文章编号:1001 - 9081(2007)02 - 0311 - 03

一种基于 ECC 的 SIP 认证方案的提出与实现

李士达[1,2],胡 玥[1],王兴秋[1],于 真[1]
(1. 北京科技大学 信息工程学院,北京 100083; 2. 中国科学院 计算技术研究所,北京 100080)
(lishidahappy@163.com)

摘 要:随着会话发起协议(SIP)应用领域的不断扩大,SIP 实体间通讯的安全问题成为了亟待解决的热点问题。对 SIP 的安全方案进行了讨论,分析了进行安全认证的方法,在此基础之上提出了一种新的基于椭圆曲线密码学(ECC)的认证方案,保证了 SIP 消息传输过程中完整性、机密性和不可抵赖性。

关键词:会话发起协议;椭圆曲线密码学;身份认证;公钥体制
中图分类号: TP393.08 **文献标识码**:A

Realization of SIP authentication scheme based on ECC

LI Shi-da[1,2], HU Yue[1], WANG Xing-qiu[1], YU Zhen[1]
(1. *School of Information Engineering, University Science technology of Beijing, Beijing* 100083, *China*;
2. *Institue of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: The Community of Session Initiation Protocol (SIP) entity is becoming an urgent problem to be solved with the continued enlargement of SIP application area. The security scheme, especially its security authentication was discussed and analyzed. Furthermore, a new authentication scheme based on Elliptic Curves Cryptography (ECC) was put forward, which assures the integrity and security during the transmission of SIP message.

Key words: Session Initiation Protocol (SIP); Elliptic Curves Cryptography (ECC); authentication; pki

0 引言

会话发起协议(Session Initiation Protocol,SIP)是由 IETF 提出的应用层协议,是 IP 网络中的呼叫控制协议。它的基本功能是创建、修改和终结会话,并且支持用户的移动性。由于自身具备简单性、灵活性和扩展性等特点,SIP 协议在下一代网络规划中可用于软交换设备之间的通信,以及软交换设备和应用服务器之间的通信。目前 SIP 已经成为 3G 移动网络的多媒体应用的协议标准,同时 SIP 协议与其他协议相结合,可以提供互联网上的音频、视频和即时消息等多媒体服务。

然而,在 SIP 协议的制定过程中,大部分精力都放在了如何才能动态的,方便快捷的来提供强大的、新型的服务功能,而安全性被予以了太少的关注,导致单纯使用 SIP 协议进行实体间网络通信面临注册欺骗、冒充服务器、篡改消息体和中断会话等各式各样的威胁和攻击,也使如何保证 IP 电话、会议系统 SIP 应用系统的安全性和隐私性成为新的研究热点。本文对 SIP 的安全方案进行了讨论,在此基础之上提出了一种新的基于 ECC 的认证方案。

1 SIP 协议及其现有的安全机制

1.1 SIP 协议概述

SIP 是一个可以建立、修改和终止用户会话的应用层协议,它是基于文本的 C/S 结构协议,即用户发送 SIP 请求会话的建立,服务器对此请求作出应答。SIP 定义了如下实体[1,2]:

1) 用户代理(User Agent):用户代理也就是客户机,它又分为两部分,分别是用户代理客户端,负责发起呼叫;用户代理服务器,负责接受呼叫并做出响应。二者组成用户代理存在于用户终端中。当接到 SIP 请求时联系用户,并代表用户返回响应。

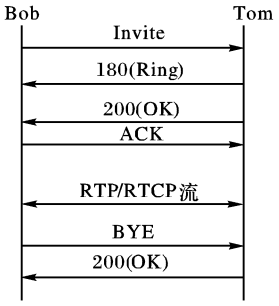

图 1 SIP 呼叫流程

2)代理服务器(Proxy Server):负责接收用户代理发来的请求,根据网络策略将请求发给相应的服务器,并根据收到的应答对用户做出响应。它可以根据需要对收到的消息改写后再发出。

3)重定向服务器(Redirect Server):它接收 SIP 请求,并把请求中的原地址映射成零个或多个新地址,返回给客户机。

4) 注册服务器(Registrar):它接收客户机的注册请求,完成用户地址的注册。

SIP 请求消息包含的三个元素是请求行、头部、消息体。

收稿日期:2006 - 08 - 31;**修订日期**:2006 - 10 - 31

作者简介:李士达(1983 -),男,山东聊城人,硕士研究生,主要研究方向:计算机网络及其应用; 胡玥(1963 -),女,山西太原人,副教授,博士,主要研究方向:自然语言处理、网络安全; 王兴秋(1981 -),女,四川成都人,硕士研究生,主要研究方向:计算机网络安全; 于真(1983 -),女,山东阳谷人,博士研究生,主要研究方向:计算机网络安全.

