Mikulášská kryptobesídka 2004
6.12. – 7.12.2004

Implementace kryptografického protokolu s využitím mobilní kryptografie*

Petr Švenda
<xsvenda@fi.muni.cz>

http://www.svenda.com/petr/securefw_cz.html

** Příspěvek vznikl na základě diplomové práce vedené V. Matyášem.*

Přehled

I. Prostředí, útoky, pozorování, nápady
   - WBACR AES

II. Stavební prvky protokolu
   - I/O kódování pro CBC
   - WBACR AES hash

III. SEcure AUthenticated Transport protocol
   - autentizační část
   - transportní část

Prostředí pro protokol

- autonomní komunikace aplikací
  - aplikace nese autentizační informace sama
  - autentizace, důvěrnost, čerstvost komunikace
- klient/server (strana B/strana A)
  - server (strana A) „bezpečné" výpočetní prostředí
  - klient (strana B) výpočetní prostředí útočníka
    - čtení/modifikace instrukcí/paměti (disassem., debugger)
- příklady použití:
  - PC/webserver, PC/smart card
  - DRM, malware, patch/plug-in download

Útoky na stranu B

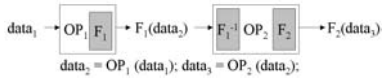
- odhalení citlivých dat
  - šifrovací klíče, zpracovávaná data
- modifikace zpracování
  - protokolu (vždy akceptuje autent. od „A")
  - dat (přijme data od „A")
- využití části kódu ve vlastní režii
  - autentizace vůči „A"
  - přístup k datům mezi A a B
- kritické operace:
  - porovnání, práce s otevřenými daty

White-Box Attack Resistant AES

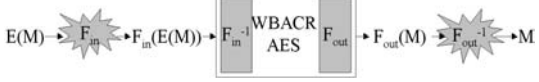
- Chow, Eisen, Johnson, Oorschot [1]
- AES (Rijndael) 128bitů klíč, 128bitů blok
- Běžná implementace AES:
  - klíč + data,
  - operace XOR, maticové násobení …
- WBACR AES:
  - jen data (klíč předem určen)
  - pouze náhledy do předpočtených tabulek T
    - $V_i == 5 \Rightarrow V_{(i+1)} = T[5]$;
    - algoritmus náhledů i tabulky „volně" přístupné

WBACR AES – výhody

- Ukrytí hodnoty používaného klíče



- Oddělitelná šifrovací/dešifrovací část
  - ~ asymetrická kryptografie
- Vstupní a výstupní kódování (IOC)



O co se snažíme?

Máme vhodně chráněnou implementaci blokové šifry (WBACR AES)

Chceme rozšířit její vlastnosti na celý protokol

Pozorování & nápady 1/2

- symetrická vs. asymetrická kryptografie
  - utajení hodnoty klíče (oddělitelnost)
- keksík (random vs. čas, sekvence)
- utajení hodnot klíčů
  - WBACR AES
  - (WBACR DES)
- nezaměnitelné zprávy (B->A za A->B)
  - šifrovat + „směrové" klíče ($K_{A->B} != K_{B->A}$)

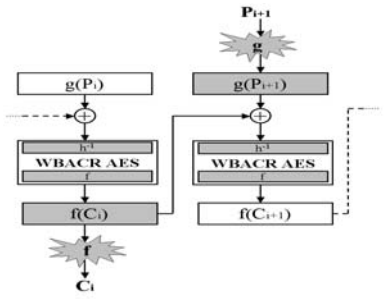
Pozorování & nápady 2/2

- čerstvé zprávy (A->B)
  - $Z_i = E(data)$; $Z_i' = R_i \oplus Z_i$;
  - aktualizace: $R_{i+1} = hash_K(R_i)$;
- důvěrnost/integrita používaných dat
  - mobilní kryptografie [2]
    - OP(data) => OP'(f(data)); f tajné
- nahrazení porovnávacích operací
  - A != A' => hash(A, A') != hash(A, A)
  - výsledek „vhodně" použit na transformaci data
    - A != A' => chybná data

I/O kódování pro CBC 1/2

- problém $F_{out}(C_i) \oplus F_{in}(P_{i+1})$
  - změna kódování ☹
- 3 kódování f, g, h
  - f … výstupní, h … vstupní WBACR AES
  - g … datové, aplikováno libovolně před šifrováním
- $f(C_i) \oplus g(P_{i+1}) = h(C_i \oplus P_{i+1})$
  - n-bitové IOC, náhodná bijekce
    - IOC ECB = $(2^k)!$
    - IOC CBC = $2^k x\, 2^k x (2^k-1) x (2^k-2) x \ldots x (2^k-k)$
    - 1 blok = šestnáct 8-bitových kódování (2^70)

