基于环签名的 SIP 认证方案设计

蒋 华[1,2],潘文吉[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:针对在使用公共网络资源情况下,中小型企业采用 SIP 构建的 Presence/IM 业务存在的注册劫持和注册删除的隐患,提出了一种基于 RSA 和 DES 结合的环签名安全匿名认证方案。方案首先构建一个可信域,公开域内的所有用户的公钥,然后在 SIP 的注册和注销过程中添加环签名认证,在整个过程中,不需要第三方参与验证,用户对于服务器是匿名的,服务器只能判断请求是否来自可信用户群,而无法从签名中获得用户身份。相比于其他常用的安全认证,环签名除了能够有效认证签名的合法性,无条件的匿名性也可以保护用户信息,在云计算等公共网络环境中减少用户信息的泄露,同时具有部署效率高,证明过程便捷的优势。最后通过运算证明方案的正确性,构建安全模型说明了方案的安全性和可行性,并采用 OpenSSL 验证方案的效率。

关键词:会话初始协议;身份认证;环签名;RSA;DES
中图分类号:TP302.1 **文献标识码**:A **文章编号**:1673-629X(2016)03-0140-04
doi:10.3969/j.issn.1673-629X.2016.03.033

Design of SIP Authentication Scheme Based on Ring Signature

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

Abstract: Under the public network, the Presence/IM established by small and middle sized enterprises with SIP exists the risks of registration hijacking and registration deleting. Aiming at this hidden danger, a security authentication scheme using ring signature based on a combination of RSA and DES is proposed. First, it builds a trusted domain and public the public key to the users in the domain. Then the scheme adds the ring signature to SIP registration and deregistration process, without the third party. For the server, users are anonymous and just knew in the domain. Compared with other security authentication, the ring signature not only ensures the legality of users, but also provides anonymity to protect user information, which will be reduced in the cloud and other public network. At the same time, it has efficient deployment and convenient proof. Last, it proves the correctness by computing in this paper, also shows the safety and feasibility by building security model. In addition, the efficiency of the scheme is verified by using OpenSSL.

Key words: SIP; authentication; ring signature; RSA; DES

0 引 言

SIP(Session Initiation Protocol,会话初始协议)是由 IETF 提出作为 IP 通信的语音协议,是目前 VOIP 领域应用最多的协议。2011 年公安部科技信息化局制定了标准 GB/T 28181-2001,提出了视频监控联网安全的技术要求,其中就采用了 SIP 协议为准则,之后的许多视频监控方案[1]也都采用了 SIP 作为会话协议。

然而 SIP 的完整性、可用性和机密性都存在问题[2]。由于是基于文本传输的协议,SIP 的认证继承了 HTTP 摘要认证,是一种挑战-响应的认证协议,而这种方式有两种致命的隐患:一个是 SIP 文件的头信息和参数缺乏保护;二是需要在服务器上预先存储用户的配置要求。

有研究者提出了一个 SIP 域信任的认证机制[3],但其解决方案主要针对于入侵检测。文中采用了环签名方式进行信任域构建,然后使用域内成员公钥和自

收稿日期:2015-06-14 **修回日期**:2015-09-17 **网络出版时间**:2016-02-18
基金项目:中央办公厅基本科研业务费(2015XS1-HRL)
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;潘文吉(1990-),男,硕士研究生,研究方向为专业密码学。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160218.1634.052.html

己的私钥进行安全匿名验证,给出了详细的认证过程,并证明了方案的正确性、安全性和可行性。

1　SIP 安全问题

SIP 的注册认证是 HTTP Digest 的身份认证[4],具体流程如下:

(1)用户首次试呼时,终端代理向代理服务器发送 REGISTER 注册请求;

(2)代理服务器通过后端认证/计费中心获知用户信息不在数据库中,便向终端代理回送 401Unauthorized 质询信息,其中包含安全认证需要的 realm 和 nonce;

(3)终端代理提示用户输入其标识和密码后,根据 username,realm,nonce,uri 将其使用 MD5 加密后,再次用 REGISTER 消息报告给代理服务器;

