文章编号:1005-0523(2008)03-0082-04

基于WPKI的3G认证方案的研究与实现

张跃进,谢 昕,黄德昌

(华东交通大学 信息工程学院,江西 南昌 330013)

摘要:通过对现有的3G安全认证中身份机密性设计的研究与分析,目前3G的接入端鉴权认证是3G安全体系认证阶段的薄弱环节,可以应用Internet及电子商务上成熟的WPKI技术来实现用户身份的实体认证问题,因此提出一种基于WPKI环境下实体认证方案,对比现有的3G中的身份认证实现措施,经过改进给出了一种新的基于WPKI环境下的用于实现3G认证的具体方案,并对方案实现过程作了简要介绍,应用该方案可以增强3G认证环节的安全性.

关 键 词:WPKI;3G;认证;安全

中图分类号:TP309 **文献标识码**:A

第三代移动通信系统(3G)安全体系结构是在改进了第二代数字蜂窝移动通信系统(2G)的弱点,适应移动通信业务新要求的目标和原则基础上建立起来的.3GPP(第三代移动通信系统伙伴计划)安全协议中的认证与密钥管理部分比2G有很大的提高.认证与密钥管理是3G安全中最重要的特性之一,认证是对实体的身份进行确认.该实体必须出示它的身份来认证自己[1].3G接入网部分的实体认证包含认证机制协商、用户身份认证、用户对他所连接的网络进行认证.两个实体之间的认证可采用零知识证明来表示它知道某个只有它才知道的秘密或借助第三方可信机构来出面担保.

随着终端处理能力的提升,公钥体制在实现用户身份机密性的过程中,相比单钥体制具有更多的优势.在单钥体制下,用户的安全依赖于网络,而现在使用公钥技术来保护用户的身份,用户的私钥只有用户自己知道,身份的机密性不再依赖于网络[2].随着3G技术的飞速发展以及无线公钥基础设施(WPKI)相关技术的应用,WPKI在3G中的应用也会越来越成熟.

1 3G中已有的身份机密性设计

目前3G采用了两种机制来识别用户身份.其一,用户与服务网之间采用临时身份机制,采用临时身份(TMSI)识别用户以保护在无线链路上传输的永久用户身份(IMSI),并隐藏其位置,为了实现用户的不可跟踪性要求TMSI要定期更换.其二,使用加密的永久身份IMSI,但3G标准没有排斥用户直接使用IMSI进行身份识别,任何可能暴露用户身份的信令和用户数据都要求进行加密.

3G系统执行认证与密钥分配协议(AKA),在移动台和服务网络之间进行双向认证,在互相确认对方身份的基础上生成数据加密密钥(CK)和数据完整性密钥(IK),为下一步的数据传输做准备.相对于2G,3G中增加了密钥协商机制,加密算法协商和完整性密钥协商都是通过用户和网络之间的安全协商机制实现的[3].

3G安全机制完全建立在用户终端(MS)和本地环境/归属位置登记处(HE/HLR)之间共享密钥(K)的基础之上.若密钥K泄漏,那么通信中的安全将无从谈起,攻击者可以轻而易举地在空中截获参与

收稿日期:2008-03-15

基金项目:华东交通大学研究生创新资金项目(YC07C009);江西省自然科学基金资助项目(2007GZS0886).

作者简介:张跃进(1978-),男,湖北钟祥人,华东交通大学信息工程学院讲师,硕士,研究方向为通信系统安全.

加密的随机数(RAND),并用相关算法取得相互认证且计算出 CK 和 IK,从而通信中的所有数据都可以被攻击者截获.由于密钥 K 是长期不变的,所以一旦泄漏 K 将对用户和网络运营商造成不可估量的损失[4~5].

在 3G 中,当服务网络不能通过 TMSI 来识别用户身份时,将使用永久用户身份标识来鉴别用户身份,特别是在移动用户第一次在服务网络内注册,以及网络不能由用户在无线链路上的 TMSI 获得相应的 IMSI 时.用户的永久身份是一个敏感而且非常重要的数据,需要得到很好的保护,用户的永久身份是用明文的形式发送的,因此 3G 需要对此进行安全改进.

