

2010

# HuaTech 应用安全防护系统 技术白皮书

北京中软华泰信息技术有限责任公司



# 目 录

1. 公司简介.....	1-
2. 产品概述.....	2-
3. 产品架构.....	3-
4. 功能介绍.....	3-
4.1 安全管理中心模块.....	3-
4.1.1 系统管理.....	4-
4.1.2 标记管理.....	4-
4.1.3 授权管理.....	4-
4.1.4 策略管理.....	4-
4.1.5 审计管理.....	4-
4.1.6 管理员权限管理.....	5-
4.2 服务器加固模块.....	5-
4.2.1 双因子强身份认证.....	5-
4.2.2 自主访问控制.....	5-
4.2.3 基于标记的强制访问控制.....	6-
4.2.4 重要资源完整性保护.....	6-
4.2.5 硬盘信息加密保护.....	6-
4.2.6 操作系统完整性保护.....	7-
4.2.7 可执行代码控制.....	7-
4.2.8 网络访问控制.....	7-
4.2.9 移动介质权限管理.....	7-
4.2.10 行为审计监控.....	7-
4.3 终端安全保护模块.....	8-
4.3.1 双因子强身份认证.....	8-
4.3.2 自主访问控制.....	9-
4.3.3 基于标记的强制访问控制.....	9-
4.3.4 数据完整性保护.....	9-
4.3.5 硬盘信息加密保护.....	10-
4.3.6 可执行代码控制.....	10-
4.3.7 网络访问控制.....	10-
4.3.8 移动介质权限管理.....	11-
4.3.9 移动介质加密保护.....	11-
4.3.10 行为审计监控.....	11-
4.4 应用安全增强模块.....	11-
4.4.1 防 SQL 注入攻击.....	12-
4.4.2 防跨站脚本攻击.....	12-
4.4.3 抗拒绝服务攻击.....	12-
4.4.4 防缓冲区溢出攻击.....	12-
4.4.5 防目录遍历.....	12-
4.4.6 防网页盗链.....	13-
4.4.7 防网络爬虫.....	13-

4.4.8 轻量级 SSL 终止.....	- 13 -
4.4.9 抗黑客扫描.....	- 13 -
<b>5. HUATECH 应用安全防护系统技术特点.....</b>	<b>- 14 -</b>
<b>6. HUATECH 应用安全防护系统产品优势.....</b>	<b>- 16 -</b>

# 1. 公司简介

北京中软华泰信息技术有限责任公司成立于 2000 年，专业从事于信息安全体系研究、信息安全产品研制、生产和销售，是国内实力雄厚的网络安全产品、可信计算产品、安全服务与解决方案的综合提供商。

公司一直把操作系统安全和信息应用系统安全作为产业方向。经过多年的技术积累与沉淀，公司在安全操作系统开发，尤其是计算机病毒木马防御、访问控制体系研究、网络攻击防御等专业领域取得重大技术突破。先后推出了防火墙、网站防护系统、终端安全保护系统、服务器安全加固系统等一系列安全产品，是国内实力雄厚的网络安全产品、主机安全产品、安全服务与解决方案的综合提供商，为国家的信息安全事业做出了重大贡献。

近年来，公司成为国家与微软公司源代码级技术合作单位，并先后参与了国家发改委产业化项目及科技部、北京市科委科研项目。2007 年成为中国可信计算联盟成员之一。2009 年参与了国家标准《信息安全技术 信息系统等级保护安全设计技术要求》的制定。

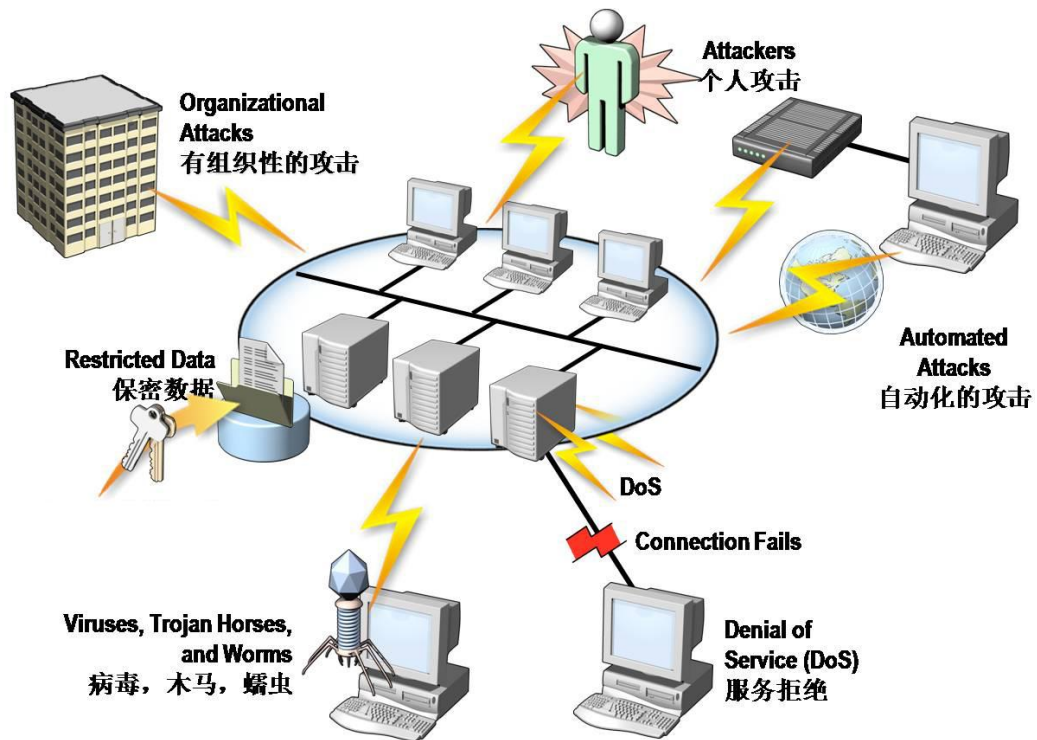
公司坚持产、学、研相结合的发展方向，与北京交通大学、北京工业大学共同成立研究生培养基地，在为国家输送大批信息安全专业人才的同时也使公司具有了坚实的技术储备。

