Bezpečnost bezdrátových technologií

Jan Krhovják, Václav Lorenc,
FI MU a ÚVT

Používání bezdrátových technologií pro přenos informací se stalo během posledních 20 let doslova hitem. Asi každý z nás v dnešní době vlastní jedno či více zařízení, s nimiž lze na menší či větší vzdálenosti snadno a pohodlně komunikovat. V té nejjednodušší formě (jednosměrný přenos) se typicky jedná o pouhé zasílání příkazů takovému zařízení – ať již si zde představíme ovládání rádia, televizoru, počítače či některých dveřních a garážových systémů. Složitější forma komunikace (obousměrný přenos) pak zahrnuje vzájemnou komunikaci dvou a více zařízení najednou a pokrývá obousměrné přenosy dat nezbytných např. k realizaci složitějších komunikačních protokolů (jaké používají modernější systémy zabezpečení motorových vozidel či dokonce celých objektů).

K bezdrátovému přenosu signálů se typicky využívá některých částí elektromagnetického spektra neviditelných lidským okem. Různé části spektra ale mají různé vlastnosti, které mají samozřejmě také vliv na celkovou kvalitu komunikačního média a udávají, mimo jiné, i snadnost šíření signálu a jeho náchylnost k různým druhům rušení. Typickým příkladem budiž právě výše zmíněné běžné ovladače rádií, audio přehrávačů, či televizorů. Ty k přenosu informací využívají infračerveného záření, které se nešíří za pevné překážky, v některých případech vyžaduje relativně přesné zaměření a navíc je poměrně snadno ovlivňováno a rušeno nepříznivými vnějšími podmínkami (ať již slunečním zářením, deštěm, mlhou, prachem). To vše je samozřejmě z pohledu bezpečnosti poměrně pozitivní chování a (jednosměrná) komunikace mezi těmito typy zařízení proto mnohdy není nijak dodatečně zabezpečena. Tato zařízení pak lze (neautorizovaně) ovládat de facto libovolným programovatelným infračerveným vysílačem, např. i dostupným v mobilním telefonu.

Ostatní běžně využívané části elektromagnetického spektra již typicky tak příznivé vlastnosti nemají. Sílu vysílaného signálu (a tedy i okruh jeho šíření) lze sice v principu vždy regulovat zeslabením výkonu vysílače, ale i zdánlivě slabý signál (přijímaný z velké dálky) může být zachycen s využitím velmi citlivého přijímače. To je hlavním důvodem, proč by měly být veškeré bezdrátové komunikační spoje, které jsou určeny k přenosu citlivých informací, vždy vhodným způsobem zabezpečeny.

Ukázkovým příkladem, jak by zabezpečení bezdrátové komunikace nemělo vypadat, jsou některé ze soudobých bezšňůrových (z angl. cordless) klávesnic. Bezpečnost zde kromě omezeného výkonu vysílače „posiluje" i přítomnost více (avšak typicky pouze dvou až čtyř) odlišných komunikačních kanálů reprezentovaných odlišnými nosnými frekvencemi. Asi netřeba detailně hluboce spekulovat nad tím, co vše se začne některým uživatelům objevovat jednoho dne na obrazovkách, vyskytne-li se v rámci jedné či více sousedních kanceláří (ne nutně stejné firmy či instituce) více kusů na tomto principu fungujících klávesnic a s nimi dodávaných přijímačů signálu. Nutno podotknout, že nemusí jít jen o zachycená jména a hesla, ale i např. o „přepisy" celých interních dokumentů velmi citlivé povahy.

Některé důmyslnější bezšňůrové klávesnice již sice využívají desítky tisíc odlišných komunikačních kanálů, čímž podobným situacím zamezují, bohužel cílený odposlech širšího komunikačního spektra (tj. všech komunikačních kanálů) je i nadále relativně snadno realizovatelný.

1 Což takhle kryptografie? A budeme vše šifrovat...

Nezbytnost zabezpečení citlivých dat (autentizace, důvěrnost, integrita) přenášených bezdrátovým médiem je tedy poměrně zřejmá a soudobé komunikační prostředky se již typicky snaží nějakým způsobem podporovat vhodné bezpečnostní mechanizmy. Zabezpečení dat však z jiného úhlu pohledu nemusí být pouze reakcí na ochranu citlivých informací, ale také mechanizmem, jak zavést např. zpoplatnění určité služby (accounting) či jiné zajímavé bezpečnostní vlastnosti (anonymita, nespojitelnost, nepopiratelnost). Ještě před srovnáním dalších používaných systémů/technologií, způsobů jejich

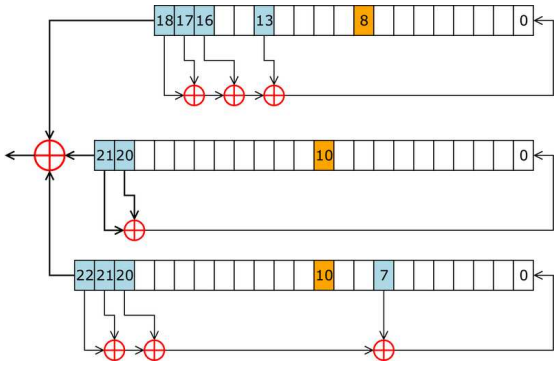
zabezpečení a problémů, kterými tyto mechanizmy trpí, je proto nutno připomenout, že mnohé ze systémů vznikaly se značně odlišnými bezpečnostními požadavky, které se navíc postupem času dynamicky vyvíjely a měnily.

