Penetrační test RFID – případ INDALA

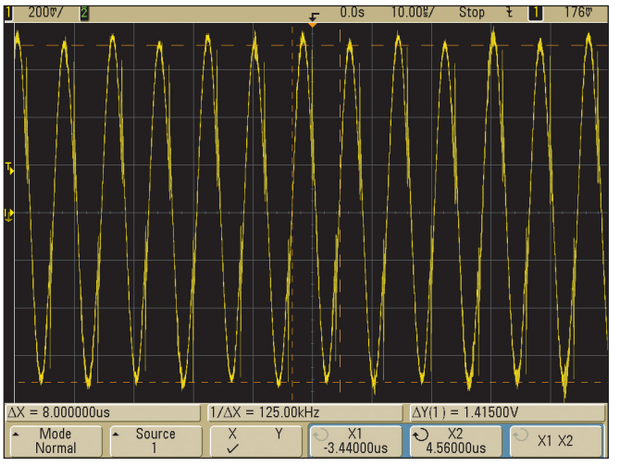
Penetrační testování je již notoricky známo coby technika umožňující simulovaným útokem prověřit odolnost konkrétní aplikace vůči napadení. V mnoha případech je to díky nedostatečné analytické, vývojové a provozní dokumentaci jediná cesta, jak se o bezpečnosti vybrané aplikace (například internetového obchodu) něco smysluplného dozvědět. Takhle to alespoň chodí v informační bezpečnosti. V sesterské oblasti zvané fyzická bezpečnost jsou počítače sice dnes už stejně důležité jako ocel, avšak penetrační testování se zde příliš nepoužívá. Pravda, vůči testování bankovní pobočky kulometem asi budou oprávněné výhrady, avšak proč se nezaměřit právě na zmíněné prvky IT? Jejich zranitelnosti jsou v zásadě stejné bez ohledu na místo a účel použití.

Ukážeme vám, jak jsme si na jednu takovou aplikaci na bázi RFID posvítili. V ruce jsme měli několik karet s povoleným přístupem do chráněné oblasti a cílem bylo vytvořit funkční duplikát alespoň jedné z nich. Nikdo nám neřekl, jak přesně systém pracuje a co jsou karty vlastně zač. Čili klasické zadání penetračního testu. Podaří se nám dostat se dovnitř?

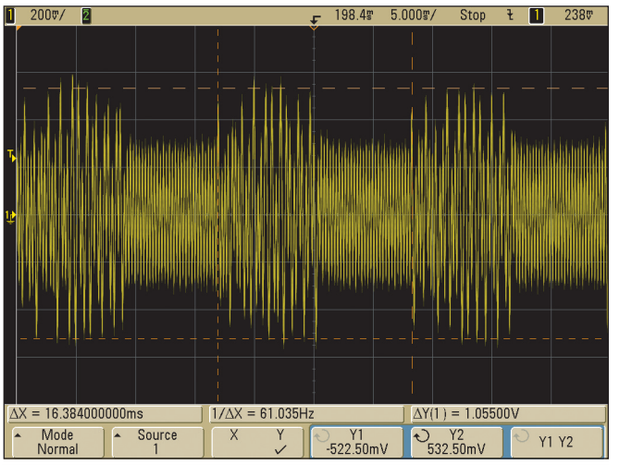
Data sem

Prvním úkolem na cestě k vytvoření duplikátu přístupové karty je pochopitelně přečtení jejího obsahu. K tomu je vhodné znát alespoň komunikační protokol. Jediné, co jsme však o kartě věděli, bylo, že je na ní uvedeno slovo „INDALA“. Na internetu jsme záhy našli produktový list [2], který nám (coby útočníkům) s typickou marketingovou dikcí vyhrožoval šifrováním dat, několikanásobnou autentizací, přístupovými hesly a bůhvíčím ještě. Možná že karty nejsou tak úplně hloupé, avšak coby útočníky nás to nesmí odradit. Pro nás je důležitý tento konkrétní systém a způsob, jakým jsou v něm karty použity.