公司不断提高产品技术水平及售后服务能力，加强营销网络体系建设，经过近十年的发展，建立起完善的销售及服务网络，累计对近 800 多个单位的上万台服务器和终端进行了安全加固。

公司今后将致力于等级保护的方案和产品的提供。不断推出符合等级保护标准的安全产品，竭尽全力为国家的信息安全事业做出贡献。

## 2. 产品概述

随着计算机网络技术的迅速发展和进步，信息和计算机网络组成的应用系统现在已经成为社会发展的重要保证。应用系统目前已经覆盖到国家的政治、金融、军事、文化、科技、教育等诸多领域。由于应用系统担负着存储、传输和处理的重要信息的职能，这些信息涵盖了各种政府宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、高科技科研数据等重要信息，其中有很多是国家敏感信息和国家机密，因此应用系统难免会吸引各种网络黑客的攻击行为（例如，信息窃取、信息泄漏、数据删除和篡改、计算机病毒、拒绝服务攻击等）。如下图所示：



图：应用系统面临的威胁

应用系统通常由应用服务器、应用系统使用及维护终端、应用系统信息资源共同组成，为了全面保障应用系统的安全，必须从这几个方面着手进行安全防护。因此为了全面解决应用系统防止来自外部及内部用户攻击的问题，中软华泰在对攻击手段及传统安全产品详尽分析的基础上，经过多年研发，于2009年2月份推出了“HuaTech 应用安全防护系统”。该系统以安全管理中心策略控制为核心，在不改变现有应用系统的基础上，通过对终端、服务器、应用系统进行安全增强，提高整套应用系统的健壮性，保证应用系统始终在可控状态下运行，从而从根源上有效抑制对应用系统安全的威胁，最终达到防止内部用户以及外部用户攻击的目的，全方位的保障应用系统的安全。

### 3. 产品架构

HuaTech 应用安全防护系统是由四大模块共同组成，包括服务器加固模块、终端安全保护模块、应用安全增强模块和安全管理中心模块四个组成部分。



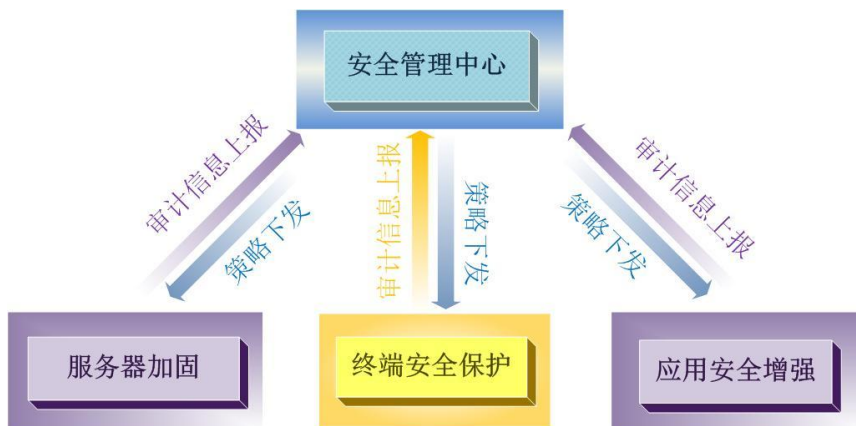
图：HuaTech 应用安全防护系统整体架构图

（注：本图介绍仅列举产品部分功能，详细功能请参见下文介绍）

### 4. 功能介绍

#### 4.1 安全管理中心模块

安全管理中心模块可对应用安全防护系统其它模块进行集中管控，从而实现对应用系统中的终端、服务器的集中策略下发、集中控制、集中日志审计。安全管理中心管理模式见下图所示：



图：HuaTech 应用安全防护系统管理模式



安全管理中心模块功能如下：

### 4.1.1 系统管理

用于对终端/服务器合法登录用户的身份管理、终端/服务器软硬件的配置管理等。其中用户身份管理是将与用户相关证书、密钥等安全属性发行到与用户绑定的硬件令牌中，以硬件令牌代表用户身份；软硬件配置管理是对终端/服务器平台身份、终端/服务器上能够使用的执行程序、终端/服务器上能够使用的移动存储设备的确认过程。提供对用户身份的管理、平台身份的管理、移动存储设备管理、执行程序管理。

