文章编号:1001 - 9081(2006)06 - 1320 - 04

视频会议系统身份认证的一种解决方案

徐彦彦[1],陈 曦[2],徐正全[1]
(1. 武汉大学 测绘遥感信息工程国家重点实验室,湖北 武汉 430079;
2. 中国船舶重工集团公司 第 701 研究所,湖北 武汉 430070)
(xuyy@lmars.whu.edu.cn)

摘 要:视频会议系统的安全问题日趋重要。身份认证是视频会议系统安全体制中最为重要的环节。总结了当前视频会议系统中对用户身份进行认证的方法,指出了它们存在的缺陷。提出了一种基于智能 IC 卡和改进的 Kerberos 协议的视频会议系统身份认证的解决方案,并对其安全性进行了分析。

关键词:身份认证;视频会议;kerberos;智能 IC 卡
中图分类号: TP309;TP393 **文献标识码**:A

Solution of authentication in video conferencing system

XU Yan-yan[1], CHEN Xi[2], XU Zheng-quan[1]
(1. *State Key Laboratory of Information Engineering in Surveying, Mapping, and Remote Sensing, Wuhan University, Wuhan Hubei* 430079, *China;*
2. *China ShipBuilding Industry Corporation, No.* 701 *Research and Development Institute, Wuhan Hubei* 430070, *China*)

Abstract: The security of video conferencing system is becoming more and more important. Authentication is the most important part of the system' s secure mechanism. The ways of authentication in present video conferencing sytem were summarized and its weakness were pointed out. A new solution which based smart IC card and improved Kerberos was put forward and its security was analysed.

Key words: authentication; video conferencing; Kerberos; smart IC card

0 引言

视频会议系统的安全需求主要体现在:身份认证(Authentication)、数据完整性(Integrity)、私密性(Privacy)、可用性(Availability)、不可抵赖性(non-Repudiation)。其中,身份认证是视频会议系统安全体制中最为重要的环节,它是所有安全服务的前提,其他安全服务都依赖于它。一旦身份认证系统被攻破,则其他所有的安全措施都形同虚设。因此,身份认证是保障视频会议系统安全性的前提。

目前公认的能比较完善地解决身份认证问题的是基于数字证书的认证方法,这种方法比较可靠,但由于是基于公钥密码体制,存在运算速度较慢,开销较大的特点,并不适用于视频会议这个对实时性要求较高的通信系统。而一些运算速度较快,实施较为简单的身份认证方法,如基于口令的认证等方式,又存在较多的安全弱点,容易造成系统的安全隐患。因此,需要一种既能有效保证视频会议系统身份认证安全性,又能满足视频会议系统对实时性要求较高特点的身份认证解决方案。

本文总结了当前视频会议系统中对用户身份进行认证的方法,提出了一种基于智能 IC 卡和 kerberos 协议的视频会议系统身份认证的解决方案。这种身份认证系统能有效对视频会议系统用户身份进行识别和认证,为视频会议系统的安全提供最基本也是最重要的保障。

1 现有的视频会议系统身份认证方法

目前视频会议系统常用的身份认证方法主要有:密码验证方法、基于共享口令的身份认证方法、基于证书的身份认证方法等等。

1.1 密码认证方法

密码认证方法通过预先设置会议密码的方式来确保只有合法的用户才能加入到会议中。用户请求加入会议时会被要求给出密码。由于密码采用明文传递,因此此种方法极易受到攻击,攻击者只需侦听合法用户的通信过程,即可获知会议密码,从而假冒合法用户加入会议。

1.2 H.235 协议中的身份认证方法

H.235 协议是 ITU-T 组织针对 H.323 系统的安全性问题制定的协议,用于保证基于 H.323 协议的视频会议系统的安全性。H.235 协议中提出的身份认证方法有:基于共享口令的身份认证方法和基于公开密钥证书的身份认证方法。

1) 基于共享口令的认证方法。要求通信双方在通信开始前以其他方式(如通过电话,电子邮件等形式)约定好通信密码。这种认证方法包括使用对称加密算法进行认证和使用哈希的进行认证。

a) 使用对称加密算法的认证方法。需要验证对方身份的一方 EPA 以明文发送一个挑战 challengeA 给 EPB,EPB 对

收稿日期:2005 - 12 - 20 **基金项目**:武汉市科技攻关计划资助项目(20031003021);湖北省科技攻关计划资助课题(2004AA101C18)
作者简介:徐彦彦(1974 -),女,河南信阳人,助理研究员,博士研究生,主要研究方向:多媒体网络通信、信息安全; 陈曦(1973 -),男,湖北武汉人,工程师,博士研究生,主要研究方向:大型网络数据库、虚拟现实; 徐正全(1962 -),男,湖北黄岗人,教授,博士生导师,博士,主要研究方向:可视电话、多媒体视频会议系统、图像处理.

