第26卷 第3期
2011年6月

郑州轻工业学院学报(自然科学版)
JOURNAL OF ZHENGZHOU UNIVERSITY OF LIGHT INDUSTRY(Natural Science)

Vol.26 No.3
Jun. 2011

文章编号:1004-1478(2011)03-0050-03

无线局域网中一种基于共享秘密的认证和密钥协商协议

王斌[1], 吕欣美[2]

(1.郑州轻工业学院 人事处, 河南 郑州 450002;
2.中州大学 就业指导中心, 河南 郑州 450044)

摘要:针对无线局域网中的便携式通信终端的计算资源、通信能力有限,难以执行大运算量的密码算法问题,提出了一种基于共享秘密的认证方式.该认证方式采用完整性校验码等安全技术为通信双方提供双向认证,由根秘密生成用于不同目的的多种密钥,并构成密钥体系.该认证方式能抵御重放攻击和中间人攻击,而且具有通信量小、计算量小、能提供密钥协商功能等优点,适合在资源受限的设备中用于保护移动通信中的信息安全.

关键词:无线局域网;EAP-SAKE;认证;密钥协商

中图分类号:TP393.08 **文献标志码**:A

Authentication and key negotiation protocol based on EAP-SAKE in WLAN

WANG Bin[1], LV Xin-mei[2]

(1. *Personnel Dept., Zhengzhou Univ. of Light Ind., Zhengzhou* 450002, *China*;
2. *Occupation-directing Center, Zhongzhou Univ., Zhengzhou* 450044, *China*)

Abstract: According to portable communication terminal has limited computation resource and communication ability. Which is difficult to implement key cryptography algorithm with large amount of calculation question. It is proposed an authentication method based on EAP-SAKE in order to solve the problem. It uses some security technologies to provide mutual authentication between peers, such as message integrity code, etc. This authentication method generates different keys for various purposes from root secret and constitutes key hierarchy. In addition, it can resist replay attack and man-in-middle attack. It has less communication load and computing amount and provides key negotiation. So it is more suitable for protecting the information security in mobile terminal which has limited resource in WLAN.

Key words: WLAN; EAP-SAKE; authentication; key negotiation

0 引言

无线局域网WLAN(wireless LAN)以其使用方便、安装快捷、经济廉价等优点受到了许多用户的欢迎.随着WLAN的逐步普及,访问它的通信终端也向着小型化、便携化的方向发展,由原来的台式计算机和笔记本计算机逐步向手机、PDA等个人便携设备过渡.在这些通信终端试图接入WLAN时,

收稿日期:2011-05-03

作者简介:王斌(1979—),男,河南省新乡市人,郑州轻工业学院讲师,硕士,主要研究方向为信息安全.

往往需要与接入服务器进行通信,验证双方的身份,并进行一些网络配置. 由于无线通信所采用的传输介质具有开放性的特点,而且便携式通信终端自身仅具有有限的带宽和计算资源,无法执行复杂的计算,使得采用便携式设备访问 WLAN 的安全形势比有线局域网更加严峻[1].

2006 年 3 月,ISO 批准了旨在提高 WLAN 安全性能的 802.11i 协议[2]作为 WLAN 安全的国际标准. 该标准采用了 IEEE 802.1x[3-4]定义的基于端口的访问控制模型、可扩展认证协议 EAP 实现认证、授权等安全功能.

EAP[5]是一个通用协议,可以由认证者自行决定使用何种认证方法,较常见的认证方法有 EAP-TLS 等[6-7]. 然而,EAP-TLS 等目前使用最多的认证方式大多用到了公钥密码算法,或者用到了基于公钥密码算法的数字证书等需要大量计算的安全技术,这些技术并不适合计算资源有限的便携式移动设备. 为解决这一问题,IETF 提出了一种新的 EAP 认证机制:EAP-SAKE[8]. 该机制能提供双向认证和密钥协商等功能,而且计算量较小. 本文根据便携式通信终端的特点,提出一种新的用于无线局域网中的基于 EAP-SAKE 的认证方式,以提高信息的安全性.

