SIP 安全认证机制研究*)

韦振名　冯久超
(华南理工大学电子与信息学院　广州 510641)

摘　要　会话发起协议(SIP)简单灵活,便于业务扩展,是使用最广泛的信令协议之一。但是它缺乏有效的安全认证机制,容易受到攻击。分析了 SIP 可能受到的攻击,对已有安全认证机制进行比较,并提出一种基于公钥的安全认证机制,增强了 SIP 域内和端到端的安全性。

关键词　会话发起协议,安全认证机制,HTTP 认证,公钥,端到端

Study on Security Authentication Mechanism for SIP

WEI Zhen-ming　FENG Jiu-chao
(School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract　SIP is one of the most widely used signaling protocols for its simplicity and scalability. However, it lacks of an effective mechanism for security authentication, which makes it vulnerable to attacks. The potential attacks to SIP were analyzed. Some existing security authentication mechanisms were compared. Then, a new security authentication mechanism based on public key was proposed to enhance the local and end-to-end security of SIP.

Keywords　SIP, Security mechanism, HTTP authentication, Public key, End-to-end

1　引言

SIP 是互联网工程任务组(IETF)提出的一种呼叫控制信令协议。它具有简单、灵活和扩展性好等优点,已得到了广泛的运用并逐渐成为网络电话(VoIP)的主流协议,还将成为下一代网络(NGN)的核心信令协议。

SIP 的消息是以文本方式发送,这便于分析和处理。面对复杂开放的互联网环境,协议本身缺乏有效的安全认证机制,面临着多种攻击的威胁。目前已提出多种安全认证机制,如 IPsec、传输层安全(TLS)协议、安全多用途网际邮件扩充协议(S/MIME)、超文本传输协议(HTTP)摘要认证、防火墙方案、智能卡认证方案等,但每种机制都存在一定的局限性。本文首先分析 SIP 所面临的攻击威胁和协议中存在的安全薄弱环节,然后对比现有安全机制的优点和局限,并结合 SIP 会话的特点,对传统 HTTP 摘要认证机制进行扩展,提出一种基于公钥的安全认证方案,包括代理服务器对本区域内用户的认证以及被叫方对主叫方的端到端认证,从而以较小的代价增强了 SIP 的安全性。

2　SIP 安全性分析

SIP 协议采用了和 HTTP 协议类似的 request/response 模式,其主要网络逻辑元素包括用户代理(User Agent)、代理服务 Proxy、注册服务器 Registrar 和重定向服务 Redirect Server[1]。用户直接发送请求或通过服务器转发请求,服务器或被叫用户对请求进行响应,从而完成注册、会话邀请、重定向、结束会话等事务。在操作这些事务的过程中,攻击者可能截获 SIP 消息,读取其中信息并针对会话中各环节的漏洞进行攻击。

2.1　SIP 事务

SIP 协议定义了 6 种请求[1]:REGISTER, INVITE, ACK, CANCEL, OPTIONS 和 BYE。响应是以状态码方式表示,该码的第一位数字用于指示响应的类型,后两位用于表示具体的响应,如 1XX 表示临时响应、2XX 表示成功处理,依此类推到 6XX 响应。由不同的请求和响应构成了不同的 SIP 事务、实现认证、会话邀请、确认、修改会话参数、结束会话等功能。

2.2　SIP 面临的攻击

SIP 协议缺乏有效的安全认证机制,容易受到以下几种类型的攻击[2-4]。

(1)注册攻击:攻击者截取用户的注册请求,得到其中的 To, Call-ID, CSeq 等关键字段信息,从而伪造用户的 Register 请求,重新进行注册,在服务器上把用户的注册项和攻击者自己的联系地址进行绑定,从而截获从服务器发向用户的所有呼叫。SIP 协议允许第三方代为注册,更容易被攻击者利用而进行恶意注册。

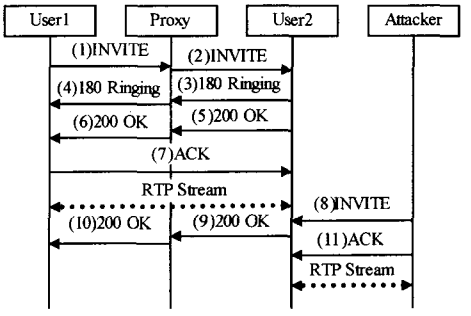

图 1　消息篡改攻击示意图

*)国家自然科学基金(60572025),教育部"新世纪优秀人才支持计划"基金(NCET-04-0813),广东省自然科学基金资助(07006496)。**韦振名**　硕士研究生,主要从事网络信息安全的研究;**冯久超**　博士,教授,博士生导师,研究领域涉及数字信号处理、数字通信、非线性动力学及混沌理论与应用。

