti bezpečnostních děr u jednotlivých použitých komponent řešení – od WWW serverů až po databáze. Velmi často jsou oznamovány nové chyby u IIS i Apache, které patří mezi nejběžnější. Zde nezbývá než sledovat situaci a pravidelně instalovat opravné balíčky - “*patche*”, které výrobci jednotlivých serverů dodávají. I tady by mělo platit pravidlo maximální obezřetnosti – tj. aplikovat opravné balíky pocházející pouze z ověřených zdrojů a testovat jejich použití v testovacím prostředí před jejich spuštěním na “ostrém” systému.

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 13. Atributové certifikáty – díl 2.

Jaroslav Pinkava, PVT a.s.

1. Úvod

V první části článku byly definovány klíčové pojmy – atributový certifikát, atributová autorita, oprávnění, rozlišen možný různý vztah k atributovým certifikátům (AC) – uživatel, ověřovatel, vydavatel, nositel, klient. Dokument rfc.3281 (lit.[1]) definuje profil atributových certifikátů při použití v rámci internetových protokolů. O požadavcích, které musí tento profil splňovat již bylo řečeno. Obrátíme se k popisu samotného profilu.

2. Profil atributového certifikátu.

Vzhledem k tomu, že atributové certifikáty lze využívat ve velmi široké škále aplikací a v různorodých systémech, klade si rfc.3281 za cíl popsat obecnou základnu využitelnou pokud možno s co nejširší působností. Konkrétně je těžiště cíleno na využitelnost v rámci internetové elektronické pošty, IPSec a webovských aplikací.

Dle normy X.509 (lit.[2]) vypadá definice AC následovně:

```
AttributeCertificate ::= SEQUENCE {
           acinfo AttributeCertificateInfo,
           signatureAlgorithm AlgorithmIdentifier,
           signatureValue BIT STRING
           }

     AttributeCertificateInfo ::= SEQUENCE {
           version AttCertVersion -- version is v2,
           holder Holder,
           issuer AttCertIssuer,
           signature AlgorithmIdentifier,
           serialNumber CertificateSerialNumber,
           attrCertValidityPeriod AttCertValidityPeriod,
           attributes SEQUENCE OF Attribute,
           issuerUniqueID UniqueIdentifier OPTIONAL,
           extensions Extensions OPTIONAL
           }

      AttCertVersion ::= INTEGER { v2(1) }
           Holder ::= SEQUENCE {
           baseCertificateID [0] IssuerSerial OPTIONAL,
                      -- the issuer and serial number of
                      -- the holder's Public Key Certificate


           entityName        [1] GeneralNames OPTIONAL,
                      -- the name of the claimant or role
           objectDigestInfo  [2] ObjectDigestInfo OPTIONAL
                      -- used to directly authenticate the holder,
                      -- for example, an executable
           }
```

```
ObjectDigestInfo ::= SEQUENCE {
      digestedObjectType ENUMERATED {
            publicKey (0),
            publicKeyCert (1),
            otherObjectTypes (2) },
                  -- otherObjectTypes MUST NOT
                  -- be used in this profile
      otherObjectTypeID OBJECT IDENTIFIER OPTIONAL,
      digestAlgorithm AlgorithmIdentifier,
      objectDigest BIT STRING
}

AttCertIssuer ::= CHOICE {
      v1Form GeneralNames, -- MUST NOT be used in this
                  -- profile
      v2Form [0] V2Form -- v2 only
}

V2Form ::= SEQUENCE {
      issuerName GeneralNames OPTIONAL,
      baseCertificateID [0] IssuerSerial OPTIONAL,
      objectDigestInfo [1] ObjectDigestInfo OPTIONAL
            -- issuerName MUST be present in this profile
            -- baseCertificateID and objectDigestInfo MUST NOT
            -- be present in this profile
}

IssuerSerial ::= SEQUENCE {
      issuer GeneralNames,
      serial CertificateSerialNumber,
      issuerUID UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
      notBeforeTime GeneralizedTime,
      notAfterTime GeneralizedTime
}


Attribute ::= SEQUENCE {
      type AttributeType,
      values SET OF AttributeValue
            -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

3. Poznámky k obsahu některých polí

1) Obsah pole GeneralName nabízí velkou volnost. Z důvodů interoperabilty jsou zde však zavedena některá omezení. Odpovídající implementace musí podporovat následující : dNSName,directoryName, uniformResourceIdentifier, a také iPAddress. Naopak nesmí být používány tyto volby: x400Address, ediPartyName, registeredID. Lze použít volbu otherName.

2) V poli pro číslo verze musí být hodnota v2 (není zpětně kompatibilní s verzí1 dle normy X.509 z roku 1997, je však kompatibilní s verzí v2 dle X.509 z roku 2000).

3) Pole Holder umožňuje následující tři volitelné syntaxe: baseCertificateID, entityName a objectDigestInfo. Je doporučováno používat aktuálně pouze jednu z těchto možností.

4) V poli issuerName musí být obsaženo jedno a pouze jen jedno GeneralName, a musí obsahovat neprázdné rozlišitelné jméno v poli directoryName. Vynechána musí být pole baseCertificateID a objectDigestInfo.

5) Pole Signature obsahuje identifikátor algoritmu, který je používán pro ověření podpisu na atributovém certifikátu.

6) dvojice issuer/serialNumber musí vytvářet jednoznačnou kombinaci (i pro krátkodobě platné AC). Vzhledem k tomu musí uživatelé AC být schopni zpracovávat hodnoty serialNumber delší než 4 oktety (nesmí být však delší než 20 oktetů).

7) Doba platnosti AC - attrCertValidityPeriod – obsahuje GeneralizedTime, které umožňuje různé reprezentace hodnot času. V rámci tohoto profilu musí hodnoty GeneralizedTime být vyjádřeny v UTC (Coordinated universal time).

8) Pole atributů udává informace vztažené k nositeli AC. V případě, že AC je používán pro autorizaci, obsahuje toto pole seznam oprávnění. AC musí obsahovat minimálně jeden atribut.

9) Identifikátor vydavatele - Issuer Unique Identifier – je využíváno pouze v případě (a právě jen v tomto případě), pokud je obsaženo také v příslušném poli certifikátu veřejného klíče vydavatele AC.

