Kryptologie pro praxi – Imunitní trik pro RSA

Na jaře roku 2003 byl na Internetu poprvé uveřejněn článek [1] kolegů ze Stanfordovy univerzity v Kalifornii, který ukazoval, že časový útok na RSA je možné úspěšně provést i v podstatně komplikovanějším prostředí, než bylo původně uvažováno. S ohledem na nutnost precizního měření časových intervalů a vyhodnocování malých diferencí (asi 1 ms a méně) byly útoky založené na časových postranních kanálech dříve zařazovány prakticky výhradně do oblasti čipových karet a jim podobných zařízení. Autorům [1] se však podařilo předvést prakticky schůdný vzdálený útok na privátní klíč serveru z prostředí lokální počítačové sítě. Tím se zásadně zvýšila pozornost věnovaná časovým postranním kanálům i při návrhu „velkých" systémů. Přesněji řečeno, měla by se zvýšit. Na základně reálných zkušeností můžeme předpokládat, že řada architektů si s tímto problémem příliš hlavu neláme, či o něm dost možná ani neví. O jejich přístupu ostatně jasně vypovídá i skutečnost, že obrana proti časovému útoku byla v kódu napadeného serveru vycházejícího z knihovny OpenSSL [3] sice připravena, ale nebyla aktivována [1]. Přitom stačí použít velmi jednoduchý trik a kryptografické schéma je rázem proti časovým útokům imunní.

Oslepení RSA

Úprava, která účinně brání časovým útokům na privátní klíč RSA, vznikla původně za zcela jiným účelem. Její návrh se odvíjí od myšlenky takzvaných slepých podpisů [2], které umožňují například dodržet určitou anonymitu klientů při placení pomocí takzvaných elektronických peněz. Označme $V = (N, e)$ veřejný a $P = (N, d)$ privátní klíč RSA. Klíče V a P se skládají ze společného modulu N a veřejného (e), respektive privátního (d) exponentu. Víme, že RSA používá dvě základní transformace, a to sice $E_V(x) = x^e \bmod N$ a $D_P(x) = x^d \bmod N$ (viz ST 3/2004, [4]). Nyní se soustředíme na transformaci $D_P(x)$, která se podle kontextu použití označuje jako odšifrovací nebo podepisovací. Nejprve si ukažme původní myšlenku slepých podpisů: Předpokládejme systém, ve kterém má určitá autorita rutinně vydávat podpisy předložených zpráv, aniž by směla znát konkrétní znění předkládaných textů. Jednou z možností je zasílat této autoritě pouze hašové kódy zpráv, což jí k výpočtu podpisu stačí, a spoléhat na to, že nebude schopna je invertovat. Tento přístup může ovšem selhat, pokud budou podepisované zprávy voleny ze známé množiny o velmi malé velikosti. Potom autorita metodou pokus-omyl jednoduše zjistí, k jaké zprávě z množiny přípustných textů zaslaný hašový kód náleží. Proto byl navržen přístup, který se na složitost hledání vzorů hašových kódů nespoléhá. Označme m zformátovanou (viz ST 10/2003) hodnotu hašového kódu zprávy, kterou má autorita podepsat. Tato autorita nechť na vyžádání vrátí hodnotu $y = D_P(x) = x^d \bmod N$ pro libovolné předložené x. Pokud bychom jí předložili hodnotu m, vypočetla by nám rovnou správný podpis $s = D_P(m) = m^d \bmod N$. Zároveň by se ale mohla pokoušet invertovat hašový kód podepisované zprávy M obsažený v m, a to my nechceme. Proto nejprve vygenerujeme náhodnou tajnou hodnotu r z intervalu $\langle 1, N-1\rangle$ splňující $\gcd(r, N) = 1$. Autoritě potom zašleme hodnotu $x = mr^e \bmod N$, přičemž ona nám vrátí $y = D_P(x) = (mr^e)^d \bmod N = m^d r \bmod N$. Díky podmínce $gcd(r, N) = 1$ existuje multiplikativní inverze $r^{-1} \bmod N$, splňující $r\,r^{-1} \bmod N = 1$. Konkrétní hodnotu $r^{-1} \bmod N$ najdeme triviálně například pomocí rozšířeného Euklidova algoritmu. Hledaný podpis s potom už snadno určíme ze znalosti hodnoty y, neboť platí $yr^{-1} \bmod N = m^d r\, r^{-1} \bmod N = m^d \bmod N = s$. Na rozdíl od přímočarého přístupu, kdy jsme autoritě zaslali rovnou hodnotu m, však nyní díky použití náhodné masky r není tato schopna z hodnoty x určit, pro jaké m vlastně podpis vytvořila. Nemůže se tedy ani snažit invertováním hašového kódu najít hodnotu podepsané zprávy M.

