第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0176—02 文献标识码：A 中图分类号：TP309

Yahalom协议及其变体的时序缺陷分析与改进

陶宏才，何大可
(西南交通大学信息科学与技术学院，成都 610031)

摘 要：研究 Yahalom 协议及其变体，发现该系列协议存在的时序缺陷，给出一种利用此缺陷攻击 Yahalom 协议及其变体的方法。尽管 Yahalom 协议历经几次修改，且被证明不存在密钥泄露问题，但 Yahalom 协议及其变体仍然存在以前没有被关注过的时序缺陷。该文从时序角度对 Yahalom-Paulson 协议进行改进。改进后的协议保持了原协议的安全性，同时能抵御原来因时序缺陷所引起的攻击。
关键词：安全协议；Yahalom 协议；协议时序；时序缺陷；安全攻击

Analysis and Improvement of Sequence Flaw for Yahalom Protocol and Its Variants

TAO Hong-cai, HE Da-ke
(School of Information Science & Technology, Southwest Jiaotong University, Chengdu 610031)

【Abstract】 This paper researches the Yahalom protocol and its variants, finds a sequence flaw existing in them and provides a kind of method to attack them by using the flaw. The Yahalom protocol has been revised several times, and no key-compromise problem is proved in the final Yahalom-Paulson protocol, but the Yahalom protocol and its variants still have the sequence flaw which has never been paid attention before. The Yahalom-Paulson protocol is improved from the angle of sequence. The improved Yahalom-Paulson protocol preserves the security of the original protocol, and can resist the attack caused by the sequence flaw.
【Key words】 security protocol; Yahalom protocol; protocol sequence; sequence flaw; security attack

协议设计人员在安全协议的设计中，对作为协议重要成分之一的时序未引起足够重视。所谓协议时序，是协议规定的协议主体“发送-接收”(简称收发)消息的次序序列。事实上，如果协议的这个收发次序序列设计得不好，可能会使协议时序本身存在缺陷。而时序本身的缺陷会削弱协议的安全性，并且时序缺陷有时无法通过协议其他部分的设计来弥补。Yahalom协议[1]及其变体[2]在这一点上表现得尤为突出。

1 Yahalom协议及其变体概述

Yahalom协议[1]由Yahalom于1988年提出，描述如下：

(1)$A\rightarrow B$: A, N_a

(2)$B\rightarrow S$: B, $\{A, N_a, N_b\}K_{bs}$

(3)$S\rightarrow A$: $\{B, k_{ab}, N_a, N_b\}K_{as}$, $\{A, k_{ab}\}K_{bs}$

(4)$A\rightarrow B$: $\{A, k_{ab}\}K_{bs}$, $\{N_b\}k_{ab}$

Yahalom协议的目标是由可信第三方(Trusted Third Party, TTP)[3]服务器S为协议主体A和B生成并分发新鲜的共享对称密钥k_{ab}，同时完成A和B间的相互认证。

文献[1]给出了一个修订后的 Yahalom 协议，称为 BAN simplified (amended) version of Yahalom，或称 BAN-Yahalom 协议，描述如下：

(1)$A\rightarrow B$: A, N_a

(2)$B\rightarrow S$: B, $\{A, N_a\}K_{bs}$, N_b

(3)$S\rightarrow A$: $\{B, k_{ab}, N_a\}K_{as}$, $\{A, k_{ab}, N_b\}K_{bs}$, N_b

(4)$A\rightarrow B$: $\{A, k_{ab}, N_b\}K_{bs}$, $\{N_b\}k_{ab}$

与原协议相比，N_b被加到消息(3)的第2个加密消息块中，以阻止恶意的A重用一个陈旧的密钥k_{ab}。不过，BAN- Yahalom协议仍存在以下2种攻击[4]。

第1种攻击如下：

(1.1)$A\rightarrow B$: A, N_a

(1.2)$B\rightarrow S$: B, $\{A, N_a\}K_{bs}$, N_b

(2.1)$I(A)\rightarrow B$: A, (N_a, N_b)

