Penetrační test RFID – Případ HID

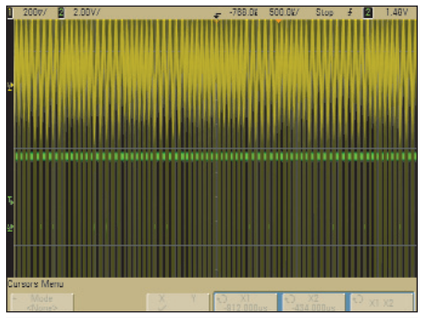
Následující článek patří do stejného kontextu jako „Případ INDALA“ publikovaný v ST 7/2008 [6]. Dále se proto omezíme na hlavní fakta nového případu. I zde bylo cílem pomocí penetračního testu prověřit systém fyzické bezpečnosti založený na čipech RFID. Otázkou k prověření bylo, zda a jak složitě lze vytvořit funkční duplikát něčí přístupové karty.

Data sem a tam

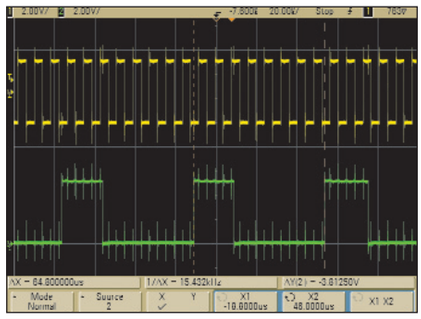
Na originálních kartách, které nám byly zapůjčeny, bylo mimo jiné decentně natištěno slovo „HID“. Na internetu nebylo složité zjistit, že firma stejného jména vyrábí celou řadu karet s daným označením. Některé z nich jsou přitom určeny pro pásmo LF, jiné pro HF. Solidní detaily však už jaksi chybějí. Dále jsme narazili na zajímavou kauzu (viz například [4]), při které tato společnost právní cestou zasáhla do obsahu přednášky poukazující na slabinu některého z jejich čipů. Inu, opět máme tu čest s pěknými pašáky!

Komunikačním přijímačem (viz ST 7/2008) jsme propátrali pole v okolí jedné z dveřních čteček, abychom zjistili, kde testované karty pracují. Nade vší pochybnost to bylo pásmo LF, a šlo tedy nejspíš o technologii HID Prox [3]. Naši multiprotokolovou čtečku jsme tentokrát ani nezkoušeli, neboť tuto platformu s jistotou nepodporuje. Místo toho jsme rovnou použili improvizovanou magnetickou sondu a podívali se, jak vypadá reakce karty v poli čtečky generující pouze základní nosnou. Prostým okem jsme zde ovšem nic zajímavého neodhalili – zjevně bylo nutné signál nejprve amplitudově demodulovat. K tomu účelu jsme využili ladicí body v naší zlodějce z ST 2/2008. Upravená zlodějka pouze generovala základní nosnou a my jsme se s osciloskopem připojili za demodulátor AM. Získaný průběh je na *obr. 1* ve žluté stopě. Zelená stopa je pomocný komparátor, který teď není podstatný. Ačkoliv je signál díky extrémní jednoduchosti rádiové části zlodějky znatelně zarušený, přesto zřetelně vidíme dvě věci. Za prvé karta po umístění do pole čtečky automaticky vysílá nějaká data, což je pro nás, coby útočníky, moc dobré znamení. Za druhé vidíme, že data jsou kódována pomocí slov nad množinou dvou základních symbolů {A, B}, které odpovídají modulaci pomocnou nosnou *f/a* respektive *f/b*, kde *f* je frekvence základní nosné.

