基于SIP协议的安全网关设计

蒋 华[1,2],杨 磊[1],胡荣磊[2]
(1.西安电子科技大学,陕西 西安 710100;
2.北京电子科技学院,北京 100070)

摘 要:SIP(会话传输协议)是基于文本的传输协议,信令发起简单,使用方便,是下一代通信网的核心协议之一,近年来得到了很大的应用。然而由于SIP协议的设计之初没有考虑到安全性问题,导致SIP协议在应用中很容易受到安全威胁。所以文中针对SIP协议面临的安全威胁进行研究,结合基于椭圆曲线的自证明公钥密码算法,提出一种解决方案;结合此方案设计一种安全网关,该网关拥有SIP代理服务器的功能,任何SIP终端用户都可以方便地接入进来,从而有效提高了SIP网络的机密性、完整性、不可否认性。

关键词:会话传输协议;SIP代理服务器;椭圆曲线;自证明公钥密码算法;安全网关
中图分类号:TP302.1 **文献标识码**:A **文章编号**:1673-629X(2015)07-0120-04
doi:10.3969/j.issn.1673-629X.2015.07.026

Design of Security Gateway Based on SIP

JIANG Hua[1,2], YANG Lei[1], HU Rong-lei[2]
(1. Xidian University, Xi'an 710100, China;
2. Beijing Electronics Science and Technology Institute, Beijing 100070, China)

Abstract: SIP is a transfer protocol based on the text, signaling simply, easy to use, is one of the core of the next generation network protocol, which has great application. However, as the SIP doesn't take into the security issues account at the beginning of design, SIP protocol is vulnerable to security threats in the application. Therefore, aiming at the security threats faced by SIP, combined with self-certified public key cryptographic algorithm based on the elliptic curve, put forward a kind of solution to solve the problem. Then design a security gateway combined with the solution. The gateway has a function of SIP proxy-server, and any SIP-user can access to it conveniently, thus effectively improving the confidentiality, integrity, non-repudiation for SIP network.

Key words: SIP; SIP-proxy server; ECC; self-certified public key cryptographic algorithm; security gateway

0 引 言

利用互联网进行实时通信已经发展成一种成熟的技术并且正在走进人们的生活;包括数据、语音和视频的多媒体实时通信是当今通信科技发展的一个热点,作为下一代通信网的热点问题,SIP协议结构简单、使用方便,受到了业界的支持。然而,IETF最初在设计SIP协议时重点是过分强调了协议的简洁性和便利性,没有注意到协议的安全性问题,因此使得SIP技术应用所带来的安全问题十分突出[1]。基于安全方面的考虑,设计一个基于SIP协议的多终端接入安全网关有一定的应用价值[2]。

1 安全网关系统架构

1.1 SIP基本呼叫流程和安全威胁

(1)SIP协议的完整流程。

用户代理服务器:此代理为发起呼叫的终端设备,分为用户代理客户机(UAC)和用户代理服务器(UAS)。用户代理客户及创建、发送请求并且接收、处理请求的应答消息。UAS接收、处理UAC的请求并且创建、发送应答消息[3]。

代理服务器:用于接收和转发请求。根据获得的SIP消息路由,转发下一跳数据。

注册服务器:接收数据,并且存储注册的信息,以供代理服务器、重定向服务器查询使用。

收稿日期:2014-08-05 **修回日期**:2014-11-06 **网络出版时间**:2015-06-23
基金项目:中办信息安全与保密重点实验室、北京市教委共建专项基金资助项目(YZDJ0804)
作者简介:蒋 华(1962-),男,教授,硕士生导师,研究方向为VoIP网络安全、宽带通信;杨 磊(1987-),男,硕士研究生,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150623.1031.022.html

