SIP 中基于身份认证的安全机制研究

吕武玲, 黎忠文
(厦门大学 信息科学与技术学院 计算机科学系, 福建 厦门 361005)

摘 要: 因为简单、灵活和易扩展等特点, SIP 将在 3GPP 中得到广泛应用, 但是 SIP 本身缺少有力的安全机制使其面临很多安全威胁。文中对 SIP 中的安全问题和安全性要求进行分析, 为了解决 SIP 中认证和消息加密的问题, 把基于身份认证这种结构简单、应用容易的安全机制引入到 SIP 协议中, 提出了一种新的认证加密方法。采用基于身份的加密机制使系统初始化简单, 不需要繁琐的密钥协商步骤, 并且维护容易。同时满足了 SIP 的安全要求, 保证了会话建立和消息通信过程中的完整性、可靠性和不可抵赖性。

关键词: SIP 协议; 安全; 身份认证
中图分类号: TP393.08 文献标识码: A 文章编号: 1673-629X(2009)02-0158-04

Research on Identity-Based Authentication in SIP

LÜ Wu-ling, LI Zhong-wen
(Dept. of Computer Sci., Sch. of Info. Sci. and Tech., Xiamen Univ., Xiamen 361005, China)

Abstract: SIP will be widely applied in 3GPP, because of its simplicity, flexibility and scalability. But a lack of powerful security mechanism, lead it to face many security threats. In this paper, analyse the issues existed and the requirements needed in SIP security mechanism. In order to solve the problems in SIP authentication and information encryption, proposed a new method about authentication by involving identity-based encryption, a security mechanism which has simple architecture and is easy to apply, to the SIP security mechanism. It makes the construction of the system easier. There is no need of complex steps about key agreement, and it is easy to maintain. At the same time it meets the safety requirements of SIP to ensure that the integrity, reliability and incontestability in the process of session establishment and messaging conversation.

Key words: SIP; security; identity-based authentication

0 引 言

会话发起协议(Session Initiation Protocol, SIP)是由 IETF 提出一个基于应用层的会话控制协议。它的基本功能是创建、修改和终结会话, 也可以邀请参与者加入到一个现有会话, 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, 使 SIP 协议成为实现新一代多媒体通信和软交换的关键技术, 目前 SIP 已经成为 3G 移动网络的多媒体用的协议标准。但由于 SIP 采用文本形式表示消息, 容易被攻击者模仿、篡改, 从而加以非法利用。所以 SIP 的安全机制是目前一个重要的研究领域。

目前 SIP 中提出的安全方案有: HTTP 摘要认证[1], PKI 机制[2], 基于密钥协商的认证方法[3]等。HTTP 摘要是 RFC3261 提出的认证方法, 不过它只提供单向认证, 不能向客户端提供服务器的认证, 无法解决服务器冒充等攻击问题。现在提出的一些改进方法, 有基于 PKI 的认证机制, 但是 PKI 本身实现复杂, 证书撤销、存储、分发、计算等需要耗费很多系统资源, 不容易管理和维护。在一些基于密钥协商的方法中, 步骤繁琐, 需要双方多次交换私有信息来完成双向认证, 并且没有一个完整的体系结构。在文献[4]中把身份认证加入到了 SIP 中, 但是提出的算法只提供了签名的过程, 未加密的消息可能会泄露用户信息, 在文中提出的算法对其进行改进, 在认证的过程中同时完成了密钥协商的问题。

基于身份的加密体制避免了证书的复杂管理, 可以根据系统公开参数还有用户的身份生成公钥。对系

收稿日期: 2008-06-30
基金项目: 福建省 2004 年自然科学基金(A0410004); 厦门大学院士基金(0630-E23011); 厦门大学新世纪优秀人才基金(0000-X07116)
作者简介: 吕武玲(1982-), 女, 硕士研究生, 研究方向为网络与信息安全、SIP 的应用; 黎忠文, 教授, 硕士生导师, 研究方向为网络安全、计算机网络与通信、智能系统可信性保障技术——安全(safety、security)、可靠和容错等。

