SIP安全机制研究

吴 劲，张凤荔，何兴高，陆 庆

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】会话初始协议(SIP)是IETF制订的多媒体通信系统框架协议之一，也是3GPP的IP多媒体子系统(IMS)的重要组成部分。面对复杂、开放的因特网环境，SIP协议自身缺乏有力的安全机制，使其在安全性方面显得较为薄弱。该文从分析SIP的安全威胁入手，针对SIP协议报文明文传送、缺乏有力的身份认证这两大脆弱性，从数据加密和身份鉴定两方面研究了相应的安全解决方案，讨论了如何利用现有技术和手段改善SIP的安全性，并提出了进一步改善SIP安全性的一些思路。

关 键 词 鉴定; 加密; 会话初始协议; 安全机制
中图分类号 TP309 文献标识码 A

Research on SIP Security Mechanism

WU Jin，ZHANG Feng-li，HE Xing-gao，LU Qing

(School of Computer Science and Engineering, University of Eletronic Science and Technology of China Chengdu 610054)

Abstract Session Initiation Protocol (SIP) is an important protocol adopted by the 3rd Generation Partnership Project (3GPP) for the IP Multimedia Subsystem (IMS). Facing the complex and open Internet environment, the security of SIP is poor. After the analysis of the security threats to SIP aiming at cleartext transmission of SIP message and lack of authentication methods, the scheme of data encryption and authentication are researched. And then, we discuss how using the existent techniques for improving the security of SIP and propose the ideas of the security solution to SIP.

Key words authentication; encryption; session initiation protocol; security mechanism

会话初始协议(Session Initiation Protocol，SIP)[1]是IETF制订的多媒体通信系统框架协议之一，是用于建立、改变或者结束多媒体会话的应用层协议。SIP协议基于文本编码，独立于UDP/TCP底层传输协议，与RTP/RTCP、SDP、RTSP、DNS等协议配合实现实时视频共享、语音即时消息、语音–视频电话、视频会议、流媒体的企业协作、点击呼叫(Click-to-call)、自动发起的电话会议、聚合的呼叫中心通信等应用[2]。目前3GPP标准组织已经把SIP作为3G移动通信中的多媒体标准R5的内容之一，即IP多媒体子系统(IP Multimedia Subsystem，IMS)的重要组成部分。

但是，面对复杂、开放的Internet应用环境，SIP协议自身缺少有力的安全机制，使其在安全性方面显得较为薄弱[3]。本文从分析SIP所面临的安全威胁入手，讨论了如何利用现有技术和手段改善SIP的安全性，并提出了进一步改善SIP安全性的一些思路。

1 SIP的安全威胁

SIP协议在设计之初充分考虑了协议的易用性和灵活性，采用了类似HTTP协议的文本方式，没有将安全性作为重点，使其在安全性方面存在一定缺陷。此外，由于SIP消息通过Internet传输，同样面临着IP网络常见的安全威胁[4]。下面分析四种针对SIP的典型安全威胁。

1.1 注册攻击

SIP的注册机制是根据From域中的标识ID来决定是否添加或者修改To域中的Contact地址。SIP协议允许第三方代表用户注册联系信息，From字头又可以由用户代理(User Agent，UA)的所有者改写，这就给攻击者恶意注册提供了方便。这类威胁表明需要一种使得SIP实体能够认证请求发送者身份的安全机制。

1.2 伪装服务器

攻击者通过伪装服务器而达到攻击目的。如用

收稿日期：2005 – 09 – 07
基金项目：国家自然科学基金(60473090)；国家242信息安全专题计划(2006C27)
作者简介：吴 劲(1972 –)，女，博士，讲师，主要从事计算机网络及分布式数据库技术方面的研究.

户发往重定向服务器的请求被攻击者截获，并被假冒成该重定向服务器向请求者发送一条伪造消息，将用户的请求定向到不正确或者不安全的地方。攻击者只需要将应答的From字段改成正确的重定向服务器就可以达到伪造服务器的目的。要想防止这类威胁，就需要UA能够对接收请求的服务器进行身份鉴定。

