高等院校信息安全专业系列教材

PKI 原理与技术

谢冬青　冷 健　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书系统全面地介绍了 PKI 原理与技术的主要内容，包括 PKI 基础设施的地位和作用，核心 PKI 服务的内容，认证中心构建，PKI 中的各种信任模型，PKI 工程所遵循的标准、协议和编码方式，并讨论了电子商务、电子政务的安全需求，给出了 PKI 解决方案的主要技术框架。

本书从工程化实用角度来讨论 PKI 原理与技术，适合作为信息安全、计算机科学与技术、软件工程、电子工程与通信工程等专业本科生、硕士生的教材，也可供从事相关专业的教学、科研和工程人员参考。

图书在版编目(CIP)数据

PKI 原理与技术/ 谢冬青，冷健编著 .—北京：清华大学出版社，2003 .12
(高等院校信息安全专业系列教材)
ISBN 7-302-07640-5

Ⅰ .P… Ⅱ .①谢… ②冷… Ⅲ .电子商务 - 安全技术 - 高等学校 - 教材 Ⅳ .F713 .36

中国版本图书馆 CIP 数据核字(2003)第 106637 号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
http:// www .tup .com .cn　　邮　　编：100084
社 总 机：010-62770175　　客户服务：010-62776969
组稿编辑：张　民
文稿编辑：王冰飞
印 刷 者：北京市清华园胶印厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×230　印张：24 .25　字数：483 千字
版　　次：2004 年 1 月第 1 版　2004 年 1 月第 1 次印刷
书　　号：ISBN 7-302-07640-5/ TP・5602
印　　数：1～5000
定　　价：32 .00 元

第 1 章 PKI 基础设施

1.1 基础设施

1.1.1 基础设施的地位

基础设施就是一个普适性基础,它在一个大环境里起着基本框架的作用,例如电子通信网络和电力供应基础设施。在电子通信网络中,局域网和广域网可以让企业内部的计算机在 Intranet 上互相交流数据,让个人用户登录 Internet 冲浪;对于电力供应基础设施,各种电气设备只要插在电源插座上,就可以获取运行所需要的电压和电流。这些设施基本原理共通,操作简便,只要遵循基本的原则,不同的实体就可以方便地使用基础设施提供的服务。

作为基础设施,需要实现“应用支撑”的功能,可以让“应用”正常工作。比如电力系统可以支撑电灯的工作。而且,电力基础设施也要具有通用性和实用性,使它能够支持各种新的应用。比如微波炉的应用在电力基础设施设计的时候并没有出现。

基础设施的使用应该就像把电气设备的插头插到墙上的插座一样简单,它应具有以下特性:

(1) 具有易于使用、众所周知的界面。

(2) 基础设施提供的服务可以预测并且有效。

(3) 应用设备无须了解基础设施的工作原理。

还以电灯为例,电灯使用者并不关心电能是怎样在发电站里产生,如何经过变电设备转换,最后以什么方式送到房间里来的,房间里遍布的各种各样的插座都没有任何区别,只要把电灯的电源插头插到任何一个插座里,它就能通过众所周知的接口(电源插座)得到指定的电压和电流,从中获得能量,于是正常地工作。

1.1.2 网络基础设施

在电子通信网络中,凡是用以连接不同的计算机,使之可以互联互通的一切基础元素

都属于网络基础设施的概念,它是包括所有的硬件、软件、人员、策略和规程的总和。也可以把它具体地当作一堆集线器、路由器和网线等。如果观察一下现在随处可见的无线应用,比如手机、寻呼机、PDA 等,这些移动设备同样组成了无线的分布网络,它们所需要的基站、无线网桥,甚至卫星等,也同样属于基础设施范畴。

1.2 安全基础设施的概念

1.2.1 安全基础设施的内容

安全基础设施必须依照同样的原理,同样提供基础服务,也就是说要具有普适性。它为整个组织提供的是保证安全的基本框架,并且可以被组织内任何需要安全的应用和对象使用。安全基础设施的“接入点”必须是统一的、便于使用的(就像墙上的插座一样)。只有这样,那些需要使用这种基础设施的对象在使用安全服务时,才不会遇到太多的麻烦。

具有普适性的安全基础设施首先应该是适用于多种环境的框架。这个框架避免了零碎的、点对点的,特别是没有互操作性的解决方案,引入了可管理的机制以及跨越多个应用和计算平台的一致的安全性。不难想象,假如每一对通信方都使用他们自己的通信线路进行通信,或者每个人都用自己的发电机来产生电压和电流,这个世界将是多么的混乱!

