基于802.11i的WLAN安全认证机制研究与实现

殷安生
(南京邮电大学 软件学院,江苏 南京 210003)

摘 要:WLAN标准IEEE 802.11的安全机制存在严重的漏洞,论证了如何以最新的IEEE 802.11i标准中的安全机制来改善WLAN的安全性。考虑安全性与效率,应侧重依靠认证机制来实施WLAN的安全防护,通过IEEE 802.11i RSN中的安全措施来更新WLAN现有的安全体系。最后基于EAP-TLS认证机制,设计了一种WLAN安全认证系统模型,该模型改变了传统认证机制中的安全策略,使用四步握手以及增强的密钥颗粒度方法提高了认证过程的安全性,并给出了该安全认证系统相应认证模块的软件实现方案,同时对该认证系统的安全性和适用性进行了相关论证。

关键词:无线局域网;802.11i协议;RSN;802.1x协议;EAP-TLS;密钥协商
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2010)09-0127-04

Research and Implementation on Secure Authentication Mechanism of WLAN Based on 802.11i Protocol

YIN An-sheng
(College of Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: IEEE 802.11 which has been issued today mostly proved ineffectiveness and insecurity in secure mechanism, present a secure mechanism of latest IEEE 802.11i to improve the security of WLAN. It should emphasize particularly on authentication to implement the safeguard of WLAN, upgrade secure system through RSN of IEEE 802.11i. Also propose a secure authentication system model for WLAN based on EAP-TLS authentication mechanism. The model has changed the traditional authentication mechanism in the security policy, using a four-step handshake, as well as particle size increased the key means to enhance the security of the certification process, gives software implementation scheme of corresponding authentication modules, proves the security and applicability of this authentication system.

Key words: WLAN; 802.11i protocol; RSN; 802.1x protocol; EAP-TLS; key negotiation

0 引 言

无线网络面临着同有线网络一样的安全威胁,同时由于自身的特点还面临着比有线网络更严重的威胁。因此应用中要求一个无线网络应能提供相应的安全服务来保障WLAN的安全性。主要的WLAN标准IEEE 802.11,其安全机制存在严重的漏洞,体现在认证、加密和数据完整性三个方面。IEEE 802.11采用以WEP为基础的共享密钥认证,而WEP协议本身的设计问题也存在重大的安全漏洞;以WEP协议进行数据保密。但WEP是基于RC4算法对称密钥流密码加密机制,无法提供有效的消息保密性;通过在WEP中引入CRC32函数计算综合检测值(ICV)来提供对数据完整性的保护。但CRC32函数不是安全的哈希函数,不具有身份认证的能力。

鉴于IEEE 802.11存在的安全漏洞,IEEE又制定了IEEE 802.11i标准,以增强IEEE 802.11的媒体接入控制功能,改进无线局域网的安全性。

IEEE 802.11i主要在MAC层对IEEE 802.11的安全机制进行了提升,从数据加密、身份认证、密钥管理等方面提升了IEEE 802.11的安全性。主要包括应用TKIP(Temporal Key Integrity Protocol)和CCMP(Counter Mode CBC-MAC Protocol)加密算法,提供比原有WEP协议更加健壮的数据保护机制;引入安全联合的概念,定义了安全联合管理协议4-WAY Handshake和Group Key Handshake,提供以往IEEE 802.11所不具备的密钥管理功能;还制定了如何利用802.1x进行有效认证的规范,推荐使用EAP-TLS认证协议,以提供更加安全的双向认证。

收稿日期:2009-12-08;**修回日期**:2010-03-27
基金项目:江苏省高技术研究计划项目(BK2007603)
作者简介:殷安生(1982-),男,讲师,博士研究生,研究方向为无线网络安全研究。

