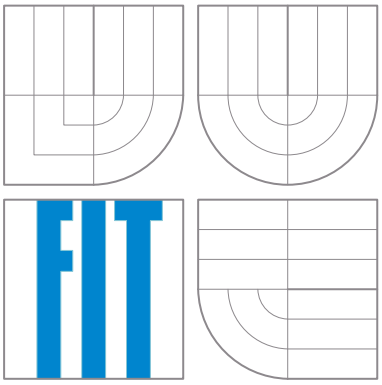


Analýza bezpečnostního protokolu

Woo Lam Π^f

projekt č. 1

10. května 2016

Autor: Pavel Frýz, xfryzp00@stud.fit.vutbr.cz
Fakulta Informačních Technologií
Vysoké Učení Technické v Brně

1 Popis protokolu

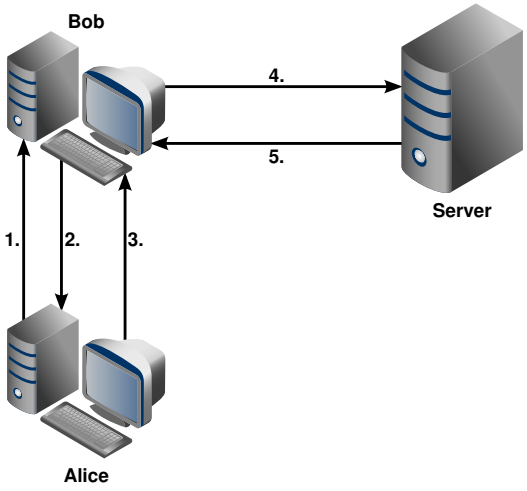
Protokol vytvořil profesor Texaské univerzity v Austinu Simon S. Lam a jeho bývalý student Thomas Y. C. Woo. Protokol Π^f byl představen v [3]. Protokol provádí pouze jednosměrnou autentizaci, autentizuje účastníka A vůči B. Autentizace probíhá na důvěryhodném serveru(S), který sdílí klíč s každým účastníkem, protokol používá symetrickou kryptografii. Komunikici zahujeje subjekt A, subjekt B poté vygeneruje nonce a pošle ho A. A zašifruje nonce, společně s identifikátory subjektů a vše pošle zpět B, který k tomu přidá téže informace a vše zašifruje. Poté autentizační server ověří obě zašifrované zprávy a provede překlad klíčů, zprávu zašifrovanou A dešifruje a znovu ji zašifruje klíčem sdíleným z B. Toto pak pošle B, který ověří nonce. Pokud B dokončí provádění protokolu, tak iniciátor spojení je subjekt A deklarovaný v první zprávě. Z protokolu Π^f jsou postupným zjednodušováním odvozeny protokoly Π^1, Π^2, Π^3 a Π, ale zatímco protokol Π^f je korektní, jeho zjednodušené verze jsou nachýlné proti podvržení identity [1].

Textová reprezentace [2]:

A, B, S: Subjekty
K_{AS}, K_{BS}: Sdílené klíče
N_B: Nonce

1. $A \rightarrow B$: A
2. $B \rightarrow A$: N_B
3. $A \rightarrow B$: $\{A, B, N_B\}_{K_{AS}}$
4. $B \rightarrow S$: $\{A, B, N_B, \{A, B, N_B\}_{K_{AS}}\}_{K_{BS}}$
5. $S \rightarrow B$: $\{A, B, N_B\}_{K_{BS}}$

Grafická reprezentace:



2 Analýza protokolu

Počáteční, zakázané a cílové znalosti a předpokladý jsou uvedeny v tabulce 2. Znalost subjektu A je označena **A:**, následované listem znalostí. Předpoklady subjektu A o znalostech B jsou označeny **A:B:**. Znalosti a předpoklady po jedtlivích krocích jsou uvedeny v tabulce 2. Nové znalosti a přepoklady jsou označeny ***takto***.

Krok	**Znalosti**	**Předpoklady**
Počáteční podmínky	**A:** A, B, S, K_{AS} **B:** B, S, N_B, K_{BS} **S:** A, B, S, K_{AS}, K_{BS}	**A:B: A:S:** K_{AS} **B:A: B:S:** K_{BS} **S:A:** K_{AS} **S:B:** K_{BS}
Cílové podmínky	**A:** N_B	**B:A:** N_B **B:S:** N_B **S:A:** N_B **S:B:** N_B
Zakázané cílové podmínky	**A:** K_{BS} **B:** K_{AS}	

