# 802.11i 中间人攻击研究

汪定[1,3]，马春光[1]，翁臣[2]，贾春福[2]

(1. 哈尔滨工程大学 计算机科学与技术学院，黑龙江 哈尔滨 150001；

2. 南开大学 信息技术科学学院，天津 300071；3. 解放军汽车管理学院，安徽 蚌埠 233011）

（wangdingg@mail.nankai.edu.cn）

**摘　要：**参照 802.1X-2004 认证者和申请者状态机模型，从强健安全网络(RSN)关联建立过程的整体视角，对 802.11i 中间人(MitM)攻击进行系统性分析。指出现有文献关于 802.11i 中 MitM 攻击问题研究方面存在片面性，改进了过渡安全网络(TSN)中 MitM 攻击框架；提出 RSN 中一个 MitM 攻击框架和有效攻击条件，并给出该框架下一个有效攻击实例。

**关键词：**802.11i；中间人攻击；RSN；802.1X；EAP

**中图分类号：**TP393.08

# Research on man in the middle attacks in 802.11i

**Abstract:** Base on the state machine of the authenticator and supplicant in 802.1X-2004,man in the middle (MitM) attacks were analyzed systematically from a prospective of the whole establishment of the robust security network (RSN) associations.With the unilateral cognition of the MitM attacks in 802.11i clarified and the framework of the MitM attacks in the transient security network (TSN) improved, a framework for the MitM attacks in RSN and its conditions of the effective launch of the attacks were brought forward, which was fully verified by an effecetive attack instance.

**Key words:** 802.11i; man in the middle attack; RSN; 802.1X; EAP

**收稿日期：**2011-06-19　**修回日期：**　　**基金项目：**国家自然科学基金(61073042)；博士后科研人员落户黑龙江科研启动资助金项目(LBH-Q10141)；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)；黑龙江省教育厅科学技术研究项目（12513049）。

**作者简介：**汪定(1985-)，男，湖北十堰人，硕士研究生，主要研究方向：密码学与无线网络安全；马春光(1974-)，男，黑龙江双鸭山人，教授，博士，主要研究方向：密码学与信息安全；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：信息安全与可信计算。

## 1 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，802.11i 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)等三种加密机制。

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 802.11i 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[4~7]。其中 MitM 攻击是常见且危害较大的一类攻击，但现有关于 802.11i 中 MitM 攻击的系统性研究成果较少，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，得出的结论具有局限性和片面性。

2002 年 MISHRA 等人[8]首次较全面的分析了 802.1X 认证机制中的 MitM 攻击缺陷，得出 802.1X 不管采用任何具体 EAP 认证方法包括 EAP-TLS 在内均遭 MitM 攻击的结论，当时的背景是 802.11i 标准尚未颁布，还没有在 802.1X 认证中引入动态密钥管理机制。此后很多文献在分析 802.11i 中 802.1X 认证机制的安全性时仍然直接沿用 MISHRA 等人的分析方法，以致得出完全相同的结论，缺乏从 RSNA 整体过程的视角进行分析，如文献[9]和文献[10]。另一方面，在 WLAN 安全领域新的技术和标准不断涌现，如果不根据最新技术和标准，也会得出局限性的结果。2002 年 ASOKN 等人[11]分析了通道型 EAP 认证方法在未采取密码绑定的情况下易受 MitM 攻击的缺陷，并以典型的通道型 EAP 认证方法 PEAP 为例证明了该观点。随后 IETF 分别于 2004 年 10 月和 2006 年 3 月发布了 PEAP v2 草案[12]和 EAP-TTLSv1 草案[13]，用以修正其中的一些安全缺陷，包括 MitM 攻击漏洞。其中 PEAP v2 在 2008 年成为正式标准，并且在业界各类产品从 2006 年开始已得到广泛支持，但文献[14~16]仍沿用 2002 年 ASOKN 等人的研究方法，出现 PEAP 和 EAP-TTLS 不抗 MitM 攻击的结论。