挑战 challengeA 使用共享口令进行加密后传递给对方,并以明文发生挑战 challengeB。如果 EPA 解密 EPB 发来的消息后得到的挑战值正确,说明对方知道共享密钥,身份合法。EPA 向对方发送加密后的挑战值 challengeB,以向对方证明自己的身份。

b) 使用哈希的认证方法。在通信过程中,需要证明自己身份的一方 EPA 将口令 password 串接在明文之后做哈希运算,并发送摘要值。接收方 EPB 收到消息后,同样将口令 password 串接在接收到的明文后进行哈希运算,比较运算得到的摘要值与接收到的摘要值是否相同。如果相同,说明对方是合法用户。因为假设只有合法用户才知道约定好的通信密码。

使用基于共享口令的认证方法虽然实施简单,但易受到字典式攻击。攻击者侦听通信过程,获得加密后的挑战值或消息摘要值后可以进行离线分析,使用特定数量的计算资源猜测口令,或将口令按照既定的方法进行转换,并与侦听得到的加密挑战值或摘要值进行比较。如果不是在较大的空间内选取的口令,则很容易被攻击者攻破。而在实际通信过程中用户为了使用方便往往选用容易记忆的口令,这增加了被攻击者破解口令的可能性。

2) 基于证书的数字签名的认证方法。需要证明自己身份的一方 EPB 使用私钥 signB 对包含挑战值 challengeA 的消息进行签名,并在消息中携带由 CA 签发的证书 Certificate。接收方使用证书中的公钥检查签名。这种方法虽然安全性较好,但由于是基于公钥加密算法,计算复杂耗时,在视频会议这种对实时性要求很高的系统中,并不适用。

2　基于智能 IC 卡和 Kerberos 协议的身份认证

视频会议系统中的身份认证问题可分为两个部分,一是要确定当前与会者的身份,即身份识别问题;二是确定与会者身份是否合法,即身份认证问题。我们采用的是一种基于智能 IC 卡和改进的 Kerberos 协议的身份认证方法,利用智能 IC 卡来识别当前与会者的身份,利用改进的 Kerberos 协议来确定与会者身份是否合法。

2.1　用户身份识别

传统视频会议系统中,通常会把终端名称作为用户身份。但这只能说明当前是哪一台物理终端参与会议,而不能说明是哪一个用户目前正在使用终端参加会议。因此,必须有其他方式辅助来帮助识别用户身份。

目前,智能芯片卡技术已成为解决身份识别问题的焦点和热点技术。作为具有最高安全性的便携式多功能身份识别和通信媒介,智能卡已成为以在线和离线方式进行可靠的个人身份认证的最佳方案。每个用户持有一张智能卡,智能卡存储用户个性化的秘密信息,同时在验证服务器中也存放该秘密信息。进行认证时,用户输入个人身份识别码,智能卡认证。成功后,即可读出智能卡中的秘密信息,进而利用该秘密信息与主机之间进行认证。智能卡具有硬件加密功能,可对智能卡中的信息进行加密处理,这样即使智能卡被窃取,用户仍不会被冒充。基于智能卡的认证方式是一种 PIN + 智能卡的双因素的认证方式,有较高的安全性。

利用智能卡在资源、实用性、功能性、安全性等方面优势,可将用户的身份、用户 PIN 值和权限信息保存到智能卡中,通过读取智能卡,获取用户身份信息,并与视频会议系统的认证服务器进行认证,实现强制性的身份认证和权限管理。同时用户 PIN 值采用加密方式存储,即使智能卡被窃取,由于无法获知加密密钥,仍无法得知用户信息。

通过使用智能卡技术,可以有效识别出当前使用视频会议系统的用户身份。

在系统运行过程中,也可通过实时监控用户 IC 卡的状态来实施系统运行过程中的身份保护。系统可实时监控 IC 卡使用状态,一旦 IC 卡状态发生变化,系统会自动退出运行,从而确保系统运行过程中的用户身份不发生变化。

