

文章编号:1001-9081(2011)11-2994-03

doi:10.3724/SP.J.1087.2011.02994

一种新的双方认证密钥协商协议的安全性分析

周四方

(永州职业技术学院 计算机系,湖南 永州 425000)

(sfzhou73@163.com)

摘要:2010年,Mohammad等人提出了一种新的双方认证密钥协商协议(MOHAMMAD Z, CHEN Y, HSU C, et al. Cryptanalysis and enhancement of two-pass authenticated key agreement with key confirmation protocols. IETE Technical Review, 2010, 27(3):252-65)。新协议以较高的运算效率实现了参与者双方的身份认证和密钥协商。对该协议的单轮版本进行了安全性分析,通过模拟协议中某些信息丢失后协议双方的通信过程,发现如果协议中的一些秘密信息丢失,敌手可以发起信息泄露伪装攻击、密钥泄露伪装攻击和一般定义下的伪装攻击,也无法抵抗中间人攻击。这些攻击都可以使得敌手冒充合法参与者发起或回应会话。

关键词:信息安全;密钥协商;伪装攻击;认证机制

中图分类号:TP309 文献标志码:A

Analysis and improvement on a new three-party password-based authenticated key agreement protocol

ZHOU Si-fang

(Computer Department, Yongzhou Vocational Technology College, Yongzhou Hunan 425000, China)

Abstract: In 2010, Z. Mohammad proposed a new two-party authenticated key agreement protocol (MOHAMMAD Z, CHEN Y, HSU C, et al. Cryptanalysis and enhancement of two-pass authenticated key agreement with key confirmation protocols. IETE Technical Review, 2010, 27(3): 252 - 65). This protocol realizes the key agreement with higher computation efficiency. However, the one-round version of this protocol cannot resist on the loss of information impersonation attack, key compromise impersonation attack and general impersonation attack, this protocol is also vulnerable to man-in-the-middle attack if some security information is lost. These security problems allow the adversary can initiate or reply the protocol with legal participants.

Key words: information security; key agreement; impersonation attack; authentication mechanism

0 引言

密钥建立协议是指两个或多个参与者在公开的网络上建立临时的秘密会话密钥的过程。利用这种协议得到的会话密钥,参与者们可以在开放的网络中建立安全信道,从而保证传输信息的安全性。密钥建立协议是密码学的基本组件,也是在不安全的网络上建立安全信道的最基本的需求。这里,会话密钥是一种短期密钥,只应用于当次会话。使用短期会话密钥可以限制攻击者可能得到的有效密文的数量,从而减少由于会话密钥丢失造成的消息泄露带来的损失;临时会话密钥还可以保证不相关的会话是相互独立的。

根据会话密钥生成方式不同,密钥建立协议通常分为两种:密钥传输协议和密钥协商协议。在密钥传输协议^[1-3]中,密钥的分发者(参与者或可信的第三方)生成一个会话密钥,并将其通过安全信道秘密地发送给各个参与者。这种做法的好处是简单,而且也有一些场合(如参与者不同时在线)必须依赖此类协议,但缺点也是显而易见的:接收会话密钥的参与者需要信任密钥的分发者或者必须存在一个可信第三方,这种要求在现实中很难实现,或者需要较高的成本,另外,维护安全信道也加重了系统的负担。而在密钥协商协议^[4-6]中,

会话密钥由所有的参与者共同协商而成,其中任何一方在密钥协商结束前都无法预测或决定会话密钥的值。尽管这种方法有计算量和通信量相对较大的缺点,但密钥协商不需要参与会话密钥生成的可信第三方和安全信道,协议的参与者也无需信任其他参与者。如果协议的参与者可以确信,除了指定的实体之外,其他任何参与者都不能得到秘密的会话密钥,我们则称此类密钥协商协议为认证密钥协商协议。本文重点研究认证密钥协商协议的安全性问题。

