Kapitola 9

Kryptografie v běžném životě

Úvod

V této knize jsme už opakovaně zdůrazňovali vliv kryptografie na podobu moderního světa a některé z důležitých prvků jsme ilustrovali na situacích z běžného života. V následující kapitole si ukážeme celou řadu dalších situací, při nichž kryptografie slouží k zajištění bezpečnosti různých služeb. Mnohé z nich jsou takové, na které narážíme skoro každý den, aniž bychom si často uvědomovali rizika, jež podstupujeme, nebo úlohu, kterou za daných okolností hraje šifrování. Pokaždé si načrtneme danou situaci, probereme si bezpečnostní rizika a ukážeme si, jakým způsobem je zde použita kryptografie.

Výběr hotovosti z bankomatu

Při výběru peněz z bankomatu je nutné použít plastovou kartu s magnetickým páskem a znát příslušný PIN. Zákazník vloží kartu do bankomatu a zadá PIN. Poté určí, jak velkou sumu si chce vybrat. Při běžné transakci musí systém ověřit, zda je PIN pro danou kartu správný, a pokud se jedná o on-line transakci, zbývá ještě zkontrolovat, zda je zákazník oprávněn požadovat určenou částku. Toto ověření probíhá většinou v centrálním počítači banky, tak-

že mezi hostitelským počítačem a bankomatem musí probíhat oboustranná komunikace. Bankomat odešle na hostitelský počítač informace o kartě a PINu a následně obdrží zprávu, v níž je transakce buď autorizována, nebo zamítnuta. Je jasné, že tato komunikace musí být chráněna.

Informace o vybírané částce sice nemusí být tajná, ale je nutné, aby částka vydaná automatem byla shodná se sumou, jež je odebrána z účtu. Zpráva tedy musí obsahovat kontrolu integrity dat. Banky se také zcela pochopitelně obávají, aby bankomat nevydal peníze po obdržení autorizace transakce vícekrát než jednou. Tím je dán požadavek na to, aby zpráva obsahovala pořadové číslo, a nebylo ji tak možné neoprávněně zachytit a vyslat do bankomatu ještě jednou.

Všechny banky své klienty nabádají k tomu, aby své PINy uchovávali v tajnosti. Pokud by někdo současně zjistil PIN a ukradl kartu, mohl by ji pak bez problémů používat. Banky se tedy musejí snažit, aby PIN nebyl v rámci systému prozrazen, a tak během vysílání a kontroly platnosti v databázi PIN musí být šifrován. Při tomto procesu bývá používán algoritmus DES v módu ECB. Vzhledem k tomu, že DES šifruje 64bitové bloky a PINy bývají běžně čtyřciferné, musí být blok s PINem před zašifrováním nějakým způsobem doplněn. Pokud by byla tato doplňující sekvence pro všechny zákazníky stejná, mohl by útočník, jenž získal přístup k zašifrovaným blokům s PINy, snadno odhalit zákazníky se stejnými identifikačními čísly, a to i v případě, kdy by neznal správný klíč. Aby k této situaci nemohlo dojít, používají se takové techniky doplňování sekvence, kdy dodatečné bity vycházejí z detailů zákazníkovy karty.

Díky tomuto způsobu šifrování nelze PIN zjistit ani v případě, kdy by někdo odposlouchával komunikaci mezi bankomatem a hostitelským počítačem. Zároveň nemohou PIN přečíst ani pracovníci banky, kteří mají přístup do databáze. Jak jsme ale již uvedli dříve, nic z toho

nebrání podvodníkům ve snaze o odhalení cizího PINu metodou pokus–omyl. Jestliže někdo najde nebo ukradne cizí kartu, může ji vsunout do bankomatu a zkusit číslo prostě uhodnout. Pro valnou většinu PINů existuje 10 000 možností, což není nijak závratné číslo. Valná většina bankomatů tedy povoluje pouze tři pokusy o zadání PINu a poté kartu „spolknou". To je považováno za rozumný kompromis mezi nebezpečím, že podvodník stačí číslo uhodnout, a rizikem, že skutečný majitel karty číslo splete nebo zadá PIN špatně. Použití šifrování ovšem nikomu nemůže zabránit správný PIN se štěstím uhodnout.

