摘 要

信息新科技不仅给全球带来飞速发展和不断变化着我们的生活,而且还给一些犯罪分子提供了一种新的犯罪类型。为了抵御这些非法的犯罪活动的产生，我们在计算机科学领域不断的尝试使用各种防御措施，目前基于 Windows 操作系统的安全防护软件虽有不少，但纯软件或是纯硬件的效果都不是太理想。这主要是由于纯软件的加密技术有时只能防住一般的远程攻击，防范的功能十分有限也有很多漏洞；而纯硬件的加密技术是功能很单一的防范措施，对现代各种应用的操作系统的兼容性不强，使用起来非常局限等缺点。为了提高系统的安全防御能力、对现代应用型操作系统的兼容性、使其功能更加完善，本文采用一种软件加密算法与硬件加密设备相结合的安全防护方法。该方法很好的解决了上述由于纯软件和纯硬件加密所存在的缺点，它通过软硬件的有机结合，基于硬件加密设备的 GINA 登录技术可以实现用户身份认证、终端资源访问控制以及安全审计等工作，从而有效地提高了网络系统的信息安全防御能力。

本文就基于 Key 的身份认证和授权系统的具体实现方法进行详细的论述:首先从各个方面对目前的网络安全现状进行探讨,并且说明了研究该项目的实际意义；然后分析了目前国际上比较成熟的身份认证和授权系统的相关技术（密码技术、身份认证技术、授权访问控制技术等）；并重点介绍了基于硬件加密锁(USB-Key)的身份认证和授权系统的具体设计与实现方法；其次，还讨论了基于硬件加密锁(USB-Key)的身份认证和授权系统的安全性；最后,作者对整个研究项目进行总结,并提出一些不足的技术问题和今后研究任务的展望。

关键词： 身份认证； 授权系统； USB-Key； GINA

Abstract

The rapid development of network technology have not just brought revolutionary changes to our daily lives, but also provide a platform for the realization of a new type of crime. There are different types of criminal activities: - some are commercial crimes committed though the Internet, some use computers to commit crime whilst some crimes are targeting against computer system.

Thus, computer network should be equipped with doughty enough measures in information security, meanwhile, it must be consider to adopt correlation techniques such as network's physics security, visit control security, system security, user correlation technique security, information encryption, security transmission and management security, in order to insure network information's secrecy, integrality and usability.

This paper first presents some basic knowledge on information security, then analyze main technology on identification authentication and authorization system. Follow in this paper has discussed the design and implementation of Identification Authentication an Authorization System Base on USB-Key. Later in this paper has discussed the security in this system. Finally, the author given a summary above this paper, and just put forward some shortcomings in this segment.

Key words: Identification Authentication; Authorization System; USB-Key; GINA

1 引 言

1.1 网络信息安全研究的国内外概况

1.1.1 网络安全的现状

随着全球经济一体化，必然带来全球化的市场竞争。在这种情况下，网络的应用应运而生。网络的发展为信息共享、信息协作和商务拓展创造了一个崭新的万能空间。在这场前所未有的信息大潮中，中国的各行各业早就已经开始感受信息化、电子化管理的冲击，用信息化、电子化手段来搭建自己规范化的、高效率的企业管理平台。在享受网络带来的快捷便利的同时，由于网络的开放性，必然存在着不同程度的安全隐患。以下以典型应用网络为例，分析目前的安全状况[1]。

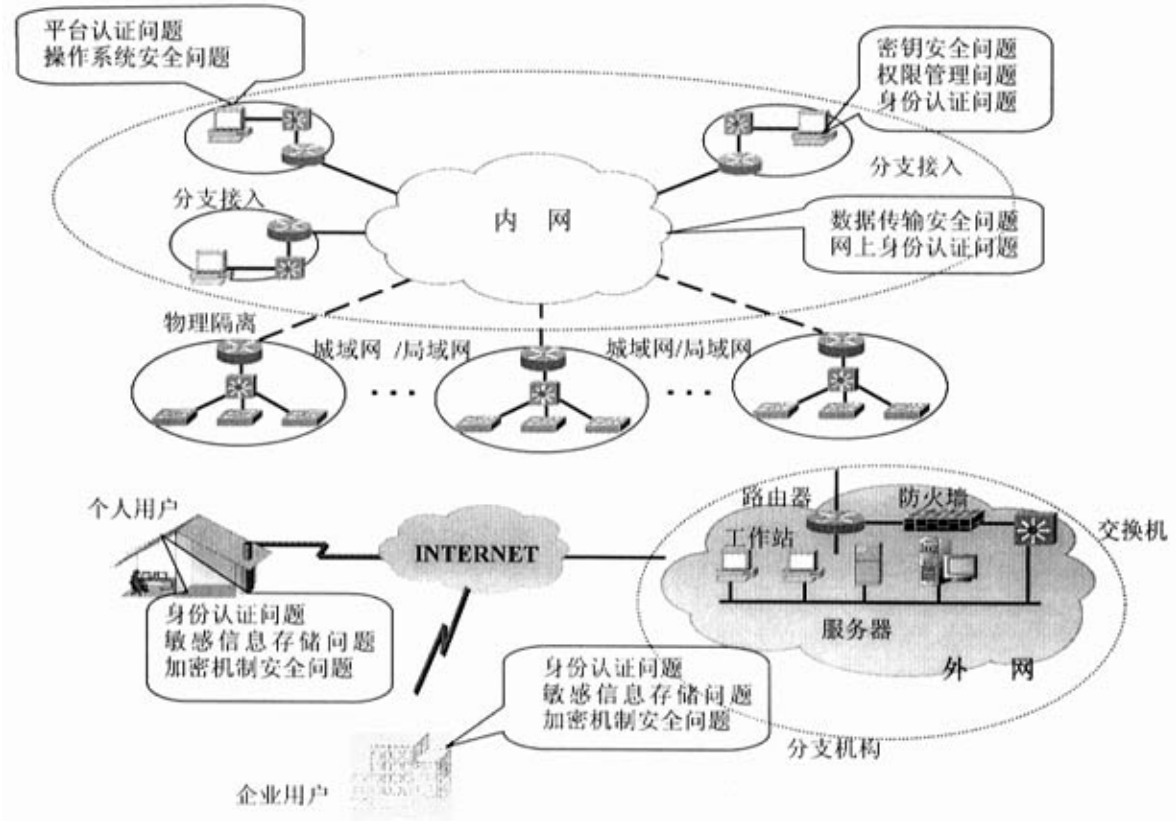

图 1.1 典型应用网络及安全隐患示意图

最初面向研究的 Internet 和它的通信协议群是为一种理想的环境而设计的。在那种理想的环境里,使用 Internet 的人就是创建 Internet 的人，用户和主机之间互相信任,志在进行自由开放的信息交换。然而，随着时间的推移,Internet 变得越来越庞大，这种理想的环境已经荡然无存[2]。

今天,在 Internet 的环境中,信任感已经所剩无几了。社会上能找到的所有的凶险,卑鄙和投机,Internet 上应有尽有，Internet 的开放性已经成为一把双刃剑。从 Internet 诞生之日起,特别是 20 世纪 90 年代向公众开放以来,它已经成为众矢之的。进入 21 世纪，网络安全事件愈演愈烈，已经成为一个越来越严重和值得关注的国际问题[3]。

最近，美国计算机安全协会公布的"计算机犯罪及安全调查"表明：计算机领域有太多的非法和侵权行为，这个数量远远大于企业与其客户、股票持有人和生意合伙人之间突出法律解决的纠纷数量[4]。

1.1.2 网络信息安全研究的国内外文献综述

为了抵御非法的网络犯罪活动的产生，我们在计算机科学领域不断的尝试使用各种防御措施，如：利用密码技术、身份认证技术、授权访问控制技术等纯软件加密技术；或是使用硬件加密芯片为代表的嵌入式硬件加密设备等纯硬件的加密技术。据了解，目前基于 Windows 操作系统的安全防护软件虽有不少，但纯软件产品（如：软件加密产品、软件身份认证产品、软件授权管理产品）或是纯硬件产品（如：智能 IC 卡、智能加密芯片、智能电子钥匙 Key）的效果都不是太理想。这主要是由于纯软件的加密技术有时只能防住一般的远程攻击，防范的功能十分有限也有很多漏洞；而纯硬件的加密技术是功能很单一的防范措施，对现代各种应用的操作系统的兼容性不强，使用起来非常局限等缺点。下面就国内外对纯软件的安全产品和纯硬件的安全产品的使用现状加以说明:

1.1.2.1 纯软件的安全产品

1、软件加密产品

密码技术是保护信息安全的主要手段之一。密码技术自古有之，到目前为止，已经从外交和军事领域走向公开，它并且是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，它不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能[5]。所以，使用软件加密产品不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、

伪造和假冒。

最典型的产品如：Safe Net 公司的加密狗系列产品[6]。

2、软件身份认证产品

在 Internet 的应用中，必须加强对用户的身份认证以及对平台的身份认证，防止非法用户进行破坏。因此需要为进行电子业务的实体定义唯一的电子身份标识，并通过该标识进行身份认证，保证身份的真实性[7]。

3、软件授权访问控制产品

网络工程和应用系统的建设为企业内部信息的开放与交换提供了可能，但是应用系统的信息在使用中对于不同类型的服务对象，信息的开放程度、内容的详细程度都有严格的管理要求。用户授权和访问控制体系的建设就是设计统一的授权策略，建立统一的用户管理中心，提供统一的应用系统访问控制基础平台和实现机制，解决企业网现有的多种不同类型的用户对多个不同业务应用系统的授权和访问控制问题，防止用户越权访问或修改数据，确保对信息的访问限制在授权范围内。

最典型的产品如：中软信息安全实验室研制的"身份认证授权与审计平台"软件产品[8]。

纯软件产品的安全技术虽然功能多、兼容性好、使用方便、成本低的特点，但是纯软件技术有时只能防住一般的远程攻击，防范的功能十分有限，而且作为软件本身也有很多漏洞和程序 Bug[9]。

1.1.2.2 纯硬件的安全产品

从现有的网络安全硬件来看，以下这几种硬件加密设备是用得最多的。下面就对这几种硬件的加密设备加以说明：

1、智能 IC 卡

在我们的日常工作和生活中已经越来越离不开智能 IC 卡了，随处都可见到它的影子。如：银行 IC 卡、公交 IC 卡、员工身份 IC 卡等。可见，这项技术现在已经趋于成熟，它不但有成本低廉、使用方便、易于携带等诸多优点，而且还具有反复使用、损耗小的特点。现在国际和国内都大量的使用着这项技术，提高处理各项事务的效率。正是由于这项技术的广泛使用，使得基于该技术的各种应用的研发工作不断改进，现在基于 IC 卡的各种加密功能已经越来越强大[10]。

典型产品如：明华澳汉公司的 M&W 智能读卡器和智能卡[11]、华正天网公司 SJW16 和 SJW16-A 密码卡[12]、北京金奥博数码信息技术有限责任公司研制的"SRZ06

身份认证系统”（其中：SRZ06 身份认证系统是具有国内自主知识产权的专利信息安全产品，采用对称加密算法体制，基于智能卡技术实现网络身份认证，对称加密算法具有安全性高和加密速度快等特点，智能卡具有较强的安全数据防护功能[13]。）

国内的一些智能卡开发和提供商开发的智能卡操作系统也有非常大的市场。如：深圳明华公司的 SmartCOS、武汉天喻公司的 TYCOS、北京握奇公司的 TimeCOS 等，这些公司对国内智能卡行业的发展起到了极大的推动作用[14]。

2、智能加密芯片

智能加密芯片是把加解密功能集成到芯片中的一项高新技术，这样就使得具有加解密功能的芯片可以成为一种功能模块，应用到各种硬软件产品之中，加强这些产品的安全功能，如：集成加密芯片的电脑主板、智能加密锁 Key、手机、MP3、自动取款机等[15]。

但是，对于智能加密芯片的研究，还在不断的提高，相信在不久的将来，这项技术将运用到更广泛的科学技术领域中去。

典型产品如：RDC 的 JK2810 芯片组[16]。

3、智能电子钥匙 Key

智能电子钥匙 Key 技术是近年来，随着 U 盘存储设备的广泛使用而发展起来的一项新兴的硬件加密设备锁。它的外观和 U 盘相似，只是内部集成了智能加密芯片和其他存储电路的硬件安全产品。

智能 Key 的特点是有标准的 USB 接口，可以很好的配合 PC 机的使用，但是目前这项技术还不是很完善，希望在以后的发展中能实现更多的具有实用性的功能，如：不但可以起到电子钥匙的作用，还可以像 U 盘一样存储数据。

典型产品如：明华澳汉公司的 M&W EKey 产品[17]。

纯硬件产品的安全技术虽然防攻击性强、稳定性好，但纯硬件的加密技术是功能很单一的防范措施，对现代各种应用的操作系统的兼容性不强，使用起来非常局限等缺点。

综上所述，国内的软硬件结合的身份认证和授权产品目前处于探索阶段，因此，研究基于 Key 的身份认证和授权系统意义重大。

1.2 网络信息安全的研究范畴

在经过系统和科学的分析之后，国际著名的网络安全研究公司 Hurwitz Group 得

出以下结论：在考虑网络安全问题的过程中，应该主要考虑以下五个方面的问题：网络是否安全？操作系统是否安全？用户是否安全？应用程序是否安全？以及数据是否安全？

目前，这个五层次的网络系统安全体系理论已得到了国际网络安全界的广泛承认和支持，均已将这一安全体系理论应用在其产品之中[18]。下面我们就将逐一对每一层的安全问题做出简单的阐述和分析。

1.2.1 网络层的安全性（Network Security）

主要技术：防火墙技术

网络层的安全性问题核心在于网络是否得到控制，即：是不是任何一个 IP 地址来源的用户都能够进入网络？如果将整个网络比作一幢办公大楼的话，对于网络层的安全考虑就如同为大楼设置守门人一样。守门人会仔细察看每一位来访者，一旦发现危险的来访者，便会将其拒之门外。

通过网络通道对网络系统进行访问的时候，每一个用户都会拥有一个独立的 IP 地址，这一 IP 地址能够大致表明用户的来源所在地和来源系统。目标网站通过对来源 IP 进行分析，便能够初步判断来自这一 IP 的数据是否安全，是否会对本网络系统造成危害，以及来自这一 IP 的用户是否有权使用本网络的数据。一旦发现某些数据来自于不可信任的 IP 地址，系统便会自动将这些数据阻挡在系统之外。并且大多数系统能够自动记录那些曾经造成过危害的 IP 地址，使得它们的数据将无法第二次造成危害。

用于解决网络层安全性问题的产品主要有防火墙产品和 VPN———虚拟专用网。防火墙的主要目的在于判断来源 IP，将危险或未经授权的 IP 数据拒之于系统之外，而只让安全的 IP 数据通过。一般来说，公司的内部网络若要与公众 Internet 相连，则应该在二者之间配置防火墙产品，以防止公司内部数据的外泄。VPN 主要解决的是数据传输的安全问题，如果公司各部在地域上跨度较大，使用专网、专线过于昂贵，则可以考虑使用 VPN。其目的在于保证公司内部的敏感关键数据能够安全地借助公共网络进行频繁地交换。

