无线局域网中的认证机制

刘 可,徐昌彪,杨士中
(重庆大学 通信工程学院,重庆 400030)

摘 要:当前无线局域网(WLAN)主要的认证技术包括了IEEE 802.11中的开放系统认证和共享密钥认证,IEEE 802.11i中的802.1x认证协议,以及我国的无线局域网安全标准WAPI中的WAI认证机制。概述了以上各种认证机制,讨论了它们各自的优缺点,并根据其存在的安全漏洞,给出了两种改进方案。最后给出了WLAN认证机制的进一步研究方向。

关键词:IEEE 802.11;认证;无线局域网
中图分类号:TN925+.93 **文献标识码**:A **文章编号**:1673-629X(2008)01-0164-04

Authentication Mechanisms in WLAN

LIU Ke, XU Chang-biao, YANG Shi-zhong
(College of Communication Engineering, Chongqing University, Chongqing 400030, China)

Abstract: Now the main authentication techniques of wireless local area network(WLAN) include open system authentication and shared key authentication in IEEE 802.11, 802.1x authentication protocol in IEEE 802.11i, and WLAN authentication infrastructure(WAI) authentication mechanism in national WLAN security standard WAPI(WLAN authentication and privacy infrastructure). In the paper, gives a detailed introduction to various anthentication mechanisms mentioned before, and discusses their respective advantages and disadvantages. According to their security leaks, gives two amelioration schemes. In the end, concludes the further research direction for WLAN authentication mechanisms.

Key words: IEEE 802.11; authentication; WLAN

0 引 言

随着WLAN的迅速发展,其安全问日题益受到人们的关注。WLAN中的数据通过射频无线电传输,恶意攻击者容易实施窃听。与有线网络相比较,WLAN难以采用物理的控制措施,因此保护WLAN的安全难度要远大于保护有线网络。人们已经认识到必须专门为WLAN设计安全保护机制,以保护在WLAN中传输数据的机密性和完整性,同时对请求接入WLAN的用户进行身份认证和访问控制。

认证是WLAN网络安全的主要业务之一。文中概述了当前几种主要的认证技术,讨论了它们各自的优缺点,并根据它们存在的安全漏洞,给出了两种改进方案。

收稿日期:2007-03-07
基金项目:国家发改委CNGI2005示范工程项目(CNGI-04-4-2D);重庆市教委科学技术研究项目(040507);重庆市科委自然科学基金项目(CSTC,2006BB2164)
作者简介:刘 可(1982-),男,重庆人,硕士研究生,研究方向为移动通信;徐昌彪,博士后,副教授,研究方向为宽带无线接入、网络性能分析;杨士中,中国工程院院士,教授,博士生导师,研究方向为无线网络通信、测控及遥感信息传感。

1 无线局域网认证机制的安全需求

认证方案主要实现以下目的:

1)认证网络用户的身份,防止非法用户假冒合法用户身份占用网络资源、删除或篡改用户存储的数据;

2)会话密钥的分配,以便于通过加密技术保护合法用户在网络上通信的内容,防止非法用户窃听。

认证的密钥建立协议具有以下特性[1]:

(1)已知密钥安全(Known Key Security, KKS)。即使攻击者知道以前的会话密钥,协议仍然能够保证当前会话密钥的安全。

(2)很好的前向保密(Perfect Forward Secrecy, PFS)。当所有通信参与者的长期私钥均被破解时,以前的会话密钥仍不受影响。

(3)无密钥泄露伪装(no Key Compromise Impersonation, Non-KCI)。当A的长期私钥泄露后,攻击者在协议中只能伪装成A,而不能把A伪装成其他任何人。

(4)无未知密钥共享(no Unknown Key Share, Non-UKS)。在未知密钥共享攻击中,攻击者E使A以为是和攻击者E共享秘密,而实际上A是和B共享秘密。

2 IEEE 802.11,IEEE 802.11i 以及 WAPI 中的认证机制

2.1 IEEE 802.11 中的认证机制

IEEE 802.11[2]规定了两种认证方式:开放系统认证(Open System Authentication)和共享密钥认证(Shared Key Authentication)。根据 IEEE 802.11 WLAN 的工作原理,另外两种机制:服务组标志符(SSID)和 MAC 地址控制也被广泛使用。

