

基于 XML 的移动艾滋病信息管理系统安全设计

徐海峰, 王秋光

(哈尔滨理工大学 电气与电子工程学院, 黑龙江 哈尔滨 150080)

摘 要:移动艾滋病信息管理系统可实现医护人员和疾病控制中心信息的时时交互. 利用该系统, 医护人员可以对已患艾滋病患者进行及时、正确的救治, 疾病控制中心可以时时掌握艾滋病疫情情况, 对该地区艾滋病疫情的预防和控制起到积极的作用. 以 XML 安全规范为基础, JavaME 为开发平台, 按照端到端的安全架构设计了移动艾滋病信息管理系统安全模型, 基本实现了系统消息的机密性、完整性、真实性和不可抵赖性要求.

关键词: XML; 安全模型; 艾滋病; 信息管理系统

中图分类号: TP393 **文献标志码:** A **文章编号:** 1007-2683(2011)01-0080-05

Design of Mobile AIDS Information Management System Security Based on XML

XU Hai-feng, WANG Qiu-guang

(School of Electrical and Electronic Engineering, Harbin University of Science and Technology, Harbin 150080, China)

Abstract Mobile AIDS information management system can be used to implement information constantly interact for health care workers and Disease Control Center. Using this system, the medical staff can give AIDS patients correct treatment timely, and Disease Control Center can always grasp the situation of the AIDS epidemic, which will play a positive role for the AIDS epidemic prevention and control in an area. This paper, based on XML security specifications and JavaME platform for the development, designed a mobile AIDS information management system security model in accordance with the end-to-end security architecture. The system achieve message confidentiality, integrity, authenticity and non-repudiation requirements basically.

Key words XML; security model; AIDS; information management system

0 引 言

随着移动通信技术和无线网络技术的快速发展, 移动 Web 服务逐渐在全球范围内普及, 真正实现了在任何时间、任何地点获取网络服务的目标. 但移动 Web 服务并没有以人们预料的速度迅速普及, 主要的瓶颈就在于安全保障没有得到很好地解决.

因此, 移动应用领域内的研究已经越来越多的集中到了移动应用的安全方面^[1].

在 JavaME 体系中, 标准的 CLDC 和 MIDP 都不提供加密 API^[2]. 因此, 要实现一个完整的无线网络安全结构, 就需要一个或多个第三方厂商提供的 JCE 产品, 称为安全供应者. 提供安全供应者的公司有 IBM, Bouncy Castle 等公司^[3].

利用移动 Web 服务部署移动艾滋病信息管理

收稿日期: 2009-11-11

作者简介: 徐海峰 (1981—), 男, 硕士研究生, E-mail: beyondain981@163.com;

王秋光 (1949—), 男, 硕士生导师.

系统,可以实现医护人员和疾病控制中心艾滋病患者信息的时时交互,对艾滋病患者进行及时、正确的救治以及对艾滋病疫情的预防和控制起到积极的作用.但现实中存在的安全问题成为该系统正常运行的最大障碍. XML 是 Web 服务的基础,所以认真研究 XML 安全规范,利用 XKMS 实现系统的公钥安全,利用 XML 加密和签名技术实现系统数据的安全,对于移动艾滋病信息管理系统顺利部署和正常运行具有很好的现实意义和应用价值.

1 XML 安全规范

XML 安全规范^[4]为保证 XML 文档和 XML 消息的应用层安全提供了解决方案,可以应用到许多领域和各种系统. XML 安全规范主要有 XML 签名规范、XML 加密规范和 XKMS 规范^[5].

1.1 XML 签名规范

XML 签名规范定义的语法和处理规则提供了在 XML 文档的不同部分添加多个签名的灵活性,从而支持多方对文档的不同内容进行签名. XML 签名可以对任何数字内容或数据对象进行签名,如 XML 或 HTML 文档、二进制数据和图像.

1) XML 签名的表示方式. XML 签名有三种表示方式:封内签名, XML 签名嵌入原始 XML 文档内容中;封外签名,原始 XML 内容嵌入 XML 签名中;分离签名, XML 内容位于数字签名外,并通过 URI 或转换标识,这种方式适用于签名文档外的数据对象和作为同胞元素位于原始 XML 文档中的数据对象.