10) Toto pole (extensions field) podává informace o samotném AC. Příklady rozšíření:
- Audit Identity (obsah tohoto pole bude uváděn v sufitních záznamech, to je užitečné v těch případech, kdy není vhodné, aby se zde objevovalo jméno, které přímo identifikuje uživatel);
- targetInformation – pokud je zde obsažena příslušná informace, je AC využitelný pouze v rámci služeb zde specifikovaných serverů (ostatní servery musí AC zamítnout);
- authorityKeyIdentifier – lze použít jako pomoc pro ověřovatele AC při ověřování podpisu AC;
- authorityInformationAccess - lze použít jako pomoc pro ověřovatele AC při ověřování revokačního statutu AC.
-crlDistributionPoints – obdobně;
- noRevAvail – informuje ověřovatele, že k tomuto certifikátu nebude dostupná žádná informace o jeho odvolání;

4. Typy atributů.

Některé z typů atributů (viz dále) používají IetfAttrSyntax. Tento typ umožňuje rozlišit vydavatele a atributovou autoritu (užitečné v situacích, kdy v instituci je jedna AA, ale je zde více vydavatelů AC). Uvedeme následující příklady atributů:

1) authenticationInfo – identifikuje držitele AC ve vztahu k serveru (službě), může obsahovat i informace použitelné pro autentizaci uživatele. Pokud je zde obsažena citlivá informace (heslo), pak je atribut obvykle zašifrován;

2) accessIdentity – identifikuje držitele AC vůči serveru (službě). Obsahuje informace o držiteli AC, které lze pak využít ověřovatelem AC vzhledem k autorizacím akcí držitele AC;

3) chargingIdentity – identifikuje držitele AC pro účely stanovení zaúčtování (například firmě držitele);

4) group – tento atribut obsahuje informace o skupině, ke které patří držitel AC;

5) role – obsahuje informace o roli držitele AC (např. administrátor);

6) clearance – závisí na bezpečnostní politice;

5. Další poznámky

Rfc3281 dále stanoví podmínky na certifikát veřejného klíče vydavatele atributových certifikátů. Musí samozřejmě vyhovovat podmínkám rfc.3280 (profil certifikátu) a kromě toho rozšíření keyUsage v tomto certifikátu nesmí explicitně označovat, že veřejný klíč vydavatele AC nelze použít k ověřování digitálního podpisu. Vydavatelem AC nesmí být vydavatel certifikátů veřejných klíčů (tj. nesmí to být certifikační autorita).

V následující části bude rozebrán zbytek dokumentu [1].

6. Literatura

[1] rfc3281: An Internet Attribute Certificate Profile for Authorization

[2] ITU-T Recommendation X.509/ISO/IEC 9594-8: Information technology – open systems interconnection – the Directory: Public-Key and Attribute Certificate Frameworks, Version 4, 2000

[3] Pinkava, J.: Atributové certifikáty a PMI, Datakon 2002

[4] Attribute Certificate Policy Extension, draft-ietf-pkix-acpolicies-extn-03.txt

[5] LDAP Schema for X.509 Attribute Certificates, draft-ietf-pkix-ldap-ac-schema-00.txt

[6] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002

C. Kryptografické protokoly s nulovým předáním znalostí

Jaroslav Pinkava, PVT a.s.

Článek je věnován problematice protokolů s nulovým předáním znalostí. Tato technika má z hlediska praktických dopadů až nečekané vlastnosti.

V článku [3] byl popsán pojem autentizačního protokolu a objasněny některé základní vlastnosti tohoto pojmu. Speciálním případem identifikačních protokolů jsou **protokoly s nulovým předáním znalostí** (anglicky zero knowledge). Tyto protokoly v zásadě používají asymetrické techniky. Neopírají se však o užití digitálních podpisů ani o užití kryptografie s veřejným klíčem. Vyhýbají se rovněž užití blokových šifer resp. technik na bázi časových značek či na základě identifikace dle číselné posloupnosti.

Stejně jako u systémů s veřejným klíčem hraje základní roli utajovaná informace sloužící k autentizaci. Tato informace se však nepoužívá k šifrování dat, ale pouze k autentizaci (resp. k vytvoření digitálního podpisu). Schémata s nulovým předáním znalostí často probíhají v několika iteracích. V rámci každého iteračního cyklu proběhne výzva a odpověď na tuto výzvu. Toto je opakováno do té doby než je dosažena požadovaná úroveň důvěry ve druhou stranu.

Snad nejužitečnější vlastností technik s nulovým předáním znalostí je ta skutečnost, že eliminují potřebu periodicky obměňovat autentizační informaci. Je to díky tomu, že ověřující strana (či potenciální narušitel) nezíská žádnou užitečnou informaci, která by mu pomohla vystupovat později v roli první strany.

Předpokládejme, že P (dokazující strana) zná určitou informaci. Může to být například znalost prvočíselného rozkladu velkého čísla. Podstatný je zde fakt, že informace, kterou P zná, je *ověřitelná*, tj. existuje efektivní procedura pro ověření její platnosti. Při matematickém dokazování to znamená, že máme určitý formální důkaz, a každý krok důkazu lze ověřit. P chce přesvědčit V (ověřující stranu), že bez jakékoliv pochybnosti je majitelem oné informace.

P může jednoduše informaci rozkrýt tak, že V si informaci ověří sám. Jestliže informace spočívá v tom, že jsou známa dvě prvočísla p a q rozkládající velké číslo n, potom P může přímo straně V sdělit čísla p a q a V si ověří, že n = pq. To je důkaz založený na tzv. **maximálním rozkrytí** (maximum disclosure proof), zde strana V získává celou informaci a může později ukázat někomu jinému, že tuto informaci zná.

Naopak při **důkazu s minimálním rozkrytím** (minimum disclosure proof), strana P dokáže straně V, že zná onu informaci, ale způsobem, který neprozradí ani bit této informace a ve svém důsledku tedy ani nepomůže straně V určit resp. získat tuto informaci. V si je skoro jistý (neboť pravděpodobnost, že P podvádí může být učiněna libovolně malou), že P zná onu informaci, např. že strana P zná faktorizaci čísla n na dvě prvočísla. Ale strana V sama nic nezjistí o samotných faktorech a nemůže o tom nic sdělit třetí straně. Pokud verifikující strana V při průběhu protokolu nezíská dokonce vůbec žádnou informaci, hovoříme o důkazech s nulovým předáním znalostí.

