基于SIP代理服务器的安全策略探讨

肖德刚　傅静涛　蒋玉明

(四川大学计算机学院　成都 610065)

摘　要　SIP是一种在IP网络中建立、修改和终止多媒体会话的应用层协议,它是IETF多媒体协议体系的一个重要部份。本文在分析SIP体系结构及不安全因素后,从代理服务器的角度提出了三方面的安全策略。

关键词　SIP,UAC,代理服务器,DoS,安全机制协定

1　引言

SIP自IETF提出以来其安全性就受到了学术界及工业界的广泛关注和研究,SIP的安全性问题可以从两个层面来考虑,一是数据包的安全性,主要体现在应用层方面;二是Internet网络的安全性,侧重于网络实体层和传输层。SIP代理服务器作为连通SIP网络中各种用户代理及服务器的桥梁,是SIP网络的重要组件之一,它的安全策略对整个SIP网络的通信起着至关重要的作用。

2　SIP概述

2.1　SIP介绍

SIP(Session Initiation Protocol)即会议初始化协议是由IETF提出的一个基于文本的作用于应用层的多媒体会话信令协议。它的主要功能是用于创建、修改和终止多媒体会议包括IP电话、分布式多媒体、多媒体会议等,它也可以用于邀请参加者加入已有的会议,如多点会议。SIP作为开放的、灵活的、可扩展的协议并不指定任何方式的实现,它必须和其它协议结合起来工作,比如SDP、RSVP、LDAP、RADIUS及RTP等多个协议[1]。

2.2　SIP的会话过程

A向B发起会话请求首先由代理服务器A对用户A进行认证,认证后将会话请求发给重定向服务器直到获得用户B的位置信息,此后代理服务器A向用户B发送会话请求,用户B响应后经代理服务器B然后代理服务器A最后到达用户A,此后用户A向用户B发送确认信息,至此会话正式建立;在会话建立完成之后,用户A和B就可以在基于RTP协议的语音通道上进行语音交流了;会话一方中断会话时都会向另一方发送结束会话的请求,另一方响应后会话正式结束。SIP的网络体系结构如图1所示。

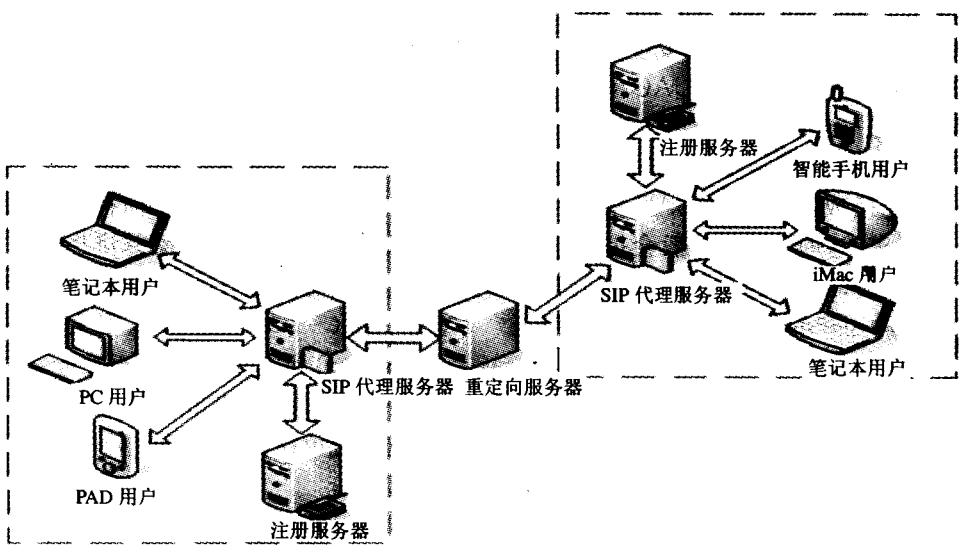


图1　SIP网络基本结构

肖德刚　硕士,主要研究方向:数据库与信息系统;傅静涛　讲师,硕士,主要研究方向:计算机网络与信息系统,集成信息系统;蒋玉明　教授,硕士生导师,主要研究方向:数据库与集成信息系统、ERP等。