统成本和运行环境要求不高, 相比之下更具有简单性和灵活性。

1　SIP 及其存在的安全问题和安全性需求

1.1　SIP 概述

SIP 协议分为功能实体、消息及呼叫 3 部分。功能实体包括用户代理(UA), 注册服务器、代理服务器和重定向服务器, 用户代理又可以分为用户代理客户端(UAC) 和用户代理服务器(UAS)。SIP 消息主要有两类: 请求消息(Request) 和响应消息(Response)。请求消息规定了六种基本方法: INVITE、ACK、CANCEL、OPTION、BYE 和 REGISTER。当 UAC 发起呼叫时, 向 UAS 发送一个 INVITE 请求, 从 UAS 接受相应的响应, 然后再发送一个 ACK 消息来确认相应, 这就是会话建立的三次握手。如果希望终止会话可以通过发送 BYE 请求实现[1]。

1.2　SIP 面临的攻击问题

SIP 在制定的过程中没有对通信中的安全性进行全面的考虑, 单纯使用 SIP 进行网络通信, 存在着不安全因素。

SIP 实体间主要存在着以下几个方面攻击和威胁[2]:

(1) 注册欺骗。

SIP 注册机制允许用户代理向注册服务器注册自己当前地址。攻击者可以假冒成授权方来更改地址记录的地址。

(2) 冒充服务器。

SIP 消息通常在 Request- URI 中指定请求的目的域。发送请求时, 用户代理直接与目的域的服务器联系。然而用户代理没有对服务器进行认证, 攻击者有可能冒充远程服务器

(3) 篡改消息体。

SIP 用户代理信任一个代理服务器并通过其发送请求时, 代理服务器并不检查或更改包含在请求中的消息体。如果代理服务器是恶意的, 并且用户代理用 SIP 消息体为媒体会话交换会话的加密密钥时, 恶意代理服务器就有可能修改会话密钥, 发起拦截式攻击或改变原用户代理请求的安全特性。这不仅对会话密钥构成威胁, 还对 SIP 用户的端到端的通讯内容构成威胁。

(4) 中断会话。

一旦会话建立, 任何一方都可以发送修改对话或会话状态的请求。如果第三方在会话建立的初期捕捉到一些原始的会话参数, 攻击者就可以假冒两方中的一方, 在会话中插入 BYE 请求, 中断会话。

1.3　SIP 中的安全需求分析

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: 端到端的安全和逐跳的安全。端到端的安全机制主要有两种: 认证和数据加密; 逐跳的安全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, 主要还是依赖网络层(IPSec) 或传输层(TLS) 的安全。这里主要讨论端到端的安全机制[5]。

(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。

(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。一般都是通过使用对称加密算法实现, 需要解决的是密钥协商问题。保证了数据的机密性。

2　基于身份的公钥密码体制

2.1　概　述

在 1984 年的美洲密码年会上, Shamir 提出一种新颖的公钥密码系统。在他的密码系统中, 用户的公钥(public- key) 可以是任何一个与主体身份有关的比特串, 而私钥是通过一个可信的权威机构(a trust authority, TA) 来生成的:

private- key= F(master- key, public- key)

其中 master- key(主密钥) 是 TA 独有。TA 就用这个主密钥来生成系统中所有用户的私钥, 并通过可信通道发送给用户[6]。

2.2　Weil 配对简介

Weil 配对记为 $\hat{e}$, 是双线性映射, 满足下列性质[7]:

1) 反对称性: $\hat{e}(P, P) = 1$

2) 双线性性: $\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$; $\hat{e}(nP, Q) = \hat{e}(P, Q)^n = \hat{e}(P, nQ)$

