第29卷 第8期 计 算 机 工 程 2003年5月
Vol.29 №8 Computer Engineering May 2003

· 安全技术 · 文章编号：1000—3428(2003)08—0122—02 文献标识码：A 中图分类号：TP 309

一种具有前向安全的数字签名方案

吴克力，王庆梅，刘凤玉
(南京理工大学计算机系，南京 210094)

摘 要：在ElGamal数字签名的基础上构造了一种具有前向安全的数字签名方案，它能有效地抵抗伪造攻击。该方案与ElGamal签名相比只增加极小的计算量，因而是一种有效实用的签名方案。

关键词：数字签名；ElGamal签名；前向安全

A Forward Security Digital Signature Scheme

WU Keli, WANG Qingmei, LIU Fengyu
(Department of Computer Science, NJUST, Nanjing 210094)

【Abstract】 A new forward security digital signature scheme is presented based on ElGamal digital signature, and it can efficiently resist forge attack. The new scheme only increases a little computation comparing with ElGamal scheme, so it is a very useful digital signature scheme.

【Key words】 Digital signature; ElGamal signature; Forward security

数字签名技术为网络信息的安全提供了其他方式难以实现的安全能力，它能确保电子文件来源的真实性以及防止发送方事后抵赖的作用。在现实环境中，由于系统的安全漏洞和人为泄漏等原因而时常引发签名秘钥被盗，致使签名被伪造，已成为安全问题中的难题。为此，许多专家和学者提出了各种解决方案，如门限数字签名方案。近年来，具有前向安全的签名体制的研究正逐渐成为密码学领域一个较为活跃的分支。术语“前向安全”最先出于文献[2]，此后，Ross Anderson提出了具有前向安全的数字签名思想[1]，Bellare和Miner在文献[3]给出了一种基于Fait-Shamir方法的具有前向安全的数字签名方案。

本文受文献[3]思路的启发，提出了一种基于ElGamal体制的具有前向安全的数字签名方案，该方案有较高的效率和更安全的特点。

1 前向安全数字签名

前向安全方法的目标是如果在某一时间段签名秘钥被暴露，但攻击者依然无法伪造先前时间段的签名。与一般签名方法不同，具有前向安全的数字签名的私钥是随时间的推移按时间段不断地改变，而相应的公钥却一直不变。通常，用户先注册一公钥PK并保存相应的私钥SK_0。将公钥的有效时间分为T个时间段，分别记为1，2，…，T。在时间段1，私钥为SK_1，在时间段2，私钥为SK_2，等等。从SK_{i-1}到SK_i的变换是利用一单向函数h，SK_i生成之后就可以删除SK_{i-1}。图1显示了私钥的变化过程。

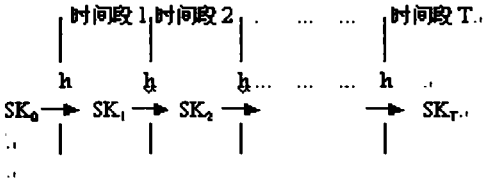

图1 私钥的转换过程

前向安全数字签名方案主要有下列4个部分：(1)公钥和初始私钥产生协议；(2)私钥更新协议；(3)签名协议；(4)验证算法。

2 ElGamal签名方案

ElGamal于1985年提出了一种基于离散对数问题的数字签名方法[4]，该方法的一个变形即为数字签名标准(DSS)，应用较为广泛。

参数：p是一大素数，g是GF(p)的生成元。私钥x，$x<p$，相应公钥$y=g^x \bmod p$。p,g,y公开。

签名：签名方随机选择一随机数k，$k<p$，且$\gcd(k,p-1)=1$。计算$r=g^k \bmod p$和$s=k^{-1}(H(m)-xr) \bmod (p-1)$。其中，m为待签名的消息，H为哈希函数。(r,s)为签名结果。

验证：如果$g^{H(m)} \equiv y^r r^s \bmod p$，认可签名有效。

3 基于ElGamal体制的具有前向安全的签名方案

我们提出的新方案是在对ElGamal签名方案进行简单修改的基础上加入私钥更新算法，使之具有前向安全的特性。

3.1 初始参数

(1)选择一大素数p，g是GF(p)的生成元和随机数SK_0(均小于p)。

(2)计算$PK = g^{SK_0^{2^{T+1}}} \bmod p$。

(3)公开p，g，T和PK。

3.2 私钥更新算法

若$j=T+1$，则SK_j为空串。

若$1 \le j < T+1$则$SK_{j+1} = SK_j^2 \bmod p-1$。

其中j表示第j个时间段。

3.3 签名

(1)签名方选择随机数k，计算$r = g^k \bmod p$。

(2)计算$\delta = (H(m) - SK_j^{2^{T+1-j}} r)k^{-1} \bmod p-1$。

(3)发送(j,r,δ)给验证方。

3.4 验证

如果$PK^r r^\delta = g^{H(m)} \bmod p$为真，则认可签名有效。

作者简介：吴克力(1963－)，男，博士生，主研方向：信息安全；王庆梅，博士生；刘凤玉，教授、博导

收稿日期：2002-05-10

否则，认为无效。

3.5 方案的有效性

方案能否有效地工作的关键是看验证方程是否正确。下面给出其证明。

$$PK^{r}r^{\delta} = g^{SK_0^{2^{T+1}} \cdot r} \cdot g^{k\delta} \bmod p$$

$$= g^{SK_0^{2^{T+1}} \cdot r} \cdot g^{k(H(m)-SK_j^{2^{T+1-j}} \cdot r)k^{-1}} \bmod p$$