Pro získání signálu, který bude možno spolehlivě dekódovat, jsme museli naši zlodějku poněkud vylepšit. Malinko jsme si ovšem usnadnili práci. Od vývojářské společnosti ASICentrum [5], která se coby součást švýcarské firmy EM Microelectronic věnuje mimo jiné právě návrhu obvodů pro RFID, jsme si zapůjčili modul



Obr. 1 Původní zlodějka a HID Prox



Obr. 2 EM4095 v akci – symbol A

P4095 DEMO BOARD [2] osazený čipem EM4095[1]. Tamní vývojář ještě přidal ideu jak tento obvod dostat do poněkud nestandardního režimu umožňujícího pasivní odposlech dat vysílaných čipem do originální čtečky. Ne že by byl nějaký problém v tom, aby EM4095 generoval napájecí pole sám, ale použití pasivního odposlechu zásadně rozšiřuje využitelnost předvedeného útoku. Blíže se na tento zajímavý obvod podíváme příště. Zde se omezíme na konstatování, že režim pasivního odposlechu (zdůrazněme, že to není standardně publikovaný modus) jsme na zapůjčeném modulu jednoduchým přepojením anténního obvodu bez problémů realizovali a rovněž tak jsme k němu bez potíží připojili digitální část naší zlodějky. Tak vznikl robustní odposlechový přípravek pro pásmo LF.

Signál získaný odposlechem komunikace s originální čtečkou je na *obr. 2*. Žlutá stopa představuje obnovené hodiny neboli základní nosnou (PLL syntéza se závěsem na anténu), zelená stopa druhého kanálu znázorňuje demodulovaný signál vysílaný testovací kartou HID. To vše nabízí přímo EM4095. Zbytky rušení patrné na průbězích jsou nejspíš cenou za to, že jsme si příliš nelámali hlavu se stíněním našeho přípravku. Nicméně při zpracování přes analogové vstupy procesoru PIC16F628, kde pracují programovatelné komparátory, jsme nezaznamenali žádné potíže. Odtud už jsme snadno určili konkrétní hodnoty pomocných frekvencí pro výše zavedené znaky: A ~ *f*/8, B ~ *f*/10. Zároveň jsme změřili, že doba trvání rámce jednoho znaku je rovna 50/*f*, kde *f* je frekvence základní nosné.

Délku výstupní posloupnosti jsme určili na základě periody opakování posloupnosti znaků A/B získaných dekódováním demodulovaného signálu karty. U všech karet se posloupnost opakovala po 96 znacích. Tím jsme měli obraz karty plně určen. Stejně jako minule, ani zde jsme se nezabývali tím jak získané slovo převést na obsah paměti karty. Letmá analýza napovídá, že bychom měli provést ještě jedno dekódování podle konvence manchester s vynecháním jisté synchronizační posloupnosti a že výsledných nejvýše 48 bitů (nevíme jak interpretovat onu synchronizaci) by pak bylo skutečným datovým obsahem karty. Nic takového my ovšem dělat nemusíme, protože nám jde o vytvoření duplikátu, nikoliv o naprogramování zcela nové karty. Namísto toho se musíme porozhlédnout po něčem, co umí získané základní slovo o délce 96 znaků podle změřených parametrů přehrát do pole čtečky. Oblíbený čip Q5 (ST 3/2008) nás ani tentokrát nenechal na holičkách. S konfiguračním slovem 60 01 80 56 a konvencí A = 0, B = 1 jsme úspěšně naklonovali všechny testované karty.

Závěr

Technika penetračních testů opět slavila úspěch. Zároveň vidíme, že obliba používání nevhodných čipů RFID aplikačními inženýry patrně nezná mezí. Nezbývá než doporučit věnovat této oblasti zvýšenou pozornost a, mimo jiné, začít provádět i takovéto testy. Pokud je nám známo, tak komerčně je dosud nikdo nepožaduje ani nenabízí. Z našeho hlediska je přitom už pár minut po dvanácté.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, tomas.rosa@rb.cz

LITERATURA

[1] EM4095 – Read/Write analog front end for 125 kHz RFID Basestation, EM Microelectronic-Marin SA, SWATCH Group, 2001

[2] EM4095 – Application Note 404, EM Microelectronic-Marin SA, SWATCH Group, 2006

[3] http://www.hidcorp.com/documents/hidprox_broch_en.pdf

[4] http://www.schneier.com/crypto-gram-0703.html#11

[5] http://www.asicentrum.cz

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