Bezpečněji s MIFARE

Bezkontaktním kartám MIFARE a základům RFID (Radio Frequency Identification) na bázi standardu ISO 14443 jsme se již věnovali v ST 1 a 2/2007. Mezitím se objevilo několik systémů využívajících tuto technologii více či méně nevhodným způsobem. Nabízíme proto pár postřehů jak je vylepšit.

Autentizační protokol

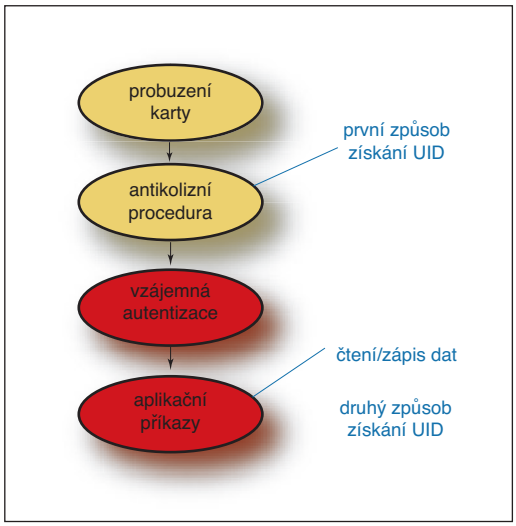
Podle sdělení výrobce je pro vzájemnou autentizaci karty a terminálu použit trojcestný protokol. V jeho průběhu je rovněž dohodnut dočasný symetrický klíč, kterým je chráněna důvěrnost a integrita dat vyměňovaných mezi kartou a terminálem. Další detaily kromě toho, že bylo vycházeno z obecného standardu ISO 9798-2, již nejsou veřejně k dispozici. Utajen je i hlavní šifrovací algoritmus Crypto1. Celý protokol včetně navazujících kryptografických ochran zpráv je k dispozici například prostřednictvím komunikačního obvodu MF RC531 [2]. Vývojový diagram typického sezení s kartou je na *obr. 1* (podrobnosti viz [1] a [2]).

Autentizace původu zpráv

Z deklarovaných vlastností zmíněného protokolu vidíme, že ho můžeme snadno rozšířit na schéma autentizace původu zpráv. Předpokládejme situaci, kdy terminál kartu úspěšně vybere, projde autentizačním protokolem a přečte data uložená v určitém datovém bloku nějakého sektoru. Potom lze předpokládat, že karta disponuje přístupovým klíčem natolik, že byla schopna se s ním autentizovat a dohodnout si dočasný klíč. Tímto dočasným klíčem potom byla schopna zašifrovat a integritně ochránit předaná data. Z pohledu praktické bezpečnosti můžeme tedy předpokládat, že karta byla schopna přístupovým klíčem autentizovat původ přečtených dat terminálu. Získaná data tak můžeme považovat například za důvěryhodně předané jméno držitele karty, atp.

V běžných aplikacích se zapomíná na to, že i když se jedná o čtecí klíč (zápisová práva mu nemusí být přidělena), je jeho utajení naprosto zásadní pro bezpečnost celého systému. Útočník, který bude chtít předstírat třeba identitu hotelového hosta Bedřicha Smolaře, totiž nemusí vůbec znát nějaký speciální klíč, aby na svou novou, prázdnou kartu zapsal třeba Bedřichovo jméno. Hotelový systém řízení přístupu ovšem s kartou nebude komunikovat, dokud na ní nebude nastaven ještě správný čtecí (čili zde autentizační) klíč. Pokud je však k ochraně tohoto klíče přistupováno laxně s tím, že je přeci „jen pro čtení“, bude se za chvilku pan Bedřich divit...

Již jsme naznačili, že k předmětnému datovému bloku bude kromě autentizačního klíče potřeba nějak přiřadit i (nejlépe jiný, nezávislý) klíč pro zápis. Abychom se vyhnuli útokům založeným na přejmenování karty a jasně zaručili, že zapisující strana musí autentizační klíč znát, je vhodné zvolit tuto konstrukci: V běžné konfiguraci jsou všechny datové bloky pouze pro čtení. Zápisovým klíčem lze měnit jen hodnotu zavaděče sektoru, ve kterém jsou uloženy konfigurace přístupových práv a hodnoty klíčů. Bude-li chtít někdo změnit například jméno držitele, musí si nejprve pomocí zápisu do zavaděče přidělit příslušné zápisové oprávnění. Tím však zároveň povinně (vyplývá z architektury karty) přepíše i hodnotu autentizačního klíče. Jakmile změnu dat dokončí, je rozumné další zápis dat změnou zavaděče opět zakázat. Nejpozději v tomto okamžiku však musí být vrácena zpět i původní hodnota autentizačního klíče. Jinak by karta podle výše popsaného paradigmatu byla odmítnuta. Triviálně tak opět dospíváme k prakticky dostačujícímu ujištění, že zapisující strana musela autentizační klíč znát.



Obr. 1 Typické sezení s MIFARE

Sériové číslo bezpečněji

Často se setkáme i se situací, kdy systém od čtečky striktně očekává, že po zachycení karty automaticky vrátí binární řetězec pevné délky. Ten je pak považován za číslo karty. Jedná se zejména o aplikace vyvinuté původně pro jednoduché čipy v pásmu LF, které nic lepšího neuměly. Skutečnost, že MIFARE tak omezená není, je bohužel v praxi slabým důvodem k tomu celý systém měnit. Budiž, i za takto špatných podmínek můžeme udělat alespoň něco. Existují totiž dva způsoby, jak sériové číslo (UID) karty získat. První spočívá v jeho zachycení v průběhu antikolizní procedury, viz *obr. 1*. Výhodou je, že čtečka může být po elektronické stránce velmi jednoduchá, zejména nemusí obsahovat obvod, jako je MF RC531, neboť s aplikačním protokolem karty nepřijde do styku. Nevýhodou je, že lze neméně snadno zkonstruovat padělek původní karty, který ve správný okamžik odvysílá správný řetězec. Blíže o útocích přes emulaci karty viz ST 1/2007 a 2/2007. Chceme-li padělání karet co nejvíc ztížit, je vhodné důsledně trvat na získání sériového čísla druhým způsobem, a sice jeho čtením z bloku 0 sektoru 0. Čtečka se tím zkomplikuje, avšak zároveň s ní musí i emulátor útočníka pokrývat významně větší část *obr. 1*. Vzhledem k neveřejným kryptoschématům to bude podstatně větší oříšek než při obcházení předchozího způsobu. Z hlediska kryptografie pochopitelně nelze takové „bastlení“ považovat za vzor, avšak z hlediska praxe je to podstatně lepší než nedělat nic.

Závěr

Srovnáme-li MIFARE s nastupující generací bezkontaktních či rovnou duálních chytrých karet, nelze se ubránit dojmu, že tato platforma je už daleko za zenitem. Mimo jiné s ohledem na délku klíče 48 bitů. Přesto se, zejména v řadě přístupových systémů, dodnes nasazuje, a to dokonce často coby horká novinka. Důvody jsou pochopitelně provozně-ekonomické a s kryptologií nemají nic společného. Na druhou stranu zmíněné chytré karty často nabízejí režim, ve kterém MIFARE emulují. Pořízením kvalitnějších karet a jejich dočasným provozem v kompatibilním módu si tak lze vytvořit jistý můstek, který postupně umožní přejít k podstatně silnějším kryptografickým prostředkům. Do té doby můžeme s rozumně (!) použitým MIFARE snad vydržet.

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] MIFARE MF RC531 – ISO 14443 Reader IC, Philips Sem., Rev. 3.2, April 2001

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