Něco jsme se z [2] přeci jen dozvěděli. Karty by měly pracovat v pásmu LF, konkrétně byla zmíněna frekvence 125 kHz. Vzali jsme proto multiprotokolovou čtečku postavenou na bázi ACG LF MultiTag OEM Module [3], přiložili kartu a ... nic. Čtečka kartu zjevně ignorovala. Bylo nutné zjistit, zda karta pasivně čeká na nějaké heslo ze čtečky, nebo zda si jen nerozumí ve způsobu modulace. Navinutím deseti závitů kusu měděného drátu na průměr 75 mm co nejblíže k sobě vznikla improvizovaná magnetická sonda, kterou jsme připojili k běžné napěťové sondě osciloskopu. Čtečku jsme přepnuli do režimu, kdy generuje jen základní nosnou 125 kHz, a kartu se sondou přiblížili k její anténě. Výsledný průběh napětí na sondě je na *obr. 1*. Zde už jsou první důvody k optimismu. Vidíme, že amplituda hlavní nosné od periody k periodě drobně „poskakuje“, což nám napovídá, že karta cosi přeci jen sama od sebe vysílá. Zjevně využívá pomocnou nosnou f_0=62,5 kHz=125/2 kHz, kterou je teprve zátěžově modulováno pole terminálu. Tento druh provozu naše čtečka už zpracovat neumí, a proto mlčí. Nabízí se obstarat si novou čtečku, avšak u neznámé nové čtečky nemáme zaručeno, že nám na výstupu podá skutečně nezkreslený obraz obsahu karty.



Obr. 1 Pole základní nosné 125 kHz modulované kartou



Obr. 2 Pomocná nosná karty zachycená v okolí 187,5 kHz

Podívejme se, jaký signál nás zajímá nejvíc. Zátěžová modulace základní nosné čtečky harmonickým signálem o frekvenci f_0=62,5 kHz vytvoří v blízkém poli dobře známá postranní pásma o frekvencích $f_{p1,2}$=125 kHz ±62,5 kHz. Pro nás je přitom velmi zajímavé horní pásmo s frekvencí f_{p2}=187,5 kHz, které už dokážeme naladit na našem komunikačním rádiu Sangean ATS 909w [4]. V podstatě jde o kvalitní rozhlasový přijímač disponující širším rozsahem a podporující kromě běžného FM a AM i provoz SSB tolik oblíbený u radioamatérů. Přijímač jsme umístili do blízkosti antény čtečky, přepnuli do režimu USB (horní postranní pásmo SSB) a začali proladovat okolí frekvence f_{p2} zleva. Nízkofrekvenční signál z rádia jsme kromě reproduktoru vedli i do osciloskopu. Po chvíli jsme byli schopni naladit chrčivo-piskavý tón, který se v okolí (jednotky až desítky cm) antény čtečky objevoval právě při přiblížení karty. Jeho snímek je na *obr. 2*. Další důvody k optimismu byly na světě.

Na *obr. 2* je zjevně zajímavý periodický průběh, který je ohraničen svislými linkami časového kurzoru. Zjistili jsme, že perioda jeho opakování d=16,384 ms je nezávislá na naladění rádia. Nejpravděpodobnější příčinou takové invariace je, že opakování tohoto průběhu odpovídá cyklickému čtení paměti karty. Co jedno sériové vyčtení, to jeden takový průběh. Nehledě na výhružky letáku [2] jsme zde tedy nejspíš na stopě obyčejné paměťové karty, podobné té z ST 2/2008. Pro získání konkrétních dat vysílaných kartou potřebujeme vědět, jak máme zachycenému analogovému signálu rozumět. Zde je nutno udělat pár odhadů. Prvním je, že data jsou na pomocnou nosnou modulována změnou fáze (tzv. fázová modulace). Proč? Protože je to v takových případech běžné (při penetračních testech hrají obrovskou roli zkušenosti). Druhým odhadem je, že pro zjištěnou periodu platí jednoduchá formulka $d=a.c/f$, kde a je počet bitů modulujících dat, c je délka bitového rámce měřená v počtu period základní nosné a f je její frekvence. Po dosazení máme $a.c$=2048. Pro hodnotu c přicházejí obvykle v úvahu čísla 16, 32, 64. My jsme zvolili c=32, což dává 64 bitů dat a s touto

konfigurací jsme dosáhli dále popsaných výsledků. Dodejme, že chybně provedené odhady se záhy projeví tím, že „nic nevychází“, takže metodou pokus-omyl se časem dospěje ke správnému výsledku.

