Bankomaty, platební karty a náhoda

Když jsme s kolegou Dr. Rosou zahajovali tento seriál ve ST před šesti lety, začínali jsme s tématem postranních kanálů a mysleli jsme si, že tímto tématem poptávku ST po kryptologii uspokojíme. Dnes čtete již 73. pokračování tohoto seriálu a je s podivem, že stále je nějaké „žhavé“ téma. Navíc poptávka neklesá, naopak roste počet kryptografických modulů a aplikací a stále je akutní nedostatek kryptograficky vzdělaných inženýrů, i když jejich počet se zvyšuje. V tomto čísle se k tématu postranních kanálů vracíme, neboť se objevila řada jejich zajímavých a technicky jednoduchých příkladů.

Postranní kanály

Postranní kanál jsme v [1] definovali jako jakýkoliv nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím. Kryptografickým modulem může být chytrý elektroměr, čipová karta, bankomat nebo platební terminál, procesor PC, zkrátka cokoliv, co obsahuje kryptografické klíče, vykonává kryptografické operace apod. Projevem postranního kanálu jsou většinou fyzikální veličiny, které je útočník schopen měřit nebo ovlivňovat. Důležité je, že hodnoty veličin, které útočník měří, určitým způsobem odrážejí průběh výpočtů uvnitř zkoumaného modulu. Odtud plyne využití postranních kanálů. Útočník se snaží z naměřených hodnot zpětně usuzovat na utajené hodnoty uložené v modulu, které zasáhly do výpočtů. Určitý fyzikální odraz těchto výpočtů pak útočník naměří a koneckonců tak zjistí věci, které by se žádným obvyklým způsobem nemohly z modulu dostat ven. Toto je velice nebezpečný způsob útoku a široká definice, která ale odráží skutečně velice široké pole postranních kanálů, jejich forem a možností útočníků, jak nakonec uvidíme dále. Pro ilustraci si ukážeme některé příklady běžných i exotičtějších postranních kanálů, např. na bankomatu a platebních kartách.

Akustický postranní kanál

Jedná se o jeden z nejstarších postranních kanálů ještě z doby, kdy se tak nenazývaly, neboť cílem nebyl kryptografický modul, nýbrž mechanický psací stroj. Traduje se příhoda, kdy na nejmenovaném velvyslanectví bylo nutné vyvrtat dírku v okenní tabuli, aby se mohl akusticky snímat klapot mechanické klávesnice psacího stroje. A potom ze zvuku rekonstruovat to, co slečna sekretářka píše. Proč se psalo na mechanických strojích v době, kdy byly už k dispozici první stolní počítače nebo elektromechanické psací stroje IBM? Tajné služby věděly, že elektromechanické stroje vyzařují, a věděly, že informaci je možné získat vyhodnocováním elektromagnetického postranního kanálu. Překvapivé je, že stejným způsobem jako dříve mechanické psací stroje vyzařují akusticky i dnešní (drátové i bezdrátové) klávesnice stolních počítačů. Jen se musí nasadit trošku jemnější technika vyhodnocování, ale princip zůstává stejný. Stručně řečeno, i dnes každá klávesa jinak skřípe. U bankomatu se zdálo nemožné, že by použitá tlačítka mohla akusticky skřípat. A už už se zdálo, že to někdo provedl, ale bylo to jen nepochopení mnoha zpravodajů. Psalo se tehdy, že útočník použil přehrávač MP3 k záznamu zvuků jdoucích z bankomatu. Ve skutečnosti prostě jen zaznamenával komunikaci bankomatu s centrálou poté, co mezi telefonní přípojku a zástrčku vložil svoje záznamové zařízení využívající onen přehrávač MP3. Současná technika snímání akustického signálu pomocí laseru byla prezentována např. ve [4].

Mechanický postranní kanál

Úsměvný příklad mechanických postranních kanálů často vidíme na domovních zámcích, kdy číselná kombinace je přímo vidět z velmi ošoupaných tlačítek. Podobně i při vkládádní kódu PIN na klávesnici bankomatu dochází k (nežádoucí) výměně informací mezi rukou a klávesnicí. Z ruky se na tlačítka přenášejí různé sloučeniny, zejména kyseliny, z klávesnice se na ruku může zase předávat jiná hmota, např. zvláštní sprej, kterým útočník klávesnici jemně popráší. Je jen otázkou času, kdy se sprejové typy útoků objeví, neboť je nasnadě, že PIN takto získávat lze. Stačí si uvědomit, že pokud někdo stiskne klávesu, nanese na ni „svoji kyselinu“ a naopak si na prstu odnese sprej. Když zmáčkne tímto prstem druhou klávesu, nanese již sprej na sprej, čili dochází k jiné chemické reakci než v prvním případě, atd. Prohlédnutím klávesnice ve zvláštním spektru bude možné určit nejen to, které klávesy byly stisknuty, ale i v jakém pořadí, neboť reakce různého množství kyseliny se sprejem vytvoří i časovou značku. Výzkumníci mohou jistě kombinovat jiné sloučeniny nanesené na různé klávesy k odlišení chemických reakcí apod.