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[17]状态机模型，802.11i 中 MitM 攻击问题的研究出现混乱局面，甚至一些文献中的研究结论出现完全相悖的情况也不足为奇，比如文献[18]和[19]中“802.11i 抗 MitM 攻击”的结论与文献[4~7]截然相悖，文献[20~21]与文献[22~24]中关于 EAP-TLS 是否抗 MitM 攻击的观点也相反。尽作者所知，目前尚没有相关文献从 RSNA 建立过程的整体视角对 802.11i 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 802.11i 中 MitM 攻击进行系统性分析，指出当前 802.11i 中 MitM 攻击问题研究方面的片面性，改进 TSN 中 MitM 攻击框架；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。

## 2 802.11i

IEEE 802.11i 为 WLAN 定义了两种类型的安全框架,即 RSN 和 Pre-RSN[1]。RSN 是指客户端(Station,STA)和接入点(Access Point,AP)都支持 RSNA 功能时,采用 RSN 安全体系结构进行安全保障；否则,就采用 Pre-RSN 机制，实现前向兼容性。RSN 和 Pre-RSN 的混合网络称为过渡安全网络(Transition Security Network,TSN)。由于 Pre-RSN 不能提供足够的数据完整性和机密性保护，其安全性方面已有充分的研究[4][25][26][27]，正逐渐被 RSN 取代，因此本文不再讨论 Pre-RSN 中的 MitM 攻击问题。

### 2.1 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)三部分构成。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 中增加了动态密钥管理机制。802.1X-2004 相较 802.1X-2001[17]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 和图 2 分别显示了 802.1X-2001 和 802.1X- 2004 中认证者状态机从 Authenticating 状态到 Authenticated 状态的迁移过程。无论是 802.1X- 2001 还是 802.1X-2004，只有 802.1X 状态机处于 Authenticated 状态时 802.1X 受控端口才开放，802.11 信道才可用。

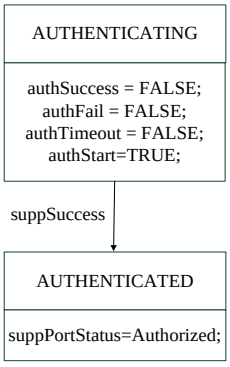


图 1　802.1X-2001 部分状态机迁移图

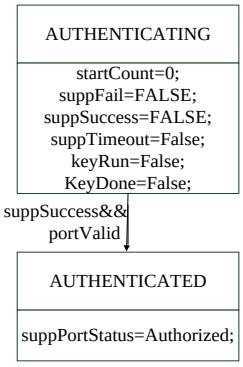


图 2　802.1X-2004 部分状态机迁移图

## 2.2 密钥管理机制

在 802.1X 认证过程中，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 AP。之后 AP 和 STA 进入四步握手阶段，期间双方互相验证是否拥有相同的 PMK，若否则断开关联。四步握手过程中 AP 和 STA 派生出(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 负责四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。以 EAP-TTLS v0[28]为例，一个完整的密钥派生过程如图 3 所示。两步组密钥握手过程派生出组临时密钥 (Group Transient Key, GTK), 以保障组播数据的安全，该过程可选。

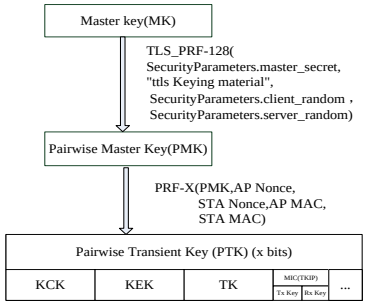


图 3　RSN 密钥派生过程

## 2.3 RSNA 建立过程

802.11i 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 TK 以提供通信数据的机密性和完整性保护。一个完整的 RSNA 建立过程如图 4 所示，包含四个阶段：

**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 运用四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 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 TK、密码套件，STA 和 AP 间的数据通信采用 RSN 数据加密机制。