Jedním ze základních problémů u většiny identifikačních technik, jako jsou ID karty, kreditní karty a hesla v počítačích je, že strana P prokazuje svoji identitu prozrazením hesla H,

které je uloženo či vytištěno na kartě. Kdokoliv, kdo spolupracuje s nečestným ověřovatelem, může získat kopii karty či jinak se seznámit s heslem H a později se za P vydávat, tedy i požadovat služby, které je oprávněn požadovat pouze P.

Řešením tohoto problému je využití protokolu s nulovým předáním znalostí. Ověřovatel V bude přesvědčen, že P zná H bez toho, aniž by byl prozrazen jediný bit hesla H.

Příkladem protokolu s nulovým předáním znalostí je **Feige-Fiat-Shamirův protokol**. V rámci tohoto protokolu prokazující strana P dokáže ověřovací straně V znalost určitého tajemství (a tak prokáže svoji totožnost). Protokol probíhá v t cyklech, v průběhu každého cyklu jsou přenášeny tři zprávy. Tajemství strany P spočívá ve znalosti soukromého klíče s. Právě tato znalost umožňuje straně P vytváření zasílaných zpráv protokolu. Zprávy jsou vytvářeny tak, že bezpečnost celého protokolu se opírá o složitost řešení úlohy faktorizace velkého čísla n.

Dalším známým příkladem protokolů s nulovým předáním znalostí je např. **protokol Guillou-Quisquatera**. Tento protokol umožňuje redukci počtu vyměněných zpráv. Známý je rovněž **Schnorrův protokol** založený na obtížnosti úlohy diskrétního logaritmu (místo na obtížnosti úlohy faktorizace). Tento protokol sestává pouze ze tří vyměněných zpráv. Každý z těchto tří zmíněných protokolů má určité výhody a nevýhody z hlediska rozsahu potřebných výpočtů, počtu vyměněných zpráv resp. dosaženého stupně bezpečnosti.

Pokud se týká vlastních implementací těchto protokolů, je nutno říci, že v praxi se s technikou nulových znalostí zatím setkáváme poměrně zřídka. Jednou ze známějších aplikací je projekt SCALPS (http://www.dice.ucl.ac.be/crypto/techreports.html). Možným využitím nulových znalostí se zabývá také projekt UNTPDC Smart Card (http://www.kita.or.kr/untpdc/eto/associates/gift/smartcard.html).

Využití aparátu nulových znalostí leží v zásadě především v oblasti identifikace. Naproti tomu, pokud je na čipové kartě implementován např. kryptografický systém s veřejným klíčem, pak takováto karta má širší možnosti praktického využití. To se týká i provádění určitých transakcí, převodu peněz atd. Výhodou technik nulových znalostí je jejich malá náročnost z hlediska potřebného programového vybavení.

Literatura

[1] Salomaa, Arto: Public-Key Cryptography, Springer-Verlag 1990
[2] Menezes, A.J. aj. : Handbook of Applied Cryptography, CRC Press 1997
[3] Pinkava, J. : Identifikace a autentizace, část II, DSM 3/98

D. Elektronické peníze

Mgr. Pavel Vondruška, ČESKÝ TELECOM a.s.

Úvod

Tento článek obsahuje materiál, který byl vytvořen jako podklad k mé přednášce na KSI (Katedra systémového inženýrství, seminář informační bezpečnosti) MFF UK Praha, 18.4.2000. Jedná se o autentický text, který jsem od té doby nijak neupravil.

Je potřeba si uvědomit, že popisovaná oblast prochází obrovským dynamickým vývojem a údaje zde obsažené platily v době, kdy jsem si materiál připravoval – tedy konec roku 1999. K tomuto datu se také váží použité materiály. Je to tedy článek již spíše „historický“, ale věřím, že jeho zveřejnění má význam, protože obecné zásady zde uvedené jsou stále platné.

I. Elektronické platební karty (eCash, Mondex)

Kreditní karty a čipové karty s elektronickými penězi jsou navenek podobné, ale oba platební systémy jsou zcela odlišné. Kreditní karty nemají uloženu žádnou hodnotu (na rozdíl od karet s elektronickými penězi), identifikují plátce (což dělají jen některé typy karet s elektronickými penězi), umožňují zjistit ON-line solventnost nebo schopnost platby, karty s elektronickými penězi jsou samozřejmě právě naopak založeny na OFF-line systému. Kreditní karty jsou prozatím stále spíše karty s magnetickým proužkem. Kvůli bezpečnosti i zde dochází k přechodu na karty čipové. Do roku 2002 se předpokládá úplný přechod na karty čipové.

Z karet s elektronickými penězi se dá dále vydělit tzv. elektronická peněženka. Jedná se o čipovou kartu s elektronickými penězi, kde při platbě je zaručena anonymita kupujícího. Obecně pak pro platební karty s elektronickými penězi platí, že je lze dobíjet z účtu majitele. Někdy se označují tyto karty jako platební "smart" karty ("chytrý", "bystrý", pohotový") a lze na ně pohlížet jako na elektronické peníze . Dále je budeme značit EPK - elektronická platební karta.

EPK je tedy čipová platební karta vydaná bankou k účtu klienta jako nosič jeho peněz v elektronické podobě. Platba probíhá off-line bez nutnosti autorizovat kartu ve vzdáleném autorizačním centru.

Kupříkladu i společnost VISA card - jako hlavní představitel "světa" kreditních karet - se živě zajímá o elektronické platební karty. Známým se stal jejich pilotní projekt VISACash. Na LOH v Atlantě (1996) byly tyto karty rozdávány účastníkům (maximální částka, která šla uložit byla, 100 USD). Karta byla přijata velice kladně. Již za rok projekt podpořilo 60 bank

ze 13-ti států a bylo vydáno 3.7 milionu elektronických peněženek VISACash, které akceptuje cca 14 000 terminálů. Viceprezident firmy VISA pan Ivan Remsik se ovšem domnívá, že EPK není vhodným platebním nástrojem pro střední a východní Evropu. Důvodem je dostupnost služeb a hlavně možné ztráty z padělání, krádeží apod..