3) 非退化性: $\hat{e}(P, Q) \neq 1$, $\hat{e}(Q, P) \neq 1$

4) 可计算性: 对所有阶为 p 的点 P、Q, 可在多项式时间内计算出 $\hat{e}(P, Q)$ 和 $\hat{e}(Q, P)$。

2.3　利用椭圆曲线 Weil 对的公钥签名体制

该系统包括了四个主要的算法[7]。

(1) 系统初始化算法: TA 初始化设置系统参数 $(G_1, G_2, \hat{e}, n, P, P_{pub}, f, h)$, 并将其公开。而保持主密钥 s 为系统私钥。

(2) 用户私钥生成算法: 设 ID 表示用户的身份, 计算用户公钥 $Q_{ID} = f(ID)$ 和用户私钥 $d_{ID} = sQ_{ID}$。

(3) 签名算法: 用私钥 d_{ID} 对明文信息 m 的摘要加密生成签名, 附加在消息后面。

(4) 认证算法: 用公钥 Q_{ID} 对签名解密, 返回 T 或 F。

3 基于身份认证的 SIP 安全机制

前面已经介绍了基于身份认证算法以及 SIP 的安全性要求, 基于身份认证具有诸多优点, 简单灵活, 实现维护都比较容易, 属于公钥密码体制, 可以用来加密也可以用来签名。文中把基于身份的加密算法和签名认证方法引入到 SIP 通信框架中, 较好地解决了 SIP 实体会话建立和通讯中的安全问题。在认证的同时进行了密钥协商, 可以作为对数据进行对称加密的密钥。

3.1 认证方法的描述

下面以 Alice 和 Bob 之间建立会话为例, 给出了基于身份认证方案认证过程的描述图(见图 1), 并提供了基于身份认证的 SIP 安全机制的具体步骤:

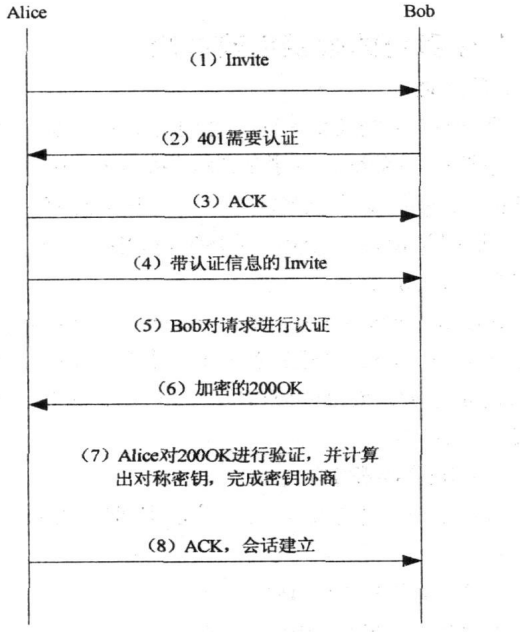

图 1 认证过程描述图

1) Alice 向 Bob 发送一个 Invite 请求, 请求建立会话连接。

2) Bob 发送 401 响应消息给 Alice, 提示 Alice 需要认证。

3) Alice 收到 Bob 需要认证的消息, 发送 ACK 给 Bob, 表示确认消息。

4) Alice 重新发送请求信息。发送的消息为 m, 对 m 进行 hash, 得到消息摘要 $m' = h_0(m)$, Alice生成一个随机数 r, 并用 Alice 的私钥 d_{Alice} 对 m' 加密得 $c_0 = \text{Encrypt}_{(d_{Alice},P)}(m')$, $c_0 = < rP_{pub}, m' \oplus h(\hat{e}(d_{Alice}, rP)) >$。计算加密密码 $k = \hat{e}(rd_{Alice}, Q_{Bob})$, 采用对称加密算法(如 DES) 对消息 $< m, c_0 >$ 进行加密得 $c_1 = Ek_{(k)}(< m, c_0 >)$。向 Bob 发送消息 $< c_1, rQ_{Alice} >$。

5) Bob 接受到消息 $< u, v >$, 计算:

$$k' = \hat{e}(v, d_{Bob}) = \hat{e}(rQ_{Alice}, sQ_{Bob}) = \hat{e}(r(sQ_{Alice}), Q_{Bob}) = \hat{e}(rd_{Alice}, Q_{Bob}) = k$$

