一种基于 SGC-PKE 的 SIP 可认证密钥协商方案

张 睿[1],蒋 华[1,2],杨亚涛[2]
ZHANG Rui[1],JIANG Hua[1,2],YANG Ya-tao[2]

1.西安电子科技大学 通信工程学院,西安 710071
2.北京电子科技学院 通信工程系,北京 100070
1.College of Communication Engineering,Xidian University,Xi'an 710071,China
2.Department of Communication Engineering,Beijing Electronic Science and Technology Institute,Beijing 100070,China
E-mail:channel_vison@163.com

ZHANG Rui,JIANG Hua,YANG Ya-tao.SIP authenticated key agreement scheme based on SGC-PKE.Computer Engineering and Applications,2010,46(5):80-82.

Abstract: Session Initiation Protocol(SIP) has played an important role in many fields.As one of the core agreements of the next generation Internet,however,SIP security is to be a crucial issue.In this paper,the existing SIP security mechanisms are analysed, and a new SIP authenticated key agreement mechanism based on Self-Generated-Certificate Public Key Encryption scheme(SGC-PKE) is presented,which assures the integrity,confidentiality and non-repudiation during the transmission of SIP message and overcomes the disadvantage of Public Key Infrastructure(PKI).

Key words: session initiation protocol;self-generated-certificate public key encryption scheme;mutual-authentication;key agreement

摘 要:会话初始协议(SIP)在许多领域已经开始发挥重要的作用。作为下一代互联网中的核心协议之一,SIP 实体间通讯的安全性成为了至关重要的问题。通过对 SIP 现有的安全机制进行分析和比较,在此基础之上提出了一种新的基于自生成证书公钥加密体制(SGC-PKE)的可认证密钥协商方案,保证了 SIP 消息在传输过程中的完整性和机密性,并克服了使用公钥基础设施(PKI)带来的缺点。

关键词:会话初始协议;自生成证书公钥加密算法;双向身份认证;密钥协商
DOI:10.3778/j.issn.1002-8331.2010.05.024 **文章编号**:1002-8331(2010)05-0080-03 **文献标识码**:A **中图分类号**:TN915.9

1 SIP 协议概述

SIP 是一个信令协议,用来处理多媒体会话的建立、更改、拆卸,是基于文本的 C/S 协议。

SIP 消息由以下三部分组成:一个起始行,零个或多个首部,任意的消息体。RFC 3261 定义了 6 种不同的方法(即有 6 种不同的请求类型):INVITE、ACK、OPTION、BYE、CANCEL 和 REGISTER[1]。

SIP 呼叫建立的过程如图 1 所示。

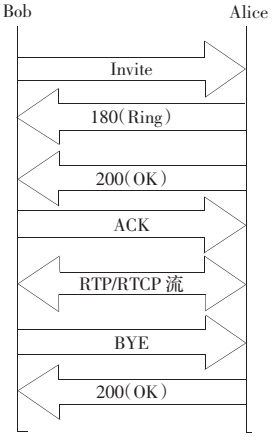

图 1 呼叫建立过程图

2 SIP 安全机制及分析比较

IETF 在 RFC3261 中推荐了几种安全方法, 包括 IPSec 或 TLS 机制,S/M IME 机制,摘要认证机制。以下是对这几种方法的分析与比较。

(1)IPsec 和 TLS

IPsec 和 TLS 给用户提供了完整的机密性。该机制能够在传输路径上的每一个代理对消息进行解密。也可以在媒体数据上应用 VPN 隧道模式[2]。

优点:保证了在数据传输线路上无法被窃听。解决了在端到端模式下,某些敏感字段(如 Via、Route 等)需要被代理服务器查看并修改,无法加密的问题。VPN 隧道模式下提供最大安全性。

缺点:IPSec 网络实施复杂,实现代价较高。TLS 不能在UDP 之上运行;对 SIP 服务器来说,同时维持大量 TLS 连接负荷较

基金项目:中央办公厅信息安全与保密重点实验室开放基金课题(Key Laboratory of Information Security and Secrecy,No.YZDJ0804)。
作者简介:张睿(1984-),男,硕士研究生,主要研究领域为密码通信技术;蒋华(1962-),男,教授,主要研究领域为信息论与编码,有线密码通信技术;杨亚涛(1979-),男,讲师,主要研究领域为无线通信系统加密技术,计算机网络安全技术。
收稿日期:2008-08-18 **修回日期**:2008-11-11

