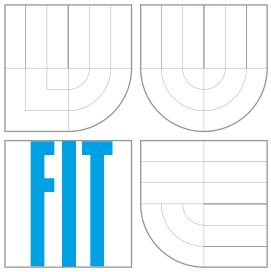
Vysoké učení technické v Brně
Brno University of Technology



Fakulta informačních technologií

Faculty of Information Technology

Lowe modified Denning-Sacco shared key

Analýza bezpečnostného protokolu do predmetu IBS

Autor práce Ladislav Šulák

Login xsulak04

Brno 5/2015

Obsah

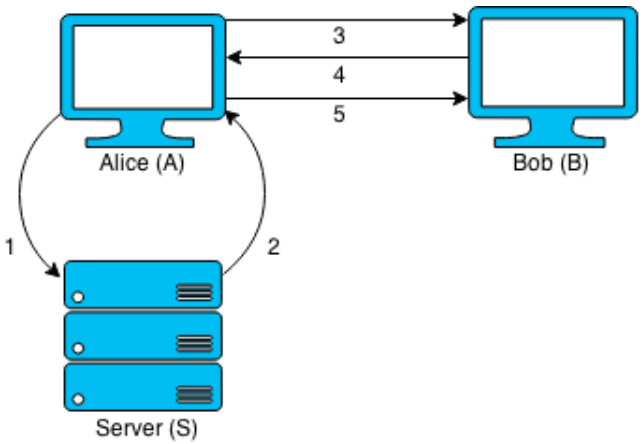
Kapitola 1

Popis protokolu

Lowe modified Denning-Sacco shared key protokol bol prvý krát predstavený v článku [2] z roku 1997. Jeho autorom je Gavin Lowe. Cieľom tohto protokolu je distribúcia zdieľaného symetrického kľúča serverom a vzájomná autentizácia klientov.

Jedná sa o modifikovanú verziu protokolu Denning-Sacco z roku 1981, ktorý vznikol z protokolu Needham Schroeder Symmetric Key z roku 1978. V protokole Needham Schroeder Symmetric Key sa využívajú noncesy, angl. *nonces*, teda náhodne vygenerované čísla jednotlivých subjektov. Tieto čísla boli nahradené z dôvodu vyššieho zabezpečenia časovým razítkom, ktorý sa generuje na strane serveru. Posledná modifikácia, teda protokol, ktorý je predmetom tejto práce, pridáva na záver komunikácie ešte *handshake* medzi jednotlivými subjektami, čo slúži pre vzájomnú autentizáciu klientov. Využíva sa pri tom vygenerovaný nonces. Nasledujúce sekcie 1.1 a 1.2 bližšie charakterizujú a reprezentujú správanie protokolu.

1.1 Grafická reprezentácia protokolu



Obr. 1.1: Grafická reprezentácia protokolu

1.2 Bežná reprezentácia protokolu

Ako ukazujú tabuľky 1.1 a 1.2, stanovené ciele boli naplnené, cieľové množiny sú podmnožinami množín po poslednom kroku protokolu.

`A, B, S`:	jednotlivé subjekty
N_b:	náhodne vygenerované číslo, tzv. *nonce*
K_{as}, K_{bs}, K_{ab}:	symetrické kľúče
`T`:	časové razítko
`dec`:	operácia s číslom *nonce*

`1. A -> S: A, B`
`2. S -> A:` $\{$`B,` K_{ab}`, T,` $\{K_{ab}$`, A, T`$\}K_{bs}\}K_{as}$
`3. A -> B:` $\{K_{ab}$`, A, T`$\}K_{bs}$
`4. B -> A:` $\{N_b\}K_{ab}$
`5. A -> B:` $\{$`dec(`N_b`)`$\}K_{ab}$

Krok	Znalosti	Predpoklady
Počiatočné podmienky	**A**: A, B, S, K_{as} **B**: B, S, K_{bs} **S**: S, T, K_{as}, K_{bs}	**A**:**S**: K_{as} **B**:**S**: K_{bs} **S**:**A**: K_{as}; **S**:**B**: K_{bs}
Cieľové podmienky	**A**: K_{ab} **B**: K_{ab} **S**:	**A**:**B**: K_{ab} **B**:**A**: K_{ab} **S**:
Zakázané cieľové podmienky	**A**: K_{bs} **B**: K_{as} **S**:	**A**: **B**: **S**:
1	**A**: A, B, S, K_{as} **B**: B, S, K_{bs} **S**: S, T, K_{as}, K_{bs}, **A**, **B**	**A**:**S**: K_{as}, **A**, **B** **B**:**S**: K_{bs} **S**:**A**: K_{as}; **S**:**B**: K_{bs}
2	**A**: A, B, S, K_{as}, $\mathbf{K_{ab}}$, **T**, $\mathbf{\{K_{ab}, A, T\}}K_{bs}$ **B**: B, S, K_{bs} **S**: S, T, K_{as}, K_{bs}, A, B	**A**:**S**: K_{as}, A, B **B**:**S**: K_{bs} **S**:**A**: K_{as}, **B**, $\mathbf{K_{ab}}$, **T**; **S**:**B**: K_{bs}

