Kladivo na pašáky – Q5

Minule jsme se seznámili s čipem RFID EM4x02, který by sám o sobě byl celkem neškodný, nebýt ovšem zarputilé snahy mnoha „pašáků“ (tedy těch, kdo nepotřebují nic moc vědět a jdou rovnou tvrdě na věc) používat ho v aplikacích, kde nemá co dělat. Představili jsme si zařízení nazvané zlodějka, s jehož pomocí může útočník bezděky okopírovat například klíč od garáže ze zavřené kabelky, aktovky či rovnou z kapsy. Někdo by snad mohl namítnout, že zlodějka není na trhu volně k dispozici a její amatérská konstrukce není úplně triviální. Nuže zde ukážeme, jak si vystačit s tím, co se v běžném obchodě koupit dá. Budeme potřebovat jednu sériově vyráběnou multiprotokolovou čtečku pro pásmo LF (je jich plný Internet) a kartu nebo jiný vhodný předmět s čipem zvláštního jména – Q5.

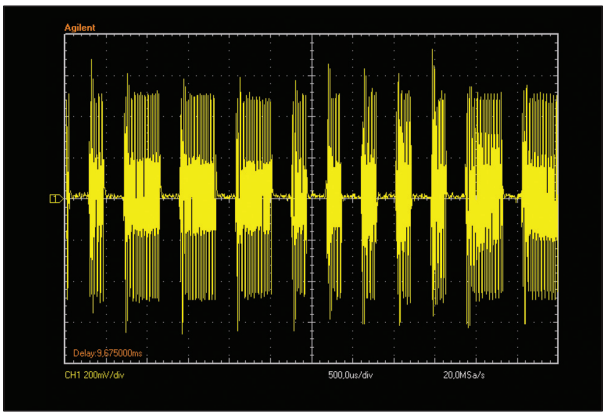
Na jedné straně

Z pohledu konstruktéra představuje Q5 jistý pokus o paměťový čip s řízeným přístupem a pamětí typu EEPROM určený pro RFID v pásmu LF. Struktura paměťové oblasti je na *obr. 1*. Dnes se setkáme téměř výhradně s kartami s 330b pamětí, rozdělenou na stránky 1 a 0. Ve starších čipech nebyla stránka číslo 1 sloužící k uchovávání identifikační hlavičky implementována, což může v novějších čtečkách vést k jejich odmítnutí. Existuje starý trik jak se s tím vypořádat, ale toto zde není předmětem našeho zájmu. Dodejme, že formát hlavičky odpovídá formátu EM4x02 představenému v předchozím díle. Nicméně toto není v našem útoku nijak využito, neboť obsah hlavičky ve stránce 1 nelze měnit. Vidíme, že stránky se dělí na bloky pevné velikosti 33 bitů, přičemž bit 0 slouží jako příznak uzamčení do stavu pouze pro čtení a sám o sobě se při vyčítání paměti nepřenáší.

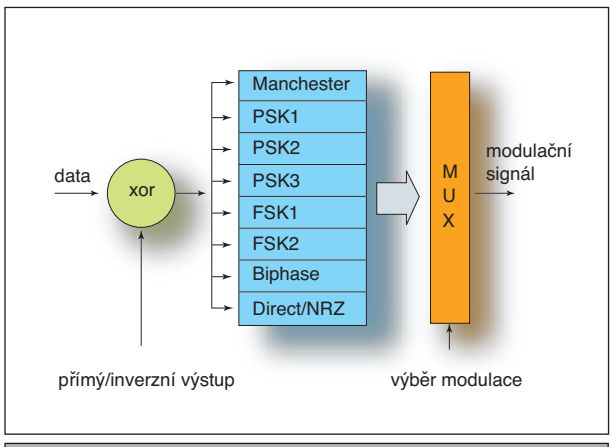
K volitelnému řízení přístupu slouží 32b heslo, které si v takovém případě alokuje blok 7. Jak jsme však zjistili, má celý mechanismus pár mušek. První z nich je přenos hesla v otevřeném tvaru, což vidíme na *obr. 2*. Kratší úseky nosné mezi dvěma mezerami odpovídají nule, delší pak jedničce. Zajímavá je rovněž sémantická kolize komunikačního protokolu. Prakticky jsme ověřili, že pokud se vhodně nakonfigurovaný čip, který neočekává heslo, dostane do pole terminálu, který heslový režim očekává, dojde během pokusu o předání hesla kartě k jeho zapsání do uživatelské části paměti, odkud si ho pak útočník může bez problémů přečíst! Takový kousek se nevidí příliš často.

stránka	blok	bit	
		0	1....32
1	2	1	tovární data – identifikační hlavička
	1	1	tovární data – identifikační hlavička
0	7	L	uživatelská data nebo heslo
	6	L	uživatelská data
	5	L	uživatelská data
	4	L	uživatelská data
	3	L	uživatelská data
	2	L	uživatelská data
	1	L	uživatelská data
	0	L	konfigurační slovo

Obr. 1 Struktura paměti Q5



Obr. 2 Záchyt předávání hesla v otevřeném tvaru



Obr. 3 Výstupní kodér Q5

Na straně druhé

Z pohledu útočníka představuje čip Q5 cosi jako univerzální švýcarský nožík. Celkem snadno jej lze totiž nakonfigurovat tak, že po probuzení v poli čtečky začne automaticky stále dokola vysílat obsah určeného počtu uživatelských bloků, počínaje blokem 1 nahoru. K dispozici je dále robustní modulátor, který kromě klasického manchesteru nabízí sedm dalších kodérů (*obr. 3*). Data z paměti se mohou číst přímo nebo inverzně. Podporováno je též několik rychlostí přenosu, pro fázové a frekvenční modulace i několik pomocných nosných. Povšimněme si, že v režimu NRZ můžeme anténu ovládat přímo digitálním signálem z datového sekvenceru. Paměťových karet, které by s tímto arzenálem nebylo možné napodobit, bude asi hodně málo. Pro čip EM4x02 se nám konkrétně osvědčilo konfigurační slovo 6001F004, tedy přímý cyklický výstup dvou bloků (64 b) s modulací manchester rychlostí nosná/64 (viz [1]). Do bloků 1 a 2 stránky 0 přitom uložíme datovou strukturu popsanou minule. Takto vybavený útočník už nemusí stavět žádná speciální zařízení. Stačí jen pomocí standardní čtečky přečíst obsah kýžené klíčenky a pomocí téže čtečky naprogramovat její duplikát do standardního čipu Q5. Čistě teoreticky by přístupový systém mohl testovat, zda se nejedná o Qpětkový padělek, ale praktické testy ukázaly, že s něčím takovým si hlavu rozhodně neláme.

Závěr

Snahou konstruktérů „kvé pětky“ nejspíš bylo jednak přijít s pamětí vybavenou solidním řízením přístupu, jednak po bezpečnostní stránce totálně deklasovat konkurenci spoléhající na čistě paměťové karty, jako je například právě EM4x02. První cíl se díky chybám v návrhu a tvrdé konkurenci podstatně vyspělejších protihráčů z pásma HF příliš nevyvedl, zato však druhý vyšel na sto procent. Q5 tak nejspíš do historie RFID vejde coby sériově vyráběný nástroj pro hackery. Snad si toho konečně všimnou i naši milí pašáci.

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