1.3 拒绝服务和放大

拒绝服务(Denial of Service，DoS)是指向特定的网络接口发送大量的信息，消耗系统资源，达到破坏系统功能或使其暂不可用的目的。通常，SIP中的Proxy需要接收SIP呼叫请求，因此，直接面对开放的IP网络的众多终端设备较容易受到DoS攻击。攻击者通过伪造一个虚假的IP地址和相应的Via字段，假装是某个主机发来的请求，然后大量发送给SIP服务器，从而使服务器资源耗尽，陷入瘫痪。SIP主机除了作为直接被攻击的对象之外，还有可能作为DoS攻击的帮凶，起到放大DoS攻击的作用。这类安全威胁问题需要一个好的安全架构，将拒绝服务攻击造成的影响最小化，并且需要在安全机制中特别留意这类攻击。

1.4 消息篡改

SIP的UA通过信任的Proxy来路由呼叫，恶意的Proxy可以改动SIP消息中的内容，将RTP媒体流指向分接线设备，对通信进行搭线窃听。另外，消息的篡改可能造成UA的误动作，如终止正常的会话，严重影响用户的使用。用户需要一种安全机制来检查消息是否被篡改，但是中间服务器由于路由的缘故，必须修改某些头字段，所以只能保护SIP消息体和一些能够保护的字段。UA可以加密SIP包体，并且对端到端的头域进行一定的限制，对包体的安全服务要求包含机密性、完整性和身份认证，这些端到端的安全服务应当不依赖于中间节点的安全机制。

2 SIP的安全机制

由于SIP协议自身没有专门的安全补充协议和安全机制，需要通过其他手段来保证SIP通信的安全性。本文针对SIP协议报文明文传送、缺乏有力的身份认证这两大脆弱性，从数据加密和身份鉴定两方面研究相应的安全解决方案。

从理论上来说，要保证SIP会话的安全性，可以使用各种已有的安全协议[5]。如通过HTTP协议的Authentication机制可以对SIP会话参与者进行身份验证；SIP协议与SMTP协议报文结构相似的特点也使得S/MIME机制可以应用到SIP会话中，保证SIP消息的机密性与完整性；可以使用传输层的TLS协议来对SIP消息进行安全保护或使用网络层的IPsec协议提供VPN通道来实现安全保护。

2.1 网络层的IPSec

IPSec作为一个公开的框架标准为IP层提供安全鉴定和加密服务。在IPSec执行中使用三种协议来完成它的功能，分别是：封装安全有效载荷协议(ESP)，它为IPSec提供机密性的服务，包括报文内容的机密性和通信量的机密性；鉴别首部协议(AH)，提供鉴别服务；因特网密钥交换协议(IKE)，用于建立一个共享密钥策略，为IPSec提供鉴别密钥信息。

基于SIP的通信网络如果采用IPSec进行安全保护[6]，能够很好地进行访问控制，进行无连接的完整性检查，拒绝重放的分组数据包攻击，保证数据包的机密性和通信的机密性。但是IPSec网络实施复杂，实现代价较高，并且存在一定的扩展性问题，对于遍布于公网上的SIP终端来说，全部都建立IPSec通道是不实际的。

IPSec的VPN通道可以在有特殊安全需求的SIP会话参与者之间，建立一个加密的VPN隧道，使得通信数据只能被通信双方理解。通过这种创建安全隧道来通过不信任的网络的方式，实现SIP会话参与者之间的安全连接。

2.2 传输层的TLS

传输层安全(Transport Layer Security，TLS)提供的是面向连接的传输层安全服务。它工作于TCP层和应用程序之间，通过其提供的TLS套接口可以保证数据在传输过程中的机密性。该协议分为上层的TLS Handshake协议和下层的TLS Record协议。

在SIP网络中应用TLS可以为需要逐跳之间安全通信的主机提供安全服务，保证会话的安全，是一个值得考虑的安全保证手段。TLS也可为SIP实体提供对邻近的服务器的鉴别服务，若要提供对客户端的鉴别服务则需要分发客户端的证书。

TLS的一个缺陷就是必须运行在TCP之上[7]，对于通常运行在UDP之上的SIP服务器来说，同时维持大量的TLS连接会引发负荷较重的问题。可以在Proxy之间通过TLS实现逐跳加密，UA和Proxy之间则采用HTTP摘要认证方式。

具体实现时可将域外的Proxy分为信任和非信任两个组，假定来自信任Proxy的呼叫都是合法的，而来自非信任Proxy的呼叫则不能保证其安全性。既然来自信任Proxy的呼叫都是安全的，那么只要保证

信任Proxy和本域内对外Proxy之间的SIP链路的安全，可以认为呼叫到本域内的对外Proxy是安全的、合法的。然后在信任的Proxy之间通过TLS加密连接来保证安全，实现Proxy逐跳加密。因为Proxy的数量不会很多，因此不会出现因使用TLS而导致Proxy负载过重的问题。

