第35卷 第12期 计 算 机 工 程 2009年6月
Vol.35 No.12 Computer Engineering June 2009
·安全技术· 文章编号：1000—3428(2009)12—0131—03 文献标识码：A 中图分类号：TP309

基于信任域的SIP认证机制

马 骥[1]，周晓光[1]，辛 阳[2]，杨义先[2]
(1. 北京邮电大学自动化学院，北京 100876；2. 北京邮电大学信息安全中心，北京 100876)

摘 要：会话初始协议(SIP)在设计之初没有考虑太多安全问题，其安全隐患十分严重。针对上述问题，介绍SIP协议的安全特性，针对其可能受到的安全威胁，讨论SIP协议的安全机制问题。在“信任域”的基础上提出一个完善的SIP安全认证机制，描述方案的具体应用场景，并指出SIP认证机制的进一步研究方向。

关键词：会话初始协议；SIP认证；信任域

SIP Authentication Mechanism Based on Trust Domain

MA Ji[1], ZHOU Xiao-guang[1], XIN Yang[2], YANG Yi-xian[2]
(1. School of Automation, Beijing University of Posts and Telecommunications, Beijing 100876;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876)

【Abstract】Due to the lack of consideration in Session Initial Protocol(SIP) security, a lot of threats to SIP are emerging and attracting enormous attention. Authentication is one important aspect of SIP security issues. The present authentication-related mechanisms are analyzed. Based on the concept of “trust domain”, a more advanced and effective authentication mechanism scheme is proposed and its implementation process is given. Further research objective in SIP authentication is discussed.

【Key words】Session Initial Protocol(SIP); SIP authentication; trust domain

1 概述

会话初始协议(Session Initial Protocol, SIP)是IETF工作组在1999年发表的一个标准[1]，用于解决IP网上的信令控制。它是基于Internet领域2个最成功的服务Web和E-mail进行设计的，能够把传统的Internet服务以及多媒体和即时消息等新服务结合起来，具有可扩展性、灵活性、互操作性、可重用性、简单高效等特点。SIP已经成为VoIP的主流协议，受到越来越多的关注。

和许多其他的网络协议一样，Internet固有的安全问题使得SIP存在很多安全隐患，如垃圾消息、隐私问题。由于VoIP的应用范围越来越广，因此急切需要解决SIP的安全问题。尤其是SIP的身份认证机制，目前处于研究和不断完善中，必须保证呼叫双方的身份就是消息中实体所声明的身份。本文描述了SIP协议面临的典型安全威胁和攻击，分析了现有的SIP认证机制及其弊端，并在此基础上设计了更加完善的认证机制，分析了SIP认证机制在未来的进一步研究方向。

2 SIP概述及典型安全威胁

SIP的系统结构中包括2种网络元素：SIP用户代理(User Agent, UA)和SIP网络服务器。UA是呼叫的终端部件，包含客户端部分(UAC)和服务端部分(UAS)；SIP服务器是处理呼叫信令的网络设备，分为代理(proxy)服务器、重定向(redirect)服务器和注册(registrar)服务器。

代理服务器能够代理前面的用户向下一跳服务器发出呼叫请求；重定向服务器在获得了下一跳的地址后，立刻告诉前面的用户，让该用户直接向下一跳地址发出请求，而自己则退出对这个呼叫的控制；注册服务器的作用是完成对UA的注册。另外，还有一个很重要的服务器：位置服务器(location server)，它存储并向用户返回可能的位置信息，注册服务器接收到位置信息时会立即将这些信息上载到位置服务器。