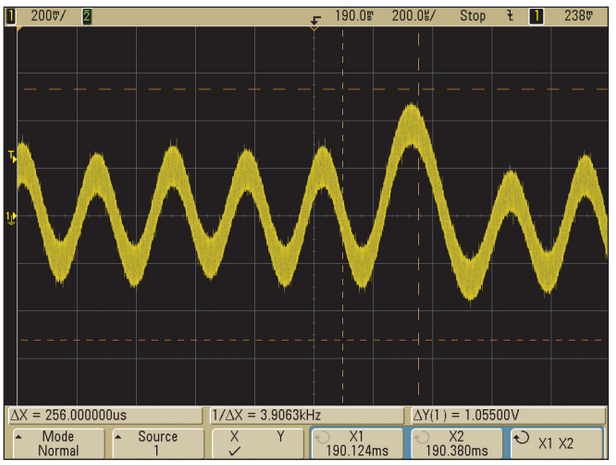
Nyní už víme o chování karty dost na to, abychom si sami postavili čtečku, které můžeme důvěřovat. Tento úkol jsme svěřili našemu dvornímu konstruktérovi Tomáši Volyňskému a sami dál pokračovali v experimentech s rádiem. Co takhle vyrobit funkční duplikát karty jen z toho vrčení, co na nás rádio pouští? Frekvence bitových rámců f/c=3906,25 Hz by měla nízkofrekvenčními obvody přijímače hravě projít, takže nebylo nad čím váhat. Přijímač jsme vyladili na frekvenci co nejblíže hodnotě (187,5–3,906) kHz, kdy perioda získaného obrazu pomocné nosné odpovídá právě jednomu bitovému rámci. Analýzou navzorkovaného signálu z našeho rádia s krokem c/f=256 µs jsme pak byli schopni rozlišit, jestli na začátku bitového rámce byla změna fáze či nikoliv, jak dokládá *obr. 3*. Změna fáze se projeví prodloužením periody a nárůstem amplitudy. Pokud naproti tomu ke změně nedochází, směřuje průběh ke zhruba konstantní amplitudě s periodou odpovídající bitovému rámci. Na *obr. 4* vidíme i složitější situace, avšak ve všech se dá po chvilce pomocí pravítka a tužky snadno vyznat.

Data tam

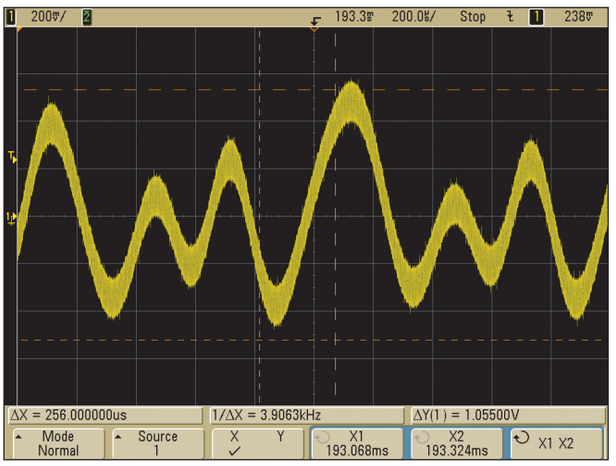
Výše popsaným způsobem se nám podařilo získat popis vysílaných dat coby slovo z množiny $\{A,B\}^{64}$, kde A znamená, že v daném rámci byla změna fáze, B že nebyla. Otázkou je, jak z takového slova získat skutečný datový obsah karty. To je úkol vyžadující stanovení dalších předpokladů a provedení dalších měření. Jenže musíme my ho vyřešit? Zde je zásadní si uvědomit, že nikoliv! O co skutečně jde, je aby náš padělek vytvořil v poli čtečky stejný signál, jaký vytváří originální karta. To je celé. Bez skrupulí proto můžeme rovnou položit A=0 a B=1 a hledat zařízení, které bude nuly vysílat jako *změny* a jedničky jako *ne-změny* fáze pomocné nosné. Na scénu přichází náš oblíbený švýcarský nožík – programovatelný čip *Q5* [1] (viz ST 3/2008). S konfiguračním slovem *60 00 F0 A4* dělá tato karta přesně to, co my potřebujeme. Pak už stačí jen uložit získaná data do bloků 1 a 2 stránky 0 a je to.

