一种基于身份的SIP认证与密钥协商机制

周计成,徐开勇,赵 彬,吴 平
ZHOU Ji-cheng,XU Kai-yong,ZHAO Bin,WU Ping

解放军信息工程大学 电子技术学院,郑州 450004
Institute of Electronic Technology,PLA University of Information Engineering,Zhengzhou 450004,China
E-mail:testforngn@sina.com

ZHOU Ji-cheng,XU Kai-yong,ZHAO Bin,et al.Identity-based authentication and key agreement scheme of SIP.Computer Engineering and Applications,2010,46(5):96-99.

Abstract: Along with Session Initiation Protocol(SIP) application in network communication widely,especially in mobility area, many wireless equipments are used.These devices have limited capacity of storage and computing.In this paper,the security schemes of SIP are discussed and analyzed.Furthermore,a new authentication and key agreement scheme based on identity is proposed,which assures the integrity and authenticity of SIP message during transmission and consults with share key.The scheme doesn't need any public key certificate;user's SIP URI is used as his public key.It needs less storage,computing capacity and communication cost,so it is simple and effective.

Key words: Session Initiation Protocol(SIP);security mechanism;Identity Based Cryptography(IBC);authentication;key agreement

摘 要:随着SIP协议在网络通信中的广泛应用,特别是向移动领域扩展,网络中大量使用无线设备,终端的运算与存储能力有限。对SIP的安全方案进行了讨论和分析,提出了一种基于身份的认证与密钥协商方案,保证了SIP消息传输过程中的完整性和真实性,并在该过程中进行了密钥协商。方案中不需要公钥证书,用户用身份标识SIP URI作为公钥,降低了对终端计算、存储能力的需求和通信开销,具有简单高效的优点。

关键词:会话发起协议;安全机制;基于身份的密码学;身份认证;密钥协商
DOI:10.3778/j.issn.1002-8331.2010.05.029 **文章编号**:1002-8331(2010)05-0096-04 **文献标识码**:A **中图分类号**:TP393.08

1 引言

SIP(Session Initiation Protocol,会话发起协议)是由IETF提出进行多媒体通信的应用层控制协议,用来实现会话的发起、建立、修改和终止[1]。SIP协议具备简单性、灵活性和扩展性等特点。它还是下一代网络(NGN,Next Generation Network)的核心协议,作为软交换与应用服务器、智能终端之间的呼叫控制协议[2],有着广泛的应用前景和重要的研发价值。

SIP消息的传递可能要经过多个代理服务器和不信任域,致使协议实体间的网络通信面临多种威胁和攻击,如何保证SIP的安全性已成为近年来的研究热点。IETF在RFC3261中提出了SIP安全解决方案,然而这些方案存在一些局限性和缺点,方案中也没有对SIP通信实体之间的密钥协商进行讨论,必须经过其他途径进行密钥交换。由于SIP协议在移动和无线领域中大量应用,终端设备的存储与计算能力受限,只有较少的网络带宽,使得如基于证书[3]等的传统安全机制无法得到广泛应用。

Shamir于1984年提出了一种公钥密码体制,该体制能大大减少公钥系统的复杂度,它选择任意比特串(通常是用户身份)作为公钥,由私钥生成中心(PKG)生成对应的私钥[4]。IBC(Identity Based Cryptography,基于身份的密码学)简化了传统基于证书的公钥体制负担最重的密钥管理过程。它不依赖于数字证书,用户的身份标识通过哈希函数即可求得其公钥, 大大减少了通信实体处理公钥的时间和存储容量;不需查询公钥目录,不需要第三方认证服务,避免了交叉认证问题,减少了网络带宽消耗。2001年,由Boneh和Franklin使用双线性对技术提出了第一个安全实用的基于身份的加密机制[5],并用可证明安全性理论证明在随机预言机模型下,它能抵抗不可区分自适应选择密文攻击。此后,大量使用双线性对技术的IBS(Identity Based Signature,基于身份的签名)以及IBAKA(Identity Based Authentication and Key Agreement,基于身份的认证密钥协商)方案被提出。

