Journal of Computer Applications
计算机应用,2012,32(1):42-44,65
ISSN 1001-9081
CODEN JYIIDU
2012-01-01
http://www.joca.cn

文章编号:1001-9081(2012)01-0042-03
doi:10.3724/SP.J.1087.2012.00042

强健安全网络中的中间人攻击研究

汪　定[1,2*],马春光[1],翁　臣[3],贾春福[3]
(1.哈尔滨工程大学 计算机科学与技术学院,哈尔滨 150001;　2.汽车管理学院 训练部,安徽 蚌埠 233011;
3.南开大学 信息技术科学学院,天津 300071)
(*通信作者电子邮箱 wangdingg@mail.nankai.edu.cn)

摘　要:中间人(MitM)攻击是强健安全网络(RSN)面临的一类严重安全威胁。参照802.1X-2004认证者和申请者状态机模型,从RSN关联建立过程的整体视角,对RSN中MitM攻击进行系统性分析。指出现有关于RSN中MitM攻击问题研究方面存在片面性,提出RSN中一个MitM攻击的框架和有效攻击条件,并给出该框架下一个有效攻击实例。分析结果表明,RSN采用强双向认证方法时可抗MitM攻击,未采用强双向认证方法时易遭MitM攻击。

关键词:中间人攻击;强健安全网络;状态机;攻击框架;可扩展认证协议
中图分类号:TP393.08　　**文献标志码**:A

Research of man-in-the-middle attack in robust security network

WANG Ding[1,2*], MA Chun-guang[1], WENG Chen[3], JIA Chun-fu[3]
(1. *College of Computer Science and Technology, Harbin Engineering University, Harbin Heilongjiang* 150001, *China*;
2. *Department of Training, Automobile Management Institute, Bengbu Anhui* 233011, *China*;
3. *College of Information Technical Science, Nankai University, Tianjin* 300071, *China*)

Abstract: Man-in-the-Middle (MitM) attacks pose severe threats to the Robust Security Network (RSN). Based on the state machine model of the authenticator and supplicant in 802.1X-2004, MitM attacks were analyzed systematically from the respect of the whole establishment of RSN associations. With the unilateral cognition of the MitM attacks in RSN clarified, a framework for the MitM attacks in RSN and its conditions of the effective launch of the attacks were brought forward, which were fully verified by an effective attack instance. The analytical results reveal that RSN can withstand MitM attacks if strong mutual authentication methods are adopted; otherwise it is vulnerable to this threat.

Key words: Man-in-the-Middle (MitM) attack; Robust Security Network (RSN); state machine; attack framework; Extensible Authentication Protocol (EAP)

0　引言

为应对不断突出的无线局域网(Wireless Local Area Network, WLAN)安全问题,2004年6月,IEEE 802.11 TGi工作组正式发布了新一代WLAN安全标准——IEEE 802.11i[1],提出了强健安全网络(Robust Security Network, RSN)的概念,主要从认证与加密两个方面来增强WLAN的安全性。在认证方面,RSN使用了基于端口的访问控制技术IEEE 802.1X[2]、扩展认证协议(Extensible Authentication Protocol, EAP)[3]和动态密钥管理机制;在加密方面,802.11i采用了TKIP(Temporal Key Integrity Protocol)、CCMP(CTR with CBC-MAC Protocol)和WRAP(Wireless Robust Authenticated Protocol)等加密机制。802.11i安全标准的推出很大程度上增强了WLAN的安全性能,但研究表明RSN仍存在众多安全缺陷,易遭DoS攻击、中间人(Man-in-the-Middle, MitM)攻击、会话劫持、安全级回滚攻击等[4-6]。

MitM攻击是RSN中常见且危害较大的一类攻击,但现有关于RSN中MitM攻击的系统性研究成果较少。由于未参照802.1X-2004[2]状态机模型,而是参照不适用于WLAN的802.1X-2001[7]状态机模型,缺乏从强健安全网络关联(RSN Association, RSNA)建立过程的整体视角进行分析,甚至一些文献中的研究结论出现完全相悖的情况,比如文献[8-9]中"802.11i抗MitM攻击"的结论与文献[4-5]截然相悖,文献[10-11]中关于EAP-TLS是否抗MitM攻击的观点也相反。就作者所知,目前尚没有相关文献从RSNA建立过程的整体视角对RSN中MitM攻击进行系统性的分析。

