Konferenci Security 2002 organizují

AEC

DATA SECURITY COMPANY

spolu s mediálním partnerem

VOGEL PUBLISHING s. r. o.

a partnery

F-SECURE

hp invent

SECURITY 2002

Praha 6. června

Pozn.: Tato publikace neprošla redakční ani jazykovou úpravou.

Obsah

REALITA ELEKTRONICKÉHO PODPISU

Jiří Mrnuštík, AEC spol. s. r. o.

Foreword

Zákon 227/2000 Sb. byl přijat, a veřejností, politiky i odbornou representací akceptován. Vyhláška 366/2001 Sb. je v praxi již nějakou dobu. Nařízení vlády pro použití elektronického podpisu při přijímání elektronických podání na úřadech je téměř již tak staré, že se chystá jeho novelizace. Jaké jsou však reálné výsledky praktické implementace elektronického podpisu? Docela dobré, ale…..ne až tak v České republice.

Úvod

Technologie elektronického podpisu je velmi užitečná a použitelná v mnoha oblastech. Počínaje těmi nejobvyklejšími, jakými je podepisování dokumentů až po antivirovou ochranu založenou na prevenci a důvěře v podpisovatele souboru, který se právě chystáme ve svém počítači otevřít. Soubor opatřený elektronickým podpisem nám dává nejen možnost odlišit například e-mail poslaný od důvěryhodného člověka, od mailu, který důvěryhodný není a proto může potenciálně obsahovat viry, ale v případě infekce i zjistit viníka šíření viru. To vzbuzuje větší zodpovědnost za antivirovou ochranu vlastního počítače.

Aplikací elektronického odpisu je však v praxi mnohem více.

Macao

Konsorcium Siemens Macao, Giesecke&Devrient a NEC získalo zakázku od vlády na národní identifikační karty v hodnotě 100M HK$. Kontrakt je zaměřen na multifunkční identifikační řešení na bázi čipových karet, které umožňuje realizovat e-government pro MACAO SAR. Pro obyvatele MACAA bude do konce letošního roku vydáno 500000 těchto identifikačních karet. Karty budou podporovat PKI na základě mezinárodních standardů, key management, autentizaci a další funkce.

Polsko

Finský výrobce čipových karet Setec ve spolupráci se svým polským distributorem dodá PKI čipové karty pro polský systém mezibankovních převodů ELIXIR, který je řízený a spravovaný institucí National Clearing House KIR. V Polsku je 80% mezibankovních transakcí provedeno pomocí systému ELIXIR. Čipové karty jsou nyní integrální součástí tohoto systému. Jsou použity pro vytváření bezpečného komunikačního kanálu mezi pobočkami polských bank a hlavní kanceláří KIR. Současně elektronicky podepisují a šifrují informace o těchto převodech.

Řidičské průkazy v Indii

Madhya Pradesh (stát v Indii) má přibližně 3 miliony vydaných řidičských průkazů a registrovaných licencí pro soukromá nebo podnikatelská (užitková) vozidla. Každoročně je zde vydáno 184000 řidičských oprávnění, 250000 registrací osobních automobilů a 15000 registrací vozidel pro podnikání. S tímto objemem dat je spojena ohromná administrativa, je to nákladný systém a vyžaduje všemožné zdroje.

Proto se v tomto státě rozhodli pro neobvyklý projekt a v Indii ojedinělý. Vydávají řidičské průkazy a technické průkazy vozidel na bázi čipových karet.

Celý systém má vysokou bezpečnost a umožňuje identifikaci, autentizaci a validaci řidičů a jejich vozidel.

Systém je kompatibilní s ISO 7816 a otevřeným standardem PCSC. Technické a řidičské průkazy vedou ke kompletní komputerizaci ministerstva dopravy. Takto byl vytvořen další krok k úplnému e-governmentu.

Policisté a dopravní inspektoři jsou vybaveni hand heald počítači. Zde jsou informace o vinících dopravních

přestupků shromažďovány v paměti načtením informací z čipů čipových karet a posléze uploadovány do centrálního počítače. Toto umožňuje vládě mít WAN síť, která okamžitě autentizuje a validuje každý průkaz vydaný ve státě.

Rakousko

V Rakousku se rozbíhá projekt elektronického podpisu. Uzavírání právně závazných smluv prostřednictvím internetu umožňuje v Rakousku projekt pro zavádění elektronického podpisu.

Elektronický podpis smlouvy je z právního hlediska postaven na stejnou úroveň jako klasické uzavírání smluv. Dceřiná společnost rakouského Telekomu Datakom, hodlá do konce roku pro tento projekt získat 50000 klientů. K využití služby si musí zájemci zakoupit čtecí zařízení a speciální čipovou kartu v hodnotě 60 Euro (1930 korun) s platností na jeden rok, jejíž prodloužení vyjde na 15 Euro (480 Kč). Potřebným čtecím zařízením na přenos údajů z čipové karty, která slouží k identifikaci uživatelů, budou postupně vybaveny všechny pošty.

Od digitálního podpisu si úspory slibuje i spolková vláda, a to zejména v mzdových nákladech a výdajích na různé tiskoviny.

Nyní je možno elektronický podpis využívat při styku se sociální pojišťovnou, od května pak u ostatních pojišťoven. Podávání daňových přiznání tímto způsobem se předpokládá od příštího roku.

Trochu to připomíná začátky éry elektronického podpisu u nás, s tím rozdílem, že v Rakousku existuje již možnost jeho praktického využívání.

Elektronické bankovní služby v ČR a elektronický podpis

Základem elektronického bankovnictví je vlastně e-obchod, kterým nabízí banka svoje služby svým klientům. Cílem je přesně to stejné jako u e-commerce, v běžně známých termínech a podmínkách. Nástroje pro provozování elektronického bankovnictví jsou také velmi podobné, i když je dlužno podotknout, že banka zde hraje roli dvojjedinou a to že jak služby poskytuje, tak zároveň zajišťuje i platby za ně.

U běžného elektronického obchodu služby zajišťuje obchodník a pro realizaci plateb musí mít ještě smlouvy s bankou. Tato cesta přece jen poněkud složitější.

Jaké možnosti nabízejí v současnosti banky pro elektronické bankovní služby s využitím elektronického podpisu?

Služby a jejich poskytování i rozsah lze rozdělit v podstatě podle možných a dostupných komunikačních médií (vynecháme-li laskavě kabelový přenos - tj. přenos dokumentů v kabele z domu k přepážce banky). Většina bank používá k zabezpečení elektronického, či internetového bankovnictví kryptografických kalkulaček, ale přece jen jsou výjimky.

ČSOB internetbanking 24

ČSOB před nedávnem zahájila svůj projekt internetového bankovnictví. Nabízí možnost získávat informace o transakcích, zůstatcích na účtech, zadávat převodní příkazy a podobně. Přístup k internetové službě je možný pomocí webového prohlížeče, ve kterém je nainstalovaný šifrovací modul umožňující šifrovat s klíčem délky 128 bitů a elektronický podpis. Tato skutečnost však není běžnou ani ve Windows 2000 a vyžaduje instalaci záplaty, kterou je možno zkopírovat z webové stránky společnosti Microsoft. Identifikace uživatele je možná buď zadáním identifikačních čísel IPPID a PIN, nebo použitím procesorové čipové karty. Nastavení bezpečného komunikačního kanálu se děje standardní jednocestnou autentizací ze strany serveru banky. V případě použití čipové karty se jedná o dvoucestnou autentizaci, při které se "představuje" svým certifikátem jak server, tak i klient. Čipová karta při autentizaci klienta spolupracuje a využívá služeb Windows a umožňuje autentizaci jak v MSIE, tak i v Netscape browseru.

Archivace elektronických dokumentů

Je další možnost jak v praxi využít elektronický podpis.

Notáři, společnosti, poradenské firmy, daňoví auditoři, účetní, různé svazové odborné komory a spolky generují velké množství dokumentů, které po podpisu zainteresovanými signatáři (ať již s notářským ověřením nebo bez něj) se nezbytně musí archivovat tak, aby i po dlouhé době byly dokumenty dostupné a podpis na nich bezpečně ověřitelný. V papírové formě je dokumenty možno dobře archivovat a metodologie pro bezpečnou archivaci je vypracována.

V době platného zákonu o elektronickém podpisu je však situace jiná a to především i z toho důvodu, že technologie elektronického podpisu je všeobecně a celosvětově uznávána a implementována. Tak vzniká potřeba a možnost bezpečné archivace elektronicky podepsaných elektronických dokumentů. Podpis na psaném dokumentu lze ověřit snadno a to pohledem. U elektronického podpisu toto ověření není technologicky ani zdaleka tak jednoduché. Proto ke službě bezpečné archivace elektronických dokumentů musí nezbytně přistoupit i služba ověření elektronické podpisu na uložených dokumentech eventuelně duplikace těchto dokumentů případně jejich převedení do papírové formy s vystaveným potvrzení o platnosti podpisů signatářů.

Uložená data (dokumenty) mohou být několikerého rázu, elektronicky podepsané soubory, elektronicky podepsané naskenované kopie papírových dokumentů, elektronicky podepsané datové formáty faxových správ a podobně.

Závěr

Teorie je vybudovaná a existuje celá řada evropských i lokálních norem, které nám umožňují elektronický podpis masově nasadit. Avšak praxe je zcela odlišná.

Neexistují metodické pokyny jak uvést ideu elektronického podpisu do praxe ve státních úřadech a vytvořit tak tzv. E-governement.

Můžeme donutit CA a RA jak se mají chovat a vnutit jim akreditaci, můžeme vytvořit zákon a prováděcí vyhlášku, ale nemůžeme lidi donutit, aby tuto technologii v praxi masově používali.

Pro masové nasazení je třeba vytvořit příležitosti, které lidem opravdu pomohou ušetřit čas a osloví je. Několik takových implementací jsme si právě představili.

CERTIFIKAČNÍ AUTORITA - CO NÁM NABÍZÍ?

JUDr. Iveta Hodková, CSc., PriceWaterhouseCoopers, Praha

Souhrn

Tento příspěvek se zabývá právními a praktickými aspekty služeb poskytovaných certifikační autoritou jak z pohledu klienta certifikační autority tak z pohledu certifikační autority. Uvádí jaké existují druhy certifikačních autorit dle zákona o elektronickém podpisu (dále jen Zákon) a prováděcí vyhlášky a řeší otázky jejich právního postavení, dokumentační základny, služeb, které může certifikační autorita v souvislosti s elektronickým podpisem a elektronickými dokumenty nabízet (dle Zákona a dále jiné Zákonem neupravené).

Úvod

Naprostá většina podnikatelů musí zpracovávat značné objemy tištěných dokumentů. Ve smyslu zaběhnuté praxe "co je psáno to je dáno" je úprava vztahů se zákazníky, dodavateli, státními úřady, zaměstnanci apod. doposud realizována většinou v listinné podobě. Je zřejmé, že vytváření a skladování těchto listinných dokumentů je drahé, stejně tak jako manipulace s nimi. Pravděpodobnost ztráty originálů důležitých dokumentů uchovávaných v podobě listin je také celkem významná.

Současné technologie umožňují v naprosté většině případů nahradit listinné dokumenty elektronickými, což vede ke značné úspoře času a nákladů, a tudíž ke zvýšení efektivity fungování společností. V okamžiku, kdy společnosti a jiní podnikatelé začnou uvažovat o "digitalizaci" svých procesů a činností, musí začít zvažovat nejen technologickou stránku plánovaných změn, ale i to, zda právní řád takovéto změny umožňuje[1]. Jde nejen o to, aby elektronické dokumenty, pokud je s nimi spojen určitý stupeň závaznosti, byly i v elektronické podobě právně platné (hmotné právo) a vymahatelné (procesní právo), ale musí být prověřeny implikace zahrnující oblast daňovou, účetní, sféru ochrany osobních údajů, práv duševního vlastnictví a případně i dalších právní odvětví, jako např. trestního práva.

Stručně o elektronickém podpisu

Jedním z nástrojů, které dle našeho právního řádu umožňují aby dokumenty existující v elektronické podobě byly právně platné, závazné a vymahatelné, je elektronický podpis, upravený Zákonem o elektronickém podpisu č. 227/2000 Sb. a následnou prováděcí vyhláškou, vládním nařízením a novelami procesních předpisů[2]. Význam elektronického podpisu, zejména slovy Zákona "zaručeného elektronického podpisu", roste s tím, jak roste rozšíření a význam elektronické komunikace obecně.

Dnes má již mnoho lidí základní představu o tom, jak elektronické podepisování většinou funguje. Přestože existují i jiné možnosti, nejčastěji se využívá technologie digitálního podpisu založeného na asymetrické kryptografii používající dva klíče - veřejný klíč a soukromý klíč, mezi nimiž existuje matematický vztah. Soukromým klíčem, který má k dispozici pouze podepisující osoba, se zpráva, dokument, datový soubor "podepíše" a veřejným klíčem příjemce takové zprávy ověří podpis. Zaručený elektronický podpis musí splňovat určité požadavky[3] zajišťující ve svém důsledku právní uznatelnost takového podpisu. Jedním z významných požadavků je důvěryhodná identifikace podepisující se osoby.

1 Ve své praxi jsem se častokrát setkala s tím, že společnost začala zavádět např. systém elektronické fakturace, kdy odpovědní pracovníci z IT oddělení případně od vnějšího dodavatele implementovali dobře fungující technologii aniž by zvažovali, zda zavedení takové aplikace s sebou nepřinese negativní právní resp. daňové dopady např. v podobě neuznatelnosti vydaných/přijatých faktur finančním úřadem s dopady jak na daň z příjmů, tak na daň z přidané hodnoty.

2 Jde o novely zákona o správě daní a poplatků, občanského soudního řádu, správního řádu, trestního řádu a dalších.

3 Zaručený elektronický podpis musí dle zákona o elektronickém podpisu splňovat tyto požadavky: a) je jednoznačně spojen s podepisující osobou, b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, d) je k datové zprávě, k níž se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Certifikační autorita

Ve světě listinných dokumentů nám podpis na listině důvěryhodně ověřuje notář. Ve světě elektronických dat a dokumentů, kdy možnost využití falešné identity je mnohem snadnější a pravděpodobnější, notář tuto funkci zastávat (bez dalšího) nemůže. Důvěryhodná třetí strana, která v určitém smyslu v elektronickém světě nahrazuje funkci notáře musí jednoznačně ověřit totožnost držitele veřejného klíče a skutečnost, že veřejný klíč podepisující osobě skutečně náleží, což stvrdí vydáním veřejně dostupného certifikátu - tento subjekt se běžně nazývá certifikační autorita, slovy Zákona "poskytovatel certifikačních služeb". Hlavním úkolem certifikační autority dle Zákona je tedy ověřovat a stvrzovat identitu držitelů veřejných klíčů a následně vydávat, evidovat a zveřejňovat případně zneplatňovat certifikáty. Tato autorita však může poskytovat další důležité související služby umožňující vytvořit z elektronického podpisu důvěryhodný a spolehlivý nástroj projevů vůle v elektronickém světě (viz níže).

Kategorie certifikačních autorit

Zákon o elektronickém podpisu rozlišuje tři kategorie certifikačních autorit (poskytovatelů certifikačních služeb):

- poskytovatel certifikačních služeb;
- poskytovatel certifikačních služeb vydávající kvalifikované certifikáty;
- akreditovaný poskytovatel certifikačních služeb.

Přestože v praxi nemusí být ve způsobu jejich fungování a tudíž ve spolehlivosti a důvěryhodnosti jejich služeb, žádný rozdíl, obecně lze říci, že zatímco "obyčejná" certifikační autorita nemusí splňovat žádné legislativní požadavky a její činnost není nikým kontrolována, další dva typy certifikačních autorit musí splňovat poměrně přísná ustanovení Zákona a prováděcí vyhlášky týkající se zejména bezpečnosti nástrojů elektronického podpisu, bezpečnosti jejich provozu[4], náležitostí kvalifikovaného certifikátu apod. Nad dodržováním těchto legislativních požadavků vykonává dozor Úřad pro ochranu osobních údajů s pravomocí poměrně rozsáhlých sankcí v případě jejich porušení. Certifikační autorita akreditovaná Úřadem pro ochranu osobních údajů (třetí typ CA) je pak jedinou autoritou, která je oprávněna vydávat certifikáty přijímané při komunikaci s orgány státní správy.

Certifikát

Certifikát je vlastně elektronickou obdobou průkazu totožnosti platnou pro elektronický svět. Je to doklad o tom, že totožnost držitele veřejného klíče byla ověřena. Certifikát spojuje jméno držitele páru soukromého a veřejného klíče s tímto veřejným klíčem a potvrzuje tak identitu osoby. Slovy zákona o elektronickém podpisu je certifikátem "datová zpráva, která je vydána poskytovatelem certifikačním služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost". Tuto ověřenou identitu lze používat nejen při podepisování dokumentů, datových souborů, ale lze ji využít také např. při přístupu k důvěrným nebo placeným informacím.

Při vydávání certifikátu certifikační autorita po ověření totožnosti žadatele podepíše svým soukromým klíčem žadatelův veřejný klíč a údaje o jeho držiteli a tímto podpisem stvrdí, že držitelem veřejného klíče je osoba uvedená v certifikátu. V řetězci důvěry je tak nutno důvěřovat certifikační autoritě a jejímu veřejnému klíči (stejně tak jako u listinných dokumentů notáři). Certifikáty většinou obsahují jméno držitele veřejného klíče/podepisující osoby, jméno CA, která vydala certifikát podepsaný jejím soukromým klíčem, dobu platnosti certifikátu, unikátní pořadové číslo a další údaje. Většina existujících certifikačních autorit v České republice však při vydávání svých certifikátů již dodržuje obsahové požadavky na kvalifikované certifikáty[5], upravené zákonem o elektronickém podpisu jako určitý vyšší a bezpečnější typ certifikátu.

Jak získat certifikát

Existuje možnost stáhnout si certifikát z www stránek aniž by naše totožnost byla důvěryhodně doložena či možnost získat certifikát dodávaný softwarovým společnostmi s programovým vybavením. Takové certi-

4 Bezpečnost certifikační autority je široký pojem a zahrnuje mimo jiné zpracování a přijetí dokumentační základny obsahující certifikační politiku, certifikační prováděcí směrnici, celkovou bezpečnostní politiku, systémovou bezpečnostní politiku, plán pro zvládání krizových situací a plán obnovy, odhad dostatečnosti finančních zdrojů a doklady o tom, že disponuje těmito finančními zdroji.

fikáty nejsou příliš průkazné a použití elektronického podpisu provázaného s těmito certifikáty pro závazné právní úkony nelze doporučit. V případném sporu by se povinná osoba dostala zřejmě do důkazní nouze.

Následující řádky se budou týkat postupu pro získání kvalifikovaného certifikátu dle Zákona. Ve většině případů je vhodná osobní návštěva certifikační autority, resp. její složky - registrační autority, která je autorizovaná ke sběru a ověřování informací o totožnosti žadatelů o certifikát a ke zpracování žádostí o certifikát. Na základě ověřených informací a dále prověření, že žadatel má data pro ověření elektronického podpisu odpovídající datům pro vytváření elektronického podpisu vydá certifikačních autorita žadateli požadovaný typ certifikátu. Před vydáním certifikátu je však certifikační autorita povinna žadatele o certifikát písemně, a to i v elektronické podobě, informovat o přesných podmínkách pro užívání certifikátu a o případných omezení jeho použití, a dále o podmínkách reklamací. Pak je nutno uzavřít mezi certifikační autoritou a klientem písemnou smlouvu o užívání certifikátu. Tato smlouva, která musí být uzavřena v listinné podobě (nelze ji uzavřít v elektronické podobě), by měla upravovat otázky práv, povinností a odpovědnosti smluvních stran i případné sankce, tzn. měla by upravovat podmínky pro vydání a užívání certifikátu, včetně postupu při zneplatnění certifikátu, otázky ochrany osobních údajů, ochrany spotřebitele, výši poplatku za vydání certifikátu apod.

Celý postup je možno realizovat také korespondenčně, zčásti elektronicky a zčásti poštou (zaslání notářsky ověřených kopií dokladů k ověření totožnosti certifikační autoritou a zaslání podepsané smlouvy o vydání a užívání certifikátu).

Povinnosti certifikační autority a její odpovědnost [6]

Veřejnoprávní

Veřejnoprávní povinnosti a odpovědnost certifikační autority se vztahují vůči státu. Jde většinou o odpovědnost administrativně správní - za přestupky a jiné správní delikty související s podnikatelskou činností. Sankcemi zde jsou ukládání pokut, popř. odebrání oprávnění. V určitých případech by mohlo dojít i k trestněprávní odpovědnosti statutárních orgánů subjektu provozujícího certifikační autoritu.

Jako certifikační autorita mohou působit výlučně soukromoprávní podnikatelské subjekty. Ač se bude jednat především o právnické osoby, právní předpisy nevylučují, aby si certifikační autoritu zřídil i podnikatel fyzická osoba. Vzhledem k nákladům spojeným s vybudováním certifikační autority to však v praxi bude spíše teoretická možnost.

Aby nedošlo k neoprávněnému podnikání, je subjekt provozující certifikační autoritu povinen získat živnostenský list[7] na "služby v oblasti administrativní správy", jehož obsahovou náplní je mimo jiné poskytování certifikačních služeb v oblasti elektronického podpisu, plnění funkce důvěryhodné třetí strany, vydávání certifikátů a provozování seznamu zneplatněných certifikátů (CRL). Jako zajímavost je možno uvést, že uvedená živnost zahrnuje i sekretářské služby, archivní služby, poskytování úvěrů a půjček nebankovními subjekty, odkup pohledávek, tedy značně různorodé činnosti spolu nesouvisející.

Vzhledem k tomu, že subjekt provozující certifikační autoritu bude většinou zpracovávat osobní údaje, a to zřejmě nejenom na základě zákona, lze doporučit oznámení této skutečnosti úřadu pro ochranu osobních údajů (dále jen Úřad).

---

5 Kvalifikovaný certifikát musí podle ZoEP obsahovat: a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona, b) obchodní jméno PCS a jeho sídlo, jakož i údaj, že certifikát byl vydán v České Republice, c)jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, d) zvláštní znaky osoby, vyžaduje-li to účel kvalifikovaného certifikátu, e) data pro ověření podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby, f) zaručený elektronický podpis PCS, který kvalifikovaný certifikát vydává, g) číslo kvalifikovaného certifikátu unikátní u daného PCS, h) počátek a konec platnosti kvalifikovaného certifikátu, i) případné údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití, j) případné omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

6 Odpovědnost je jakousi sekundární povinností vzniklou na základě porušení primární povinnosti, která má zásadně sankční povahu.

7 Tato povinnost vyplývá z nařízení vlády č. 140/2000 Sb., které stanoví seznam oborů živností volných, a dále nařízení vlády č. 469/2000 Sb., kterým se stanoví obsahové náplně jednotlivých živností.

Další veřejnoprávní povinnosti jsou pak spojeny s vydáváním kvalifikovaných certifikátů dle Zákona, kdy mimo jiné je nutno ohlásit Úřadu nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu tento záměr. Akreditovaná certifikační autorita se nesmí za takovouto vydávat až do okamžiku akreditace úřadem a při ukončení činnosti musí tento záměr oznámit Úřadu nejméně tři měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jinou akreditovanou certifikační autoritou. Pokud toto nelze zajistit, předá evidenci kvalifikovaných certifikátů Úřadu a informuje o tom dotčené osoby.

S porušením výše uvedených povinností jsou spojeny nepříjemné sankce většinou finanční povahy. Porušení živnostenského zákona (viz neoprávněné podnikání) může být pokutováno částkou až do výše 500 tisíc Kč, porušení zákona na ochranu osobních údajů (viz zpracování osobních údajů) částkou až do výše 10 miliónů Kč, při opakovaném porušení až do výše 20 miliónů Kč, porušení zákona o elektronickém podpisu může vést k uložení pokut až do výše 10 miliónů Kč, při opakovaném do výše 20 miliónů Kč, případně k odnětí akreditace.

Soukromoprávní

Soukromoprávní povinnosti a odpovědnost certifikační autority se projevuje vůči jiným soukromým subjektům, tzn. klientům, případně třetím osobám spoléhajícím se na certifikát. Povinnosti, které musí certifikační autorita dodržovat, jsou jednak speciální související se specifickou povahou její činnosti, a jsou upravené Zákonem, a dále obecné, upravené jinými právními předpisy týkajícími se všech podnikatelů (těmito obecnými povinnostmi se zde nebudu zabývat). Dle Zákona je certifikační autorita zejména povinna náležitě prověřit všechny údaje, které jsou obsahem kvalifikovaného certifikátu, i informace týkající se zneplatnění certifikátu a prověřit, zda odpovídají data pro vytvoření a ověření podpisu.

Z prováděcí vyhlášky k Zákonu specifikující mimo jiné náležitosti dokumentační základny, kterou musí certifikační autorita přijmout, vyplývají další rozsáhlé povinnosti certifikační autority.

Následkem porušení právní povinnosti, ať už speciální či obecné, může být povinnost nahradit způsobenou škodu, která musí být prokázána poškozeným, bezplatně odstranit vady případně zaplatit smluvní pokutu. Trestněprávní odpovědnost ani v těchto případech není vyloučena.

Certifikační autorita je zásadně odpovědná za zavinění, jedná se o odpovědnost subjektivní a této odpovědnosti se lze zprostit, pokud se podaří certifikační autoritě prokázat, že škodu nezavinila (na rozdíl od odpovědnosti objektivní, kdy se odpovídá za objektivně způsobený následek). Důkazní břemeno při takovém prokazování leží na certifikační autoritě. Toto prokazování za účelem zproštění se odpovědnosti může být obtížné zejména u nevědomé nedbalosti, tedy tehdy, kdy osoba (např. zaměstnanec) nevěděla, že svým jednáním může způsobit škodlivý následek, ale vzhledem ke svým osobním poměrům to vědět mohla a měla (např. přístroj se přehřívá, osoba odpovědná za obsluhu přístroje ho má vypnout).

Povinnosti podepisující se osoby a její odpovědnost

Držiteli soukromého klíče vznikají z tohoto titulu pouze soukromoprávní povinnosti, případně odpovědnost. Jeho povinností je podávat přesné, pravdivé a úplné informace certifikační autoritě ve vztahu ke kvalifikovanému certifikátu a dodržovat případná omezení v kvalifikovaném certifikátu uvedená. Pomineme-li však tuto dosti zřejmou povinnost, je jeho hlavní povinností zacházet se soukromým klíčem, tzn. s prostředky a daty pro vytváření elektronického podpisu tak, aby nemohlo dojít k jejich neoprávněnému použití. V případě odcizení či podezření na odcizení soukromého klíče je držitel certifikátu povinen neprodleně uvědomit certifikační autoritu a požádat ji o zneplatnění certifikátu. Zde je nutno upozornit na to, že Zákon jednoznačně neupravuje okamžik, kdy dochází k přechodu odpovědnosti za škodu způsobenou zneužitím soukromého klíče. Pouze přijetí novely Zákona či v určité míře soudní rozhodnutí může vyjasnit rozhodný okamžik, kdy v procesu zneplatnění certifikátu odpovídá za škodu certifikační autorita, držitel certifikátu a tudíž soukromého klíče či strana spoléhající se na certifikát.

I v případě podepisující se osoby jde o odpovědnost za zavinění.

Povinnosti osoby spoléhající se na certifikát

Tato osoba má v zásadě jedinou povinnost, a to ověřit si, zda kvalifikovaný certifikát podepisující se osoby je platný (nevypršela lhůta platnosti na něm uvedená), a zda nebyl zneplatněn (před ukončením lhůty platnosti). Toto lze ověřit v seznamu zneplatněných certifikátů (CRL) vydávaném pravidelně certifikační autoritou a neustále dostupném. Jak jsem však již uvedla výše, vzhledem k nešťastné právní úpravě lze jen doporučit, aby osoba, která se na certifikát spoléhá provedla ověření toho, že nebyl zneplatněn nejen v okamžiku přijetí dokumentu s elektronickým podpisem a certifikátem, ale i v následné aktualizaci seznamu zneplatněných certifikátů.

Další služby certifikační autority

Činnost certifikační autority nespočívá jen ve vydávání certifikátů, jejich evidenci, obhospodařování a zneplatňování, tak jak nařizuje Zákon. Dalšími službami, přestože Zákonem neupravenými, které může certifikační autorita poskytovat jsou:

Časové razítko

- časová razítka nebo časové značky ověřují, ke kterému okamžiku elektronicky podepsaný dokument existoval. Toto ověření je nesmírně důležité nejen z hlediska určení takového okamžiku, ale i z hlediska ověření, že dokument byl podepsán v době platnosti certifikátu. Tento druhý aspekt nabývá na významu zejména pokud se taková skutečnost ověřuje po mnoha letech. Časová razítka by měla být i součástí certifikátů a údajů o jejich zneplatnění.

Doručenky

- potvrzení přijetí dokumentu příjemcem. Tato služba je obdobou nám známého dopisu s doručenkou či potvrzení z podatelny úřadu o učiněném podání.

Díky tomu, že certifikační autorita je nezávislý subjekt, může být doručenka cenným dokladem pro obě strany smluvního vztahu a v kombinaci s časovým razítkem vytvořit dokonalý důkazní materiál ověřující čas podepsání a čas doručení daného dokumentu.

Archivační služby

Cílem této služby, jejíž poskytování by opět mělo být zajištěno důvěryhodnou stranou s přesně vymezeným a do značné míry veřejností kontrolovatelným způsobem fungování by bylo zajistit bezpečnou archivaci dokumentů při níž se klienti i třetí strany budou moci spolehnout na to, že archivované dokumenty bude možno kdykoliv vyhledat a stvrdit jejich atributy způsobem přijímaným jak soukromými subjekty, tak úřady státní správy a soudy. Z tohoto důvodu by nemělo jít jen o prostou archivaci dokumentů, ale o převzetí elektronických dokumentů k archivaci při němž by došlo k ověření pravosti elektronického podpisu klienta, neporušenosti dat a připojení podpisu archivační autority s časovým razítkem. Klient by následně, a to i po velmi dlouhé době, mohl požádat archivační autoritu o vystavení potvrzení o pravosti a neporušenosti dokumentu, platnosti podpisu či údaje k jakému okamžiku dokument existoval. Dále by archivační autorita mohla vytvořit duplikát dokumentu v elektronické či listinné podobě.

Veškeré výše uvedené služby mohou certifikační autority po technické stránce zajistit již nyní. Rozhodující pro jejich rozšíření do praxe však bude jednak vývoj v legislativní oblasti (na Slovensku je např. časové razítko dle zákona o elektronickém podpisu vyžadováno a certifikační autority tuto službu budou povinny poskytovat a klienti na druhé straně využívat) a jednak zájem klientů o tyto služby. Ten bude podmíněn nejen tím, že o existenci takových služeb a jejich přínosech se budou muset dozvědět, ale i cenou těchto služeb.

Časová razítka a jejich důvěryhodnost

Jan Staudek[1]

Dlouhodobá znalost doby vzniku/existence dané verze dokumentu umožňuje dokument použít jako důkazní materiály pro soudní při, pro registraci podání patentové přihlášky, zasílání objednávek, vydávání plánů, podepisování smluv, generování certifikátů a/nebo kryptografických klíčů apod. Není přitom podstatné, zda se jedná o textové dokumenty, databázová data nebo např. o binární soubory s programy, výpisy obsahů pamětí, evidenční záznamy monitorovacích systémů, kopie paketů přenášených sítí apod. Potřeba možnosti získání důkazu, že daná kolekce dat v daném čase existovala a že po zafixování znalosti této doby nebyla změněna, je neoddiskutovatelná. Případný fakt, že takový dokument je navíc i podepsán, pouze zesiluje důkazní sílu o bezpečnostní rys nepopiratelnosti. Tento článek ve stručnosti diskutuje problematiku prokazování dlouhodobé znalosti doby vzniku/existence dokumentu nebo dat,

Jak dlouho platí digitální podpis?

Při neodpovědně urychleném přijímání zákona o elektronickém podpisu v ČR, vesměs motivovaném osobními a politickými ambicemi mnohých na straně jedné a snahou poskytnout podpisový nástroj pro bezprostřední uplatnění v oblastech e-komerce na straně druhé, se plně ignoroval fakt, že v dlouhodobém horizontu je možnost získání důkazu, že daný dokument v jisté době existoval, minimálně stejně důležitá jako možnost získání důkazu, že daný dokument někdo konkrétní podepsal. Tento fakt se čtenáři ostře zvýrazní, když si uvědomí, jak je krátká doba platnosti podpisových nástrojů elektronického podpisu, a že samotný elektronický podpis nic nevypovídá o tom, kdy k vlastnímu aktu podpisu došlo.

Existence důkazu existence dokumentu v daném čase se ukazuje jako extrémně důležitý, ne-li nezbytný, nástroj pro udržování dlouhodobé validity dokumentů, např. po dobu několika desítek let. Nájemce si např. chce pronajmout nemovitost na dvacet let. Podpisové klíče majitele a nájemce nemovitosti platí ale obvykle pouze po dobu dvou let. Prodlužování klíčů obou smluvních stran, resp. jejich inovace vyžaduje tudíž spolupráci obou zúčastněných stran i po podpisu smlouvy, a to ještě po dobu mnoha let. Jestliže by jedna ze zúčastněných stran po jisté době s podmínkami nájmu nesouhlasila, mohla by další spolupráci odmítnout a řetězec důvěryhodnosti následných certifikátů prodlužujících platnost původního podpisu by byl přerušen. Opatření podepsané nájemní smlouvy časovým razítkem při jejím podpisu a předáním kopie časově orazítkované podepsané smlouvy oběma stranám problém uspokojivě řeší. Oběma stranám se tak umožňuje ověřit zachování integrity originální smlouvy i mnoho let po jejím podpisu. Ověření podpisu časově orazítkovaného podepsaného textu elektronicky publikované eseje, nalezeného např. po 100 letech, může být možná jediným způsobem, jak prokázat jeho autentičnost. Prokázání její autentičnosti fyzickými prostředky, podobně jak se prokazuje autentičnost např. Mozartových partitur, je v podstatě nemožná.

Razítko a značka

Jedním řešením je registrace existence takového dokumentu pomocí digitálního časového razítka, DTS (Digital Time-Stamp) potvrzujícího, že dokument v dané verzi existoval před dobou udanou v časovém razítku. Vlastní časová razítka mívají obvykle charakter digitálního (kvalifikovaného) certifikátu.

Důkaz existence dané verze dokumentu před udanou dobou může mít i charakter časové značky, kterou typicky bývá veřejně auditovatelný záznam ve veřejně dostupné registrační knize bezpečně vedené nějakou důvěryhodnou třetí stranou. Poskytovatel služby registrování časových značek obvykle používá pro dosažení důvěryhodnosti techniky, které kombinují charakteristiky dokumentů do charakteristik kořenových hodnot postupně budovaných datových struktur typu strom a kořenové hodnoty periodicky veřejně publikuje (např. Surety, *www.surety.com*, veřejné svědectví publikuje v nedělních NY Times od r. 1992). Vzhledem k vlastnostem jednosměrných hašovacích funkcí používaných pro výpočet charakteristik je takto vytvářená množina ověřovacích charakteristik odolná proti útokům. Časová značka, podobně jako časové razítko, prokazuje, že daná kolekce dat existovala před dobou vymezenou časovou značkou.

1 Fakulta informatiky, MU v Brně, e-mail: staudek@fi.muni.cz

Časové razítko i časová značka se vesměs uchovává odděleně od originálních dat, která lze tudíž časově označovat aniž by se měnil (a/nebo odhaloval) jejich obsah. Zatímco používání časových značek je vesměs doménou působnosti komerčních firem, používání časových razítek je v současné době předmětem rozsáhlých standardizačních snah "na de jure úrovni" (především v rámci iniciativ podporujících pod patronací evropských standardizačních organizací uplatňování elektronického podpisu). Poněvadž oba způsoby označování času se (i když diametrálně) liší pouze uplatněnou technologií, pokud explicitně neoznačíme diskutovaný nástroj, budeme termín časové razítko používat jako generický termín.

Pokud časové razítko splňuje předem (legislativně) stanovené podmínky důvěryhodnosti, lze např. platnost podpisu věřit i o uplynutí doby platnosti použitého podpisového klíče. Časové razítko totiž umožní ověřit, že dokument byl podepsán ještě v době, kdy podpisový klíč byl platný. Ověřovatel *(strana spoléhající se na časové razítko)* může zjistit i po revokaci podpisových klíčů podepsané osoby *(držitele časového razítka, resp. abonenta služby poskytování časových razítek)*, zda podpis byl vytvořen ještě před touto revokací.

