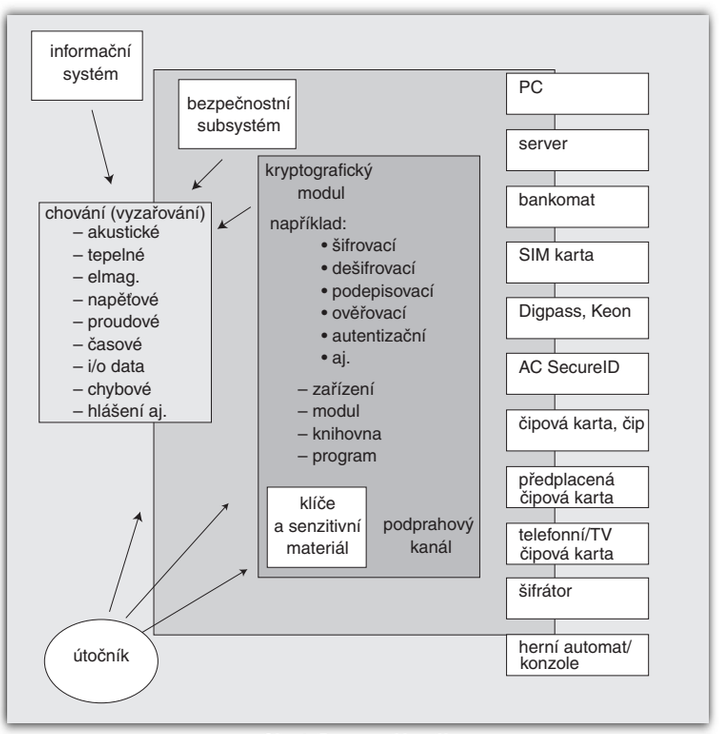
Vybrané aspekty moderní kryptoanalýzy

Kryptoanalýza je věda zabývající se luštěním matematických mechanizmů ochrany dat. Jako taková je nerozlučně spjata s kryptografií, která na základě potřeb architektů informačních systémů a aktuálních kryptoanalytických poznatků tyto mechanizmy navrhuje a inovuje. Sjednocením obou těchto oblastí vzniká interdisciplinární obor nazvaný kryptologie. Těžiště kryptologie se pochopitelně nachází v matematice, avšak je to právě kryptoanalýza, která nutí kryptology podnikat stále exotičtější výlety do jiných oblastí, zejména pak do teoretické informatiky a aplikované fyziky.

Úvod

Komplexní a interdisciplinární zkoumání praktických problémů kryptoanalýzy není jistě samoúčelné, neboť jedno z řešení přineslo před několika málo lety zcela nový pohled na útoky proti kryptografickým modulům. Jedná se o teorii postranních kanálů, s níž vznikla úplně nová kategorie útočných metod, které co do elegance a účinnosti prakticky nemají v historii konkurenci. Do jejich příchodu bývalo velmi neobvyklé, aby se i na těch nejprestižnějších konferencích objevovaly útoky vedoucí k totálnímu prolomení napadaného systému. Karikaturista by asi uvedl, že většinou šlo „jen“ o oslabení efektivní délky klíče z hodnoty 256 b na 255,25 b. S příchodem postranních kanálů se však situace rázem změnila a kryptoanalýza opět přicházela s totálními průniky. Navíc tento jev má, zdá se, stále rostoucí tendenci, což celou oblast z praktického hlediska silně exponuje. Riziko prolomení nedbale navrženého systému je enormní a doba, kdy kryptologové byli autory informačních systémů považováni za „dotěrný hmyz“, který se vyžívá v tvoření šroubovaných a veskrze nepraktických konstrukcí, je rázem pryč. V následujícím textu se pokusíme čtenáře s nastíněnou problematikou alespoň přehledově seznámit a ukázat, čeho všeho a jak se tato oblast dotýká.

Důležitou částí každého bezpečnostního systému jsou kryptografické moduly, které pracují s tajnými klíči a zajišťují elementární citlivé operace šifrování, autentizace, vytváření nebo ověřování elektronických podpisů apod. Tyto moduly také určitým zamýšleným a žádoucím způsobem komunikují s okolím prostřednictvím vstupně-výstupních kanálů, jak ukazuje *obr. 1*. Postranní kanály vznikají většinou nevědomky jako nežádoucí a nezamýšlené a definujeme je následovně. *Postranním kanálem (PK) nazýváme každý nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím [23].* Z fyzikálního hlediska mívají tyto kanály často podobu fyzikálních veličin, které je útočník schopen měřit a jejichž hodnoty jsou určitým způsobem závislé na průběhu výpočtů uvnitř napadeného modulu. Z jistého hlediska z tohoto hrubého popisu poněkud vybočují více abstraktní druhy postranních kanálů, jako jsou například kanály chybové. V těchto případech je citlivá informace vynášena díky chybě v napadeném zařízení (viz dále) přímo po běžných datových výstupech. Tato chyba může být neúmyslná nebo způsobena záměrným aktivním působením na modul. Poznamenejme, že postranní kanály by mohly vznikat v různých částech informačního systému, ale jejich definici jsme zúžili na kryptografické moduly právě proto, že bývají nejvíce chráněnou a nejcitlivější součástí systémů. Proto jsou také vyhledávaným místem útoků.