(4)代理服务器获取 REGISTER 消息中的用户信息,通过认证/计费中心验证 response 合法后,将该用户信息登记到数据库中,并向终端代理 A 返回成功响应消息 200 OK。

而注销过程分为两步:

(1)用户 A 向代理服务器发送 REGISTER,其头域的 expire 字段置 0,表示取消注册,Contact 值为 * 表示这个请求应用与所有有关该用户的联系信息;

(2)代理服务器收到后回送 200 OK 响应,并将数据库中的用户信息注销。

从上面的认证过程可以看出,摘要认证简便而且无法通过欺骗获取密钥,但仍然存在安全问题[5]:

(1)服务器伪装。SIP 认证是预共享密钥的挑战-响应认证,只有服务器对用户进行认证,而用户无法对服务器进行认证,这样如果用于被重定向到一个假冒的服务器,原有的认证无法识别服务器的真伪;

(2)注册删除。在一个没有安全认证的 UDP 环境下,只要攻击者接入了系统的网络,注册删除是一件很简单的事,所以一个部署在公网上的 SIP 系统很容易被干扰;

(3)注册劫持。攻击者通过离线字典攻击获得口令实现劫持,或者通过注册删除再进行中间人攻击实现。

2　环签名认证方案

2.1　环签名概述

环签名是由 Rivest,Shamir 和 Tauman 提出的一种无管理者的群签名方案[6]。一个环签名方案允许每个组成员的签名消息代表该群体而且不会泄露他们的身份,这被称为签名人匿名,与群签名需要用户之间在线合作才能完成相比,环签名只要环的成员存在合作即是有用的。而对于传统的 PKI,公共密钥构造为与用户身份无关的随机比特串,因此需要一个可信的第三方或者认证机构(CA)来证明用户和加密密钥之间的关系,而在环签名方案中,身份和公钥都能在环中得到验证[7]。

环签名的主要优点在于灵活性和高效性,每个签名者可以独立完成签名并自己选择匿名范围,一些方案中离线情况下就可生成获得签名所需要的参数[8],在线通过较小的计算就能够完成签名,没有管理者,所有成员地位平等,这些特点对于应用到 SIP 来说都是非常有实用价值的。

2.2　环签名方案

SIP 系统模型如图 1 所示。

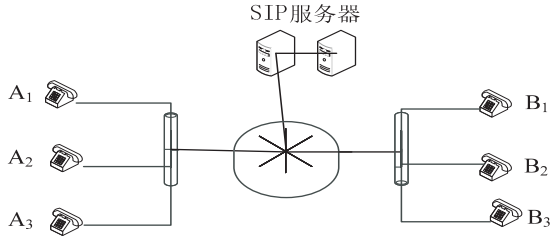

图 1　SIP 系统框架

根据环签名的性质,构建两种验证思路:

(1)A_1,A_2,A_3之间构建内部通信认证,即使用环签名来代替 VPN 部署虚拟专用网络通话;

(2)环 A 与环 B 之间进行会话认证,构建各环之间的信任通信。

考虑到技术的成熟性和实用性,这里参考 RST 签名方案[9],并根据 SIP 协议的特性加强原有算法的安全性,提出以下签名认证方案:

参数设置:设 l_1, l_2, l_3 表示三个安全参数, E 是一个在 $\{0,1\}^{l_1}$ 上的对称加密函数,解密函数为 D,密钥长度为 l_2。令 H: $\{0,1\}^{x} \rightarrow \{0,1\}^{l_2}$ 为一个安全 Hash 函数,设用户 A_i 的 RSA 公钥为 e_i,私钥为 d_i,满足 $d_i = e_i^{-1} \bmod \varphi(n_i)$,为满足 RSA 大素数的乘积,每个用户可计算 RSA 函数,其中 $t_i \in \{0,1\}^{l_3}$,用户 A_k 认证的具体过程如下:

1)用户 A_k 生成身份消息 m,然后 REGISTER 消息上发送给服务器;

2)服务器接收消息后获知用户 A_k 还未在数据库中注册,便向用户回送 401 Unauthorized(代理服务器为 407)询问信息,并保存消息 m,然后按照标准将 realm,nonce 发送给用户;

