面向 XMPP 的端到端安全通信研究

解雪妮,戴 航,罗 怡,张慧翔
(西北工业大学 自动化学院,陕西 西安 710072)

摘 要:随着即时通信系统应用的日益广泛,其安全性也成为关注的焦点。XMPP 协议的出现解决了即时通信系统的兼容问题,但伴随更多功能扩展而来的是安全问题。文中首先分析了 XMPP 协议现有的安全机制 TLS 和 SASL 协议,给出了其安全机制存在的问题。然后通过对端到端加密和签名协议的研究,给出了 IM 客户端端到端加密和签名的具体方案,并对加密系统和安全参数进行了性能测试。通过实验分析可知,采用不同的加密系统和安全参数,系统运行的时间效率不同,从而可以使用户在自身需求、操作效率和安全性之间获得最佳平衡。

关键词:即时通信;可扩展消息和出席协议;端到端安全;OpenSSL
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2015)07-0116-04
doi:10.3969/j.issn.1673-629X.2015.07.025

Research on End-to-end Secure Comunication for XMPP

XIE Xue-ni,DAI Hang,LUO Yi,ZHANG Hui-xiang
(School of Automation,Northwestern Polytechnical University,Xi'an 710072,China)

Absract:With the increasingly widespread of instant messaging system application,its security has become the focus of attention. XMPP protocol solves the instant communication system compatibility,but with more functions extension comes the security issues. In this paper,first analyze TLS protocol and SASL protocol,the existing security mechanism of XMPP,then point out the problems of them,on this basis,give the proposal of end-to-end encryption and signature for IM Client through the study of the end-to-end encryption and signature protocol,also test the performance of the encryption system and security parameters. Through the experiments,find that using different kinds of encryption system and security parameters,the effiency of the system is different,so users can achieve the optimal trade-off between the requirements of themselves,the effiency of the operation and system security.

Key words:instant messaging;XMPP;end-to-end security;OpenSSL

0 引 言

即时通信(Instant Messaging,IM)是一种基于互联网的实时通信系统,它允许两人或多人使用网络实时地传递文字消息、文件或实现语音视频交流。由于具有高效、实时和方便快捷等优点,IM 已经迅速成为个人和企业应用的重要工具。比较典型的 IM 软件有 QQ、MSN、飞信、阿里旺旺和来往等。但是在技术和应用获得巨大成就的同时,安全性和互通性也成为制约 IM 发展的主要原因所在。经研究分析发现 IM 面临的安全威胁主要有如下四种[1]:账号假冒、蠕虫传播、拒绝服务式攻击、第三方窃听。

互联网工程任务组 IETF 提出的 XMPP(eXtensible Messaging and Presence Extensions)协议是专门针对即时消息传递和处理的 XML 数据流协议[2]。作为 IM 的标准协议,它的出现可以有效解决 IM 的互通性问题,且 XMPP 自身的安全机制能在一定程度上解决 IM 面临的安全威胁问题。XMPP 的现有安全机制主要包括用户身份认证和传输过程加密两部分。身份认证采用 SASL(Simple Authentication and Security Layer,简单验证和安全层),数据加密利用 TLS(Transport Layer Security,传输层安全协议)[3]。

XMPP 的安全机制能够比较有效地解决传统的安全威胁,比如窃听、账号假冒及破解等源自外部的威胁,但是对于来自服务器的内部威胁则无能为力[4]。这是因为 XMPP 采用 C/S 架构,消息的传递要在服务器进行中转;虽然经过了 TLS 加密,但是加密之后的信息需要在服务器中被解密后再重新加密发给目标用户。这样只实现了点到点的安全,信息被泄露给了服

收稿日期:2014-08-20 **修回日期**:2014-11-21 **网络出版时间**:2015-06-23
基金项目:国家自然科学基金资助项目(61303224);西北工业大学研究生创业种子基金项目(Z2014151)
作者简介:解雪妮(1991-),女,硕士研究生,研究方向为网络与信息安全;戴 航,硕士生导师,研究方向为网络与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150623.1005.009.html