1976年,Diffie等人^[7]提出的双方密钥协商协议为密钥协商提供了第一个实际的解决方案,它允许以前从未共享过密钥的双方在开放的网络环境中通过交换信息建立共享的会话密钥。基本的Diffie-Hellman协议对共享密钥提供的保护,能够抵抗来自被动攻击者的窃听,但不能抵抗具有篡改、删除消息等攻击能力的主动攻击者的破坏活动。由于方案不提供身份认证,所以也无法抵抗中间人攻击。随后,学者们围绕原始的Diffie-Hellman协议存在的问题展开研究,设计了大量的满足不同安全需求和应用目标的协议。1986年,Matsumoto等人^[8]扩展了Diffie-Hellman协议,提出了三个双方认证密钥协商协议:MTL/A0、MTL/B0和MTL/C0。这些协议能够通过巧妙的消息传递而不需要签名,为通信双方产生能够抵抗被

动攻击者攻击的双向认证的会话密钥。

Menezes 和 Law 等人^[9-10]指出了 MTI 系列协议的漏洞,并证明 MTI/AO 和 MTI/CO 容易受到小子群攻击和未知密钥共享攻击。为此,他们提出了一种高效的可认证密钥协商协议 MQV。这一协议被许多权威机构,如 ANSI(美国国家标准学会)、IEEE(美国电气与电子工程师学会)等广泛采纳为密码标准。NSA(美国国家安全局)甚至将 MQV 协议纳入“下一代密码技术”标准体系,用来保护密级达到国家级机密的重要和敏感数据。值得一提的是,MQV 协议和 MTI 协议相比,不仅提供了更多的安全属性,其计算效率也有显著提高,协议的每方只需 2.5 个模指数运算。但遗憾的是,协议也未达到设计者预想的安全目标。协议的效率也是学者们一直关注的热点。

2010 年,Mohammad 等人^[11]基于基本的 Diffie-Hellman 协议思想提出了一种新的双方认证密钥协商协议(利用作者姓名首字母简称 MCHL-2 协议),新协议最大的特点是仅需两轮即可实现参与者的相互认证和参与双方的密钥协商。为了将新协议用于能耗要求更高的移动网络中,作者在该文献中还提出了一种新的单轮双方认证密钥协商协议(MCHL-1 协议)。

本文对上述单轮双方认证密钥协商协议(MCHL-1 协议)进行了安全性分析,发现如果该协议中的某些秘密信息丢失,协议将无法抵抗信息泄露冒充攻击、密钥泄露伪装攻击和一般定义下的冒充攻击,也无法抵抗中间人攻击。为此,本文对这些攻击进行了详细的描述,并分析了导致这些攻击的原因。

1 MCHL-1 协议简介

本节简要介绍 MCHL-1 协议。在此之前,先定义一些符号,这些定义适用于本文的剩余部分。

1.1 符号说明

A, B :两个参与者;

E :协议中的敌手,我们允许敌手任意监听、延迟、重放和修改消息等,换句话说, E 可以完全控制通信网络;

p, q :两个大素数,其中 $q \mid (p-1)$;

g :阶为 q 的群 G 的生成元;

r_A, r_B : A 和 B 在会话过程中各自选取的随机数;

x_A, X_A :参与者 A 的长期公私钥对,其中 $X_A = g^{x_A} \bmod p$;

x_B, X_B :参与者 B 的长期公私钥对,其中 $X_B = g^{x_B} \bmod p$;

\bar{x}_A, \bar{x}_B : x_A 和 x_B 的乘法逆;

H : $\{0,1\}^*$ $\rightarrow \{0,1\}^l$:理想的 Hash 函数,其中 l 是安全参数;

k_s : A 和 B 协商得到的会话密钥。

1.2 协议描述

本节首先介绍 MCHL-2 协议,如图 1, MCHL-2 协议中的两个参与者 A 和 B 将依次执行以下步骤:

- 1) A 随机地从 Z_q^* 选取 r_A 和 a ,并计算 $M_A = X_A^{r_A} = g^{x_A r_A}$,
 $N_A = g^a, S_A = x_A r_A + x_A + a$,并将 (M_A, N_A, S_A) 发送给 B ;
- 2) 同理, B 随机地从 Z_q^* 选取 r_B 和 b ,并计算 $M_B = X_B^{r_B} = g^{x_B r_B}$,
 $N_B = g^b, S_B = x_B r_B + x_B + b$,并将 (M_B, N_B, S_B) 发送给 A ;
- 3) 在收到 (M_B, N_B, S_B) 后, A 计算 $S'_B = g^{s_B} = g^{r_B x_B + x_B + b}$,
 并验证 $X_B = S'_B M_B^{-1} N_B^{-1}$ 和 $X_B = g^{r_B x_B + x_B + b} g^{-r_B x_B} g^{-b} = g^{x_B}$ 。如果

上述等式成立, A 计算 $k_e = M_B^{x_A} = g^{r_A x_A r_B x_B}$ 和 $k_s = H(k_e, M_A, M_B, S_A, S_B, A, B)$;

- 4) 在收到 (M_A, N_A, S_A) 后, B 计算 $S'_A = g^{s_A} = g^{r_A x_A + x_A + a}$,
 并验证 $X_A = S'_A M_A^{-1} N_A^{-1}$ 和 $X_A = g^{r_A x_A + x_A + a} g^{-r_A x_A} g^{-a} = g^{x_A}$ 。如果上述等式成立, B 计算 $k_e = M_A^{x_B} = g^{r_B x_B r_A x_A}$ 和 $k_s = H(k_e, M_A, M_B, S_A, S_B, A, B)$ 。

在单轮的 MCHL-1 协议中, B 的临时公钥 M_B 被其的长期公钥 X_B 代替。因此, B 不需要发送任何消息给 A ,这时 A 计算 $k_e = X_B^{x_A}$,同时 B 计算 $k_e = M_A^B$ 。具体过程不再赘述。

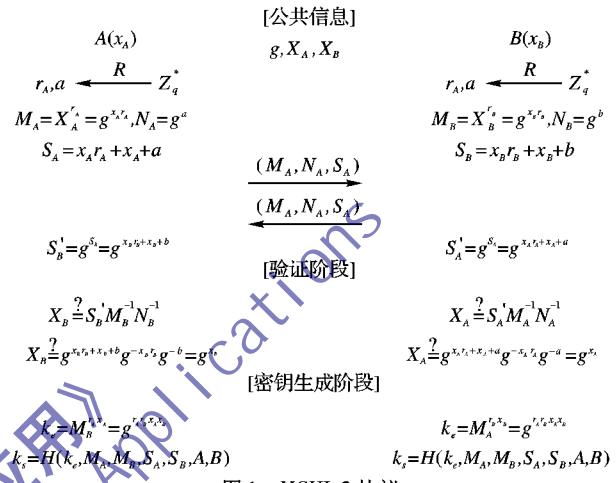


图 1 MCHL-2 协议

2 协议的安全性分析

本章讨论 MCHL-1 协议中存在的安全问题。这些问题包括:新协议不能抵抗信息泄露伪装攻击、密钥泄露伪装攻击和一般定义下的伪装攻击,也无法抵抗中间人攻击。

2.1 不能抵抗信息泄露伪装攻击

协议不能抵抗信息泄露伪装攻击是指当协议中的一些除私钥外的一些秘密信息泄露后,协议不能抵抗敌手的伪装攻击。

在本协议中,假设 $x_A, X_A = g^{x_A}$ 和 $x_B, X_B = g^{x_B}$ 分别是参与者 A 和 B 的长期公私钥对。假设泄露的信息为 $c = g^{x_A x_B}$ 。事实上,该信息是有可能泄露的:如果在某次会话中,中间值 k_e 和随机数 r_A 泄露后,敌手就可以得到 c 。通过以下步骤,敌手 E 利用其拥有的 c 即可冒充参与者 A ,反之亦然。

1) 敌手 E 主动发起 MCHL-1 协议,并计算 $M_A = X_A^{-1} g^t = g^{t-x_A}, N_A = g^{k-t}$ 和 $S_A = k$,这里, k 和 t 是敌手选取的随机数;

2) 敌手 E 将 M_A, N_A 和 S_A 发送给 B ,并计算 $k_e = c^{-1} X_B^t = g^{-x_A x_B + t x_B}, B$ 在收到上述数值后,验证等式 $X_A = g^{s_A} M_A^{-1} N_A^{-1} = g^k g^{x_A - 1} g^{t-k} = g^{x_A}$ 。根据协议的规则,该等式是显然成立的,因此 B 错误地将 E 认为成是 A ,从而完成了与敌手的会话过程。