本文在参照802.1X-2004认证者和申请者状态机模型的基础上,从RSNA建立过程的整体视角,对RSN中MitM攻击进行系统性分析,指出当前RSN中MitM攻击问题研究方面的片面性,提出RSN中一个MitM攻击框架和有效攻击条件,最后给出该框架下一个完整的有效攻击实例证明。

1　IEEE 802.1X分析

1.1　IEEE 802.1X-2004端口控制机制

IEEE 802.1X最初是IEEE于2001年6月通过的基于端口的访问控制标准,用于对IEEE 802局域网用户的接入认证。802.1X协议体系结构由申请者(Supplicant)、认证者(Authenticator)和认证服务器(Authentication Server, AS)构成。2004年6月,IEEE将802.1X技术引入802.11i标准中,称为802.1X-2004[2],并且结合EAP在802.1X中增加了动态

收稿日期:2011-08-01;修回日期:2011-09-05。　基金项目:国家自然科学基金资助项目(61073042);黑龙江科研启动资金资助项目(LBH-Q10141);黑龙江省教育厅科学技术研究项目(12513049);北京邮电大学网络与交换技术国家重点实验室开放课题(SKLNST-2009-1-10)。
作者简介:汪定(1985-),男,湖北十堰人,硕士研究生,主要研究方向:密码学、无线网络安全;　马春光(1974-),男,黑龙江双鸭山人,教授,博士,主要研究方向:密码学、信息安全;　翁臣(1986-),男,湖北恩施人,硕士研究生,主要研究方向:网络信息安全;　贾春福(1967-),男,河北文安人,教授,博士,主要研究方向:信息安全、可信计算。

密钥管理机制。802.1X-2004 相较 802.1X-2001[7] 在两个方面增强了基于端口的控制: 1) 在申请者中也引入 802.1X 端口控制机制,而 802.1X-2001 中只有认证者有 802.1X 端口控制机制; 2) 增强了 802.1X 受控端口的开放条件,在 802.1X 认证通过且成功安装对等临时密钥后才打开 802.1X 受控端口,而 802.1X-2001 中受控端口在认证通过之后就打开。图 1 显示了 802.1X-2004 中认证者状态机从 Authenticating 状态到 Authenticated 状态的迁移过程。只有 802.1X 状态机处于 Authenticated 状态时受控端口才开放,802.11 信道才可用。

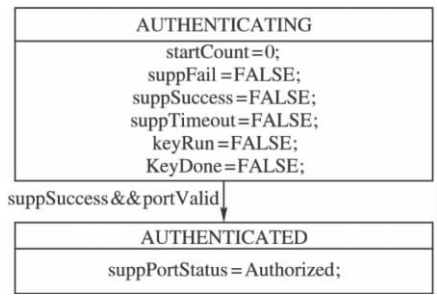

图 1　802.1X-2004 部分状态机迁移图

1.2　IEEE 802.1X-2004 密钥管理机制

在 802.1X 认证过程中,客户端(Station, STA)和 AS 之间通过 EAP-Message 产生密钥材料,在认证通过之后双方成功共享一个相同的主密钥(Master Key, MK),MK 通过伪随机函数(Pseudo-Random Function, PRF)产生对等主密钥(Pairwise Master Key, PMK)。PMK 是从 MK 派生出来,并由 AS 传递给无线接入点(Access Point, AP)。之后 AP 和 STA 进入 4 步握手阶段,期间双方互相验证是否拥有相同的 PMK,若不同则断开关联。4 步握手过程中 AP 和 STA 派生出对等临时密钥(Pairwise Transient Key, PTK),该密钥被分成三部分: 密钥确认密钥(Key Confirmation Key, KCK)、密钥加密密钥(Key Encryption Key, KEK)和临时加密密钥(Temporary Key, TK)。其中 KCK 负责 4 次握手过程中数据完整性校验码(Message Integrity Code, MIC)的计算和验证,KEK 负责随后组密钥分发过程中密钥数据的加密,而此后会话数据帧的加密和完整性校验由 TK 完成。

2　RSNA 建立过程

RSN 利用 RSNA 过程来完成 STA 和网络之间的双向认证,并产生动态会话密钥以提供通信数据的机密性和完整性保护。一个完整的 RSNA 建立过程包含如下 4 个阶段。

