Security Analysis and Improvement of Yahalom Protocol

Li Chen [1,2] and Mingxia Shi[3]
1. Computer Centre, Henan University of Finance and Economics,
Zhengzhou, Henan 450002, China
2. Department of Network Engineering, Information Engineering University,
Zhengzhou, Henan 450002, China
3. Basic Courses Department, Henan Light Industry Training College,
Zhengzhou, Henan 450002, China

Abstract- **Logic-based formal analysis methods are the efficient methods for analyzing the security of cryptography protocols. The paper analyzes the security of the Yahalom protocol by employing the formal method SVO logic and finds that the protocol does not achieve the authentication goals. By modifying message format and adding handshake message, the paper also proposes a novel improved Yahalom protocol, which removes the limitations that the original Yahalom protocol cannot against the reply attack and the BAN-Yahalom protocol cannot resist impersonation attack. The analysis results of the improved Yahalom protocol reveal that the protocol completes the strong goals of identity authentication and key negotiation.**

I. INTRODUCTION

With the phenomenal growth of the Internet and open networks in general, how to identify the principal in the Internet and open networks environment, known as identity authentication, presents many interesting challenges in the network security area. Authentication protocols are efficient methods resolving the problem now. Some protocols depending upon cryptography were specially designed to guarantee the security of communication. Another key requirement related to identity authentication is to build secure tunnel through exchanging keys between two communicating entities. In fact, many authentication protocols, such as Yahalom protocol [1], Kerberos protocol [2] and Internet Key Exchange protocol (IKE) [3], are all designed to both of the above two requirements. However it is very difficult to design the protocols meeting the above requirements because the potential security vulnerabilities are covert. For example, Reference [1] found that the Yahalom protocol could not against the reply attack, and it also proposed an improved BAN-Yahalom protocol. However Reference [4] research results revealed that the BAN-Yahalom protocol could not resist the impersonation attack, etc.

Formal methods have been widely used to analyze the security of authentication protocols in recent years. Many significant results have been achieved in the area since formal methods began to apply to cryptographic protocol security analysis. The SVO logic [5,6] used for authentication protocol analysis is a many-sorted modal logic, which captures the desirable properties of BAN-Like logic, such as BAN logic [1], GNY logic [7], AT logic [8] and VO logic [9]. It not only has better linguistic expressibility and logical derivability, but also is easily extended and has more sound semantics than BAN-like logic.

In the paper, we employ the SVO logic to analyze the security of the Yahalom protocol and propose a new improved protocol.

Rest of the paper is organized as follows –in the next section we present the Yahalom protocol and the SVO logic, and analyze security of the protocol by using the SVO logic. In section 3, the improved Yahalom protocol is proposed and analyzed. Section 4 concludes the paper.

II. THE YAHALOM PROTOCOL AND ITS ANALYSIS

2.1. The Yahalom Protocol

The Yahalom protocol is a key distribution protocol that also guarantees authentication. It assumes a shared-key cryptosystem, in which each participant shares a master key with a trusted party, the Key Distribution Sever. The Yahalom protocol is described as follows.

(1) A→B：A, N_A

(2) B→S：$B, \{A, N_A, N_B\}K_{BS}$

(3) S→A：$\{B, K_{AB}, N_A, N_B\}K_{AS}, \{A, K_{AB}\}K_{BS}$

(4) A→B：$\{A, K_{AB}\}K_{BS}, \{N_B\}K_{AB}$

In the Yahalom protocol shown in fig. 1 below, we refer to the protocol initiator A as 'Alice' and the other participant B as 'Bob'. Initially, Alice and Bob share keys K_{AS} and K_{BS} with the server S respectively. Alice firstly sends her identify A, together with a nonce N_A to Bob. In the second message, Bob sends to the server S his identify B and an encrypted chunk $\{A, N_A, N_B\}K_{BS}$, where N_B is Bob's nonce. In the third message, the server S sends to Alice two encrypted chunks $\{B, K_{AB}, N_A, N_B\}K_{AS}$ and $\{A, K_{AB}\}K_{BS}$, where the first encrypted part tells Alice that K_{AB} is a good session key for communicating with Bob, and also tells her that N_B is Bob's nonce. The second encrypted part is intended for Bob. In the fourth message, Alice sends to Bob this encrypted part, along with Bob's nonce N_B encrypted with K_{AB}. Bob decrypts the first encrypted part of the message to get K_{AB}, and uses it to