2.2　用户身份认证

在 H.323 通信过程中,只有当来自一个节点的 H.323 呼叫首先被确认身份之后,才能够提供进一步的安全保证,因此身份认证过程须在通信过程的开始建立阶段实施。我们选择在 H.323 通信中最早开始的呼叫连接建立阶段对用户身份进行鉴别。

在 H.323 点到点通信过程中,终端需要相互进行身份认证,以确认身份是否合法;在多点通信过程中,身份认证过程可被认为是终端和 MCU 之间的确认身份的过程。我们考虑在系统中部署一台认证服务器存储合法用户信息,并对用户身份进行认证。Kerberos 是一种为 TCP/IP 网络设计的可信第三方认证协议,Kerberos 有一个存储所有客户和他们的秘密密钥的数据库,能向一个实体证实另一个实体的身份,还能产生会话密钥,供一个实体和另一个实体使用,因此非常适合做视频会议系统中身份认证服务器。

2.2.1　Kerberos 协议

Kerberos 提供一种基于对称密钥、在网络上实施认证的服务,它是一个三方认证协议,根据被称为密钥分发中心(KDC)的第三方服务中心来验证网络中计算机相互的身份,并建立密钥以保证计算机间安全连接。KDC 有两个部分组成:认证服务器 AS 和门票分发服务器 TGS。一旦身份得到验证,Kerberos 协议将会给这两台计算机提供密钥,以进行安全通信对话。Kerberos 协议可以认证用户的身份,并通过使用密钥和对称加密算法为用户间的通信加密。

Kerberos 的认证分为三个阶段:

1) 初始化阶段。在这个过程中,用户取得访问 TGS 的门票访问门票 TGT 和与 TGS 通信时使用的会话密钥;

2) 门票分发过程。这个过程完成后,用户取得访问远端用户的门票 Ticket 和通信时使用的会话密钥;

3) 用户之间的相互认证过程。至此,完成双向认证过程。

在 Kerberos 认证过程中,存在若干缺陷[3]。在初始化阶段,用户主密钥由用户口令根据公开算法计算得出,这种方式生成的密钥通常被认为是弱密钥,不能抵御攻击者的字典式攻击。另外,当用户通过用户名/口令登录系统时,攻击者也可以很容易地使用非法程序记录用户口令,得到用户主密钥,系统将不再安全。另外,在门票分发过程和用户间的相互认证过程中,Kerberos 使用基于时间的鉴别符防止重放攻击,鉴别符的有效时间范围通常为 5min。在 5min 的时间内攻击者足够发起新的攻击。并且这种防止重放攻击的方法依赖于机器的时钟被精确同步。如果时钟失去同步,那么过期的鉴别符也会被重放。而在实际的视频会议系统中,各终端的部署往往非常分散,难以做到所有的终端保持时钟同步。

针对以上 Kerberos 协议的缺陷,对 Kerberos 协议进行了部分改造,以满足实际的需求。采用智能卡和用户口令相结合的方法,获取用户主密钥;采用挑战/响应的方法来证实用

户身份,避免了使用基于时间的鉴别符时,Kerberos 对系统时间同步精度要求较高的缺点。

2.2.2 用户身份认证模型

视频会议系统身份认证模型如图 1 所示。

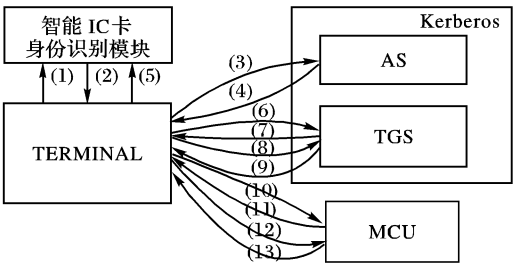

图 1 视频会议系统身份认证模型

其中,身份认证服务器由 AS 和 TGS 组成,AS 为认证服务器,TGS 为门票分发服务器。认证服务器上保存用户数据库,对终端用户身份进行认证。门票分发服务器为合法终端提供访问 MCU 的证书。

2.2.3 身份认证过程

1)符号描述

在对视频会议系统身份认证过程的描述中,我们使用如下符号:

ID_t = 终端用户名信息;