对SIP的安全威胁进行了讨论与分析,研究了基于身份的密码学,在此基础之上提出了一种基于身份的SIP认证与密钥协商方案。

基金项目:国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2008AA01Z404);国家部委预研基金资助项目(the Pre-Research Foundation of China Ministries and Commissions)。

作者简介:周计成(1982-),男,硕士研究生,主研方向:网络管理技术,信息安全技术; 徐开勇(1963-),男,研究员,硕士生导师,主研方向:网络管理技术,计算机应用;赵彬(1975-),男,博士研究生,主研方向:信息安全技术;吴平(1981-),男,硕士研究生,主研方向:信息安全技术。

收稿日期:2008-08-25 **修回日期**:2008-11-06

2　SIP协议及其安全机制

2.1　SIP协议简介

SIP系统采用C/S(客户端/服务器)的工作方式,由用户代理和网络服务器组成。用户代理(User Agent,UA)负责发起呼叫请求和对呼叫请求做出响应。网络服务器在逻辑功能上分为代理服务器、重定向服务器和注册服务器,主要作用是提供名字解析和用户定位以及为用户代理提供注册、认证、鉴权、路由等服务。SIP协议使用SIP URI(Uniform Resource Identifier,统一资源标识符)标识用户身份。

SIP会话的一般通信流程分为以下几步:

(1)注册:用户用REGISTER消息向注册服务器注册自己的位置和当前联系地址;

(2)呼叫发起:用户向代理服务器提交请求,使用INVITE消息;

(3)定位与重定向:代理服务器通过位置查询得到被呼叫方的地址,然后将INVITE消息转发给被呼叫方;

(4)响应:被呼叫方响应呼叫方并进行参数协商,然后建立会话连接传输数据;

(5)会话终止:数据传输完成后,用户发出BYE消息请求退出会话,呼叫结束。

图1所示是经过一个代理服务器的呼叫实现过程。

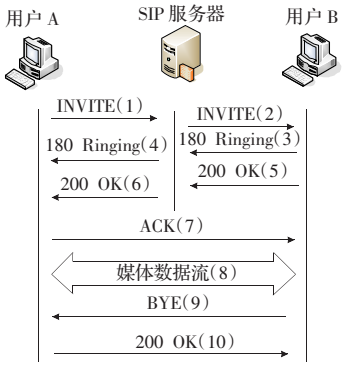

图1　用户A向用户B发起会话的流程图

2.2　SIP协议安全威胁与安全机制

SIP协议在实现的过程中使用了很多网络服务器作为中间设备,因此使SIP的安全问题十分复杂。SIP主要面临以下几种安全威胁[1]:

(1)注册攻击

终端用户通过用户代理发送REGISTER消息到注册服务器上,并定时刷新。在REGISTER消息中使用To字段中的address-of-record项表明终端用户的地址。注册服务器会检查From字段所提供的身份说明,来决定是否修改联系地址。这两个头域字段通常是相同的,也可以由第三方代替终端用户注册联系地址。注册攻击正是利用了SIP注册机制的漏洞,通过重新注册来假冒合法用户。

(2)伪装服务器攻击

攻击者假装自己是服务器并伪造一个响应,原来的消息就可能被错误地传送至伪装的服务器。

(3)修改消息包体

SIP消息的传递一般要经过多个代理,在通信过程中存在被截获和篡改的风险。恶意代理服务器可以像中间人一样修改消息的属性,包括MIME包体、SDP或者电话信令等内容,或者改变原始请求UA的安全特性。

(4)断开会话攻击

在通话过程当中,攻击者向通话的一方发送BYE/CANCEL消息,使其代理服务器误认为对方已经终止或是取消通话。或者伪造来自代理服务器的BYE/CANCEL消息给UAC,使得UAC误以为UAS要求结束或者取消通话。其攻击效果是造成通话中断,或者用户根本接不到来电。

(5)DOS(拒绝服务)攻击

DOS攻击主要是使得一个特定网络节点无法工作,通常是通过转发超大量的网络通讯阻塞目标网络接口。攻击者可以发出包含假IP地址及其相关的Via头域的请求,这个Via头域标志了被攻击的主机地址。然后把这个请求发给大量的SIP节点,这些SIP节点就会给被攻击的主机产生大量的垃圾应答,从而形成拒绝服务攻击。