Obr. 1 Postranní kanály

Příklad z oblasti symetrických šifer – modus CBC

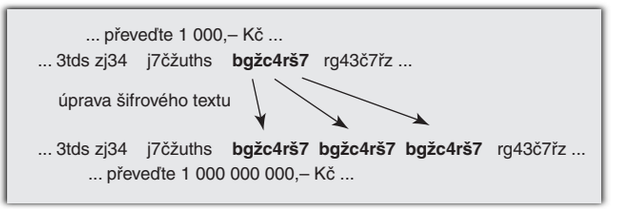
Vezměme si standard AES s 256bitovým klíčem, tedy šifru, která je pokládána za dostatečně bezpečnou. Víme ovšem, že pokud je použita k šifrování dat tak, jak je zobrazeno na *obr. 2*, je to většinou špatně. Pokud se totiž v šifrovém textu objeví dva bloky stejné, útočník dostává informaci o tom, že odpovídající bloky otevřeného textu jsou stejné. A to není dobré. Navíc někdy může být útočník schopen ovlivňovat šifrový text, a co by se mohlo stát, když zopakuje pár bloků šifrového textu na správném místě, je vidět na *obr. 2*. Poučení: samotná šifra AES je bezpečná, ale způsob jejího použití (tzv. operační modus), tj. konkrétní realizace šifrování, je špatný.

Aby se stejná zpráva nebo i jednotlivé bloky otevřeného textu šifrovaly vždy jinak, byl zaveden tzv. operační modus CBC. V něm se každý nový blok otevřeného textu ještě před zašifrováním modifikuje předchozím šifrovým textem, čímž jsou eventuelní stejné bloky otevřeného textu nezávisle modifikovány tak, že jejich šifrové bloky jsou s vysokou pravděpodobností rozdílné.

Z matematického hlediska se problém se stejnými bloky v ECB jeví přechodem na modus CBC jako vyřešený, neboť formálně již neexistují žádné další námitky. V květnu 2002 byl však v tomto operačním modu veřejně popsán záludný a nebezpečný postranní kanál, který při původním náhledu nebyl vůbec patrný. Přesněji řečeno útok byl objeven u některých konkrétních realizacích modu CBC. Tato poznámka je důležitá, protože obecně platí, že postranní kanály nevisí ve vzduchu, ale jsou vždy vázány na zcela konkrétní realizace norem, šifer apod.

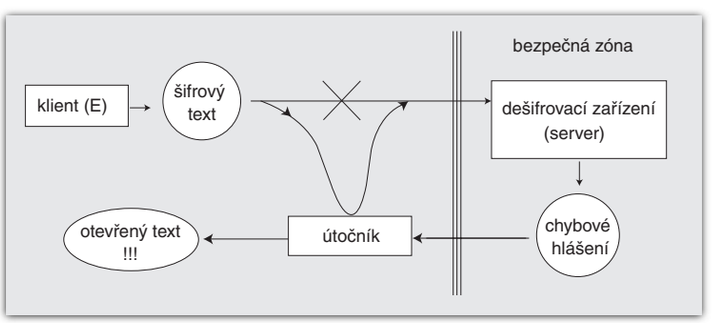
Ve skutečnosti jsou postranní kanály založeny na těch nejnicotnějších detailech. Konkrétně si to ukážeme právě na příkladu modu CBC, aniž bychom zabíhali do detailů. Protože bloková šifra šifruje bloky pevné délky, musí se zprávy o délce nerovné násobku délky bloku něčím doplnit. Přijímající strana pak po dešifrování otevřeného textu musí rozhodnout, kolik bajtů bylo při šifrování uměle přidáno

a tento doplněk odstranit. Často se používá doplněk podle standardu PKCS#5, kdy všechny přidané bajty mají hodnotu, která se rovná právě počtu přidaných bajtů (při zarovnané délce zprávy se přidává celý blok navíc). Například se doplní 2 B s hodnotou 2 nebo 3 B s hodnotou 3 atd. Při odšifrování se přečte poslední bajt a z něho se určí, kolik bajtů bylo přidáno. Všechny tyto bajty musí mít stejnou hodnotu. Pokud ne, pak někde určitě nastala chyba na přenosovém kanálu. Přijímající strana potom většinou nějakým chybovým hlášením informuje odesilatele, že nastala chyba. A právě toto, na první pohled korektní a neškodné, chybové hlášení vytváří postranní kanál, jehož důsledné využití vede až k získání otevřeného textu celé zprávy. Určitě je to dosti šokující zjištění, protože útočník nemusí použít žádné superpočítače, ale pouze využívá postranního kanálu, jak je zobrazeno na *obr. 3*. Tento útok by měl být dostatečně motivující pro revize všech systémů používajících tento modus (je to nejpoužívanější modus blokových šifer).