(2)消息篡改:用户 A 向用户 B 发送 INVITE 请求,经过一系列步骤后成功发起会话。攻击者截获会话的关键信息后,向用户 B 发送伪造的 re-INVITE 请求,要求改变会话参数,使用户 B 将数据流发往攻击者指定的地址。图 1 表示了这一过程。

(3)拆卸会话攻击:在用户 A 和用户 B 会话过程中,攻击者在截获会话关键信息后伪造用户 A 的 BYE 请求并发向用户 B,从而结束 A 与 B 的会话。图 2 表示了这一过程。

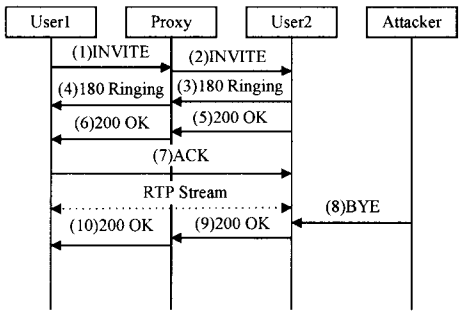

图 2 拆卸会话攻击示意图

可见,SIP 容易受到安全威胁主要是由于其消息以明文发送,容易被截获加以利用,并且缺乏有效的安全认证机制。而 SIP 协议中的头字段需要被中继服务器读取以进行转发,不宜进行加密,因此有必要研究有效的安全认证机制来对抗攻击。

3 SIP 安全认证机制

现有的可用于 SIP 的安全认证机制中的 IPsec 实施过程复杂,扩展性差,实现代价较高;TLS 工作于 TCP 之上,不能在 UDP 上实现;S/MIME 加密安全性高,但需要有集中的证书分发机构[3,4];防火墙和智能卡认证等方案可靠性很高,但使用领域有限。HTTP 摘要认证实现相对简单,而且可扩展性较强。本文在 HTTP 摘要认证的基础上,提出一种基于公钥的安全认证机制。和已有机制相比,它的实现代价较小,而且增强了 SIP 域内和端到端的安全性。

3.1 HTTP 摘要认证机制

SIP 借鉴 HTTP 协议中的摘要认证机制,在 SIP 消息中定义了 Proxy-Authenticate, Proxy-Authorization, Authorization 等字段,用于实现域内的身份鉴定[5]。典型的 HTTP 摘要认证过程如图 3 所示[6,7]。

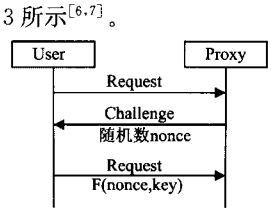

图 3 典型的 HTTP 摘要认证过程

在已有的 HTTP 摘要认证机制的基础上,我们针对 SIP 会话的特点对该机制进行扩展,提出一种基于公钥算法的认证机制,不仅使用传统的发起 challenge 的方式实现了服务器对域内用户的认证,还结合 SIP 自身特点实现了用户和用户之间的端到端认证。

3.2 公钥算法

公钥算法是非对称的加密算法,包含成对的公钥和私钥。如果用公钥对数据进行加密,只有用对应的私钥才能解密;如果用私钥对数据进行加密,只有用对应的公钥才能解密。自从 D2H 公钥算法出现以后,目前已相继提出多种公钥算法,较为著名的有 ECC 和 RSA,其中 RSA 算法应用最为广泛。RSA 密钥的产生方法[8]是:产生两个素数 P 和 Q,计算 $N=P\times Q$,$\varphi(N)=(P-1)(Q-1)$,再产生一随机整数 E,使该数满足 $gcd(E,\varphi(N))=1$,然后计算 $D=(E-1) \bmod \varphi(N)$,将 E,N 作为公钥;D,P,Q 作为私钥。设 M 是明文,C 是密文,则加密时 $C=M^{E \bmod N}$,解密时 $M=C^{D \bmod N}$。RSA 算法的主要问题在于模幂运算和质数的产生使得它比较复杂。目前已有 Montgomery 算法、Yacobi 算法等模幂算法和 Rabin Miller 等素数产生方法,提高了 RSA 算法的效率。