Research supported by the Key Technologies R&D Program of Henan Province of China (No. 0524220044, 0624260017, 072102210029)

978-1-4244-1718-6/08/$25.00 ©2008 IEEE

decrypt the second encrypted part. If the latter decryption yields his nonce N_B, then he obtains assurance that K_{AB} is a good session key for communicating with Alice.

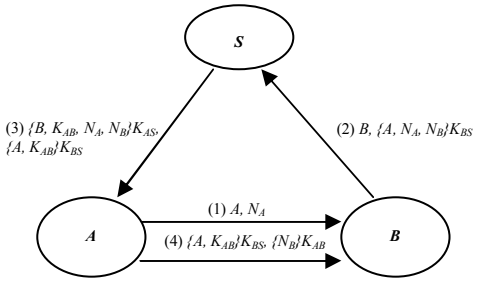

Fig. 1. The Yahalom protocol

The nonces N_A and N_B in the protocol are fresh quantities which have never been used before for their intended purpose.

The Yahalom protocol aims to enable every two agents to agree on a session key — *key distribution* — to be used to ensure the secrecy of the subsequent communication. It also guarantees each party that the other one has been involved in current run — *authentication*.

2.2. The SVO Logic

In the SVO logic, the notations $|\equiv$, $\lhd$, $|\sim$, $|\approx$, $|\Rightarrow$, $\ni$, #, $\equiv$ are used to indicate *believes*, *received*, *said*, *says*, *controls*, *has*, *fresh* and *equivalent*.

The SVO logic includes twenty axioms and two inference rules. We only describe the required inference rules, axioms and definitions in the protocol analyses later.

1) Inference Rules

Modus Ponens (MP): $\varphi \wedge (\varphi \rightarrow \Psi) \rightarrow \Psi$

Necessitation (Nec): $\vdash \varphi \rightarrow (\vdash P \mid\equiv \varphi)$

2) The SVO Logic Axioms

(1) *believing axiom*

A1 $P \mid\equiv \varphi \wedge P \mid\equiv (\varphi \rightarrow \Psi) \rightarrow (P \mid\equiv \Psi)$

(2) *source associations axiom*

A3 $(P \xleftrightarrow{K} Q \wedge R \lhd \{X^Q\}_K) \rightarrow (Q \mid\sim X \wedge Q \ni K)$

(3) *Receiving axioms*

A7 $P \lhd (X_1, \ldots, X_n) \rightarrow P \lhd X_i$

(4) *Seeing axiom*

A10 $P \lhd X \rightarrow P \ni X$

(5) *Saying axiom*

A14 $P \mid\sim (X_1, \ldots, X_n) \rightarrow P \mid\sim X_i \cdots P \ni X_i$

(6) *Jurisdiction axioms*

A16 $P \mid\Rightarrow \varphi \wedge P \mid\approx \varphi \rightarrow \varphi$

(7) *Freshness axiom*

A17 $\#(X_i) \rightarrow \#(X_1, \ldots, X_n)$

(8) *Nonce-verification axiom*

A19 $(\#(X) \wedge P \mid\sim X) \rightarrow P \mid\approx X$

3) The SVO Logic Definitions

$P \xleftrightarrow{K} Q$: K is a good key for P and Q regardless of whether either of them knows it.

In addition, a common consequence can be inferred from the axiom A1 and the rule MP.

A1+MP A1 $P \mid\equiv \varphi \wedge P \mid\equiv (\varphi \rightarrow \Psi) \vdash (P \mid\equiv \Psi)$

We also need to add the believing axiom A0 to the SVO logic. A0 must be used in the analysis later and cannot be deduced from the other axioms.