(2.2)$B\rightarrow I(S)$: B, $\{A, N_a, N_b\}K_{bs}$, N'_b

(1.3)…

(1.4)$I(A)\rightarrow B$: $\{A, N_a (=k_{ab}), N_b\}K_{bs}$, $\{N_b\}k_{ab}$

攻击者I在协议第2轮，假冒A将N_a和N_b连接作为临时值发给B，最后I在第(1.4)步向B冒充A而获得会话密钥。

第2种攻击如下：

(1.1)$A\rightarrow I(B)$: A, N_a

(2.1)$I(B)\rightarrow A$: B, N_a

(2.2)$A\rightarrow I(S)$: A, $\{B, N_a\}K_{as}$, N'_a

(3.2)$I(A)\rightarrow S$: A, $\{B, N_a\}K_{as}$, N_a

(3.3)$S\rightarrow I(B)$: $\{A, k_{ab}, N_a\}K_{bs}$, $\{B, k_{ab}, N_a\}K_{as}$, N_a

(1.2)…

(1.3)$I(S)\rightarrow A$: $\{B, k_{ab}, N_a\}K_{as}$, $\{A, k_{ab}, N_a\}K_{bs}$, N_i

(1.4)$A\rightarrow I(B)$: $\{A, k_{ab}, N_a\}K_{bs}$, $\{N_i\}k_{ab}$

为阻止对 BAN-Yahalom 协议的上述攻击，文献[2]修订了 BAN-Yahalom 协议，得到 Yahalom-Paulson 协议，描述

基金项目：成都市科技攻关计划基金资助项目(07GGYB050GX)
作者简介：陶宏才(1964－)，男，副教授、博士，主研方向：信息安全，网络与信息系统；何大可，教授、博士生导师
收稿日期：2007-10-12 **E-mail：**taohongcai@126.com

如下：

(1)$A\rightarrow B$: A, N_a

(2)$B\rightarrow S$: B, N_b, $\{A, N_a\}K_{bs}$

(3)$S\rightarrow A$: N_b, $\{B, k_{ab}, N_a\}K_{as}$, $\{A, B, k_{ab}, N_b\}K_{bs}$

(4)$A\rightarrow B$: $\{A, B, k_{ab}, N_b\}K_{bs}$, $\{N_b\}k_{ab}$

在 Yahalom-Paulson 协议中，B 的名字被加入到消息(3)的第 2 个加密块中，并由 A 在消息(4)传给 B。

由上所述，尽管 Yahalom 协议几经修订，但其协议各步的收发主体及次序均保持未变，仍为：$A\rightarrow B$,$B\rightarrow S$,$S\rightarrow A$,$A\rightarrow B$，称其为 Yahalom 协议时序。

2 协议时序缺陷分析

由第 1 节协议描述可知，该协议时序各步的用意大致为：

(1)A 告诉 B 想与其通信；

(2)B 为认证 A，将 A 的消息发给 S；

(3)S 产生 A 与 B 的会话密钥，加密后传给 A，同时还有需要转发给 B 的含有此密钥的消息块(A 不能解密)；

(4)A 将含有密钥的消息块发给 B，从而完成 B 对 A 的认证。

仅从协议时序看，该时序可达到认证性目标，协议主体的消息交换也是紧凑、高效的。不过，在协议主体 A 与 B 的直接消息交换过程中，只有 A 到 B 方向的，即 $A\rightarrow B$，没有 B 到 A 方向的。也就是说，主体 A 在协议执行过程中始终未得到过来自 B 的直接响应，这是该协议时序最大的问题。尽管 Guttman 在文献[5]中通过一系列的入测试(incoming test)证明了 Yahalom-Paulson 协议不存在密钥泄露(key compromise)问题，但该协议仍然存在如下欺骗主体 A 的攻击：

(1.1)$A\rightarrow I(B)$: A, N_a

(2.1)$I(A)\rightarrow B$: A, N_a

(2.2)$B\rightarrow S$: B, N_b, $\{A, N_a\}K_{bs}$

(2.3)$S\rightarrow I(A)$: N_b, $\{B, k_{ab}, N_a\}K_{as}$, $\{A, B, k_{ab}, N_b\}K_{bs}$

(1.2)…

(1.3)$I(S)\rightarrow A$: N_i, $\{B, k_{ab}, N_a\}K_{as}$, bit-string

(1.4)$A\rightarrow I(B)$: bit-string, $\{N_i\}k_{ab}$

导致以上攻击的根本原因，正是由于主体A在协议执行过程中始终未得到过来自B的直接响应。显然，这是由该协议时序本身的先天不足带来的，并且无法纯粹通过协议消息的设计来克服。以上攻击不仅对Yahalom-Paulson协议有效，对具有相同时序的Yahalom协议和BAN-Yahalom协议也是有效的[6]。