2.3 HTTP摘要认证机制

HTTP摘要认证是一种基于挑战-响应结构的安全机制。采用这种机制，使得密码不采用明文形式在网络上发送，保证了一定程度的完整性，但不提供保密性。

HTTP的认证方式可以不需要太多改动就可直接应用于SIP，任何时候Proxy或者用户接收到一个请求，它尝试检查请求发起者的身份，当发起方身份确认了，请求的接受方确认这个用户是否通过认证。SIP协议的单向身份认证过程如下：

(1) Proxy收到用户请求后对用户发起挑战，挑战一般包括只用于此次挑战的随机数nonce、作用域realm等信息。

(2) 用户将收到的随机数、作用域和用户名、密码(与服务器共享)等信息经摘要算法运算后生成响应值response，然后把响应值嵌入到一个新的请求消息中，重新发送给Proxy。

(3) Proxy通过将收到的响应值同预期计算值相比较来判断用户的合法性。

为了实现双向认证，需要对基本的HTTP摘要认证机制作些扩展，即用户使用HTTPAuthentication-Info消息头认证Proxy。双向认证与单向认证的不同之处就在于：当用户重新发送请求消息时，他/她会在请求消息中加入一个nonce值。新的请求中包括用户对Proxy挑战的应答，并且用户对Proxy也发起了挑战。Proxy认证用户后，发送一个200 OK的响应消息，该响应中包含了Authentication-Info消息头，消息头中包含了Proxy对用户挑战的应答。当用户收到200 OK响应后，用户对代理服务器进行认证[8]，就完成了双向认证的整个过程。

SIP鉴别只适用于用户到用户或用户到Proxy的通信，Proxy到Proxy的鉴别要依赖其他的机制，如IPsec或TLS。

2.4 S/MIME机制

安全/多用途网络邮件扩展(Secure/Multipurpose Internet Mail Extension，S/MIME)机制是基于通用关键子密码算法(Rivest-Shamir-Adleman，RSA)数据安全技术的MIME Internet电子邮件格式标准的安全扩充协议。S/MIME采用了单向散列算法和公/私钥加密体系；认证机制依赖于严格的层次结构，采用与PGP类似的不严格的信任模型；证书格式采用X.509，加密采用对称加密与非对称加密结合，用公钥加密会话密钥，会话密钥加密消息，密钥采用768～1 024位之间的密钥对，常用的加密算法有RC4、RC2、DES、3DES等。

SIP消息中可以携带MIME消息内容，所以也采用S/MIME安全机制为MIME消息内容提供安全保护[9]。采用S/MIME可以为端到端之间的SIP消息内容提供机密性和完整性服务。支持S/MIME的UA必须为每个最终用户保存一份用户的公钥证书，在用户账号与相应的证书之间建立对应关系，维护公钥钥匙圈，同时维护本地的私钥钥匙圈。在没有可靠的第三方证书机构的情况下，用户可以生成自签名的证书，即由用户自己签发X.509证书。也可以使用预置证书，在所有的SIP实体间建立信任关系。如果没有集中的分发用户证书的机构，UA客户端必须支持手动或自动从公开网站上获得证书。

S/MIME可以对消息体(如SDP)进行加密，也可以对包括消息头在内的整个消息进行加密。对整个消息进行S/MIME加密也称为S/MIME隧道机制，加密后消息分为“inter”和“outer”两个部分，外部保留一部分明文的消息头字段以供Proxy正常完成路由功能，后面是S/MIME头字段，加密后的消息附在S/MIME头字段之后。某些消息头字段必须在“outer”中保留一份明文版本，如To、From、Call-ID、Cseq、Contact。

S/MIME加密可以很好地保护被加密消息部分的完整性和私密性。实现时首先将全部或部分SIP消息(包括消息头)的拷贝封装在message/sip类型的MIME消息体中，称为“inner”，然后对这个大的包体用S/MIME安全性来保护。采用S/MIME隧道方式可以对包括头字段在内的整个SIP消息进行保护，这对保护那些不需要被SIP中间实体读取的头字段时非常有效。

2.5 PGP机制

优良保密协议(Pretty Good Privacy，PGP)是另一种端到端的加密签名算法，SIP消息体和部分信息头部也可以通过PGP进行加密。PGP同样采用对称加密与非对称加密结合，对称加密采用国际数据加密标准(International Data Encryption Standard，IDEA)，公钥加密采用128位RSA算法。加密密钥包括：公钥、私钥和一次性的会话密钥。能够提供保密、鉴别、

