# 基于PXE技术的动态分布式无盘网络存储安全研究

黄冠利[1] 金 岩[2] 勾传静[3] 王 萍[1]
(北京电子科技职业学院 北京 100029)[1] (中国人民解放军91202部队 葫芦岛 125004)[2]
(北京航空航天大学 北京 100191)[3]

**摘 要** PXE(Pre-boot Execution Environment)技术因其强大的兼容性与易维护性在互联网的发展中作用越来越高,但是将PXE技术用于提高数据安全的研究却相对不够。在分析当前网络数据安全的现状及特点基础上,提出了将无盘网络及动态分布式数据存储技术应用于已有PXE网络系统中的方案,并对其主要构造进行了设计与研究。新的系统降低了数据泄漏风险,提高了网络数据的安全性及可靠性。该方案经济可行,大大降低了网络安全维护成本,并随着成果的普及与应用,将会带来更大的经济效益。

**关键词** PXE技术,人为因素,无盘网络,安全信息管理系统
**中图法分类号** TP393 **文献标识码** A

## Research on Storage Security of Dynamic Distributed Diskless Network Based on PXE

HUANG Guan-li[1] JIN Yan[2] GOU Chuan-jing[3] WANG Ping[1]
(Beijing Vocational College of Electronic Science, Beijing 100029, China)[1]
(No. 91202 Unit of the CPLA, Huludao 125004, China)[2] (Beihang University, Beijing 100191, China)[3]

**Abstract** PXE(Pre-boot Execution Environment) tech. has played great roles for the powerful compatibility and ease for maintenance. Internet requirement for data safety is more and more important while PXE methods is lackly. The applications of diskless tech and dynamic distributed security system in data storage were analyzed. Designing and studing the PXE tech. , reduced the risk of letting out and dependability of the network data under the strict data management. The function may bring huge economic benefit with the popularization of the applications and low maintenance cost.

**Keywords** PXE(Pre-boot Execution Environment), Anthropic factor, Diskless network, SIMS(Secure Information Management System)

## 1 引言

安全问题中80%是关于如何安全存储企业中的敏感信息,如银行用户信息、信用记录、教育机构教学记录、商业客户信息、消费记录、税务申报信息等,这些信息可以通过现有的安全协议在网络上流通。但是作为后端的存储,是否安全成为企业关心的关键问题。全球化竞争的环境使得国内企业信息化的比率在不断提升,经济发达地区的众多企业和西部地区的部分企业在移动办公的需求,以及对内部信息便捷安全的存储及准确应用的需求也在日益高涨。

### 1.1 PXE数据安全核心问题分析

PXE数据安全从本质上来讲就是网络上的信息安全。具体来讲,是指网络系统的硬件、软件及其系统中的数据受到保护,不因为偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。从广义来说,凡是涉及到PXE网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是数据安全所要研究的领域。由于网络联结形式的多样性、终端分布的不均匀性以及开放性、互联性等,致使PXE计算机网络容易受到黑客、恶意软件、病毒、木马等攻击,而计算机网络中的核心数据安全便成为一个至关重要的问题。如何加强网络数据存储、传输、管理、备份的安全性,已成为近年来人们关注的焦点。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。尽管目前已经有了很多关于加强网络数据安全的方式方法,但总会存在这样或那样的漏洞。虽然企业依赖于数据库安全技术,但数据库不能存储所有资料数据,有很多资料数据采用数据库存储是没有必要并且严重影响数据存储效率的。因而,安全的数据(文件)存储方案必将成为未来的热门技术。根据网络存储市场的发展趋势与技术进步,网络安全存储势必代替传统网络存储市场。本研究基于PXE无盘网络技术,结合动态分布式数据存储,在不影响使用的前提下将需要严密保护的数据严格管控,实现全方位的网络数据安全管理。

目前对于PXE数据安全的处理主要依靠人为管理并辅助相关的软硬件。网络管理软件相对较多,主要集中在两个

到稿日期:2009-10-21 返修日期:2010-01-07 本文受北京市教委2010年科技面上项目(项目编号:KM201000002002)资助。
**黄冠利**(1975—),硕士生,副教授,主要研究方向为信息论等,E-mail:huangguanli@sina.com;**金 岩**(1970—),高级工程师,主要研究方向为通信控制等;**勾传静**(1985—),主要研究方向为虚拟现实等;**王 萍**(1973—),副教授,主要研究方向为网络应用程序开发等。