3.3 域内认证机制

由前面的分析可知,注册攻击主要利用了 SIP 对前来注册的用户缺少有效身份认证,以及对第三方认证缺乏有效授权机制的漏洞。为此,应该有针对性地对注册进行更严格的管理。在原用户已经正常注册的基础上,攻击者为了成功进行注册注销和重新注册,必须获取其注册信息的 to,Call_ID,CSeq 等字段。因此,为了阻止攻击者进行注册注销,用户可以在首次向服务器注册的时候提供自己的公钥,服务器得到公钥并记录到注册项中,此后针对本用户进行的注册请求,服务器都要利用公钥和随机数对注册方发起 challenge,要求其进行认证,如图 4 所示。

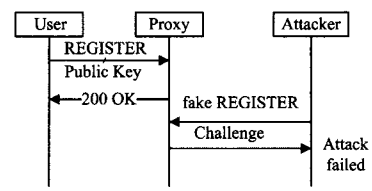

图 4 域内认证机制

建立以上机制后,即使攻击者截获用户的首个 REGISTER 消息,得到了注册所需的 to,Call_ID,CSeq 等字段信息,也不能通过服务器发起认证,因此无法伪装用户进行注册注销和重新注册。对于第三方注册的情况,第三方注册者在接到服务器的认证要求时,需要向原用户询问私钥解密结果才能成功通过认证,从而为第三方注册提供了严格的授权机制。

3.4 端到端认证方案

由 2.2 节的分析可知,消息篡改和拆卸会话这两种攻击都是利用了 SIP 协议缺乏端到端认证机制的安全漏洞。为此,可以增加基于公钥的端到端认证机制。与上面不同的是,端到端认证发生在处于不同区域的用户之间,公钥的分发相对困难,无法对用户与其公钥进行长期的绑定。

鉴于消息篡改和拆卸会话两种攻击都是在两个合法用户正常通话过程中进行,本方案要求在主叫方首次发出的 INVITE 请求中包含自己的公钥,此公钥仅在本次会话中有效。在会话过程中,被叫方如果收到 re-INVITE 请求或者 BYE 请求,就可以利用公钥对其进行认证。但是 3.2 节中服务器对本区域内用户发起 challenge 的认证方式不适合用于端到端的情况,端到端认证应该采用简化的方法。

SIP 消息中的 CSeq 字段由请求类型标识和一个任意的 32 比特的无符号整数组成,用于标识各个 SIP 事务[1],即在一次通话过程的不同事务中,请求信息中的 CSeq 字段有着不同的值。可以考虑利用这一字段进行端到端认证,而无需对协议本身进行过多扩展,也不需要增加专门的 challenge 过程而增加流量开销。具体方法是:通话过程中,主叫方如果需要发出 re-INVITE 请求或者 BYE 请求,就用私钥对最近一个 INVITE 报文的 CSeq 字段进行加密,把密文加入到 re-IN-

VITE 请求或者 BYE 请求中进行发送。由于 CSeq 字段在一次会话的不同 SIP 事务中不会重复出现，因此这一密文即使被截获，也不能被攻击者重复使用。被叫方用公钥解密这一密文后进行检查，如果符合最近一个 CSeq 值，则认为是合法的 re-INVITE 或 BYE 请求，否则丢弃。图 5 显示了这一过程。应用这一认证机制后，攻击者发出的伪造 BYE 请求无法通过认证，拆卸会话攻击失败，而用户发出的含有正确加密信息的 BYE 请求则合法地结束了会话。

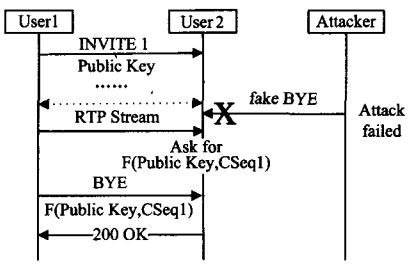

图 5　端到端认证机制

在图 5 的场景中，User 1 发出的 INVITE 请求包含有公钥信息 E 和 N，报文内容如图 6 所示。

```
INVITE sip:0109@10.6.2.162:5060 SIP/2.0
From:sip:0116@10.6.12.98:5061;tag=1205
Call-ID:6335122000@10.6.12.98
CSeq:2666 INVITE
Authentication-Info:E="162D",N="8F932EF1"
.....
```

图 6　INVITE 报文内容

User 1 最终发出的 BYE 请求包含用私钥加密上述 CSeq 字段 2666 生成的密文，因而可以通过认证并正常结束会话，报文内容如图 7 所示。

```
BYE sip:0109@10.6.2.162:5060 SIP/2.0
From:sip:0116@10.6.12.98:5061;tag=9962
Call-ID:6335481563@10.6.12.98
CSeq:10 BYE
Authorization:C="534DA5C7"
```