在SIP网络中，一次正常的呼叫流程包括：

(1)UAC向网络服务器(proxy或者redirect)发出呼叫请求；

(2)网络服务器通过名字查找和用户定位，最终找到UAS；

(3)被叫UAS响应用户请求；

(4)主叫UAC收到响应后，接通被叫或者终止这次呼叫请求。

虽然SIP协议具有简单、灵活和易于扩展等特点，但单纯使用SIP协议进行网络通信存在着很多不安全因素。一方面，SIP是基于IP网络的实时通信协议，这种开放性使其非常容易受到攻击。通过SIP的构架以及呼叫流程的分析可以发现，各个网络元素之间的通信都仅依赖于对各节点的相互信任，从而导致了相当多的安全威胁。

另一方面，SIP的基于Web和E-mail的文本消息特性赋予了其强大的可扩展性和可操作性，但导致消息容易被模仿、篡改，从而被非法利用。SIP面临的典型攻击主要有注册劫持、服务器伪装、消息篡改、拆卸会话、拒绝服务、垃圾消息攻击等。表1列出了以上攻击手段对SIP消息的可用性、机密性、不可否认性和完整性的影响[2]。

基金项目：国家“973”计划基金资助项目(2007CB310704)；国家“863”计划基金资助项目(2007AA01Z466)

作者简介：马 骥(1984－)，男，硕士研究生，主研方向：网络协议，网络安全；周晓光，博士生导师；辛 阳，讲师、博士；杨义先，教授、博士生导师

收稿日期：2008-11-06 E-mail：mjhorse@qq.com

表 1　SIP 攻击及其威胁

	含义	典型威胁	对策
机密性	信息不可被非授权者利用	注册劫持，服务器伪装，消息篡改，拆卸会话	信息加密
真实性	信息不被伪造、篡改和冒充	注册劫持，服务器伪装，消息篡改，拆卸会话	身份认证 加密校验
可用性	信息卡被授权者正常使用	拆卸会话 DoS	身份认证 系统容侵
可控性	信息的流动可被选择性阻断	DoS	防火墙过滤

3　现有安全机制

由上述威胁模型可见，SIP 认证必须提供基本的安全服务：保证消息的完整性；防止重放攻击或者消息欺骗；提供会话参与者的认证和隐私；防止拒绝服务攻击等。下面介绍一些已有的 SIP 安全机制，并分析其在身份认证方面的缺陷。

3.1　IPSec 和 TLS

对消息完全加密是保证消息机密性最可靠的方式，理论上 SIP 协议可以通过底层的安全机制来保证其安全，如通过网络层的 IPSec 或传输层的 TLS 对 SIP 消息实现完全加密。由于 IPSec 网络实施复杂，因此实现代价比较高。TLS 虽然可能遭受 IP 欺骗，但可以保证会话的安全，是一个值得考虑的安全保证手段。

TLS 是面向连接即 TCP 之上的传输层安全，工作于 TCP 层和应用程序之间，通过它提供的 TLS 套接口可以保证数据在传输过程中的机密性。但是 TLS 不能在 UDP 之上运行，对 SIP 服务器来说，同时维持大量的 TLS 连接负荷较重，存在扩展性的问题。此外，TLS 的防火墙穿越问题也是必须考虑的。

3.2　SIP Digest

SIP 的摘要认证机制采用与 HTTP 摘要认证[3]类似的认证机制，解决了 Proxy 或者 USA 对 USC 的鉴权。HTTP 摘要认证根据用户名和密码验证来一个用户。身份认证过程如下：服务器收到客户机请求后对客户机发起挑战，挑战一般包括只用于此次挑战的随机数 nonce，作用域 realm 和算法 F 等信息。客户机将收到的随机数、作用域和用户名、密码(与服务器共享)等信息经摘要算法 F 运算后生成响应值 response，并将其发送给服务器继续请求。服务器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。

3.3　S/MIME

S/MIME(Secure Multipurpose Internet Mail Extensions)是用于保证电子邮件端到端的安全技术。SIP 使用的 S/MIME 安全功能包括消息体加密和隧道加密，提供了消息体端到端的机密性、完整性和相互认证。但由于 SIP 消息的某些头域以及某些情况下的消息体必须对 Proxy 可见才能正确路由，因此不能通过端到端的加密方式对 SIP 完全加密。并且其加密机制实现复杂，缺少有效的密钥分发和管理机制。