### 4.1.2 标记管理

提供主体标记管理功能，为系统中的各用户配置安全级别和安全范畴；提供客体标记管理功能，为系统中各与安全业务相关的客体设定安全标记。安全标记包括与文件名直接相关的安全标记、目录安全标记、设备安全标记等类型。同时提供安全标记的修改接口，供安全管理员人工参与安全级别的制定和更改。

### 4.1.3 授权管理

提供授权管理界面，制定强制访问控制策略、自主访问控制策略、级别调整策略等，将对特定客体的打开、读、写、执行、删除、改名等权限赋予相应的用户。具体包括：终端/服务器授权用户策略，限定用户登录指定终端/服务器的权限；可执行代码控制和校验策略，提供可执行程序预期值白名单；终端/服务器访问控制策略，控制用户登录后对文件、设备等资源的访问权限；网络访问控制策略，限定主机对网络其它主机的连接权限，控制用户访问上传服务器各种信息的权限等。

### 4.1.4 策略管理

提供策略下载和更新的功能，将生成的访问控制策略表组合发送到各终端/服务器平台的安全部件；提供策略维护界面，为安全管理员的策略查找、策略更新等操作提供支持，并能够实现策略文件的导入和导出操作，支持离线状态下的策略管理，提高安全管理员的策略管理操作的方便性和易用性。

### 4.1.5 审计管理

针对受控终端/服务器，根据审计需求，制定详尽的审计策略，其中包括用户登录、资源访问、进程启动等；对已收集的审计信息，分类别提供详细的审计查询，包括按照平台 ID 查询、按操作类型作查询、按操作结果查询等，支持对审计信息的收集、归并、查询、备份等操作。

## 4.1.6 管理员权限管理

为了方便权限管理，安全管理中心模块引入以下三个角色：系统管理员、安全管理员和安全审计员。根据最小权限原则，系统只赋予每个角色完成任务所需的最小权限。

系统管理员具有对终端/服务器进行日常维护的权限，其操作权限由安全管理员制定，其行为由系统审计机制监控。安全管理员只有完成安全管理任务的权限，即配置系统安全策略等，并且安全管理员的一切操作行为都被记入审计日志。安全审计员只负责审计日志的存取控制，不具有安全管理员和系统操作员的权限。

安全管理中心模块正是通过上述“三权分立”的机制，使得系统中的不同用户相互监督、相互制约，每个角色各司其职，共同保障信息系统的安全。

## 4.2 服务器加固模块

### 4.2.1 双因子强身份认证

现有的服务器操作系统采用口令认证方式对用户身份进行鉴别，容易受到字典攻击。在服务器加固模块中，引入一个硬件 USB-KEY 令牌。该 USB-KEY 为用户身份的唯一标识，当用户登录系统时，需要插入 USB-KEY，然后系统对用户进行双因子身份认证，用户只有拥有合法的 USB-KEY，并且输入正确的操作系统口令+ USB-KEY 口令，才能登录服务器系统。

登录成功后，如果用户需要临时外出，可以拔除 USB-KEY，这样安全内核会自动保存用户的工作环境，并且锁定服务器桌面。除了持有原 USB-KEY 的用户外，任何人都不能进入服务器环境。由此，服务器加固模块实现了基于硬件 USB-KEY 的双因子身份认证，使得非授权用户无法进入服务器环境。

### 4.2.2 自主访问控制

在现有服务器操作系统中，如果用户以管理员身份登陆，则可以访问服务器系统中的任何文件，并且服务器经常是混用的，用户很难保护自己的隐私。但是安装了服务器加固模块后，每个用户可以拥有自己的文件保密柜，即设置自己的私有目录。安全内核使用用户的私有密钥加密保密柜中的文件，并且禁止本用户以外的其它用户访问保密柜中的文件，从而有效地保护了用户的私有信息。

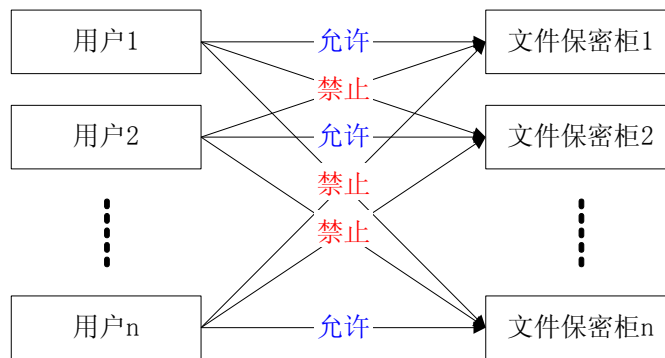


图 4.2.2 文件保密柜示意图

### 4.2.3 基于标记的强制访问控制

服务器加固模块提供了强制访问控制机制，通过对执行程序的强制访问控制、对信息资源的强制访问控制、对移动设备的强制访问控制等机制实现对应用进行安全“隔离”。该机制由统一安全管理平台对服务器系统中的主体（用户、进程）及客体（文件、执行程序、外部设备等）进行安全标识，根据客体类型的不同，分别制定了不同的访问控制规则，严格控制用户行为，保证用户的任何行为都在安全策略的支撑下，从而全方位地确保服务器中的重要数据的“拿不走”，保护服务器系统的机密性。

