Bezkontaktní chytré karty

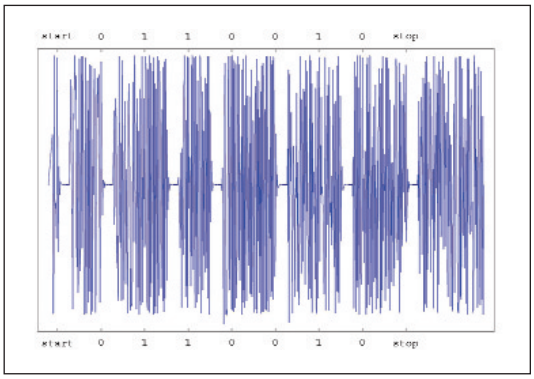
V praxi se používá mnoho pasivních bezkontaktních zařízení, jejichž účelem je pouze nést a předat nějaký krátký, předem naprogramovaný řetězec znaků. Řízení přístupu je přitom velmi jednoduché nebo vůbec žádné. Často pouze nahrazují nespolehlivé štítky s čárovými kódy, takže bezpečnost tu není primární. I zde sice hrozí například útoky známou technikou vkládání nežádoucích příkazů SQL, ale těm se tu věnovat nechceme. Nás zajímají karty, které jsou schopny provádět kryptografické operace v podobném rozsahu jako dnes již klasické karty s kontaktním rozhraním podle standardu ISO 7816. Budeme jim říkat bezkontaktní chytré karty.

Standardy a aplikace

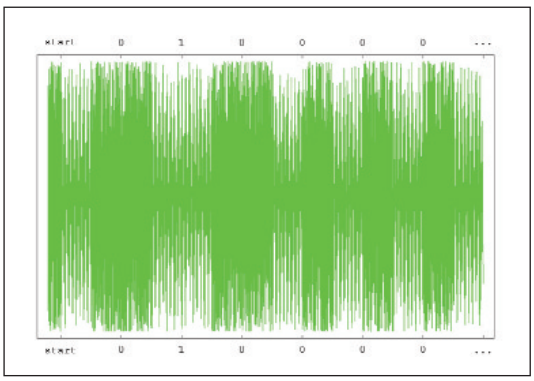
S bezkontaktními chytrými kartami se dnes setkáme například v roli platebních karet nebo elektronických pasů s biometrickými údaji. Hlavní motivací pro jejich zavedení ovšem často není zvětšení komunikační vzdálenosti, nýbrž zvýšení spolehlivosti eliminací poruchových kontaktů. Napájecí a datové rozhraní těchto karet je popsáno ve standardu ISO 14443, který je dostupný i jako soubor českých technických norem ČSN ISO/IEC 14443-1, 2, 3, 4. Standard rozeznává dva příbuzné typy karet, které označuje písmeny A a B. Odlišnosti jsou v detailech provedení rádiové komunikace a v řídicích příkazech. Konkrétní příkazy pro přístup k datům a kryptografickým operacím však tyto standardy nepopisují, neboť zde se předpokládá využití bohaté základny definované v ISO 7816-3 a vyšších. Formalizace tohoto přístupu dosud chybí, což pak v praxi často vede k nutnosti uplatnění metody pokus-omyl, ale idea je jasná – bezkontaktní a kontaktní chytré karty by se na aplikační úrovni měly chovat stejně, bez ohledu na technologii použitou v nižších vrstvách. Pěkným příkladem jsou již zmíněné elektronické pasy, se kterými lze s jistým úsilím pracovat jako s „obyčejnou“ čipovou kartou typu SIM.

Základy komunikace

Chytré karty podle ISO 14443 jsou pasivní, čili nemají vlastní zdroj elektrické energie. Napájení jim obstarává elektromagnetické pole terminálu, které je zároveň komunikačním médiem. Tomuto principu pak podléhá vše ostatní včetně antény. Na soustavu tvořenou anténou terminálu, anténou karty a prostředím v jejich okolí je zde nahlíženo spíše jako na vysokofrekvenční transformátor. Množství energie, které se v této soustavě přenese z primárního okruhu terminálu do sekundárního okruhu karty, je zhruba nepřímo úměrné třetí mocnině vzdálenosti mezi oběma anténami (hranice je běžně kolem 10 cm). Svou roli hraje i jejich rozměr a tvar, který je na straně karty jasně limitován, a ani na straně terminálu se to s ním příliš nepřehání. Z hlediska přenosu signálu na větší vzdálenosti jsou pak navržené antény velmi nevhodné, což je zároveň vítaným vedlejším opatřením proti odposlechu.