3.4　现有机制的缺陷

通过对已有的 SIP 安全解决方案的分析可以发现，SIP 的安全问题没有得到彻底解决，尤其是在用户的身份认证方面有很大的缺陷。如针对终端的 PKI 基础设施普遍缺乏，使 TLS 和 S/MIME 很少或无法使用；Digest 机制只能用于有预共享密钥的实体之间，而这种前提在 SIP 跨域的通信中很难实现；SIP 消息头中含有的用户隐私信息易被攻击者窃取和利用，并且有些信息在消息路由时要用到，因此，很难完全解决隐私问题。表 2 列出了现有机制在认证方面的缺陷。

表 2　已有安全机制和缺陷

方案	认证方面的问题
TLS/IPSec	在应用层路由只能逐跳进行(hop-by-hop)；终端很少使用 IPSec 和 TLS；TLS 对于服务器负担比较大
SIP Digest	前提是共享密钥关系，跨域范围内很难实现
S/MIME	加密机制复杂；缺乏有效的证书分发和管理机制；路由信息和消息体不能进行完全的隐私保护

4　基于信任域的认证方案

针对 SIP 的潜在安全隐患，本文设计了一个完整的 SIP 认证机制，同时保证了域内和域间的身份认证安全，并给出了相应的交互细节和实现流程。

4.1　域内认证

SIP 允许用户在消息中加入 ID 来申明自己的身份，一般情况下 SIP 消息只有一个 ID 标识，形式为 sip: /sips: /tel: URI。但是这个 ID 并不能提供不同 SIP 节点之间的信任关系(如 X 被 Y 信任，表示为 Y->X)。判断信任关系有 2 个要素(信任准则)：(1)X 和 Y 间的连接是安全的；(2)节点 Y 知道 X 是一个可信任节点。

基于信任准则，文献[4]提出信任域的概念，指出用户可以分为在信任域内和在信任域外 2 类，信任域内和域外使用 SIP 进行通信应采用不同的机制和安全级别。在信任域内的节点就是可信任节点，因此，可以在此基础上建立一个信任连接表。信任连接表的数学语言描述如下：

设网络中的节点集合为 $S = \{p_1, p_2, \cdots, p_i\}, i \in N$。属于信任域的节点集合为 $M = \{a_{t1}, a_{t2}, \cdots, a_{tk}\}, k \leqslant i$，则连接矩阵和信任矩阵分别为

$P = (p_{ij})_{n\times n}$，若 p_i 与 p_j 有安全连接，则 p_{ij} =1，否则 $p_{ij} = 0$；

$T = (t_{ij})_{n\times n}$，若 a_{ti} 属于信任域，则 $t_{ij} = 1(i = j)$，否则 $t_{ij} = 0$。

信任连接表 TP 的矩阵计算公式为

$TP = T \times P = (tp_{ij})$，若 $tp_{ij} = 0$，则 p_i 不信任 p_j。若 $tp_{ij} = 1$，则 p_i->p_j

在 SIP 框架中，各 UA 间需要一种机制可以让通信双方得知对方是否可信任，即需要知道该 UA 是否处于信任域中以及与其的连接是否安全。由于 Proxy 可以通过 HTTP 摘要认证用户并获取 UA 的安全能力，因此可以利用 Proxy 为域内通信双方提供相关的认证信息。本文设计了一种机制，在消息认证成功后 Proxy 在头域添加一个新的身份标识，即 NAI(Network Asserted Identity)，用来作为通过验证以后的 ID。这样，就可以在信任域内标识可信 UA。其流程如图 1 所示。

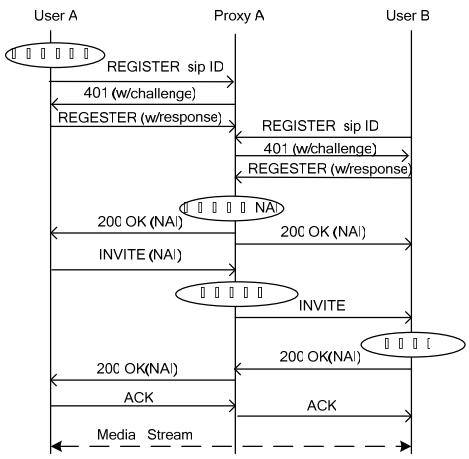

图 1　使用 NAI 的域内通信

在有些情况下，User A 得到一个 NAI 以后，还可能再向域内其他服务器发送消息，如果这时其他 Proxy 再分配一个 NAI，则会导致重复认证。因此，实现时规定其他 Proxy 和 UA 看到这个 NAI 后，就认为该消息是可信的，不必重新分配 NAI，这样解决了可信任域内重复鉴权的问题。但 NAI 只能在一定程度上解决域内的身份认证问题，因为 NAI 本身也需要被保护。另外在域间通信时，不应该将 NAI 泄露到信任域外部，因为 NAI 通常与用户的隐私信息相关；还需要保证 NAI 的完整性问题，下面设计的域间签名机制解决了这些问题。

4.2 域间认证

在域间通信中，用户通常希望自己的身份和消息内容不会被第三方查看或者篡改，前面分析过，现有的安全机制并不能很好地保证域间通信认证。在没有终端证书情况下，文献[5]提出了使用域间签名的方案，但是并不完善，并且没有包括域内认证的设计。本文在现有方案基础上进行了改进，同时保证了域内和域间通信身份认证安全。通过使用信任域的域证书对请求消息进行签名，消息的接收方所在域服务器对签名进行验证。由于 2 个信任域之间通过域证书建立了可信连接，因此终端用户相信来自远端信任域的请求方身份，避免了终端证书操作，又提供了跨域认证和身份隐藏，其具体流程如图 2 所示。

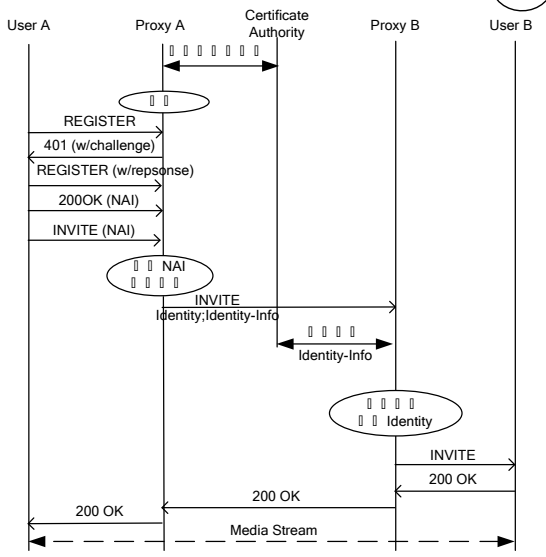

图 2 新机制域间通信流程

信任域 A 需要在权威认证服务器上注册并获取自己的公钥证书，然后就可以用私钥对发往信任域 B 的请求签名。如果发往域外的请求消息中包含了 NAI，则应该删除 NAI，不让域外实体获取。信任域 B 的 Proxy 收到请求后，根据 Identity-Info 获取域 A 的证书，然后验证签名。如果签名正确，则表示身份认证通过，将请求转发给信任域 B 的用户，否则返回 451 Domain Authentication Failed 响应。

上述签名机制也可以进一步保证域内的通信安全，如将请求方的 Proxy 将 NAI 包含在签名计算中以保证其完整性，或者接收方 Proxy 重新计算签名以保证与接收 UA 的域内通信安全。这种情况下，使用的密钥是 Proxy 相应 UA 的共享密钥，并通过 Identity 和 Identity-Info 告知接收方 UA 该请求已由域内服务器签名。另外，计算哈希值时要包含 Date, Content-Length 等多个字段，假如请求消息没有该字段，Proxy A 需要在 SIP 头域中插入这些字段，利用这些字段就可以提供双重的安全机制。