由此可见,大多数安全威胁都是由于身份认证和加密问题没得到好的解决而产生的。研究SIP协议的身份认证与密钥协商机制对于保证SIP的安全性至关重要。

RFC3261中讨论了目前SIP的安全机制,按其功能可以划分为加密机制、认证机制和访问控制机制。主要有以下几种机制。

(1)HTTP摘要鉴权机制

HTTP摘要鉴权机制提供了对消息中的Request-URI和请求方法的完整性保护,但是并没有对UA希望提供加密的所有头域进行保护。它只能提供服务器对客户端的认证,无法提供对服务器的认证,易受到伪装服务器攻击。

(2)S/MIME

S/MIME能够较好地实现端到端的安全性。然而它最大的一个限制是对终端用户来说,缺少广泛的公共密钥机构。如果使用的是自签名信任书,其密钥交换机制就容易遭受中间人攻击,攻击者可以悄悄截获并修改S/MIME包体。

(3)TLS

TLS提供了严格的节点到节点的安全性。TLS最大的问题是它仅能应用于面向连接的协议之上即TCP协议,并且只允许SIP实体到相邻的认证服务器的连接。

(4)基于证书的安全机制

它能够很好地保证SIP协议的安全性,提供用户身份认证与消息加密。然而全球仍然缺少统一的证书机构,互操作与交叉认证问题难以解决。证书的存储需要占用较多的空间,证书的查询与运算需要占用大量的网络带宽与运算资源,因此对终端要求较高。

3　一种基于身份的SIP认证与密钥协商机制

3.1　基于身份的认证与密钥协商算法

基于身份的密码学方案的安全性大多建立在Diffie-Hellman等难解数学问题上,通过在超奇异椭圆曲线上的线性对技术构造实现,描述如下:

设p,q为两个大素数,$E(F_p)$是定义的在有限域F_p上的椭圆曲线[6]$y^2=x^3+ax+b$,$(G_1,+)$是定义在$E(F_p)$上的一个q阶循环子加群,$(G_2,\times)$定义在有限域$F_{p^2}^*$上的q阶循环子乘群,在G_1,G_2中离散对数问题是难解的。双线性对$\hat{e}:G_1\times G_1\rightarrow G_2$是满足以下条件的映射:

(1)双线性：$\forall P,Q,R,S\in G_1$，满足：$\hat{e}(P+Q,R+S)=\hat{e}(P,R)\hat{e}(P,S)\hat{e}(Q,R)\hat{e}(Q,S)$；

(2)非退化：P 是 G_1 的生成元，$\hat{e}(P,P)\in F_{p^2}^*$，且 $\hat{e}(P,P)\neq 1_G$，1_G 为 G_2 的单位元；

(3)可计算：$\forall P,Q\in G_1$ 存在一个有效的算法计算出 $\hat{e}(P,Q)$。

Cha J 和 Cheon J H 使用双线性对技术提出了基于身份的签名(IBS)方案[7]。该方案由四个算法组成，即参数生成(Setup)算法，密钥生成(Extract)算法，签名(Sign)算法，验签(Verify)算法。

(1)Setup：PKG 随机选择 $s\in Z_q^*$ 作为系统主密钥，计算系统公钥 $P_{pub}=sP$，然后选择杂凑函数 $H_1:G_2\rightarrow\{0,1\}^n$，杂凑函数 $H_2:\{0,1\}^*\rightarrow G_1$，PKG 保存主密钥 s，并公开系统参数 $<G_1,H_1,H_2,G_2,\hat{e},P,P_{pub}>$；

(2)Extract：用户将身份标识 ID 发送给 PKG，由 PKG 生成用户私钥 $d_{ID}=sQ_{ID}$，其中 $Q_{ID}=H_2(ID)$ 是用户的公钥；

(3)Sign：签名者使用私钥 d_{ID} 对消息 $m\in\{0,1\}^*$ 签名：选择随机数 $r\in Z_q^*$，计算 $U=rQ_{ID}$，$V=(H_1(m,U)+r)\cdot d_{ID}$。输出签名 $\sigma=(U,V)$；

(4)Verify：为确认 $\sigma=(U,V)$ 是否为用户对消息 m 的签名，验证者需要执行计算：$v=\hat{e}(U+H_1(m,U)Q_{ID},P_{pub})$ 与 $u=\hat{e}(V,P)$，若 $u=v$ 则接受签名，否则拒绝。

将上述签名认证方案应用到 SIP 安全机制中以解决 SIP 实体通信中端到端的身份认证问题。SIP URI 是用户的身份标识，经过哈希函数处理后作为其公钥。

在实时多媒体通信中对加密速度要求较高，一般用对称密码算法对媒体数据流进行加密，而通过公钥密码算法进行密钥协商。因此，参照 Chen-Kudla-IBAKA 机制[8]在方案中增加了如下密钥协商(Key Agreement)算法：

设在签名算法中 UA 选择的随机数为 a，Server 选择的随机数为 b。UA 计算共享密钥 $K=H_1(\hat{e}(d_{UA},U_{Server}+aQ_{Server}))$，Server 计算共享密钥为 $K'=H_1(\hat{e}(U_{UA}+bQ_{UA},d_{Server}))$。由双线性对性质可得方案一致性 $K=K'=H_1(\hat{e}(Q_{UA},Q_{Server})^{s(a+b)})$。

通过该算法可以得到固定长度的会话密钥，同时也给密钥破解增加了难度，增强了密钥的安全性。

3.2 SIP 认证与密钥协商方案实现流程

在如图 2 所示的 SIP 会话中，将提出的方案进行了实现。用户 UA 身份 ID 为 sip:User@realm.com，服务器 Server 身份 ID 为 sip:Server@realm.com，由 PKG 生成用户私钥 d_{UA} 和服务器私钥 d_{Server}。

实施流程如下：

(1)UA 发送请求：用户发出一个 SIP 消息请求，该请求消息可以是发给代理服务器的 INVITE 请求，也可以是发给注册服务器的 REGISTER 请求。以后者为例进行说明。UA 运行 Sign 算法，将请求消息用其私钥 D_{UA} 进行签名，附在请求消息的 Authorization 头域中发送。消息应包含以下信息：realm，opaque，current time，Sign(M)。其中，realm 为Server 的安全域标识，opaque 为此次会话标识，current time 为时间戳，Sign(M)为对消息的签名值。

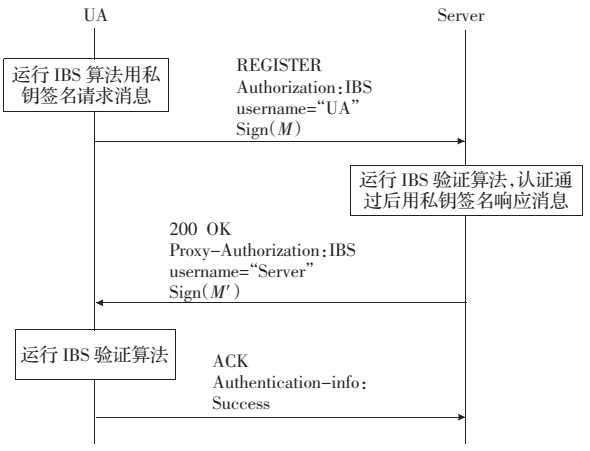

图 2 用户与服务器间的认证与密钥协商流程图

(2)Server 验证请求并响应：Server 查看 UA 的用户名是否在合法用户名单内，如不合法，则直接丢弃该消息。Server 查检请求消息的内容，若未包含如第(1)步中的认证信息，则 Server 响应 UA，返回 401 或 407 消息，提示用户需要认证。若包含认证信息，则 Server 运行 Verify 算法使用 UA 的公钥 Q_{UA} 来验证 UA 的请求。验证通过则向 Server 发出响应消息，继续下一步，否则认证失败。该步骤可实现对用户的身份认证。Server 响应 UA，首先运行 Sign 算法，将响应消息由其私钥 d_{Server} 进行签名，然后附在 200OK 响应消息后发送。