Tabuľka 1.1: Analýza správania protokolu podľa [1], časť 1.

Krok	Znalosti	Predpoklady
3	**A**: A, B, S, K_{as}, K_{ab}, T, $\{K_{ab}$, A, T$\}K_{bs}$ **B**: B, S, K_{bs}, $\mathbf{K_{ab}}$, **A**, **T** **S**: S, T, K_{as}, K_{bs}, A, B	**A**:**S**: K_{as}, A, B; **A**:**B**: $\mathbf{K_{bs}}$, $\mathbf{K_{ab}}$, **A**, **T** **B**:**S**: K_{bs} **S**:**A**: K_{as}, B, K_{ab}, T; **S**:**B**: K_{bs}
4	**A**: A, B, S, K_{as}, K_{ab}, T, $\{K_{ab}$, A, T$\}K_{bs}$, $\mathbf{N_b}$ **B**: B, S, K_{bs}, K_{ab}, A, T **S**: S, T, K_{as}, K_{bs}, A, B	**A**:**S**: K_{as}, A, B; **A**:**B**: K_{bs}, K_{ab}, A, T **B**:**S**: K_{bs}; **B**:**A**: $\mathbf{K_{ab}}$, $\mathbf{N_b}$ **S**:**A**: K_{as}, B, K_{ab}, T; **S**:**B**: K_{bs}
5	**A**: A, B, S, K_{as}, K_{ab}, T, $\{K_{ab}$, A, T$\}K_{bs}$, N_b **B**: B, S, K_{bs}, K_{ab}, A, T, $\mathbf{dec(N_b)}$ **S**: S, T, K_{as}, K_{bs}, A, B	**A**:**S**: K_{as}, A, B; **A**:**B**: K_{bs}, K_{ab}, A, T, $\mathbf{dec(N_b)}$ **B**:**S**: K_{bs}; **B**:**A**: K_{ab}, N_b **S**:**A**: K_{as}, B, K_{ab}, T; **S**:**B**: K_{bs}

Tabuľka 1.2: Analýza správania protokolu podľa [1], časť 2.

1.3 Analýza protokolu z pohľadu jednotlivých subjektov

V tejto sekcii bude analyzovaná komunikácia z pohľadu 3 subjektov: A, B a S. Tento princíp bol uvedený v technickej správe [1].

1.3.1 Analýza z pohľadu subjektu A

`A1: A ->: A, B`	A zašle správu
`A2: -> A:` $\{$`B,` K_{ab}`, T,` $\{K_{ab}$`, A, T`$\}K_{bs}\}K_{as}$	A prijíma správu
`A3: A: decrypt`$\{$`X`$\}K_{as}$	A rozšifruje správu
`A4: A proves (A` $\xrightarrow{K_{ab}}$ `B)`	A validuje kľúč
`A5: A proves fresh(`K_{ab}`)`	A validuje čerstvosť kľúča
`A6: A ->:` $\{K_{ab}$`, A, T`$\}K_{bs}$	A zasiela správu
`A7: -> A:` $\{N_b\}K_{ab}$	A prijíma správu
`A8: A: decrypt`$\{N_b\}K_{ab}$	A rozšifruje správu
`A9: A: F(`N_b`) = dec(`N_b`)`	A modifikuje nonces
`A10: A: F(dec(`N_b`),` K_{ab}`) =` $\{$`dec(`N_b`)`$\}K_{ab}$	A zašifruje správu
`A11: A ->:` $\{$`dec(`N_b`)`$\}K_{ab}$	A zasiela správu

