对两个双方密码协议运行模式的攻击及改进*)

姬东耀　冯登国

(中国科学院研究生院信息安全国家重点实验室　北京100039)

Attack on and Improvement of the Running Mode of the Two-Party Cryptographic Protocols

JI Dong-Yao, FENG Deng-Guo

(State Key Laboratory of Information Security, Graduate School, Chinese Academy of Sciences, Beijing, 100039, China)

Abstract In this paper, the running modes of the two-party cryptographic protocols are used to analyze the two authentication and key agreenment protocols, and attack on the protocols is discovered. Finally, two improved protocols are given.

Keywords Cryptographic protocol, Information security, Protocol analysis

1. 引言

密码协议是许多分布式系统安全的基础，确保这些协议能够安全运行是十分重要的。虽然认证与密钥建立协议中仅仅进行很少的几组消息传输，但是其中的每一消息的组成都是经过巧妙设计的，而且这些消息之间有着复杂的相互作用和制约。而目前密码协议设计多采用非形式的方法，以致于一个协议使用多年后才发现它有安全漏洞[1,2](如 NS 公钥协议，TMN 协议)。如何发现并弥补协议的安全漏洞，从而增强协议的安全性，不给以后的使用留下安全隐患，无疑是一件有意义的工作，目前的协议分析方法主要有：直观的分析、实际攻击手段的测试、形式化的逻辑推理和模型检验。其中后者以手段严密和分析自动化而见长，但在形式化逻辑分析中，协议理想化过程的非形式化常常导致分析错误；模型检验则有搜索状态空间太大的缺陷。在运用形式化逻辑和模型检验分析双方密码协议方面已有大量工作，文中考察了攻击者存在的情况下双边通信可能存在攻击的7种运行模式[3]：

(1) A⇒B　(2)A⇒I; I⇒B　(3)A⇒I; I(A)⇒B

(4)A⇒I(B)　(5) A⇒I(B);I⇒B

(6) A⇒I(B); I(A)⇒B　(7) I(A)⇒B

其中 X⇒Y 表示：X 是一个协议引发者，Y 是一个响应者，X 和 Y 进行一次协议运行；I(x)表示 I 模仿 X 和另一方运行协议。在这7种模式上对两个认证与密钥建立协议 AKA 和 SSH 进行了分析，发现了这两个协议中受到的攻击，并对它们进行了改进。

2. 自治的密钥授权(AKA)协议

2.1 协议描述

AKA 协议有几个变体，但它们都有类似的消息，我们分析其中典型的一个[4]。这种情况下协议是：

消息1　$A\rightarrow B: K_A$

消息2　$B\rightarrow A: K_{Bk}, K_{B_t}$

消息3　$A\rightarrow B: \{N_A, A\}_{K_{B_t}}$

消息4　$B\rightarrow A: \{N_B\}_{K_A}$

消息5　$B\rightarrow A: \{\{N_A\}_{K_{Bk}^{-1}}\}_{K_A}$

消息6　$A\rightarrow B: \{H(N_B)\}_{K_{B_t}}$

这个协议的目标是建立 $N_A\oplus N_B$ 作为其后 A 和 B 之间通信的会话钥，在消息1和2中，A 和 B 交换公钥；其中 K_{Bk} 为 B 的长期公钥，K_{Bk}^{-1} 为其对应的私钥，K_{B_t} 为 B 的一次性服务钥；在消息3和4中，A 和 B 交换随机数 N_A 和 N_B，这两个随机数用来导出其后的会话钥；在消息5中，B 用他的私钥 K_{Bk}^{-1} 对随机数 N_A 签字并发给 A；最后，在消息6中，A 计算随机数 N_B 的 HASH 值并用 B 的一次性服务钥 K_{B_t} 加密发给 B。因为使用了公钥及一次性密钥加密，在消息3、4和5中随机数的秘密得到了保护，我们可以推断只有 A 和 B 知道最后导出的会话钥。

2.2 协议上的一个攻击

我们按照上述7种运行模式逐一执行协议，在其中模式(6)A⇒I(B);I(A)⇒B 上执行 AKA 协议发现了一个攻击者 I 通过截取消息既假冒协议引发者又假冒响应者的两次运行攻击。这一攻击发生在 A 和 B 开始一个正常会话时，假定攻击者 I 能截取(接收方不能收到)和替换一些消息，而且 I 不需要是系统的一合法用户。

