• 网络与通信技术 •

基于 802.11i 的 EAP-TLS 认证机制的安全分析

曹 利, 杨凌凤, 顾 翔, 朱晓辉

(南通大学 计算机科学与技术学院, 江苏 南通 226019)

摘 要:为了有效解决无线网安全认证的问题,分析了无线网的新一代安全标准 IEEE802.11i 的 RSNA 建立过程。通过对关键步骤 EAP-TLS 实体认证机制的研究,指出 EAP-TLS 认证协议在使用过程中由于配置不当而导致的安全漏洞,以及数据帧没有加密可能受到的 DoS 攻击,并从降低攻击的发生和协议的改进方面提出了基于隧道的认证新方案。

关键词:无线局域网; 802.11i; 健壮安全网络联合; 扩展认证协议; 拒绝服务攻击

中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1000-7024 (2010) 04-0756-04

EAP-TLS authentication mechanism security analysis-based 802.11i

CAO Li, YANG Ling-feng, GU Xiang, ZHU Xiao-hui

(College of Computer Science and Technology, Nantong University, Nantong 226019, China)

Abstract: To deal with the problem wireless network authentication security issues, the RSNA building process of a new generation wireless network security standards IEEE802.11i is analyzed. Via research the key steps of EAP-TLS entity authentication mechanisms, the security vulnerabilities caused by the improper configuration is pointed out during the using process of EAP-TLS authentication protocol as well as data frames that may be attacked without the encryption of the DoS, meanwhile the new tunnel certification settlements is proposed based on reduction of the occurrence of attacks and the improvement of agreement.

Key words: WLAN; 802.11i; RSNA; EAP; DoS

0 引 言

无线局域网在无线通信领域具有很大的发展前景,但由于其开放性的特点,使得它更容易遭受各种安全攻击,建立与完善一种可靠的面向无线网的安全标准成为亟待解决的关键问题。IEEE 组织在 2004 年 6 月 24 日批准了无线局域网新的安全标准 802.11i,该标准定义了两类安全构架:健壮安全网络联合 RSNA(robust security network association)和预健壮安全网络联合 Pre-RSNA,其中后者是为了实现对目前的 802.11 协议的向前兼容,前者则从无线网数据保密性和完整性、实体认证以及可用性等方面提出新的安全构架[1]。本文主要针对 RSNA 网络的认证机制的安全性和可用性进行分析和研究。

1 RSNA 建立过程

新安全标准 IEEE802.11i 在数据加密方面定义了 TKIP 和 CCMP 两种加密机制。TKIP 采用 WEP 机制的 RC4 作为核心加密算法,通过在现有的 WEP 设备上升级固件和驱动程序达到提高网络安全性的目的,是一种过渡性方案。CCMP 采用 AES 加密算法和 CCM 模式,使得 WLAN 的安全程度大大提高,但 AES 对硬件要求比较高,无法在现有设备基础上升级实现。但根据 Dolev-Yao 模型,本文把安全协议本身和安全协议采用的具体的密码系统分开,在假定密码系统是完善的基础上讨论安全协议的正确性和安全性。

IEEE802.11iRSNA 建立的过程包括身份认证和密钥管理。主要分为 5 个阶段[2]:

(1) 网络与安全能力的发现:无线接入点 AP 通过在特定信道发送信标帧 RSN IE 周期广播其安全能力或通过发送探测响应帧响应一个移动站 STA 的探测请求,将 RSN IE 传递给 STA,RSN IE 信标帧中包含 AP 的安全能力。

(2)初始化关联:STA 可以先执行开放系统认证,再连接到选择的 AP,在连接的过程中利用 RSN IE 协商安全参数;

(3)实体间认证:当初始连接完成后,AP 的认证者激发双向的 802.1x 认证;

(4)四次握手和组密钥握手:802.1x 通过认证,在 AS 和 STA 之间建立了共享密钥,AS 把密钥安全传送给 AP,AP 和 STA 进行 4 步的握手过程和组密钥握手,完成安全连接。