Pouze u prvních bezdrátových systémů nebyl, vyjma ojedinělých případů, žádný z výše uvedených bezpečnostních mechanizmů vyžadován. Dobrým příkladem budiž využití celosvětového družicového navigačního resp. polohového systému GPS (Global Positioning System) pro civilní sektor, kde jsou data z GPS satelitů vysílána nešifrovaná. Možnost ověření autenticity a integrity dat by však i zde byla vítaným vylepšením celého systému a nová generace systému GPS již počítá i se zajištěním důvěrnosti (z důvodu možného zpoplatnění služby, podobně jako v případě televizního satelitního vysílání). Poznamenejme, že i stávající systém GPS vysílá na odlišném kanálu mnohem přesnější informace (určené pro vojenské účely) a ty jsou již celkově lépe zabezpečeny (jedním z cílů je např. i zvýšená odolnost proti úmyslnému rušení či zmatení přijímače neautentizovaným signálem).

Plošné nasazení vhodných bezpečnostních mechanizmů ale komplikuje v tomto případě fakt, že satelitní vysílání jsou z pohledu běžných uživatelů typickým příkladem pouze jednosměrné komunikace. V současné době proto např. satelity vysílající televizní signál selektivně šifrují vysílaná data (rádia, televizní programy) různými šifrovacími klíči s omezenou časovou platností. V případě, že má uživatel nějakou službu (televizní program) předplacenu, tak od poskytovatele typicky obdrží kryptografickou čipovou kartu s odpovídajícími dešifrovacími klíči, které se periodicky obměňují na základě řídicích signálů pravidelně vysílaných z vysílajícího satelitu.

Dalším příkladem v Evropě asi nejpoužívanější bezdrátové technologie je GSM (Global System for Mobile Communication). Oproti svým analogovým předchůdcům již GSM podporuje digitální přenosy hlasu a dat (což je nezbytný předpoklad pro zavedení moderních bezpečnostních mechanizmů) a GSM telefon dnes v Evropě vlastní drtivá většina obyvatel. Bezdrátový signál je ve skutečnosti přenášen pouze mezi koncovými stanicemi (mobilní telefon) a základnovými stanicemi (BTS, Base Transceiving Station). Základnové stanice jsou pak připojeny do zbytku sítě metalickými spoji a pouze ve výjimečných případech i nákladnějším obousměrným satelitním spojem.

V době, kdy se GSM systém navrhoval, bylo základním požadavkem dosažení alespoň takové bezpečnosti, jakou poskytovaly tehdejší pevné linky – především se jednalo o zajištění autentizace (jednostranné ověření identity vlastníka telefonu a ochrana telefonu proti klonování), důvěrnosti (ochrana citlivých signalizačních a uživatelských dat) a anonymity (nemožnost vystopování polohy uživatele sledováním rádiové komunikační linky). GSM k tomuto účelu využívá bezpečného prostředí kryptografické čipové karty (SIM, Subscriber Identity Module), dočasných identifikátorů, a několika typů proprietárních algoritmů (A3 pro autentizaci, A5 pro šifrování, A8 pro generování šifrovacích klíčů), jejichž princip fungování nebyl nikdy oficiální cestou publikován. Algoritmy A5/1 (viz obrázek 1) a A5/2 však byly v roce 1999 reverzním inženýrstvím odhaleny a následně zveřejněny [1].



Obrázek 1: Schéma šifrovacího algoritmu A5/1.

Mezi základní nedostatky celého GSM patří v dnešní době použití slabé 64bitové proudové šifry A5/1 či A5/2 (krom faktu, že je v obou případech šifra pouze 64bitová, byly v obou návrzích odhaleny i četné bezpečnostní slabiny), využití pouze jednosměrné autentizace (BTS se neautentizuje vůči mobilnímu zařízení a může být tedy nahrazena falešnou BTS, která mobilu navíc dokáže zakázat použití šifrování) a šifrování komunikace pouze v bezdrátové části sítě (na páteřní metalické síti či satelitním spoji jsou data typicky nešifrovaná).

