Jak pašáci aplikují RFID

V rámci problematiky RFID nelze neuvést alespoň jeden exemplární příklad toho, že pašáci (tedy ti, kdo nepotřebují nic moc vědět a jdou rovnou tvrdě na věc) jsou i zde. Přitom nejde zrovna o málo, neboť níže popsané prostředky a postupy často chrání nejen hmotný majetek, ale i bezpečí samotných lidí.

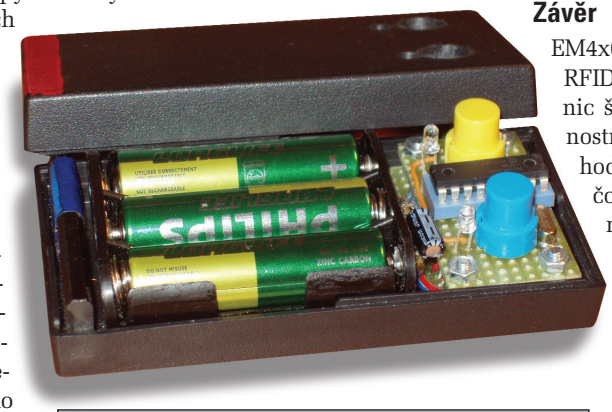
LF transpondéry EM4x02

Čipy, o kterých bude řeč, pracují v pásmu nízkých frekvencí. Konkrétně v rozsahu 100–150 kHz. Jedná se o jednu z historicky nejstarších kategorií RFID, o které se všeobecně ví, že nějaké zázraky na poli bezpečnosti tu čekat nemůžeme. Nicméně jisté rozdíly, i když občas diskutabilní, zde přeci jen najít lze. Zatímco například čipy používané v současných imobilizérech osobních aut obvykle implementují alespoň nepovedenou proudovou šifru (viz ST 6/2005), tak čip typu EM4x02 představuje v podstatě jen sériovou paměť s kapacitou 64 bitů a konstantním obsahem.

Obsah a struktura paměti je na *obr. 1*. Jakmile se čip dostane do správného pole čtečky, začne vysílat obsah své paměti coby 64b binární řetězec počínaje indexem 1 a konče pozicí 64. Tuto sekvenci pak opakuje, dokud pole čtečky nezmizí. Pro vlastní přenos se stejně jako u čipů v pásmu HF používá zátěžová modulace. Obvykle je použit kód Manchester bez pomocné nosné. Kromě něho přicházejí v úvahu ještě další dvě kódová schémata. Ani jedno z nich však nemá přenos kryptograficky chránit, takže se jimi zde zabývat nemusíme. Stačí konstatování, že jsou veřejně k dispozici [1]. O interpretaci vysílaných dat se čip nestará, to je věcí čtecího terminálu. Z *obr. 1* vidíme, že blok začíná devítibitovou hlavičkou, která je v celé posloupnosti jedinečná. To je dáno použitím sudých řádkových (R_0 až R_9) a sloupcových (C_0 až C_3) parit chránících datovou matici ($D_{i,j}$). Většina čteček se chová tak, že po kontrole integrity (nejedná se ovšem o kryptografickou integritu, účelem je jen detekce chyb v přenosu) zpracuje datovou matici do podoby řetězce délky 5 B, který coby sériové číslo čipu předá na svůj výstup. Odtud si ho vyzvednou další komponenty systému (řízení zámků, atp.). Prakticky jsme se setkali se dvěma drobně odlišnými prezentacemi datových bitů, jak ukazuje *obr. 1*. Sestavené bajty pak byly v obou případech čteny tak, že směr zleva doprava (též od nižší adresy k vyšší) odpovídá v tabulce směru shora dolů. Pro úplnost dodejme, že komunikační kanál ve směru čtečka → čip zde nepopisujeme ze zjevného důvodu – žádný není.