方面：一是用于网络的管理和监控，主要是对网络进行防护、对系统软件的使用进行监控、对网络接入设备进行管理和监控等（如防火墙）；二是用于对数据的管理和备份，主要涉及数据的加密、传输、备份处理等，如大多数加密软件及数据冗余备份系统等。提供与以上软件功能相似的硬件也有很多，如硬件防火墙、硬件加密狗等。问题是，工具只有到了会用的人手上才能真正发挥作用。由于 PXE 使用系统及数据的人员素质高低不一，常常会因为个人原因而放弃工具的保护，如用户经常由于类似的原因关闭桌面防火墙。再如，内部和外部采用不同的标准，同样使得整个系统的安全防护形同虚设。根据有关数据统计，泄密事件大多由于个人操作失误以及防范意识薄弱导致数据泄漏，其核心在于人们并没有意识到自己的机密数据已经暴露在黑客等非法入侵人员的视野下。以上情况的出现正是由于目前的大多数数据安全系统还没有将安全管理与控制进行很好地结合。为了减少这种泄密事件的发生，非常有必要构建一套满足要求的、减少和避免秘密数据泄漏的基于 PXE 的数据安全管理系统。

### 1.2 国外与信息系统存储管理安全相关的系统对比分析

下面就国际上与信息系统存储管理安全相关的系统加以比较和说明。

Encrypted File System（EFS）主要运行在 Windows 2000 和 Windows XP 系统上，对文件系统上的数据进行加密，只有文件的创建用户或者拥有者才能访问该文件。该系统有较可靠的安全性，但是不能提供多用户的文件共享。

Self-Certifying File System（SCFS）是纽约大学 2000 年的科研成果，该系统主要实现了对系统服务器的客户端认证。它提出了多种有效的认证方式，但是不提供对客户在服务器端的认证和对信息的安全保证。

Fast and Secure Distributed Read-Only File System（FSDROFS）是 2001 年的一项科研成果，尚未进入产品开发阶段。该系统提出了一种对整个文件系统进行签名的方法，并且每个读取的文件都可以带有相应的签名。这样，文件即使被存储在不被信任的主机之上，也不用担心文件被篡改。但是，该文件系统只可提供读取功能，并无修改文件的功能。

Secure Information Management System（SIMS）是一个大型信息安全项目的一项核心产品，成功地实现了在不同机器上分别提供信息存储和访问授权认证：文件服务器和密钥服务器。所有信息以加密的形式存储在文件服务器上，密钥服务器将确认文件访问的权限并将确认的结果传递给文件服务器。SIMS 的主要目的是为了在多人口（个体用户或公司）间分布地共享数据。密钥服务器则集中控制访问权限和加密信息的密钥。所以，被信任主机系统的密钥管理成本比较低，可以用比较少的人力集中力量维护大型系统的安全控制部分。当然，这种集中的密钥服务器体系容易使密钥服务器成为整个系统的网络瓶颈，容易受到分布式拒绝访问服务（DDOS）的攻击[1,2]。

## 2 PXE 动态分布式无盘网络数据存储的特点与构成

### 2.1 PXE 动态分布式无盘网络数据存储平台构成

动态分布式无盘网络数据存储平台是数据存储技术的一个极有前景的发展方向。其平台是一个分布式的文件存储管理平台，可以提供加密存储和动态分布认证技术，有较高的认证效率和抗攻击能力。通过分布存储实现数据异地备份，可以提供更安全、完整的信息存储方案。该体系分为 4 个系统部分：

应用文件加密存储系统，提供可单独评价的加密、数字签名、访问控制、数据完整性、业务流填充、路由控制、公证、鉴别审计等安全机制，并有相应的安全管理解决方案。

用户甄别系统，通过 PXE 平台为远程客户访问重要的应用服务提供的鉴别服务器，严格执行鉴别过程和访问控制。

安全应用服务器系统，密钥管理中心、访问控制中心、安全鉴别服务器、授权服务器等，负责访问控制以及密钥、证书等安全材料的产生、更换、配置和销毁等相应的安全管理活动。采用 PXE 技术，实现远程自动控制。

密钥分布存储系统，采用 PXE 无盘存储技术，具备分布存储、抗侦听、抗截获能力；能对抗传输信息的篡改、删除、插入、重放、选取明文密码破译等主动攻击和被动攻击，保护信息的机密性，保证信息和系统的完整性。