3)用户 A_k 收到未经授权信息 401 后,将 nonce,realm,用户信息 m,口令以及 uri 进行 MD5 运算,得到 response,再进行如下计算:

(1)用户在 $\{0,1\}^{l_3}$ 上获得随机数 $x_1,\cdots,x_{k-1}$, $x_{k+1},\cdots,x_r$;

(2)计算 $y_i = f_i(x_i)$;

(3)计算 $H(m)$ 为对称加密密钥,根据下式计算出 y_k ;

$$\text{response} = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots \oplus E_{H(m)}(y_1 \oplus v)\cdots)))$$

(4)用户根据自己密钥 d_k 计算出 $x_k = y_k^{d_k} \bmod n_k$;

(5)生成消息 m 的环签名 $(x_1, x_2, \cdots, x_r)$,将 $(x_1, x_2, \cdots, x_r)$ 添加到消息中,发送给服务器。

4)服务器收到消息后,计算得到 response,然后由 $y_i = f_i(x_i)$ 得到 $(y_1, y_2, \cdots, y_r)$,然后计算环方程 $\text{response}' = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots \oplus E_{H(m)}(y_1 \oplus v)\cdots)))$,并验证 response′ = response 的正确性,若合法,将用户信息(m ,response)记录到数据库中,并向用户返回响应消息 200 OK。

改进后 SIP 注册认证流程如图 2 所示。

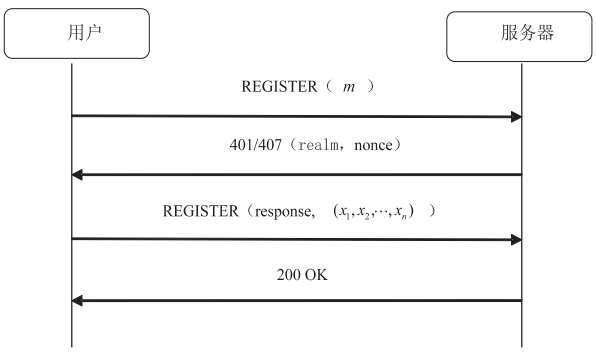

图 2 改进后 SIP 注册认证流程

注销过程如图 3 所示。具体如下:

(1)用户根据注册的值 m 和 response,使注册第三步的计算得到环签名 $(x_1', x_2', \cdots, x_n')$,然后生成注销信息发送给服务器;

(2)服务器收到后,根据存储的用户信息验证环签名,通过后返回 200 OK 消息,注销数据库中的用户信息。

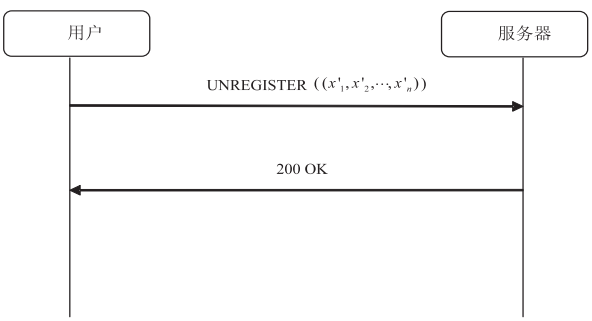

图 3 用户注销流程

3 方案特性分析

3.1 方案正确性

方案的正确性在于 y_k 和 v' 的计算,根据上述式子有:

$$v = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots \oplus E_{H(m)}(y_1 \oplus v)\cdots))) \Rightarrow y_k = D_{H(m)}(y_{k+1} \oplus D_{H(m)}(\cdots D_{H(m)}(y_n \oplus D_{H(m)}(v)))) \oplus E_{H(m)}(y_{k-1} \oplus E_{H(m)}(\cdots \oplus E_{H(m)}(y_1 \oplus v)))$$