### 4.2.4 重要资源完整性保护

服务器加固模块允许用户或进程以不同访问权限对文件/目录设置强制访问控制规则，在不改变原有服务器文件系统格式的基础上，通过全路径名对服务器系统中的重要客体进行标记。安全内核启动时，将策略加载到内存中，这样内存中就维护了一张服务器系统重要客体的链表。安全内核截获应用层的访问请求后，查询链表中客体的保密性和完整性级别，实现强制访问控制。任何用户及其调用的进程对服务器敏感文件或目录进行操作行为时都要进行严格的控制，杜绝用户数据被篡改、删除、插入等情况的发生，从而全方位地确保重要数据的完整性不被破坏。

### 4.2.5 硬盘信息加密保护

数据存储保护是防止信息泄露最有效的手段，服务器加固模块支持对服务器硬盘数据透明加解密，达到了重要信息即使被盗取，信息盗取者也“看不懂”的效果。

所谓透明加解密是指该加解密过程对用户是透明的，这一过程在操作系统层实现，对上层应用透明，用户感觉不到它的存在。这一特性可以保证信息系统中的重要信息在存储和传播过程中都以密文的形式存在，即使意外断电，也不会导致明文信息的外泄。

在服务器加固模块中，安全管理员可以根据客体的不同安全级制定不同的数据保护策略，方便信

息系统和外界进行数据交换。

#### 4.2.6 操作系统完整性保护

对服务器操作系统文件进行实时的保护，禁止任何的非法修改行为，保证服务器操作系统完整性不被破坏。

#### 4.2.7 可执行代码控制

服务器加固模块提供执行程序真实性和完整性度量功能。执行程序真实性度量可以确保系统中的执行程序都是合法的，从而阻止非授权程序运行。执行程序完整性度量用来保证系统所启动的执行程序都是可信的，禁止不符合预期的程序启动。执行程序启动前，服务器加固模块中的核心模块会度量该程序相关模块的真实性和完整性，只有在度量结果和预存值一致的前提下，该程序才允许启动，否则拒绝其执行。因此即使系统中的某一执行程序被病毒或木马感染，由于其不再可信，服务器加固模块将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了服务器操作系统完整性被破坏的风险。正是由于上述安全机制，服务器加固模块实现了服务器对于病毒、木马、攻击程序等恶意代码自免疫。

#### 4.2.8 网络访问控制

服务器加固模块增强了服务器操作系统的网络访问控制能力，通过对通信平台身份的认证，达到对接入的控制，实现对应用环境边界的保护，从而阻止非法接入服务器系统。

安全管理员可以规定哪个终端可以接入服务器系统。因此在终端尝试接入服务器系统时，服务器加固模块检查该终端的平台身份，只有检验通过后，该终端方能与服务器进行通信。

#### 4.2.9 移动介质权限管理

服务器加固模块对于移动介质进行严格的控制，所有移动介质在使用之前都需经过授权，未经授权的移动介质一律禁止其使用。对于已授权的移动介质进行标记管理，对其使用行为进行全程的严格控制，从而防止通过移动介质非法拷贝敏感信息等恶意事件的发生。

#### 4.2.10 行为审计监控

服务器加固模块监督服务器系统中关于安全相关的行为，尤其是安全管理员对安全策略的制定、修改以及授权用户违反安全策略的行为，达到非法行为“赖不掉”的效果。具体包括：用户登录审计、文件访问审计、进程启动审计等等。审计内容包括：平台、时间、用户、对象及操作结果等。

## 4.3 终端安全保护模块

终端安全保护模块是在现有终端操作系统基础上，强化了其身份鉴别、数据完整性保护、数据保密性保护、系统完整性保护以及行为审计机制，增加了强制访问控制机制，为全面防内提供了基础。

产品功能如下表：

适用范围	功能要求	产品功能
计算环境	用户身份鉴别	基于 USB-Key 的双因子增强身份认证。
	自主访问控制	提供私有目录保护。
	标记与强制访问控制	主、客体的全程标记；基于 BLP 和 BIBA 相结合的二维标识模型的强制访问控制机制。访问控制主体类型包括用户、进程；客体类型包括文件、程序、外部设备；操作类型包括打开、读、写、执行、改名、删除等。
	系统安全审计	审计信息包括主体、客体、操作、成功与否等。审计事件包括用户对文件的访问、对网络的访问、对移动存储设备的访问等。
	系统完整性保护	通过可执行代码的完整性和一致性度量保护系统完整性不被破坏。
	数据完整性保护	依据 BIBA 模型保护用户数据完整性。
	数据保密性保护	重要文件透明加解密保护、移动存储设备加密保护。
	客体安全重用	信息在使用后被完全清除，实现对剩余信息的安全保护。
	可信代码防篡改	可执行代码的可信校验，实现可信代码防篡改。
	网络可信接入	防非法接入系统。

终端安全保护模块详细功能介绍如下：

### 4.3.1 双因子强身份认证

现有的终端操作系统采用口令认证方式对用户身份进行鉴别，容易受到字典攻击。在终端安全保护模块中，引入一个硬件 USB-KEY 令牌。该 USB-KEY 为用户身份的唯一标识，当用户登录系统时，需要插入 USB-KEY，然后系统对用户进行双因子身份认证，用户只有拥有合法的 USB-KEY，并且输入正确的操作系统口令+ USB-KEY 口令，才能登录终端系统。