安全基础设施能够保证应用程序增强数据和资源的安全,保证增强与其他数据和资源进行交换中的安全。如何使增加安全功能变得更加简单、更加实用是最值得关心的。安全基础设施还必须具有同样友好的接入点,应用程序无须了解基础设施提供安全服务的原理,它只要能得到服务就行了。对于安全基础设施来说,能够提供一致有效的安全服务是最重要的。

安全基础设施提供的服务主要包含以下几个方面。

1.安全登录

在访问网络资源,或者使用某些应用程序的时候,用户往往会被要求首先“登录”或者“注册”。在这一步骤中,典型的操作过程包括用户输入用户身份的信息(如用户标识或姓名、昵称)以及认证信息(如口令或其他机密信息)。如果除了合法用户没有人能够获取用户的认证信息,采用这种方法能够安全地允许合法用户进入系统或者指定的应用程序。

绝大多数使用过计算机的人都对这种操作比较熟悉。登录是广泛使用的一种保护措施,但是它所带来的问题也是显而易见的。比如,当一个网页要求用户进行登录,这个用户是远程的(也就是从不同的设备,比如另外一台计算机登录),所以口令信息会在未受保

护的网络上传递,这就非常容易被截取或监听,所谓的重放攻击就是通过中途截取来实施的。即使口令已经被加密也无法防范重放攻击(有的安全基础设施会增加时间信息来做到防止重放攻击,这在后面会详细说明)。而且,进一步讲,要选用“好”的口令(所谓“好”的口令就是具有足够的长度,并且没有规律,不容易被熟悉或不熟悉你的人轻易猜测得到),还得记住而不是写下口令,并且按照本地的安全策略要求,经常修改口令,这对用户来说并不容易。

这正是安全基础设施提供的服务之一,它可以解决这些问题。尤其是对于那些将安全服务作为普适性的基础设施的环境,登录到基础设施的事件只会发生在本地(也就是说,用户与设备需要进行物理性的接触)。并且,如果需要的话,可以将成功登录的结果安全地传递到远程的应用程序。因此,可以在远程登录事件中引入一种足够强壮的认证机制,而口令本身无须在网络上传递(事实上,根本不会出现在用户设备以外的任何地方)。

实施安全基础设施并不意味着取消口令的使用,因为口令方式是用户进入基础设施本身的认证机制。在生物识别技术成熟并大规模使用之前,用户还是需要输入自己的口令才能使用安全基础设施提供的服务。安全基础设施只是解决了使用口令方式时存在的最严重的一个问题:它可以避免口令在不可信或不安全的网络中传递,从根本上避免了被截获的危险。

现在的操作系统基本都是多任务的,可以很方便地同时运行多个应用程序,如果这些程序都需要登录认证,登录过程(输入登录信息)就可能变成一个严重问题:对所有的应用程序使用相同的口令字会降低全局的安全性(提供了多个攻击点,一个被攻破则会遭受到全面的危险);每个应用程序使用不同的口令字又不易使用(用户总是要记住好几个字符串,而且往往还是杂乱无章的)。在友好的登录进程中,应该指导用户的操作,但如果这个进程显得太麻烦,妨碍到用户的工作,用户就会寻找绕过这些进程的方法,而这肯定会降低安全性。

使用普适性的安全基础设施可以极大地改善这种状况。安全基础设施能将一个成功登录的结果安全地通知到其他需要登录的设备,减少远程登录的需求。这一特征可以进行扩展,一次成功登录可以通知许多远程设备(根据需要),而无须多次登录。这个特征就是安全基础设施完整性的概念。就像需要用户登录的任何系统或应用程序一样,安全基础设施拥有一个明确编码的用户“身份”(用来鉴别合法用户的登录)。由于“身份”可以在整个基础设施中被识别,所以,还可以应用于任何使用基础设施的系统和应用程序(甚至可以扩展到全球)。

所以,一次登录就可以使用多个设备、域、服务器、系统和应用程序等(注意登录事件还可以与其他访问控制机制如认证等混用)。所以,从使用的角度上看,安全单点登录是十分必要的,因为用户只需记忆一个口令,只需知道一个简单的过程就可以访问多个系

统。从安全角度考虑,也是十分需要的,因为可以减少口令在网络上传递的频率,自然也就降低了泄露的风险。由于只需记忆单个口令,用户可能也更愿意采用一个“好”口令。这就像拥有一张 VIP 卡可以随处消费一样。可是实际上,由于以前已经存在大量应用程序,单点登录是难以实现的,甚至是不可能的。在这种情况下,比较好的办法是减少登录次数,使终端用户需要记忆和管理的不同口令的数目尽可能少,这同样可以有效地提高安全性。

安全单点登录是安全基础设施提供的一项服务,适用于所有应用程序和设备。在任何时候和地方,如果需要使用安全传送认证信息的机制,基础设施就可以为之提供;应用程序在必要时接入基础设施,从而获得认证信息。这种基础服务减少了用户必须登录的次数。另外,在安全性上的另一个重要好处是,一个设计良好的基础设施能保证用户只需在他们工作的机器上登录。所以,至少在某些情况下,口令无须在易于遭到攻击的网络上传递,极大地降低了口令被窃听和口令存储/重放攻击的风险。

