Šifrovat?…..Rozhodně Ano!

Co nového je ve světě kryptografie?

Úvod.

Důležitost kryptografie v současných digitálních komunikacích roste, o tom není pochyby. Její úloha je nezaměnitelná, kryptografie plní řadu stěžejních funkcí: utajení, autentizace, nepopiratelnost, nenarušenost (integrita) zpráv atd. Používá k tomu celou škálu prostředků jako jsou šifrovací algoritmy, metody digitálních podpisů, kryptografické protokoly, časové značky (time stamping) a další.

Obrysy kryptografie však v současné době dostávají určitou konkrétní podobu především prostřednictvím celé škály norem, doporučení, standartů. Dnes již nejde o to nějak zašifrovat data, nějak se digitálně podepsat, nějak utajeně komunikovat. Do hry vstupují (a to především prostřednictvím Internetu) rozsáhlé počítačové sitě s množstvím jednotlivých účastníků. Je třeba vytvořit prostředky chráněné komunikace v takovýchto sítích, kde spolu odpovídajícím bezpečným způsobem mohou v principu chtít komunikovat libovolní dva účastníci této sítě. Aby toto bylo vůbec možné, musí být prostředky chráněného přenosu dat, vzájemné autentizace účastníků atd., určitým způsobem unifikovány. To je potom cílem vytváření jednotlivých kryptografických norem a doporučení. V současnosti je již takovýchto norem celá přehršel. Proč jich je tolik a čeho se vlastně týkají?

Základní kryptografické normy samozřejmě pojednávají o vlastních šifrovacích algoritmech a to jak symetrických tak i algoritmech s veřejným klíčem. Běžným pojmem se stal digitální certifikát a jeho precizace je opět součástí příslušných norem. Klepe nám na ramena zákon o digitálním podpisu. Aby vůbec mohl fungovat bezpečný elektronický obchod je třeba vytvořit bezpečné prostředky chránicí obě strany – děje se tak opět pomocí celé řady iniciativ v oblasti vytváření výchozích norem a doporučení. Architektura samotného Internetu (známý sedmivrstvý model ISO) vede k různým variantám chráněného přenosu dat na jednotlivých vrstvách. Finanční instituce si vytváří svou samostatnou třídu norem (ANSI) atd.

Symetrická kryptografie

Éra DES již skončila, na rozhraní tohoto a minulého roku byla vydána nová norma FIPS-46-3, ve které je DES nahrazena algoritmem 3-DES (fakticky již delší dobu používaným). Kanadská firma Entrust prostřednictvím IETF dala mezinárodní kryptografické veřejnosti k volnému použití moderní algoritmus CAST.

Americký vládní úřad pro normy NIST již vkročil do dalšího kola výběru symetrického šifrovacího algoritmu – Advanced Encryption Standard (AES). Vzhledem ke stávajícím blokovým šifrám se tyto algoritmy liší především v délce zpracovávaného bloku. Zatímco současné algoritmy pracují s délkou bloku 64 bitů, algoritmy pro AES zpracovávají blok v délce 128 bitů. Důvod je zřejmý – hranici 2^{64} se začínají přibližovat reálné výpočetní možnosti a v určitých situacích by mohlo začít být možné vytvoření kompletního slovníku (tj. všech dvojic otevřený text a šifrový text) pro neznámý klíč.

AES algoritmy musí umět pracovat s klíči tří povinných délek (128, 192 a 256 bitů). V srpnu 1998 byla NIST oficiálně oznámena jména 15 přihlášených kandidátů. Druhá AES konference v březnu letošního roku byla věnována analýze vlastností těchto přihlášených algoritmů. Na základě této analýzy a zaslaných doporučení vybrala NIST jména pěti finalistů, která oznámila v srpnu 1999. Jsou to:
MARS (IBM), **RC6** (RSA Laboratories), **Rijndael** (belgičtí kryptologové Daemen, Rijmen), **Serpent** (Anderson, Biham , Knudsen), **Twofish** (Bruce Schneier se spolupracovníky).

V dubnu 2000 se bude konat třetí AES konference, jejímž obsahem budou příspěvky věnující se analýze těchto pěti algoritmů. Na základě jejich výsledků bude vybrán jeden (či více) algoritmů, který jako navrhovana norma FIPS se stane ještě předmětem veřejné diskuse. Předpokládá se, že nová norma by měla být známa v létě roku 2001.

Asymetrická kryptografie

Do závěrečné etapy pokročily rovněž práce skupiny P1363. Tato skupina odvedla veliký kus práce jejímž obsahem bylo detailní zpracování popisu a metod využívání následujích systémů s veřejným klíčem: RSA, Rabin-Williams, kryptosystém založený na využití problému diskrétního logaritmu a konečně kryptosystémy na bázi eliptických křivek. V současné době se již vyjasnilo, že kryptosystémy s veřejným klíčem umožňují v zásadě trojí typ využití a to jako systémy pro:

a) výměnu klíčů pro symetrickou kryptografii
b) digitální podpis
c) šifrování (obvykle krátkých zpráv, většinou služebního charakteru).

