一种改进的可修复密钥分配协议

李 琥,陈黄海,诸鸿文
(上海交通大学电子工程系,上海 200030)

摘 要: Hwang 和 Ku 提出了密钥分配协议可修复特性的概念. 在本文中针对 Hwang 和 Ku 所提出的密钥分配协议进行分析,指出该协议存在的安全问题及在该协议是否具有完全可修复特性问题上出现的争论. 本文所提出的基于可修复特性的密钥分配协议解决了原协议所存在的安全问题,而且提出了隐藏重复事件标记方法,并将其应用于可修复密钥分配协议从而成功解决了原协议的完全可修复性问题.

关键词: 可修复性, 密钥分配, 事件标记
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2000) 10-0143-03

An Improved Reparable Key Distribution Protocol

LI Hu, CHEN Huang-hai, ZHU Hong-wen
(*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai* 200030, *China*)

Abstract: Hwang and Ku introduced a concept of reparability feature into key distribution protocol. In this paper, the key distribution protocol, proposed by Hwang and Ku, is analyzed. This paper also presentes security problems in Hwang and Ku's protocol, and furthermore, the argument on whether the protocol has the perfect reparability feature. So, an improved reparable key distribution protocol is proposed in this paper, which solves these security problems. A method, hiding the duplicated event markers, is also proposed and is applied in the protocol to successfully solve the perfect reparability problem.

Key words: reparability; key distribution; event marker

1 引言

使用密码方法实现网络中的安全通信,是目前实现网络安全的主要方法. 其中不仅包含设计强壮的加解密算法,而且必须具备安全的密钥分配协议. 密钥分配协议(KDP, Key Distribution Protocol)是一种在网络通信双方之间以有效而安全的方法分配加解密密钥的协议. 对于共享密钥密码系统,最基本的是 Needham 和 Schroeder 提出的单网络中密钥分配协议. Denning 和 Sacco 又利用网络环境下的同步时钟在协议中引入了时间戳,Bauer 等则引入了事件标记(EM, Event Marker). 无论是时间戳或事件标记都是为了保护重要信息避免重传攻击.

Hwang 和 Ku 在文[1]中提出了 KDP 可修复特性的概念: 一个 KDP 对于共享密钥被破所出现的安全漏洞,如果通过用新共享密钥替换被破共享密钥就可弥补之,则称该 KDP 是可修复的,亦即具有可修复特性.

对于 Lu 和 Sundareshan[2,3]所提出的等级 KDP, Hwang 和 Ku 证明了它不具备可修复特性,同时也说明了诸如 Needham 和 Schroeder 等提出的各自 KDP 的可修复性. 因此, Hwang 和 Ku 利用 EM 提出了两种基本密钥分配协议,证明了它们具备可修复特性,并在这两种基本协议基础上构建了等级 KDP 协议,同样也证明了它是可修复的.

但是 Xiao-dong Lin 等[4]指出, Hwang 和 Ku 所提出的第二种基本 KDP 存在安全缺陷使得其不具备可修复特性并给出了证明,同时做了改进. 但随后 Hwang 和 Ku 又撰文[5]指出 Xiao-dong Lin 等的改进方案也存在同样的缺陷,并得出了要避免这种安全缺陷的出现需要无限长 EM 的结论.

在本文中针对 Hwang 和 Ku 的第二种基本 KDP,分析其存在的安全问题,提出了改进的可修复 KDP. 并证明该协议对所存在的争论有了很好的解决.

2 Hwang 和 Ku 的第二种基本密钥分配协议及其安全问题分析

为了分析的方便,沿用 Hwang 和 Ku 所使用的符号表示. A 和 B 表示通信双方, AS 表示 A 和 B 所信任的认证服务器, EM_A 表示 A 所使用的事件标记,为一随机数. $A \rightarrow B: Z$ 表示 A 发送消息给 B. $(X)Y$ 表示消息 X 用密钥 Y 加密. SK 表示会话密钥. MK_A 表示 A 与 AS 共享的主密钥,并且对于协议可修复性问题的分析是基于 A 的主密钥 MK_A 被破的假设.