4.3 认证机制的实现

上述认证方案的完整流程如图 3 所示。

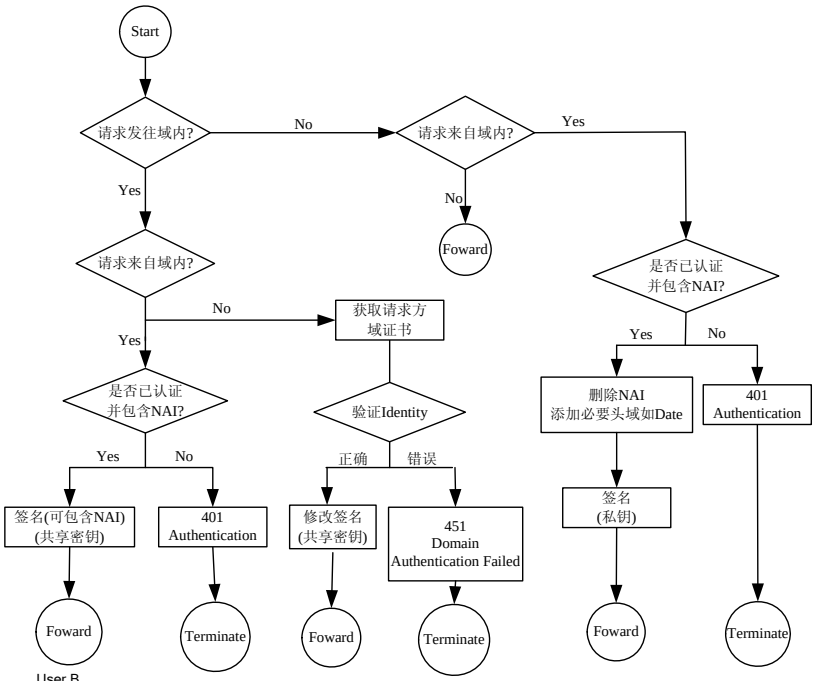

图 3 认证机制系统流程

本方案中摘要使用 HMAC[6]机制进行计算，具体计算公式为

signedIdentityDigest = HMAC_alg (key, (NAI) || From addr-spec || To addr-spec || callid ||1*DIGIT SP Method || SIP-date || Contact addr-spec || message-body)

其中，||表示连接符；NAI 为可选字段，根据安全需求选择是否加入计算；签名算法参数 HMAC_alg 可以赋值为不同的字符串来指定不同的算法，如 HMAC-MD5，HMAC-SHA1。

4.4 安全性能分析和研究展望

本文提出的安全方案将域内认证和域间认证相结合，较其他方案更为完善和可靠，域证书的分发相对终端证书来说容易得多。同时由于服务器精简了一些终端目前很难实现或者需要耗费大量资源的功能，如 IPsec/TLS，而单纯的摘要算法不会大幅度增加复杂度，因此网络的负载不会明显增大，在不需要大幅度提高终端性能的情况下保证了通信的有效和安全。

随着 SIP 安全隐患越来越受到关注，新的问题和需求层出不穷，SIP 的认证机制仍然存在很多需要研究和改进的地方。比如，在一些情况下，用户希望对其 NAI 进行保密，即 NAI 不被其他人看到，即使是信任域内的用户。这一问题目前还没有得到很好的解决[5]。响应的可能情况相对更加复杂，对于响应消息的攻击也难以避免，目前相关的研究正在进行之中。另外，此方案仅仅依赖于发送方，若 Proxy A 对其域内的请求不能采取完善的安全策略，接收者就不能保证其安全。

(下转第 136 页)