第 33 卷　第 23 期　　计　算　机　工　程　　2007 年 12 月
Vol.33　No.23　　Computer Engineering　　December 2007
·安全技术·　　文章编号：1000—3428(2007)23—0179—03　　文献标识码：A　　中图分类号：TP309

CA 系统安全性的分层多方面设计

兰丽娜[1]，杨涛海[2]
（1. 北京邮电大学网络教育学院，北京 100088；2. 信息产业部电信研究院，北京 100083）

摘　要：CA系统本身的安全性是影响Internet电子商务安全的关键问题。分析了CA系统的总体网络结构，提出了一种CA系统的分层多方面安全性设计方案，阐述了网络层安全设计和应用层安全设计。网络层安全采用划分安全区、多层防火墙保护、交换以太网等方法；应用层采用软件代码签名防篡改、数据包增加时间戳防重放攻击、敏感数据内存零化及数据库加密存储、集中监控等 8 个方面的安全性设计。该设计已实际应用于某CA中心，达到了良好的安全性目标。

关键词：CA 系统；网络层安全；应用层安全；防火墙；时间戳

Multi-layer and Multi-aspect Design of CA System Security

LAN Li-na[1], YANG Tao-hai[2]
(1. School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100088;
2. Telecom Research Institute, Ministry of Information Industry, Beijing 100083)

【Abstract】CA system security is the key problem to influence the security in E-commerce. This paper analyzes the network architecture of CA system, and presents a multi-layer and multi-aspect security architecture of CA system. The security design focuses on the network layer and application layer. Firewalls divide CA system network into different security grade areas. The following methods are employed in the application layer for security protects: add the digital signature at the end of the software to prevent invalid code modify, add the sender time stamp in the packets to prevent repeat packets attack, clear to zero in memory and save the important data as encrypted in the database to prevent invalid reading, use central monitor system. The design is employed in a real CA system successfully.

【Key words】certificate authority (CA) system; network layer security; application layer security; firewall; time stamp

CA安全认证系统是Internet电子商务的安全基础[1]，如果CA系统被攻击瘫痪，那么电子商务业务的安全就成为空中楼阁，其安全就不复存在。因此，如何进行CA系统本身的安全性设计，提供完整的安全性解决方案，成为一个非常重要的值得深入研究的课题。

本文提出了一种通用的 CA 系统分层次多方面综合性安全性设计方案，该方案深入分析了 CA 系统面临的多种安全性威胁，制定出对应的安全性策略和保护措施，对于 CA 系统的安全性建设具有重要参考价值。

1　CA 系统总体网络结构

CA 系统的总体网络结构如图 1 所示。

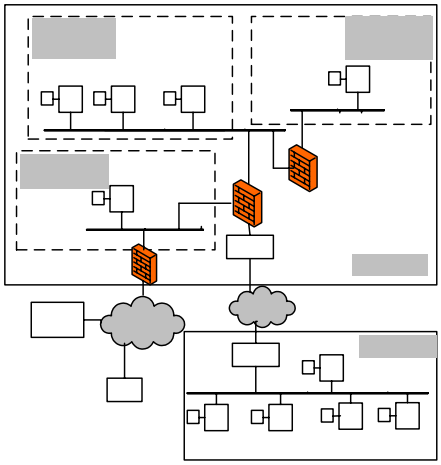

图 1　CA 系统总体网络结构

CA 系统由 2 个子系统组成：CA 中心子系统和 RA 中心子系统。CA 中心只设一个，负责证书的制作和管理；RA 中心作为业务受理点，可设置多个，负责用户证书申请的受理和审核工作。

2　CA 系统安全分层结构

分析CA系统的结构，可设计CA系统的安全层次结构如图 2 所示[2~4]。

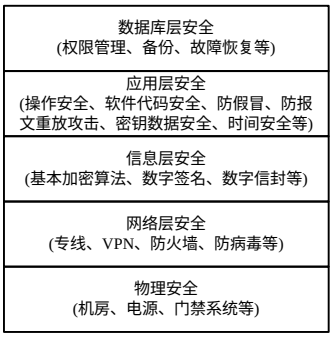

图 2　CA 系统安全层次结构

自下至上依次为物理安全，网络层安全，信息层安全，应用层安全，数据库层安全。各层应采用相应的安全手段。

物理安全主要包括机房安全，采用安全的门禁系统，保证电源的安全，保证不间断供电等。

作者简介：兰丽娜(1972－)，女，讲师、硕士，主研方向：信息安全，软件技术，网络教育技术；杨涛海，高级工程师

收稿日期：2007-07-25　**E-mail：**lindalan2002@sina.com

网络层安全是指网络层的安全保护，可采用专线、VPN、防火墙等技术，防止网络层的非法访问。

信息层安全指通信内容的安全保护，可采用各种加密算法，如对称密钥加密算法、非对称密钥加密算法，采用 CA 证书技术的数字信封、数字签名等技术来保证通信内容的保密性、数据的完整性，并进行通信双方的身份认证。

应用层安全指应用软件的安全，包括软件代码的安全，如何保证代码不被篡改；如何防止应用层的攻击，比如报文重放攻击；软件的操作安全，防止非法操作；防止敏感数据被窃取；防假冒服务器等。

数据库层的安全指数据存储的安全，包括数据库的权限设置、数据库系统的安全、数据库的备份和故障恢复机制等。

CA 系统的安全必须从各个层次的安全入手，保障各层的安全，从而保证整个系统的安全。本文重点讨论网络层、应用层的安全。

3 网络层安全性设计

如图 1 所示，CA 系统的网络层安全性设计主要有以下几点：

(1)网络安全区域的划分

在 CA 安全中心，根据不同应用系统对安全性要求的不同，划分为 3 个安全区域：第 1 区域是证书信息发布系统，是 CA 系统的最外层，包括 WWW 服务、OCSP(online certificate status query)、CRL 服务。第 2 区域是 CA 中心管理系统，位于 CA 中心内部，包括证书管理服务器、监控系统、备份系统。第 2 区域与远程 RA 系统连接。第 3 区域是 CA 中心签发系统，是 CA 系统的核心，位于 CA 中心的最内层，包括证书签名服务器、CRL 签名服务器等。

3 个安全区安全级别从第 1 区域到第 3 区域越来越高，第 3 区域为最高级别安全区。这种划分的原因是由于在一个 LAN 中所有机器的安全性等同于其中安全性最低的系统的安全性，而 CA 系统中有 Win2000、Win NT、Unix 等操作系统，其安全性等级不同，相同的操作系统由于应用系统对安全性要求的不同，应用系统物理位置和服务范围不同，其安全风险也不同。因此，采用划分网段、多层次保护方案，将安全性要求不同的系统分隔开来，便于系统的安全性管理，提高了整个系统的安全性。

(2)多层次防火墙保护

防火墙保护是网络安全性设计中重要的一环，图 1 中采用多层次的防火墙保护，既限制外部对系统的非授权访问，也限制内部对外部的非授权访问，还限制内部系统之间特别是安全级别低的系统对安全级别高的系统的非授权访问。

防火墙系统屏蔽所有常用的网络访问，如 Telnet, Ftp, Smtp, Pop3, RPC, NFS 等，对每一层次的防火墙的功能设计如下：

第 1 层防火墙(FW1#)，接入 Internet，保护对外发布 WWW/OCSP/CRL 服务器安全接入 Internet。通过隔离内部网络和外部网络，防火墙只允许 WWW/OCSP/CRL 服务器的 80 端口对外提供服务，既隔离外部网络对服务器及 CA 中心管理系统以及 CA 中心签发系统的非授权访问，也限制从 OCSP 服务器对外部网络的不必要访问。

第 2 层防火墙(FW2#)，位于 CA 中心证书信息发布系统、CA 中心管理系统与远程 RA 系统三者之间，实现三方的访问控制。FW2#可保护 CA 中心系统不会被远程 RA 系统非授权访问；也限制 CA 中心系统对远程 RA 系统的非授权访问。连接远程 RA 系统的路由器也连接在 FW2#上，使用静态路由方式在路由器上限制 CA 中心的管理系统和远程 RA 系统对 Internet 的访问。

第 3 层防火墙(FW3#)，位于 CA 中心最里层，主要用于保护签名服务器。签名服务器负责证书签名制作和 CRL 签名制作，只与证书管理服务器通过 FW3#通信。

