Kryptologie pro praxi – jak se podělit o tajemství

Mějme za úkol vyřešit problém bezpečné dopravy tajného šifrovacího klíče z jednoho místa na druhé. Z nějakého důvodu k tomu přitom nechceme nebo nemůžeme použít příslušná asymetrická schémata, která jsme si představili v předchozích dílech tohoto seriálu (viz [4]). Nezbývá nám proto, než se spolehnout na nějaký chráněný kanál, kterým pro nás bude fyzická osoba, říkejme jí agent-kurýr. V praxi tato situace nastává například při zavádění hlavních šifrovacích klíčů do kryptografických modulů bankomatů. Je jasné, že své agenty si budeme vybírat podle kritéria maximální důvěry. Z praxe však víme, že každá důvěra má svou mez a každý agent svojí cenu. Dostáváme se tak k jádru našeho problému, a to k otázce, zda a jak se můžeme bránit pokusům o kompromitaci přenášeného klíče při selhání kurýra. I když za uvedených podmínek (vzdali jsme se veškerých výhod asymetrické kryptografie) vypadá situace beznadějně, řešení existuje a není ani nijak extrémně náročné. Jmenuje se schéma pro sdílení tajemství typu (t,n), kde $t \le n$. Umožňuje nám rozdělit příslušný tajný řetězec na n částí, takzvaných podílů (v originále *shares*), takovým způsobem, že původní tajný řetězec (tajemství) lze obnovit pouze při znalosti alespoň t z jeho n podílů. Pro výše popsaný účel se nám výborně hodí schéma typu (n,n), přičemž místo jednoho kurýra použijeme kurýrů hned n. Každý z kurýrů dostane jeden podíl, který přenese do cílového bodu, kde jej samostatně vloží do důvěryhodného kryptografického modulu. Po vložení všech n podílů si modul uvnitř autonomně složí původní tajný klíč, přičemž původní podíly jsou skartovány. Je zřejmé, že s rostoucím n klesá při správném výběru agentů (nesmí to být lidé s významnou osobní vazbou, atp.) pravděpodobnost, že všichni naráz selžou. Pokud by selhala jen nějaká jejich podskupina, nebylo by jim to nic platné, neboť bez získání podílů jejich loajálních kolegů se jim nepodaří přenášený klíč rekonstruovat. Zkušenosti ukazují, že v praxi si vystačíme už se schématy typu (2,2) pro běžné a (3,3) pro zvlášť citlivé přenosy. Kromě právě nastíněného příkladu lze diskutovaná schémata nasadit například i v situaci, kdy potřebujeme bezpečně archivovat nějaký hlavní klíč.

Schéma typu (n,n)

Jeho účel lze spatřovat zejména v bezpečné distribuci klíčového materiálu, pročež se často označuje jako *schéma pro rozdělení klíče*. Konkrétní realizace může vypadat následujícím způsobem (schéma lze následně upravit i pro jiný vhodný operátor, například součet modulo p): Označme K přenášený klíč v délce b bitů. Pro jeho rozdělení na n podílů vygenerujeme celkem $n-1$ náhodných čísel $S_1, S_2, \ldots, S_{n-1}$, každé z nich v délce b bitů. Dále vypočteme $S_n = K \oplus S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1}$. Podíly S_1 až S_n pak po jednom rozdělíme mezi kurýry a vyšleme je nezávisle na cestu. Po vložení všech podílů do cílového kryptografického modulu bude původní klíč složen opět jednoduchou operací vektorového eXclusive OR (XOR) jako $K = S_1 \oplus S_2 \oplus \ldots \oplus S_n$. Zároveň je vidět, že jakákoliv podmnožina $n-1$ kurýrů může dohromady složit pouze náhodné číslo, které nedává žádnou informaci o klíči K.