从而:

$$v' = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots y_k \oplus E_{H(m)}(\cdots E_{H(m)}(y_1 \oplus v)\cdots)))) \Rightarrow v' = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots D_{H(m)}(y_{k+1} \oplus D_{H(m)}(\cdots D_{H(m)}(y_r \oplus D_{H(m)}(v)))) \oplus E_{H(m)}(y_{k-1} \oplus E_{H(m)}(\cdots \oplus E_{H(m)}(y_1 \oplus v))) \oplus E_{H(m)}(\cdots E_{H(m)}(y_1 \oplus v)\cdots)))) = E_{H(m)}(y_r \oplus E_{H(m)}(y_{r-1} \oplus E_{H(m)}(\cdots E_{H(m)}(D_{H(m)}(y_{k+1} \oplus D_{H(m)}(\cdots D_{H(m)}(y_r \oplus D_{H(m)}(v)))))))) = E_{H(m)}(y_r \oplus y_r \oplus D_{H(m)}(v)) = v$$

3.2 签名的盲性

如果能证明签名者与服务器在交互执行协议后所得到的签名概率分布与任何可能消息进行签名所得到的概率分布是不可区分的[10],那么该方案满足盲性。

证明:在方案中, v 是在 $\{0,1\}^{l_3}$ 随机生成的,其分布是随机均匀的,与消息 m 相独立;对于签名 $(x_1, x_2, \cdots, x_r)$, x_k 取决于 v 和 $x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_r$,而 v 和 $x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_r$ 都是随机选取的,与 m 无关,所以方案最后得到的环签名 $(x_1, x_2, \cdots, x_r)$ 与消息 m 是相互独立的,不同消息对应的环签名的概率分布是不可区分的。

3.3 不可伪造性

假设攻击者 B 能够适应性选择 v 和 m 获得 A 的签名,同时获得了除私钥外的系统参数 $(H, e_1, e_2, \cdots, e_r, n_1, n_2, \cdots, n_r)$ 。当 B 获得多项式次数的签名时,首先可以进行对 RSA 的攻击获取密钥,一般有共模攻击、小解密指数攻击和利用 RSA 的同态性攻击[11]。

(1)共模攻击。B 需要获得私钥 d 分别对消息 x 和 $x+1$ 进行加密后的密文,而 x 是每次加密前随机产生的,可能的结果有 2^{l_3} 种,所以进行共模攻击的概率为 $\frac{1}{2^{l_3}}$,几乎不可能成功;

(2)小解密指数攻击。假若 $N = pq$ 且 $q < p < 2q$, $d < N^{1/4}/3$ 时,根据公钥 e 和 n 求解私钥 d 的一种多项式时间算法,而当下 RSA 都采用 1 024 bit 以上长度,对素数 p 和 q 都有严格要求,所以小解密指数攻击现在也不适用;

(3)利用 RSA 的同态性攻击,需要用户使用私钥对攻击者提供的值进行加密,在本方案模型中攻击者 B 只能选择不同的 v 和 m ,无法控制 RSA 加密的具体内容,所以这种攻击也是无效的。

所以该方案一定程度上优化了 RSA 的安全性,另外,攻击者 B 还可以根据已有的签名进行冒充,而每个不同的 v 和 m ,可以产生 $(2^{l_3})^{r-1}$ 种签名,这个伪造的概率可以忽略。

3.4　效率分析

环签名主要集中在基于强 RSA 生成的方案以及基于双线性配对的方案[8],由于基于双线性的方案较多,而且复杂度类似,这里选用文献[6]中的方案在相同条件下进行比较。为了方便,使用 E 表示一次配对运算; R 表示一次 RSA 加/解密运算; H 表示哈希运算; P 表示配对密码中循环群的运算; D 表示 DES(或其他对称密码)运算; n 为环成员数量,两种运算的对比见表 1。

表 1　效率分析

验证方案	准备阶段	签名阶段	验证阶段
双线性环签名	nP	$2(n-1)P+H$	$nE+H$
RSA 环签名	0	$H+nR+nD$	$H+nR+nD$

在表 1 中,双线性方案主要是把签名的一部分工作量放到了准备阶段,而 RSA 方案是签名与验证阶段计算量相等,整体来说计算次数都需要 $4n$ 次。在实际应用中,配对运算和循环群运算较为复杂,而 RSA 和 DES 则比较成熟,算法优化也有较大优势,两种方案现在都是需要选择适量的环成员,在文献[12]中也有类似的对比说明。