$$= g^{SK_0^{2^{T+1}} \cdot r + H(m) - SK_0^{2^{j+T+1-j}} \cdot r} \bmod p$$

$$= g^{H(m)} \bmod p$$

4 安全性分析

本方案是基于ElGamal数字签名的一种改进，其安全性是依赖于计算有限域上离散对数的难度。因而它具有较强的抗蛮力、选择密文等攻击的能力。

由于签名私钥的泄漏，致使攻击者可以伪造先前的签名或者签名者抵赖原来的签名。而这些攻击恰是ElGamal签名所不能抵抗的。通过使用单向函数将私钥按时间段不断地自动改变的方法，使攻击者即使知道当前时间段的私钥但依然无法获知以前时间段的私钥。这就是前向安全所提供的安全能力。可见单向函数的安全性在此起了关键性的作用。本文所采用的单向函数是基于求合数的模平方根的难度，其困难性等价于因子分解问题。

5 结束语

本文通过用单向函数为变换函数的方法，将某一时间段的签名私钥转变为下一时间段的私钥，而验证用公钥却一直保持不变。如果当前的私钥被暴露，攻击者也只能伪造当前时间段的签名，却无法伪造先前时间段的签名。这种具有前向安全性的方法在签名的同时也为签名加上了“时间戳”，并且能防止签名者的对先前时间段签名的抵赖。

参考文献

1 Anderson R. Invited Lecture.Fourth Annual Conference on Computer and Communications Security, ACM, 1997

2 Günther C G. An Identity-based Key-exchange Protocol. Advances in Cryptology EUROCRYPT'89, LNCS 434, Berlin: Springer-Verlag, 1990: 29-37

3 Bellare M, Miner S K. A Forward-secure Digital Signature Scheme. Advances in Cryptology-CRPTO'99, LNCS 1666, Berlin: Springer-Verlag, 1999: 431-448

4 ElGamal T. A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms. IEEE Trans., 1985, IT-31(4): 469-472

☆☆

(上接第121页)

(7)可扩展性。SSO的后台认证服务器可以提供抗毁性和负载平衡，负载平衡可根据站点需求允许用户重定向到不同的服务器，提高整个系统的可靠性和可用性。

(8)审计与报告。对用户登录的记录以及他们的授权情况进行跟踪。提供对安全策略的执行情况以及责任的跟踪。

3 案例视图

在此，我们对关键的服务层的设计实现进行描述，笔者采用Rational Rose工具进行分析，用UML语言对服务层的功能模块和应用调用接口进行表达。

服务层的功能模块的UML使用案例视图如图2。

这些功能模块分两类操作人员：系统管理员和信息维护员。系统管理员负责管理UUA服务的操作权限，并对系统访问日志进行管理；信息维护员负责用户、应用等管理。

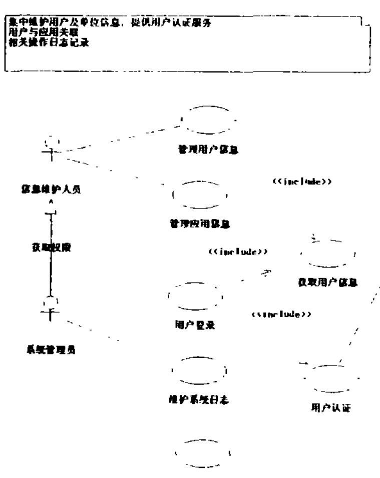

图2 服务层的功能模块的UML使用案例视图

服务层应用调用接口的UML使用案例视图如图3。

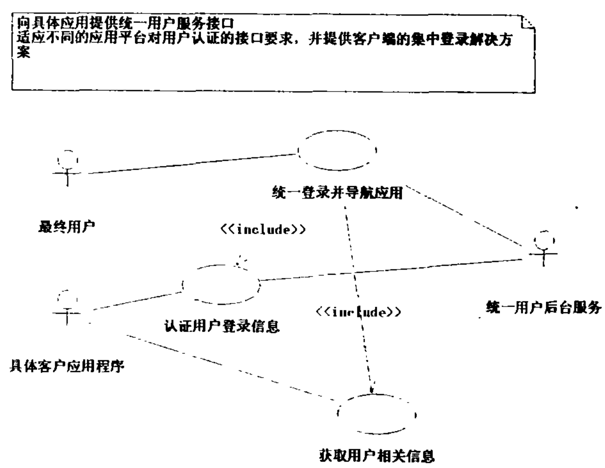

图3 服务层应用调用接口的UML使用案例视图

4 结论

该系统的设计，经过了细致的客户需求分析，参考了同行业的产品的设计优点，不仅满足了现阶段用户管理的主要需求，同时在设计上也考虑到功能的拓展。同时，系统采用通用的Web服务方式，能为其他系统提供开放的调用接口。该系统产品化，有极大的市场前景。

参考文献

1 (美)肯尼思·C·兰登,简·P·兰登.管理信息系统精要——网络企业中的组织和技术(第四版).北京:经济科学出版社,2002-05

2 吴 际,金茂忠.UML面向对象分析.北京:北京航空航天大学出版社,2002

3 (美)考克斯(Cox N.).组建与管理Web服务系统.北京:机械工业出版社,1997-06