SIP 协议的认证机制及其性能分析

金康双，王泽兵，冯 雁，陈海燕
(浙江大学 计算机科学与技术学院，浙江 杭州 310027)

摘 要：SIP 协议是 IETF 提出的 IP 电话标准，有着很好的应用前景。讨论了 SIP 协议的安全认证机制，并通过基于开放源码的 Java 程序在一个 SIP 代理服务器上的执行，对该应用中 SIP 协议安全机制及有关性能进行了分析评价。

关键词：SIP；安全认证；IPSec；TCP；UDP；TLS
中图法分类号：TN915.04 **文献标识码**：A **文章编号**：1001-3695(2004)08-0110-03

SIP Authentication Mechanism and Its Performace Analysis

JIN Kang-shuang, WANG Ze-bing, FENG Yan, CHEN Hai-yan
(College of Computer Science & Technology, Zhejiang University, Hangzhou Zhejiang 310027, China)

Abstract: Session Initiation Protocol(SIP) is the Internet Engineering Task Force (IETF) standard for IP telephony, and it has a promising applied prospect. In this work, the security authentication mechanism used by SIP is described. Moreover an experimental performance analysis of the SIP security mechanisms is provided, which based on the open source Java implementation of a SIP proxy server.

Key words: SIP; Security Authentication; IPSec; TCP; UDP; TLS

1 引言

SIP 是 IETF(the Internet Engineering Task Force)的 IP 电话标准，将会成为未来 IP 电话服务中最有前途的呼叫建立信令协议；同时还被 3GPP(the Third-Generation Partnership Project)指定作为 3G 移动网络的多媒体应用协议。经过多年的发展，PSTN 已经建立起比较好的 QoS 和安全。因此，如果新的 IP 电话体系结构和 SIP 协议想取代 PSTN，至少需要提供具有相抗衡的 QoS 和网络安全的电话服务。一般来说，QoS 的问题大部分都涉及到 IP 网络层，而安全的问题主要与网络层、服务控制体系结构和它采用的信令协议等有关。以下的一些安全特征必须得到保证：服务有效性高、系统运行稳定和无差错，以及对用户-网络、用户-用户间的通信安全的保证(包括控制数据和用户数据)。本文主要考虑 SIP 的用户-网络、用户-用户间通信安全，并着重阐述 SIP 协议的安全认证机制。

2 SIP 及安全认证机制

2.1 SIP 介绍

SIP 是基于文本的客户服务器协议，客户端发起请求，服务器进行响应。SIP 协议中定义了各种不同的实体：用户代理(User Agents)、代理服务器(Proxy Servers)、重定向服务器(Redirect Servers)和注册服务器(Registrar Servers)。用户代理代表终端(如一个包含用户代理客户端和用户代理服务器的应用)；代理服务器是中间实体，它同时扮演客户机和服务器的角色，代表其他的客户机发出请求；重定向服务器接收来自客户端的请求和响应，并反馈响应信息(通常提供被呼叫者的联系地址)；注册服务器是一种特殊的服务器，它接收客户机的注册请求。

当客户端发起呼叫时，一个 INVITE 请求发送到服务器，并从服务器接收相应的响应。一个成功的 SIP 邀请(Invitation)包括两个请求：INVITE 消息以及随后的 ACK 消息。INVITE 请求邀请被呼叫者加入或建立呼叫，如果被呼叫者的响应显示接收呼叫(通过提供 200 OK 响应消息)，呼叫者通过发送 ACK 消息来确认响应；当呼叫者或被呼叫者希望终止呼叫，他们通过发送 BYE 请求实现。为了改变会话参数，在已存在的会话中可能需要发送再邀请(Reinvitation)请求，通过再发送一个带有新的会话参数的 INVITE 消息来实现。SIP 消息中包含消息体，主要是关于会话创建时的一些信息，其格式主要使用 SDP(Session Description Protocol)协议。

