基于对称密钥加密的RSN密钥协商改进方法

吴一尘[1],鲍苏苏[2]
(1. 中国人民解放军电子工程学院 网络系,安徽 合肥 230037;
2. 华南师范大学 计算机学院,广东 广州 510631)

摘 要:通过对IEEE802.11i无线局域网安全标准中动态密钥协商机制的详细分析,发现四次握手过程存在缺陷并且有可能遭受伪造消息的拒绝服务(DoS)攻击。针对这一安全漏洞,提出一种基于对称密钥加密技术的四次握手过程改进方法。这一改进方法改变了IEEE802.11i四次握手过程中明文传送密钥材料的策略,使用AES加密算法对密钥材料进行加密,从而避免了攻击者通过伪造消息进行DoS攻击。为了验证这一改进方法的有效性,利用Python和pyCrypto组件对其进行了模拟与分析,从模拟结果可以看出,这一改进方法能够很好地避免DoS攻击,同时不会引起申请者的内存耗尽和CPU性能下降,进一步增强了WLAN的安全性。

关键词:无线局域网;IEEE802.11i;密钥协商;四次握手;拒绝服务;对称密钥
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)06-0132-04
doi:10.3969/j.issn.1673-629X.2013.06.034

An Improved Method of RSN Key Negotiation Based on Pairwise Key Encryption Technology

WU Yi-chen[1], BAO Su-su[2]
(1. Network Department, Electronic Engineering Institute of PLA, Hefei 230037, China;
2. School of Computer, South China Normal University, Guangzhou 510631, China)

Abstract: Through the analysis of IEEE802.11i key negotiation mechanisms, it is found that there exists security vulnerability in 4-way handshake, which will lead to a DoS attack. Aiming at this security flaw, an improved method based on pairwise key encryption technology is developed. This improved method encrypts keying material using AES encryption algorithm, which changes the transfer key material strategy in 4-way handshake process, so as to avoid DoS attack. This improved method is simulated by using Python and the pyCrypto module. From the simulation results it can be seen that the improved method can well avoid DoS attack, at the same time will not cause the applicant's run out of memory and CPU performance decline, further enhance the security of WLAN.

Key words: WLAN; IEEE802.11i; key negotiation; 4-way handshake; DoS; pairwise key

0 引 言

随着无线网络应用的蓬勃发展,无线局域网(WLAN)的安全问题越来越受到人们的关注。2004年发布的WLAN安全标准IEEE802.11i[1]定义了强健安全网络RSN(Robust Security Network)的概念,增强了WLAN的认证和数据加密性能,被认为是WLAN安全问题的最终解决方案。然而,很多研究[2-7]表明,IEEE802.11i标准中用于实现申请者与认证者之间动态密钥协商的四次握手过程存在安全缺陷,攻击者可以通过伪造消息实现拒绝服务(DoS)攻击,对WLAN的安全性造成威胁。针对这一安全漏洞,目前已经提出多种改进方法[8,9],但这些改进方法在避免DoS攻击的同时,给WLAN带来了新的安全威胁。IEEE802.11i小组针对这一安全漏洞提出了基于TPTK(Temporary Pairwise Transient Key)技术的改进方案,该方案可以避免伪造消息的DoS攻击,但容易导致申请者的内存耗尽。文献[8]提出了基于重用Nonce(随机值)技术的改进方法,该方法能够避免申请者的内存耗尽,但申请者有可能因为大量的计算导致CPU耗尽。文献[9]提出了基于身份认证技术的改进方法,该方法

收稿日期:2012-09-07 **修回日期**:2012-12-13 **网络出版时间**:2013-03-05
基金项目:国家"863"高技术发展计划项目(2012AA021105)
作者简介:吴一尘(1984-),女,安徽合肥人,助教,硕士,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130305.0815.011.html