重定向服务器:实现 NAT 穿越,一般在公网上,用于用户数据的转发[4]。

SIP 数据包中包含建立会话的 IP 地址和端口号,这些信息在穿越 NAT 时变得无效,IP 地址是系统的内网地址,两个 SIP 终端之间不能通过这些 IP 地址互相找到对方,所以在设计系统时启用了代理服务器和网络服务器[5],网络拓扑图如图 1 所示。SIP 终端向 SIP 代理服务器首先注册自己的 IP 地址和端口号,SIP 代理服务器通过 Internet 网络向网络 SIP 服务器注册自己的 IP 地址和端口号;采用这种模式,由于网络服务器采用的是公网地址,因此每个 SIP 代理服务器都能够发现它的地址,通过网络服务器实现 NAT 的穿越功能;而采用 SIP 代理服务器,任何的 SIP 终端都可以接入到 SIP 代理服务器,实现了系统的多终端接入模式并且增强了系统的可扩展性[6]。

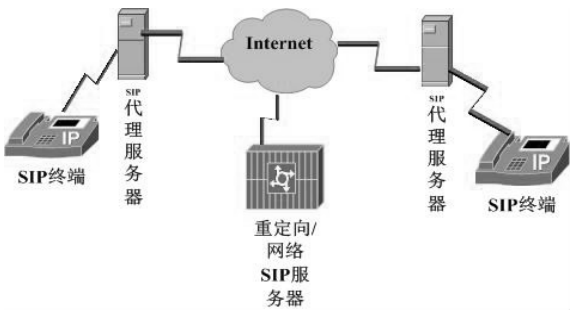

图 1　SIP 网络系统原型方案

(2)安全威胁。

注册攻击:用户向注册服务器/SIP 代理服务器注册时,攻击者可以取消原来已有的合法用户的注册,冒充原来的用户,这样攻击者就可以发送自己所有的请求了。

伪装代理服务器/重定向服务器:用户注册时发往服务器的消息被拦截,然后假冒一个服务器让用户发送消息,以此用来窃取用户信息。

篡改消息:修改 SIP 消息体从而扮演中间人进行攻击。

DOS 攻击:攻击者伪造一台主机的 SIP 消息,然后把消息大量的发送给其他的 SIP 用户终端和服务器,造成系统瘫痪。

1.2　解决方案框架设计

针对以上安全威胁进行分析,SIP 消息面临着机密性、不可否认性、完整性、可靠性等方面的安全威胁,通用的 SIP 协议的两种安全机制分别是身份认证和数据加密。认证主要用来确保合法身份,确保信息的可靠性和完整性;认证用到的密码协议有数字签名、HASH 算法等,一般使用公钥密码;为确保数据的安全性,一般都是使用分组密码算法进行加密的。

由于本设计考虑的是 SIP 终端只是普通的多媒体接入设备,因此,只要两个安全网关之间进行了必要的认证和数据加密,那么所有能接入到安全网关的终端设备进行通信时都能确保数据传输的安全性。

图 2 是在图 1 的基础上扩展的。在图 1 的基础上,对 SIP 代理服务器进行修改,增加身份认证和数据加密等安全性方案的功能,实现 SIP 消息的安全保护,把 SIP 代理服务器和安全性方案结合在一起,使之成为一个安全网关,结合 KDC(密钥分发中心)第三方权威机构,确保 SIP 消息在传输过程中的机密性、完整性和不可否认性。安全网关的方案设计在下一节提出[7]。