4　实验验证

对于 SIP 协议来说,并没有增加额外的信令流程,保持了原有的交互流程,主要的额外开销是网络传输中需要传输环签名,当环成员数量较多时,可能造成阻塞[13]。

实验配置:采用虚拟机模拟,内存为 512 M,单核处理器 3.4 GHz,密码算法为 OpenSSL 库提供,系统为 ubuntu10.04(内核 2.632)。

实验测试 RSA 和 DES 的计算[14],RSA 采用 1 024 字节大小,即 8 192 bit。图 4 是整个程序流程,具体实验结果如图 5 所示。

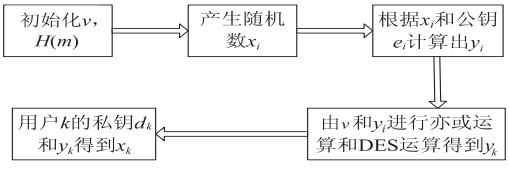

图 4　实验程序流程

可以看到,算法消耗的时间基本不会影响 SIP 原有的效率,然而产生的签名大小为 n kB, n 为环成员大小。SIP 采用的是 UDP 传输,ip 数据包最大为 64 kB,所以环成员大小控制在 50 以下,有利于传输的效率和丢包率。

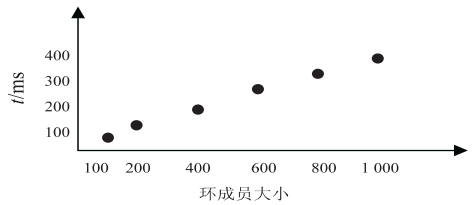

图 5　环签名运算时间

5　结束语

环签名从提出以来就引起了许多研究者的重视,也有很多签名方案被提出,而对于环签名的应用还比较模糊。文中提出应用环签名认证来构建安全域内通信,并利用环签名的无条件匿名保护用户信息,以此可使得中小型企业通过 SIP 在公共网络资源上来构建自己的呼叫中心以及安全监控系统,今后还可以将这种方案扩展到跨域认证和多方安全会话认证中。

参考文献:

[1] 徐鹏宇,许子灿. 基于 SIP 协议的监视系统设计与实现[J]. 计算机工程,2013,39(11):289-294.

[2] 俞志春,方滨兴,张兆心. SIP 协议的安全性研究[J]. 计算机应用,2006,26(9):2124-2126.

[3] 马　骥,周晓光,辛　阳,等. 基于信任域的 SIP 认证机制[J]. 计算机工程,2009,35(12):131-133.

[4] Wu Liufei, Zhang Yuqing, Wang Fengjiao. A new provably secure authentication and key agreement protocol for SIP using ECC[J]. Computer Standards & Interfaces, 2009, 31(2): 286-291.

[5] Endler D, Collier M. Hacking ExposedTM VOIP: voice over IP security secrets and solutions[M]. [s. l.]: Osborne/McGraw-Hill, 2007.

[6] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]// Proc of ASIACRYPT. Berlin: Springer-Verlag, 2001: 552-565.

[7] 胡程瑜. 环签名体制的研究[D]. 济南:山东大学,2008.

[8] Liu J K, Au M H, Susilo W, et al. Online/offline ring signature scheme[C]//Proc of ICICS. Berlin: Springer-Verlag, 2009.

[9] 刘　彪. 环签名算法研究与应用[D]. 西安:西安电子科技大学,2012.

[10] 孙　华,王爱民,郑雪峰. 一个可证明安全的无证书盲环签名方案[J]. 计算机应用研究,2013,30(8):2510-2514.

[11] 杨晓元. 现代密码学[M]. 西安:西安电子科技大学出版社,2009.

[12] 杨绍禹,王世卿,郭晓峰. 一种基于环签名的跨域云服务资源远程证明方法[J]. 小型微型计算机系统,2014,35(2):324-328.

[13] 陶怡栋. 基于无线网络的 IP 电话终端的设计与实现[D]. 兰州:兰州交通大学,2012.

[14] 王志海,童新海,沈寒辉. OpenSSL 与网络信息安全:基础、结构和指令[M]. 北京:清华大学出版社,2007.