务器。这就导致了几种常见的针对服务器的安全威胁[5]:

(1)窃听者监听实体服务器的所有对外通信;

(2)攻击者攻击实体服务器以便获取该服务器的所有通信;

(3)攻击者伪装成实体服务器骗取实体连接到自己的计算机上。

针对上述安全威胁,IETF 工作组于 2013 年提出了端到端对象加密和签名草案,该草案是为基于 XMPP 协议的即时通信提供安全保护[6]。目前,还未发现针对该草案的相关实践研究,故文中考虑将该草案付诸实践,设计实现一种具备端到端安全功能的即时通信系统,从而有效提高通信的安全性。

1　XMPP 端到端对象加密和签名协议

端到端对象加密和签名协议为基于 XMPP 协议的即时通信提供了两种保证对象安全的方法。第一种方法是加密节以提供机密性保护,另一种方法是节签名以提供认证和完整性保护。这里对象通常指 XML 节,XML 节指一个 XML 节是一个实体通过 XML 流向另一个实体发送的结构化信息中的一个离散的语义单位。此协议使得两个实体可以进行高效安全的异步通信,并且允许每个实体包含多个同时运行的终端设备[7]。

1.1　端到端加密方案

端到端加密的主要思想是允许数据在从源节点到终点的传输过程中始终以密文形式存在,消息在到达终点之前不能进行解密,即使经过服务器中转也不会有消息泄露的威胁出现[8]。文中的端到端加密方案主要基于这种思想,在发送消息之前对消息节进行封装改造,实现消息节在整个传输过程中的安全。

在进行端到端加密之前,发送方需确认能获得以下内容:发送方自己的 JID/接收方的 JID(裸 JID);会话密钥 SMK/SMK 的标识符 SID(保证 SID 对于每组(sender,recipient,SMK)来说是唯一的)[9]。

文中端到端加密的主要流程如下:

(1)构造信封 M,使用<forwarded/>元素,包含时间戳<delay/>元素和明文节 S 两部分。

(2)将信封 M 转换成 UTF-8 编码的字符串 M',即 M' =UTF-8(M)。

(3)随机生成内容加密密钥 CEK 和初始化向量 IV。

(4)用会话密钥 SMK 加密 CEK,记为 E,加密算法记为 alg。

(5)构造<e2e/>节,属性 type 设置为“enc”,其中子节点包含四部分:C 和 E 分别经过 base64 编码后记为<data/>和<cmk/>,IV 经过 base64 编码之后记为<iv/>,alg||enc 经过编码之后记为<encheader/>。

(6)将<e2e/>作为明文节 S 的子节点按正常方式发送。

1.2　端到端签名方案

端到端加密主要用来保证数据的机密性,端到端签名主要用来保护数据的完整性和不可否认性。文中端到端签名的主要流程如下:

(1)构造信封 M,使用<forwarded/>元素,包含时间戳<delay/>元素和明文节 S 两部分。

(2)将信封 M 转换成 UTF-8 编码的字符串 M',即 M' =UTF-8(M)。

(3)发送方从自己的公私钥对里选择一组接收方已知其公钥的私钥,记为 PK。

(4)将 PK 作为密钥,对 M' 进行签名操作,签名值记为 I,签名算法记为 alg。

(5)构造<e2e/>节,属性 type 设置为“sig”,其中子节点包含三部分:M' 经过 base64 编码后记为<data/>,I 经过 base64 编码之后记为<sig/>,alg 经过 base64 编码之后记为<sigheader/>。

(6)将<e2e/>作为明文 S 的子节点按正常方式发送出去。

2　端到端安全即时通信系统的设计与实现

2.1　端到端安全即时通信系统总体结构

文中设计实现了一个端到端安全即时通信系统,系统包括服务器端和客户端两部分。端到端安全指的是在终端主机为即时通信系统增加安全功能,XMPP 服务器只进行消息转发功能[10],文中设计的原型系统的服务器端采用 Openfire 搭建。