能够避免申请者的内存和CPU被耗尽,但攻击者可以通过暴力破解的方式获取申请者与认证者此次会话的密钥,对WLAN的安全性造成致命的影响。文中分析了四次握手过程的安全漏洞以及上述三种改进方法的优缺点,在此基础之上,提出了一种基于对称密钥加密技术的改进方法。这一改进方法改变了IEEE802.11i四次握手过程中明文传送密钥材料的策略,使用AES加密算法对密钥材料进行加密,从而避免了攻击者通过伪造消息进行DoS攻击。为了验证这一改进方法的有效性,利用Python和pyCrypto组件对其进行了模拟与分析,从模拟结果可以看出,这一改进方法能够很好地避免DoS攻击,同时不会引起申请者的内存耗尽和CPU性能下降,从而使WLAN的安全性得到进一步增强。

1 IEEE802.1X

IEEE802.11i标准中规定使用IEEE802.1X认证和密钥管理机制。IEEE802.1X是一种基于端口的认证协议,包括3个实体:申请者,认证者和认证服务器。对于WLAN来说,申请者请求接入无线网络,通常为支持802.1X的工作站。认证者指的是需要进行访问控制的端口,一般为无线接入点,认证者只负责链路层的认证交换过程,并不维护任何用户信息,任何认证请求均会被转送至认证服务器进行实际的处理。认证服务器实现具体的认证功能,并通知认证者是否允许用户访问端口所提供的服务,通常是一个RADIUS(Remote Authentication Dial-In User Service)服务器,用户身份信息存储在该服务器上。认证通过后,申请者和认证服务器生成一个共同的主会话密钥(Master Session Key,MSK)。认证服务器将MSK安全地传输给认证者。申请者和认证者利用MSK生成成对主密钥(Pairwise Master Key,PMK)。如果WLAN中没有配置认证服务器,申请者和认证者可以使用预共享密钥(Pre-Shared Key,PSK)代替PMK。

2 四次握手过程的分析及可能存在的攻击

当申请者和认证者生成相同并且最新的PMK之后,双方发起四次握手过程[10]。申请者和认证者之间的消息均由EAPOL-Key帧格式封装。STA和AP分别代表申请者和认证者,SNonce和ANonce分别为申请者和认证者所产生的随机数,MIC(Message Integrity Code)是消息完整性校验值,RSN IE(Robust Security Network Information Element)为健壮安全网络信息元素。

(1)消息1:AP生成并向STA发送ANonce。

(2)消息2:STA收到ANonce之后,生成SNonce,计算PTK。

PTK包含3个部分,分别是:EAPOL密钥确认密钥(EAPOL Key Confirmation Key,KCK),EAPOL密钥加密密钥(EAPOL Key Encryption Key,KEK),临时密钥(Temporal Key,TK)。其中,KCK用于计算EAPOL-Key帧的校验和,KEK用来加密EAPOL-Key帧的数据,TK用以加解密STA与AP之间的单播数据。在计算得到PTK之后,STA向AP发送SNonce、STA的RSN IE,整个消息2使用KCK进行MIC校验。

(3)消息3:AP收到SNonce之后,利用同样的方法计算得到PTK,并用KCK对消息2进行MIC校验,如果校验失败则丢弃消息2,成功则向STA发送ANonce,AP的RSN IE,MIC,是否安装PTK以及使用KEK加密的组临时密钥(Group Temporal Key,GTK)。

(4)消息4:STA收到消息3并校验正确后即装入PTK,然后向AP发送消息4,表示已经装入PTK和GTK。AP收到消息4并校验正确后也装入PTK。至此,四次握手过程完成。

经过对四次握手过程的分析发现,攻击者可以在消息2发送后冒充AP向STA发送伪造的消息1。STA将根据新的消息1中的随机值ANonce'和本身产生的新的随机值SNonce'重新计算PTK',而PTK'与AP收到消息2后产生的PTK显然是不一致的,这样STA收到消息3后无法正确校验,就会导致四次握手过程被终止,造成DoS攻击。

