Elektronický cestovní pas: BAC

Z technického hlediska je elektronický pas bezkontaktní čipová karta, která ochotně komunikuje s jakýmkoliv zařízením, které je v účinném dosahu a ovládá příslušný protokol (viz ST 3/2007). Osobní údaje držitele jsou na této kartě uloženy v podobě běžných datových souborů dle ISO 7816. Jako ochranu proti jejich zcizení navrhla ICAO doplňkovou metodu BAC (Basic Access Control), která umožňuje vzájemnou autentizaci terminálu a karty včetně dohody klíčů pro zabezpečení rádiové komunikace. Použití BAC ve světě je velmi populární, v členských zemích EU je pro vydávané pasy povinné. S ohledem na výčet států a míst, kde je zapotřebí elektronické pasy akceptovat, bylo klíčové hospodářství poněkud zjednodušeno. Heslo pro BAC je nyní tvořeno přímo z údajů vytištěných v pasu. Tím je přístup k chráněným souborům a funkcím umožněn každému, kdo má možnost nahlédnout do „papírové“ části dokladu.

```
T4:  02 00 84 00 00 08 2F EC
P4:  02 FE 59 BF 3C 81 BB E3 DB 90 00 B2 12
T5:  03 00 82 00 00 28 CE 69 96 64 EF 9D 6D 3E 81 7C 2D B2 9A D0 09 EB E9 29
     E6 D9 0E DD C1 DA D3 CF AF 16 8F 9A 0E 39 F9 39 41 7C CA F3 8C D3 28 8E
     96
P5:  03 90 5A 08 CB 8C 82 E6 5D D3 A6 55 AF 6B 23 78 A7 B8 41 C2 85 3F 89 66
     F5 8C 6F 94 52 23 D0 7E 2E 8F 50 5A BC 1C 04 03 31 90 00 68 2C
```

Obr. 1 Výměna zpráv při autentizaci pro BAC

Postup a slabiny

Tříprůchodovou autentizační proceduru s dohodou na klíči zahajuje terminál obvykle v okamžiku, kdy už ví, že komunikuje s pasem vyžadujícím BAC. Tedy například v tom momentě, kdy naše ukázková výměna zpráv v minulém dílu končila. Tomu odpovídá i číslování zpráv na *obr. 1*. Bloky APDU podle ISO 7816 jsou vyznačeny tučně, jejich datová pole jsou zvýrazněna modrou barvou. K provedení autentizace bude terminál potřebovat primární heslo *W*. To získá zřetězením ASCII zápisů těchto položek: číslo pasu, datum narození držitele, datum exspirace. Číslo pasu je případně doplněno znaky „<“ na minimální délku 9 znaků, obě data jsou ve formátu YYMMDD. Položky jsou spojeny v uvedeném pořadí včetně jejich kontrolních číslic (podle veřejného algoritmu). Podrobnosti a příklady viz [1]. Nyní je vypočtena hodnota *S* jako prvních 16 B zleva z hodnoty SHA–1(*W*), tj. *S*=SHA–1(*W*)[1..16]. S jejím využitím jsou odvozeny dva 16B klíče K_E a K_M jako K_E = (SHA-1(*S*||00 00 00 01))[1..16]*$\boldsymbol{B}$ a K_M = (SHA-1(*S*||00 00 00 02))[1..16]*$\boldsymbol{B}$. Násobení vhodnou binární maticí $\boldsymbol{B}$ typu 128x128 dosazuje paritní bity pro DES (některé jeho implementace to nevyžadují). V BAC je použit dvouklíčový algoritmus 3DES (Triple DES) jednak pro šifrování (s klíčem K_E), jednak pro kontrolní kód MAC (s klíčem K_M).

Příkazem Get Challenge nyní terminál požádá pas o 8B náhodnou výzvu R_P (viz T_4, P_4), sám vygeneruje 8B náhodné číslo R_T a 16B náhodné číslo K_T. Na jejich základě sestaví kryptogram tvořený 8B bloky C_1 až C_5, který v T_5 zašle pasu v příkazu Mutual Authenticate. Bloky C_1 až C_4 tvoří šifrový text 32B zprávy $R_T||R_P||K_T$ šifrované algoritmem 3DES v modu CBC s nulovým inicializačním vektorem s klíčem K_E. Přirozeně zarovnaná zpráva se v tomto případě už před šifrováním nedoplňuje. Blok C_5 je kontrolní kód MAC vypočtený pro zarovnanou zprávu tvořenou bloky šifrového textu $C_1||C_2||C_3||C_4$. Nyní už je (!) vstup doplňován konstantním blokem 80 00 … 00 v délce 8 B, ačkoliv by také nemusel být. Doplněk je podle ISO 9797-1 typ 2, schéma MAC vychází z kombinace algoritmů DES a 3DES v módu CBC, podrobně viz kontrolní příklady v [1] příloze E (doporučujeme pečlivě prostudovat).