2) XML 签名的基本结构. 用 XML 元素表示 XML 数字签名,它们是 < Signature> 元素. 原始数据经过摘要和签名后嵌入到 < Signature> 元素中. 以下代码显示了 XML 签名的核心结构和元素(其中,“?”号表示 0 个或 1 个匹配项,“+”号表示 1 个或多个匹配项,“*”号表示 0 个或多个匹配项):

```
< Signature ID? >
< SignedInfo>
< CanonicalizationMethod />
< SignatureMethod />
( < Reference URI? >
( < Transform s> )?
```

```
< DigestMethod>
< DigestValue>
< Reference> ) +
< /SignedInfo>
< SignatureValue>
( < KeyInfo> )?
( < Object ID? > ) *
< /Signature>
```

1.2 XML 加密

在 XML 加密中,加密后的数据以 XML 格式来表示,并且由 < EncryptedData> 元素来标识,该元素包含数据的密文. 被加密的数据可以是 XML 元素,也可以是包括完整 XML 文档在内的任何数据. 加密密钥值是由 < EncryptedKey> 元素来标识.

XML 加密的基本框架及核心元素可以表示如下:

```
< EncryptedData ID? Type? MimeType? Encoding? >
< EncryptionMethod />?
< ds KeyInfo>
< EncryptedKey>?
< AgreementMethod>?
< ds KeyName>?
< ds RetrievalMethod>?
< ds * >?
< /ds KeyInfo>
< CipherData>
< CipherValue>?
< CipherReference URI? >?
< /CipherData>
< EncryptionProperties>?
< /EncryptedData>
```

1.3 XML 密钥管理规范

XKMS (XML 密钥管理规范)^[6]主要用于公钥的注册及管理,并且结合 XML 数字签名和 XML 加密规范,提高网络数据传输的安全性. XKMS 规范包含两部分, X-KISS (XML 公钥信息服务规范) 和 X-KRSS (XML 公钥注册服务规范). X-KISS 用于公钥的定位和查询等服务, X-KRSS 用于公钥的注

册. XKMS一般用于与公钥基础设施 (PKI) 技术结合, 以简化公钥的注册、管理和查询服务, 减少客户端应用程序设置的复杂性, 降低与 PKI 建立信任关系的复杂度.

2 基于 XML 的移动 Web 服务系统安全模型

安全是一个涉及面很广的重要问题, 在软件系统的各个环节中都至关重要. 信息安全的目标主要有以下 4 个方面: 机密性, 完整性, 真实性, 不可抵赖性^[7].

安全模型的设计以满足以上要素为准则. 基于 XML 的移动安全方案的设计思想是: 保护内容而不是连接的安全策略, 采用安全的 XML 作为信息传输格式. 在移动终端利用 JavaME 程序实现 XML 文档的加密、数字签名等安全处理; 通过基于 XML 的消息传递机制与 XKMS 接口通信获得公钥管理服务, 从而实现与应用服务器之间的安全通信.

系统中 XML 数字签名使用 RSA 算法, 这种算法基于大素数因子的分解, 是目前被广泛接受的通用公钥加密算法. 加密算法将使用对称加密算法中的 AES 算法, 它安全性与 3DES 相当, 但具有更好的执行性能^[8].

2.1 系统公钥管理

由于 PKI 的部署非常繁琐, 每个用户都要自己验证他们与之通信的每个用户的身份, 以确保对方的身份真实有效, 这对于系统的开发人员来说是相当困难的, 所以, 我们选择 XKMS 服务器作为中间层, 使得客户端和 Web 服务器可以共享 XKMS 服务来处理彼此的公钥注册和验证请求, 将复杂性从客户机应用程序转移到了基础设施层^[9].

首先, 移动客户端和 Web 服务器端分别生成各自的密钥对, 利用注册服务在 XKMS 服务器上注册各自的公钥. 公钥注册完成后, 我们假设移动客户端要上传消息给 Web 服务器, 那么移动客户端要向 XKMS 服务器发出一个查询请求, 查询 Web 服务器的公钥. 由于 Web 服务器已经在 XKMS 服务器注册了自己的公钥, 所以, XKMS 服务器将 Web 服务器的公钥以响应的方式发送给移动客户端. 移动客户端收到 Web 服务器的公钥后使用该公钥加密所要发送的消息, 并且用自己的私钥签署消息, 然后将消息发送给 Web 服务器.