2.终端用户透明

用户使用安全基础设施时,基础设施只是一个黑盒子,他们需要的是服务而不是如何提供服务的细节。换句话说,对终端用户是完全透明的,这是普适性基础设施的一个极其重要但经常忽略的特征。使用通信基础设施的绝大多数用户无须知道 IP 报头或以太网包的结构,类似地,电力基础设施的绝大多数用户也无须知道电压和电流频率。对于用户来说,基础设施如何提供服务,应该是彻底地封装起来的。一个合理设计的基础设施,必须做到:所有的安全隐藏在用户的后面,无须额外地干预,无须用户注意密钥和算法,不会因为用户的错误操作对安全造成危害。

换言之,安全不应当成为用户完成任务的障碍。安全不需要用户具有特别的知识,无须用户进行特殊的处理,不会严重加重用户的负担,除了初始的登录操作外,基础设施应当用一种对用户完全透明的方式完成所有与安全相关的工作。

以上都是基于安全基础设施工作正常的情况。如果发生了错误呢?比如用户不能成功登录,这时需要及时反馈给用户。所以,在“黑盒子”原则中存在两个例外的情形:用户需要知道第一次与基础设施连接的情况(在一些初始化过程中),以及何时安全基础设施无法提供服务,何时认证没有成功,何时无法与远程用户建立安全通信通道,正如用户需要知道何时远程的服务器正在维护、不能接收 IP 包,何时电力公司限制用电一样。简单地说,基础设施提供的透明性意味着用户相信基础设施正在正常地工作,能够提供安全服务。每当处理失败,必须马上通知用户,因为缺乏安全通常会改变用户的行为。

3.全面的安全性

作为一个普适性安全基础设施,最大的益处是在整个环境中实施的是单一的、可信的

安全技术(如公钥密码技术),所以它能够提供跟设备无关的安全服务。它能够保证数目不受限制的应用程序、设备和服务器无缝地协调工作,安全地传输、存储和检索数据,安全地进行事务处理,安全地访问服务器等。无论是电子邮件应用、Web 浏览器、防火墙、远程访问设备、应用服务器、文件服务器、数据库,还是更多的其他设备,都能够用一种统一的方式理解和使用安全基础设施提供的服务。这种环境不仅极大地简化了终端用户使用各种设备和应用程序的方式,而且简化了设备和应用程序的管理工作,保证他们遵循同样级别的安全策略(策略可以根据特定的应用程序或设备的需要制定)。

使基础设施达到全面安全性所采取的重要机制之一就是保证大范围的组织实体和设备采用统一的方式使用、理解和处理密钥。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 PKI(Public Key Infrastructure,公钥基础设施)技术,PKI 技术采用证书管理公钥,通过第三方的可信任机构——认证中心(Certificate Authority,CA),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 上验证用户的身份。目前,通用的办法是采用建立在 PKI 基础之上的数字证书,通过对要传输的数字信息进行加密和签名,保证信息传输的机密性、真实性、完整性和不可否认性,从而保证信息的安全传输。

双钥密码算法又称公钥密码算法,是指加密密钥和解密密钥为两个不同密钥的密码算法。公钥密码算法不同于单钥密码算法又称对称密码算法,它使用了一对密钥,一个用于加密信息,另一个则用于解密信息,通信双方无须事先交换密钥就可进行保密通信。其中加密密钥不同于解密密钥,加密密钥公之于众,谁都可以用,解密密钥只有解密人自己知道。这两个密钥之间存在着相互依存关系,即用其中任一个密钥加密的信息只能用另一个密钥进行解密。若以公钥作为加密密钥,以用户专用密钥(私钥)作为解密密钥,则可实现多个用户加密的信息只能由一个用户解读;反之,以用户私钥作为加密密钥而以公钥作为解密密钥,则可实现由一个用户加密的信息而由多个用户解读。前者可用于数字加密,后者可用于数字签名。

在通过网络传输信息时,公钥密码算法体现出了单密钥加密算法不可替代的优越性。对于参加电子交易的商户来说,希望通过公开网络与成千上万的客户进行交易。若使用对称密码算法,则每个客户都需要由商户直接分配一个密钥,并且密钥的传输必须通过一个单独的安全通道。相反,在公钥密码算法中,同一个商户只需自己产生一对密钥,并且将公钥对外公开。客户只需用商户的公钥加密信息,就可以保证将信息安全地传送给商户。

公钥密码算法中的密钥依据性质划分,可分为公钥和私钥两种。用户产生一对密钥,将其中的一个向外界公开,称为公钥;另一个则自己保留,称为私钥。凡是获悉用户公钥

的任何人若想向用户传送信息,只需用用户的公钥对信息加密,将信息密文传送给用户即可。因为公钥与私钥之间存在着依存关系,在用户安全保存私钥的前提下,只有用户本身才能解密该信息,任何未受用户授权的人包括信息的发送者都无法将此信息解密。

RSA 公钥密码算法是一种公认十分安全的公钥密码算法。它的命名取自 3 个创始人:Rivest、Shamir 和 Adelman。RSA 公钥密码算法是目前网络上进行保密通信和数字签名的最有效的安全算法。RSA 算法的安全性基于数论中大整数分解的困难性,所以,RSA 需采用足够大的整数。因子分解越困难,密码就越难以破译,加密强度就越高。

1.2.2 安全基础设施在信息基础设施中的地位

一个组织可能存在着千差万别的实体,它们可能有不同的特性,有各自的需求,那么在它们互相交流时,如何保证通信安全呢?