### 2.2 PXE 动态分布式无盘网络数据存储特点

PXE（Pre-boot Execution Environment）由 Intel 设计，可以使计算机通过网络启动的协议。协议分为 client 和 server 两端。技术从最初成功实现 Windows 98 的远程启动和运行后，可靠性和稳定性不断提高，目前已经能够实现大多操作系统的无盘运行，包括 Linux，DOS 以及包括 WIN2003，WIN VISAT 的全系列 Windows 操作系统。PXE 是 RPL 的升级品，在启动中可以采用动态分配 IP 的 DHCP 方式，也可以采用固定 IP 的 BOOTP 方式。通信协议采用 TCP/IP，与 Internet 连接高效而可靠。PXE 无盘工作站的启动如下：客户端开机后，由 Bootrom 接管系统启动，并通过广播送出 BOOTP/DHCP 要求以取得 IP。这个请求帧中包含了客户机的网卡 MAC 地址，服务器收到验证 MAC 地址后送回客户端的 IP 地址、预设网关及开机影像文件，Bootprom 通过 TFTP 协议从服务器下载开机影像文件，客户机通过这个开机影像文件开机。这个开机文件可以只是单纯的开机程序，也可以是操作系统。开机影像文件在工作站内存模拟成磁盘，从这个模拟磁盘启动，并连接服务器，将无盘启动预置好的各种环境，如操作系统所在路径、相关注册表的调整等导入[3]。

因为 PXE 能支持多种操作系统，所以现有的各种应用软件都能得到非常好的应用；客户机上的所有计算功能均在本机运行，无需占用服务器资源，因此使得一台服务器能带超过 100 台的工作站；只要终端硬件配置相同，则无论多少台工作站，系统和应用软件只需安装一套；操作维护简便，升级软件只需向服务器重新传一遍系统，所有工作站即已全部升级了；提供更加可靠的数据存储和应用行为管理，实现更加有效的内部 PC 安全管理体系。

## 3 PXE 动态分布式无盘网络数据存储体系

### 3.1 PXE 信息存储和访问授权认证的分离

基于 PXE 技术的动态分布式无盘网络数据存储体系构成的信息安全平台系统采用 SIMS 技术，成功地实现了在不同服务器主机上分别提供信息存储和访问授权认证，即文件服务器和密钥服务器。所有信息以加密的形式存储在文件服务器上，密钥服务器将确认文件访问的权限并将确认的结果传递给文件服务器。采用 SIMS 技术的主要目的是为了在多

入口(个体用户或公司)间分布地共享数据,密钥服务器则集中控制访问权限和加密信息的密钥。所以,信任主机系统的密钥管理成本比较低,可以用比较少的人力集中力量维护大型系统的安全控制部分。

动态分布式无盘网络数据存储体系实现了对系统服务器的客户端和对客户在服务器端的双向认证,并可以采用多种有效的认证方式。本系统同时借鉴和改进的 FSDROFS 技术,采取对整个文件系统进行动态签名的方法,并且每个读取的文件都可以带有相应的签名。这样。文件系统就可以被存储在不被信任的主机之上,而不用担心文件被篡改。文件信息系统可以具备读取和修改的双重能力。

动态分布式无盘网络数据存储安全解决方案构成的信息安全平台采用"通过密钥分割共享实现的分布信息安全存储管理系统"(Distributed Secure Information Management System with Split Secret Sharing,DSIMSwSSS)来解决现有安全体系的弊病。分布存储密钥技术的主要思路是把密钥分解成 $n$ 个带校验的片段,分别存储在 $n$ 个主机上。需要认证的用户只要在 $m$ 个主机($m<n$)上取回密钥片段,即可拼装成原始密钥而获得认证。而当取回的密钥片段小于 $m$ 时,则无法生成原始的密钥,即无法获取数据文件。该体系要求所有的服务器维护一个加密文件访问控制表(ACL),在用户请求访问特定的文件的时候,需要跟 ACL 进行比对确认。ACL 需要一套同步机制进行同步操作,采取 DSIMSwSSS 技术,提高了系统的安全性和稳定性,并大大提高了系统的容错能力。即便有 $d$ 台存储密钥的主机出错,甚至无法提供服务,只要 $d<n-m$,用户照样读取或存储信息。