3 SIP的不安全因素

由于SIP协议自身的灵活、可扩展及开放性等特点，使其成为一个不容易进行安全保护的协议，在整个SIP体系结构中，面临的不安全因素主要有以下几点[1,2]。

(1) UAC(用户代理客户端)的消息被窃听。在SIP网络中如果UAC的请求或者应答是以明文发送，任何恶意用户都可以窃听并获取会话信息，从而可以轻而易举地发动各种拦截类的攻击，比如拆除会话。

(2) UAC的消息被修改。消息被修改包括三种类型：会话重定向、取消会话和消息体被修改。

(3) 拒绝服务攻击。攻击者通过发送伪造的SIP请求(包含伪造的IP地址及相关的Via头域)产生大量的垃圾应答，使被Via头域指定的主机网络通信阻塞，致使拒绝服务。

(4) 服务器受到攻击。主要包括服务器被冒充、注册攻击和拒绝服务攻击。其中服务器受到的拒绝服务攻击与(3)类似，只是阻塞的是服务器的网络接口。

4 SIP代理服务器的安全策略

从上述分析可以看出，在SIP中需要的基本安全服务有保护消息的完整性和隐私性、防止消息欺骗、对参与会话的用户的信息保密及身份认证等。

4.1 SIP现有安全策略

SIP的安全策略主要是从三个方面来考虑的：端到点、点到点和端到端。端即终端如UAC，点主要指中间服务器如代理服务器和注册服务器。

(1)端到点的安全考虑。端到点安全主要是通过基于TLS的认证来实现的。当UAC第一次发送请求时，UAC需要先与服务器建立TLS连接，此时服务器向UAC提供证书，接受UAC的验证，若通过验证则TLS连接成功。随后UAC基于TLS连接发起第一次请求，这时UAC一般会提供HTTP摘要认证或自己的证书进行认证。HTTP摘要认证适合对众多移动用户的各种管理，UAC提供证书可防止恶意注册。

(2)点到点的安全考虑。点到点的安全主要采用层的IP/SEC或TLS安全机制。这种底层的安全机制假设SIP服务器数量不多且相对稳定，通过服务器间提供自己的证书来证明自身的合法，且在消息中可以记录路由的代理服务器信息，这些信息即是已证明安全的连接，这种逐跳机制可防止终结会话攻击，因为BYE请求不能被伪造。

(3)端到端的安全考虑。因为逐跳加密/解密的方式使SIP消息对中间服务器完全开放，端到端安全更多地结合了S/MIME机制来保证消息体的机密性、完整性和相互认证。要在SIP中实现S/MIME机制必须依赖证书，通信的两个终端在通信之前需要交换证书，证书被双方认可后才可进行通信。

此外还有基于S/MIME实现隧道方式的安全机制，此安全机制用S/MIME方式处理要传送的SIP消息(包括请求行、消息头和消息体)，处理结果当作要传送的消息体，而中间服务器需要用到的信息作为消息头。这样既可保护消息体不被泄露，也可根据比较处理后的消息体信息和头部信息来检查完整性是否被破坏。

4.2 基于代理服务器的安全策略

从代理服务器的角度来考虑安全问题可将安全策略设计得更加灵活、可靠和完善[3,7]。由于无状态代理服务器在对消息进行转发后将会删除转发的信息，即不会记录任何信息，因此本文主要是从有状态代理服务器的角度设计了安全策略。