得到Alice 加密消息的对称密钥, 用该密钥对 u 进行解密, 解密后得消息 $< x, y, z >$, 用 Alice 的公钥对 z 进行解密得消息摘要:

$$\begin{aligned} m_0 &= z \oplus h(\hat{e}(Q_{Alice}, y)) \\ &= m' \oplus h(\hat{e}(d_{Alice}, rP)) \oplus h(\hat{e}(Q_{Alice}, rP_{pub})) \\ &= m' \oplus h(\hat{e}(Q_{Alice}, P)^{rs}) \oplus h(\hat{e}(Q_{Alice}, P)^{rs}) \\ &= m' \end{aligned}$$

验证 $m_0 = h_0(x) = h_0(m)$ 是否成立。如果相等说明请求是 Alice 发出并且消息没有被篡改。

6) Bob发送 200Ok 消息给 Alice, 随机产生 r', 消息的加密过程同上, 发送加密消息和 $r'Q_{Bob}$ 给 Alice。这样能对服务器进行认证, 防止服务器假冒攻击。

7) Alice 对 200OK 消息进行认证, 认证方法同(5), 并且计算密钥 $K = \hat{e}(rQ_{Alice}, r'Q_{Bob})$ 作为 Alice 和 Bob 的共享密码。可以用来对会话建立后通信的数据进行加密。

8) Alice 认证消息是从 Bob 发送的, 向 Bob 发送 ACK 消息, 会话建立成功。

3.2 安全机制比较与安全性分析

文中描述的方案具有结构简单、实现容易等特点, 只用了两条消息, 通过 Alice 向 Bob 发送加密的 Invite 请求和 Bob 向 Alice 发送加密的 200OK 消息就进行了双向认证, 并完成了密钥协商。不需要对证书进行复杂的维护和管理, 比传统的密钥协商机制步骤简单, 而且有 TA 的参与构成一个整体的系统, 结构清晰。

在 SIP 中存在注册欺骗、冒充服务器、篡改消息体和中断会话等主要安全问题。文中提出的认证方案, 在注册和会话建立的过程中, 用户代理和服务器之间进行了双向认证, 所以解决了注册欺骗和冒充服务器这两个问题。另外对发送的消息进行签名后又对整个消息进行加密, 使消息对其他用户不可见, 所以解决窃听和篡改消息等问题。对所有发送的消息都要进行判断是否是期待的用户发送的, 所以非合法用户发送的任何请求都会被拒绝, 当然包括中断会话请求。

首先对发送的请求消息用 Alice 的私钥加密的签名, Bob 可以通过 Alice 的公钥来认证消息是否是 Alice 发出的, 同时签名能保证消息的完整性, 然后用协商的共享密钥对发送的消息和签名加密, 保证了数据的保密性, 满足了 SIP 的安全性要求。

4　基于身份认证安全机制问题与解决方法

基于身份认证中的私钥是由 TA 生成, 所以并不是只有用户才知道自己的私钥, 密钥托管的问题与生俱来, 这样就存在一些安全隐患, 比如说主密钥泄漏将引起整个系统崩溃等, 恶意的 TA 可以伪造任何用户的签名。

另外私钥与证书一样需要一定的有效期, 这里对私钥的更新也是需要研究的一个问题。

4.1　密钥托管问题

因为私钥是集中产生后分发给用户, TA 知道所有用户的私钥。为了解决这个问题, 可以构造一种新的实体 PKG(Private Key Generator) 用来生成并分发用户私钥。

系统可以分成不同的安全域, 每个域内会有一个 PKG_i 用来为用户生成部分私钥 s_iQ_{ID}, s_i 为 PKG_i 的主密钥。域内的通信定义为安全的, 域间的通信可以用发送方和接收方的PKG协同生成用户私钥 $d_{ID}= s_iQ_{ID}+ s_jQ_{ID}$, 只有两个 PKG 共谋时才能知道用户的私钥, 增加了密钥的机密性, 一个 PKG 受到攻击时也不会使整个系统崩溃[8]。