### 3.2 构建用于数据安全的无盘网络

#### 3.2.1 通过无盘技术提升网络数据的安全性,建立符合要求的无盘网络

如图 1 所示,整个网络系统分设在数据安全中心、网管中心和工作区域。数据被划分为两部分,即安全数据与普通数据。安全数据存放在不与外界相连的服务器上,普通数据可以存放在接入 Internet 的服务器上。采用传统的数据安全防护方法,个人计算机上不存储任何数据,根据需要接入不同的服务器。

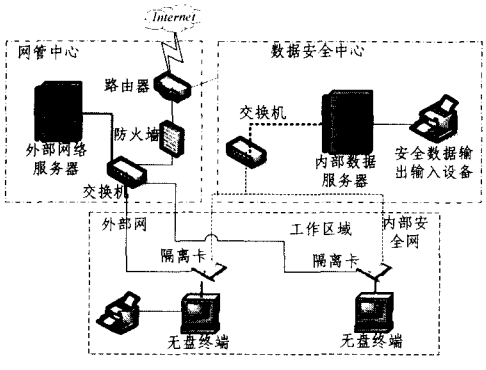


图 1 无盘网络拓扑图

数据安全中心放置内部网络数据及远程启动服务器。终端本地不配备存储设备(硬盘等),不安装任何系统和程序,所有数据及操作系统均集中存储在服务器上统一管理,且整个内部网络与 Internet 物理隔离。

网管中心放置外部网络数据及远程启动服务器。终端本地不配备存储设备(硬盘等),不安装任何系统和程序,所有数据及操作系统均集中存储在服务器上统一管理。整个外部网络可以与 Internet 连接,从而保证外部网络上的终端可以接入 Internet 网络。

同一个终端可以通过隔离卡分别接入内部网或外部网,且内部网与外部网物理隔离。接入内部网时处理安全信息,接入外部网时可以上 Internet 网。隔离卡采用继电器控制技术,可以保证内外网的物理隔离。隔离卡的原理如图 2 所示。

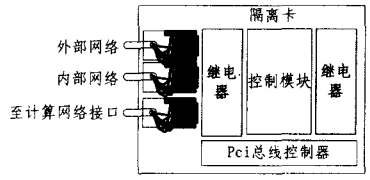


图 2 隔离卡原理示意图

#### 3.2.2 整个网络特点

终端本地不配备存储设备(硬盘等),不安装任何系统和程序;

终端接入网络可自动获得该网络相应的操作系统和应用;

终端支持个性化配置;

终端具有更高效的应用速度性、易用性、稳定性、可管理性;

终端可以提供多种操作系统和应用软件功能的瞬间切换,实现多功能分组应用环境;

提供更加可靠的数据存储和应用行为管理,实现更加有效的内部 PC 安全管理体系;

提供系统和软件的瞬间增量统一部署功能,完全取代陈旧的软件分发功能;

每台双翼操作系统服务器可管理多达 100 台终端 PC,管理工作量极大缩小;

标准 PC 性能可以发挥 PC100%的计算能力,可以高效运行大型软件和计算型软件;

标准 PC 兼容性可以全面支持 DOS/Windows/Linux/Unix 等操作系统,并直接兼容各种应用软件和外设;

标准的管理体系可以与原有管理系统和管理软件共存使用,共同提升管理效率。

### 3.3 合理配置系统和数据管理软件的关键

整个系统的软件架构如图 3 所示。

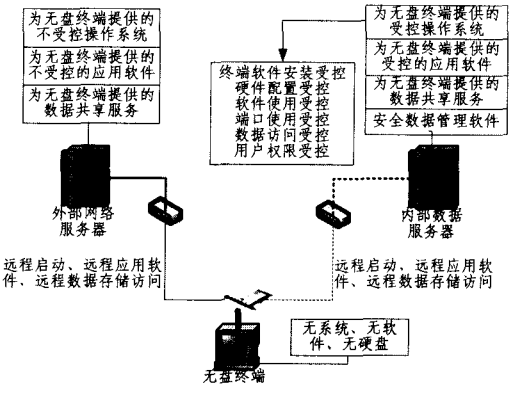


图 3 系统软件配置示意图

当终端接入外部网络时,由于系统不存在核心安全数据,可以采用传统的方法,无需提供特殊的管控软件。

当终端接入内部网络时,由于内部网络运行有数据管理

系统，则能够保证内网数据的安全。数据管理系统包括如下功能模块：

(1)终端操作系统管控，管理控制各个终端的操作系统，使得用户无法自行修改操作系统各种权限。

(2)终端软件安装管控，使得终端系统安装、卸载各种应用软件均在服务器的控制之下，保证用户无法私自修改系统。

(3)终端硬件配置受控，使得终端上的各项硬件设备接入和使用均在服务器的控制之下，从而保证数据的出入口在管控之下，用户无法私自将需要保护的数据输入输出网络。

(4)网络设备接入管控，使得接入网络的各种设备(如终端、打印机等)必须经过授权登记才能接入并访问网络数据，非授权设备无法接入。

(5)终端软件使用管控，使得终端上的各种软件均具有使用权限，用户只能根据权限使用，低级权限的用户无法使用高级权限的软件。

(6)用户身份鉴别，对使用网络设备的用户身份进行鉴别，非经授权用户无法访问网络。

(7)访问控制，每一用户只能访问与自己权限对应的数据，无法访问权限外数据。

(8)审计记录，可以对设备的接入、用户的访问、操作等行为进行审计记录。

(9)使用灵活性，将受保护数据隔离出外部网络，增加了外部网络使用的灵活性。

(10)数据备份与加密处理，采用软硬件技术对数据进行实时备份，保证数据的存储可靠性；对数据的存储和传输采用合适的加密方法，保证安全性。

(11)数据访问权限控制，所有需要保护的数据均集中存放、集中管理，用户只能根据其权限对这些数据进行访问，无法私自查阅和获取未经授权的信息[4]。

### 3.4 使用时间标记解决 PXE 存储安全问题

#### 3.4.1 对 SIMS 进行全面的改进并借鉴数字签名技术

对 PXE 密钥服务器实现分布式管理，从而提高系统整体效率并且提高了系统的安全性。常用的基于对称密码算法，是使用对称密码系统和仲裁者对数据进行签名。基于对称算法的数字签名有很多的缺点，对仲裁者来说非常耗时，要求必须备有数据库，将成为软件系统中的瓶颈。而且，数据库必须完全安全，否则会出现假文件。所以，使用对称密码系统和仲裁者对数据签名是很难保证数据安全的。而基于非对称密码算法，是使用公开密钥密码术对数据进行签名。在某些公开密钥算法中，公钥或私钥都可用作加密。但基于非对称密钥的数字签名也有缺点，例如，1)对长文件签名速度较慢，不能满足时间效率要求；2)用户对文件的签名会出现任何时候都有效的情况，会导致一张银行支票任何时候都可以取钱，这显然是不可行的。综上算法的缺点，动态分布式无盘网络数据存储体系中的数字签名技术更倾向于使用时间标记和单向散列函数来解决数据存储安全问题。

PXE 动态分布无盘网络数据存储体系签名中因无盘技术网上控制时序性而使用时间标记(又叫时间戳)，对日期和时间的签名附在消息中，并跟消息中的其他部分一起签名。这样签名文件就不可重用了。散列函数是把可变输入长度串(叫做预映射)转换成固定长度输出串(散列值)的一种函数。单向散列函数是在一个方向上工作的散列函数，根据预映射的值很容易计算其散列值，但从其散列值推出预映射的值就非常难了[5,7]。