(5)在完成安全连接后可以实现安全的数据传输。当 STA 收到 AP Deassociates 或 Deauthenticates 消息以及 STA 连接到一

收稿日期:2009-03-12;修订日期:2009-10-23。

基金项目:高校自然科学基础研究基金项目(08KJB520009);江苏省现代教育技术研究“十一·五”规划 2009 年滚动课题基金项目(13254);南通市应用研究计划基金项目(K2008005)

作者简介:曹利(1974-),男,江苏宜兴人,硕士,讲师,研究方向为计算机网络和信息安全; 杨凌凤(1977-),女,江苏南通人,硕士,实验师,研究方向为计算机网络与安全; 顾翔(1973-),男,江苏南通人,副教授,硕士生导师,研究方向为网络协议安全; 朱晓辉(1976-),男,江苏南通人,硕士,讲师,研究方向为软件与理论、软件中间件技术。E-mail:cl@ntu.edu.cn

个新 AP 时，一个安全连接结束。

以上 5 个阶段中关键是实体认证阶段，在该阶段主要是实现对无线网实体 STA 和 AP 的双向认证。具体的认证协议是 802.1x/EAP-TLS 认证。

下面主要从两个方面来分析 802.1x/EAP-TLS 认证协议在无线网中的安全性能：协议本身的安全漏洞、可用性方面的安全漏洞。

2　EAP-TLS 认证协议可选项攻击

802.1X 协议是 IEEE 于 2001 年 6 月提出的一种基于端口的访问控制协议，该协议原本是为有线局域网 IEEE 802 提供一种用户认证和授权的技术，目的是实现合法用户接入，保护网络安全的目，无线网借用该协议实现移动端的身份鉴别和认证。802.1x 体系结构主要由 3 个部分构成：客户端，也称为申请、认证系统、认证服务器。图 1 说明了 802.1x 的 3 部分之间的关系[3]。

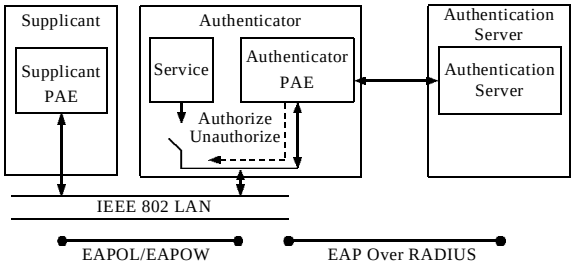

图 1　IEEE802.1x 端口控制原理

客户端系统，称作申请者，在该申请者终端上一般需安装一个发起 802.1x 认证的客户软件，为了支持基于端口的接入控制，客户端系统需支持 EAPOL 协议。

认证系统，在 WLAN 中就是无线接入点 AP(wireless access point)，本身并不能完成认证过程，只能实现认证数据报在客户端和认证服务器之间的转发，认证工作是在客户端和认证服务器之间完成。

认证服务器，采用的是远程接入用户认证服务器 (remote authentication dial-in service，RADIUS)。其实现了各种类型客户端和集中存放认证信息的 RADIUS 服务器之间传输认证、授权和配置信息的功能。

认证者有两个逻辑端口：控制端口和非控制端口。非控制端口一直处在双向连通的状态，保证随时接受客户端发出的认证 EAPOL 报文；而控制端口一般处在关闭状态，只有认证通过后才打开，进行正常的网络业务数据的通信[4]。

这里需要指出的是在 802.11i 协议中并没有指定为了实现 802.1x 认证，具体必须使用什么认证协议，但建议标准是 EAP-TLS 协议，在认证服务器端的建议标准是 RADIUS 服务器。