用电子手段入侵并破坏基础设施的可能性是完全存在的。一些行业和国家部门已经注意到这一点。2002 年由美国海军军事学院和 Gartner 联手举行的"数字珍珠港"演习中,就模拟了恐怖分子对美国基础设施进行大规模的数字袭击。虽然这次演习得出的结论是:"要成功实施袭击任务需要至少 2 亿美元资金、非常专业的知识以及 5 年多的准备时间","此类袭击虽然可能毁坏人口密集地区的通信网络,但决不会导致人员伤亡或其他灾难性后果",结论看上去似乎令人乐观,但是对于信息安全基础设施来说,面对攻击的实际表现往往非常不让人放心。

对信息基础设施的数字袭击一般采用两种形式:攻击数据和攻击控制系统。攻击数据主要是窃取或破坏数据、拒绝服务,大多数针对 Internet 及计算机的攻击属于这一类型,如窃取信用卡信息、毁坏网站和阻塞服务等。而控制系统攻击是毁掉或掌握维护物理设施的权限,如控制供水、供电网络及铁路系统的"分布式控制系统(DCS)"。黑客通常是通过电话拨号来远程入侵控制系统的,这类系统常利用 Internet 传输数据或将内部网通过防火墙接入 Internet,而防火墙则有时可以被攻破。这些攻击可以在不造成伤亡的情况下带来巨大危害,比如许多电厂和水利设施(这些都是与国民经济、生活息息相关的重要基础设施)是在计算机控制设备组成的网络上运行的,这种"监控及数据采集系统(SCADA)"也可能受到黑客攻击。2001 年 11 月,49 岁的 Vitek Boden 因涉嫌 Internet 犯罪而被判处两年徒刑,他利用无线设备窃取了控制软件,并向河流以及澳大利亚昆士兰州的沿海水域中释放了 100 万公升的污水。Boden 是一位水利工程顾问,2000 年 3 月被 Maroochy Shire 政府解除全职工作,此后心怀嫉恨试图攻破该系统,前后共进行了 45 次入侵的尝试,最后一次他终于获得成功,使得可以向水道中排放污水。

澳大利亚环境保护协会调查专员 Janelle Bryant 这样形容所造成的后果:"海洋生物大片死亡,小溪变成黑色并且恶臭熏天,使得周围居民无法忍受。"

该系统未能检测到前 44 次入侵的事实暴露了该基础设施的安全薄弱环节。1997 年美国的 Barry C . Ezell 上校发现 40%的水利设施允许通过 Internet 操作控制,60%的 SCADA 系统可以通过调制解调器拨号连接。北美电子可靠性委员会专家 Ellen Vancko 说,这些访问也不见得不安全,她说:“所有电子公司都通过网络相互连接,但这并不意味着我们的控制系统和公网相连。”

现实中实际采用的防火墙和其他内部保护通常不够安全,因此如果这些网络和 Internet 相连就增大了危险性。

在信息化最为发达的美国,过去的十年内,曾有过几次大型的数字袭击行动。虽然还没有一次导致人员伤亡或大规模破坏,但是都不同程度地威胁到了美国的基础设施。

1988 年:

Robert Morris 发布了一种蠕虫病毒,感染了 Internet 上三四千台 PC 机、六千多台服务器。

1989 年:

“Doom 兵团”黑客小组完全控制了南部贝尔的电话系统,黑客可以像该公司技术人员一样分接线路、转移呼叫等,甚至可以关闭 911 电话报警系统。

1990 年:

AT&T 路由器的故障导致长话业务中断 9 小时,许多人都认为是黑客所为。

1994 年:

一个名叫 Merc 的黑客拨号侵入了 Salt River 项目的服务器,入侵了监控菲尼克斯市河流的计算机。

1997 年:

美国弗吉尼亚州的一家小 ISP 公司的技术员错误地修改了该公司的路由器信息,导致了大量重要的 Internet 路由器崩溃。3 月,一个十几岁的少年破坏了美国马萨诸塞州伍斯特一个小机场的电话系统,指挥塔失灵长达 6 小时之久,然而飞机仍旧可以从周围其他机场接收无线电信息。

2000 年:

2 月,“拒绝服务攻击”用大量数据阻塞了 Yahoo、eBay、CNN 及 ZDNet 的网络,致使用户无法正常访问长达两三小时之久。“爱虫”病毒 5 月袭击了全球许多公司的邮件服务器。