Časovým razítkem lze opatřit jakýkoliv digitální dokument. Zavedením časového razítkování problém daný konečností doby platnosti digitálního podpisu převádíme na snadněji řešitelný problém konečnosti doby platnosti časového razítka, resp. na problém zajištění dlouhodobé důvěryhodnosti služby časového razítkování, *DTSS* (Digital Time-Stamping Service). Předpokládá se, že DTSS dostatečně silným kryptografickým způsobem spojuje daný konkrétní digitální dokument s okamžitou hodnotou času. Místo dlouhodobého udržování podpisové důvěryhodnosti pro spoustu autorů mnoha dokumentů můžeme řešit podobný problém pro omezený počet autorit vydávajících časová razítka, které se obvykle označují zkratkou *TSA* (Time Stamping Authority).

Co se rozumí službou časového razítkování?

Poněvadž škála potenciálních digitálních dokumentů je z hlediska možných obsahů i rozsahů velmi široká, DTSS vesměs nepracují přímo s dokumenty, ale s jejich jednoznačnými reprezentacemi - *charakteristikami* (message digests) získávanými vhodnými jednosměrnými hašovacími funkcemi (h). Charakteristiky jsou bitové vzorky pevné délky (desítky až stovky bitů bez ohledu na skutečnou délku původního dokumentu).

Například - Novák, *abonent DTSS*, podepíše dokument D a chce ho opatřit časovým razítkem:

- Nechá si vypočítat charakteristiku $h_D = h(D)$ pomocí vhodné hašovací funkce h (SHA-1, MD5, SHA-256, ...)
- spočtenou charakteristiku hD, nikoliv dokument D, pošle DTSS
- DTSS Novákovi vrátí DTS_D obsahující kopii dodané charakteristiky hD a udání času, ve kterém DTSS charakteristiku h_D obdržela
  - DTS_D má charakter certifikátu podepsaného TSA provozující DTSS. Protože charakteristika dokumentu hD nic nevypovídá o obsahu dokumentu D, TSA nemůže nic zjistit o obsahu dokumentu D
  - Novák může kdykoliv později předložit D a DTS_D a pomocí DTS_D prokázat dobu, kdy (podepsaný) dokument D určitě existoval

Strana spoléhající se na DTS spočte charakteristiku dokumentu D a ověří shodu spočtené charakteristiky s charakteristikou udanou v DTS_D

- strana spoléhající se na DTS_D musí být schopna ověřit platnost DTSD
  - DTSD má proto formát např. certifikátu podepsaného TSA a TSA tudíž musí splňovat minimálně tatáž pravidla, jako každá autorita vydávající (kvalifikované) certifikáty
- strana spoléhající se na DTS musí znát i způsob výpočtu charakteristiky
  - tento požadavek lze snadno splnit udáním ID použité hašovací funkce pro výpočet charakteristiky v DTS.

Schéma musí být odolné proti falšování DTS. DTS, resp. zařízení plnící služby časového razítkování odolné proti útokům, musí splňovat následující generické bezpečnostní požadavky:

- DTS musí být podepsáno dostatečně dlouhým klíčem, který vyhovuje požadavkům spolehlivosti po dobu např. několika dekád
- podpisový klíč TSA musí být uchováván s nejvyšší možnou zárukou bezpečnosti v zařízení odolnému proti potenciálním útokům (tamperproof box)
- udání času (datum, čas) musí být odvozeno z hodin, které jsou udržovány v analogicky bezpečném prostředí jako podpisový klíč TSA, které nelze opakovaně nastavit na dřívější hodnotu času a které mají zaručenou přesnost běhu po stejnou dobu, po kterou se požaduje platnost klíčů TSA
- DTS nesmí být možné vytvořit bez výše zmíněných nástrojů uchovávaných v zařízení vykonávajícímu DTSS odolnému proti útokům.

Dlouhodobou důvěryhodnost časového údaje o digitálním dokumentu - časového razítka - nelze implicitně zajistit ani rozhodnutím žádné vyšší moci, ani žádnými volními (etickými) pravidly. Časové razítko je produktem a nástrojem IT. Je proto nutné jeho důvěryhodnost explicitně podpořit uplatněním bezpečnostních technologií známých z návrhů a prosazování nástrojů podobného charakteru. Pro vytvoření spolehlivého digitálního důkazu zvládnutelným způsobem je nutné používat pro spojení transakce s údajem o času, ve kterém transakce proběhla, nekontraverzní všeobecně uznávanou metodu. Ta musí navíc i umožnit časová razítka kdykoliv později porovnávat. Kvalita digitálního důkazu se odvozuje z kvality postupu, kterým se získává datová struktura reprezentující příslušnou událost a z kvality parametrů, které daný důkaz vhodně vážou s reálným světem (v tomto případě z kvality odvození údaje o času).

Mezi takové technologie bez diskuse patří služby podporující nepopiratelnost, autentičnost a prokazatelnost zachování integrity dat. Při důvěryhodné a bezpečné implementaci těchto služeb naleznou uplatnění kryptografické algoritmy, formální nástroje pro specifikaci a analýzu bezpečnostních protokolů a pro dokazování jejich vlastností a principy konstruování odolných "atestovatelných" (elektronických) zařízení. A konečně, poněvadž se požaduje důvěryhodná znalost času, musí být hodnota časového razítka prokazatelně odvozena ze spolehlivého zdroje reálného času.

Důvěryhodné zdroje reálného času

Mezinárodní standard časové škály založené na základní jednotce sekunda, který platí od r. 1972, kdy nahradil standard GMT (Greenwich Mean Time) se nazývá UTC (Coordinated Universal Time, *Koordinovaná časová stupnice* podle Českého metrologického ústavu).

Obě normy (UTC i GMT) jsou v podstatě shodné, prakticky se neliší o více než o 1 sekundu. Nula hodin UTC odpovídá půlnoci v Greenwich (UK). Definici UTC udává doporučení ITU-R označované TF.460-4, časovou škálu definuje doporučení TF:460-5. Univerzální čas začíná o půlnoci nulou, je počítán v jednotkách modulo 24 hodin. Z praktického pohledu je UTC základní časovou osou ekvivalentní běhu průměrného slunečního času na poledníku 0°. Je jistým kompromisem mezi *stabilním atomickým časem* (TAI, Temps Atomique International), který je odvozen z fyzikálního chování jistého prvku jako průměr z měření prováděných přibližně 200 laboratořemi, a slunečním časem, a to při respektování vlivů rotace země. UTC definoval výbor *ITU-R* (International Telecommunications Radio Committee), centrální celosvětovou udržovací péči UTC pověřil Mezinárodní úřad pro míry a váhy, *BIPM* (Bureau International des Poids et Measures). *BIPM* vypočítává hodnotu UTC v kooperaci s národními reprezentacemi pro UTC, tj. s národními metrologickými instituty a s národními astronomickými observatořemi.

Hlavním zdrojem českého etalonu času je generátor v ÚRE AVČR, ze kterého se odvozuje česká realizace sekundy. Z ní se dále vytváří koordinovaná časová stupnice UCT(TP), kde TP značí Tempus Pragense, která reprezentuje čas pražského etalonu a je zároveň českou realizací světové časové stupnice UTC, [1], resp. podrobnější popis principů viz např. [2]. Další dva normály jsou v budově ÚTB SPT Telecom v Praze na

Žižkově. Pro koordinaci UTC(TP) s UTC bylo zpočátku používáno unikátní česko-slovenské televizní metody, poté bylo využíváno navigačního systému LORAN-C, [7], a od září 1991 je využíván družicový navigační systém GPS, [3].

Hodiny v počítači lze synchronizovat (nastavovat) více způsoby - např. pomocí modemu využíváním služby NIST Automated Computer Time Service (ACTS), [4], pomocí Internetu, [5] (přehled adres a jmen příslušných serverů uvádí [6], získávání denního času definuje RFC 867, získávání UTC definuje RFC 868 a vhodným protokolem je protokol NTP, Network Time Protocol, RFC-1305, který umožňuje trvale běžícími klientu udržovat čas na počítači vůči UTC[NIST] s milisekundovou přesností), lze používat hodiny řízené rozhlasovými signály nebo signály z některých geostacionárních družic. Nejpřesnějšími signály, které lze přijímat např. radiohodinami, jsou signály GPS (Global Positioning System), systému vyvinutého Ministerstvem obrany USA, mající celosvětové pokrytí, [8].

Formy implementace DTSS

Poskytovatelé DTSS využívají více technologických principů pro splnění bezpečnostních požadavků na DTSS. Dostatečně kryptograficky silnou DTSS lze implementovat jak technickými (elektronickými) prostředky, tak logickými (softwarovými prostředky), resp. jejich kombinací. Poskytování digitálního důkazu existence digitálního dokumentu v jistém čase může být vyjádřeno více principálně odlišnými formami, každou formu vyjádření lze získávat více způsoby (postupy).

- Důkaz může být přímou součástí dokumentu
  - akt udání času v takovém případě mění obsah dokumentu a bývá vykonáván jako součást plnění jiné bezpečnostní služby
- důkaz může mít charakter doprovodného vhodně podepsaného časového certifikátu, časového razítka, vydaného k udané kolekci dat a prokazujícího, že daná kolekce dat existovala před dobou udanou časovým certifikátem; časové razítko lze uchovávat odděleně od originálních dat, která lze tudíž časově razítkovat, aniž by se měnil (a/nebo odhaloval) jejich obsah - důkaz lze získávat jako produkt služby DTSS poskytované důvěryhodnou třetí stranou, tzv. časovou autoritou, TSA (Time Stamping Authority), obvykle podporované na straně TSA bezpečným generátorem časových razítek (DTSG, DTS Generator).
- důkaz může mít charakter časové značky udané kolekce dat, kterou bývá veřejně auditovatelný záznam ve veřejně dostupné registrační knize bezpečně vedené nějakou důvěryhodnou třetí stranou (notářem), která prokazuje, že daná kolekce dat existovala před dobou specifikovanou časovou značkou. Časová značka se opět uchovává odděleně od originálních dat, která lze tudíž časově označovat, aniž by se měnil (a/nebo odhaloval) jejich obsah.

Časová autorita, TSA

Standard protokolu pro časové razítkování v prostředí sítě Internet vyvinula pracovní skupina PKIX činná v rámci IETF, [9], Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, který specifikuje formáty žádostí o DTS a formáty odpovědí. PKIX stanovila základní bezpečnostní požadavky vlastnosti poskytovatele DTSS na Internetu, tj. na TSA, důvěryhodné třetí strany vydávající časové certifikáty, takto:

- používá důvěryhodný zdroj času
- do DTS vkládá důvěryhodnou hodnotu času
- do DTS vkládá jedinečnou identifikaci každého DTS
- do DTS vkládá jedinečnou identifikaci bezpečnostní politiky podle které bylo DTS vytvořeno
- DTS se vydává pouze k charakteristice dat získané identifikovanou jednosměrnou hašovací funkcí

- dodanou charakteristiku dat nijak neanalyzuje s výjimkou formátových kontrol vůči indikované hašovací funkci
- v DTS se neuvádí žádná identifikace požadující strany
- DTS podpisuje klíčem výhradně používaným pro tento účel
- DTS může být na žádost požadující strany doplněno o rozšíření obsahující dodatečné informace, pokud TA taková rozšíření podporuje.

Požadavky na politiku, které musí TSA vyhovět, jsou v současné době předmětem vývoje. Aktuální stav vývoje charakterizuje pracovní dokument PKIX Policy Requirements for Time-Stamping Authorities, [10], resp. jeho varianta vydaná ETSI počátkem roku 2002 jako TS 102 023 V1.1.1 (2002-01), [11]. Tyto dokumenty uvádějí požadavky na provozní a správní procedury TSA podporující důvěru žadatele o DTS, abonenta DTSS, a strany spoléhající se na DTS v bezpečnost poskytované DTSS.

Pro hlubší poznání fundamentů, ze kterých se odvozují požadavky na politiku TSA, je vhodné se seznámit s dalšími úzce souvisejícími materiály vydané iniciativami PKIX a ETSI počátkem roku 2002 - [12], [13], [14], [15]. Odpovídající funkčnost a bezpečnostní vlastnosti TSA vydávající svým abonentům DTS, kterým může spoléhající se strana důvěřovat, charakterizují následující odstavce. Popsaná politika je orientována především na podporu používání kvalifikovaných elektronických podpisů (viz čl. 5.1. *European Directive on a community framework for electronic signatures*, [19]), lze ji však použít v kterýchkoliv aplikacích požadujících prokazatelnost existence dat před jistým konkrétním časem. Současný stav standardizačních činností v oblasti požadavků na politiku TSA prozatím neřeší ani problém protokolů přístupu k TSA (protokol vlastního časového razítkování definuje RFC 3161, jeho v současné době aktuální volby - tj. povolené hašovací funkce, algoritmy podpisu, položky certifikátů - upřesňuje Time Stamping Profile, ETSI TS 101 861, [12]), ani způsob prezentace politiky TSA nezávislým stranám (požadované vlastnosti výstižně charakterizuje ETSI CWA 14172, [16]).

Požadavky na principy činnosti TSA

Abonentem TSA může být jak individuální koncový uživatel, tak i organizace. Abonent získává od TSA časová razítka svých dokumentů. Stranu, která se spoléhá na důvěryhodnost vydaných časových razítek, nazýváme *spoléhající se strana*.

Pravidla indikující použitelnost jisté třídy DTS pro jistou třídou aplikací nebo jistou komunitou spoléhajících se stran se shodnými požadavky na bezpečnost definuje dokument *Politika DTS*. Způsob, jakým konkrétní TSA plní DTSS definuje TSA v dokumentu *Prováděcí směrnice TSA*. Prováděcí směrnice TSA je dokument podrobnější než dokument Politika DTS. Sděluje, jakým způsobem daná TSA prosazuje pravidla stanovená udanou Politikou DTS v rovině technických, organizačních a provozních požadavků na kvalitu DTSS. Politika DTS je obvykle definovaná nezávisle na konkrétních detailech konkrétního provozního prostředí nějaké TSA. Politiku DTS může stanovit např. vhodná zájmová skupina abonentů a spoléhajících se stran, Prováděcí směrnici TSA definuje poskytovatel DTSS, tj. TSA. Abonent nebývá vázán žádnými dalšími povinnostmi vyjma těch, ke kterým je vázán smlouvou uzavřenou s TSA. Spoléhající se strana musí ověřovat podpis TSA uvedený v DTS, platnost takového podpisu na základě certifikátu TSA[2] , respektovat omezení použitelnosti DTS podle Politiky DTS indikované v DTS a dodržovat závazky stanovené případnou další smlouvou. TSA může specifikovat závazky v souladu s odpovídajícími právními normami.

Prováděcí směrnice TSA

TSA Prováděcí směrnicí TSA demonstruje svoji spolehlivost nutnou pro poskytování DTSS. Opatření definovaná v Prováděcí směrnici TSA plní požadavky stanovené plněnou Politikou DTS a vycházejí z provedení adekvátní analýzy rizik. Prováděcí směrnice musí explicitně deklarovat závazky externích organizací podporujících plnění služeb TSA vč. jejich politik a jejich prováděcích směrnic. Prováděcí směrnice TSA a ostatní dokumenty demonstrující shodu činnosti TSA s deklarovanou Politikou DTS jsou abonenty a spoléhajícími se stranami na akceptovatelné úrovni podrobností auditovatelné. TSA je řízena manage-

2 řešení problému dlouhodobé ověřitelnosti DTS se diskutujeme v závěru příspěvku

mentem s jasně vymezenou pravomocí a odpovědností, Prováděcí směrnice TSA a její plnění musí být periodicky oponovány, především vůči stanoveným Politikám DTS.

Způsob poskytování DTSS danou TSA je zájmovým stranám deklarován veřejně dostupnou *Politikou poskytování DTSS* dané TSA (TSA Disclosure Statement). Politika poskytování DTSS dané TSA musí obsahovat kontaktní informace, identifikace

- používané Politiky DTS
- alespoň jedné používané hašovací funkce
- očekávané doby použitelnosti podpisu na DTS
- přesnosti času uváděného v DTS ve srovnání s UTC
- veškerých omezení na použití DTSS
- závazků abonenta a spoléhajících se stran
- doby po kterou podle odpovídajících právních norem TSA udržuje auditní záznamy o transakčních událostech v TSA
- právních norem, které vymezují činnost TSA
- svých závazků vůči abonentům a spoléhajícím se stranám
- postupů aplikovatelných při soudních přích
- evaluační organizace, která posoudila činnost TSA apod.

Politika poskytování DTSS může být součástí smlouvy uzavírané mezi TSA a abonenty, resp.mezi TSA a spoléhajícími se stranami.

Klíčové hospodářství

TSA musí ručit za to, že veškeré kryptografické klíče generuje za podmínek a v prostředí, které jsou plně pod její kontrolou. Klíče musí být generovány ve fyzicky bezpečném prostředí osobami činnými v TSA v důvěryhodných rolích a za podmínek alespoň zdvojeného oprávnění, které jsou v souladu s Prováděcí směrnicí TSA.

Typickými specifikacemi adekvátních vlastnosti použitých kryptografických modulů jsou dokumenty *FIPS 140-1, úroveň 3 a výše, ETSI CAW 14167-2* nebo specifikace vlastností pro úroveň *EAL4 IS0 15408* (Common Criteria) apod.

Algoritmus pro generování klíčů, délka klíče a algoritmus použitý pro podpisování musí splňovat požadavky dané současným stavem rozvoje těchto technologií, resp. požadavky příslušných národních (akreditačních) organizací. Směrnici vymezující vhodné algoritmy digitálního podpisování a potřebné délky klíčů v současné době připravuje řídicí výbor EESSI (European Electronic Signature Initiative).

TSA musí ručit za uchování důvěrnosti podpisového klíče a jeho integrity, typicky ve shodě s omezeními danými stejnými dokumenty jako jsou uvedeny pro definici omezení pro generování klíčů. Pokud jsou podpisové klíče zálohovány, lze tak činit pouze ve fyzicky bezpečném prostředí v souladu s Prováděcí směrnicí TSA osobami v TSA činnými v důvěryhodných rolích a za podmínek alespoň zdvojeného oprávnění. Dříve než zálohovaný klíč opustí zařízení pro vydávání DTS, musí být kryptografickým modulem zaručena jeho důvěrnost. Je potřeba si uvědomit, že odolnost klíčů proti odhalení není dána pouze použitým kryptografickým modulem. Je silně ovlivněna i dalšími faktory, jakými jsou např. zmíněný export klíčů a způsob inicializace činnosti kryptografického modulu.

Při distribuci ověřovacího klíče podpisu TSA spoléhajícím se stranám ručí TSA za integritu a autenticitu tohoto klíče. Důvěryhodnost CA, která vydala certifikát TSA, musí být stejná nebo vyšší než důvěryhodnost dané TSA. Doba platnosti certifikátu ověřovacího klíče TSA nesmí překročit meze dané zvoleným algoritmem podpisu a délkou podpisových klíčů TSA.

Po ukončení platnosti podpisového klíče TSA musí být tento klíč (a všechny jeho kopie) zničen. Po uplynutí expirační doby podpisového klíče musí DTSG odmítnout vydávání DTS. Za bezpečnost použitých kryptografických modulů odpovídá TSA a to nejen během řádného provozu, ale i v době procesů jejich dodávky, uchovávání záloh, instalace, aktivace a obnovy klíčů, provozu DTSG, oprav apod.

Vlastní vydávání časových razítek

Časové razítko musí obsahovat identifikaci Politiky DTS, v rámci jejíž působnosti je časové razítko považované za důvěryhodné. Každé razítko musí mít jednoznačný identifikátor, musí obsahovat identifikaci TSA, charakteristiku časově razítkovaných dat a udání času. Zdrojem hodnoty času musí prokazatelně být některá z laboratoří UTC[k]. Přesnost synchronizace času udávaného v DTS udává Politika DTS. Bezprostředně po detekci ztráty této synchronizace musí TSA vydávání DTS přerušit. Časové razítko musí být podepisováno klíčem, který je výhradně používán jen pro službu DTSS.

Protokol tvorby DTS předpisuje RFC 3631, [9], odpovídající bezpečnostní profil vymezuje ETSI TS 101 861, [12]. Hodiny používané TSA musí být kalibrovány pravidelně, podle požadavků daných Politikou DTS a Prováděcí směrnicí TSA. Kalibrace musí být prováděna bezpečným, chráněným způsobem, který zajišťuje ochranu před útoky vedenými např. neutorizovanými osobami, radiovými i elektrickými šoky apod.

Nepožaduje se po TSA, aby TSA v rámci intervalů daných přesností udávaného času udržovala (udávala) pořadí žádostí abonentů o vydání DTS.

Správa řízení a provoz TSA

TSA musí zajistit plnění všech administrativních a správních postupů a procedur způsobem, který je odpovídající nejlepším známým praktikám. Příslušná opatření specifikuje Politika DTS, způsoby jejich dodržování a aplikace určuje Prováděcí směrnice TSA. Pokud plnění některých dílčích funkcí při poskytování DTSS TSA outsourcuje od subdodavatelů, nezprošťuje ji tato skutečnost odpovědnosti. Odpovědnost případných třetích stran musí TSA explicitně deklarovat ve své Politice poskytování DTSS. Politika poskytování DTSS, Prováděcí směrnice TSA a ostatní dokumenty předpisující činnost TSA musí být v souladu s bezpečnostními politikami IT organizace, která TSA provozuje.

Velmi důležitou roli z tohoto hlediska má personální bezpečnostní politika. Zaměstnanci TSA musí mít prokazatelnou znalost, zkušenost a kvalifikaci pro práce potřebné pro poskytování DTSS. Prokazatelností se rozumí držení odpovídajících kvalifikačních certifikátů, absolvování dostatečně dlouhé praxe, kurzů apod. Role a odpovědnosti Politikou DTS musí být explicitně vyjádřeny v popisech práce, důvěryhodné role, tj. role na kterých závisí bezpečnost TSA, musí být identifikovány explicitně. Za technologie bezpodmínečně zvládané pracovníky TSA se považují technologie vydávání DTS, digitálních podpisů, kalibrace a synchronizace hodin TSA s UTC, tvorby a provozu bezpečných systémů IT a správy rizik. Mezi typické důvěryhodné role v TSA patří bezpečnostní manažer, správce systému, operátor systému a pracovník vnitřního auditu. Zaměstnanci přijímaní do pracovního poměru v těchto rolích se musí podrobit stanoveným bezpečnostním prověrkám.

TSA ručí za to, že fyzický přístup ke kritickým službám je řízený a rizika fyzických útoků jsou minimální. Adekvátní opatření se musí týkat jak vydávání, tak správy vydávání DTS, zvláště pak přístupu ke kryptografickému modulu. Bezpečnostní hranice chráněné oblasti musí být vymezena zřetelně, tj. fyzicky. Tato oblast nesmí být sdílena jinými organizacemi apod. Adekvátním dokumentem vymezujícím požadavky na fyzickou bezpečnost zařízení tohoto typu je standard ISO/IEC 17799.

TSA ručí za bezpečné provozování DTSS. S tím souvisí požadavky na stanovení a prosazování politiky správy, na bezpečnost a manipulaci s médii, na plánování provozní činnosti TSA, na vypracování plánů reakcí na bezpečnostní incidenty a havarijních plánů a na stanovení postupů a odpovědností pro vlastní rutinní provoz zařízení TSA (monitorování auditních žurnálů, běžná údržba, správa sítě, antivirová ochrana atd.). Uplatněním řízení přístupu musí TSA zajistit, že přístup k prostředí poskytování DTSS mají pouze správně autorizovaní jednotlivci. Řízení přístupu se prosazuje pomocí firewallů, administrativními opatřeními, technicko-logickými nástroji a dodatečnými opatřeními typu monitorování, auditování záznamů o událostech apod. Musí být uplatněna opatření chránící zařízení TSA při jejich údržbě, opravách a inovacích.

Veškeré události, které ovlivňují bezpečnost poskytování DTSS musí TSA oznámit abonentům a spoléhajícím se stranám bez zbytečného prodlení. Ukončení své činnosti musí TSA oznámit svým abonentům

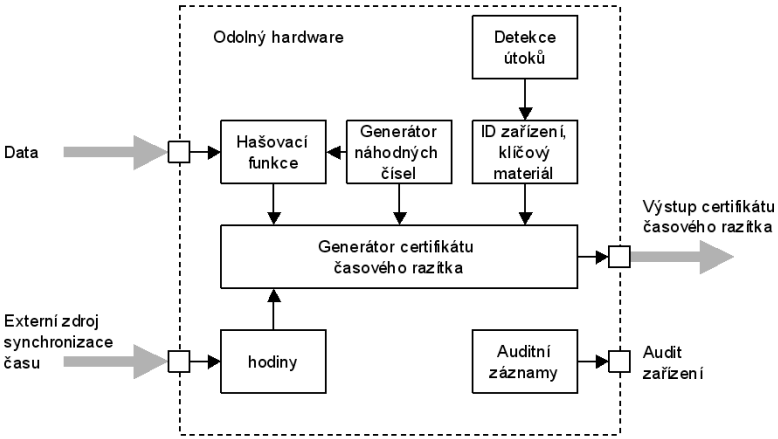
a spoléhajícím se stranám v dostatečném předstihu. Záznamy o událostech v TSA a podobné žurnály musí TSA ještě před ukončením své činnosti uložit u vhodné spolehlivé třetí strany ve formě použitelné pro případné použití jako důkazy. Klíče a případné jejich kopie musí TSA zničit.

Generování DTS generátorem časových razítek (DTSG)

Princip ilustruje obrázek Obr.2. Ideje zde uvedené jsou převzaty z [17]. Jedná se ilustrační příklad zařízení poskytujícího DTSS v rámci uzavřeného systému, který si neklade za cíl plné dosažení podmínek stanovených iniciativami PKXI a ETSI. Zdrojová data se čtou přímo do generátoru DTSG. DTSG vygeneruje vhodnou jednosměrnou hašovací funkcí (SHA-1, MD5, SHA-256, ...) charakteristiku shromážděných dat a získá ze svých vnitřních bezpečných hodin reálného času údaj o čase a vygeneruje časové razítko - certifikát obsahující charakteristiku, údaj o čase a ID daného DTSG a tento certifikát podepíše svým podpisovým klíčem uchovávaným uvnitř DTSG.

Při ověřování časového razítka se ověřuje platnost generovaného certifikátu časového razítka pomocí ověřovacího klíče DTSG. Po ověření platnosti certifikátu lze ověřit shodu certifikované a vypočtené charakteristiky časově razítkovaných dat. Pokud se vypočtená a certifikovaná charakteristika neshoduje, pak buď certifikát neodpovídá ověřované kolekci dat nebo ověřovaná kolekce byla po vydání časového razítka modifikovaná. V obou těchto případech ověřovací proces vydá negativní stanovisko, jinak autenticitu data a času potvrdí.

Certifikát časového razítka vydaný konkrétním (identifikovatelným) DTSG bude nezpochybnitelným důkazem potvrzení existence dané verze kolekce dat v daném čase tehdy, když příslušné DTSG bude vyhovovat podmínkám stanoveným uznávanou (akreditační) autoritou. Ze zkušeností se zaváděním legislativních podmínek pro uznávání digitálních podpisů jak důkazních materiálů plyne, že mezi takovými podmínkami nutně musí být specifikace kryptografických mechanismů, bezpečného zdroje času, auditních záznamů o činnosti takového zařízení, odolnosti zařízení proti útokům a identifikovatelnost zařízení.



Obr.2 Generátor časových razítek, DTSG

Podpisový (privátní) klíč DTSG musí být jedinečný, měl by být generován uvnitř DTSG v shodě s odpovídajícími požadavky na jeho bezpečnost (např. podle FIPS 140-1 level 3 nebo 4) a jeho hodnota nesmí opustit

vlastní zařízení DTSG. Pokud je klíč generován softwarově v nějakém univerzálním zařízení, je nutné dalšími bezpečnostními postupy např. zajistit, aby se nikdy neobjevil v paměti takového zařízení jako celek.

Problém bezpečného zdroje času

Použitý zdroj reálného času musí být přesný a důvěryhodný. Samotná přesnost jejich běhu pro dosažení potřebné důvěryhodnosti nepostačuje. Vnitřní hodiny DTSG musí být periodicky rekalibrovatelné a rekalibrace musí být certifikovatelná a auditovatelná. Pro rekalibraci lze použít důvěryhodný radiový zdroj nebo odpovídající internetový protokol [20], [21], [22]. Pro získání dostatečné úrovně důvěryhodnosti DTSG je nutné, aby byl zdroj času DTSG schválen příslušnou certifikační laboratoří, aby taková certifikační laboratoř po procesu rekalibrace a certifikace vydala pro daný DTSG podepsaný certifikát o rekalibraci a aby tento certifikát byl v DTSG dostupný pro účely následných bezpečnostních auditů. O každé změně hodnoty vnitřních hodin DTSG musí být vypracován bezpečný auditní záznam obsahující starou a novou hodnotu času, specifikaci zdroje času atd.

Bezpečnostní audit

Auditní záznamy jsou pořadově číslovány souvislou číselnou řadou, aby bylo možné určit přesné pořadí všech událostí (udávání času přesnost pořadí nezaručí, hodnota vnitřních hodin se může modifikovat). Mimo výše zmíněných auditních záznamů o změnách času se v této řadě typicky udržují auditní záznamy o zapínání a vypínání DTSG, o korekcích jeho firmware a software, o manipulacích s hardware, o výsledcích periodicky prováděných vnitřních testech DTSG apod. Každý takový záznam musí být podepsán DTSG jako celek a lze podepisovat i jednotlivé jejich položky.

Hrozby DTSG a možná bezpečnostní opatření

Při provozu DTSG je nutné respektovat řadu hrozeb. DTS se vydává k charakteristice dokumentu, nikoli k originálu dokumentu. Velmi známou hrozbou při práci s charakteristikami je tzv. Birthday Attack (narozeninový útok)[3] . DTSG je vystaven riziku fyzického útoku cílenému na přečtení soukromého podpisového klíče z paměti DTSG a na získání možnosti vydávat falešná DTS. Cílem fyzického může být přeprogramování DTSG tak, aby byl používán jiný, známý podpisový klíč. Pokud není dostatečně zajištěná autentičnost ověřovacího (veřejného) klíče DTSG, útočník může šířit falešný ověřovací klíč a tím podvodně ověřovat falešná DTS. Útočník na technické prostředky DTSG může změnit, resp. posunout, hodnotu vnitřních hodin DTSG a způsobit, že DTSG bude legitimní formou vydávat falešná DTS.

Princip "narozeninového útoku" je dán vlastnostmi jednosměrných hašovacích funkcí používaných pro výpočet charakteristik dokumentů. Tyto funkce zajišťují snadný výpočet charakteristiky dokumentu a přitom neumožňují snadné nalezení jiného dokumentu se stejnou charakteristikou. Každá minimální změna původního dokumentu vyvolá náhodnou změnu charakteristiky dokumentu. Jednosměrné hašovací funkce jsou v podstatě generátory pseudonáhodných čísel. Nalezení dvou dokumentů se stejnou charakteristikou vyžaduje provedení útoku hrubou silou - zkoušením všech možností. Jestliže hašovací funkce MD-5 generuje 128 bitové charakteristiky, provedení útoku hrubou silou požaduje provedení 2^{128} kroků, což je technologicky nemožné. Narozeninový útok spočívá v postupném generování dokumentů a hledání libovolných dvou, které mají shodné charakteristiky, což je úloha podstatně snazší, než útok hrubou silou (pro MD-5 vyžaduje provedení pouze 2^{64} kroků). Útočník tak může naleznout dva dokumenty, jeden s legálními daty a druhý šikovně upravený tak, aby původní data vhodně modifikoval. Oba budou mít shodnou charakteristiku. Musí pro útok ale použít pokud možno nějaký vhodný masivně paralelní výpočetní systém. Jakmile nalezne takovou dvojici dokumentů, stačí předložit DTSS jeden z nich a získané DTS bude platné pro oba dva. Eliminaci útoků tohoto typu lze dosáhnout např. tím, že DTSG přidává před generováním charakteristiky náhodné jedinečné číslo (nonce - number used once). Přidání téhož čísla ke dvou různým dokumentům původně se stejnými charakteristikami způsobí, že charakteristiky modifikovaných dokumentů pomocí "nonce" budou odlišné. Číslo nonce DTSG generuje pro každý předložený dokument nově, neopakovatelně. Hodnota "nonce" je uváděna v DTS.

3 Známý problém z teorie pravděpodobnosti, který říká, že když je místnosti více než 23 lidí, pak je vysoce pravděpodobné, že některá dvojice bude slavit narozeniny ve stejném dni.

Cílem *hardwarové odolnosti proti útokům* je dosažení toho, že zařízení nelze napadnou fyzicky s cílem zjistit hodnotu soukromého klíče, provést modifikaci hodnoty času, modifikovat software, nahradit podpisové kliče falešnou dvojicí apod. Je potřeba do pouzdra DTSG zabudovat poplašné zařízení, které při otevření pouzdra vypracuje odpovídající auditní záznam, zničí všechna kritická data a zařízení dezaktivuje. Pokud součástí zařízení je zdroj energie, pak lze kritická data uložit do energeticky závislé paměti a otevřením pouzdra zdroj energie vypnout. nCipher[4] v zařízeních vyhovujících FIPS 140-1 level 3 např. tištěné spoje zalévá (epoxydovou) substancí, její odstranění má za následek zničení čipů na desce a tím i zničení kritických dat. Je nutné vyřešit získání důkazových materiálů prokazujících, že došlo provedení útoku na zařízení. Na povrch pouzdra jak z vnější, tak i zvnitřní strany lze umístit pro útočníka obtížně detekovatelné bezpečnostní značky např. holografickou formou. Indikací je i sebezničení zařízení po otevření pouzdra zařízení.

Pokud je DTSG implementovaný pouze softwarově nelze využít přínosy ochrany na hardwarové úrovni. Musí se použít jiné techniky pro podporu odolnosti - nestrukturovanou a nemodulární implementaci, samomodifikující se kód, šifrované segmenty kódu, dělení klíčů a kritických dat do více částí, vyžadování používání pomocných autentizačních (kryptografických) zařízení na bázi např. čipových karet, "dongles" apod. Na straně serveru lze podpisový klíč šifrovat symetrickou kryptografií pomocí klíče odvozovaného z hesla, které zná pouze důvěryhodný administrátor. Dešifrovaný podpisový klíč lze ukládat pouze do energeticky závislé paměti, nikdy se nesmí objevit v energeticky nezávislé paměti typu flash memory, pevný disk apod. Integritu kritických dat, programů a firmware uvnitř DTSG lze chránit podpisem, uložením v ROM.

Důvěryhodné generování a ověřování DTS

Počátečně si DTSG vnitřně vygeneruje dvojici podpisových klíčů a svoje jedinečné identifikační číslo, ID. Tyto hodnoty jsou generovány jednorázově a jsou uloženy hodnoty v energeticky nezávislé RAM.

Po požádání o časové razítko DTSG načte označovaná vstupní data, vygeneruje výše zmíněný "nonce", připojí ho k údajům a vypočte charakteristiku takto modifikovaných dat. Poté vytvoří tělo DTS skládající se z "nonce", charakteristiky, údaje o čase a ID DSTG (součástí DTS jsou pochopitelně i organizační režijní data typu identifikace použitého podpisového systému apod.), toto tělo podepíše (standardní formou, tj. šifruje podpisovým klíčem charakteristiku těla) a výsledné DST předá na výstup.

Při ověřování kontrole autentičnosti dat kontrolující strana důvěryhodně (bezpečným kanálem, např. fyzickým point-to-point spojením) získá ověřovací klíč a ID DSTG. Po ověření shody ID si ověří platnost podpisu DTS. Platnost podpisu potvrzuje, že DTS byl vygenerován tímto DTSG a ověří se autentičnost dat - vypočte se charakteristika dat modifikovaných pomocí "nonce" z DTS a porovná se s charakteristikou uvedenou v DTS. Shoda indikuje autentičnost dat, data a DTS jsou párovou dvojicí. Tím se potvrdí doba, ve které byla tato data časově orazítkovaná.

Naznačený proces ověření je pro uživatele důvěryhodný tehdy, když DTSG bude odolný proti útokům a tato vlastnost bude potvrditelná bezpečnostním auditem. Řetěz důvěry dávající uživateli záruku za bezpečnost DTS má svůj počátek v samotném zařízení typu DTSG. DTSG poskytuje ověřovací klíč svého podpisu, tento klíč autentikuje DTS, DTS autentikuje data. Každé DTS identifikuje jeden konkrétní DTSG, ten lze podrobit fyzické inspekci zjišťující, zda nedošlo k útoku na hardware DTSG a bezpečnostnímu auditu. Nedokonalá odolnost DTSG by útočníkovi mohla umožnit veřejný ověřovací klíč a DTS falšovat.