2 Kryptografie znova a lépe. Šifrujeme, ale přestaneme utajovat!

Na přelomu tisíciletí se začaly bezdrátové technologie používat i k běžným přenosům mezi jednotlivými uživatelskými PC a tento trend byl o pár let později ještě umocněn masivním rozmachem používání přenosných počítačů (notebooky, PDA atp.). V této době vznikaly technologie jako Bluetooth a WiFi, které měly umožnit bezdrátové přenosy na relativně krátké vzdálenosti (desítky až stovky metrů). Se zabezpečením (autenticita, integrita, důvěrnost) přenášených dat se při návrhu počítalo, vědělo se o chybách existujících systémů, ale i přesto se v nových metodách zabezpečení objevilo několik zcela zásadních slabin (jak v návrhu, tak i v samotné implementaci). Otevřenost kryptografických algoritmů a jejich dostupnost širší veřejnosti však pomohla v relativně krátké době (jednotky let) řady z těchto nedostatků detekovat a odstranit (a to jak v reálných zařízeních, tak i v novějších verzích specifikací).

Bluetooth zařízení používají k vytvoření šifrovacího klíče proceduru tzv. párování, kdy je klíč vytvořen na základě krátkého hesla či PINu. Samotná procedura párování se však ukázala jako zranitelná a konstrukcí vhodné zprávy umožňuje útočníkovi párování i bez znalosti PINu. V mnoha jednodušších zařízeních je navíc PIN přednastaven (typicky s hodnotou 0000), což činí útok ještě snadnější. Se získaným šifrovacím klíčem již lze pak snadno pasivně odposlouchávat probíhající komunikaci (s tzv. Bluetooth puškou i na více než 1,5 km). Poznamenejme dále, že slabiny obsahuje i použitý šifrovací algoritmus E0, na jehož prolomení a získání 128bitového klíče je se znalostí dostatečného množství otevřeného textu potřeba jen 2^{38} operací (oproti očekávaným 2^{128}), což odpovídá cca 19 hodinám (na sběr dostatečného množství dat je potřeba 37 hodin). Více informací lze nalézt v [2, 3].

Bezdrátové sítě založené na standardu IEEE 802.11 (označované a certifikované jako Wi-Fi kompatibilní) a jejich zabezpečení prošly v uplynulých letech také poměrně drastickými změnami. Nejstarším podporovaným kryptografickým bezpečnostním mechanizmem je WEP (Wired Equivalent Privacy), zamýšlený zejména pro zajištění důvěrnosti (ale používaný i pro autentizaci). Existuje několik variant jeho implementací, které jsou vždy založené na proudové šifře RC4, a rozdíl mezi nimi je pouze v podporované délce šifrovacího klíče (64, 128 či někdy i 256 bitů). Na WEP existuje v současné době celá řada pasivních i aktivních útoků – jak na nevhodný autentizační mechanizmus (všichni uživatelé sdílejí stejné klíče, protokol typu výzva-odpověď využívá proudovou šifru, stanice si samy volí tzv. inicializační vektor), tak na samotný šifrovací mechanizmus využívající nevhodně navržený management klíčů (s využitím statistických metod může útočník v řádech minut nepozorovaně odvodit statický tajný klíč). Podrobnosti lze nalézt například v [4, 5].

Novějším bezpečnostním mechanizmem, který řeší mnohé z výše uvedených nedostatků, je WPA (Wi-Fi Protected Access). Ten v principu zachovává použití WEP, ale pouze v rámci protokolu TKIP (Temporal Key Integrity Protocol). Pro šifrování každého paketu je zde již vygenerován zcela nový (dočasný) šifrovací klíč, zdvojnásbila se délka požadovaných inicializačních vektorů a k zajištění integrity zprávy se kromě nekryptografického CRC-32 (detekční a opravný kód) používá i kryptografický MIC (Message Integrity Code) označovaný jako Michael. Na WPA se až teprve nyní začínají objevovat první úspěšné útoky – jeden např. umožňuje zaslat po 12–15 minutách do šifrované sítě 5–7 vlastních rámců [6].

Posledním bezpečnostním mechanizmem je WPA2 (někdy označován jako RSN, Robust Security Network). WPA2 je standardizován v IEEE 802.11i a přidává podporu 128bitového algoritmu AES-CCMP (AES Counter Mode with Cipher Block Chaining Message Authentication Code), který slouží pro zajištění důvěrnosti i integrity. V současné době nejsou známy žádné praktické útoky na tento mechanizmus. Podpora AES však již vyžaduje i výměnu hardware (přechod z WEP na WPA vyžadoval pouze upgrade firmware) a některé starší operační systémy jej nepodporují.