Račte vstoupit!

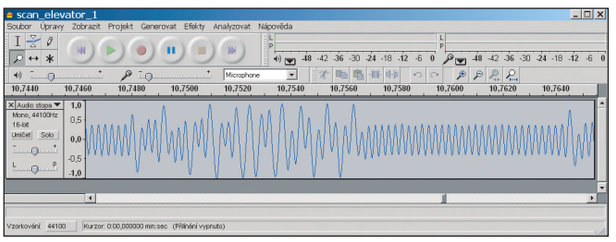
Od všech předložených karet se nám podařilo vyrobit funkční duplikáty. U některých jsme použili přesně popsanou metodu, jiné jsme přečetli prototypovou čtečkou, kterou kolega Volyňský mezitím sestavil. Možnost využití radiopřijímače byla tak zajímavá, že jsme se rozhodli zkusit další útok – pasivní odposlechnutí dat karty, kterou před námi její oprávněný držitel použije. Jeden z nás proto nastoupil do výtahu, ve kterém je nutné se před volbou patra nejprve prokázat správnou kartou. Byl vyzbrojen brašnou s ukrytým rádiem, ze které vedl drát do notebooku se spuštěným programem pro záznam audiosignálů. Otevřený notebook držel v ruce před sebou a pro jistotu měl ještě v uších sluchátka pro příposlech zachycovaného signálu. Brašna s rádiem mu visela přes rameno ve vzdálenosti asi 20 cm od čtečky výtahu. I tahle komedie měla svůj důvod. Ukázalo se totiž, že všichni spolucestující pilně přikládali své kartičky ke čtečce, aniž by v nich naše divadlo vzbudilo jakékoliv podezření. Signál zachycený v této situaci z testovací karty je na *obr. 5*. Signály ostatních karet vypadaly obdobně, s tím drobným rozdílem, že nesly data, která po naplnění do *Q5* dovolí dojet do správného patra a otevřít tam ty správné dveře. Poznamenejme ještě, že v tomto případě byla vzdálenost rádia útočníka dosti limitována už beztak poněkud unavenou čtečkou výtahu fungující na několik cm. Nicméně víme o instalacích těchto karet, kde jsou použity velké rámové antény, jejichž předností je operační dosah pro čipy INDALA v řádu desítek cm. Lze si snadno domyslet, že i možnosti odposlechu jsou touto instalací rovněž patřičně vylepšeny.



Obr. 3 Posloupnost ...BBBBABB...



Obr. 4 Posloupnost ...ABBAABB...



Obr. 5 Demonstrační úlovek z výtahu

Závěr

Podobně jako u dříve probíraných čipů nechceme tímto tvrdit, že karty INDALA jako takové by měly být za všech okolností zatraceny. Kritika patří jejich konkrétní aplikaci. Navíc bylo naším cílem především názorně demonstrovat sílu a vhodnost provádění penetračního testování prvků fyzické bezpečnosti se stejnou rutinou a samozřejmostí, s jakou se dnes tato technika používá v bezpečnosti informační. Popisovaný postup také pěkně demonstruje, že i s relativně jednoduchými prostředky a dobrou strategií lze dospět ke kýženému cíli.

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

LITERATURA

[1] Specification Q5B – ASIC for RFID, SID TAG Switzerland, SOKYMAT s.a., 2001
[2] http://www.hidglobal.com/documents/indala_flexiso_card_ds_en.pdf
[3] http://acg-id.aaitg.com/index.php?id=97
[4] http://www.sangean.nl/English/?opt3=ATS-909%20w&opt5=38
[5] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz