文章编号:1001 - 9081(2006)12 - 2894 - 03

IEEE 802.1x 协议的认证机制及其改进

周贤伟,刘 宁,覃伯平
(北京科技大学 信息工程学院, 北京 100083)
(up2renjian@163.com)

摘 要:在分析 IEEE 802.1x 协议认证机制的基础上,针对 IEEE 802.1x 缺乏源真实性和完整性保护的缺陷,提出 IEEE 802.1x 协议认证机制的改进方案(AIP)。该方案通过在 EAPOL 包中增加了一个 Protection 字段,可弥补 IEEE 802.1x 的中间人攻击和会话劫持等缺陷。经性能分析,该方案相对原方案而言,具有源真实性和完整性保护等优点。

关键词:强安全网络;可扩展认证协议;IEEE 802.11x
中图分类号: TP393 **文献标识码**:A

Authentication mechanism and improvement of IEEE 802.1x protocol

ZHOU Xian-wei, LIU Ning, QIN Bo-ping
(*School of Information Engineering, University of Science and technology Beijing, Beijing* 100083, *China*)

Abstract: Based on the analysis of the IEEE 802.1x authentication mechanism, to fetch up the flaws that IEEE 802.1x lacks source authenticity and integrity protection, an improved IEEE 802.1x authentication mechanism (AIP) was proposed. By adding a Protection part into EAPOL packets, this scheme can fetch up the flaws of IEEE 802.1x, such as intermediary attack and session hijack. Through the capability analysis, the scheme has more advantages as source authenticity and integrity protection than the original one.

Key words: robust security network; extensible authentication protocol; IEEE 802.11x

0 引言

鉴于无线局域网的开放广播特性,IEEE 802.11 标准定义了两种认证方式,即开放系统认证和共享密钥认证,并运用 RC4 流加密算法的 WEP 安全机制来加强其安全性。但是 IEEE 802.11 标准被证实存在致命缺陷[1],因此 IEEE 802.11 工作组(Task Group,TG)产生了研究讨论不同方向内容的任务组,其中 TGi 的主要目的就是提高当前媒体接入控制层的安全性能。IEEE 于 2004 年 6 月正式颁布了 IEEE 802.11i 标准,定义了强安全网络(Robust Security Network,RSN)。RSN 主要包括 IEEE802.1x 认证、密钥管理机制以及 TKIP 和 CCMP 加密算法。

IEEE 802.1x 协议被称为基于端口的访问控制协议,符合 IEEE 802 协议集的局域网接入控制协议,主要目的是为了解决无线局域网用户的接入认证问题。

IEEE 802.1x 标准采用现有的可扩展认证协议(Extensible Authentication Protocol,EAP),它是 IETF 提出的 PPP 协议的扩展。EAP 消息包含在 IEEE 802.1x 消息中,被称为 EAPOL,即 EAP over LAN,在 Supplicant(申请者)和 Authenticator(认证者)之间传输;Authenticator 和 Authentication Server(认证服务器)间同样运行 EAP 协议,EAP 帧中封装了认证数据,将该协议承载在其他高层协议中,如 Radius,以便穿越复杂的网络到达认证服务器,称为 EAP over RADIUS[2]。

本文分析和讨论了 IEEE 802.1x 的原理以及应用到无线局域网存在的安全问题,对于现有的解决方案的不足进行分析,提出合适的解决方案。

1 IEEE 802.1x 协议的认证机制

1.1 IEEE 802.1x 协议认证过程

下面以认证者和认证服务器分离,并在它们之间采用 RADIUS 协议(也可以使用其他高层协议)封装 EAP 协议包,上层认证协议采用 TLS 为例,简要说明 802.1x 协议的认证过程[3]:

1)客户端(也就是申请者)发出 EAP Start 消息发起认证过程;

2)AP 发出请求帧,要求客户输入用户名;

3)客户机响应请求,将自己的用户名信息通过数据帧发送给 AP;

4)AP 将客户的用户名信息重新封装成 RADIUS Access Request 包发送给服务器;

5)RADIUS 服务器验证用户名合法后客户机发送自己的数字证书;

6)客户机通过证书验证服务器的身份;

7)客户机给服务器发送自己的数字证书;

8)服务器通过证书验证客户身份,完成相互认证;

9)在相互认证的过程中,客户机和服务器也获得了主会话密钥 Master_Session_Key;

10)认证成功,RADIUS 服务器向 AP 发送 RADIUS ACCEPT 消息,其中包括密钥信息;

11)AP 向客户机转发 EAP Success 消息,认证成功。

1.2 IEEE802.1x 协议的缺陷

1)中间人攻击

IEEE 802.1x 协议最重要的缺陷是申请者和认证者的状

收稿日期:2006 - 06 - 20;**修订日期**:2006 - 09 - 05 **基金项目**:国家自然科学基金资助项目(60573050)

作者简介:周贤伟(1963 -),男,四川成都人,教授,博士,主要研究方向:通信网安全、宽带移动通信和组播安全; 刘宁(1982 -),男,内蒙古呼和浩特人,硕士研究生,主要研究方向:网络安全; 覃伯平(1971 -),男,四川江安人,博士研究生,主要研究方向:信息安全、无线传感器网络安全路由.

态机不平等。根据标准,认证者的端口只有当会话通过认证后才打开。而对于申请者,端口始终是处于已认证状态。这种申请者与认证者之间的单向认证将使申请者遭到中间人攻击。

802.1x 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。显然状态机执行的是单向认证。如果上层协议采用的是单向认证将使整个体系更加脆弱。

EAP/TLS 确实能提供强相互认证但不是强制的而且也可以饶过 EAP/TLS 进行中间人攻击。下面是一个简单的中间人攻击的例子:

当认证者从 RADIUS 服务器收到 RADIUS-Access-Accept 消息后,就向申请者发送一个 EAP-Success 消息。这就提示状态机认证已经成功。无论上层认证方法采用 EAP-TLS, EAP-MD5 或者其他认证,这条消息都没有完整性保护。而且申请者的状态机无条件的转换到已认证状态,不管当前的是什么。因此,攻击者可以伪造这个数据包来冒充认证者实现中间人攻击。这样被攻击的申请者会认为冒充的认证者就是合法的认证者,并把数据包发送到这个冒充的认证者[4]。

2)会话劫持

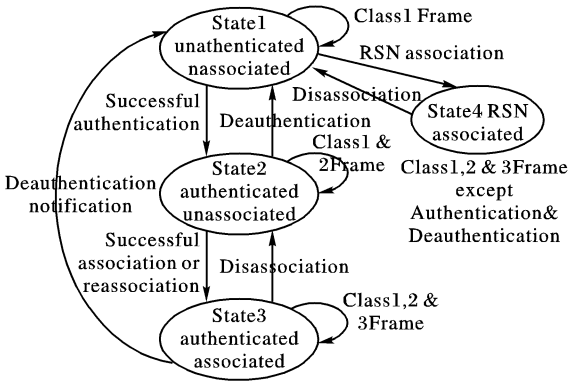

图 1　RSN 状态机

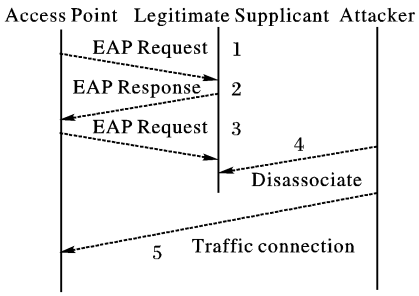

图 2　会话劫持攻击

图 1 是 RSN 状态机,共四种状态。之后进行 IEEE 802.1x认证。因此共有两种状态机:RSN 和 802.1x 状态机,它们共同指示认证的状态[5]。但是它们缺乏清晰的通信和消息真实性,所以很可能遭到会话劫持攻击。图 2 显示了会话劫持是如何实现的,攻击的过程如下:

(1)消息 1,2 和 3:合法的申请者进行认证(假设 EAP 认证只包含这 3 条消息,实际的 EAP 认证多于 3 条消息)。

(2)消息 4:攻击者冒充 AP 的 MAC 地址发送一条 disassociate 管理帧给申请者。这使得申请者的状态为 disassociated。这条消息使 RSN 状态机被设置为 Unassociated,而 802.1x 状态机的状态仍为 authenticated。

(3)消息 5:这时攻击者冒充申请者的 MAC 地址接入到网络。

3) DoS 攻击

IEEE 802.1x 没有提供 DoS 保护,使得服务器容易耗尽计算资源以及存储资源,而且可能导致合法用户无法正常接入。比如攻击者伪造一个合法用户的 MAC 地址向认证者发送 EAP-Logoff 消息,那么这个合法用户将与认证者中断连接[6]。

1.3　现有的解决方案

1)四步握手认证

目前已经使用的解决方案是四步握手认证方案,其基本思想是要求认证者基于 RADIUS 为申请者生成会话密钥,与请求者完成双向认证。其过程为:

(1)认证者首先向申请者发送第一个密钥确认消息,消息中包含一个随机数;

(2)申请者收到后,产生自己的一个新随机数,并将它发送给认证者;

(3)此时,申请者和认证者同时拥有对方的随机数。他们各自使用约定的加密原语,并将收到的随机数与本次会话密钥混合生成新的操作密钥;