2.1.1 开放系统认证

根据 IEEE 802.11 规范的描述,开放系统认证实质上是空认证,采用这种认证方式任何用户都可以成功认证。

2.1.2 共享密钥认证

采用共享密钥认证的工作站必须执行 WEP(the Wired Equivalent Privacy),共享密钥必须以只读的形式存放在工作站的 MIB 中。

由于 WEP 是采用将明文和密钥进行异或的方式产生密文,同时认证过程中密文和明文都暴露在无线链路上,因此攻击者通过被动窃听攻击手段捕获密文和明文,将密文和明文进行异或即可恢复出密钥[3]。

由于 AP 的挑战一般是固定的 128B 数据,一旦攻击者得到密钥,他就可以利用该密钥产生 AP 挑战的响应,从而不需知道共享密钥就可成功获得认证。如果后续的网络通信没有使用加密手段的话,则攻击者已经完成了伪装的攻击,否则,攻击者还将采用其他的攻击手段来辅助完成其攻击。

对于另外的两种机制,首先由于 SSID 在 AP 广播的信标侦中是以明文形式传送的,非授权用户可以轻易得到它。即使有些生产厂家在信标侦中关闭了 SSID,使其不出现在信标侦中,非授权用户也可通过监听轮询响应侦来得到 SSID,因此 SSID 并不能用来提供用户认证;其次由于用户可以重新配置无线网卡的 MAC 地址,非授权用户可以在监听到一个合法用户的 MAC 地址后,通过改变他的 MAC 地址来获得资源访问权限,所以 MAC 地址控制功能也不能真正地阻止非授权用户访问资源。

根据以上的分析,IEEE 802.11 提供的认证手段以及从其工作原理衍生的附加手段都不能有效地实现认证目的。另外,必须注意到,IEEE 802.11 提供的认证只是单向认证,即只认证工作站的合法性,而没有认证 AP 的合法性,这使得伪装 AP 的攻击很容易实现。根据参考文献[4]的描述,存在会话劫持和中间人攻击的可能性。

2.2 IEEE 802.11i 中的认证机制

在 IEEE 802.11i 定义的新的安全体系——坚固安全网络(RSN)[5]中采用了基于 802.1x 的对于 AP 和 STA 的双向增强认证机制。802.1x 协议于 2001 年 6 月由 IEEE 正式公布,它是基于端口的网络访问控制方案。它不仅提供访问控制功能,还提供用户认证和计费的能力。802.1x 并非专门针对 WLAN 设计,它适用于符合 IEEE 802 标准系列的各种网络(如以太网)。它的核心是 EAPoL(Extensible Authentication Protocol (EAP) over LANs)的框架[6],主要有三个实体:申请者(Supplicant)、认证者(Authenticator)和认证服务器(Authentication Server)。认证服务器在通常情况下为 RADIUS(Remote Authentication Dial In User Service)服务器[7],用户帐户信息存储在该服务器中。扩展认证协议 EAP 只是一种封装协议,在具体应用中可以选择 EAP-TLS,EAP-SIM,PEAP,EAP-TTLS 等任一种认证协议,因此 802.1x 在实现上具有较大的灵活性。

然而在 PKI(Public Key Infrastructure)[8]没有广泛部署时,在实践中操作起来比较困难。另外,AP 和 Radius 服务器之间需手工设置共享密钥,其管理存在安全隐患,并使得构建和扩展易用性差,用户身份凭证简单,易被盗取,且被盗取后可任意使用。最后,STA 未鉴别 AP 的合法性,使得假冒 AP 变得可能。

2.3 WAPI 中的认证机制

我国早在 2003 年 5 月份就提出了无线局域网国家标准 GB 15629.11,这是目前我国在这一领域惟一获得批准的协议。标准中包含了全新的 WAPI(WLAN Authentication and Privacy Infrastructure)安全机制,这种安全机制由 WAI(WLAN Authentication Infrastructure)和 WPI (WLAN Privacy Infrastructure)两部分组成,WAI 和 WPI 分别实现对用户身份的鉴别和对传输的数据加密[9]。