阶段 1　网络安全能力发现和关联。STA 首先发现可用网络及相应 AP 安全能力参数,然后选择一个网络并与相应 AP 进行开放系统认证和关联,整个过程以明文方式进行。

阶段 2　802.1X 认证。STA 和 AS 之间运行一个双向认证协议,AP 作为转发通道,认证通过之后 STA 和 AS 之间共享 PMK,AS 并且将 PMK 传送给 AP。

阶段 3　802.1X 密钥管理。STA 和 AP 运用 4 步握手协议来确认双方拥有相同的 PMK,并协商密码套件和产生 PTK。此阶段完成之后,STA 和 AP 之间拥有相同的 PTK 并装载,802.1X 受控端口打开。然后 AP 和 STA 之间协商组临时密钥(Group Transient Key, GTK)用以组播通信,此阶段可选。

阶段 4　安全数据通信。利用此前协商的 PTK、密码套件,STA 和 AP 间的数据通信采用 RSN 数据加密机制。

3　RSN 中的 MitM 攻击

802.1X 协议的重大缺陷是客户端和认证者状态机不平等,导致执行的只是客户端到认证者的单向认证,而无论具体采用何种 EAP 认证方法。虽然 802.1X 存在本质上执行的是客户端到认证者单向认证的缺陷,但文献[13]中所提出的利用该缺陷针对 802.1X-EAP 的 MitM 攻击并不总是有效,更不能以此得出如文献[11]所示的"EAP-TLS 也遭受 MitM 攻击"的结论。下面详细分析这些结论存在局限性和片面性的原因,给出 RSN 中 MitM 攻击框架、有效攻击的条件和一个攻击实例。

3.1　RSN 中的 MitM 攻击框架

802.1X 以 EAP 为认证框架,现今已有近 50 种 EAP 认证方法被授权了方法号。RFC 4017 明确规定了应用于 WLAN 环境下 EAP 认证方法的 7 个强制性、2 个推荐和 2 个可选安全性能参数[14]。EAP-MD5 不符合 RFC 4017 所有强制性要求,这种认证方法不应在 WLAN 中应用,而且 WLAN 中实际应用的很少。因此,如文献[13]仅以 EAP-MD5 例证明 802.1X在 WLAN 中易受 MitM 攻击是不恰当的。

根据 802.1X-2004 中申请者状态机,申请者完成 802.1X 认证后 suppSuccess 变量被置为 TRUE,PTK 成功安装后 portValid 变量被置为 TRUE,此时状态机进入 Authenticated 状态,802.1X 受控端口才开放,才会向 AP 发送数据帧; 802.1X-2004中认证者状态机也类似。802.1X-2001 中客户端状态机在收到 EAP-Success 消息后 suppSuccess 变量被置为 TRUE,立即进入 Authenticated 状态,客户端网卡便会开始传输数据帧,认证者在 802.1X 认证通过即收到 Radius-accept 消息便开放受控端口。文献[15]中参考的客户端状态机模型正是来自于 802.1X-2001,基于该状态机模型的 EAP-Success 消息攻击方案在基于 802.1X-2004 标准的 802.11i 环境中是不可行的,因为客户端在收到 EAP-Success 消息(无论是真实的还是伪造的)后不会立即进行数据帧的传输,而是进入 RSNA 第三阶段。在 RSNA 第 3 阶段中,如果攻击者未获得 PMK 或者无法破解 MIC 校验,合法 AP 和 STA 将检测到异常的存在,会断开与攻击者的关联,返回 RSNA 原点,这种攻击实质上是一种低级的 DoS 攻击。

文献[15]还给出了一个针对 WLAN 中 802.1X 单向认证缺陷的 MitM 攻击框架,如图 2 所示。该框架中,攻击者与 STA 和 AP 通信使用的是 802.11 信道,这在 RSN 中是不正确的。802.11i 的端口授权机制明确要求只有安装 PTK 后 STA 和 AP 才被授权使用 802.11 信道,因而此时 802.11 信道已是受 PTK 保护的加密信道,即 802.11 RSN 信道,修正的攻击框架如图 3 所示。