Web 服务器收到来自移动客户端的消息后, 首先向 XKMS 服务器查询移动客户端的公钥, 然后利

用该公钥验证移动客户端的签名, 如果签名通过, 那么就用自己的私钥对密文消息进行解密, 获得解密后的明文消息.

XKMS 的交互过程如图 1 所示.

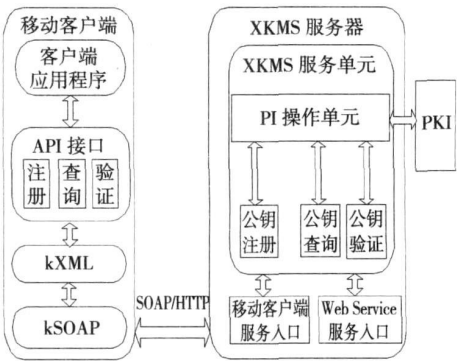


图 1 XKMS 的交互过程

2.2 系统安全模型

系统安全首要解决的问题是真实性问题, 也就是身份认证的问题. 通过用户名和口令进行身份认证是最简单、最常见的认证方式, 也是最快速、最方便的认证方式.

操作的不可抵赖性通过数字签名来实现. 发送数据端在发送消息前进行数字签名, 接收端收到消息后, 验证签名, 如果验证通过则证明消息是由声明的发送方发送的, 如果验证没有通过则拒绝接受消息.

信息的完整性同样可以通过数字签名的方式来实现. 因为在进行数字签名前, 要先通过一个散列函数对要签名的消息产生一个散列值, 然后再对散列值进行签名, 这可以大大缩短签名时间, 并提高安全性. 而散列函数具有差错检测能力, 原始消息的任一位发生改变都会导致散列值的改变, 从而导致签名的改变, 因此, 接收端可由此判断消息是否完整. 本系统采用 SHA-1 散列算法.

消息的机密性要由加密技术来实施. 发送端先生成一个随机的 AES 对称密钥, 并用该对称密钥对消息进行加密, 然后再由事先接收到的接收端的非对称密钥的公钥来对该随机的对称密钥进行加密, 然后将加密后的密文和密钥信息一起发送给接收端.

本系统安全算法的实现用适用于 JavaME 客户端的第三方工具包 Bouncy Castle 来提供^[10]. 由于我们的研究重点在移动客户端, 因此服务端和数据库以及 XKMS 服务器端的实现我们不做具体介绍. 系统的安全架构如图 2 所示.

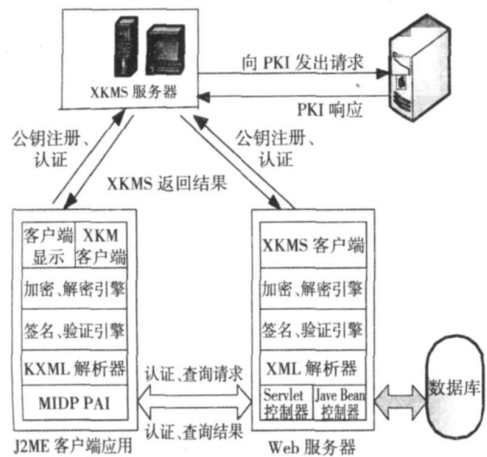


图 2 系统安全架构图

3 安全模型在移动艾滋病信息管理系统中的应用

由于人们认识上的偏见以及对艾滋病的恐惧, 艾滋病患者往往受到不公正的待遇, 甚至是歧视, 为了保护患者的合法权益, 对患者的个人信息保密成为医护人员义不容辞的责任和义务. 所以, 在移动艾滋病信息管理系统中, 需要对患者的所有个人信息做好保密工作.

该系统实现了医护人员与疾控中心的实时信息共享. 主要包括两大功能: 一是医护人员及时发现新发艾滋病患者, 及时向疾控中心上报患者的个人信息, 如姓名, 年龄, 身份证号, 家庭地址以及患病情况; 二是查询艾滋病患者的个人信息, 以便对患者进行更好的救治. 系统分 3 个部分: 移动客户端、服务提供端、数据库. 在移动客户端, 主要包括两个功能模块: 患者信息上报和患者信息查询. 服务提供端接收客户端上报的信息以及提供客户端要查询的信息.

3.1 系统流程

1)移动客户端公钥注册. 移动客户端公钥注册界面如图 3所示.



图 3 公钥注册界面

客户端首先通过软件系统生成一对公、私钥对, 通过客户端软件中的 XKMS 客户端向 XKMS 服务器注册自己的公钥, XKMS 服务器通过注册后向客户端返回注册成功信息.

2)注册登录. 用户启动移动艾滋病信息管理系统后, 首先要进行身份验证, 系统将会连接服务器, 获取用户的注册帐号信息, 然后与当前用户的输入信息进行比较, 如果该用户名不存在则提示用户应该先注册, 如果密码错误则提示用户重新输入, 只有验证通过才能应用系统.

3)患者信息上报. 医护人员利用该模块上传新确诊的艾滋病患者的个人信息以及病情, 服务器端接收到该信息后进行登记统计, 存储到数据库.

4)患者信息查询. 患者信息查询界面如图 4 所示.

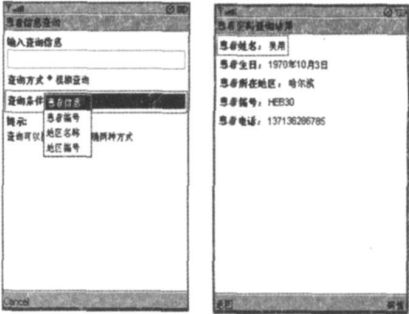


图 4 患者信息查询界面

医护人员通过该模块查询艾滋病患者信息, 以便对患者进行更好的救治以及做好该疾病的预防工作.

3.2 系统的实现

1)开发环境及工具. Eclipse Eclipse 是一个开放源代码的、基于 Java 的可扩展开发平台. 用于通过插件组件构建开发环境.

WTK 2.5.2 它支持 MIDP 应用程序的创建, 并提供了一个手机模拟器.

Bouncy Castle 第三方的安全工具包, 提供各种加密、签名的密码术包.

kSOAP 包: 应用于移动设备端的第三方 Web 服务解析工具包.

kXML 包: 适用于移动设备端的轻量级 XML 解析工具包.

2)移动客户端公钥注册. 移动客户端首先要产生一对公私钥, 完成在 XKMS 服务器端的公钥注册. 下面以在移动客户端使用 Bouncy Castle Crypto API 的 RSA 算法实现生成一对公私钥为例, 说明在

移动客户端产生公私钥的过程.

```
private static BigInteger pubExp= new BigInteger
(“ 11”, 16);
SecureRandom sr= new SecureRandom ();
RSAKeyGenerationParameters RSAKeyGenPara=
new RSAKeyGenerationParameters ( pubExp sr 1024
80);
RSAKeyPairGenerator RSAKeyPairGen = new
RSAKeyPairGenerator();
RSAKeyPairGen.init(RSAKeyGenPara);
AsymmetricCipherKeyPair keyPair = RSAKeyPairGen
generateKeyPair();
PrivateKey = ( RSAPrivateC rKeyParameters ) key-
Pair.getPrivate();
PublicKey = ( RSAKeyParameters ) keyPair.getPublic
();
```

生成的公钥发送到 XKMS端进行公钥注册, 私钥保存到本地密钥库用来进行签名和解密.