Odlišné mechanizmy zabezpečení, jejichž základní principy jsou ale do jisté míry velmi podobné mechanizmům použitým v Bluetooth či Wi-Fi, pak využívají i modernější sítě typu ZigBee, WiMAX a mnohé další…

3 Jednočipová kryptografická zařízení. Utajujeme za každých okolností...

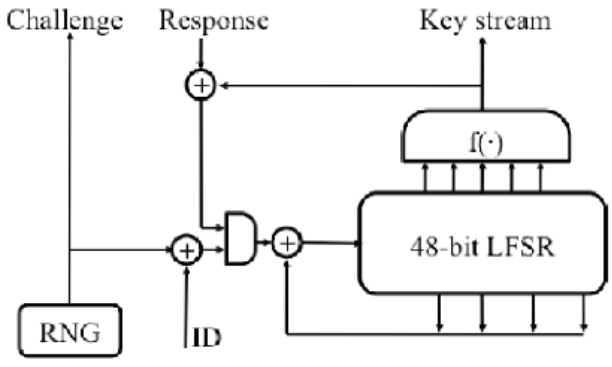
Během popisu bezpečnostní architektury některých systémů jsme také několikrát zmiňovali využití kontaktních kryptografických čipových karet (karty pro předplacené televizní vysílání, SIM karty v telefonech). Čipové karty jsou ale často využívány např. i jako platební či identifikační a přístupové karty. Tyto karty pak běžně slouží jako tzv. bezpečné nosiče dat, které navíc disponují určitým (i když značně omezeným) výpočetním výkonem. Jejich hlavním účelem je chránit citlivá data jejich vydavatelů (např. operátor mobilní telefonní sítě či banka) a musí proto být schopny zajistit těmto datům bezpečnost i v potenciálně nepřátelském prostředí (tj. v rukou uživatelů).

Kontaktní rozhraní, jehož prostřednictvím je po zasunutí do čtečky čip napájen, je ale z praktického hlediska poměrně omezující (vložení karty do čtečky zabere čas). Tento problém byl odstraněn až zavedením bezkontaktních čipových karet resp. obecně RFID čipů (často též označovaných jako RFID tagů). Existuje poměrně široká škála produktů založených na RFID, které se liší ať již metodami napájení (aktivní RFID obsahují vlastní zdroj napájení, pasivní RFID využívají k napájení elektromagnetické indukce), komunikační frekvencí, komunikačními protokoly atp. V současnosti je tato technologie využívána jednak k označení a identifikaci zboží (náhrada za čárové kódy), v bezdrátových čipových kartách (určeno zejména k identifikaci osob, umožnění přístupu do budovy/místnosti, k provádění mikroplateb) či ve státem vydávaných elektronických identifikačních dokumentech (elektronické pasy).

Starší systémy využívající bezkontaktní karty či jiné tagy typicky nemají žádné bezpečnostní mechanizmy implementovány – čip pak pouze v blízkosti přijímače vysílá nějaký identifikační kód, a na jeho základě systém rozpozná o jaký produkt/osobu se jedná. Udávaná vzdálenost vysílání pasivních tagů je totiž mnohdy limitována na několik centimetrů a odposlech z větší vzdálenosti (zejména od tagu ke čtečce) není tak snadný, protože přenos signálových prvků využívá tzv. zátěžové modulace. Zkopírování takového dostatečně blízkého (či nepozorovaně vypůjčeného) tagu ale není příliš obtížné a zabere jen jednotky sekund.

Základními bezpečnostními požadavky moderních čipů (ať již s kontaktním či bezkontaktním rozhraním) jsou u kryptografických čipových karet odolnost proti neautorizovanému přečtení uchovávaných dat a s tím související obtížnost padělání. U výrobců (nejen těchto) jednočipových zařízení stále přetrvává pro snazší „splnění" těchto požadavků zcela utajený návrh daného čipu, a mnohdy i vytváření proprietárních protokolů či šifrovacích algoritmů. Ukázkovým příkladem produktu se zcela utajeným návrhem (jež se z bezpečnostního hlediska ukázal jako zcela nedostatečný) je bezkontaktní čipová karta MIFARE Classic.

Tuto bezkontaktní kartu využívají mnohé instituce pro identifikační účely, systémy podnikové docházky či mikroplatby (např. za služby hromadné dopravy některých měst nebo celých zemí). Na konferenci Chaos Communication Camp (CCC) 2007 odhalili pánové Nohl, Evans a Plötz první schémata čipu MIFARE Classic. Jejich metoda reverzního inženýrství spočívala v rozřezání a nasnímání jednotlivých vrstev čipu. Následným poloautomatickým zpracováním získaných snímků po rozpoznání jednotlivých hradel vlastně zjistili, jak čip funguje. Odhalili jednak princip proprietárního algoritmu Crypto-1 (viz obrázek 2) a jeho slabiny (včetně možného útoku hrubou silou pod 50 minut).



Obrázek 2: Schéma šifrovacího algoritmu Crypto1.