Pas u kryptogramu zaslaného v T_5 jednak ověří správnost MAC v C_5, jednak odšifruje C_1 až C_4 a zkontroluje výskyt svého R_P na správném místě (druhý blok otevřeného textu). Poté vygeneruje 16B náhodné číslo K_P, sestaví zprávu $R_P||R_T||K_P$, kterou podle výše uvedeného postupu zašifruje a opatří kódem MAC. Výsledný kryptogram C_1', …, C_5' vrátí v kroku P_5 terminálu, který jej rovněž ověří. Pokud všechny kontroly vyšly, považují se terminál a pas navzájem za autentizované. Navíc si z vyměněných 16B řetězců K_T a K_P spočítají hodnotu $K_T \oplus K_P$, která je výchozím sdíleným tajemstvím pro odvození klíčů navazujícího mechanismu Secure Messaging (viz ISO 7816 a [1]) chránícím důvěrnost a integritu komunikace.

Zjevnou slabinou BAC je nízká entropie primárního hesla. Uvažujeme-li nahodilý drcavý útok (viz ST 3/2007), je síla BAC ještě celkem adekvátní. Proti útoku s využitím zachycené řádné komunikace (například s letištním terminálem) však už tato metoda bude v řadě případů slabá. S ohledem na možnosti odposlechu zmíněné v minulém dílu dodejme, že útočník může hledat *W* hrubou silou už jen na základě odposlechu pouze signálu terminálu. Využije k tomu hodnotu *MAC* u dat v T_5. Získanou hodnotu *W* si může schovat a použít později. Navíc už i samotná hodnota *W* může být pro někoho zajímavá. Útočník může také detekovat, že kdesi v dosahu jeho pasivního přijímače byl zpracován pas se známým heslem (sledovaná osoba prošla turniketem, atp.). Ohledně navazující metody Secure Messaging dodejme, že tato zde chrání důvěrnost jen dat, nikoliv už hlavičky příkazu či statusu odpovědi *SW1SW2* (viz ISO 7816). V odposlechu je proto i bez klíčů vidět, jaké příkazy terminál vydává a jak na ně pas reaguje. Takhle útočník rychle zjistí, zda zachycená komunikace obsahuje požadovaná data a zda má vůbec cenu ji luštit. Patří se uvést, že ICAO si je hlavních slabin BAC vědoma a pro ochranu budoucích (nejpozději od 28. 6. 2009) dat s otisky prstů plánuje zavést metodu rozšířeného řízení přístupu (EAC). Ta však dosud nemá konečnou podobu.

Pozor – soutěž luštitelů!

Příkladem na *obr. 1* možná poněkud riskujeme, neboť dáváme šanci odhalit přístupové heslo pasu použitého v našem experimentu. Tím lze získat číslo dokladu, datum exspirace a datum narození jeho držitele. Ano, to je pravda, a nejen to – my si vás, vážení čtenáři, dokonce dovolujeme vyzvat, abyste to zkusili! Vyhlašujeme soutěž, ve které sedm nejrychlejších luštitelů odměníme celebrováním jejich jména či přezdívky v našem seriálu. Uzávěrka je 31. 7. 2007, úkolem je na naše adresy (na obě dvě) co nejdříve poslat údaje tvořící heslo v příkladu na *obr. 1*. Šlo o český pas osoby starší 15 let. Doporučujeme podívat se na číslování našich pasů, typickou dobu platnosti a uvážit začátek vydávání 1. 9. 2006. Těšíme se na vaše výsledky. Příště se budeme věnovat ochranným prvkům českých pasů založeným na digitálních podpisech.

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

LITERATURA

[1] PKI for Machine Readable Travel Documents offering ICC Read-Only Access, IACO, ver. 1.1, 2004

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