Schéma typu (t,n) pro $t<n$

Zásadním přínosem těchto schémat je zvýšená odolnost proti ztrátám (nejen kurýrů, ale třeba i nedostupnosti některých zdrojů podílů), které je zde dosaženo díky redundantnímu počtu podílů. Použijeme-li místo typu (2,2) typ (2,4), získáme stejný stupeň důvěrnosti, avšak sdílené tajemství budeme stále schopni sestavit, i když se nám nějaké dva podíly ztratí. Toho se v praxi využívá zejména při archivaci důležitých klíčů, kde hrozí, že některý z podílů může být časem zničen, nebo nemusí být v okamžiku obnovy zrovna dostupný. Reálné uplatnění je nutné (bohužel) hledat například i při přenosu klíče v místech intenzivních vojenských konfliktů, kde je jistá pravděpodobnost, že některý z kurýrů do cílového místa nedorazí. Ze stejného prostředí je i sdílení kódů pro aktivaci jaderných zbraní, které může provést jakákoliv dostatečně velká skupina přítomných vysokých důstojníků. Poklidnějším uplatněním je (snad) zasílání klíčů pomocí poštovní či kurýrní služby.

Představíme si dnes již klasické, avšak stále hojně využívané Shamirovo schéma z roku 1979 [3]. Označme K celé číslo reprezentující tajemství, které chceme rozdělit mezi n agentů. Zvolíme prvočíslo p, $p > \max\{K,n\}$ a položíme $a_0 = K$. Dále vygenerujeme náhodné koeficienty $a_1, a_2, \ldots, a_{t-1}$, splňující $0 \le a_i \le p-1$. Ze získaných koeficientů sestavíme polynom $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots + a_0$ nad tělesem $\mathbf{Z}_p$. Označíme-li podíl j-tého agenta jako S_j, pro $1 \le j \le n$, potom jednotlivé podíly vytvoříme jako $S_j = f(j) \bmod p$, čili jako funkční hodnoty polynomu $f(x)$ v bodech $x = 1, 2, \ldots, n$. Připomeňme, že díky konstrukci $f(x)$ platí $K = f(0)$. Známe-li polynom $f(x)$, jsme triviálně schopni sestavit sdílené tajemství. Lze dále ukázat, že ke kompletní rekonstrukci $f(x)$ postačí znát jeho funkční hodnoty v t různých, známých bodech. Na této skutečnosti je založena hlavní idea Shamirova schématu: Jednotlivé podíly totiž představují právě takové hodnoty, takže nám postačí získat t různých podílů $S_{\pi(1)}, S_{\pi(2)}, \ldots, S_{\pi(t)}$, abychom byli na základě Lagrangeova interpolačního vzorce (viz [2], [3]) schopni rekonstruovat polynom $f(x)$ a následně určit sdílené tajemství $K = f(0)$.

Bezpečnost

Obě schémata, která jsme si zde představili, poskytují takzvanou perfektní bezpečnost. To znamená, že při získání méně než t podílů útočník stále nezískává žádnou informaci o sdíleném tajemství. Z teoretického hlediska jsou tím tato schémata v jistém směru dokonce bezpečnější než běžné asymetrické techniky, kde například při zachycení šifrového textu RSA přenášejícího tajný symetrický klíč (*ST 3/2004*) útočník jistou informaci získá – díky výpočetní složitosti je pro něho nevyužitelná. Neznamená to však, že by zde neexistovaly potenciální slabiny. Při implementaci schémat pro sdílení tajemství musíme dávat pozor na aktivní útoky založené na tom, že někteří z agentů do procesu obnovy záměrně podstrčí falešné podíly a na základě odezvy systému se budou snažit samostatně sestavit sdílené tajemství. Například v prvním z uvedených schémat by mohl podvodný agent místo svého b-bitového podílu S_j do systému vložit hodnotu $S_j \oplus W$, kde W je jím zvolená nenulová náhodná hodnota v délce b bitů. Snadno nahlédneme, že místo K pak bude sestavena hodnota $K' = K \oplus W$. Pod záminkou, že sestavený klíč stejně nefunguje, a že zkusí „prověřit“ proč, získá agent-útočník hodnotu K', ze které již snadno odvodí správné K. Poté přesvědčí ostatní kurýry, aby zkusili provést sestavení znovu, přičemž nyní již poskytne správnou hodnotu svého podílu. Vše „zázrakem“ zafunguje, kurýři se zaradují, podepíší příslušný protokol a rozejdou se ke svým dalším úkolům. Věc má však, jak víme, háček – jeden z nich zná hodnotu aktivovaného klíče… Základní obranou je provádět po