消息1　$A\rightarrow B: K_A$

消息2　$B\rightarrow\cdots: K_{Bk}, K_{B_t}$

消息2'　$I(B)\rightarrow A: K_{Bk}, K_{I_t}$

消息3　$A\rightarrow\cdots: \{N_A, A\}_{K_{I_t}}$

消息3'　$I(A)\rightarrow B: \{N_A, A\}_{K_{B_t}}$

消息4　$B\rightarrow\cdots: \{N_B\}_{K_A}$

消息4'　$I(B)\rightarrow A: \{N_I\}_{K_A}$

消息5　$B\rightarrow A: \{\{N_A\}_{K_{Bk}^{-1}}\}_{K_A}$

消息6　$A\rightarrow\cdots: \{H(N_I)\}_{K_{I_t}}$

其中 $A\rightarrow\cdots$ 表示这条消息被攻击者 I 截取，接收方不能收到。I 首先截取消息2，用他自己的临时密钥 K_{I_t} 替换 B 的一次性服务钥 K_{B_t}，并假冒 B 发给 A，这一替换使得攻击者 I 可以得到 A 在消息3中所发的随机数 N_A；I 截取了消息3之后，产生一个和原协议中消息3相同的消息3'发给 B；I 然后截取消息4，把他自己产生的随机数 N_I 用 A 的公钥 K_A 加密发给 A，并让消息5通过，截取消息6。这样 I 虽然不能和 B 进一步通信，但他却欺骗了 A，使 A 相信 $N_A\oplus N_I$ 是 A 和 B 共享的会话密

*)国家自然科学基金(60273029)。

钥，但事实上 I 也有 $N_A \oplus N_I$。

2.3 一个改进的 AKA 协议

只要在消息5中 B 的签名域上加上他的长期和短期公钥的 HASH 值就可以挫败此攻击。

消息1 $A \rightarrow B: K_A$

消息2 $B \rightarrow A: K_{Bh}, K_{Bs}$

消息3 $A \rightarrow B: \{N_A, A\}_{K_{Bs}}$

消息4 $B \rightarrow A: \{N_B\}_{K_A}$

消息5 $B \rightarrow A: \{\{N_A, H(K_{Bh}, K_{Bs})\}_{K_{Bh}^{-1}}\}_{K_A}$

消息6 $A \rightarrow B: \{H(N_B)\}_{K_{Bs}}$

这样由 $H(K_{Bh}, K_{Is}) \neq H(K_{Bh}, K_{Bs})$ A 就可以发现错误，使得攻击者 I 无法欺骗 A。

3. 安全登录连接(SSH)协议

3.1 协议描述

SSH 协议是草拟的 Internet 安全协议中的一个认证与密钥分配协议，它也有几个变体[5]，这里我们仅考察服务器 B 利用公钥认证客户 A 的情况。这种情况下协议是：

消息1 $A \rightarrow B: N_A$

消息2 $B \rightarrow A: N_B$

消息3 $B \rightarrow A: K_{Bh}, K_{Bs}$

消息4 $A \rightarrow B: \{\{H(previous.msge), k\}_{K_{Bs}}\}_{K_{Bh}}$

消息5 $A \rightarrow B: \{A, K_A, \{H(A, N_A, N_B)\}_{K_A^{-1}}\}_{K'}$

传递这些消息是为其后 A 和 B 之间通信建立会话密钥 K。在消息1和2中，A 和 B 交换随机数 N_A 和 N_B；消息3中 B 提供他的长期公钥和短期服务公钥 K_{Bh} 和 K_{Bs}；消息4中，A 把会话密钥 K 用 B 的两个公钥加密后传给 B，其中包含先前传递消息的 HASH 值；消息5中，A 提供他的身份 A 及公钥 K_A，并对他的身份及随机数 N_A 和 N_B 的单向 HASH 值用他的私钥 K_A^{-1} 签名，这些消息都用他们其后要共享的密钥 K` 加密，且 K` 可从 K、N_A 及 N_B 导出。通过这个协议的运行服务器 B 对用户 A 的身份获得认证，同时建立了一会话密钥 K`。