重,每跳需要加解密增加了传输节点的处理负担并增加了延迟。

(2)S/MIME

S/MIME 通过 X.509 格式的证书保证 SIP 消息的完整性和认证,机密性则由对称加密算法保证,证书用于传送会话密钥[3]。

优点:可以很好地保护被加密消息的完整性和私密性。

缺点:S/MIME 的最大缺陷是需要 PKI。实际应用中,目前多数 SIP 终端和设备不支持 S/MIME 加密。

(3)摘要认证

SIP 摘要认证大部分采用了 HTTP 摘要认证机制,文献[4]对该机制作了详细的描述。文献[5]中提出了双向的摘要认证机制。

优点:对请求方进行身份认证,保证消息可靠性,防止重放攻击。

缺点:仅能提供认证,易遭受离线密码猜测攻击,过于依赖预先共享的秘密。并且无法提供数据保密性服务。

另外,文献[6]中提出的基于 SAKA 的密钥协商方案,虽然客服了上面三种方案的缺点,但该方案也依赖于预共享秘密。

由于上面种种安全机制各自都具有一定缺陷,带来了安全问题,经过分析,提出了一种新的基于自生成证书公钥密码体制的 SIP 安全方案。

3　基于自生成证书公钥体制的 SIP 安全通信

3.1　无需配对的自生成证书公钥加密算法

在传统的公钥基础设施(PKI)中,需要第三方保证公钥和其拥有者身份的绑定关系。然而,PKI 在应用中面临很多挑战,例如证书的吊销,存储以及分发,因此提出了无证书的公钥密码算法。

J.Lai 和 W.Kou 提出了无需配对的自生成证书的公钥密码体制(SGC-PKC),能够抵抗"拒绝解密攻击"攻击并保留了无证书公钥密码体制(CL-PKC)的所有优点[7]。文献[8]发现了J.Lai 和 W.Kou 的算法易受到一种特殊的身份伪装攻击,并对此进行了改进,使改进的算法能够抵抗该攻击。

算法构成:

Setup(k):生成 2 个大素数 p 和 q,$q|p-1$。选取生成元 $g\in\mathbb{Z}_p^*$。随机选取 $x\in\mathbb{Z}_q^*$ 并计算 $y=g^x$。选择哈希函数 $H_0:\{0,1\}^*\times\mathbb{Z}_p^*\times\mathbb{Z}_p^*\times\mathbb{Z}_p^*\times\mathbb{Z}_p^*\to\mathbb{Z}_p^*$;$H_1:\{0,1\}^*\times\mathbb{Z}_p^*\times\mathbb{Z}_p^*\to\mathbb{Z}_q^*$;$H_2:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to\mathbb{Z}_q^*$;和 $H_3:\mathbb{Z}_p^*\to\{0,1\}^l$,$l=l_0+l_1\in N$。返回参数组 $param=(p,q,g,y,H_0,H_1,H_2,H_3)$和主密钥 $mk=(p,q,g,x,H_0,H_1,H_2,H_3)$。密钥产生中心运行。

UserKeyGeneration($param$):随机选取 $z\in\mathbb{Z}_q^*$ 并计算 $\mu=g^z$。返回$(sk,pk)=(z,\mu)$。用户运行。

PartialKeyExtract($param,mk,ID,pk$):随机选取 $s\in\mathbb{Z}_q^*$ 并计算 $\omega=g^s$ 和 $t=s+xH_1(ID,\omega,pk)=s+xH_1(ID,\omega,\mu)$,返回$(P_{ID},D_{ID})=(\omega,t)$。密钥产生中心运行,并将结果发送给用户。

SetPrivateKey($param,D_{ID},sk$):令 $SK_{ID}=sk+D_{ID}=z+t$。返回 SK_{ID}。用户运行。

SetPublicKey($param,P_{ID},pk,ID,SK_{ID}$):计算 $PK_{ID}^1=(pk,P_{ID})=(\mu,\omega)$和 $PK_{ID}^2=pk*P_{ID}*y^{H_1(ID,pk,P_{ID})}=\mu\omega y^{H_1(ID,\mu,\omega)}=g^{z+t}=g^{SK_{ID}}$。然后用户使用 Schnorr 签名机制使用用户自己的私钥 SK_{ID}对用户的标识符 ID,PK_{ID}^1和 PK_{ID}^2进行签名。(1)随机选择 $r\in\mathbb{Z}_q^*$;(2)计算 $R=g^r \bmod p$;并且(3)得到签名为(R,σ),$\sigma=r+SK_{ID}*H_0(ID,\mu,\omega,PK_{ID}^2,R)$。最后 $PK_{ID}=(PK_{ID}^1,PK_{ID}^2,(R,\sigma))$,返回。用户运行。