Tabulka 1: Počáteční, zakázané a cílové znalosti a předpoklady

1	**A:** A, B, S, K_{AS} **B:** ***A***, B, S, N_B, K_{BS} **S:** A, B, S, K_{AS}, K_{BS}	**A:B:** ***A*** **A:S:** K_{AS} **B:A:** ***A*** **B:S:** K_{BS} **S:A:** K_{AS} **S:B:** K_{BS}
2	**A:** A, B, S, $\boldsymbol{N_B}$, K_{AS} **B:** A, B, S, N_B, K_{BS} **S:** A, B, S, K_{AS}, K_{BS}	**A:B:** A, $\boldsymbol{N_B}$ **A:S:** K_{AS} **B:A:** A, $\boldsymbol{N_B}$ **B:S:** K_{BS} **S:A:** K_{AS} **S:B:** K_{BS}
3	**A:** A, B, S, N_B, K_{AS} **B:** A, B, S, N_B, K_{BS}, $\boldsymbol{\{A, B, N_B\}_{K_{AS}}}$ **S:** A, B, S, K_{AS}, K_{BS}	**A:B:** A, N_B, $\boldsymbol{\{A, B, N_B\}_{K_{AS}}}$ **A:S:** K_{AS} **B:A:** A, N_B, $\boldsymbol{\{A, B, N_B\}_{K_{AS}}}$ **B:S:** K_{BS} **S:A:** K_{AS} **S:B:** K_{BS}
4	**A:** A, B, S, N_B, K_{AS} **B:** A, B, S, N_B, K_{BS}, $\{A, B, N_B\}_{K_{AS}}$ **S:** A, B, S, $\boldsymbol{N_B}$, K_{AS}, K_{BS}	**A:B:** A, N_B, $\{A, B, N_B\}_{K_{AS}}$ **A:S:** K_{AS} **B:A:** A, N_B, $\{A, B, N_B\}_{K_{AS}}$ **B:S:** ***A***, ***B***, $\boldsymbol{N_B}$, K_{BS}, $\boldsymbol{\{A, B, N_B\}_{K_{AS}}}$ **S:A:** ***A***, ***B***, $\boldsymbol{N_B}$, K_{AS} **S:B:** ***A***, ***B***, $\boldsymbol{N_B}$, K_{BS}, $\boldsymbol{\{A, B, N_B\}_{K_{AS}}}$
5	**A:** A, B, S, N_B, K_{AS} **B:** A, B, S, N_B, K_{BS}, $\{A, B, N_B\}_{K_{AS}}$ **S:** A, B, S, N_B, K_{AS}, K_{BS}	**A:B:** A, N_B, $\{A, B, N_B\}_{K_{AS}}$ **A:S:** K_{AS} **B:A:** A, N_B, $\{A, B, N_B\}_{K_{AS}}$ **B:S:** A, B, N_B, K_{BS}, $\{A, B, N_B\}_{K_{AS}}$ **S:A:** A, B, N_B, K_{AS} **S:B:** A, B, N_B, K_{BS}, $\{A, B, N_B\}_{K_{AS}}$

Tabulka 2: Znalosti a předpoklady po vykonání jednotlivých kroků

Po provedení všech kroků byly splněny cílové podmínky a předpoklady.

3 Komunikace z pohledu subjektů

3.1 Z pohledu A

1. $A \rightarrow$: A -posílá zprávu
2. $\rightarrow A$: N_B -přijímá zprávu
3. $F(A, B, N_B, K_{AS}) = \{A, B, N_B\}_{K_{AS}}$ -šifruje zprávu
4. $A \rightarrow$: $\{A, B, N_B\}_{K_{AS}}$ -posílá zprávu

3.2 Z pohledu B

1. $\rightarrow B$: A -přijímá zprávu
2. $B \rightarrow$: N_B -posílá zprávu
3. $\rightarrow B$: $\{A, B, N_B\}_{K_{AS}}$ -přijímá zprávu
4. $F(A, B, N_B, \{A, B, N_B\}_{K_{AS}}, K_{BS}) = \{A, B, N_B, \{A, B, N_B\}_{K_{AB}}\}_{K_{BS}}$ -šifruje zprávu
5. $B \rightarrow$: $\{A, B, N_B, \{A, B, N_B\}_{K_{AB}}\}_{K_{BS}}$ -posílá zprávu
6. $\rightarrow B$: $\{A, B, N_B\}_{K_{BS}}$ -přijímá zprávu
7. $decrypt(\{A, B, N_B\}_{K_{BS}}, K_{BS})$ -dešifruje
8. $proves(fresh(N_B))$ -ověřuje nonce