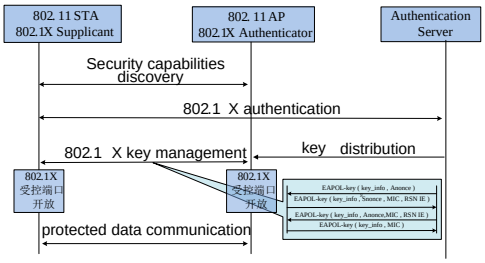


图 4　RSNA 建立过程

## 3 TSN 中的 MitM 攻击

802.11i TSN 网络中最大的安全威胁就是安全级回滚攻击，该攻击是一个典型的 MitM 攻击。攻击者完全绕开 RSN 安全机制，攻击者与 STA 以及攻击者与合法 AP 间的通信均采用 Pre-RSN 机制，下面给出攻击过程：1）MitM 假冒合法 AP 向 STA 发送 Deauthentication/ Disassociation 帧使 STA 断开与合法 AP 的连接；2）MitM 假冒 STA 向合法 AP 发送 Deauthentication/Disassociation 帧使合法 AP 断开与 STA 的连接；3) MitM 假冒合法 AP 向 STA 发送 beacon 或 Probe-Response 帧，在相关安全参数中设置为只支持 Pre-RSN；4）MitM 假冒 STA 向合法 AP 发送 Association-Request 帧，在相关安全参数中设置为只支持 Pre-RSN；5）MitM 采用 Pre-RSN 安全机制在 STA 和合法 AP 间中转通信。攻击框架如图 5 所示。

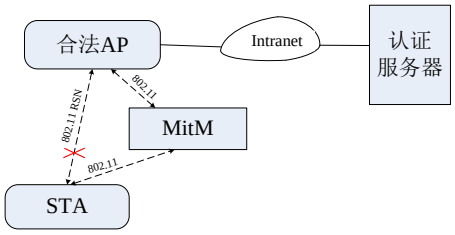


图 5　TSN 中 MitM 攻击框架

上述传统 MitM 攻击存在一个严重问题：攻击者必须与合法 AP 必须工作在不同的信道，否则在攻击者与 STA 通信过程中合法 AP 会检测到有 STA 非法接入，作为应激，合法 AP 会向 STA 发送 Deauthentication /Disassociation 帧使 STA 断开与其的连接，实际上这会断开攻击者与 STA 的连接，使攻击失效。从 STA 的角度来看，攻击者实质是 Rogue AP，众多的无线入侵检测工具[29~31]正是基于“Rogue AP 与合法 AP 工作在不同的信道”这一基本假设定义检测规则的。近期 MARTINOVIC 等人[32]的研究指出，AP 在超负荷状态下工作时会产生异常现象，如处于“清醒”状态但保持“缄默”。若利用或制造此现象，攻击者可以将信道也设置得与合法 AP 相同，那么依据此规则的无线入侵检测工具将失灵，成功实施 MitM 攻击，称之为“缄默”攻击，图 6 给出该攻击框架。

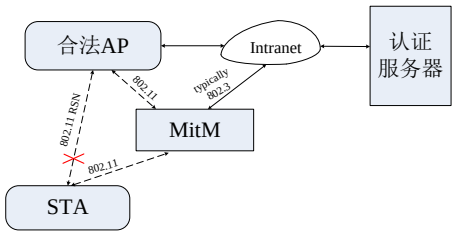


图 6　改进的 TSN 中 MitM 攻击框架

“缄默”攻击虽然避开了“Rogue AP 与合法 AP 工作在不同的信道”的局限，但攻击者必须在合法 AP 超负荷工作状态下时才能行动，若人为制造合法 AP 超负荷工作状态，需首先发动对合法 AP 的 DoS 攻击，这样容易被检测发现。“缄默”攻击的攻击者须有接入内部网络的机会，属于内部攻击者，研究表明，攻击往往来自内部，因此“接入内网”对攻击的限制不大。此外，如果攻击者设法取得 AS 的信任，该攻击不仅可以针对 TSN，而且在 RSN 内也有效。AP 和

AS 之间的通信不在 802.11i 保护范围内，实际中 AP 和 AS(如 Radius 认证服务器)之间只是共享一个静态密钥用来相互认证，而且这个密钥在较长时间内有效，AP 和 AS 之间链路的威胁十分严峻[33]，故内部攻击者“取得 AS 的信任”具有较大可能性。因此，改进后的 MitM 攻击虽有一定局限性，但仍然十分有效，并且可以针对 RSN。

## 4 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。认证者状态机只接受 EAP-Response 消息，并且只发送 EAP-Request 消息，而申请者状态机不发送 EAP-Request 消息，只响应来自认证者的 EAP-Request 消息，显然状态机执行的是单向认证，即便上层 EAP 协议采用强双向认证方法如 EAP-TLS。