A0 $(P \mid\equiv \varphi \wedge P \mid\equiv \Psi) \equiv (P \mid\equiv \varphi \wedge \Psi)$

2.3. Security Analysis of the Yahalom Protocol

Now we utilize to the SVO logic to analyze the security of the Yahalom protocol. In every step of the analysis process, we first describe the inference result, then give the required inference rules, axioms, definitions, assumptions and formulae, which are used to reason the result.

1) Yahalom Goals

$A \mid\equiv A \xleftrightarrow{K_{AB}} B$

$A \mid\equiv \#(K_{AB})$

$A \mid\equiv B \mid\equiv A \xleftrightarrow{K_{AB}} B$

$A \mid\equiv B \mid\equiv \#(K_{AB})$

$B \mid\equiv A \xleftrightarrow{K_{AB}} B$

$B \mid\equiv \#(K_{AB})$

$B \mid\equiv A \mid\equiv A \xleftrightarrow{K_{AB}} B$

$B \mid\equiv A \mid\equiv \#(K_{AB})$

2) Yahalom Initial Assumptions

P1 $A \mid\equiv A \xleftrightarrow{K_{AS}} S$

P2 $B \mid\equiv B \xleftrightarrow{K_{BS}} S$

P3 $A \mid\equiv S \mid\Rightarrow A \xleftrightarrow{K} B$

P4 $B \mid\equiv S \mid\Rightarrow A \xleftrightarrow{K} B$

P5 $A \mid\equiv S \mid\Rightarrow \#(A \xleftrightarrow{K_{AB}} B)$

P6 $B \mid\equiv S \mid\Rightarrow \#(A \xleftrightarrow{K_{AB}} B)$

P7 $A \mid\equiv \#(N_A)$

P8 $B \mid\equiv \#(N_B)$

3) Yahalom Received Message Assumptions

P9 $B \lhd (A, N_A)$

P10 $S \lhd (B, \{A, N_A, N_B\} K_{BS})$

P11 $A \lhd (\{B, K_{AB}, N_A, N_B\} K_{AS}, \{A, K_{AB}\} K_{BS})$

P12 $B \lhd (\{A, K_{AB}\} K_{BS}, \{N_B\} K_{AB})$

4) Yahalom Comprehension Assumptions

P13 $B \mid\equiv B \lhd (A, <N_A>_{*B})$

P14 $S \mid\equiv S \lhd (B, <\{A, N_A, N_B\} K_{BS}>_{*S})$

P15 $A \mid\equiv A \lhd (\{B, <K_{AB}>_{*A}, N_A, <N_B>_{*A}\} K_{AS}, <\{A, K_{AB}\} K_{BS}>_{*A})$

P16 $B \mid\equiv B \lhd (\{A, <K_{AB}>_{*B}\} K_{BS}, \{N_B\} <K_{AB}>_{*B})$

5) Yahalom Interpretation Assumptions

P17 $A \mid\equiv A \lhd (\{B, <K_{AB}>_{*A}, N_A, <N_B>_{*A}\}K_{AS}, <\{A, K_{AB}\} K_{BS}>_{*A}) \rightarrow A \mid\equiv A \lhd (\{B, A \xleftrightarrow{<K_{AB}>_{*A}} B, \#(<K_{AB}>_{*A}), N_A, <N_B>_{*A}\}K_{AS}, <\{A, K_{AB}\} K_{BS}>_{*A})$

P18 $B \mid\equiv B \lhd (\{A, <K_{AB}>_{*B}\} K_{BS}, \{N_B\} <K_{AB}>_{*B}) \rightarrow B \mid\equiv B \lhd (\{A, A \xleftrightarrow{<K_{AB}>_{*B}} B\} K_{BS}, \{N_B\} <K_{AB}>_{*B})$

6) Yahalom Derivation for Alice

(1) $A \mid\equiv A \lhd (\{B, A \xleftrightarrow{<K_{AB}>_{*A}} B, \#(<K_{AB}>_{*A}), N_A, <N_B>_{*A}\}K_{AS}, <\{A, K_{AB}\} K_{BS}>_{*A})$
By A0, MP, P15 and P17