Obr. 2 Útok na operační modus ECB blokové šifry

Postup útoku je jednoduchý. Útočník nejprve zachytí zašifrovanou zprávu, o níž má zájem. Poté dešifrovacímu zařízení (například nějaký server, viz *obr. 3*) posílá své zprávy (s využitím fragmentů původní zprávy) a vyhodnocuje chybová hlášení od serveru. Na získání otevřeného textu původní zprávy délky N bajtů je potřeba v průměru přibližně pouze $128 \times N$ dotazů dešifrovacímu zařízení. Nic víc. Výsledkem je odšifrovaná původní zpráva. Podrobnosti lze nalézt v práci [27] (popis v češtině viz [11]). Proti využití tohoto postranního kanálu je možné navrhnout řadu opatření. Jsou to například technická opatření, spočívající v doporučení jak implementovat dešifrovací proces. Ta ovšem mohou být programátory nebo tvůrci systému z nedbalosti nebo neznalosti opomenuta. Bezpečnější jsou proto kryptologická opatření, která nelze opomenout, protože by došlo ke ztrátě funkčnosti (komunikující strany by se vůbec nedomluvily). Taková protiopatření jsme pro modus CBC navrhli například v [12] (v češtině viz [11]).



Obr. 3 Postranní kanál vznikající na základě chybového hlášení dešifrovacího modulu

Podprahový kanál

Postranní kanál by neměl být obecně zaměňován s tzv. podprahovým kanálem (angl. subliminal). Je to kanál, který je v kryptografickém modulu záměrně vytvořen útočníkem, aby vynášel citlivé informace. Klasický je příklad vynášení hodnot klíčů v pseudonáhodně volených inicializačních vektorech, doplňcích pro asymetrické šifrování a digitální podpis apod. Jedná se o informace, které jsou pod úrovní rozlišovací schopnosti daného modulu, protokolu, typu spojení atp. Téma podprahových kanálů má samo o sobě poměrně blízko ke steganografii studované z pohledu informačních kanálů (viz [9]). Pokud je takový kanál implementován do nějakého kryptografického zařízení bez vědomí jeho uživatele, potom se z něho stává zvláštní druh postranního kanálu, který označujeme jako kleptografický (pojem kleptografie viz [28]). Problematika těchto kanálů je zatím poměrně nová, avšak v souvislosti s oblastí ochrany základního soukromí občanů industriálně vyspělých států se jistě brzy stane velmi exponovanou (viz například připravovaný systém Palladium [24]). V tomto příspěvku se však budeme dále věnovat pouze těm postranním kanálům, které vznikají nevědomky a to jak na straně výrobce, tak na straně uživatele.

Kryptografický modul

Kryptografickým modulem může být software, hardwarový modul, čip, linkový šifrátor, samostatný blok (černá skříňka), předplacená telefonní nebo televizní karta, bankomat nebo jeho část, server, SIM karta mobilního telefonu, autentizační token (například pro internet banking) apod. Moduly žijí a interagují s okolím nejrůznějšími způsoby, čímž dávají určitým způsobem najevo informace o svých činnostech i vnitřních stavech, aniž by to nutně jejich tvůrci zamýšleli a chtěli. Jedná se například o elektromagnetické, akustické, či dokonce tepelné vyzařování. Moduly se projevují rovněž také spotřebou proudu, času, paměti a chybovými či jinými hlášeními. Na každou jejich aktivitu může být také namodulována nějaká senzitivní informace (většinou je tento jev v povědomí pouze ve spojení s tzv. parazitním elektromagnetickým vyzařováním). Kromě pasivního sledování činnosti modulu existuje i celá škála aktivních invazivních i neinvazivních zásahů útočníka, které příslušný postranní kanál vytvářejí nebo aktivují. Jedná se například o světelné, tepelné, ultrafialové, čili obecně elektromagnetické ozařování nebo „bombardování“ zařízení jiným způsobem, který vyvolá integritní poruchy klíčového materiálu, softwaru i hardwaru. Vzhledem k potenciální existenci velkého množství postranních kanálů zatím ani známá norma FIPS PUB 140-2 (vydáno americkou autoritou NIST), zabývající se bezpečností kryptografických modulů, ochranu proti nim neřeší.

Princip časového postranního kanálu

Časový postranní kanál využívá jednoduchý princip, kdy určité operace závislé na tajném klíči trvají krátce nebo déle v závislosti na konkrétních hodnotách jednotlivých bitů klíče. Různé útoky, založené na tomto principu využívají různá místa příslušného kryptografického modulu (programu) a různé sofistikované hypotézy a nástroje na vyhodnocování získaných časových údajů. Nyní uvedeme Kocherovu ideu [17] (popis v češtině viz [22], [23]) časového útoku na privátní klíč RSA v operaci odšifrování nebo podpisu: $y=(m^d) \bmod n$. Výpočet modulární mocniny se provádí známým algoritmem square and multiply, kdy se postupně zpracovávají jednotlivé bity privátního klíče – exponentu d. Počet platných bitů čísla d označme b, tj. $d=d_0 d_1 \ldots d_{b-1}$ a nejvyšší bit d_0 je jedničkový. Algoritmus vidíme na *obr. 4*.