2.2 SIP 的安全机制

SIP 消息头可能会透露关于交流模式或其他需要保密的信息，SIP 消息体也可能包含不应该透露的用户的信息(媒体类型、编解码方式、地址和端口等)。应用在 SIP 中的安全机制可以分为两类：end-to-end 的保护和 hop-by-hop 的保护。End-to-end 机制主要涉及呼叫者和被呼叫者的 SIP 用户代理，是 SIP 特意对安全方面所做的一些考虑，如 SIP 认证和 SIP 消息体加密等；Hop-by-hop 机制是为了保证在消息的传送路径上两个连续的 SIP 实体之间的通信安全。SIP 并没有专门提供用于 hop-by-hop 安全保护的功能，主要还是依赖网络层(IPSec)或传输层(TLS)的安全。

SIP 中主要使用两种安全机制：认证和数据加密。

(1)认证用于鉴别消息发送者的合法性，以确保一些机密信息在传输过程中没有被窜改，防止攻击者修改或冒名发送 SIP 请求或响应。SIP 使用代理认证、代理授权、授权和 WWW 认证头字段(类似 HTTP 认证)等，以数字签名的方式进行终端

收稿日期：2003-06-05；修返日期：2003-10-11

的认证。相反, hop-by-hop 认证可以利用传输层或网络层的安全协议(如 TLS 或 IPSec) 进行。

(2) 数据加密用于保证 SIP 通信的保密性, 只有特定的接收者才可以解密并浏览数据。一般都是通过使用加密算法如 DES(Data Encryption Standard) 或 AES(Advanced Encryption Standard) 实现的。SIP 支持两种形式的数据加密: end-to-end 和 hop-by-hop。End-to-end 加密提供所有不需要中间代理服务器处理的所有信息(一些 SIP 协议头字段和消息体) 的安全性保障; End-to-end 加密通过 S/MIME 机制实现。相反, hop-by-hop 加密是为了保护需要中间实体访问的 SIP 消息(如 From, To 和 Via 字段) , 对这些消息进行加密可以防止恶意攻击者了解到呼叫的双方或访问路由信息。Hop-by-hop 加密可以通过 SIP 外部的安全机制(如 IPSec 或 TLS) 来实现。

2.3　SIP 安全认证过程

SIP 认证过程源自 HTTP 摘要式认证(HTTP Digest Authentication) , 它是一种基于质疑(Challenge-based) 的安全机制: 当服务器收到一个请求, 将向质疑请求的发起者提供相应的身份信息。服务器发出的质疑中会包含生成的唯一字符串序列, 仅可用于本次质疑。请求者和服务器共享同一密码, 请求者使用该密码和临时生成的字符串序列得到一个响应值。当请求者再次发送包含这个响应值的请求时, 服务器就可以用来对请求进行认证。利用这种机制, 密码就可以不用明文的方式传送, 图 1 给出了摘要式认证的过程。

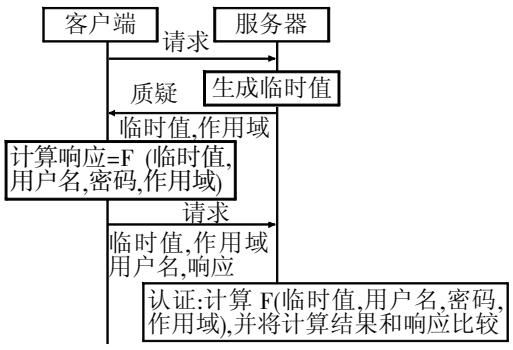


图 1　摘要式认证的过程

图 1 中, 函数 F 用于计算响应值, 规定输入的参数如何与摘要式(Digest) 算法的叠代相结合。摘要式算法可以在质疑中指定, 缺省为 MD5。要求进行 HTTP 认证的服务器可以是目的服务器也可以是代理服务器: 包含在质疑中的一个头字段用来判别这两种情况。SIP 的认证过程比较简单: 当服务器或接收呼叫, 或转发呼叫, 或接受注册前会要求认证呼叫方(UAC) , 认证过程就开始启动。用户代理客户端(UAC) 开始发送明文的 SIP 请求消息(如 INVITE 请求用于建立呼叫或 Register 请求用于更改位置信息) , 服务器接收到该请求后确定需要进行认证, 将会返回给客户端一个特定的要求认证的 SIP 错误消息, 这个错误消息就表示质疑, 并包含临时字符串序列和作用域内容。其中, 用户代理服务器(UAS) 和注册服务器返回的是未授权错误消息 401, 而代理服务器返回的是未认证错误消息 407。用户代理客户端收到错误消息后, 计算出响应值, 并将它放入到新的 SIP 请求消息中。图 2 显示了代理服务器要求的认证消息序列。