4.2.1 代理服务器之间必须支持相互认证

代理服务器间可以用逐跳机制和安全机制协定来实现彼此间的安全通信。

逐跳认证给消息提供了完整的机密性。逐跳认证体系要求代理服务器对消息进行解密，且依赖服务器间的信任关系，而信任关系主要由TLS和IP/SEC[4,5]在传输层和网络层实现。在以TLS实现认证、完整性和机密性的SIP体系中要求所有SIP实体都要使用SIPS URI，即UAC在To消息头中放置一个SIPS URI后，若下一跳URI或SIP请求的请求URI包含SIPS URI，则UAC需要在Contact消息头里放置一个SIPS URI，若请求URI包含一个SIPS URI，则请求的任何备选目的地也必须用TSL来联系，且TSL必须使用可靠的传输层协议。

在代理服务器间可以使用安全机制协定(SecAgree)[6]，该协定本来是用于在不同终端与第一跳SIP实体间协调选择何种安全机制的。本文以安全机制协定为基本框架并将其扩展到代理服务器之间上，这需要在消息头部增加三个新的部分：安全客户头部(Security-Client)、安全服务器头部(Security-Server)和安全认证头部(Security-Verify)，但需要考虑当请求发生错误时如何采取基本的安全协定方法，避免在代理服务器处增加头部引起大范围的错误[6]。

当代理服务器需要向下一跳代理服务器发起通信请求时，它将把所有该服务器支持的安全机制清单加到Security-Client头部，并在命令头部标明是安全协定；当下一跳代理服务器收到标明是安全协定的请求时，它将返回一个收到响应给代理服务器，并把它所支持的所有安全机制存入这个响应的Se-

curity-Server 头部，代理服务器在收到响应后根据优先级原则选择两者都支持的最优安全机制进行初始化，如图 2 所示。

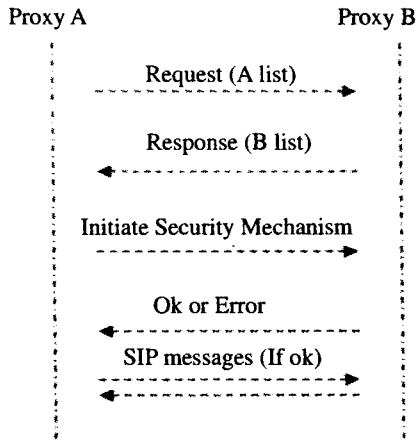


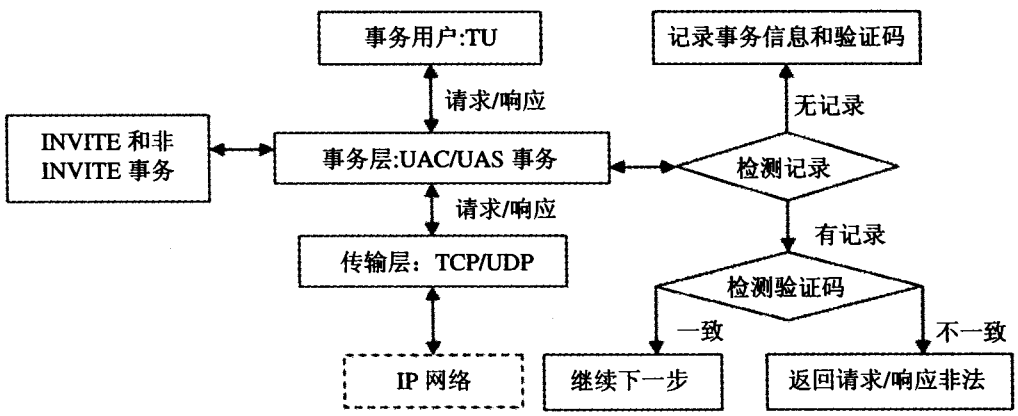
图 2　SIP 代理服务器安全机制协定过程

在安全机制协商的过程中也存在一些安全风险，在实现过程中应尽量避免，比如 Proxy A 在第一次发起安全协定请求过程中，请求所包含的支持清单被攻击者修改，如果此修改会影响 Proxy B 在安全协定时的选择，那么 Proxy B 需要通知 Proxy A 重新进行安全协定，否则可以继续进行下一步；当 Proxy B 向 Proxy A 响应的安全协定请求被攻击者修改时 Proxy B 可以通过对收到的下一步 Proxy A 的安全清单进行检测并发现，攻击者有可能把 Proxy A 返回的清单也进行修改，这就需要对这个返回清单进行编码或完整性保护。