úspěšném složení tajemství ověření jeho integrity (u bankomatů se například provádí takzvaný kontrolní výběr). Pokud se zjistí nesrovnalost, generuje se nový klíč, znovu se rozdělí a celá distribuce se opakuje znovu. Případně může být celý postup obnovy opakován s tím, že celý proces nesmí v žádném případě otevřeně poskytovat hodnotu, byť nefungujícího, výsledku. Obranou přímo na základní úrovni protokolu se pak zabývají schémata vycházející z konceptu [1].

Závěrem lze konstatovat, že schémata pro sdílení tajemství patří mezi elegantní nástroje současné kryptografie, které umožňují bezpečně vyřešit řadu praktických problémů z oblasti informační bezpečnosti, aniž by bylo bezprostředně nutné sahat k technikám o několik řádů komplikovanějším. Podtrhují tak nesprávnost zakořeněného názoru „zkušených expertů“, že bez asymetrické kryptografie nelze postavit kvalitní bezpečnostní infrastrukturu.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Chaum, D., Evertese, J.-H., Chor, J.-B., Goldwasser, S., Micali, S., and B. Awerbuch: Verifiable secret sharing and achieving simultaneity in the presence of faults, in Proc. of the IEEE 26th Annual Symposium on Foundations of Computer Science, pp. 383–395, 1985

[2] Menezes, A.-J., van Oorschot, P.-C., and Vanstone, S.-A.: Handbook of Applied Cryptography, CRC Press, 1996

[3] Shamir, A.: How to share a secret, Communications of the ACM, 22, pp. 612–613, 1979

[4] E-archivy http://cryptography.hyperlink.cz a http://crypto.hyperlink.cz

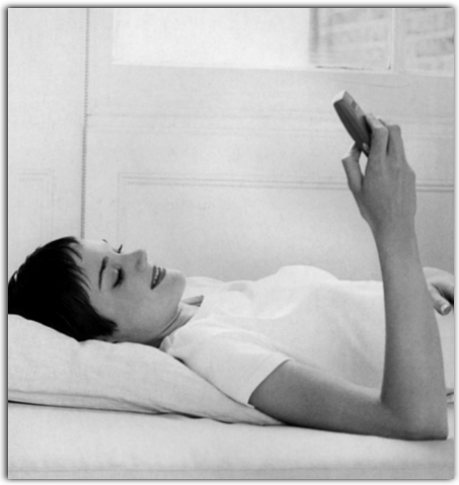
Realita falešných SMS a způsob obrany

V polovině loňského prosince byly prezentovány řadou veřejnoprávních médií komentované důkazy o prolomení důvěryhodnosti zpráv SMS. Při současném stavu softwarové obsluhy servisních SMS-center všech tří provozovatelů mobilních sítí v ČR je, jak se zdá, pro programátora obeznámeného s technickým řešením relativně jednoduché zfalšovat identitu odesílatele ve fázi odbavování zakázky v centru pro doručování zpráv na číslo adresáta. Spoluautor série článků Kryptologie pro praxi, Tomáš Rosa, vysvětluje:

„Tématu autentizace a původu zpráv se už několik let věnuji ve svých přednáškách pro studenty MFF UK a na uvedenou slabinu jsem už v minulosti upozorňoval také v jednom svém článku pro Sdělovací techniku. Prolomení důvěryhodnosti SMS je jenom jedním z dalších důkazů toho, jak se každá technicky vyspělá společnost dříve či později může stát nepřiměřeně závislou na rozlehlých (tudíž snadno zranitelných) elektronických systémech. Představa, že bezpečnostní incidenty by mohly v masovém měřítku poměrně snadno způsobit rozvinutým ekonomikám nepředstavitelné hospodářské ztráty, je v této souvislosti docela reálná. Hlavními příčinami se jeví téměř živelný rozvoj hardwarových prostředků informačních a komunikačních technologií, ztráta kontroly nad vznikem a růstem rozmanitých typů sítí i jejich sílící konektivita.