Dlouhodobá ověřitelnost časového razítka

DTS je obvykle neověřitelné v době, která následuje po uplynutí platnosti certifikátu TSA, protože žádná CA po této době nezaručuje, že bude dále publikovat revokační informace např. z důvodu kompromitace podpisového klíče TSA. Ověření DTS po uplynutí platnosti certifikátu TSA je možné ověřit pouze tehdy, když se ví, že

- do doby, kdy spoléhající se strana ověřuje DTS, nedošlo ke kompromitaci klíčů TSA
- hašovací funkce použitá při tvorbě DTS vylučuje jakékoliv kolize i v době, kdy spoléhající se strana ověřuje DTS,

4 www.ncipher.com

- algoritmus podpisu a délka podpisového klíče použité při tvorbě DTS jsou odolné kryptografickým útokům i v době, kdy spoléhající se strana ověřuje DTS.

Pokud nelze platnost těchto podmínek zaručit, musí být integrita DTS chráněna např. následnými DTS nebo časovým značkováním zmíněným v následujícím odstavci nebo se musí časově razítkovaná data uchovávat v adekvátně bezpečné paměti. Ověřování platnosti DTS může poskytovat jako službu TSA nebo jiná důvěryhodná třetí strana.

DTSS notářského charakteru (časové značkování)

Čistě softwarová řešení DTSS obvykle používají pro dosažení důvěryhodnosti techniky, které kombinují charakteristiky dokumentů do charakteristik kořenových hodnot postupně budovaných datových struktur typu strom a kořenové hodnoty se periodicky veřejně publikují (např. Surety Techn, www.surety.com veřejné svědectví publikuje v nedělních NY Times od r. 1992). Vzhledem k vlastnostem jednosměrných hašovacích funkcí používaných pro výpočet charakteristik je takto vytvářená množina ověřovacích charakteristik odolná proti útokům. DTS v takových případech pochopitelně potvrzují dobu existence dokumentu v intervalech publikování kořenových charakteristik. Zevrubnější rozbor technologií a vlastností DTSS tohoto typu lze nalézt v příspěvku [18] z konference Security 2001.

Slovo závěrem

Neodpovědně urychlené přijetí zákona o elektronickém podpisu v ČR problém času plně ignorovalo. Díky tomu lze důkaz existence jakýchkoliv dat v době předcházející době udané získat asi pouze jejich uchováním v adekvátně bezpečné paměti - tj. fyzicky u klasického notáře. Taková úschova bez dalších ošetření přirozeně neřeší problém odmítnutí poskytnutí služby např. z důvodu nezpracovatelnosti média.

Reference

[1] Český metrologický ústav, http://www.cmi.cz

[2] Otokar Buzek, *Etalonáž sekundy SI a vytváření časových stupnic*, http://www.astro.cz/win/cas/praha/crp/0011b.phtml

[3] Martin Poupa, *Vše o času*, http://home.zcu.cz/~poupa/oma50.html

[4] *Set Your Computer's Clock Via the Telephone*, NIST Automated Computer Time Service (ACTS), http://www.boulder.nist.gov/timefreq/service/acts.htm

[5] *Set Your Computer Clock Via the Internet*, NIST Internet Time Service (ITS) http://www.boulder.nist.gov/timefreq/service/its.htm

[6] *NIST Internet Time Servers*, http://www.boulder.nist.gov/timefreq/service/time-servers.html

[7] *The Official Source of Time for the Department of Defense and the Standard of Time for the United States*, http://tycho.usno.navy.mil/loran.html

[8] *GPS World*, http://www.gpsworld.com/gpsworld/

[9] *Internet X.509 Public Key Infrastructure Time-Stamp Protocol* (TSP), RFC 3161, http://www.ietf.org/rfc/rfc3161.txt

[10] *PKIX Policy Requirements for Time-Stamping Authorities*, http://www.ietf.org/internet-drafts/draft-ietf-pkix-pr-tsa-00.tx

[11] *Policy Requirements for Time-Stamping Authorities*, ETSI TS 102 023 V1.1.1 (2002-01), http://portal.etsi.org/sec/ts_102023v010101p.pdf

[12] *Time stamping profile* - ETSI TS 101 861 v1.2.1 (z března 2002), http://portal.etsi.org/sec/el-sign.asp

[13] *Signature Policies Report* - ETSI TR 102 041 (z února 2002), http://portal.etsi.org/sec/el-sign.asp

[14] *XML Advanced Electronic Signatures* (XAdES) - ETSI TS 101 903 (z února 2002), http://portal.etsi.org/sec/el-sign.asp

[15] *Electronic Signature Formats* - ETSI TS 101 733 v 1.3.1 (z února 2002), http://portal.etsi.org/sec/el-sign.asp

[16] *EESSI Conformity Assessment Guidance*, CEN Workshop Agreements 14172, http://www.cenorm.be/isss/cwa_download_area/cwa14172-1.pdf,

[17] *Chris Russell, Analysis of a Secure Time Stamp Device*, October 17, 2001, http://rr.sans.org

[18] J. Staudek, *Čas a důvěryhodnost digitálních dokumentů*, Security 2001, AEC, Praha 2001

[19] *European Directive on a community framework for electronic signatures* http://europa.eu.int/ISPO/ecommerce/legal/documents/1999_93/1999_93_en.pdf

[20] NIST *Internet Time Service*, http://www.boulder.nist.gov/timefreq/service/its.htm

[21] *NIST Radio Station*, http://www.bldrdoc.gov/timefreq/stations/www.html

[22] *Secure Network Time Protocol (stime)*, http://www.ietf.org/html.charters/stime-charter.html

ODPOVĚDNOST V SOUVISLOSTI S ÚTOKY NA "ELEKTRONICKÝ PODPIS"

Mgr. Pavel Vondruška, Úřad pro ochranu osobních údajů
a JUDr. Ján Matejka, Ústav státu a práva AV ČR

Problematika elektronického podpisu a především elektronického podpisu založeného na kvalifikovaném certifikátu zůstává i po účinnosti zákona č. 227/2000 Sb. o elektronickém podpisu (dále jen zákon) nadále v právních kruzích poměrně opomíjena. Přitom samotný význam podpisu (a to i elektronického) vyplývá právě ze skutečnosti, že podpis jednající osoby je předpokladem platnosti písemných právních úkonů (§ 40 odst. 3 občanského zákoníku). V současné době však bývá význam elektronického podpisu spojován výlučně či převážně s tímto zákonem.

Odpovědnostní aspekty vyplývající z této zvláštní právní úpravy obsahují řadu zcela zásadních a zvláštních náležitostí. Nejen tato, ale i další související problematika však právní teorii a praxí zůstává zcela neřešena (jde zejména o odpovědnostní důsledky za zneužití elektronických podpisů, problematika užívaní těchto podpisu v oblasti orgánů veřejné moci, podávání daňových přiznání, apod.). Na tyto a jim podobné otázky jsme se v poslední době zaměřili a společnými silami chceme hledat odpovědi.

Vzhledem k našemu společnému zájmu o tuto oblast jsme se přihlásili o udělení grantu na toto téma. Grantová agentura České republiky nám v tomto roce takovýto grant udělila. Jeho název je "The responsibility of some persons concerning the attacks to the electronic signature devices and to the procedures according to the Act # 227/2000 Sb. (Odpovědnost některých osob v souvislosti s útoky na nástroje elektronického podpisu a související postupy dle zákony č. 227/2000 Sb.). Grant je dvouletý.

Na této konferenci jsme se rozhodli prezentovat naše prozatimní výsledky a podělit se tak o některé z našich myšlenek a část připravovaných materiálů.

Příloha č.1 Právní důsledky zneužití elektronického podpisu
(otázky související s platností/neplatností elektronicky učiněného úkonu, který byl elektronicky podepsán za pomoci vybraných útoků)

Příloha č.2 Základní přehled možných útoků
(obecná klasifikace útoků na různé subjekty a různé druhy útoků)

Příloha č.3 Problémy spojené s certifikátem poskytovatele
(řešena je otázka jak zabránit útokům, které jsou založeny na tom, že není dostatečně ověřen certifikát poskytovatele, navržený postup lze uplatnit u kvalifikovaných certifikátů akreditovaného poskytovatele certifikačních služeb)

Příloha č.4 Jak získat podpis k textu od jiné osoby
(předvádí se, jak lze za jistých okolností získat podpis nějaké osoby pod připravený text, aniž by ve skutečnosti daná osoba vědomě tento text podepsala.)

Příloha č.1

Právní důsledky zneužití elektronického podpisu

Odpovědnost podepisující osoby

Jak již bylo výše zmíněno, zákon obsahuje zvláštní právní úpravu odpovědnosti v souvislosti s porušením povinností podepisující osoby, tedy fyzické osoby, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby. V zákoně je totiž stanoveno, že za škodu způsobenou porušením povinností (vyjmenovaných v §5 odst. 1) odpovídá podepisující osoba podle občanského zákoníku. Odpovědnosti se pak podepisující osoba může zprostit, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Ve smyslu této zvláštní úpravy je pak pamatováno především na možnost zneužití elektronického podpisu ze strany třetích osob. V tomto smyslu je pak i konstruována odpovědnost podepisujících osob.

Jak již bylo zmíněno výše, autorství pravého odesílatele datové zprávy, tedy toho, čí vůle byla projevem vůle manifestována, tento zákon pochopitelně nezaručuje. Zákon nám zde pouze pomáhá potvrdit to, že datová zpráva byla elektronicky podepsána prostřednictvím dat, (případně prostředku) pro vytváření těchto podpisů a nikoli tedy to, že datovou zprávu podepsala osoba o které předpokládáme, že tak učinila. Takový případ je ostatně v některých směrech srovnatelný s krádeží (či nalezením) osobních dokladů a jejich následného zneužití (např. při zapůjčení osobního automobilu na základě těchto dokladů a jeho násl. odcizení). Hlavní problém pak spočívá ve složitém a mnohdy komplikovaném dokazováním, což v praxi jistě nebude bez komplikací. Nelze však vyloučit možnost, že se podaří jednoznačně prokázat, že datovou zprávu podepsala či naopak nepodepsala uvedená osoba (např. v e-mailu či na certifikátu). V praxi to ale nebude rozhodně bez komplikací

S ohledem na výše uvedená rizika, která se nepochybně snižují v závislosti na používání jednotlivých forem elektronických podpisů byl v § 5 odst. 1 je podepisující osoba povinna:

- zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu,
- podávat přesné, pravdivé a úplné informace poskytovateli služeb ve vztahu ke kvalifikovanému certifikátu.

Za prostředek zaručeného elektronického podpisu může být považován veškerý hardware potřebný k provedení samotného elektronického podpisu, za data zaručeného elektronického podpisu naopak veškeré programové vybavení, jehož je k podpisu užito. Co se rozumí náležitou péčí ve vztahu k výše uvedenému, není příliš snadné vyložit. Žádný zákon -a co je mi známo ani žádné soudní rozhodnutí- neobsahuje legální definici tohoto pojmu) Obecně však lze konstatovat, že jde o takové zacházení, které nejenom, že je na potřebné odborné úrovni, ale spočívá i v dodržování výše uvedených zásad. Dále je zde vyjádřena oznamovací povinnost ve vztahu k poskytovateli certifikačních služeb ohledně existence - byť sebemenší - možnosti hrozby nebezpečí zneužití programového vybavení, jehož je k podpisu užito. Výraz neprodleně je třeba chápat vzhledem k okamžiku zjištění samotné možnosti takové hrozby (a tedy subjektivně). Povinnost podávat (tedy i opakovaně) přesné, pravdivé a úplné informace poskytovateli služeb je zde stanovena pouze ve vztahu vůči kvalifikovanému certifikátu a nikoli tedy certifikátu běžnému, což se jeví jako poměrně zvláštní.

Za škodu způsobenou porušením jakékoliv z výše uvedených povinností se tedy odpovídá - až na jednu výjimku[1] - podle občanského zákoníku.

1 § 5 odst. 2 druhá věta zákona

Právní důsledky zneužití elektronického podpisu

Pokud je podpis prokazatelně (např. pomocí grafologa - soudního znalce) napsán vlastnoručně (nebo za použití el.podpisu), je to rozhodující důkaz stvrzující vůli provést určitý právní úkon (například uzavřít smlouvu). Lze tedy očekávat pozvolný nárůst důvěry a následného užívání, a to nejen v elektronických obchodech. O to však horší mohou být následky zneužití takovéhoto podpisu.

Samozřejmě ZoEP na jedné straně sice obsahuje celou řadu ustanovení směřujících k eliminaci takovýchto rizik, ale vyhnout se možnosti takového zneužití se nezdaří ani té nejlépe zformulované a vyvážené normě. Možností zneužití je celá řada, ve svých důsledcích si jsou ale velmi podobné (k popisu těchto útoků viz. výše).

U vlastnoručního podpisu je vždy šance, že grafolog (soudní znalec) padělek pozná a tím mne **zprostí vzniklé odpovědnosti**. U podpisu elektronického toto však možné není. Jak tedy bude probíhat dokazování, že vzniklou škodu jste nezpůsobili právě vy? A kdo v takovém případě tedy nese odpovídá za způsobenou škodu?

Odpověď (byť ne úplnou) nalezneme v zákoně č.40/1964 Sb. ČR v platném znění (**Občanský zákon**, dále jen OZ), jehož §34 a následující upravuji to, čemu se v našem právním řádu říká **právní úkon**. K tomu aby došlo ke vzniku, změně nebo zániku práv a povinností (a tedy jistému závazku) je třeba aby šlo o platný **právní úkon**.

V případě užití e-mailu musí být tento právní úkon (?) podepsán jednající osobou, jinak je neplatný (§40 odst. 3 OZ). E-mail je jednoznačně elektronický prostředek umožňující zachytit jak obsah právního úkonu, tak i jeho podpis (případně podpisy obou stran v jednou e-mailu). Právní úkon (dle § 34 OZ) zahrnuje následující pojmové znaky:

- **projevy vůle směřující ke vzniku, změně nebo zániku (zrušení) práv a povinností nebo ke způsobení jiných právních následků, které právní předpisy s takovými projevy vůle spojují**

Z uvedených znaků má -pro účely tohoto článku- klíčový význam ***jednota vůle a jejího projevu***. Projev vůle tedy musí zahrnovat dvě složky: **vůli a projev**. To znamená, že k tomu , aby vznikl právní úkon, je třeba, aby byly dány obě jeho základní složky, tj. **jak vůle, tak i její adekvátní projev**. Kdyby nebylo vůle (např. pro fyzické či jiné donucení), **nebylo by ani právního úkonu** a tedy -v našem případě- ani žádného přímého závazku. Právního úkonu by však nebylo ani tehdy, kdyby se nedostávalo projevu, stejně tak, kdyby projev vůle učinila jiná osoba, než ta, která právní úkon podepsala.

Vůli lze považovat za psychickou kategorii, která vyjadřuje *vnitřní psychický vztah jednajícího zamýšlenému (a tedy i chtěnému) následku*. (Vůli je třeba ale odlišovat od pohnutky /motivu/ a cíle právního úkonu. Pohnutka se stává právně významnou jen tehdy, bude-li zahrnuta do projevené vůle, když se stane její součástí. Cíl právního úkonu pak označuje jen výsledek, kterého chce jednající právním úkonem dosáhnout.) Požadavek existence vůle však **vyvolává některé problémy**.

Odhlédneme li od sporných otázek kolem **zjišťování, zda osoba projevila skutečně to, co projevit chtěla** (p*sychologické zkoumání toho, zda byla projevena skutečně adekvátní vůle není dost dobře možné*), je pro nás prvním takovým -a pro nás nepochybně nejdůležitějším- oříškem **zjišťování existence projevu vůle ve vztahu určitému subjektu**, tj. zjišťování, zda při určitém projevu vůle ten, kdo vůli projevil, ji skutečně i projevit měl, resp. zda jde o vůli toho, kdo ji projevuje, resp. jinak řečeno **zjištění, čí vůle se projevem vůle manifestovala**. Nález Ústavního soudu (č. 53, svazek 8), jasně říká, že **náležitostí vůle** jednající osoby je **svoboda a vážnost při jejím projevu při zachování absence omylu a tísně**. V občanském právu tyto dvě stránky vůle nelze zkoumat odděleně, protože ač jsou z teoretického hlediska oba atributy vůle rovnocenné, pro možnost posouzení náležitosti právního úkonu je rozhodnuti svoboda projevu vůle.

Pravidlem je, že **vůle projevená právním úkonem je vůle toho, kdo ji projevuje**. To však není bezvýjimečné. Pokud dojde ke zneužití soukromého klíče (např. v důsledku jeho neoprávněného zkopírování), **je nesporné, že nejde o právní úkon (právní úkon nebyl vůbec učiněn), ale o úkon protiprávní** (případně i o trestný čin **Poškození a zneužití záznamu na nosiči informací** dle § 257a Trestního zákona). To však bude třeba dokázat. **Problém tedy opět spočívá v určení osoby, která právní úkon skutečně učinila**.

ZoEP se poměrně snadno (s vydatnou pomocí asymetrické kryptografie, i když o žádné konkrétní technologii zákon nehovoří) vyrovnal s potenciální možností změny obsahu zprávy během jejího přenosu od autora k adresátovi. Možnost této změny je dnes již opravdu minimální. Co se ale týče opravdového autorství zprávy, tedy toho, **čí vůle se projevem vůle manifestovala, tak to zákon pochopitelně nezaručuje. ZoEP (PCS) nám zde pouze pomáhá potvrdit to, že zpráva byla podepsána autorovým soukromým (tajným ?) klíčem, který odpovídá jeho deklarovanému veřejnému klíči. - a nikoli to, že ji podepsala osoba, která je skutečným majitelem soukromého klíče**.

Takový případ je ostatně v některých směrech srovnatelný s krádeží (či nalezením) osobních dokladů (např. OP) a jejich následného zneužití (např. při zapůjčení osobního automobilu a jeho násl. odcizení). Dokazování v tomto směru vidím jako **poměrně problematické**. Předně proto, že si nedovedu dost dobře představit jak se soudy vypořádají s důkazními prostředky ve formě různých elektronických záznamů a posudky. Je sice pravdou, že některé části soudního řízení jsou založeny na **zásadě volného hodnocení důkazů**, která spočívá na skutečnosti, že soud provedené důkazy hodnotí podle svých vlastních závěrů (své úvahy) a v jejich vzájemné souvislosti. (viz. např. § 132 OSŘ). A je tedy opravdu možné, že by se v konkrétním případě podařilo dokázat, že datovou zprávu podepsala či naopak nepodepsala osoba uvedená na certifikátu. V praxi to ale nebude rozhodně bez komplikací.

Jak již bylo konstatováno výše, ZoEP působí jednak na PCS (PCS může ÚOOÚ na základě zákona uložit pokutu až do výše 10 000 000 Kč, příp. 20 000 000 Kč), ale také **na samotné -dle ZoEP se- podepisující osoby**. Nedodržení těchto povinností má poměrně závažné odpovědnostní důsledky. **Podepisující osoba je tedy povinna** (§5 odst. 1 ZoEP):

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,

c) podávat přesné, pravdivé a úplné informace poskytovateli služeb ve vztahu ke kvalifikovanému certifikátu.

Ad a) Za **prostředek zaručeného elektronického** podpisu může být považován *veškerý hardware potřebný k provedení samotného elektronického podpisu*, za **data zaručeného elektronického podpisu** naopak *veškeré programové vybavení, jehož je k podpisu užito*. Co se rozumí náležitou péčí ve vztahu k výše uvedenému není příliš snadné vyložit. (žádný zákon -a co je mi známo ani žádné soudní rozhodnutí- neobsahuje legální definici tohoto pojmu) Obecně však lze konstatovat, že jde o *takové zacházení, které nejenom, že je na potřebné odborné úrovni, ale spočívá i v dodržování výše uvedených zásad.*

Ad b) Zde je vyjádřena **oznamovací povinnost** ve vztahu k poskytovateli certifikačních služeb ohledně existence -byť sebemenší- možnosti hrozby nebezpečí zneužití programové vybavení, jehož je k podpisu užito. Výraz **neprodleně** je třeba chápat vzhledem k okamžiku zjištění samotné možnosti takové hrozby (a tedy subjektivně).

Ad c) **Povinnost podávat** (tedy i opakovaně) **přesné, pravdivé a úplné informace** poskytovateli služeb je zde stanovena pouze ve vztahu vůči kvalifikovanému certifikátu a nikoli tedy certifikátu běžnému. Význam tohoto ustanovení mi není zcela jasný. Buď tedy zákonodárce nabádá občany k tomu, aby všem ostatním poskytovatelům certifikačních služeb lhali, nebo se snaží v jistém smyslu degradovat ty poskytovatele, nad kterými nevykonává dohled ÚOOÚ. Možné jsou i obě varianty. Nemyslím, že by v případě porušením zde stanovené povinnosti (lhaní poskytovateli služeb ve vztahu ke kvalifikovanému certifikátu) mohlo dojít i k nedodržení §36 odst. 1 písm. d) zákona č. 200/1990 Sb. ČR o přestupcích v platném znění, a tedy uložit pokutu až do výše 3000 Kč.

Za škodu způsobenou porušením jakékoliv z výše uvedených povinností **odpovídá podepisující osoba podle OZ. Odpovědnosti se však** zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Pro případné zneužití soukromého klíče neoprávněnou osobou se jako nejpraktičtější jeví povinnost uvedená Ad a), jejíž nesplnění však automaticky neznamená, že za **způsobenou škodu odpovídá pouze podepisující osoba**, tedy ta, která je skutečným majitelem soukromého klíče

K odpovědnosti dle OZ (§ 420 a násl.) **je totiž zapotřebí splnění následujících znaků**:

a) Musí jít o protiprávní úkon

b) Muselo dojít k vzniku nějaké škody

c) Škoda je důsledkem protiprávního úkonu

d) V některých případech je zapotřebí i zavinění

Ad a) **Protiprávní úkon** je takový úkon, který je v rozporu s právním řádem. Tento znak tedy představuje určité porušení právní povinnosti. A to buď tedy naší (např. hromadné rozesílání svého soukromého klíče e-mailem - porušení §5 odst. 1 a) ZoEP a dalších norem zejména OZ), nebo osoby zneužívající náš soukromý klíč (byť by jej získala přímo do nás e-mailem) . V druhém případě přichází v úvahu **nejen odpovědnost občanskoprávní** (v důsledku porušení zejména § 415, §42 OZ a dalších), **ale i trestněprávní** (§ 257a TZ a další)

Ad b) Škodou se ve smyslu občanského práva rozumí **majetková újma (ztráta), kterou lze objektivně vyjádřit (vyčíslit) penězi**. Nemusí zde jít pouze o škodu skutečnou, ale i o ušlý zisk.

Ad c) Skutečnost, že **škoda musí být důsledkem protiprávního úkonu** vyjadřuje vztah aby mezi protiprávním úkonem na straně jedné a škodnou událostí na straně druhé existoval vztah příčiny a následku (příčinná souvislost).

Ad d) Při úpravě obecné odpovědnosti za škodu (dle § 420 a násl.) se vychází ze zavinění předpokládaného (nikoli tedy ze zavinění dokazovaného), což znamená, že **je to poškozený, kdo musí v jednotlivém případě prokazovat porušení právní povinnosti** (protiprávní úkon), dále **vznik a rozsah (výši) škody a příčinnou souvislost mezi způsobenou škodou a porušením právní povinnosti** (protiprávním úkonem). § 420 odst. 2 ale zároveň říká, že ".Odpovědnosti se občan zprostí, jestliže prokáže, že škodu nezavinil." Z toho tedy vyplývá, že se zde zavinění presumuje (předpokládá). Neprovede li úspěšně důkaz o vyvinění bude za škodu odpovídat. V této souvislosti zbývá pouze dodat, že se zde presumuje pouze nedbalost, a to navíc nedbalost nevědomá. Naproti tomu úmysl škůdce (např. § 424 OZ) musí poškozený škůdci vždy dokazovat.

Ve všech těchto věcech tedy spočívá **důkazní povinnost** (břemeno) na **poškozeném**. (a tedy buď ***na osobě, které byl elektronicky podepsaný e-mail adresován***, anebo **ne osobě, která je majitelem soukromého klíče, který byl zneužit**. Jak ale vyplývá z výše uvedeného, **dokazování v podobných věcech není rozhodně procházka růžovým sadem**.

V dnešní době nemusí být pro zkušeného experta vždy problém, kdykoliv se připojit k vašim přenosům, monitorovat je a takto zjistit potřebná hesla, snímat třebas i na dálku text psaný na klávesnici nebo zobrazovaný na monitoru. To však lze v rozumné míře považovat za nezbytné riziko. Co už se prokázat nemusí, je **selhání lidského faktoru ve formě neopatrnosti majitele soukromého klíče**. Rozhodně tedy doporučuji všem potenciálním uživatelům (ať "zaručených" nebo "obyčejných") elektronických podpisů aby si svůj soukromý klíč opravdu velmi pečlivě uschovali. Myslím, že pokud tak učiní, bude to dobře nejenom pro ně samotné, ale také pro samotný rozvoj e-mailů a internetového obchodu (komunikace) vůbec.

Příloha č.2

Základní přehled možných útoků

Zatímco klasický (ať již vlastnoruční či mechanickými prostředky učiněný) podpis umožňuje v zásadě jen málo druhů "útoků", zavádí elektronický podpis celou škálu nových možných metod a způsobů takových útoků.

"Klasický podpis" v zásadě umožňuje jen následující situace :
- někdo se snaží napodobit cizí podpis (padělání podpisu)
- někdo nechce uznat podpis, který skutečně vytvořil (odmítnutelnost podpisu)
- někomu se podaří získat podpis na "čistý" papír nebo "vymění několik stran" podepsaného dokumentu (integrita)
- osoba není schopna správně vyplnit podpisový vzor (např. při výběru peněz) (identifikace)

Nechceme se zde do hloubky zabývat teorií elektronického podpisu, ale každý, kdo se touto problematikou zabývá, ví že právě technika, která se používá, je zvolena tak, aby předchozí útoky na "klasický podpis" nebyly na elektronický podpis možné (nebo byly velice obtížné).

Přímo v definici zaručeného elektronického podpisu se říká, že je to takový elektronický podpis, který splňuje následující požadavky:
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Zaručený elektronický podpis tedy splňuje základní požadavky, které chceme, aby podpis v elektronickém světě měl - zachování integrity dokumentu po podepsání, identifikaci podepsané osoby a v neposlední řadě právní akceptovatelnost takovéhoto aktu .

Elektronický podpis však umožňuje teoreticky řadu nových typů útoků. Nejznámější je samozřejmě případ, kdy útočník získá data pro vytváření elektronického podpisu. Může se pak za tuto osobu podepsat a neexistuje žádný technický či technologický způsob ("elektronický grafolog"), jak takto padělaný podpis rozeznat od originálu.

Zatímco útok na klasický podpis má jen dva subjekty, na které lze útočit - osobu, která se podepisuje a osobu, která se spoléhá na podpis, elektronický podpis, který používá k předání dat pro ověření podpisu služeb nějaké třetí důvěryhodné strany (poskytovatele certifikačních služeb) - umožňuje zcela nový typ útoků - útok na poskytovatele certifikačních služeb.

Připravili jsme tabulku přehledu některých možných cílů útoků na elektronický podpis.

Pro jednoduchost si označme A (podepisující se osoba), B (osoba spoléhající se na podpis) , PCS (poskytovatel certifikačních služeb), X - útočník (tedy není to ani A,B nebo PCS). V tabulce dále označme : CRL - seznam zneplatněných certifikátů, DVEP - data pro vytvoření elektronického podpisu, EP - elektronický podpis, P - podpis).

Útočník/podvodník	Stručný popis útoku / pokusu o podvod	EP	P
A	tvrdí, že se nepodepsal	!	*
A	tvrdí, že text byl zaměněn	!	*
A	A zneplatní klíč u PCS a provede transakci, dříve než PCS vydá CRL, A pak odmítne odpovědnost za škodu		
A	tvrdí, že dokument, který podepsal dříve, vznikl až po zneplatnění DVEP, A se chce se zbavit odpovědnosti		
B	tvrdí, že je podepsán A	!	*
B	zamění část podepsaného textu	!	*
B	získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním		
A,B (domluví se)	A zneplatní klíč, než PCS vytvoří CRL , B provede transakci, škodu chce nahradit od PCS		
X	podepíše se za A	! 4	*
X	zamění text	!	*
X	získá DVEP a dále se může vydávat a podepisovat za A !!!		
X	Získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním (chce poškodit A)		
X	zneplatní u PCS certifikát A (poškodí A)		
X	X zachytí podepsanou zprávu (bez časového údaje), X ji odešle B znovu (cíl poškodit původního odesílatele nebo i příjemce)		
X	Získá u PCS certifikát za někoho jiného		
X (má k dispozici PCSX)	zamění certifikát PCS za PCSX u B a tím si umožní vydávat se za A (zasláním certifikátu, který si X vydal za A a podepsal jako PCSX) - dočasný útok	3	
X	získá osobní data zákazníků PCS		
PCS	zneplatní bezdůvodně certifikát A a tím jej poškodí		
PCS	vytvoří certifikát pro neexistující osobu		
PCS	vytvoří z dat v certifikátu A certifikát pro C (C i A mohou být poškozeny, B se totiž domnívá, že komunikuje s C nikoliv s A)		
PCS	při generaci klíčů pro A si PCS ponechá jeho DVEP		
PCS	úmyslně neuvede zneplatněný certifikát v CRL		
PCS	zneužije osobní data svých zákazníků		

* lze nalézt ekvivalenci u klasického podpisu
! definice ZEP by měla zabránit tomuto typu útoků, bez DVEP by neměl být možný
3 situace řešena v příloze č.3
4 jeden z možných útoků předveden v příloze č.4

Je vidět, že řada útoků na zaručený elektronický podpis, který se spoléhá na použití certifikátu, nemá obdobu v klasickém světě podpisů na listinu.

Příloha č. 3

Problémy spojené s certifikátem poskytovatele

Jestliže chceme v e-mailové komunikaci používat zaručené elektronické podpisy založené na certifikátech, je nutné pro jejich ověření nainstalovat certifikát vystavitele. Ověření elektronického podpisu se totiž skládá z kontroly neporušenosti obsahu zprávy (integrity), dále z kontroly, zda je certifikát platný (přesněji : zda nevypršel čas, na který byl vydán a zda není certifikát uveden na seznamu certifikátů, které byly zneplatněny) a dále z kontroly podpisu vystavitele certifikátu. Certifikát vystavitele potřebujeme i při kontrole seznamu certifikátů, které byly zneplatněny (tzv. CRL). Tento seznam je podepsán vystavitelem a při jeho ověření se používají data k ověření jeho elektronického podpisu uvedená v certifikátu poskytovatele.

Abychom mohli důvěryhodně ověřit certifikát podepsané osoby, je nutné mít k dispozici (nainstalovaný) skutečný (pravý, důvěryhodný) certifikát vystavitele certifikátu podepsané osoby.

V zákoně o elektronickém podpisu č. 227/2000 Sb. je v § 5 (Povinnosti podepisující osoby) odst. 2 uvedeno:

(2) …. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Každý, kdo ověřuje kvalifikovaný certifikát, by tedy jistě měl nejprve zjistit, zda certifikát poskytovatele (vydavatele certifikátu podepsané osoby) je platný a je skutečně vydán příslušným poskytovatelem.

Často se tento požadavek zjednodušuje na výklad, že je třeba získat certifikát poskytovatele důvěryhodným způsobem (nejlépe osobním převzetím na elektronickém nosiči).

A zde se setkáváme se dvěma problémy :

a) Lze získat důvěryhodným způsobem kvalifikovaný certifikát akreditovaného poskytovatele pouhým stažením z jeho www stránky ? A je tento způsob potom považován za dostatečný - není porušen § 5 zákona o elektronickém podpisu?
b) Pokud důvěryhodným způsobem získaný kvalifikovaný certifikát akreditovaného poskytovatele je nainstalován do PC, jsou tím již dostatečně splněny všechny povinnosti, které souvisí s implementací takového certifikátu? Není třeba provést (provádět) ještě nějaké jiné činnosti?

Než na tyto otázky odpovíme, popíšeme ještě další problém.

c) Představte si, že někdo cizí získá přístup k vašemu počítači a jednoduše smaže (nebo jen přidá!) z úložiště certifikátů certifikát (akreditovaného) poskytovatele certifikačních služeb a uloží do něj certifikát, který si předem připravil. Tento certifikát bude formálně obsahovat všechny položky stejné jako smazaný certifikát - včetně jména vydavatele. Lišit se bude samozřejmě v podpisu vydavatele/útočníka a dále v datech na ověření podpisu vystavitele. Od této chvíle budeme považovat (resp. náš software) za důvěryhodné i ty elektronické podpisy, kterým vydal certifikát dotyčný útočník. Pokud se podíváme pouze na jméno vydavatele - budeme si myslet, že se jedná o poskytovatele, kterému jsme důvěřovali, a proto jsme si jeho certifikát do svého počítače nainstalovali.

V případě, že se jedná o komunikaci podle zákona o elektronickém podpisu, musíme mít k dispozici nějakou možnost, jak rychle zkontrolovat, že nainstalovaný kvalifikovaný certifikát poskytovatele resp. akreditovaného poskytovatele je skutečně ten, který příslušný poskytovatel používá pro podpisy jím vydaných kvalifikovaných certifikátů a k podpisu seznamu kvalifikovaných certifikátů, které byly zneplatněny.

Odpověď na všechny tři problémy a), b) a c) není úplně jednoduchá - osoba spoléhající se na podpis by měla ve vlastním zájmu kontrolovat, zda jím implementovaný kvalifikovaný certifikát (akreditovaného) poskytovatele je skutečně tímto poskytovatelem vydán a je tedy autentický. Ze zákona však přímo nevyplývá povinnost ověřit či ověřovat kvalifokovaný certifikát poskytovatele. Rychlý, jednoduchý a pitom důvěryhodný způsob jak toto kontrolovat, je založen na využití ověření kvalifikovaného certifikátu akreditovaného

poskytovatele, který provedl Úřad pro ochranu osobních dat ve smyslu § 10 odst. 7 zákona č. 227/2000 Sb.

Ve zbývající části uvedeme potřebné informace a postup, jak by mohl ten, kdo se spoléhá na zaručené elektronické podpisy založené na kvalifikovaných certifikátech od akreditovaného poskytovatele (tedy podpisy podle § 11 zákona o elektronickém podpisu používané v oblasti veřejné moci) toto provádět.

Ověření kvalifikovaného certifikátu akreditovaného poskytovatele Úřadem

Úřad pro ochranu osobních údajů (dále Úřad) ověřil ve smyslu § 10 odst. 7 zákona č. 227/2000 Sb., elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) kvalifikovaný certifikát akreditovaného poskytovatele certifikačních služeb První certifikační autority, a.s. Výsledek zveřejnil na své webové stránce www.uoou.cz a ve Věstníku Úřadu č.17.

Poř. čís.	Ověření kvalifikovaného certifikátu poskytovatele			Věstník ÚOOÚ č.
	Subjekt:		Adresa:	
1.	První certifikační autorita, a.s., identifikační č. 26 43 93 95		Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	17
Výsledky ověření:				
A.	Jméno:	qica_root_cert_20020321.pem	Délka: 2265	Poslední změna: 22. 3. 2002 v 11:14 hod.
	Formát certifikátu:		Otisk:	
	PEM	SHA-1	4BFB ED36 68FC 2B0A B729 8EC0 53B5 3649 6E15 0AAE	
		MD5	297C 49A7 B63C B15A F3B7 0F45 2D3B 5132	
B.	Jméno:	qica_root_cert_20020321.der	Délka: 1630	Poslední změna: 21. 3. 2002 v 21:02 hod.
	Formát certifikátu:		Otisk:	
	DER	SHA-1	6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE	
		MD5	C3F3 5AB5 24C7 9276 634B 4DB4 E86A FE57	
C.	Jméno:	qica_root_cert_20020321.txt	Délka: 6256	Poslední změna: 22. 3. 2002 v 11:18 hod.
	Formát certifikátu:		Otisk:	
	TXT	SHA-1	AC46 FB40 E929 F12D 758A 0B8E 0192 516B 1B65 6C8A	
		MD5	5EAC 0082 F5F5 9E3D EAB4 0FE6 27BE 5ED2	

V podmínkách udělení akreditace pro poskytování certifikačních služeb (§ 10 zákona č. 227/2000 Sb.) v odstavci 7 je uložena následující povinnost :

"Součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem".