登录成功后，如果用户需要临时外出，可以拔除 USB-KEY，这样安全内核会自动保存用户的工作环境，并且锁定终端桌面。除了持有原 USB-KEY 的用户外，任何人都不能进入终端环境。由此，终端安全保护模块实现了基于硬件 USB-KEY 的双因子身份认证，使得非授权用户无法进入终端环境。

### 4.3.2 自主访问控制

在现有操作系统中，如果用户以管理员身份登陆，则可以访问系统中的任何文件，用户很难保护自己的隐私。但是安装了终端安全保护模块后，用户可以拥有自己的文件保密柜，即设置自己的私有目录。安全内核使用用户的私有密钥加密保密柜中的文件，并且禁止本用户以外的其它用户访问保密柜中的文件，从而有效地保护了用户的私有信息。

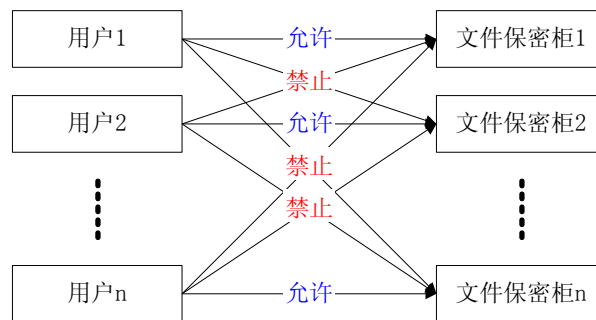


图 4.3.2 文件保密柜示意图

### 4.3.3 基于标记的强制访问控制

终端安全保护模块提供了强制访问控制机制，通过对执行程序的强制访问控制、对信息资源的强制访问控制、对移动设备的强制访问控制等机制实现对应用进行安全“隔离”。该机制由统一安全管理平台对终端系统中的主体（用户、进程）及客体（文件、执行程序、外部设备等）进行安全标识，根据客体类型的不同，分别制定了不同的访问控制规则，严格控制用户行为，保证用户的任何行为都在安全策略的支撑下，从而全方位地确保终端中的重要数据的“拿不走”，保护终端系统的机密性。

### 4.3.4 数据完整性保护

终端安全保护模块允许用户或进程以不同访问权限对文件/目录设置强制访问控制规则，在不改变原有终端文件系统格式的基础上，通过全路径名对终端系统中的重要客体进行标记。安全内核启动时，将策略加载到内存中，这样内存中就维护了一张终端系统重要客体的链表。安全内核截获应用层的访问请求后，查询链表中客体的保密性和完整性级别，实现强制访问控制。任何用户及其调用的进程对终端敏感文件或目录进行操作行为时都要进行严格的控制，杜绝用户数据被篡改、删除、插入等情况的发生，从而全方位地确保重要数据的完整性不被破坏。

### 4.3.5 硬盘信息加密保护

数据存储保护是防止信息泄露最有效的手段，终端安全保护模块支持对硬盘数据透明加解密、对移动存储介质透明加解密，达到了重要信息即使被盗取，信息盗取者也“看不懂”的效果。

所谓透明加解密是指该加解密过程对用户是透明的，这一过程在操作系统层实现，对上层应用透明，用户感觉不到它的存在。这一特性可以保证信息系统中的重要信息在存储和传播过程中都以密文的形式存在，即使意外断电，也不会导致明文信息的外泄。

在终端安全保护模块中，安全管理员可以根据客体的不同安全级制定不同的数据保护策略，方便信息系统和外界进行数据交换。

### 4.3.6 可执行代码控制

终端安全保护模块提供执行程序真实性和完整性度量功能。执行程序真实性度量可以确保系统中的执行程序都是合法的，从而阻止非授权程序的运行。执行程序完整性度量用来保证系统所启动的执行程序都是可信的，禁止不符合预期的程序的启动。执行程序启动前，终端安全保护模块中的核心模块会度量该程序相关模块的真实性和完整性，只有在度量结果和预存值一致的前提下，该程序才允许启动，否则拒绝其执行。因此即使系统中的某一执行程序被病毒或木马感染，由于其不再可信，终端安全保护模块将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了终端操作系统完整性被破坏的风险。正是由于上述安全机制，终端安全保护模块实现了终端对于病毒、木马、攻击程序等恶意代码自免疫。

### 4.3.7 网络访问控制

终端安全保护模块增强了操作系统的网络访问控制能力，通过对终端平台的身份认证和对网络出站的访问控制，达到对接入和外联的控制，实现对应用环境边界的保护，能够防止非法终端接入内部网络，限制内部用户访问网络的权限。

#### ➤ 非法内联控制

在常见的非法内联控制系统中，使用的是“发现+阻断”的控制技术，往往存在漏发现和阻断延迟问题，特别是在入侵终端开启了个人防火墙或采取静默接入方式时，系统往往不能发现非法接入终端。

在终端安全保护模块中，安全管理员规定那个终端可以接入系统，终端运行状态满足什么样的条

件后才能接入系统。因此在终端尝试接入系统时，安全内核检查该终端的平台身份和安全状态，只有检验通过后，终端方能接入网络与其他终端进行网络通信，否则它无法使用任何网络资源。