显然, E 也可以冒充 B 与 A 发起密钥协商。

2.2 不能抵抗密钥泄露伪装攻击

假设实体 A 和 B 是协议的两个参与者,当 A 的长期私钥被敌手获得后,该敌手显然能够冒充 A 与其他协议的参与者(例如 B)进行通信。然而如果协议可以抵抗密钥泄露伪装攻击,则这一密钥泄露不能使得敌手反过来向 A 冒充为其他参与者(例如 B)。

在 MCHL-1 协议中,设 $x_A, X_A = g^{x_A}$ 和 $x_B, X_B = g^{x_B}$ 是参与者 A 和 B 的长期公私钥对,泄露的信息是 x_B 。敌手 E 生成两个随机数 k 和 t ,并计算 $M_A = X_A^{-1}g^t = g^{t-x_A}, N_A = g^{k-t}$ 以及 $S_A = k$ 。随后,E 将 M_A, N_A 和 S_A 发送给 B,并计算 $k_E = (X_A^{-1}g^t)^{x_B} = (g^{-x_A}g^t)^{x_B} = g^{-x_A x_B + t x_B}$ 。

B 验证等式 $X_A = g^{S_A}M_A^{-1}N_A^{-1} = g^k g^{x_A-t} g^{t-k} = g^{x_A}$,根据上述分析,验证的这一等式肯定成立的。因此,B 将错误地认为 E 就是参与者 A。这时,B 计算 $k_e = M_A^{x_B} = g^{(t-x_A)x_B} = k_E$ 。显然,这一攻击也适用于 MCHL-2 协议。

事实上,根据文献[12]的研究,目前已有的单轮双方认证密钥协商协议中,只有文献[13]可以抵抗密钥泄露伪装攻击。

2.3 不能抵抗伪装攻击

所谓伪装攻击,是指敌手在不知道某个参与者(例如 A)的长期私钥的前提下仍然可以冒充其发起与其他协议的参与者(例如 B)。设 $x_A, X_A = g^{x_A}$ 和 $x_B, X_B = g^{x_B}$ 是参与者 A 和 B 的长期公私钥对,敌手 E 生成两个随机数 k 和 t ,并计算 $M_A = g^{k-t}, N_A = X_A^{-1}g^t = g^{t-x_A}$ 以及 $S_A = k$ 。然后,E 将 M_A, N_A 和 S_A 发送给 B,并计算 $k_E = X_B^{k-t} = g^{(k-t)x_B}$ 。

B 验证等式 $X_A = g^{S_A}M_A^{-1}N_A^{-1} = g^k g^{x_A-t} g^{t-k} = g^{x_A}$,根据上述分析,验证的这一等式肯定成立的。因此,B 将错误地认为 E 就是参与者 A。这时,B 计算 $k_e = M_A^{x_B} = g^{(t-x_A)x_B} = k_E$ 。显然,这一攻击也适用于 MCHL-2 协议。

2.4 不能抵抗中间人攻击

分析发现敌手 E 可以通过介入 A 和 B 之间的通信发起中间人攻击。而导致这一攻击的原因是原文中定理 4.1 本身的论证就是有问题的。

原文献的定理 4.1 指出,只有一个拥有 x_A 的参与者 A 才能通过验证 $X_A = S_A M_A^{-1} N_A^{-1}$,但事实上上述等式不能用于对 A 的身份验证。特别地,下面将展示在没有私钥 x_A 的情况下,为 A 生成正确的签名。

对于等式 $X_A = S_A M_A^{-1} N_A^{-1}$,我们可以记为 $KXY = X_A$,这里 $K = S_A = g^k, X = M_A^{-1}, Y = N_A^{-1}, k \in \mathbf{Z}_q^*$ 是一个随机数。两边相乘 $X_A^{-1} = g^{-x_A}$,有 $KXYX_A^{-1} = X_A g^{-x_A}$ 。令 $X = K^{-1}$,则 $M_A = K, Y = X_A$,因此 $N_A = X_A^{-1}$ 。这样,原等式可以写成 $KK^{-1}X_A X_A^{-1} = g^0$ 。这说明定理 4.1 是错误的。

