Kryptologie pro praxi – Achillova pata RSA

Vývoj kryptoanalytických metod v minulosti zaznamenal postupnou změnu v taktice vedení útoků, která po roce 1996 vyvrcholila příchodem dnes již dobře známých technik založených na postranních kanálech (ST 3/2003, [8]). V počátcích kryptoanalýzy měl luštitel k dispozici toliko šifrový text a v lepším případě i popis šifrovacího algoritmu. Cílem bylo najít odpovídající otevřený text a případně rovnou i kompletní šifrovací klíč, jehož znalost by umožnila rutinní luštění dalších zpráv. Čím víc však docházelo k používání kryptografických metod v masových výpočetních systémech, tím lepší nástroje dostávali analytici do rukou. Zatímco u ručně obsluhovaného šifrátoru bylo většinou nereálné uvažovat o tom, že obsluha bude ochotna předkládat šifrovacímu stroji útočníkem volené výzvy a poskytovat mu obdržené výsledky, tak u dnešního serveru, který musí během minuty obsloužit i několik tisíc požadavků, tento scénář už tak naivně nevypadá. Oproti minulosti proto analytici kromě zachycených dat a znalosti algoritmu získali ještě možnost určitým způsobem klást dotazy přímo kryptografickým zařízením. Tato na první pohled drobná výhoda zcela změnila pohled na odolnost kryptografických zařízení i algoritmů. To je závažná skutečnost, neboť se ukazuje, že starší zařízení z 90. let minulého století mohou být novými metodami snadno napadnutelná. Dokládá to například nedávné prolomení některých automobilových imobilizérů obsahujících bezkontaktní kryptografické čipy.

Každé zařízení je ovšem ochotno útočníkovi zodpovědět jiný druh otázek, a to navíc jiným způsobem. Některé odpovědi mohou mít doslova cenu zlata, jiné jsou zase k ničemu. Vzniká proto problém, jak tyto potenciální výhody zakomponovat do nějaké jednotné teorie popisující slabiny příslušného algoritmu. Zatím se s výhodou používá přístup založený na tzv. orákulech („černá skříňka“), která se používají následujícím způsobem: Analytik studuje obecné možnosti luštění nějakého algoritmu tak dlouho, dokud nedospěje k určité „propasti“, přes kterou se, díky výpočetní složitosti nebo nedostatku informace, už nedokáže ve svém postupu přenést. Dříve by to v tomto bodě pravděpodobně vzdal. Dnes to sice možná vzdá také, ale připíše k postupu k poznámku, že pokud by existovalo orákulum, které by bylo schopné cosi vypočítat a tím propast překlenout, vedla by tudy cesta k prolomení. Takový popis pak může ležet v knihovně i několik let, až si někdo jiný povšimne, že za určitých podmínek lze danému zařízení klást takové otázky, které z něho s trochou matematiky vytvoří právě ono orákulum. Tím je cesta k úspěšnému útoku otevřena. V praxi to tak jednoduché a přímočaré pochopitelně není, nicméně toto je základní kostra, kterou najdeme ve většině dnešních útoků postranními kanály [7].

Dvě strany jedné mince

Cílem tohoto článku je upozornit na jeden konkrétní druh orákula, které je potenciálně velmi nebezpečné pro RSA (ST 3/2004, [8]). Vše vychází z následujícího tvrzení (uvádíme zjednodušenou formulaci), které se též označuje jako *tvrzení o individuálních bitech RSA* [2]: Buď N veřejný modul a d privátní klíč RSA. Označme $Ora(x)$ orákulum poskytující nezanedbatelnou informaci o nějakém individuálním bitu z hodnoty $y=x^d \bmod N$ pro libovolné $x \in <0, N)$. Pokud $Ora(x)$ existuje, potom existuje polynomiálně složitý pravděpodobnostní algoritmus, který pro libovolný šifrový text C vrací hodnotu $m=C^d \bmod N$. Poznamenejme, že m je v kontextu celého šifrovacího schématu hodnota otevřeného textu RSA před operací dekódování (viz ST 10/2003). Tato operace už neobsahuje žádné tajné prvky, takže výpočet vlastní přenášené zprávy M je již triviální záležitostí.