Dále odhalili také zcela zásadní chybu v návrhu generátoru (pseudo)náhodných čísel, spočívající v možnosti využití konstantního semínka, závislého pouze na počtu hodinových cyklů, jež uběhly od přivedení energie do čipu. Pseudonáhodná čísla generovaná pomoci registru s lineární zpětnou vazbou (LFSR) jsou navíc pouze 16bitová, což je v dnešní době zcela nedostatečné. Prezentovaná metoda snímání a automatické rekonstrukce funkcionality čipu je zcela jasným signálem, že bezpečnosti založené na utajování algoritmu již skutečně odzvonilo. V témže roce se na MIFARE Classic objevilo i několik dalších (nezávislých) útoků, demonstrujících jak chyby v komunikačním protokolu vedoucí až k získání části tajných informací uložených v čipu, tak také přítomnost nejrůznějších postranních kanálů [7, 8].

V posledních letech se v souvislosti s bojem proti terorizmu poměrně razantně prosadily a stále prosazují nejrůznější elektronické identifikační dokumenty (pasy, identifikační karty, řidičská oprávnění). V České republice se v současné době můžeme setkat zejména s elektronickými pasy. Součástí těchto pasů je kryptografická čipová karta s bezkontaktním komunikačním rozhraním. Uvnitř této karty jsou nahrány veškeré informace, které jsou v tištěné formě viditelné v pasu, ale také dodatečné tzv. biometrické údaje (např. fotografie, otisk prstu) sloužící k přesnější identifikaci předkladatele pasu. Tato data již zcela evidentně nejsou vlastnictvím vydavatele daného dokumentu (tj. státu), ale jedná se o osobní údaje držitelů pasů. Ochrana a mechanizmy zabezpečení těchto dat jsou proto v popředí zájmu nemalé části potenciálních držitelů pasu (nejen z akademických kruhů).

I v případě elektronických pasů se však začaly objevovat určité nedostatky. Mechanizmy sloužící proti padělání pasu (tzv. pasivní a aktivní autentizace) jsou do značné míry podobné s mechanizmy použitými u kontaktních čipových platebních karet kompatibilních se specifikací EMV (tzv. statická a dynamická autentizace dat). Problematickým místem je ale řízení přístupu, které je v první verzi navrženo tak, že k autentizaci využívá dat snímaných ze strojově čitelné zóny pasu (MRZ, Machine Readable Zone). Původním předpokladem (pro zamezení neoprávněného, neautorizovaného a nepozorovaného kopírování pasu) bylo, že přístup k čipu získá jen ten, kdo pas fyzicky vlastní (a má tedy přístup k MRZ). Ukázalo se však, že data v MRZ obsahují jen málo entropie – namísto teoretických 58/74 bitů obsahují data jen 32 bitů (tj. jsou snadněji předvídatelná). To umožňuje bezkontaktní a nepozorovaný přístup k citlivým informacím mnohem většímu okruhu útočníků.

Tento problém je vyřešen až rozšířeným řízením přístupu, které je založeno na důmyslnějších metodách symetrické a asymetrické kryptografie. Celý mechanizmus je navržen tak, aby jednotlivé státy mohly ovlivnit, které ostatní státy budou mít přístup k citlivým osobním (zejména biometrickým) údajům jejich občanů a držitelů pasů. Více informací lze nalézt v [9].

4 I kryptologové mohou jezdit v drahých autech. Nebo se do nich alespoň dostat...

Dalším z velmi často používaných bezkontaktních zařízení je i tak běžná a nenápadná věc, jako dálkové uzamykání a odemykání auta či garáže.

První klíče se u aut objevily v roce 1919, jako obrana před krádeží. Nešlo o klíče bránící přístup do automobilu, ostatně mnohá z aut neměla ani střechu, ale o klasické startovací klíčky. Teprve od konce dvacátých let minulého století se u aut se střechou bránilo přístupu do vozu právě zámkem na dveřích.

Snaha výrobců aut a garážových systémů poskytnout řidičům co nejvíce pohodlí při běžných činnostech vedla k tomu, že se v padesátých letech objevil systém vzdáleného přístupu do garáží bez klíče (RKE, Remote Keyless Entry), který byl od roku 1983 zaveden i pro automobily. Vlastník vozidla dostal s klíčkem od startéru i bezdrátový vysílač, jenž umožňoval ovládat zámky u dveří auta.

Původní myšlenka jistě šikovná, systémy dodávané do devadesátých let však trpěly nepříjemným problémem – vhodně vybavený útočník mohl kód (libovolně dlouhý a komplikovaný) posílaný bezdrátovým klíčem nahrát a kdykoliv zopakovat tak, aby si vyhlédnuté auto či garáž znovu otevřel. Frekvence dodávaných systémů

byly veřejně známé (315 MHz v Severní Americe a Japonsku, 433.92 MHz v Evropě) a sestrojit podobný přístroj nebylo technicky neřešitelné. Řečeno odborně – systém nebyl chráněný proti útokům přehráním.