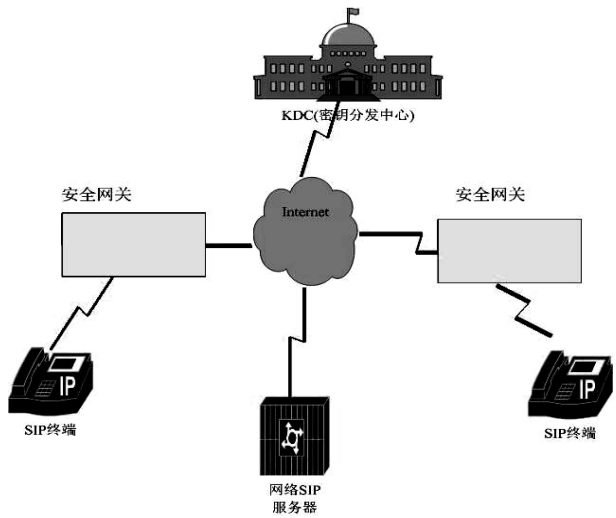

图 2　基于 SIP 协议的安全网关原型系统

2　安全方案设计

由于椭圆曲线密码方案能够比 RSA 等方案使用更小的密钥并提出更好的安全性,所以选择椭圆曲线而不是 RSA 或者其他方案。

2.1　椭圆曲线密码学

椭圆曲线是指由韦尔斯特拉斯(Weierstrass)方程:$y^2 + a_1xy + a_3y = x^3a_2x^2 + a_4x + a_6, a_i \in F_q$ 所确定的曲线。有限域 F_q 可以是以素数为模的整数域,或是特征为 2 的伽罗华域。椭圆曲线密码学(Elliptic Curve Cryptography,ECC)是基于椭圆曲线的公钥密码方法。在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的,ECC 的安全性依赖于有限域上椭圆曲线加法群的离散对数问题的困难性[8]。

离散对数问题(Discrete Logarithm Problem,DLP)定义为:给定一个素数 p,Z_q^* 的一个生成元 α 和一个元素 $\beta \in Z_q^*$,求解整数 x,$0 \leqslant x \leqslant p-2$,使得 $\alpha^x = \beta(\mathrm{mod}p)$。

椭圆曲线上的离散对数问题(Elliptic Curves Discrete Logarithm Problem,ECDLP)定义为:给定有限域 F_q 上的椭圆曲线 E,点 $p \in E(F_q)$ 的阶为 n,对于点 Q

$= lp, 0 \leqslant l \leqslant n-1$,确定 l 的问题。与 DLP 相比,ECDLP 的安全性更高,因为 ECDLP 问题的计算复杂度为全指数时间,DLP 问题的计算复杂度为亚指数时间。

2.2 基于 ECC 的自证明公钥生成算法

鉴于椭圆曲线安全性高,设计一种基于 ECC 的自证明公钥的密码系统,来实现 SIP 的认证功能。该方式需要一个第三方权威机构 KDC(密钥分发中心)[9]。

首先,选定大素数 p 和三次方程 $y^2 = x^3 + ax + b$ 的参数 a 和 b,确定椭圆曲线群 $E_p(a,b)$,设阶为 n 的元素 $G = (x_G, y_G)$ 作为生成元,n 为大素数,此生成元称为基点。用基点 $G = (x_G, y_G)$ 的所有倍点构成一个子群,$E_p(a,b)$ 的子群 $S: S = \{G, 2G, \cdots, nG\}$,就可以很简单地得到椭圆曲线的 5 个参数 $\{a,b,G,n,p\}$。$\mathrm{sk_{KDC}}$ 为密钥分发中心的私钥,$\mathrm{PK_{KDC}} = \mathrm{sk_{KDC}} \cdot P$ 为 KDC(密钥分发中心)的公钥,$h(*)$ 为消息摘要函数,$X(*)$ 函数表示取椭圆曲线上点的横坐标;KDC(密钥分发中心)公布 $a,b,G,n,p,\mathrm{PK_{KDC}}$ 与 h,秘密保存 $\mathrm{sk_{KDC}}$ 作为私钥。

其次,生成公私钥对:用户 U_i 向 KDC 注册。

第 1 步:用户 U_i 完成以下任务:

(1)产生一个随机数 $x_i \in [2, n-2]$。

(2)计算用户自身的身份信息为 $I_i, V_i = h(I_i \| x_i) \cdot G$。

(3)将 (I_i, V_i) 传输给 KDC(密钥分发中心)。

第 2 步:KDC 接到消息后,进行如下运算:

(1)随机产生一个随机数 $x_i \in [2, n-2]$。

(2)计算用户 U_i 的自证明公钥 $\mathrm{TP}_i = kG_i + V_i = kG_i + h(I_i \| x_i) \cdot G$,并且证明 $w_i = (I_i \cdot k_i - X(\mathrm{TP}_i) \mathrm{sk_{KDC}}) (\mathrm{mod}n)$。

(3)将 (TP_i, w_i) 发送给用户 U_i。

第 3 步:用户 U_i 完成以下任务:

(1)推导私钥 $s_i = (w_i + h(I_i \| x_i) \cdot I_i) (\mathrm{mod}n)$。

(2)验证自证明公钥 TP_i:$s \cdot G_i = I_i \cdot \mathrm{TP}_i - X(\mathrm{TP}_i) \cdot \mathrm{PK_{KDC}}$。用户得到初始自证明公钥与私钥为 (TP_i, s_i)。对以上验证等式的证明如下:

$$
\begin{aligned}
s_i \cdot G &= (w_i + h(I_i \| x_i) \cdot I_i) (\mathrm{mod}n) \cdot G = \\
&I_i \cdot k_i \cdot G - X(\mathrm{TP}_i) \cdot \mathrm{sk_{KDC}} \cdot G + \\
&h(I_i \| x_i) \cdot I_i \cdot G = I_i \cdot (k_i \cdot G + \\
&h(I_i \| x_i) \cdot G) - X(\mathrm{TP}_i) \cdot \mathrm{PK_{KDC}} = \\
&I_i \cdot \mathrm{TP}_i - X(\mathrm{TP}_i) \cdot \mathrm{PK_{KDC}}
\end{aligned}
$$

用户私钥的随机性较强,安全性响应的就越高。

基于自证明公钥用户自主更新的思想,采用在随机预言模型(ROM)下被证明为安全的 Schnorr 签名算法,得到基于 ECC 的用户更新自证明公钥。

用户 U_i 得到初始密钥 (TP_i, s_i) 后执行以下算法,生成新密钥。

(1)选择一个随机数 $t_i \in [2, n-2]$;

(2)计算 $T_i = t_i \cdot G$;

(3)推导出新私钥:$s_i' = (s_i \cdot h(I_i \| X(\mathrm{TP}_i \| X(T_i))) + t_i) (\mathrm{mod}n)$。

新的自证明公钥为 (TP_i, T_i),再次更新时,只需变换随机数 T_i,使用同样的算法在初始公私钥 (TP_i, s_i) 的基础上进行更新[10]。

2.3 认证、数字签名、密钥分配和加解密算法实现

通过 2.2 的分析,系统为每个用户都产生了一个公私钥对 $(\mathrm{TP_{usr}}, s_{\mathrm{usr}})$。

结合 SIP 消息流,SIP 协议的认证流程如图 3 所示。

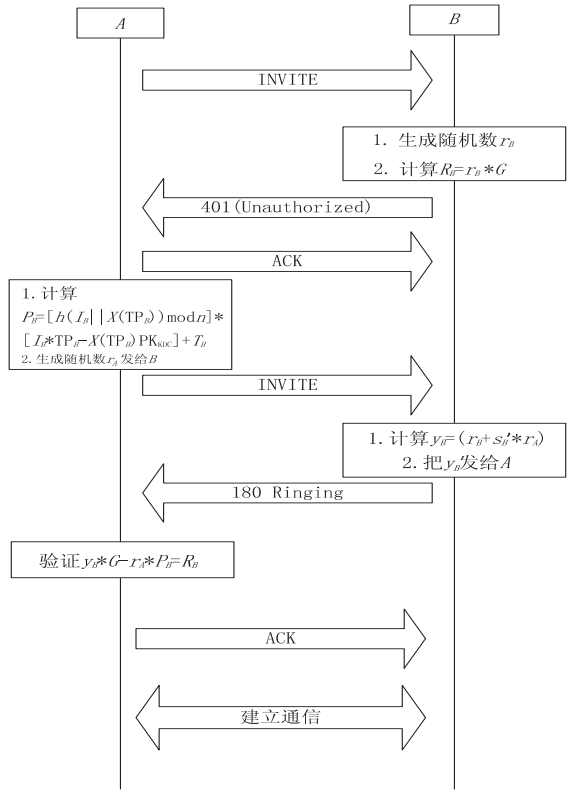

图 3 消息认证示意图

(1)A 向 B 发起 INVITE 请求;