Encrypt($param,ID,PK_{ID},M$):把 PK_{ID} 分解为$(PK_{ID}^1,PK_{ID}^2,(R,\sigma))$,将 PK_{ID}^1分解为(μ,ω)。如果 $PK_{ID}^2\neq\mu\omega*y^{H_1(ID,\mu,\omega)}$ 或者 $g^\sigma\neq R*(PK_{ID}^2)^{H_0(ID,\mu,\omega,PK_{ID}^2,R)}$,那么返回 $\perp$,否则按如下方法计算:如果 M 的比特数为 l_0:已知 $PK_{ID}=(PK_{ID}^1,PK_{ID}^2)$,随机选取 $\sigma\in\{0,1\}^{l_1}$ 并计算 $r=H_2(M,\sigma)$。计算 $C=(c_1,c_2)$,$c_1=g^r$;$c_2=H_3((\mu\omega y^{H_1(ID,\omega,\mu)})^r)\oplus(M\|\sigma)=H_3((PK_{ID}^2)^r)\oplus(M\|\sigma)$。

Decrypt($param,SK_{ID},C$):已知 $C=(c_1,c_2)$,$SK_{ID}=(z,t)$。计算 $M\|\sigma=H_3((c_1)^{z+t})\oplus c_2$。如果 $g^{H_2(M,\sigma)}=c_1$,则返回明文 M。否则返回"拒绝"。

3.2　基于自生成证书公钥体制的 SIP 可认证密钥协商方案

为了克服现有安全机制的不足,提出了一种基于自生成证书公钥体制的 SIP 可认证密钥协商方案。该方案拥有公钥密码算法的优点,提供双向认证,又无需预先共享秘密,同时不需要 PKI 的支持。

在认证过程进行之前,主被叫双方已经各自从 KGC 那里取得了公开参数组 $param$ 并且产生了各自的公私钥对:客户端 A 的 ID 和公私钥对分别用 A 和(PK_A,SK_A)表示,客户端 B 的ID 和公私钥对分别用 B 和(PK_B,SK_B),$realm\_s$ 表示作用域。此时,客户端 A 准备向客户端 B 发起请求:

步骤 1　客户端 A 向客户端 B 发出 Invite 请求,并在请求消息体中附上自己的公钥 PK_A 和支持的对称加密算法列表。

步骤 2　客户端 B 认为客户端没有通过认证,发起挑战。客户端 B 首先产生临时会话密钥 S_1 和随机数 N_1。

假设选定的对称密钥算法是 AES,那么客户端 B 使用 S_1 作为密钥将$(realm_s\|N_1)$用 AES 加密得到密文[9]C_1;然后使用客户端 A 的公钥加密临时会话密钥 S_1,得到密文 C_2=Encrypt$(param,A,PK_A,S_1)$。

如果 Encrypt 方法返回的值是 $\perp$,那么说明对方公钥错误,那么立即发送 403(禁止)消息,通知对方认证失败。否则,C_1 和 C_2 共同组成了挑战值(C_1,C_2),客户端 B 产生状态号为 401(未授权)的回应消息,将(C_1,C_2)放在 WWW-Authenticate 首部中,将自己的公钥 PK_B 放入消息体内,将该消息发送给客户端 A,发出了挑战。

步骤 3　客户端 A 收到 401 响应后立即发送 ACK 消息给客户端 B,表示接受挑战。客户端 A 从收到的消息中的 WWW-Authenticate 中提取出(C_1,C_2),从消息体得到客户端 B 的公钥 PK_B。

客户端 A 使用自己的私钥解密 C_2:S_1=Decrypt$(param,SK_A,C_2)$,如果解密结果是"拒绝",那么说明自己的公钥或者是受到的密文在传输途中出错或者被修改,则终止认证过程。否则使用 S_1 解密 C_1 得到$(realm_s\|N_1')$。