1　WLAN 中基于 EAP-SAKE 的认证和密钥协商

1.1　双向认证过程

在 WLAN 客户端与认证服务器进行报文交换前,即初始化阶段,通信双方被分配共享 1 个根秘密值(Root-Secret),并将其分成 2 个相互独立的长度均为 16 B 的根秘密信息,其中 Root-Secret-A 主要用于进行认证和生成临时 EAP 密钥 TEK(transient EAP keys),Root-Secret-B 主要用来计算主会话密钥 MSK(master session key)和扩展主会话密钥 EMSK(extended master session key).

该双向认证过程包括 4 个阶段,如图 1 所示.

第 1 阶段:WLAN 服务器发现有新的客户端想要访问网络资源后,发送 EAP. Request/SAKE/Challenge 报文给客户端,其中包括服务器生成的随机数 AT_RAND_S 和服务器的身份标识 AT_SERVERID.

第 2 阶段:WLAN 客户端收到服务器发送的报文后发送 EAP. Response/SAKE/Challenge 报文作为

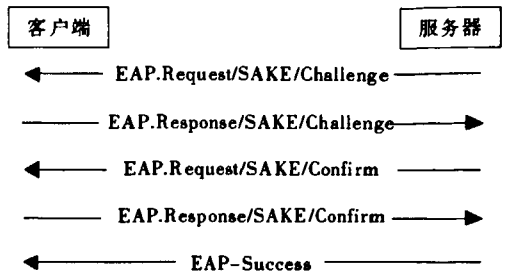

图 1　EAP-SAKE 的报文交换机制

响应,其中主要包括客户端生成的随机数 AT_RAND_P,客户端身份标识符 AT_PEERID,支持的密文族 AT_SPI_P,访问时长 Lifetime_P 和完整性校验码 AT_MIC_P,其中访问时长是该客户端向服务器申请的提供服务的时间长度值,可以设定为 2 h,4 h 等. 达到访问时长后,客户端需要重新与服务器进行认证. AT_MIC_P 的计算方法为

MIC_P = KDF-16 (TEK-Auth, "Peer MIC", RAND_S| RAND_P| Lifetime_P| PEERID| 0x00| SERVERID | 0x00 | <EAP-packet>)

其中,KDF-16 为一输出为 16 B 的钥控 Hash 函数,<EAP-packet>代表该 EAP 报文.

第 3 阶段:服务器收到客户端发送的 EAP. Response/SAKE/Challenge 报文后,采用相同的方法计算出 MIC_P,并与收到的 MIC_P 进行比较,如果两者相等,则通过对客户端的身份认证. 然后服务器发送 EAP. Response/SAKE/Confirm 报文,其中包括从客户端支持的密文族中选择适当的参数 AT_SPI_S,服务器批准的访问时长 Lifetime_S,加密后的信息 AT_ENCR_DATA 和完整性校验码 AT_MIC_S. AT_MIC_S 的计算方法为

MIC_S = KDF-16 (TEK-Auth, "Server MIC", RAND_P| RAND_S| Lifetime_S| SERVERID |0x00 | PEERID| 0x00 | <EAP-packet>)

服务器通过对客户端的认证后,开始计时,达到批准的访问时长后就停止为该客户端提供服务.

第 4 阶段:客户端收到服务器发送的 EAP. Response/SAKE/Confirm 报文后认为服务器已经通过了对它的认证,采用同样的计算方式来计算完整性校验值,并将计算结果与收到的 AT_MIC_S 进行比较,若相等,则通过对服务器的身份认证,并发送 EAP. Response/SAKE /Confirm 报文给服务器,其中包括完整性校验码 AT_MIC_P. 此时,客户端开始计时,达到服务器批准的访问时长后重新向服务器发

起认证.

最后,服务器收到 EAP. Response/SAKE/Confirm 报文后,发送 EAP-Success 报文给客户端,结束 EAP 会话.

1.2 密钥协商过程

在 EAP-SAKE 中,用到了多个密钥,这些密钥的体系结构[9]如图 2 所示.