简单描述 EAP 认证过程如下所示：

(1)客户机发起 802.1x 认证(EAP Start 消息，请求认证)；

(2)AP 发出请求身份鉴别帧，需要客户提供身份信息；

(3)客户机响应请求，将身份信息发送给 AP；

(4)AP 无法验证，只是将该身份信息重新封装成 RADIUS Access Request 包转发送给 RADIUS 服务器，请求验证；

(5)RADIUS 服务器验证用户身份通过后向客户机发送自己的数字证书；

(6)客户机验证完服务器的身份后，放送自己的数字证书；

(7)服务器通过证书验证客户的身份，由此完成了双向的身份认证；

(8)认证成功后，RADIUS 服务器向 AP 发送 RADIUS Accept 消息，其中包含了认证过程中产生的主密钥信息；

(9)AP 向客户机转发认证成功的消息(EAP success)。

具体认证过程如图 2 所示[5]。

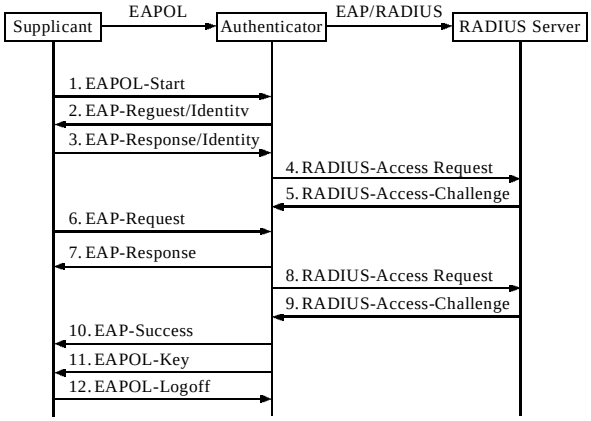

图 2　基于 EAP-TLS 的认证过程

根据图 2 可以知道 TLS 协议消息是以 EAP 形式封装进行传递的，由于受 MAC 层帧长度限制，一个消息流可能需要被拆分成多个消息进行传递，下文将分析 TLS 自身的这个弱点也成为 802.11i 配置的 EAP-TLS 的弱点。EAP-TLS 的核心协议是 TLS，TLS 的设计是为了实现对等客户端 STA 和服务器 AS 之间的相互认证，RFC2716 描述了 TLS(transport layer security) 认证协议。协议过程如图 3 所示。

EAP-TLS、RADIUS 认证协议并不是为无线网认证新设计的，其实早就在有线网中广泛使用。使用这些协议的目的是

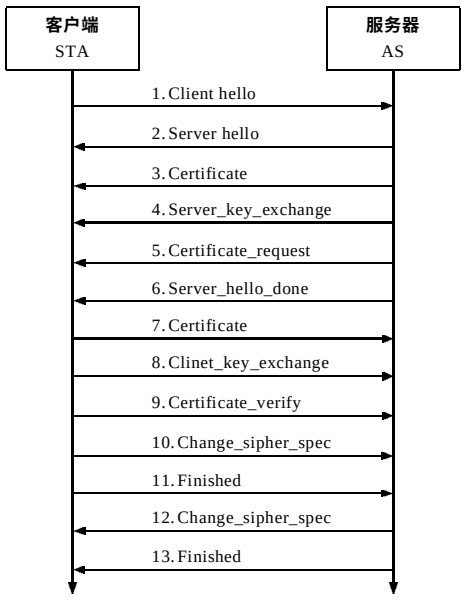

图 3　TLS 双向认证流程

因为其在有线网络中经历了很长时间的历史考验，从实际应用中检验了它们的安全性。但无线网具有开放信道，带宽低，网络不稳定，极易实施窃听和消息插入攻击等新特点，若直接引用有线网的安全协议，可能不完全符合RSNA安全要求，会存在一些不足[6]：

(1) 未针对无线网特点进行必要的优化，执行效率低下；

(2) EAP-TLS使用基于证书的认证，而AS使用的是RADIUS服务器不直接支持数字证书应用，对RADIUS认证服务需要改造，否则系统将无法直接使用；

(3) EAP-TLS认证过程交换的消息流很多，不能实现第一时间对STA的显式认证，将给攻击者很大的机会实施DoS攻击；

(4) EAP-TLS认证需要借助于数字证书实现实体认证和密钥协商，因此需要复杂的PKI(public key infrastructure)设施的支撑来实现证书应用。