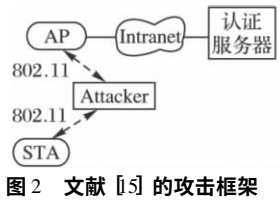

图 2　文献[15]的攻击框架

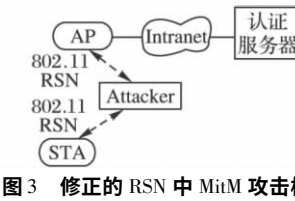

图 3　修正的 RSN 中 MitM 攻击框架

利用修正后的攻击框架实施中间人攻击的流程如下:

1) 攻击者通过侦听 AP 与合法 STA 之间的网络通信,获得相应通信信道信息;

2) 攻击者根据侦听到的信息设置自己的 MAC、SSID 及通信信道等信息;

3) 攻击者切断合法 STA 与 AP 网络通信;

4) 合法 STA 重新扫描可用的 AP,并且连接到攻击者设置的假冒 AP 上;

5) 攻击者假装对合法 STA 进行认证并向其发送认证成功的认证响应帧,同时攻击者假冒合法 STA 向 AP 认证;

6) 攻击者与合法 STA、AP 之间分别协商会话密钥,此后开始保密通信。

通过上述步骤,攻击者完成 MitM 攻击,实现对合法 STA 与 AP 间通信的控制。其中步骤 1) 至步骤 4),构成常见的非法 AP 攻击,这对攻击者不是一个难事; 在步骤 5) 中攻击者需要完成 RSNA 的第 2 阶段,由于此时通信链路尚未加密,攻击者只需要做简单的信息中转,实际上攻击者也可以主动发起一个认证过程; 在步骤 6) 中,攻击者要想完成 RSNA 的第 3 阶段,需要获得 PMK,而 EAP 认证方法的安全强度又决定了获取 PMK 的难度。因此,在修正的框架下实施 MitM 攻击的难易主要取决于 EAP 认证方法的强弱。

在 802.11i 和 802.1X-2004 标准颁布多年后,文献[11]基于"802.1X 认证通过则受控端口打开"的认知和文献[15]所提出的 MitM 攻击框架,认为"802.1X 的 MitM 攻击缺陷是协议自身的漏洞,与具体认证方法无关",得出了"EAP-TLS 不抗 MitM 攻击"的结论。由前面的分析可知,这种认知的基础在 RSN 环境中是完全错误的,得出的"EAP-TLS 不抗 MitM 攻击"的结论也是不正确的。

3.2 有效攻击条件

802.1X-2004 相较 802.1X-2001 主要是增加了密钥管理功能,802.11i 中 EAP 在提供认证服务的同时也完成 STA 和 AS 间主密钥 MK 的协商功能,然后 STA 和 AS 由 MK 派生出 PMK,AS 并将 PMK 传送给 AP,之后开始 RSNA 第 3 阶段。这样,802.11i 通过 PMK 将 RSNA 的阶段 2 与阶段 3 关联起来。在 4 步握手阶段,通过消息 2 和消息 3,STA 和 AP 互相验证双方是否拥有相同的 PMK,若通不过验证则双方断开关联,实质上 RSNA 第 3 阶段也是一个 AP 和 STA 双向认证的过程。由于消息 2 和 3 受 MIC 保护,攻击者要通过该阶段必须具备两个条件之一: 1) 获得 PMK; 2) 破解 MIC。文献[10]证明了当 802.1X 采用强双向认证方法如 EAP-TLS 时攻击者获得 PMK 的概率可忽略; 破解计算 MIC 采用的算法,典型的如 160-bit的 HMAC-SHA-1,当前公认是计算上不可行的。因此,这两个必须条件进一步降低了 RSNA 中 MitM 攻击的成功实施的可能性,4 步握手协议隐含的双向认证过程一定程度上弥补了 802.1X 单向认证的缺陷,成为对来自 802.1X 认证阶段潜在 MitM 攻击行为的一个有效阻断机制。

3.3 一个攻击实例

2002 年 Asokan 等[16]指出,通道型 EAP 认证方法由于 TLS 通道内部认证方法对其外部是否存在 TLS 通道一无所知,可遭 MitM 攻击,并给出了一个针对 PEAP v0 的攻击实例。由于当时 802.11i 和 802.1X-2004 标准尚未颁布,该实例只证明了攻击在 802.1X-2001 下有效,在 RSN 环境下是否依然能够成功尚不得知。本文给出了一个 RSN 环境下针对 EAP-TTLS v0 的 MitM 攻击完整实例,攻击流程如图 4 所示。

