文章编号:1001 - 9081(2006)02 - 0316 - 02

证书更新时加密私钥拥有证明研究

谭成翔,王 福,刘 欣
(同济大学 计算机学院,上海 210031)
(fwang@ trimps. ac. cn)

摘 要:为了解决证书更新过程时的加密私钥的拥有证明(Proof of Possession,POP)问题,首先对加密私钥的一些 POP 方法进行了研究,然后提出一个间接、基于轻量级目录服务器(the Lightweight Directory Access Protocol,LDAP)目录服务协议的 Schema,它在证书更新的过程中和加密私钥 POP 紧密地联系在一起,很好地解决了加密私钥的 POP 问题,最后用实例来说明了加密私钥 POP 的管理过程。

关键词:加密私钥;证书;Schema 协议;私钥拥有证明;轻量级目录服务器
中图分类号: TP309.7 **文献标识码**:A

Research on the POP of encryption key as certificate updating

TAN Cheng-xiang, WANG Fu, LIU Xin
(*Institute of Computer Engineering, Tongji University, Shanghai* 210031, *China*)

Abstract: To deal with the POP of encryption key as certificates update, all walys about the POP were researched, and the scheme similar to the indirect method based on LDAP was proposed, the Schema could link PoP with the private key as certificates update. This way could solve the POP well. At last a example was given to describle the management process of the POP with the LDAP server.

Key words: encryption key; certificate; Schema; POP; LDAP

为解决 Internet 的安全问题,世界各国对其进行了多年的研究,初步形成了一套完整的 Internet 安全解决方案,即目前被广泛采用的公钥基础设施(Public Key Infrastructure,PKI),PKI 把用户的公钥和用户的其他标识信息(如名称、E-mail、身份证号等)捆绑在一起,在 Internet 网上验证用户的身份,用户使用私钥进行通信。PKI 主要有三部分组成:认证中心 CA(Certificate Authority),密钥管理中心(Key Management Center),注册中心 RA(Register Authority)。

1 证书更新请求信息

PKI 认证中心 CA 主要完成证书的签发、管理等功能;密钥管理中心 KMC 主要完成密钥的生成、管理、存储等功能;注册中心 RA 主要完成实体证书申请、更新、撤销等功能,其中当一个实体需要申请证书或更新公私钥对,或更改了可区分名即证书的 DN 项的情况下,必须由 RA 向 CA 发送证书申请或更新请求。

证书申请或更新时候,CA 必须决定实体是否拥有通讯私钥,因此实体必须提供一个私钥拥有证明 POP,在证书请求语法中有几个字段提供了 POP 的验证,但是验证的信息量很大。对于签名密钥来说相对容易一些,只需要在申请或更新申请时,直接提供一个签名即可,但是对于加密密钥来说就比较困难,较好的解决办法是提供一个间接的 Schema,CA 证书中包含的公钥将申请或更新后的证书加密后发布到轻量级目录服务器(LDAP),让拥有私钥的实体从 LDAP 服务器上下载接受证书。基于 LDAP 目录服务协议容易实现 Schema,它能在证书申请或更新的过程中和 POP 紧密地联系在一起,能够在证书申请或更新的过程中证明实体拥有通信私钥。

2 证书更新请求信息和 POP

在证书更新请求的过程中,为了防止某些攻击以及允许 CA/RA 检验终端实体和密钥对之间对应的有效性,PKI 管理操作使终端实体有能力证明拥有(也就是说能用)与证书公钥所对应的私钥。CA/RA 在证书交换中可自由选择如何实施 POP(例如带外的方法或 CRMF 带内的方法)。然而,因为现在有许多非 PKIX 的操作协议在使用(例如许多电子邮件协议),它们并不检验终端实体和私钥之间的对应性,这要求 CA/RA 必须通过一些方法来实施 POP。这种对应性仅能被 CA/RA 假设为已证实,直到普遍存在可操作的协议(如签名、加密、协议密钥对),这样才能证明对应性的存在。因此若 CA/RA 没有证实对应性,在英特网 PKI 中的证书将没有意义。

在 PKI 环境中,更新一个终端实体的通常做法是使用特殊的证书请求信息语法,有如下所述的几种形式,这些语法里面通常都包含了对 POP 的支持。

最常用的方法是 PKCS#10,它定义了一种语法,该语法在实体更新时,向 CA 提供能签发证书的信息。另外,该语法还包括证书申请中和申请后的其他数据。为了安全,这种语法请求信息是经过数字签名的。在签名信息被 RA 或 CA 收到后,这种语法还能提供用于私钥通信的 POP,但是这种语法不能用于加密密钥的 POP,加密密钥的 POP 可能要根据不同的

收稿日期:2005 - 08 - 11;**修订日期**:2005 - 10 - 25 **基金项目**:国家发展改革委员会批准项目(发改高技[2003]1203 号)

作者简介:谭成翔(1965 -),男,湖北红安人,研究员,博士生导师,主要研究方向:计算机网络安全、网络数据库等; 王福(1972 -),男,湖北黄冈人,助理研究员,博士,主要研究方向:计算机网络安全、计算机反病毒和防入侵等; 刘欣(1969 -),男,江西南昌人,副研究员,博士,主要研究方向:计算机病毒、计算机入侵等.