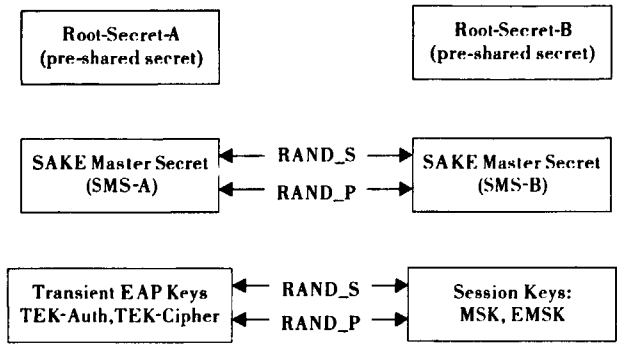

图 2 EAP-SAKE 密钥体系结构图

根秘密 A 主要用于生成 SAKE 主秘密 A 以及用于认证的密钥 TEK-Auth 和用于加密的密钥 TEK-Cipher;根秘密 B 主要用于生成 SAKE 主秘密 B 以及供底层使用的 MSK 和 EMSK.

在认证过程的第 2 阶段和第 3 阶段,客户端和服务器分别计算出 SAKE 和 TEK,计算方法为

SMS-A = KDF-16 (Root-Secret-A, "SAKE Master Secret A", RAND_P|RAND_S)

TEK = KDF-32 (SMS-A, "Transient EAP Key", RAND_S | RAND_P)

其中,TEK-Auth 和 TEK-Cipher 分别是 TEK 的前 16 B 和后 16 B.

在协议运行过程中,还需要计算出 SMS-B 和 MSK,EMSK,其计算方法为:

SMS-B = KDF-16 (Root-Secret-B, "SAKE Master Secret B", RAND_P|RAND_S)

Session-Key-Block = KDF-128 (SMS-B, "Master Session Key", RAND_S|RAND_P)

其中,MSK 和 EMSK 分别为 Session-Key-Block 的前 64 B 和后 64 B.

2 性能及安全性分析

2.1 性能分析

在 WLAN 的基于 EAP-SAKE 的认证方式中,客户端与服务器之间不需要进行同步,两者之间的同步在设备初始化阶段已经完成. 通信双方通过4 步通信就可以实现相互认证和密钥协商等功能,降低了认证过程中对通信能力的要求. 此外,由于该认证方式中只使用了对称密码算法和单向散列函数,没有用到非对称密码算法,降低了对客户端的计算能力的要求. 因此,该认证方式具有通信量小、对客户端计算能力要求低等优点.

2.2 安全性分析

1)双向认证. 在 EAP-SAKE 中,接入服务器通过检查客户端发送来的 MIC_P 和自己计算的 MIC_P 是否一致来对客户端进行身份认证,决定是否为该客户端提供服务. 类似地,在第 4 步中,客户端通过检查服务器发送来的 MIC_S 是否正确,来对服务器进行身份认证. 因此,EAP-SAKE 提供了客户端和服务器的双向认证.

2)密钥协商. 在 EAP-SAKE 中,初始状态下客户端与服务器共享相同的根秘密,由该秘密值生成多个密钥 TEK,MSK 和 EMSK 等. 这些密钥的生成方法不同,用途也不同,每个密钥只用于特定的用途. 这样能够有效避免因密钥使用次数过多而暴露密钥的相关信息.

3)抵御重放攻击. 在客户端与服务器进行双向认证时,通信双方分别检查收到的 MIC_S 和 MIC_P 是否正确,来决定是否通过对对方的认证. 在 MIC_S 和 MIC_P 的计算过程中,均包含由客户端和服务器生成的随机数 RAND_P 和 RAND_S. 每轮认证所生成的随机数都不同,进而导致由此产生的 MIC_S 和 MIC_P 也不相同. 因此,即使攻击者窃听了客户端与服务器之间的通信,也无法采用简单的重放攻击通过认证.

4)抵御中间人攻击. 在双向认证过程中,主要用到了钥控 Hash 函数. 由于 Hash 函数具有单向性,即使攻击者获取了通信双方的通信,也无法从获取的消息中计算出密钥. 因此,该协议能抵御中间人攻击.