Některé dnešní bankomaty používají karty, u nichž lze využít kryptografii s veřejnými klíči. V takovém případě obsahuje uživatelova karta jeho soukromý klíč, jehož veřejnou hodnotu ověřuje certifikát podepsaný vydavatelem karty. Bankomat ověří kartu tím, že jí vyšle požadavek, který musí karta podepsat. Stejně jako je tomu u ostatních systémů založených na certifikátech, i pro bankomat platí, že k ověření platnosti certifikátu musí mít k dispozici autentickou kopii veřejného klíče vydavatele karty. U některých systémů to funguje tak, že tato hodnota bývá do bankomatů předem zabudována.

Placená televize

Jestliže se stanete předplatitelem systému placené televize, očekáváte, že se budete moci dívat na vybrané kanály, zatímco lidé, kteří si za ně neplatí, je sledovat moci nebudou. Systémy placené televize jsou ukázkou distribuce dat s řízeným přístupem. U takové informační sítě, v našem případě televizního vysílání, dochází k volnému vysílání dat, ale informaci obsaženou v signálu dokáže správně interpretovat jen omezená skupina příjemců. Běžným postupem je, že vysílaný signál bývá zašifrovaný

a klíč dostanou k dispozici pouze oprávnění příjemci informace. Takové systémy lze vytvářet a provozovat mnoha různými způsoby.

U běžného systému placené televize je každý kanál před samotným vysíláním zašifrovaný svým unikátním klíčem. Lidé, kteří mají takovýto program předplacený, platí de facto za přístup ke klíči jako takovému. Tím samozřejmě vznikají různé problémy se správou klíčů, především jak je rozeslat správným jednotlivcům. Obvyklým řešením je distribuce karet s unikátními soukromými klíči pro asymetrický šifrovací algoritmus jednotlivým uživatelům. Tyto karty se pak vkládají do čtecího zařízení, jež může být buď součástí televize, nebo se jedná o speciální zařízení dodané provozovatelem placené televizní sítě. Když divák zaplatí za nějaký konkrétní program, je symetrický klíč sloužící k zakódování programu před vysláním zašifrován pomocí předplatitelova veřejného klíče. Použijeme-li terminologii z kapitoly 8, jedná se o sytém s dvouvrstvou hierarchií klíčů a hybridním využitím symetrických a asymetrických algoritmů.

Pretty Good Privacy (PGP)

Původní systém Pretty Good Privacy neboli PGP vytvořil koncem 80. let minulého století Phil Zimmermann. PGP, které mělo sloužit jako uživatelsky přívětivý program pro počítačové šifrování, využívá jak symetrickou, tak asymetrickou kryptografii. Nyní je používána celá řada různých verzí. Dále se zaměříme především na základní koncept, aniž bychom se soustředili na nějakou konkrétní verzi či aplikaci.

PGP využívá dvouvrstvou hierarchii klíčů, přičemž symetrické klíče chrání data a asymetrické slouží jak

k podepisování, tak k šifrování symetrických pracovních klíčů. Využití PGP je velmi různorodé, příkladem je zabezpečování elektronické pošty či uložených souborů. Zveřejnění PGP v roce 1991 přivedlo Phila Zimmermana do sporů jak s vládou USA (kvůli údajnému nezákonnému vývozu kryptografie), tak s držiteli různých patentů. K urovnání těchto sporů došlo až roku 1997. Základní verze PGP je dnes k dispozici ve formě freewaru (za jeho používání není třeba platit) a je dodávána jako součást softwarové výbavy mnoha nových počítačů.

Jak jsme již uvedli, hlavním problémem při používání asymetrického šifrování je ověřování klíčů. Jedno z možných řešení, které jsme si představili výše, představuje síť certifikačních autorit (CA) a infrastruktura veřejných klíčů (PKI). PGP přišlo s jiným způsobem, jak se vypořádat s problémem ověřování veřejných klíčů: pomocí *sítě důvěry*.

Síť důvěry lze vytvořit následujícím způsobem. Nejprve si každý uživatel sám označí svůj vlastní veřejný klíč jako autentický, každý tedy zpočátku funguje jako vlastní certifikační středisko. Nyní předpokládejme, že máme uživatele A a B, přičemž každý z nich má klíče podepsané sám sebou. Jestliže uživatel B „důvěřuje“ uživateli A, pak B bez problémů podepíše veřejný klíč A jako autentický. Uživatel B se tedy v zásadě zachová jako certifikační středisko pro uživatele A. Teď si vezměme uživatele C, který uživatele A nezná, ale chtěl by mít jistotu, že veřejný klíč A je autentický. Pokud C „důvěřuje“ některému z lidí, kteří podepsali veřejný klíč A, bude C bez obav považovat veřejný klíč A za autentický. Takovýto uživatel je považován za *doporučovatele* A pro C. Takovýmto křížovým podepisováním veřejných klíčů postupem času vznikne široká a propletená síť ověřených veřejných klíčů, neboli síť důvěry. Díky tomu si

může uživatel sám stanovit úroveň důvěry ke každému z klíčů podle toho, nakolik věří jednotlivým podpisům stvrzujícím autenticitu klíče.