RFC2716描述中把EAP-TLS的许多消息流定义为可选项，如图3中证书交换的消息3和消息7，证书请求的消息5和证书确认的消息9等，而且标准中并未规定这些可选项什么时候要强制使用。当协议运行配置或实现不当时，TLS很可能无法实现双向认证。分析如下：

首先TLS肯定可以实现STA对AS的认证，该过程是隐性的，STA获得AS的证书并验证其有效性，然后通过消息8(Clinet_key_exchange)使用AS的公钥加密预主密钥发送给AS，进而只有合法的AS才能解密或计算出正确的预主密钥，完成接下去的认证过程，计算有效的消息13(finished)，从而STA确认AS合法有效。但AS对STA的认证却可以显式实现、隐式实现，甚至无法实现。

在显式实现模式中STA使用自己持有合法证书绑定的公钥对应的合法私钥对TLS已经交换的协议消息流进行数字签名，AS接收到该消息流，在认证STA公钥证书合法性基础上，验证签名有效性，从而认证STA的合法性。

在证书认证消息缺失的情况下可通过隐式认证方式验证STA的有效性，但STA和AS必须共同协商预主密钥。这种情况下，AS和STA双方验证对方结束TLS认证过程的完成消息11和12可以验证对方的有效性，因为只有合法的实体才能正确协商出预主密钥。

最后一种情况是若STA证书绑定RSA或DSS公钥算法，但STA又不产生并发送验证消息，那AS就无法认证STA，因为此时STA并不支持密钥协商，只是使用AS公钥加密一个密钥传递给AS，合法的AS可以获得加密的密钥，但却无法确定消息源。因为只能认证STA发送的证书是有效的，并不代表其是合法证书持有者。证书可以通过被动窃听或到CA的发布目录下载得到。在802.11i的RSNA网络中，攻击者可以通过这种情况轻易通过认证消息，并完成后续所有步骤。攻击者只提供TLS定义的强制消息流，并确定一个预密钥使用AS的公钥加密发送给AS，这样攻击者拥有预密钥和只有产生的主会话密钥PSK，接下来就可计算出主密钥对PMK，进一步攻击者可以完成四步握手密钥协商的全过程，并协商产生出合法的PTK。这样由于TLS协议中可选项定义及实现协议的不完整性，使得攻击者可欺骗通过EAP-TLS认证，这是很严重的威胁，它使得802.11i定义的RSNA丧失了全部安全性。

这个漏洞其实不是RSNA协议本身的缺陷，而是认证协议TLS使用过程中配置不当，丧失了双向认证功能，从而被攻击者利用所所造成的结果，为了防止该漏洞的出现，应该规定TLS协议消息可选项必须强制使用，实现客户端/服务器端的双向认证，在客户端绑定证书支持数字签名操作时，必须签发证书确认消息，当不支持数字签名操作时，必须使用DH密钥协商机制，由AS和STA双方共同确定预主密钥，否则中断认证并丢弃此次认证。

3 EAP-TLS认证协议Dos攻击

EAP-TLS可能由于配置不当无法实现双向认证，同时数据帧没有加密保护也很容易受到DoS攻击，攻击者通过伪造EAP-TLS消息可以实施对认证实体STA、AP、AS三者的攻击。

如图2所示，攻击者通过伪造EAP-TLS的消息1(EAPOL-Start)和3(EAP-Response)，即开始消息和应答消息，向AP发出伪认证请求，因为AP需要对每个认证请求进行记录，若同时有很多伪造认证请求到达，可能导致AP内存溢出或消耗掉AP的计算量而无法响应合法STA的认证请求，AP在无线网中充当重要角色，一旦其不可用，其管理范围内的设备均无法连接网络。同样伪造AP的应答消息2(EAP-Request)，也能实现对STA的攻击，导致合法STA认证失败，影响网络可用性。