2.1 第二种基本密钥分配协议 KDP2[1]

协议过程为:

①$A \rightarrow B: A, EM_A$

②$B \rightarrow AS: A, EM_A, B, EM_B$

收稿日期:1999-07-05;修回日期:2000-01-26

③$AS \rightarrow A: (EM_B, A, SK)MK_B, (EM_A, B, SK)MK_A$

④$A \rightarrow B: (EM_B, A, SK)MK_B$

2.2 KDP2 存在的安全问题

2.2.1 可猜测密钥问题 在 KDP2 中如果使用的 MK_A 为可猜测密钥诸如可理解且便于记忆的字母组合,同时使用的消息加密方式为 DES—CBC,则 KDP2 将会受到以下两种方式的攻击.

一种方式是窃听攻击,也称为被动攻击. 通过窃听 A、B 及 AS 之间交换的消息,窃听者可以得到 $EM_A \Leftrightarrow (EM_A, B, SK)MK_A$ 消息对. 另一种方式是假冒攻击. 假冒者可以轻易地假冒 A 向 B 发送消息 (A, EM_A),而 B 和 AS 都无法判别 A 的真假,从而使假冒者得到 $(EM_A, B, SK)MK_A$.

使用 DES—CBC 方式的加密形式如图 1 所示(图中 M_1、M_2 …为消息明文, C_1、C_2 …为消息密文, E 为 DES 算法加密, IV 为初始化变量, $\oplus$为模 2 加). 可以重新组合序列从而得到若干子消息加密序列(数据块序列顺序不变). 利用拆分可以从 $(EM_A, B, SK)MK_A$ 中分离出 $(EM_A)MK_A$,从而得到 $EM_A \Leftrightarrow (EM_A)MK_A$ 消息对. 在 MK_A 为可猜测密钥的条件下,由于所需搜索的密钥空间较随机密钥所处密钥空间小得多,窃听者可以构建一个密钥字典,利用所得到的足够多 $EM_A \Leftrightarrow (EM_A)MK_A$ 消息对,从而破解 A 的主密钥 MK_A.

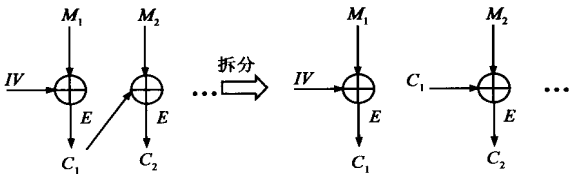

图 1 DES-CBC 加密方式的拆分

尽管我们可要求系统在产生共享密钥时要求高质量密钥,且不接受可猜测性密钥从而达到抵御上述两种攻击的目的. 但是可以对 KDP2 作很小的改动,从而使得即使用可猜测性密钥亦可免受上述两种攻击. 这将在文中提出的可修复性密钥分配协议中进行阐述.

2.2.2 重复事件标记问题 Xiao-dong Lin 等在文[4]中证明 KDP2 不具备可修复性. KDP2 中 EM_B 的明文传送使得攻击者 C 可以判断 EM_B 的重复出现. 因此 C 在 MK_A 被破解时,可以通过假冒或记录历史的方法得到足够多的数据组合 EM_B, SK 和 $(EM_B, A, SK)MK_B$ 而构成信息库. 即使 A 使用新的 MK_A,一旦 B 使用了重复的 EM_B, C 便可以发送所记录的 $(EM_B, A, SK)MK_B$ 给 B. 由于 B 的主密钥并没有被破解从而也没有更换新密钥, B 将接受 SK 作为与 A 的会话密钥. 这样 C 就可以假冒 A 与 B 进行通信.

Xiao-dong Lin 等提出可以加密 EM_B 来抵御上述攻击,从而得到改进的 KDP2 协议,协议过程为:

①$A \rightarrow B; A, EM_A$

②$B \rightarrow AS: (A, EM_A, B, EM_B)MK_B$

③$AS \rightarrow A: (A, B, EM_A, SK, (A, EM_A, B, EM_B, SK)MK_B)MK_A$

④$A \rightarrow B: (A, EM_A, B, EM_B, SK)MK_B$

但是,正如 Hwang 和 Ku 在文[5]中指出的那样,这种改进并没有解决重复事件标记问题. 因为攻击者 C 不需得到 EM_B,而只需识别出重复 EM_B,所以数据组合变为 A, EM_A, $(A, EM_A, B, EM_B)MK_B$, SK 和 $(A, EM_A, B, EM_B, SK)MK_B$. 这样,在更换主密钥 MK_A 后, C 可以假冒 A 发送 (A, EM_A) 给 B,并查找与 B 发送给 AS 的消息相匹配的数据组合. 一旦找到匹配项,则说明 B 使用了重复的 EM_B,于是 C 即可假冒 A 与 B 通信.