3.2 协议上的一个攻击

我们同样按照上述7种运行模式逐一执行协议，在其中模式(2)A⇒I;I⇒B 上执行 SSH 协议发现了一个攻击者 I 既作协议引发者又作响应者的两次运行攻击：

消息1 $A \rightarrow I: N_A$

消息1' $I \rightarrow B: N_A$

消息2' $B \rightarrow I: N_B$

消息2 $I \rightarrow A: N_B$

消息3' $B \rightarrow I: K_{Bh}, K_{Bs}$

消息3 $I \rightarrow A: K_{Ih}, K_{Is}$

消息4 $A \rightarrow I: \{\{H(previous.msgs), K\}_{K_{Is}}\}_{KIh}$

消息4' $I \rightarrow B: \{\{H(previous.msgs), K\}_{K_{Bs}}\}_{KBh}$

消息5 $A \rightarrow I: \{A, K_A, \{H(A, N_A, N_B)\}_{K_A^{-1}}\}_K$

消息5' $I \rightarrow B: \{A, K_A, \{H(A, N_A, N_B)\}_{K_A^{-1}}\}_{K'}$

在该攻击中，入侵者 I 是网络中一合法服务器且具有长期和短期公钥 K_{Ih}, K_{Is}，它能模仿 A 与 B 会话，而且只要在 A 和 I 开始一个正常会话时该攻击就是可能的。当 A 和 I 开始会话时，I 立刻开始和 B 会话以确保两个会话中随机数是一样的，从而 I 能在和 B 的会话中使用 A 的签名消息。这样 B 认为他和 A 使用会话密钥 K 开始了一个会话，事实上 I 也有此会话密钥 K，而且 A 也不会立刻发现错误。

3.3 一个改进的 SSH 协议

为了抵抗此攻击，我们可以在 A 的签名域中增加一些元素，如 B 的身份、证书、公钥或会话钥 K 的 HASH 值。

消息1 $A \rightarrow B: N_A$

消息2 $B \rightarrow A: N_B$

消息3 $B \rightarrow A: K_{Bh}, K_{Bs}$

消息4 $A \rightarrow B: \{\{H(previous.msgs), K\}_{K_{Bs}}\}_{K_{Bh}}$

消息5 $A \rightarrow B: \{A, K_A, \{H(A, B, H'(K), N_A, N_B)\}_{K_A^{-1}}\}_{K'}$

这样 I 就不能在和 B 的会话中使用 A 的签名消息，从而不能欺骗 B。

结束语 我们运用双方密码协议的运行模式分析了两个认证与密钥分配协议，从中可以发现这两协议有一共同弱点，就是签名域没有包含足够的信息，从而留下安全隐患。实际上，这也是一类利用签名进行认证的协议设计共有的问题，仔细设计签名域以抵抗攻击者的假冒应该是这类协议设计遵循的一个原则。

参 考 文 献

1 Lowe G, Rosse B. Using CSP to detect errors in the TMN protocols. IEEE Transactions on software engineering. 1997, 23(10): 659～669

2 Lowe G. Breaking and fixing the needham-schroeder public-key protocol using FDR. In: Proc. of TACAS(Tools and Algorithms for the Construction and Analysis of Systems), vol. 1055, Springer Verlag, 1996. 147～166

3 Zhang yuqing, Li Jihong, Xiao Guozhen. An approach to the formal verification of the two-party cryptographic protocols. ACM Operating System Review, 1999, 33(4): 48～5

4 Safford D, Schales D, Hess D. Texas A&M University anarchistic key authorization. In: Proc. of the Sixth Usenix Security Symposium, New york, 1996. 179～185

5 Ylonen T. SSH--secure login connections over the internet. In: Proc. of the Sixth Usenix Security Symposium, New york, 1996. 37～42

(上接第68页)

2 Honavar V, Miller L, Wong J S K. Distributed knowledge networks. In: Proc. IEEE Information Technology Conf. Syracuse, NY, USA, Sep. 1998. 87～90

3 Jansen W, Mell P, Karygiannis T, Marks D. Mobile agents in intrusion detection and response. In: Proc. of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada, June 2000

4 ObjectSpace, Inc., Dallas, TX. ObjectSpace Voyager Core Technology User Guide, Version 3.0.0, 1999

5 Sun Microsystems. Java Development Kit Version 1.2.x. Online, September 2001. http://www.javasoft.com/products/jdk/1.2.

6 蒋建春，马恒太，任党恩，卿斯汉. 网络安全入侵检测：研究综述. 软件学报，2000, 11(11): 1460～1466