V průběhu devadesátých let minulého století se tak začala postupně užívat zařízení firmy Microchips, která v sobě obsahovala algoritmus KeeLoq, který už tomuto jednoduchému útoku byl schopen odolat. Ostatně posuďte sami – jeden z přístupů, tzv. „rolling codes" spočívá v tom, že zámek i fyzický klíč mají synchronizovaný čítač, který s každým dalším zmáčknutím fyzického klíče obě strany zvýší. Toto číslo je navíc pouze vstupem do speciální funkce, jejímž výsledkem je špatně predikovatelná posloupnost bitů posílaná směrem k zámku. Odposlechnutí tedy možné je, ale prosté zopakování již poslané sekvence útočníka k úspěšné krádeži nedovede.

Čistě teoreticky vzato bylo tedy zabezpečení systému KeeLoq zvoleno tak, aby odolávalo útokům. Nebo v to alespoň většina zúčastněných věřila.

Vývoj těchto vzdálených (ne)klíčů se nezastavil a pokračuje úspěšně dál, představena byla další zařízení od různých výrobců, která v sobě kombinují krom klíčů i platební karty a ještě více usnadňují život uživatelům automobilů. My se však zastavíme u zmiňovaného systému KeeLoq, který se v průběhu let dočkal masivního nasazení po celém světě (a používají jej automobilky jako Fiat, Chrysler, Daewoo, VW, Honda, Jaguar a další).

4.1 Postranní kanály, odběrová analýza

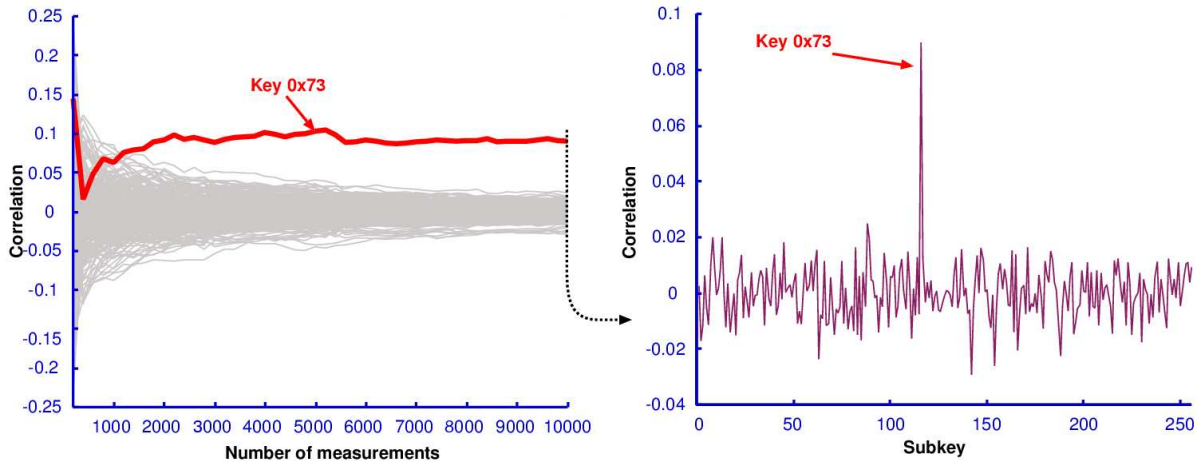
Aby bylo možno pokračovat ve výkladu slabin kryptografických zařízení, provedeme drobnou odbočku a vysvětlíme termín analýzy postranních kanálů, konkrétně oblast odběrové analýzy. Tento nápad se zrodil kolem roku 1998 v laboratořích Cryptographic Research, Inc., a to v hlavě Paula Kochera a jeho týmu během snahy o vyčítání tajných dat z kryptografických čipových karet [10].

Během práce libovolných počítačových čipů, tvořených milióny tranzistorů, nejsou jednotlivé bloky čipu vytěžovány stejnou měrou. Tento fakt sám o sobě nijak převratný není, právě tato vlastnost čipů je jejich návrhářům známa již od počátku. Co přišlo v roce 1998, byla úvaha, že zpracovává-li kryptografický čip tajná data a provádí tedy nějaký algoritmus, pak jednotlivé části takového algoritmu, kupříkladu blokové šifry, se na procesoru projeví v různý okamžik jinak velkým odběrem. Pro ilustraci – násobení a umocňování jsou dvě různě náročné operace, při kterých se zapojí jiné množství tranzistorů daného obvodu. Pečlivým sledováním odběru je tedy možné, bez dalších znalostí čipu či konkrétního prováděného algoritmu, tyto operace identifikovat. Tento přístup je znám pod názvem jednoduchá odběrová analýza (SPA, Simple Power Analysis).

Při využití statistických metod a násobného měření (prováděného i na různých vstupních datech) je možné odhalit pomocí diferenciální odběrové analýzy (DPA, Differential Power Analysis) nejen samotné operace, ale i jednotlivé bity tajných dat, které do procesu šifrování také vstupují (viz obrázek 3). Tedy krom získání informace, že právě probíhá operace násobení, zjistí útočník například i to, že čip s vysokou pravděpodobností násobí čísla lichá. Zdá se vám to málo? Věřte, že postupným odhalováním dalších a dalších vlastností operací a jejich operandů je možné se postupně dobrat až k celému tajnému klíči.