Povšimněme si nyní, že doba každého průchodu smyčkou závisí na tom, zda daný bit klíče je nula nebo jedna. Je-li nula, výpočet je rychlejší. Je-li jedna, výpočet trvá déle. Dále je dobré mít na paměti, že vstupní hodnotu m útočník zná, a pokud zná i přesnou realizaci algoritmu, může si každý krok uvedené smyčky simulovat na svém zařízení a zjišťovat tak přesné doby průchodu smyčkou. Na *obr. 5* vidíme, jak se liší doby průchodu smyčkou pro dvacetibitový klíč. Z jednotlivých dob můžeme okamžitě odvozovat bity klíče d. V praxi to tak jednoduché ovšem není, neboť neznáme délky jednotlivých časových intervalů zvlášť, ale víme pouze celkový čas trvání dané makroskopické operace. Díky více či méně propracovaným statistickým metodám (na jejich kvalitě přímo a silně závisí možnost a schůdnost případného útoku)

jsme však schopni i takovou informaci účelně využít.

V současné době lze tyto postupy do značné míry automatizovat a jejich účinnost stoupla zejména se zavedením metod založených na metodách korelační signálové analýzy (kryptologové však s oblibou používají notaci založenou na práci s různými orákuly, což jsou zařízeni s definovanými vlastnostmi.). Například v práci [7] (popis v češtině viz [22], [23]) je použito dvou orákul (což odráží testování dvou hypotéz současně). Automatická detekce chyby při odhadu některého bitu klíče je patrná z *obr. 6*, kde v okolí 149. bitu klíče došlo k jeho chybnému odhadu. Uvedený časový útok se týkal modulární mocniny, což se týká zejména algoritmů RSA, Diffieho-Hellmanova protokolu a DSA, ale podobné principy lze nalézt i u symetrických šifer, kde existují klíčově závislé operace, čili vzniká podobný prostor pro časové útoky. Jedná se zejména o algoritmy AES (operace MixColumn), DES (příprava klíče), IDEA (operace modulárního násobení je časově závislá na vstupech), RC5 (časově závislé bitové rotace) apod.

Napěťově-proudové postranní kanály

Omezíme-li se na čistě fyzikální druhy postranních kanálů, pak v současné době mezi nejexponovanější případy bezesporu patří právě kanály založené na sledování spotřeby proudu napadeného modulu. Pokud si však odmyslíme rozdílný způsob měření zpracovávaných dat, tak zjistíme, že mezi způsobem využití časových a napěťově-proudových kanálů je z obecného hlediska řada společných rysů. Toto pozorování bylo poprvé formalizováno v práci [20] a dále rozvinuto v [22], [23], kde je zavedena obecná analýza založená na orákulích. Základní výhodou, kterou útočník získává při sledování spotřeby proudu namísto doby trvání celého výpočtu je, že na určitý úsek obdrženého signálu je modulována informace o chování poměrně malého fragmentu kódu, čímž se jeho analýza stává efektivnější. V současné době se také začínají objevovat první náznaky souběžného spojení časové a napěťově-proudové analýzy. Poněkud překvapivě se také až nyní rozvíjí studium elektromagnetických postranních kanálů, které, jak se zdá, bude dosahovat ještě lepších výsledků [2].

Postranní kanály u asymetrických šifer

Nyní si uvedeme několik exemplárních případů efektivního využití útoků založených na postranních kanálech z oblasti asymetrických šifer, konkrétně algoritmu RSA podle standardu PKCS#1. Proti bezpečnosti samotného algoritmu RSA není zatím výhrad, ale postranní kanály vznikají při jeho implementaci, ostatně jako i u jiných kvalitních kryptografických nástrojů. Přestože následky následujících útoků postranními kanály budou dosti zničující, zdůrazňujeme ještě jednou, že na vině není pouze algoritmus sám (i když určité vlastnosti RSA útoky tohoto typu bezesporu přímo přitahují), ale především způsob jeho realizace, případně pak způsob jeho použití v celém kryptografickém schématu (metody doplňování dat apod.).

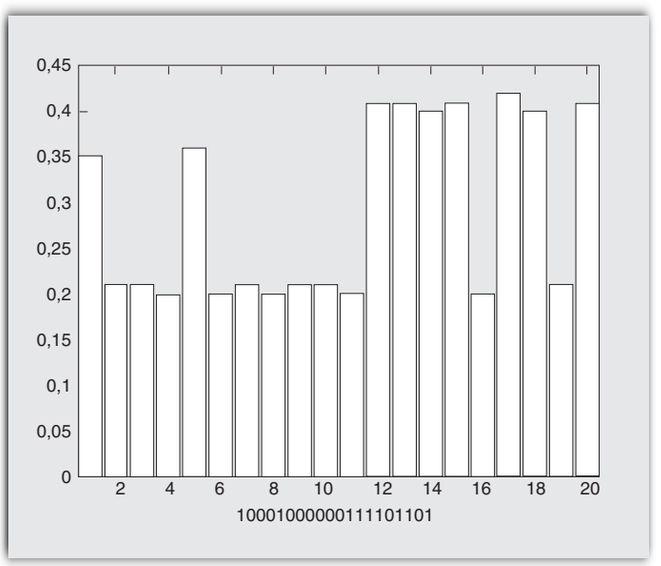
```
výpočet y=(m^d mod n) algoritmem square and multiply
d=d_0 d_1 ... d_{b-1}(nejvyšší bit d_0 =1)
R=m
for i=1 to b–1
{
    R=R^2 mod n
    if (d_i==1) then R=R*m mod n  (*)
}
return R

pozn: časová náročnost operace (*) vyzařuje informaci o bitu klíče d_i
```