(2) $A \mid\equiv A \lhd (\{B, A \xleftrightarrow{<K_{AB}>_{*A}} B, \#(<K_{AB}>_{*A}), N_A, <N_B>_{*A}\}K_{AS})$
By A1+MP, A7and (1)

(3) $A \mid\equiv S \mid\sim (B, A \xleftrightarrow{<K_{AB}>_{*A}} B, \#(<K_{AB}>_{*A}), N_A, <N_B>_{*A})$
By A0, A3, P1 and (2)

(4) $A \mid\equiv S \mid\approx (B, A \xleftrightarrow{<K_{AB}>_{*A}} B, \#(<K_{AB}>_{*A}), N_A, <N_B>_{*A})$
By A0, A17, A19, P5, P7 and (3)

(5) $A \mid\equiv A \xleftrightarrow{<K_{AB}>_{*A}} B$
By A0, A14, A16, P3 and (4)

(6) $A \mid\equiv \#(<K_{AB}>_{*A})$
By A0, A17, A19, P5, P7 and (4)

On the basis of the above analyses, we can conclude that the Yahalom protocol does not satisfy the authentication goals for Alice .

7) Yahalom Derivation for Bob

(1) $B \mid\equiv B \lhd (\{A, A \xleftrightarrow{<K_{AB}>_{*B}} B\} K_{BS}, \{N_B\} <K_{AB}>_{*B})$
By A0, A1+MP, P16 and P18

(2) $B \mid\equiv B \lhd (\{A, A \xleftrightarrow{<K_{AB}>_{*B}} B\} K_{BS})$
By A0, A1+MP, A7 and (1)

(3) $B \mid\equiv S \mid\sim (A, A \xleftrightarrow{<K_{AB}>_{*B}} B)$
By A0, A3, P2 and (2)

(4) $B \mid\equiv A \xleftrightarrow{<K_{AB}>_{*B}} B$
By A0, A14, P4 and (3)

(5) $B \mid\equiv B \lhd (\{N_B\} <K_{AB}>_{*B})$
By A0, A1+MP, A7 and (1)

(6) $B \mid\equiv A \ni <K_{AB}>_{*B}$
By A0, A3, (4) and (5)

(7) $B \mid\equiv A \mid\sim N_B$
By A0, A3, (5) and (6)

(8) $B \mid\equiv A \mid\approx N_B$
By A0, A17, A19, (5), (6) and (7)

(9) $B \mid\equiv A \mid\equiv A \xleftrightarrow{<K_{AB}>_{*B}} B$
By A0, A14, A16 and (8)

(10) $B \mid\equiv A \mid\equiv \#(<K_{AB}>_{*B})$
By A0, A17, A19, P8 and (9)

The above analyses only prove most of the goals for Bob. Beause the first encrypted chunk in the fourth message does not include the terms used for proving the freshness of the session key, such as N_B, We cannot prove Bob's important goal $B \mid\equiv \#(K_{AB})$. This is a mortal flaw. The encrypted chunk could be a replayed message. The above analyses show that the Yahalom protocol does not completely achieve the authentication goals for Bob.

III. The Improved Yahalom Protocol and its Analysis

We propose an improved Yahalom protocol based on the analyses in section 2.3. The message flow of improved protocol is described formally as follows.