2001 年:

9 月,尼姆达病毒疯狂泛滥在服务器、网络中,使金融业遭受了严重的影响。

许多事实已经证明,一定要有一个共同的基础设施来提供一致的安全特性,这就明确了安全基础设施在信息基础设施中的重要性。公钥基础设施(PKI)就是基于公开密钥体制理论和技术建立起来的这样的安全体系,是提供信息安全服务的具有普适性的安全基

础设施,其核心是解决网络空间中的信任问题,确定网络空间各行为主体身份的惟一性、真实性。随着全球经济一体化的进展,世界各国都已经意识到 PKI 对国家和社会信息化的重要性,纷纷推进与 PKI 相关的法律、法规、标准、应用、技术和相关组织。

一些安全服务提供商和应用软件提供商也开始合作推出基于标准的安全电子商务解决方案。这些服务的目标是实现安全的消息传递、安全的外部网、内部网、电子交易网站和安全的文档管理。它们可以提供一个开放的互联网基础设施,这一基础设施能够更加安全和可靠地完成电子商务的处理。比如 IBM 的 Tivoli Risk Manager 中就有一项叫做“心跳”的功能可以事先显示安全基础设施中可能发生的故障,从而使管理员能够采取预防措施。

我国安全基础设施的建设也呈现出良好的发展势头,成立了专门的组织机构,众多厂商和 IT 企业投资建设,以满足各个行业和部门的安全需要。

1.3 公钥基础设施

公钥基础设施(PKI)是一个用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施。PKI 是一种遵循标准的利用公钥加密技术为电子商务、电子政务的开展提供一整套安全的基础设施。用户利用 PKI 平台提供的安全服务进行安全通信。PKI 这种遵循标准的密钥管理平台,能够为所有网络应用透明地提供采用加密和数字签名等密码服务所需要的密码和证书管理。

使用基于公开密钥技术平台的用户建立安全通信信任机制的基础是,网上进行的任何需要提供安全服务的通信都是建立在公钥的基础之上的,而与公钥成对的私钥只掌握在他们与之通信的对方。这个信任的基础是通过公钥证书的使用来实现的。公钥证书就是用户的身份与之所持有的公钥的结合,在结合之前,由一个可信任的权威机构——认证机构(CA)来证实用户的身份。然后由可信任的 CA 对该用户身份及对应公钥相结合的证书进行数字签名,用来证明证书的有效性。

PKI 首先必须具有可信任的认证机构,在公钥加密技术基础上实现证书的产生、管理、存档、发放以及证书撤销管理等功能,并包括实现这些功能的硬件、软件、人力资源、相关政策和操作规范以及为 PKI 体系中的各成员提供全部的安全服务,例如,身份认证、数据保密性、完整性以及不可否认性服务等。

构建实施一个 PKI 系统主要包括以下内容:

(1) 认证机构

证书的签发机构,它是 PKI 的核心,是 PKI 应用中权威的、可信任的、公正的第三方机构。

(2) 证书库

证书的集中存放地,提供公众查询。

(3) 密钥备份及恢复系统

对用户的解密密钥进行备份,当丢失时进行恢复,而签名密钥不能备份和恢复。

(4) 证书撤销处理系统

证书由于某种原因需要作废,终止使用,将通过证书撤销列表 CRL 来实现。

(5) PKI 应用接口系统

为各种各样的应用提供安全、一致、可信任的方式与 PKI 交互,确保所建立起来的网络环境安全可靠,并降低管理成本。

综上所述,PKI 是一种新的安全技术,它基于公开密钥密码技术,通过数字证书建立信任关系。PKI 是利用公钥技术实现电子商务安全的一种体系,是一种基础设施,可以保证网络通信、网上交易的安全。

PKI 公钥基础设施是提供公钥加密和数字签名服务的系统或平台,目的是为了管理密钥和证书。一个机构通过采用 PKI 框架管理密钥和证书可以建立一个安全的网络环境。PKI 主要包括 4 个部分:X.509 格式的证书(X.509 v3)和证书注销列表 CRL(X.509 v2); CA/ RA 操作协议;CA 管理协议;CA 政策制定。一个典型、完整、有效的 PKI 应用系统至少应包括以下部分:

(1) 认证中心(CA)

CA 是 PKI 的核心,CA 负责管理 PKI 结构下的所有用户(包括各种应用程序)的证书,把用户的公钥和用户的其他信息捆绑在一起,在网上验证用户的身份,CA 还要负责用户证书的证书注销列表登记和证书注销列表发布。