而 SIP 响应消息包含的三个元素是状态行、头部、消息体。请求行和头部根据业务、地址和协议特征定义了呼叫的本质,消息体独立于 SIP 协议并且可包含任何内容。

SIP 还定义了 INVITE、BYE、OPT10NS、ACK 、REGISTER、INFO 六种方法。

SIP 系统的呼叫流程如图 1 所示。

1.2 SIP 协议面临的攻击问题

基于 SIP 协议的应用系统和其他网络应用一样,主要面临以下形式的攻击:

1)拒绝服务攻击(Denial of Service,DoS)。拒绝服务攻击对网络中的 SIP 代理服务器或者网关,发动未被授权的数据封包炸弹,以停止服务器的正常运作。

2)网络窃听(Eavesdropping)。未经授权地拦截语音数据封包或是 RTP 的媒体数据流,而后将所获得的数据进行解码,窃取信息。

3)封包伪装(Packet Spoofing)。攻击者伪装成合法的使用者来传送资料。

4)重复传递信息(Replay)。攻击者不断重复传送一个合法的伪造信息给被叫方,致使被叫方的 UA 重新处理这个伪造信息。

5)破坏信息完整性(Message Integ—rity)。攻击者在信息数据中插入具有攻击性质的数据,破坏通信双方传送信息的完整性[3]。

1.3 目前 SIP 协议中使用的安全方案

在图 1 中 SIP 请求和应答的 Invite,Via,From 等头部和消息体内部可能包含用户或者服务器的隐私信息。消息头部可以包含通信格式的信息和私人信息或其他私有信息。消息体也可能包含用户信息(媒体类型、编码方式、地址和端口号等),这些信息对系统外实体应该透明。为了在一定程度上保护私有用户的信息,同时为了防止假冒合法用户身份的非法用户建立或修改会话信息,SIP 针对其头部和消息实体信息提供了安全机制。

文献[1]中详细的讨论了目前 SIP 的安全机制,按其功能可以划分为加密机制、鉴别机制和访问控制机制三类安全机制。根据安全机制身份认证的具体实现来讲分为端到端和点到点的认证方法,其中前者包括 S/MIME 机制,HTTP 鉴别机制,后者包括 IPSec 或 TLS 机制。

根据通信时具体情形和认证要求,可以选择以上几种不同的认证机制,但是无论是现在采用端到端还是点到点的认证方法,它们存在不同的缺陷,以 HTTP 鉴别机制为例[4]:

它是一种基于邀请(challenge_based)的机制,当一个服务器收到一个请求的时候,它要求请求的发起方能够证实其自身身份。这个邀请包括一个临时生成的值,此值只用于特定的一次邀请。请求端和服务器端共享一个密码,请求方使用这个密码和上述临时生成的值,来生成一个响应值。请求方再次发送请求,这个请求包括计算出来的响应值,服务器端利用这个响应值来完成请求的认证。使用这种机制可以保证密码从不以明文传送,SIP 的 HTTP 鉴别机制直接应用了这种认证方法,在用户代理服务器端,中间代理服务器端,注册服务器接受一个呼叫,转发一个呼叫,接受注册信息之前,它们要对呼叫端(用户代理客户端)进行认证。用户代理服务器端开始发送一个 SIP 请求信息,当接受到这个请求信息后,被呼叫端发送一个错误的代码来指明需要对呼叫方进行认证。这个错误的信息包括一个邀请和临时值,realm(域,表明允许哪些用户可以接受服务)。呼叫端收到这个要求后,利用其中的信息可以计算出响应值,发送一个包含响应值的新的 SIP 请求消息。