(1) A→B：A, N_A

(2) B→S：$B, \{A, N_A, N_B\}K_{BS}$

(3) S→A：$\{B, K_{AB}, N_A, N_B\}K_{AS}, \{A, N_B, K_{AB}\}K_{BS}$

(4) A→B：$\{A, N_B, K_{AB}\}K_{BS}, \{A, N_B\}K_{AB}$

(5) B→A：$\{B, N_A\text{-}1\}K_{AB}$

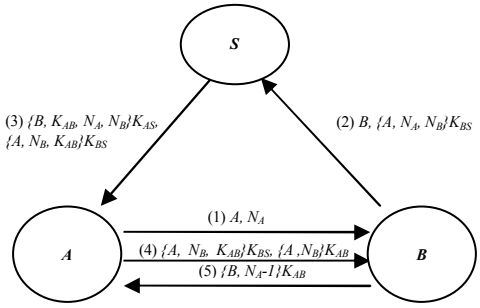

Fig. 2. The improved Yahalom protocol

In the improved Yahalom protocol, we add a nonce N_B generated by Bob to both the second encrypted chunk in the third message and the first encrypted chunk in the fourth message. To do so, the replay attack can be efficiently avoided. The second improvement is that the identify A of Alice is added to the second encrypted chunk in the fourth message. In addition, we also add the fifth message (5) to resist impersonation attack. Alice may acknowledge that Bob has obtained the good session key K_{AB} through the handshake message (5).

The goals of the improved Yahalom protocol are the same as the goals described in section 2.3. Next, we formally analyze the improved protocol goals. In section 2.3, we have analyzed some authentication goals. The following analyses are in response to the rest goals. Some assumptions and derivations in section 2.3 will be directly used and modified to use here.

1) Improved Yahalom Assumptions

P12' $B \lhd (\{A, N_B, K_{AB}\} K_{BS}, \{A, N_B\} K_{AB})$

P16' $B \mid\equiv B \lhd (\{A, N_B, <K_{AB}>_{*B}\} K_{BS}, \{A, N_B\} <K_{AB}>_{*B})$

P18' $B \mid\equiv B \lhd (\{A, N_B, <K_{AB}>_{*B}\} K_{BS}, \{A, N_B\} <K_{AB}>_{*B}) \rightarrow$

$B \mid\equiv B \lhd (\{A, N_B, A \xleftarrow{<K_{AB}>_{*B}} B, \#(<K_{AB}>_{*B})\} K_{BS}, \{A, N_B\} <K_{AB}>_{*B})$

P19 $A \lhd \{B, N_A\text{-}1\}K_{AB}$

P20 $A \mid\equiv A \lhd (\{B, N_A\text{-}1\}<K_{AB}>_{*A})$

P21 $A \mid\equiv A \lhd (\{B, N_A\text{-}1\}<K_{AB}>_{*A}) \wedge (A \mid\equiv A \xleftarrow{<K_{AB}>_{*A}} B) \rightarrow A \mid\equiv A \lhd (\{B, N_A\text{-}1, A \xleftarrow{<K_{AB}>_{*A}} B\}<K_{AB}>_{*A})$

In the above assumptions, P12', P16' and P18' are given by modifying P12, P16 and P18 in section 2.3. Meanwhile, the required assumptions P19, P20 and P21 are added to the assumption set because the improved protocol is added the fifth message.

2) Improved Yahalom Derivation for Alice

The first six steps analyses are the same as the analyses described in section 2.3.

(7) $A \mid\equiv B \mid\sim (B, N_A\text{-}1, A \xleftarrow{<K_{AB}>_{*A}} B)$
By A0, A1+MP, A3, P21 and (5)

(8) $A \mid\equiv B \ni <K_{AB}>_{*A}$
By A0, A1+MP, A3, P21 and (5)

(9) $A \mid\equiv B \mid\approx (B, N_A\text{-}1, A \xleftarrow{<K_{AB}>_{*A}} B)$
By A0, A17, A19, (6) and (7)

(10) $A \mid\equiv B \mid\equiv A \xleftarrow{<K_{AB}>_{*A}} B$
By A0, A14, A16 and (9)

(11) $A \mid\equiv B \mid\equiv \#(<K_{AB}>_{*A})$
By A0, A17, A19, P7 and (9)

3) Improved Yahalom Derivation for Bob

(1) $B \mid\equiv B \lhd (\{A, N_B, A \xleftarrow{<K_{AB}>_{*B}} B, \#(<K_{AB}>_{*B})\} K_{BS}, \{A, N_B\} <K_{AB}>_{*B})$
By A0, MP, P16' and P18'

