Bezkontaktní karty MIFARE

Karty typu MIFARE [1], kterým se budeme věnovat, jsou dnes už spíš klasickým než přímo vzorovým příkladem chytrých karet. Jejich základní komunikační rozhraní je kompatibilní se standardem ISO 14443-A, který jsme si představili minule. Nad tímto rozhraním však už nenajdeme pokračování dle ISO 7816, ale příkazy proprietárního aplikačního protokolu MIFARE, který si společně s algoritmem CRYPTO1 firma Philips dobře hlídá. Kromě podnikových docházkových systémů se s technologií MIFARE setkáme například při placení za služby hromadné dopravy některých měst České republiky.

Paměťová karta „plus“

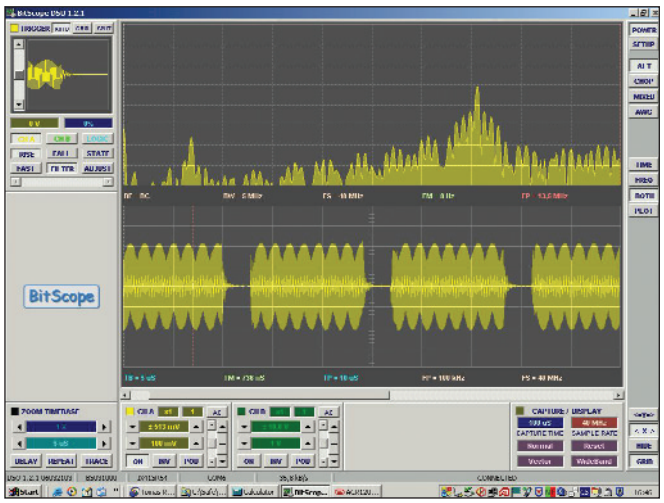
V praxi se můžeme setkat s kartami MIFARE o kapacitě 1 KB nebo 4 KB. Dostupná paměť se dělí do bloků po 16 bajtech a tyto bloky se dále sdružují do takzvaných sektorů. Na rozdíl od čistě paměťových karet řídí MIFARE přístup k paměťovým blokům na základě prokázání znalosti příslušného kryptografického klíče. Zde je použita varianta tříprůchodové autentizace dle ISO 9798-2, při níž se zároveň dohodnou klíče pro šifrování komunikace mezi kartou a terminálem. Primární autentizační klíč má sice jen 48 bitů a hlavní kryptografický algoritmus s názvem CRYPTO1 je neveřejný, ale i tak můžeme považovat příchod MIFARE za slušný úspěch.

Volné datové bloky karty je možné využít buď pro ukládání libovolných 16B řetězců, nebo jako čítače nějakých jednotek (peněz, telefonních impulzů, jízdenek, atp.). To, jaké operace jsou s blokem povoleny, popisuje v rámci jeho sektoru speciální blok označovaný jako zavaděč sektoru. V případě 1KB karty tvoří sektor (vč. bloku zavaděče) celkem čtyři paměťové bloky. V zavaděči sektoru mohou být současně uloženy až dva 48b klíče označované písmeny A a B. Dále je zde pole příznaků, které pro každý datový blok sektoru zvlášť předepisuje jedno z osmi možných řízení přístupu (*tabulka 1*). Například konfigurace s indexem 0, označovaná též jako transportní, dovoluje všechny bajtově i čítačově orientované operace na základě prokázání znalosti klíče A nebo B (pro B jsou zde výjimky, které pro přehlednost vynecháme). Podobná tabulka pro řízení přístupu platí i pro samotný blok zavaděče.

Blok 0 sektoru 0 má speciální význam, neboť obsahuje pevné údaje výrobce, kde je mimo jiné i 4B sériové číslo karty. Ostatní datové bloky karty jsou již návrhářům aplikací plně k dispozici. Kapacitu karty je přitom výhodné rozdělit po sektorech, neboť každý sektor definuje pro řízení přístupu ke svým blokům své vlastní klíče A a B a tím jednotlivé aplikace kryptograficky odděluje.

Tabulka 1 Přístupové podmínky pro operace s paměťovými bloky

Index konfigurace	Typ přístupu			
	read	write	increment	decrement, transfer, restore
0	klíč A|B	klíč A|B	klíč A|B	klíč A|B
1	klíč A|B	nelze	nelze	nelze
2	klíč A|B	klíč B	nelze	nelze
3	klíč A|B	klíč B	klíč B	klíč A|B
4	klíč A|B	nelze	nelze	klíč A|B
5	klíč B	klíč B	nelze	nelze
6	klíč B	nelze	nelze	nelze
7	nelze	nelze	nelze	nelze



Obr. 1 Záchyt komunikace od terminálu do karty

Ukázkové faux pas

… aneb pár tipů jak to nedělat. Viděli jsme například systém elektronického vrátného, kterého z celé karty zajímalo pouze volně přístupné sériové číslo z bloku 0 sektoru 0. Pokud bylo konkrétní číslo v systému registrováno, vstup byl povolen. Co k tomu dodat? Snad jen malou perličku. Zdálo by se, že pro výrobu emulátoru-padělku se útočník musí dostat buď přímo ke kartě oběti, nebo musí získat seznam registrovaných čísel jinak. S dálkovým odposlechem dat vysílaných kartou bychom příliš nepočítali, neboť tento signál je fyzikálně obtížné kvalitně zachytit na vzdálenost delší než cca metry (i to ale může stačit). Jenže ono sériové číslo vystupuje zároveň jako identifikátor karty během tzv. antikolizní procedury, která je povinná a s níž si terminál z množiny čipů v dosahu vybírá, s kým bude komunikovat. I zde sice nejprve vysílá svůj identifikátor (slabě) karta, ale podle standardního postupu dle ISO 14443-A jej terminál alespoň jednou (silně) zopakuje. Zachycení signálu terminálu je přitom s kvalitními přístroji možné na vzdálenost řádově desítek metrů! Profil signálu terminálu ilustruje amatérský záchyt na *obrázku 1*, který byl čistě pro demonstrační účely vytvořen v blízkosti terminálu pomocí obdélníkové antény v podobě cívky 9 cm x 5,6 cm o pěti závitech laděné jako paralelní rezonanční obvod podle doporučení dr. Lee [2]. Lze soudit, že motivovaný útočník by s mnohem dokonalejšími pomůckami dokázal získat de facto přístupové kódy do takto „střežených“ prostor například i z vedlejšího bytu či kanceláře.

Stává se také, že kdosi zapomene změnit tovární hodnoty klíčů. Výrobce s nimi sice dělá drahoty, ale implicitní hodnota A0A1A2A3A4A5 pro klíč A, respektive B0B1B2B3B4B5 pro klíč B jistě není to pravé.

Závěr

Pomineme-li délku klíče, neveřejný algoritmus a prakticky neznámé prvky ochrany proti postranním kanálům, jsou karty MIFARE robustním, snadno uchopitelným a aplikovatelným prostředkem, který právem nalézá svá dobrá uplatnění v bezpečnostních systémech „běžné spotřeby“. Na druhou stranu je nezbytné zdůraznit, že bohužel stále existují exponované systémy, které tyto karty využívají až nezodpovědně špatným způsobem.

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

LITERATURA

[1] MIFARE MF1 IC S50, Philips Semiconductors, Rev. 5.1, May 2005

[2] Lee, Y.: Antenna Circuit Design for RFID Applications, AN 710, Microchip Tech. Inc., 2003

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