(2) X.500 目录服务器

X.500 目录服务器用于发布用户的证书和证书注销列表信息,用户可通过标准的 LDAP 协议查询自己或其他人的证书和下载证书注销列表信息。

(3) 具有高强度密码算法(SSL)的安全 WWW 服务器

出口到中国的 WWW 服务器,如微软的 IIS、Netscape 的 WWW 服务器等,受出口限制,其 RSA 算法的模长最高为 512 位,对称算法为 40 位,不能满足对安全性要求很高的场合,为解决这一问题,必须开发具有自主知识版权的 SSL 安全模块,并且把 SSL 模块集成在 Apache WWW 服务器中,Apache WWW 服务器在 WWW 服务器市场中占有 50% 以上的份额,其可移植性和稳定性很高。

(4) Web(安全通信平台)

Web 有 Web Client 端和 Web Server 端两部分,分别安装在客户端和服务器端,通过

具有高强度密码算法的 SSL 协议保证客户端和服务器端数据的机密性、完整性、身份验证。

(5) 自开发安全应用系统

自开发安全应用系统是指各行业自开发的各种具体应用系统,例如银行、证券的应用系统等。

完整的 PKI 包括认证政策的制定(包括遵循的技术标准、各 CA 之间的上下级或同级关系、安全策略、安全程度、服务对象、管理原则和框架等)、认证规则、运作制度的制定、所涉及的各方法律关系内容以及技术的实现。

1.3.1 认证机构

为保证网上数字信息的传输安全,除了在通信传输中采用更强的加密算法等措施之外,必须建立一种信任及信任验证机制,即参加电子商务的各方必须有一个可以被验证的标识,这就是数字证书。数字证书是各实体(持卡人/ 个人、商户/ 企业、网关/ 银行等)在网上信息交流及商务交易活动中的身份证明。该数字证书具有惟一性。它将实体的公开密钥同实体本身联系在一起,为实现这一目的,必须使数字证书符合 X .509 国际标准,同时数字证书的来源必须是可靠的。这就意味着应有一个网上各方都信任的机构,专门负责数字证书的发放和管理,确保网上信息的安全,这个机构就是 CA 认证机构。各级 CA 认证机构的存在组成了整个电子商务的信任链。如果 CA 机构不安全或发放的数字证书不具有权威性、公正性和可信赖性,电子商务就根本无从谈起。

认证中心是电子商务体系中的核心环节,是电子交易中信赖的基础。它通过自身的注册审核体系,检查核实进行证书申请的用户身份和各项相关信息,使网上交易的用户属性客观真实性与证书的真实性一致。认证中心作为权威的、可信赖的、公正的第三方机构,专门负责发放并管理所有参与网上交易的实体所需的数字证书。

概括地说,认证中心的功能有证书发放、证书更新、证书注销和证书验证。CA 的核心功能就是发放和管理数字证书,具体描述如下:

(1) 接收验证最终用户数字证书的申请。

(2) 确定是否接受最终用户数字证书的申请——证书的审批。

(3) 向申请者颁发、拒绝颁发数字证书——证书的发放。

(4) 接收、处理最终用户的数字证书更新请求——证书的更新。

(5) 接收最终用户数字证书的查询、撤销。

(6) 产生和发布证书注销列表(CRL)。

(7) 数字证书的归档。

(8) 密钥归档。

(9) 历史数据归档。

CA 的数字签名保证了证书的合法性和权威性。主体的公钥可有两种产生方式:

(1) 用户自己生成密钥对,然后将公钥以安全的方式传给 CA,该过程必须保证用户公钥的可验证性和完整性。

(2) CA 替用户生成密钥对,然后将其以安全的方式传送给用户,该过程必须确保密钥的机密性、完整性和可验证性。该方式下由于用户的私钥为 CA 所产生,故对 CA 的可信性有更高的要求。CA 必须在事后销毁用户的私钥,或做解密密钥备份。

一般地,公钥有两大类用途:

(1) 用于验证数字签名。消息的接收者使用发送者的公钥对消息的数字签名进行验证。

(2) 用于加密信息。消息发送者使用接收者的公钥加密用于加密消息的密钥,进行数据加密密钥的传递。

相应地,系统中需要配置用于数字签名/ 验证的密钥对和用于数据加密/ 解密的密钥对,这里分别称为签名密钥对和加密密钥对。这两对密钥对于密钥管理有不同的要求。

(1) 签名密钥对

签名密钥对由签名私钥和验证公钥组成。签名私钥具有日常生活中公章、私章的作用,为了保证其惟一性,签名私钥绝对不能做备份和存档,丢失后只需重新生成新的密钥对,原来的签名可以使用旧公钥的备份来进行验证。验证公钥是需要存档的,用于验证旧的数字签名。用来做数字签名的这一对密钥一般可以有较长时间的生命期。

(2) 加密密钥对

加密密钥对由加密公钥和解密私钥组成。为了防止密钥丢失时丢失数据,解密私钥应该进行备份,同时还需要存档,以便在任何时候脱密历史密文数据。加密公钥无须备份和存档,加密公钥丢失时,只需重新产生密钥对。

从上面可以看出,这两对密钥的密钥管理机制要求存在相互冲突的地方,因此,系统必须针对不同的作用使用不同的密钥对。

为了实现其功能,认证中心主要由以下 3 部分组成:

(1) 注册服务器　通过 Web Server 建立的站点,可为客户提供每天 24 小时的服务。因此客户可在自己方便的时候在网上提出证书申请和填写相应的证书申请表,免去了排队等候等烦恼。

(2) 证书申请受理和审核机构　负责证书的申请和审核。它的主要功能是接受客户证书申请并进行审核。

(3) 认证中心服务器　是数字证书生成、发放的运行实体,同时提供发放证书的管理、证书注销列表(CRL)的生成和处理等服务。

1.3.2 证书签发

证书的发放分为两种方式:一是离线方式发放,即面对面发放,特别是企业高级证书,最好是面对面的离线方式发放;二是在线方式发放,即通过 Internet 使用 LDAP,在 i500 目录服务器上下载证书。

1.离线方式发放

离线方式发放的步骤如下:

① 一个企业级用户证书的申请被批准注册以后,审核授权部门(Registry Authority, RA)端的应用程序初始化申请者信息,在 LDAP 目录服务器中添加企业证书申请人的有关信息。

② RA 将申请者信息初始化后传给 CA,CA 为申请者产生一个参照号和一个认证码。参照号 Ref .number 及认证码 Auth .code 在 PKI 中有时也称做 user ID 及 Password。参照号是一次性密钥。RA 将 Ref .number 和 Auth .code 使用电子邮件或打印在保密信封中,通过可靠途径传递给企业高级证书的申请人。企业高级证书的申请人输入参照号及认证码,在 RA 面对面领取证书。证书介质可以存入软盘或者存放于 IC 卡中。

2.在线方式发放

在线方式发放证书的步骤如下:

① 个人证书申请者将个人信息写入 CA 的申请人信息数据库中,RA 端即可接收到从 CA 中心发放的 Ref .number 和 Auth .code,并将在屏幕上显示的参照号和授权码打印出来,当面提交给证书申请人。

② 证书申请人回到自己的微机上,登录到网站,通过浏览器安装 Root CA 证书(根 CA 证书)。

③ 申请人在网页上按提示填入参照号和授权码,自助式地下载自己的证书。

1.3.3 证书撤销

证书废止的原因如下:

(1) 密钥泄密。证书的私钥泄密。

(2) 从属变更。某些关于密钥的信息变更,如机构从属变更等。

(3) 终止使用。该密钥对已不再用于原用途。

(4) CA 本身原因。由于 CA 系统私钥泄密,在更新自身密钥和证书的同时,必须用新的私钥重新签发所有它发放的下级证书。

CA 所发证书要定期归档,以备查询。除用于用户的签名密钥外,对证书所有数据信息都要进行归档处理。CA 使用符合 X.500 标准的目录服务器系统存储证书和证书注销列表。目录和数据库备份,可以根据组织机构的安全策略执行归档,最长时间可以达到 7 年保存期。数据库还保存审计和安全记录。对于用户密钥对,CA 通过专用程序自动存储和管理密钥历史及密钥备份。

在证书的有效期内,由于私钥丢失泄密等原因,必须废除证书。此时证书持有者要提出证书废除申请。注册管理中心一旦收到证书撤销请求,就可以立即执行证书撤销,并同时通知用户,使之知道特定证书已被撤销。PKI(CA)提供了一套成熟、易用和基于标准的证书撤销系统。从安全角度来说,每次使用证书的时候,系统都要检查证书是否已被撤销。为了保证执行这种检查,证书撤销是自动进行的,而且对用户是透明的。这种自动透明的检查大多针对企业证书进行,而个人证书则需要人工查询。

根据申请人的协议,可规定申请人可以在任何时间以任何理由对其拥有的证书提出撤销。撤销申请必须先向 CA 或者 RA 提交。提出撤销的理由是证书持有人的密钥泄露、私钥介质和公钥证书介质的安全受到危害。

CA 可由于以下原因撤销证书:

(1) 知道或者有理由怀疑证书持有人私钥已经被破坏,或者证书细节不真实、不可信。

(2) 证书持有者没有履行其职责和登记人协议。

(3) 证书持有者死亡、违反电子交易规则或者已经被判定犯罪。CA 撤销证书首先要制定撤销程序。证书持有者通过各种通信手段向 RA 提出申请,再由 RA 提交给 CA。CA 暂时“留存”证书,然后撤销失效;提交申请与最后确认处理要规定有效期。将已经撤销的证书存于 CRL 中,在撤销与发布 CRL 之间的时间间隔要有明确规定。

1.3.4 密钥生成、备份和恢复

用户由于某种原因丢失了解密数据的密钥,无法打开被加密的密文,造成数据的丢失。为了避免这种情况的发生,PKI 提供了密钥备份与解密密钥的恢复机制,这就是密钥备份和恢复系统。

在一个可操作的 PKI 环境中,在证书的生命周期内,都会有一小部分用户丢失他们的私钥,通常的原因有:

(1) 遗失或者忘记了口令。虽然用户的加密私钥在物理上是存在的,但实际上不可使用。

(2) 介质的破坏。如硬盘和 IC 卡遭到破坏。

在很多的环境中,特别是在一些企业中,由于丢失密钥造成被保护数据的丢失是不可

接受的。例如,某项业务的重要文件被对称密钥保护起来,而对称密钥又被某个用户的公钥加密起来,假如该用户的解密私钥丢失了,无法恢复这些文件,可能会对这次业务造成严重损失甚至导致业务停止,这是不可接受的事情。

解决上述问题的一个通用可行的方法就是对密钥进行备份并能够及时恢复。密钥的备份与恢复应该由可信的机构 CA 来完成,但值得强调的是,密钥备份与恢复只能针对解密密钥,而签名密钥是不能做备份的。

密钥的备份与恢复形成了 PKI 定义的重要部分。

一个证书的生命周期主要包括 3 个阶段,即证书初始化注册阶段、颁发阶段和取消阶段。而证书密钥的备份与恢复就发生在初始注册阶段和证书的颁发阶段。

1.密钥生成

密钥/ 证书的生命周期中,初始化阶段是终端用户实体在使用 PKI 的支持服务之前,必须经过初始化进入 PKI。它由以下几步组成:

(1) 终端实体注册。

(2) 密钥对产生。

(3) 证书创建和密钥/ 证书分发。

(4) 证书分发。

(5) 密钥备份。

一旦私钥和公钥证书产生即可进入颁发阶段。主要包括以下内容:

(1) 证书检索　远程资料库的证书检索。

(2) 证书验证　确定一个证书的有效性。

(3) 密钥恢复　不能正常解读加密文件时,从 CA 中恢复。

(4) 密钥更新　当一个合法的密钥对将要过期时,新的公/ 私钥密钥自动产生并颁发。

2.密钥备份

用户在申请证书的初始阶段,如果注册声明公/ 私钥对是用于数据加密,出于对数据的机密性安全需要,在初始化阶段,可信任的第三方机构 CA 即可对该用户的密钥和证书进行备份。当然,一个用户的密钥是否由可信任的第三方机构 CA 备份,是一个安全管理策略的问题。一般 CA 机构的安全策略能满足用户的可信任的需求。备份设备的位置可以从一个 PKI 域变到另一个 PKI 域,密钥备份功能可以由颁发相应证书的 CA 机构执行。

注意: 用户用于数据签名目的的私钥是绝对不能备份的,因为数字签名是用于支持不可否认性服务的,不可否认性服务要与时间戳服务相结合,即数字签名有时间性要求,私钥不能备份和恢复。

3.密钥恢复

密钥恢复功能发生在密钥管理生命周期的颁发阶段,是对终端用户因为某种原因而丢失的加密密钥给以恢复。这种恢复由可信任的密钥恢复中心或者 CA 来完成。密钥恢复的手段可以是从远程设备恢复,也可以是通过本地设备恢复。为了可扩展性,减小 PKI 管理员和终端用户的负担,这个恢复过程必须尽可能最大限度地自动化、透明化。任何综合的管理协议都必须包括对这个能力的支持。

密钥的恢复和密钥的备份一样,只适合于用户的加密密钥,签名私钥不应备份,因为这样将影响到提供不可否认性的能力问题。

1.3.5 证书注销列表处理

证书注销列表(Certificate Revocation List,CRL)中记录尚未过期但已声明作废的用户证书序列号,供证书使用者在认证对方证书时查询使用。

证书撤销是在正常过期之前由于密钥泄露或者证书所有者状态改变等情况导致证书颁发机构使证书作废。所以,PKI 必须提供一种允许用户检查证书的撤销状态的状态机制。目前的 X 509 允许下列 3 种情况:

(1) 证书不可撤销。

(2) 颁发证书的认证机构撤销该证书。

(3) 颁发证书的认证机构授予其他机构撤销权限并由其他机构撤销该证书。

X .509 说明的撤销机制使用了证书撤销列表(CRL),该规范也允许使用其他机制。

1.3.6 信息发布

证书和证书撤销信息的发布可能出现很多的情形。

1.私下分发

最简单的分发机制是私下分发。私下分发模型中,撤销信息的交换是非正式和不可靠的。撤销通知可以通过电话或者 E-mail 来传送,但不能保障撤销的消息被可靠地传送到每一个相关的个体,也不存在一个软件可以在用户收到撤销消息的时候帮用户决定下一步最合适的活动。

虽然私下分发可行的环境确实存在,但对于企业级的范围,它是不合适的,至少存在 3 个关键的问题:

(1) 私下分发不具有可扩展性。也就是说,它只能可信地支持一个较小的用户群。

(2) 撤销信息的专门分发是内在不可靠的。例如,在一个足够大的群体内,如 1000 个用户甚至更多,非正式的撤销通知不太可能到达所有的依赖方。