Od roku 1991, kdy vyšla první verze PGP, došlo k mnoha aktualizacím, přičemž poslední má číslo 9.0. Zatímco rané verze PGP využívaly jako symetrické a asymetrické kryptografické algoritmy RSA a IDEA, do pozdějších verzí již byly k symetrickému a asymetrickému šifrování implicitně zapracovány algoritmy Diffie-Hellman/El Gamal a CAST. Nyní si v krátkosti načrtneme šifrovací procesy, k nimž u PGP dochází při různých nastaveních šifrování elektronické pošty.

Klíče PGP (PGP Keys)

Při tomto nastavení se zobrazí okno, kde jsou vypsané všechny dvojice uložených asymetrických klíčů daného uživatele, uložené veřejné klíče ostatních uživatelů i s úrovní důvěry a rovněž seznam podpisů spojených s každým z těchto klíčů. V tomto okně lze ověřovat a podepisovat veřejné klíče ostatních uživatelů a exportovat či importovat veřejné klíče s jejich podpisy. Toto nastavení také umožňuje generování nových párů asymetrických klíčů, jejichž podoba se odvíjí od pohybů myši a stisknutých kláves. Soukromý klíč z tohoto páru je následně uložen v šifrované podobě, přičemž k zašifrování je použit symetrický algoritmus a uživatelem zvolená klíčová věta.

Zašifrovat (Encrypt)

Tato volba zašifruje zprávu pomocí symetrického šifrovacího algoritmu a pracovního klíče, jehož podoba se odvíjí od pohybů myši a stisknutých kláves. Tento pracovní klíč je následně zašifrován veřejným klíčem příjemce. Zašifrovanou zprávu s přiloženým zašifrovaným

klíčem lze poté odeslat příjemci. Ten pak může pomocí svého soukromého klíče získat symetrický pracovní klíč a tím pádem i samotnou zprávu.

Podepsat (Sign)

Tato volba podepíše zprávu soukromým klíčem odesílatele. Příjemce si může tento podpis ověřit pomocí odesílatelova veřejného klíče.

Zašifrovat a podepsat (Encrypt and Sign)

Tato volba podepíše a poté zašifruje zprávu dle výše uvedených postupů.

Dešifrovat/Ověřit (Decrypt(Verify)

Tato volba umožní příjemci dešifrovat zašifrovanou zprávu nebo ověřit podpis (případně obojí).

Zabezpečené brouzdání po internetu

V současnosti na internetu nakupuje mnoho lidí. Často k tomu potřebují kreditní kartu, přičemž informace o ní jsou odesílány na různé internetové servery. Jako jeden z hlavních důvodů, proč se elektronické nakupování nevyužívá ve větší míře, bývá často uváděna právě obava o bezpečí těchto údajů. V této krátké kapitolce si probereme, jakým způsobem jsou informace o kartě na internetu chráněny, a poté se podíváme i na další bezpečnostní problémy.

Zabezpečený pohyb po internetu je pro elektronické obchodování naprosto nezbytný. K ověření autenticity stránek bývají používány především protokoly *Secure Sockets Layer* (SSL) a *Transport Layer Security* (TLS). Tyto protokoly se starají o šifrování citlivých dat a po-

máhají s kontrolou integrity informací vyměňovaných mezi webovými prohlížeči a internetovými servery. V dalším textu se zaměříme na SSL.

SSL je příkladem protokolu klient-server, přičemž klientem je v tomto případě webový prohlížeč. Klient iniciuje zabezpečenou komunikaci a server odpovídá na jeho požadavky. Nejzákladnější funkcí, ke které je SSL využíváno, je vytvoření kanálu pro posílání šifrovaných dat z prohlížeče na zvolenou stránku (respektive server). Těmito daty mohou být například podrobnosti o kreditní kartě.

Ještě než se zaměříme na samotné protokoly, měli bychom uvést, že webové prohlížeče běžně obsahují některé kryptografické algoritmy a hodnoty veřejných klíčů celé řady nejvýznamnějších certifikačních středisek.