1 无线局域网的认证技术

1.1 IEEE 802.1x 认证机制

基于端口的访问控制协议 IEEE 802.1x 能够在利用 IEEE 802 局域网优势的基础上提供对接入用户的认证和授权。相对以往的认证方式，IEEE 802.1x 协议要更加可靠，主要通过划分控制端口和非控制端口，将认证结果表现在不同的端口状态上，抛弃传统的身份与地址相一致的概念，提高了自身的安全性，但是同时也存在着一些不足，主要表现在：1) 在 802.1x 协议中用户和网络的地位不相等，用户始终处于一种被鉴别的状态，但是攻击者有时候可能通过劫持一个网络来攻击用户，可能会产生窃听无线终端 STA 和无线 AP 间的通信实施中间人(MIM)攻击；2) 无线终端 STA 和无线 AP 间传送的底层信号不具备安全性，容易被欺诈和劫持。

1.2 EAP 认证协议和 EAP－TLS 认证

EAP(Extensible Authentication Protocol)协议是 802.1x 标准中采用的认证协议。EAP 协议可运行在任何链路层之上(PPP、802.11、802.3)，具有良好的适用性。同时，采用高层认证技术，支持多种 IETF 安全协议标准(TLS、IKE 等)，但是 EAP 并不提供完整性和机密性保护。

为保证传输层的安全，对 EAP 包再一次封装，目前 EAP 与传输层技术 TLS(Transport Layer Security)结合的 EAP－TLS[1]是一种广泛应用，能够提供强大的交互认证及会话密钥协商的安全认证机制。用于在客户机和服务器之间构建安全的通信通道，以提供更高的安全级别。EAP－TLS 提供基于证书和公钥的双向认证，而且动态更新密钥，生成的密钥只有在一定范围的用户才能够知道。从而最大限度上保证了认证过程的安全性。

2 WLAN 安全认证系统模型

2.1 WLAN 安全认证模型

系统应用 IEEE 802.1x 协议和 EAP－TLS。包括 AS(认证服务器)、Authenticator(认证者)、Supplicant(客户端)三部分；整个认证过程相对 AP(接入点)来说是透明的，包含有主体模块、认证模块、加密模块等，主体流程由认证模块完成，主要负责客户端与 AS 之间的通讯；认证服务器采用成熟的 RADIUS 服务器[2]，密钥管理模块参考 802.11i RSN 中的约定，采用四步握手密钥协商机制[3]，动态地产生和分配密钥。其中认证协议和密钥管理模块则可在应用层通过软件实现，认证服务器可在一台 Linux 主机上，对其配置开源的 FreeRadius。RADIUS 协议可实现认证、授权、计费在内的 3A 协议，支持多种 EAP 认证方式，通过建立 RADIUS 服务器和 SQL Server 并使之相连，通过用户数据库和计费数据库对用户信息和计费信息进行有效管理。拓扑结构如图 1 所示。

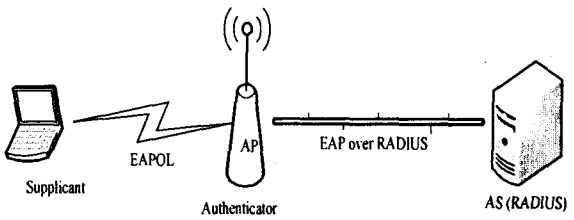

图 1 WLAN 安全认证系统拓扑结构

2.2 WLAN 安全认证系统软件设计方案

设计中将逻辑上独立的认证者(Authenticator)和认证服务器(AS)都配置到一台 Linux 服务器上，在该服务器上实现认证者和认证服务器的功能[4]。为了实现认证服务器的功能，文中通过配置 FreeRADIUS 服务器来实现(openssl + FreeRADIUS)，并对其源码作了相应修改，以实现 EAP－TLS 认证。具体设计中，对 802.1x/EAP－TLS 认证的软件部分，主要考虑在 Authenticator 上实现的认证功能。

文中在 Linux(Redhat 9.0)环境下，设计了 WLAN 安全认证系统的软件实现方案，包括安全认证、密钥管理等功能，用户只有通过认证之后才能登录到网络，并且整个认证过程和之后的数据交换都在安全的信道中进行，保证了安全性和可靠性。认证系统中认证状态机主要使用的是 802.1x 状态机[5]。