具体过程如下:

1) MitM 分别与 AP、STA 完成 RSNA 的阶段 1(MitM 与 STA 间的这个过程也可能在随后某个时间进行);

2) MitM 发起同 AS 的通道型 EAP 方法 802.1X 认证;

3) 在 MitM 同 AS 的通道型认证第 1 阶段完成后,MitM 发起同 STA 的认证;

4) MitM 从 EAP-TTLSv0 第 1 阶段外部 TLS 会话中得到 MK,生成 PMK;

5) MitM 与 AP 进行 4 步握手过程,成功生成 PTK;

6) MitM 取得本应属于 STA 的无线信道。

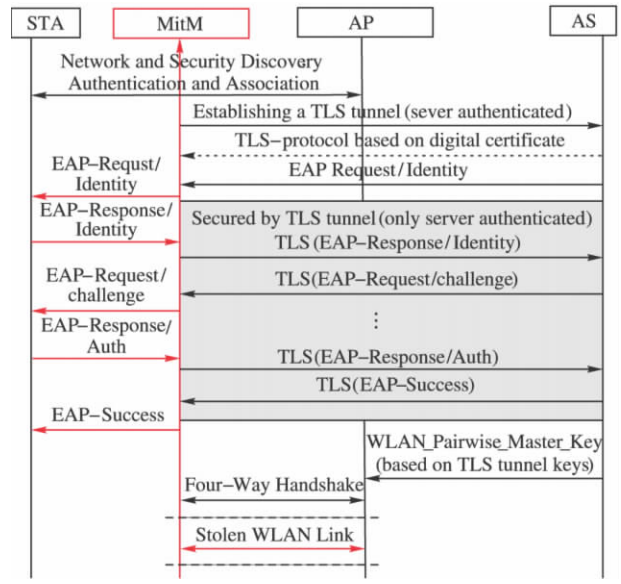

图 4 RSN 中针对 EAP-TTLS v0 的 MitM 攻击

在 EAP-TTLS v0 中,对等主密钥 PMK = TLS_PRF-128 (SecurityParameters. master _ secret," ttlsKeyingmaterial ", SecurityParameters. client _ random, SecurityParameters. server _ random) 。

可以看出,PMK 的生成参数完全来自 EAP-TTLSv0 第 1 阶段外部 TLS 会话过程,而该会话过程完全由 MitM 控制。因而 MitM 能够获得 PMK,满足 3.2 节中有效攻击的条件 1,攻击能够成功通过 RSNA 的 4 步握手阶段,进而取得 802.11 RSN 信道,攻击成功。

4 结语

本文从 RSNA 建立过程的整体视角,系统分析了 RSN 中 MitM 攻击的攻击框架和有效攻击的条件,给出了一个基于 EAP-TTLS v0 的完整攻击实例,并得出以下结论: EAP-TLS 是抗 MitM 攻击的,EAP-TTLS 和 PEAP 是否抗 MitM 攻击与具体实现版本相关,RSN 未采用强双向认证方法时易遭 MitM 攻击。随着 WLAN 移动应用的推广,RSN 在漫游环境中的 MitM 攻击问题是下一步的研究内容。

参考文献:

[1] IEEE-SA. IEEE Std 802.11i, Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) security enhancements [S]. Washington, DC: IEEE Computer Society, 2004.

[2] IEEE-SA. IEEE Std 802.1X-2004, port-based network access control [S]. Washington, DC: IEEE Computer Society, 2004.

[3] ABOBA B, BLUNK L, VOLLBRECHT J, *et al*. IETF RFC 3748, Extensible Authentication Protocol (EAP) [S]. Reston: IETF, 2004.

[4] 郭渊博,杨奎武,张畅,等. 无线局域网安全: 设计及实现[M]. 北京: 国防工业出版社,2010: 11 - 39.

[5] WANG L, SRINIVASAN B, BHATTACHARJEE N. Security analysis and improvements on WLANs [J]. Journal of Networks, 2011, 6(3): 470 - 481.