ID_{tgs} = TGS 用户名信息;

ID_m = MCU 用户名信息;

Times = 时间标志,表示门票开始使用时间、截至使用时间;

Nonce = 随机数;用于防止重放攻击;

Realm = 指明用户所属的领域;

Options = 用户请求的将在返回的票据中设定的特定标志;

K_t = 终端用户对应的主密钥;

K_{tgs} = TGS 共享的会话密钥;

$K_{t,tgs}$ = 终端用户和 TGS 共享的会话密钥;

$K_{t,m}$ = 终端用户和 MCU 共享的会话密钥。

2)工作过程

terminal→智能 IC 卡身份识别模块:系统提示用户插入 IC 卡

智能 IC 卡身份识别模块→terminal:用户插入智能卡,系统读取卡内用户名信息

terminal→AS:KRB_AS_REQ,Options ‖ ID_t ‖ $Realm_t$ ‖ ID_{tgs} ‖ Times ‖ Nonce1

AS→terminal:KRB_AS_RSP,

ID_t ‖ $Realm_t$ ‖ $Ticket_{tgs}$ ‖ $Ek_t[K_{t,tgs}$ ‖ Times ‖ Nonce1 ‖ $Realm_{tgs}$ ‖ $ID_{tgs}]$

其中 $Ticket_{tgs} = Ek_{tgs}[K_{t,tgs}$ ‖ $Realm_t$ ‖ ID_t ‖ Times];

系统提示用户输入口令,以口令为密钥,解密智能卡上加密的 K_t 值;并以 K_t 值为密钥,解密 AS 发来的加密信息;

Terminal→TGS:KRB_TGS_REQ,Options ‖ ID_m ‖ Times ‖ $Ticket_{tgs}$

TGS→terminal:$Ek_{t,tgs}$[Nonce2]

Terminal→TGS:Nonce2

TGS→terminal:KRB_TGS_RSP

$Realm_t$ ‖ ID_t ‖ $Ticket_{mcu}$ ‖ $Ek_{t,tgs}[K_{t,m}$ ‖ ID_m ‖ $Realm_m$ ‖ Times]

其中,$Ticket_{mcu} = Ek_{mcu}[K_{t,m}$ ‖ ID_t ‖ Times];

Terminal → MCU: setup, Options ‖ $Ek_{t,m}$ [Nonce3] ‖ $Ticket_{mcu}$

MCU→terminal:$Ek_{t,m}$[Nonce4]

Terminal→MCU:Nonce4

MCU→terminal:connect,Nonce3

3)工作原理

系统启动后,首先会提示用户插入智能 IC 卡,用户插入 IC 卡后,由身份识别模块读取卡内用户名信息 ID_t。

终端向认证服务器 AS 发送一个认证服务请求 KRB_AS_REQ,给出用户名信息 ID_t 和 ID_{tgs},表明这个用户要访问 TGS。

认证服务器 AS 收到消息后,查询数据库,检查此用户名是否合法,如果是合法用户,AS 发送认证服务响应消息 KRB_AS_RSP,此消息由门票访问门票 $Ticket_{tgs}$ 和一个用 K_t 加密的分组构成,分组中包含用于终端和 TGS 通信的会话密钥 $K_{t,tgs}$;$Ticket_{tgs}$ 包含用户名信息 ID_t 和会话密钥 $K_{t,tgs}$,并使用 K_{tgs} 加密。

终端收到响应消息后,提示用户输入用户口令,并以口令为密钥,解密获得存储在卡内的用户主密钥信息 K_t,以 K_t 为密钥,对加密分组进行解密,获得与 TGS 进行通信的会话密钥 $K_{t,tgs}$。

终端向门票分发服务器 TGS 发送 KRB_TGS_REQ 消息,请求获得访问 MCU 的门票。请求消息中包含终端用户名 ID_t、要访问的 MCU 用户名 ID_m、门票访问门票 $Ticket_{tgs}$。