Obr. 4 Časový postranní kanál u algoritmu square and multiply

Bleichenbacherův útok

Zopakujme stručně, že základními parametry algoritmu RSA jsou jeho tzv. modul *n*, privátní exponent *d* a veřejný exponent *e*. Šifrování probíhá tak, že vstupní zpráva *M* se musí zformátovat (použití RSA bez tohoto kroku nelze považovat za bezpečné – viz [4]) a doplnit tak, aby jako číslo byla menší než modul *n* (jinak by nešla jednoznačně odšifrovat). Uveďme si nyní velmi krátce konkrétní postup formátování a doplňování zprávy podle PKCS#1 v1.5 pro 1024bitový modul RSA. To je nejčastější případ v protokolu *SSL*/*TLS* [21], používaném často i v systémech internetového bankovnictví. Vstupní zprávu označme *D* a předpokládejme, že má 48 B (v *SSL*/*TLS* je to náhodný základ pro odvození klíčů pro symetrické šifrování navazovaného spojení). Doplnění bloku *D* do plných 128 B bloku *EB* je definováno jako *EB*=00 || 02 || *PS* || 00 || *D*, kde || označuje zřetězení a *PS* obsahuje 77 náhodných nenulových bajtů, a pak následují bajty 02 a 00. Poslední nulový bajt zajistí platnost *EB*<*n*. Bajt s hodnotou 02 indikuje, že se jedná o blok typu 02, určený pro šifrování klíčů. Bleichenbacher v roce 1998 ukázal, že zde existuje postranní kanál, který umožňuje zjištění původní otevřené zprávy. Postačí, pokud se příslušný dešifrovací stroj (server) chová přirozeně a na nesprávný šifrový text (po odšifrování neodpovídá uvedenému formátu) zareaguje chybovou hláškou, kterou útočník využije. V závislosti na délce modulu, délce bloku *D* a dodatečných integritních kontrolách jsou zde potřeba řádově milióny dotazů na server (podrobnosti viz [3], 10]).



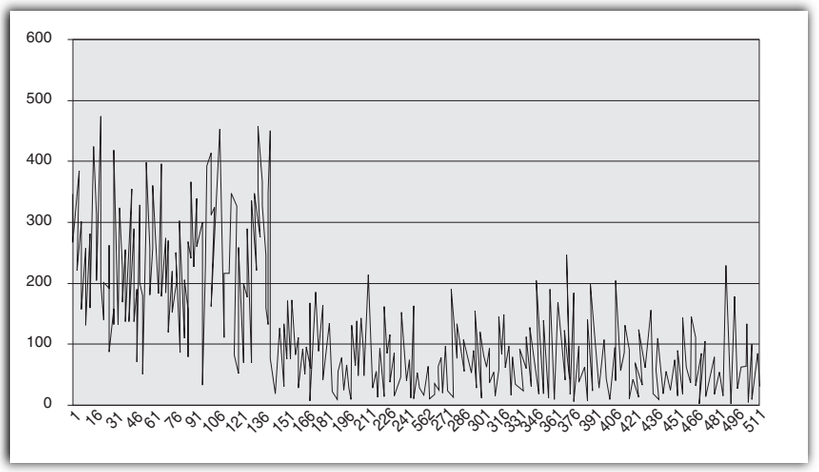
Obr. 5 Čas průchodu smyčkou z obr. 4 pro 1.–20. bit klíče *d* [5]

Mangerův útok

Příčinou předchozího útoku byla skutečnost, že zformátovaná zpráva používala pro kontrolu integrity takový druh kódování, který na základě výsledku integritní kontroly umožňoval útočníkovi zjistit poměrně vydatnou informaci o konkrétních částech otevřeného textu. Z teorie je známo, že RSA je na takovéto vynášení částečné informace velmi citlivé (viz [8]). Proto bylo navrženo mnohem dokonalejší formátování – tzv. metoda OAEP (viz PKCS#1 v2.1 [19]), které celou zprávu znáhodňuje tak, že informaci o výsledku integritní kontroly nelze schůdně převést na parciální informaci o hodnotě vzniklé bezprostředně po operaci odšifrování.