### ➤ 非法外联控制

目前，我国主管部门规定重要信息系统必须和其他公共网络进行物理隔离，但是在实际信息系统中，恶意用户仍可以通过拨号、内外网切换等方式避开这一管理规定，连接公共网络，将重要信息泄露出去，从而对整个信息系统安全造成威胁。

终端安全保护模块可以在操作系统层对网络协议栈进行监控和过滤，禁止任何试图连接公共网络的操作，能够对用户访问 URL、IP 地址进行限制，同时能够限制执行程序访问网络的行为，确保用户无法连接到公共网上，从而在操作系统层实现了真正的物理隔离。

## 4.3.8 移动介质权限管理

终端安全保护模块对于移动介质进行严格的控制，所有移动介质在使用之前都需经过授权，未经授权的移动介质一律禁止其使用。对于已授权的移动介质进行标记管理，对其使用行为进行全程的严格控制，从而防止通过移动介质非法拷贝敏感信息等恶意事件的发生。

## 4.3.9 移动介质加密保护

终端安全保护模块可对存放敏感数据的移动介质进行加密保护，只有合法的访问过程才具有解密的权利，从而防止通过移动介质泄露敏感信息事件的发生。加密保护采用透明加解密机制，加解密过程在合法的访问过程中自动执行，既保证了信息的机密性，又不影响正常操作。

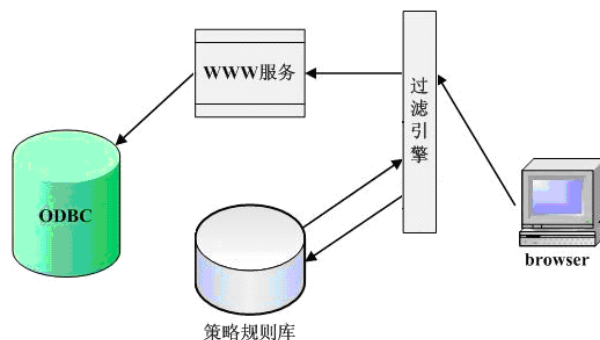
## 4.3.10 行为审计监控

终端安全保护模块监督终端系统中关于安全相关的行为，尤其是安全管理员对安全策略的制定、修改以及授权用户违反安全策略的行为，达到非法行为“赖不掉”的效果。具体包括：用户登录审计、文件访问审计、进程启动审计、网络访问审计等等。审计内容包括：平台、时间、用户、对象及操作结果等。

## 4.4 应用安全增强模块

应用安全增强模块完成 www 服务请求的安全检测和过滤功能。在用户的 http 请求被 www 服务解析之前，过滤引擎捕获该请求，并与策略规则库中进行特征匹配，如果确定该请求有攻击性质，则丢

弃该请求，否则给予放行。这样就可以有效防御诸如 SQL 注入攻击、跨站脚本攻击、CGI 等流行攻击等等。应用安全增强模块工作流程如下图所示：



图：应用安全增强模块工作流程示意图

应用安全增强模块功能如下：

#### 4.4.1 防 SQL 注入攻击

应用安全增强模块通过高效的 URL 过滤技术，截获包含 SQL 注入关键字的数据包，并将其丢弃，从而起到防 SQL 注入的效果。

#### 4.4.2 防跨站脚本攻击

利用数据包正则表达式匹配原理，应用安全增强模块会截获包含跨站攻击关键字的数据包，并将其丢弃，从而起到防跨站脚本攻击的效果。

#### 4.4.3 抗拒绝服务攻击

使用应用安全增强模块的速率限制和 TCP 连接数限制实现。

#### 4.4.4 防缓冲区溢出攻击

应用安全增强模块通过过滤 http 协议头长度，如果检测到超过系统所规定的长度，阻止该数据包通过，从而实现防缓冲区溢出攻击。

#### 4.4.5 防目录遍历

应用安全增强模块基于特征分析，检查用户提交的参数数据，如果检测到目录遍历的特征，及时发现和阻断该攻击。

#### 4.4.6 防网页盗链

应用安全增强模块会对指定的文件类型进行参考域的检查，有效阻止网页盗链攻击。

#### 4.4.7 防网络爬虫

应用安全增强模块在 http 头中过滤 reference 参数，如果含有 spinder、selected 等关键字，阻止该数据包通过，从而起到防网络爬虫攻击。

#### 4.4.8 轻量级 SSL 终止

如今，几乎所有的安全应用都使用 HTTPS 确保通信的保密性。然而，SSL 数据流采用了端到端加密，因而对被动探测器如入侵检测系统（IDS）产品来说是不透明的。为了阻止恶意流量，应用安全增强模块可以终止 SSL 安全连接，对数据流进行解码，以便检查明文格式是否含有恶意的流量。