2　WPKI 应用下的实体认证

WPKI 技术是一项不断发展和完善的技术,它能够从技术上保证无线通信的安全,从而满足 3G 对安全的要求.随着移动通信技术及信息安全技术的发展,人们对不受时空限制的无线数据服务的需求会不断增加,移动支付、移动商务、移动订票、移动娱乐等业务会不断发展,它们都对安全性有很高的需求,这些都会促使 WPKI 更加完善,保障服务的安全性[6~7].

在 3G 中,WPKI 主要为 3G 提供的安全服务中涉及无线传输层安全协议(WTLS)提供安全策略.根据 WPKI 规范,WPKI 系统实现包括认证发布系统认证机构(CA)、注册审批中心(RA)、3G 网关、用户终端的安全嵌入模块、公共接口(PUB)等部分[8].图 1 是实现 WPKI 的示意图.

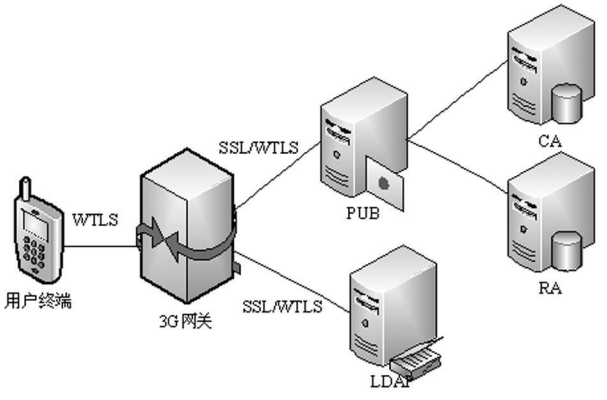

图 1　WPKI 的实现

该系统中各个组成部分功能如下:

(1) 用户终端　用户应该拥有两个密钥对,一个用于认证和密钥协商,一个用于数字签名,用户应该为这两个密钥分别向 HE 申请证书,以建立初始信任.用户也存储一定数量的 CA 证书,这些 CA 为 3G 用户和应用服务器颁发证书,为两者之间建立信任关系.

(2) 3G 网关　在 3G 用户成功接入 3G 网络后,3G 网关就为 3G 与服务器之间的数据传输进行转发,这种数据转发对 WTLS 是透明的.

(3) 服务器　CA 负责用户对证书申请、撤销申请等请求,对 CA 实现管理;RA 负责证书的颁发和管理;PUB 是用户实现证书申请、下载、撤销等请求的接口.

以下是在 3G 中基于 WPKI 的用户和网络服务商之间双向认证的一个详细过程:

(1) 用户终端与服务网络进行相互认证,用户终端获得授权访问网络资源;

(2) 服务器向 WPKI 入口请求证书;

(3) WPKI 入口确认手机的 ID,把证书转发给认证机构;

(4) 认证机构给服务器颁发证书;

(5) 用户终端经过 3G 服务网络和 3G 网关向 WPKI 入口请求证书;

(6) WPKI 入口确认用户 ID,把证书请求发给认证机构;

(7) 认证机构产生用户证书,把证书 URL 发给用户终端;

(8) 认证机构把用户证书发布到数据库;

(9) 用户终端用认证公钥与服务器建立 WTLS 会话.

系统的实现主要是基于公共网关界面(CGI)程序,用户请求等通过 WEB/WAP 页面提交给后台的 CGI 程序,CGI 程序做自己的工作,对数据进行后台处理,根据结果返回相应的回应页面代码到服务器,服务器再把代码送给浏览器来显示.

系统支持广泛使用的 X.509 证书,同时支持 WTLS 证书.支持的公钥加密算法包括 RSA 和 ECC 算法.实现了基于轻量目录访问协议(LDAP)和超文本传输协议(HTTP)格式的统一资源定位(URL)证书检索、证书状态查询功能.认证中心可以进行证书的颁发、证书的撤销;注册中心可以验证用户身份,审批证书申请请求和证书撤销请求,并与 LDAP 服务器交互实现快速证书查询;LDAP 服务器可以存放证书、CRL 等供用户查询、下载;用户可以方便地登录到入口,进行证书的申请、撤销和查询.