3.3 Z pohledu S

1. $\rightarrow S$: $\{A, B, N_B, \{A, B, N_B\}_{K_{AB}}\}_{K_{BS}}$ -přijímá zprávu
2. $decrypt(\{A, B, N_B, \{A, B, N_B\}_{K_{AB}}\}_{K_{BS}}, K_{BS})$ -dešifruje
3. $decrypt(\{A, B, N_B\}_{K_{AB}}, K_{AS})$ -dešifruje
4. $controls(N_B)$ -kontroluje shodu nonců
5. $translate(\{A, B, N_B\}_{K_{AS}}, K_{AS}, K_{BS}) = \{A, B, N_B\}_{K_{BS}}$ -překládá zprávu
6. $S \rightarrow$: $\{A, B, N_B\}_{K_{BS}}$ -posílá zprávu

4 Analýza pomocí nástroje SPAN

Protokol byl implementován v nástroji span. Na začátku je deklarován protokol s jeho názvem.

```
protocol WooLamPiF;
```

Poté jsou deklarování jednotlivý účastníci, nonce a sdílené klíče.

```
identifiers
A,B,S : user;
Nb : number;
Kas,Kbs : symmetric_key;
```

Dále jsou definovány jednotlivé zprávy, které si subjekty vyměňují a jejich pořadí.

```
messages
1. A -> B : A
2. B -> A : Nb
3. A -> B : {A, B, Nb}Kas
4. B -> S : {A, B, Nb, {A, B, Nb}Kas}Kbs
5. S -> B : {A, B, Nb}Kbs
```

V další části jsou definovány počáteční znalosti jednotlivých subjektů.

```
knowledge
A: A,B,S,Kas;
B: B,S,Kbs;
S: S,A,B,Kas,Kbs;
```

Přiřazení konkrétních hodnot jednotlivým účastníkům

```
session_instances
[A:alice,B:bob,S:server,Kas:key1,Kbs:key2];
```

Specifikace cíle protokolu, tedy autentizace ucastnika A vuci B.

```
goal
A authenticates B on Nb;
```

Poté byly spuštěny jednotlivé testy, výsledky jsou uvedeny v přílohách. Všechny metody označily protokol za bezpečný, vyjma metody TA4SP, která nemohla výsledek rozhodnout.

5 Závěr

Na protokol nebyl nalezen žádný známý útok, útok nebyl nalezen ani pomocí automatického ověření pomocí nástroje Span. Výdledky automatického ověřování i analytické metody tedy ukazují, že protokol Woo Lam Π^f měl být bezpečný.

Použité zdroje

[1] Clark, J. a Jacob, J. *A Survey of Authentication Protocol Literature*. November 1997. Dostupné na: <http://www.cs.york.ac.uk/~jac/PublishedPapers/reviewV1_1997.pdf>.

[2] Jacquemard, F. *Woo and Lam Pi f* [online]. Last modified 2001-10-27 [cit. 2012-5-1]. Dostupné na: <http://www.lsv.ens-cachan.fr/Software/spore/wooLamPif.html>.

[3] Woo, T. Y. C. a Lam, S. S. A lesson on authentication protocol design. *SIGOPS Oper. Syst. Rev.* červenec 1994, roč. 28, č. 3. S. 24–37. ISSN 0163-5980.

A Výsledek metody ATSE

SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
WooLamPiF.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed : 26 states
Reachable : 12 states
Translation : 0.01 seconds
Computation : 0.00 seconds

B Výsledek metody OFMC

% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
WooLamPiF.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime : 0.00s
searchTime : 0.02s
visitedNodes : 9 nodes
depth : 6 plies

C Výsledek metody SATMC

SUMMARY
SAFE
DETAILS
STRONGLY_TYPED_MODEL
BOUNDED_NUMBER_OF_SESSIONS
BOUNDED_MESSAGE_DEPTH
PROTOCOL
WooLamPiF.if
GOAL
%% see the HLPSL specification..
BACKEND
SATMC
COMMENTS
STATISTICS

attackFound	false	boolean
stopConditionReached	true	boolean
fixedpointReached	6	steps
stepsNumber	6	steps
atomsNumber	0	atoms
clausesNumber	0	clauses
encodingTime	0.02	seconds
solvingTime	0	seconds
if2sateCompilationTime	0.11	seconds

ATTACK TRACE
%% no attacks have been found..

D Výsledek metody TA4SP

SUMMARY
INCONCLUSIVE
DETAILS:
NOT_SUPPORTED
PROTOCOL:
WooLamPiF.if
GOAL:
SECRECY
BACKEND:
TA4SP
COMMENTS:
For technical reasons about non-left-linearity in term rewriting with tree automaton, this protocol cannot be checked.
Sorry.
STATISTICS:
Translation: 0.00 seconds