但是 WAI 仍然存在许多安全缺陷:

(1)WAI 协议不具备身份保护的功能[10]。

(2)在认证协议中缺乏对用户私钥的验证环节。

(3)密钥协商过于简单,不具备相应的安全属性。如无法抵抗密钥一致性攻击[11]。

(4)密钥协商算法的安全是基于加密算法的安全性。另外,异或运算可能使会话密钥与随机数间保持一种代数关系,在产生的会话密钥中可能有以不可忽略的概率被预测的弱密钥位存在,导致其安全性受到影响[12]。

(5)该算法不具有 PFS 等安全属性也无法防止密钥控制(Key Control)。

(6)该算法使用时间戳来抵抗重放攻击:其安全性主要依赖于时间的同步。然而时间戳技术的实现比较

困难,从而降低了该算法的性能。

3 两种改进方案

3.1 改进的共享密钥认证

共享密钥认证检验 STA 是否拥有 WEP 共享密钥,基于"询问—应答"模式,但是由于设计存在漏洞,没有实现双向认证,也无法防范中间人攻击,而且联合 RC4 的弱点还存在更大的安全隐患。鉴于共享密钥认证目前应用较多,漏洞较大,引入数字公钥证书对共享密钥认证进行改进[13],以达到实现双向认证的目的。

首先,AP 需要在 PKI 系统中注册自己的公钥证书,并取得相应的私钥将私钥和证书安装在 AP 端。STA 移动站需要取得 CA 证书,用于验证 AP 公钥证书的真实性。

改进的共享密钥认证协议的协商过程使用 802.11 协议族的 MAC 帧来进行,改进协议使用帧类型中的管理帧进行,使用认证帧来进行消息的封装。可在 MAC 帧的 Data 域中设定两个相关字段:改进协议字段(Improved)和 AP 证书字段(Certificate)。使用改进协议进行认证则 Improved 字段置 1,若首次与 AP 进行认证,则 Certificate 字段置 0,否则置 1。认证过程如图 1 所示。

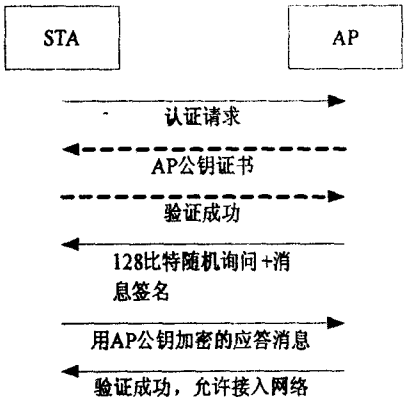

图 1 改进的共享密钥认证

改进的共享密钥认证协议,通过公钥密码技术来验证 AP 身份,仍通过检验是否拥有 WEP 密钥来验证 STA 身份。

此改进协议使欺诈 AP 无法成功。此协议依照 AP 公钥证书并检验 AP 是否拥有 AP 私钥来确定 AP 身份。若欺诈 AP 在(2)中传送伪造公钥的证书,因为改进协议建立在 CA 是绝对安全的基础上,欺诈 AP 不可能获得 CA 私钥,所以 STA 在(3)中,用 CA 公钥验证证书时,即可发现 AP 为欺诈 AP。若欺诈 AP(2) 中传送一个真正的 AP 公钥证书给 STA,由于欺诈 AP 不知道该 AP 公钥证书对应的私钥,所以欺诈 AP 在(4)中构造对消息的签名时,无法得到正确的签名,所以 STA 在(5)中用正确的公钥验证签名时必定失败,从而取消连接。由于 STA 在 AP 身份得到完全验证后才传送应答消息,所以欺诈 AP 无法通过未完成的协议得到 WEP 密钥的任何信息。