4.2.2　代理服务器的事务认证

SIP 是事务型协议，事务在事务层实现，它包括事务客户端和事务服务器端。事务客户端保证可靠性传输，它发送上层 TU(事务用户)的请求，接收响应，并进行选择过滤和产生 ACK 响应；事务服务器端接收请求并下发由 TU 传来的响应，其间包括事务状态的变化情况和处理响应与请求之间的匹配。一般 UAC 作为事务客户端，代理服务器既可作为事务客户端又可作为事务服务器端[1]。由于代理服务器本身提供路由、选择下一跳位置、有效性检测、处理重传请求及响应等服务，使其工作量很大，对事务的支持会占用代理服务器的大部分性能，因此设计一个简化的对事务进行认证的方法，即在事务层增加验证码的功能。

TU 在初始化事务时产生一个标识自己的唯一码值，该码值被加密后随请求或响应送到下一跳目的地，下一跳目的地的事务在处理请求或响应时对该码值解码并记录该码值，并以该码值为依据判断之后收到的请求或响应是否合法或是伪造的。因为潜在的攻击者即使能伪造请求或响应头部，但也不能提供正确的码值。事务在生成码值和检查码值的过程如图 3 所示。



TU=Transaction User

图 3　SIP 事务层对验证码的处理

在事务的整个过程中仅有事务客户端和服务器端知道彼此的验证码，其它非法的用户因为无法获取该验证码，因此无法在会话建立期间破坏会话信息，不能向事务内的用户发送 CANCEL 请求来取消会话，也不能发送 BYE 请求来终止会话，此外代理服务器还可以记录这些非法的用户请求并对其进行屏蔽。

4.2.3　UAC 的认证、保证数据机密性和完整性

代理服务器可使用 HTTP 摘要认证、CMS (Cryptographic Message Syntax)及 S/MIME 等来实现 UAC 的身份认证、数据机密性和完整性。身份认证及机密性可沿用已有的方法，而对于数据完整性可用 CMS 来实现，但代理服务器并不用这种方法来实现数据完整性的验证，UAC 也没有合适的方式请求代理服务器实现此功能，因此需要良好的机制来实现数据完整性。

代理服务器要实现数据完整性，需要代理服务器对消息进行额外的处理，比如可以数据解密、签名认证和打开 MIME 结构。实现了这些功能的代理服务器也使其易受到拒绝服务攻击和重放攻击，如

(下转第 59 页)

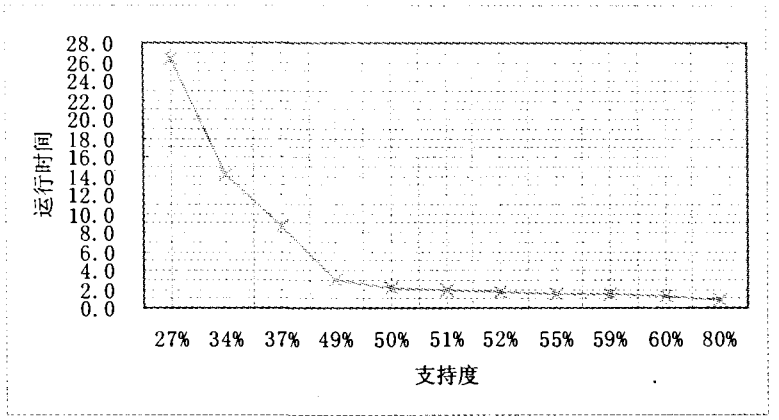


图5 系统运行时间 VS 支持度

参 考 文 献

1 Lee W, Stolfo S J. Data Mining Approaches for Intrusion Detection. http://www1. cs. columbia. edu /~ sal/hpapers/USENIX/usenix. html