1.2.2 系统的安全性（System Security）

主要技术：入侵检测技术、反病毒技术

在系统安全性问题中，主要考虑的问题有两个：一是病毒对于网络的威胁；二是黑客对于网络的破坏和入侵。

病毒的主要传播途径已由过去的软盘、光盘等存储介质变成了网络，多数病毒不仅能够直接感染网络上的计算机，也能够将自身在网络上进行复制。同时，电子邮件、文件传输（FTP）以及网络页面中的恶意 Java 小程序和 ActiveX 控件，甚至文档文件都能够携带对网络和系统有破坏作用的病毒。这些病毒在网络上进行传播和破坏的多种途径和手段，使得网络环境中的防病毒工作变得更加复杂，网络防病毒工具必须能够针对网络中各个可能的病毒入口来进行防护。

对于网络黑客而言，他们的主要目的在于窃取数据和非法修改系统，其手段之一是窃取合法用户的口令，在合法身份的掩护下进行非法操作；其手段之二便是利用网络操作系统的某些合法但不为系统管理员和合法用户所熟知的操作指令。例如在 Unix 系统的缺省安装过程中，会自动安装大多数系统指令。据统计，其中大概有约 300 个指令是大多数合法用户所根本不会使用的，但这些指令往往会被黑客所利用。

要弥补这些漏洞，我们就需要使用专门的系统风险评估工具，来帮助系统管理员找出哪些指令是不应该安装的，哪些指令是应该缩小其用户使用权限的。在完成了这些工作之后，操作系统自身的安全性问题将在一定程度上得到保障。

1.2.3 用户的安全性（User Security）

主要技术：身份认证技术

对于用户的安全性问题，所要考虑的问题是：是否只有那些真正被授权的用户才能够使用系统中的资源和数据？

首先要做的是应该对用户进行分组管理，并且这种分组管理应该是针对安全性问题而考虑的分组。也就是说，应该根据不同的安全级别将用户分为若干等级，每一等级的用户只能访问与其等级相对应的系统资源和数据。

其次应该考虑的是强有力的身份认证，其目的是确保用户的密码不会被他人所猜测到。在大型的应用系统之中，有时会存在多重的登录体系，用户如需进入最高层的应用，往往需要多次输入多个不同的密码，如果管理不严，多重密码的存在也会造成安全问题上的漏洞。所以在某些先进的登录系统中，用户只需要输入一个密码，系统就能够自动识别用户的安全级别，从而使用户进入不同的应用层次。这种单一登录体系要比多重登录体系能够提供更大的系统安全性。

1.2.4 应用程序的安全性（Application Security）

主要技术：访问控制技术

在这一层中我们需要回答的问题是：是否只有合法的用户才能够对特定的数据进行合法的操作？

这其中涉及两个方面的问题：一是应用程序对数据的合法权限；二是应用程序对用户的合法权限。例如在公司内部，上级部门的应用程序应该能够存取下级部门的数据，而下级部门的应用程序一般不应该允许存取上级部门的数据。同级部门的应用程序的存取权限也应有所限制，例如同一部门不同业务的应用程序也不应该互相访问对方的数据，一方面可以避免数据的意外损坏，另一方面也是安全方面的考虑。

1.2.5 数据的安全性（Application Confidentiality）

主要技术：密码技术

数据的安全性问题所要回答的问题是：机密数据是否还处于机密状态？

在数据的保存过程中，机密的数据即使处于安全的空间，也要对其进行加密处理，以保证万一数据失窃，偷盗者（如网络黑客）也读不懂其中的内容。这是一种比较被动的安全手段，但往往能够收到最好的效果。

上述的五层安全体系并非孤立分散。如果将网络系统比作一幢办公大楼的话，门卫就相当于对网络层的安全性考虑，他负责判断每一位来访者是否能够被允许进入办公大楼，发现具有危险性的来访者则将其拒之门外，而不是让所有人都能够随意出入。操作系统的安全性在这里相当于整个大楼的办公制度，办公流程的每一环节紧密相连，环环相扣，不让外人有可乘之机。如果对整个大楼的安全性有更高的要求的话，还应该在每一楼层中设置警卫，办公人员只能进入相应的楼层，而如果要进入其它楼层，则需要获得相应的权限，这实际是对用户的分组管理，类似于网络系统中对于用户安全问题的考虑。应用程序的安全性在这里相当于部门与部门间的分工，每一部门只做自己的工作，而不会干扰其它部门的工作。数据的安全性则类似于使用保险柜来存放机密文件，即使窃贼进入了办公室，也很难将保险柜打开，取得其中的文件。

1.3 课题的来源及其主要研究任务

1.3.1 课题的来源

本课题来源于信息安全国家重点实验室产品化项目。

目前，为了抵御网络非法的犯罪活动的产生，我们在计算机科学领域不断的尝试使用各种防御措施，如：利用密码技术、身份认证技术、授权访问控制技术等纯软件加密技术；或是使用硬件加密芯片为代表的嵌入式硬件加密设备等纯硬件的加密技术。据了解，目前基于 Windows 操作系统的安全防护软件虽有不少，但纯软件或是纯硬件的效果都不是太理想。这主要是由于纯软件的加密技术有时只能防住一般的远程攻击，防范的功能十分有限也有很多漏洞；而纯硬件的加密技术是功能很单一的防范措施，对现代各种应用的操作系统的兼容性不强，使用起来非常局限等缺点[19]。为了提高系统的安全防御能力、对现代应用型操作系统的兼容性、使其功能更加完善，本文提出了一种采用软件加密算法与硬件加密设备相结合的安全防护方法一"基于 Key 的身份认证和授权系统"。该方法很好的解决了上述由于纯软件和纯硬件加密所存在的缺点，[20]它主要是采用加密锁（Key）作为硬件加密设备，并利用 Winlogon（Windows Logon Process）调用 GINA（Graphical Identification and Authentication）动态连接库监视安全认证序列，通过软硬件的有机结合，基于硬件加密设备 Key 的 GINA 登录技术可以实现用户身份认证、终端资源访问控制以及安全审计等工作，从而有效地提高了网络系统的信息安全防御能力。

"基于硬件加密设备的身份认证与授权系统"是在电子化办公的需求下提出的,目的是要求解决当前日常办公中出现的资料外泄和用机管理混乱等情况[21]。这些问题的存在极大的影响了日常办公的效率和对机密资料的管理,所以,为了解决这些问题,我们通过不断的研究与实现,提出了在智能电子钥匙 Key 的技术基础上，结合用户对通用计算机上安全控制的普遍需求，通过硬件智能电子钥匙 Key、安全软件包与 Windows 操作系统的有机结合，为现代通用的计算机在 Windows 操作系统环境下建立和提供了一套有效的、可靠的安全控制体系，使系统具有以智能电子钥匙 Key 支持的权限管理、身份认证、外部设备使用控制、安全审计、系统安全挂起、私有文件保密等安全控制功能。

通过对该系统的研究，更好的完善了硬件电子钥匙在安全领域的应用范围，加强了 Windows 操作系统的安全性、可靠性、实用性等诸多适应当代科学计算机发展的

新优点。也是即 IBM 推出安全计算机以来又一个软硬件相结合的安全计算平台，故从实际的应用出发,研究该系统为以后的相应研究提供一定的参考价值[22]。

1.3.2 本文的主要研究任务

本文首先从各个方面对目前的网络安全现状进行探讨；然后,分析了目前国际上比较成熟的身份认证和授权系统的相关技术（密码技术、身份认证技术、授权访问控制技术等）的实现方法和使用情况；并且，重点介绍了基于硬件加密锁 Key 的身份认证和授权系统的具体设计思想和实现方法；其次，还讨论了基于硬件加密锁 Key 的身份认证和授权系统的实际应用情况和系统的安全性；最后,作者对整个研究项目进行总结。现将本文对基于硬件加密锁 Key 的身份认证和授权系统所做的相关研究及实践工作概括如下：

1、在继承了当前硬件加密锁 Key 和身份认证及授权软件产品的所有功能的基础上，提出并实现基于硬件加密锁 Key 的身份认证和授权系统的解决方案。该系统克服以往由纯软件和纯硬件产品所不具备的更加完善的功能、更加强大的管理机制和更加稳定的系统性能等特点；

2、软件方面：

(1)利用 Winlogon（Windows Logon Process）调用 GINA（Graphical Identification and Authentication）动态连接库监视安全认证序列来实现用户的身份认证功能;

(2)全面地分析了客户/服务器模式和控制中心技术，并以动态链接库技术为基础，实现稳定、灵活的 Windows 软件开发环境，以此作为基于硬件加密锁 Key 的身份认证和授权实现的软件技术基础;

(3)采用 Single DES 或 Triple DES 完善的文件加解密技术实现对文件及数据的加解密功能;

(4)采用虚拟磁盘区间存放加密文件,并且采取权限控制,防止非法用户浏览和使用保密文件。

3、硬件方面：利用现在流行的加密技术集成芯片为基础制作的智能电子钥匙 Key,与其现行的 PC 机的 USB 接口相连，和上述的安全软件包形成一套硬软件相结合的系统，在 Windows 操作系统下实现了具有安全身份认证、授权、审计等多项功能；

4、将 GINA 登录技术融入系统身份认证的工作中，并作为 Windows 操作平台的用户操作界面，该思想具有一定的新颖性。

2 网络信息安全的基本原理及技术

2.1 网络信息安全的基本原理

信息安全系统以密码技术为核心，以数据加密、数字签名、访问控制等安全技术为基础，充分考虑身份认证机制、信息传输安全、权限控制等安全因素，在网络上实现了强有力的身份认证和访问控制功能。使合法用户能够访问网络上的所授权的资源，将非法用户拒绝于网络之外。

身份认证实现了网络用户与服务器之间的双向身份认证，又将 RBAC（基于角色的访问控制）溶入到网络协议代理中，对访问网络的用户实施基于角色的访问控制。本系统代理了应用系统的网络协议，并代理用户访问系统的提供的服务，因而，可对网络用户的行为进行全面的审计，大大的提高了系统的安全性。

2.1.1 网络用户身份认证

网络用户访问网络中的应用服务器时，需完成用户与客户端认证设备(KEY)之间的认证，并利用客户端认证设备(KEY)实现用户与身份认证服务器之间的单、双向身份认证。再通过身份认证服务器的认证后，用户才具有访问应用服务器的令牌。

2.1.2 重要服务器的访问控制

除了用户在访问网络中服务器时需要对其进行身份认证外，系统还对重要的服务器进行访问控制限制。一方面是用户是否有权限访问服务器，另一方面是用户能访问服务器提供的的哪些服务。例如：一些用户能只能访问服务器提供的 WEB 服务，另外一些用户只能访问服务器提供的 FTP 服务；更进一步，某些用户可以访问 WEB 服务中的所有页面，而某些用户则只能访问 WEB 服务中的部分页面。

2.1.3 对资源基于角色的访问控制

RBAC 是基于角色的访问控制的英文缩写，基于角色的访问控制技术的特点是：将对访问者的控制转换为对角色的控制，从而使授权管理更为方便实用、效率更高。同时，角色与角色之间可以继承权限，使各个角色的权限划分更为清晰、明确,降低

了权限管理的复杂性。

角色可以对应现实生活中的行政角色关系，不同角色的用户可以访问不同权限级别的资源。

2.2 密码技术

密码技术是保护信息安全的主要手段之一。[23]密码技术自古有之，到目前为止，已经从外交和军事领域走向公开，它并且是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，它不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

从密码体制方面而言，密码体制有对称密钥密码技术和非对称密钥密码技术。对称密钥密码技术要求加密解密双方拥有相同的密钥．而非对称密钥密码技术是加密解密双方拥有不相同的密钥，在不知道门陷信息的情况下，加密密钥和解密密钥在计算上是不能相互算出的[24]。

2.2.1 对称密钥密码技术

对称（传统）密码体制是从传统的简单换位，代替密码发展而来的，对称密钥密码体制从加密模式上可分为序列密码和分组密码两大类[25]。

序列密码的主要原理是，通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流，（逐比特加密）得到密文序列，所以，序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏。产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列。

分组密码的工作方式是将明文分成固定长度的组（块），用同一密钥和算法对每一块加密，输出也是固定长度的密文。设计分组密码算法的核心技术是：在相信复杂函数可以通过简单函数迭代若干圈得到的原则下，利用简单圈函数及对合等运算，充分利用非线性运算。

对称密钥算法的优点是加解密速度快，适合对大数据量进行加解密运算。

缺点是密钥的分发，管理复杂，在用户群较大的情况下尤其困难[26]。

2.2.2 非对称密钥密码技术

1976 年 Diffie 和 Hellman 以及 Merkle 分别提出了公开密钥密码体制的思想，这不同于传统的对称密钥密码体制，它要求密钥成对出现，一个为加密密钥(e)，另一个为解密密钥(d)，且不可能从其中一个推导出另一个[27]。

非对称密钥算法也称公钥加密算法，用两对密钥：一个公共密钥和一个私有密钥。用户要保障私有密钥的安全；公共密钥则可以发布出去。公共密钥与私有密钥是有紧密关系的，用公共密钥加密的信息只能用私有密钥解密，反之亦然。除加密功能外，公钥算法还可以提供数字签名。经典的公共密钥加密算法有:RSA、DSA、ECC。

公开密钥密码体制的优点就在于：由于加密密钥是公开的，密钥的分配和管理就很简单。公开密钥加密算法能够很容易地实现数字签名，因此，最适合于电子商务应用需要。另外，由于基于尖端的数学难题，所以它有更好的安全性。

其缺点在于：非对称密钥算法较对称密钥算法运算复杂的多，处理速度慢。因此，通常把非对称密钥密码技术与对称密钥密码技术结合起来实现最佳性能。即用非对称密钥密码技术在通信双方之间传送对称密钥，而用对称密钥密码技术来对实际传输的数据加密解密。

2.3 身份认证技术及方式

2.3.1 基于公共密钥的认证机制

目前在 Internet 上也使用基于公共密钥的安全策略进行身份认证，具体而言，使用符合 X.509 的身份证明。使用这种方法必须有一个第三方的证明授权（CA）中心为客户签发身份证明。客户和服务器各自从 CA 获取证明，并且信任该证明授权中心。在会话和通讯时首先交换身份证明，其中包含了将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名、交换通讯的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认该证明是否有效(图 2.1)[28]。

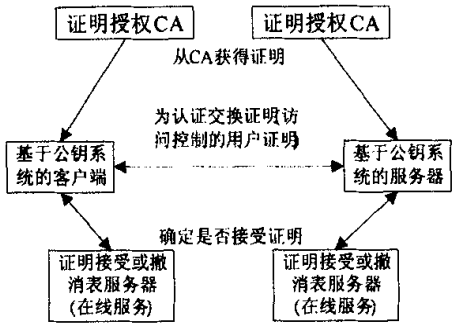

图 2.1 基于公共密钥的认证系统

2.3.2 公共密钥管理服务器（PKMS）

在一般的实现机制中，常将基于公共密钥的 SSL 策略集成在一起，多用在 Web 应用方面。认证服务器通过公共密钥管理服务器（PKMS）与 SSL 连接起来。PKMS 实际是身份认证网关和建立基于 SSL 的加密通道，客户端不必使用客户端软件，可使用 SSL 浏览器登录到 PKMS，PKMS 将用户的身份映射成系统用户身份并且通过 RPC 进行传输，也就是将 SSL 的用户标识传递给认证服务器。[29]PKMS 是用来与 Internet 用户之间临时建立起相互信任的安全会话过程，然后将 Internet 用户身份映射到系统访问控制机制可以管理的用户身份(图 2.2)。

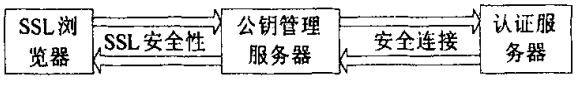

图 2.2 SSL 浏览器、PKMS、认证服务器的交互

2.3.3 基于公共密钥的认证过程

在 PKMS 和使用支持 SSL、S-HTTP 的浏览器用户之间的身份验证是建立在公开密钥加密数字签名和授权证明之上的。数字签名工作如下：

①用户产生一段文字信息然后对这段文字信息进行单向不可逆的变换。用户再用自己的秘密密钥对生成的文字变换进行加密，并将原始的文字信息和加密后的文字变换结果传送给指定的接收者。这段经过加密的文字变换结果就被称作数字签名。

②文字信息和加密后的文字变换的接收者将收到的文字信息进行同样的单项不可逆的变换。同时也用发送方的公开密钥对加密的文字变换进行解密。如果解密后

的文字变换和接收方自己产生的文字变换一致，那么接收方就可以相信对方的身份，因为只有发送方的秘密密钥能够产生加密后的文字变换[30]。

③要向发送方验证接收方的身份，接收方根据自己的密钥创建一个新的数字签名然后重复

上述过程。

一旦两个用户互相验证了身份，他们就可以交换用来加密数据的密钥（如 DES 加密密钥）。（公开密钥加密方法对于大量的数据加密来说速度太慢）。浏览器应该能够在类似的交换过程使用它的公开/秘密密钥组合对来验证它的身份。但是目前还没有出现支持浏览器身份验证的产品。

为了利用数字签名，接收方必须拥有发送方的公开密钥。公开密钥是通过授权证明（Certificates of Authority, CA）来发布的。PKMS 把它的经公开密钥加密的 CA 发送给浏览器。（多数公钥产品只使用了服务器方的身份验证，所以在 CA 中只需要包含 PKMS 的公开密钥）这些授权证明是由可信赖的第三方生成的并且经过可信赖的第三方用秘密密钥"数字签名"的。

用户的浏览器（或者其他客户方的程序）要接收由受信赖的第三方签发的正确的 CA 就必须要配置受信赖的第三方的公开密钥。（浏览器用户使用配置好受信赖的第三方公开密钥的浏览器，来验证 CA 中的受信赖的第三方的数字签名）。如果该浏览器没有配置受信赖的第三方的公开密钥，它就无法验证安全网关的身份。一些浏览器预先配置有受信赖的第三方公开密钥，并且用户不能增加其他的签发 CA 的受信赖的第三方。这限制了将无关公司推出的浏览器的用户与公司拥有的服务器之间建立相互信任关系的能力。

基于 DCE/Kerberos 和公共密钥的用户身份认证是非常安全的用户认证形式，但是，它们实现起来比较复杂，要求通信的次数多，而且计算量较大，下面介绍一种简易、高效、安全的用户身份认证机制-挑战/应答式身份认证[31]。

2.3.4 身份认证的方式

大致上来讲，身份认证可分为用户与主机间的认证和主机与主机之间的认证。本文只讨论用户与主机间的身份认证。用户与主机之间的认证可以基于如下一个或几个因素：

①用户所知道的东西，如口令；

②用户拥有的东西，如智能卡；

③用户所具有的生物特征，如指纹、声音、视网膜扫描等。

下面逐一进行讨论。

2.3.4.1 基于口令的认证方式

基于口令的认证方式是最常用的一种技术，但它存在严重的安全问题。它是一种单因素的认证，安全性仅依赖于口令，口令一旦泄露，用户即可被冒充。更严重的是用户往往选择简单、容易被猜测的口令，如：与用户名相同的口令、生日、单词等。这个问题往往成为安全系统最薄弱的突破口。口令一般是经过加密后存放在口令文件中，如果口令文件被窃取，那么就可以进行离线的字典式攻击。这也是黑客最常用的手段之一[32]。

2.3.4.2 基于智能卡的认证方式

智能卡具有硬件加密功能，有较高的安全性。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 PIN（个人身份识别码），智能卡认证 PIN，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。

基于智能卡的认证方式是一种双因素的认证方式（PIN＋智能卡），即使 PIN 或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能，例如：可以把智能卡设置成用户只能得到加密后的某个秘密信息，从而防止秘密信息的泄露[33]。

2.3.4.3 基于生物特征的认证方式

这种认证方式以人体惟一的、可靠的、稳定的生物特征（如指纹、虹膜、脸部、掌纹等）为依据，采用计算机的强大功能和网络技术进行图像处理和模式识别。该技术具有很好的安全性、可靠性和有效性，与传统的身份确认手段相比，无疑产生了质的飞跃。近几年来，全球的生物识别技术已从研究阶段转向应用阶段，对该技术的研究和应用如火如荼，前景十分广阔[34]。

2.4 授权访问控制技术

2.4.1 传统访问控制机制安全性的分析

传统的访问控制机制包括DAC和MAC两种机制。DAC机制主要用于商用系统，而MAC机制主要用于军用系统。这两种机制也是目前研究最为成熟，应用最为广泛的访问控制机制。

（1）自主性访问控制（DAC）

自主性访问控制基于矩阵模型，它将系统中的实体分为主体S和客体O。在访问控制的矩阵模型下，主体S要对客O进行访问，访问控制机制要检查权利矩阵的元素a，看S是否拥有对O的访问权力以决定是否可以对O进行访问。而且对其他主体具有授与某种访问权力的主体能够自主的将访问特权或访问特权的某以子集授予其他主体。目前，大多数的UNIX、LINUX系统都是基于自主性访问控制。

（2）强制性访问控制（MAC）

自主性访问控制的矩阵模型是基于单级安全模型，而强制性访问控制是基于多级安全模型的。在这些安全模型中，最著名的的便是Bell&La padula模型（简称BLP模型），它在军事系统中有着广泛的应用。在BLP模型中，每一个信息都有一个密级，每个用户也都拥有一个签证。一个人是否允许阅读某一个文件，通过比较该用户的签证与该文件的密级要求是否相符来确定。

2.4.2 新兴访问控制——RBAC机制安全性的分析

科研人员在对传统的DAC和MAC机制研究的基础上，针对这两种访问控制机制的不足提出了一种新的访问控制机制——RBAC机制。

RBAC的基本思想是：授权给用户访问权限，通常由用户在一个组织中担任的角色来确定。角色不同，拥有的权限也各不相同。RBAC根据用户在系统内所处的角色作出访问授权与控制，单用户不能自主的将访问权限传给他人[35]。用户能够对一个客体执行访问操作的必要条件是，该用户被授权了一定的角色，并且由一个在当前时刻处于激活状态，而且这个角色对客体拥有相应的访问权限。RBAC具有以下特点：

①访问权限与角色相关联；

②角色继承；

③最小特权原则；

④职责分离；

⑤角色容量。

2.5 用户授权和访问控制系统

网络工程和应用系统的建设为企业内部信息的开放与交换提供了可能，但是应用系统的信息在使用中对于不同类型的服务对象，信息的开放程度、内容的详细程度都有严格的管理要求。用户授权和访问控制体系的建设就是设计统一的授权策略，建立统一的用户管理中心，提供统一的应用系统访问控制基础平台和实现机制，解决企业网现有的多种不同类型的用户对多个不同业务应用系统的授权和访问控制问题，防止用户越权访问或修改数据，确保对信息的访问限制在授权范围内[36]。

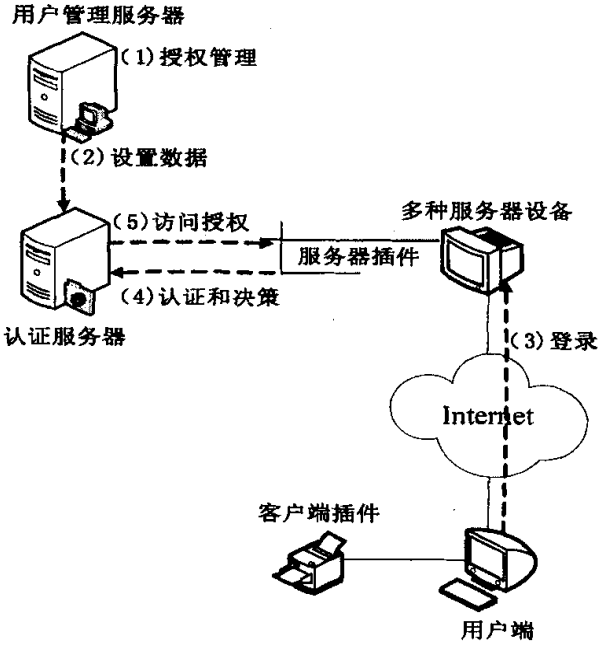

图 2.3 授权和认证服务系统的构成和工作流程

如图 2.3 所示，本设计的访问控制体系包括的基础功能组建主要有：安全客户端插件、安全服务器插件、用户授权管理服务器以及用户认证决策服务器等。

1、安全客户端插件

安全客户端插件设计为浏览器的安全插件，为 B/S 系统提供身份认证、访问控制和安全通信的功能。该插件也支持 VPN 通信方式，或客户本地安全代理方式，也可以为典型的 C/S 系统提供安全代理通信服务。同时，插件还提供了标准的 API 接口，供 B/S 和 C/S 客户端的嵌入式开发和附加功能开发。

2、安全服务器插件

安全服务器插件直接安装在应用服务器上，协助应用系统完成用户认证和访问控制，是为实现访问控制规则、认证和资源之间的联接而设计的插件。在受保护的应用服务器上配置安全服务器插件，访问控制体系可以适应不同的系统环境，并为应用系统实现统一安全策略下的访问控制。

用户授权管理服务器

用户授权管理服务器是一台独立主机，负责建立用户信息、完成用户集中管理、建立访问控制策略、设置认证方法和数据，完成用户的分组或角色定义，权限数据的建立等。权限数据交用户认证服务器使用和提供服务。

3、用户认证决策服务器

用户认证服务器是一台独立的服务器，包括 LDAP 服务器和认证决策模块。数据库内存放着从用户管理服务器获得的权限信息，依据安全服务器插件提供的用户信息完成用户类型的认证并就其访问权限做出决策，决策结果交回给安全服务器插件执行。拥有多个应用系统的大型网络中心可以配备多个用户认证服务器，互为备份，以便提高服务能力，构成冗余配置和提高系统的可用性。

3 基于硬件加密设备的身份认证与授权系统设计原理及实现

3.1 概述

目前各行各业对网络应用的需求已越来越多，随之而来的网络信息安全的管理也变得越来越重要。如何对一个庞大网络的用户身份和信息资源进行有效的安全的管理，如：网络用户身份认证的管理；用户认证后所能获得的应用访问权限的管理，特别是对跨地域、跨组织机构、跨行业的网络用户身份认证和授权访问应用权限的管理等等。对于这些基于网络信息安全的管理问题，国外的许多厂家利用当前的网络先进技术提出了一些很好的解决方案。

随着计算机应用的深入，各行各业迅速向电子化、网络化发展。许多企业或机构相继构建了局域网。内网的建立提高了企业工作效率，加强了内部信息交流，降低了公司运营成本；但同时也给公司带来了业务数据的保密性和安全性等问题，企业不得不考虑如何有效防止使用者通过网络非法拷贝和利用电子邮件等手段轻易地获取公司的核心数据与文件。因此，建立一套在局域网环境下的计算机安全系统已成为企业必须面对和亟待解决的重要问题[48]。

目前，基于 Windows 操作系统的安全防护软件虽有不少，但纯软件的效果有时不是太理想。为了提高系统的安全防御能力，本文提出了一种采用软件加密算法与硬件加密设备相结合的安全防护方法。该方法采用加密锁（USB-Key）作为硬件加密设备，并利用 Winlogon（Windows Logon Process）调用 GINA（Graphical Identification and Authentication）动态连接库监视安全认证序列，通过软硬件的有机结合，基于硬件加密设备的 GINA 登录技术可以实现用户身份认证、终端资源访问控制以及安全审计等工作，从而有效地提高了网络系统的信息安全防御能力。

3.2 基于硬件加密设备的身份认证与授权系统的设计方案

3.2.1 系统功能

“基于硬件加密设备的身份认证与授权系统”是在智能电子钥匙 Key 的技术基础上，结合用户对通用计算机上安全控制的普遍需求，通过硬件智能电子钥匙 Key、

安全软件包与 Windows 操作系统的有机结合，为现代通用的计算机在 Windows 操作系统环境下建立和提供了一套有效的、可靠的安全控制体系，使系统具有以智能电子钥匙 Key 支持的权限管理、身份认证、外部设备使用控制、安全审计、系统安全挂起、私有文件保密等安全控制功能，本系统制作的安全产品所提供个人用户对计算机使用方面的安全控制，具体功能主要有：

1、避免非法登陆、使用计算机；

2、避免计算机丢失后，非法使用自己的保密信息；

3、避免短暂离开，他人偷窥自己的信息；

4、附加功能(加强同一计算机多人使用时不同用户的使用权限的控制，如将计算机短暂借给朋友使用，家长需要控制自己子女对家里计算机的使用)包括有：

- 避免他人对外部设备的非法访问（如：光驱、软驱等）；
- 避免他人对文件的非法访问与操作 ，特别对可执行文件的执行权限的控制；
- 避免他人非法访问网络资源；包括：

a. 限制对指定网址（URL）的访问；

b. 限制上网时间；

c. 对网页内容的过滤；

d. 对网上文件下载的限制；

- 避免他人在自己的计算机上非法安装程序。

3.2.2 运行环境

本系统的运行环境兼容于 Windows 的几个当前流行的操作系统，它们包括：

- Windows 2000Pro；
- Windows 2000Ser；
- WindowsXP.

3.2.3 系统结构

3.2.3.1 系统模块设计

根据系统的功能，如图 3.1 所示，系统模块包括三个部分组成：控制中心软件；客户端软件；系统安全硬件。前面两个是属于软件部分，后面的“系统安全硬件”是属于硬件部分，即电子钥匙 Key。其中控制中心软件还包括：用户管理模块、资源

管理模块、授权管理模块、审计管理模块这四个部分；客户端软件包括：文件保密柜和文件加解密模块。

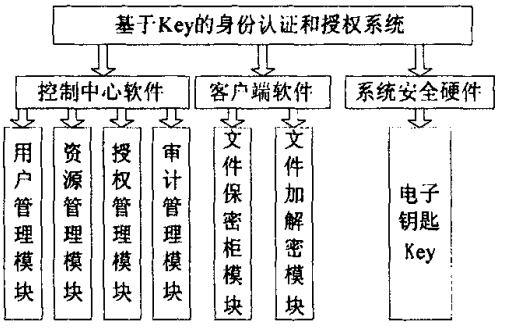

图 3.1 系统基本模块图

这样，系统就是由控制中心和客户端软件包和系统安全硬件三个大部分组成。

3.3 基于硬件加密设备的身份认证与授权系统的实现方法

3.3.1 身份认证登录流程与接口实现

3.3.1.1 GINA 登录基本流程

通过对 GINA. dll 的登录方式的修改，可实现这些新的安全性要求，主要技术原理和实现方法进行具体的详述。首先，我们利用 Windows 安全子系统的认证方式（Winlogon->GINA）进入本地操作；然后，我们在此设置判断 Key 的操作，若系统检测到了 Key，打开一个存储区域以便存放加密文件；反之，如果系统没有检测到 Key 的存在，那么就按照日常的 Windows 方式进行登录。

接下来，以上两种不同的判断结果，将造成不同的操作（如图 3.2 所示）：

有 Key 时，设置一个保存保密文件的存储区域（称为：文件保密箱）；这儿共设置了两种登录方式可供用户选择（自动登录方式和密码登录方式）；

无 Key 时，直接按照日常的 Windows 方式登录，按照输入密码的正误来判断是否可以登录 Windows 操作系统。

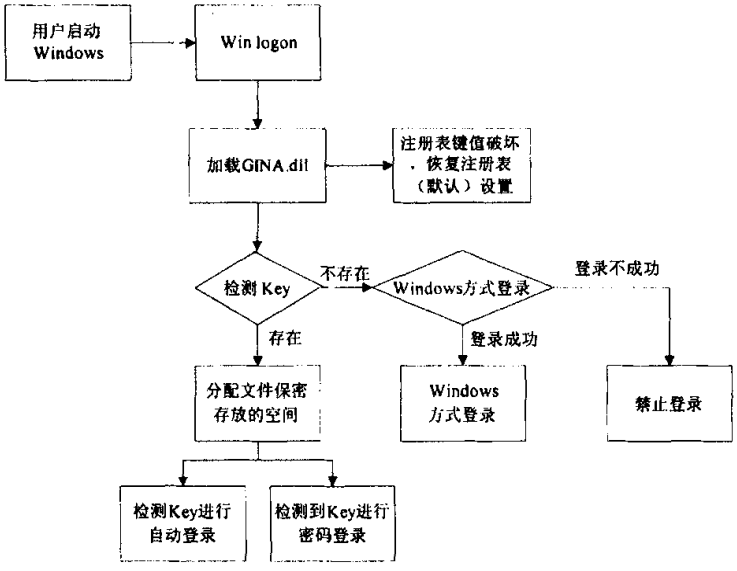

图 3.2 GINA 登录基本流程图

在检测 Key 时，对以下三个条件进行判断：

1、 有Key登录流程

（1） 检测到Key，自动登录方式流程如图3.3所示：

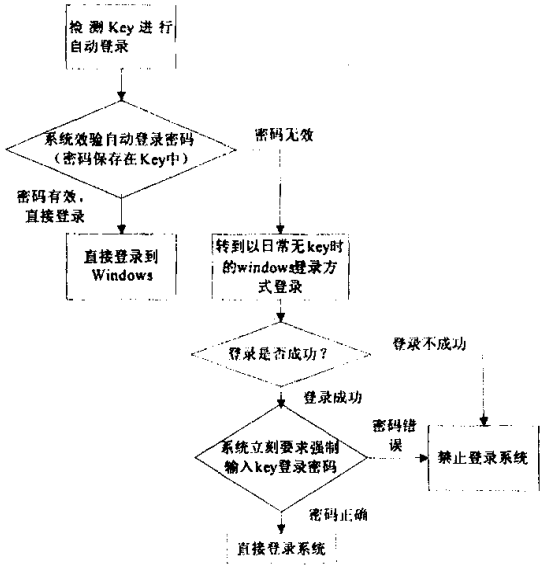

图 3.3 检测到 Key 时自动登录方式流程

第一步：检测到 Key，系统使用自动登录方式登录；

第二步：系统校验自动登录密码（密码就保存在 Key 中）和 Key 的序列号；

第三步：如果校验结果正确（密码有效）,则直接登录到 Windows 操作系统；

第四步：如果校验结果错误（密码无效），则转到日常无 Key 时的 Windows 登录方式进行登录；（这时要继续判断是否登录成功，若登录成功，系统将立刻要求强制输入 Key 的登录密码，这时若输入密码正确，则可直接登录系统；若登录不成功，则禁止登录。）

（2）检测到 Key，密码登录方式流程如图 3.4 所示：

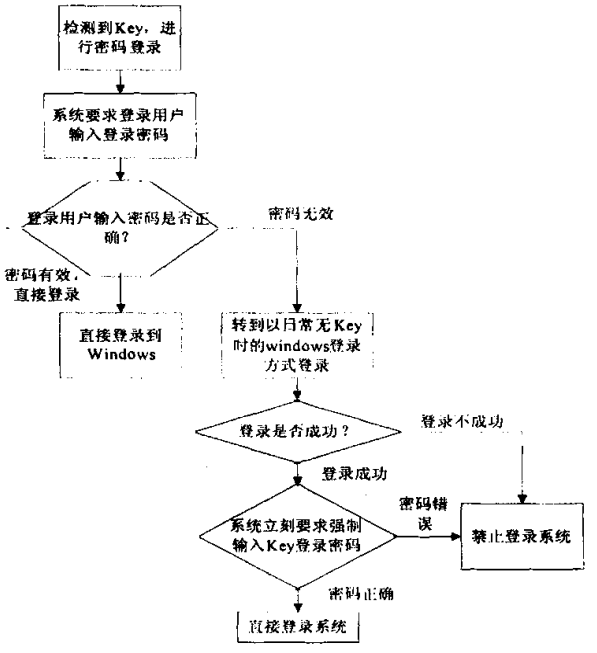

图 3.4 检测到 Key 时密码登录方式流程

第一步：检测到 Key，以密码登录方式登录（出现用户登录界面，请求用户输入登录密码）；

第二步：判断登录用户输入的密码是否正确，如果密码正确，则直接登录到 Windows；如果密码错误，则转到日常无 Key 时的登录方式登录；

第三步：判断此时日常无 Key 时的登录方式是否成功，若登录成功，系统将立刻要求强制输入 Key 的登录密码，这时若输入密码正确，则可直接登录系统；若登录不成功，则禁止登录。）

2、 无 Key 登录流程

无 Key 登录流程如图 3.5 所示：

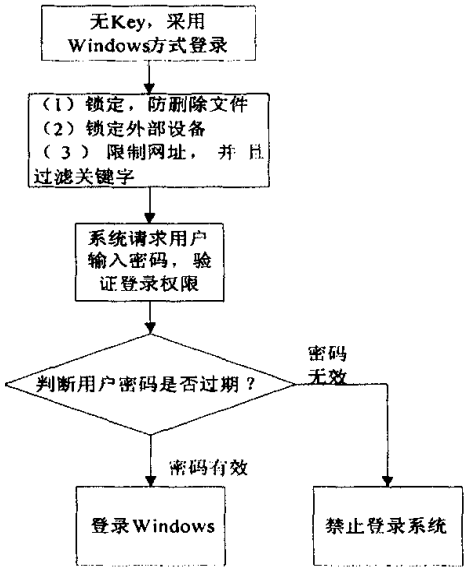

图 3.5 无 Key 时的登录流程图

第一步：无 Key 登录时，以 Windows 方式登录，首先将所有文件锁定，启动防删除功能保护文件；然后锁定外部设备，不许非法用户使用外部设备（如光驱、软驱、USB 口等）；然后限制网址，并且过滤关键字，限制非法用户使用上网功能；

第二步：系统请求用户输入 Windows 密码，验证登录权限；

第三步：判断用户输入的密码是否过期，如果密码有效，则登录到 Windows 系统；如果密码无效，则禁止登录系统。

3.3.1.2 GINA 登录成功后的控制流程

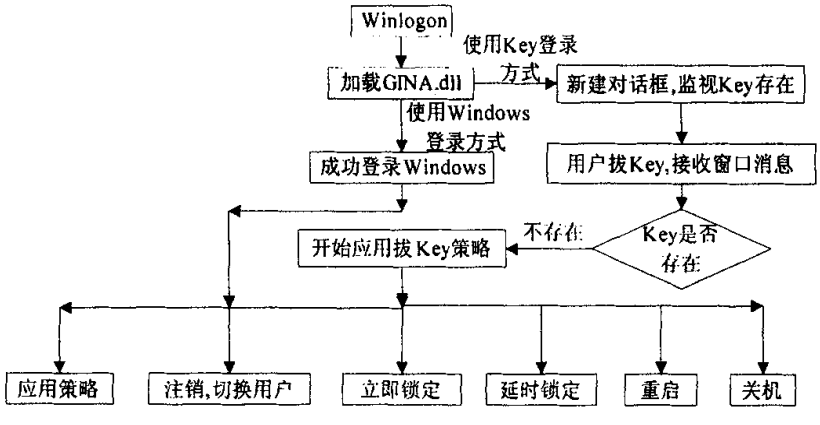

图 3.6 GINA 控制流程图

如上图 3.6 所示，在 GINA 登录成功后的控制流程是按照实际情况来判断选择不同的操作的。其具体的判断与操作如下：

第一步：首先是 Windows 登录“Winlogon”，然后自动加载 GINA.dll 进行 GINA 登录（GINA 登录方式在前面已经讲到）；

第二步：这时，系统会有两项选择，用户根据实际需要选择“使用 Windows 登录方式”或“使用 Key 登录方式”：如果此时用户选择“使用 Windows 登录方式”，则直接登录到 Windows 操作系统中，但是此情况下，系统将锁定一部分 Windows 功能，禁止用户使用；如果此时用户选择“使用 Key 登录方式”，则系统将新建用户对话框，监视 Key 的存在；

第三步：此时，根据第二步中所提到的“使用 Windows 登录方式”和“使用 Key 登录方式”将系统操作分两层：①“使用 Windows 登录方式”后，系统成功登录到 Windows 操作系统，然后系统将各项系统功能进行保护：如“应用策略”、“注销，切换用户”、“立即锁定”、“延时锁定”、“重启”、“关机”等功能提供给不同级别的 Windows 用户；②“使用 Key 登录方式”后，如果用户拔 Key，系统立刻判断 Key 是否存在，一旦系统判断出 Key 不存在，就应用“拔 Key 策略”，即将和直接登录 Windows 操作系统一样应用系统的保护策略，如“应用策略”、“注销，切换用户”、“立即锁定”、“延时锁定”、“重启”、“关机”等功能提供给不同级别的 Windows 用户。

3.3.1.3 GINA 接口设计与实现

1、GINA.dll 与外部设备控制程序之间的接口

（1）实现功能：控制外设；

（2）接口函数：

```
//锁住外设
__declspec(dllexport) long __stdcall LockDevicesMap
(
IN LPCWSTR lpDeviceMap,                    //需要锁住的外部设备
DWORD Flag                                 //0x00 表示锁住设备
);    //0x01 表示解锁
```

2、GINA.dll 与文件控制程序之间的接口

1.实现功能：控制文件加解密、文件防删除、文件锁定；

2.接口函数：

```
FILEACT_API long __stdcall EncryptFile(PFILE pFile);        //加密文件
FILEACT_API long __stdcall DecryptFile(PFILE pFile);        //解密文件
FILEACT_API long __stdcall EnableDelAllFile();              //允许删除所有文件
FILEACT_API long __stdcall DisableDelAllFile();             //不允许删除所有文件
FILEACT_API long __stdcall EnableDelFile(PFILE pFile);      // 允许删除文件
FILEACT_API long __stdcall DisableDelFile(PFILE pFile);     // 不允许删除文件
FILEACT_API long __stdcall LockAllFile();                   //锁定所有文件
FILEACT_API long __stdcall UnLockAllFile();                 //对所有文件解锁
FILEACT_API long __stdcall LockFile(PFILE pFile);           //锁定文件
FILEACT_API long __stdcall UnLockFile(PFILE pFile);         //文件解锁
```

3.3.2 控制中心基本流程与接口实现

3.3.2.1 控制中心基本流程

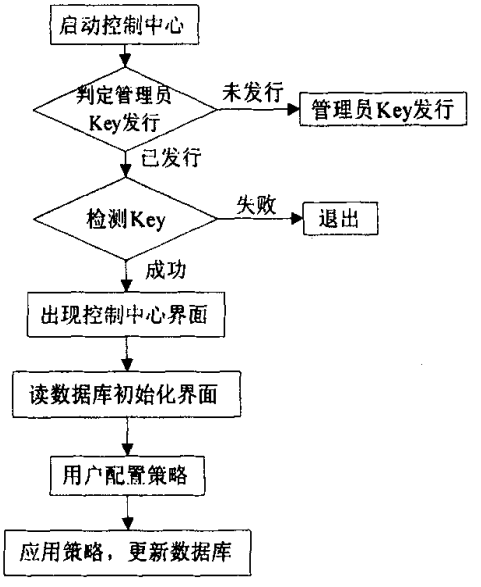

图 3.7 控制中心基本流程图

控制中心是整个系统的核心部分，对于该核心模块的工作流程对整个系统来说非常关键，下面就以图 3.7 所示的流程来具体说明其基本的运行流程：

第一步：首先，启动“系统控制中心”程序；

第二步：判定“管理员 Key”是否发行：若未发行，则直接调用管理员 Key 发行程序，

对管理员 Key 进行发行；若已发行，则检测 Key（检测 Key 通过三个条件判断：a.Key 存在与否；b.Key 的序列号；c.Key 的内外部认证）是否符合要求：①若检测成功，则出现控制中心界面，用户可以对控制中心进行操作；②若检测失败，则立刻退出控制中心判断程序，回到启动控制中心以前的状态下。

第三步：已经经过检测，进入控制中心界面下，此时系统读数据库初始化界面，对系统进行初始化。然后用户根据需要对用户应用策略进行配置，接着，用户策略得到相应，系统应用策略，更新数据库内容。

3.3.2.2 控制中心接口实现

1、控制中心（ControlCenter.exe）与文件设置（FileDB.dll）之间的接口

1）、实现功能：

防删除，加减密，锁定用户指定的文件；

将受限的文件信息写到数据库。

2）、主要数据结构：

```
typedef struct
{
//FILE 信息
    WCHAR KeyID[100];                          //KeyID
    WCHAR UserName[50];                        //用户名
    WCHAR FileName[MAX_RESERVEL_LEN*4];        //FileName
    bool CanDel;                               //能否删除
    bool HasEncryted;                          //是否已经加密
    bool Locked;                               //是否锁定
    WCHAR FileState[4];                        //File 状态
WCHAR reserve1[MAX_RESERVEL_LEN];      //保留字段 1
    WCHAR reserve2[MAX_RESERVEL_LEN];      //保留字段 2
    WCHAR reserve3[MAX_RESERVEL_LEN];      //保留字段 3
}FILEINFO;
```

