Elektronický cestovní pas: Komunikační rozhraní

Elektronické pasy jsou občanům České republiky vydávány zhruba od poloviny loňského roku. Jedná se přitom nejen o slibný instrument mezinárodní bezpečnosti, ale i o ukázkovou moderní aplikaci bezkontaktních chytrých karet (viz ST 1/2007). Příslušné standardy a doporučení má na starosti Mezinárodní organizace pro civilní letectví – ICAO, základem je standard číslo 9303. Řada materiálů je volně ke stažení na webu mrtd.icao.int.

Kříženec ISO 14443 a 7816

Pro komunikaci s pasem potřebujeme v první řadě terminál podporující ISO 14443. Pas vydaný v ČR, se kterým jsme experimentovali, odpovídal konkrétně typu A s náhodně volenou hodnotou identifikátoru UID. Toto opatření zabraňuje sledování pohybu daného pasu přes pevné UID. Příkazy ve formě bloků APDU standardu ISO 7816 a odpovědi na ně jsou pak přenášeny v takzvaných I-blocích poloduplexního protokolu definovaného v části 7 ISO 14443-4. Svým způsobem jde o průkopnický přístup, který dosud není formálně podchycen. V případě nejasností je nutné postupovat dle jistých provizorních doporučení ICAO. Ilustrační příklad diskutovaného zapouzdřování je možné vidět i v záznamu našeho experimentu níže.

Zajímáme-li se o neautorizovanou rádiovou komunikaci či její odposlech, je nutné rozlišovat situace uvedené v *tabulce 1*. Například útok vyžadující aktivní komunikaci útočníka s pasem je proveditelný jen na poměrně blízkou vzdálenost a s jistým hygienickým rizikem. V experimentu na hranici 25 cm [3] bylo pole tak silné, že poškodilo záznam na disku vedle stojícího počítače. V hackerské hantýrce se jim proto říká „drcavé útoky“ (bumping attacks), neboť jedna z možností, jak se dostat se čtečkou dostatečně blízko, je do oběti prostě „omylem“ drcnout. Značně příznivější jsou naproti tomu možnosti dálkové aktivní komunikace s terminálem metodou emulace postranních pásem (viz ST 1/2007).

Hledáme pas v poli

Ve zprávě pro spotřebitele [4] jsme uvedli hypotézu, že i přes všechna kvalitní bezpečnostní opatření, která jsou v elektronických pasech implementována, zde existuje potenciální protokolová slabina umožňující i bez znalosti jakýchkoliv tajných klíčů detekovat přítomnost pasu v elektromagnetickém poli terminálu. Následující experiment s pasem jednoho našince tuto hypotézu potvrzuje.

SEL ID: 08 94 34 37
T_1: E0 50 BC A5
P_1: 0E 78 77 A5 02 80 91 E1 65 77 01 02 01 01 D0 4A
T_2: 02 **00 A4 04 0C 07 A0 00 00 02 47 10 01** 98 B8
P_2: 02 **90 00** F1 09
T_3: 03 **00 A4 02 0C 02 01 1E** A7 9B
P_3: 03 **69 82** 27 5F

Vidíme typický začátek komunikace s pasem. Zapsané řetězce jsou dále skládány do tzv. standardních rámců a vysílány dle principů ISO 14443-A (viz ST 1/2007). Zapouzdřené příkazy a odpovědi dle ISO 7816 jsou vyznačeny tučně. Zdůrazněme, že k této komunikaci nebylo zapotřebí znát žádná tajemství, stačilo mít pas v dosahu pole terminálu. Začínáme aktivací pasu a provedením antikolizního výběru. Vidíme, že pas si vygeneroval náhodný identifikátor s efektivní délkou 3 bajty (první bajt má hodnotu danou standardem). Dále terminál (T) zasílá příkaz RATS inicializující mj. vyšší vrstvy protokolu ISO 14443-A a pas (P) odpovídá konfigurační strukturou ATS (obdoba ATR pro kontaktní karty) doplněnou polem historických znaků (význam jako v ISO 7816). Dále následuje výběr aplikace elektronického pasu příkazem SELECT AID, pas hlásí úspěch návratovým kódem 90 00. Poté zkoušíme vybrat soubor EF.COM. To už pas odmítá a návratovým kódem 69 82 hlásí nutnost provedení kryptografické autentizační procedury.

Pokud by zařízením v poli terminálu nebyl pas, vypadala by uvedená komunikace s vysokou pravděpodobností jinak. Předně by asi nebyla k dispozici požadovaná aplikace ICAO s kódem A0 00 00 02 47 10 01, takže v kroku P2 by místo úspěchu byla hlášena chyba. Rovněž tak (a tím spíš) by se zařízení v kroku P3 nedožadovalo provedení autentizace, ale hlásilo by nějakou jinou chybu. Na tomto pozorování lze založit detekční proceduru, která s vysokou pravděpodobností správně odliší pas (byť naprosto neznámý) od jiné bezkontaktní čipové karty. S ohledem na *tabulku 1* to sice neznamená žádnou katastrofu, ale, jak jsme už předeslali v [4], je dobré to vědět. Dodejme, že uvedená vlastnost se týká celosvětově všech pasů vydávaných dle standardu ICAO 9303.

Obr. 1 Experimentální komunikace s tuzemským pasem

Tabulka 1 Aktuální meze rádiové komunikace s pasem

aktivní komunikace s pasem	desítky cm
odposlech – terminál i pas	jednotky m
odposlech – pouze terminál	desítky m
aktivní komunikace s terminálem	desítky m

Závěr

Představili jsme si fenomén současné doby – elektronický pas z pohledu komunikačního rozhraní. Ukázali jsme si, že přes všechnu péči se sem vloudila drobná slabina, kterou je vhodné mít na zřeteli, zejména pokud u sebe máme pas v prostředích, jako jsou kluby, kina, trhy, pláže, atp. Ve všech těchto případech může pasuchtivý zloděj své potenciální oběti napřed nenápadně oskenovat a potom jít na jisto. Na druhou stranu nechceme celou záležitost nijak přefukovat – stačí o tom vědět a dávat pozor. Příště se podíváme na specifické bezpečnostní prvky českých pasů.

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

LITERATURA

[1] Finke, T., Kelter, H.: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems

[2] Kfir, Z., Wool, A.: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, IACR ePrint, Report 2005/052

[3] Kirschenbaum, I., Wool, A.: How to Build a Low-Cost, Extended-Range RFID Skimmer, USENIX 2006

[4] Klíma, V., Rosa, T.: Diskuze o bezpečnosti českých biometrických pasů, Sdružení ochrany spotřebitelů, http://www.spotrebitele.info/clanek.shtml?x=2222544

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