可以看到,问题的出现是由于事件标记发生重复且 B 的主密钥 MK_B 没有更换. 但是,不可能要求系统因一个成员主密钥被破而更换所有成员主密钥,这样做是不合理的. 因此问题的解决就在于事件标记重复问题的解决. Hwang 和 Ku 由此得出要避免这种安全缺陷的出现只有使用无限长 EM 的结论. 但是,使用无限长的 EM 是不实际的,所提出的可修复 KDP 解决了重复事件标记问题而不需无限长 EM.

3 改进的可修复密钥分配协议

协议过程为:

①$A \rightarrow B: (EM_A, A)MK_A$

②$B \rightarrow AS: (g^{R_B} \bmod p, B)MK_B$

③$AS \rightarrow B: (g^{R_{AS}} \bmod p, AS)MK_B$

④$B \rightarrow AS: (EM_A, A)MK_A, (EM_B \oplus K_0, B)MK_B$

⑤$AS \rightarrow A: (EM_A, B, SK, (EM_B, A, SK)MK_B)MK_A$

⑥$A \rightarrow B: (EM_B, A, SK)MK_B$

3.1 可猜测密钥问题的解决

将原 KDP2 步骤①中明文传送的 EM_A 和 EM_B,改为分别用主密钥 MK_A 和 MK_B 加密的密文. 这样,对于窃听攻击,窃听者不可能象原 KDP2 中一样获取 $EM_A \Leftrightarrow (EM_A)MK_A$ 数据对. 因为没有明文传送的 EM_A,窃听者虽可猜测密钥 MK_A 并用其解密 $(EM_A)MK_A$,但无法判断所猜测的密钥 MK_A 是否正确,也就无法破解密钥.

对于假冒攻击,假冒者虽然可以假冒 A 发送消息 $(EM_A, A)MK_A$ 给 B,并使 B 和 AS 发送相应的消息. 但假冒者这样做并不能使他得到比窃听者更多关于 MK_A 的信息.

因此,该 KDP2 可以抵御上述两种攻击,即使使用的是可猜测密钥.

3.2 重复事件标记问题的解决

对于重复事件标记问题,是基于一个基本思想:虽然在实际中不能使用无限长事件标记来避免事件标记的重复,但是可以通过设计隐藏事件标记的重复,使其不被攻击者发现,从而解决重复事件标记带来的安全问题.

在该协议过程中可以看到,在 B 向 AS 申请会话密钥 SK 分配之前,在 B 和 AS 之间利用 Diffie-Hellman 算法生成一个共享密钥 K_0,在这里, $K_0 = g^{R_B R_{AS}} \bmod p$. 并在随后的密钥分配申请中不传送 EM_B,而是 $EM_B \oplus K_0$ ($\oplus$表示模 2 加). AS 收到申请后,由于 AS 知道 K_0, AS 可以通过计算 $(EM_B \oplus K_0) \oplus K_0$ 来复原 EM_B,并将其用 MK_B 加密后放在给 A 的密文中. 而 B 则照常验证 EM_B.

通过对事件标记的如此处理,可以完全隐藏事件标记的重复性. 再通过两个方面来说明. 首先,考虑 B 确实使用重复

事件标记 EM_B 的情况. 当 EM_B 发生重复时,由于 B 发送中的消息中使用的是 $EM_B \oplus K_0$,所以不会发生重复. 同时,由于 K_0 的建立是通过 Diffie-Hellman 算法来完成的,攻击者无从知晓. 从而可修复 KDP2 隐藏了 EM_B 发生重复的情况.