(3)与远程 RA 系统的安全连接

CA 中心与远程 RA 系统的连接有 2 种方案：DDN 专线方式和 VPN 方式。建议采用 DDN 连接方式。采用 DDN 专线方式连接，远程 RA 系统与公众 Internet 网物理上是分开的，加上采用防火墙控制访问权限，能有效保证系统的安全性。

(4)交换以太网

网络设计采用交换式以太网。共享式以太网的主机以共享一个 10M/100M/1000M 的方式来传送数据包，导致主机存在被窃听的可能，即当其中一台机器被控制，网络适配器被设置为混杂模式时，就能接收其他机器的所有数据包，如果口令被窃听，将导致同一网络中所有主机被控制。如果两台正在通信的机器之间传递的数据包被窃听，就可能将数据包经过修改，然后进行重放或欺骗性攻击。而采用交换式以太网，数据包在 LAN 上是从一台机器到另一台机器，其他机器无法窃听，从而提高了网络安全性。

(5)病毒防范

在防止病毒的感染和传播方面，各服务器及终端均安装防病毒软件，实时监控并杀死病毒，及时更新病毒库，经常彻底查杀病毒。

4 应用层安全性设计

应用层安全是CA系统应用软件安全性设计的重要内容。分析从操作人员进入系统到系统运行过程中，可能出现的各种安全隐患。比如：非法进入系统，网络出现假冒服务器，非法篡改软件代码，恶意修改系统时钟，窃取敏感数据，报文重放攻击，密钥的安全存储等。对于这些安全隐患，必须有针对性地进行防范和保护[3]。

应用层安全性设计主要包括以下多个方面[4]：

(1)操作员安全

操作员安全可分为操作员身份认证和操作防抵赖保护。

1)操作员身份认证

CA 系统操作员进入系统均需通过身份认证。全部采用智能 IC 卡进行身份鉴别和权限控制，防止未授权者的非法操作。

2)操作员操作防抵赖

为了防止受理点操作员在违规操作后的抵赖行为，在操作员操作记录中加入操作员的数字签名，并对操作员的所有操作进行完整的日志记录和监控。如果出现问题，可以通过系统的审计功能，检查监控日志中的数字签名等记录查找问题原因。

(2)服务器安全

服务器安全可分为如下 3 方面保护：

1)服务器间的身份认证

目的是确认通信双方的身份，防止冒充行为及抵御重放攻击。在 CA 系统中主要通过 CA 系统软件使用数字证书和数字签名的身份认证以及 IP 地址验证来完成。

2)IP 地址验证

通过配置文件设置该服务器所允许接入的其他服务器或客户机的 IP 地址，只有具有指定 IP 地址的主机的请求才会

被该服务器程序接受，其他 IP 地址的主机的请求将被拒绝。

3)身份认证

服务器之间发送的每一个数据包都使用数字签名，并将其签名用的数字证书附在数据包中。数据包的接收者接收到该数据包后，首先用证书验证数据包的签名完整性，然后检查证书的合法性(签发者，有效期，作废状态)。如果均成功，则检查其权限是否符合该请求的要求。

(3)时间安全

关于时间的安全性分为证书到期报警和系统时钟更改报警保护。

1)服务器证书到期报警

为了让 CA 系统各服务器在证书失效前能够通知管理员作好准备，各服务器会定时监测系统当前时钟，并与服务器证书的有效期进行比较，如果当前时间离证书的失效期在设定的时间内(比如设定为 8 天)，则每天报警一次，并向监控系统发送报警信息。

2)系统时钟更改报警

CA 系统中的主要服务器都定时监测系统时钟，以防止系统时钟被非法篡改。服务器程序在启动时记录当前系统时钟，然后定时检测系统时钟，将上次记录时间加上定时间隔后，与当前时间比较，如果误差在允许范围内，则认为系统时钟正常，并将当前时间设置为记录时间，等待下次检验。如果误差超过允许范围，则认为系统时钟被更改，立即向监控系统发送告警信息，然后终止运行。

(4)密钥安全

密钥安全包括服务器和用户密钥的安全性保护。

1)服务器密钥的安全存储和使用

为了保证服务器密钥的安全，所有服务器均采用加密机或加密卡，私钥保存在加密机或加密卡中，即使有人非法入侵，也无法得到私钥。所有的加密运算均由加密机或加密卡完成，私钥不出加密机/加密卡，保证密钥的安全性。