步骤 4　客户端 A 产生会话密钥 S 和随机数 N_2,计算临时会话密钥 $S_2=S\oplus S_1$。

客户端 A 使用 S_2 作为密钥将$(realm_s\|N_1'\|N_2)$用 AES 加密得到密文 C_3;然后使用客户端 B 的公钥加密临时会话密钥 S_2,得到密文 C_4=Encrypt$(param,B,PK_B,S_2)$。

如果 Encrypt 方法返回的值是 $\perp$,那么说明对方公钥错误,那么终止认证过程。否则,C_3 和 C_4 共同组成了(C_3,C_4),客户端 A 重

新产生带认证的 Invite 请求,将(C_3,C_4)放在 Authorization 首部中,使用 S_2 作为密钥将消息体用 AES 加密,该请求发送给客户端 B。

步骤 5　客户端 B 收到 Invite 请求后,立即发送 180 Ringing 消息作为临时回应。

步骤 6　从 Authorization 首部中提取出(C_3,C_4),使用自己的私钥解密 C_4:S_2=Decrypt($param$,SK_B,C_4),如果解密结果是"拒绝",那么说明自己的公钥或者是受到的密文在传输途中出错或者被修改,那么立即返回 403(禁止)消息,通知对方认证失败。

使用 S_2 解密 C_3 得到($realm\_s \parallel N_1'' \parallel N_2'$),如果 $N_1''\neq N_1$,那么返回 403(禁止)消息,通知对方认证失败。如果 $N_1''=N_1$,则计算 $S'=S_2\oplus S_1$,使用 S'作为密钥将($realm\_s \parallel N_2'$)用 AES 加密得到密文 C_5,如果有需要携带的消息体,则使用 S'作为密钥将其用 AES 加密。

产生 200OK 响应消息,在该消息的 Authorization 首部中携带 C_5,将该消息发送给客户端 A,表示客户端 A 通过了身份验证。

步骤 7　客户端 A 收到 200OK 响应消息后,从 Authorization 首部中提取出 C_5,使用会话密钥 S 解密得到($realm\_s \parallel N_2''$),如果 $N_2''\neq N_2$ 表示对客户端 B 的认证失败,发送 CANCEL 请求终止会话。如果 $N_2''=N_2$ 则发送 ACK 请求,并在请求中附带 C_6=AES_En (S,N_1+N_2),客户端 B 收到该 ACK 请求后解密 C_6 和 N_1+N_2 比较,相同则确认双方认证通过,密钥交换完成。否则立即发送 BYE。