Podíváme-li se podrobněji na klasickou strukturu sítí GSM, pak (pokud nedojde k bezprecedentnímu narušení základních bezpečnostních zásad) má mobilní operátor k dispozici všechny prostředky k tomu, aby neoprávněnému přístupu k vnitřním procesům a tokům dat dokázal zabránit. Přístup k datům klientů v zákaznických dohledových centrech má pouze obsluha vybavená přístupovými právy a nikdo jiný. Útok ze strany obsluhy je málo pravděpodobný. Praktická zkušenost však ukázala, že část tohoto řetězce je nedomyšlená. Mám na mysli externí komunikační kanály SMS-centra, u nichž lze, jsou-li tyto kanály otevřeny, zamaskovat autentizaci. Naše servisní SMS-centra (jak mne ujistil Martin Volyňský, který veřejně demonstroval, že umí odesílat falešné SMS do českých lokálních sítí, aby konečně vyvolal tuto diskuzi) jsou z tohoto pohledu bezpečná.

Stačí však najít jedno jediné centrum SMS na světě, které funguje také jako roamingový partner našeho operátora, aby se celá lokální síť vystavila nebezpečí zranitelnosti právě přes tuto obtížně identifikovatelnou cestu. Z obecného hlediska tvorby kryptologických algoritmů se náhle objevuje nová, fascinující dimenze. Roste míra neuspořádanosti sítí nesoucí sebou nebezpečí vzniku „vedlejších“, relativně snadno prolomitelných kanálů. Přitom stačí najít jediné zahraniční nedostatečně chráněné centrum, které je v roamingovém vztahu k našemu operátorovi a rázem mohou být potenciálně ohroženi i všichni uživatelé pracující v síti daného operátora.



Z tohoto příkladu vyplývá, že absolutní důvěra v dokonalost elektronických komunikací se může uživateli velice nepříjemně vymstít. Je nezbytné mít stále na paměti, že opatrnosti, zdravého rozumu a informační bezpečnosti není nikdy dost. Jinak se všichni vystavujeme nebezpečí, že se chytneme do pastičky, kterou si na sebe už dlouho a s vysokými náklady chystáme!

Lze se však poměrně účinně bránit i jednoduchými prostředky a tak neustále ztěžovat potenciálnímu útočníkovi jeho pozici. Doporučuji nespoléhat se na zabezpečení poskytované operátorem a používat i tzv. „vlastní protokoly“. To je cesta, kterou se vydaly banky a některé společnosti poskytující finanční poradenství, dodavatelé systémů pro vzdálené ovládání přístupu do budov, pro přímý vstup do automatizovaných systémů řízení výrobních a technologických procesů atd. Další, prostou ale v praxi dostatečně účinnou možností, je posílat v těle zprávy skryté autentizační kódy (certifikační kódy), které jsou srozumitelné pouze správnému adresátovi. To je i jedna z cest, kterou by se měli vydat i návrháři dálkově ovládaných modulů, v nichž by do budoucna neměla chybět ani služba automatické odpovědi a potvrzení akce. Samozřejmě se nabízí i volba adekvátní kryptologické ochrany. Uváděné způsoby lze obvykle i kombinovat.

Existuje také řada jednoduchých, řekněme „manuálních“ metod, jejichž účinnost byla ověřena např. spojeneckými vojsky za druhé světové války (každá autentická zpráva musí začínat smluveným heslem, které se ve smluvenou hodinu mění), řada modernějších mobilních telefonů umožňuje kontrolu čísla SMS-centra, které zprávu posílá (pokud uvidíte jiné číslo než to, které používá váš operátor, je zpráva podezřelá). Obávám se, že prolomení důvěryhodnosti SMS zpráv znamená odhalení koncepční slabiny, kterou operátor nevyřeší jednoduchým mávnutím kouzelného proutku. Tlaky na řešení vzniklé situace lze v ČR očekávat i z nejvyšších politických a ekonomických pozic. Pokud se jedná o vývoj nových architektur a nových telekomunikačních služeb, měla by se otázka důsledné aplikace kryptologických metod považovat významné kritérium při výběrových řízeních a při rozhodování o velkých státních zakázkách.“

Jik