2 朱秋萍,毛平平,罗俊. 基于关联规则的入侵检测系统. 计算机工程与应用,2004,26:160~173

3 Agrawal R, Srikant R. Fast algorithms for mining association rules. http://citeseer. csail. mit. edu/cache/papers/cs/1451/http: zSzzSzwww. almaden. ibm. comzSzcszSzpeoplezSzragrawalzSzpaperszSzvldb94_rj. pdf/agrawal94fast. pdf

4 连一峰,戴英侠,胡 艳,许一凡. 分布式入侵检测模型研究. 计算机研究与发展,2003,40(8)

5 KDD Cup 1999Data. http://kdd. ics. uci. edu/databases/kddcup99/kddcup. data. gz

6 Mitchell M. An introduction to genetic algorithms. Cambridge, MA: The MIT Press, 1996

7 Rudolph G. Convergence analysis of canonical genetic algorithms. IEEE Transactions on Neural Networks, 1994, 5(1): 86~101

(上接第 49 页)

恶意用户发送大量复杂的 MIME 结构的消息到代理服务器,恶意代理服务器发送大量复杂的 MIME 结构的包含源 IP 和邻近代理服务器的 Via 头消息来使代理服务器不能提供有效服务及总体性能下降。基于此代理服务器必须支持对用户认证免受重放攻击、对服务器认证免受重放攻击,支持用户认证和数据完整性保护、服务器认证和数据完整性保护,防止重放攻击和拒绝服务攻击。

结束语 随着 SIP 技术的不断成熟和应用的不断发展,SIP 的安全性将会得到越来越深入的研究。本文从代理服务器的角度分析了 SIP 体系结构中 UAC 与代理服务器之间、代理服务器自身以及代理服务器与代理服务器之间现有的安全策略,并提出了用事务的概念及协商机制来实现 SIP 安全性的策略。这种安全策略将会占用代理服务器的部分资源并对性能有一定影响,因此还需要根据实际情况采取相应程度的安全策略,并在实施的过程中考虑人为因素的影响,如管理员及终端用户的干涉。

参 考 文 献

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

2 Burger E, Van Dyke J, Spitzer A. Basic Network Media Services with SIP IETF, RFC4240, December 2005

3 Ono K, Tachimoto S, Corporation NTT. Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP) RFC 4189, Octorber 2005

4 Dierks T, Independent E, Rescorla RTFM, Inc. The Transport Layer Security (TLS) Protocol(Version 1.1) RFC 4346, April 2006

5 Blaze AT M, Labs T A. Keromytis Columbia University M. Richardson Sandelman Software Works L. Sanchez Xapiens Corporation IP Security Policy (IPSP) Requirements RFC 3586, August 2003

6 Arkko J, Torvinen V, Camarillo G, Ericsson, Niemi A, Haukka T, Nokia. Security Mechanism Agreement for the Session Initiation Protocol (SIP). RFC3329, January 2003

7 Rosenberg J, Systems C, Schulzrinne H, Columbia University. Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP), RFC4485, May 2006

8 Camarillo G 著. 白建军,彭晖,田敏译. SIP 揭密[M]. 北京:人民邮电出版社,2003

9 Poikselka M, Mayer G, Khartabil, Niemi A 著. 赵鹏,周胜,望玉梅译. IMS:移动领域的 IP 多媒体概念和服务[M]. 北京:机械工业出版社,2005

10 张智江,张云勇,刘韵洁. SIP 协议及其应用[M]. 北京:电子工业出版社,2005

11 卿斯汉. 安全协议[M]. 北京:清华大学出版社,2005

12 Pfleeger C P 著. 李毅超,等译. 信息安全原理与应用[M]. 北京:电子工业出版社,2004