Obr. 1 Přenos dat z terminálu do karty (REQA)



Obr. 2 Přenos dat z karty do terminálu (ATQA)

Pro napájení karet typu A i B vysílá terminál základní sinusový signál o frekvenci 13,56 MHz. Tentýž signál s vhodnou modulací je použit i pro datovou komunikaci. Zde se typy A a B poněkud liší, my se zaměříme na typ A, který odpovídá i českým pasům. Pro předávání dat terminálu kartě jsou tato nejprve kódována modifikovanou Millerovou metodou, jejíž výsledek je poté amplitudově modulován na základní nosnou 13,56 MHz. Hloubka modulace je 100 %, rychlost přenosu cca 106 kbit/s (bitový rámec trvá 128 period základní nosné). Podrobnosti viz ISO 14443-2. Ukázku přenosu příkazu REQA, kterým terminál periodicky vyzývá nové karty ve svém poli, aby se ohlásily a připravily na proceduru výběru, vidíme na *obr. 1*. Značky na rámečku ukazují začátky bitových rámců a návěští popisují jejich význam.

Obdobně jako kontaktní karty vysílají ty bezkontaktní jen tehdy, jsou-li k tomu vyzvány. Pro přenos dat do terminálu je použita technika zvaná modulace zátěží. Při ní rozlišujeme dva základní stavy: Jeden, kdy karta svou anténu zatěžuje pouze běžnou spotřebou, a druhý, kdy ji účelově zatěžuje pomocným sinusovým průběhem o frekvenci 13,56 MHz / 16 = 847,5 kHz. Pomocí těchto dvou stavů jsou potom kódována a vysílána data pro terminál. Z jeho pohledu existují v zásadě dva způsoby jak tento přenos detekovat a zpracovat, přičemž oba v podstatě modelují tutéž fyzikální realitu. Většinou se vychází z již zmíněné představy vysokofrekvenčního transformátoru, kde se zatěžování sekundárního okruhu karty známým způsobem promítá do chování primárního okruhu terminálu. Útočník aktivně zasahující do komunikace z větší vzdálenosti může zase využít toho, že proměnná zátěž antény karty podle Maxwellových rovnic sama způsobuje sekundární indukci elektromagnetické vlny odpovídající amplitudově modulovanému signálu původní nosné. Bylo experimentálně potvrzeno, že aktivní vyslání správné vlny je pro běžný terminál nerozlišitelné od zátěžově modulovaného signálu karty. Modulující sinusový signál má konstantní frekvenci 847,5 kHz, což v obou případech znamená, že vysílání karty lze detekovat i simulovat přes výskyt symetrických produktů amplitudové modulace o frekvencích 13,56 MHz ± 847,5 kHz. Příklad přenosu části rámce odpovědi ATQA, kterou karta reaguje na předchozí REQA terminálu, vidíme s jistým úsilím na *obr. 2*. Kódování dat se opírá o to, ve které polovině bitového rámce dochází k zátěži pomocným signálem. Základní rychlost přenosu je opět cca 106 kbit/s.

Závěr

Představili jsme si základní radioelektronické principy bezkontaktních chytrých karet. Přitom jsme si naznačili, že i přes nespornou technickou složitost těchto zařízení nelze vyloučit úspěšné odposlouchávání přenášené komunikace a dokonce ani případné aktivní zásahy do ní. Je toho pochopitelně mnoho, co by k tomuto tématu mohlo a mělo být řečeno, počínaje rozdílnými možnosti v dálkovém příjmu silnějšího signálu terminálu a poměrně slabého vysílání karty až po aktivní emulaci karty. Na řadu věcí postupně dojdeme při ukázkách konkrétních aplikací, jakou jsou třeba právě elektronické pasy.

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