(3)UA 验证 Server 响应：UA 使用 Server 的公钥 Q_{Server} 来验证 Server 的响应，运行 Verify 算法进行验证。验证通过则向 Server 发出 ACK 响应消息，否则发送认证失败消息，结束本轮的认证流程。该步骤可实现对服务器的身份认证。

若要进行会话密钥协商，则在第(2)、(3)步运行上文提出的 Key Agreement 算法。至此双方成功建立了认证关系，完成了会话密钥协商。

4 方案的安全性及效率分析

4.1 方案安全性分析

(1)方案实现了双向身份认证

证明 使用的数字签名算法，在点乘与双线性对的运算步骤上完全一致，因而在 DLP 和 CDHP 难解的假设下，签名难以伪造。会话双方通过用各自的私钥对消息签名，保证了消息的真实性、完整性与不可否认性，通过第(2)、(3)步实现了双向身份认证。

在签名消息中由于含有时间戳、随机数以及本次会话的标识，从而能够抵御重放攻击。攻击者无从获得双方的私钥，所以无法伪造 Server 或 UA 的身份来签名一个正确的响应消息。因此，攻击者无法通过身份认证，能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。同时，在该方案中由于首先对客户端 UA 进行了身份认证，可以在一定程度上防止对服务器的 DOS 攻击。

(2)会话密钥协商具有 AKA 安全属性

证明 会话密钥协商机制安全主要满足以下 AKA 安全属性，即已知会话密钥安全性、前向安全性、密钥泄露扮演、未知密钥共享和控制密钥安全性，其证明过程与文献[8]类似。

由于攻击者虽然能够截获密钥协商参数 U_{UA} 与 U_{Server}，但攻击者不能获取双方各自生成的随机数，仍无法计算出会话密

钥。该密钥协商的参数是在认证过程中传递的,签名认证算法确保了其真实性,因此攻击者不能发起中间人攻击。

4.2　方案效率分析

在实现用户与服务器之间的双向认证的条件下,对几种典型的SIP认证方案通信量与计算复杂性进行了分析比较,如表1所示。

表1　三种认证方案效率比较表

Scheme	双向HTTP摘要方案	基于证书认证方案[5]	基于身份的认证方案
前提条件	需存储双方用户名与共享密钥	由CA生成实体公私密钥对,将私钥发送给用户分布公钥与证书	由PKG为网络中的节点生成私钥,以用户ID作为公钥
通信量	8次交互	8次交互	3次交互
计算复杂性	双方各进行1次加密与验证	双方各进行1次签名与验证	双方各进行1次签名与验证

在认证方案中,签名和验证算法的计算复杂性决定了方案的执行效率。HTTP摘要方案的计算复杂性主要取决于加密函数F的选取[9]。基于证书的方案中使用如RSA、ECC等公钥密码算法进行签名和验证,要经常进行指数运算,运算量较大。使用的方案在群G上共进行2次对运算、2次点加运算、2次杂凑函数运算、3次数乘运算,没有指数运算。从以上分析可知,基于身份的认证方案只需要最少的通信量与较小的计算代价就可以实现SIP实体间的双向认证。

算法中参数U既用于签名,又用于密钥协商,基于身份的密钥协商过程无需另外进行,只需在互换签名后运行Key Agreement算法。该算法包含1次对运算、1次点加运算、1次杂凑函数运算和1次数乘运算,所以计算复杂度也很低。若仅进行认证,则不用运行密钥协商算法,提高了方案效率和灵活性。

5　结束语

在SIP协议新的应用环境下,提出了一种基于身份的认证与密钥协商方案。方案不需要公钥证书,节省了用户的计算量、存储容量和通信带宽开销,特别适用于运算与存储能力有限的通信设备。通过将身份认证与密钥协商有机地融入到SIP协议当中,使用SIP缺省认证方法的消息格式与语法,使得对原有系统改动较小,保证了SIP协议的安全。

参考文献:

[1] Rosenberg J,Schulzrinne H,Camarillo G,et al.RFC3261 SIP:Session initiation protocol[S].2002-06.

[2] 张智江,张云勇.SIP协议及其应用[M].北京:电子工业出版社,2006.

[3] 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.

[4] Shamir A.Identity based cryptosystems and signature schemes[C]//LNCS 196:Advances in Cryptology,CRYPTO 1984.Berlin:Springer,1984:47-53.