AS是基础架构WLAN安全的核心设备，一旦遭受DoS攻击，将严重影响网络安全性能。攻击者可以利用图2的消息1(EAPOL-Start)、3(EAP-Response)、6(EAP-Request)进行攻击，其中前两个消息由于没有任何加密或认证保护，可以很方便的伪造，甚至消息6，也可以随意伪造，当AS验证消息6发现错误时，EAP-TLS已经传递了多轮认证消息，消耗了AS、AP大量的计算资源、存储资源，并发送了大量的信息[7]。

综上所述，EAP-TLS存在DoS攻击威胁是由于其没有在协议开始或较前的消息流携带实体认证消息，多数的协议消息没有消息源认证和完整性保护。解决的办法可以采用隧道TLS可扩展认证协议，即EAP-TTLS协议。

EAP-TTLS(隧道TLS可扩展认证协议)是EAP-TLS的一种扩展。此安全方法提供了一种基于证书的验证方法，通过由EAP-TLS协议建立的加密的通道(或“隧道”)进行客户端和认证服务器的相互验证。

S802.1x支持TTLS种认证模式，TTLS认证数据由上层的EAP协议封装，在客户端和认证系统间认证消息的传递则使用EAPOL封装EAP协议，在认证系统与认证服务器之间的认证消息的传递是通过RADIUS协议[8]。认证体系协议栈如图4所示。

EAP-TTLS认证主要分两个阶段：TTLS握手建立秘密隧道阶段和在隧道内身份认证阶段。

在第一阶段主要是在客户端和认证服务器端建立一个TTLS认证的安全隧道，在此阶段，客户端对AS发送过来的证书的认证，如果认证通过，则建立TLS安全隧道，反之则认证失败。此时TTLS认证和TLS认证的区别就是不需要客户端的证书，只需要客户端验证服务器的证书是否正确即可。

第二阶段是在TLS安全隧道保护下，进行强口令认证，但和一般身份认证不同的是，该阶段的认证所需要的STA数据

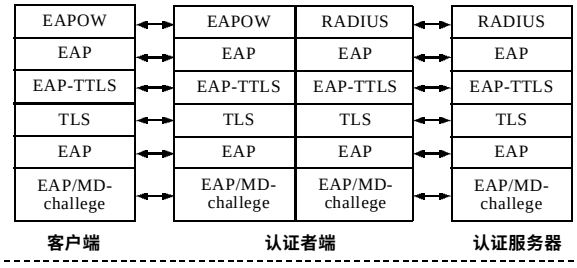

图 4 EAP-TTLS 协议栈

是经过 SSL 记录协议进行加密的，以保护用户的信息不被窃取或者伪造，这也是 TTLS 之所以建立安全隧道的原因。这在根本上断绝了 TLS 认证协议的认证报文伪造的可能，杜绝了 DoS 估计发生的可能性。

TTLS 协议中引入了 AVP 封装格式。所有的数据都用 AVP 包封装好之后再进行加密，然后再封装在 EAP 包中，AVP 包的基本结构如图 5 所示。

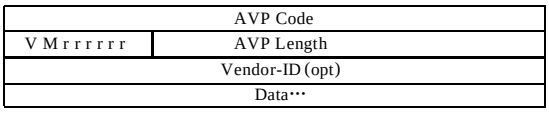

图 5 AVP 包结构

TTLS 的基本认证过程如下：

在客户端，客户软件首先发出 802.1x 认证请求，则认证服务器发出请求身份验证 (ID request) 包，客户端发出身份响应 (ID response) 包；认证服务器发送 TTLS-Start 包给客户端后，客户端开始发起 TLS 中验证的第一步：client hello；服务器随之发送证书，客户端进行验证，如果通过，则发送密文族修改协定，反之，则发送告警信息。(以下均以验证通过为例，TLS 的安全隧道此时已经建立)。客户端接收到服务器发送的修改协定后发送 TTLS 的 EAP-RESPONSEID 包，此时采用真实的用户 ID(真实用户名的格式如下：username@realm，此时先前所建立的 TLS 安全隧道开始保护数据。如果 TTLS 服务器搜索不到该用户，或者不支持 EAP 的隧道认证方法，则认证失败)；客户端收到认证服务器通知认证方式信息，则发送相应的 Response，X-Challenge。(X 表示某认证方法)；接受到 Success 或者 Fail 信息。