此外,改进协议也很好地防范了原共享密钥认证中存在的中间人攻击。若有敌对者一直在认证过程中监听信道,他可在(4)中获得 128 比特随机询问的消息明文和 AP 对其进行的签名,但 STA 用 WEP 密钥加密的询问消息由 AP 公钥保护,由于监听者不知道 AP 私钥,所以他无法解开由 AP 公钥加密的应答消息,从而反解出 WEP 密钥。

由以上分析可以看出,此协议的安全性依赖于公钥算法的安全性以及 AP 私钥的保密性,安全假设建立在只有真正的 AP 知道 AP 私钥的基础上,所以,一旦 AP 私钥泄漏,协议将失去作用。

另外,改进协议无法抵抗字典式攻击。在改进协议中,AP 对于 STA 的验证仅依靠验证 STA 构造的用 AP 公钥加密的应答消息的正确性来获得。由于 AP 公钥以及 WEP 密钥都是固定不变的,所以相同的明文询问相对应的 STA 的加密应答消息相同。而由于(4)中,询问消息明文传输,所以攻击者可以监听信道,将明文随机询问和加密的应答消息对应建立字典,若发现随机询问发生重复时,即可找出对应的加密应答消息,冒充合法的 STA 接入网络。

3.2 基于 PKI 系统的双向身份认证方案

整个身份认证系统由用户 MT、接入点 AP 和认证服务器组成:其中,认证服务器的主要功能是负责证书的发放、验证与吊销等;用户与 AP 上都安装有认证服务器发放的数字证书(证书包含 AS 的公钥以及证书持有者的身份和公钥)作为自己的数字身份凭证。当用户登陆至无线接入点 AP 时,在使用或访问网络之前必须通过 AS 进行双向身份验证。根据验证的结果,只有持有合法证书的用户才能接入持有合法证书的无线接入点 AP。具体的认证过程如图 2 所示,详细流程参见参考文献[14]。

值得注意的是,当加密和数字签名相结合时,加密和数字签名过程的顺序不一样将导致不同的安全强度[15],最好是先签名后加密。

该方案增加了认证服务器对 AP 的认证,确保假冒 AP 的攻击不可能实现,并且增加了临时密钥分发给接入点 AP 过程中的加密,确保只有合法的 AP 才能解密得到临时密钥。但是该方案仍然存在以下问题:

(1)身份认证的性能优化,为了确保安全,身份认证机制采用基于数字证书的双向身份认证机制,效率比较低,虽然用户认证的时间在认证中所占的比率比

较小,但还是会影响到用户的效率,需要提高身份认证的效率。

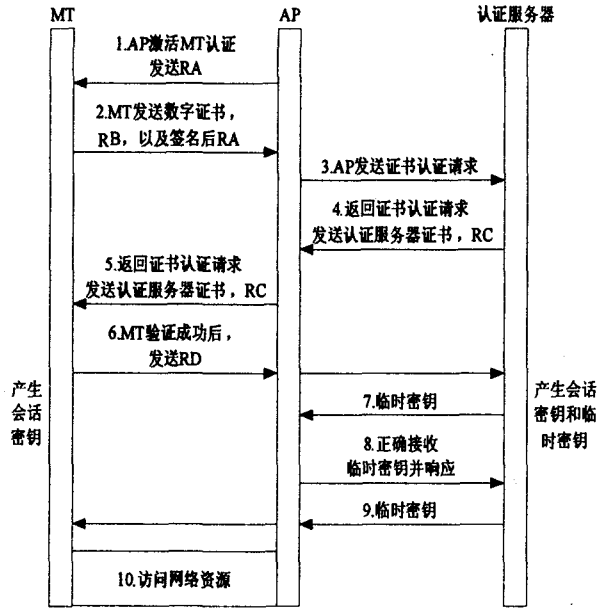

图 2　双向身份认证过程

(2)每个站点需要一定的计算能力,不方便,并且操作的同步不易实现,此外,临时密钥生命期的确定应结合实际情况来确定,因为即使是一个局域网,其网络通讯量随时间变化而不同,过分频繁地更换临时密钥会造成浪费。