2、控制中心（ControlCenter.exe）与文件保密柜设置程序 （SECBOX.dll）之间的接口

1）、实现功能：

- 添加文件保密柜；

- 删除文件保密柜；
- 察看文件保密柜内容。

2)、主要数据结构：

```
typedef struct
{  //密钥结构
WCHAR      VolumeName[33];    //卷标名。NTFS 不能超过 32 个字节；FAT32 不能超过 11 个字节.
WCHAR      RootPathName[64];          //虚拟分区的驱动器盘符
DWORD      VirtualDiskSize;           //虚拟分区的容量
WCHAR      ImageFileName[MAX_PATH+1];     //映像文件名
WCHAR      Key[17];                   //虚拟分区的密钥
DWORD      FormatType;                //虚拟分区的格式化类型。0x100 表示 FAT32；0x200 表示 NTFS
BYTE reserve[MAXLEN_KeyRESERVE];  //保留字段
}VIRTUAL_DISK,*PVIRTUAL_DISK;
```

3)、接口函数

```
//新建虚拟盘
SECBOX_API long__stdcall Mount(PVIRTUAL_DISK pVirtualDisk);
//删除虚拟盘
SECBOX_API long__stdcall UnMount(PVIRTUAL_DISK pVirtualDisk);
//判断当前磁盘是否为虚拟盘,如果是虚拟盘，返回虚拟盘信息。
SECBOX_API long__stdcall CheckDisk(LPCTSTR lpRootPathName);
//虚拟盘信息
SECBOX_API long__stdcall VirtualDiskInfo(PVIRTUAL_DISK pVirtualDisk);
//Mount 所有虚拟盘
SECBOX_API long__stdcall MountAll();
//UnMount 所有虚拟盘
SECBOX_API long__stdcall UnMountAll();
```

3、 GINA 登录程序（GINA.dll）与外部设备控制（devicelock.exe)之间的接口

1)、实现功能：控制外设。

2)、主要数据结构：略

3)、接口函数：

```
//锁住外设
__declspec(dllexport) long__stdcall LockDevicesMap
(
IN LPCWSTR lpDeviceMap,     //需要锁住的外部设备
DWORD uFlag                 //0x00 表示锁住设备
);                          //0x01 表示解锁
```

4、GINA 登录程序（GINA.dll）与文件控制(FileAction.exe)之间的接口

1)、实现功能：控制文件加解密，文件防删除，文件锁定。

2)、主要数据结构：略

3)、接口函数：

```
FILEACT_API long __stdcall EncryptFile(PFILE pFile);
FILEACT_API long __stdcall DecryptFile(PFILE pFile);
FILEACT_API long __stdcall EnableDelAllFile();
FILEACT_API long __stdcall DisableDelAllFile();
FILEACT_API long __stdcall EnableDelFile(PFILE pFile);
FILEACT_API long __stdcall DisableDelFile(PFILE pFile);
FILEACT_API long __stdcall LockAllFile();
FILEACT_API long __stdcall UnLockAllFile();
FILEACT_API long __stdcall LockFile(PFILE pFile);
FILEACT_API long __stdcall UnLockFile(PFILE pFile);
```

3.3.3 数据加解密的实现过程

3.3.3.1 数据加密的模式（Single DES 或 Triple DES）

如图 3.8 和 3.9 所示，使用 Single DES 或 Triple DES 算法进行数据加密的方法具体如下：

第一步：用 LD 表示明文数据的长度，在明文数据前加上 LD 产生的新数据块。

第二步：将第一步中生成的数据块分解成 8 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块的长度有可能不足 8 字节。

第三步：如果最后（或唯一）的数据块长度等于 8 字节，转入第四步；如果不足 8 字节，在右边添加 16 进制数字'80'。如果添加后长度已达 8 字节，转入第四步；否

则，在其右边添加 16 进制数字'00'直到长度达到 8 字节。

第四步：对每个数据块用相应的密钥进行加密，根据密钥的长度可以使用 SingleDES 或 TripleDES。

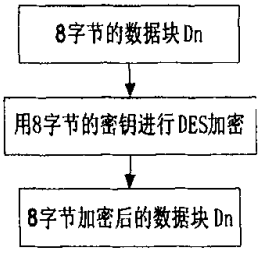

图 3.8 用长度为 8 字节的密钥实现 DES 加密

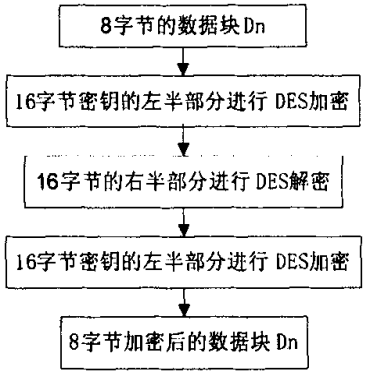

图 3.9 用长度为 16 字节的密钥实现 TripleDES 加密

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的 D1，加密后的 D2，等等）。并将结果数据块插入到命令的数据域中。

3.3.3.2 数据加密的模式（AES）

如图 3.10 所示，使用 AES 算法进行数据加密的方法具体如下：

第一步：用 LD 表示明文数据的长度，在明文数据前加上 LD 产生的新数据块。

第二步：将第一步中生成的数据块分解成 16 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块的长度有可能不足 16 字节。

第三步：如果最后（或唯一）的数据块长度等于 16 字节，转入第四步；如果不足 16 字节，在右边添加 16 进制数字'80'。如果添加后长度已达 16 字节，转入第四步；否则，在其右边添加 16 进制数字'00'直到长度达到 16 字节。

第四步：对每个数据块用相应的密钥（16 字节）进行加密，算法是 AES。

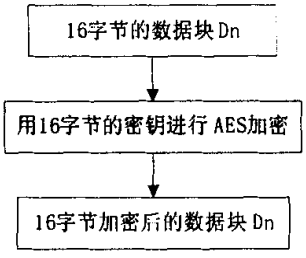

图 3.10 用长度为 16 字节的密钥实现 AES 加密

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的 D1，加密后的 D2，等等）。并将结果数据块插入到命令的数据域中。

3.3.3.3 数据解密的模式（Single DES 或 Triple DES）

如图 3.11 和图 3.12 所示，使用 Single DES 或 Triple DES 算法进行数据解密的方法具体如下：

第一步：将命令数据域中的数据块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如下过程进行解密。

第二步：对每一个数据块使用与数据加密相同的密钥进行解密。

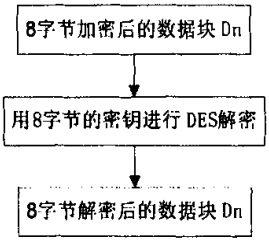

图 3.11 用长度为 8 字节的密钥实现 DES 解密

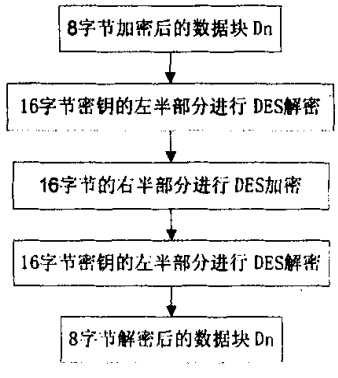

图 3.12 用长度为 16 字节的密钥实现 TripleDES 解密

第三步：计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2 等等）链接在一起。数据块由 LD、明文数据、填充字符组成。

第四步：因为 LD 表示明文数据长度，因此，它被用来恢复明文数据。

3.3.3.4 数据解密的模式（AES）

如图 3.13 所示，使用 AES 算法进行数据解密的方法具体如下：

第一步：将命令数据域中的数据块分解成 16 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如下过程进行解密。

第二步：对每一个数据块使用与数据加密相同的密钥进行解密。

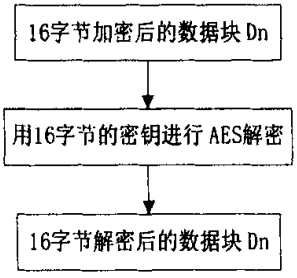

图 3.13 用长度为 16 字节的密钥实现 AES 解密

第三步：计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2 等等）链接在一起。数据块由 LD、明文数据、填充字符组成。

第四步：因为 LD 表示明文数据长度，因此，它被用来恢复明文数据。

3.3.4 系统安装程序流程

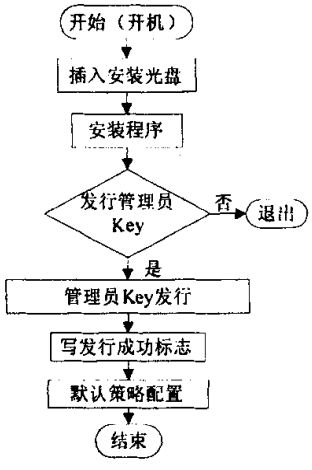

图 3.14 安装系统的控制流程图

如图 3.14 所示，系统软件打包完成后，便可以安装该系统的程序：

第一步：首先开机，插入系统的安装光盘开始安装程序；

第二步：发行管理员 Key 时，通过数据库中存在的纪录来判断是否已发行了管理员 Key：若已发行（查找数据库中有相应 Key 的纪录来判断），则发行管理员 Key，并写发行成功的标志，设置相应的默认策略配置（如：写注册表值）。（具体的步骤见"管理员 Key 发行流程"）

3.3.4.1 管理员 Key 发行流程

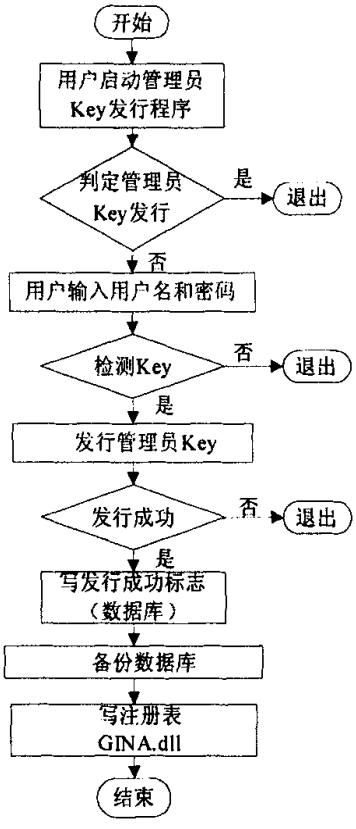

图 3.15 管理员 Key 发行流程图

管理员 Key 的发行流程如图 3.15 所示，具体操作是：首先，开机，安装基于 Key 的身份认证和授权系统后，插入 Key 并使用格式化程序（见安装程序套间），将其初始化，然后启动该系统到主界面下，按照以下的四个步骤进行：

第一步：启动管理员 Key 发行程序；

第二步：判定管理员 Key 是否发行是通过数据库中存在的纪录来判断是否已发行：若以发行，直接退出管理员 Key 发行程序；若未发行管理员 Key，用户在弹出的对话框中输入具有用户身份认证的用户名和密码；

第三步：检测 Key 是否是具有发行管理员 Key 权限：若没有此项权限，则直接退出管理员 Key 发行程序；若有此项权限，则调用发行管理员 Key 功能项，进行发行管理员 Key；

第四步：判断管理员 Key 是否发行成功：若发行成功，则写发行成功标志到数据库中保存、对数据库进行备份，并写注册表加入"GINA.dll"子项；若发行失败，则退到发行管理员 Key 之前的状态。

3.3.4.2 用户 Key 发行流程

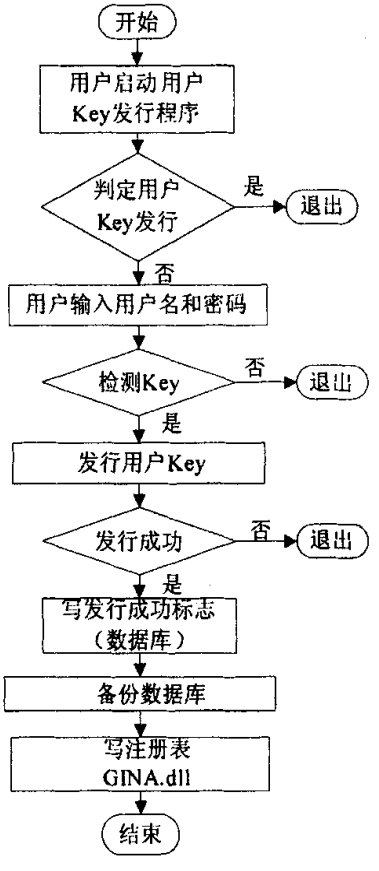

图 3.16 用户 Key 发行流程图

用户 Key 的发行流程如图 3.16 所示，具体操作是：首先，开机，安装基于 Key 的身份认证和授权系统后，插入 Key 并使用格式化程序（见安装程序套间），将其初始化，然后启动该系统到主界面下，按照以下的四个步骤进行：

第一步：启动用户 Key 发行程序；

第二步：判定用户 Key 是否发行是通过数据库中存在的纪录来判断是否已发行：若已发行，直接退出用户 Key 发行程序；若未发行用户 Key，用户在弹出的对话框中输入具有用户身份认证的用户名和密码；

第三步：检测 Key 是否是具有发行用户 Key 权限：若没有此项权限，则直接退出用户 Key 发行程序；若有此项权限，则调用发行用户 Key 功能项，进行发行用户 Key；

第四步：判断用户 Key 是否发行成功：若发行成功，则写发行成功标志到数据库中保存、对数据库进行备份，并写注册表加入“GINA.dll”子项；若发行失败，则退到发行用户 Key 之前的状态。

4 基于硬件加密设备的身份认证与授权系统的安全性分析

4.1 用户身份认证的安全

对于用户身份认证的安全是本系统中最受关注的问题。在系统中定义安全管理员为最高的控制权限，安全管理员可定义系统中不同用户的权限，并存储在硬件 Key 中，防止非法篡改。如下图 4.1 用户和操作系统用户安全身份认证截图所示，是运行系统控制中心软件发 Key 程序后的截图。

图 4.1 用户和操作系统用户安全身份认证截图

下面就身份认证的安全性进行剖析，分析常见的攻击方法对认证服务器的攻击效果。

4.1.1 网络侦听（sniffer）

认证过程中，密钥和口令字不在网络上传输，所以网络侦听攻击无效。而在密钥的在线修改过程中，新口令字使用旧的密钥加密传送，网络侦听攻击仍然无效。由于采用了单向 Hash 函数来对口令字和随机数进行处理，侦听者很难从侦听到的报文得到用户的口令字。

4.1.2 口令字猜测（password guessing）

侦听者在知道了认证算法后，可以对用户的口令字进行猜测：使用计算机猜测口令字，利用得到的报文进行验证。这种攻击办法直接有效，特别是当用户的口令

字有缺陷时，比如口令字短、使用名字做口令字、使用一个字（word）做口令字（可以使用字典攻击）等。对付这种攻击的办法是使用一个很长的口令字，并避免使用用户名字中的字，避免使用一个字（word）做口令字等。系统本身对口令字要求严格，首先口令字必须取的足够长（至少 8 字节）。用户的登记和修改口令字的程序强制用户的口令字长度。其次，离线的口令字检查工具，将弱口令字标记，强制用户限期修改。这样，用户的口令字就有足够的抗攻击强度。