软件的认证和密钥管理部分主要有以下模块：

(1)认证系统主函数运行在认证者端，系统启动之后运行一个多线程的程序，对每一个要求加入系统的用户进行鉴别，如果用户已经通过认证并存入了系统数据库中，则将更新一次用户的身份信息和密钥。如果收到退出系统的要求则直接将用户从数据库中删除，所有这些用户的加入和退出都是并发的。

(2)认证者功能模块的功能为：1)负责 802.1x 协议中对 STA 和 AS 之间认证过程的控制，用户到达之后要对其进行认证，认证通过加入。如果用户突然离开网络，要能够进行离线操作，在用户恢复之后要能够进行重新认证，以确保安全；2)首先通过 EAPOL 转发 STA 和认证服务器之间的认证信息，然后通过 Radius 进行转发；3)网络通过最终认证的结果决定 STA 是否允许接入；4) 在数据库中保存通过认证或正在通过认证的无线终端 STA 状态信息；5)从 AS 处获取 PMK。

(3)认证服务器功能模块的实现，是将逻辑上独立的认证者和认证服务器都配置到一台 Linux 服务器上，在该服务器上实现认证者和认证服务器的功能，在

Linux 平台上,使用网络编程技术,由于 RADIUS 服务器上传输层协议为 UDP,STA 和 AS 支持 EAPOL 协议,认证和申请都可以在链路层进行通信,使用进程与线程技术,UI 与底层通信时通过进程传递消息,认证者和 AS 的程序之间通过线程实现各种互动。

(4)认证服务器协商密钥,使用四步握手密钥协商机制,这里的四步握手密钥协商主要确认认证服务器和申请认证者之间拥有一致的 PMK(Pairwise Master Key),以产生新的 PTK(Pairwise Transient Key),也用来通知申请者端加载加密/整体性校验机制。

(5)客户端功能的实现模块程序,首先设置模式和参数,然后应用认证系统通过 802.1x 进行认证,同时返回一个最终的结果。如果认证成功,这时候进行第四步的操作,进行密钥协商,协商成功后就可以进行加密和整体性校验,整个认证过程完成,用户可以进行通信了;相反,如果认证过程和密钥协商过程没有成功,那么就直接退出。用户可以在合适的时机重新提起一次认证过程。

2.3 EAP-TLS 认证改进

EAP-TLS 作为基于 TLS 的认证方式,在认证服务器与客户端采用 TLS 协议协商会话密钥。而 TLS 协议比通常分析的密码协议要复杂的多,这种复杂的密码协议一般都有比较多的安全漏洞,在 TLS 协议握手过程中存在一些不稳定的因素。

TLS 协议的主要部分为记录协议和握手协议。记录协议提供 TLS 连接状态的环境,透明封装高层应用协议,从高层协议接收到数据后,对数据进行分段、压缩、认证和加密形成 TLS 记录。而握手协议的安全性是整个 TLS 协议安全性的基础,用于在服务器和客户传输数据之前进行必要的准备工作,协商建立会话状态的各种参数。

2.3.1 TLS 认证过程的改进

TLS 认证在建立安全信道后使用加密数据进行传输,但是在建立安全信道之前却是使用明文进行数据的传输,这是一个很大的安全漏洞,攻击者可以使用一些工具或方法来套取服务的密钥,在交换证书或认证之初都有可能泄漏证书身份和证书隐私信息,通过这些信息的破解,攻击者完全可能掌握 master_secret[6]。要想提高认证过程的安全性,就必须对 TLS 握手机制进行改进,完善握手协议协商过程[7],使得整个过程一直都处于一种安全加密的通道内,减少被攻击的可能性。