Jaksi stranou pozornosti však zůstalo, že i toto schéma stále ponechávalo levostrannou nulu. Tím zde vlastně zůstala v podstatě primární integritní kontrola, která zjevně parciální informaci o otevřeném textu RSA vynáší. Manger v roce 2001 ukázal, že na tomto principu je možné vystavět další útok s využitím postranního kanálu podávajícím informaci o výsledku této primární kontroly. Navíc byl mnohem realističtější, neboť vyžadoval řádově jen 1024 dotazů na dešifrovací server. K úspěšnosti útoku

postačovalo opět to, aby implementátoři ponechali odpovídající (zcela běžné) chybové hlášení. Podrobnější popis útoku je uveden v [18] a [13]. Pokud by bylo toto hlášení nerozlišitelně spojeno s oznámením o výsledku sekundární integritní kontroly (vlastní metoda OAEP), pak by tento útok nebyl možný. Slovo nerozlišitelně je však třeba chápat velmi důsledně. Pokud by se například chybové hlášení vydávalo sice vždy stejné, ale s jinou prodlevou (pokud by nebyla nalezena levostranná nula, tak by se kontrola metodou OAEP už neprováděla), útočník by stejně z doby trvání operace zjistil, že chyba nastala už při primární kontrole. Je tedy potřeba zabránit i všem ostatním postranním kanálům, které by mohly umožnit tato chybová hlášení odlišit (například záznamy do logovacích souborů).



Obr. 6 Chybu v odhadu *k*-tého bitu klíče lze detekovat automaticky [7], zde *k*=149

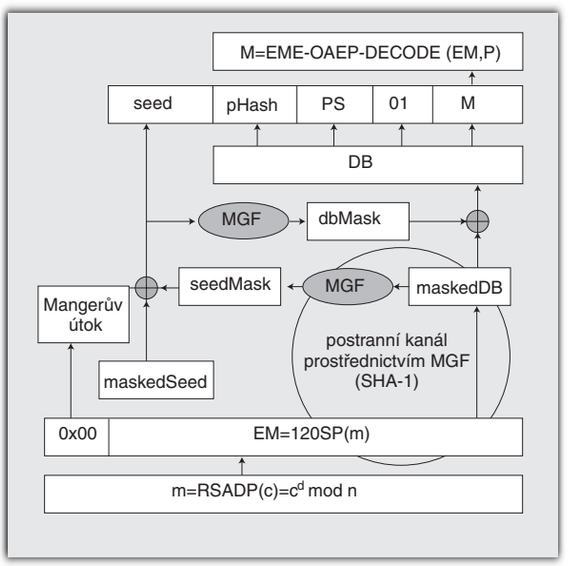
V nové práci [14] jsme však ukázali, že ani vyřešení problémů s primární integritní kontrolou nemusí ještě stačit, a pokud je umožněn napěťově-proudový postranní kanál, je za určitých celkem reálných předpokladů možné útočit i na správně implementovanou metodu OAEP, a to v době dekódování obdržené zprávy – viz *obr. 7*.

Útok na RSA-KEM

Teoretici pochopili, že jakékoliv doplňování indukující integritní kontroly vnáší do implementací postranní kanály, a proto byla navržena nová definice formátování, která dala vzniknout schématu RSA-KEM (Key Encapsulation Method – viz [25]), které je zamýšleno jako součást normy ISO pro RSA. Podstatou nového formátu je, že vstupní otevřený text (r) se generuje zcela náhodně v délce modulu a menší než modul. Tento náhodný otevřený text pak bez jakéhokoliv dalšího dekódování rovnou slouží jako základ symetrického klíče (derivuje se z něj pomocí jednosměrné funkce $KDF(r)$), kterým se šifruje vlastní zpráva. Po odšifrování otevřeného textu (klíče) algoritmem RSA tedy není co kontrolovat, protože vzniklá data jsou náhodná a neobsahují žádné integritní kontroly ani jakékoliv jiné formátování. Tato definice měla postranním kanálům definitivně zabránit. V [14] jsme však ukázali, že i v RSA-KEM vzniká velmi vydatný chybový postranní kanál, jehož využití je překvapivě ještě nebezpečnější než u Mangerova útoku. Tehdy útočník získal otevřený text, nyní získá i privátní klíč. Bylo tak názorně ukázáno, že ani RSA-KEM není zcela univerzálním východiskem proti útokům postranními kanály a že i u něj velmi záleží na implementaci.

Chybové postranní kanály

Oblast chybových útoků se ukazuje být velmi nebezpečnou, neboť to byly právě chybové postranní kanály, které byly efektivně využity u RSA-KEM. Zajímavé také je, že dříve se vytvářely tzv. systémy odolné proti chybám (fault-tolerant systems) proto, aby se zabránilo chybě při výpočtu. Osud případných chybných výsledků nikoho nezajímal – pozornost se soustředila na správnost výpočtu a korektní data. Přitom kryptologové ukázali, že právě to, co bylo dříve považováno za bezcenné smetí, tj. výsledky vzniklé při chybě nebo eventuálním výpadku části systému, jsou zdrojem cenných informací o senzitivních datech uvnitř modulu. Chyby lze vyvolat různými invazivními i neinvazivními metodami. Příkladem takového útoku je zanesení chyby do klíčového materiálu chráněného šifrováním založeném na přístupovém hesle. Tímto způsobem bylo možné postranním kanálem získat privátní podpisový klíč systémů RSA i DSA, jak bylo popsáno v [15] (český výtah viz [16]). Systémy odolné proti chybám tak nabývají v tomto světle nového významu, neboť kromě přirozených chyb mohou zabránit i jinému pochybení při práci s citlivým kryptografickým materiálem.