3 基于 WPKI 的认证方案实现

根据 WPKI 系统设计方案，在 3G 网络中加入 CA 及 RA，用于验证用户身份、颁发和恢复证书；每个用户都拥有一对在入网的时候由公众陆地移动电话网(PLMN)产生的密钥对，一个用于 AKA，一个用于数字签名，其中私钥存储在用户业务识别模块(USIM)卡中；3G 网络中每一个参与 AKA 过程的网络组件，必须有一对密钥以及相应的数字证书；每一个参与 AKA 过程的网络组件必须持有现有的 PLMN 中存在的所有 CA 的公钥；3G 网络中至少有一个隶属于 PLMN 中的 CA 的存储数据库，存储所有的数字证书；至少有一个隶属于 PLMN 中的 CA 的证书恢复数据库，核心网中的所有组件都可以访问到它，然后进行证书验证.

首先 WPKI 实体都要求具有一个公钥证书，有了公钥证书，实体间才可以通过证书鉴定的方式来建立起信任关系，也更方便进行认证. 为了保证用户与其公钥的一一对应. 证书权威需要首先验证终端实体的身份.

证书颁发、认证过程的算法实现具体过程如下图 2 所示.

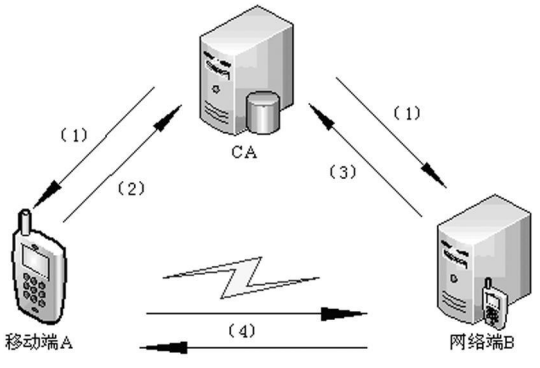

图 2 证书颁发、双向认证的过程

(1) 先初始化移动端 A、网络端 B；

(2) 移动端 A 向 CA 中心请求验证通过；

(3) 网络端 B 向 CA 中心请求验证通过；

(4) 移动端 A 和网络端 B 进行双向认证.

证书颁发过程可以采用离线的方式，如在 USIM 的生产过程中就加入初始用户的证书，或者也可以采用在线的方式或通过可信任的第三者进行证书的办法. 为验证一个用户的公共密钥证书，需要获得颁发这个用户证书的 CA 的公共密钥，才能检查用户证书上的签名. 有了证书之后，用户首次入网注册时，就可以使用证书和 IMSI 一起进行注册了，同样在用户的 USIM 中，存有 CA 的公钥，自己的私钥，如果已经取得自己的证书，则应该也保存在 USIM 中.

在实际应用中，可能还会涉及到无线定位服务，该服务同样需要到认证中心进行鉴权授权后，方可启动定位操作，在收到 MS 要求定位的信息后，由基站或者基站移动台联合测量后将数据发往核心网络进行定位计算，然后将结果返回给 MS.

通过以上的认证过程，在入网过程中，用户的永久身份标识 IMSI 从头至尾都没有用明文的形式在链路上传输，而得到了网络的认证并且获得 TMSI 用于以后的服务. 所有使用 IMSI 来向网络进行认证时，通过以上方案可以保证用户的机密性. 在 3G 中实现了用户与网络的相互认证，通过双向认证机制，3G 有效地保护了用户与运营商双方的利益.

以上的方案可以基于 WPKI 完成一套完整的鉴权认证过程，通过该方案实现 3G 终端和服务网络之间双方的身份认证、加密传输、完整性保护传输等在 3G 安全体系中需要实现的功能. 对于 IMSI 的传送采用非对称加密机制保护，可增强传输的安全性.