3)身份验证. 本系统的身份验证在移动客户进行合法身份注册的同时一并完成, 节省了很多系统资源和时间. 首先, 移动客户用自己的用户名和密码在移动艾滋病信息管理系统进行注册, 用户名采用明文传输, 而密码和注册请求采用密文传输. 密码和注册请求先用客户自己的私钥进行加密, 然后再用通过 XKMS服务器上查询获得的 Web服务器端的公钥进行加密, 把加密后的信息发送给 Web服务器. Web服务器接收到注册信息后, 先用自己的私钥进行解密, 如果可以解密, 则接收, 不能, 则拒绝, 因为只有真正的 Web服务器才拥有其私钥, 所以该过程也同时完成了客户端对 Web服务器端的身份认证; 然后再用通过 XKMS服务器获得的移动客户的公钥进行解密, 如果解密通过, 则注册成功, 解密不通过, 则注册失败, 这样就完成了服务器对客户的认证. 服务器把注册成功的客户信息存储到注册用户信息库. 客户端与服务器端在完成注册的同时, 也完成了彼此身份的认证, 注册成功的用户只须通过用户名和密码进行登陆即可应用系统服务.

客户端注册流程如图 5所示.

4)数据加密和签名. 客户端先随机生成一个 AES对称密钥, 用此密钥加密要发送的明文数据; 再从密钥库中读取自己的 RSA私钥, 对要发送明文数据的摘要进行数字签名; 最后再用服务端的 RSA公钥将对称密钥进行加密, 加密处理完后重新格式化为 SOAP的形式发送给服务端. 服务端接收到客户端发

送过来的 SOAP信息后, 先从密钥库中读取自己的 RSA私钥, 并对消息进行解密, 获得 AES对称密钥; 再用 AES对称密钥解密消息, 获得客户端发来的数据; 然后再用客户端的公钥验证其签名, 若验证通过则接受其请求, 同时获得客户端的摘要, 验证不通过则拒绝服务; 最后服务器端用同样的摘要算法对解密出来的明文数据进行摘要计算, 计算后与客户端摘要进行比对, 若一样, 则输出明文, 不一样, 则拒绝服务. 图 6描述了系统中消息签名和加密的数据流程.

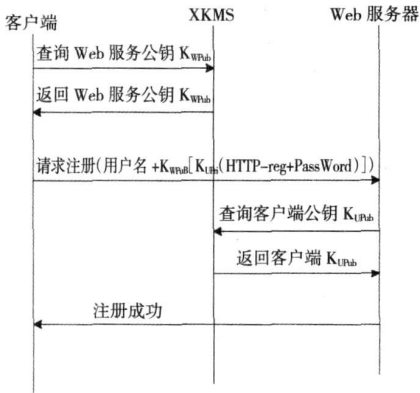


图 5 客户端注册流程

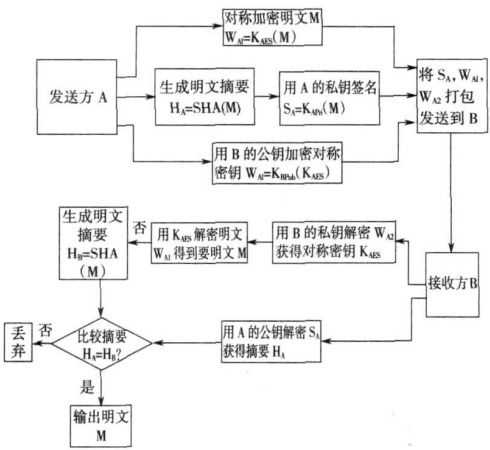


图 6 数据签名、加密流程图

4 结 语

根据移动艾滋病信息管理系统的特点设计了一个基于 XML的移动艾滋病信息管理系统安全模型, 并在客户端进行了实现. 系统中, 利用 XML加密技术, 采用 RSA非对称密钥算法和 AES对称密钥算法设计了一个端到端的安全架构, 基本实现了系统消息的机密性、完整性、真实性和不可抵赖性要求.

(下转第 89页)

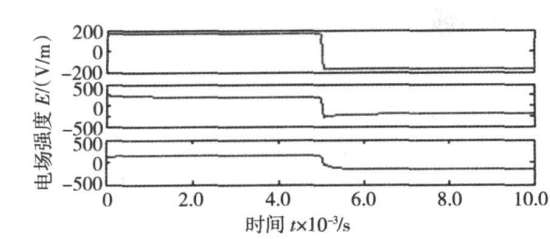


图 8 电阻率之比为 1:1 时场强曲线

4 结 论

- 1) 在油纸复合绝缘系统中, 极性反转电压会引起油、纸中电场强度重新分配的过渡过程. 在此过程中油中电场会出现一个很高的场强.
- 2) 影响油中电场畸变程度的因素主要是电压反转过程持续的时间及纸板和油的体积电阻率之比、介电常数之比、厚度之比、油的介电常数和纸的体积电阻率之积.
- 3) 电场的畸变程度随着电压反转时间的增加而减小, 随着电阻率比值的增加而增加, 与其它几种因素的关系不是单调的.