#### 3.4.2 使用公开密钥密码术、单向散列函数数据签名

图 4 给出了数据签名协议图。

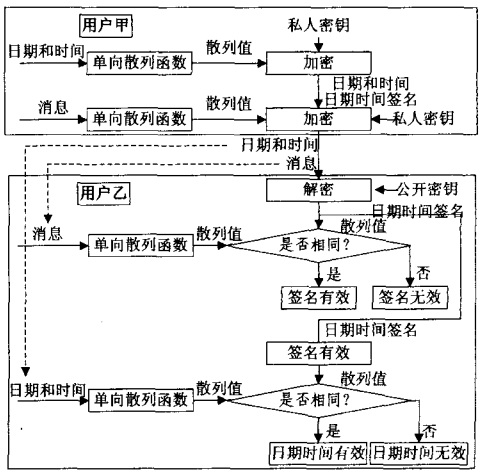


图 4 使用公开密钥密码术、单向散列函数和时间标记对数据进行签名协议图

该数字签章验证通过的 PXE 动态分布式无盘网络数据存储安全解决方案体系具有数据真实性、不可入侵性、不可否认性、不可重用性[6]。

#### 3.4.3 算法需求与分析

PXE 动态分布存储密钥体系通过设立分布存储的安全体系加强整体的安全性，本身不进行数据加密算法的研究。该系统通过开放的存储访问层挂接不同的加密接口，实现同一体系、不同加密方法的管理和转换。比如，对称加密标准 DES，3DES，IDEA 以及被普通看好的 AES；非对称加密标准 RSA；VPN 标准 IPSec；传输层加密标准 SSL；安全电子邮件标准 S-MIME；安全电子交易标准 SET；通过脆弱性描述标准 CVE。这些都是经过一个自发的选择过程后被普通采用的算法和协议，也就是所谓的“事实标准”。通常建议使用 1:1 的加密算法，这样可以不增加网络吞吐流量。动态分布存储密钥体系使用非对称算法来对数据签名和进行密钥交换，该算法的处理复杂性要不小于 $2^{512}$，并且可以导出公钥和公私钥对，算法速度不能比 RSA 慢。系统使用对称算法来保护公私钥对和 Memory 卡上的用户信息，此算法的处理复杂性不能小于 $2^{64}$，速度不能慢于 DES 算法。系统使用单向散列函数保证签名文档的完整性和 Memory 卡中信息的完整性，算法的处理复杂性不能小于 $2^{128}$，速度不能慢于 MD5 算法，见表 1。

表 1 算法需求表

| 需要算法 | 应用范围 | 算法要求 |
|---|---|---|
| 非对称算法 | 用来交换密钥和数据签名 | 处理复杂性大于等于 $2^{512}$<br>可导出公钥<br>可导出公/私钥对<br>速度大于等于 RSA 算法 |
| 对称算法 | 用来对密钥进行加解密 | 处理复杂性大于等于 $2^{64}$<br>速度大于等于 DES 算法 |
| 单向散列函数 | 对文档进行哈希运算 | 处理复杂性大于等于 $2^{128}$<br>速度大于等于 MD5 算法 |

算法的安全性依赖于密钥。好密钥是指那些由自动处理设备产生的随机位串。如果用一个弱的密钥产生方法，那么整个系统都将是弱的。许多加密算法都有弱密钥，所以在产

生密钥前，通过算法说明书了解算法的弱密钥。密钥产生时，必须防止弱密钥的产生。密钥的传输有很多方式，初期的离线产品不涉及到密钥传输。ANSI X9.17 标准表述了两种密钥：密钥加密密钥和数据密钥。二期的在线产品需要通过网络传输公开密钥，采用密钥加密密钥将数据密钥加密或使用公开密钥密码术体系里的密钥传输协议来传输密钥。公开密钥密码术有一个缺陷，就是如果用户甲的公开密钥被中间人替换了，用户乙是很难发现的。所以在给用户的 Memory 卡中，一定会加上对所有密钥的校验码，就是使用单项散列函数分别对所有密钥进行运算。

PXE 动态分布存储密钥体系通常不采用软件加密（加密算法用软件实现），因其加密过程是在本机内实现的，破坏者可以对内存进行检测，对算法进行分析。如果算法被攻破，后果将是可怕的，故动态分布存储密钥体系通常使用硬件实现算法，加解密都在硬件中进行，无法追踪检测，所以更加安全。在系统中控制密钥的使用方案是：在密钥后面附加一个控制向量，用来标定密钥的使用和限制。对控制向量取单向散列运算，然后与主密钥异或，把等到的结果作为密钥对会话密钥进行加密，再把合成的加密的会话密钥跟控制向量存在一起。恢复会话密钥时，对控制向量取单向散列运算，再与主密钥异或，最后用结果进行解密。另外，密钥在使用完后，会立即从机器中销毁，决不会在磁盘上保存。用户如果想更新密钥，必须先收回旧密钥，在确认旧密钥无误的情况下，为用户提供新的密钥。旧密钥要进行销毁。

**结束语** 如上所述，PXE 动态分布式无盘网络数据存储安全解决方案的信息安全平台对 SIMS 进行了全面的改进，借鉴了数字签章、无盘网络等相关技术的优点。通过分布存储实现数据异地网络备份，对密钥服务器实现分布式管理，从而提高了数据存储系统整体效率并且提高了系统的安全性。基于 PXE 技术的动态分布式数据存储体系的最终用户为信息化较高的行业：证券、保险、银行、教育、交通、旅游、互联网、电信、大型零售企业、会员制行业以及医药企业的内部信息平台以及电子政务等公众网络信息服务。

