1000-9825/2001/12(11)1581-05 ©2001 Journal of Software 软件学报 Vol. 12, No. 11

Notes on 'A Simple Logic for Authentication Protocol Design'*

JI Qing-guang, FENG Deng-guo

(*Engineering Research Center of Information Security Technology, Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*)

E-mail: {qgji,fengdg}@ercist.iscas.ac.cn

http://www.ios.ac.cn

Received January 10, 2001; accepted April 28, 2001

Abstract: Buttyan *et al.* proposed a simple logic and used it to revise Woo-Lam protocol; without proving, they claimed that revised protocol is resistant against the interaction attacks between a protocol and itself. In this paper, in order to show that their results are incorrect, two different attacks on revised protocol are found out and set out in detail for their implementations. The fashions to construct the two attacks are essentially analogous to the ones described by Debbabi etc. except more complicated than them. The further analysis show that the logic of Buttyan etc. has no enough capacity to sufficiently capture protocol flaws, which stem from interaction of protocol itself. This logic needs to be improved.

Key words: protocol; interaction attack; security; modal logic; analysis

In formal methods of protocol verification, the approach to make use of modal logic is one of prevailing approaches. In order to verify security properties, the various kinds of modal propositions are posed. By means of inferring these propositions from logic system, modal logic has been successfully applied to discovery flaws in a variety of authentication protocols and has also been helpful in simplifying redundancy messages of protocols and understanding the basic concepts of security.

In Ref. [1], Buttyan etc. constructed a logic, belong to the BAN logic family. It combines channel with some concepts from GNY logic, and is a simple logic. The main advantage of this logic is that by means of choosing synthetic rules, the designer may make the most of this logic in the design process of protocol at a high abstraction level, without dealing with the problems of implementations. The authors claim that by using their synthetic method, they can generate a correction of the Woo and Lam symmetric key authentication protocol[2], which is resistant against the attacks that are presented in Refs. [2,3]. In this paper, we attempt to construct concrete attacks on the Buttyan-Staamann-Wilhelm's version of Woo-Lam protocol to show that though a protocol gets its logic goals presented in Ref. [1], it does not mean that this protocol has no analogous weakness found in Ref. [4]. That is to say, their logic is not enough to capture those flaws akin to ones in Ref. [1] and needs further improvement. In addition to, we will take into account other security characteristics of revised protocol.

---

* Supported by the National Grant Foundamental Research 973 Program of China under Grant No. G1999035802 (国家重点基础研究973发展规划); the National Outstanding Youth Foundation of China under Grant No. 60025205 (国家杰出青年基金)

JI Qing-guang was born in 1968. He is a Ph. D. student at the Engineering Research Center of Information Security Technology, Institute of Software, The Chinese Academy of Sciences. His research interests are formal analysis of computer securitysystems and security design of application system. **FENG Deng-guo** was born 1965. He is a research member and doctoral supervisor of the Institute of Software, The Chinese Academy of Sciences. His current research areas are information security and computer network security.

The balance of paper is organized as follows. In Section 1, we briefly review the Buttyan-Staamann-Wilhelm's version of Woo-Lam protocol. Section 2 describes the attacks upon the corrected protocol, and gives some analysis on reasons for inefficiency of logic in Ref. [1] when it is used to find out the attacks akin to ones presented in Ref. [4]. Finally, in Section 3, we conclude the paper.

1 The revised Woo-Lam Authentication Protocol

In order to show their logic useful, the authors of Ref. [1] use their logic to adapt original Woo-Lam protocol to be resistant against those attacks presented in Refs. [3,4]. The revised protocol is designed by using synthetic rules described in Ref. [1], and it satisfies with diverse logic goals expressed in Ref. [1]. This protocol is expected to reach that participant A authenticates itself to participant B with the help of an authentication sever S.

The revised protocol follows:

1. $A \to B: A$
2. $B \to A: B, N_b$
3. $A \to B: \{B, N_b\}_{K_{as}}$
4. $B \to S: A, \{B, N_b\}_{K_{as}}$
5. $S \to B: \{A, B, N_b\}_{K_{bs}}$

In this protocol, A sends its identifier to B, who responds with its identifier and a freshly generated nonce N_b. A encrypts B's identifier and the nonce with the key K_{as}, which is shared between A and S, and sends the result to B. B cannot decrypt this message, so B sends it to S together with A's identifier. S uses key K_{as} to decrypt the message and sends back to B the identifiers A, B and the nonce N_b encrypted with key K_{bs}, which is shared between B and S. Now, B can decrypt the message and it can verify if it received back its challenge, If so, it concludes that it talks with A.

2 Security Analysis

In this section, some security flaws of the revised protocol are pointed out. Especially, two attacks essentially similar to those presented in Ref. [4] are found out, this shows that the logic in Ref. [1] needs to be improved.

First we give the constructions of two attacks:

(1) Attack 1

1.1. $B \to I(A): B$

2.1. $I(A) \to B: A$

2.2. $B \to I(A): B, N_b$

1.2. $I(A) \to B: A, \{B, N_b\}$

1.3. $B \to I(A): \{A, B, N_b\}_{K_{bs}}$

2.3. $I(A) \to B: G$

2.4. $B \to I(S): A, G$

2.5. $I(S) \to B: \{A, B, N_b\}_{K_{bs}}$

where $I(A)$, $I(S)$ mean that intruder I respectively replaces A and S to execute protocol.