1.3.2 Analýza z pohľadu subjektu B

`B1: -> B:` $\{K_{ab}$`, A, T`$\}K_{bs}$	B obdrží správu
`B2: B: decrypt`$\{$`X`$\}K_{bs}$	B rozšifruje správu
`B3: B proves (A` $\xrightarrow{K_{ab}}$ `B)`	B validuje kľúč
`B4: B proves fresh(`K_{ab}`)`	B validuje čerstvosť kľúča
`B5: B: F(`$\{N_b\}$`,` K_{ab}`) =` $\{N_b\}K_{ab}$	B zašifruje správu
`B6: B ->:` $\{N_b\}K_{ab}$	B zasiela správu

B7: -> B: $\{\texttt{dec}(N_b)\}K_{ab}$	B prijíma správu
B8: B: decrypt$\{\texttt{dec}(N_b)\}K_{ab}$	B rozšifruje správu

1.3.3 Analýza z pohľadu subjektu S

S1: -> S: A, B	S prijíma správu
S2: S: X = F(B, K_{ab}, T, $\{K_{ab}$, A, T$\}K_{bs}$)	S vytvára správu
S3: S: F($\{$X$\}$, K_{as}) = $\{$X$\}K_{as}$	S zašifruje správu
S4: S ->: $\{$X$\}K_{as}$	S zasiela správu

1.4 Analýza správania protokolu pomocou nástroja SPAN

Verifikácia pomocou automatického nástroja prebiehala pomocou 4 metód:

- **ATSE** prehlásil, že protokol nie je bezpečný. Na základe zdrojového súboru CAS nástroj našiel útok, ktorého cieľom je narušiť utajenie.
- **OMFC, SATMC** vygenerovali výsledky podobné ako v predchádzajúcej metóde. Protokol nebol prehlásený za bezpečný, pretože sa našiel útok na porušenie utajenia.
- **TA4SP**. Pri použití tejto metódy sa program nedopracoval k výsledku, kvôli neznámej chybe. Operačný systém, ktorý sa používal, bol Windows XP s 32-bitovou architektúrou. Táto metóda nefungovala ani na webovom rozhraní projektu AVISPA[1].

[1] Automated Validation of Internet Security Protocols and Applications, skrátene AVISPA, je projekt pre automatickú validáciu bezpečnosťných protokolov. K dispozícií je GUI aplikácia a aj webové rozhranie pre validáciu protokolov. http://www.avispa-project.org/.

Kapitola 2

Útoky na protokol

Ako bolo uvedené vyššie, tento protokol vznikol postupne z ďalších a dalo by sa povedať, že je to ich bezpečnejšia verzia. Podľa [3] má Needham-Schroeder shared-key protocol zraniteľnosť v tom, že ak sú kľúče patriace do danej relácie kompromitované, môže byť vystavený útoku prehrávaním, angl. *replay attack*. Kvôli tomu bol protokol modifikovaný tak, aby k tomu nedošlo, použitím časového razítka. Server posiela správu s týmto vygenerovaným časovým razítkom podľa aktuálneho času, čo je zároveň čas vzniku relačného kľúču K_{ab}. Subjekt A obdrží túto správu a verifikuje ju na základe porovnania tohto a aktuálneho času. Na základe určitého intervalu je schopný určiť, či je kľúč aktuálny v danej relálcii. Ak áno, časové razítko vygenerované serverom je poslané subjektu B, ktoré tiež verifikuje správu. Lowe objavil slabinu v tomto protokole, ktorá funguje na princípe okamžitého opätovného zaslania správy útočníkom. Táto správa obsahuje časové razítko od serveru a už bola verifikovaná subjektom A. Subjektu B dôjdu 2 správy a reaguje na ne tak, akoby prišli požiadavky od subjektu A na započatie 2 relácií. Finálna verzia protokolu je odolná voči tomuto útoku, pretože verifikácia subjektov je posilnená číslom *nonce* a naviac je obojsmerná.

Program pre automatizovanú verifikáciu však neprehlásil tento protokol za bezpečný, kvôli možnosti porušiť utajenie symetrických kľúčov. Je to realizované tak, že útočník zachytáva komunikáciu. Serveru sa môže vydávať ako klient, a klientom ako server, ktorý distribuuje kľúče.

Literatúra

[1] Alves-Foss J., Soule T.: A Weakest Precondition Calculus for Analysis of Cryptographic Protocols. In *DIMACS Workshop on Design and Formal Verification of Crypto Protocols*, 1997.

[2] Lowe, G.: A family of attacks upon authentication protocols. Technická zpráva, Department of Mathematics and Computer Science, University of Leicester, 1997.

[3] Q., W.: Verification of Security Protocols Using A Formal Approach. Technická zpráva, Technical University of Denmark, 2007.