图 2 显示了利用这种机制来进行认证的流程[6]。

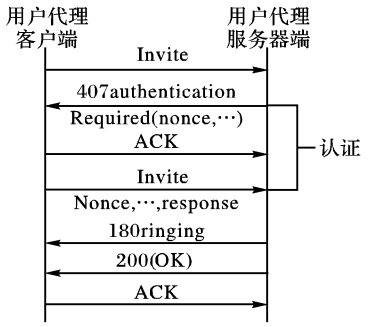

图 2 目前 SIP 采用的基于 HTTP 的认证机制

这种认证方法采取了共享密钥的方法来避免密码以明文传输,但是因为没有应用到公开密钥体制,同样也不能最大限度地保证安全性。面对伪造数据装扮成合法用户攻击类型,这种认证机制显得无能为力。

至于 S/MIME,由于缺乏有效的 PKI 机制,在通信双方第一次交换密钥的时候,S/MIME 包的内容可能被中间人篡改,同时使用 Tunneling SIP 时产生的特长消息也影响了认证效率[5]。不仅是此种鉴别机制,其他鉴别机制也同样具有各自的缺陷,正是基于以上安全问题,本文经过分析试验,提出了一种新型的认证方案即基于 ECC 的 SIP 认证方案。

2 基于 ECC 的 SIP 认证方案及其实施

要解决数据安全问题,对数据加密是一种有效而实用的方法,在数据加密的种种体制中,非对称公钥体制的代表 RSA 加密体制和对称加密体制的代表 DES 体制在特定的范围内均有着各自的特点,椭圆曲线加密作为一种新兴的加密方法,正逐渐在电子商务中成为应用的主流[7]。ECC 不但拥有比 RSA 算法加密速度快、节省时间的特点,与 RSA 一样,作为一种公钥算法, ECC 也可以应用于数字签名,目前已经有部分企业正尝试着将 ECC 技术应用于智能卡、安全数据库等方面。正是因为 ECC 基于 PKI 安全体制所具备的诸多优点[8,9],以及相比其他认证、签名方法所具备的诸多优势,本文将 ECC 的加密算法和签名认证方法引入到 SIP 的通信框架中,较好地解决了 SIP 实体通讯时的安全问题。

本文给出了 SIP 通信时采用基于 ECC 的认证方案进行认证的时刻描述(图 3),并且提供了包括接收方对发送方进行 ECC 认证的具体步骤:

1)Tom 向 Bob 发送 INVITE 请求,请求建立会话连接。

2)Bob 发送 401 状态码给 Tom,提示 Tom 没有认证。

3)Tom 发送 ACK 给 Bob,表示确认消息。

4)发送方对信息进行 Hash 运算,得到一个信息摘要。由于对整个报文实施加密通常不切实际,对于大的数据分组的使用,像 ECC 这样的函数可能也太昂贵了。在这种情况下,可以采用 Hash 函数。Hash 函数有两个重要的特性:①它

的输出一般相对较短,通常为 128 位; ②也是更重要的一点,Hash 函数具有抗碰撞性,即保证不会有两个不同的数据产生相同的摘要,即当 $x \neq y$ 时 $f(x) \neq f(y)$。因此,攻击者不能根据截获到的真正的散列值,构造出欺骗明文并通过鉴别。

图 3　基于 ECC 的 SIP 认证方案流程

5)发送方用自己的椭圆加密算法的私钥(SK)对信息摘要进行加密,得到发送方的数字签名,并将其附在明文信息之后。

6)发送方随机产生一个加密密钥(DES 密钥),并用此密钥对要发送的信息(此时明文信息中已包含发送方数字签名)进行加密,形成密文。

7)发送方用接收方的公钥(PK)对刚才随机产生的加密密钥(DES 密钥)进行加密,将加密后的 DES 密钥连同密文一起传送给接收方。

8)Tom 发送带上述认证信息的 INVITE 请求给 Bob。

9)接收方收到发送方传送过来的密文和加过密的 DES 密钥,先用自己的私钥(SK)对加密的 DES 密钥进行解密,得到 DES 密钥。

10)然后接收方用 DES 密钥对收到的密文进行解密,得到明文的数字信息,再将 DES 密钥抛弃(即 DES 密钥作废)。

11)接收方用发送方的公钥(PK)对发送方的数字签名进行解密,得到信息摘要,同时实现了双向认证的效果。

12)接收方用相同的 Hash 算法对收到的明文再进行一次 Hash 运算,得到一个新的信息摘要。

13)接收方将收到的信息摘要和新产生的信息摘要进行比较。由于单向 Hash 函数具有良好的抗碰撞性,所以如果两份信息摘要内容一致,则可以说明收到的信息没有被修改过。签名验证通过,接收方向发送方发送 200 OK 状态码,表示签名验证通过。