In this attack, the intruder I waits for some principal, say B, to begin a running protocol with some principal, say A. In the communication step "1.1.", intruder I gets the identifier of principal B by intercepting the message sent by this principal and the identifier of principal A by analyzing IP destination address; then, I initiates another protocol run with B claimed that his identifier is A, this is first step in session 2 (i.e. the protocol run enabled by I), and denoted as "2.1." in above; at second step of session 2, B responds with its identifier B and a freshly generated nonce N_b. After I received B and N_b, it substitutes for A to go on session 1 (i.e. running protocol initiated by B), at second step of session 1, I replies by identifier A and $\{B,N_b\}$ which is treated as freshly generated nonce since B cannot do any verification; in the step 3 of this session, B must react according to the protocol by sending the message $\{A,B,N_b\}_{K_{bs}}$.

While session 1 is proceeding, session 2 can be proceeded concurrently; at the step 3 of session 2, I can impersonate A to reply by message G which is any message since B cannot recognize it, or rather in protocol specification, B need not understand it; at step 4 of session 2, B must respond with message A,G.

When intruder I intercepts $\{A,B,N_b\}_{K_{bs}}$ and convinces itself the end of first four steps of session 2, then it may complete the masquerade in session 2 by replaying message $\{A,B,N_b\}_{K_{bs}}$ stemmed from session 1. At last, intruder I makes B believe that it talks with A.

In order to implement attack 1, we only assume that intruder can achieve principal's identifier to run protocol by intercepting IP packet and analyzing IP destination address, and a number of independent communication processes between two fixed principals can be enable concurrently. Clearly, these two postulates can easily be satisfied under the distributed network circumstance, so this attack is practical.

(2) Attack 2

1.1. $A\to I(B):A$

2.1. $I(A)\to B:A$

2.2. $B\to I(A):B,N_b$

1.2. $I(B)\to A:B,N_b$

2.3. $I(A)\to B:G$

1.3. $A\to I(B):\{B,N_b\}_{K_{as}}$

2.4. $B\to I(S):A,G$

1.4. $I(B)\to S:A,\{B,N_b\}_{K_{as}}$

1.5. $S\to I(B):\{A,B,N_b\}_{K_{as}}$

2.5. $I(S)\to B:\{A,B,N_b\}_{K_{bs}}$

where $I(A)$, $I(B)$, $I(S)$ have same means as previous attack 1.

In this scenario, the main session is session 2 where I is trying to convince B that it is the principal A. As same as attack 1, the intruder I waits for some principal, say A, to begin a running protocol with some principal, say B. In the communication step "1.1." (we called it first step of session 1), intruder I gets the identifier of principal A by intercepting the message sent by this principal and the identifier of principal B by analyzing IP destination address; then, I actively initiates another protocol run with B claimed that his identifier is A, this is session 2. In session 2, the intruder I sends the identifier A to the principal B which replies by sending its identifier B and a nonce N_b. After I accepts B and N_b, I pretends to be B to go on session 1, at second step of session 1, I replies by replaying message received in the step 2 of session 1; in the next, the session 1 and the session 2 can interleave to proceed. As explained previously, at step "2.3.", I can respond any arbitrary value G because B is unable to perform any verification on the received message. But at third step of session 1, A must react according to the protocol by sending message $\{B,N_b\}_{K_{as}}$. At step four of session 2, B replies by message A, G according to protocol specification. At step four of session 1, I impersonates B to send A, $\{B,N_b\}_{K_{as}}$ to authentication sever S. At fifth step of session 1, the authentication sever S is subject to protocol specification to generate message $\{A,B,N_b\}_{K_{bs}}$ and then sends it to I. After I received it, I replays it to B, this completes session 2.

The conditions to implement attack 2 are the same as ones in attack 1, but they are quite different. The implementation of attack 2 needs the help of authentication sever, but that of attack 1 does not. As far as intruder is concerned, it is more like man-in-the-middle in the attack 2 than in the attack 1.

In the sequel, we analyze the extensional characteristic of protocol security: in order to convince B that it talks with A and convince C that it talks with A should be different two goals, so if A can't distinguish them by execution of protocol, this protocol is hard to be considered to reach its goal. Moreover, if A can't ascertain whether or not B accepts A, the entity authentication of A to B should be failure (see Ref. [5]). If protocol's party whom A authenticates itself to is dishonest, the revised Woo-Lam protocol has those flaws mentioned above.

Suppose A concurrently expects to convince B and C that they talk with A, and C is of dishonesty. If in the second message of running this protocol, C responds A with B's identifier (instead of its own identifier) and a nonce N_c, while B responds A according to protocol specification, in this situation, A thinks it has already authenticated itself to B and failed to convince C of its identity, but in fact A has only proceeded to communicate with C. On the other hand, because A can't obtain any information on that B accepts A when it has done execution of the protocol, A has no good reasons for wishing to communicate with B, that is to say, this protocol can't completely reach its extensional goal of entity authentication described in Ref. [6].

