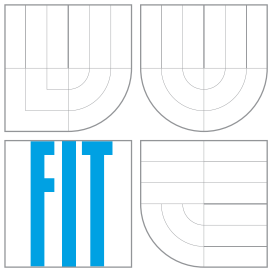
Vysoké učení technické v Brně
Brno University of Technology



Fakulta informačních technologií

Faculty of Information Technology

Bull's Authentication Protocol

Analýza bezpečnostného protokolu

Autor práce Lukáš Vrabec

Brno 2015

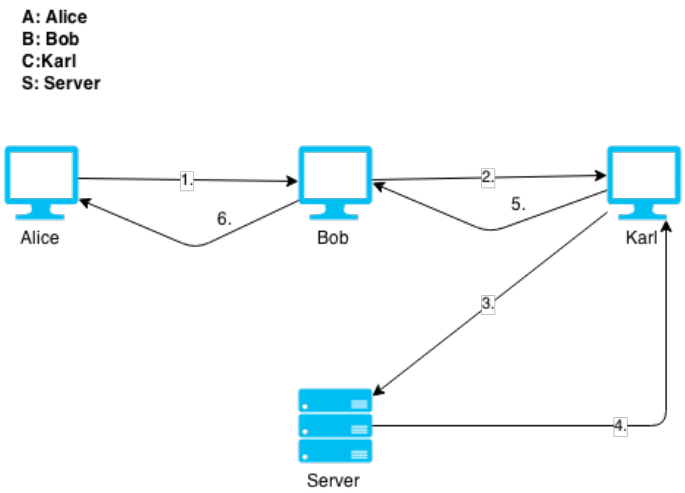
Obsah

Kapitola 1

Popis protokolu

Bull's Authentication Protokol[2] bol predstavený v roku 1997. Jeho autorom je J.Bull po ktorom nesie meno aj autentifikačný protokol. Úlohou tohto protokolu je distribúcia nových kľúčov cez fixný počet klientov a server, pričom každá susedná dvojica vlastní jeden takýto kľúč.

Popis protokolu je nasledovný. V prvom kroku žiadajú účastníci server o kľúče pre dvojice susedných klientov. Táto žiadosť prebieha tak, že klienti vytvoria akúsi "reťaz", kedy prvý klient požiada o kľúč susedného klienta, ten ďalšieho susedného klienta až posledný klient pošle zabalené správy so žiadostami o kľúče serveru. Takto je vytvorená "reťaz"kedy sú správy o žiadosť kľúča zabalené rekurzívne. V momente ked server príjme túto zabalenú správu, server vygeneruje relačné kľúče pre dvojice klientov. Tieto dvojice kľúčov sú odoslané späť najbližsiemu klientovi (tomu, ktorý odosielal správu serveru). Následne tento klient pošle spoločný kľuč pre dvojicu spolu so všetkými zvyšnými kľúčami späť svojmu predchodzovi, tento úkon sa opakuje kým nieje kľúč odoslaný prvému klientovi. Grafická reprezentácia je obsiahnutá v obrázku(1.1)



Obr. 1.1: Grafická reprezentácia protokolu

`A, B, C, S` : klienti a server
`Kab, Kbc` : symetrické kľuče pre dvojicu susedných klientov
`Na, Nb, Nc` : číslo - nonce
`Kas, Kbs, Kcs` : symetrické kľúče
`h` : hashovacia funkcia

```
A computes Xa = h((A,B,Na),Kas), (A,B,Na)
1. A -> B : Xa
B computes Xb = h((B,C,Nb,Xa),Kbs), (B,C,Nb,Xa)
2. B -> C : Xb
C computes Xc = h((C,S,Nc,Xb),Kcs), (C,S,Nc,Xb)
3. C -> S : Xc
4. S -> C : A, B, Kab xor h(Na,Kas), A,B,NaKab,
B, A, Kab xor h(Nb,Kbs), B,A,NbKab,
B, C, Kbc xor h(Nb,Kbs), B,C,NbKbc,
C, B, Kbc xor h(Nc,Kcs), C,B,NcKbc
5. C -> B : A, B, Kab xor h(Na,Kas), A,B,NaKab,
B, A, Kab xor h(Nb,Kbs), B,A,NbKab,
B, C, Kbc xor h(Nb,Kbs), B,C,NbKbc
6. B -> A : A, B, Kab xor h(Na,Kas), A,B,NaKab
```

Známe útoky

V roku 1998 bol publikovaný útok na tento autentifikačný protokol. Útok sa nazýva "domino attack". Tento útok predstavili P. Y. A Ryan a S. A. Schneider[3]. K tomuto útoku je potrebné aby útočník bol v pomyselnej "reťazi"pri žiadaní a následne prijímaní susedných kľúčov. Ak je útočník(Carl) posledným klientom, server mu (4. krok) pošle všetky kľúče pre dvojice klientov, teda zachytí aj nasledujúce správy: `Kab xor h(Nb,Kbs)` a `Kbc xor h(Nb,Kbs)`. Carl pozná kľúč `Kbc`, a kedže `Kab = Kbc xor Kab xor h(Nb, Kbs) xor Kbc xor h(Nb,Kbs)`, takto Carl vlastní kľúč `Kab`, ktorý bol pôvodne určený len pre Alice a Boba.

Kapitola 2

Analitycká analýza chovania protokolu

Kapitola 3

Analýza komunikácie BP z rôznych pohľadov subjektov

Nasleduje analýza komunikácie jak je uvedené v článku od Alvesa-fossa[1]

BP z pohľadu subjektu A:

Správa	**Popis**
`A1: A: computes Xa = h((A, B, Na), Kas), (A, B, Na)`	A vytvorí správu
`A2: A?: Xa`	A pošele správu
`A3: ?A: A, B, Kab xor h(Na, Kas), {A, B, Na}Kab`	A príjme správu
`A4: A: compute h(Na, Kas)`	A vypočíta správu
`A5: A: h(Na, Kas) xor (Kab xor h(Na, Kas))`	A získa kľúč
`A6: A: decrypt {A, B, Na}Kab`	A dešifruje správu

Literatúra

[1] Alves-Foss, J.; Soule, T.: A weakest precondition calculus for analysis of cryptographic protocols. In *DIMACS Workshop on Design and Formal Verifictaion of Security Protocols*, 1997.

[2] Bull, J.; Otway., D. J.: The authentication protocol DRA/CIS3/PROJ/CORBA/SC/1/CSM/436-04/03. Technická zpráva, Defence Research Agency, 1997.

[3] Ryan, P. Y. A.; Schneider, S. A.: An attack on a recursive authentication protocol: A cautionary tale. 65(1):7–10, Information Processing Letters, 1998.