#### 4.4.9 抗黑客扫描

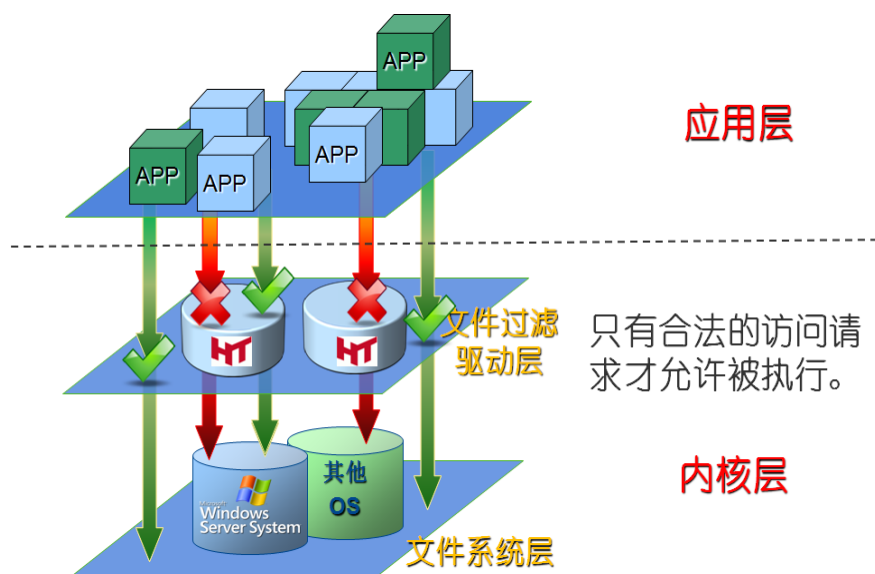
应用安全增强模块基于特征分析，及时发现并阻断黑客的恶意扫描行为，保护服务器敏感信息不被泄露。

## 5. HuaTech 应用安全防护系统技术特点

中软华泰公司推出的 HuaTech 应用安全防护系统为整个应用系统提供安全服务的基础性平台，为应用系统提供包括数据机密性、完整性、真实性、可用性和不可抵赖性在内的安全服务。有了这一基础设施，整个应用系统的安全策略便有了实现的保证。HuaTech 应用安全防护系统具有如下特点：

### 1) 采用内核性能优化和安全加固技术

对服务器的安全加固工作建立于操作系统文件过滤驱动层，由于文件过滤驱动工作在系统的核心层，因此既能准确全面的截获应用层的访问请求，又降低了系统安全机制被旁路的危险，这也为系统的安全模块自我保护，防卸载等构筑了坚固的防线。当操作系统中的磁盘驱动启动后安全防护模块驱动马上启动并对服务器系统实施保护，从而杜绝了旁路和隐通道，增强了安全性。系统中用户行为控制、重要资源保护、执行程序控制等安全手段都是从操作系统内核着手。安全模块随操作系统一起加载，安全布控时机早，可有效防止安全机制被旁路的可能。如下图所示：



图：先进的内核加固技术

同时本产品特有的与上层应用程序无关的安全设计除了为文件资源提供强制型存取控制、以及特权管理以外还能防止关键应用程序被篡改并且能为关键应用程序定制灵活的保护策略，做到“量体裁衣”。针对 HuaTech 终端安全保护系统（服务器加固）中的服务模块，采用多种内核性能优化技术，大大提高了 HuaTech 终端安全保护系统（服务器加固）的工作效率以及系统本身的健壮性。

### 2) 结合可信计算技术实现对执行程序的可信度量

结合可信计算技术，在操作系统、应用等程序代码运行控制转移过程中，对下一级可执行代码的真实性 and 完整性加以验证，通过可信链传递模式建立起一个安全可信的系统运行环境。系统通过执行

程序的真实性度量来判断执行程序是否是合法的；通过执行程序的完整性度量来判断授权程序是否是可信的，禁止不符合预期的程序的启动。即使系统中的某一执行程序被病毒感染，由于其不再可信，HuaTech 终端安全保护系统（服务器加固）将禁止其执行，从而阻止了恶意代码继续传播和破坏，降低了服务器系统完整性被破坏的风险。

### 3) 以强制访问控制为核心严格控制用户行为

在原有系统自主访问控制基础上，研发基于 BLP 模型与 BIBA 模型相结合的强制访问控制模型，通过对重要主体（用户、进程）及客体（程序、文件、移动介质）的安全标记，控制主体对于客体的访问权限，实施强制访问控制，严格控制用户行为。保证用户的任何行为都在安全策略的支撑下，使得用户登录服务器系统后，其权限受到安全策略的严格限制，不能为所欲为。

### 4) 基于硬件的系统层加解密技术

通过 USB-KEY 进行加解密，既具备了类似 TPM 功能模块加解密的优势：加密速度快、占用计算机资源少、安全性高等，又无需对现有计算机体系结构进行改造。

在服务器操作系统层实现的加密技术，文档从产生的第一时刻就是自动加密的，避免用户在编写过程中有意或无意地留下明文，且信息被黑客等非法窃取后，由于缺少解密容器，获取者只能得到密文，从而确保了数据的保密性不被破坏。



## 6. HuaTech 应用安全防护系统产品优势

### 1) 先进的设计理念

以应用安全、数据安全、管理安全为核心。随着计算机和网络信息技术的发展，基于单机的应用已不能满足应用需求，越来越多的应用已发展成基于 B/S 或 C/S 模式的网络应用，这时候数据便成为应用的核心，数据安全也就成为核心中的核心。因此，HuaTech 应用安全防护系统从保障单个操作系统安全，转变为支撑整个应用系统的安全，更重要的是保障应用系统中数据的应用、存储安全。确保信息在应用过程中，既不会被非法窃取，又不会遭到病毒等的恶意篡改。