V praxi to znamená, že akreditovaný poskytovatel certifikačních služeb předloží Úřadu všechny své kvalifikované certifikáty, které chce používat, a to ve všech formátech, které nabízí (zpravidla DER, TXT a PEM, případně EDI). Jedná se o kvalifikované certifikáty poskytovatele, které je nutné instalovat do uživatelských aplikací a které slouží k ověření podpisů kvalifikovaných certifikátů a CRL (seznamu kvalifikovaných certifikátů, které byly zneplatněny). Těmto certifikátům musí uživatel důvěřovat a měl by je získat nějakým důvěryhodným způsobem. Poskytovatel (zjednodušeně řečeno) nesmí používat pro výše uvedené účely jiné než tyto ověřené kvalifikované certifikáty.

Otisky zveřejněné Úřadem byly počítány z obsahu celého souboru - certifikátu v příslušném formátu, a to podle následujících standardů:

SHA-1 (National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-1, April 17, 1995)
a
MD5 (Request for Comments: 1321, The MD5 Message-Digest Algorithm, R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992).

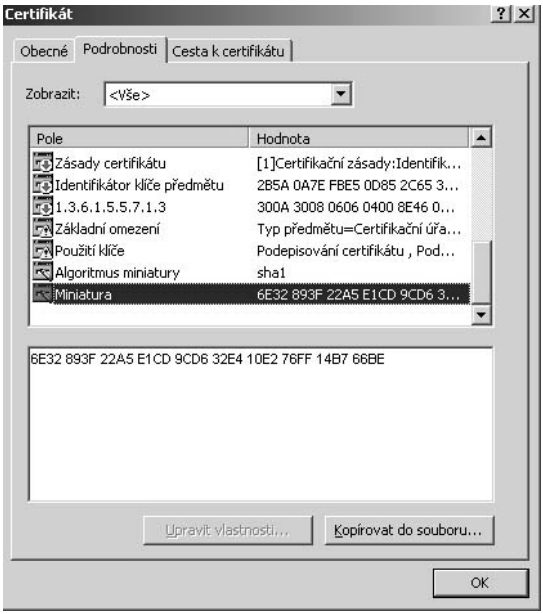
Možná kontrola kvalifikovaného certifikátu akreditovaného poskytovatele osobou spoléhající se na podpis (resp. podepisující se osobou)

Zveřejněné otisky ověřených kvalifikovaných certifikátů akreditovaného poskytovatele slouží k tomu, aby před instalací kvalifikovaného certifikátu akreditovaného poskytovatele certifikačních služeb byla možnost porovnáním otisků zjistit, zda:

- kvalifikovaný certifikát byl skutečně ověřen Úřadem,

- zda kvalifikovaný certifikát byl vydán příslušným akreditovaným poskytovatelem certifikačních služeb,

- zda se jedná o kvalifikovaný certifikát, který "certifikuje" data pro ověřování elektronického podpisu, kterým odpovídají data pro vytváření elektronického podpisu, kterými akreditovaný poskytovatel "podepisuje" vydávané kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny.



Obr. 1 - Kvalifkovaný certifikát poskytovatele

Tuto kontrolu je nutné provádět i následně. Jejím smyslem je ochrana proti možným útokům popsaným v úvodu pod body a), b) a c).

V případě kvalifikovaného certifikátu poskytovatele (v nejběžněji používaném formátu DER) se můžete velice jednoduše přesvědčit, zda máte stažený/nainstalovaný certifikát ověřený Úřadem. Stačí v některém z viewerů (např. v systémovém prohlížeči nebo přímo v programech MS Outlook, MS Internet Explorer) otevřít certifikát, o němž chceme rozhodnout, zda je či není ověřen Úřadem. Zobrazí se nám následující (nebo jemu velice podobný - podle verze produktu) výsledek - viz. obr. 1.

V položce "miniatura" pak najdeme otisk certifikátu. Použitá hashovací funkce je uvedena v položce "algoritmus miniatury" (zpravidla SHA-1). Nyni stačí porovnat tento otisk s otiskem uvedeným ve Věstníku Úřadu, resp. s otiskem, který je zveřejněn na webovské stránce Úřadu, nebo jej máte z jiného zdroje - např. z tohoto sborníku. Věstník Úřadu lze považovat za důvěryhodný zdroj, další zdroje mají pochopitelně spíše informativní povahu.

Pro otisk kvalifikovaného certifikátu První certifikační autority a.s. ve formátu DER je uvedena v těchto zdrojích hodnota: 6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE.

Porovnáním zjistíme, že tato hodnota je shodná s údajem v miniatuře - jedná se tedy o kvalifikovaný certifikát poskytovatele, který byl ověřen Úřadem. Na takovýto certifikát se můžete spolehnout a nic nebrání jeho instalaci.

Pro porovnání certifikátů v ostatních formátech potřebujete k výpočtu otisků použít některou z dostupných aplikací. Takto vypočtený výsledek opět jednoduše porovnáte s hodnotou otištěnou ve Věstníku. Úřad připravuje zveřejnění vhodné aplikace pro výpočet otisků certifikátů pomocí hashovacích funkcí SHA-1 a MD5 na své webovské stránce (http://www.uoou.cz).

Příloha č.4

Jak získat podpis k textu od jiné osoby

(pomocné programy RSAM, Equation budou k dispozici společně s prezentací na CD)

Předvedeme si, jak lze za jistých okolností získat podpis nějaké osoby pod (námi připravený) text, aniž by ve skutečnosti daná osoba vědomě tento text podepsala.

Pro srozumitelnost výkladu zvolme následující jednoduché podpisové schéma. (Útok však lze realizovat v určitých obměnách i na skutečně používaných podpisových schématech SHA1/RSA, MD5/RSA apod.).

Podpisové schéma Security 2002

(V podstatě se jedná o klasické podpisové schéma, kde je však vynechána hashovací funkce a text není formátován podle PKCS #1.5, ale podle námi zadaných pravidel, která nazveme Security #2002).

Vyjdeme z klasického RSA. Zvolíme prvočísla p a q a vypočteme

$$N = p*q$$

$$\Phi(N) = (p-1)*(q-1)$$

Dále zvolíme náhodné číslo e, kde

$1 < e < \Phi(N)$, takové, že e a $\Phi(N)$ jsou nesoudělná.

Vypočteme číslo d takové, že

$1 < d < \Phi(N)$ a

$e*d \equiv 1 \bmod \Phi(N)$.

Dvojici (N,d) nazveme soukromý - tajný - podpisový klíč a (N,e) veřejný klíč - data na ověření podpisu.

Podpis zprávy M

Zprávu M překódujeme nejprve do číselného tvaru. K tomu použijeme některou vhodnou převodovou tabulku. Např. tuto tabulku:

	0	1	2	3	4	5	6	7	8	9
6	**0**	**Mezera**	**2**	**3**	**4**	**A**	**B**	**C**	**D**	**E**
7	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
8	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
9	**Z**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Zprávu M pak zformátujeme do posloupnosti čísel pevné délky (délka bude rovna délce modulu N). K tomu použijeme vlastní formátování Security#2002:

Formátování Security#2002 :

1) Má-li modul délku k, budeme zprávu v dekadickém tvaru dělit na skupiny délky k-1.
2) Všechny skupiny musí mít délku k-1, nemá-li poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
3) Skupiny nyní doplníme zleva jednou nulou. Délka každé skupiny je tedy rovna k.
4) Výsledek po podpisové transformaci má délku rovnou maximálně k, nemá-li ji doplníme výsledek zleva nulami.

Získaný výsledek po formátování M označme M = m1 m2 m3 .....

Podpisem zprávy M pak nazveme řetězec

P = C1 C2 C3 ..... , kde

$C1 \; m1^d \bmod N$, $C_2 \; m2^d \bmod N$, $C_3 \; m3^d \bmod N$ ..... $Ci \equiv mi^d \bmod N$

Ověření podpisu zprávy M se pak provede tak, že vypočteme pomocí dat na ověření podpisu následující výrazy

$V1 \equiv C1^e \bmod N$, $V2 \; C2^e \bmod N$, $V3 \; C3^e \bmod N$ .... $Vi \; Cie \bmod N$

Pokud Vi = m i pro všechna i, řekneme, že ověření podpisu bylo úspěšně provedeno.

Pokud podepisující osoba dokáže udržet svá data na podepisování v tajnosti (a čísla p a q byla dostatečně velká), pak je výpočetně složité ze znalosti podpisu zprávy a dat na ověření podpisu vypočítat soukromý - podepisovací klíč.

Nyní si ukážeme, jak lze získat podpis majitele soukromého klíče (N,d) pod zprávu M, aniž by majitel soukromého klíče tuto zprávu sám přímo podepsal.

Celá myšlenka je založena na tom, že RSA je distributivní vzhledem k násobení, protože platí: $\forall \; a,b \in Z$, $k \in N : (ab)^k \; a^k b^k \bmod N$.

Postup

Mějme zprávu M, ke které chceme získat podpis nějaké osoby (Boba), tj. hodnotu $M^d \bmod N$. Bobovi předložíme místo vlastní hodnoty M , kterou by Bob mohl z pochopitelných důvodů odmítnout podepsat, (zdánlivě) náhodnou hodnotu X. Tuto hodnotu X však předem pečlivě připravíme a to jako $M \, c^e \bmod N$. Zde c je

náhodně zvolená veličina, (N,e) veřejný klíč Boba, M zpráva. Pokud Bob takovýto zdánlivě "nesmyslný" text podepíše a my se k výsledku dostaneme, pak jsme schopni poměrně jednoduše vypočítat podpis Boba pro zprávu M.

Vše si ukážeme na konkrétním příkladě:

Nejprve vytvoříme nějaký Bobův soukromý a veřejný klíč.

Zvolíme prvočísla: p=47, q=71,

Spočteme modul : N= p*q = 47*71 = 3337

a dále: $\Phi(N) = (p-1)*(q-1) = 46*70 = 3220$

Zvolíme veřejný exponent e (nesmí mít společné dělitele s 3220) , volíme např. 79

Spočteme soukromý exponent d:

d …… 79*d ≡1 mod 3220

d 79^{-1} mod 3220

d = 1019

(k výpočtu použijeme Eukleidův algoritmus)

Získali jsme:
e ……. veřejný klíč (3337, 79) ,
d ……. soukromý klíč (3337, 1019)

Chceme získat Bobův podpis pod zprávu M=DLUH JE 10 USD
Nejprve si převedeme pomocí kódové tabulky text zprávy M do číselné posloupnosti .
M= D L U H J E 1 0 U S D
M= 68 76 85 72 61 74 69 61 91 60 61 85 83 68

M dále zformátujeme podle pravidla Security#2002 na bloky m1 m2 m3 …..
M = m1 m2 m3 ….. = 0687 0685 0726 0174 0696 0191 0606 0185 0836 0800

Předpokládejme, že Bob má k dispozici program / prohlížeč, který by mu tuto zprávu zobrazil jako : DLUH JE 10 USD

Kdyby Bob podepsal pomocí svého soukromého klíče d tuto zprávu
(tj. spočtel M^d mod N, pro N=3337, d=1019) dostaneme (RSAM):

1592 0585 1494 3172 644 3080 0647 1855 0707 1740 (*).

Naším cílem je tedy získat tuto posloupnost jiným způsobem, tedy bez toho, že bychom použili Bobův soukromý klíč.

K tomuto účelu si připravíme zprávu jinou.

Zvolíme nějaké libovolné číslo c, např. 105 a dále spočteme číslo $x \equiv c^e \bmod N$.
Pro konkrétní hodnoty Bobova veřejného klíče dostaneme $x \equiv 105^{79} \bmod 3337 \equiv 193$.
Dále připravíme k podpisu (zdánlivě) náhodnou nic nevyjadřující hodnotu M c^e mod N.

Pro naše konkrétní hodnoty spočteme (využití standardní kalkulačky ve Windows):
M = m1 m2 m3 ….. = 687 685 726 174 696 191 606 185 836 800
M c^e mod N = m1 c^e mod N m2 c^e mod N m3 c^e mod N ….. =
687*193 mod 3337 685*193 mod 3337 726*193 mod 3337 …..

M	0687	0685	0726	0174	696	0191	0606	0185	0836	800
M c^e mod N	2448	2062	3301	0212	848	0156	0163	2335	1172	898

Bob svým prohlížečem vidí text, který zdánlivě nemá žádný smysl. Po ukázce, jak se text dá elektronicky podepsat, jej požádáme o podpis připraveného textu (" slovy aby nám ukázal jak se umí elektronicky podepsat…"). Pochválíme jej a text, včetně podpisu si "schováme" na památku.

Vraťme se k našemu příkladu. Text, který jsme připravili, je tento:

M c^e mod N 2448 2062 3301 0212 848 0156 0163 2335 1172 898

Nyní jej předložíme Bobovi k podpisu. Ten vidí nesmyslný obsah a text proto klidně podepíše. Bob tedy spočte $(M*c^e)^d$ mod N a dostane (RSAM):

0310 1359 0031 2697 880 3048 1195 1229 0821 2502

Nyní použijeme trochu matematiky (řada kroků je vynechána nebo jen naznačena):
$(M\ c^e \bmod N)^d \bmod N \quad M^d * c^{ed} \bmod N \quad M^d * c \bmod N$ (využito $e*d \equiv 1 \bmod \Phi(N)$)
Výsledek lze zapsat jako $M^d * c \bmod N$.

Pokud se k tomuto podpisu dostaneme, lze ze znalosti hodnoty $Md * c \bmod N$ a hodnoty C vypočítat podpis zprávy M tj. hodnotu $Md \bmod N$

K tomu potřebujeme postupně řešit následující soustavu modulárních rovnic:

$0310 \equiv 105 * M^d \bmod 3337$

$1359 \equiv 105 * M^d \bmod 3337$

$0031 \equiv 105 * M^d \bmod 3337$

$2697 \equiv 105 * M^d \bmod 3337$

….

$2502\ 105 * M^d \bmod 3337$
(K řešení těchto rovnic je potřeba napsat krátký program. Lze poměrně snadno realizovat i pro velká čísla.)

```
Procedure Equation;

Begin

writeln('Reseni modularni rovnice A=C*X mod N pro ruzna A');

      j:=0; M:=1;
    repeat
      inc(j);
      M1:=C*j-A;
      if M1>0 then
      begin
        M2:=((c*j-A) div N)*N;
        M:=M1-M2;
      end;
    until M=0;
    writeln('A=C*X mod N, X=',j);
end;
```

Jejich vyřešením (Equation) dostaneme následující hodnoty. Označíme je jako posloupnost (**).

1592 0585 1494 3172 644 3080 0647 1855 0707 1740

Posloupnost (**) je Bobův podpis zprávy M = DLUH JE 10 USD (viz. posloupnost * z úvodu této přílohy).

Našli jsme tedy postup, jak ke zprávě M získat podpis a to bez toho, že by Bob zprávu vědomě podepsal, a výpočet jsme provedli bez znalosti Bobova soukromého klíče (dat na vytvoření elektronického podpisu).

Literatura:

[1] Vondruska, P., Matejka, J.: The basic terms and legal aspects of the ESA from the practical use and security points of view, sborník mezinárodní konference IDET, Brno 2001

[2] Vondruška,P.: Bezpečnost elektronického podpisu, sborník Konference Security 2001, Praha

[3] Vondruška,P.: Ověření certifikátu poskytovatele, Crypto-World 5/2002

[4] Vondruška,P.: Jak získat podpis k textu od jiné osoby, Crypto-World 12/2001

[5] Vondruška,P.: Asymetrický šifrovací algoritmus RSA (využití a zneužití), přednáška 6.3.2002, Laboratoř inteligentních systémů, VŠE, Praha

BEZPEČNOST MOBILNÍCH ZAŘÍZENÍ VE SVĚTLE NOVÝCH APLIKACÍ

Petr Hanáček, FIT VUT Brno, Božetěchova 2, 612 66 Brno,
e-mail: hanacek@fit.vutbr.cz

Klíčová slova:
mobilní zařízení, GSM, GPRS, PDA, čipové karty, bezpečnost kryptografických modulů.

Abstrakt: *Příspěvek se zabývá problematikou bezpečnosti mobilních zařízení (mobilních telefonů, PDA atd.), které jsou využity pro aplikace, citlivé z hlediska bezpečnosti. Mezi tyto aplikace patří například bankovní aplikace, aplikace pracující s osobními daty a aplikace vzdáleného přístupu. Při jejich provozování je třeba se zabývat otázkami, jak lze důvěřovat jednotlivým zařízením, v čí prospěch které zařízení pracuje a zda důvěra v některá zařízení není již neopodstatněná..*

1 Zájmy ve světě mobilních zařízení

Abychom lépe pochopili problematiku bezpečnosti mobilních zařízení, je třeba se podívat blíže na zájmy jednotlivých stran u mobilních aplikací a na to, kdo je hájí. Představme si systém, který používá např. mobilní telefon pro komunikaci a pro provádění platebních operací s bankou. V tomto systému jsou tři subjekty (uživatel, mobilní operátor a banka), kteří spolu pomocí různých zařízení komunikují a jejichž cílem je v tomto systému provést platbu. Tyto tři subjekty však mají v tomto systému zcela rozdílné a principielně protichůdné zájmy. Podstatnou část transakce však provádí mobilní telefon. Čí zájmy tento telefon hájí? Zájmy uživatele, operátora nebo banky? Samozřejmě musí hájit zájmy všech tří stran, avšak rozdílným způsobem. Především musí hájit zájmy uživatele, protože uživatel ho vlastní a pokud by telefon jeho zájmy nehájil, uživatel jej zahodí. Stejně tak však musí bezpečným způsobem hájit i zájmy operátora a banky. Protože telefon je však v držení uživatele, musíme najít prostředek, který umožní, aby telefon také hájil zájmy nepřítomného operátora a banky na dálku. Za tímto účelem musí mít telefon jisté zařízení, které je před uživatelem bezpečné a dovolí hájit zájmy jiných stran v jeho telefonu. Tímto zařízením je u mobilních telefonů *SIM modul* (zkratka SIM znamená Subscriber Identity Module), který je v podstatě čipovou kartou. Tento SIM modul hraje v mobilním telefonu roli tzv. **bezpečného kryptografického modulu**.

Obr. 1. Čí zájmy hájí různá zařízení

2 Bezpečné kryptografické moduly - čipové karty

Nejčastější implementací bezpečných kryptografických modulů jsou čipové karty. Čipové karty totiž poskytují velmi levnou implementaci jednoho z bezpečnostních konceptů, který se anglicky nazývá "tamper resistant hardware". Tento pojem je možno přibližně přeložit do češtiny jako "hardware odolný proti fyzickému útoku" nebo "bezpečný hardware". Bezpečný hardware je hardwarový modul, obvykle vybavený mikroprocesorem, který obsahuje nějaká chráněná data a algoritmy, které na základě příkazů z vnějšího světa s těmito daty manipulují.

Tato vlastnost se obvykle využívá dvojím způsobem:

1. Bezpečný hardware v sobě obsahuje data, se kterými je možno manipulovat pouze jistým způsobem. Příkladem může být předplatní (telefonní) telefonní čipová karta, která v sobě obsahuje čítač impulsů (chráněná data), který je možno pouze snižovat a nikdy ne zvyšovat.

2. Bezpečný hardware má v sobě tajný kryptografický klíč, který nikdy nevypustí ven a je pouze ochoten s tímto klíčem provést jistou kryptografickou operaci (například zašifrovat data zaslaná z vnějšího světa). Příkladem může být autentizační čipová karta, která prokazuje svou totožnost pomocí zašifrování vložených dat uloženým tajným klíčem. Tomuto typu bezpečného hardware se někdy také říká kryptografický bezpečný hardware.

Co je na výše uvedených vlastnostech čipové karty tak zvláštního? To, že tyto vlastnosti nelze implementovat čistě softwarově bez pomocí speciálního hardware. Např. výše uvedenou předplatní kartu nelze realizovat softwarově, protože útočník by prostě pomocí binárního editoru přepsal obsah čítače na libovolnou hodnotu a měl by tak nevyčerpatelný zdroj bodů nebo impulsů. Stejně tak softwarová implementace kryptografického bezpečného hardware nemůže dostatečně ochránit tajný kryptografický klíč - pokud bude klíč sebelépe uložen v programu, útočník jej tam vždy najde.

2.1 Security through obscurity

Velmi rozšířeným jevem, se kterým je možno se setkat u čipových karet, je utajování algoritmů. Algoritmy, použité v aplikacích s čipovými kartami (kryptografické i nekryptografické) bývají poměrně často utajovány nebo aspoň "nezveřejňovány". Děje se tak v daleko větší míře než u softwarových aplikací. Proč tomu tak je? Důvodem je to, že vlastnost bezpečného hardware (tj. ochránit "chráněná data" před neoprávněným přístupem) se dá velmi snadno využít i pro ochranu použitých algoritmů před prozrazením. Zatímco u čistě softwarového systému nelze efektivně utajit žádný algoritmus, protože nakonec to vždycky někdo "zreverzuje" a zveřejní (o čemž svědčí příklad kdysi utajovaných kryptografických algoritmů RC2 a RC4), u hardwarového systému tato možnost existuje. A vývojáři aplikací s čipovými kartami ji také zhusta využívají. Zvlášť v minulých letech panovaly v této oblasti až paranoidní názory. Nejen že se utajovaly algoritmy, kryptografické protokoly a datové struktury, ale "nezveřejňovaly" se i samotné příkazy čipových karet. Zvláště komické bylo to, že čipové karty se dodávaly pouze "spolehlivým" a "prověřeným" odběratelům, po podepsání různých závazků a prohlášení doprovázených vysokými smluvními pokutami.

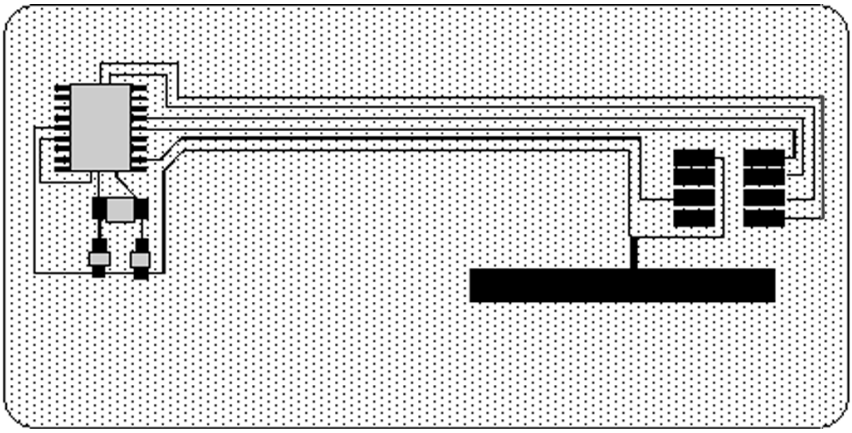
Tento způsob zabezpečení, zvaný "security through obscurity", což znamená přibližně "zabezpečení pomocí zatemnění", je svou účinností asi tak bezpečný, jako ukládání klíče pod rohožku. Samozřejmě, pokud se celá domácnost domluví, že klíč bude pod rohožkou a nikdo o této dohodě neví, je tento způsob bezpečný. Ale stačí, aby jediný člen domácnosti byl viděn, jak ukládá klíč pod rohožku a bezpečnost je okamžitě zkompromitována. Je pak třeba změnit algoritmus (např. ukládat klíč pod květináč).

V současné době, kdy se snažíme o maximální interoperabilitu, o standardizaci a o veřejný audit algoritmů, je způsob zabezpečení "security through obscurity" považován za nevhodný a v běžných softwarových aplikacích se vyskytuje stále méně. Dokonce i v oblasti čipových karet je vidět jistý posun od utajovaných algoritmů a protokolů k veřejným. Svědčí o tom jak silná standardizace (kde standard samozřejmě nemůže být tajný) tak také například technologie JavaCard (která znamená čipovou kartu, programovanou v jazyce Java), která je zcela veřejná.

2.2 První nesmělé pokusy - emulace telefonních karet

První pokusy o útoky na čipové karty se vyskytly v oblasti telefonních karet. Telefonní karta typicky není procesorová karta, ale jde o kartu se speciální logikou. Současná telefonní karta ani není vybavena žádnou kryptografií (ale v blízké budoucnosti pravděpodobně bude). Telefonní karta má nějaký elektrický protokol, kterým říká své identifikační číslo a počet impulsů, které ještě na ní zbývají. Tento protokol samozřejmě není utajován a každý, kdo vyvine určitou energii si jej může opatřit. Pak ovšem platí, že jakékoli zařízení, které odpoví na dotazy telefonního automatu a bude dodržovat tento protokol, bude telefonním automatem akceptováno jako platná telefonní karta. Tím je také dáno, že nejčastějším útokem na telefonní karty je tzv. emulace. Spočívá ve vytvoření zařízení (emulátoru), které se chová z hlediska elektrického protokolu jako platná telefonní karta s jediným rozdílem - neklesá na něm počet impulsů.

Konstruktéři stávajícího systému telefonních karet se ani nesnažili o nějaké lepší zabezpečení - bezpečnost systému totiž spočívá v tom, že cena emulátoru je natolik vysoká, že neodpovídá zisku útočníka. Což poměrně slušně platí ve Francii nebo v Německu, ale už méně to platí v naší republice nebo ještě dále na východ. Existence emulátorů - "věčných telefonních karet" - v tomto případě tudíž neznamená selhání bezpečnostního mechanismu, ale selhání člověka, který vzal systém, vytvořený pro konkrétní provozní prostředí a bez provedení bezpečnostní analýzy jej přemístil do provozního prostředí zcela jiného.



Obr. 2. Hackerská telefonní karta (Phrack Magazine, Volume 7, Issue 48, Electronic Telephone Cards: How to make your own!)

2.3 Hackerství jako obchod - satelitní karty

Emulace telefonních karet v praxi neznamená vážné ohrožení napadeného systému. "Věčných telefonních karet" je poměrně málo, provozovatel systému je zahrne do procenta svých ztrát a pro hackery není tato oblast příliš populární. Není příliš technicky zajímavá, prodávání věčných karet je riskantní, nedá se na tom získat sláva (protože to umí každý, kdo je trochu kutil v elektronice) a především nedá se na tom vydělat.

Hacker potřebuje oblast, která je pro něj intelektuální výzvou, dá se na ní získat sláva, má z ní jistý okamžitý prospěch, činnost je beztrestná a pokud možno se na tom dají vydělat peníze. Tyto podmínky přesně splňují satelitní šifrovací karty.

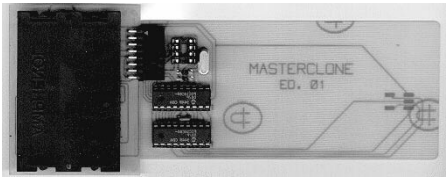
Satelitní karty slouží pro dekódování satelitních televizních programů, které jsou vysílány zakódované (správně by se mělo říkat zašifrované) a které jsou určeny pouze pro ty diváky, kteří si za nemalý peníz koupí odpovídající dekódovací kartu. Dekódovací karta je čipová karta, která v sobě obsahuje tajný klíč (nebo několik klíčů) a šifrovací algoritmus, který je někdy tajný a někdy veřejný. Satelitní přijímač do karty občas zasílá krátkou zprávu, kterou karta pomocí klíče dešifruje a tím se získá tajná hodnota, se kterou je možno dekódovat několik dalších sekund obrazu. Je jasné, že pokud by byl prozrazen klíč (a algoritmus), je možno opět vytvořit emulátor karty, jehož pomocí je možno dekódovat přijímaný signál.

Pokud je takový emulátor (obvykle nazývaný pirátská karta) prodáván za rozumnou cenu, může se stát masově prodávaným zbožím. A to se právě stalo. Během několika málo let se vytvořil takříkajíc průmysl na výrobu pirátských čipových karet, který plynule zásobuje své zákazníky kartami. A nejde o malé počty. Jenom počet pirátských karet pro šifrovací systém Videocrypt se odhaduje na 250 000 až 500 000 kusů. Provozovatelé satelitního vysílání s tímto jevem samozřejmě intenzivně bojují. Pravidelně (např. jednou za dva roky) mění karty a jejich algoritmy, daleko častěji mění kryptografické klíče a používají také drobné technické změny v protokolu, zvané ECM (zkratka od Electronic CounterMeasure). Výsledkem je neustálý závod mezi provozovateli a výrobci pirátských karet, kteří musí zjišťovat nové algoritmy (typicky jim to trvá několik týdnů) a nové klíče (obvykle do hodin nebo několika dní).

Samotná existence satelitních pirátských karet není z globálního pohledu příliš závažná. Týká se několika málo společností (které si tento stav zavinily samy) a jiných technologických odvětví se tato činnost příliš netýká, protože kromě satelitní televize se tímto způsobem čipové karty prakticky nepoužívají. Problém je zcela jiný, a mnohem závažnější. Tak, jak provozovatelé satelitního vysílání postupem let začínali u slabých bezpečnostních algoritmů a postupovali k silnějším, vytvářela se zde souběžně s tím komunita hackerů, která byla zpočátku poměrně bezmocná, ale postupem času se na satelitních kartách "naučila" útočit na stále lepší čipové karty. Satelitní čipové karty se staly školou, na které se vyučili vysokým schopnostem hackeři, kteří by se jinak pravděpodobně vůbec nepustili do útoků na čipové karty. Současný stav je takový, že struktura komunity firem (ano, čtete dobře, firem, nikoli jednotlivců), které se zabývají výrobou satelitních pirátských karet je několikaúrovňová. A v nejvyšší úrovni se nacházejí firmy, které nevyrábějí samotné pirátské karty, to nechávají firmám na nižší úrovni, ale které provádějí zjišťování utajených algoritmů a tajných klíčů. Při této činnosti využívají chyb v algoritmech a protokolech, nedostatečnou fyzickou bezpečnost čipů a v případě nutnosti si mohou pronajmout i laboratorní technologii. Průmysl pirátských karet tyto výdaje hravě zaplatí.

Právě tím, že provozovatelé satelitního vysílání umožnili (a nepřímo zaplatili) vytvoření těchto firem, prokázali medvědí službu ostatním uživatelům čipových karet.

Obr. 3. Ukázka vybavení hackerů satelitních karet - "Battery Card " satelitních karet -"Blocker" a "Phoenix"



Obr. 4. Ukázka vybavení hackerů

2.4 Levné útoky na kryptografické moduly

Ve výše uvedeném příkladě bylo již naznačeno, že v některých případech je možné narušit fyzickou bezpečnost čipu čipové karty - tedy porušit donedávna všeobecně uznávané dogma o absolutní bezpečnosti karet. Bylo by proto vhodné si ukázat příklady některých útoků, kterými může útočník tohoto cíle dosáhnout.

Asi nejjednodušším způsobem, jak "obelstít" čipovou kartu, je využít některé chyby v software čipové karty. Přestože se může zdát, že pravděpodobnost chyby v software je velmi malá opak je pravdou. V software čipových karet se vyskytují často jak funkční chyby (např. špatná kontrola mezních hodnot parametrů některých příkazů a nesprávná reakce na chybné příkazy), tak i chyby v kryptografických algoritmech. Existence funkčních chyb je způsobena především tím, že se jedná o chyby, které nenarušují funkčnost karty v bezpečném prostředí, a proto zůstávají při běžném testování systému neodhaleny. Vzhledem k poměrně důslednému dodržování principu "security through obscurity" tyto chyby často v systému přetrvávají značnou dobu. Nedostatky kryptografických algoritmů bývají často způsobeny poměrně malou paměťovou kapacitou čipové karty a problémy vývojáře s paměťovým prostorem. Je jasné, že první věc, na které se začne šetřit, je kryptografie.

Nenalezne-li útočník v software karty chyby, má další možnosti. Jednou z nich je diferenciální chybová analýza (zkráceně DFA, Differential Fault Analysis). DFA vychází z následující myšlenky: software čipové karty (nebo jiného hardwarového kryptografického zařízení) byl navržen tak, aby se choval správně za předpokladu, že při činnosti procesoru karty nedojde k hardwarové chybě. Pokud ale při provádění programu čipové karty dojde k hardwarové chybě (například k nesprávnému provedení některé instrukce procesoru) je pravděpodobné, že karta se zachová nestandardně způsobem, který napomůže útočníkovi při útoku na kartu. Je jasné, že útočník nebude čekat, až při provádění programu dojde k chybě, ale pokusí se chybu sám vyvolat. Jaké má proto možnosti? Velmi široké. Jednou z prvních diskutovaných možností je ozařování čipu rentgenovými paprsky nebo jiným podobným zářením. Tento útok při dostatečné intenzitě záření vede k úspěchu, ale je poměrně nesnadno proveditelný v amatérských podmínkách. Útočník však má mnoho jiných možností. Může vyvolat chybu pomocí drastického zvýšení frekvence hodinového signálu (uvědomme si, že hodinový signál je téměř u všech čipových karet generován externě) nebo pomocí velmi krátkých impulsů na některém signálovém vodiči (tzv. "glitch attack"). Útočník také může dostat čip do nestandardního stavu zvýšením nebo snížením teploty (tzv. teplotní útok) a zvýšením nebo snížením napájecího napětí (tzv. napěťový útok). Z těchto typů útoku je nejvíce používaný "glitch attack", neboť dovoluje útočníkovi zaměřit se na chybné provedení konkrétní instrukce procesoru.

Časový útok (timing attack) objevil poměrně nedávno (v roce 1996) Paul Kocher. Tento útok vychází z předpokladu, že některé algoritmy potřebují různý čas pro zpracování různých vstupních dat.

Příčiny této časové závislosti jsou rozmanité. Mezi nejčastější příčiny časové závislosti programů na datech patří:

- optimalizace programů (například neprovedení některých matematických operací při nulové nebo jedničkové hodnotě operandů)
- podmíněné skoky
- nestejná lokalita odkazů do paměti v případě použití vyrovnávací paměti (cache hits)
- existence instrukcí s různou dobou provádění (např. násobení, dělení, rotace, posuvy)

Výsledkem je, že čas provádění programu závisí na zpracovávaných datech i na klíči, což oboje útočníka zajímá. Vzniká tedy časový skrytý kanál, kterým "vytéká" část informace (někdy jen několik bitů, ale i to je pro útočníka cenná informace) z bezpečného hardware ven.

Principu "vytékání" informace z bezpečného hardware využívá i jiný zajímavý útok - výkonová analýza (PA, Power Analysis) a diferenciální výkonová analýza (DPA, Differential Power Analysis). Tyto útoky měří během činnosti kryptografického mosulu jeho proudový odběr a podle něj se znaží zjistit, jaké instrukce modul

právě provádí a s jakými daty je provádí.

2.5 Náročnější útoky

Výše uvedené útoky patřily mezi útoky logické, neboť nevyžadovaly fyzickou manipulaci s čipem karty. Pokud tyto útoky nejsou pro danou čipovou kartu použitelné, nastupují útoky, které přímo manipulují s čipem karty, a které se nazývají útoky fyzické. Přestože pro tyto útoky je již třeba speciální technické vybavení, tyto útoky nemusí být mimo možnosti amatérů, protože často se toto vybavení nachází na univerzitách nebo bývá možné si toto vybavení na několik hodin pronajmout v laboratoři. A pro průmysl hackerských satelitních karet, který disponuje poměrně značným kapitálem, je většina těchto útoků cenově dostupná.

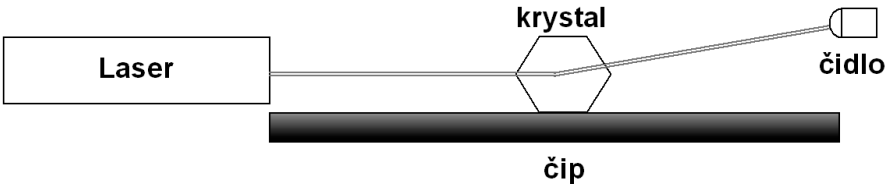
Jako příklad uveďme alespoň příklady některých fyzických útoků:

Pasivní útoky

- Mikroskopické sondy (microprobes), které často obsahují až 9 jehel, umožňují elektrické sledování signálů na čipu.
- Elektronový mikroskop umožní sledování signálů na sběrnici.
- Elektrooptické vzorkování sleduje krystal niobátu lithia laserovým paprskem a tím zjišťuje přítomnost elektrostatického pole pod krystalem (viz Obr. 6).
- Spodní rentgenování umožňuje pozorování tranzistorů zespod čipu na vlnové délce, pro kterou je křemíkový substrát průhledný.

Aktivní útoky

- Laserový nůž umožňuje přerušení spojů a odstranění pasivační vrstvy
- Iontový paprsek umožní vytvoření nových spojů
- Selektivní suché leptání umožňuje oklamat senzory, testující přítomnost pasivační vrstvy



Obr. 5. Elektrooptické vzorkování - krystal niobátu lithia je prosvěcován laserovým paprskem a tím zjišťuje přítomnost elektrostatického pole pod krystalem

Výše uvedeným výčtem samozřejmě nekončí možnost útoků na čipové karty. Na druhé straně čipová karta má možnost těmto útokům odolat a skutečně dobré čipové karty jim odolají. Vše zůstává na vývojářích systémů, jaké čipové karty si z poměrně široké nabídky vyberou a jakým způsobem je použijí.