客户端主要包括三部分,用户 GUI 模块、XMPP 协议栈和端到端安全代理。图 1 为客户端系统结构图。用户 GUI 模块为用户提供操作界面,主要包括登录、主界面和聊天对话框等,采用 Qt 实现。XMPP 协议栈实现和服务器端及其他客户端之间的即时消息通信,基于 Gloox 库实现[11]。端到端安全代理实现端到端对象加密和签名操作,保证通信实体之间即时消息的完整性和机密性,基于 OpenSSL 算法库实现。

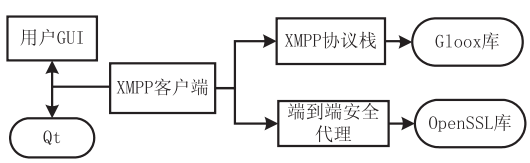

图 1　客户端系统结构图

2.2　XMPP 协议栈

即时通信系统的基本功能主要包括用户登录、消息传输、文件传输和用户好友管理等[12]。Gloox 是一个开源跨平台的 C++实现的 XMPP 协议栈,它实现了

这些基础功能。在 Gloox 开源协议栈基础上实现端到端安全,主要包括消息接收和消息发送两部分,流程图如图 2 所示。

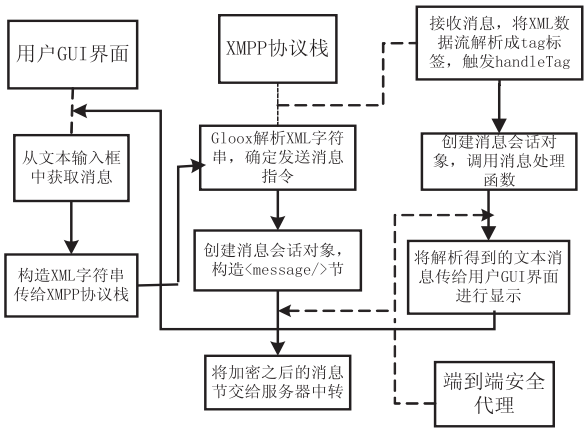

图 2 即时消息收发流程图

过程描述如下:

(1)消息发送:用户在聊天对话框中输入文字消息,点击“发送”按钮,QDomDocument 类将文本消息封装成 XML 字符串通过命名管道传给 XMPP 协议栈 Gloox[13],Gloox 的底层协议解析模块将消息解析为 XMPP 的<message/>消息节点,并利用 OpenSSL 库函数对其进行安全封装操作,然后通过底层通信模块将加密后的消息节发送到服务器进行转发。

(2)消息接收:Gloox 的底层通信模块接收到来自服务器的 XML 数据流,将其解析为 tag 标签,触发 notifyMessageHandler 监听器,并由监听器对消息进行解密等一系列操作之后将文本消息经命名管道传给用户 GUI 界面进行显示。

2.3 端到端安全代理

端到端安全代理负责为客户端之间传递的即时消息提供安全保证,主要实现两个标准功能:消息加密/解密和消息签名/确认。当用户发送消息时,可自主选择加密算法和加密参数,连同需要发送的内容一起提交,端到端安全代理会根据用户的选择对消息进行安全封装操作。服务器收到此种类型的加密消息,只需要获取到目标用户的地址,而不会试图对加密的消息进行解密操作,所以即使服务器遭到攻击,用户之间发送的消息也不会泄露,服务器这时执行真正的”转发”功能。

如图 2 所示,端到端安全代理基于 OpenSSL 加密算法库实现,使用 OpenSSL 提供的高级加密函数 EVP 封装了所有的加密算法,使得各种算法能够使用统一的 API。文中针对消息加解密采用对称加密算法,使用 EVP API 中的 EVP_Encrypt 和 EVP_Decrypt 函数;针对消息签名采用非对称加密算法,使用 EVP API 中的 EVP_Sign 和 EVP_Verify 函数。