14)Tom 向 Bob 发送 ACK 确认信息。

15)Bob 作为发送方,Tom 作为接收方,重复进行 4) ~ 11)的验证过程。

16)Tom 向 Bob 发送 200 OK 状态码,表示签名验证通过。

17)Bob 向 Tom 发送 ACK 确认信息。

18)双方认证通过后,Tom 重新发送会话邀请。

19)Bob 向 Tom 发送 200 OK 状态码,同意建立会话。

20)Tom 向 Bob 发送 ACK 确认信息。

21)Tom 和 Bob 进行双方通话。

上面的流程仅仅是 SIP 端到端的实体认证过程,在 SIP 的其他实体之间的认证流程同端到端的流程基本一致。例如,跳到跳的认证,即两个代理服务器之间的认证,同样可以采用这种认证方式。因此,基于数字证书的认证方式可以普遍使用在 SIP 网络中,来确认实体的身份。

3　基于 ECC 的 SIP 认证方案的优点

1)ECC 是目前已知的所有公钥密码体制中能够提供最高比特强度的一种公钥密码体制,保证了这种认证方案的安全性,同时与 RSA 相比,可以用少得多的比特大小取得与 RSA 相等的安全性,因此减少了处理开销。

2)在整个过程中,对比较庞大的明文信息使用速度最快的 DES 进行加密,而对于需要保密的 DES 密钥和信息摘要采用强度较高的 ECC 进行加密,这样可以充分发挥 DES 和 ECC 各自的长处,在不降低安全性的情况下,节省了加密的时间,并达到相互认证的效果 。

3)攻击者由于无法获得请求方的私钥,也就无法向其他服务器确认自己的身份,有效地防止注册欺骗攻击、冒充服务器、篡改消息体和中断会话等攻击。

4)本方法不仅可以用来认证,在更进一步认证的基础上可以使用基于数字证书的 SIP 消息体加密机制传输 SIP 消息,这样双重机制保证 SIP 实体不被攻击 。

4　结语

本文提出的基于 ECC 的 SIP 认证方案,结合数字证书认证机制,实现了对 SIP 协议进行呼叫控制过程和数据传送过程中的身份认证,有效地解决了 SIP 网络中存在的安全问题。近年来,随着 SIP 及其应用研究的不断完善,已经受到业界普遍的关注,尤其是 3GPP 将 SIP 选定为未来 3G 全 IP 网络多媒体子系统的控制协议。本文提出的基于 ECC 的 SIP 认证方案,在实现了身份认证的同时由于其具有的最高比特强度,保证了应用时的加密速度和认证效率,具有较高的理论和研究价值 。

参考文献:

[1] ROSEOBERG J, SCHULZRINNE H, CAMARILLO G. SIP: session InitiationProtocol[S]. IETF RFC 3261, June 2002.

[2] HAODLEY M, SCHULZRINNE H, SCHOOLER E, *et al*. SIP: Session Initiation Protocol[S]. IETF RFC 2543, Mar. 1999.

[3] ARKKO J, TORVINEN V, CAMARILLO G, *et al*. Security Mechanism Agreement for the Session Initiation Protocol[S]. RFC 3329 IETF, 2003.

[4] FRAOKS J, HALLAM - BAKER P, HOSTETLER J, *et al*. HTTP Authentication: Basic and Digest Access Authentication[S]. IETF RFC 2617, June 1999.

[5] B. RAMSDELL. S / MIME version 3 message specification [S]. IETF RFC 2633, June 1999.

[6] SALSAOO S, VELTRI L, PAPALILO D. SIP Security Issues: The SIP authentication procedure and its processing load[Z]. IEEE Network, 2002.

[7] 徐秋亮, 李大兴. 椭圆曲线密码体制[J]. 计算机研究与发展, 1999, 36(11): 1281 - 1288.

[8] 刘华, 王琨. 基于 PKI 的 SIP 协议安全的研究[J]. 电子科技, 2005, 2: 37 - 40.

[9] FU D-S, SUN W-J. Realization of data encryption, scheme based on triple DES and ECC[EB/OL]. x//www. tvdiita. com, pp, 2006.