Hodila by se vám analogie? Vlastníci notebooků se dozajista potkali se situací, kdy je procesor vytížený natolik, že se větráčky chladící celý systém točí jako splašené. Tímto způsobem je tedy možné alespoň určit, a to bez jakéhokoliv dalšího zkoumání notebooku a jeho softwarového vybavení, že je jádro procesoru zatíženo nějakou náročnou operací. Právě jste úspěšně provedli pozorování postranního kanálu!

U speciálních kryptografických čipů, jejichž hlavním cílem je udržet v sobě tajný klíč, který se nikdy nesmí dostat do světa, jde o závažný problém, který od té doby neustále motivuje další a další výzkumníky a vývojáře kryptografického hardware, a to jak z pohledu útočníků, tak i obránců.



Obrázek 3: Naměřené odběry během kryptooperací.

A samozřejmě – proti těmto i dalším útokům existují i obranné mechanizmy. Stejně jako existují nové a stále účinnější útoky.

4.2 Útoky na KeeLoq

Vraťme se k zabezpečení automobilů. Více než dvacet let vydrželo firmě MicroChips tvrzení, že jejich systém je dokonalým zabezpečením draze pořízených automobilů.

To se však zásadně změnilo roku 2006, když se do světa dostala část zodpovědná za kryptografickou stránku systému KeeLoq a vědci se rozhodli přijít na kloub celému procesu. Mezi tvrzením, že je systém bezpečný, a bezpečným systémem jako takovým, je totiž propastný rozdíl.

Uvnitř KeeLoqu se skrývá algoritmus generování přístupových kódů, který využívá principu tzv. posuvných registrů s nelineární zpětnou vazbou, NLFSR, (Non-Linear Feedback Shift Registers). Jednoduše přiblíženo – funkce dostává na vstupu sadu bitů a na základě svého předchozího stavu a vstupu vygeneruje nejen výsledek, ale i stav pro další výpočet. Tyto funkce se často používají jako základ pro generátory pseudonáhodných čísel, a v KeeLoqu měly za úkol zabránit možnosti odposlechu a následného přehrání kódu pro manipulaci se zámky.

Andrey Bogdanov [11] a Nicolas Courtois se tedy pokusili v roce 2006 zaútočit za pomoci algebraických postupů a lineárních transformací na část zodpovědnou za generování kódů. Jednalo se však pouze o první krůčky – ve skutečnosti byla celá řada zámků mnohem více náchylná na útoky hrubou silou, kdy útočníci s kvalitním vybavením (zařízením založeným na tzv. programovatelných hradlových polích) byli schopni během několika týdnů odhalit klíč používaný konkrétním majitelem auta.

Týdny času a náročné zařízení však pořád představovaly poměrně velké překážky pro běžné útoky, a pro výrobce KeeLoqu to celé byla spíše nepříjemnost, než konkrétní problém. V roce 2007 skupina studentů a výzkumníků z univerzity v Leuvenu ve spolupráci s dalšími týmy nalezla další útok [12]. Ukázalo se, že pokud by se jim podařilo odhalit klíč pro konkrétního výrobce zařízení založených na KeeLoqu, stačilo by jim k úspěšnému útoku jen odposlechnout komunikaci mezi zámkem a klíčem. Teoretický pokrok značný, ale z praktického hlediska to stále nebylo ono – zjištění oněch tajných klíčů výrobců byla netriviální překážka.

Nicméně důležitý poznatek byl, že KeeLoq předpokládá, že vysílač v daném systému vlastní unikátní tajemství, kterým šifruje sekvence posílané směrem k přijímači, zatímco přijímač obsahuje tzv. hlavní klíč (z angl. master key) – bez znalosti konkrétního tajemství vysílače je tak schopen ověřit, že komunikace, která s ním probíhá, pochází od „správného" výrobce.

A v tuto chvíli nastupuje na scénu poslední příspěvek z řad akademické obce. 31. března roku 2008 přišel tým z univerzity v Bochumi s kompletním postupem, který v důsledku umožňuje

útočníkovi opravdu odposlechnout pouze dvě zprávy vyměněné mezi klíčem a automobilem či garážovými vraty, aby z toho následně bylo možné zrekonstruovat původní klíč[13]. Klíčovou se ukázala právě analýza postranních kanálů, která umožnila vyčtení výše zmiňovaných tajných klíčů výrobců z přijímačů zabudovaných v garážových vratech. Neb se tyto hlavní klíče nemění, stačí si pořídit dostatečnou zásobu zařízení pro vzdálené odemykání a klíče si např. přes Internet vyměnit s ostatními útočníky. Výroba padělku klíče od vašeho automobilu, a to i na vzdálenosti stovek metrů, je následně záležitostí pár vteřin.