4.2 密码应用的安全

软件加解密在安全性、速度等方面都存在一些不可克服的问题。系统提供的加密平台，对密钥进行保护、对整个加密过程进行控制。该系统采用一种安全的密钥生成算法，在可以控制的安全的部件上生成密钥。密钥也使用一种安全的信道来传输到存储部件上。对于密钥的访问也进行了控制，只有合法的用户才能够使用他们的可以使用的密钥。密钥的更新要在特定的权限控制下才可以进行。密钥也要根据一定的销毁规则进行销毁。对密钥的用途进行了分类，密钥的职责钥分明。

数据加密所用的密钥是和特定平台相关的，而且密钥的使用要求用户授权，因而攻击者攻击成功必须同时获得密钥文件，并且知道密钥的授权（如：PIN），并且这个密钥仅在某一特定的上才可以起作用。

4.3 数据存储安全

在计算机信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。对纯粹数据信息的安全保护，以数据库信息的保护最为典型。而对各种功能文件的保护，终端安全很重要。

身份认证和授权系统的设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略，实现了数据的存储安全。

在计算机中有很多敏感数据需要保护，而现有的计算机无法对秘密信息进行有效的安全保护。单纯的自主访问控制显然难以满足要求。身份认证和授权系统保护秘密信息的手段是用文件加密的方式加强用户信息的保护。对于要使用秘密信息的实体提供一些安全属性用于访问控制，对于不能提供该安全属性的实体将拒绝其访问。系统利用特殊的密码机制，将密钥和加密文件进行有效的隔离，使加密文件只

能在本机上用合法用户的密钥进行解密访问，在其它计算机上将无法读出此加密文件，从而实现了敏感数据的加密存储，使数据的机密性得到保障。

4.4 信息内容审计

身份认证和授权系统采用二级日志结构，分别记录主机活动的情况，实时对进出内部网络的信息进行内容审计，以防止或追查可能的泄密行为。利用日志记录可以监测关于硬件、软件、系统问题和安全方面的信息。可以通过查看这些日志，检测需要注意的活动和事件，日志还可以用来提供事件的历史记录。通过对日志信息实行有效的审计，可以充分发挥日志的事后监督作用。

本系统具有强大的审计功能，主要包括以下几个主要方面：

- 系统审计：记录了用户访问资源终端的时间，管理员可以很清晰的监测到什么时间是什么人在使用什么设备。
- 文件审计：在此功能里，记录了用户对什么文件进行的哪些操作（例如修改、新建、删除等）。
- 窗口审计：可以看到资源终端上的进程审计记录及其打开、关闭窗口的时间。保存用户各种操作的审计记录。
- 打印审计：记录了用户所打印的文件及其相关信息。

4.5 对外设的控制

身份认证和授权系统提供用户对外设进行有效的控制，在用户需要离开或者挂起系统等各种安全操作的时候，可以控制其它非法用户对计算机的非法使用，有一套行之有效的对外设的控制手段，让用户离开或者进行各种安全操作的时候可以控制外设的使用。

系统挂起功能为用户因为某种原因而暂时离开时使系统进入挂起状态。系统挂起的主要功能包括：锁定系统输入外设、系统不断检测是否有认证密码输入、验证密码进入操作界面。为了将因为突然断电等原因造成文件丢失，挂起模块会在使系统进入挂起状态前提示用户将正在编辑的文件存盘。

4.6 系统安全性评估

身份认证和授权系统的设计首先考虑的就是系统整体的安全性，从整体上构建出一个安全可信的PC平台。

首先，身份认证和授权系统采用了强制性的身份认证以确保用户的身份，同时设有分级的权限管理，只有相关人员才可以使用该系统。

其次，身份认证和授权系统能够提供数字签名和身份认证。在网络中，许多重要文件需要确定其真实性，用户可以通过系统工具对文件进行数字签名，这样就可以获得认证，确保了文件的真实性、完整性和不可否认性，同时也对文件传输者的身份进行了确认。

第三，身份认证和授权系统可以提供安全的计算环境和可靠的加解密运算。通过软件控制操作系统关闭I/O，形成一个相对封闭的运算环境，在此环境中可进行安全级别较高的特殊运算。

通过使用文件加解密和数字签名，可以防止机密信息和数据在传输过程中被非法用户截取，同时也保证了数据的完整型和不可抵赖性，从而给网络提供了一个安全可靠的内部信息平台。

第四，身份认证和授权系统中认证都采用证书机制，可以使用更可靠的PKI认证手段。

第五，身份认证和授权系统通过PKI、分级管理等技术，结合安全增强的操作系统，很大程度上解决了网络信息系统中存在的脆弱性如：操作系统的安全漏洞、用户身份的假冒、应用程序的非授权使用、损害或破坏性程序的引入以及数据库安全问题，建立了可靠安全网络互联。

最后，身份认证和授权系统整合一个庞大网络系统内相互分散的用户身份管理子系统以及整合授权用户访问信息资源权限的管理[37]。整个系统产品的设计从网络基础设施结构和用户实际应用的角度出发，提出了一个满足用户需求的完整解决方案。该系统在基于LDAP标准协议的基础上对一个企业网络内的用户身份和信息资源实现了集中与分布式的管理，使得网络系统管理人员能够很方便地对整个企事业单位内原来分散的、独立的网络用户身份管理和信息资源管理采取了集中的认证和授权访问管理，包括跨地域的内联网络和外联网络用户身份的认证和授权访问应用权限的管理[38]。参见图4.2，除此之外，系统还具备对整个网络内用户的各种行为采

取集中与分布式的审计服务功能。

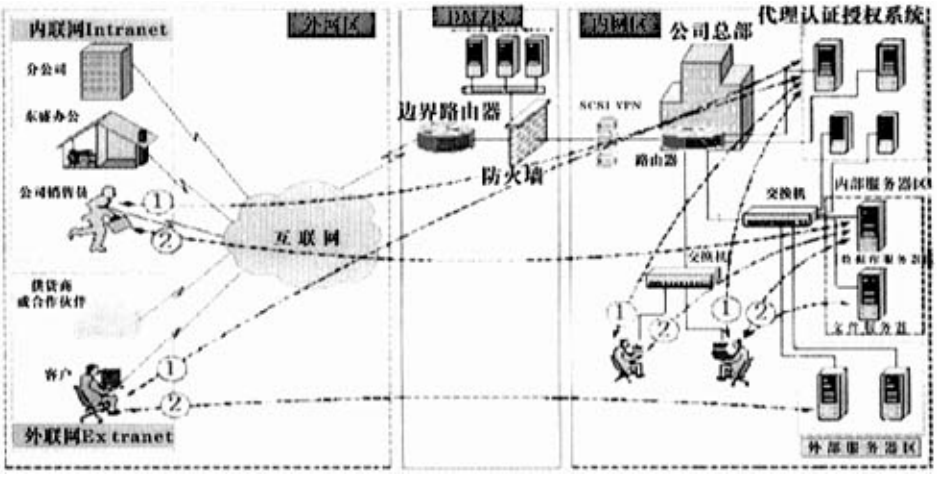

图 4.2 基于 WEB 浏览器方式的认证授权系统总体架构设计网络拓朴示意图

注：① 表示用户身份认证和授权过程；

② 表示用户授权后所获得的访问应用的过程。

5 本系统的实际应用

5.1 应用需求

SUN 阳光是在中国国家信息化建设浪潮和教育体制改革中发展起来的股份制教育培训投资和运营机构。面向全社会提供信息化咨询、培训、人才教育及输出的 IT 服务型专业机构。

置身于中国建立市场经济体制、完善现代企业制度的进程中，立志于成为一家股权清晰、管理规范、决策民主、市场导向的学习型企业。 公司视"教育强国"为己任，秉承专业精神和科学态度，诚信、严谨、笃实，以知识和智慧服务社会。在教学体系和科学管理上锐意创新，致力于为国家和行业培养大批实用型人才，推动信息化知识的普及和应用。

阳光公司的需求是：

①公司高层希望在内部 Intranet 开放一个共有资料夹来存放电子文件，使各办事人员皆能依其各自工作需要来进行阅读及修改，以降低信息传递的等待时间。

②客户资料及报价单属于公司之机密资料，若将其存放在开放性的共有资料夹中，会有被他人窃取之疑虑。

③办事人员经常为了这些急用的机密资料，因为等待时间过长而被压得喘不过气来。

④对于公司财务的管理方面，用传统纯操作系统软件的方式来实现用户身份认证，很容易被窃取及盗用，会导致财务数据的泄漏。

5.2 阳光公司身份认证与授权系统的设计与实现

5.2.1 系统软件部分设计

1、控制中心软件设计

控制中心软件设计包括用户管理模块设计、资源管理模块设计、授权管理模块设计和审计管理模块设计四个部分组成，其主要设计思想如下：

（1）用户管理模块设计

用户管理模块设计，主要是为了有效地控制用户登录方式，本系统设计了一套切实可行的身份认证方式，其设计的基本思路是：在 Windows 安全子系统中，Winlogon 调用 GINA.dll，并监视安全认证序列；而 GINA.dll 则提供一个交互式的界面为用户登录提供认证请求。由于 GINA.dll 是一个独立的动态连接库，因此，我们可以考虑采用硬件强制认证的方式来替换 GINA.dll 认证方式。Windows 系统进行安全认证时，由 Winlogon 在注册表中查找 \HKLM\Software\ Microsoft\ WindowsNT\CurrentVersion\Winlogon，如果存在 GINA.dll 键，Winlogon 将使用该 dll，反之，Winlogon 使用默认的 MSGINA.dll。为了使认证机制更完善，可以通过对 Windows 的 GINA 登录过程的二次开发实现具有安全防御功能的认证体系。

系统身份认证设计方案如图 5.1 所示，系统操作平台为 Windows 2000，编程语言采用可视化编程语言 VC++，后台数据库采用 SQL Server 2000。基于 Key 的 GINA 登录系统包括一个后台数据库和一个文件存储箱。以 Key 为硬件加密设备利用 GINA 登录技术来完成安全认证的方案其优点是既可以充分利用 GINA.dll 对安全认证的交互式认证界面直接构建出与用户交互的认证机制，又可以直接利用其与注册表项的键值紧密结合的特点，以满足不同系统对登录认证体系的需要。

下面，就将该系统的功能模块组成和各个模块之间的联系来加以说明：

1、系统身份认证的组成

本 GINA 登录共有 15 个模块组成,它们是：

1) 管理员 Key 发行程序 UserKey.exe
2) 控制面板增加图标 CPL.cpl
3) 控制中心 ControlCenter.exe
4) GINA 登录程序 GINA.dll
5) 文件保密柜设置程序 SECBOX.dll
6) Shell 程序 Shellext.dll
7) 文件保密柜驱动程序 Filedisk.sys
8) 外部设备控制 DeviceLock.dll
9) 文件操作设置 FileAction.dll
10) 网络资源配置 SPI.dll
11) 系统托盘程序 Ico.exe
12) 安全模式解决 CheckPin.exe

13) 限制卸载程序　　Unwise.exe /Unwise32.exe

14) Key 动态库　　Key.dll

15) 数据库操作　　FileDB.dll

2、各功能模块之间的联系（如图 5.1 所示）

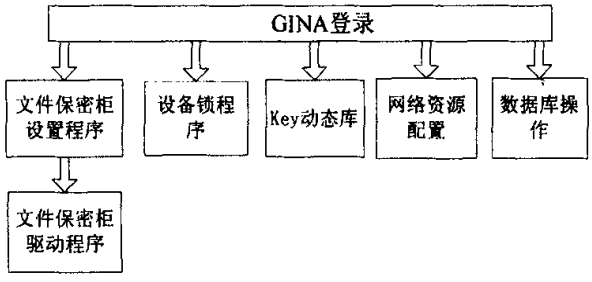

图 5.1 身份认证设计方案示意图

如图 5.1 所示是身份认证设计方案示意图，整个系统是以 GINA 登录作为一个平台，然后在其上做二次开发，运用动态连接库技术，分别将文件保密柜设置程序（SECBOX.dll）、设备锁定程序（Devicelock.dll）、Key 动态库（Key.dll）、网络资源配置（SPI.dll）、数据库文件操作（FileDB.dll）运用到 GINA 登录系统中来，极大的加强了 Windows 登录操作的安全性。另外，系统中用来存放保密文件的文件保密柜，还为它专门写了 Filedisk.sys 的驱动程序以保障文件保密柜的正常使用。

以下是外部设备控制程序源码：

```
// DeviceChange.cpp : implementation file
#include "stdafx.h"
#include "DeviceLock.h"
#include "DeviceChange.h"
#include <Dbt.h>
#ifdef _DEBUG
#define new DEBUG_NEW
#undef THIS_FILE
static char THIS_FILE[] = __FILE__;
#endif
const DWORD LOCK_REMOVE_DISK = 0x00000001;
const DWORD LOCK_REMOVE_DEVICE = 0x00000002;
```

```
// CDeviceChange dialog
CDeviceChange::CDeviceChange(CWnd* pParent /*=NULL*/)
    : CDialog(CDeviceChange::IDD, pParent)
{
    //{{AFX_DATA_INIT(CDeviceChange)
    m_dwLockFlag = 0;
    //}}AFX_DATA_INIT
}

void CDeviceChange::DoDataExchange(CDataExchange* pDX)
{
    CDialog::DoDataExchange(pDX);
    //{{AFX_DATA_MAP(CDeviceChange)
        // NOTE: the ClassWizard will add DDX and DDV calls here
    //}}AFX_DATA_MAP
}

BEGIN_MESSAGE_MAP(CDeviceChange, CDialog)
    //{{AFX_MSG_MAP(CDeviceChange)
    ON_WM_NCPAINT()
    ON_WM_CLOSE()
    ON_WM_CREATE()
    //}}AFX_MSG_MAP
    ON_WM_DEVICECHANGE()
END_MESSAGE_MAP()

// CDeviceChange message handlers
void CDeviceChange::OnCancel()
{
}
```

```
void CDeviceChange::OnOK()
{
}
void CDeviceChange::OnClose()
{
}
int CDeviceChange::OnCreate(LPCREATESTRUCT lpCreateStruct)
{
    if (CDialog::OnCreate(lpCreateStruct) == -1)
        return -1;
    ShowWindow(SW_HIDE);
    return 0;
}
void CDeviceChange::OnNcPaint()
{
    static int i = 2;
    if(i > 0)
    {
        i = 0;
        ShowWindow(SW_HIDE);
    }
    else
    {
        CDialog::OnNcPaint();
    }
}
BOOL CDeviceChange::OnDeviceChange(UINT nEventType, DWORD dwData)
{
    //检查移动设备
    switch (nEventType)
```

```
    {
    case DBT_DEVICEARRIVAL:
    case DBT_DEVICEREMOVECOMPLETE:
    case DBT_DEVNODES_CHANGED:
        if(m_dwLockFlag & LOCK_REMOVE_DISK)
        {
            SearchRemoveDisk();
        }
        if(m_dwLockFlag & LOCK_REMOVE_DEVICE)
        {
            SearchRemoveDevice();
        }
        LockRemoveDevices();
        break;
    default:
        break;
    }
    return TRUE;
}
void CDeviceChange::SearchRemoveDisk()
{   //搜索移动磁盘
    return;
}
void CDeviceChange::SearchRemoveDevice()
{   //搜索移动设备
    return;
}
void CDeviceChange::LockRemoveDevices()
{   //锁定移动设备
    return;
}
```