Možná bude působit poněkud ironicky, že uvedené tvrzení bylo původně dokázáno jako významný argument pro (nikoliv proti) bezpečnost RSA a dodnes je za něj považováno. Jeho negací totiž získáme výrok, který zhruba říká, že každý individuální bit hodnoty m je chráněn stejně dobře, jako celá hodnota m. Pokud nejsme schopni získat celé m, potom nezískáme ani jeho jednotlivé bity. Tímto postupem lze například prokázat kvalitu určitého typu generátoru pseudonáhodných čísel [2], [6]. V kryptologii (podobně jako ve fyzice) však hodně záleží na konkrétní interpretaci každého formálního výroku. S nástupem RSA do masivních informačních systémů začali kryptoanalytici využívat toto tvrzení přesně tak, jak je napsáno: Uniká-li z dešifrátoru RSA informace byť jen o jediném bitu odšifrované hodnoty m, potom může útočník pro libovolný šifrový text vyluštit celou hodnotu otevřeného textu. Podotkněme, že podobné vlastnosti lze očekávat i u ostatních kvalitních algoritmů.

Složitost luštění

Z výše uvedeného tvrzení sice plyne, že pro luštění RSA lze využít postranní informaci o jakémkoliv bitu hodnoty m, avšak podstatné rozdíly jsou v efektivitě konkrétních lušticích postupů. Vysloveným šampiónem je v tomto směru orákulum poskytující informaci o nejméně významném bitu právě dešifrovaného otevřeného textu, tj. $Ora_{lsb}(x) \sim lsb(y)$ pro $y=x^d \bmod N$, $lsb(y)=y \bmod 2$. Ukážeme si, že pracuje-li toto orákulum bezchybně, čili $Ora_{lsb}(x)=lsb(y)=(x^d \bmod N) \bmod 2$, potom lze libovolný šifrový text x vyluštit s banální složitostí řádově $\log_2 N$ počtu volání Ora_{lsb}. Postup luštění je založený na prohledávání metodou půlení intervalů a je navíc v tomto případě velice jednoduchý. Nejdříve si připomeňme, jak se chová operace modulárního násobení hodnoty $y \in <0, N)$ číslem $2^{-1} \bmod N$.

Platí $y.2^{-1} \bmod N=(y+\mathrm{lsb}(y).N)/2$. Pokud je y sudé, potom výsledek přímo odpovídá „klasickému“ dělení dvěma. V opačném případě před vlastním dělením k hodnotě y pomyslně přičteme modul N. Nyní položme $x=C$ a voláním $Ora_{\mathrm{lsb}}(x)$ získejme hodnotu lsb(y) pro $y=m=C^d \bmod N$. Předpokládejme, že $E \le y \le F$, kde E a F jsou nějaká celá čísla reprezentující náš odhad neznámé hodnoty y. Nevíme-li vůbec nic o hledaném m, položíme $E=0$, $F=N-1$. Podívejme se nyní, v jakých intervalech se pohybuje hodnota $y'=y^*2^{-1} \bmod N$. Snadno odvodíme, že platí $E' \le y' \le F'$, kde $E'=(E+\mathrm{lsb}(y).N)/2$ a $F'=(F+\mathrm{lsb}(y).N)/2$. Vidíme, že hodnota y' leží buď v intervalu $<E/2, F/2>$, nebo v intervalu $<E/2+N/2, F/2+N/2>$, a to v závislosti na lsb(y). Součet velikostí obou intervalů je roven velikosti původního intervalu $<E, F>$, takže bez znalosti lsb(y) bychom tímto krokem žádného zpřesnění odhadu hodnoty y nedosáhli. Ležela by tu před námi právě výše zmíněná propast. Díky našemu orákulu však lsb(y) známe, takže můžeme pokračovat dál. Všimněme si, že zpráva y' pro nás sice zůstává stále neznámou, avšak velikost intervalu možných kandidátů jsme oproti y snížili na polovinu. S využitím základních vlastností transformace RSA navíc víme, že zpráva y' odpovídá šifrovému $x'=x.2^{-e} \bmod N$, kde e je veřejný exponent RSA. Pokračujeme proto jednoduše tím, že celý postup rekurzivně opakujeme s nastavením $E \leftarrow E'$, $F \leftarrow F'$, $y \leftarrow y'$, $x \leftarrow x'$. Postupně tak po t opakováních uvedeného postupu, kde $t < \log_2 N+1$, dospějeme do stavu, kdy nám zbude interval obsahující jediné celé číslo. Tím bude hodnota $z=m.2^{-t} \bmod N$, ze které již snadno vypočteme hledaný otevřený text RSA $m=z.2^t \bmod N$.