安全系统和不同的安全需要区别对待。

另外的一种形式是证书请求信息格式(CRMF),签名密钥的 POP 处理方法和 PKCS#10 相类似,对于加密密钥的 POP 处理,提供了三种方法,第一种方法是把私钥直接传给 CA;第二种方法,又叫直接方法,直接方法需要交换 POP 验证信息,并且需要大量额外的附加信息支持;第三种方法,又称为非直接方法,用包含的公钥加密将要发布的证书,让实体将证书解密并且返回一个验证信息,通过这种方法来说明通信私钥的拥有关系,间接方法也需要额外的信息支持。

类似地,在证书管理协议(CMP)中也有对 POP 的描述,建立在证书管理信息(CMS)之上的 CMC 也非常关注加密密钥的 POP,CMC 为 POP 指定了一种机制,不过该机制比证书请求和返回完整的过程要复杂得多。XML 密钥管理规范(XML Key Management Specification,XKMS)除签名密钥外也考虑了加密密钥的 POP 问题。

POP 对于加密密钥是非常重要的,终端实体拥有的一个包含公钥的证书如果没有对应的私钥或者根本没有私钥,那么这个证书是不可用的,一些被这个公钥加密的信息根本不能被实体解密。这在原始信息被破坏了且只有加密信息的时候最危险,因为没有先前的私钥背景,没有人能使用公钥加密后的信息。

上面提到的几种方法都有缺点,不能很好地解决加密密钥的 POP 问题。因此本文提出一个基于 LDAP 的 Schema 方法,较好地解决了加密密钥的 POP 问题。基于 LDAP 的 Schema 的 POP 管理方法类似如上面 CRMF 中讲的间接解决方法,终端实体是 LDAP 目录的授权用户,能从 LDAP 服务器上下载和激活自己的证书,但是下载的证书是用公钥加密的信息,必须用私钥将证书解密,并且将其返回到 LDAP 服务器上。用基于 LDAP 的 Schema 方式,可以避免为验证 POP 而须要向 CA 提交额外的验证信息。

3　新 Schema

3.1　LDAP 简介

LDAP 从 X500 的基础上简化而来,当前的版本是 LDAPV3,具有查询效率高、树状的信息管理模式、分布式的部署框架以及灵活而细腻的访问控制,现在成为 PKI 信息发布的首选,为证书和证书撤销信息(Certificate RevocationList , CRL) 提供了有效的存储库。LDAP 不仅仅能支持 PKI,它还有自己独特的安全特点,它不仅提供了用户名/密码的方式来给用户一个简单的授权,另外还支持简单的授权安全层 SASL 协议和 TLS 协议,使用 TLS 协议可以保证 LDAP 目录和客户之间数据通信的整体性和私密性,口令的方法可以和 TLS 方法联合在一起,避免口令采用明文的方式传送。

3.2　用 LDAP 提供 POP 管理

3.2.1　Schema 设计

在 LDAP 中,把对象类、属性类型、语法和匹配规则统称为 Schema,Schema 可以分成系统 Schema 和自定义 Schema,在 LDAP 中有许多系统对象类、属性类型、语法和匹配规则,这些系统 Schema 在 LDAP 标准中进行了规定,同时不同的应用领域也定义了自己的 Schema,另外用户在应用时,也可以根据需要自定义 Schema。这有些类似于 XML,除了 XML 标准中的 XML 定义外,每个行业都有自己标准的 DTD 或 DOM 定义,用户也可以自扩展;也如同 XML,在 LDAP 中也鼓励用户尽量使用标准的 Schema,以增强信息的互联互通。为了管理加密证书更新中的 POP,本文引进了一个新的 Schema 对象类 pkiPopManagement,如下所示:

```
Object Classes
  (1.3.6.1.4.1.8301.3.2.2.1.6 NAME'pkiPopManagement'
  SUP
  topAUXILIARY MAY ( userEncryptedPassword $
  userEncryptedCertifcate) )
Attributes
(1.3.6.1.4.1.8301.3.2.2.1.7 NAME'userEncryptedPassword'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE )
(1.3.6.1.4.1.8301.3.2.2.1.8 NAME'userEncryptedCertifcate'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE )
```