Naštěstí to však neznamená, že by útočník mohl s autem odjet. V dalším pokračování úspěšného útoku mu brání imobilizér a startér, často používající odlišné mechanizmy nebo alespoň způsoby odvozování klíčů. Jen první úroveň obrany již padla.

Je poměrně zajímavé, že slabina není ani tak vázaná na samotnou funkci použitou uvnitř KeeLoqu, stejně dobře by bylo možné napadnout i další symetrické šifry (včetně AES) použité na jejím místě. Dalším zajímavým faktem je i skutečnost, že autoři KeeLoqu nabízeli od konce devadesátých let i systémy s větší délkou klíče, které by v mnohém ztížily celou analýzu a v podstatě eliminovaly útoky hrubou silou – ty se však v reálné výrobě jaksi neobjevily.

5 Závěr

Jak plyne z předchozích odstavců, bezkontaktní či bezdrátové technologie představují nelehkou technologickou oblast, alespoň co se zabezpečení týče. Jejich odposlech je často technicky realizovatelný i s menšími prostředky a všechny důležité věci kolem zajištění autentizace, integrity či důvěrnosti je tedy třeba řešit na úrovni kryptografických operací. A to je i místo, kdy přichází do hry tzv. Kerckhoffův princip, nabádající k tomu, že je mnohem snazší utajit pouze privátní klíče než celý algoritmus. V některých oblastech (bezdrátové sítě, přístupové karty, elektronické pasy) tento přístup již funguje, v jiných je utajení algoritmů stále základní součástí zabezpečení.

V posledních letech se navíc ukazuje, že softwarová a hardwarová stránka kryptografických zařízení spolu velmi těsně souvisí, a chyba na jedné nebo druhé straně může vést k dalekosáhlým důsledkům a nemalým investicím na záchranu nezabezpečených systémů. V době značných technologických pokroků a rychlých komunikačních sítí, je i termín tzv. výpočetní bezpečnosti podrobován neustálým zkouškám. Objevují se proto i nové, neotřelé přístupy s cílem lépe bránit tajné klíče a bránit jejich kopírování do jiných zařízení rovnou na fyzické úrovni (PUF, Physical Unclonable Functions).

Bezpečí je velmi křehký stav a je nutné o něj neustále pečovat. Pro začátek přinejmenším informováním o existujících problémech a možnostech jejich náprav.

A co systémy fungující denně kolem vás? Důvěřujete jejich bezpečnosti? Nezapomeňte, že každý systém je pouze tak bezpečný, jak je bezpečný jeho nejslabší článek...

Literatura

[1] M. Briceno, I. Goldberg, and D. Wagner. *A pedagogical implementation of A5/1*. 1999. Dostupné na: `http://www.scard.org/gsm/a51.html`.

[2] A. Becker. *Bluetooth Security & Hacks*. 2007. Dostupné na: `http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf`.

[3] Y. Lu, and S. Vaudenay. *Faster Correlation Attack on Bluetooth Keystream Generator E0*. 2004. Dostupné na: `http://lasecwww.epfl.ch/pub/lasec/doc/YV04a.pdf`.

[4] N. Borisov, I. Goldberg, D. Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. 2001. Dostupné na: `http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf`.

[5] E. Tews, A. Pychkine, and R.-P. Weinmann. Breaking 104 bit WEP in less than 60 seconds. 2007. Dostupné na: `http://eprint.iacr.org/2007/120.pdf`.

[6] M. Beck, and E. Tews. *Practical attacks against WEP and WPA*. Prosinec, 2008. Do-

stupné na: http://dl.aircrack-ng.org/breakingwepandwpa.pdf.

[7] F. D. Garcia et al. *Dismantling MIFARE Classic*. 2008. Dostupné na: http://www.cs.ru.nl/~flaviog/publications/Dismantling.Mifare.pdf.

[8] F. D. Garcia et al. *Wirelessly Pickpocketing a Mifare Classic Card*. 2009 Dostupné na: http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf.

[9] Z. Říha, P. Švenda, V. Matyáš. *Bezpečnost elektronických pasů (část II)*. Crypto-World 1/2007. Dostupné na: http://crypto-world.info/casop9/crypto01_07.pdf.

[10] P. Kocher, J. Jaffe, B. Jun. *Differential Power Analysis*. 1999. Dostupné na: http://www.cryptography.com/resources/whitepapers/DPA.pdf

[11] A. Bogdanov. *Cryptanalysis of the KeeLoq block cipher*. Cryptology ePrint Archive: Report 2007/055. Dostupné na: http://eprint.iacr.org/2007/055

[12] E. Biham, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel. *How To Steal Cars – A Practical Attack on KeeLoq*. 2007. Dostupné na: http://www.cosic.esat.kuleuven.be/keeloq/

[13] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar et al. *Physical Cryptanalysis of KeeLoq Code Hopping Applications*. Cryptology ePrint Archive: Report 2008/058. Dostupné na: http://www.crypto.rub.de/keeloq/

□