Proudový postranní kanál

V červenci t. r. na konferenci Black Hat byl ukázán následující, již starý dobrý známý

trik, jen v reálných podmínkách a na příkladu klávesnice PS/2. Útok funguje do vzdálenosti 10 až 15 m, a to i v silně „zarušeném“ prostředí, např. v úřadě nebo v hotelovém prostředí. Princip útoku spočívá v tom, že informace, která klávesa byla stisknuta, lze získávat z elektrického vedení, z kterého je počítač napájen. Klávesnice PS/2 mají většinou špatně stíněné kabely vedoucí do počítače, takže informace o klávese je vyzařována i na zemnicí vodič. Ten je spojen s napájením počítače a odtud jde informace do elektrické sítě, kde je naměřena a snadno vyfiltrována [4].

Zamčení oscilátorů v generátorech náhodných znaků

Předchozí útoky byly pasivní, pouze modul pozorovaly. Nyní uvedeme příklad aktivního útoku na generátor náhodných znaků, který byl prezentován v době psaní článku na kryptografické konferenci CHES 2009. Generátor modulu se vystaví působení silného elektromagnetického vlnění, které způsobí sesynchronizování oscilátorů, obvykle použitých v generátoru náhodných znaků. Náhodnost se v nich ovšem vytváří právě tím, že se vyhodnocují odchylky fází těchto oscilátorů, které jsou (za normálních okolností) náhodně závislé pouze na různých vnějších tepelných a elektrických poměrech. Silné elektromagnetické vlnění, kterému je modul vystaven, však způsobí, že fázový posun se zamkne, a náhoda se tak nevytváří. Experimenty ukázaly, že zkoumaný generátor místo čtyř miliard náhodných hodnot pro 32bitové číslo produkoval jen 225 hodnot. Zajímavé je i technické použití tohoto útoku na čipové karty a na bankomaty. V bankomatu vyrábí náhodné bity příslušný hardwarový modul, který nemusí být ochráněn proti ozařování (v bankomatu, na nějž byl útok proveden, chráněn nebyl). Útok může vypadat následovně. Stačí zaparkovat auto poblíž bankomatu a vysílat 10GHz signál, amplitudově modulovaný frekvencí 1,8 MHz. Signál projde ventilačními škvírami bankomatu, ale pak je vyfiltrován tak, že namodulovaných 1,8 MHz působí na napájení. A to způsobí zamčení generátoru. Když auto odjede, neexistuje žádný důkaz toho, že generátor náhodných znaků neprodukoval náhodné znaky. Druhou stranou útoku je čipová karta. Byla vybrána čipová karta EMV, používaná jednou z hlavních britských bank. Na konferenci bylo ukázáno, jak lze kartu upravit tak, aby se docílilo zamknutí jejího generátoru (do 5V napájení se přivede 1V 24,04MHz sinusoida). I v této úpravě karta běžně pracuje, přičemž „úprava“ může být i součástí skimmeru, nikoliv karty samé. Paradoxem je, že tyto karty jsou chráněny proti promyšlenějšímu postrannímu kanálu DPA, který sleduje a využívá napěťově-proudové změny při činnosti karty, a přitom nejsou chráněny proti daleko méně náročnému útoku na generátor. Podrobnosti i reálnost použití útoku je možné nalézt v [5].

Etika zveřejňování útoků

Výzkumníci, kteří publikují podobná zjištění, jako jsou uvedena v tomto článku, řeší vždy etickou stránku svého konání. Závěr je ale jednoduchý, tato zjištění jsou ve prospěch spotřebitelů, uživatelů. Chrání je před producenty podobných slabých zařízení a dávají jim do rukou argumenty pro případ, že by se oni stali terčem útoku hackerů. Pokud vám z bankovního konta zmizí peníze, které jste si z bankomatu zcela jistě nevybrali, můžete alespoň mít argumenty na svoji obranu, když vám někdo bude tvrdit, že peníze nemohly být z vašeho účtu vybrány bez znalosti PIN vaší karty a bez této karty. Uvedené útoky i podrobnosti v citované literatuře jasně ukazují, že podvedený uživatel nemusel udělat žádnou chybu a nemusel nijak porušit povinnosti při ochraně své bankovní karty a PIN.

Varování ENISA

V současné době činí roční objem bankomatové kriminality v Evropě už půl miliardy eur. Proto evropská bezpečnostní organizace ENISA (European Network and Information Security Agency) vydala 7. září 2009 prohlášení, v němž varuje uživatele, aby si byli více vědomi rizik a protiopatření, aby se v maximální možné míře vyloučily osobní ztráty. Ve zprávě se mj. říká, že rychlý nárůst počtu bankomatů a rostoucí propracovanost útoků vedla v minulém roce k alarmujícímu 149% nárůstu počtu útoků na bankomaty. Jenom incidentů pomocí již dobře známých skimmerů bylo v minulém roce v Evropě hlášeno 10 302. ENISA také vydala seznam „zlatých pravidel“, jejichž dodržování uživateli nabízí maximum bezpečnosti s minimálním úsilím [6].

Vlastimil Klíma,
nezávislý kryptolog, v.klima@volny.cz

LITERATURA

[1] Klíma, V., Rosa, T.: Vybrané aspekty moderní kryptoanalýzy. ST, 3/2003, s. 3–7
[2] Archiv autora a seriálu článků : http://cryptography.hyperlink.cz
[3] Tygar, D.: Snooping on keyboards. UC Berkeley, 2006, http://www.cs.cityu.edu.hk/~asi06/downloads/ (Part I).
[4] http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html
[5] www.cl.cam.ac.uk/research/security
[6] Markettos, A. T., Moore, S.: The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators. http://www.enisa.europa.eu/pages/02_01_press_2009_09_07_atm_crime_paper.html