图 1 中给出了一个使用上述属性的 LDAP 实例。

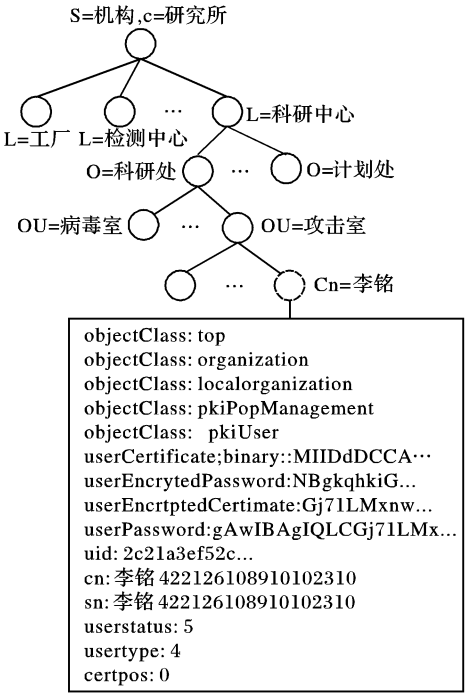

图 1　LDAP 实例

在这个 Schema 中,CA 接受一个加密证书更新请求时,先假设私钥是存在的,象通常的做法一样,发布更新的证书,在 LDAP 上创建一个实体。不同的是,首先这个发布的证书被存放在属性 userEncryptedCertificate 中的公钥加密了;其次,CA 随机地选择一个 LDAP 用户密码,密码的哈希值放在实体属性 userPassword 中,用于 LDAP 的简单授权过程。同时也用公钥加密用户密码放在特殊的属性 userEncryptedPassword 中,在这个意义上,即使用户自己也不知道自己的密码,因为用户看到的仅仅是哈希值和加密版本号。

拥有加密私钥的终端实体,首先下载用公钥加密了的证书和 LDAP 的访问密码,并用自己的私钥解密后,获得了访问 LDAP 的密码,同时获得了解密后的证书,现在可以使用密码作为一个授权的用户绑定到目录服务系统中,并且将解密的证书写进实体。随着解密的过程完成即实现了 POP,将解密后的证书返回到 LDAP 服务器上同时激活证书,另外的用户能使用它。相反,对于没有私钥的终端实体,证书和密码仍然在目录中以加密形式存在,不能被使用。在这个过程中,授权用户和 LDAP 服务器之间的通信必须用 SASL 协议或 TLS 协议以保准密码和证书的传输安全。

CA 必须做的一个步骤就是通过 ACLs 列表强制 LDAP 目

(下转第 340 页)

3 随机花指令加密算法实践

3.1 随机花指令算法的实验步骤与结果

1）实验环境

硬件环境：celeron1.7GHz/256M Memory/20G HardDisk

软件环境：操作系统 Windows XP + SP2/JCEE 变换器/W32Dasm8.93/实验用可执行程序 test.exe。其中 JCEE 变换器是为实现变换而编制的测试程序，W32Dasm 是应用广泛的反汇编器调试器，程序 test.exe 是用来进行变换的程序。

2）实验步骤

a）对实验用原程序进行反汇编，得到汇编伪码 P；

b）用 JCEE 变换器对原程序进行变换，得到变换后的程序；

c）用反汇编器对变换后的程序进行反汇编，得到汇编伪码 P'；

d）比较 P 和 P' 得到结论 R。

3）实验结果

候选块的大小选为 10 条指令，每条 JMP 指令后最大添加 8 个字节花指令。test.exe 程序经变换后得到的数据如表 1 所示。

表 1 随机花指令变换结果相关数据（单位：bytes）

	代码长度	空闲空间	指令数目	JMP 数目	Jcc 数目	JunkCode
P	528	499	151	22	40	
P′	858	169	200	61	4232	
P′ - P	330	-330	49	49	0232	

经验证，采用本随机花指令加密方法对 test.exe 文件进行花指令变换，采用花指令去除工具对变换后的结果进行花指令搜索，均未能发现相关的花指令特征。

3.2 实验分析

经过“JMP 扩展”变换后的代码要跳过一定数量的正常指令，然后在三条 JMP 指令后添加花指令，总共存在的特征值是 8 * 8 * 8 * 10 = 5 120 种，如果基数扩大，特征值数量更多。因此想要定义所有的特征不太实际。在 JMP 后添加了花指令后不能自动去除还有一个原因是 JMP 指令作为原始代码的组成部分是不能被去除的，否则程序逻辑遭到破坏。

4 结语

文章提出的随机花指令加密算法所产生的花指令具有无特征码的特点，不能用工具自动去除；并且对原始指令变换后可以添加更多的花指令，达到较高的模糊度，起到了软件保护的目的。本文以实例的方式对随机花指令加密算法的有效性进行了验证，今后需要更为深入地研究程序逻辑一致性的形式化证明方法，由此，才能更为有效地保证该算法的有效性。

参考文献：

[1] Hume. 病毒和网络攻击中的多态、变形技术原理分析及对策[R/OL]. http://www.xfocus.net/pro jects/Xcon/2003/Xcon2003_hume.pdf, 2003, 12.