4 结束语

基于 WPKI 的 3G 安全认证方式相比较于 3G 现在的安全体系而言，相对比较复杂，可在无线终端用增加加密模块来实现用户证书的存储管理，使无线终端实现加解密、数据完整性保护等各方面的功能. 在本文提出的基于 WPKI 的安全框架基础上，可在 3G 接入网络实施网络安全环境的构建，最终实现面向 3G 网络的整体实施方案. 在 3G 网络中应用 WPKI 技术增强接入安全机制，并对在无线接入基于 WTLS 的认证的流程进行开发和验证，需要进一步提高的运行效率，3G 中的安全还需要有更多的技术加以保障.

参考文献：

[1] 白廷国，郭建梅. PKI 技术与应用[J]. 齐齐哈尔师范高等专科学校学报，2006，(2)：115－117.

[2] 王晓松，王 瑛. 浅谈公钥基础设施 PKI[J]. 科技信息(学术版)，2006，(9)：264－265.

[3] 刘 峰，李大兴. 3G 认证与密钥分配协议的改进[J]. 计算机工程与设计，2006，27(14)：2705－2707.

[4] 杨博雄，李红雷，胡新和，等. 3G 移动通信系统的安全体系与防范策略[J]. 电信工程技术与标准化，2006，(5)：18－21.

[5] 孔凡坤，李 钢，傅海阳. 基于双钥体制的 3G 系统安全

认证方案[J].重庆邮电学院学报,2004,16 (6):81－83.
[6] 赖欣,阮志刚,彭代渊.基于公钥密码体制的 3G 认证协议改进[J].信息安全与通信保密,2006,(5):104－105.
[7] 张方舟,王东安,叶润国,等.一种基于公钥技术的 3G 安全体系结构及其实现[J].计算机工程与应用,2005,(11):124－126.
[8] 陈银凤,吴承勇.PKI 初识及应用[J].内蒙古电大学刊,2006,(1):59－60.

Study and Implement of 3G Authentication Based on WPKI

ZHANG Yue－jin, XIE Xin, HUANG De－chang

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: Through analyzing the present situation of 3G authentications, the paper solves the problem of 3G accessing terminal applications implementation users' authentication. The paper presents a security system based on WPKI by comparing current identity 3G authentication system. A new way of the 3G authentications system based on WPKI is presented and realized, which may enhance security of 3G authentication.

Key words: WPKI; 3G; authentication; security

(**责任编辑:周尚超**)

简讯 2

我校杨辉教授获 2008 年度国家 863 项目资助

我校杨辉教授获 2008 年度国家 863 项目资助,项目名称:稀土萃取过程智能建模与优化控制技术(2008AA04Z129).资助经费:80 万.本课题主要研究内容如下:

针对稀土萃取生产过程控制特点和元素组分含量在线检测的难题,研究开发稀土萃取过程多点、多组分含量及产品质量软测量技术.

研究稀土萃取过程的智能建模技术,综合运用工艺知识、生产过程数据和操作经验,建立产品质量指标、直收率指标与生产过程操作变量和边界条件之间的多模式混合模型.

基于稀土萃取过程操作优化多模式混合模型的特点,研究以产品质量波动最小、满足产量和金属直收率约束条件的实时优化控制算法.

从智能信息处理、过程建模和优化控制相集成角度考虑构建稀土萃取过程建模与优化控制实现平台;研究开发具有自主知识产权的稀土萃取过程智能优化控制系统原型;并在稀土萃取生产过程中进行应用验证,实现稀土产品质量合格率和金属直收率提高 2 个百分点以上,为企业创造显著的经济和社会效益.

我国稀土工业生产过程控制仍停留在"离线分析、经验控制、手工调整"水平;导致企业生产效率低、资源消耗大、产品质量不稳定、市场竞争力差.研究与开发适合我国稀土工业生产过程的自动化装备已成为发展我国稀土工业迫切需要解决的关键科技问题.课题研究对提升我国稀土工业生产自动化水平,确保稀土产品质量稳定、减少资源消耗,降低生产成本、增强企业国际竞争能力,实现我国稀土工业由资源优势向产业优势转化具有重要现实意义.

(**科研处**)