3 一种四次握手过程的改进方法

通过以上分析可以看出:DoS攻击源于STA无法判断接收到的消息1是否来自于合法AP,因此STA必须为每一个接收到的消息1运行一个四次握手实例。如果能够表明消息1的来源,STA收到攻击者伪造的消息1后,通过验证发现该消息1不是由合法AP发送的,将直接丢弃该消息1,就可以避免DoS攻击。根据这一点,文中提出一种基于对称密钥加密技术的四次握手改进方法。

在消息1的传递过程中,PTK还没有被计算出来,AP和STA共享的密钥只有PMK,根据公式(1)将PMK展开成IPEK(Initial Pairwise Encryption Key),作为专门供消息1使用的对称密钥,其中,AA和SPA分别代表AP和STA的MAC地址,"||"表示连接操作。

$$IPEK = PRF-X(PMK, "Initial\ Pairwise\ Encryption\ Key", Min(AA,SPA)||Max(AA,SPA)) \quad (1)$$

在这种改进的四次握手过程中,AP与STA之间的消息传递如图1所示。

(1)消息1:AP生成随机值ANonce,计算IPEK并向STA发送用IPEK加密的ANonce,加密采用AES(Ad-

vanced Encryption Standard)算法[11,12]。

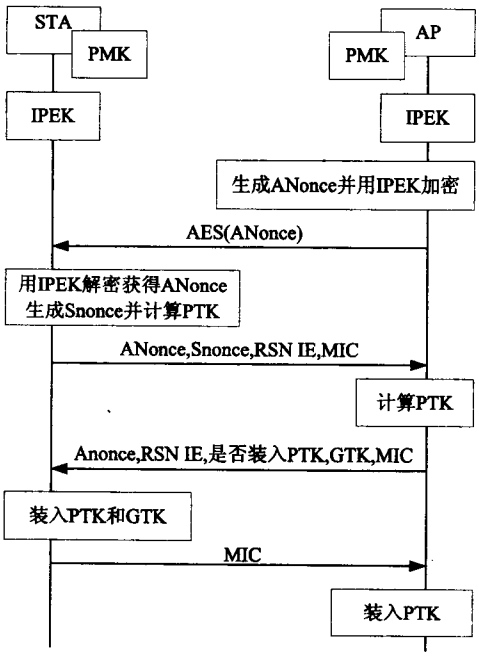

图 1 改进的四次握手过程

(2)消息 2:STA 计算 IPEK,对收到的消息 1 解密获得 ANonce,STA 生成随机值 SNonce 并计算 PTK,然后向 AP 发送 ANonce,SNonce,STA 的 RSN IE 以及用 KCK 计算得到的 MIC 值。

(3)消息 3:AP 收到 SNonce 之后,利用同样的方法计算得到 PTK,并用 KCK 对消息 2 进行 MIC 校验,如果校验失败则丢弃消息 2,成功则向 STA 发送 ANonce,AP 的 RSN IE,MIC,是否安装 PTK 以及使用 KEK 加密的 GTK。

(4)消息 4:STA 收到消息 3 并校验正确后即装入 PTK 和 GTK,然后向 AP 发送消息 4,表示已经装入 PTK 和 GTK。AP 收到消息 4 并校验正确后也装入 PTK。至此,四次握手过程完成。

由于攻击者不知道 IPEK,无法正确对伪造的 ANonce 加密。STA 收到伪造的消息 1,解密后必然会有某些不可读的符号和字符,STA 将丢弃该消息 1,从而避免了伪造消息的 DoS 攻击。

在 IEEE802.11i 四次握手过程中,AP 和 STA 之间的消息都是通过 EAPOL-Key 帧格式封装的。为了尽可能减少对协议的修改,应该保证改进的四次握手过程中所产生的新的数据传递能够封装在 EAPOL-Key 帧中,同时不会打乱已有数据在该帧格式中存放的位置。EAPOL-Key 帧格式如图 2 所示。