可以利用 DH(Diffie-Hellman)密钥交换算法建立初始加密通道,对 TLS 握手协商过程进行改进。改进后的 TLS 握手协议如图 2 所示。

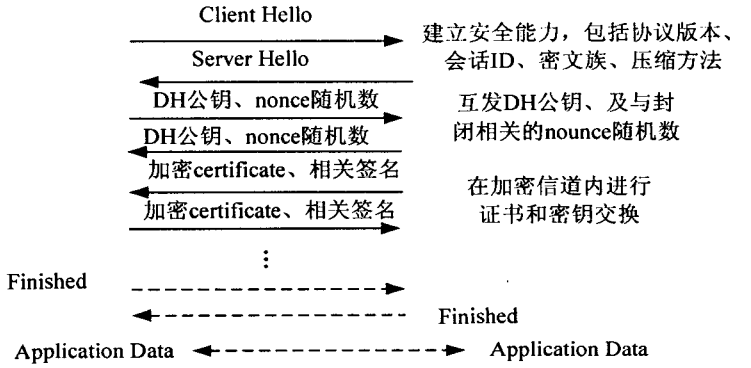

图 2　TLS 协议握手协商过程的改进

这种改进方法借鉴了 IKE 协议的思想,利用 DH 密钥交换算法建立初始加密通道。减少了 TLS 认证过程中的漏洞,可以在加密之初就对信道进行安全保证,减少了对握手协商过程进行窃听和分析的可能性。

2.3.2 TLS 加密过程中的漏洞和相应改进措施

在 TLS 加密过程中,是以 KeyExchange 产生 pre_master_secret,然后利用 PRF 函数产生 master_secret,最后由当时所选用的算法及相关参数,使用 PRF 计算出长度足够的 Key_block,从 Key_block 中依次取出所需的各种密钥,再利用这些密钥对应用层数据进行加密和密码校验。

TLS 协议中用单一的密钥来加密数据[8],其中可能包括一些长度很大的数据,这样就为攻击者提供了大量的密文信息(针对某一固定的密钥),增加其破解密码获得密钥的可能性;此外由于网络环境的因素,网络中的数据传输速率有可能较慢,这会使得密钥在很长一段时间内不能得到更新,增加了被破解的危险性。

为防止潜在的对 TLS 加密数据的分析攻击,有必要根据密码学一次一密的思想对 TLS 的加密方式进行改进。主要是通过改变数据的长度颗粒度和时间颗粒度来对握手协议进行改进,以增加破解的难度,提高安全性,改进的握手协议如下:

```
Struct{
    Random random;
    SessionID session_id;
    CipherSuite ciphersuites;
    Uint8 lenrefresh;
    Uint8 timerefresh;
}ClientHello
```

这种改进不需要改变 TLS 原有的计算方法,只需在加密和鉴别时稍加改进就可以。

通过对握手协议的改进,在一定程度上保证了

master_secret 和服务器私钥的安全，保证生成的随机数的质量，对证书进行严格的认证，就可以保证 TLS 协议的安全。

2.4 安全机制对网络性能的影响

根据 802.1x 认证机制，基于 802.11 和 802.1x 标准，将无线网络中的安全机制按等级分为六个层次，第一层不提供任何安全保障机制；第二层和第三层共享密钥认证；第三层同时应用 128 位的 WEP 加密；第四层到第六层都采用 EAP－TLS 认证，只是第五层和第六层分别应用 40 位和 128 位的 WEP 加密。

实验的网络结构是由 1 个 AP 和 3 个用户组成的单一区域，无越区切换。其中无线 STA 和 AP 之间传输速率为 11Mbps，AP 与服务器之间以 100M 以太网连接。该模型提供具有用户识别、集中认证和动态管理的可控的无线网络。试验内容是测试在不同安全机制下，以及拥塞情况下网络对 TCP 和 UDP 两种数据包类型的吞吐量和响应时间。

图 3 反映了网络拥塞[9]状态下（数据流量为 12Mbps），TCP 和 UDP 在不同安全层次的网络吞吐量。图 4 反映了网络拥塞状态下，TCP 和 UDP 两种传输类型的响应时间。