To sum up analysis above, we think that there are some disadvantages and problems to use logic in Ref. [1] to design protocol.

1. The security properties to be considered in process of design are too simple, they are hard to reflect a variety of known attacks. Recently, Perrig and Song in Ref. [7] develop an approach to automatically generate security protocols, they consider the more security properties, such as correspondence and secrecy. But the method to be used in Ref. [1] is more concise than in Ref. [7].

2. Those attacks mentioned above show that the belief logic presented in Ref. [1] can't efficiently character security properties such as agreement described in Ref. [8]. How to improve this logic to make it possible to make do with agreement is useful.

3. We think that if a protocol to be designed by some formal method satisfies some formal security properties but not some intuitive requirements stemmed from experiences, this formal design method is not successful. The revised protocol in Ref. [1] violates some requirements presented in Ref. [9], for example, in order to resist oracle session attacks, the message format from one to another must be different from one another, since if so, one cryptographic message flow can never be used to derive the necessary message for another flow, but from attacks described above, the message format of the revised protocol can be utilized by intruders.

4. Whether can we give an example to show that we can check agreement properties defined by Lowe in Ref. [8], but the richer and perhaps more intuitive belief properties (including belief property in Ref. [1]) are out of reach? Recently, Hopper, Seshia and Wing in Ref. [10] compare the approach based on belief logic with one based on analysis data flow, and tend to think that they seem to present a certain complement.

3 Conclusion

In this paper, we point out that it is wrong that the authors of Ref. [1] intend to use their logic to adapt old Woo-Lam protocol to be resistant against similar to those attacks presented in Ref. [3,4], and we construct two attacks akin to those presented in Ref. [3,4]. Some remarks and problems are posed.

Acknowledgement We are very grateful to the anonymous referees for their useful suggestions. It is due to their suggestions that we provide two attack detailed explanation and improve this paper.

References:

[1] Buttyan, L., Staamann, S., Wilhelm, U. A simple logic for authentication protocol design. In: Simon Foley, Jonnathan Milien, eds. Proceedings of the 11th Computer Security Foundations Workshop. Massachusetts: IEEE Computer Society

Press, 1998. 153~162.

[2] Woo, T.Y.C., Lam, S.S. Authentication for distributed system. Computer, 1992,25(1):39~52.

[3] Abadi, M., Needham, R. Prudent engineering practice for cryptographic protocols. In: Li Gong, Ravi Sandu, eds. Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy. USA: IEEE Computer Society Press, May 1994. 122~136.

[4] Debbabi, M., Mejri, M., Tawbi, N., *et al*. A new algorithm for the automatic verification of authentication protocols: from specifications to flaws and attack scenarios. In: Proceedings of the DIMACS Workshop on Design and Formal Verification of Security Protocols. 1997. http://dimacs.rutgers.edu/workshops/security/programs/program.html

[5] Boyd, C. Towards extensional goals in authentication protocols. In: Proceedings of the DIMACS workshop on Design and Formal Verification of Security Protocols. 1997. http://dimacs.rutgers.edu/workshops/security/programs/program.html

[6] Roscoe, A.W. Intensional specifications of security protocols. In: Proceedings of the 9th Computer Security Foundations Workshop. Michael Merritt: IEEE Computer Society Press, 1996. 28~38.

[7] Perrig, A., Song, D. Looking for diamonds in the desert-extending automatic protocol generation to three-party authentication and key agreement protocols. In: Lee, E.S., Syverson, P. eds. Proceedings of the 13th Computer Security Foundations Workshop. Cambrides: IEEE Computer Society Press, 2000.

[8] Lowe, G. A heirarchy of authentication specifications. In: Foley, S., Millen, J., eds. Proceedings of the 10th Computer Security Foundations Workshop. Massachusetts: IEEE Computer Society Press, 1997.

[9] Bird, R., Gopal, I., Herzberg, A., *et al*. Systematic design of a family of attack-resistant authentication protocols. IEEE Journal on Selected Areas in Communications, 1993,11(5):679~693.

[10] Hopper, M.J., Seshia, S.A., Wing, J.M. Combining theory generation and model checking for security protocol analysis. Research Report CMU-CS-00-107, 2000.

关于“为设计认证协议的一个简明逻辑”一文的注记

季庆光，冯登国

(中国科学院 软件研究所 信息安全工程研究中心,北京 100080)

摘要：Buttyan 等人提出了一个简洁的逻辑,他们把它用于改进 Woo Lam 协议,并且未证明地声称:改进后的协议是抗协议与自身的交互攻击的.为表明他们的结论是不正确的,找到了改进协议的两个不同的攻击,并详细解释如何加以实现.构造攻击的方式除了要求更细致之外,与 Debbabi 等人的方式在本质上是相似的.进一步的分析表明 Debbabi 等人的逻辑没有足够的能力推理交互攻击,该逻辑有待改进.

关键词：协议;交互攻击;安全性;模态逻辑;分析

中图法分类号：TP309 **文献标识码**：A