图 7　BYE 报文内容

通过上述被叫方对主叫方的认证，有效阻止了攻击者在两个用户正常通话过程中冒充主叫方发送 re-INVITE 和 BYE 请求。同理，被叫用户可以在首个对主叫用户的响应信息中加入自己的公钥，采取与上面相同的方法，主叫方就可以对被叫方的 BYE 请求进行认证。这样就实现了主叫和被叫的双向端到端认证，阻止了消息篡改和拆卸会话攻击。

结束语　本文针对 SIP 协议存在的安全问题，在原有的 HTTP 摘要认证机制的基础上进行了扩展。针对 SIP 会话的特点，引入简单可行的公钥分发方式，以较小的代价加强了域内认证，并实现了原有机制所不能提供的端到端认证，增强了 SIP 的安全性。在未来的工作中，我们将进一步研究用户对服务器的认证机制和更高效可行的公钥分发机制。

参 考 文 献

[1] Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol. RFC 3261, 2002

[2] Hong Y, Hui Z, Sripanidkulchal K, et al. Information leak vulnerabilities in SIP implementations. IEEE Networks, 2006, 20(5): 6-13

[3] 俞志春，方滨兴，张兆心. SIP 协议的安全性研究. 计算机应用，2006，26(9)：2124-2126

[4] Samer S, Pascal U. SIP Security Attacks and Solutions: A State-of-the-Art Review// Proc. of IEEE International Conference on Information and Communication Technologies. 2006, 2: 3187-3191

[5] 王宇飞，范明钰，王光卫. 一种基于 HTTP 摘要认证的 SIP 安全机制. 重庆邮电学院学报：自然科学版，2005，12(17)：749-751

[6] Schmidt H, Chi-Tai D, Hauck F J. Proxy-based Security for the Session Initiation Protocol (SIP)// Proc. of the Second International Conference on Systems and Networks Communications. 2007: 24-28

[7] Stefano S, Luca V, Donald P, et al. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network, 2002, 16(6): 38-44

[8] 李荣森，秦杰，窦文华. RSA 系列算法在工程中的应用研究. 计算机科学，2007，34(2)：86-90

(上接第 41 页)

进方案提供了很有价值的参考。

结束语　本文在深入分析可信计算信任模型可信性影响因素的基础上，提出了针对可信计算应用环境的可信性评估方法。分析结果表明，利用所提出的方法较好地实现了对可信计算信任模型的评估。基于评估过程，能够发现影响信任模型可信度的因素，为信任模型的改进和完善提供参考。下一步的工作是为新一代移动网络设计可信接入模型，并且对模型进行评估分析，根据分析结果完善可信接入方案。

参 考 文 献

[1] TCG. TPM Work Group[EB/OL]. https://www.trustedcomputinggroup.org/groups/tpm/, 2007-10

[2] Microsoft. Next-Generation Secure Computing Base home page [EB/OL]. http://www.microsoft.com/resources/ngscb, 007-01

[3] Intel. LaGrande Technology Architectural Overview [EB/OL]. http://www.intel.com/technology/security/downloads/LT_Arch_Overview.pdf, 2007-01

[4] Alan Z. Coming soon to VMware, Microsoft, and Xen: AMD Virtualization Technology Solves Virtualization Challenges [EB/OL]. http://www.devx.com/amd/Article/30186, 2007-01

[5] 郑宇，何大可，何明星. 基于可信计算的移动终端用户认证方案. 计算机学报，2006，29(8)：1255-1264

[6] 余发江，张焕国. 可信安全计算平台的一种实现. 武汉大学学报，2004，50(1)：69-75

[7] JØsang A. A Subjective Metric of Authentication// Proceedings of the European Symposium on Research in Security (ESORICS'98). Louvain-la-Neuve, Belgium, 1998: 329-344

[8] 李小勇，桂小林. 大规模分布式环境下动态信任模型研究. 软件学报，2007，18(6)：1510-1521

[9] Patel J, Teacy W T, Luke, et al. A Probabilistic Trust Model for Handling Inaccurate Reputation Sources// Proceedings of Trust Management Third International Conference (iTrust 2005). INRIA-Rocquencourt, France, 2005: 193-209

[10] TCG. TCPA Main Specification version 1.1b[EB/OL]. https://www.trustedcomputinggroup.org/specs/TPM/TCPA_Main_TCG_Architecture_v1_1b.pdf, 2007-10