[2] 卿斯汉. 恶意代码机理[Z]. 北京：北京大学软件学院, 2004.

[3] 段钢. 加密与解密[M]. 第 2 版. 北京：电子工业出版社, 2003.

[4] 于淼, 孙强. 对加壳技术的改进：超粒度混杂技术[J]. 计算机应用, 2004, 24(8)：137 - 139.

[5] 林宣雄, 李怀祖, 张文修. 扰码机制在反静态分析中的应用[J]. 微电子学与计算机, 1996,(1)：16 - 19.

[6] LINN C, DEBRAY S. Obfuscation of Executable Code to Improve Resistance to Static Disassembly[A]. Proceedings of the 10th ACM conference on Computer and communications security[C]. 2003. 290 - 299.

[7] GRIFFITHS AL. Binary protection schemes [J]. CodeBreakers - Journal, 2005, 2(1)：1 - 91.

（上接第 317 页）

录服务器仅仅接受授权用户的写请求，和接受拥有 userCertificate 属性的实体的写请求，当然授权用户只能将解密后的证书写入属于自己实体的目录下。另外，ACLs 列表必须经过某种策略配置，配置后，用户密码不能被其他的用户看见。这样就会减少其他终端用户进行字典攻击的可能性。

拥有加密私钥的终端用户必须下载对应更新后的证书，本文提供的 Schema 有一个可选变量，这个可选变量可以将身份表示和 POP 信息更紧密地联系在一起，并且保证用户下载的是对应的证书。实现过程如下：用户在 LDAP 目录上使用的加密密码仅仅是用户密码的一半，另外一半在用户申请更新的过程中提供，这部分密码作为 CA 和终端用户的秘密共享，用户必须把两半密码合并后，才能得到目录的授权和下载对应的更新后被加密的证书。

CA 可以基于不同的策略来释放 Schema，例如，如果三天后在目录里证书仍然是加密状态，证书将被删除掉，让用户不能到目录上来使用证书。另外，证书解密后，用户在 LDAP 上的密码也被删除掉，这样就可以使用户没有权限访问其他的目录。

3.3 可用性问题

用 LDAP 管理 PKI 过程的应用提高了 PKI 的应用性，对于用户来说，解密一个数据包，比让自己的私钥暴露在通信过程中更安全。解密一个象证书和密码的数据包是解密密钥的功能，这些已经在很多客户端软件中使用了。另外很多被 LDAP 支持的客户端软件能够拿到其他的证书，这些特点能够扩展和联合，自动地从目录中得到加密数据，将它解密并且将证书存回目录中，最后的这个过程对于终端实体来说是透明的。

4 结语

本文在首先对几种传统的加密证书更新时的 POP 方法的优缺点进行分析，提出一种基于 LDAP 的 Schema 来解决加密证书更新时的 POP 管理方法。实践表明，本方法过程简单，私钥不暴露，安全性高，还可以用于加密证书的撤销等过程，提高了 PKI 的应用性。

参考文献：

[1] BICAKCI K, BAYKAL N. A New Design of Privilege Management Infrastructure with Binding Signature Semantics[A]. EuroPKI 2004[C]. LNCS 3093, 2004. 306 - 313.

[2] KARATISLIS V, LIPPERT M, WIESMAIER A. Using LDAP Directories for Management of PKI Processes[A]. EuroPKI 2004[C]. LNCS 3093, 2004. 126 - 134.

[3] 王春耕. 朱建涛. 大规模机群系统中基于 LDAP 的用户管理[J]. 计算机工程与应用, 2004, 40(18)：47 - 49.

[4] 赵妍, 袁野, 刘冰. 基于 LDAP 协议与 Kerberos 认证机制的统一认证[J]. 信息技术, 2004, 12(28)：46 - 49.

[5] ITU-T X.509[DB/OL]. http://houmb.qlsc.sdu.edu.cn/ebook/is/X509/X509_4thEditionDraftV8.pdf, 2001 - 05 - 03.