3、安全性考虑

1）三级用户体系

①安全管理员：超级用户，持有母 Key，对系统操作的权限为：安装计算机安全加固系统，操作本系统 Key 的发放管理，进行用户级别定义、对所有用户的外部设备操作权限进行授权操作和管理、使用私人文件保密箱、可以进行所有的 I/O 操作。

②安全审计员：审计用户，持有安全审计用户 Key，可以操作本系统的安全审计管理程序、使用私人文件保密箱、可以对授权的 I/O 进行操作。

③普通用户：普通用户，持有用户 Key，可以使用私人文件保密箱、对授权的 I/O 进行操作。

各用户的权限信息被存储在智能电子钥匙 Key 和安全加固软件包中，除安全管理员外，无法更改。使用单位可以严格按照分离原则建立各级用户，同时也可按照最小原则实现用户划分。如安全管理员可以兼任安全审计员。

2）用户身份认证

GINA 登录系统的身份认证是在原 Windows 环境下身份认证的基础上引入了智能电子钥匙 Key 在身份认证环节中的应用。本系统将用户掌握的用户密码与 Key 中的卡 ID、用户密码、卡内外部认证密钥、系统中的认证文件信息绑定在一起。合法用户登录系统时，必须首先将其所拥有的 Key 插入计算机的 USB 接口上，仅当输入的 PIN 码与 Key 中的密码一致，才能通过该身份认证。单独获取用户密码或 Key 都无法登录系统，伪造的电子钥匙无法通过系统的内外部认证。

3）安全审计

①系统提供管理工具供安全审计员配置审计策略和生成审计报告。安全审计员可根据需要将私有文件夹以外的目录或文件（程序）加入到审计配置中去。安全日志（审计文件）的记录包括 Key-ID(即 Key 的序列号)、操作类型、操作对象、操作结果、操作时间等。

②安全日志以密文的形式存储在具有安全审计权限的安全审计员的私有保密文件柜中，确保了审计文件的安全性。明文只能存在于系统内存中，明文的恢复只能由安全审计员来实现，安全管理员操作安全日志只可读，不可写。

③安全审计员可以将受控资源的使用情况列入须审计内容，便于发现“可疑”情况，及时追查安全事故责任。

（2）资源管理模块设计

资源管理模块相当于一个后台的数据库，它是维持整个系统正常运行的重要环

节，此数据库中存放了用户所有要用到的信息，其中包括：用户基本信息、审计信息、系统资源信息和授权相关信息。按照具体的数据库资源表将以上内容分别制作了用户基本属性表（user_basic_info）、用户扩展信息表（user_extend_info）、审计信息表（audit_info）、部门分组表（user_Group）、部门信息表（GroupInfo）、终端信息表（ComputerInfo）、终端资源信息表（Computer_Source_Info）、用户授权表（UserGrant）、安全信息表（UserSafeInfo）、用户授权资源表（user_grant_src）共十张表，如下表 3.1 至表 3.10 所示。

表 5.1 用户基本属性（user_basic_info）

字段名	说明	类型	长度	主键	NULL	备注
user_id	用户标识	Int unsigned	32 位			系统
user_name	姓名	Char	50			用户
user_sex	性别	Char	1			用户
user_age	出生	Datetime	8			用户
user_ nation	民族	Char	10			用户
User_stature	身高	Tinyint unsigned	1			用户
User_avoirdupois	体重	Tinyint unsigned	1			用户
User_native	籍贯	Char	50			用户

表 5.2 用户扩展信息（user_extend_info）

字段名	说明	类型	长度	主键	NULL	备注
user_id	用户标识	Int unsigned	32 位			系统
user_idcard_num	身份证号	Char	30			用户
user_knowledge	学历	Char	30			用户
user_ dwelling_place	家庭住址	Char	50			用户
user_title	职务	Char	50			用户
user_phone_code	办公室电话	Char	20			用户
user_fax	传真	char	20			用户
user_ home_phone	宅电	Char	20			用户
User_mobile	移动电话	char	20			用户
User_post_code	邮编	char	10			用户
User_home_post_code	家邮编	Char	10			用户
User_email	邮箱	char	50			用户
User_polity	政治面貌	Char	10			用户
User_school	毕业学校	Char	50			用户

表 5.3 审计信息（audit_info）

字段名	说明	类型	长度	主键	NULL	备注
CAuditTime	终端审计时间	datetime	8			系统
SAuditTime	服务器审计时间	datetime	8			系统
KeyID	Key_id	Char	30			系统
Netmac	网卡编号	Char	18			系统
Auditclass	审计类别	Int unsigned	32 位			系统
AuditInfo	审计信息	char	600			系统

表 5.4 分组表（user_Group）

字段名	说明	类型	长度	主键	NULL	备注
Group_ID	部门标号	Int unsigned	32 位	Y	N	
Group_RootID	根 ID	Int unsigned	32 位			
Group_ParentID	父部门 ID	Int unsigned	32 位			
Group_Depth	部门深度	Int unsigned	32 位			
Group_Name	部门名	char	50			

表 5.5 部门信息表（GroupInfo）

字段名	说明	类型	长度	主键	NULL	备注
Group_ID	部门标号	Int unsigned	32 位	Y	N	
FullName	部门全名	char	256			
Phone1	办公司电话 1	char	20			
Phone2	办公司电话 2	char	20			
Phone3	办公司电话 3	char	20			
Fax	传真	char	20			
E_mail	电子邮件	char	50			
Address	办公室地址	char	256			
PostCode	邮政编码	char	10			

表 5.6 终端信息表（ComputerInfo）

字段名	说明	类型	长度	主键	NULL	备注
PcID	终端 ID	Int unsigned	32 位	Y	N	
PcName	客户端名称	char	50			
IP	客户端 IP	char	50			
NetMac	网卡 MAC	char	18			
Current_online	在线状态	char	1			
Group_ID	部门标号	Int unsigned	32 位			

表 5.7 终端资源信息表（Computer_Source_Info）

字段名	说明	类型	长度	主键	NULL	备注
PcID	终端 ID	Int unsigned	32 位	Y	N	
SrcID	资源 ID	Int unsigned	32 位			
Src_RootID	根资源 ID	Int unsigned	32 位			
Src_ParentID	父资源 ID	Int unsigned	32 位			
Src_Depth	深度	Int unsigned	32 位			
Src_Name	资源名	char	255			

表 5.8 用户授权表（UserGrant）

字段名	说明	类型	长度	主键	NULL	备注
user_id	用户 ID	Int unsigned	32 位	Y	N	
KeyID	KeyID	char	30			
NetMac	网卡 MAC	char	18			
StartTime	登录有效期限	DATETIME	8 字节			开始时间
EndTime	登录有效期限	DATETIME	8 字节			结束时间
StartPc	每天开机时间	TIME	3 字节			
ShutoffPc	每天关机时间	TIME	3 字节			
LogonRight	登录权限	char	20			

表 5.9 安全信息表（UserSafeInfo）

字段名	说明	类型	长度	主键	NULL	备注
user_id	用户 ID	Int unsigned	32 位	Y	N	
KeyID	KeyID	char	30			
KeyRelease	Key 发放标志	char	1			
KeyState	Key 的状态	Int unsigned	32 位			有效失效
NetMac	网卡 MAC	char	18			默认登录
Key_grant	Key 权限	Int unsigned	32 位			管理员，审计员

表 5.10 用户授权资源表（user_grant_src）

字段名	说明	类型	长度	主键	NULL	备注
user_id	用户 ID	Int unsigned	32 位	Y	N	
Src_Name	资源名	char	255			

（3）授权管理模块设计

1)、单机授权

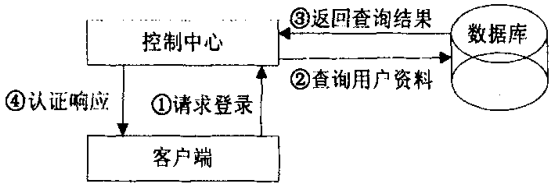

图 5.2 授权管理模块设计图

如图 5.2 所示，授权管理模块的设计方法是通过控制中心和客户端这两个独立的软件之间建立一定的请求和响应关系，从而达到系统授权的管理功能，其中：

第一步：客户端发出“①请求登录”给控制中心；

第二步：是由控制中心到数据库中查询用户的资料，验证用户的合法身份；

第三步：是数据库通过查找，确定一个返回结果给控制中心；

第四步：就是控制中心根据返回的结果来判断，是否分配该用户相应的权限，即授权用户使用资源的范围。

2)、网络授权

参见图 2.3 所示，授权和认证服务系统的构成和工作流程图。

（4）审计管理模块设计

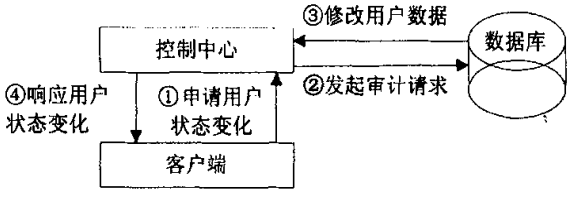

图 5.3 审计管理模块设计图

如图 5.3 所示，审计管理模块的设计方法是与授权管理模块一样，是通过控制中心和客户端这两个独立的软件之间建立一定的请求和响应关系，从而达到系统审计的管理功能，其中：

第一步：客户端发出"①申请用户状态变化"给控制中心；（即当用户信息发生改变时，即用户状态发生变化时，用户必须提交更新的内容给控制中心审计，否则，更新的内容不能生效。）

第二步：是由控制中心向数据库发起审计的请求，请求数据库验证用户的合法信息的变化情况；

第三步：是数据库通过查找并修改相应的用户设置，确定一个返回结果给控制中心；

第四步：就是控制中心最终把审计的信息返回给用户，用户得到申请的状态变化是否生效的结果。

2、客户端软件设计

客户端软件设计就包括文件保密柜模块设计和文件加解密模块设计两部分组成，其主要设计思想如下：

（1）文件保密柜模块设计

如图 5.1 所示，身份认证设计方案示意图中有关 GINA 登录时所要调用的模块就包括"文件保密柜模块"，此模块的作用是生成一个虚拟的磁盘空间，大小可以调节，一般缺省值定为 2G。这个磁盘空间是虚拟的，是在 GINA 登录时，系统验证用户合法权限后，自动加载的一个磁盘区间。系统为每个合法用户创建一个私有文件保密柜，提供方便快捷的对文件/文件夹加解密功能，用户在存储和读取私有文件保密柜的文件时，系统自动进行加解密。文件的加解密过程对用户透明，加密后的文件内

容以密文形式存放。它就像普通的本地磁盘一样在“我的电脑”中是可见的，可以随意的打开存放文件，非常方便。我们之所以把它叫“文件保密柜”，就是相当把它当成一个专门存放文件的文件柜，一般的用户是无法看到这个“文件保密柜”中的文件的。

那么，为了达到这样的目的，我们对要进行保密操作的外来文件在拖动到“文件保密柜”中去的同时，就对此文件进行加密。一般用户的权限是无法看到文件的内容，因为只有对“文件保密柜”具有操作权限（由系统管理员来分配，默认情况下，一般是系统管理员）的用户才可对文件进行解密，观看文件内容。

“文件保密柜”除了需要一个“文件保密柜的驱动程序”（见图 5.1 所示）以外，其具体的设计中还应包括以下几个内容来确保以上功能的实现：

创建一个新文件保密柜子函数；

- 删除文件保密柜子函数；
- 检查磁盘空间子函数；
- 得到虚拟磁盘信息子函数；
- 虚拟磁盘格式化子函数。

（2）文件加解密模块设计

上面已经提到，在“文件保密柜”中存放的文件都得到了文件加解密的保护，那么文件加解密模块与文件保密柜模块之间是相互关联的两个模块。对于文件如何加密，采用各种加密方法，此系统中将利用 Single DES/Triple DES 算法来实现，此算法包括加密算法和解密算法。这里对 Single DES/Triple DES 算法的推导过程就不再复述了，其具体实现过程见“3.3.3.1 数据加密的模式（Single DES 或 Triple DES）”。

5.2.2 系统硬件部分设计

（1）功能描述

1、USB Key 的功能，具体包括如下部分：

- 标识 U 盘的唯一 ID 号，该 ID 号为硬件固化；
- 一段独立于 U 盘的存储空间（简称 Key 空间），Key 空间不随格式化 U 盘的操作而消失或是被覆盖；
- 对 Key 空间进行读写操作，需要应用程序与 U 盘双向验证机制；
- 基本的密码算法，如 DES 和 3DES；

2、U 盘的增强功能，具体包括如下两部分功能：

- 对整个 U 盘（简称 U 盘空间）的读写，也需要双向验证机制；
- 可以对 U 盘的分区或是某些扇区加密；
- Key 空间与 U 盘空间作为两块独立的空间，能否动态调整 Key 空间与 U 盘空间的大小。

（2）加密算法

Key 是支持 Single DES、Triple DES、AES 算法的。

在建立 DES 密钥时，若密钥长度为 8 字节则运行时使用 Single DES 算法，若密钥长度为 16 字节则运算时使用 Triple DES 算法。在建立 AES 密钥时，要求密钥长度必须为 16 字节。运算时使用加密还是解密算法完全由密钥类型决定，如：用于外部认证的密钥不可用于内部认证[49]。

Key 在使用 DES 算法时，若数据长度大于 8 字节时使用 CBC（加密数据块）模式，若数据长度不是 8 的倍数时在计算过程重自动在数据后补 80 00...00 使其为 8 的倍数。例如数据为 00 11 22 33 44 55 66 77 88，由于数据长度不是 8 的倍数，那么在计算过程中自动将数据改写成 00 11 22 33 44 55 66 77 88 80 00 00 00 00 00 00 后再进行计算[50]。

Key 在使用 AES 算法时，若数据长度大于 16 字节时使用 CBC 模式，若数据长度不是 16 的倍数时自动在数据后补 80 00...00 使其为 16 的倍数。例如数据为 00 11 22 33 44 55 66 77 88，由于数据长度不是 8 的倍数，那么在计算过程中自动将数据改写成 00 11 22 33 44 55 66 77 88 80 00 00 00 00 00 00 后再进行计算。

Key 用于生成子密钥/过程密钥。它使用 SAM 卡上的主密钥对数据生成子密钥或过程密钥存储在 RAM 中以供后续命令使用。如果使用的不是 SAM 卡的主密钥，则返回 9403（密钥不存在）[51]。