2.6 Budeme zatloukat a zatloukat - Mondex

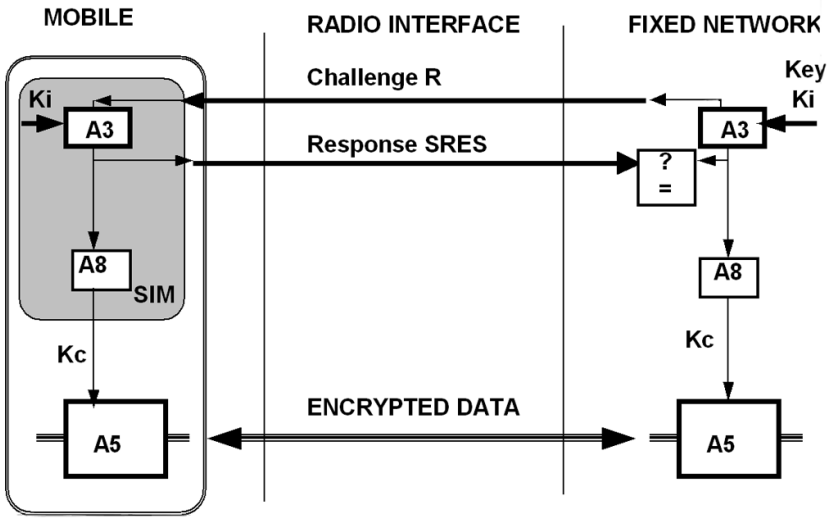
Pokud se pozornost útočníků soustředila na satelitní čipové karty, mohli vývojáři finančních aplikací s čipovými kartami (tedy především vývojáři elektronických peněženek) tvrdit, že satelitní čipové karty tvoří v bezpečnosti čipových karet "druhou ligu" a že jejich "bankovní" čipové karty jsou na tom z hlediska bezpečnosti zcela jinak. Vzhledem k důslednému utajování jak vlastností čipů, tak i samotných kryptografických protokolů, bylo obtížné jim v tomto oponovat. Nezbývalo, než jim věřit. Jednou z těchto elek-

tronických peněženek je systém Mondex, o kterém se tvrdí, že je jedním z nejrozšířenějších systémů. Jeho výrobce tvrdil např. že "systém poskytuje úroveň bezpečnosti, která předbíhá současnou úroveň zločinců dnes a bude je předbíhat i zítra", že "systém poskytuje světovou úroveň fyzického a logického zabezpečení" a podobně. Tato tvrzení bylo opět obtížné zpochybnit. Až v květnu 1996 si Národní banka Nového Zélandu (NBNZ) v rámci pilotního projektu nechala otestovat bezpečnost systému Mondex nezávislou organizací. Výsledkem bylo memorandum, které konstatovalo, že bezpečnost prověřované verze systému je nedostatečná a systém není dostatečně odolný proti útoku (auditor to demonstroval pomocí útoku, při kterém se mikrojehlami spojí dvě testovací plošky na čipu a tím se čip dostane do testovacího režimu). Dalo by se čekat, že toto odhalení způsobí poprask. Bylo tomu však zcela jinak. Výsledky auditu byly před veřejností více než rok utajovány, než bylo memorandum v roce 1997 únikem informací z NBNZ prozrazeno a zveřejněno na Internetu organizací EFF (Electronic Frontier Foundation). Reakce NBNZ byla téměř hysterická - NBNZ žádalo EFF o okamžité stažení textu memoranda z Internetu a v případě neuposlechnutí hrozila soudními následky (odpovědní činitelé se zřejmě domnívali, že stažením zprávy z Internetu se zvýší bezpečnost systému).

Kdo je však viník? Asi nikdo. Výrobce čipu čipové karty (Hitachi) prohlásil, že čip je staré verze a není již v současnosti podporován a neměl být použit. Výrobce systému (Mondex) prohlásil, že bezpečnost systému je "odpovídající způsobu použití", přičemž "způsob použití", což je jinými slovy maximální částka, uložená v elektronické peněžence, nebyla nikde jasně definována. Takže Černý Petr zůstal asi v rukou bance.

2.7 Mrtvý brouk - GSM SIM karty

Další velmi rozšířenou aplikací čipových karet jsou mobilní telefony GSM, kde čipová karta (zvaná SIM - Subscriber Identity Module) plní velmi důležitou úlohu v zabezpečení telefonu. Karta především slouží jako identifikační prostředek majitele telefonu, který jednoznačně definuje, kdo je volající a zabraňuje možnosti vydávat se za jiného účastníka. Druhým úkolem je generování dočasného klíče, kterým je šifrován samotný hovor, což tvoří účinnou ochranu před odposloucháváním. Kryptografické zabezpečení je provedeno pomocí tří algoritmů. V kartě je uložen pro každou kartu jedinečný klíč Ki a dva kryptografické algoritmy A3 a A8. Algoritmus A3 slouží pro kryptografickou autentizaci mobilního telefonu a algoritmus A8 slouží pro vygenerování jednorázového klíče relace Kc, kterým bude šifrován samotný hovor. Algoritmus A5, který není umístěn v kartě, ale v mobilním telefonu, slouží pro zašifrování samotného hovoru klíčem Kc.



Obr. 6. Princip zabezpečení telefonů GSM

Z výše uvedeného popisu plyne, že celá bezpečnost karty SIM je závislá na utajení klíče Ki. A teď pozor. Algoritmy A5 a A3/A8 (které jsou vlastně algoritmem jediným, nazývaným COMP128) jsou utajované a nepublikované. Opět "security through obscurity" jako hrom. Až do jara roku 1998, kdy z jisté firmy (raději ji nebudeme jmenovat), unikl dokument s názvem "TECHNICAL INFORMATION - GSM System Security Study", obsahující mimo jiné popis algoritmu COMP128. Několik osob, sdružených v zájmové organizaci "Smartcard Developer Association" podrobilo tento algoritmus analýze a velmi rychle zjistili - že je špatný. Díky chybám v algoritmu je možné během několika hodin ze SIM karty zjistit klíč Ki a vytvořit tak kopii této karty, zvanou klon. Asociace GSM MoU, která sdružuje operátory GSM telefonů na tento útok reagovala prohlášením, že algoritmus COMP128 je pouze vzorový, nikoli povinný, a každý GSM operátor si měl zvolit sám svůj bezpečný algoritmus. Většina z nich to neudělala. Černý Petr opět zůstal v rukou jednotlivých operátorů GSM.

Na tomto příkladě je asi nejmarkantněji vidět škodlivost přístupu "security through obscurity" a utajování algoritmů. Pokud by algoritmus COMP128 nebyl utajován, jeho nedostatky by byly již před lety nalezeny a buď by byly odstraněny nebo by se tento algoritmus nepoužíval. Utajování algoritmů však vede k přežívání bezpečnostních chyb po dlouhá léta.

3 Co na závěr

Doufám, že čtenář si z výše uvedených exemplárních případů vezme správné poučení. Bylo by krátkozraké tvrdit, že tyto případy svědčí o nedostatečné bezpečnosti kryptografických modulů a zejména čipových karet. Spíše svědčí o tom, že čipové karty jsou jako každý jiný produkt: jsou čipové karty kvalitní a tedy bezpečné, jsou čipové karty méně kvalitní a tedy i méně bezpečné. Kvalitu čipových karet však nemůžeme nikdy posuzovat podle marketingových tvrzení výrobce nebo vývojáře aplikace, ale pouze podle výsledků nezávislého auditu. A výše uvedené příklady nebyly selháním čipové karty jako takové, ale selháním člověka, který ve své nafoukanosti a domýšlivosti nerespektoval základní bezpečnostní zásady a použil tyto karty způsobem, který nebyl správný.

4 Literatura

[And94] RJ Anderson, „Why Cryptosystems Fail“, in Communications of the „ACM v 37 no 11 (Nov 94) pp 32-40

[And96] RJ Anderson, MG Kuhn, „Tamper Resistance — a Cautionary Note“, in The Second USENIX Workshop on Electronic Commerce Proceedings (Nov 1996) pp 1–11

[Bih96] E Biham, A Shamir, „Differential Fault Analysis: Identifying the Structure of Unknown Ciphers Sealed in Tamper-Proof Devices“, preprint, 10/11/96

[FIP94] Security Requirements for Cryptographic Modules, FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, January 11, 1994

[TUN87] Tunstall, J.S., Electronic currency. (North-Holland, Amsterdam, Netherlands, p. 47-8, 1989) (Conference: Smart Card 2000: The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference, Laxenburg, Austria, 19-20 Oct. 1987)

[VME95] Integrated Circuit Card Specifications for Payment Systems, VISA, MasterCard, Europay, 1995

NOVÉ TRENDY V OBLASTI AUTENTIZAČNÍCH ZAŘÍZENÍ

Jaromír Klimek, AEC, spol. s r.o., Bayerova 799/30, 602 00 Brno
e-mail: jaromir.klimek@aec.cz

Po 11. září loňského roku prudce vzrostl zájem o firemní bezpečnost a o sofistikovanější formy autentizace; do popředí zájmu se stále více dostávají biometrická zařízení, prognózy dynamiky trhu v této oblasti jsou velmi optimistické.

Největší nárust se samozřejmě odehrává a očekává především ve státní správě, dopravě atd, ale zřetelným trendem je i zvyšování zájmu o otázky bezpečnosti i ve firmách středních a menších.

Podívejme se na základní možnosti autentizace a také na některé z možností využití biometrických zařízení.

Základní typy autentizace:

1) Něco co osoba zná - heslo, PIN
2) Něco co osoba má - token, čipová (smart) karta
3) Čím osoba je - biometrika

Samozřejmě je možná i kombinace výše uvedených typů.

S hesly a PINy máme zkušenosti prakticky všichni a jsme si také vědomi jejich kladů a záporů. Co se týče čipových karet, tak zde platí totéž, ale jistě také platí to, že většina z nás „vlastní“ podstatně více hesel než vlastní čipových karet (ať těch platebních nebo SIM karet v mobilních telefonech atd.).

Uživatelů tokenů zde bude asi méně a ještě méně z nás se dostává do pravidelného kontaktu se zařízení biometrickými.

Netroufnu si odhadnout, jak bude situace vypadat za 2, 5 či 10 let, ale je jisté, že pro ochranu svých citlivých údajů budeme chtít používat stále bezpečnější a přitom pohodlnější metody. Tudíž zde jistě vstoupí do hry biometrická zařízení, zvláště pokud se dostanou na rozumnou cenovou úroveň při dobré úrovni zabezpečení a spolehlivosti.

Domnívám se, že dobrou představu o budoucím rozšíření jednotlivých typů si můžeme udělat i na základě toho, co bylo k vidění na letošním CEBITu, neboť tento veletrh jistě není jen přehlídkou toho, co je aktuálně na trhu k dispozici, ale z velké části se jedná o přehlídku technologií bližší či vzdálenější budoucnosti.

Co se týče tokenů, které jsou v oblasti autentizace stále populárnější, tak na letošním Cebitu rozhodně bylo z čeho vybírat, ale právě proto je potřeba poměrně značné obezřetnosti. Zkušenosti firmy s 2500 zaměstnanci, která se pokoušela přejít na autentizační model využívající tokenů, jsou takové, že byl vybrán nevhodný model a díky tomu byli naplno vytíženi dva správci na plný úvazek, kteří řešili poruchy tokenů.

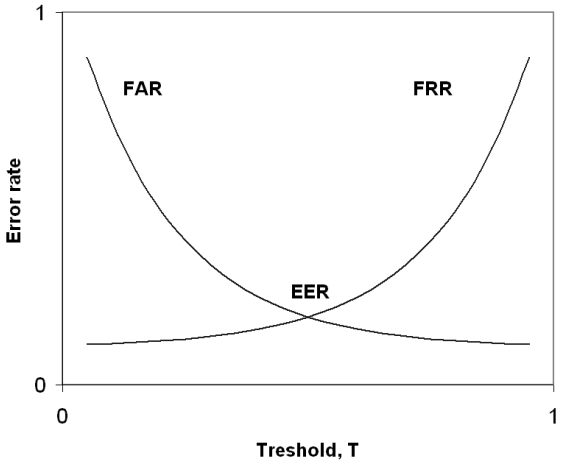
Z tohoto důvodu přistoupila jiná firma k řešení problému důkladněji: než vybrali konkrétní model tokenu, tak otestovali produkty jednotlivých dodavatelů: tloukli do nich, chodili po nich, ponořili je do šálku kávy. A byl vybrán ten nejodolnější model, který opravdu vydržel i to kafe.

Než zmíníme některá z biometrických zařízení, připomeňme si některé podstatné rozdíly, mezi autentizací metodami na které jsme dnes zvyklí a metodami, které se teprve dostávají do popředí zájmu.

U autentizace heslem, PINem, tokenem, kartou je vždy vyžadována 100% shoda, tzn. dané heslo, PIN, certifikát, který je uživatelem zadán je porovnán s údaji v databázi a obojí musí přesně souhlasit.

V případě biometrických zařízení, ale není 100% shoda vždy vyžadována. Hledá se zde optimální poměr mezi pravděpodobností chybného přijetí přijetí - False Acceptance Rate (FAR) a pravděpodobností chybného odmítnutí - False Rejection Rate (FRR) při autentizaci uživatele. Pokud má dané zařízení vysokou hodnotu pravděpodobnosti chybného přijetí, pak nelze hovořit o zařízení bezpečném. Pokud je příliš vysoká

pravděpodobnost chybného odmítnutí, pak nás uživatelé jistě chválit nebudou. Ze znalosti průběhu hodnot FAR a FRR můžeme určit Equal Error Rate (EER):



Hodnoty FAR A FRR jsou pro každý systém charakteristické a jsou jedním z důležitých kritérií kvality daného zařízení. Úroveň zabezpečení (Trashold) je nastavitelná, aby mohl být biometrický systém doladěn dle požadavků konkrétního zadání:

Tentýž systém bude jinak naladěn pro autentizaci čtenářů při vstupu do knihovny a jinak při autentizaci do vojenského objektu. V knihovně nám bude méně vadit to, že jeden z tisíců uživatelů projde neoprávněně, než to, kdyby nás bombardovali čtenáři s nárokem na vstup, kteří vpuštěni nebyli. V tomto případě tedy zabezpečení nastavíme co nejblíže hodnoty EER, popř. poněkud vlevo. Použijeme-li totéž zařízení pro ochranu vojenského zařízení, pak zřejmě úroveň zabezpečení nastavíme více vpravo od EER, protože nemůžeme tolerovat byť jednoho neoprávněně vpuštěného narušitele.

Samozřejmě se budeme především snažit naladit systém tak, aby se bod EER posunul co nejníže.

Charakteristiky využívané biometrickými zařízeními

nejčastěji:

- *otisk prstu*
- *geometrie ruky, prstu*
- *obličej*
- *duhovka*
- *sítnice*

méně často:

- *zbarvení hlasu*
- *žilkování*
- *DNA*
- *tvar ucha*

V nabídce biometrických zařízení na letošním Cebitu zřetelně převažovala zařízení založená na snímačích otisku prstu, které byly implantovány snad ve všech možných periféríích - klávesnicích, myších, flash discích atd. Záměr je zřejmý - nahradit autentizaci heslem autentizací pomocí otisku prstu.

O tom, že zájem o tyto produkty je opravdu velký jsme se přesvědčili na vlastní kůži:

V grafickém provedení našeho stánku byl mimo jiné i otisk prstu, a protože naše produkty byly z jiné oblasti, museli jsme mnohokrát za den vysvětlovat, že biometrická zařízení nevyrábíme.

Nicméně se u tohoto zařízení objevuje velké riziko přijetí aktivního podvrhu **(Active Impostor Acceptance)**. Popis postupu je například zde:
http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf

Co je v postupu popisovaném T. Matsumotem z Jokohama National Univerzity velmi nepříjemné, je fakt, že vytvoření „želatinového prstu“, který může být použit útočníkem jako podvrh, je poměrně snadné, a to i v případě, že otisk prstu bude sejmut např. ze sklenice na kterou daná osoba sáhla. Matsumoto se jím vyrobenými "želatinovými prsty" pokusil oklamat 11 komerčních systémů a u všech se mu to podařilo. Dokonce uspěl i u těch zařízení, která měla detekovat jen "živé prsty".

Bude tedy zajímavé sledovat, jak se jednotliví výrobci snímačů otisku prstů s touto výzvou vyrovnají.

Pro opravdu bezpečné aplikace bude zřejmě potřeba vybrat zařízení, která využívají některé z jiných biometrických charakteristik.

Z těch rozšířenějších můžeme zmínit např. zařízení využívajících např. **geometrii ruky**. Samozřejmě i zde je teoreticky možný útok „želatinovou rukou“, která bude vyrobena podobným způsobem jako výše popsaný otisk prstu, ale to je pouze teoretická úvaha a navíc by bylo nutné získat otisk (odlitek) celé ruky, což je podstatně hůře proveditelné než v případě prstu a samozřejmě nepřichází v úvahu sejmutí odlitku ruky ze stop na sklenici.

Dále zde jsou zařízení využívající **vzhled duhovky či sítnice**. V případě duhovky je počet různých jejích vzorů-forem o několik řádů vyšší než v případě otisku prstu a tato zařízení jsou obecně považována za jedny z nejbezpečnějších. Falšování duhovky či sítnice je prakticky nemožné, a tak jediným záporem zde zůstává psychologická zábrana spočívající v tom, že neradi vystavujeme své oči jakémukoliv zřízení, které je bude snímat.

Jako poslední typ zařízení bych uvedl ta, která jsou založena na **snímání tvaru a geometrie obličeje**. Zde je poměrně široká škála technologií, které jsou uplatňovány při zpracovávání získaných údajů (polohy a vzdálenost významných bodů na tváři, trojrozměrný obraz obličeje atd.).

Za zmínku zde stojí např. „scanner davu“, který vyhledává a ukládá jednotlivé obličeje procházejících osob, přičemž jednotlivá tvář je vyhledána za dobu kratší než 200 milisekund a její „otisk“ o velikosti 84 bajtů může být uložen do databáze. Spolehlivost této metody (EER = 0.68%) sice není tak vysoká jako u jiných technologií patřících do této kategorie, ale vzhledem k velké rychlosti sejmutí obrazu, může toto zařízení nalézt uplatnění především v preventivním nebo doplňkovém scanování např.na letištích, ve vstupních halách budov atd.

SVĚŘENÁ SPRÁVA INFORMAČNÍ BEZPEČNOSTI

JUDr. Luděk Rataj, předseda asociace AFOI

Úvod

O tom, že řešení informační bezpečnosti je nezbytnou podmínkou pro úspěšné fungování a rozvoj organizace se již přesvědčovat nemusíme. Potvrzuje to rovněž studie provedená společností Infonetics Research, podle které vzrostou výdaje na bezpečnost informačních systémů v západní Evropě v letech 2001 - 2005 více než 4-krát, z 1,5 miliardy dolarů na 7,7 miliardy. Tento odhad zahrnuje bezpečnostní služby, bezpečnostní technologie a PKI. Celosvětově pak tyto výdaje vzrostou ve stejném období z 5,3 miliardy dolarů na 22,7 miliardy.

"Všichni o potřebách bezpečnosti IT vědí, ale mnozí si s ní nevědí rady" - tvrdí Peter Judge, analytik společnosti Infonetics Research. "Naše studie ukazuje, že Evropané nyní podnikají praktické kroky k ochraně dat a využívají k tomu služeb třetích stran: 2/3 našich respondentů již využily nějakou formu bezpečnostních služeb a odhaduje se, že do roku 2003 bude tyto služby využívat prakticky každý."

Další zajímavý průzkum provedla firma Resource, která je největší nezávislou agenturou pro výzkum technologií se sídlem ve Velké Británii. Průzkum byl zaměřen na hodnocení důležitosti aktuálních problémů v oboru IT a jako nejdůležitější problém byla manažery útvarů IT předních evropských firem vyhodnocena bezpečnost dat. Pořadí problémů je dle zmíněného průzkumu následující (1=nedůležité, až 5=velmi důležité):

1) bezpečnost dat (4,55)
2) kontinuita podnikání (4,05)
3) náklady (4,04)
4) management infrastruktury (4,01)
5) návratnost investic (3,92)
6) přenosová kapacita (3,87)
7) konsolidace systémů (3,83)
8) rychlost změn (3,54)
9) konsolidace uchování dat (3,50)
10) smlouvy o úrovni poskytovaných služeb (3,49)
11) personál (3,47)
12) Internet (3,46)
13) e-podnikání (2,98)

Bezpečnost dat je však spíše technologickou problematikou v oblasti informační bezpečnosti, kam spadají i mnohé další z vysoce hodnocených problémů.

Aby využívání bezpečnostních služeb bylo účelné a efektivní, je v prvé řadě potřebné zavést systém řízení informační bezpečnosti, resp. systém řízení rizik informačního systému. Existence a úroveň takového systému je společným jmenovatelem užití jakékoli informační technologie a jakéhokoli bezpečnostního produktu v informačním systému každé organizace.

Pro takto pojímaný systém bezpečnosti je na základě některých mezinárodních norem užíván termín "správa informační bezpečnosti", resp. "systém řízení informační bezpečnosti" (ISMS), a pakliže je tento proces zajišťován formou outsourcingu, hovoříme o "svěřené správě informační bezpečnosti". Svěřenou správu lze tedy považovat za formu outsourcingu, kdy dodavatel poskytuje kromě výkonu smluvených činností i jejich řízení a kontrolu. Jaké může mít svěřená správa výhody a nevýhody si povíme dále, ale již nyní je patrné, že se jedná o přenesení více činností a větší zodpovědnosti na dodavatele. Dodavatel pak získává větší nezávislost v jednotlivých činnostech a snáze může definovat rozhraní poskytované služby.

Dále si uvedeme ještě jeden pojem či zkratku: MSS (Managed Security Services). Tato zkratka označuje obchodní model, kde kvalifikovaný externí poskytovatel služeb provozuje zákazníkovu bezpečnostní infrastrukturu. Bezpečnostní infrastrukturou se zde myslí konkrétní technologické řešení např. připojení k Internetu, nebo i celý systém řízení informační bezpečnosti organizace. Poskytovaná služba zahrnuje návrh, konfiguraci, provoz, údržbu a monitoring bezpečnostní infrastruktury. Služba MSS tedy představuje právě svěřenou správu informační bezpečnosti v určitém vymezeném rozsahu.

Služby dodavatelů

S nabízením služeb, které s informační bezpečnostní úzce souvisí nebo ji alespoň do jisté míry ovlivňují, se setkáváme prakticky na každém kroku. Na několika příkladech si zde uvedeme, kdy bývají často využívány služby dodavatelů.

Nejrozšířenější je využívání služeb dodavatelů informačních technologií. Poskytování služeb v této oblasti dosáhlo opravdu významného rozsahu od pouhého dodání zařízení, přes jeho údržbu, až po outsourcování celého informačního systému:

- Dodání hardwaru
- Pravidelné profilaxe
- Správa operačního a aplikačního systému
- Pronájem informačních a komunikačních technologií
- Zálohování a obnova systémů

Efektivita informačního systému je do značné míry závislá na kvalitním aplikačního softwaru. To s sebou vedle pravidelné aktualizace přináší i nezbytné změny funkčnosti v souladu s měnícími se potřebami organizace a často i legislativy. Dodavatelé aplikačního softwaru nabízejí např.:

- Procesní analýzy
- Vývoj softwaru
- Parametrizaci systému
- Design a správu webu
- Integraci prvků silné autentizace
- Integraci antivirové kontroly

S nároky moderních informačních systémů rostou neustále i požadavky na komunikační infrastrukturu. Pronájem komunikačních kanálů a správa příslušných zařízení se stává samozřejmostí. Využívání veřejných datových sítí přináší kromě nových možností i nová rizika, což je díky velmi rychlému vývoji v této oblasti a velkému rozsahu problematiky perspektivní oblastí pro využívání služeb specializovaných odborníků:

- Vybudování a údržba infrastruktury LAN
- Pronájem komunikačních linek, údržba aktivních prvků
- Připojení k Internetu, Web Hosting, údržba firewallu
- Dohled nad provozem a bezpečností sítě
- Detekce průniků
- Certifikační služby, provoz CA

Jednou z podmínek pro úspěšné poskytování všech služeb je vyřešení bezpečnosti, proto bychom se jejím řešením měli zabývat i u služeb, které s informační bezpečností zdánlivě nesouvisí. Informační bezpečnost přesahuje hranice informačních technologií i informačního systému a její úspěšné řešení závisí na komplexním a metodickém přístupu.

- Organizační a personální zajištění řízení informační bezpečnosti
- Provedení rizikové analýzy, aktualizace
- Návrh bezpečnostní infrastruktury a procesů
- Zpracování bezpečnostní politiky, definice cílů
- Zpracování bezpečnostní dokumentace a předpisů
- Vytvoření a správa plánů kontinuity hlavních činností
- Nezávislá konzultační a poradenská podpora při implementaci
- Příprava vzdělávacího programu, školení
- Zpracování auditních záznamů, monitoring
- Kontrola souladu s bezpečnostní politikou
- Audit informační bezpečnosti

Information Security Management System

Příklady poskytovaných služeb uvedené v předchozí kapitole vedou nezbytně k úvaze, že tyto služby jsou ve značné míře navzájem závislé. Tato úvaha je nejen správná, ale potvrzuje ji i současný vývoj v oblasti outsourcingu, kdy předmětem smluvního vztahu je obvykle více souvisejících služeb, např. poskytování připojení k Internetu včetně pronájmu firewallu, jeho správa, web hosting, antivirová kontrola apod.

Služby nabízené v oblasti řízení informační bezpečnosti spolu rovněž úzce souvisí a bývají nabízeny společně. Výjimečné je postavení auditu představujícího v případě svěřené správy informační bezpečnosti zásadní kontrolní nástroj, který by měl být prováděn nezávisle.

Podoba těchto služeb s činnostmi a opatřeními tvořícími systém řízení informační bezpečnosti (ISMS - Information Security Management System) podle britské normy BS 7799-2:1999 není náhodná, neboť tato norma a zejména norma ČSN ISO/IEC 17799 poskytují ucelené řešení celé problematiky informační bezpečnosti a popisují mnohá bezpečnostní opatření. Pro organizaci, která chce řešit informační bezpečnost metodicky a systémově, by tato norma měla být etalonem informační bezpečnosti. Pro poskytovatele služeb může norma představovat zadání popisující proces a požadavky dosažní cílového stavu informační bezpečnosti.

Norma ČSN ISO/IEC 17799 je v současné době uznávanou zárukou kvality řešení informační bezpečnosti a úzce souvisí s normami pro řízení a zabezpečení jakosti ISO 9000. Bohužel dosud není v ČR zaveden žádný systém formální certifikace, který by umožnil zhodnotit soulad s jejím plněním. Z tohoto důvodu zůstává jediným nezávislým hodnocení kvality výkonu svěřené správy informační bezpečnosti výrok nezávislého auditora.

Činnosti svěřené správy

Prvním krokem při výkonu svěřené správy informační bezpečnosti je samotná její definice v prostředí zákazníka. Musí být stanoveny hranice informačního systému a rozhraní pro výměnu informací, identifikovány hrozby a zranitelnosti a popsána již implementovaná bezpečnostní opatření. Toto je náplní rizikové analýzy, jejíž výstupy popisující cenu aktiv, rizika a možné dopady incidentů jsou základním vstupem pro stanovení cílů informační bezpečnosti, rozdělení zodpovědnosti a zpracování bezpečnostní politiky.

Bezpečnostní politika

Ačkoli dodavatel samozřejmě nemůže bezpečnostní politiku sám schválit, může vhodně zúročit znalosti získané v průběhu rizikové analýzy a své zkušenosti z jiných organizací. Návrh bezpečnostní politiky vyžaduje nejen dobré znalosti prostředí organizace, ale i znalost různých přístupů ověřených praxí. Schvalování bezpečnostní politiky ve struktuře stávajících řídících předpisů a zvyklostí je obvykle provázeno mnoha kompromisy, které jsou příčinou toho, že bezpečnostní politika je prakticky ve všech organizacích jedinečným souborem předpisů.

Zpracování bezpečnostní politiky a souvisejících řídících dokumentů je jednou z obvykle nabízených služeb dodavatelů. V rámci svěřené správy informační bezpečnosti se však jedná nejenom o její zpracování a přípravu ke schválení, ale o správu bezpečnostní politiky a řídících předpisů po celou dobu jejich platnosti. Tím je myšlena zejména pravidelná revize dokumentů, doporučení k aktualizaci a návrhy nových řídících dokumentů v souvislosti s rozvojem informačního systému.

Organizace bezpečnosti

Vytvoření bezpečnostní infrastruktury počínaje řídícím výborem, přes bezpečnostního manažera a vlastníky informací konče je sice významným, ale z hlediska realizace obtížně plnitelným požadavkem normy. Vytváření výborů nebo komisí je často problematické a mnohdy končí pouze u formálního jmenování. Vytváření nových pracovních pozic bývá v rozporu s personální politikou organizace nebo naráží na cíle restrukturalizace, případně se jedná o problém ryze ekonomický. Rozdělení jednotlivých činností informační bezpečnosti a jejich přidělení stávajícím pracovním pozicím naopak naráží na problémy s určením zodpovědnosti a přidělením pravomocí.

Cílem svěřené správy je přenesení co největšího množství relevantních činností na dodavatele, který v rámci jediného kontrolního týmu zajistí řízení a výkon činností informační bezpečnosti. Vzhledem k tomu, že se jedná o jediný subjekt, je definice a rozdělení zodpovědnosti a pravomocí mnohem snazší a lze ji jednoduše zachytit ve smlouvě.

Přenesení určité zodpovědnosti a zejména pravomocí by se mělo týkat rovněž spolupráce s dodavateli informačních technologií a poskytovateli služeb, tak aby dodavatel mohl řešit ochranu informací již ve fázi přípravy smluvního vztahu. Řízení a kontrola informační bezpečnosti ve vztahu ke třetím stranám a poskytovatelům služeb je důležitou součástí svěřené správy, neboť dodavatel může obvykle využít větších zkušeností svých pracovníků v různých oblastech informační bezpečnosti, od technologií až po legislativu.

Klasifikace a řízení aktiv

Seznam a charakteristika aktiv relevantních pro bezpečnost je jedním z významných výstupů rizikové analýzy. Dohled nad nimi, včetně jejich evidence a správy, je jednou z činností, které mohou být předmětem činnosti svěřené správy informační bezpečnosti.

Klasifikace, označování a manipulace s informacemi představují opět požadavky normy, které je nezbytné upravit podle konkrétních potřeb organizace, tak aby bylo reálné jejich začlenění do pracovních postupů a denní praxe zaměstnanců.

Předmětem svěřené správy informační bezpečnosti je zde správa klasifikačního schématu, předpisů a pravidel pro manipulaci s citlivými informacemi a poskytování podpory zaměstnancům.

Personální bezpečnost

Personální bezpečnost zahrnuje několik oblastí, které mohou být předmětem svěřené správy informační bezpečnosti. V první řadě se jedná o právní úpravu ochrany informací v rámci zaměstnaneckého poměru a současně vymezení náplně práce, pravomocí a zodpovědnosti pracovních pozic ve vztahu k informační bezpečnosti.

Druhou oblastí je začlenění informační bezpečnosti do programu školení a vzdělávání zaměstnanců, příprava obsahové náplně školení, poskytnutí lektorů nebo zajištění školení externími spolupracovníky se specializací pro příslušnou problematiku.

Další oblastí týkající se personální bezpečnosti je ohlašování bezpečnostních incidentů a poruch. Zde může být předmětem svěřené správy zajištění kanálu pro ohlašování incidentů, jejich evidence a dokumentace, zajištění nápravy ve spolupráci s dodavateli nebo poskytovateli služeb, zúročení zkušeností při návrhu a aktualizaci bezpečnostních opatření a zajištění podkladů pro případnou eskalaci problému nebo vyšetřování incidentu.

Fyzická bezpečnost a bezpečnost prostředí

Fyzická bezpečnost bývá obvykle z celé informační bezpečnosti zajištěna nejlépe, rovněž zde většina organizací využívá služeb třetích stran a najímá si specializované bezpečnostní agentury. Cílem fyzické bezpečnosti je však primárně ochrana majetku. Informace, zejména pokud jsou na přenosných elektronických médiích nebo v papírových dokumentech, bývají opomíjeny. Bezpečnost provozního prostředí informačních technologií bývá s ohledem na jejich cenu rovněž zajištěna kvalitně.

Předmětem činnosti dodavatele je v rámci svěřené správy zejména návrh doplňujících bezpečnostních opatření a kontrola výkonu a účinnosti režimových opatření. Spolu s dodavateli technologií a poskytovateli služeb by se měl dodavatel podílet na implementaci a aktualizaci bezpečnostních opatření.

Zpracování a výměna informací

Zpracování a výměna informací je velmi široká oblast zahrnující jak činnosti uživatelů, tak i činnosti správy systému. Veškeré tyto činnosti by měly být vhodnou formou zdokumentovány v řídících předpisech nebo provozní dokumentaci.

Důležitou roli zde sehrává výměna informací s třetími stranami, která je rostoucí měrou realizována v elektronické formě, a za využití veřejných datových sítí.

Předmětem svěřené správy informační bezpečnosti je v této oblasti zejména správa předpisové základny, návrhy nových bezpečnostních opatření, včetně zohlednění legislativních požadavků při zpracování informací. Ve spolupráci s dodavateli je pak předmětem svěřené správy účast na implementaci bezpečnostních opatření, zpracování a aktualizace příslušných řídících dokumentů a pracovních postupů.

Řízení přístupu

Požadavky na přístup k informacím vyplývají z pracovní náplně, pracovních postupů a měly by se řídit klasifikací informací. Takto jednoduché to však bývá spíše výjimečně a v praxi jsou obvyklé časté změny přístupových práv a mnohé výjimky.

Dodavatel by měl na základě rizikové analýzy, klasifikačního schématu, pracovních procesů a reálných potřeb zaměstnanců navrhnout vhodný systém přidělování přístupových práv. Reálné možnosti takového systému jsou samozřejmě závislé na použitých informačních technologiích, a proto se na jeho přípravě a zvláště implementaci musí podílet i jednotliví dodavatelé informačních technologií a aplikačního softwaru. Zvláště citlivou problematikou je zde dostatečně silný způsob autentizace a ochrany autentizačních údajů. Rovněž sem spadá monitorování přístupů a činností uživatelů, včetně vyhodnocování kontrolních záznamů, tato oblast informační bezpečnosti bývá mnohdy řešena nedostatečně.

Předmětem svěřené správy může být celý proces přidělování přístupových práv, od přijetí požadavků, přes jejich evidenci a vedení historie, až po samotné nastavení práv v jednotlivých systémech. Výkon této činnosti je vhodné rozdělit mezi jednotlivé dodavatele informačních technologií a poskytovatele služeb a předávat jim po zaevidování oprávněné požadavky na změny přístupových práv a uživatelů systému. Co by však mělo zůstat v rámci svěřené správy informační bezpečnosti, je vyhodnocování kontrolních záznamů a aktuálního stavu přidělených přístupových práv ve srovnání s evidencí.

Vývoj a údržba systému

V této oblasti je spolupráce s dodavateli informačních technologií a zvláště aplikačního softwaru nezbytností, avšak nesmí být opomenut ani vlastní vývoj, a to i v případě pomůcek psaných např. ve VBA. Drobné aplikace psané svépomocí se mohou časem rozšířit a často na nich mohou záviset důležité činnosti. Cílem by naopak měl být řízený rozvoj funkčnosti informačního systému, který eliminuje potřebu takovýchto pomůcek a drobných aplikací.

Předmětem svěřené správy informační bezpečnosti může být příprava smluvního zajištění vývoje, nákupu a správy informačních technologií. Dodavatel může poskytovat konzultace při volbě technologií a v rámci výběrového řízení, rovněž se může podílet na přípravě jeho kritérií.

Dále může být v rámci svěřené správy informační bezpečnosti zajištěn dohled nad celým procesem vývoje, od stanovení požadavků, přes jejich implementaci a testování až po zavedení do provozního prostředí. V celém procesu vývoje může dodavatel z pozice správce bezpečnostní dokumentace dohlížet na dokumentaci vývoje a nakonec i dohlížet na kvalitu manuálů pro správce a uživatele. Rovněž by měl dodavatel kontrolovat bezpečnost testovacích dat, pokud byla použita provozní data bez úprav.