[5] Boneh D,Franklin M.Identity based encryption from the Weil pairing[C]//LNCS 2139:Advances in Cryptology,CRYPTO 2001.Berlin:Springer,2001:213-229.

[6] Koblitz N.Elliptic curve cryptosystems[J].Mathematics of Computation,1987,48:203-208.

[7] Cha J,Cheon J H.An identity based signature from gap diffie-hellman groups[C]//LNCS 2567:Practice and Theory in Public Key Cryptography,PKC 2003.Berlin:Springer,2003:18-30.

[8] Chen L,Kudla C.Identity based authenticated key agreement form pairings,2002/184[R].Cryptology Print Archive,2002.

[9] Franks J,Hallam B P,Hostetler J,et al.RFC 2617 HTTP authentication:Basic and digest access authentication[S].1999-06.

(上接82页)

方法可以有效地防止重放攻击。

(3)离线密码攻击:即使攻击者截取到了所有的通信数据,他也无法得到会话密钥S,因为:

①攻击者无法从公钥推出对应的私钥和猜测到正确的私钥,因为其难度等同于解决CDH问题。这也就是说,通过破解SGC-PKE得到S_1的难度等同于CDH问题。

②攻击者猜测到正确的S_1的难度等同于破解AES。并且由于S_1在每次通信时的值都会更换,而执行该过程是在每次进行关键方法(如BYE,Invite)时,因此破解所需的时间远大于S_1实际应用时间,因此是计算安全的。

很明显,该方案对离线密码攻击是计算安全的。

5　结语

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。提出的基于自生成证书公钥体制的SIP可认证密钥方案,结合摘要认证机制,实现了对SIP协议进行呼叫控制过程和数据传送过程中的双向身份认证和密钥协商,为后续的加密通信提供了安全保障,有效地解决了SIP网络中存在的安全问题。当然,由于自生成证书公钥体制暂时不支持私钥签名,在方案中无法依赖其实现数据完整性保护,而只能在会话密钥协商结束后使用会话密钥来加密摘要,以此实现数据完整性保护;也因此导致认证过程略显复杂,但是随着进一步研究,一定会有同时支持加密和签名的算法,这些不足都是可以被克服的。

参考文献:

[1] Rosenberg J,Schulzrinne H,Camarillo G,et al.IETF:RFC3261 SIP:Session initiation protocol[S/OL].2002-06.http://www.ietf.org/rfc/rfc3261.txt.

[2] Diab W B,Tohme S,Bassil C.Critical VPN security analysis and new approach for securing VoIP communications over VPN networks[C]//WMuNeP'07,Chania,Crete Island,Greece.ACM,2007:92-96.

[3] IETF:RFC2634 Enhanced security services for S/MIME[S/OL].Hoffman P.1999.http://www.ietf.org/rfc/rfc2634.txt.

[4] Franks J.IETF:RFC2671 HTTP authentication:Basic and digest access authentication[S/OL].1999.http://www.ietf.org/rfc/rfc2671.txt.

[5] 王宇飞,范明钰.一种基于HTTP摘要认证的SIP安全通信系统的实现[D].成都:电子科技大学,2005.

[6] 李晓霞,宋茂强.基于SIP的安全通信机制的研究[D].北京:北京邮电大学,2007.

[7] Lai Jun-zuo,Kou Wei-dong.Self-generated-certificate public key encryption without pairing[C]//LNCS 4450:PKC 2007,Beijing,China,2007.Germany:Springer-Verlag,2007:476-489.

[8] Wang Xu an,Yang Xiao-yuan,Han Yi-liang.Cryptanalysis of self-generated-certificate public key encryption without pairing in PKC07,cryptology ePrint archive:Report 2008/191[R/OL].2008.http://eprint.iacr.org/2008/191.

[9] 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.

[10] Zhang Rui-shan,Wang Xin-yuan,Yang Xiao-hui,et al.Billing attacks on SIP-based VoIP systems[C/OL]//First USENIX Workshop on Offensive Technologies(WOOT'07),Boston,MA,2007.http://www.usenix.org/event/woot07/tech/full_papers/zhang/zhang.pdf.