TGS 收到请求消息后,产生一个随机数挑战 Nonce2,使用 $k_{t,tgs}$ 加密后发送给终端。终端收到加密值后,解密得出 Nonce2,并发送给对方。如果终端能正确解密 Nonce2,说明终端知道会话密钥 $k_{t,tgs}$,是合法终端。TGS 在证明终端身份后,构造一个新的密钥 $K_{t,m}$ 用于终端和 MCU 之间的通信,同时生成一个门票 $Ticket_{mcu}$,该门票包含新生成的用于终端和 MCU 通信的密钥 $K_{t,m}$。TGS 将门票及使用 $k_{t,tgs}$ 加密的分组信息,以响应消息 KRB_TGS_RSP 发送给终端,分组信息包括 MCU 的用户名 ID_m、密钥 $K_{t,m}$ 及其他一些信息。

终端收到 KRB_TGS_RSP 消息后得到访问 MCU 的门票 $Ticket_{mcu}$,同时解密后得到密钥 $K_{t,m}$。接着,终端发送请求建立连接的 setup 消息给 MCU,消息中包含门票 $Ticket_{mcu}$ 和使用会话密钥 $K_{t,m}$ 加密的随机数 Nonce3。

MCU 收到消息后,产生一个随机数挑战 Nonce4,使用 $k_{t,m}$ 加密后发送给终端。终端解密得出 Nonce4,并发送给对方。如果终端能正确解密 Nonce4,说明终端知道会话密钥 $k_{t,m}$,是合法终端。MCU 在证明终端终端身份后,发送响应消息 connect,并在响应消息中将解密后的 Nonce3 发送给终端,以向终端认证自己的身份。至此,终端和 MCU 完成了双向身份认证,建立了可靠的呼叫连接。

2.3 系统安全性分析

身份认证系统常常受到的攻击包括:侦听、假冒合法用户身份、攻击存储用户信息的数据库、重放攻击、字典式口令猜测攻击等等。

我们提出的视频会议系统身份认证解决方案,能有效抵御以上攻击,安全性较好,并具有实施简单、效率高的特点,非常适合应用于视频会议系统这一应用场合。

系统具备的优点有:

1)采用智能 IC 卡进行用户身份识别。每个合法用户对应一张 IC 卡,在 IC 卡中写入用户身份信息,防止假冒。视频会议终端或 MCU 启动时,智能 IC 卡身份识别模块读取用户信息,识别出当前是哪个用户在使用系统。没有智能 IC 卡则

无法使用系统。在系统运行过程中,此模块动态监控 IC 卡状态,一旦用户抽掉 IC 卡,系统立即能够识别,停止运行,保障了系统运行过程中的用户身份安全。同时,IC 卡内用户密钥信息采用加密方式存储,即使遗失,由于不知道用户口令,也无法获取。通过以上方式,能有效防止攻击者的假冒合法用户身份的攻击。

2) 用户主密钥是在发卡时由伪随机序列产生,并以用户口令为密钥加密存储于智能卡中。只有在智能卡和用户口令都具备的情况下,才能成功获取主密钥,二者缺一不可。攻击者很难通过字典式口令猜测攻击等非法手段得到用户主密钥。

3) 在对用户身份进行认证时使用认证服务器生成的随机会话密钥,而不是使用用户口令做为密钥。从而避免攻击者使用非法手段获取用户口令,获得会话密钥。并且随机会话密钥只用于本次会话,只在本次会话有效,有效时间很短。即使攻击者采用离线攻击方式窃取了会话密钥,但当会话密钥失效后也无法冒充合法用户。

4) 在终端对服务器发出门票请求消息后,服务器生成随机数,并以会话密钥加密后做为挑战发送给对方。终端只有在返回正确的随机数后,服务器才通过对终端的身份的确认。使用这种挑战/响应的方法,解决了 kerberos 协议中存在的基于时间戳的鉴别符不能有效防止重放攻击,且分布式系统很难维持比较精确的时间同步的弱点。

5) 认证服务器的安全得到保证,并易于维护。记录用户信息的数据库中,用户对应主密钥采用加密方式存储,攻击者即使能访问数据库,但因为无法获得认证服务器对应主密钥,也无法窃取合法用户信息,认证服务器的安全得到保障。在每一次身份认证过程中,与终端一次通信所需的全部有用数据均保存在 TGT 中,包括用户名、会话密钥、门票过期时间等等。认证服务器只需解密 TGT 即可获得此次通信所需全部信息。这样可使认证服务器无须进行状态维护,也不需要存储任何临时数据,只需要有一个记录合法用户信息的静态数据库,从而减轻认证服务器的负担,很容易地实现认证服务器的维护。