3 实验测试

为了测试端到端安全即时通信系统采用何种加密算法和安全参数才能更好地满足用户需求,对时间效率进行了测试评估。时间效率是衡量一个加密算法性能的重要标准,对于不同的加密算法,采用不同的安全参数,它们的加解密时间会有较大差距[14]。根据实验图分析比较各个加密算法的时间效率,方便用户更好地选择加密系统和安全参数。

针对时间效率的测试分为三种,主要是改变输入长度、密钥长度和加密算法种类三个参数。注意两点:

(1)此处的输入长度是相对于用户聊天界面来说的,而不是加密算法真正的明文长度。

(2)测试得到的运行时间是包括加解密时间在内的消息发送和接收的时间,单位是 ms。

· 定长明文和密钥,不同加密算法。

选取 DES、IDEA、CAST、AES_128、RC4 这五种算法以及不进行加密(图 3 中记为 None)的消息发送和接收时间进行测试。测试时统一标准,均采用 128 位密钥长度(DES 是 64 位密钥)和 128 位明文输入,每组加密算法测量多次,然后求其平均值,得到的时间效率图如图 3 所示。

实验预期结果:不加密时时间最快,其次是 RC4 算法和 AES 算法,IDEA 算法和 CAST 算法时间相当,DES 算法由于算法结构问题速度最慢。

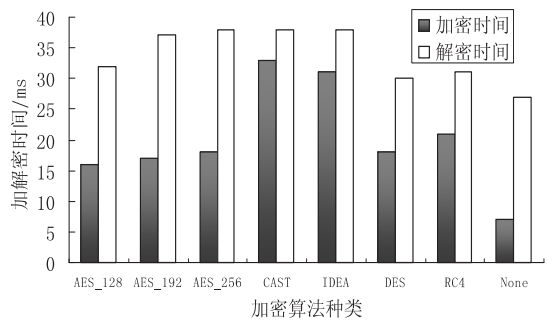

图 3 不同加密算法时间效率图

· 定长明文,同一加密算法,不同密钥长度。

选取 AES 加密算法,输入明文长度为 128 位,密钥长度分别为 128 位、192 位和 256 位,得出变密钥长度加密算法的时间效率图如图 3 所示。

· 定长密钥,同一加密算法,输入明文长度不同。

选取 AES 加密算法,采用 128 位密钥长度,输入明文长度从 64 位 ~ 2 048 位变化,得出变明文长度加密算法的时间效率曲线如图 4 所示。

分析上述两个时间图,发现图 3 所得的结果并未按预期发展,RC4 算法相对预期值慢很多,甚至比 DES 算法时间还要长。变明文长度和变密钥长度的加解密时间图基本和预期一致,随着密钥长度和明文长度的增加,AES 算法轮询次数增加,加密时间也随之增长。

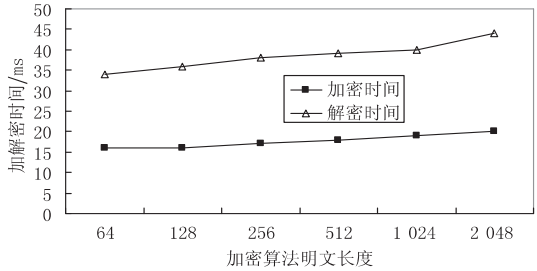

图 4　变明文长度加密算法时间效率图

为了进一步研究图 3 产生非预期情况的原因,进行了 CPU 利用率测试,主要针对 DES 和 RC4 算法。检测到了采用 DES 算法和 RC4 算法时的 CPU 利用率,如图 5 所示。

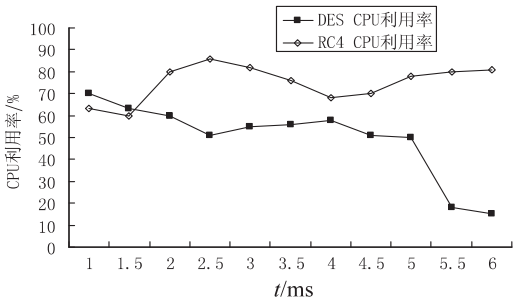

图 5　DES 和 RC4 算法的 CPU 利用率图

从图中可以看出,在采用 DES 算法时,CPU 利用率相对采用 RC4 算法时要低很多,这也就很好地解释了 DES 加解密速度比 RC4 要快的原因。由于和预期值不符,猜测应该是采用 OpenSSL 封装算法的原因,内部优化程度不同,导致使用结果与理想预测存在一定偏差。