Správa kontinuity hlavních činností

Zpracování a údržba havarijních plánů a plánů kontinuity je dnes nabízenou službou, která získává na popularitě. Přestože kontinuita hlavních činností v mnohém překračuje hranice informační bezpečnosti, základem plánování je riziková analýza, která stanoví požadavky na dostupnost hlavních činností, resp. aktiv, jež jsou pro tyto činnosti nezbytná.

Předmětem svěřené správy informační bezpečnosti může být zavedení systému plánů kontinuity hlavních činností a jejich správa, zejména vyhodnocování testů a pravidelná aktualizace plánů. Dodavatel by měl rovněž navrhnout oprávněná bezpečnostní opatření ke zlepšení dostupnosti služeb informačního systému a snížení následků jeho výpadku.

Kontrola shody

Kontrolu shody lze rozdělit do dvou oblastí. V prvním případě se jedná o kontrolu dodržování právních předpisů, bezpečnostní politiky a řídících předpisů a dokumentace vztahujících se k zajištění informační bezpečnosti. Jednoduše řečeno jedná se o právní poradenství a kontrolu provozních činností zajišťovanou dodavatelem v rámci svěřené správy informační bezpečnosti.

Ve druhém případě jde o kontrolu shody s požadavky normy ČSN ISO/IEC 17799, nebo kontrolu efektivnosti vynakládaných prostředků, kterou obvykle provádí auditor, a zajišťuje tak nezávislou kontrolu dodavatele. Forma auditu může být různá, důležitou roli hraje interní audit prováděný vlastními silami nebo nezávislým dodavatelem, externí audit má obvykle jiné cíle, avšak i jeho výsledky lze využít ke kontrole stavu informační bezpečnosti.

Obě tyto kontroly musí probíhat nezávisle a jejich výsledky musí být pravidelně předávány vedení organizace.

Výhody a rizika

Nepochybnou výhodou svěřené správy informační bezpečnosti je rychlé získání znalostí problematiky a praktických zkušeností, které s sebou dodavatel přináší. Tyto zkušenosti lze využít nikoli pouze k rychlému schválení bezpečnostní politiky a zavedení systému řízení informační bezpečnosti, ale zejména při implementaci dílčích bezpečnostních opatření. Dodavatel může poskytnout nezávislou kontrolu dodavatelů informačních technologií a poskytovatelů služeb a v mnohých případech může zastupovat zákazníka při řešení specifických problémů informační bezpečnosti.

Svěřená správa umožňuje často efektivnější a pružnější řešení problémů, neboť prioritou dodavatele je vyhovět zákazníkovi a současně má dodavatel obvykle pružnější systém řízení než je tomu u velkých organizací.

Otázka finančních nákladů je na pomezí výhod a rizik, neboť ne vždy znamená využívání služeb třetí strany úsporu. Avšak výhoda svěřené správy jako celku je v tom, že zákazníkovi odpadnou mnohé náklady spojené s režií a přidanou hodnotou jednotlivě využívaných služeb.

Určitou nevýhodou může pro zákazníka být uniformita řešení. I když je cílem informační bezpečnosti dosažení souladu s normou ČSN ISO/IEC 17799, možnosti jak dostát znění normy jsou rozmanité a je skutečností, že pokud dodavatel nedokáže přizpůsobit svůj přístup potřebám zákazníka, může spolupráce skončit neúspěchem.

Významným rizikem svěření správy informační bezpečnosti je skutečnost, že se do značné míry jedná o činnosti, které zajišťují kontrolu ochrany informací. Přenesení zodpovědnosti za kontrolní činnosti na dodavatele však nezbavuje zodpovědnosti vedení organizace a následky případného incidentu ponese vždy značnou měrou zákazník.

Závěr

Svěřená správa informační bezpečnosti představuje zejména činnosti, které jsou připisovány útvaru nebo roli bezpečnostního manažera. Pouhý výčet těchto činností uváděný různými zdroji však napovídá, že tyto činnosti nelze přidělit jedinému pracovníkovi ani jedinému útvaru v organizaci, například útvaru informačních technologií. Svěření těchto činností dodavateli by mělo přinést efektivní a rychlé řešení potřeb informační bezpečnosti zákazníka, avšak představuje i jistá rizika, která s sebou přináší každá změna informačního systému a každý nový dodavatel.

TECHNOLÓGIE POUŽÍVANÉ INFILTRÁCIAMI ŠIRIACIMI SA E-MAILOM

Ing. Miroslav Trnka, ESET s. r. o., Svoradova 1, 811 03 Bratislava, trnka@eset.com

Abstrakt: Príspevok rozoberá technológie, ktoré sú používané na prienik infiltrácií

do informačného systému užívatele cestou e-mailu. Ako príklad popisuje najrozšírenejšie červy, no zároveň poukazuje aj na potencionálne zatial nepoužité bezpečnostné diery. Záverom prináša niekolko návrhov na zlepšenie bezpečnosti systémov elektronickej pošty.

1. Úvod

E-mail dnes patrí k nevyhnutnostiam moderného človeka. Vraví sa, že rošírenie jeho používania prinieslo rovnakú sociálnu a ekonomickú revolúciu ako zavedenie spoľahlivo a rýchlo fungujúcej pošty vo viktoriánskom anglicku. Dnes veľa ľudí z vlastnej skúsenosti vie, že efektivita komunikácie pomocou e-mailu prudko klesá s narastajúcim počtom denne prijatých e-mailov. V každom prípade e-mail znamená jednoduchšiu a hlavne rýchlejšiu formu archivovateľnej komunikácie medzi ľuďmi. Preto sa tak rozšíril hlavne v obchodnom prostredí. Pravdou však je aj to, že je rovnako ľahko zneužiteľný na šírenie nevyžiadanej pošty (spam), prípadne na šírenie poplašných správ, fám (hoax) a v neposlednom rade aj infiltrácií.

2. História

2.1. Začiatky e-mailu

Prvý e-mail zaslal koncom roku 1971 Ray Tomlinson, ktorý pracoval na projekte ARPANET. Jeho obsah si už celkom presne nepamätá ale s najväčšou pravdepodobnosťou to bola sekvencia "QWERTYUIOP". Správa bola zaslaná pomocou programu SNDMSG a Ray je aj autorom myšlienky použiť @ na oddelenie login mena užívateľa a mena jeho počítača, čím vznikla e-mailová adresa v podobe ako ju dnes poznáme.

Ďalším dôležitým počinom z hľadiska infiltrácií bol dokument RFC 1341 z roku 1992 pojednávajúci o MIME (Multipurpose Internet Mail Extensions) používanom mimo iného aj na prenos všeobecných (čiže nielen textových) dát pomocou e-mailu. Potrebné prostredie však vyvorilo až masové používanie internetu. Užívatelia samozrejme okamžite začali používať e-mail aj na výmenu súborov. A vtedy sa začali šíriť e-mailom infiltrácie dovtedy "odkázané" len na výmenné médiá.

2.2. Nástup makrovírusov

Skutočne veľké šírenie infiltrácií e-mailom začalo až s objavením sa makrovírusov. Prvý z nich WM/Concept sa objavil sa v júli 1995 a vo Wildliste bol zaznamenaný v septembri 1995. Koniec roku 1995 a hlavne rok 1996 už bol v znamení nebývalého nárastu zaznamenaných infiltrácií.

2.3. Červy

Označenie tohoto druhu infiltrácií pochádza zo Sci-Fi knihy The Shockwave Rider, ktorú napísal John Brunner v roku 1975. Pravdepodobne prvý program ktorý by sa mohol označiť ako červ bol Creeper od Boba Thomasa z roku 1971. Začiatkom osemdesiatych rokov John Hepps a John Shock vo výskumnom stredisku firmy Xerox napísali sadu experimentálnych červov s jednoduchými užitočnými funkciami. Už vtedy však havária výskumnej siete poukázala na potenciálnu nebezpečnosť červov. Do povedomia verejnosti sa však zapísal až nechvalne známy Morrisov červ z novembra 1988. Prvý zámerne deštrukčný červ niesol názov Wank a zjavil sa o rok neskôr. Platforma PC červom dlho odolávala, pretože používané operačné systémy neumožňovali jednoducho zabezpečiť spustenie tela červa na vzdialenom počítači. V honbe za množstvom funkcií však Microsoft čoskoro vytvoril vhodné podmienky. Prvou infiltráciou pre PC ktorá sa rozšírila do celého sveta pomocou E-mailu bol v marci 1999 vírus Melissa, ktorý kombinoval v sebe červa s makrovirusom a zjavil sa aj červ Bubbleboy prvá infiltrácia na PC ktorá na šírenie nepotrebovala

spúšťať prílohu k e-mailu.. O rok neskôr šokoval svet jednoduchý červ napísaný v scripte s menom LoveLetter. Dnes je vo svete približne jedna veľká epidémia zapríčinená novým červom mesačne.

2.4. Trójske kone

Tento druh infiltrácií sa samostatne nereplikuje a preto jeho výskyt nie je natoľko početný. Svojou podstatou je však oveľa nebezpečnejší. Problémom je hlavne veľmi rozšírené posielanie trójskych koní do e-mailových koferencií Usenetu.

3. Technológie používané pri zasielaní infiltrácií e-mailom

3.1. Príloha k e-mailu (attachment)

Klasická forma ktorá dnes však už aby bola skutočne úspešná vyžaduje aplikáciu nejakej formy "sociálneho inžinierstva". Stále častejšie sa autori infiltrácií snažia zakryť pravú funciu prílohy trikom s dvojitými príponami. Podstatou triku je fakt, že mnohé poštové klienty ukazovali užívateľovi len prvú príponu v poradí, ale pri spustení sa systém riadil podľa poslednej. Pretože táto chyba bola do istej miery odstránená záplatami, novšie varianty používajú na skrytie druhej prípony sadu medzier alebo Class ID (CLSID).

3.2. HTML e-maily

Používanie e-mailov vo formáte HTML dosť výrazne zhoršuje bezpečnosť komunikácie. Môžu totiž obsahovať skripty (JavaScript, VB) alebo odkaz na ActiveX komponent. Množstvo bezpečnostných dier v tejto časti OS stále dáva autorom infiltrácií široké pole na uplatnenie.

3.3. Modifikované MIME hlavičky e-mailov

Táto technológia umožnila červu Nimda (a niekoľkým ďalším) automatickú aktiváciu. Trik spočíva v sfalšovaní MIME hlavičky tak, aby označovala priložený vykonávateľný súbor za zvukový súbor WAW. Chybou Outlook Expessu a Internet Explorera potom dôjde k spusteniu prílohy obsahujúcej telo červa.

Príklad normálnej prílohy:

```
Content-Type: image/jpeg;
 name="logo.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="logo.jpg
```

Tu je príklad infiltrácie:

```
Content-Type: audio/x-wav;
  name="Sorry_about_yesterday.MP3.pif"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>
```

V tele html e-mailu sú nasledovné riadky:

```
 <iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
```

Vidíme, že pomocou "Content-ID" (cid) je to prelinkovane na súbor, ktorý sa nachádza v správe a ktorý má vyššie uvedenú hlavičku.

3.4. Ďalšie potenciálne zneužiteľné chyby

- Rozdiely v implementácii RFC. Vážnym problémom je fakt že niektoré e-mailové klienty aplikujú RFC veľmi benevolentne. Čiže dekódujú aj také prílohy, ktoré by nemali byť dekódované prípadne nesprávne určia ich typ. Tým vystavujú užívateľov nezanedbateľnému riziku.
- Neschopnosť dekódovania špecifických dát niektorými antivírovými produktami. Ide o Unicode (UCT-2), UTF-7/UTF-8, prípadne o hodnotu poľa MIME Content-Length, ktorá môže byť zmanipulovaná.
- Mnoho ďalších bezpečnostných dier. Stále sa objavujú nové a záplaty neprichádzajú tak rýchlo aby zabránili ich zneužitiu autorom infiltrácií.

3.5. Zdroje e-mailových adries používané červami

- Windows address book
- Personal address book
- Web stránky
- ICQ databáza
- Súbory na lokálnom disku

4. Možné cesty zlepšenia bezpečnosti sytémov elektronickej pošty

4.1. Správcovia systémov by mali:

- Venovať dostatočnú pozornosť ochrane staníc. To je totiž miesto, kam je v drvivej väčšine infiltrácia cielená a kde sa teda nachádza vo vykonávateľnej a teda ľahšie detekovateľnej forme.
- Používať viac úrovní ochrany. Tento postup minimalizuje záťaž systému, hlavne pri veľkých epidémiách.
- Nepoužívať automatické zasielanie upozornenia o zachytenej infiltrácii odosielateľovi.
- Nepodceňovať všeobecné bezpečnostné opatrenia (používanie autentifikácie, uzavretie nepoužívaných služieb, dohľad a pod.)
- Školiť užívateľov o možných rizikách a o bezpečnom správaní pri práci s internetom.

4.2. Výrobcovia všetkého software by mali aplikovať systém automatizovaného a bezpečného aktualizovania.

4.3. Výrobcovia klientských systémov by mali pokiaľ je to možné striktne dodržiavať RFC. Mali by dať možnosť aby si užívateľ sám zvolil restrikcie formátu a obsahu správ.

4.4. Výrobcovia riešení pre servery by mali dbať aby ich riešenia blokovali e-maily nespĺňajúce RFC doporučenia. Mali by sledovať kompatibilitu svojich produktov s e-mail klientskými systémami.

5. Zopár príkladov

5.1. Win32/Nimda.A

Jedná sa o kombináciu červa a vírusu, ktorá sa šíri prostredníctvom elektronickej pošty a prostredníctvom známych dier v Internet Information Serveri (IIS) a Internet Exploreri. Šírenie sa začalo veľmi prudko 18. septembra medzi 15.00 a 16.00 nášho času. Rýchlosť šírenia červa bola v počiatočnom štádiu taká rýchla, že viedla k značnému zahlteniu a tým aj spomaleniu internetu.

Červ aktívne vyhľadáva počítače, na ktorý je nainštalovaný IIS s neošetrenými bezpečnostnými dierami. Toto skenovanie IP adries vytvára v súhrne masívnu prevádzku na internete. Ak nájde server, skúša ho napadnúť. V prípade, že server bol napadnutý červom Code Red 2, prostredníctvom dvoch backdoorov (root.exe a cmd.exe), ktoré na počítači Code Red 2 nainštaluje, sa snaží stiahnuť súbor ktorý obsahuje Win32/Nimda.A. Na svoje šírenie využíva aj chyby MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability (popis na www.securityfocus.com/bid/2708, záplata na www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp) a Microsoft IIS and PWS

Extended Unicode Directory Traversal Vulnerability (popis na www.securityfocus.com/bid/1806, záplata na www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp). Výsledkom napadnutia červom je, prítomnosť súboru *admin.dll* (čo je súbor obsahujúci červa) na serveri v koreňovom adresári disku a zároveň to, že návštevníci stránok na takomto webserveri môžu byť napadnutý červom po zobrazení stránky vo svojom prehliadači.

Červ na takýto spôsob napadnutia využíva chybu, ktorá sa vyskytuje v rozličných verziách Internet Explorera. Táto chyba, Microsoft IE MIME Header Attachment Execution Vulnerability, umožnuje spustenie programu na cieľovom počítači pri zobrazení webstránky. Presne takýmto spôsobom, prostredníctvom súboru *readme.eml*, dôjde k infekcií červom Win32/Nimda.A. Popis chyby nájdete na www.securityfocus.com/bid/2524, záplatu na www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp.

Po preniknutí červa a jeho spustení na cieľovom počítači dôjde k vytvoreniu kópie červa v dočasnom adresári, prípadne k nahradeniu súboru *mcc.exe*. Budú napadnuté súbory, ktoré sa nachádzajú v kľúčoch registru systému v HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths - tento kľúč obsahuje cesty k dôležitým systémovým súborom a tiež v HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders - ten obsahuje cesty k často používaným adresárom (napr. Desktop, Documents alebo Templates). V adresári s Windows v podaresári SYSTEM vytvorí súbor *load.exe* a zároveň doplní riadok s textom *shell=explorer.exe load.exe - dontrunold* do súboru *system.ini,* čím zabezpečí svoju opätovnú aktiváciu.

Červ tiež modifikuje nájdené súbory s príponami HTM, HTML, ASP a súbory s menami v ktorých sú slová INDEX, MAIN, DEFAULT a README a pridá k nim kód, ktorý pri zobrazení týchto súborov v prehliadači otvorí súbor s vírusom. Červ infikuje spustiteľné súbory po lokálnej sieti na zdieľaných diskoch, pričom nenapadne súbor winzip32.exe.

Adresy na šírenie prostredníctvom elektronickej pošty získava z html dokumentov (prípony HTM a HTML) uložených na disku, a zo správ elektronickej pošty. Červ posiela svoje kópie sám, pričom adresa aktuálneho užívateľa napadnutého počítača nie je adresou odosielateľa správy. Správa s červom má náhodný názov, v prípone sa nachádza súbor *readme.exe*.

5.2. Win32/Nimda.E

Na rozdiel od predošlých variánt (Nimda B, C, D), ktoré sa líšili len použitím rozličných metód komprimácie, táto je nekomprimovaná a mierne zmenený je kód červa. V tele sa nachádza text:

Concept Virus(CV) V.6, Copyright(C)2001, (This's CV, No Nimda.)

Príloha má názov *sample.exe*. Červ oproti starej verzii má zmenené aj niektoré mená vytváraných súborov (napr. *httpodbc.dll* namiesto *admin.dll*). Záplata, ktorá odstraňuje bezpečnostnú dieru v Internet Exploreri využívanú týmto červom je na: www.microsoft.com/windows/ie/downloads/critical/q290108/default.asp.

5.3. Win32/SirCam červ

Je to nebezpečný červ napísaný v Delphi, s dĺžkou približne 137 kilobajtov. Má schopnosť šíriť sa prostredníctvom elektronickej pošty a po zdieľaných diskoch v lokálnych počítačových sieťach.

Po lokálnej počítačovej sieti sa šíri tak, že v adresári \RECYCLED na dostupných zdieľaných sieťových diskoch vytvorí svoju kópiu pod názvom *SirC32.exe*. Potom zabezpečí svoju aktiváciu na tomto disku tým, že do súboru *autoexec.bat* pridá text *"@win \recycled\SirC32.exe"* alebo tým, že súbor *rundll32.exe* premenuje na *run32.exe* a pôvodný súbor funkčne nahradí svojou kópiou umiestnenou v adresári *\RECYCLED.*

Červ prichádza ako súbor v prílohe správy elektronickej pošty. Tento súbor má dve prípony, pričom druhou príponou je *pif, com, bat* alebo *lnk*. Táto správa má ako predmet nastavené meno súboru v prílohe. Telo správy obsahuje potom španiesky alebo anglický text. Voľba jazyka textu v tele správy závisí od nastavenie

preferovaného jazyka. Ak je ako preferovaný jazyk nastavená španielčina, text je v tomto jazyku, inak je v angličtine. Správu červ zostavuje náhodne z niekoľkých predvolených viet, pričom prvý a posledný riadok textu je vždy ten istý. V angličtine sú použité nasledovné texty:
Prvá veta: Hi! How are you?
Posledná veta: See you later. Thanks
Ostatné možné vety: I send you this file in order to have your advice
I hope you can help me with this file that I send
I hope you like the file that I sendo you
This is the file with the information that you ask for

V španielčine sú použité nasledovné texty:
Prvá veta: Hola como estas ?
Posledná veta: Nos vemos pronto, gracias.
Ostatné možné vety: Te mando este archivo para que me des tu punto de vista
Espero me puedas ayudar con el archivo que te mando
Espero te guste este archivo que te mando
Este es el archivo con la informacion que me pediste

Po spustení súboru v prílohe dôjde k aktivácií červa. Ten sa potom skopíruje pod menom *Sirc32.exe* do adresára *C:|RECYCLED* a pod menom *SCam32.exe* do podadresára \SYSTEM v adresári v ktorom je nainštalovaný operačný systém Windows. V registri systému červ v HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices pridá položku s hodnotou *Driver32=C:|WINDOWS|SYSTEM|SCam32.exe*, čím zabezpečí svoju opätovnú aktiváciu. Kľúč HKEY_CLASSES_ROOT\exefile\shell\open\command nastaví na hodnotu C:\recycled\SirC32.exe\ "%1\" %*", čo spôsobí že pri spustení akéhokoľvek súboru s príponou EXE sa spustí najprv kópia červa. V kľúči HKEY_LOCAL_MACHINE\Software\SirCam si červ uchováva niektoré údaje o aktuálne napadnutom počítači- napríklad počet spustení červa či meno pod ktorým je uložený.

Červ má niekoľko aktivačných rutín. Jedna z nich môže 16. októbra spôsobiť vymazenie všetkých súborov na disku C:. Ďalšia vytvorí v adresári C:\RECYCLED súbor sircam.sys a bude do neho zapísovať text *[SirCam_2rP_Ein_NoC_Rma_CuiTzeO_MicH_MeX]* alebo *[SirCam Version 1.0 Copyright (c) 2001 2rP Made in / Hecho en - Cuitzeo, Michoacan Mexico]* až pokým sa nevyčerpá voľné miesto na disku. Červ môže získať adresy na ktorá sa odošle dvoma spôsobmi - zo súborov s prípomani wab, ktoré obsahujú adresáre elektronickej pošty alebo z niektorých súborov na disku.

5.4. Win32/Klez.E

Win32/Klez.E je červ, ktorý sa šíri ako súbor v prílohe správ elektronickej pošty. Predmet správy, meno súboru v prílohe (ale nie jeho prípona) a telo správy je náhodné.

Využíva chybu v poštových klientoch Microsoft Outlook a Outlook Express popísanú na http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp, čo môže na počítačoch, ktoré nemajú túto chybu ošetrenú viesť k aktivácií červa už len zobrazením náhľadu správy.

Červ sa po aktivácií skopíruje do podadresára *SYSTEM* (Windows 9x/ME) alebo *SYSTEM32* (Windows NT/XP/2000) v adresári s operačným systémom ako súbor *Wink*.exe*. Miesto znaku "*" sa v mene súboru budú vyskytovať 2 až 3 malé písmená. Na zabezpečenie svojej aktivácie po reštarte systému vytvorí kľúč v HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Červ sa snaží deaktivovať rezidentné antírusové programy Norton Antivirus, Scan, Antivir, Sophos Antivirus, AVP/KAV, F-Secure, F-PROT, NOD32, PC-cillin, prípadne vymazáva súbory, ktoré obsahujú kontrolné súčty jednotlivých antívírusových programov.

Červ sa má schopnosť šíriť po lokálnych počítačových sieťach ako EXE súbor s dvojitou príponou, prípadne ako RAR archív obsahujúci červa s dvojitou príponou.

Červ získava adresy, na ktoré sa bude rozposielať z WAB súborov a zoznamu užívateľov ICQ. Súbor pripojený ku správe odoslanej červom má príponu *PIF, SCR, EXE* alebo *BAT*. Meno súboru je náhodne generované. Červ vytvára na disku vírus Win32/ElKern.B. Šiesty deň nepárnych mesiacov prepisuje súbory na disku na náhodnými údajmi.

5.5. Win32/Mylife.B

Je to červ, napísaný vo Visual Basicu a skomprimovaný utilitou UPX. Šíri sa ako príloha správ elektronickej pošty s predmetom *bill caricature* a prílohou cari.src.

V tele správy sa nachádza text:

Hiiii

How are youuuuuuuu?

look to bill caricature it't vvery verrrry ffffunny :-):-)

i promise you will love it? ok

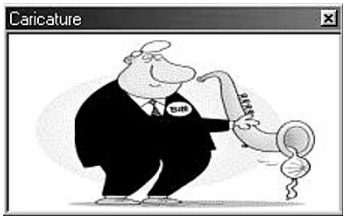
buy

========No Viruse Found========

MCAFEE.COM

Autor sa neumelo snaží vyvolať dojem, že správa bola skontrolovaná antivírusovým programom. V texte ale urobil niekoľko chýb, čo naznačuje, že angličtina nie je jeho materským jazykom.

Po spustení súboru v prílohe sa zobrazí nasledovné okno:



Červ sa skopíruje ako súbor cari.scr do podadresára SYSTEM v adresári s nainštalovaným operačným systémom Windows. Svoju aktiváciu po reštarte zabezpečí vytvorením kľúca HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run s hodnotou *"win"="C:|WINDOWS|SYSTEM|cari.scr".* Červ rozpošle svoje kópie na všetky adresy, ktoré nájde v adresári klienta elektronickej pošty Microsoft Outlook.

Červ obsahuje nebezpečnú deštrukčnú rutinu, ktorá sa aktivuje, pokiaľ je červ spustený pri reštarte systému medzi 8:00 a 8:59 podľa vnútorných hodín počítača. V takomto prípade vymaže súbory s príponou sys, vxd, ocx a nls v adresári s nainštalovaným operačným systémom Windows a súbory nachádzajúce sa v koreňovom adresári diskov C: až F:.

6. Záver

Infiltrácie z našich e-mailov hneď tak nezmiznú. Snáď sa ale možno dožijeme doby keď nebudú predstavovať tak výrazný ekonomický a sociálny problém. Často by stačilo aby tvorcovia e-mail systémov mali na pamäti jednoduchú zásadu: Dovoliť spustiť prílohu k e-mailu je podobné ako dovoliť používať svoj počítač hocikomu.

7. Literatúra a linky

7.1. What is Wild?, Sarah Gordon, 20th National Information Systems Security Conference, October 1997 - Baltimore, Maryland

7.2. The First E-mail message, Todd Campbell, Pretext magazine, issue 5, The Hidden History of Internet

7.3. The Morris Internet Worm, Thomas Darby a Charles Schmidt, 1998

7.4. Protecting your network against email threats: How to block email attacks & viruses, GFI Software Ltd., 2002

7.5. Vírusová encyklopédia NOD32, Ing. Miroslav Trnka a MUDr. Peter Kováč, Eset s. r. o., 1992-2002

Informácie o nových bezpečnostných dierach:

http://www.microsoft.com/technet/security/
http://www.guninski.com
http://security.nnov.ru/advisories/content.asp
http://msgs.securepoint.com/bugtraq/

TROŠKA ŠPINAVÝCH TRIKŮ

Petr Odehnal, Grisoft Software

Mailem se šířící viry musí pro své úspěšné přežití přesvědčit příjemce infikované zprávy že otevření přiloženého dokumentu je dobrý nápad.

Pokusme se podívat na prostředky, které k tomu používají.

Internet

Nevím jak budou jednou badatelé říkat naší epoše, ale nejspíš "mladší doba internetová". Skoro si troufám říct, že internet přinesl revoluční změnu (třetí v pořadí) v komunikaci mezi lidmi.

Objev řeči dovolil výměnu informací mezi jedinci, vynález knihtisku umožnil autorovi sdělit jeho moudra "všem" lidem a internet efektivně zprostředkovává komunikaci "všech se všemi".

Ostatně se domnívám, že rozmach internetu definitivně dokázal známou cimrmanologickou poučku, že řeč nevznikla z potřeby domluvy při společné práci, ale že se člověk prostě potřebuje vykecat.

Internet je dnes neuvěřitelně rozsáhlou sbírkou zbytečných a nepřesných informací, přehlídkou silných řečí vedených z bezpečné anonymity nějaké freemailové adresy a neustále opakovaných poťouchlostí všeho druhu.

Předpokládám, že každý kdo internet používal déle jak hodinu už příliš dobře ví jak se anglicky řekne Kryštof Harant z Polžic a Bezdružic nebo dokáže rozluštit hádanku "je to černé a ťuká to na sklo".

Kromě blábolů všeho druhu ale internet obsahuje také slušné množství užitečných informací (tedy alespoň zatím) a tak s ním víceméně spokojeně přežíváme a každou minutu se k nám přidávají mraky dalších uživatelů.

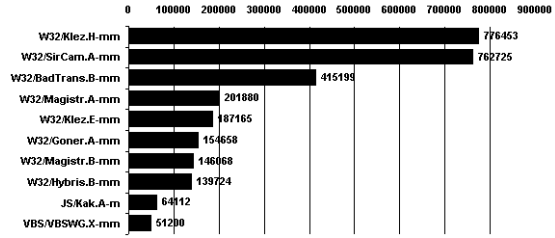
Internet a viry

Jak by na světě bylo krásně, kdyby jediným problémem internetu byl trošku vyšší podíl blábolení na jeho obsahu.

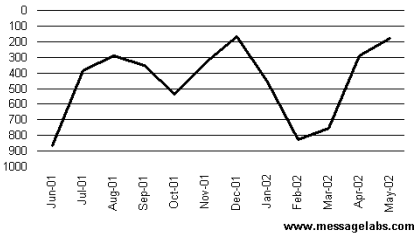
Internet je ale také bohužel nejnebezpečnějším zdrojem infekce. Ne snad že by ostatní způsoby šíření virů vymíraly, ale email dnes v tomto orchestru jednoznačně hraje první housle.

Umožňuje totiž masivní šíření infekce v relativně krátkém čase. Například první mass mailing virus - W97M/Melissa.A - potřeboval ke svému celosvětovému rozšíření čtyři dny a byla to rychlost na tu dobu nevídaná. I-Worm/ExploreZIP to zvládnul za den - byť jeho epidemie nezasáhla takové množství počítačů jako bývá zvykem u ostatních rozšířenějších mass-mailing virů. VBS/LoveLetter (známý jako Iloveyou) byl všude za čtyři hodiny a (zatím) poslední rekordman (I-Worm/Klez.H) potřeboval jenom půl hodiny.

Jenom pro ilustraci jsem vytáhnul pár dat sesbíraných firmou Messagelabs, která kontroluje maily svých zákazníků:



Tuhle "all-time" hitparádu, sčítající nalezené exempláře virů za celou dobu fungování Messagelabs, mám velmi rád. Je nutně nepřesná protože počet klientů (a tím i kontrolovaných emailových adres) se v čase mění, ale pro hrubou představu o tom jak vypadá "první liga" ve virové hitparádě bohatě stačí.



Tento graf zobrazuje na kolik mailů zkontrolovaných

v Messagelabs připadl jeden zavirovaný. Asi nepřekvapí, že rekordní hodnoty najdeme v dobách epidemie vrcholící virů I-Worm/SirCam (prosinec 2001) a I-Worm/Klez.H (květen 2002), ale za pozornost určitě stojí ta čísla jako taková: V dobách zuřících epidemií je v každých 200 mailech nalezen alespoň jeden virus!

A to se prosím pěkně bavíme o všech emailech. Pokud se podíváme na maily, které jako přílohu obsahují spustitelný program, tak dostaneme mnohem zábavnější čísla. Tohle je například reálná statistika jednoho "běžného" dne v Messagelabs:

Zachyceno bylo celkem 11000 EXE souborů. Z toho bylo 8000 známých virů a 2700 známých žertovných programů, takže jenom 300 souborů bylo snad možná případně mohlo obsahovat něco užitečného. Domnívám se ovšem že většina z toho byly také žertovné programy, pouze v čase toho testování ještě neznámé.

Zdá se tedy, že implementovat na mailserveru pravidlo blokující doručení všech spustitelných souborů vůbec není špatný nápad!

Spustím se sám

Čestnou výjimkou z pravidla o "nutnosti spolupráce" uživatele při šíření emailového viru představují viryvyužívající chyb ve starších verzích Internet Exploreru. Na první pohled se pravda může zdát že webový browser má se zpracováním pošty společného asi tolik jako tuzemské politické strany se slušností, ale v integrovaném světě Windows používají mailery Outlook a Outlook Express pro zobrazení HTML formátované zprávy služeb Exploreru.

Vedlejším účinkem tohoto řešení je, že HTML mail je zpracováván opravdu důkladně - včetně třeba věcí jako automatického přehrání přiloženého souboru se zvuky. To je sice jenom pitomoučké, ale zase až tak by to nevadilo. Kdyby. Kdyby se do zpracování nevloudila drobná chybička. Starší verze Exploreru totiž narazí na informaci, že přiložen je zvukový doprovod a odešle ten soubor do dalších vrstev Windows s pokynem "přehrejte to".

Pokud je ovšem místo korektního audio souboru přiložen spustitelný program, tak je díky svému původu prohlášen za bezpečný kus kódu a bez milosti spuštěn.

Tento trik patří k běžné výbavě většiny novějších virů a proto bych uživatelům Outlooku a Outlook Expressu vřele doporučil stáhnout a aplikovat bezpečnostní záplaty které pro zavření pár bezpečnostních děr Microsoft vydal.

Jak zamaskovat co jsem zač

Ve Windowsoidním světě o typu souboru rozhoduje jeho jméno, resp. přípona a jen trošku zkušenější

uživatelé jsou už zvyklí si dávat pozor na napadnutelné soubory nejprofláknutějších typů. Proto konstrukce jméno souboru připojeného k virem poslané zprávě hraje důležitou roli.

Tři králové: SCR, PIF a LNK

Soubor AHOJ.EXE doraziví mailem si dnes už za normálních spustí pravděpodobně jenom velmi dobrodružná povaha. Viroví pisálci ale objevili další přípony, které mají z praktického pohledu na věc stejný význam. Stačí vzít normální EXE soubor, přejmenovat ho s použitím některé z těchto přípon a double click ve Windows ho spolehlivě spustí.

Ikona

Soubor typu EXE v sobě nese i informaci o tom, jak má vypadat jeho "prezentace" na ploše Windows ikonu. Na toto konto použil pěkným trik virus I-Worm/Naked, který používal ikonku EXE souborů vyráběných populárním programem pro vytváření animací.

Překvapivě velké množství uživatelů (i těch zkušenějších) si tento virus spustilo v domnění, že uvidí nějaké legrácky.

Schovám se za bratříčka

Ve starých dobrých dobách DOSu bylo vše jasné. Vlastní jméno souboru mělo maximálně 8 znaků a tečkou oddělená přípona nanejvýš 3 znaky.

Dlouhé názvy souborů do tohoto zaběhaného systému vnesly trošku zmatku a to je samozřejmě situace, která virovým pisálkům vyhovuje. Jméno souboru tak totiž může obsahovat libovolné množství teček a teprve za poslední z nich je to, co Windows použijí jako příponu pro rozlišení typu souboru.

A aby to bylo ještě o trošku zábavnější, tak konfigurace Windows dovoluje tuto skutečnou příponu skrýt a typ souboru je pak vyjádřen pouze odpovídající ikonou.

Takže soubor se jménem TAJNE.ZIP.EXE může uživatel vidět jako TAJNE.ZIP a pokud byl autor viru jenom o fous chytřejší než hromada bláta, tak ho vybavil typickou ikonkou datového souboru WinZIPu a ke spuštění takového souboru je pak jenom krůček.

Schovám se daleko

Další milou vlastností dlouhých jmen souborů je, že mohou bát opravdu velmi dlooooooouhá. Prostor pro zobrazení názvu souboru v aplikacích ale bývá omezen a příliš dlouhá jména je zvykem ořezávat. Takže stačí použít před poslední a rozhodující příponou dostatečné množství mezer:

KOZY.JPG [*SPOUSTA MEZER, PRIPONA JE HODNE VPRAVO*] .EXE

a příjemce tohoto souboru uvidí jenom lákavé KOZY.JPG. No a je snad jasné, že takový obrázek si každý chlap (který má rád přírodu) s chutí otevře v domnění že uvidí fotografii kamzíků skotačících na hřebenech Karpat.

Takhle se přece viry neposílají

Přece jenom máme zažité jakési "obvyklé modely chování virů" a pokud se virus pošle dostatečně netypickým způsobem, tak příjemci nemusí začít "blikat červená kontrolka".

Příkladem z doby relativně nedávné je český I-Worm/Cervivec, který se posílá jako EXE soubor zabalený uvnitř archivu .ZIP s tímto textem:

Cau posilam ti cerviky tak se na to podivej (virus to neni) Když k tomu připočítáme že ten mail dorazí od člověka kterého adresát dobře zná (měl jeho mail ve svém seznamu kontaktů v ICQ) a ve správném jazyce (virus si vybírá text zprávy podle koncovky internetové adresy z osmi různých jazykových verzí), tak je jasné že spoustě adresátů vůbec nepřipadal podezřelý.

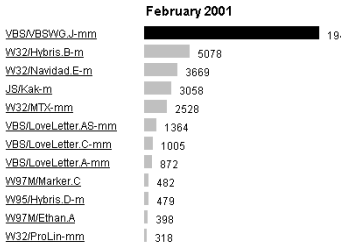
Dlužno ovšem podotknout, že díky tomuto způsobu šíření se sice Cervivec dokázal rychle rozšířit v uzavřené komunitě lidí "co si spolu píšou na ICQ" ale svým rozšířením nedosáhl běžným mass-mailing virům (tedy těm které se bezhlavě rozesílají na všechno co vypadá jako emailová adresa) ani po kotníky.