UAC 在收到错误消息后会马上发送 ACK 消息, 同时第一个通信事务结束; 然后 UAC 再次发送 INVITE 消息, 并开始一个新的通信事务。包含在质疑和已认证的请求中的作用域(Realm) 参数用来表示域, 在该域内用户才享有服务。在要求提供用户名和密码的时候, 用户可以看到这个作用域参数。在原来的 SIP(IETF RFC 2543) [2] 中允许基于 HTTP 基本认证(HTTP Basic Authentication) 的认证过程。这种认证中, 用户名和密码以明文的方式传送, 易受包侦听的攻击, 因此根本就不安全。最新版本的 SIP(IETF RFC 3261) [1] 反对使用这种方法, 并且只有摘要式认证可以使用。从现在安全的标准来看, 摘要式认证的安全级别还是不够高, 一个原因就是它采用共享密码方式而不是公钥加密机制。SIP 协议推荐使用公钥加密机制。

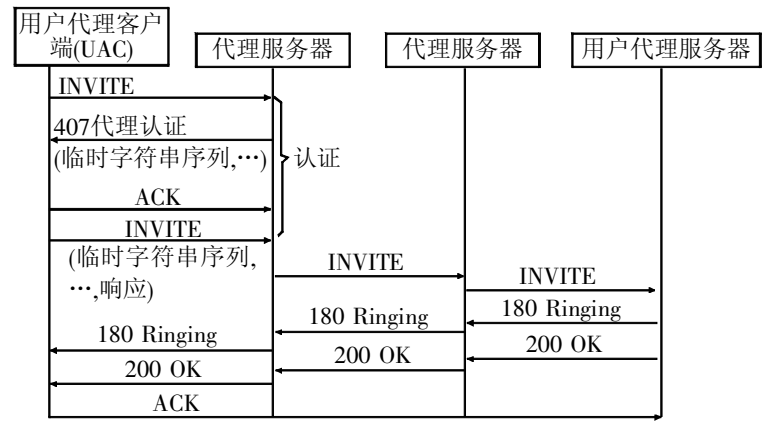


图 2　经由代理和认证的 SIP 呼叫建立过程

3　基于SIP 的IP 电话服务

为了更好地分析 SIP 安全认证机制, 这里给出一个基于 SIP 的 IP 电话服务应用实例。该服务由用户连接 ISP 呼叫 PSTN 中的用户, ISP 实际上是由 ITSP(Internet Telephony Service Provider, 提供网关, 传送呼叫到 PSTN) 来实现。ISP 网络中的 SIP 代理服务器必须配置成为 SIP 客户端缺省的对外代理服务器, 这个代理服务器会将呼叫递交到 ITSP 代理服务器, 然后再选择联系更合适的 SIP 网关(图 3) 。