Perspektivními jsou zejména systémy na bázi eliptických křivek. Relativně krátká délka klíče těchto kryptosystémů je jejich ústřední předností. Z hlediska volby konkrétních parametrů umožňují eliptické kryptosystémy velkou variabilitu. Toto je jejich předností, na druhou stranu je však třeba vytvářet opět určitý jednotný přístup (aby se jednotliví účastníci vůbec domluvili, musí jejich utajená komunikace probíhat v rámci jednoho konkrétního kryptosystému s pevně danými parametry, mění se pouze soukromé a veřejné klíče). Proto také např. vznikla pracovní skupina SECG, jejímž cílem je vytvořit určitou jednotnou platformu pro eliptickou kryptografii (AEC je členem této skupiny). Rovněž tak americký vládní úřad NIST si tentokráte pospíšil a vydal doporučení stanovující určitou množinu parametrů pro kryptosystémy na bázi eliptických křivek.

A co kryptoanalýza?

Během období posledního jednoho až dvou roků došlo samozřejmě i k řadě význačných výsledků v oblasti kryptoanalýzy. S vyjímkou DES a algoritmu A5 pro GSM se tyto výsledky však netýkají přímo šifrovacích algoritmů, ale spíše určitých způsobů práce s nimi (kryptografické protokoly, vlastnosti fyzické realizace algoritmů).

PKCS 1

Normy PKCS vytvářené vývojáři známé firmy RSA jsou svým způsobem jedněmi z nejznámějších a nejčastěji využívaných specifikací pro vytváření konkrétních kryptografických produktů. Popisují např. syntaxi kryptografické zprávy, způsoby práce s některými kryptosystémy s veřejným klíčem, práci s digitálními certifikáty, s klíči, hesly atd. V srpnu 1998 na konferenci Crypto v Santa Barbaře vystoupil Daniel Bleichenbacher (Bell Laboratories) s novým útokem proti PKCS 1, tato norma popisuje šifrování, vytváření digitálních podpisů pomocí algoritmu RSA. Útok spočívá v existující možnosti zasílat (např. automaticky odpovídajícímu serveru) velké množství zpráv s cílem zjistit otevřený text pro jeden konkrétní šifrový text zašifrovaný pomocí algoritmu RSA. Analýza reakcí na tyto zprávy umožňuje pak přímým matematickým postupem získat příslušný otevřený text. V daném případě útočník nezíská utajovaný klíč, ale pouze jeden otevřený text. Pokud je to však např. tajný klíč pro symetrickou šifru, získá útočník samozřejmě všechnu komunikaci zašifrovanou tímto tajným klíčem. Aby toto mohlo vůbec fungovat, musí útočník získávat nějakou informaci od příslušné oběti útoku, určitou reakci (stačí např. sdělení, zda příslušná zpráva je platnou zprávou či nikoliv). Bohužel některé kryptografické protokoly toto umožňují. Týká se to např. většiny variant SSL vzniklých před opublikováním útoku. Jsou takto zranitelné i některé čipové karty, pokud útočník má možnost vsunout je do vlastního zařízení.

V současné době je již v platnosti nová varianta doporučení PKCS 1, kde jsou výše popsané problémy odstraněny. To co se týká obecných norem (tj. skutečnost, že máme možnost je opravit) se však nemusí zdaleka týkat konkrétní praxe. A například uživatelé SSL by měli vědět, zda pracují již z opravenou verzí či nikoliv. Bohužel praxe může být ještě horší, někdy je dokonce používana exportní verze SSL z minulých let, která se opírá pouze o 40 bitové šifrování. Uživatelé by proto apriori neměli mít důvěru v systémy, kde jejich řešitel není např. ochoten sdělit detaily o jím implementovaném řešení.

DES-Cracker

Konečně bylo fyzicky zrealizováno to co kryptologové avízovali již dlouhou řadu let. Algoritmus DES není bezpečným především z hlediska délky svého klíče (56 bitů není v dnešní době výkonných počítačů rozhodně dostatečnou velikostí). 17. července 1998 Electronic Frontier Foundation oznámila zkonstruování hardwarového zařízení, které rozbíjí DES. Zařízení v ceně 220 000 dolarů zjistí klíč algoritmu DES v průměru za čtyři a půl dne.

Následovala (a zde slovo konečně je opravdu na místě) reakce amerických oficiálních institucí, po dvacet jedna letech své existence (od roku 1977) je norma DES nahrazena šifrovacím algoritmem s podstatně delší (nejméně dvojnásobnou) délkou klíče. I když zjevně je to řešení prozatímní (čeká se na AES) přesto opravený algoritmus 3-DES je nepochybně bezpečnější cestou k ochraně dat.

Postranní kanály

Zvýšená pozornost je v posledních létech věnována útokům z tzv. postranního kanálu (side-channel attack). Např. Paul Kocher demonstroval využití tzv. časového útoku (timing attack). Přesným měřením

času při provádění různých kryptografických operací lze rozbít některé realizace (v určitých situacích – např. on-line odezvy) šifrovacích algoritmů. V zásadě přitom nezáleží na typu algoritmu. Podobné výsledky dosáhl stejný autor při analýze spotřeby proudu. Tímto způsobem lze např. extrahovat utajovaný klíč z čipové karty.