(下转第 65 页)

表 3　协议可用性实验结果一览表

序号	计时模块时间(分: 秒: 毫秒)	时间戳时间(分: 秒: 毫秒)		
		第 1 组	第 2 组	第 3 组
1	00: 10: 000. 00	00: 10: 002. 47	00: 10: 002. 26	00: 10: 002. 40
2	00: 40: 000. 00	00: 40: 005. 26	00: 40: 005. 71	00: 40: 005. 20
3	01: 10: 000. 00	01: 10: 008. 19	01: 10: 008. 32	01: 10: 008. 10
4	01: 40: 000. 00	01: 40: 010. 93	01: 40: 011. 02	01: 40: 010. 90
5	02: 10: 000. 00	02: 10: 014. 32	02: 10: 014. 57	02: 10: 014. 30
6	02: 40: 000. 00	02: 40: 017. 22	02: 40: 017. 67	02: 40: 017. 20
7	03: 10: 000. 00	03: 10: 003. 31	03: 10: 002. 35	03: 10: 020. 50
8	03: 40: 000. 00	03: 40: 006. 17	03: 40: 005. 53	03: 40: 023. 10
9	04: 10: 000. 00	04: 10: 009. 66	04: 10: 008. 86	04: 10: 026. 00
10	04: 40: 000. 00	04: 40: 011. 91	04: 40: 011. 34	04: 40: 030. 01
11	05: 10: 000. 00	05: 10: 015. 17	05: 10: 014. 76	05: 10: 032. 70
12	05: 40: 000. 00	05: 40: 018. 34	05: 40: 017. 82	05: 40: 035. 20
13	06: 10: 000. 00	06: 10: 002. 10	06: 10: 020. 10	06: 10: 038. 50
14	06: 40: 000. 00	06: 40: 005. 37	06: 40: 023. 34	06: 40: 041. 72
15	07: 10: 000. 00	07: 10: 008. 40	07: 10: 026. 23	07: 10: 044. 64
16	07: 40: 000. 00	07: 40: 010. 96	07: 40: 028. 87	07: 40: 046. 97
17	08: 10: 000. 00	08: 10: 014. 35	08: 10: 032. 42	08: 10: 050. 02
18	08: 40: 000. 00	08: 40: 017. 60	08: 40: 035. 61	08: 40: 053. 37
19	09: 10: 000. 00	09: 10: 001. 98	09: 10: 003. 10	09: 10: 001. 98
20	09: 40: 000. 00	09: 40: 005. 21	09: 40: 005. 73	09: 40: 005. 73
21	10: 10: 000. 00	10: 10: 008. 32	10: 10: 009. 10	10: 10: 008. 23
22	10: 40: 000. 00	10: 40: 011. 65	10: 40: 012. 16	10: 40: 011. 45
23	11: 10: 000. 00	11: 10: 014. 43	11: 10: 015. 91	11: 10: 014. 76
24	11: 40: 000. 00	11: 40: 017. 22	11: 40: 018. 45	11: 40: 017. 82
25	12: 10: 000. 00	12: 10: 002. 70	12: 10: 021. 33	12: 10: 002. 13
26	12: 40: 000. 00	12: 40: 005. 31	12: 40: 023. 65	12: 40: 005. 56
27	13: 10: 000. 00	13: 10: 008. 44	13: 10: 026. 79	13: 10: 008. 61
28	13: 40: 000. 00	13: 40: 011. 43	13: 40: 030. 01	13: 40: 011. 76
29	14: 10: 000. 00	14: 10: 014. 19	14: 10: 033. 32	14: 10: 014. 30
30	14: 40: 000. 00	14: 40: 018. 05	14: 40: 036. 15	14: 40: 018. 64

4　结语

本文结合不可靠网络环境的特点提出了一种在网络状况差的条件下进行时间戳服务的方法，设计了一个不实时依赖 TSA 的时间服务模型。该模型通过本地可信平台来进行时间戳服务，可信平台通过定期与 TSA 交互来获取对 TPM 模块滴答计数器计数状态的时间戳签名作为时间基准，当用户需要进行时间戳服务时，由本地时间戳生成模块调用 TPM 模块计算出当前时间信息，并把基准时间戳信息、TPM 对当前滴答计数值的签名和当前时间一起作为时间戳信息提供给验证方，进而完成本地时间戳服务。本文还提出了一种不可靠网络环境下基于 TPM 的数字时间戳服务协议，并对协议性能和协议安全性进行了分析。结果表明，协议产生的时间误差是可控的; 在进行时间戳服务时，协议不再需要计算平台与时间戳服务器 TSA 之间进行交互，对不可靠网络有很好的适应性。

参考文献:

[1] 邵志远. 数字时间戳应用初探[J]. 金融电子化, 2005(12): 65 – 67.