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[15]和[34]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[9]、[22~24]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。

### 4.1 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[35]。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[36]。表 1 列出了这些参数并分析了 EAP-MD5、EAP-TLS、PEAP 等几种常见认证方法对这些参数满足情况。

**表 1　常见 EAP 方法满足安全参数情况**

| 安全参数声明 | EAP 方法 | | | |
|---|---|---|---|---|
| | MD5 | TLS | TTLS | PEAP |
| 密钥派生* | 否 | 是 | 是 | 是 |
| 密钥强度* | 无 | 是 | 是 | 是 |
| 双向认证* | 否 | 是 | 实现相关 | 实现相关 |
| 共享状态对等* | 否 | 是 | 是 | 是 |
| 抗字典攻击* | 否 | 是 | 是 | 是 |
| 抗 MitM 攻击* | 否 | 是 | 实现相关 | 实现相关 |
| 密钥套件保护* | 否 | 是 | 是 | 是 |
| 分片 | 否 | 是 | 是 | 是 |
| 信道绑定 | 否 | 无 | 可选 | 实现相关 |
| 快速重联 | 否 | 实现相关 | 是 | 是 |
| 机密性 | 否 | 是 | 是 | 是 |

(*表示强制性要求)

由表 1 可知，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[15]和[34]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(见图 2)，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[8]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 第三阶段中，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，这种攻击造成的危害不过是网络可用性下降，实质上是一种低级的 DoS 攻击。

文献[8]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 8 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 9 所示。

在 802.11i 和 802.1x-2004 标准颁布多年后，文献[22~24]基于“802.1X 认证通过则受控端口打开”的认知和文献[8]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

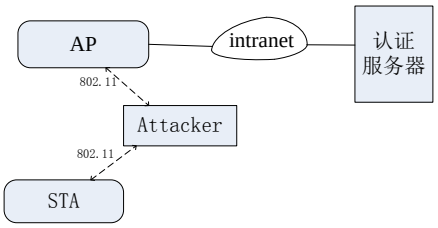


图 8　文献[8]的攻击框架

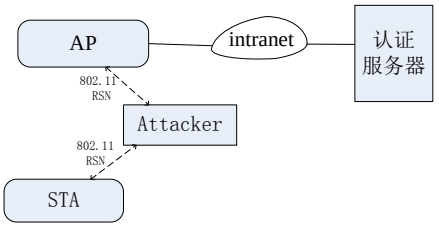


图 9　修正的 RSN 中 MitM 攻击框架

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 802.11i 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。

### 4.2 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。在四步握手阶段，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[24]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 128-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，四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。

### 4.3 一个攻击实例

EAP-TTLS 和 PEAP 是最典型的两个通道型 EAP 认证方法，所谓通道就是它们在认证的第一阶段建立的一个 TLS 安全通道，用于第二阶段用户认证信息的加密保护。通道型 EAP 认证方法一般在第一阶段中完成 STA 对 AS 的认证，第二阶段的认证在 TLS 加密通道内进行，TLS 通道内的认证方法可以是任意一种 EAP 方法，完成 AS 对 STA 的认证。

2002 年 ASOKAN 等人[11]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，是否在 802.11i 环境中依然能够成功尚不得知。我们给出了一个 802.11i 环境下针对 EAP-TTLS v0 的 MitM 攻击完整实例，攻击流程如图 10 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 的通道型认证第一阶段完成后，MitM 发起同 STA 的认证；
4) MitM 从 EAP-TTLSv0 第一阶段外部 TLS 会话中得到 MK，按 2.2 节中图 3