Ve světě existují i jiné známé projekty elektronických platebních karet : především je to MONDEX (Hitachi), DANMONT (opět z produkce VISA), CLIP (společnost Europay), PROTON (American Express), CAFE (projekt podporovaný Evropskou komisí), Cybercoin (pouze pro internetové transakce). V České republice existuje projekt EPK České spořitelny (pilotní projekt již 1994 , Zlín) . Obchodní název této první EPK se nazývá - ne zcela přesně - Elektronická peněženka MONET. Protokol používaný v této EPK si probereme ve druhé části podrobněji.

Nejdříve obecně několik slov k bezpečnosti EPK.

V současné době se za nejbezpečnější považuje protokol společnosti Digicash (technologie EPK eCash). Systém navrhl holandský kryptolog David Chaum. David Chaum je vynálezce slepých digitálních podpisů, které právě v protokolu eCash hrají zásadní úlohu. Protokol je v současné době vysoce hodnocen. Vzhledem k anonymitě kupujícího se tedy jedná o skutečnou elektronickou peněženku. Zaváděn je téměř po celém světě. Připomenu zde např. tyto implemantace : USA - Mark Twain Bank, říjen 1995, Finsko - banka Merita + EUnet, březen 1996, Německo - Deutsche Bank, květen 1996, Asijsko-pacifický region - Advance Bank, říjen 1996. Detaily protokolu zde minulou přednášku předvedl Mgr. Antonín Beneš, a proto tento systém, který vítězně dobývá jednu oblast za druhou opustíme a podíváme se na další systémy.

Systém MONDEX . Zásadní a významnou odlišností systému MONDEX od všech ostatních systémů je, že dokáže elektronickou hotovost předávat z jedné čipové karty do druhé. Stručně řečeno reklamním sloganem firmy MONDEX - "MONDEX jsou skutečné peníze". Tato vlastnost je však z hlediska bezpečnosti velice riskantní, a proto nebyla z počátku k systému veliká důvěra. Mondex vymysleli v roce 1990 Angličané Tim Jones a Graham Higgins s použitím digitálních podpisů, což byla na tu dobu dost odvážná kryptologická aplikace. V roce 1995 byl zahájen v Anglii první pilotní projekt, který přinesl neuvěřitelně pozitivní reakce veřejnosti. Zákazník obdrží komplet Mondex, který se skládá z karty vydané k bankovnímu účtu držitele, dále kartu (rodinou kartu), která se vztahuje k témuž účtu (lze dobíjet z hlavní karty např. pro děti) a čtecího zařízení, které slouží ke čtení informací o zůstatku na kartě. Načtení peněz do karty lze provádět nejen z bankomatů k tomu určených, ale (a to byla v době zavedení supernovinka) pomocí speciálně upravených veřejných telefonních automatů (v Anglii British Telecom). Po vytočení zvláštního čísla, zadání PIN a částky došlo ke spojení s bankovním účtem a po ověření se částka přesunula do čipu. Prostřednictvím těchto telefonů se dají uskutečnit i přesuny do jiné čipové karty (otec např. může dobít synovi rodinou kartu). Při platbě u obchodníka se PIN nezadává, ale terminál si uchovává informace o platbách, včetně identifikace plátce - nejedná se tedy o pravou elektronickou peněženku. Ztráta anonymity kupujícího , ale zvyšuje podstatně bezpečnost systému. Projekt byl tak úspěšný, že v červenci 1996 vznikla společnost Mondex International Ltd. , kterou založilo 17 velkých mezinárodních bank. Brzy nato společnost MasterCard ohlásila zájem o nákup 51 % podílu společnosti MONDEX a mohlo začít vítězné tažení. MasterCard plánuje, že v čipové kartě by se mohly v budoucnu spojit všechny tři hlavní aplikace - karta kreditní, karta s uloženou hodnotou a elektronická peněženka. Vážný zájem o tento systém má celý asijský región (včetně Číny).

Bezpečnost a technická data. Výrobce (fitma HITACHI) tvrdí : "…systém poskytuje úroveň bezpečnosti, která předbíhá současnou úroveň zločinců a bude ji předbíhat i zítra." Karty Mondex jsou vybaveny čipem Hitachi H8/310 s pamětí EEPROM (8Kb) a mikroprocesorem a vyrobila je firma Dai Nippon. Vzhledem k důslednému utajování jak vlastností čipů, tak i samotných kryptografických protokolů, se o tomto systému moc neví ("Security through obscurity"). Při platbách a dobíjení spolu přímo tyto čipy komunikují a je tedy utajován i komunikační protokol. Původní systém byl údajně založen na symetrické kryptografii, čipy neměly dostatečný výkon pro asymetrickou kryptografii, přitom se ovšem mluvilo o digitálních podpisech. Tvůrci tvrdí, že účastnické banky mohou sledovat finanční toky elektronických peněz, a tak zjistit podvodné transakce. Bezpečnost je založena na speciální úpravě čipu, která brání zpětnému inženýrství. Údajně je zakomponována možnost přechodu karet na jiné kryptografické funkce za chodu systému bez nutnosti výměny všech karet. Velice zajímavá je realizace automatické kaskádovité propagace tzv. hotlistů (blackboard listů) ukradených karet. Držitel karty si ji sám může také zablokovat proti výdeji peněz jednoduchým vestavěným tlačítkem (peníze přijímat lze i po této blokaci), odblokovat kartu lze po vložení PIN. V květnu 1996 si nechala Národní banka Nového Zélandu (NBNZ) otestovat bezpečnost systému MONDEX nezávislou organizací. Výsledkem bylo memorandum, které konstatovalo, že bezpečnost prověřované verze systému je nedostatečná a systém není odolný proti útoku . Auditor to údajně demonstroval mimo jiné pomocí útoku, při kterém se mikrojehlami spojí 2 plošky na čipu a tím se čip dostane do testovacího režimu, ve kterém lze měnit některá data. Výsledek auditu byl před veřejností více než rok utajován. V roce 1997 došlo k úniku informací z NBNZ a výsledek auditu byl zveřejněn na Internetu organizací EFF (Electronic Frontier Foundation). NBNZ žádala EFF o okamžité stažení trestu, při neuposlechnutí hrozila soudní dohrou. Výrobce čipu (Hitachi) prohlásil, že se jednalo o starou verzi, která již není podporována a proto neměl být čip použit … Společnost MONDEX prohlásila, že bezpečnost systému je "odpovídající způsobu použití" . Způsob použití je jinými slovy maximální částka, uložená v EPK, ale tato částka není nikde definována.