[2] MISKINIS R, SMIRNOW D, URBA E, *et al*. Digital time stamping system based on open source technologies [J]. IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control, 2010, 57(3): 721 – 727.

[3] MERKLE R C. A certified digital signature [C]// Crypto89: Proceedings of Advances in Cryptology, LNCS 1990. Berlin: Springer-Verlag, 1989: 218 – 238.

[4] 潘娴, 郑建立. 分层请求时间戳协议[J]. 上海理工大学学报, 2009, 31(1): 90 – 94.

[5] GUO WEI, HUA YU, SONG KEXIN. Study on the security of time-stamping service architecture [C]// Proceedings of the 2009 International Conference on Electronic Commerce and Business Intelligence. Washington, DC: IEEE Computer Society, 2009: 28 – 32.

[6] 郭莉. 时间戳技术研究[J]. 高性能计算技术, 2003, 16(2): 30 – 33.

[7] 谢应科, 王建东, 祝超, 等. 网络测量中高精度时间戳研究与实现[J]. 计算机研究与发展, 2010, 47(12): 2049 – 2058.

[8] 黄卿, 王亚弟, 韩继红, 等. 基于事件顺序的时间戳协议处理[J]. 计算机工程, 2010, 36(23): 124 – 126.

[9] PAN XIAN, ZHENG J L. Hierarchical time-stamp protocol: Acquiring reliable time-stamp from local time stamping server [C]// ISECS'09: Proceedings of the Second International Symposium on Electronic Commerce and Security. Washington, DC: IEEE Computer Society, 2009: 251 – 254.

[10] IETF. Internet X.509 public key infrastructure time-stamp protocol (TSP) RFC time stamping, RFC 3161 [S/OL]. [2011-03-20]. http://www.ietf.org/rfc/rfc3161.txt?number=3161.

[11] MUTIA R I, SADEQUE N, ANDERSSON J A, *et al*. Time-stamping accuracy in virtualized environments [C]// Proceedings of the 13th International Conference on Advanced Communication Technology. Washington, DC: IEEE Computer Society, 2011: 475 – 480.

(上接第 44 页)

[6] 周超, 周城, 郭亮. IEEE 802.1X 的安全性分析及改进[J]. 计算机应用, 2011, 31(5): 1165 – 1270.

[7] IEEE-SA. IEEE Std 802.1X-2001, port-based network access control [S]. Washington, DC: IEEE Computer Society, 2001.

[8] TURAB N, MOLDOVE F. A comparison between wireless LAN security protocols [J]. Electrical Engineering and Computer Science, 2009, 71(1): 61 – 80.

[9] LEI J, FU X M, HOGREF D, *et al*. Comparative studies on authentication and key exchange methods for 802.11 wireless LAN [J]. Computers and Security, 2007, 26(5): 401 – 409.

[10] DANTU R, CLOTHIER G, ATRI A. EAP methods for wireless networks [J]. Computer Standards and Interfaces, 2007, 29(3): 289 – 301.

[11] 宋宇波, 胡爱群, 姚冰心. 802.11i 认证协议可验安全性形式化分析[J]. 中国工程科学, 2010, 12(1): 67 – 73.

[12] FUNK P, WILSON S B. IETF RFC5281, extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (EAP-TTLSv0) [S]. Reston: IETF, 2008.

[13] 李永强, 汪海航. 针对 802.1x-EAP 安全认证协议的中间人攻击[J]. 计算机工程, 2008, 34(22): 192 – 197.

[14] STANLEY D, WALKER J, ABOBA B. IETF RFC4017, Extensible Authentication Protocol (EAP) method requirements for wireless LANs [S]. Reston: IETF, 2005.

[15] MISHRA A, ARBAUGH W A. An initial security analysis of the IEEE 802.1x standard, CS2TR2 4328 [R]. Maryland: Maryland University, Department of Computer Science, 2002.

[16] ASOKAN N, NIEMI V, NYBERG K. Man-in-the-middle in tunneled authentication protocols [C]// Proceedings of 2003 Security Protocols Workshop, LNCS 3364. Berlin: Springer-Verlag, 2005: 28 – 41.