3 协议时序改进

Yahalom协议的时序满足认证性及高效性[7]，但在安全协议的设计中，仅满足这 2 点是不完整的，还应该考虑因时序缺陷造成的协议安全攻击。由上分析可知，Yahalom协议及其变体的时序存在致命的缺陷，这种时序本身固有的缺陷使得协议易遭受欺骗A的攻击，导致其安全性在一定程度上的削弱。因此，需要从时序上对协议进行改进。

为表述方便，称 Yahalom 协议及其变体的现有时序为原时序。在改进协议时序时，应注意以下 2 点：

(1)尽量不改变或打乱原时序的模式[7]，以保证原时序的完整。毕竟，原时序满足认证性和高效性，改变或打乱原时序模式，会使改进的协议与原协议面目全非。

(2)为提高协议的抗攻击能力或安全性，应消除协议时序中协议主体之间直接消息交换的单向性，即 2 个协议主体之间既要有直接的发送还要有直接的接收。此处的协议主体，是指协议中需要进行实质通信的主体，不包括 TTP。所谓直接的发送或接收，是指 2 个协议主体之间的消息交换不是通过 TTP 来转发的，否则称为间接发送或接收。如果某个主体在一次协议会话中只参与直接接收而没有直接发送(或只有直接发送而没有直接接收)，则该协议极易受到欺骗攻击或假冒攻击。为此，通过消除协议时序中协议主体之间直接消息交换的单向性，即可避免这类协议攻击。

由上述分析可知，Yahalom 协议原时序最大的问题，是主体 A 在协议执行过程中始终未得到过来自 B 的直接响应。针对这一问题，并结合以上 2 点注意事项，对 Yahalom-Paulson 协议的改进如下：

(1)$A\rightarrow B$: A, N_a

(2)$B\rightarrow S$: B, N_b, $\{A, N_a\}K_{bs}$

(3)$S\rightarrow A$: N_b, $\{B, k_{ab}, N_a\}K_{as}$, $\{A, B, k_{ab}, N_b\}K_{bs}$

(4)$A\rightarrow B$: $\{A, B, k_{ab}, N_b\}K_{bs}$, $\{N_b\}k_{ab}$

(5)$B\rightarrow A$: $\{N_a\}k_{ab}$

改进后的协议在原协议基础上，增加了主体 B 直接响应 A 的第(5)步。显然，改进后的协议既保持了 Yahalom-Paulson 协议的认证性、高效性和安全性，同时还能够抵御上述欺骗 A 的攻击。

4 结束语

通过对 Yahalom 协议、其变体时序缺陷以及引起的攻击的分析，充分地说明了协议时序的固有缺陷将导致协议存在安全攻击。分析结果表明，在协议的设计过程中，应该重视协议时序的设计，以避免因协议时序缺陷导致协议安全性的削弱。

参考文献

[1] Burrows M, Abadi M, Needham R. A Logic of Authentication[R]. Digital Systems Research Center, Palo Alto, Technical Report: 39, 1989.

[2] Paulson L C. Relations Between Secrets: Two Formal Analyses of the Yahalom Protocol[J]. Journal of Computer Security, 2001, 9(3): 197-216.

[3] 鲁荣波, 何大可, 缪祥华. 一种原子性和公平匿名性的电子支付协议[J]. 计算机工程, 2006, 32(17): 30-31, 34.

[4] Syverson P. A Taxonomy of Replay Attacks[C]//Proc. of the 1994 IEEE Computer Security Foundations Workshop VII. Los Alamitos, USA: IEEE Computer Society Press, 1994: 187-191.

[5] Guttman J D. Key Compromise, Strand spaces, and the Authentication Tests[C]//Proc. of the 7th Conference on the Mathematical Foundations of Programming Semantics, Electronic Notes in Theoretical Computer Science. London, UK: Springer-Verlag, 2001: 141-161.

[6] Xu Chong, Kedem G, Gong Fengmin. Categorizing Attacks on Cryptographic Protocols Based on Intruders Objectives and Roles[EB/OL]. (2001-09-20). http://citeseer.ist.psu.edu/xu00categorizing.html.

[7] Tao Hongcai, He Dake. Sequence Patterns of Identity Authentication Protocols[J]. Journal of Southwest Jiaotong University: English Edition, 2006, 14(3): 205-211.