Málo známé nebezpečí

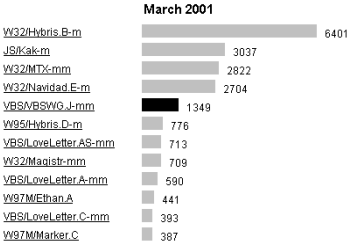
S rostoucí složitostí Windows se objevují stále nové a nové typy souborů, které mohou být nosičem infekce. Příkladem mohou být třeba HLP nebo THEME soubory. Už se sice objevily viry demonstrující zneužitelnost těchto souborů ale dokud nebudou použity v nějakém rozsáhlejším útoku, který by si získal publicitu, tak se o tom moc lidí nedozví a při prvním setkání s takovouto infekcí budou pravděpodobně ochotni přiložený soubor spustit.

Lákavé jméno

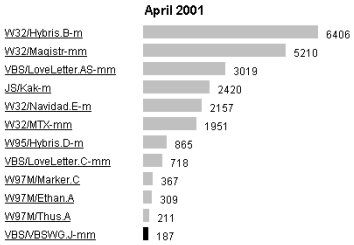
Zkušenosti s virem VBS/VBSWG.J (známějším jako AnnKournikovova) ukazují, že občas není třeba vymýšlet nějaké perfektní finty a triky. Dostatečně lákavé jméno přiloženého souboru s virem se může postarat o šíření takřka zázračné. Tahle taktika stačí k rychlému rozšíření ale dlouhodobější úspěch takové viry nemají.



Poprvé byl tento virus zachycen 12. února a za dva týdny nasbíral docela vysoké skóre.



V březnu už zůstal po běžnými viry.



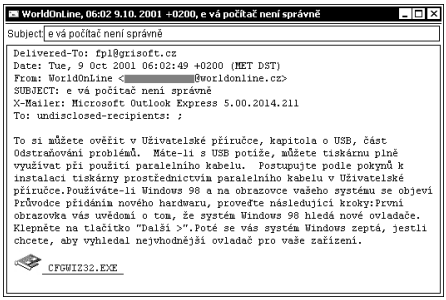
V dubnu pak dosáhl stádia "klinické smrti" a v květnu už nebyl zachycen ani jednou.

Dodnes se sice ojediněle objeví, ale dny jeho slávy jsou zjevně sečteny.

Důvěryhodný text

Nějaké méně podezřelé jméno souboru není zase až takový problém vymyslet, ale s vlastním obsahem mailu to není tak jednoduché. Zkuste si schválně vzít textový editor a napsat pár řádků mailu, který by neměl vzbudit podezření - uvidíte že to není nic triviálního.

Různé viry přinesly různé pokusy o vyřešení tohoto problémů. Docela zajímavý (a překvapivě úspěšný) způsob používá I-Worm/Magistr - prostě si náhodně "vylosuje" nějaký text z disku a jeho fragment vloží do těla zprávy.


WorldOnLine, 06:02 9.10. 2001 +0200, e vá počítač není správně

Subject: e vá počítač není správně

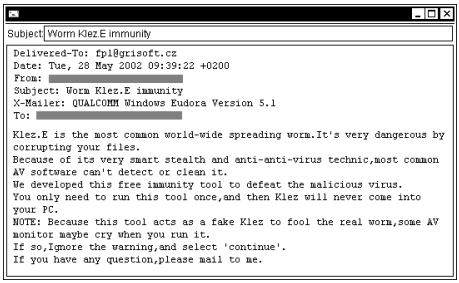
```
Delivered-To: fpl@grisoft.cz
Date: Tue, 9 Oct 2001 06:02:49 +0200 (MET DST)
From: WorldOnLine <[redacted]@worldonline.cz>
SUBJECT: e vá počítač není správně
X-Mailer: Microsoft Outlook Express 5.00.2014.211
To: undisclosed-recipients: ;

To si můžete ověřit v Uživatelské příručce, kapitola o USB, část
Odstraňování problémů.  Máte-li s USB potíže, můžete tiskárnu plně
využívat při použití paralelního kabelu.  Postupujte podle pokynů k
instalaci tiskárny prostřednictvím paralelního kabelu v Uživatelské
příručce.Používáte-li Windows 98 a na obrazovce vašeho systému se objeví
Průvodce přidáním nového hardwaru, proveďte následující kroky:První
obrazovka vás uvědomí o tom, že systém Windows 98 hledá nové ovladače.
Klepněte na tlačítko "Další >".Poté se vás systém Windows zeptá, jestli
chcete, aby vyhledal nejvhodnější ovladač pro vaše zařízení.
```

CFGWIZ32.EXE

Tohle je příklad reálného mailu vyrobeného Magistrem. Je to sice ryzí blábol, ale musím připustit že jsem už dostal už spoustu ještě šílenějších mailů, napsaných reálnými lidmi.

I-Worm/Klez.H si generuje krátké anglické větičky pomocí malého slovníčku a jednoduché sady pravidel. Kromě toho se ale občas pošle i v tomto půvabném mailu:


Subject: Worm Klez.E immunity

```
Delivered-To: fpl@grisoft.cz
Date: Tue, 28 May 2002 09:39:22 +0200
From: [redacted]
Subject: Worm Klez.E immunity
X-Mailer: QUALCOMM Windows Eudora Version 5.1
To: [redacted]

Klez.E is the most common world-wide spreading worm.It's very dangerous by
corrupting your files.
Because of its very smart stealth and anti-anti-virus technic,most common
AV software can't detect or clean it.
We developed this free immunity tool to defeat the malicious virus.
You only need to run this tool once,and then Klez will never come into
your PC.
NOTE: Because this tool acts as a fake Klez to fool the real worm,some AV
monitor maybe cry when you run it.
If so,Ignore the warning,and select 'continue'.
If you have any question,please mail to me.
```

Drzost s jakou se vydává za prostředek k odléčení svého staršího bratříčka je půvabná. A závěrečné upozornění, že se přiložený soubor možná nebude některým antivirům líbit - to už je jenom taková třešňička na dortu.

Událost kterou čekám

Obsah zprávy není jediným kritériem podle kterého příjemce posuzuje důvěryhodnost zprávy. Důležitou roli také hraje zda vůbec podobný mail čeká.

Proto například Win32/Ska (známější jako Happy99) monitoruje poštu odesílanou z napadeného počítače a za každým mailem pošle ještě další prázdnou zprávu, ke které se připojí.

A ještě o fous chytřeji to dělá I-Worm/ExploreZip který sleduje přijatou poštu a na zprávy sám odpovídá ve smyslu "nemám teď čas zatím se podívej na přiložený dokument". Že je místo dokumentu přiložená kopie viru asi není nutné říkat.

Nožičky a závěr

Strašně rád bych na tomhle místě napsal něco na způsob "kupte si antivirový program XYZ, nainstalujte ho a pak už můžete po zbytek života se založenýma rukama sledovat marné pokusy virů o průnik do vašeho systému". Nemůžu. Je sice pravda že antivirové programy jsou pořád ještě mnohem účinnější než třeba zařikávání, ale 100% bezpečnost sám o sobě žádný takový systém nezajistí.

Riziko, že zrovna vy obdržíte vzorek nějaké novinky hned v "první vlně" (v prvních pár minutách světové epidemie) je reálné a nelze ho podceňovat.

Pořád tedy platí, že opatrné zacházení s doručenou poštou je základním předpokladem pro bezpečné přežití.

CELKOVÝ OBRAZ VIROVÉ A ANTIVIROVÉ PROBLEMATIKY V ROCE 2001, VÝHLEDY NA ROK 2002

Pavel Baudiš, ALWIL Software, Průběžná 76, 100 00, Praha 10
e-mail: baudis@asw.cz, www: http://www.asw.cz

Co nás potkalo v roce 2001

Události za poslední rok na virové scéně rozhodně nelze označit za nudné. Objevila se celá řada nových virů, nových epidemií a nových problémů. Autoři virů se naučili opravdu naplno používat možností, které jim současné operační systémy, aplikace a připojení na Internet nabízejí. Zvykli si též masívně využívat bezpečnostní díry v nejpoužívanějších aplikacích, a tak je možno říci, že se situace s viry dost zhoršila. Zažili jsme několik velkých epidemií, které zasáhly během velice krátkého času celý svět. A právě rychlost a mohutnost těchto událostí byla bohužel největší novinkou uplynulého roku.

Obecné trendy

Poslední vývoj potvrzuje trendy z minulého roku - tedy ústup makrovirů, bouřlivý nástup Win32 virů, které pro své šíření aktivně využívají elektronickou poštu a na řadě počítačů kvůli bezpečnostním dírám ani nepotřebují pro svoji aktivaci spolupráci chudáka uživatele.

Viry jsou většinou psány ve vyšším programovacím jazyce (např. C++ kompilovaný VB či Delphi). Jejich velikost často přesahuje hranici 100 kB, což příliš neomezuje jejich šíření, ale značně znepříjemňuje jejich analýzu a takřka vyřazuje ze hry detekci heuristickými metodami, protože jejich virální či destruktivní činnost je skryta hluboko uvnitř balastu, vytvářeného překladači vyšších programovacích jazyků.

Elektronická pošta rozhodně zůstala nejdůležitějším kanálem šíření virů, její podíl se dokonce ještě zvýšil. Velkou roli zde kromě už zmíněných bezpečnostních děr hraje psychologie - autoři virů prokázali, že jsou velmi vynalézaví. Pár příkladů z této oblasti si ukážeme dále na konkrétních případech virů.

Viry se prostě dnes šíří velmi rychle - během několika málo hodin jsou schopny "zaplavit" celý svět. Zcela klíčovým problémem se tak stává rychlost aktualizace antivirových programů a její okamžitá aplikace u uživatelů. Detekci nového viru není problém do programu přidat - daleko obtížnější je dostat takto vytvořenou ochranu co nejrychleji a nejjednodušeji k uživatelům. Budoucnost zcela bezpochyby patří k malým, rozdílovým a zcela automaticky bez zásahu uživatele probíhajícím aktualizacím. Programy, které je nutno kvůli každému přidanému viru celé stáhnout a znovu naistalovat, již dnes snad vůbec neexistují a pokud ano, měly by se co nejrychleji přesunout mezi dinosaury.

Spolupráce antivirových firem

Je zcela jasné, že antivirové firmy reagovaly na poslední vývoj, zejména vzestup virů orientovaných na e-mail. Technická spolupráce již funguje řadu let, ale nové problémy si vyžádaly její rozšíření. Většina firem spolu po technické stránce velmi úzce spolupracuje a je zapojena do systémů, které slouží k okamžité výměně informací o nových virech, popřípadě i jejich vzorků. To vše přispívá k jeho rychlejší detekci a k minimalizaci jeho šíření i jím způsobených škod. Diskusní skupiny ale umožňují řešení dalších důležitých otázek: jak se bude virus jmenovat, co vlastně dělá a jak rychle se opravdu šíří. Díky tomu pak mohou firmy rychleji přidat detekci nových virů a také informovat své zákazníky i média. Funkčnost této spolupráce se již mnohokrát potvrdila.

Konkrétní případy virů za poslední rok

Win32:Sircam

Tento virus se objevil v červenci 2001 a je v době psaní příspěvku dosud nejrozšířenějším virem vůbec, i když ho v době, kdy tyto řádky budete číst překoná Klez-H. Za své úspěšné šíření vděčí jednak nové metodě sbírání adres z HTML dokumentů na lokálním disku, jednak tomu, že posílá náhodně vybrané doku-

menty, které po otevření v poštovním klientovi adresáta fungují (samozřejmě spolu s aktivací viru). To je také jeho největším nebezpečím - tak masový únik často citlivých dat ještě Internet určitě nezaznamenal! Dalším problémem bylo zahlcení poštovních stránek, protože připojené dokumenty mohou být velmi rozsáhlé a v době největší epidemie v srpnu 2001 tím trpěli hlavně uživatelé, používající vytáčenou linku.

Win32:CodeRed

Tento worm je velice zvláštní. Pro svoji aktivaci využívá bezpečnostní díru MS IIS Web serveru a na napadeném počítači existuje pouze v paměti. Sebe sama posílá jako HTTP požadavek, chyba v přetečení zásobníku ale způsobí spuštění kódu viru. Worm se též pokoušel o masivní DoS útok na webové stránky Bílého domu, ale naštěstí přes fixní IP adresu, takže obrana byla triviální. Worm získal obrovskou publicitu ve všech médiích, vyjadřovali se k němu politici a dokonce i Dalajláma. Brzy nato se objevilo několik variant, z nichž za zmínku stojí Win32:CodeRed.C. Ta totiž již zasahovala do systému a poměrně jednoduchým způsobem otevírala jakási zadní vrátka případným dalším útokům či virům. U takto napadeného systému není možno zaručit jeho integritu. Podle střídmých odhadů CodeRed napadl kolem 300 000 počítačů, kolik z nich má dodnes problémy se zadními vrátky se lze jen dohadovat. Objevily se i pokusy bojovat proti wormu podobným wormem, ale to už je spíše vytloukání klínu klínem.

Win32:Nimda

Jedná se o velmi komplikovaný virus, který využívá spoustu cest, jakými proniknout do systému: šíří se elektronickou poštou (bez záplaty může být spuštěn při zobrazení zprávy), po lokálních sítích a hledá i MS IIS Web Servery se zadními vrátky otevřenými wormem CodeRed.C (viz výše). Pokud najde na lokálním disku HTML či ASP soubory, upraví je tak, že při jejich zobrazení dojde pomocí skriptu k nabídce stažení viru ve formě EML souboru. Kromě toho, že využívá bezpečnostní díry a zadní vrátka, manipuluje sám s nastavením sítí: povoluje sdílení lokálních disků a mění práva uživatele Guest. V září virus způsobil menší epidemii, částečně aktivní je dodnes, což je vidět na záznamech o hledání zadních vrátek wormu CodeRed.C.

Win32:Badtrans

Tento virus odpovídá na všechny nepřečtené zprávy v programu Outlook. Do systému vypouští trojského koně, který zaznamenává a odesílá všechny stisknuté klávesy v určitých oknech. Opět se jedná o únik citlivých informací od uživatele k autoru viru. Velmi rozšířená byla na přelomu listopadu a prosince varianta Badtrans.B, která začala využívat novinky poslední doby: bezpečnostní díru IFrame a vyhledávání adres v HTML/ASP souborech. Před jméno odesílatele je přidán znak podtržítko, který způsobí, že případné varování před virem nenalezne svého adresáta.

Win32:MyParty

Virus se objevil v lednu a byl zajímavý dvěma věcmi: nabízel prohlédnutí fotografií z oslavy, přičemž připojený soubor se jmenoval www.myparty.yahoo.com, což na první pohled vypadá jako neškodná a důvěryhodná webová adresa, přestože se jedná o spustitelný soubor s příponou "COM". Virus samotný se byl schopen šířit jen v krátkém období pěti dnů. Později objevená varianta měla toto časové okno posunuto. Naštěstí se nepotrvdily obavy, že se budeme setkávat s novými a novými modifikacemi.

Win32:Mylife

Jedná se o velice primitivní worm, napsaný v jazyce Visual Basic a komprimovaný pomocí UPX (to je velmi oblíbená kombinace). Zajímavé je to, že jeho autor během letošních velikonoc vypustil minimálně čtyři odlišné varianty. Něco podobného se stalo i v prosinci, kdy se ve velmi krátkém časovém úseku objevilo více než 30 variant viru Win32:Shoho.

Win32:Cervivec

Tento worm je napsaný v Delphi a zabalený programem UPX. Je s největší pravděpodobností českého původu. Po spuštění na monitoru zobrazuje zvláštní efekty: různobarevné čáry "lezou" po obrazovce až ji celou zaplní.

Šířil se v komunitě uživatelů programu ICQ, jehož databázi adres také využívá pro hledání dalších obětí. Worm se posílá ve formě souboru ZIP, takže program nemůže být spuštěn přímo. Používá však zajímavou psychologickou fintu, aby přinutil uživatele soubor rozbalit a spustit. Upozorňuje totiž na zajímavý program, který ale neobsahuje virus. Toto upozornění vypadá velmi věrohodně, navíc může být napsáno v jednom z osmi jazyků. Naštěstí neobsahuje žádnou destrukční činnost.

Win32:Klez

Jedná se o poměrně velkou rodinu virů, které pocházejí pravděpodobně z Číny. K nejrozšířenějším zcela určitě patří Klez-E z listopadu 2001 a Klez-H, který se objevil 17. dubna 2002. Win32:Klez-H způsobil dosud vůbec největší epidemii a v době, kdy čtete tento materiál, již takřka zcela jistě překonal v počtu výskytů dosud vedoucí Sircam. Virus nepřináší žádné převratné novinky, kombinuje ale řadu vlastností, které se objevily v posledním půlroce a které zásadním způsobem ovlivňují jeho šíření. Tou nejdůležitější je využití bezpečnostní díry v Internet Exploreru, která způsobí automatické spuštění viru již při náhledu zprávy v programech Outlook a Outlook Express. Opravná záplata na tuto nebezpečnou díru existuje již mnoho měsíců, ale počet uživatelů, kteří ji nemají instalovanou, je bohužel natolik veliký, že celkově oprava nemá žádný vliv. K úspěšnému šíření přispívají i další skutečnosti: rodina virů Klez má totiž další nepříjemnou vlastnost: do položky odesílatele nenapíší emailovou adresu skutečného uživatele infikovaného počítače, ale místo toho vyberou adresu, kterou buď najdou v souborech na disku nebo vyberou ze seznamu, který si uchovávají v sobě. Adresu skutečně infikovaného počítače je možno zjistit pouze z detailních záznamů ve zprávě, jeho email však většinou nikoli. To má dva velice nepříjemné důsledky: jednak není možno uvědomit skutečně infikovanou osobu o tom, že je její počítač zavirován a jednak často vede k nepravdivému obvinění: "Vy jste nám poslal virus", a to jak k ručně vytvořenému, tak vygenerovanému automaticky, nejčastěji antivirovými programy na poštovních serverech. Adresát takového upozornění je pak často zmaten a marně se snaží virus na svém počítači najít. Zprávy vytvořené virem Klez-H jsou velice proměnlivé. Předmět zprávy je vytvářen komplikovaným způsobem z několika "náhodných" částí nebo dokonce z textu, který virus najde někde na disku a občas vypadá docela věrohodně. Někdy se dokonce vydává za program, sloužící k odstranění viru Klez-E, zaslaný některou z antivirových firem! Psychologické finty, které dnes viry používají, jsou zkrátka čím dál tím propracovanější. Virus Klez-H (na rozdíl od předchozí varianty Klez-E) neprovádí žádnou destrukční činnost, spočívající v ničení souborů. Přesto může být velmi nepříjemný i z dalšího důvodu: čas od času posílá kromě viru i náhodně zvolený soubor. Může tak dojít (podobně jako u viru Sircam, který to ale provádí zcela systematicky) k úniku citlivých dat, které by se v žádném případě neměly dostat z počítače ven.

2002: Co nás tedy čeká?

Brzy po objevení wormu CodeRed se objevilo několik teoretických studií, které se zabývaly zkoumáním optimálního chování fiktivního wormu budoucnosti. Bylo prokázáno, že pokud by takový worm využíval dosud neznámou bezpečnostní díru a měl předem alespoň částečně vytvořený seznam možných cílů, bylo by jeho šíření mnohem rychlejší. Worm popsaný pod jménem Warhol by pak byl schopen infikovat všechny vhodné cíle během patnácti minut (od jeho patnácti minut slávy pro každého je také odvozeno jeho jméno :). Jeho optimalizovaná varianta, pojmenovaná Flash, která si zpočátku nese celý seznam obětí a která má navržen i přesný vektor šíření (beroucí v potaz propustnost jednotlivých částí sítě) by totéž dokázala za třicet sekund! Je vidět, že podobné scénáře by dokázaly Internet ochromit a reakce na ně by mohla být víc než problematická.

Ale zpět k elektronické poště: největším problémem dneška je obrovské množství instalovaných systémů, ve kterých nejsou ošetřeny bezpečnostní díry. To umožňuje virům úspěšně přežívat a množit se na další a další počítače, přičemž naděje na jejich úplné vymýcení je mizivá. Uživatelé také často nepoužívají žádný antivirový program, popřípadě jej dostatečně často neaktualizují. Virus Win32:Aliz, který se objevil v listopadu, znaly všechny antivirové programy minimálně půl roku. Přesto se dokázal během krátké doby dost rozšířit… Tento problém se týká hlavně domácích uživatelů, a to přesto, že některé antivirové programy mohou používat legálně zcela zdarma. Firemní sítě jsou na tom o něco lépe, a proto je možné sledovat zajímavý jev: nové úspěšné viry se šíří zpočátku hlavně mezi firemními uživateli ale po uplynutí několika dní se hlavní zdroj šíření přesouvá právě k domácím uživatelům - firemní sítě už jsou totiž většinou chráněny.

Přesto je i zde co zlepšovat a hlavně dodržovat určitá pravidla prevence virové nákazy. Je důležité zavést ochranu poštovních serverů, nastavit potřebné filtry (odstanění nebezpečných typů souborů je velice efektivní!), používat a pravidelně aktualizovat antivirové programy a vypracovat krizový scénář, který by minimalizoval případné škody, způsobené virem a zkrátil na minimum možný výpadek firemní pošty. Ke správné ochraně patří bezpochyby i kvalitní zálohování.

Pro viry a jejich autory se už brzy objeví nové zajímavé platformy: PDA počítače spojené do jednoho zařízení s mobilním telefonem a podporujícím zasílání programů/skriptů a multimediálních dat. Pak už opravdu může jít do tuhého, protože veškeré vlastnosti, potřebné ke vzniku a úspěšnému šíření virů, budou k dispozici. A skutečně bude záležet na tom, zda použitý operační systém se zaměří spíše na bezpečnost než na uživatelský komfort. Bill Gates se v lednu začal na základě velkého tlaku uživatelů chytat za hlavu a prohlásil, že do budoucna je pro Microsoft bezpečnost důležitější než nové vlastnosti. Pro Windows je už možná trochu pozdě, teď jde o to, aby se podobné chyby neopakovaly na nových platformách a aby se malé počítače budoucnosti nestaly noční můrou!

ANTIVIROVÁ ŘEŠENÍ PRO VSTUPNÍ BRÁNY A UNIXOVÉ SERVERY

Tomáš Vobruba, AEC, tomas.vobruba@aec.cz

Přednáška se, jak již je patrno ze samotného názvu, dělí na dvě na sobě nezávislé části. Jediné co ji doopravdy spojuje je sama podstata; tedy řešit antivirovou ochranu na proprietárních řešeních. Slovo "proprietární" přitom značí jakousi unikátnost či spíše jedinečnost použití.

Snad první otázkou, která každému přijde okamžitě na mysl je, zda má vůbec antivirová ochrana na těchto systémech smysl. Odpověď na ni není zcela jednoznačná, celá problematika by se dala uvést následující větou: "Antivirová ochrana na vstupních branách do internetu a na unixových systémech rozhodně smysl má, ale…"

To "ale" by mělo každého upozornit na skutečnost, že oblast antivirové ochrany na výše zmíněných úrovních má svá úskalí a omezení a zároveň, že není ještě všem dnům konec. Pusťme se proto do rozboru dnešní situace v obou kategoriích a zároveň se pokusme zdůraznit jejich klady a zápory.

Antivirová řešení pro internetové vstupní brány

Po nedávné katastrofě s červem Klez.H, který stihnul obletět svět za neuvěřitelných šest hodin, se jistě všichni shodneme, že důležitost antivirové ochrany se přesouvá ze stanic a souborových serverů na servery poštovní nebo ještě lépe na vstupní brány.

Vstupními branami máme na mysli jakékoliv "pojítko" do internetu. Takovým místem je samozřejmě podnikový firewall. Snad již dnes neexistuje firma s vlastním připojením do internetu, která by svá data nechránila proti zcizení nebo jinému druhu zneužití.

Ovšem bylo by chybou považovat za vstupní bránu pouze firewall, dalším bodem je poštovní server, ale ten již svým vlastním umístěním v řetězci serverů v každé společnosti je až druhým členem (hned za firewallem). Některé společnosti (zvláště pak ty menší) spoléhají hlavně na integrovaná řešení. Tedy například poštovní server je zároveň i firewallem. Příkladem jsou zcela nepochybně velmi levná linuxová řešení vstupních bran.

Dále můžeme zmínit různé "chytré" routery, bridge, modemy nebo hardwarové firewally, které mají funkce firewallování. Pořád se ale veškerá diskuze točí kolem firewallu. Zaměřme se proto na možná antivirová řešení právě kolem firewallů.

Poslední dobou se lze velmi často setkávat s poptávkou na antivirová řešení právě hned na úrovni firewallů nebo těsně za nimi. Přitom debata na toto téma se zájemcem není v žádném případě jednoduchá. Otevřeně si přiznejme, že samotná nabídka spolehlivých a velmi rychlých antivirových řešení pro vstupní brány je mnohem menší, než jakou je například nabídka antivirových programů pro pracovní stanice.

První věcí, kterou si administrátor poptávající antivirové řešení pro vstupní brány musí uvědomit, je jakou vstupní bránu vlastně má. Proto zde uvádíme následující (asi nejčastěji) používaná řešení:

- velký podnikový firewall se speciálním software. Typickým představitelem je například Firewall-1 od firmy Checkpoint. Mezi tyto firewally ale záměrně nezařazujeme linuxové firewally, které mají ve světě antivirových řešení trošku zvláštní pozici.
- Hardwarové firewally. Typickým příkladem je zcela jistě Cisco PIX firewall. Ale i zde je nepřeberné množství jiných produktů.
- Linuxové firewally. Velmi často se zde zároveň objevují poštovní servery, nebo fungují jako relay servery pro poštu. Prostě firewall, ale postavený na Linux OS.
- Proxy servery a firewally jako je Winroute, WinProxy a jiné obdobné programy.

Pokud se omezíme na toto základní členění, získáme jakousi nabídku antivirových řešení, která jsou více či méně schopna ochránit podnikovou síť před viry.

Asi by v tuto chvíli bylo vhodné zmínit, co vlastně se má na vstupních branách chránit. Nemůžeme v tomto ohledu mluvit o ochraně e-mailů nebo souborů, neboť na vstupních branách se žádné soubory fyzicky (tak, jak je máme uloženy na disku) nevyskytují. Ale můžeme se na problém podívat jinak: jaké jsou možnosti infiltrace viru do sítě?

1) Především je to elektronická pošta. Ta se Internetem přenáší na úrovni aplikačního protokolu SMTP. Z hlediska virů a e-mailových červů je dnes otázka ochrany elektronické pošty zásadní. Ochrana na úrovni SMTP protokolu je tedy řešením.

2) Druhou možností infiltrace je komunikace pomocí protokolu HTTP. Tento protokol je dnes hlavně využíván pro zobrazování WWW stránek a jenom na českém internetu je spousta freemailových serverů, které antivirovou ochranu nemají (nebo ji mají, ale standardně vypnutou a nabízí uživateli, aby si ji sám zapnul) a poskytují rozhraní pomocí www stránek. Tedy každý, kdo má svůj účet na těchto freemailech, může pochopitelně obdržet virus. Tento virus samozřejmě leží v nějakém souboru a první co běžný uživatel udělá, je, že soubor i s virem stáhne na svůj pracovní počítač a spustí jej. Dalším typickým příkladem je stále se zvyšující počet trojských koňů a červů v podobě skriptů na některých webových stránkách. I toto je důvod proč se zamyslet nad antivirovou ochranou protokolu HTTP. Později si ale vysvětlíme, že s ochranou HTTP protokolu to není vůbec jednoduché.

3) Posledním významnou baštou přenosu virů Internetem jsou veřejné FTP servery. Není nic jednoduššího než zveřejnit na takovém serveru soubor, který je nakažen. Třeba virem Nimda. Problém, který administrátorovi po stažení a spuštění takového souboru ve vnitřní síti v případě nedostatečné ochrany stanic vznikne, je silně znepokojující. Z čehož vyplývá, že i ochrana protokolu FTP má svůj smysl.

4) Existují samozřejmě i další protokoly, které má cenu kontrolovat, zda se v nich neobjevil virus. První věcí, která někoho napadne je protokol POP3. Jiného zase například LDAP. Nedomníváme se, že je zase až tak důležité toto chránit - a to z jednoho prostého důvodu. Snad jen šílený administrátor by dovolil uživatelům POP3 připojení do Internetu - takovouto hrubou bezpečnostní chybu snad dnes již nikdo neudělá. A protokol LDAP? Existují řešení, která jsou schopna tento protokol zohlednit, ale v současné době není znám virus, který by jej aktivně používal ke svému šíření.

Z výše zmíněného rozboru je patrné, že valná většina antivirových firem se zaměřuje na kontrolu právě protokolů HTTP, FTP a SMTP, přičemž důraz je dnes kladen na ochranu SMTP.

Popišme si tedy, jaké možnosti v případě ochrany této skupiny aplikačních protokolů vztažené k rozdělení podle typu vstupní brány existují. Co taková řešení nabízejí a co nikdy splnit nemohou.

Podnikové firewally

Základem každého antivirového řešení pro tyto velké (a také značně finančně nákladné) podnikové firewally je protokol CVP (Content Vectoring Protocol). Tento protokol slouží k přesměrování paketů s HTTP, SMTP nebo FTP hlavičkou na speciální zařízení v "demilitarizované" nebo vnitřní síti. Tím zařízením je vyhrazený antivirový server.

Diskuze nad tím, proč neexistují antiviry, které se instalují přímo na firewall, nemá smysl. Snad jenom pro pořádek uvádíme hlavní důvody:
- firewall musí být robustní a stabilní řešení;
- firewall nesmí mít nainstalovaný žádný další aplikační software, který by tuto robustnost mohl snížit;
- firewall musí být maximálně bezpečný;
- každá aplikace instalovaná přímo na firewall tuto základní myšlenku značně ohrožuje.

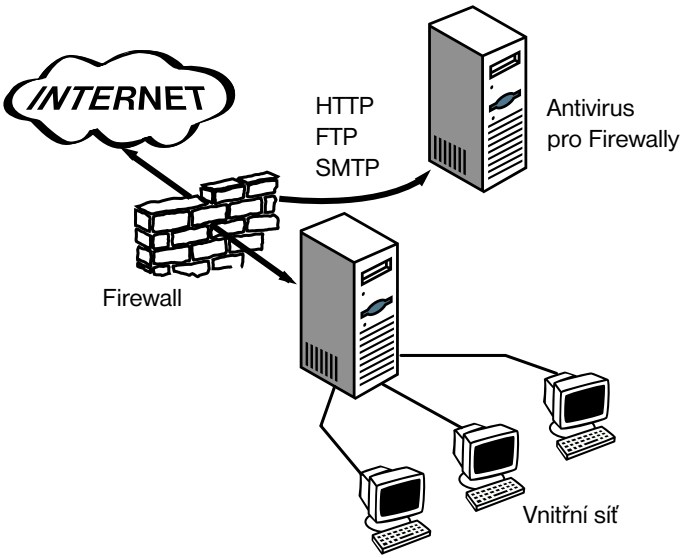
Abychom byli nestranní - existují samozřejmě i firewally, které mají již ve svém vlastním jádru antivirový program. Takovým příkladem je Gauntlet Firewall, který využívá antivirových prostředků McAfee. Ale tato řešení nejsou zase až tak obvyklá, jak by se na první pohled mohlo zdát. Obvyklejší je již samotná možnost využití protokolu CVP.

Protokol CVP

Antivirový program je nainstalován na speciálním serveru, kde je brán důraz na rychlost diskového zařízení i procesoru a velikost operační paměti. Tento stroj musí být připojen k firewallu pokud možno co nejkratší cestou. Nejlépe tedy křížením kabelem s rychlou topologií bez jakýchkoliv meziprvků.

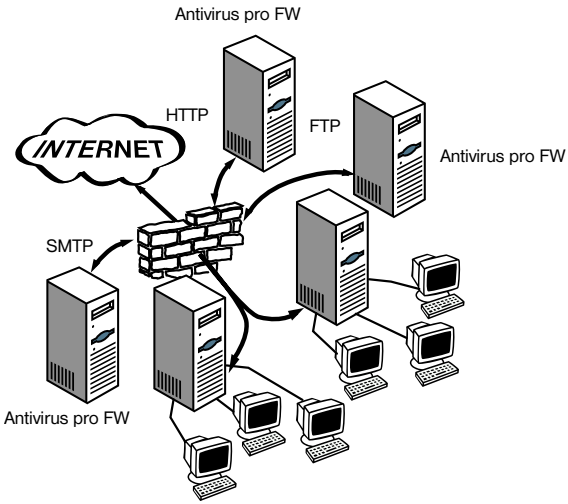
Důvodem, proč je třeba klást takové výrazné nároky na výkon sítě i serveru, je samotný průběh antivirového skenování pomocí protokolu CVP. Tento protokol slouží k přesměrování paketů na aplikačních protokolech HTTP, FTP a SMTP na jiný, bezpečný server, kde dojde k jejich zpracování, v našem případě k antivirovému skenování, a jejich vrácení firewallu. Firewall na základě vyhodnocení výsledků ze skenovacího serveru pakety do vnitřní či vnější sítě pustí nebo nepustí.

Můžeme si to zjednodušeně představit na následujícím obrázku:



Z tohoto obrázku je jasně vidět, že veškerý (dnes často používaný) internetový provoz je kontrolován jedním antivirovým serverem. Proto tak vysoké nároky na potřebný hardware skenovacího serveru.

Na druhou stranu je ale možné pomocí tohoto řešení skládat celé serverové farmy, kdy podle zátěže a rychlosti připojení můžeme skenovat jednotlivé internetové protokoly na samostatných strojích. Jako třeba na následujícím obrázku:



Rozložení znázorněné na tomto obrázku nám umožňuje standardně jakýkoliv firewall, který má podporu protokolu CVP. Ale co se stále rychlejšími linkami, nebo pokud internetové připojení používá příliš mnoho uživatelů v jeden čas?

Existuje několik možností. Jednou z nich je použít software Firewall-1 NG od firmy Checkpoint, který umí oproti konkurenčním firewallovacím produktům ne jeden CVP skener na jeden aplikační protokol, ale dva antivirové servery pro každý protokol. Ve výsledku bychom tedy dostali šest antivirových serverů připojených k firewallu. V tomto případě se již jedná o řešení schopné obsluhovat v reálném čase internetová připojení o rychlosti kolem 10 - 12 MB/s.

Další a nejsložitější možností je tzv. Clustering, kde serverů může být relativně neomezeně mnoho a jejich síla je sčítána pomocí software třetí strany - StoneBeat Security Server od firmy StoneSoft. Výhodou tohoto řešení není jenom pokrytí rychlých linek a velkého průtoku dat, který je tolik obvyklý například u ISP, ale i zálohování. Stane-li se, že některý z antivirových serverů zhavaruje, je komunikace přesměrována automaticky na zbylé (funkční) servery.

Jak poznáte, které firewally rozhraní CVP podporují? Vždy se jedná o komerční softwarové firewally. V žádném případě se nejedná o hardwarové firewally firmy CISCO, linuxové packet-screeningové firewally založené na IPTABLES/IPCHAINS nebo okruhové brány.

Výpis těch hlavních, které podporují CVP, je poměrně krátký:

- Altavista Firewall
- Check Point FireWall-1
- Cyberguard Firewall for NT
- Gauntlet
- Milkyway/SLM SecurIT Firewall for Solaris
- Secure Computing Firewall for NT
- Secure Computing SecureZone
- Sun Solstice Firewall

V případě Checkpoint Firewall-1, mluvíme o speciálním rozhraní CVP, takzvaném OpSec CVP. Celé rozhraní CVP bylo v zásadě navrženo úzkou skupinou lidí, kolem společnosti Checkpoint, která je později

uvolnila i pro ostatní společnosti, ale stále je za standard v této oblasti považováno pouze rozhraní OpSec CVP. Proto je veškerý antivirový software psaný pro firewally s rozhraním CVP testován vůči rozhraní OpSec.

Firma Checkpoint na základě tohoto uvolněného rozhraní provádí certifikace antivirových produktů vzhledem k jejich firewallu. O tuto certifikaci může požádat každá firma, vyvíjející software pro toto rozhraní a seznam certifikovaných antivirových produktů je možné nalézt na www stránkách http://www.checkpoint.com/opsec/security.html#Content_Security.

Z této certifikace by měl každý zájemce o antivirové řešení pomocí protokolu CVP vycházet a vybírat si podle ní.