方式生成 PMK；

5) MitM 与 AP 进行四步握手过程；

6) MitM 取得本应属于 STA 的无线信道。

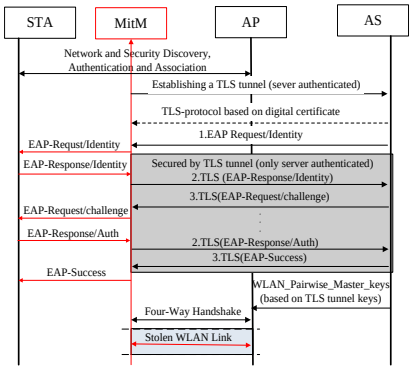


图 10　RSN 中针对 EAP-TTLS v0 的 MitM 攻击

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 第一阶段外部 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 4.2 节中有效攻击的条件 1，攻击能够成功通过 RSNA 的四步握手阶段，进而取得 802.11 RSN 信道，攻击成功。

避免这种 MitM 攻击有两种方法：一是采取密码绑定，使 PMK 的部分生成参数来自内部认证过程；二是认证绑定，使内部认证过程的结果与外部 TLS 会话过程相关。通道型认证方法的最大优势就是内部认证方法保持独立性，若采用认证绑定的办法，将会使通道型认证方法失去优势。EAP-TTLSv1 采用了密码绑定的办法：

PMK = TLS_PRF-128(

inner_secret,"ttls v1 keying material",

SecurityParameters.client _random,

Security Parameter.server_ random).

在采用 EAP-TTLSv1 的 RSN 环境中，上述攻击能成功通过 RSNA 第二阶段，无法通过第三阶段消息 2 的 MIC 检验，攻击将失败。

虽然EAP-TTLS v0不抗MitM攻击，不满足RFC 4017中有关WLAN环境中EAP认证方法的强制性要求，但现在绝大多数802.11i产品都支持EAP-TTLSv0，仍被广泛使用[33][37]。遗憾的是，EAP-TTLSv1在2006年成为IETF草案后至今未成为标准，而EAP-TTLS v0在2008年却成为正式标准，也就意味着我们的这个MitM攻击在未来较长一段时间内有效。

## 5 结束语

本文从 RSNA 建立过程的整体视角，系统分析了 802.11i 中 MitM 攻击的攻击框架、有效攻击的条件，给出了一个基于 EAP-TTLSv0 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，802.11i 未采用强双向认证方法时易遭 MitM 攻击。随着 WLAN 漫游应用的推广，802.11i 在漫游环境中的 MitM 攻击问题将是我们进一步研究内容。

## 参考文献：


[1] Wireless medium access control (MAC) and physical layer (PHY) specincations :medium Access control (MAC) secufity enhance-ments[S]. IEEE Std 802.11i,July 2004.

[2] Port-based Network Access Control[S]. IEEE Std 802.1x-2004, Dec 2004.

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

[4] AHMED M, NAAMANY A, SHIDHANI A A, et al. IEEE 802.11 Wireless LAN Security Overview[J]. International Journal of Computer Science and Network Security, 2006, 6(5B): 138-156.

[5] HE C H, MITCHELL J C. Security Analysis and Improvements for IEEE 802.11i [A]. In Proceedings of the 12th Annual Network and Distributed System Security Symposium[C]. San Diego, 2005.

[6] MA J F, MA Z, WANG C G, et al. Security Access in Wireless Local Area Networks[M]. Beijing: Higher Education Press, Apr 2009.

[7] WANG L, SRINIVASAN B, BHATTA-

CHARJEE N. Security Analysis and Improvements on WLANs[J]. Journal of Networks,2011, 6(3):470-481.

[8] MISHRA A, ARBAUGH W A. An Initial Security Analysis of the IEEE 802.1x Standard [R].Technical Report Collection (CS2TR2 4328), University of Maryland Computer Science Department, USA 2002.

[9] 周贤伟, 刘宁, 覃伯平. IEEE 802.1x协议的认证机制及其改进[J]. 计算机应用, 2006, 26 (12):2894-2896.
ZHOU X W,LIU N,QIN B P. Authentication mechanism and improvement of IEEE 802.1x protocol[J]. Computer Applications, 2006, 26(12): 2894-2896.

[10] ALI K M, OWENS T J. Access Mechanisms in Wi-Fi networks State of Art, Flaws and Proposed Solutions[A]. 17th International Conference on Telecommunications[C]. Doha, 2010: 280-287.

[11] ASOKN N, NIEMI V, NYBERG K. Man-in-the-Middle in tunneled authentication protocols [R]. Technical Report 2002/163, IACR ePrint archive,October,2002.http://eprint.iacr.org/2002/163/.