在服务器端，在认证服务器发出 ID request 包后会接收到客户端发出的 ID response 包，认证服务器在自己的数据库中搜索到了 ID，则发起 TTLS 认证 (发送 TTLS-Start 包)；认证服务器在接收到客户端发出的 client hello 包后发送 server hello，并验证自己的身份，发送自己的证书；认证服务器接收到客户端发出的密文族修改协定包，发送密文族修改协定。(TLS 的安全隧道此时已经建立)；认证服务器接收到客户端发出的 ID response 包，则在自己的数据库中搜索 ID 对应的认证方式；收到客户端发出的 X-Challenge (X 表示某认证方法)，进行认证，成功则发 Success 失败则发 Fail 信息。

通过隧道 TLS 可以有效地解决协议消息的消息源认证和完整性保护，从而防止拒绝服务攻击的发生。但 TTLS 的缺点是协议复杂，计算量很大。所以尽管 TTLS 提供了比 TLS 更安全的认证方式，但对于一般的公共信息安全措施来说相对比较复杂，这也直接会影响到该协议未来在 WLAN 安全通信中的应用。

4 结束语

802.11i 定义了 WLAN 的数据加密和认证的新标准，本文在回顾它的 RSNA 建立过程的基础上，具体分析和研究了 EAP-TLS 实体认证机制。结合实际情况，指出 EAP-TLS 认证协议在使用过程中配置不当，丧失了双向认证功能，导致的安全漏洞，以及数据帧没有加密保护可能受到的 DoS 攻击，并从降低攻击的发生和协议的改进方面给出了改进的设计方案。如果在现实中能考虑无线网络协议存在的安全问题，那么无疑可以提高网络的安全性。

参考文献:

[1] 曹秀英,耿嘉,沈平.无线局域网安全系统[M].北京:电子工业出版社,2004:96-98.

[2] 马建蜂,朱建明.无线局域网安全-方法与技术[M].北京:机械工业出版社,2005:87-90.

[3] 袁建国,朱恺,方宁生.802.1x/EAP-PEAP 的研究与应用[J].计算机工程与设计,2006,27(10):1818-1820.

[4] 郑晓蕾,曹秀英.802.1x:基于端口的网络接入控制标准[J].通信技术,2002,6(6):101-103.

[5] Blunk L, Vollbrecht J, Aboba B, et al. Extensible authentication protocol (EAP)[Z]. Internet Draft draft-ietf-eap-rfc2284bis-06.txt,2003.

[6] Jon Edney,William A Arbaugh.无线局域网安全实务—WPA 与 802.11i[M].北京:人民邮电出版社,2006:120-125.

[7] Bellardo J,Savage S.802.11 denial-of-service attacks:Real vulnerabilities and practical solutions [C]. Proceedings of the USENIX Security Symposium,2003:15-28.

[8] 张志峰. EAP-TLS 认证机制的研究 [J]. 中国水运, 2005 (9): 183-184.

(上接第 739 页)

[8] 陈国磊,罗家融,舒双宝.基于 TMS320F2812 的电网谐波监测系统[J].微计算机信息,2009,25(5):144-146.

[9] Love,Janine.GSM/GPRS phone chip sees sharp cut in parts count[J]. Electronic Engineering Times, 2005,22(6): 61-62.

[10] Samsung Electronics.S3C2410A user's manual [EB/OL]. http://www.samsung.com/global/system/business/semiconductor/product/2008/2/11/125571ptb_s3c2410a_rev11.pdf.

[11] Dalheimer M K,Hansen S.Embedded development with Qt/embedded[J].Dr Dobbπs Journal,2002,27(3):48-53.