采用多个 PKG 共同生成用户私钥的方法, 安全性的提高和计算复杂度的增加是成正比的, 这里采用了一种折中的办法。简单的证书由 TA 颁发只有在向 PKG 申请的部分私钥是才会用到, 用来证明用户的合法身份[9]。

4.2　密钥管理

对于私钥的管理, 在 PKI 机制中注销和更新证书过程还是相对复杂, 工作量很大的。同一个私钥用的时间过久会降低安全性, 而且对于 SIP 系统中的用户代理对服务的使用权需要有一定的有效期, 所以密钥更新是系统需要解决的一个问题。

在文中提到的系统中密钥是根据用户身份和主密钥共同生成的, 如果重新生成主密钥将会导致整个系统私钥的变化, 但是用户的身份也是广播到各个用户, 变化起来也会比较麻烦。在文献[8] 中描述了一种解决方法, 可以把有效期写在 ID 后面用来生成公钥, $Q_{ID} = h((ID, current- year))$, 再根据公钥生成私钥, 超过有效期的私钥就不起作用, 用户需要重新向 PKG 申请新的私钥。应用在 SIP 中可以在 SIP 头中添加一个表示有效期的头字段, 在发送请求消息的同时把有效期传递给目标服务器。这种方案使私钥的管理简单方便, 减轻了密钥管理的负担, 同时增强了系统的安全性。

5　结束语

介绍了 SIP 协议的安全需要, 基于身份认证的原理和特点, 提出了一种基于身份加密的 SIP 认证方案, 保持了基于身份认证的结构简单、维护容易等特点, 不需要复杂的证书管理和维护。对于身份认证本身固有的密钥托管问题, 提出了一种简单的缓解方案。提高了 SIP 的安全性能, 同时又能保持系统的高效性。

参考文献:

[1] Roseoberg J, Schulzr I H, Camar I G. SIP: Session Initiation Protocol[S]. IETF RFC 3261, 2002.

[2] 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.

[3] 李士达, 胡　玥, 王兴秋, 等. 一种基于 ECC 的SIP 认证方案的提出与实现[J]. 计算机应用, 2007, 27(2): 311- 313.

[4] 庞红玲, 安　可, 戎锋洪. 基于身份加密系统的 SIP 认证机制[J]. 信息安全与通信保密, 2007(5): 133- 135.

[5] 金康双, 王泽兵, 冯　雁, 等. SIP 协议的认证机制及其性能分析[J]. 计算机应用研究, 2004(8): 110- 112.

[6] Shamir A. Identity- based Crypto Systems and Signature Schemes[C]//Advance in Cryptology- crypto'84. Germany: Springer- Verlag, 1984: 47- 53.

[7] Boneh D, Franklin M. Identity- based Encryption from the Weil Paring in Advance[C]//Cryptology- Crypto'01. Germany: Springer- Verlag, 2001: 213- 229.

[8] 徐茂智, 游　林. 信息安全与密码学[M]. 北京: 清华大学出版社, 2007.

[9] 李新国, 葛建华, 赵春明. IBE 公钥加密系统的用户私钥分发方案[J]. 西安电子科技大学学报: 自然科学版, 2004, 31(4): 569- 573.

(上接第 157 页)

dicting intruder's next goal with Hidden Colored Petri- Net Computer Networks[J]. The International Journal of Computer and Telecommunications Networking, 2007, 51(3): 632- 654.

[11] 穆成坡, 黄厚宽, 田盛丰, 等. 基于模糊综合评判的入侵检测报警信息处理[J]. 计算机研究与发展, 2005, 42(10): 1679- 1685.

[12] 龚　俭, 梅海彬, 丁　勇, 等. 多特征关联的入侵事件冗余消除[J]. 东南大学学报, 2005, 35(3): 366- 371.

[13] 段海新, 于雪利, 王兰佳. 基于地址关联图的分布式 IDS 关联算法[J]. 大连理工大学学报, 2005, 45(10): 126- 131.