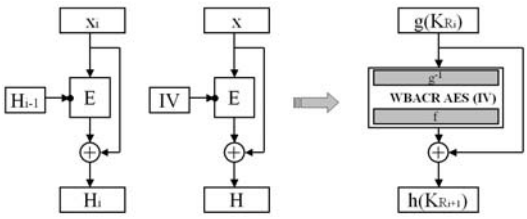
I/O kódování pro CBC 2/2



Klíčovaná hashovací funkce

- z blokového šifrovače (WBACR AES)
  - Matyas-Mayer-Oseas
  - I/O kódování pro CBC
  - použito pro aktualizaci K_R
  - jen jediný blok dat ☹
- vlastnosti
  - ochrana předchozí/následující hodnoty K_R
  - ochrana proti (smysluplné) modifikaci
  - není otevřená podoba K_R

Klíčovaná hashovací funkce



SEcure AUthenticated Transport protocol

- není nový protokol, je nová implementace
  - založeno na 3-průchodovém ISO9798-2 [2]
- provázanost autentizace a přenosu dat
- speciální implementace jen u strany B
  - odstranění porovnávacích operací
  - autentizační/šifrovací klíče WBACR AES
  - ukrytí zpracovávaných dat
  - okolní operace dle mobilní kryptografie
- uniformní operace, modifikace
  - výhodné pro „obfuscation" [4], kontrolu integrity

SEAUT - autentizační část

- 3-průchodový ISO9798-2
  - pokud $KD_{auth} == KE_{auth}$
- oddělená šifrovací a dešifrovací funkčnost
  - extrakce tabulek KD_{AUTH} nevytvoří 2. zprávu
- ustanovení iniciální hodnoty K_R

1. $A \leftarrow B : \{id_B, N_B\}.$
2. $A \rightarrow B : \{id_A, [redacted](N_A, N_B, id_B)\}.$
3. $A \leftarrow B : \{[redacted](N_B, N_A)\}.$
4. $K_{R_0} = [redacted]$

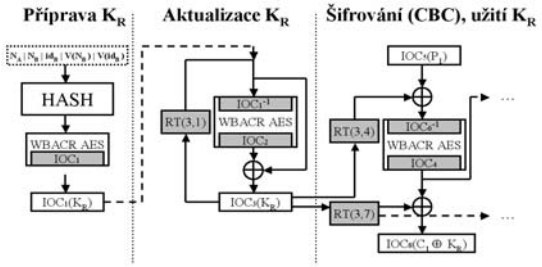
SEAUT - transportní část

- důvěrnost, čerstvost zpráv mezi A a B
- vstupní a výstupní kódování
  - provázanost s okolním kódem (mobilní kryptografie)
  - zvyšuje robustnost použití K_R (nelze odstranit bez IOC)
- čerstvost pomocí K_R
  - aktualizace po každé zprávě (není nutný čítač …)
  - chybná hodnota znehodnotí zprávu

5. A, B výpočtou: $K_{R_i} = H_{K_2}(K_{R_{i-1}})$.
6. $A \leftarrow B : \{idA, idB, [redacted](data))\}.$
7. A, B výpočtou: $K_{R_{i+1}} = H_{K_2}(K_{R_i})$.
8. $A \rightarrow B : \{idA, idB, [redacted](data))\}.$

Provázanost IOC

- RT tabulky ($IOC_X(5)$ -> $IOC_Y(5)$)



Závěr

- implementace na straně B:
  - utajení klíčů ~ WBACR AES
  - nezaměnitelnost ~ „směrové" klíče & oddělitelnost
  - čerstvost zpráv ~ užití & změna K_R
  - hodnota dat, provázanost ~ MC (náhodná bijekce)
- není samonosné, kombinovat ochrany
  - „obfuscation", kontrola integrity
- nezávislá využitelnost stavebních bloků
  - IOC pro CBC, WBACR AES hash

http://www.svenda.com/petr/securefw_cz.html

Literatura

[1] Chow, S., Eisen, P., Johnson, H., van Oorschot, P.C.: White-Box Cryptography and an AES implementation. Springer LNCS 2595, Berlin, 2003, s. 250-270.

[2] ISO/IEC 9798-2:1999 Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms. Popis protokolu je také dostupný v [3].

[3] Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press 1996/2001. Dostupné také na URL http://www.cacr.math.uwaterloo.ca/hac/ (listopad 2004).

[4] Collberg, Ch., Thomborson, C. Low, D.: A Taxonomy Of Obsfuscating Transformations. New Zeland, University Of Aucland, 1997. Dokument dostupný na URL http://www.cs.arizona.edu/collberg/Research/Publications/CollbergThomborsonLow97a/A4.pdf (listopad 2004)