[12] PALEKAR A, SIMON D, SALOWEY J, et al. Protected EAP Protocol (PEAP) Version 2[S]. IETF Internet Draft, October 2004.

[13] FUNK P, Juniper Networks, WILSON S B, et al. EAP Tunneled TLS Authentication Protocol Version 1[S]. IETF Internet Draft, Mar 2006.

[14] BADRAA M, URIENA P, HAJJEH L. Flexible and fast security solution for wireless LAN[A]. Pervasive and Mobile Computing, 2007,3(1): 1–14.

[15] HWANG H, JUNG G, SOHN K, et al. A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP [A].International Conference on Information Science and Security [C]. Daejeon, 2008: 8-12.

[16] YOUM H Y. Extensible Authentication Protocol Overview and Its Applications [J] .IEICE TRANSACTIONS on Information and Systems, 2009, E92-D(5):766-776.

[17] Port-based Network Access Control[S]. IEEE Std 802.1x-2001,June 2001.

[18] TURAB N, MOLDOVEANU F. A COMPARISON BETWEEN WIRELESS LAN SECURITY PROTOCOLS [J]. Electrical Engineering and Computer Science, 2009, 71(1): 61-80.

[19] LEI J, Fu X M, HOGREF D, et al. Comparative Studies on Authentication and Key Exchange Methods for 802.11 Wireless LAN[J]. Computers & Security , 2007, 26(5): 401-409.

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

[21] ALI K M, OWENS T J. Selection of an EAP authentication method for a WLAN[J]. International Journal of Information and Computer Security, 2007, 1:1-2.

[22] ABOUDAGGA N, GIRY D, QUISQUATER J J. WIRELESS SECURITY DESIGN OVE RVIEW[A]. IEEE Twenty-fifth Symposium on TeleCommunications[C],Kingston,2006.

[23] HUANG W, LI R L.WLAN Authentication System Based on the Improved EAP-TLS Protocol [A].IEEE Second Pacific-Asia Conference on Web Mining and Web-based Application[C],Wuhan, 2009:112-115.

[24] 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.
SONG Y B,HU A Q,YAO B X. The provable security formal analysis of 802.11i authenticcation scheme[J]. Engineering Science, 2010, 12(1):67-73.

[25] FLUHRER S, MANTIN I, SHAMIR A. Weakness in the key scheduling algorithm of RC4[J]. Selected Areas in Crptography, 2001, 2559 (10): 101-117.

[26] BECK M, TEWS E. Practical attacks against WEP and WPA[A]. Proceedings of the Second ACM Conference on Wireless Network security[C].Zurich,2008. 79-85.

[27] 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年3月.

GUO Y B,YANG K W,ZHANG C, et al. Wireless Lan Secutiry:design and implementation[M]. Beijing: national defence industrial press, Mar 2010.

[28] FUNK P, WILSON S B. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) [S]. IETF RFC5281,Augst 2008.

[29] AirDefense[EB/OL]. http://www.airdefense.net, 2011- 05-20.

[30] AirMagnet[EB/OL].http://www.airmagnet.com, 2011- 05-20.

[31] 3ComAirProtect[EB/OL].http://www.3com.com, 2011-05-20.

[32] MARTINOVIC I, PICHOTA P, WILHELM M, et al. Bringing law and order to IEEE 802.11 networks-A case for DiscoSec[J]. Pervasive and Mobile Computing,2009,5(5):510–525.

[33] FRANKEL S, EYDT B, OWENS L, et al. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i[R]. NIST Special Publication 800-97,2007.

[34] 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.
LI Y Q,WANG H H.MIM Attack to Secure Authentication Protocol with 802.1x-EAP[J]. Computer Engineering, 2008, 34(22): 192-197.

[35] Extensible Authentication Protocol (EAP) Registry[EB/OL]. http://www.iana.org/assignments/eap numbers/eap-numbers.xml#Ashwin_Palekar,2011-06-10.

[36] STANLEY D, WALKER J, ABOBA B. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs[S]. IETF RFC4017,Mar 2005.

[37] Wi-Fi Alliance[EB/OL]. http://www.wi-fi.org/, 2011-06-10.