(2)B 接到请求后,生成随机数 r_B,并计算 $R_B = r_B \cdot G$,且向用户 B 发送自己的公开信息 $(I_B, \mathrm{TP}_B, T_B)$ 和 R_B;然后向 A 发送一个错误的 SIP 响应消息表示挑战,响应代码为 401;

(3)A 向 B 发送 ACK 请求消息,表示成功接收到挑战;

(4)A 利用 $(I_B, \mathrm{TP}_B, T_B)$ 计算 $P_B = [h(I_B \| X(\mathrm{TP}_B)) \| \mathrm{mod}n] \cdot [I_B \cdot \mathrm{TP}_B - X(\mathrm{TP}_B) \cdot \mathrm{PK_{KDC}}] + T_B$,并且选择随机数 r_A 发给 B;

(5)用户 B 计算 $y_B = (r_B + s_B' \cdot r_A) (\mathrm{mod}n)$ 并将 y_B 发给 A;

(6) A 验证 $y_B \cdot G - r_A \cdot P_B = R_B$;证明:

$$y_B \cdot G - r_A \cdot P_B = [(r_B + s_B' \cdot r_A) \bmod n] \cdot G - r_A \cdot P_B = r_B \cdot G + (s_B' \cdot r_A \bmod n) G - r_A \cdot (s_B' \cdot G) = R_B$$

本协议是基于离散对数的协议,并且利用了盲签名协议的思想,所以盲签名的安全性在协议中也能体现出来,并且算法是基于椭圆曲线离散对数问题和哈希函数的单向求逆问题,能抵抗目前 SIP 协议面临的许多安全威胁,有比较强的工程实践意义[11]。

数字签名的实现方案如下:

(1)用户 A 向 KDC 去认证自己的公钥,首先用私钥加密自己的消息 ID 发给 KDC,KDC 用 A 的公钥解密消息,用私钥 sk_{KDC} 对 A 发送的消息和 A 的公钥进行加密生成数字证书 CER,然后发送给用户 A 。

(2) A 给 B 发送消息 M 时,对消息用摘要函数计算,然后用自己的私钥进行签名,把签名信息和消息 M 和证书一起发送给 B 。

(3) B 收到消息后,用 KDC 的公钥 PK_{KDC} 解开数字证书,拿到 A 的公钥,未经修改和欺骗后的,然后验证,防止伪造和篡改[12]。

密钥分配实现方案如下:

(1) A 产生一个随机数 n_1,并用 B 的公钥加密 n_1 和 ID_A ,然后发送给 B 。

(2) B 收到后用 B 的私钥解密得出 ID_A 和 n_1,确定消息是由 A 发出的; B 把消息 n_1,ID_A 和自己产生的随机数 n_2,自己的消息 ID_B 用 A 的公钥加密,然后发送给 A 。

(3) A 收到消息后用 A 的私钥解密出消息 ID_B,n_2,n_1,ID_A ,确认消息是由 B 发出的。

(4) A 计算 $K_{mes} = n_1 n_2$ 作为会话密钥,用 A 的私钥进行加密,然后用 B 的公钥进行加密,得到的信息发送给 B 。

(5) B 接到消息后用 B 的公钥进行解密,并用 A 的公钥进行解密,得出会话密钥 $K_{mes} = n_1 n_2$。

密钥分配以后,通信双方 A , B 都得到了会话密钥,就可以进行加解密通信了。数据加密一般使用分组密码进行加密,分组密码比较常用的有 DES,AES,SM4 等,分组密码实现起来比较简单。