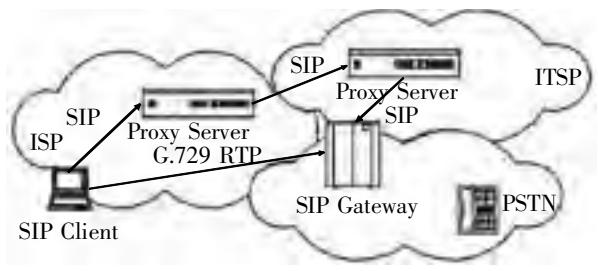


图 3　PC-Phone 呼叫

在这个例子中, 用于呼叫过程的一种可行的安全实现机制如下: ①ISP 代理服务器使用 SIP 代理认证方法对呼叫用户进行认证。由于 ISP 是对其客户进行认证, 所以将会利用已经建立的用户账号资料, 已知的一些认证体系结构和协议(如 RADIUS) 可以用于解决 ISP 端获取用户账号信息的安全问题, 并且对于 SIP 是透明的。②一旦用户得到代理服务器的认证, 代理服务器会核实用户是否授权发起该呼叫。如果确实被授权, 代理会将 SIP 请求传递到 ITSP 服务器。由于不存在基于 SIP 的安全机制, 让 ITSP 代理去认证以前的代理, 因此对于 ITSP 代理来说, 有两种选择: ①要求进一步的用户代理认证; ②依赖 SIP 之外的一些安全机制去认证以前的代理。第①种方式是不合理的, ITSP 需要再次取得用户账号信息, 既然 ITSP 会直接去认证用户, 因此 ISP 中第一次认证就显得多余。相反, 第②种方式即 ITSP 将整个 ISP 作为用户, 因此, 两个代理服务器之间采用 hop-by-hop 认证方式将非常合适, 并且可以应用 TLS 或 IPSec。图 2 提供了呼叫建立过程产生的呼叫流。在该 IP 电话服务的基础上, 接下来将讨论有关安全性能的问题。

4 性能分析和评价

为了测试 SIP 协议中的认证机制性能,我们特意用 Java 语言开发了 SIP 服务器,并搭建了一测试平台。测试平台由安装 Linux 或 Windows 98/2000 操作系统的 PC 机组成,分别作为 SIP 客户端、SIP 服务器、DiffServ(Differentiated Services) 路由器以及 DiffServ 宽带代理。

测试平台的目标有两部分: (1) 验证各种 SIP 成员的功能行为和他们的互操作性; (2) 实现进行一些性能分析的可能。其中重点是性能分析,尤其是 SIP 中引入安全机制后(如认证过程) 的性能损耗评估。为了达到这样的目标,我们采用纯粹实验的方法来评测平台上各种安全过程的运行开销。当然,既然测试结果如此依赖测试执行模块和测试平台的特定的特性,我们必须意识到这种方法的局限性,虽然得到完全有效的实验结果是不可能的,但是对于评估各种不同的安全过程的相对运行开销还是非常有用的。我们特别将注意力集中在 SIP 代理服务器上,因为它是基于 SIP 的电话服务系统的潜在瓶颈。基于这个认识,我们特别定义一种方法来评估 SIP 代理服务器上的 SIP 进程运行开销,该方法的主要思路就是测估代理服务可达到的最大性能(单位时间处理进程的吞吐量) ,处理进程的开销就可以从吞吐量的倒数推算出来。图 4 显示了测试代理服务器性能的环境。

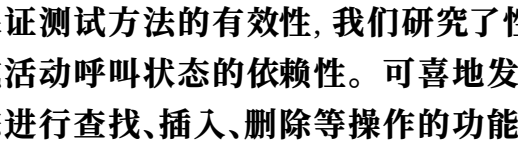


图 4 测试 SIP 服务器性能

图 4 中左边的测试端 UAC 是个多线程 Java 应用,它可以产生 SIP 呼叫并评价呼叫的吞吐量; 被测试对象代理服务器真正处理呼叫; 图 4 中右边测试端 UAS 是个简单的 Java 应用,根据正确的 SIP 消息流返回预先定义的回答。三个模块都运行在单独的 PC 机(300 MHz Pentium/128MB RAM) 上,机器上无其他应用运行,并且 PC 机间通过快速以太 Hub 互连。测试端 UAC 中的每个线程(最多 6 个) 接连产生一系列 SIP 呼叫(测试中为 100 个) ,当一个呼叫完成(收到 200 OK 消息或发送 ACK 消息) 时,一个新的呼叫马上建立。这样做的目的就是使代理服务器的处理容量达到饱和,从而可以测量服务器最大吞吐量。正因为这个目的,测试端 UAC 需用多个线程。从前面介绍的基于 SIP 电话服务来看,有八种认证处理过程(方案) 需要考虑,详见表 1 和表 2。如表 2 所示,基本的处理过程 1 是没有安全认证的 SIP 呼叫建立过程,代理服务器是无状态服务器,一般使用 UDP 协议进行通信; 处理过程 2 包含安全认证,其呼叫流程如图 2 所示; 处理过程 3 中主要为了比较 UDP 协议及 TCP 协议的运行开销差别; 在处理过程 4 中,我们评估了在代理服务器和测试端 UAS 之间使用 TLS 安全连接的运行开销。考虑基于 TCP 的 SIP 通信的动机是为了进一步地分析基于 TLS 的 SIP 通信情况,处理过程 5 ~8 和处理过程 1 ~4 分别对应,不同的只是考虑了状态代理服务器(Stateful Proxy Server) 的情况。在处理过程 5 ~8 中,状态代理服务器接收并处理来自呼叫端 UAC 的 ACK 消息以及终止呼叫的 BYE/OK 消息,并会保持活动呼叫的状态,同时在呼叫结束时删除状态。