(2) $B \mid\equiv B \lhd (\{A, N_B, A \xleftarrow{<K_{AB}>_{*B}} B, \#(<K_{AB}>_{*B})\} K_{BS})$
By A0, A1+MP, A7 and (1)

(3) $B \mid\equiv B \lhd (\{A, N_B\} <K_{AB}>_{*B})$
By A0, A1+MP, A7 and (1)

(4) $B \mid\equiv S \mid\sim (A, N_B, A \xleftarrow{<K_{AB}>_{*B}} B, \#(<K_{AB}>_{*B}))$
By A0, A3, P2 and (2)

(5) $B \mid\equiv S \mid\approx (A, N_B, A \xleftarrow{<K_{AB}>_{*B}} B, \#(<K_{AB}>_{*B}))$
By A0, A17, A19, P6, P8 and (4)

(6) $B \mid\equiv A \xleftarrow{<K_{AB}>_{*B}} B$
By A0, A14, A16, P4 and (5)

(7) $B \mid\equiv \#(<K_{AB}>_{*B})$
By A0, A17, A19, P6, P8 and (4)

(8) $B \mid\equiv B \lhd <K_{AB}>_{*B}$
By A0, A3, P2 and (2)

(9) $B \mid\equiv A \mid\sim (\{A, N_B\} <K_{AB}>_{*B})$
By A0, A3, (3), (6) and (8)

(10) $B \mid\equiv A \mid\approx (\{A, N_B\} <K_{AB}>_{*B})$
By A0, A17, A19, (7) and (9)

(11) $B \mid\equiv A \mid\equiv A \xleftarrow{<K_{AB}>_{*B}} B$
By A0, A14, A16 and (10)

(12) $B \mid\equiv A \mid\equiv \#(<K_{AB}>_{*B})$
By A0, A17, A19, P8 and (10)

The above analyses show that the improved Yahalom protocol meets the strong authentication goals.

IV. CONCLUSION

With the explosion of the Internet, electronic transactions have become more and more common. However the transactions' security is crucial to many applications, e.g. electronic commerce, digital contract signing, electronic voting, and so on. The problems of efficient entities identities authentication and key negotiation arouse broad attention of the researchers. Authentication protocols can resolve efficiently the above problems. However, their security must be analyzed strictly by using the formal methods. The SVO logic is an efficient formal method for analyzing authentication protocols. By employing the formal method, the paper analyzes the security of the Yahalom protocol. In addition, it also proposes an improved protocol and analyzes the objective and security of the protocol by the formal analytical process. The analyses indicate that the improved protocol satisfies the security goals.

REFERENCES

[1] M. Burrows, M.Abadi, R. Needham. "A logic of authentication". *ACM Transactions on Computer Systems (TOCS)*, 1990, vol.8, no.1, pp.18-36.

[2] Kohl JT, Neuman BC. "The Kerberos Network Authentication Service". *RFC1510*, 1993.

[3] Harkins D, Carrel D. "The Internet Key Exchange (IKE)". *RFC2409*, 1998.

[4] Paul F. Syverson. "A taxonomy of replay attacks". *In 7th Computer Security Foundations Workshop*, 1994, pp.187–191.

[5] Paul F. Syverson, Paul C. van Oorschot. "On Unifying Some Cryptographic Protocol Logics". *Proceedings of the IEEE Computer Society Symposium in Security and Privacy in Los Alamitos*, 1994, pp.14-28.

[6] J. Wen, M. Zhang, X. Li. "The study on the application of SVO logic in formal analysis of authentication protocols". *Proceedings of the 7th international conference on Electronic commerce*.2005, Vol.113, pp.744-747

[7] Gong L, Needham R, Yahalom R. "Reasoning about belief in cryptographic protocols". *In: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press*, 1990, pp.234-248.

[8] Abadi M, Tuttle MR. "A semantics for a logic of authentication". *In: Proceedings of the 10th ACM Symposium on Principles of Distributed Computing. ACM Press*, 1991, pp. 201-216.

[9] Van Oorschot PC. "Extending cryptographic logics of belief to key agreement protocols". *In: Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM Press*, 1993, pp. 233-243.