(1) A 把需要发送的消息通过分组密码加密后发送给 B ;

(2) B 解密出数据;

(3)然后 B 发送加密后数据给 A ,完成会话。

3　结束语

首先 SIP 协议的消息会话模型设计了安全网关原型系统,在系统中,安全网关既有 SIP 代理服务器的作用,又有认证和密钥协商和数据加密的功能;系统的认证和加密都是安全网关通过网络 SIP 服务器进行的,SIP 多媒体通信终端只是一个接入设备,一个安全网关可以同时接入多个不同的 SIP 多媒体通信终端,为应用提供了很大的便利性[13];同时,采用基于 ECC[14] 的自证明公钥认证和密钥协商,确保了在通信过程中的安全性。该系统能有效抵抗 SIP 网络常见的攻击,例如重放攻击、拒绝服务攻击、中间相遇攻击、电子欺骗等,不足之处在于只对系统的安全性进行了简要的理论分析,且系统的安全性很大程度上依赖于算法的安全性。

参考文献:

[1] Endler D. 黑客大曝光:VoIP 安全机密与解决方案[M]. 北京:电子工业出版社,2010.

[2] 宋秀红,肖宗水,魏本见. 基于 SIP 的 VoIP 网络中 DoS 攻击的分析与研究[J]. 计算机工程与设计,2008,29(10):2479-2482.

[3] Subramanian S V, Dutta R. Measuring SIP proxy server performance[M]. Raleigh:Cisco Systems, Inc,2013.

[4] 李　卿,乔元松,郑　慧. SIP 穿越防火墙/NAT(-PT)的探讨和设计[J]. 计算机工程与设计,2005,26(5):1294-1298.

[5] 李　杨,熊淑华,李梦涵,等. 基于 SIP 协议的实时通信系统研究与实现[J]. 计算机技术与发展,2014,24(4):53-56.

[6] 姜秀玉,杨　峰,崔再惠. SIP 协议实现中消息解析的研究[J]. 计算机工程与设计,2010,31(13):2988-2991.

[7] 储泰山,潘雪增. SIP 安全模型研究及实现[J]. 计算机应用与软件,2004,21(12):101-104.

[8] 杨　波. 现代密码学[M]. 北京:清华大学出版社,2003.

[9] 肖攸安,周祖德. 一种基于椭圆曲线的高效自证明密钥分配协议[J]. 大连海事大学学报:自然科学版,2007,33(4):56-59.

[10] 闫晓芳,苏锦海,查　俊. 一种新的 ECC 自证明公钥生成算法[J]. 计算机工程,2011,37(4):128-130.

[11] Pear C. 深入浅出密码学:常用加密技术原理与应用[M]. 北京:清华大学出版社,2012.

[12] Salomaa A. Public-key cryptography[M]. 2nd ed. [s. l.]: Springer-Verlag,1996.

[13] Zhou Jin, Li Jie, Xia Yinben, et al. SIP network discovery by using SIP message probing[C]//Proc of network operations and management symposium. Salvador:IEEE,2008:791-794.

[14] Athavale A, Singh K, Sood S. Design of a private credentials scheme based on elliptic curve cryptography[C]//Proc of first international conference on computational intelligence, communication systems and networks. [s. l.]:[s. n.],2009:332-335.

基于SIP协议的安全网关设计

作者： 蒋华， 杨磊， 胡荣磊， JIANG Hua， YANG Lei， HU Rong-lei

作者单位： 蒋华,JIANG Hua(西安电子科技大学，陕西 西安 710100；北京电子科技学院，北京 100070)， 杨磊,YANG Lei(西安电子科技大学,陕西 西安,710100)， 胡荣磊,HU Rong-lei(北京电子科技学院,北京,100070)

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2015(7)