用主密钥对输入数据的左 8 个字节加密生成子密钥的左半部分；然后用主密钥对输入数据的左 8 个字节求反后的结果加密后生成子密钥的右半部分，其中使用的加密算法是主密钥算法标识中所指定的算法，生成的子密钥的算法标识沿用。如果是要生成过程密钥，那么就是用生成的子密钥对输入数据的右 8 个字节加密（使用 Triple DES 算法），其结果即为过程密钥，过程密钥的算法标识符沿用子密钥的算法标识符（即为主密钥的算法标识符）。主密钥的算法标志符为 0：使用 Single DES 算法；为 1：使用 Triple DES 算法[52]。

5.3 应用与分析

在阳光公司共部署了 30 套身份认证与授权系统软件产品，分别是在财务部、市场部、技术开发部、总工程师办公室等 6 个部门。其重点解决如下问题：

①利用本系统的文件加密功能对业务部的机密文件进行加密；

②在需要使用公司机密文件时，通过系统管理员授权给公司内部的其它工作伙伴使用，唯有被授权者的 Key 才有权限来使用档案；

③身份认证方式的改变，主要是 USB－Key 身份认证技术，采用软硬件相结合、一次一密的强双因子认证模式。USB－Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB－Key 内置的密码算法实现对用户身份的认证。基于 USB－Key 身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式，二是基于 PKI 体系的认证模式。

每个 USB－Key 硬件都具有用户 PIN 码，以实现双因子认证功能。USB－Key 内置单向散列算法（MD5），预先在 USB－Key 和服务器中存储一个证明用户身份的密钥，当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数并通过网络传输给客户端（此为冲击）。客户端将收到的随机数提供给插在客户端上的 USB－Key，由 USB－Key 使用该随机数与存储在 USB－Key 中的密钥进行带密钥的单向散列运算（HMAC-MD5）并得到一个结果作为认证证据传送给服务器（此为响应）。与此同时，服务器使用该随机数与存储在服务器数据库中的该客户密钥进行 HMAC-MD5 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户。

④各部门员工可以放心地将机密文件放置在各自的文件保密柜中，完全杜绝非文件授权者来使用或阅读。

从去年 9 月份使用本系统开始，通过半年多的实际应用，阳光公司从应用之前的文件管理混乱、人员流失严重的恶性循环的阴影中成功的走出来，增强公司内部系统平台的安全策略，通过集中的控制中心等安全策略的应用，保证公司内部系统平台的安全性（见图 5.4 人员流动率及系统的稳定性变化趋势）。根据公司管理部门统计，在使用此安全身份认证产品之后公司的工作效率大大提高。原来需要层层审批才能查阅的文件，平均需要 2－3 天时间才能得到。现在只要有授权，马上就可以查阅。管理成本降低，效果却增强了，无文件丢失或泄漏情况出现（见表 5.11 使用

安全身份认证产品前后情况对比)。阳光公司高层管理决定，将继续在全公司使用基于USB－Key的身份认证安全产品。

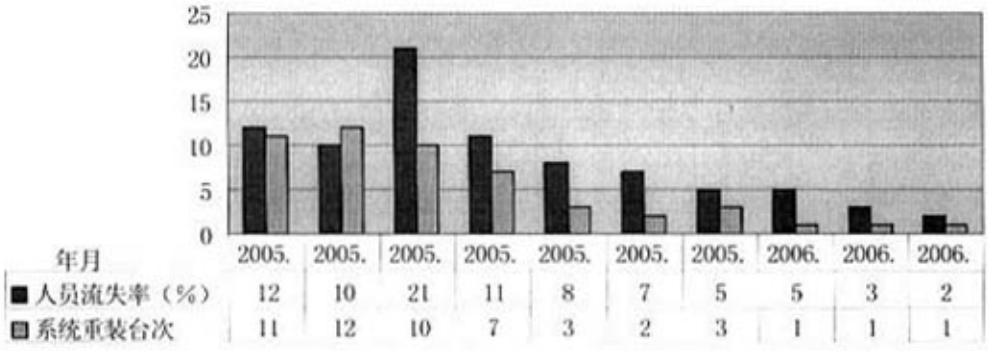

图 5.4 人员流动率及系统的稳定性变化趋势

表 5.11 使用安全身份认证产品前后情况对比

对比项目	使用安全身份认证产品之前	使用安全身份认证产品之后
查阅保密文件的等待时间	2－3 天	有授权，5 分钟之内
文件管理人员	3 人	1 人
文件管理情况	丢失现象时有发生，有泄密现象	没有丢失，不会泄密

实践证明,利用GINA登录技术可以较好地解决系统登录时的安全认证问题，并且还可以针对计算机系统的安全性，利用GINA登录技术与硬件加密锁KEY的结合进行二次开发。这种软件和硬件、内部与外部的双重认证方式不但可以提高Windows操作系统的安全性,而且该项技术还具有较大的灵活性、可扩展性和兼容性等诸多优点。

实际使用过程中，上述技术也存在一些问题：一是进行系统安全加密的速度较慢，工作效率相对低下；二是所支持的操作系统有限，对于Linux系统等操作系统暂时还不能使用GINA登录方式；三是硬件加密锁KEY是与PC机相分离的独立硬件设备,容易遗失,不易管理。随着应用的不断深入，基于硬件加密锁的GINA登录技术将会得到进一步的完善。

6 总 结

综上所述，利用 GINA 登录技术可以较好地解决系统登录时的安全认证问题，并且还可以针对计算机系统的安全性，利用 GINA 登录技术与硬件加密锁 Key 的结合进行二次开发。这种软件和硬件、内部与外部的双重认证方式不但可以提高 Windows 操作系统的安全性,而且该项技术还具有较大的灵活性、可扩展性和兼容性等诸多优点。

论文在分析和比较现有的软硬件的网络安全产品中存在的安全漏洞基础之上，详细论述了基于 Key 的身份认证和授权系统的设计思想及其实现方法。现将对该系统所做研究及相关实践工作总结如下：

1、在继承了当前硬件加密锁 Key 和身份认证及授权软件产品的所有功能的基础上，提出并实现了基于硬件加密锁 Key 的身份认证和授权系统的解决方案。该系统克服了以往由纯软件和纯硬件产品所不具备的更加完善的功能、更加强大的管理机制和更加稳定的系统性能等特点；

2、软件方面：

(1)利用 Winlogon（Windows Logon Process）调用 GINA（Graphical Identification and Authentication）动态连接库监视安全认证序列来实现用户的身份认证功能;

(2)全面地分析了客户/服务器模式和控制中心技术，并以动态链接库技术为基础，实现了稳定、灵活的 Windows 软件开发环境，以此作为基于硬件加密锁 Key 的身份认证和授权实现的软件技术基础;

(3)采用 Single DES 或 Triple DES 完善的文件加解密技术实现对文件及数据的加解密功能;

(4)采用虚拟磁盘区间存放加密文件,并且采取权限控制,防止非法用户浏览和使用保密文件。

3、硬件方面：利用现在流行的加密技术集成芯片为基础制作的智能电子钥匙 Key,与其现行的 PC 机的 USB 接口相连，和上述的安全软件包形成一套硬软件相结合的系统，在 Windows 操作系统下实现了具有安全身份认证、授权、审计等多项功能；

4、所开发的身份认证和授权系统工作良好，对新型的信息安全产品的开发和研制工作有一定的借鉴意义。

制工作有一定的借鉴意义。

致 谢

一年多来，我在导师陈海清教授的指导下圆满地完成了各项学习和研究任务。导师严谨求实的治学态度使我受益匪浅；宽阔的育人胸怀更使我终生难忘。导师殷切的关怀令我感动不已，他不但教我们如何做事，更重要的是教我如何做人。研究生两年的时间，导师给了我们大量实践的机会，在工作中，我们学到了书本上学不到的知识与经验，丰富了自己的专业知识，积累了大量宝贵的工作经验，做到了真正意义上的理论与实践相结合。我在此向导师致以最崇高的敬意和最衷心的感谢！

同时，我还十分感谢光电工程学院的老师们和同学们。在我研究生阶段的工作实践中，各位老师给予了我不少的指导与帮助。我不仅从老师们那里学到了专业技能方面的知识，老师们耐心细致的工作态度，认真负责的工作作风也是我永远的学习榜样。在此，我也要向各位老师们致以诚挚的感谢！

最后，衷心地感谢我的家人多年来对我的关心、理解和支持。

谨以此文献给所有曾给予我关心、爱护和帮助的朋友们！

参考文献

[1] Zhang song and Yan baoping. Network management based on mobile agent architechure and implementation,Journal of computer research and development, Vol 36,No.8,1999,1007-1011

[2] Kotz D Gray R,AGENT TCL:Targeting the Needs of Mobile Computer,IEEE Internet Computing,July,August 1997:58-67

[3] R.Oppliger,Security issues related to mobile code and agent-based systems，IEEE computer communications,1999(22):1165-1170

[4] Midori Asaka Ipa. The Implementation of IDA: An Intrusion Detection Agent System ASAKA IPA asaka@ipa.go.jp asaka at ipa.go&#x2ejp Atsushi Taguchi IPA a-tag@ipa.go.jp a-tag at ipa.go.jp Shigeki

[5] Midori Asaka, Takefumi Onabura. Tadashi Inoue Information-technololy，Remote Attack Detection Method in IDA: MLSI-Based Intrusion Detection using Discriminant Analysis

[6] Peter Mell, Mark McLarnon. Mobie Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems，National Institute of Standards and Technology，100 Bureau Dr. Stop 8930，Gaithersburg, MD 20899，1999.8.10

[7] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez,David Isaco, Eugene Spaord, Diego Zamboniy,An Architecture for Intrusion Detection using Autonomous Agents, Center for Education and Research in Information Assurance and Security, Purdue UniversityCERIAS Technical Report 1998.5

[8] Howes，T.，Kille，S.，Yeong，W.，和 C. Robbins，“轻目录访问协议”，RFC 1488，Michigan 大学，ISODE 协会，Performance Systems International，NeXor Ltd.，1993.7

[9] Bruce Schneier. 网络信息安全的真相. 机械工业出版社，2001.9

[10] Zhang song and Yan baoping, Network management based on mobile agent architechure and implementation, Journal of computer research and development, Vol 36,No.8, 1999,1007-1011

[11] Kotz D Gray R, AGENT TCL: Targeting the Needs of Mobile Computer, IEEE Internet Computing, July, Aug 1997:58-67

[12] R.Oppliger,Security issues related to mobile code and agent-based systems，IEEE computer communications,1999(22):1165-1170

[13] Midori Asaka Ipa，The Implementation of IDA: An Intrusion Detection Agent System, ASAKA IPA asaka, Atsushi Taguchi IPA Shigeki

[14] Midori Asaka, Takefumi Onabura, Tadashi Inoue Information-technololy. Remote Attack Detection Method in IDA: MLSI-Based Intrusion Detection using Discriminant Analysis

[15] Peter Mell, Mark McLarnon，Mobie Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems，National Institute of Standards and Technology，100 Bureau Dr. Stop 8930，Gaithersburg, MD 20899，1999.8

[16] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isaco. Eugene Spaord, Diego Zamboniy. An Architecture for Intrusion Detection using Autonomous Agents, Center for Education and Research in Information Assurance and Security, Purdue UniversityCERIAS Technical Report 1998.5

[17] Diego Zamboni, Mahesh Tripunitara, AAFID2 Users Guide. COAST Laboratory Purdue University, 1999.9

[18] Eugene Spafford, Diego Zamboni,A framework and prototype for a distributed intrusion detection system,COAST Laboratory Purdue University, 1998.6

[19] William M. Farmer, Joshua D. Guttman, and Vipin Swarup. Security for mobile agents: Issues and requirements, In Proceedings of the 19th National Information Systems Security Conference, volume 2, pages 591-597. National Institute of Standards and Technology, 1996.10

[20] Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levitt. Network intrusion detection. IEEE Network, 8(3):26, 1994.5

[21] K Thomson,G J Miller，R Wilder. Wide-area traffic patterns and characteristics[J]. IEEE,Network,1997.12

[22] Kerberos 认证和授权系统. S.P. Miller，B.C. Neuman，J.I. Schiller，J.H. Saltzer; MIT Project Athena 文档 E.2.1 节，1987.12

[23] Rose，M.“目录辅助服务”RFC 1202，Performance Systems International，Inc.，1991.2

[24] Howes，T.，Smith，M，和 B.Beecher.“DIXIE 协议规范”，RFC 1249，Michigan 大学，1991.8

[25] InternationalTechnicalSupportOrganization“LDAP Implementation Cookbook”，1999.6

[26] http://www.westone.com.cn

[27] 张焕国等.计算机安全保密，机械工业出版社，1997

[28] 陈爱民等.计算机的安全与保密，电子工业出版社，1992

[29] 严伟等译.Internet 网络安全专业参考手册，机械工业出版社，1998

[30] 卢开澄.计算机密码学，清华大学出版社，1998

[31] 国家信息安全基础设施研究中心标准化工作组，RFC1777 轻目录访问协议—LDAP

[32] 汤子赢，哲风屏，汤小丹.计算机操作系统，西安电子科技大学出版社，1999

[33] 何炎祥，宋文欣，彭锋等.高级操作系统，科学出版社，1999.4

[34] Stephen Northcutt，网络入侵检测分析员手册 人民邮电出版社，2000.10

[35] 唐正军.黑客入侵防护系统源代码分析，机械工业出版社，2002.3

[36] 蒋建春,冯登国.网络入侵检测原理与技术，国防工业出版社，2001.7

[37] 威胁继续存在---美国计算机安全协会公布,计算机犯罪及安全调查结果:信息网络安全 ,2002（9）:11

[38] 网络隐患扫描系统的设计. 信息网络安全 ,2002（9）:30

[39] 国外计算机犯罪的现状. 信息网络安全,2002（10）:21

[40] SSL 协议工作过程及其应用. 网络安全技术与应用,2004(46):12

[41] 杜滨 杨寿保 ,基于入侵检测的立体防御系统体系结构研究,计算机工程与应用 2002(20)

[42] 冯东雷,叶奇等. 多层交换技术在宽带防火墙系统中的应用，计算机工程与应用 2002(18)

[43] 吴承荣，多层次、全方位、分布式的网络安全解决方案. 中国信息协会信息安全专业委员会年会文集，2002.9

[44] 万燕. 一个安全移动代理系统的设计与实现，上海交通大学博士论文，2001.6

[45] 文传洪. 移动代理在入侵检测中的应用研究，电子科技大学硕士论文，2001.1

[46] Bruce Schneier. 应用密码学－协议、算法与 C 源程序，机械工业出版社，2001

[47] Bruce Schneier. 网络信息安全的真相，机械工业出版社，2001.9

[48] Charles P. Pfleeger, Shair Lawrence Pfleeger, 信息安全原理与应用（第三版），电子工业出版社，2004.7

[49] James Stanger ，CIW：安全专家全息教程，电子工业出版社，2003.1

[50] Wendy Boggs， Michael Boggs. UML with Rational Rose 从入门到精通. 电子工业出版社，2000.3

[51] 张涣国，覃中平，王丽娜. 信息和通信安全－CCICS'2003，科学出版社，2004.3

[52] Sriranga Veeraraghavan. 精通 shell 编程（第三版），人民邮电出版社，2005.2

[53] James Stanger. CIW:安全专家全息教程. 电子工业出版社，2005.3