数字签名和压缩等功能。

发送方用自己的私钥来对“消息摘要”进行加密形成数字签名，用接收方的公钥来加密一次性的传送会话密钥。接收方用自己的私钥来恢复会话密钥，再用会话密钥解密消息。对数字签名则用发送方的公钥来恢复，并通过对“消息摘要”的验证确认发送方的身份。但PGP没有严格的公/私钥分发机制，它更像是一种基于双方信任的加密机制，可由信任的用户之间建立信任网，相互传递公钥，实现公钥的传播。PGP用户由系统产生公/私钥对，在本地钥匙圈保存自己的私钥，在第三方站点上公布公钥信息使通信对方获得自己的公钥。为了提高密钥分发的安全性，避免中间人攻击，用户可以通过电话验证密钥的指纹(16个2位16进制数)或从双方都信任的个体处获得对方的公钥，也可从信任的CA中心获取对方的公钥。PGP还提供增加所分发的公钥可信度的机制，即用户可收集多份经过共同信任的不同的第三方个体来签发公钥证书。被验证次数较多的公钥获得较高的可信度，因而可以有效地减少证书被篡改的可能性。

同S/MIME类似，PGP加密机制实现起来较为复杂，缺少有效的密钥分发和管理机制也是其最大的缺陷。另外基于改进的HTTP摘要认证机制，可以为客户端到服务器及服务器到客户端之间的消息保证一定程度的完整性，但是安全性不如基于公钥的机制。在安全要求很高的场合，可以考虑采用S/MIME、PGP等端到端的签名技术以满足更高层次上对安全的需要[10]。

3 结 束 语

在分析目前可借鉴的用来对SIP通信进行保护的较成熟的网络安全技术的基础上，对这些安全机制的优缺点、适用场合进行了说明，通过必要的改进，应用到SIP中，并给出了包括TLS逐跳加密、HTTP摘要认证、S/MIME、PGP端到端加密签名等技术的实现方式。SIP安全研究需要进一步解决的问题包括：建立更有效的身份认证体系，对SIP会话参与者进行身份认证；寻找轻载的数字签名方案，来对SIP消息进行完整性保护；建立高效的密钥管理与协商机制，快速的协商会话密钥，对SIP信令流与媒体流进行机密性保护。

参 考 文 献

[1] ROSENBERG J, SCHULZRINNE H, CAMARILLO G, et al. SIP: Session initiation protocol[EB/OL]. http://www.ietf.org/rfc/rfc3261.txt, 2002-06-05.

[2] SALSANO S, VELTRI L. QoS control by means of COPS to support SIP-based applications[J]. IEEE Network, 2002, 16(Issue 2): 27-33.

[3] ARKKO J, TORVINEN V, CAMARILLO G, et al. Security mechanism agreement for the session initiation protocol (SIP)[EB/OL]. http://www.ietf.org/rfc/rfc3329.txt? number=3329, 2003-01-10.

[4] TAT C, SENGODAN S. On applying SIP security to networked appliances[C]//Networked Appliances. Gaithersburg: IEEE 4th International Workshop on. [S. l.]: IEEE, 2002: 31-40.

[5] SI Duan-feng, LONG Qin, HAN Xin-hui, et al. Security mechanisms for SIP-based multimedia communication infrastructure[J]. ICCCAS, 2004, 1: 575-578.

[6] CAMARILLO G, BLANCO G. The session initiation protocol (SIP) P-user-database private-header (P-Header) [EB/OL]. http://www.ietf.org/rfc/rfc4457.txt, 2006-04-08.

[7] GEOFF D. TLS as the SIP security mechanism[EB/OL]. http://www.voipsa.org/pipermail/voipsec_voipsa.org/2005-August/000613.html, 2005-08-06.

[8]SALSANO S, VELTRI L, PAPALILO D. SIP security issues: the SIP authentication procedure and its processing load[J]. Network, IEEE, 2002, 16(6): 38-44.

[9] PETERSON J. Neustar Ericsson security, S/MIME advanced encryption standard (AES) requirement for the session initiation protocol (SIP)[EB/OL]. http:// www.ietf.org/rfc/rfc3853.txt, 2004-07-03.

[10] ONO K, TACHIMOTO S. SIP signaling security for end-to-end communication[J]. APCC, 2003, 3: 1042-1046.

编 辑 漆 蓉