(4)然后,认证者设置它的暂时密钥完整性协议(比如 TKIP)实例,认证者向申请者发送第三个密钥确认消息。此时,允许接收申请者的数据;

(5)当收到第三个密钥确认消息后,申请者设置它的暂时密钥完整性协议实例在操作密钥下发送和接收数据,并将第四个密钥确认消息发送给认证者;

(6)当认证者收到第四个密钥确认消息后设置 802.1x 端口,允许向申请者发送数据。

此协议可以保证,只有在暂时密钥完整性协议产生会话密钥之后才在网络上传输数据,可以抵御中间人攻击和会话劫持,然而此协议没有 DoS 保护和源真实性保护,对重放攻击和 DoS 攻击没有任何抵御。

2)完整性保护

其他的一些方案主要是在 EAPOL 的数据帧中加上一个完整性保护字段,一般是加上签名或者是 MD5 散列值,但是对源真实性保护仍然不够,黑客可以利用这一点进行重放攻击以及 DoS 攻击。

2　IEEE802.1x 协议认证机制的改进

目前 IEEE 802.1x 在无线局域网中起着不可替代的作用,如果采用新的协议不但难于被采纳还需要很长时间的安全性验证,又由于目前的方案仍不完善,因此我们在充分考虑了源真实性和完整性的基础上提出了改进的 IEEE 802.1x 认证——AIP(Authenticity and Integrity Protection)认证。

IEEE 802.1x 认证中存在上述缺陷的主要原因在于缺乏源真实性和完整性保护,所以 AIP 认证在 EAPOL 包中增加了一个 Protection 字段。如图 3 所示。

PAE Ethernet type	Protocol version	Type
Length	Packet Body	Protection

图 3　AIP 认证的数据包格式

这个 Protection 字段由两部分组成(Protection = HMAC + Key),第 1 部分为前 5 个字段的 MD5 散列,第 2 部分为上一个 EAPOL 数据包中 HMAC 的密钥。每条消息的密钥是随机的。在发送一个 EAPOL 数据包时并不携带这个散列函数的密钥,相反,这个密钥将在下一个数据包中携带。接收方在收到一个 EAPOL 包时首先进行存储,用接收到的下一个包的密钥验证上一个包的源真实性和完整性。AIP 认证的过程如图 4 所示。

1)客户端向认证者发送 EAPOL-Start 发起认证。认证过程同样可以由认证者发起,但是它直接发送 EAP-Request/ Identity 而不是 EAPOL-Start 消息。在第 1 条消息封装的最后

一部分是 Protection 字段,其中 HMAC 是数据帧随机用密钥 Ks_1(Ks 代表客户端的散列函数密钥)的散列值,因为是客户端的第 1 条消息,所以 Key 字段为 0。事实上,认证者在检测到端口从"disable"状态转移到"enable"状态时就向客户端发送认证请求。如果客户端没有收到来自认证者的认证请求,那么它就会在适当的时候通过 EAPOL-Start 消息发起认证过程;

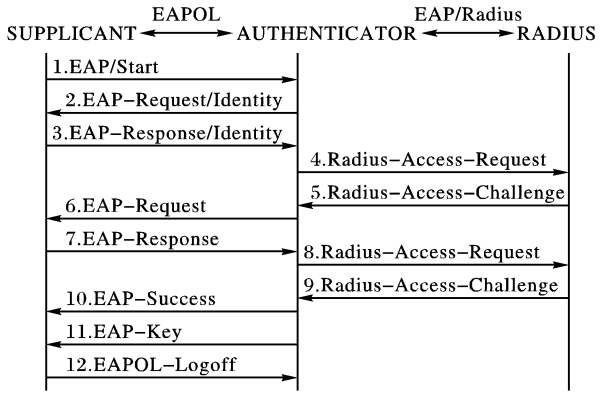

图 4 AIP 认证的过程

2)当认证者不知道用户身份时就发送该消息(EAP-Request/Identity)。其中 HMAC 是数据帧随机用密钥 Ka_1(Ka 代表认证者的散列函数密钥)的散列值,因为是认证者的第 1 条消息,所以 Key 字段为 0;

3)客户端收到 EAP-Request/Identity 消息,就用其用户名响应,发送 EAP-Response/Identity 消息给认证者,HMAC 是数据帧随机用密钥 Ks_2的散列值,Key 字段为 Ks_1;

4)认证者把包含有用户身份的 EAP 响应包重新以 RADIUS 协议格式封装,并把重新封装后的包由 RADIUS 客户端发送至 RADIUS 服务器;

5)RADIUS 服务器在收到该包后将选择具体的认证机制,并发送相应的 EAP 请求包到认证者;