Obdobným únikovým kanálem jsou také různé vyzařovací charakteristiky (i proti čipové kartě lze použít tento způsob útoku). Navíc pokud jsou výše uvedené metody doprovázeny vnucenými poruchami (tzv. fault analysis), pak pro případného útočníka se zde ukazuje mnoho cest k proniknutí ke chráněným informacím.

Při hledání ochran oproti těmto technikám je vhodné zamýšlet se spíše nad vlastní konstrukcí celého ochranného systému než vynakládat úsilí na vylepšování fyzikálních charakteristik systému. Takováto cesta by mohla být nakonec příliš drahá a přitom s největší pravděpodobností by se vynaložený efekt minul s účinkem. Změna koncepce systému může sice vést k složitějšímu modelu, na druhou stranu při odborné konstrukci dokáže výrazně zvýšit jeho bezpečnostní charakteristiky.

Proč potřebujeme dobrou kryptografii

Podívejme se nejprve na jedno v současnosti se rychle rozvíjející a perspektivní odvětví – na elektronický obchod. Automatizace úkonů – právě ta činí ze systémů elektronického obchodu systémy efektivnější než jsou klasické „papírové“ systémy. Na druhou stranu právě ona činí tyto systémy zranitelnějšími. Útočník může být fyzicky velmi vzdálen vzhledem k objektu svého útoku a pokud jednou uspěje, pak proč by oproti shodnému systému ochran neuspěl i vícekrát?

Velká díra v bezpečnosti elektronického obchodu tak může vést k bankrotu firmy během jediného dne. Jestliže používám nedostatečně bezpečný systém dnes a třeba již i několik roků předtím, pak to vůbec neznamená, že jednoho dne nepřijde nějaký Babinský a jednoduše a rázně přivede moji firmu na mizinu. Úspěšný elektronický systém musí být konstruován i s ohledem na bezpečnou budoucnost, musí být schopný opřít se i proti silnějším protivníkům než jsou ti dnešní.

Co však říci o systémech zabezpečujících kryptografickou ochranu, které jsou dnes na trhu (našem i světovém)? Řada těchto systémů nebyla konstruována ve spolupráci s odborníky kryptology. Konstruovali je (byť vysoce kvalifikovaní) inženýři, kteří brali kryptografii jako jednu z dalších komponent systému. Ovšem kryptologie je především věda o zranitelnosti. Zranitelnost systému je jak známo dána nejslabším článkem celého systému. A na to se někdy zapomíná. Nepomůže použití sebevíce kvalitního šifrovacího algoritmu, jestliže bude například práce s klíči nedostatečně ošetřena.

Takovou známou, avšak přitom stále běžnou slabinou je například přilogování se do lokální sítě. Co mi je platné, že mám pečlivě odděleny jednotlivé uživatele, každý z nich se hlásí do systému pomocí hesla jen pouze jemu známému, když nakonec tato hesla chodí po síti otevřeně a nemusím být ani příliš zručným hackerem, abych se k takovému to heslu dostal.

Řada kryptografických resp. obecněji bezpečnostních a ochranných systémů zatím zdánlivě stále funguje. Ale již dnes se setkáváme s elektronickým vandalismem, kdy předmětem útoku se stávají webovské stránky známých institucí, poskytovatelé internetových služeb jsou zahlcováni umělými e-maily. Existence méně kvalitních ochranných systémů je samozřejmě zdrojem perspektivní počítačové kriminality.

Dnes již dobře umíme konstruovat kvalitní šifrovací algoritmy. Praktická kryptografie však vyžaduje nejen to. Vyžaduje jejich kvalitní a bezpečnou implementaci, vyžaduje všestranné a hluboké posouzení řady souvisejících aspektů, ať je to klíčové hospodářství se všemi jeho stránkami (protokoly k výměně klíčů, práce s digitálními certifikáty atd.), ať jsou to různé autentizační prostředky a protokoly či ať to je všestranné posouzení bezpečnosti systému v němž je kryptografie implementována.

A jestliže vrátíme k úvodu, pak z hlediska současného rozvoje kryptologie jsou zcela jasná následující doporučení:

l. Používejte kryptografická řešení, která se opírají o hluboké a všestranné použití mezinárodních norem.
2. Používejte řešení zpracovaná skutečnými odborníky na danou problematiku, spolupracujte s těmito odborníky.
3. Nekupujte zajíce v pytli. Nechte si předložit veškerou dokumentaci nakupovaného řešení.
4. Nepoužívejte neznámé či tzv. proprietární algoritmy.
5. Nechte si provést celkovou bezpečnostní analýzu toku Vašich důvěrných dat.
6. Šifrujte, rozhodně šifrujte!

Některé zajímavé WWW stránky:

Dnes pouze jedna, za to na ní najdete určitě i ten odkaz, který zajímá právě Vás:

http://www.cs.auckland.ac.nz/~pgut001/links.html