II. Elektronické platební karty v ČR (MONET+)

První česká bankovní elektronická peněženka (přesněji podle naší definice elektronická platební karta) se objevila již v době prvních pilotních projektů ve světě a to v roce 1994. U jejího zrodu stála Česká spořitelna, později se do projektu přiřadila Union Banka (podle dostupných informací se již na projektu opět nepodílí). EPK byla vydána pod obchodním názvem START, byla vyvinuta akciovou společností Derby a její dceřinou společností MONET+ (www.monetplus.cz). Karta je v současné době realizována kartou MPCOS-EMV francouzské firmy GEMPLUS (doplněná o vlastní firemní kód tzv. CFD filtr). Podle informací na webu firmy MONET+ její nasazení na Zlínsku a okolí je stále živé a je zde stále používána. Poslední na webu dostupné statistické údaje jsou k roku 1998 (květen) :

3.500 vydaných karet
150 obchodních míst přijímající karty MONET
17 parkovacích automatů
8 nabíjecích terminálů (tankomatů) - z toho 3x v pobočkách České spořitelny, 5x na veřejných místech mimo pobočky ČS

Název EPK se několikráte měnil. Název "Start" nahradil název karty "Elektronická peněženka MONET" (1996), Karta BEP (Bankovní elektronická peněženka), "Bankovní elektronická peněženka MONET". V současné době se tato karta vydává všem osobám disponujícím sporožirovým účtem u České spořitelny. Na příslušné www stránce firmy MONET jsou uvedeny základní teze, proč kartou platit a proč je pro obchodníky výhodné si pořídit přijímací aparát POS (Point of Sale). Držitel nemusí počítat drobné, platba je rychlejší, kartu na rozdíl od peněz může držitel i ztratit , lze si vytisknout přehled o platebních transakcích a tím mít přehled o svých útratách, kartu si může držitel kdykoliv dobít - místa dobíjení jsou přístupná 24 hodin. Pro obchodníka znamená akceptování těchto plateb snížení rizika (méně hotovosti v pokladně, nemůže mít v tržbě falešnou bankovku, jednodušší manipulace s penězi a při odvodu tržby), přilákání zákazníků, vyšší tržba (zákazník z karty zaplatí "lehčeji" než hotovostí, tzv. efekt "Card Lift"), záruka úhrady platby (peníze na BEP jsou vždy kryty bankou). Maximální výše peněz uložených v kartě je v současné době omezena na 20 000,- Kč.

Některé technické parametry v současné době používané platební karty
MPCOS-EMV
Multiaplikační OS
Dle ISO7816 -1,-2,-3,-4 EMV
Protokoly T=0,1,14
Paměť EEPROM **8**, 16, 32, 64 kbit
Rychlost komunikace 9,6 - 115,2 kbd
Generování náhodných čísel
Kryptografie DES, 3DES
CFD filtr
Autentizace, secure messaging
Těleso ABS, PVC

CFD filtr umožňuje hlídat tzv. kumulativní limit (tím se např. liší od EP CLIP od společnosti EUROPAY). To je částka, kterou si klient sám volí a která mu dovolí postupně utratit peníze do této výše bez zadání PIN (po zadání PIN se tato částka samozřejmě opět nastaví). Karta má i druhý PIN, který je určen pro nabíjení (ON-line) na tankomatech. V kartě jsou také uloženy informace jako např. sériové číslo, logické číslo, zůstatek, označení banky klienta, číslo pobočky, která kartu vydala, doba platnosti, data držitele, 20 posledních transakcí karty. Pro úplnost dodejme, že systém ještě obsahuje zařízení obchodníků POS (s obsáhlými vnitřními daty) a transportní karty obchodníků. Zařízení a karty umožňují šifrování 3DES a výpočet zabezpečovacího kódu MAC pomocí algoritmu 3DES, změnu PIN a další funkce.

Podívejme se na provozovaný systém této EPK z hlediska kryptologie. Především se zde používá tzv. elektronický certifikát. Elektronický certifikát je potvrzení dat pomocí MAC - Message Authentication Code. MAC je generován pomocí určitého algoritmu, který závisí na zprávě a nějakém klíči (tajném klíči) , délka má pevnou velikost díky následnému použití nějaké hashovací funkce. Systém dále používá zašifrování dat tajným klíčem (společně sdíleným účastníky systému).

V kartě jsou uloženy šifrovací klíče KM (MasterKey, uložen jen jeho derivát) a KI (Identification Key, klíč držitele karty). V POS (přesněji zde použitých SAM modulech) jsou uloženy klíče KM a KR (klíč obchodníka). KM zná pouze operátor systému. KI zná jen banka vydávající kartu, KR zná jen banka obchodníka (obecně to nemusí být banka držitele karty).

Situace 1 / Dobíjení:
Dobíjení karty (zde nazývané tankování). Probíhá při ON-line spojení mezi kartou a bankou držitele karty. OS karty zvýší o požadovanou částku vestavěný čítač pouze tehdy, pokud dostane pokyn od banky, že je to možné.
Autentizace pomocí zadání PIN.
Výzva k nabití o požadovanou částku a potvrzení této transakce probíhá šifrovaně pomocí 3DES s klíčem KI (klíčem držitele karty). Připomeňme, že klíč je uložen v kartě a banka jej zná.

Situace 2 / Platba:

- Autentizace mezi čipovou kartou a platebním automatem proběhne za použití sdíleného klíče KM. Pokud autentizace proběhne, jsou POS podstoupena otevřená data karty.
- Platba se provádí pomocí certifikátu s klíčem KI . CK (certifikát karty) = 3DES(KI, data karty, částka) .