Praktické důsledky

Připomeňme, že schéma RSA dnes najdeme ve většině současných aplikací, přičemž řada z nich pracuje v natolik automatickém režimu, že přístup útočníka k dotazům na příslušná zařízení je jen s trochou úsilí snadno zaručen (například servery SSL/TLS). Proto má smysl důkladně prověřovat všechny možné kanály, kterými může informace o individuálních bitech otevřeného textu unikat. Nejčastější maléry přitom vznikají během operace dekódování otevřeného textu RSA (viz ST 10/2003, [8]). Zdánlivě nepatrná informace, že odšifrovaná hodnota (ne)odpovídá požadovanému formátu, je pro kryptoanalytika velmi cenná. Například když u používaného formátu EME-PKCS1-v1_5 dostaneme informaci, že dekódování proběhlo v pořádku, víme, že řetězec m začínal zleva posloupností bytů 00 02…, čili příslušné orákulum (například server SSL, který vrací chybové hlášení v případě nekorektního formátu) nám zde dává k dispozici přímo 16 čistých bitů otevřeného textu! Uvedené vlastnosti vedly k řadě útoků na tento formát [1], [3] a jsou důvodem k přechodu na formát označovaný jako EME-OAEP. I u něho je však nutné na možný únik informace o m dávat dobrý pozor [5], [4].

Závěr

Představená vlastnost RSA je jednou z těch, které by každý bezpečnostní architekt měl mít při návrhu aplikací na zřeteli. Únik individuálních bitů může způsobit i zbytková informace v nedbale čištěné paměťové oblasti, auditních záznamech, ladicích výpisech, atp. K tomu všemu může snadno dojít, pokud se bude návrhář řídit heslem: „Vždyť jde jen o pár bitů…“ Právě jsme si ale ukázali, že ve skutečnosti jde v takovém případě „jen“ o bezpečnost celé aplikace.

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

LITERATURA

[1] Bleichenbacher, D.: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, in Proc. of CRYPTO '98, pp. 1-12, 1998

[2] Hastad, J. and Näslund, M.: The Security of Individual RSA Bits, in Proc. of FOCS '98, pp. 510-521, 1998

[3] Klíma, V., Pokorný, O., and Rosa, T.: Attacking RSA-based Sessions in SSL/TLS, in Proc. of CHES '03, Cologne, Germany, September 7-11, 2003

[4] Klíma, V., Rosa, T.: Further Results and Considerations on Side Channel Attacks on RSA, in Proc. of CHES '02, San Francisco Bay, CA - USA, pp. 245 - 260, Springer-Verlag, 2002

[5] Manger, J.: A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1, in Proc. of CRYPTO 2001, pp. 230-238, 2001

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

[7] Rosa,T.: Modern Cryptology – Standards Are Not Enough, doktorská disertační práce, 2001-2004, dostupné v [8]

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