通过时间效率评估实验可知,虽然采用加密算法对即时通信系统收发消息时间产生了一定影响,但基本都维持在十几毫秒以内,并不会对即时消息的传输产生较大干扰,这充分说明端到端安全即时通信系统方案是可行的,且时间测试也在一定程度上为用户在自身需求和操作效率之间寻找平衡提供了支持。

4　结束语

文中依据 XMPP 的端到端对象加密和签名协议设计实现了一个具备端到端安全的即时通信原型系统,并对系统的时间效率进行了测试评估。实验结果表明,该原型系统方案是可行的,能为基于 XMPP 协议的即时通信系统提供安全保护。

参考文献:

[1] Gurel, Oral, Cakir M U. Promising XMPP based applications for military and defense systems[C]//Proceedings of IEEE 37th annual conf on International computer software and applicationse. Kyoto: IEEE, 2013: 716-717.

[2] Saint-Andre P. RFC3920: Extensible Messaging and Presence Protocol (XMPP) Core[S/OL]. 2004. http://www.ietf.org/rfc/rfc3920.txt.

[3] Klauck R, Kirsche M. XMPP to the rescue: enhancing post disaster management and joint task force work[C]//Proceedings of pervasive computing and communications workshops. [s.l.]: [s.n.], 2012: 752-757.

[4] Herbsleb J D, Atkins D L. Introducing instant messaging and chat in the workplace[C]//Proceedings of the seventh European conference on computer-supported cooperative work. [s.l.]: [s.n.], 2012: 171-178.

[5] Saint-Andre P. Requirements for end-to-end object encryption in the Extensible Messaging and Presence Protocol (XMPP)[EB/OL]. 2010. http://tools.ietf.org/html/draft-ietf-xmpp-e2e-requirements-01.

[6] Miller M. End-to-end object encryption and signatures for the Extensible Messaging and Presence Protocol (XMPP)[EB/OL]. 2013. http://tools.ietf.org/html/draft-miller-xmpp-e2e-06.

[7] 侯　可. 一种基于 XMPP 的企业即时消息技术[J]. 科技情报开发与经济, 2008, 18(26): 146-148.

[8] 潘振香, 翟明岳. Jabber 协议在即时通信系统中的应用[J]. 网络安全技术与应用, 2007(10): 79-81.

[9] 杜　玲, 苗　放, 李　刚. XMPP 协议研究及其在 IM 系统群组通信中的应用[J]. 湖南工程学院学报: 自然科学版, 2008, 18(3): 71-75.

[10] Saint-Andre P. RFC3921: Extensible Messaging and Presence Protocol(XMPP) instant messaging and presence[S/OL]. 2004. http://www.ietf.org/rfc/rfc3921.txt.

[11] 张　震, 刘　勃. 基于 XMPP 协议的 Jabber 及 Web 客户端应用实践[J]. 中国新通信, 2009(15): 60-62.

[12] 谢　波, 蒋志平. XMPP 研究与应用[J]. 科技广场, 2008(10): 30-31.

[13] 潘　凤, 王华军, 苗　放, 等. 基于 XMPP 协议和 Openfire 的即时通信系统的开发[J]. 计算机时代, 2008(3): 15-16.

[14] 乔道迹, 李宏宇. 基于 Jabber 协议的移动即时通讯系统研究与实现[J]. 计算机与信息技术, 2008(7): 23-26.

面向XMPP的端到端安全通信研究

作者： 解雪妮， 戴航， 罗怡， 张慧翔， XIE Xue-ni， DAI Hang， LUO Yi， ZHANG Hui-xiang

作者单位： 西北工业大学 自动化学院,陕西 西安,710072

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2015(7)