并行攻击的讨论 [1]

田建波 郑 东 王育民

(西安电子科技大学 105 室 西安 710071)

摘 要 本文从 BAN 逻辑的语义角度讨论了并行攻击，并提出了对并行攻击的判断方法.

关键词 BAN 逻辑，语义，并行攻击

中图号 TM918

1 引 言

BAN 逻辑诞生以来，在对认证协议的安全分析方面取得了一定成功 [1,2]。但同时它又存在着局限性 [3−6]。为此 GNY[7]、AT[8]、SVO[9]、VO[10] 等类 BAN 逻辑对 BAN 逻辑在语法和语义上进行了扩展和完善，在一定程度上克服了 BAN 逻辑的局限性，使其分析能力得到了进一步提高。

BAN 逻辑的一个重要方面是其语义，只有一个完善的语义才能保证其语法规则的合理性. AT 中定义了协议的计算模型，并在此基础上提出了类 BAN 逻辑的语义。它定义了协议运行的概念，而且提出了好的协议运行的构造方法，进而在此基础上定义了信仰的含义。并且根据所定义的语义证明了其提出的逻辑公理是安全的。

而 SVO 类 BAN 逻辑，包括了 GNY、AT、VO 等类 BAN 逻辑和 BAN 逻辑的逻辑特征。而且用语义证明了其逻辑公理的正确性. 文献 [11] 中，语义的定义更加形式化和精确，其中定义了局部化信息 (Localized Message)： $(M)_p$ 和 $\mathrm{Sight}_p^{r,k}$。而且此类 BAN 逻辑对协议进行分析时，省去了对协议的理想化的步骤，从而避免了理想化协议时造成的模糊性。

从 BAN 逻辑的语义定义可以看出，其协议运行的定义中含有并行的思想。而任何一种 BAN 逻辑都没有一种能反应并行运行的语法规则 [12]。这是因为对协议进行分析，都是采用时间序列的方法，这样协议的并行运行的时间都是现在。如果协议设计的不合理，并行协议运行可能会相互影响，造成并行攻击。本文提出一个简单的判断方法，来判定是否存在着并行攻击。

2 并行攻击的判别

2.1 定义

(1) 协议运行 R 一次协议运行 R 是主体的行为 $H^{r,k}$ 的序列，即 $R=\{H^{r,k}|k\geq 0\}$, 其中 $H^{r,k}$={ 信息接收 (M), 信息发送 (M,Q), 信息生成 (M)}。

从以上协议运行的定义可以看到在一个协议运行的时间 $0\leq k_r\leq k'$ 中，可能同时存在数个协议运行 R_i, $\{1\leq i\leq n\}$。说明了一个系统中可以并行存在几个协议运行。而这时表示协议中所传送消息新鲜性的一次性随机数，显然起不到相应的新鲜性的作用。这是因为本次协议运行 R_i 中任何一个一次性随机数的使用，都可以被另一个并行的协议运行 R_j 使用. 这样有可能被外在的对手利用达到攻击目的。实际上存在的并行攻击，恰恰是攻击者采用并行的协议运行，由一次协议运行所得的结果应用到同时存在的另一次协议运行中获得了攻

[1] 1997-12-16 收到，1998-12-11 定稿
国家自然科学基金和国防预研基金资助

击的成功. 这时的结果是通信主体 P 、 Q 中的任一方和攻击者 P_e 所理解的信息的意义相同. 即 $(M)_p = (M)_{p_e}$ 或 $(M)_Q = (M)_{p_e}$ 。

(2) 敏感信息 受保护的信息 (除通信主体外), 如受保护的一次性随机数, 密钥。

2.2 判别方法

(1) 如在一次协议运行 R_i 期间, 通信中的任一方 P 同时又涉及另外的一个协议运行 R_j, 这时定义对敏感信息 (除通信主体外) 的比较: $C = \text{Compare}(\text{recognizes}_p^{r_i}(M^i) = \text{recognizes}_p^{r_j}(M^j))$, 如果 C 是 "真", 则 P 断定有人在进行并行攻击。如 (1) 不成立, 则转 (2),

(2) 当任何一个通信主体 P 知道自己涉及两个并行协议运行 R_i 、 R_j 时, P 把其中一个协议运行 R_i 发送的信息替代另外的一个协议运行 R_j 中 P 所发送的信息, 然后来观察是否有重要的信息泄漏来判断是否存在着并行攻击。即

第一步 赋值 $\text{Send}(M^i)$=$\text{Send}(M^j)$ 。

第二步 执行协议 R^j 。

如果有敏感信息泄露, 则有并行攻击。

2.3 例子

例 1 图 1 中, N_B 是一次性随机数. 此认证协议可以被攻击者进行并行攻击. 攻击如图 2 所示。

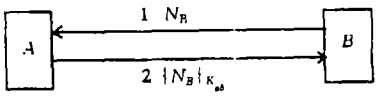

图 1 激励 - 响应协议

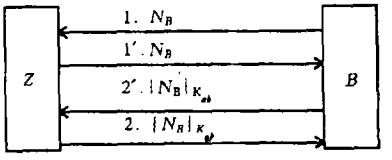

图 2 并行攻击

说明 Z 为了冒充 A 而获得 B 的认证, 当收到 B 发送的信息 N_B 后, 又冒充 A 并行地发起了一次协议运行, 使用的还是一次性的随机数 N_B, B 收到后, 响应发出 $\{N_B\}_{K_{ab}}$, Z 收到响应后, 把其应用到前面的协议运行, 从而获得 B 的认证。