在文中所提出的改进方法中,消息 2、3、4 的数据传递与 IEEE802.11i 四次握手过程一致,没有发生改变,只是将 IEEE802.11i 四次握手过程消息 1 中明文传送的随机值 ANonce 通过 AES 加密算法加密传送。在 IEEE802.11i 四次握手过程消息 1 传递过程中,EAPOL-Key 帧中的 Key Data Length 字段和 Key Data 字段没有被使用,因此,在改进方法中,可以将加密后的 ANonce 存放在 Key Data 字段中,而密文的长度可以存放在 Key Data Length 字段中。由此可见,文中所提出的四次握手过程改进方法不需要修改 EAPOL-Key 帧的帧格式,另外也不会打乱帧中已经存放的数据的位置。

Descriptor Type - 1 octet	
Key Information - 2 octets	Key Length - 2 octets
Key Replay Counter - 8 octets	
Key Nonce - 32 octets	
EAPOL-Key IV - 16 octets	
Key RSC - 8 octets	
Reserved - 8 octets	
Key MIC - 16 octets	
Key Data Length - 2 octets	Key Data - n octets

图 2 EAPOL-Key 帧格式

4 改进方法的模拟与分析

利用 Python 和 pyCrypto 组件对四次握手过程中 STA、AP 和攻击者之间的消息 1 交换进行了模拟。为了与 IEEE802.11i 四次握手过程进行对比,进行了 2 组模拟。第一组模拟了 IEEE802.11i 四次握手过程,第二组模拟了文中提出的改进四次握手过程。在第一组对 IEEE802.11i 四次握手过程的模拟中,所有发送的消息 1 中的 ANonce 都是明文传送的。在第二组对改进四次握手过程的模拟中,STA 和 AP 使用相同的 PMK,攻击者分成两种情况,一种是使用与 PMK 不同的密钥,另一种是不使用密钥。在两组模拟中,为了模拟典型的网络环境,攻击者分别以 0.2s、0.02s 和 0.002s 的延迟时间向 STA 发送 50 个消息 1 数据包,AP 则随机发送 5 个消息 1 数据包。两组模拟的结果如表 1 和表 2 所示。

从表 1 和表 2 可以看出:在 IEEE802.11i 四次握手过程中,随着攻击者每秒发送的伪造消息 1 的增多,STA 的内存耗尽时间迅速下降,而在整个模拟过程中,改进四次握手过程中 STA 的内存都没有被耗尽。

在改进四次握手过程中,消息 1 需要经过加密,为了测试这一加密过程对消息 1 数据包传送时间的影

响,进行了第3组模拟。在这组模拟中,分别向STA连续发送50个未加密和经过加密的消息1数据包,通过3次独立测试,计算发送50个消息1数据包所需的平均时间。模拟结果如表3所示。

表1　对IEEE802.11i四次握手过程的DoS攻击

延迟时间(s)	内存耗尽的平均时间(s)
0.2	1.825
0.02	0.310
0.002	0.160

表2　对改进四次握手过程的DoS攻击

延迟时间(s)	内存耗尽的平均时间(s)
0.2	-
0.02	-
0.002	-

表3　加密ANonce对消息1传送时间的影响

测试	1	2	3	平均时间(s)
未加密ANonce	0.031	0.031	0.031	0.031
加密ANonce	0.031	0.047	0.047	0.042

发送一个消息1数据包所需的平均时间t可以通过t=平均时间/50来计算。从表3可以看出,发送一个未加密ANonce的消息1数据包平均需要0.00062秒,发送一个加密ANonce的消息1数据包平均需要0.00084秒,因此,发送一个加密ANonce的消息1数据包平均多花费0.00022秒,这个时间增加非常小,几乎可以忽略不计。