结合可信计算技术。HuaTech 应用安全防护系统通过结合可信计算技术，以可信密码模块为基础，通过可信计算模块提供的服务，来构建可信计算的密码支撑平台，变被动防御为主动防御，通过身份认证、可信度量、数据密封等技术，最终在整个平台中形成了可以有效防御恶意攻击的安全体系。

### 2) 先进的管理体系

三权分立的管理模式。HuaTech 应用安全防护系统对系统管理员、安全管理员和安全审计员的权限进行严格的分配和管理，授予其各自完成自己承担任务所需的最小权限，三个管理员之间既相互制约又相互联系，从而防止“超级用户”的形成。通过三权分立的管理体系，为应用系统设置“保卫部”、“保密室”和“监控中心”，实现对整个应用系统的统一管理。

### 3) 对应用系统中终端/服务器统一管控，构建整体安全防线

构造终端/服务器统一管控的管理体系。信息安全具有“短板效应”，任何一个终端/服务器的安全漏洞都可能对整个应用系统的安全造成威胁。HuaTech 应用安全防护系统构建全系统统一的“安全管理中心”，对系统中的所有终端/服务器进行统一管理、统一配置，审计信息统一存储、统一分析，消除了各个终端/服务器由于配置不同造成的安全隐患，最终构建一道针对整个应用系统的整体安全防线，有效保护应用系统及应用系统中的信息安全。

### 4) 恶意代码自免疫

通过可信度量技术，HuaTech 应用安全防护系统赋予了应用系统对恶意代码的主动防御的能力，使得应用系统做到了对已知/未知病毒、木马、攻击程序等恶意代码的自免疫，从而有效替代或配合传统的病毒查杀类产品。

## 5) 应用的安全隔离及透明的应用支撑

HuaTech 应用安全防护系统通过对执行程序的强制访问控制、对用户行为的强制访问控制、对网络访问的强制访问控制、对文件系统的强制访问控制，达到对应用进行“安全隔离”的效果。

HuaTech 应用安全防护系统兼容现有系统的全部应用。现有操作系统的应用多种多样，HuaTech 应用安全防护系统在对大量应用的细致分析的基础上，得到应用系统运行的一般规律，通过与应用无关的透明支撑设计，使得产品能兼容现有系统的全部应用，且不影响原有应用系统的效率。

不改变现有应用。HuaTech 应用安全防护系统部署后，无需改变现有应用的应用模式、网络部署等，通过透明支撑，既使得用户在原有应用中感觉不到安全操作系统的存在，又实现了对应用的安全保护。

## 6) 优化的加解密机制

HuaTech 应用安全防护系统采用基于硬件的透明加解密，占用系统资源少，安全性高，加解密动作对用户及应用透明。

## 7) 足够的安全强度

HuaTech 应用安全防护系统采用内核级的安全机制，系统的访问控制等安全机制均在操作系统核心层实现，采用文件过滤驱动技术，安全布控时机早，降低安全机制被旁路的危险，有效防止安全模块被恶意篡改或卸载。

## 版权声明

本手册的所有内容，其版权属于北京中软华泰信息技术有限责任公司（以下简称中软华泰）所有，未经中软华泰许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，中软华泰恕不承担另行通知之义务。

版权所有 不得翻印©2000-2010 中软华泰公司

### 公司联系方式：

用户可以通过如下的联系方式详细了解该产品：

北京中软华泰信息技术有限责任公司

- 地 址：北京市海淀区远大路1号金源时代商务中心B区写字楼705-706室
- 邮 编：100097
- 网址：<http://www.huatechsec.com.cn>
- 服务热线：010-62191614、62198781、62144177、62133838
- 传真：010-62133939

北京中软华泰信息技术有限责任公司上海分公司

- 地 址：上海市静安区延平路三和大厦E5层
- 邮编：200042
- 电 话：021-62462228、62462229

北京中软华泰信息技术有限责任公司南京分公司

- 地 址：南京市玄武区成贤街50号成贤大厦308室
- 邮编：210018
- 电 话：025-83699268

北京中软华泰信息技术有限责任公司西安分公司

- 地 址：陕西省西安市高新区高新一路25号创新大厦F7室
- 邮编：710075
- 电 话：029-88839373

深圳中软华泰信息技术有限责任公司

- 地 址：深圳市福田区八卦一路鹏基商务时空大厦 2408-2409A
- 邮编：518029
- 网 址：www.szhuatechsec.cn
- 电 话：0755-22200019、0755-22200026

北京中软华泰信息技术有限责任公司天津分公司

- 地 址：天津市华苑产业园区华天道海泰信息广场 D 座 601 室
- 邮编：300384
- 电 话：022-83716303, 83711786, 83718234

北京中软华泰信息技术有限责任公司武汉办事处

- 地 址：武汉市洪山区雄楚大道 229 号春林庭苑 C-1702
- 邮编：430070
- 电 话：027-87397339

北京中软华泰信息技术有限责任公司东北办事处

- 地 址：吉林省长春市亚泰大街繁荣路东南阳光小区 5 号楼 3 门 406
- 邮 编：130000
- 电 话：0431-85332050

北京中软华泰信息技术有限责任公司贵州办事处

- 地 址：贵阳市延安中路 1 号振华科技大厦 24 层 A-B 座
- 邮 编：550001
- 电 话：0851-6907223