Obrana proti časovému útoku

Současné metody využití časových postranních kanálů (viz ST 3/2003, [4]) vycházejí z toho, že je k dispozici nejen přesná informace o době trvání výpočtu transformace $D_P(x)$, ale že útočník rovněž zná nebo dokonce může sám volit vstupní hodnotu x. Pokud je hodnota x pro útočníka neznámá, jeho šance na úspěch je prakticky nulová. Díky této skutečnosti našla technika slepých podpisů po bezmála dvaceti letech živoření v nepříliš žádaných schématech elektronických peněz zcela nové a podstatně více žádané uplatnění. Ukazuje se, že jako obrana proti současným časovým útokům na RSA prakticky zcela postačuje rozšířit kód pro výpočet $D_P(x)$ o vstupní maskování náhodnou hodnotou r a jemu korespondující výstupní demaskování hodnotou $r^{-1} \bmod N$, přesně podle výše popsaného postupu. Úprava se provádí jednotným způsobem pro šifrovací i podepisovací transformace. Zdůrazněme, že hodnota r musí být náhodná s rovnoměrným rozdělením na uvedeném intervalu, že ji musíme volit vždy znovu pro každý výpočet maskované transformace a pečlivě utajit před útočníkem.

Obrana proti ostatním postranním kanálům

Podobně jako časové jsou i napěťově-proudové či elektromagnetické útoky často založeny na postupu, kdy útočník simuluje průběh luštěné transformace pro jistou odhadnutou hodnotu části klíče a sleduje, nakolik jeho simulace koresponduje se signálem přijatým z daného postranního kanálu. Pokud simulace odpovídá signálu z kanálu, prohlásí odhad této části klíče za správný a pokračuje v luštění další části. V opačném případě odhad upraví a ověřovací simulaci opakuje. V příslušné teorii bývá celý tento postup obvykle popsán vhodnou korelační analýzou. Z praktického hlediska je podstatné, že neznalost konkrétní vstupní hodnoty v napadené transformaci znemožňuje jednoduchou simulaci výpočtu a útočník musí informaci z postranního kanálu dolovat podstatně složitější metodou. Narozdíl od časového útoku sice nemůžeme tvrdit, že by neměl žádnou praktickou šanci na úspěch, nicméně jeho role je i zde zásadním způsobem ztížena. Ztížena natolik, že bude patrně muset nakoupit mnohem dražší přístroje a použít mnohem složitější a pomalejší postupy. V praktické rovině tak lze doufat v úplné odvrácení útoku.

Závěr

Popsané opatření umožňuje velmi jednoduchým způsobem razantně omezit riziko útoků nejen časovými, ale do značné míry i napěťově-proudovými či elektromagnetickými postranními kanály. Jeho implementace je kromě nutnosti mít k dispozici kvalitní generátor náhodných čísel prakticky naprosto nenáročná. Proto je vhodné vybavovat tímto opatřením automaticky každý kryptografický modul, a to bez dlouhého bádání, jestli zde postranní kanály momentálně hrozí nebo ne. Mějme stále na mysli, že kdyby bývalo bylo zde popsané maskování důsledně používáno všemi implementacemi RSA, museli by bývali pánové Brumley a Boneh na jaře roku 2003 přiznat porážku. Místo toho ale mohli světu předvést elegantní útok, o jehož reálnosti řada odborníků do té doby pochybovala. Naštěstí to tehdy byli vědci, kteří slavili triumfální úspěch a je určitě zbytečné čekat, kdo to bude příště. Zvlášť když je obrana tak snadná…

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

LITERATURA

[1] Brumley, D. and Boneh, D.: Remote Timing Attacks are Practical, Proc. of 12th USENIX Security Symposium, pp. 1-14, 2003

[2] Chaum, D.: Blind Signatures For Untraceable Payments, Proc. of Crypto '82, pp. 199-203, Springer-Verlag, 1983

[3] Projekt OpenSSL, http://www.openssl.org

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