pozice bitu	+0	+1	+2	+3	+4	prezentace A	prezentace B
0	-	1	1	1	1	-	-
5	1	1	1	1	1		
10	$D_{0,0}$	$D_{0,1}$	$D_{0,2}$	$D_{0,3}$	R_0	$D_{1,3} \dots D_{0,3} \dots D_{0,0}$	$D_{0,0} \dots D_{1,0} \dots D_{1,3}$
15	$D_{1,0}$	$D_{1,1}$	$D_{1,2}$	$D_{1,3}$	R_1		
20	$D_{2,0}$	$D_{2,1}$	$D_{2,2}$	$D_{2,3}$	R_2	$D_{3,3} \dots D_{2,3} \dots D_{2,0}$	$D_{2,0} \dots D_{3,0} \dots D_{3,3}$
25	$D_{3,0}$	$D_{3,1}$	$D_{3,2}$	$D_{3,3}$	R_3		
30	$D_{4,0}$	$D_{4,1}$	$D_{4,2}$	$D_{4,3}$	R_4	$D_{5,3} \dots D_{4,3} \dots D_{4,0}$	$D_{4,0} \dots D_{5,0} \dots D_{5,3}$
35	$D_{5,0}$	$D_{5,1}$	$D_{5,2}$	$D_{5,3}$	R_5		
40	$D_{6,0}$	$D_{6,1}$	$D_{6,2}$	$D_{6,3}$	R_6	$D_{7,3} \dots D_{6,3} \dots D_{6,0}$	$D_{6,0} \dots D_{7,0} \dots D_{7,3}$
45	$D_{7,0}$	$D_{7,1}$	$D_{7,2}$	$D_{7,3}$	R_7		
50	$D_{8,0}$	$D_{8,1}$	$D_{8,2}$	$D_{8,3}$	R_8	$D_{9,3} \dots D_{8,3} \dots D_{8,0}$	$D_{8,0} \dots D_{9,0} \dots D_{9,3}$
55	$D_{9,0}$	$D_{9,1}$	$D_{9,2}$	$D_{9,3}$	R_9		
60	C_0	C_1	C_2	C_3	0	-	-

Obr. 1 Struktura 64b řetězce vysílaného čipem EM4x02



Obr. 2 Zlodějka pro pásmo LF

Zlodějka za 12 dolarů

Jak jinak nazvat zařízení velikosti mobilního telefonu, které při přiblížení k výše popsanému typu čipu přečte a uloží obsah jeho paměti, aby ho potom kdykoliv později aktivně přehrálo do libovolné čtečky? Z elektronického hlediska přitom není překvapující, že něco takového lze sestrojit. Překvapující je, jak málo si toho jsou pašáci vědomi. Na *obr. 2* proto ukazujeme funkční exemplář, který sestavil náš spolupracovník Tomáš Volyňský volně podle návodu Jonathana Westhuese [2]. Originální návrh byl určen pro jiné čipy, které se pašáci snaží cpát lidem dokonce doslova pod kůži (viz [2]). Jeho přizpůsobení pro EM4x02 je otázkou úpravy obslužného programu pro vestavěný procesor PIC16F628. Tím jsou realizovány dva základní režimy – čtečka a emulátor. Coby čtečka generuje procesor základní nosnou 125 kHz, kterou přes dvojčinný emitorový sledovač budí feritovou anténu v sériové rezonanci. Odpověď čipu v poli antény je čtena přes diodový detektor (demodulátor AM) a s využitím vestavěného komparátoru programově zpracována. V režimu emulátoru se obvod antény mění na paralelní a přes vestavěný komparátor procesor sleduje nosnou čtečky. Jakmile ji zachytí, přejde do zátěžové modulace (pomocí už zmíněného sledovače) podle dříve zachycených dat. Uvedené zařízení patří do kategorie „SW rádio“, neboť mnoho věcí lze řídit a měnit vhodným programem. V laboratoři RFID s ním proto mimo jiné lze dobře studovat i všelijaké svérázné protokoly složitějších čipů (imobilizéry, atp.).

Závěr

EM4x02 je jednoduchý identifikační čip RFID v pásmu LF. Samo o sobě na něm nic špatného není. Jistě existují bezpečnostně nenáročné aplikace, kde se s výhodou dobře uplatní – například označování stáda dobytku. Průšvih ovšem nastává v okamžiku, kdy ho nějaký pašák použije k řízení přístupu do garáží, domů či kanceláří. Hrozba, že si někdo postaví popsanou zlodějku, se kterou pak někomu pohodlně ukradne klíče z uzavřené kabelky, je totiž zjevná. Z vlastní zkušenosti přitom víme, že bezpečnost RFID je to poslední, na co běžný občan pomyslí, když najde v garáži vykradené auto nebo když mu zmizí věci z komory. To jsme zde ještě nepsali o specializované technice, o které lze uvažovat, známe-li přesně scénář a situaci útoku. Potom lze postupovat buď mnohem agresivněji (vhodnou zlodějku umístit přímo do blízkosti originálního čtecího panelu u vchodu či vjezdu), nebo pro změnu méně technicky náročně. Příště si ukážeme, jak lze popsané čipy snadno emulovat, aniž bychom museli stavět jakékoliv speciální zařízení.

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

LITERATURA

[1] H4102 – Read Only Contactless Identification Device, EM Microelectronic-Marin SA, SWATCH Group, 2000

[2] http://cq.cx/vchdiy.pl

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