Při odeslání úvodní zprávy z prohlížeče na server (označované jako „Client Hello“) musí prohlížeč poslat na server seznam podporovaných kryptografických parametrů. Ačkoliv ale tato zpráva inicializuje výměnu informací umožňující použití šifrování, žádným způsobem neidentifikuje serveru prohlížeč jako takový. U mnoha aplikací dokonce obecně platí, že prohlížeč není serverem nijak ověřován a ověřovací protokol pouze autentizuje server prohlížeči. Dává to smysl. Jestliže si například někdo chce něco koupit prostřednictvím internetového prohlížeče, je velice důležité, aby měl možnost zjistit, zda se připojuje k zamýšlenému serveru. Na druhou stranu prodejce mívá jiné prostředky, jak zjistit totožnost nakupujícího, nebo se o ni ani nemusí zajímat. Jakmile totiž obchodník obdrží číslo kreditní karty, může si ověřit tuto kartu – a to pro jeho účely bohatě postačuje.

Webová stránka se prohlížeči autentizuje zasláním svého certifikátu veřejného klíče, a pokud prohlížeč příslušný veřejný klíč má, dostane i autentickou kopii veřejného klíče serveru. Při vytváření bezpečného kanálu odešle prohlížeč serveru pracovní klíč pro smluvený sy-

metrický algoritmus. Tento pracovní klíč je následně zašifrován pomocí veřejného klíče serveru, díky čemuž má prohlížeč jistotu, že jej může použít jen zamýšlená internetová stránka. SSL je tedy dalším běžným příkladem systému s hybridní správou klíčů, o kterých jsme mluvili v kapitole 8. Je též ukázkou využití PKI pro ověření entit.

Používání mobilního telefonu GSM

Jednou z hlavních výhod mobilních telefonů, která stojí za jejich stále rostoucí oblibou, je možnost volat prakticky odkudkoliv. Mobilní telefony nemají pochopitelně žádné dráty, takže hovor je vysílán vzduchem, kudy doputuje k nejbližší základnové stanici, z níž je pak odeslán po pevné pozemní lince. Vzhledem k tomu, že zachycení rádiového signálu je mnohem snazší než zachycení hovoru po pevné pozemní lince, jedním z hlavních bezpečnostních požadavků na GSM bylo, aby zabezpečení systému dosahovalo alespoň stejné úrovně, jako je tomu u pevných telefonů. Tento požadavek byl splněn zašifrováním přenosu z telefonního přístroje k nejbližší základnové stanici. Dalším vážným bezpečnostním problémem bylo zajistit operátorovi možnost zjistit, kdo volá, aby věděl, na čí účet hovor připsat. S provozováním sítě GSM jsou tedy spojeny dva hlavní bezpečnostní požadavky: utajení, které chtějí uživatelé, a ověření uživatele, což zase vyžaduje systém samotný.

Každý uživatel má vlastní kartu zvanou SIM, která obsahuje 128bitovou tajnou autentizační hodnotu, s níž je seznámen pouze operátor. Toto číslo slouží jako klíč pro ověřovací protokol typu výzva – odpověď; algoritmus protokolu si zvolí sám operátor. Když chce uživatel někomu zavolat, je informace o jeho identitě odeslána operátorovi přes základnovou stanici. Vzhledem k tomu,

že základnová stanice nezná tajný kód SIM a ani nemusí být seznámena s autentizačním protokolem, vygeneruje centrální systém požadavek a odešle jej i s odpovědí pro příslušnou kartu zpět na základnovou stanici. Tímto způsobem může základnová stanice ověřit platnost odpovědi.

Karta SIM obsahuje kromě autentizačního algoritmu také proudový šifrovací algoritmus, který je společný pro celou síť. Tento algoritmus slouží k zašifrování hovoru při přenosu z telefonu na základnovou stanici. Správa šifrovacích klíčů je velice propracovaná a využívá autentizačního algoritmu. Ten přijímá 128bitovou výzvu a počítá 128bitovou odpověď, která se odvíjí od autentizačního klíče karty. Z této odpovědi je však ze SIM na základnovou stanici odesláno pouze 32 bitů.

Z toho vyplývá, že po dokončení autentizačního procesu je 96 bitů z tajné informace známo pouze SIM, základnové stanici a řídícímu počítači. Z tohoto řetězce je 64 bitů vyhrazeno pro určení šifrovacího klíče. Nutno ještě dodat, že po každé autentizaci je šifrovací klíč jiný.