2.3 与 EAP-TLS 的对比分析

EAP-TLS 是一种常用的认证方式,在表 1 中,将该认证方式与 EAP-SAKE 进行了对比. 从表中可以看出,EAP-SAKE 与目前常用的 EAP-TLS 相比,两者均能提供双向认证、密钥协商功能,并能抵御重放攻击和中间人攻击. 两者的主要区别在于执行的

(下转第 62 页)

较改进的带宽优先算法相差0.714倍.由实验参数可知,覆盖网半径越小,延迟越短.因此改进后的算法延迟性较好.

2)流服务质量分析.由表1可知,流服务质量是相同的,都是74%,由此看出,改进后的算法并没有因为节点排序方法改变或者模型构造方法改变而影响系统的流服务质量.

3)覆盖网压力性能分析.评价模型的拓扑树平衡性的好坏,主要通过P2P覆盖网压力性能进行分析.从表1中覆盖网压力的大小可知,通过最优平衡树的构造方法后,模型结构趋于更加合理,覆盖网压力明显减小,为67%,较原来减少8%.

5 结语

本文以一个开源的P2P流媒体系统PeerCast为研究对象,通过分析基于PeerCast模型的Overcast系统节点选择算法的工作原理,针对延迟性和构造树的平衡问题,对传统的带宽优先选择策略中查找最优带宽节点算法进行改进,并对其节点树予以平衡.仿真实验结果表明,改进后的算法可较好地优化系统性能.

参考文献:

[1] 郑春浩,颜金尧.基于PeerCast的P2P流媒体系统[J].中国传媒大学学报,2009,16(9):51.

[2] Deshpande H,Bawa M,Garcia Molina H. Streaming live media over peers[R]. Wikipedia: Stanford University, 2002:4-18.

[3] 葛宇,梁静.改进的高度优先策略在P2P流媒体节点选择机制中的研究[J].计算机系统应用,2009(11):45.

[4] 郑婕,张松,齐洁,等.P2P流媒体节点选择机制的研究与仿真[J].计算机工程与设计,2007,28(22):5398.

[5] 杨雪.PeerCast节点选择机制的分析及改进[J].计算机工程,2009,35(3):60.

(上接第52页)

效率上:EAP-TLS中用到了基于公钥密码算法(如RSA算法)的数字证书,验证数字证书中的签名需要执行公钥密码算法,计算量较大;而EAP-SAKE中只用到了带有密钥的Hash函数.显然,公钥密码算法的计算量要比Hash函数大很多,因此EAP-SAKE更适合用于计算资源有限的小型便携式通信设备.

表1 EAP-TLS与EAP-SAKE对比

认证方式	双向认证	密钥协商	抵御重放攻击	抵御中间人攻击	是否用到公钥密码算法	计算复杂度
EAP-TLS	可以	可以	可以	可以	是	大
EAP-SAKE	可以	可以	可以	可以	否	小

3 结语

随着访问WLAN的通信设备向着便携化、小型化的方向发展,原来使用的认证方式由于需要较多的计算资源和较高的通信能力而不适应这种发展趋势.本文提出了一种基于EAP-SAKE的WLAN认证方式,具有通信量小、计算量小、能提供双向认证和密钥协商功能、可抵御重放攻击和中间人攻击等优点,适合在资源受限的设备中用于保护移动通信的信息安全.

参考文献:

[1] 汪晓华.WLAN安全风险分析及解决方案[J].陕西师范大学学报:自然科学版,2007,35(11):157.

[2] 802.11i, Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications[S].

[3] 余泰勇.802.1x协议分析及其应用[J].信息安全与通信保密,2005(1):85.

[4] 王丽霞.基于802.1x/EAP的WLAN安全认证分析与应用研究[J].气象科技,2010(3):347.

[5] RFC3748, Extensible Authentication Protocol (EAP)[S].

[6] 曹利,杨凌凤,顾翔,等.基于802.11i的EAP-TLS认证机制的安全分析[J].计算机工程与设计,2010,31(4):756.

[7] RFC 5216,The EAP-TLS Authentication Protocol[S].

[8] RFC4763, Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)[S].

[9] RFC5247, Extensible Authentication Protocol (EAP) Key Management Framework[S].