更为重要的是,对于攻击者 C,他可以通过破解 MK_A 来记录 $(EM_B \oplus K_0, B)MK_B$,会话密钥 SK 以及 $(EM_B, A, SK)MK_B$ 数据组合. 但 C 判断事件标记重复的依据是 $(EM_B \oplus K_0, B)MK_B$ 的重复. 而现在即使 $(EM_B \oplus K_0, B)MK_B$ 发生重复,C 不知道 K_0 也就无从判断 B 是否使用了重复的事件标记 EM_B,因为 $EM_B \oplus K_0$ 结果虽然相同,却有不同的 (EM_B, K_0) 组合方式. 同时,B 也能从 C 发送的 $(EM_B, A, SK)MK_B$ 中发现事件标记不匹配,从而察觉假冒者在假冒 A 通信.

由以上论述,可以得出结论,可修复 KDP2 通过隐藏重复事件标记实现了密钥分配的完全可修复特性.

4 结论

隐藏重复事件标记,实现完全可修复性,是本文所提出的密钥分配协议的特点. 这也说明了即使没有无限长的事件标记,同样可以使密钥分配协议具备可修复特性. 以文中提出的密钥分配协议作基础,Hwang 和 Ku 的等级 KDP 亦将具备可修复性. 另外,事件标记在许多涉及网络安全的协议中使用,所提出的隐藏事件标记的方法也可应用到这些协议中,从而增强协议的安全性.

参考文献:

[1] Tzonelih Hwang and Wei-Chi Ku. Reparable key distribution protocols for internet environments [J]. IEEE Trans. Comm., May 1995, 43(5): 1947 - 1949.

[2] Wen-Pai Lu and Malur K. Sundareshan. Secure communication in internet environments: A hierarchical key management scheme for end-to-end encryption [J]. IEEE Trans. Comm., Oct. 1989, 37(10): 1014 - 1023.

[3] Wen-Pai Lu and Malur K. Sundareshan. Enhanced protocols for hierarchical key management for secure communications in internet environments [J]. IEEE Trans. Comm., April 1992, 40(4): 658 - 660.

[4] XiaoDong Lin, YuSen Xing and Yi Xian Yang. Comment on "Reparable key distribution protocols for internet environments" [J]. IEEE Trans. Comm., Jan. 1998, 46(1): 20 - 21.

[5] Tzonelih Hwang. Author's Reply [J]. IEEE Trans. Comm., Jan. 1998, 46(1): 22.

作者简介:

李 琥 1991 年进入上海交通大学电子工程系通信工程专业学习. 1995 年获得工学学士学位并开始攻读通信与电子系统专业硕士学位. 1998 年获工学硕士学位并继续攻读通信与信息系统专业博士学位至今. 研究方向为计算机通信网络和网络安全.

陈黄海 1991 年进入上海交通大学电子工程系通信工程专业学习. 1995 年获得工学学士学位并开始攻读通信与电子系统专业硕士学位. 1998 年获工学硕士学位并继续攻读通信与信息系统专业博士学位至今. 研究方向为计算机通信网络和综合业务.

电子学报

2000 年第 10 期 Acta Electronica Sinica No. 10 2000

(总期 199 期) (Monthly) (Series No. 199)

主办单位	中国电子学会	Published by the Chinese Institute of Electronics, Beijing
协办单位	中国计算机报社	China Infoworld
编辑	《电子学报》编辑委员会	Edited by Editorial Board of Acta Electronica Sinica
主编	王守觉	Chief Editor: Wang Shoujue
总编辑	刘力	Director: Liu Li
通信处	北京 165 信箱 (邮政编码 100036)	Editorial Office of Acta Electronica Sinica (P.O. Box 165, Beijing 100036, China)
电话	(010) 68285082	Tel 86-10-68285082
传真	(010) 68173796	Fax 86-10-68173796
排版印刷	中国纺织印刷厂	Printed by Textile Printinghouse, China
国内总发行	北京市报刊发行局	Distributed by Domestic: Beijing Baokan Faxingju, China
国外总发行	中国国际图书贸易总公司	Foreign: China International Book Trading Corporation
国内订购处	全国各邮电局	Subscription Office ——All Local Post Offices in China

刊号: ISSN 0372-2112 CN11-2087/TN 邮发代号(国内/国外): 2-891/M436 国内定价 20.00