6) 在终端和 MCU 身份认证过程中生成的用于终端和 MCU 之间进行通信的会话密钥,除了用于终端和 MCU 相互进行认证外,还可用于终端和 MCU 在 H.245 通信过程中产生的媒体流会话密钥的加密密钥,无须另外再次生成密钥,提高系统效率。

7) 系统对用户身份认证基于 Kerberos 协议,Kerberos 采用对称加密算法,运算速度比公钥算法高出百倍,效率很高,能满足视频会议系统对实时性要求较高的特点。

3　结语

视频会议系统中的身份认证问题是视频会议系统安全最基础也是最重要的保障。本文提出的一种视频会议系统身份认证的解决方案,利用智能 IC 卡对用户身份进行识别,不仅在通信开始前对用户身份的进行识别,还能在系统运行过程中动态监控用户身份变化。利用改进的 Kerberos 实现对视频会议系统用户身份的认证,能有效防止攻击者的各种攻击,并解决了 Kerberos 协议存在的缺陷,安全性好。同时能满足视频会议系统对实时性要求较高的特点,是一种非常适合视频会议系统特点的身份认证解决方案。

参考文献:

[1] ITU-T Recommendation H.323. Packet-Based Multimedia Communications Systems[S], 1998.

[2] ITU-T Recommendation H.235. Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals[S], 2000.

[3] BELLOVIN SM, MERRITT M. Limitations of the Kerberos Authentication System[J]. Computer Communications Review, 1990, 20(5):119 - 132.

[4] NEUMAN BC, TS' O T. An Authentication Service for Computer Networks[A]. IEEE Communications Magazine[C]. September, 1994.33 - 38.

[5] STALLINGS W. 密码编码学与网络安全:原理与实践[M]. 第 2 版. 北京:电子工业出版社,2001.

[6] 刘玉,徐一新,王长强,等. 机要公文安全分发的一种解决方案[J]. 华中科技大学学报(自然科学版),2003,31(8):102 - 104.

(上接第 1319 页)

的真实身份。对于典型的 CA 认证中心签发的证书,可以用证书主题信息作为判断对方真实身份的可靠依据。而对于自助型 CA 认证中心,只能从系统的用户表中提取对方信息。相对与典型的 CA 认证中心严格的身份审核机制和高度安全的网络环境,应用系统的安全可靠性要差得多,因此,用自助型 CA 签发的证书进行签名/加密,有一定的安全风险。

为了弥补自助型 CA 认证中心签发证书的随意性带来的安全隐患,图 2(b)对自助型 CA 认证中心进行了一定的改进。改进后的 CA 服务器不再直接面对用户接受申请、签发证书,而是运行在应用服务器后台,用户通过应用服务器身份认证后才能申请证书。证书主题的内容也不再是用户随意填写,而是由应用系统从用户信息表里自动提取。用户信息表中的用户身份关键数据(如:用户姓名、所属部门、职位等),只能由有特殊权限的管理员填写,普通用户不能直接更改。这样可以在一定程度上保证证书主题的可靠性,从而提升自助型 CA 认证中心的权威性。

5　结语

相对于典型的 CA 认证中心,自助型 CA 认证中心的建设和运营成本大大降低,但是这种成本的降低是在牺牲 CA 认证中心的权威性的前提下取得的。自助型 CA 认证中心在结构上与企业应用系统融为一体,具有简单、方便的特点。

考虑企业应用的具体情况,很多时候对 CA 认证中心的权威性的需求并不显著,这时,采用自助型 CA 认证中心颁发数字证书,可以充分利用 CA 的技术为企业的信息安全提供保证。

参考文献:

[1] 袁卫忠,王德强,茅兵,等. 公钥基础设施的研究与进展[J]. 计算机科学,2004,31(2):82 - 88.

[2] 孟桂蛾,董邦文,场宇航. 公钥基础设施 PKI 的设计[J]. 计算机工程,2001,27(6):111 - 113.

[3] 金晓秋,郭巍,金亿平,等. PKI 中的证书和发证机构[J]. 计算机科学,1999,26(7):83 - 86,76.

[4] 李新,孙玉芳. 基于关系型数据库的 CA 系统[J]. 计算机工程,2004,30(8):1 - 3.

[5] 李新,张继东,孙玉芳. 签名加密技术在公文系统中的应用[J]. 计算机应用研究,2004,21(4):98 - 99.