6)认证者并不解释来自 RADIUS 的 EAP 包的具体内容,而只是检查 RADIUS 协议包的类型,由于是质询包,因此认证者将其毫不改变的转发给客户端,HMAC 是数据帧随机用密钥 Ka_2的散列值,Key 字段为 Ka_1;

7)客户端收到上述请求包后,如果支持 RADIUS 服务器选择的认证机制,就根据认证机制的要求作出响应,并通过 EAP 封装后发送给认证者,HMAC 是用客户端私钥对数据帧的签名,Key 字段为 Ks_2;如果不支持 RADIUS 服务器选择的认证机制,则发送 NAK 包,这样 RADIUS 服务器将重新选择认证机制,并从第 5 步重新开始;

8)认证者把来自客户端的 EAP 响应包中继到 RADIUS 服务器;

9)如果 RADIUS 认证服务器通过了对客户端的认证,则向认证者发送 RADIUS-Access-Accept 消息;否则就向其发送 RADIUS-Access-Reject 消息;

10)如果认证者收到 RADIUS-Access-Accept 消息,则认为认证成功,于是打开受控端口,并向客户端发送 EAP-Success 消息,此后客户端就可以进行授权的正常通信过程,如果认证者收到 RADIUS-Access-Reject 消息,则认为认证失败,于是关闭受控端口,并向客户端发送 EAP-Failure 消息,HMAC 是用认证者的私钥对数据帧的签名,Key 字段为 Ka_2;

11)当客户端通过认证(重认证)之后,无线接入点 AP 将向客户端发送用来加密广播帧的广播密钥 EAPOL-Key。广播密钥的发送保证了客户端用于单播时会话密钥的保密性。而会话密钥的派生与发送与认证服务器选择的具体的认证机制有关;

12)当客户端离线时,向认证者发送离线通知 EAPOL-Logoff,HMAC 为客户端私钥对数据帧的签名,Key 字段为 0,认证者收到消息后重新关闭受控端口。

认证过程中 EAP-Request 和 EAP-Response 可能有多条消息构成,这里我们只用 6 和 7 两条消息代表。

3 AIP 认证的性能分析

AIP 协议将弥补第 2 部分所分析的中间人攻击和会话劫持两个缺陷,同时在很大程度上弥补缺乏 DoS 保护的缺陷。

由于 AIP 认证中对于客户端和认证者的交互消息引入源认证以及完整性保护。这样即保证了源真实性也保证了完整性,使得重放攻击对于认证过程以及认证实体的影响降低到较小的程度。

同时,如果攻击者想伪造一个 EAPOL 包,那么他必须还要有前一个 EAPOL 包中散列函数的密钥,这对于攻击者几乎是不可能的。由于在改进的协议中,接收者要存储一个数据包,等下一个数据包到来时才进行验证,这里只要限制存储的数据包只能为 1,这样即使攻击者进行 DoS 攻击也不能耗尽服务器的计算资源和存储资源。

由于 AIP 认证过程中认证者和客户端在交互认证消息时还要计算完整性校验以及存储一条消息,所以协议的复杂度就提高了。

4 结语

由于 802.1x 缺乏相互认证以及源真实性和完整性保护,使无线局域网容易遭到中间人攻击、会话劫持以及 DoS 攻击。为了解决这些缺陷,目前已提出了四步握手认证和完整性保护,但是这些方案没有考虑源真实性保护,仍然存在遭受这些攻击的可能性。本文充分考虑了源真实性和完整性保护,提出了一个新的改进方案。如果将四步握手认证与该改进方案结合,将达到更好的效果,但需要服务器和客户端有更强的计算能力。

参考文献:

[1] IEEE Std 802.11. Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications[S]. LAN/MAN Standards Committee of the IEEE Computer Society, 1999.

[2] IEEE Std 802.1X-2004. IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control[S]. LAN/MAN Standards Committee of the IEEE Computer Society, 2004.

[3] 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, 2004.40-57.

[4] MISHRA A, ARBAUGH WA. An Initial Security Analysis of the IEEE 802.1x Standard[R]. Technical Report Collection CS-TR-4328, University of Maryland Computer Science Department, 2002.

[5] IEEE Std 802.11i-2004. IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications-Amendment 6: Medium Access Control (MAC) Security Enhancements[S]. LAN/MAN Standards Committee of the IEEE Computer Society, 2004.

[6] WAN ZG, ZHU B, DENG BH. DoS-Resistant Access Control Protocol with Identity Confidentiality for Wireless Networks[R]. IEEE Wireless Communications and Networking Conference 2005 (WCNC'05)[C]. New Orleans, LA, USA, 2005.