参 考 文 献:

- [1] 宓传龙. 超高压换流变压器和平波电抗器绝缘结构简述 [J]. 高压电器, 2003 39(1): 7- 15
- [2] 傅铁军, 王建, 钟俊涛, 等. 直流输电 ±800kV 换流变压器的绝缘结构分析 [J]. 变压器, 2009 3(6): 1- 5
- [3] 陈庆国, 张杰, 高原, 等. 混合电场作用下换流变压器阀侧绕组电场分析 [J]. 高电压技术, 2008, 3(3): 484- 488
- [4] 李文平, 陈志伟, 宋秀生. ±800kV 直流输电工程用换流变压器主绝缘结构的分析 [J]. 电力设备, 2008, 3(8): 5- 7.
- [5] 王冰, 王清璞, 孙优良. 换流变压器阀侧绕组端部极性反转瞬态电场的计算分析 [J]. 变压器, 2007, 6(6): 11- 15
- [6] 贺以燕. 高压直流换流变压器结构、标准及试验 [J]. 电力设备, 2006, 11(7): 53- 57
- [7] 吕晓德, 陈世坤. 换流变压器端部极性反转电场的数值算法及其绝缘设计 [J]. 西安交通大学学报, 1997, 11(11): 8- 12
- [8] 梁鹏, 魏新劳, 陈庆国, 等. 极性可反程控高压发生器的设计 [J]. 黑龙江水专学报, 2007 34(2): 87- 90
- [9] FORREST JA C, ALLARD B. Thermal Problems Caused by Harmonic Frequency Leakage Fluxes in Three-phase Three-winding Converter Transformers [J]. IEEE Transactions on Power Delivery, 2004 19(1): 208- 213.
- [10] 王春玲, 李建华. 换流变压器阀侧绕组极性反转试验端部电场的计算与分析 [J]. 变压器, 2005 42(2): 11- 14

(编辑: 温泽宇)

(上接第 84 页)

参 考 文 献:

- [1] 石勇. Web 服务安全问题及其对策研究 [D]. 北京: 北京师范大学, 2008 7- 10.
- [2] (美) LIGong GARY Ellison, MARY D ageforde 深入 Java™ 2 平台安全——体系架构、API 设计和实现 [M]. 2 版, 朱岱, 译. 北京: 电子工业出版社, 2004. 9: 35- 41
- [3] 杨建强. 无线 Java 安全研究 [D]. 武汉: 武汉理工大学, 2005: 23- 25
- [4] BLAKE Doumaee XML 安全基础 [M]. 周永彬, 贺也平, 刘娟译. 北京: 清华大学出版社, 2003: 94- 172 207- 255
- [5] (美) 多尼, 周永彬, 贺也平. XML 安全基础 [M]. 刘娟译. 北京: 清华大学出版社, 2003: 78- 90
- [6] 郑志华. 基于 XKMS 的 PKI 服务研究与实现 [D]. 青岛: 山东大学, 2005: 12- 14
- [7] 马恒大. Web 服务安全 [M]. 北京: 电子工业出版社, 2007: 124- 132
- [8] ENGELEN V, RRBERT A, ZHANG W. An Overview and Evaluation of web Services Security Performance Optimizations [C] // IEEE ICWS, Beijing 2008 137- 144.
- [9] 王晓俊, 周晓峰, 王志坚. 基于 PKI/PMI 的 Web 服务安全框架 [J]. 计算机科学, 2008(4): 67- 69.
- [10] 姚一永, 沈琳. 基于 Bouncy Castle Crypto API 的无线 Web Services 应用安全 [J]. 计算机应用, 2004(3): 46- 57.

(编辑: 王 萍)