Samozřejmě, že žádné řešení není bez vady a má svá omezení. Nejinak je tomu i u řešení CVP:

1) Zásadním omezením pro řešení CVP je jejich relativní rychlost. Řešení postavená na tomto protokolu trpí relativně vysokým zpomalením co se týká rychlosti linky. Tento problém existuje pouze u protokolů HTTP a FTP. Na sítích, kde je velký počet konkurenčních spojení a požadavků na externí webové zdroje, dochází ke zpomalení při zapnutém skenování. Obecně platí, že CVP skenery zvládají přibližně tok do 1,8 - 2 MB/s, ale toto je pouze průměrovaná hodnota. Má-li společnost rychlejší připojení, je už nutné uvažovat o loadbalancingu nebo clusteru. Ale v takovýchto případech se jeví jako výhodnější proxy architektura antivirového skenování (viz níže).

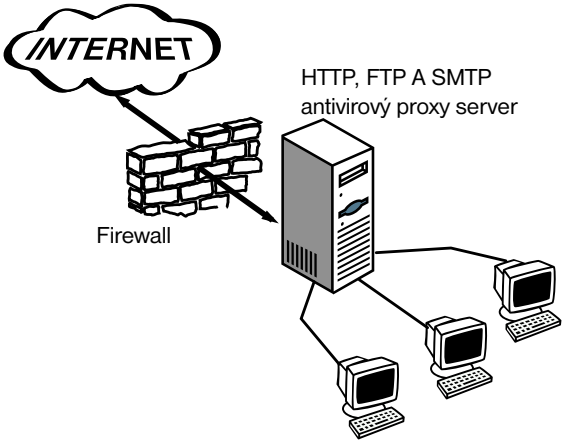
2) V případě, že zákazník hledá velmi robustní řešení, které bude využívat externích clusterovacích zdrojů, je konfigurace celého systému složitá a tudíž náchylná k nestabilitě.

Na druhou stranu je nutno podotknout, že tato řešení patří mezi levnější a pořád stále velmi spolehlivá. Jejich hlavní výhodou je právě škálovatelnost.

Co ale dělat, nemáte-li některý z vyjmenovaných firewallů, nebo se kvůli zmíněným omezením nechcete vázat na protokol CVP? Zde je již popsaná situace o poznání horší, alespoň co se týče antivirových produktů. Chceme-li totiž chránit celou skupinu protokolů (jenom pro pořádek připomenu, že se jedná o FTP, HTTP a SMTP), musíme se téměř výhradně spolehnout na proxy architekturu.

Proxy antivirová architektura

Samotná funkce tohoto řešení je velmi jednoduchá:



Z tohoto obrázku je zřejmé, že základním principem antivirového skenování je vložení serveru mezi vstupní bránu, v tomto případě firewall a uživatelské stanice. Veškerá komunikace je na vstupní bráně přesměrována na antivirový server, na něm je proveden antivirový test souborů poskládaných z paketového tvaru a po testu jsou zase v rozloženém stavu odeslány na cílové místo, lokální stanici.

Antivirové testování je možné provádět i na odchozí data, ale je nutné provést konfiguraci stanic a poštovních serverů v celé společnosti. Složitost takového kroku ve velkých firmách je zřejmá.

Antivirová řešení na úrovní antivirových proxy přináší některé výhody a zároveň i nevýhody.

Výhodami jsou:
- Rychlost - pakety prochází skrz, není zde žádný prvek, který pakety přeposílá tam a zpět. Z toho plyne, že tato řešení jsou vhodná pro velmi rychlé linky s požadavkem na rychlé odezvy
- Snadnější instalace a konfigurace. Konfigurace na straně firewallu přináší značné zjednodušení. Není potřeba nastavovat žádné směrování pomocí CVP a pravidla práce s nimi. Je potřeba pouze definovat, kam budou HTTP, FTP a SMTP pakety směrovány.
- Nejedná se o zátěž na procesor a paměť firewallu.
- Tyto proxy umožňují skenování i jiných protokolů, např. LDAP nebo POP3.
- Nevyžaduje firewall s CVP protokolem

Nevýhody:
- Vysoká cena - obvykle se jedná o kombinaci hardware a software, přičemž výsledná cena se pohybuje v tisících dolarech.
- Nemožnost rozkládat zátěž mezi více skenerů zaráz. Ve chvíli, kdy dojde k povýšení rychlosti komunikačních linek, nemusí toto zařízení stíhat nové (rychlejší) toky dat.
- Zálohování - v případě, že zařízení selže, není možné dále pokračovat v antivirovém skenování. Metoda CVP umožňuje zálohování v případě výpadku.
- Tato zařízení jsou "černé skříňky", které se nedají aktualizovat tak snadno jako CVP - softwarové skenery. Tím pádem velmi rychle technologicky zastarávají.
- V případě kontroly výstupních dat je potřeba konfigurovat stanice a ostatní servery, na rozdíl od CVP.

V poslední době se podobná řešení založená na HW/SW architektuře jenom "vyrojila". Některá z nich rozhodně stojí za zmínku. Například řada @-pliance od firmy NAI. Tyto produkty jsou i přes svoji cenu velmi kvalitní a dá se říci, že většina nevýhod výše zmíněných u nich odpadá.

A v neposlední řadě bychom rádi zmínili novinku na antivirovém trhu, od které si lze hodně slibovat, protože se jedná o zásadní přelom v antivirovém skenování. Toto řešení není proxy serverem, ale jedná se o síťový prvek typu bridge. To znamená, že cokoliv zde bylo zmíněno o potřebách překonfigurovávat klientská nastavení a firewally v této chvíli úplně odpadává. Ovšem je nutné podotknout, že se určitě v budoucnu nějaké nevýhody najdou. Pouze čas ukáže…

Jak vidno, situace kolem skenování všech protokolů je vcelku neradostná. O něco veselejší je situace kolem skenování pouze některého z protokolů. Typické bývá skenování pouze SMTP nebo pouze HTTP/FTP.

V případě protokolu SMTP není v podstatě co řešit, jedná se o čisté řešení pro jakékoliv vstupní brány. Naopak řešení pro HTTP a FTP jsou ve skrze aplikačního charakteru.

Ochrana SMTP vstupní brány

Protože jednotlivých řešení pro ochranu e-mailu existuje dnes již nepřeberné množství, zmíníme se pouze o jejich základním přehledu a rozebereme řešení, které je vhodné pro všechny možné konfigurace poštovní komunikace. Navíc je toto řešení zajímavé i z pohledu konfigurace a implementace.

Důležité je vědět, zda chceme chránit e-mailovou komunikaci na úrovni vstupní brány nebo až na úrovni poštovního serveru. Otázka, zda to není totéž, je na místě a je správná, a jak za chvíli ukážu, ve většině případů tomu tak bývá (ale i zde existují výjimky).

Ochranu e-mailu můžeme provádět na:

1) MS Exchange 5.x nebo 2000 - zde existuje opravdu nepřeberné množství ať již kvalitních, nebo méně kvalitních programů.

2) Podobná situace jako s MS Exchange je i s Lotus Notes nebo Domino serverem. V obou případech se jedná o Groupware prostředí, které ale obvykle neslouží jako vstupní brána do internetu. Pochopitelně i zde existují konfigurační výjimky.

3) Jiné poštovní servery. Tyto poštovní systémy obvykle neumožňují implementovat antivirovou ochranu, je-li ale antivirová ochrana podporována, tak pouze určitým antivirovým programem od jednoho výrobce, se kterým programátoři poštovního systému uzavřeli dohodu. Světlou výjimkou je například Kerio Mail server, který podporuje více antivirových programů, ovšem v daném okamžiku spolupracuje pouze s jedním.

4) V tomto ohledu často používaná jsou právě řešení typu Winprox nebo Winroute, nebo zase obráceně řešení postavená na Novell Os (GroupWise nebo Mercury), zde je situace obdobná jako u bodu 3.

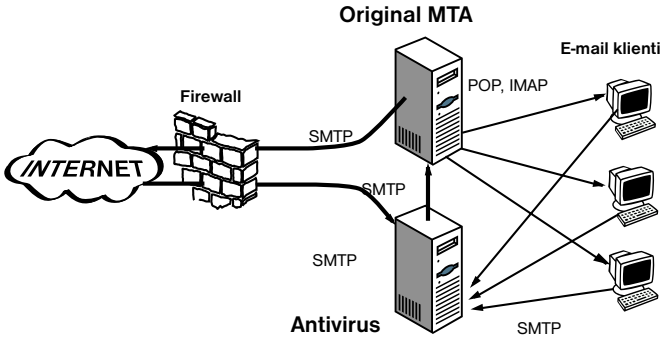
5) Linuxové poštovní servery jako Qmail, Sendmail, Postfix nebo Exim jsou dnes již hojně podporovány. Takže zde je situace s antivirovými programy přímo psanými pod Linux OS a jejich "poštáky" vcelku radostná. První vlaštovkou, která už před lety přišla s antivirovým programem pro linuxové poštovní servery, byl Kaspersky - dnes v tom pokračuje a zdá se, že velmi úspěšně.

Už teď je většině z Vás jasné, že pokud nemáte Linux a některý z jeho poštovních serverů (nebo Exchange, popřípadě Lotus Notes), tak máte, co se týče antivirové ochrany - lidově řečeno - smůlu. To naštěstí tak docela není pravda. Zde přichází na řadu řešení, které je velmi obdobné proxy řešení pro firewally, ale má i svá specifika, která jej odlišují.

Tyto antivirové programy fungují na základě SMTP-relay serveru, kde pošta je z Internetu nejdříve doručena na tento server. Zde je antivirově oskenována (popřípadě jsou provedeny další kroky, jako je odfiltrování nebezpečných příloh nebo spamu) a následně přeposlána na původní poštovní server ve společnosti.

Obráceně, tj. při e-mailové komunikaci odchozí ze společnosti, systém pracuje obdobně. E-mail je pravidlem přeposlán na tento antivirový server, zde se zkontroluje a je odeslán adresátovi. Tímto stylem pracuje i lokálně posílaná e-mailová komunikace.

Z obrázku by mělo být patrné, jak takový server pracuje:



Obrovskou výhodou takovéhoto řešení je rychlost. Díky tomuto systému je antivirové skenování možné i s poměrně nemoderním hardware, na kterém je antivirový software provozován - a přitom je dosahováno špičkových výkonů. Díky své rychlosti jsou podobná antivirová řešení používána hlavně u Internet Service Provider nebo poskytovatelů freemailových služeb.

HTTP a FTP skenování

Co tedy brání tomu aby vznikala takto rychlá antivirová řešení na podobném principu i pro HTTP a FTP komunikaci? Je sice pravdou, že elektronická pošta v Internetu funguje zcela odlišným způsobem, než jakákoliv jiná komunikace, ale přece i zde jsou podobné prvky, které je možno využít. Vlastně existuje už pár softwarových vlaštovek, které pracují na podobném principu jako antivirové SMTP-relay servery. Naneštěstí spousta z nich je ještě stále v beta verzích - a jak se zdá, ještě dlouho bude.

V případě, že by se takovéto řešení dotáhlo do konce, byl by problém se všemi proxy a CVP skenery vyřešen. V současné době je ale nutné spoléhat právě na ně. Poslední možností, jak tento palčivý problém vyřešit, je využít antivirové plug-iny založené na ISAPI rozhraní nebo moduly pro Windows socket.

Antivirové plug-iny pro ISAPI rozhraní jsou v podstatě moduly pro MS Proxy servery. Má-li tedy společnost MS proxy server, může s výhodou využít toto rozhraní pro antivirovou kontrolu. V současné době existují antivirové programy pro MS proxy 2.0 nebo pro ISA Server.

Windows socket antivirové moduly mají tu výhodu, že se nemusí omezovat pouze na HTTP/FTP skenování, ale jsou použitelné třeba i na SMTP, LDAP nebo POP3. Zde totiž vše záleží pouze na fantazii programátora, jaké drivery pro Windows socket napíše a co na této nízké úrovni Windows bude skenovat. Aby nedošlo k nějaké mýlce: v tomto případě se již jedná o řešení pouze pro Windows stanice.

Tímto bych uzavřel zcela jistě neúplnou kapitolu o antivirové ochraně na vstupních branách. Předmětem diskuze mohou být další možnosti řešení a zase se odvoláváme pouze na pokrok a hlavně čas, který je potřeba k tomu, aby se objevily nové technologie, které zjednoduší práci administrátorům. Ale pozor, techniky antivirových systémů jsou obvykle technologicky o krok zpátky oproti virům a i přes snahy v tomto bodě něco změnit, zatím povětšinou zpětně reagují na vývoj virů. Ostatně kdyby nebylo virů, nebylo by ani antivirových programů (a já bych neměl za co žít - pozn. autora).

Antivirová řešení pro UNIX servery

Neméně zajímavou a hodně diskutovanou oblastí antivirového zabezpečování jsou zcela nepochybně UNIXové platformy. Tato přednáška v žádném případě nebude rozebírat existenci a nebo neexistenci unixových virů a diskutovat nad jejich škodlivostí či vlivem na uživatele a data uložená unixových serverech. Prostě a jednoduše viry v unixových prostředích jsou a budou.

Na začátek je asi dobré říci, že antivirové programy na unixových serverech nechrání samotný server před napadením unixového viru. Současné antivirové programy chrání data uložena na těchto serverech před napadením. Aby byl virus schopen napadnout unixový server, musí jej někdo spustit a vzhledem k bezpečnostním prvkům, které jsou na unixových systémech samozřejmostí již bezmála dvě desetiletí, to není nic snadného.

Taktéž různorodost jednotlivých klonů unixových operačních systémů a samotná různorodost jednotlivých instalací činí z unixových systémů velmi nehostinné prostředí pro šíření virů. Virus totiž k tomu, aby se mohl šířit, potřebuje dostatek hostitelských souborů a počítačů. Operační systémy Windows se svým jednotným prostředím jsou mnohem "použitelnějsími" pro šíření virů. Tedy i přesto, že existují unixové viry, jsou spíše laboratorními vzorky, které nejsou běžného kybernetického života schopny. Proč tedy vlastně mluvit o ochraně unixových serverů, když bylo právě řečeno, že zde nejsou žádné unixové viry, které by se opravdu šířily?

To proto, že unixové systémy často fungují jako souborové nebo e-mailové systémy pro poskytování internetových a souborových služeb klientům s Windows operačními systémy. A protože takový klient si přes

tyto servery vyměňuje data ve formátech běžných na Windows OS, tak je možné na unixový server uložit například *.DOC dokument, který obsahuje makrovirus.

V tuto chvíli už samozřejmě antivirová ochrana nabývá smyslu podobně jako je tomu na Windows NT/2000 serverech nebo Novell serverech. Bohužel antivirová řešení na unixech nejsou již v tak dokonalém stavu jako je tomu na Windows nebo Novellu. Podobně jako je tomu v případě problémů šíření virů v Unix systémech, vznikají podobné, ne-li stejné, problémy s bezpečností i pro antivirové produkty.

Není ale pravdou, že by nebylo možné napsat antivirový program, který bude mít rezidentní ochranu podobnou té, jakou ji mají systémy Windows - unixové řešení residentního štítu je "jen" mnohem nákladnější na vývoj. Proto se většina antivirových firem omezuje pouze na vývoj tzv. řádkových antivirových skenerů, jejichž sláva byla největší v době epochy MS-DOS. Takovýto příkazový řádek je velmi jednoduchý a výkonný - nicméně jeho nevýhodou je právě to, že nedokáže odhalit viry v reálném čase, ale pouze tehdy, je-li spuštěn.

Obratem této situace je výborné řešení Kaspersky Antivirus, které má právě rezidentní štít pro detekci virů v reálném čase na unixových systémech.

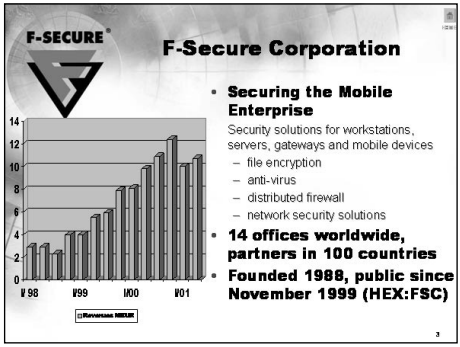
Často se lze setkat s otázkou, zda je nutné chránit před viry unixové systémy s databázovou aplikací. Odpověď je velmi jednoduchá a kdo pozorně četl předchozí řádky, si na ni dokáže odpovědět sám.

Není to nutné, protože data ukládaná v databázích nemají pro viry smysl. Jediné, co by stálo za zmínku, jsou například databáze, které mohou obsahovat dokumenty DOC. Tyto dokumenty pochopitelně již mohou nést makroviry. Ale protože databáze je přístupná pouze speciálním databázovým klientem, který provede s položkami a soubory uvnitř databáze potřebné akce, dojde k spuštění nebo stažení infikovaného DOC dokumentu až na stanici, kde pochopitelně již je antivirový program.

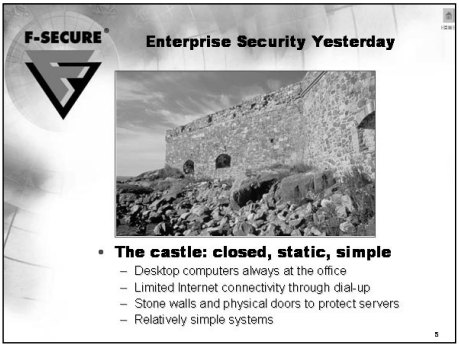
Zde se ale dostáváme do logické rozporu, protože je-li na stanici aktivní antivirový program, pak není možné, aby se makrovirus umístěný v DOC dokumentu mohl uložit společně s tímto dokumentem do databáze na serveru, protože jej tam musí uložit přes svou databázovou aplikaci uživatel, který ale má aktivní antivirový program. Uložení infikovaných souborů do databáze není teoreticky možné.

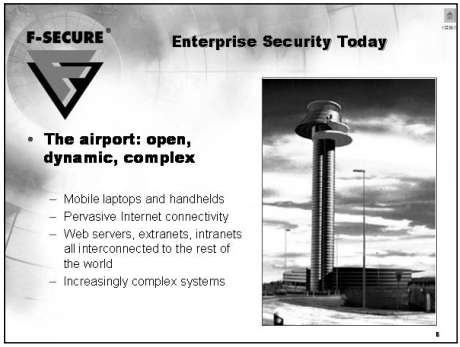
Shrneme-li výše uvedené, pak jediné, co má z unixových systémů smysl chránit, jsou souborové systémy a internetové vstupní brány (popřípadě poštovní servery). Pro dvě posledně zmíněné skupiny ale platí předchozí kapitola o antivirové ochraně na vstupních branách.

A tímto se kruh antivirové ochrany na speciálních informačních systémech uzavřel - a uzavírá se i tento rozbor spojený s polemikou nad antivirovými řešeními.



WHAT IS MOBILE?





F-SECURE

Today's Corporation

- **Allows for flexibility and mobility**
  - Extensive use of laptops and handheld devices
- **Is Networked**
  - Allows access to services in public networks
  - Local area networks are interconnected
  - Allows remotes access to corporate network
- **Processes confidential information**
  - Extensive use of eMail
  - Confidential and business critical documents

7

F-SECURE

So, environment has changed.

What about technology?

8

F-SECURE

Personal Computer 1998

- 266 MHz Intel Mobile Pentium® II processor
- 64-MB SDRAM

Compaq Armada 7800 notebook
Announced April 2nd, 1998

"With the addition of the Armada 7800, we are better able to address the needs of power users who require superior, reliable systems"

– Michael Winkler, SVP, PC Products Group, Compaq

9

F-SECURE

Personal Computer Today

- 206 MHz Intel StrongARM Processor
- 64-MB SDRAM

Compaq iPAQ H3800 Pocket PC
Announced October 4th, 2001

A real business tool for mobile productivity

– Only easier to use and easier to lose...

10

F-SECURE

12.9 million PDA devices were sold in 2000

85 million PDA devices will ship in 2006

11

F-SECURE

64,000 mobile phones were left in London taxis during January – June 2001, as well as

2,900 Laptops 1,300 PDAs

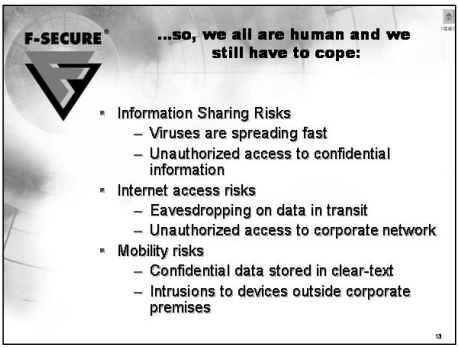
+ one baby,
one plastic bag with a goldfish in it
and a suitcase full of diamonds

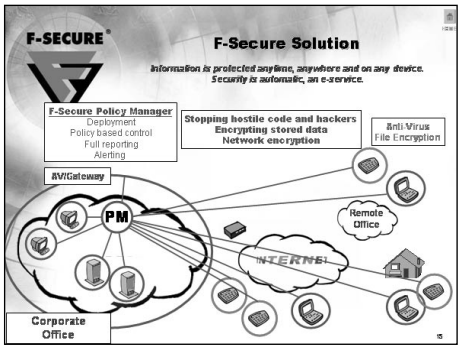
250,000 handheld devices will be left behind or lost at U.S. airports this year

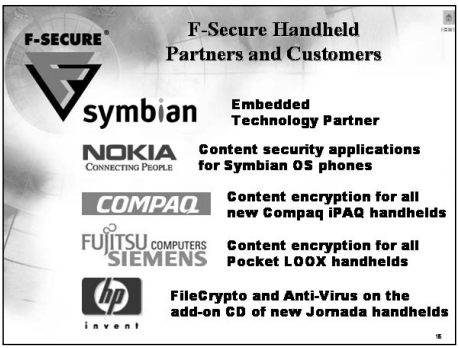
387,000 laptops were stolen last year in the US

12

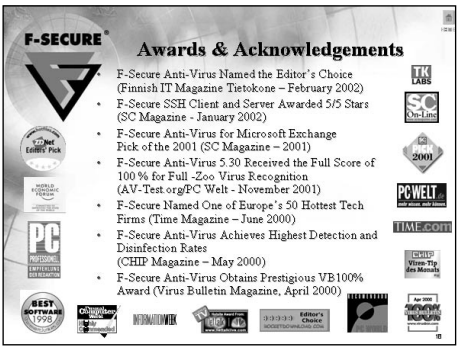
SOLUTION

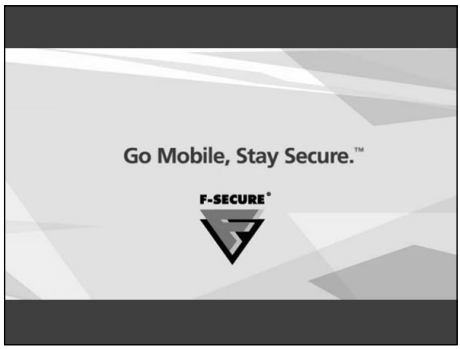

F-SECURE
...so, we all are human and we still have to cope:
Information Sharing Risks
– Viruses are spreading fast
– Unauthorized access to confidential information
Internet access risks
– Eavesdropping on data in transit
– Unauthorized access to corporate network
Mobility risks
– Confidential data stored in clear-text
– Intrusions to devices outside corporate premises


F-SECURE
F-Secure Solution
Information is protected anytime, anywhere and on any device.
Security is automatic, an e-service.
F-Secure Policy Manager
Deployment
Policy based control
Full reporting
Alerting
Stopping hostile code and hackers
Encrypting stored data
Network encryption
Anti-Virus
File Encryption
AV/Gateway
PM
Remote Office
INTERNET
Corporate Office


F-SECURE
F-Secure Handheld Partners and Customers
symbian
Embedded Technology Partner
NOKIA
CONNECTING PEOPLE
Content security applications for Symbian OS phones
COMPAQ
Content encryption for all new Compaq iPAQ handhelds
FUJITSU COMPUTERS SIEMENS
Content encryption for all Pocket LOOX handhelds
hp
invent
FileCrypto and Anti-Virus on the add-on CD of new Jornada handhelds

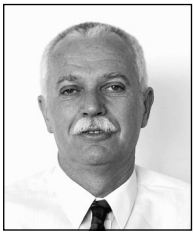

F-SECURE
Certifications
F-Secure Anti-Virus for Internet Mail Verified for Interoperability with Cisco PIX 500 Firewall
F-Secure SSH for Unix and Windows Verified for Interoperability with Cisco IOS Release 12.1(1)T and Cisco PIX 5.2
F-Secure Anti-Virus for Firewall 6.01, Windows version OPSEC Certified and Interoperable with Check Point FireWall-1
F-Secure SSH Client for Windows Containing FIPS 140-1 Certified Cryptographic Components
F-Secure Anti-Virus and F-Secure SSH Certified by ICSA Labs
In addition, close co-operation with the following technology partners:
CISCO SYSTEMS
Verified
Microsoft CERTIFIED
symbian Technology Partner
COMPAQ
ICSA Labs CERTIFIED
BALTIMORE


F-SECURE
Awards & Acknowledgements
F-Secure Anti-Virus Named the Editor's Choice (Finnish IT Magazine Tietokone – February 2002)
F-Secure SSH Client and Server Awarded 5/5 Stars (SC Magazine - January 2002)
F-Secure Anti-Virus for Microsoft Exchange Pick of the 2001 (SC Magazine – 2001)
F-Secure Anti-Virus 5.30 Received the Full Score of 100 % for Full -Zoo Virus Recognition (AV-Test org/PC Welt - November 2001)
F-Secure Named One of Europe's 50 Hottest Tech Firms (Time Magazine – June 2000)
F-Secure Anti-Virus Achieves Highest Detection and Disinfection Rates (CHIP Magazine – May 2000)
F-Secure Anti-Virus Obtains Prestigious VB100% Award (Virus Bulletin Magazine, April 2000)
TIME.com


Go Mobile, Stay Secure.™
F-SECURE

Ing. Jiří Mrnuštík, vystudoval Fakultu nukleární fyziky Českého vysokého učení technického. Věnoval se výzkumu elektronové mikroskopie v České akademii věd pod vedením akademika Armina Delonga, studoval matematickou analýzu na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze, pracoval na výzkumu penetrace radioaktivních plynů ve Výzkumném ústavu stavebních hmot v Brně a od roku 1989 se věnuje bezpečnosti informačních systémů a kryptologii. Zastává funkci ředitele vývojového oddělení ve společnosti AEC. Je členem Jednoty matematiků a fyziků, členem Evropské fyzikální společnosti, členem Association Online Professionals, ISACA a dalších společností.

JUDr. Iveta Hodková, CSc., (narozena 1963) vystudovala Právnickou fakultu Univerzity Karlovy v Praze. Zabývala se vědeckou činností v oblasti mezinárodního práva veřejného v Ústavu státu a práva ČSAV, ve které začátkem devadesátých let pokračovala v rámci jednoletých pobytů na právnické fakultě University of Connecticut (USA) a na právnické fakultě University of Houston (USA). Dále působila jako právní poradce Federálního výboru pro životní prostředí. Od roku 1993 působí ve společnosti Coopers & Lybrand, nyní PricewaterhouseCoopers (PwC), kde se původně specializovala na daňové právo a později na právo obchodní, občanské a na právní aspekty elektronického obchodování a elektronického podpisu. Je členkou české advokátní komory a členkou PwC mezinárodní diskusní a informační skupiny pro elektronický obchod. V rámci PwC ČR je odpovědná za rozvoj právních znalostí a produktů v oblasti elektronického obchodování.
Je autorkou monografie a řady odborných článků z oblasti mezinárodního práva, práva životního prostředí. V poslední době zaměřuje publikační činnost na problematiku elektronického podpisu.



Doc. Ing. Jan Staudek, CSc., docent Fakulty informatiky Masarykovy university v Brně, vedoucí Katedry programových systémů a komunikací. Zabývá se bezpečností informačních systémů, budováním bezpečnostních politik IS v organizacích typu bankovní dům, vysoká škola a instituce státní či veřejné správy, analýzou rizik, bezpečnostním auditem a aplikovanou kryptografií. Pracuje jako nezávislý konzultant v těchto oblastech, přednáší o bezpečnosti informačních systémů v Bankovní akademii Praha. Mimo to se zabývá výukou v oblasti operač-ních systémů a počítačových sítí. Organizátor mezinárodních konferencí MFCS, SOFSEM, CONCUR, konferencí s mezinárodní účastí DATAKON, seminářů AFOI atd. Člen ACM a České informatické společnosti

Mgr. Pavel Vondruška (*1956). Vystudoval Matematicko-fyzikální fakultu Univerzity Karlovy v Praze. Patnáct let se věnuje profesionálně kryptologii a informační bezpečnosti. V současně době pracuje na Úřadu pro ochranu osobních údajů v odboru elektronického podpisu.

Je členem kryptologické skupiny JČMF (GCUCMP), členem IACR, BITIS. Byl členem organizačního výboru mezinárodních konferencí Pragocrypt ´96 a Eurocrypt ´99. Odborné veřejnosti jsou známé jím vydávané elektronické sešity GCUCMP - Crypto-World
(http://www.mujweb.cz/veda/gcucmp).

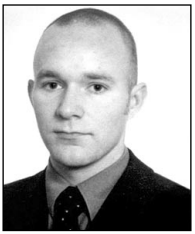
JUDr. Ján Matejka (*1976) je vědeckým pracovníkem Ústavu státu a práva Akademie věd ČR a učitelem na Právnické fakultě ZČU v Plzni, kde je garantem předmětu Internetové a počítačové právo". V minulosti se mimo jiné podílel na přípravě prováděcích předpisů k zákonu o elektronickém podpisu. Je rovněž prezidentem Společnosti pro právo informačních technologií (SPIT), která mimo jiné provozuje stránky www.ITPravo.cz . Pravidelně publikuje v časopisech Právník, Bulletin advokacie a na Internetu.

Petr Hanáček, Dr. Ing., pracuje na Fakultě informačních technologií VUT v Brně. Zabývá se několik let bezpečností informačních systémů, analýzou rizik, aplikovanou kryptografií, elektronickými platebními systémy. Je nezávislý konzultant v této oblasti a přednáší několik kurzů o bezpečnosti informačních systémů.

Adresa autora: Ing. Petr Hanáček, Fakulta informačních technologií, Vysoké učení technické v Brně, Božetěchova 2, 612 66 Brno
tel. 4114 1216, e-mail: hanacek@fit.vutbr.cz

Mgr. Jaromír Klimek se narodil 23.7. 1971 v Českém Těšíně, absolvoval přírodovědeckou fakultu Masarykovy univerzity, obor matematika-fyzika. Ve firmě AEC pracuje na pozici produktového specialisty - produkty Norman Virus Control a Kaspersky Antivirus, dále také přednáší o problematice bezpečnosti v oblasti IT.

JUDr. Luděk Rataj, Autor pracuje ve společnosti INFOSEC s.r.o. na projektech řízení rizik informačních systémů. Zabývá se analýzou organizační a odpovědnostní struktury organizací a implementací právních institutů informační bezpečnosti. Je jedním ze zakládajících členů Asociace firem pro ochranu informací, je pověřen zastávat funkci předsedy asociace.



Ing. Radek Komanický, Autor absolvoval FEL na ČVUT. Ve společnosti INFOSEC se specializuje na rizikové analýzy s využitím metodiky CRAMM, bezpečnost ICT a systémy řízení informační bezpečnosti. = S pozdravem Luděk Rataj

Ing. Miroslav Trnka, technický riaditeľ Eset spol. s r. o. Bratislava, Slovenská republika, prezident a CEO Eset LLC, San Diego, USA konateľ Eset software spol. s r. o., Praha, Česká republika.

Vysokoškolský titul získal na Slovenskej technickej univerzite v odbore Automatizované systémy riadenia. Pracoval vo výpočtovom stredisku Trnavských automobilových závodov a na Katedre informatiky Materiálovo-technologickej fakulty Slovenskej technickej univerzity v Trnave.

Od roku 1987 pracuje na vývoji antivírusového systému NOD. V roku 1992 založil so spoločníkmi firmu Eset, spol. s r.o., kde zastáva funkciu technického riaditeľa. Okrem toho je prezidentom a CEO spoločnosti Eset LLC. v San Diegu, USA a konateľom spoločnosti Eset software spol. s r.o. v Prahe, ČR.

Od roku 1993 vedie v časopise PC Revue rubriku Vírusový radar, kde sa populárnou formou zaoberá novinkami zo sveta vírusov a ich vzťahom k spoločnosti. Je členom profesných organizácií ASIT (Association for Security of Information Technologies), SASIB (Slovak Association for Information Security) a predseda SAC (Slovak Antivirus Center). Je zástupcom Slovenska v organizácii Wildlist International a mesačne spracováva hlásenia o situácii v oblasti počítačových infiltrácií na Slovensku. Pravidelne prednáša doma i v zahraničí a prispieva článkami do rôznych periodík a poskytujem konzultácie, prípadne odborné komentáre týkajúce sa problematiky vírusových infiltrácií pre masovokomunikačné prostriedky.

Medzi jeho záľuby patrí plávanie, archeológia, paragliding, cestovanie a hranie na gitaru.

Eset spol. s r. o., Pionierska 9/A, 831 02 Bratislava, Slovenská republika
tel.: +421-2-44457937, +421-2-44457938,
fax: +421-2-44457939, e-mail: trnka@eset.sk, trnka@nod32.cz

Petr Odehnal, narozen 26. 12. 1966, vystudoval VUT Brno. Pracuje jako patolog (pitvá počítačové viry) ve firmě Grisoft. Pokud náhodou zrovna nepitvá, tak sedí U Bláhovky a pokouší se přijít na to, proč zrovna tam mají nejlepší Plzeň.

Pavel Baudiš, tvrdě pracuje ve firmě ALWIL Software. Když se nezabývá počítači, viry či obecně počítačovou bezpečností (což je po pravdě řečeno dost zřídka), snaží se co nejvíce času trávit se svou rodinou. Rád cestuje po exotických krajích, obstojně lyžuje (hlavně v Dolomitech) a jednou ročně jezdí na kole po Šumavě. Ve volných chvílích relaxuje při čtení a poslouchání kvalitní rockové hudby.

Tomáš Vobruba, narozen 3.12.1976 v Liberci. Věnuje se informatice již od ranných let. Od ukončení studií na katedře matematiky Masarykovi Univerzity pracuje ve společnosti AEC na pozici technik, kde se věnuje antivirových řešením ve všech podobách.

Jeho nejoblíbenější antivirový program je F-Secure Anti-Virus.

Bezpečnost s HP

Společnost Hewlett-Packard působí na trhu jako dodavatel nejrůznějších komponent tvořících infrastrukturu IT. K jednotlivým technologiím se připojí služby, které zabezpečí plynulý chod oddělení IT. V současnosti se nepřetržitý provoz, dostupnost a bezpečnost klíčových částí informačních systémů stává nutnou podmínkou pro fungování obchodní, průmyslové, telekomunikační nebo státní organizace. HP nabízí svým zákazníkům také výraznou přidanou hodnotu v podobě silného týmu úzce specializovaných odborníků, kteří staví nejen na vlastních zkušenostech, ale také na sdílení znalostí z celosvětových projektů.

Rozvoj Internetu, provázanost a otevřenost informačních systémů mezi obchodními partnery a zákazníky klade zvýšené nároky na bezpečnost informačních technologií. HP v této oblasti není nikterak pozadu za svými konkurenty. Oblasti, které HP řeší v rámci bezpečnosti IT jsou především:

- **síťová bezpečnost**
- **e-business**
- **infrastruktura veřejných klíčů (PKI - Public Key Infrastructure)**
- **předpisová základna**
- **procesy IT**
- **vysoká dostupnost**
- **ochrana důvěrnosti a integrity**
- **kryptoanalytický rozbor**
- **příprava certifikace a akreditace**
- **bezpečnostní analýza, analýza rizik**
- **bezpečnostní audit prostředí IT**
- **fyzická bezpečnost**
- **bezpečné výpočetní prostředí (Virtualvault)**
- **bezpečnostní školení a semináře.**

HP pomáhá svým zákazníkům vytvářet, zavádět a spravovat účinná bezpečnostní řešení za použití odzkoušených metod a nejlepších technologií ve své třídě. O kvalitě produktů a služeb svědčí nejrůznější ocenění. Loni v Londýně získala společnost Hewlett-Packard v rámci pátého ročníku "Secure Computing Awards", cenu za nejlepší bezpečnostní služby "Best Security Service Award" a HP Virtualvault získal cenu za nejlepší produkt všeobecné bezpečnosti "Best General Security Product".

HP udělalo strategické rozhodnutí ohledně bezpečnosti zhruba před čtyřmi lety a od té doby v oblasti pokračuje. Nabízí tak svým zákazníkům ucelené portfolio nástrojů, produktů a služeb pro tvorbu, správu, měření a účtování jejich zisků.

Neváhejte se proto obrátit na společnost Hewlett-Packard a vaše potřeby i přání s námi konzultovat.

Hewlett-Packard, Vyskočilova 1/1410, 140 00 Praha 4, Tel: +420-2-613 07 111,
Fax: +420-2-613 07 613, e-mail: info_cz@hp.com