(3)在方案中用到了公钥基础设施 PKI,目前看起来是不太现实的。如何建立这样的 PKI 已经超越了建立 WLAN 安全体系的范围,是一个更加重大的问题,有待于开展进一步的研究。

4　结束语

文中讨论了当前无线局域网主要的认证技术,通过分析每种协议的认证流程,得出其优点和缺点,然后还给出了两种改进方案。可以看出,要想做到完全满足无线局域网的安全需求是相当困难的,认证协议不仅应该实现显式密钥认证以及相关敏感数据的机密性,还应该具有文中开头所提到的 4 个安全性质(KKS,PFS,non - KCI 和 non - UKS),但是同时无线环境中传送的包容易损坏和丢失,而且漫游也很普遍,这就要求认证协议的交互轮数尽量少,从而达到较高的效率和性能。在安全和性能间如何取舍,设计出最适合无线局域网的认证方案,是我们研究的重点。此外,无线网络还将面临拒绝式服务 DOS(Denial Of Service)攻击的威胁,DOS 攻击利用了 TCP/IP 协议在设计上的缺陷,又具有极佳的隐蔽性,致使至今人们也没有找到一个比较完善的解决办法,虽然无线环境下的 DOS 攻击只是崭露头角,但是如果不能尽早地予以重视,这种攻击方式将给无线网络未来的发展带来长久的危害。

目前 WLAN 多种安全机制并存并且互不兼容,特别是我国自己的安全标准 WAPI 与先行标准 IEEE 系列差异较大,存在漫游及设备兼容等一些问题,因此多种安全机制的兼容性问题也有待于进一步研究,从而推动 WLAN 产业的发展。

参考文献:

[1] SONG B, KIM K. Two - pass authenticated key agreement protocol with key confirmation[C]//Progress in CryptologyINDOCRYPT 2000, LNCS 1977. [s. l.]: Springer - Verlag, 2000: 237 - 249.

[2] IEEE Standard 802. 11. IEEE STANDARDS BOARD. 802 part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications[S]. 1999.

[3] CISCO. A Comprehensive Review of 802. 11 Wireless LAN Security and the Cisco Wireless Security Suite[EB/OL]. 2002. http://security. itworld. com/4942/030328review, Roshan P.

[4] MISHRE A, ARBANGH W A. An Initial Security Analysis of the IEEE802. 1x Standard[EB/OL]. 2002 - 02. http://www. prism. gatech. edu/gte369k/csc/802-1x. pdf.

[5] IEEE P802. 11i D3. 0. Specification for Enhanced Security[S/OL]. 2002 - 11. http://www. cs. umd. edu/~mhshin/doc/802. 11/802. 11i - D3. 0. pdf.

[6] IEEE Std 802. 1x. IEEE Standard for Local and Metropolitan Network - Port Based Network Access Control[S]. 2001.

[7] 朱　恺,曹秀英. 无线局域网中 RADIUS 协议原理与实现[J]. 微计算机信息,2004(9):118 - 120.

[8] GASSKO I, GEMMELL P S, MACKENZIE P. Efficient and Fresh Certification[C]//Proceedings of the Conference Public Key Cryptography 2000. [s. l.]: Springer, 2000: 342 - 353.

[9] GB15629. 11 - 2003. 信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分:无线局域网媒体访问(MAC)和物理(PHY)层规范[S]. 2003.

[10] 曹秀英,耿　嘉,沈　平,等. 无线局域网安全系统[M]. 北京:电子工业出版社,2004.

[11] 徐　朴,卢平平,江　溯. 无线局域网 HiperLan/2 标准综述[J]. 中兴通讯技术(简讯),2001(8):20 - 22.

[12] 韩　玮. 无线局域网安全技术研究[D]. 西安:西安电子科技大学,2003.

[13] 吴　瑜. 无线局域网安全与 PKI 安全体系[D]. 北京:北京邮电大学,2005.

[14] 李　歆. 无线局域网安全技术研究与改进[D]. 武汉:华中科技大学,2005.

[15] 张龙军. 无线局域网安全技术研究[R]. 广州:中山大学图书馆,2003.