2)用户密钥的安全

使用智能 IC 卡，密钥对由 IC 卡生成，私钥不出卡。CA 系统只将公钥取出，用于制作证书。在证书制作后回写入 IC 卡，然后发放给用户。在这种方式中，由于私钥不出 IC 卡，即使是 CA 系统操作员也无法获得用户的私钥，因此可以保证用户密钥的安全。

(5)软件代码安全

为了防止程序执行代码被篡改，系统的主要服务器软件均采用代码签名，即在代码后附加数字签名文件。程序在启动时，首先检验自身的签名与签名文件是否一致。如果签名验证通过，则进入正常运行状态；如果签名验证失败，说明代码被篡改，则提示告警后退出运行。

(6)抵御重放攻击

CA 系统软件通过在数据包中增加时间戳或随机数来抵御防重放攻击。加时间戳的数据包格式如图 3 所示。

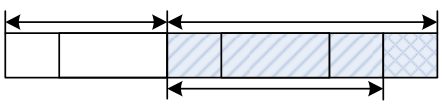

图 3　加时间戳的数据包格式

处理流程如下：在数据包包头和包体中均带上发送者的时间戳或随机数；包体由数字信封及数字签名保护；接收方维护原发者数据包的时戳或随机数的一个缓存；接收者接收到数据包后，首先检查包头中的时戳或随机数与该原发者的时戳或随机数缓存记录比较，如果与缓存中的某个相同，说明该数据包为重复包，则丢弃该数据包；检查数据包的完整性和合法性(包括数字信封、数字签名、数字证书的验证)；检查包体与包头的时戳或随机数是否一致，以防篡改，如果不一致，则丢弃该数据包；如果验证通过，则将该数据包中的时戳或随机数替代该数据包原发者的记录中最旧的时戳或随机数；处理该数据包[5~6]。

(7)敏感数据存储安全

考虑敏感数据在数据库存储安全和在内存中的安全保护。

1)敏感数据的数据库存储安全

为了保证用户信息的安全，对用户资料使用加密机的主密钥加密后再存放到数据库中。该信息的读取由 CA 系统软件自动完成加解密运算，因而防止有人(包括数据库系统管理员)直接从数据库中窃取用户资料。采用数据加密存储后，不用担心用户数据失密，从而可以弥补数据库本身安全不足的问题。

2)敏感数据的内存零化

在 CA 系统程序内部，所有涉及敏感数据的内存在处理后释放这些内存前均将该内存清零后再释放，防止因内存泄漏引起敏感数据的失密。

(8)集中监控的实现

系统监控从日志和实时入侵检测 2 个方面进行：

1)运行监测日志记载

对 CA 系统内部各服务器的运行状况进行集中监视，能够通过监控终端了解各服务器的运行状态及处理数据的正确情况。记录两种日志：操作员的操作记录和系统的业务记录。详尽的日志记录方便出现问题时查找问题根源。

2)非法入侵检测

在主要服务器上安装实时检测引擎，定时检测运行的进程中是否有非法进程，如 Telnet, FTP 等不允许的进程，如果检查到这些非法进程，立即向监控系统发送报警信息，并可根据设定将非法进程杀掉。

5　结束语

CA系统作为电子商务的安全基础，其本身的安全性至关重要；而CA系统的网络分布式特点又决定了其安全性设计的复杂性和多层次性。本文针对CA系统进行分层多方面安全性设计，设计具有通用性和实用性，其中应用层的安全性设计深入、全面，多种方法对于一般的网络服务器软件具有很好的借鉴意义。该设计已实际应用于某CA中心，取得了良好的安全性保护。

参考文献

1 王　茜, 杨德礼. 电子商务安全体系结构及技术研究[J]. 计算机工程, 2003, 29(1): 72-75.

2 聂小逢, 郑　东, 顾　健. 认证机构 CA 的安全体系设计[J]. 计算机工程, 2004, 30(12): 288-290.

3 Nash A. 公钥基础设施(PKI)实现和管理电子安全[M]. 北京: 清华大学出版社, 2002.

4 文俊浩, 徐传运, 徐光侠, 等. 分布式管理信息系统安全策略研究[J]. 计算机应用研究, 2006, 23(9): 130-132.

5 ITU-T Recommendation X.509[Z]. (2002-03). http://www.itu.com.

6 IETF. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework[S]. RFC 2527, 1999-03.