Obr. 7 Formátování podle PKCS#1, ver. 2.1 a útoky na něj při odšifrování a dekódování

Co může být cílem útoků postranními kanály

Uvedli jsme si některé příklady, které však zdaleka nevyčerpávají celé spektrum útoků na HW nebo SW moduly. Za nejpravděpodobnější cíle těchto útoků lze považovat ty moduly, které jsou velmi rozšířené (produkty masové spotřeby), což přináší útočníkovi viditelný profit. Z tohoto pohledu se bude jednat zejména o nástroje internetového bankovnictví, mobilních telefonů, systémů pro přístup do počítačových sítí nebo předplacených služeb. Mnoho z těchto prostředků je založeno na čipových kartách nebo využívá čipy v jiné formě (například SIM karty, telefonní karty, placená televize, herní konzole apod.). Díky své technologické podstatě jsou to právě tyto autonomní čipové moduly, které jsou nejvíce zranitelné popisovanými útoky. Na rozdíl od velkých počítačů jsou totiž jejich fyzikální projevy mnohem snáze analyzovatelné a měřitelné. Rovněž tak cílené vnášení chyb do takových zařízení bývá o poznání jednodušší (viz například [26]). Samozřejmě, že výrobci těchto modulů se těmto útokům snaží bránit tím, že implementují nejrůznější technologické a kryptografické ochranné mechanizmy. Bohužel však žádná z dosud představených ochran nemůže být považována za definitivní, a tak na tomto poli dochází k neustálému iterativnímu zlepšování. Ne každý výrobce se však snaží držet toto rychlé tempo ze všech sil (i když všichni samozřejmě tvrdí, že ano), a tak celá situace začíná zajímat i bezprostřední odběratele těchto modulů. Ne náhodou se tak na předních kryptologických konferencích čím dál častěji objevují na toto téma práce pocházející nejen od pracovníků samotných výrobců, ale i od předních mobilních operátorů a bank.

Závěr

Příspěvek stručně seznamuje s pojmem postranního kanálu, který byl ještě před několi-

ka lety zcela neznámý. Poukazuje na různé druhy postranních kanálů a možnosti jejich zneužití v různých systémech. Ukazuje se, že tato nová oblast, která se rozvíjí teprve jednotky let, musí být vzata velmi vážně v úvahu při návrzích informačních, komunikačních a bezpečnostních systémů a při jejich revizi.

Až donedávna se zájem kryptologů soustředil zejména na návrh a analýzu základních kryptografických schémat a jejich funkčně správnou realizaci. Ukázalo se, že toto nestačí, a že to byla práce na abstraktním modelu, odtrženém od reálného života, kde nakonec záleží na každém chybovém hlášení, časové prodlevě nebo jakémkoliv jiném fyzikálním projevu modulu. Objev postranních kanálů ukázal, že je nutné sledovat bezpečnostní moduly v celém spektru jejich interakce s okolím, vstupně-výstupní kanály, napěťově-proudové chování, elektromagnetické vyzařování atd., a to jak za stavu normálního, tak předvídat jejich chování za stavu záměrně vynucené nebo vnesené chyby.

V češtině lze za základní práci v oblasti postranních kanálů považovat [23], kde se kromě přehledu v té době známých útoků definuje postranní kanál, zavádí kategorizace útoků postranními kanály a formalizují společné rysy časových a napěťově-proudových postranních kanálů. Populární články na toto téma pak tvoří seriál článků [22]. Výzkum v oblasti postranních kanálů byl motivován prací na tzv. modulech CSP (Cryptographic Service Provider), poskytujících kryptografické služby na platformě MS Windows, v rámci projektů pro Národní bezpečnostní úřad. V těchto projektech [6] byla také řada opatření proti postranním kanálům aplikována. Podrobně byla uvedená problematika diskutována i v samostatném referátu na konferenci BIN 2002.