- POS připojí svá data certifikována svým klíčem KR. CP (certifikát platebního terminálu) = MAC(KR, data karty, data POS, částka)
- Sníží se částka čítače karty a zvýší se částka čítače POS

Situace 3/ Dokladování operací
- Oba certifikáty jsou odeslány operátorovi systému (buď modemem nebo pomocí transportní karty)
- Ten rozdělí data na dvě části a odešle jednu bance držitele karty a druhou část bance majitele POS
- Obě banky mohou svými klíči zkontrolovat certifikáty a dokladovat příslušné operace

Nedostatek dalších informací (opět klasická situace "Security through obscurity"), typická pro platební systémy z čipovými kartami, mi nedovoluje specifikovat detailněji průběh jednotlivých operací.

III. Ochrana kreditních karet na Internetu

V současnosti jsou nejrozšířenějším způsobem placení na Internetu kreditní karty. Kupříkladu VISA karta jako jeden z nejznámějších představitelů světa kreditních karet, sdružuje více jak 20 000 členských bank, vydala již na 600 milionů platebních karet a platby jsou přijímány na přibližně 14-ti miliónech platebních místech. Tato společnost souhlasila s tím, že platby lze provádět pomocí Internetu (podobně samozřejmě i jiné velké kreditní společnosti jako např. MasterCard , AmericanCard, SecureCard apod). Jedná se tedy o obrovský platební potenciál, který lze na Internetu využít. Používání a zneužívání kreditních karet při placení na Internetu byla věnována velká pozornost a dá se říci, že veřejnost je o rizicích poměrně dobře informována. Platby se však provádí stále. Často stačí jen vyvolat pomocí svého browseru nějakou www stránku, vyplnit objednávku a odeslat ji klepnutím myši. Za nějakou dobu obdržíme dodané zboží (nebo jsme ihned vpuštěny např. do placené www oblasti příslušné stránky). Na našem účtu si můžeme zkontrolovat položku o platbě. Tento způsob platby se ujal, protože fungoval již dávno před Internetem. Číslo kreditní karty se prostě vpisovalo na objednávku nebo diktovalo do telefonu. I když určitá část transakcí

byly transakce podvodné, vcelku byla a je k této formě značná důvěra. Vlastníci karet totiž neměli v úmyslu dělat podvody. Objednávky byly většinou na hmotné zboží, které bylo doručeno na jejich adresu a oni podepsali jejich převzetí. Pokus o podvod na bance (nepřiznání dodávky) se trestal odnětím karty a to v USA byla pro dotyčného opravdová pohroma. Ze stejných důvodů se ani obchodník o pokus podvádět nepokoušel. Jediné trestné činy byly tvořeny kradenými kartami v době, kdy ještě jejich majitel jejich ztrátu nenahlásil. S internetem je to jiné. Platby za vstupy do informačních systémů, prohlížení sexy stránek apod. jsou platby za zboží nehmotné povahy a důkaz zda uživatel tuto službu použil nebo ne, je buď složitý , nebo nákladný a firmám se kontrola nevyplatí, a tak buď obchodník prostě sníží svůj zisk nebo banka zaplatí ztrátu (podle toho o jaký druh podvodu se jedná). Na Internetu se objevily celé seznamy lidí a jejich kreditních karet, které byly získány ze špatně zabezpečených serverů. Jeden z největších úniků byl např. roku 1997, kdy Carlos Felipe Sagado (přezdívka "Smak") získal z počítače v San Diegu 100 000 čísel kreditních karet. Teoreticky lze, ale získat tyto senzitivní informace na Internetu jednodušeji. Po Internetu totiž "běhají" tyto informace často nedostatečně zabezpečené a pomocí již jednoduchých programů se k nim lze dostat.

Nedůvěru v elektronický obchod na Internetu a narůstající ztráty si uvědomily dvě vedoucí společnosti v této oblasti - Visa a MaterCard a společně navrhly protokol SET . Pro vývoj protokolu SET a implementaci softwaru potřebného k zajištění bezpečnosti prostředí, ve kterém se budou na Internetu kreditní karty používat, byla vybrána společnost RSA corporation. Úkolem protokolu SET je zajistit pomocí šifrovacích technik bezpečnost on-line transakcí. Protokol SET zde představil na své přednášce RNDr. Jiří Souček, DrSc., a proto jej vynecháme. Konstatuji jen, že pro jeho implementační složitost se zatím příliš nerozšířil.

Protokol SET, ale není jediné řešení bezpečnosti kreditních karet na Internetu.

Zajímavé řešení (pro svoji jednoduchost) vytvořila např. firma "First Virtual". Ve svém řešení se dokonce obejde bez šifrovacích technik. Zákazník, který chce na Internetu používat svojí kreditní kartu, se nejprve zaregistruje u organizace "First Virtual". Zde je mu udělen vlastní účet a zákazník dostane identifikační číslo tohoto účtu (klasickou poštou). Majitel karty potom zašle své identifikační údaje (poštou, faxem, telefonicky), které se jednoznačně přiřadí k tomuto identifikačnímu číslu. Nakupovat lze u obchodníků, kteří souhlasí s procesem nákupu a prodeje přes First Virtual (FV). Samotný proces pak vypadá následovně.