由于定理 4.1 本身是错误的,因此一个可以更改 ID 的敌手可以发起中间人攻击。这里的中间人攻击应该是一种特殊的未知密钥共享攻击。下面描述这一攻击。

假设参与者 A 准备与 B 发起 MCHL 协议(单轮和两轮均适用)。敌手 E 介入这一过程并用 $N_A^* = N_A M_A X_C^{-1} = g^{a+x_A-x_C}$ 。当收到 M_A, N_A^* 和 S_A 后,B 执行正常的验证环节 $X_C = S_A M_A^{-1} N_A^{*-1} = g^{r_A x_A + x_A + a} g^{-r_A x_A} g^{x_C - x_A - a} = g^{x_C}$,由于显然是正确的,B 相信其与 C 建立了临时会话密钥。在实际场景中,B 可能是一个服务提供商,这一攻击将会导致错误认证,进而发生 DoS 攻击。

3 结语

协议的安全性和效率是衡量协议能否真正用于实际的重要指标。尽管 2010 年 Mohammad 等人提出的 MCHL-1 协议仅仅用单轮就实现了协议双方的身份认证和密钥协商,但该

协议并不能抵抗信息泄露伪装攻击。密钥泄露伪装攻击和一般定义下的伪装攻击,也无法抵抗中间人攻击。本文详细描述了这些攻击,并分析了引起这些攻击的原因。

需要指出的是,本文的安全性分析仍然是基于启发式的。这样做尽管简单明了,但并不能完全确保协议没有其他的攻击。利用可证明安全理论对协议进行严格的形式化证明是下一步值得研究的问题。

参考文献:

- [1] SHOUP V, RUBIN A. Session key distribution using smart cards [C]// EUROCRYPT'96: Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer-Verlag, 1996: 321–331.
- [2] WILSON S B, MENEZES A. Authenticated Diffie-Hellman key agreement protocols[C]// SAC'98: Proceedings of the Selected Areas in Cryptography. Berlin: Springer-Verlag, 1999: 339–361.
- [3] WILSON S B, JOHNSON D, MENEZES A. Key exchange protocols and their security analysis[C]// Proceedings of Sixth IMA International Conference on Cryptography and Coding, LNCS 1355. Berlin: Springer-Verlag, 1997: 30–45.
- [4] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]// EUROCRYPT'01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer-Verlag, 2001: 451–472.
- [5] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]// ProvSec'07: Proceedings of the 1st International Conference on Provable Security. Berlin: Springer-Verlag, 2007: 1–16.
- [6] BELLOVIN S, MERRITT M. Encrypted key exchange: Password based protocols secure against dictionary attacks[C]// Proceedings of IEEE Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 1992: 72–84.
- [7] DIFFIE W, HELLMAN M. New directions in cryptography[EB/OL].[2011-01-01]. <http://securerespeech.cs.cmu.edu/reports/DiffieHellman.pdf>.
- [8] MATSUMOTO T, TAKASHIMA Y, IMAI H. On seeking smart public-keydistribution systems[J]. The Transactions of the IEICE, , 1986, E69-E(2): 99–106.
- [9] MENEZES A, QU M, VANSTONE S. Some new key agreement protocols providing mutual implicit authentication[C]// SAC '95: Proceedings of the Second Workshop on Selected Areas in Cryptography. New York: ACM Press, 1995: 22–32.
- [10] LAW L, MENEZES A, QU M, et al. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119–134.
- [11] MOHAMMAD Z, CHEN Y, HSU C, et al. Cryptanalysis and enhancement of two-pass authenticated key agreement with key confirmation protocols[J]. IETE Technical Review, 2010, 27(3): 252–65.
- [12] CHALKIAS K, BALDIMTSI F, HRISTU-VARSAKELIS D, et al. Two types of key-compromise impersonation attacks against one-pass key establishment protocols[EB/OL].[2011-02-01]. www.springerlink.com/index/ql1744427175j3u.pdf.
- [13] CHALKIAS K, HALKIDIS S, HRISTU-VARSAKELIS D, et al. A provably secure one-pass two-party key establishment protocol[C]// Proceedings of 3rd International SKLOIS Conference on Information Security and Cryptology-Inscrypt. Berlin: Springer-Verlag, 2007: 115–119.