RNDr. Vlastimil Klíma, Ing. Tomáš Rosa,
vlastimil.klima@i.cz, tomas.rosa@i.cz

LITERATURA

[1] Archiv článků: http://www.decros.cz/bezpecnost/kryptografie.html, řada ostatních citací je tamtéž dostupná v elektronické podobě

[2] Agrawal, D., Archambeault, B., Rao, J. , R., Rohatki, P.: The EM-side channel(s), in Proc of CHES 2002, pp. 13 -29, 2002

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

[4] Boneh, D., Joux, A. and Nguyen, P.-Q.: Why Textbook ElGamal and RSA Encryption Are Insecure, in Proc. of ASIACRYPT 2000, pp. 30-43, 2002

[5] Canvel, B. and Dobson, C., T., J.: Public Key Cryptosystem Timing Analysis: Evaluating Obscuring Techniques, August 27, 2000, Rump session, Crypto 2000

[6] Cryptographic Service Provider CSP-I /CSP-II MicroCzech, http://www.i.cz/onas/csp.html

[7] Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P. and Quisquater, J.-J. and Willems, J.-L.: A Practical Implementation of the Timing Attack, Technical Report CG-1998/1, 1998

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

[9] Hopper, N., J., Langford, J., Luis von Ahn: Provably Secure Steganography, in Proc of CRYPTO '02, pp. 77–92

[10] Klíma, V.: Bezpečné použití RSA, Chip, listopad 2000, str. 52–56

[11] Klíma, V.: Překvapivý útok a česká obrana, Chip, červen 2002, str. 156–157

[12] Klíma, V., Rosa, T.: Strengthened Encryption in the CBC Mode, Cryptology ePrint Archive: Report 2002/061, http://eprint.iacr.org/2002/061.pdf

[13] Klíma,V., Rosa, T.: RSA v novém světle (1), Chip, listopad 2001, str. 172–175

[14] Klíma, V. a Rosa, T.: Further Results and Considerations on Side Channel Attacks on RSA, in Proc. of CHES '2002, pp. 245–260, 2002, preliminary version on Cryptology ePrint Archive: Report 2002/071, http://eprint.iacr.org/2002/071.pdf

[15] Klíma, V., Rosa, T.: Attack on Private Signature Keys of the OpenPGP format, PGP (TM) Programs and Other Applications Compatible with OpenPGP, Cryptology ePrint Archive: Report 2002/076, http://eprint.iacr.org/2002/076.pdf

[16] Klíma, V., Rosa, T.: Útok na privátní podepisovací klíče PGP, Chip 5/2001, s. 164–167, 2001

[17] Kocher, P.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, in Proc. of CRYPTO '96, pp. 104–113, 1996

[18] 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

[19] PKCS#1 v2.1: RSA Cryptography Standard, RSA Laboratories, DRAFT2 – January 5, 2001, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/

[20] Rosa, T.: Future Cryptography: Standards are not Enoungh, in Proc. of Security and Protection of Information 2001, Military Academy in Brno, pp. 237–245, 2001

[21] Rescorla, E.: SSL and TLS, Addison-Wesley, 2001

[22] Rosa, T: Kryptografie v klidu a bezpečí (1 až 6), Chip, únor až září 2001

[23] Rosa T.: Kryptoanalýza s využitím postranních kanálů, Vojenská kryptografie IV, Brno, 30., 31. 10. 2001, str. 113–156

[24] Schneier, B.: Palladium and the TCPA, Crypto-Gram Newsletter, August 15, 2002.

[25] Shoup, V.: A Proposal for an ISO Standard for Public Key Encryption (version 2.0), September 17, 2001

[26] Skorobogatoav, S. and Anderson, R.: Optical Fault Induction Attacks, in Proc. of CHES 2002, pp. 2–12, 2002

[27] Vaudenay, S.: Security Flaws Induced by CBC Padding – Applications to SSL, IPSEC, WTLS, Eurocrypt 2002, pp. 534–545

[28] Young, A., Yung, M.: Kleptography: Using Cryptography Against Cryptography, in Proc. of EUROCRYPT '97, pp. 62–74, 1997

Mezinárodní konference Applied Electronics

Osmý ročník mezinárodní konference Applied Electronics 2003 proběhne letos 10. a 11. září na Západočeské univerzitě v Plzni. Příspěvky autorů jsou přijímány do do konce dubna, prostřednictvím www.fel.zcu.cz/konfae.

Cílem pořadatelů je organizovat setkání odborníků z oblasti aplikované elektroniky při udržení minimálního vložného (pouhých 1000,– Kč) a při zachování vysoké odborné úrovně, což vyhoví zejména autorům z našich zchudlých akademických institucí. To se týká hlavně mladých autorů a doktorandů, kteří zde mohou získat praxi ve vystupování na mezinárodních akcích při prezentaci svých prací v angličtině. Tato šance je skutečně také využívána. Ke snížení nákladů přispívá Internet, pomoc sponzorů a též podpora ZČU, která poskytuje posluchárny a jejich vybavení zdarma. Všechny příspěvky v anglické verzi jsou recenzovány mezinárodním programovým výborem a jsou uvedeny ve sborníku. Konferenci technicky podporuje i IEEE. S ohledem na nízké vložné neprovází setkání žádné společenské akce a bankety. Programový výbor upřednostňuje kvalitní referáty, zejména mladých autorů. Doporučená témata pro letošní jednání:

- Electronics in Measurement,
- Electronics Manufacturing Technology,
- Electronics in Industry and Transport (HW & SW),
- Teaching of Electronics,
- Electronics in Telecommunication,
- Design of Electronic Systems – Methods and Tools,
- Signal Processing,
- Electronics in Biomedical Engineering.

Prof. Ing. Jiří Pinker, CSc, ZČU-FEL