为了保证测试方法的有效性,我们研究了性能对于未定的认证状态或活动呼叫状态的依赖性。可喜地发现: 用于对认证和呼叫状态进行查找、插入、删除等操作的功能,其运行开销基本上取决于活动认证状态的数目; 另一方面应仔细分析和调整测试端 UAC 中的活动进程数。表 1 显示了处理过程 1 中采用不同数目的线程所能达到的吞吐量。从并行的两个线程开始,逐渐使服务器处理容量达到饱和。N 个线程中每个获取服务器处理容量的 1/N,从而就可以得到最大吞吐量。

表 1 采用不同线程数能达到的吞吐量

无认证,无状态服务器,UDP(“基本”呼叫建立过程)						
活动线程数	1	2	3	4	5	6
单线程吞吐量(S^{-1})	27.8	15.9	10.6	7.9	6.4	5.3
总吞吐量(S^{-1})	27.8	31.7	31.9	31.7	31.8	31.7

表 2 显示的是我们评测的结果,表 2 的第三列显示的是代理服务器可达到的理论最大吞吐量。只有在服务器资源 100% 利用的情况下才能达到,实际上是很难达到的,表 2 中最右边的两列数据表示由吞吐量换算而来的相对处理开销。处理过程 1 的相对处理开销设为参考值 100,同时处理过程 5 的相对处理开销也设为参考值 100。

表 2 评测结果

	处理过程	总的吞吐量(S^{-1})	相对处理开销	
1	无认证,无状态服务器,UDP(“基本”呼叫建立过程)	34.8	100	
2	认证,无状态服务器,UDP	19.6	177	
3	认证,无状态服务器,TCP	19.4	180	
4	认证,无状态服务器,TLS	19.2	182	
5	无认证,有状态服务器,UDP	21.0	166	100
6	认证,有状态服务器,UDP	14.6	239	144
7	认证,有状态服务器,TCP	13.8	253	152
8	认证,有状态服务器,TLS	13.6	256	154

测试结果显示,引入 SIP 安全认证机制,对于无状态服务器来说,增加了将近 80% 的处理开销; 对于有状态服务器来说,增加了近 45% 的处理开销。开销的主要原因是需交换的 SIP 消息增多及安全的实际处理开销(包括加密算法) ,我们发现其中 70% 的额外开销用于消息处理,30% 的额外开销用于实际的安全处理。这些测试结果是在认为 SIP 消息发送的时候 TCP 和 TLS 连接已经建立并可用的情况下获得的,这样的假设在 ISP 和 ITSP 代理服务器之间存在相对稳定的连接时是完全可能的。

5 结论

本文讨论了 SIP 安全认证机制,描述了基于 HTTP 摘要式认证的认证过程,最后通过纯实验的方法分析了 SIP 认证的性能情况。虽然实验结果明显受到测试平台的影响,但还是提供了 SIP 安全认证过程的处理开销的定量分析。

参考文献:

[1] Rosenberg, et al. IETF RFC 3261, SIP: Session Initiation Protocol [S] . 2002.

[2] Handley, et al. IETF RFC 2543, SIP: Session Initiation Protocol [S] . 1999.

[3] Kent, R Atkinson. IETF RFC 2401, Security Architecture for the Internet Protocol[S] . 1998.

[4] Dierks, C Allen. IETF RFC 2246, The TLS Protocol version 1.0 [S] . 1999.

[5] Ramsdell, et al. IETF RFC 2633, S/MIME version 3 Message Specification[S] . 1999.

[6] Thomas. SIP Security Requirements[R] . IETF Internet Draft Raft-thomassip-sec-req-00. txt, 2001.

[7] Arkko, et al. Security Mechanism Agreement for SIP Sessions[R] . IETF Internet Draft-ietfsip-sec-agree-04. txt, 2002.

作者简介:

金康双(1977-) ,男,浙江乐清人,硕士研究生,主要研究方向为网络通信、电子商务。