1) Nakupující si vybere zboží a sdělí obchodníkovi identifikační číslo účtu u FV
2) Obchodník předá informace o objednávce + identifikační číslo účtu serveru u FV
3) Server FV vygeneruje o transakci zprávu, kterou pošle zákazníkovi (zná jeho totožnost a adresu)
4) Zákazník buď transakci potvrdí (volba ANO) nebo odmítne (rozmyslel si nákup !, volba NE) nebo ohlásí pokus o podvod (volba = zpronevěra)
5) FV v případě ANO informuje o potvrzení transakce obchodníka
6) FV předloží požadavek k odčerpání částky z kreditní karty zákazníka kartovému centru banky zákazníka
7) Banka provede požadovanou platbu (strhnutí částky z částky zákazníka) a převede peníze na účet FV
8) Na účtu FV leží peníze po dobu 90-ti dnů (z důvodu bezpečnosti a také z důvodu zisku FV)
9) Není-li obchod zpochybněn jsou peníze převedeny na účet obchodníka

Jiné používané řešení je z dílny známé firmy CyberCash. Zde se využívá speciálního softwaru a z kryptologického hlediska především asymetrická kryptologie. Velice zjednodušeně celý proces vypadá takto:

1) Zákazník si nainstaluje program CyberCash (umožňuje šifrování, uchovává informace o povedených transakcích)
2) Zákazník uloží své číslo kreditní karty (lze uložit více čísel kreditních karet) a vygeneruje soukromý a veřejný klíč (pro identifikaci kreditní karty)
3) Zákazník zašle svůj veřejný klíč firmě CyberCash
4) Zákazník při nákupu otevřeně zašle svůj požadavek obchodníkovi (který je také již zaregistrován obdobným způsobem jako zákazník u firmy CyberCash a musí vlastnit program CyberCash)
5) Obchodník údaje z otevřeného textu (objednávky) zákazníka vrátí programu CyberCash zákazníka s tím, že přidá informaci, které karty akceptuje (VISA, MasterCard, atd.)
6) Zákazník doplní tuto zprávu o číslo své kreditní karty příslušného typu, zprávu digitálně podepíše a dále zašifruje pomocí veřejného klíče firmy CyberCash a odešle obchodníkovi
7) Obchodník připraví vlastní verzi o transakci, také on ji podepíše svým klíčem a zašifruje veřejným klíčem firmy CyberCash.
8) Obchodník odešle svoji verzi a verzi zákazníka firmě CyberCash
9) Server CyberCash došlou zprávu kompletně dešifruje a porovná verzi obchodníka a verzi zákazníka
10) Pokud se obě verze shodují, předloží kartovému centru zákazníka požadavek o provedení platby
11) Firma CyberCash pošle potvrzení o provedené platbě obchodníkovi
12) Obchodník pošle programu zákazníka informaci o provedené transakci. Program tuto transakci uchovává.

Uvedená řešení nejsou jedinou možnou a používanou variantou bezpečných plateb na Internetu. Patří však mezi nejvíce rozšířená řešení. Mezi obchodníky však nejsou tato řešení příliš v oblibě. Někteří odborníci se domnívají, že vhodnějším řešením bude přece jen ústup od přímých plateb pomocí kreditních karet (příliš velká složitost) a pro platby na Internetu používat softwarové elektronické peněženky (očekává se, že zde bude řada plateb v malých "centových" částkách a systém kreditních plateb není v tomto případě zcela optimální).

Obecný postup tedy bude nejspíš tento :

I. Protokol A

Uživatel si nainstaluje software na svém PC a protokolem A si naplní svůj "zásobník" penězi. Vznikne elektronická peněženka.

II. Protokol B

Platby na Internetu (několik úrovní dle požadavku zákazníka a obchodníka)

- anonymní platba zaručená
- anonymní platba s malou částkou (tzv. nulová platba) (určeno pro platby, kde se nevyplatí složitý protokol, který blokuje připojení a vyžaduje reakce obchodníka)
- zaručená platba s identifikací uživatele

Výše uvedenou cestou se např. vydala firma CyberCash z Restonu (USA, Virginia) a vyvinula systém Cybercoin. Jedná se vlastně o softwarovou peněženku, která je určena pro "malé" platby na Internetu.

Odborníci tvrdí, že oblíbenost kreditních karet a jejich rozšíření neumožní jejich jednoduchou náhradu pro platbu na Internetu, ale řešení, kdy si uživatel "nabíjí" svůj počítač pomocí své kreditní karty a pak platí z této elektronické peněženky (viz předložené obecné schéma), je pro majitele kreditní karty přijatelné, již proto, že "běžný uživatel" si ani neuvědomí, že platbu vlastně neprovádí svojí "kreditkou". Navíc multifunkce kreditní karty a její přeměna v elektronickou peněženku a elektronickou platební kartu je také středem zájmu vývojářů hlavních kreditních společností. Všechny druhy plateb (včetně platby na Internetu) by pak bylo možné provádět touto jedinou multifunkční kartou.

Použité materiály:

1) V.Klíma : Nakopírujte si milion, CHIP, 1/1997

2) V.Klíma: S kartami do Evropy, CHIP, 6/1997

3) I.Novotný : Bill´s bill, CHIP, 3/1997

4) V.Klíma: Peníze v čipu, CHIP, 3/1997

5) P.Hanáček : Bezpečnost čipových karet, ComputerWorld, 32/1998

6) V.Klíma : První česká elektronická peněženka, 7/1997

7) V.Matos,S.Misra,L.Garceau: Elektronické peníze III, DSM 4/1999

8) http://www.monetplus.cz

9) http://www.digicash.com/news/archive/cardcom.html

10) http://a.dn.cybercash.com/cybercash/merchants/crnss/htmladmin/coin.html

11) http://www.firstvirtual.com/

12) Hacker Sold Credit Card Numbers : http://www.infowar.com/hacker/hackzj.html

13) http://www.rsa.com/

14) http://www.visa.com/

E. Letem šifrovým světem

Přečtěte si :

V archívu IACR další příspěvek z Čech

V archívu IACR (International Association for Cryptographic Resarch) byl uložen další příspěvek českých kryptologů. Příspěvek byl přednesen na konferenci NATO, která se konala letos v dubnu v Brně. Je to nejen ocenění kvality tohoto příspěvku, ale i dobrá zpráva pro české zájemce o kryptologii - za kvalitními příspěvky (prvé kategorie) nemusí jezdit na mezinárodní konference do ciziny, ale mohou je slyšet i na setkání českých kryptologů zde v Čechách.

Vlastimil Klíma and Tomáš Rosa: Side Channel Attacks on CBC Encrypted Messages in the PKCS#7 Format, Security and Protection of Information 2003, 2nd International Scientific Conference, NATO PfP/PWP – CATE, Brno, Czech Republic, 28.4.-30.4.2003
http://eprint.iacr.org/2003/098/

Odchod odborníků z ICZ a.s.