如果 B 应用判别方法, B 意识到本身涉及两个并行的协议运行 R_i, R_j, 则 B 进行判断: $C = \text{Compare}(\text{recognizes}(M1 = N_B) = \text{recognizes}(M2 = N_B))$, 则 C 是 "真"。则 B 认为有并行攻击, 停止本次协议运行。

例 2 认证协议如图 3 。

(1) $A \to B$: $A, \{N_a, A\}_{K_{as}}$ 。

(2) $B \to S$: $A, B, \{N_a, A\}_{K_{as}}\ \{N_b, B\}_{K_{bs}}$ 。

(3) $S \to A$: $\{K_{ab}, B\}_{K_{bs}}, \{N_b, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}}$ 。

(4) $A \to B$: $\{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$ 。

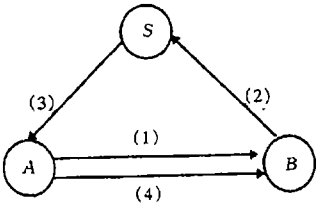

图 3

攻击者 C

(1) $A \to C_b$:　$A, \{N_a, A\}_{K_{as}}$ 。

(1') $C \to A$:　$C, \{N_c, C\}_{K_{cs}}$ 。

(2') $A \to S$:　$C, A, \{N_c, C\}_{K_{cs}}, \{N_a, A\}_{K_{as}}$ 。

(3') $S \to C$:　$\{K_{ca}, A\}_{K_{cs}}, \{N_c, N_a, \{K_{cb}, C, N_a\}_{K_{as}}\}_{K_{ca}}$ 。

(2) 略。

(3) $C_s \to A$:　$\{K'_{ab}, B\}_{K_{as}}, \{N_a, N_c, \cdots\cdots\}_{K'_{ab}}$ 。

(4) $A \to B$:　$\cdots\cdots$ 。

上面的攻击者 C 假冒 B 进行攻击的前提是 C 曾经窃听过 A 、 B 之间的通信并获得过信息 $\{K'_{ab}, B\}_{K_{as}}$ 而且破译了会话密钥 K'_{ab}, 这样在 (3') 步获得 A 所发送的随机数 N_a 后，在第 (3) 步重放 $\{K'_{ab}, B\}_{K_{as}}$ ，而且进行了伪造发给 A ，攻击成功。

判断 当攻击协议开始运行时，主体 A 知道自己涉及两次并行协议运行，首先 (1) 不成立，则转 (2)： A 发送了两次信息 $(1) = M_1$ 、 $(2') = M_2$, A 用 M_1 替代 M_2, 然后执行协议运行，这时 N_a 就会被 A 发现泄漏。由此判断此协议可以被并行攻击。

3 结　论

本文对认证协议的并行攻击进行了讨论，提出了判别方法，因为无法把认证协议理想化为并行协议，所以有必要提出抗并行攻击的方法。

参　考　文　献

[1] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transacation on Computer Systems, 1990, 8(1): 18–36.

[2] Gaarder P, Snekkenes E. Applying a formal analysis technique to CCITT X.509 strong two-way authentication protocol, Journal of Cryptology 1991, (3): 81–98.

[3] Boyd C, Mao W. On a Limitations of BAN Logic. In Lecture Notes in Computer Science 765Advances in Cryptology-Eurocrypt'93, Lofthus Norway: Springer-Verlag, 1993, 240–247.

[4] Wenbo Mao. An augmentation of BAN-like logics. 8th IEEE Computer Security Foundations Workshop, Dromquinna Manor Kenmare County Kerry, Ireland: 1995, 44–58.

[5] Paul F. Syverson. A new look at old protocol. Operating System Review, 1997, 31(1): 1–4.

[6] Nessett D M. A Critique of Burrows, Abadi and Needham Logic, Operating Systems Review, 1990, 24(2): 35–38.

[7] Li Gong, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. In Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California: 1990, 234–248.

[8] Abadi M, Tuttle M. A semantics for a logic of authentication. In Proceedings of the Tenth ACM Symposium on Principles of Distributed Computing, ACM Press, Sanantonio, Texas: 1991, 201–216.

[9] Syverson P, Van Oorschot P C. On unifying some cryptographic protocol logics. In Proceeding of 1994 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Okland California: 1994.

[10] Van Oorschot P C. Extending cryptographic logics of belief to key agreement protocols(Extended Abstract). In Proceeding of the First ACM Conference on Computer and Communications Security, Faixfax Virginia: 1993, 232–243.

[11] Wedel G, Kessler V. Formal semantics for authentication logics. Computer Security—ESORICS'96, United Kingdom: 1996, 219–239.

[12] Kesser V, Wedel G. AUTOLOG-An Advanced Logic of Authentication. Proc. of the Computer Security Foundations Workshop VII, Franconia, IEEE Computer Society Press. New Hampshire: 1990, 90–94.

THE DISCUSSION OF PARALLEL ATTACK

Tian Jianbo Zheng Dong Wang Yumin

(*Xidian University, Xi'an* 710071)

Abstract The parallel attack is discussed in this paper from the semantics, and the method of decision is presented.

Key words BAN Logic, Semantic, Parallel attack

田建波： 男， 1971 年生，博士生，研究方向：密码学.

郑 东： 男， 1964 年生，博士生，研究方向：密码学.

王育民： 男， 1936 年生，教授，博士生导师，研究方向：网络安全，信道编码，密码.