通过以上3组模拟可以看出,改进的四次握手过程可以很好地避免DoS攻击,同时不会对内存消耗和CPU性能产生影响,弥补了基于TPTK技术和基于重用Nonce技术两种改进方法的缺陷。另外,在改进四次握手过程中,对消息1加解密没有直接使用PMK,而是通过PRF伪随机函数将PMK展开成IPEK之后再作为对称密钥使用的。这一处理保证了PMK的保密性,弥补了基于消息1身份认证技术的改进方法的缺陷。

5　结束语

文中对IEEE802.11i四次握手过程及其安全性进行了详细地分析,发现四次握手过程的设计缺陷使它容易遭受伪造消息的DoS攻击。针对这一安全隐患,文中提出了一种基于对称密钥加密技术的改进方法。改进后的四次握手过程很好地避免了DoS攻击,使WLAN的安全性得到进一步增强。

参考文献:

[1] IEEE Std 802.11i™ Amendment 6: Medium Access Control (MAC) Security Enhancements[S]. 2004.

[2] He Changhua, Mitchell J C. 1 Message Attack on the 4-Way Handshake[EB/OL]. 2004. http://theory.stanford.edu/~changhua/11-04-0497-02-000i-1-message-attack-on-4-way-handshake.doc.

[3] He Changhua, Mitchell J C. Security Analysis and Improvements for IEEE 802.11i[EB/OL]. 2004. http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf.

[4] 刘　可,徐昌彪,杨士中. 无线局域网中的认证机制[J]. 计算机技术与发展,2008,18(1):164-167.

[5] 陈占计,陈　芳,陈中双,等. 基于IEEE802.11i标准的WLAN安全性分析[J]. 中国数据通信,2005(5):77-80.

[6] 李　波,雷维礼. IEEE 802.11i标准与WLAN的安全性[J]. 通信与信息技术,2004(8):27-31.

[7] 王　磊,梁华庆. 浅谈无线局域网安全技术的发展[J]. 微型机与应用,2011,30(6):1-2.

[8] 梁　峰,史杏荣,曲阜平. IEEE802.11i中四次握手过程的安全分析和改进[J]. 计算机工程,2007,33(3):149-150.

[9] 王小军,陆建德. 基于802.11i四次握手协议的攻击分析与改进[J]. 计算机工程,2007,33(3):169-171.

[10] Gast M S. 802.11无线网络权威指南[M]. 南京:东南大学出版社,2007.

[11] 柯海清,冯启明. 数据加密技术及网络应用[J]. 武汉理工大学学报(交通科学与工程版),2002,26(6):818-821.

[12] 肖国镇,白恩健,刘晓娟. AES密码分析的若干新进展[J]. 电子学报,2003(10):1549-1554.

(上接第131页)

理工学院学报(自然科学版),2005,18(1):57-59.

[6] 陈圩贤,廖洪銮,冯登国. 一种基于SSL/TLS的Web安全代理的设计与实现[J]. 计算机工程,2004,30(11):40-42.

[7] 周敬利,曾海鹏. SSL VPN服务器关键技术研究[J]. 计算机工程与科学,2005,27(6):7-9.

[8] Andrew H. SSL Virtual Private Networks[J]. Computers and Security,2003,22(5):416-420.

[9] Araujo K. SSL VPN gateways: A new approach to secure remote access[J]. Database and Network Journal,2003,33(6):3-5.

[10] Khanvilkar S, Khokhar A. Virtual private networks: an overview with performance evaluation[J]. IEEE Communications Magazine,2004,42(10):146-154.

[11] Corrfa C, Druschel P, Wallach D S. Performance Analysis of TLS Web Servers[J]. ACM Transactions on Computer Systems,2006,24(1):39-69.

基于对称密钥加密的RSN密钥协商改进方法

作者： 吴一尘， 鲍苏苏， WU Yi-chen， BAO Su-su
作者单位： 吴一尘,WU Yi-chen(中国人民解放军电子工程学院网络系,安徽合肥,230037)， 鲍苏苏,BAO Su-su(华南师范大学计算机学院,广东广州,510631)
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013,23(6)