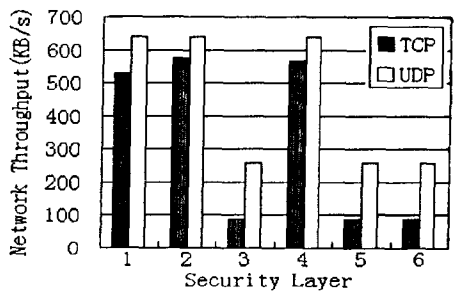

图 3 拥塞网络中 TCP 和 UDP 的吞吐量

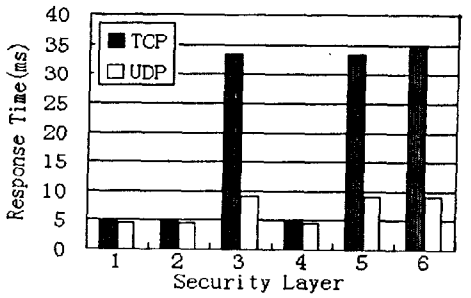

图 4 拥塞网络中 TCP 与 UDP 的响应时间

由图可知在拥塞网络中，安全层次 3、5、6 层因为采用了更高级别的加密机制[10]，使每个分组增加了额外的开销，明显降低了网络的性能，而认证机制对网络性能的影响则相对较弱。认证和加密机制的使用增加了数据包冗余，使网络性能下降。但影响网络性能的主要因素是复杂的加密机制，认证机制对网络性能的影响有限[11]。特别当网络拥塞时，使用认证机制对网络性能的影响比采用高级别加密机制要小的多。因此在无线网络中依靠可靠的认证机制，结合使用相应复杂度的加密机制，能够以更小的代价获得更高的网络性能收益。

3 结束语

EAP－TLS 认证也并非绝对的安全稳固，也存在有安全问题需要继续研究[12]，如认证初始阶段对用户身份的保护，TLS 交互过程中两端消息的规约也还存在安全隐患，需要继续升级完善。

无线局域网的安全接入或访问，涉及到多个层面安全协议和算法的综合配置与应用，目前各种技术论坛和相关厂商提出了多种认证技术，如 PEAP，LEAP，EAP－TTLS，EAP－PSK 及 EAP－AKA 等，虽然文中在分析比较后选择以 EAP－TLS 作为 WLAN 安全认证技术，但其他认证技术中也有值得参考和借鉴的方面，都可以继续研究。

参考文献：

[1] Aboba B, Simon D. PPP EAP TLS Authentication Protocol [S]. RFC 2716, 1999.

[2] 肖永生. Linux 网络服务器设置与管理[M]. 北京：海洋出版社，2006：109－116.

[3] Chen Jrh－Cheng, Wang Yuping. Extensible Authentication Protocol(EAP) and IEEE 802.1x: Tutorial and Empirical Experience[J]. IEEE Radio Communications, 2005(9): 26－32.

[4] Bakirdan A, Qaddour J, Jalozie I K. Security Algorithms in Wireless LAN: Proprietary or non－Proprietary[J]. IEEE GLOBECOM, 2003(11): 1425 － 1429.

[5] Apostolopoulos G, Peris V, Saha D. Transport layer security: how much does it really cost[C]// Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. [s.l.]: [s.n.], 1999(1): 717 － 725.

[6] 张仕斌. 网络安全技术[M]. 北京：清华大学出版社，2004.

[7] 马建峰，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.

[8] Whiting D, Housley R, Ferguson N. AES Encryption and Authentication Using CTR Mode & CBC－MAC[S]. IEEE 802.11 doc 02－001r1, 2002.

[9] 李新国. 基于拥塞控制的 AQM 算法研究[J]. 计算机技术与发展，2007，17(5)：199－202.

[10] 李雄伟，赵彦然. 无线局域网的安全性及其攻击方法研究[J]. 无线电通信技术，2005，31(1)：14－16.

[11] 吉建峰. 基于 802.1x 的无线局域网的接入认证研究与应用[D]. 南京：河海大学，2004.

[12] 徐 敏，罗汉文. 无线局域网安全问题研究[J]. 通信技术，2003(7)：65－66.