步骤 8　客户端 A 和客户端 B 使用协商好的会话密钥 S=S'建立加密的媒体连接,进行通信。

图 2 展示了一次成功密钥协商的流程。

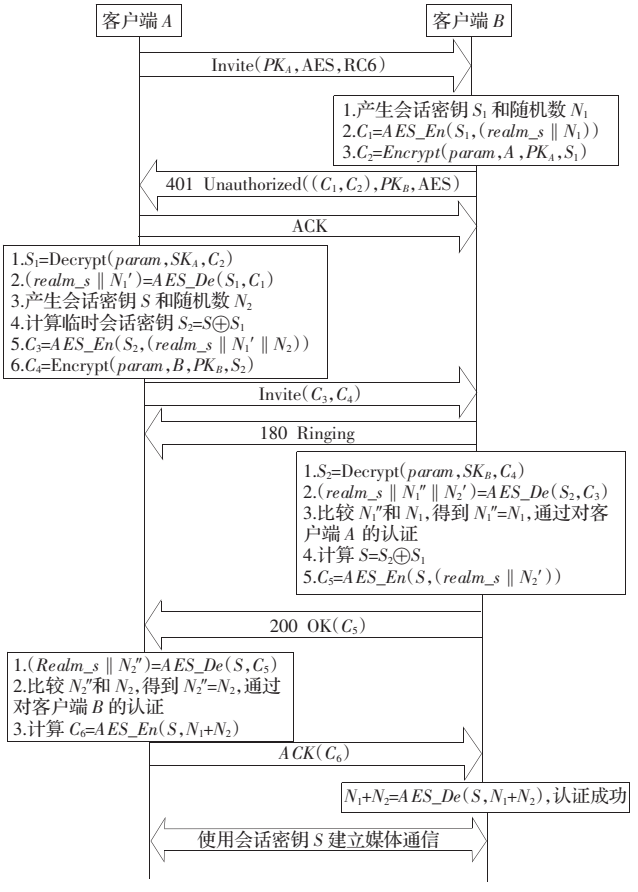

图 2　基于自生成证书公钥体制的 SIP 可认证密钥协商成功流程图

上述过程仅仅使用了 SIP 端到端的通信的 Invite 请求做了说明,在 SIP 客户端和代理服务器中,在 Register、Option 和 Bye 方法同样可以使用该过程。在 SIP 客户端和代理服务器通信中,仅仅需要将客户端 B 返回的 401 消息改成代理返回的 407 消息,代理发出的挑战值不再放在 WWW-Authenticate 中而是放在 Proxy-Authenticate 中,客户端的响应值不再放在Authorization 中而是放在 Proxy-Authorization 中。因此,方案可以广泛地应用在 SIP 网络中,来进行身份认证和密钥交换。

4　基于 SGC-PKE 的 SIP 可认证密钥协商方案分析

4.1　可认证密钥协商方案分析

选择采用摘要认证的格式和流程,仅仅使用单向认证的流程实现了双向认证和密钥协商,提高了兼容性和网络利用率,更简化了实现,可在已有的摘要认证基础上修改即可。除此之外,该方案还有以下优点:

(1)自生成证书公钥体制保留了公钥密码体制全部的优点,公钥可以广泛分发,通信的双方无需预先共享秘密;并且无需 CA 支持,减少了繁琐的 PKI 系统的维护。

(2)在整个过程中,使用 AES 对大量的明文信息进行加密,而使用公钥算法加密 AES 密钥,既不降低安全性,又节省了加解密的时间,并实现了双向认证和密钥协商。

(3)攻击者由于无法得到合法用户 ID 对应的私钥,而使用公钥加密需要用对应 ID 作为输入,攻击者无法以自己的公钥替换合法用户的公钥来实现中间人攻击,也就无法向其他实体确认自己的身份,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。

但是,方案无法抵抗文献[10]中提到的 BYE 延迟和丢弃攻击,攻击者虽然由于不知道会话密钥而无法进行"免费"呼叫,但是在商用系统中可能导致用户费用异常升高,影响运营商声誉。

4.2　可认证密钥协商过程的安全性分析

整个密钥协商过程中,通信双方传输的信息有 PK_A,PK_B,C_1=AES(S_1,($realm\_s \| N_1$)),C_2=Encrypt($param$,A,PK_A,S_1),C_3=AES(S_2,($realm\_s \parallel N_1' \parallel N_2$)),$C_4$=Encrypt($param$,$B$,$PK_B$,$S_2$),$C_5$=AES($S'$,($realm\_s \parallel N_2'$))。下面主要分析这些数据信息被第三方攻击者窃取后对该 SIP 安全通信方案安全性能的影响。在分析中,使用主叫客户端 A 和被叫客户端 B 来表示合法通信方。

(1)身份欺骗:如果第三方攻击者截取到上面所有信息,由于不知道 A 的私钥 SK_A,以及离散对数的难解性,攻击者无法获取 S_1 和 N_1,也就不可能计算出正确的 AES(S_2,($realm\_s \parallel N_1' \parallel N_2$))来伪装成主叫用户 A。如果攻击者将用户 A 的公钥替换为自己的公钥,由于 SGC-PKE 的公钥和用户 A 的 ID 是绑定的,被叫用户 B 能够发现 A 的公钥有问题,从而使攻击者无法伪装为主叫用户 A。在密钥协商过程中,即使第三方攻击者使用自己产生的会话密钥 S 和随机数 N 对合法通信双方传送的信息进行修改,由于攻击者不知道 A 的私钥 SK_A,再加上双方随机数和 AES 加密的原因,无法共享密钥,无法达到对通信双方的欺骗的目的。

(2)重放攻击:攻击者截取了上一次 A 和 B 协商时的所有通信数据,然后向用户 B 发送先前 A 向 B 发送过的数据。由于 B 会产生新的临时会话密钥和新的随机数作为挑战值,但攻击者无法知道新的随机数并且无法修改截取到的信息,只能发送上一次通信中的数据,所以攻击者无法通过 B 对其的认证。该

(下转 99 页)