数据存储安全是一个关系国家安全和社会稳定的重要问题，涉及网络技术、密码技术、信息安全技术、应用数学、信息论等多种学科。为了保证信息安全的可靠性，开发拥有独立知识产权的安全存储技术系列产品势在必行。本文提供了一种提高网络数据安全的解决方案，方案采用最新的动态分布式存储技术及 PXE 无盘网络技术，将所有网络数据及操作系统集中存放在单个服务器上，从而实现数据的集中存储与集中管理，从网络边界安全、数据传输安全、数据存储安全 3 个方面降低各种数据泄漏风险，从技术上解决可能存在的管理漏洞，为如何有效保证网络数据安全、真正实现数据的安全可靠提供参考。随着成果的普及与行业应用，其经济价值前景可观。

## 参 考 文 献


[1] Sinha P K. Distributed Operating Systems [M]. IEEE Computer Society Press, 2000

[2] Garrett P. Making, Breaking Codes [M]. Prentice-Hall, 2001

[3] 闵军，等. 最新 PXE\RPL 无盘站和终端[M]. 北京：清华大学出版社，2003

[4] 黄冠利，等. 动态分布式无盘网络数据安全解决方案设计与改进[C]//2009 国际信息技术与应用论坛. 2009

[5] 斯托林斯. 密码学与网络安全[M]. 北京：清华大学出版社，2002

[6] 黄冠利，胡亦，等. 基于 PKI 体系的数字签章安全系统设计[J]. 计算机安全，2008，9：78-80

[7] 钟阿林，许方恒，董方敏. 一种理想的数据库加密方案[J]. 重庆邮电大学学报：自然科学版，2007，19(6)：131-133


（上接第 289 页）

删除等具有较好的鲁棒性。

**结束语** 经过对视频序列的多次实验测试，本文提出的基于 MPEG-7 形状轮廓编码的视频水印算法，具有以下特点：将视频信号分成一系列的视频组，对视频组中的帧进行 MPEG-7 形状轮廓编码得到一些局部的点，并将这些点作为各种变换域的区域以及水印嵌入的区域，从而避免了全局的计算，降低了算法的运算复杂度；利用 Hash 的思想实现部分水印信号的无损嵌入，在保证不可见性的同时，使水印具有较好的鲁棒性；采用混沌技术，提高了水印的嵌入量和算法的鲁棒性；水印提取时不需要原始视频信号，并可以进行多重水印的校验。

## 参 考 文 献


[1] Hartung F, Birod B. Watermarking of uncompressed and compressed video[J]. Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66(3): 283-301

[2] 梁华庆，王磊，双凯，等. 一种在原始视频帧中嵌入的鲁棒的数字水印[J]. 电子与信息学报，2003，25(9)：1281-1284

[3] SwansonM D, Zhu B, Tewfik A H. Multiresolution scene based video watermarking using perceptual models[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 540-550

[4] Deguillarme F, Csurka G, Ruanaidh J O, et al. Robust 3D DFT video watermarking[C]// Proceedings of SPIE. Security and Watermarking of Multimedia Contents. San Jose, California, 1999, 3657: 113-124

[5] 张立和，伍宏涛，胡昌利. 基于三维 Gabor 变换的视频水印算法[J]. 软件学报，2004，15(8)：1252-1258

[6] Martinez J. MPEG-7 Overview(Versions 10) [S]. 150/IECJTCI/SC29/WGl. http://www. chiariglione. org/mpeg/standards/mpeg-7/mpeg-7. htm, 2002

[7] Pereira F, Koenen R. MPEG-7: A standard for multimedia content description[J]. International Journal of Image and Graphies, 2001, 3(1): 527-546

[8] Mokhtarian F, Mackworth A K. A Theory of Multiscale, Curvature-Based Shape Representation for Planar Curves[J]. IEEE transactions on pattern analysis and machine intelligence, 1992, 14(8): 789-805

[9] Lin H B. Staring with parabolas: an introduction to chaotic dynamics[M]. Scientific and Technological Education Publishing House, Shanghai, 1993

[10] 张欣，杨德刚. 一种基于混沌映射的图像加密方法[J]. 重庆工学院学报：自然科学版，2009，23(10)：104-107