Významní čeští kryptologové a bezpečnostní odborníci RNDr. Vlastimil Klíma a Ing. Tomáš Rosa odcházejí (po vzájemné dohodě se svým zaměstnavatelem) k 30.6.2003 ze společnosti ICZ a.s. (http://www.i.cz). Dosáhli zde během svého působení řady mezinárodně uznávaných a ceněných výsledků. Některé z čerstvých novinek budou oba pánové prezentovat ve zvaném příspěvku na mezinárodní kryptologické konferenci TATRACRYPT (http://www.elf.stuba.sk/Katedry/KM/TATRACRYPT/index.htm) v Bratislavě ve dnech 26.-28.6.2003 a na prestižní vědecké konferenci CHES (Cryptographic Hardware and Embedded System, http://www.chesworkshop.org) v Kolíně nad Rýnem ve dnech 7.-10.9.2003.

Ze společnosti ICZ a.s. k výše uvedenému datu odcházejí i další pracovníci např. i přední specialista na informační bezpečnost ing. Jiří Hejl.

Slovensko zažilo největší únik osobních informací ve svých dějinách

Začátkem června jste se mohli v různých médiích (včetně krátkého sdělení v české televizi) dozvědět, že hackeři zaútočili na síť Slovenských telekomunikací. V tomto informačním systému se delší čas pohybovali a získali tak informace o klientech. Mezi klienty Slovenských telekomunikací patří vládní instituce, velké banky a pojišťovny. Hackeři rovněž získali databázi všech majitelů pevných linek na Slovensku a zveřejnili ji na svých internetových stránkách. O průniku informovali samotní hackeři ve svém e-zinu prielom #20, 06.06.03.

Více viz ezin binarnych sxizofrenikov, prielom(at)hysteria.sk, http://hysteria.sk/prielom/

Policie je proti hackerům bezmocná

Pod tímto názvem byl na Lupě zveřejněn 11.6.2003 zajímavý článek, který popisuje boj české policie proti hackerům. Článek Ondřeje Tolara je velice čtivě napsán a obsahuje mnoho zajímavých údajů k zamyšlení.

Článek naleznete v rubrice Internet, nebo http://www.lupa.cz/clanek.php3?show=2873

RFC 3537

Koncem května 2003 bylo publikováno devítistránkové RFC 3537 (Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES) Key). Obsah dokumentu je zřejmý již ze samotného názvu – definovány jsou dvě metody pro vytváření HMAC. Prvá metoda je založena na kryptografickém standardu TripleDES a druhá na novém symetrickém šifrovém standardu AES. Využití popsaných algoritmů se předpokládá především pro autentizaci dat - CMS (Cryptographic Message Syntax). RFC je zařazeno do "Internet Official Protocol Standards" (STD 1). Autory jsou J. Schaad, R. Housley. (ftp://ftp.rfc-editor.org/in-notes/rfc3537.txt)

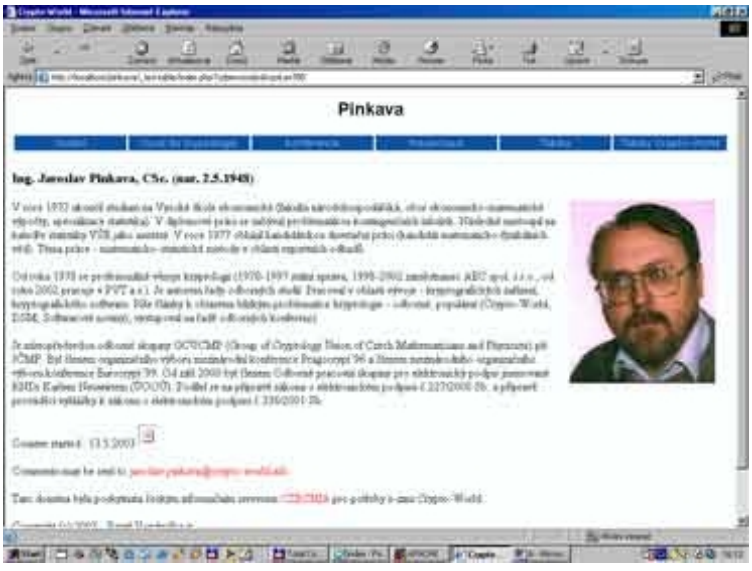
Kvantové počítače – informace z fronty:

Čtenáře Crypto-Worldu bude jistě zajímat následující odkaz: http://news.bbc.co.uk/2/hi/science/nature/3043731.stm .

Hovoří se v něm o zajímavém pokroku ve výzkumu vlastností tzv. svázaných (entangled) částic. Konstrukce modelů se svázanými částicemi má zásadní význam při budování kvantových počítačů. Vědcům (University of Maryland – USA, pan Andrew Berkley se spolupracovníky) se podařilo poprvé "svázat" dvě částice (na subatomární úrovni), kdy tyto částice jsou od sebe vzdáleny na obrovskou vzdálenost – 1 milimetr (samozřejmě velikou z hlediska pohledu na samotné částice). Pokud jsou nějaké dvě částice takto svázány, pak se chovají jedna závisle na druhé. Vzdálenost zde potom nehraje žádnou roli. Milimetrová škála je obrovská z hlediska částic, ale naopak je již přijatelná pro vytváření mechanických modelů kvantových počítačů. (připravil J.Pinkava)

Domácí stránka e-zinu Crypto-World doplněna o práce J.Pinkavy

Ing. Jaroslav Pinkava umožní zájemcům na domácí stránce Crypto-Worldu seznámit se s jeho staršími články, prezentacemi a příspěvky na domácích i zahraničních konferencích.



První část předaných dokumentů je na této stránce dostupná od neděle 15.6.2003..

Stránka bude v průběhu června a července průběžně aktu-alizována. Vstup na stránku je přes ikonu „Pinkava“ na http://crypto-world.info/ nebo ji lze volat přímo : http://crypto-world.info/pinkava/ .

(Osobní stránku vytvořil nově „jmenovaný“ webmaster e-zinu Crypto-World můj syn - Pavel Vondruška jr., 16 let).

O čem jsme psali v dubnu 2000 - 2002

Crypto-World 6/2000

Příloha :
Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 6/2001

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

Crypto-World 6/2002

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 (zkonvertovány do PDF formátu), 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 !). 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@post.cz
pavel.vondruska@ct.cz