广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):350~352
Vol. 23,No. 4 November 2007

基于动态安全保护技术的内部信息安全系统
The Internal Information Security System Based on Dynamic Protecting Technology

杨丽芳[1],邢海韬[2],庞 辉[3],李 玥[1]
YANG Li-fang[1],XING Hai-tao[2],PANG Hui[3],LI Yue[1]

(1.广西计算中心,广西南宁 530022;2.广西柳工机械股份有限公司,广西柳州 545007;3.南宁市公安局交通警察支队,广西南宁 530028)
(1. Computing Center of Guangxi, Nanning, Guangxi, 530022, China; 2. Guangxi Liugong Machinery Co., Ltd, Liuzhou, Guangxi, 545007, China; 3. The Traffic Police Department of Nanning, Nanning, Guangxi, 530028, China)

摘要:从大规模多网络环境的特点出发,采用实时透明加解密技术、通讯认证技术和加解密算法,设计基于动态安全保护技术的内部信息安全系统。系统主要由管理中心和终端用户两个部分构成,能够对电子文档进行全过程的保护,避免电子文档/技术资料可能从各种非法途径流失并为竞争对手有效使用的潜在风险,充分保护了企业的核心技术机密。

关键词:网络安全 内部信息 多网络协同环境
中图法分类号:TP309.2 **文献标识码**:A **文章编号**:1002-7378(2007)04-0350-03

Abstract: The internal information security system based on dynamic protecting technology is designed via the real time and transparent addition decipher technology, communication authentication technology and addition decipher algorithm. The system, made up of administrative center and terminals, can protect the electronic documents from illegal use and the enterprises' core techniques.

Key words: network security, internal information, multi-network cooperative environment

众所周知,电子文档极易复制且复制后不留任何痕迹。目前随着电子政务、电子商务的深入开展,无纸办公、MIS、ERP等系统也在政府及企业广泛应用,利用网络发布、传递信息的个人和企业数量更是日益增长。但是,人们议论到信息安全时,往往首先想到的是外部攻击,关注到的是防火墙、入侵检测、内网和外网物理隔离等技术,内部信息泄露往往得不到应有的重视。实际上,内部信息泄露造成的危害也是相当巨大的。CSI/FBI统计2005年各种安全漏洞造成的损失中,30%~40%是由于电子文件的泄露造成的;而Fortune排名前1 000家的公司中,每次电子文件泄露所造成的损失平均是500 000美元。媒体报道的信息安全事件,通常只占到所有安全事件的20%~30%,还有70%~80%来自于内部信息的安全事件被忽略[1]。内部信息从政府文件、企业工程图纸、标准操作程序到销售展示,有的文档具有非常高的机密性,一旦泄露将很可能会造成严重后果。内部信息安全和电子文档保护问题已经日益严峻。

随着内部人员威胁的加剧,内部人员犯罪已经体现出了"危害大、难抵御、难发现"的特点。内部人员最容易接触敏感信息,并且他们的行动非常具有针对性,危害的往往是机构最核心的数据、资源等。一般说来,各机构的信息安全保护措施都是防外不防内,比如很多公司赖以保障其安全的防火墙对内部人员攻击毫无作用,形同虚设。内部人员对一个机构的运作、结构、文化等情况非常熟悉,导致他们行动时不易被发觉,事后难以被发现。此外,由于员工群体信息安全意识的淡薄或者由于管理方面的疏漏,员工无意间违反规定将组织内部的电子形态文

收稿日期:2007-09-29
修回日期:2007-10-23
作者简介:杨丽芳(1973-),女,经济师,主要从事项目管理、应用软件和电子商务研究。

件资料很方便地通过网络或者各种存储载体随意向组织外部传递的事情也会时有发生,这些防不胜防的事件或现象,都使得网络化协同工作环境下组织机构的信息安全变得极为脆弱[2,3]。

在此背景下,一方面是网络时代的组织机构极度需要能够防范网络环境信息泄漏的安全产品支撑,另一方面是这一类产品的供给目前在市场上仍然处于空白状态,要解决基于内部信息安全需求的问题,我们设计并研发了这个基于动态安全保护技术的内部信息安全系统(以下简称:动态安全保护系统),并成功地在广西柳工机械股份有限公司及其子公司应用。

1 动态安全保护系统的结构

动态安全保护系统的系统结构如图 1 所示。

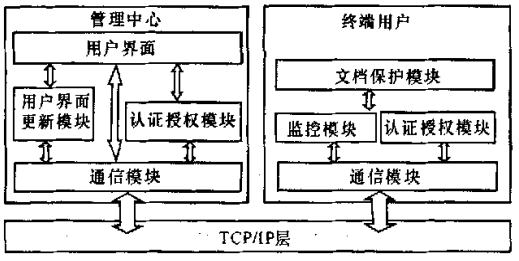

图 1 动态安全保护系统的结构

从图 1 可以看出,Infoguard 电子文档保护系统由两个部分构成:管理中心和终端用户。管理中心的主要作用是提供终端用户的认证、授权等功能,其主要包括通信模块、认证授权模块、用户界面更新模块、用户界面等;终端用户的主要作用是根据管理中心的授权在客户机上提供电子文档保护的功能,主要包括通信模块、认证授权模块、文档保护模块等。

2 系统的功能

动态安全保护系统的功能主要分为管理中心和终端用户两大模块的不同功能。

管理中心各模块的功能如下:(1)通信模块的主要作用是接收和发送信息,根据需要调用认证模块进行认证,将接收到信息传给用户界面更新模块更新用户界面,根据用户界面的要求发送消息。(2)认证授权模块的主要作用是对登陆的终端进行认证和对申请外出的终端进行审批。(3)用户界面更新模块的主要作用是根据通信模块接收的消息实时更新用户界面。(4)用户界面的主要作用是通过各种管理接口,如授权、添加、删除、更新终端等。

终端用户各模块的功能如下:(1)通信模块的主要作用是接收和发送消息,根据需要调用认证模块进行认证等。(2)监控模块的主要作用是根据系统的规定控制文档保护模块的运行。(3)认证授权模块的主要作用是认证管理中心是否为规定的服务端,根据服务端的授权使用监控模块控制文档保护模块的运行。(4)文档保护模块的主要作用是负责对规定类型文档进行保护。

从用户体验的角度出发,为了使用户能够更好的使用该系统而不至于影响工作的正常进行,为此我们还为系统设计了辅助性的用户离线申请和解密申请等功能和用户解密申请功能。用户的离线申请功能,使用户可以通过简单的界面来进行离线的申请与回复,让笔记本或有移动办公需要的用户的工作既受到该安全系统的保护又不会使用户无法移动办公;用户解密申请功能可以提供用户在需要对外发送文件的时候快速解密文件的通道,但是该通道也是受到系统监控的,可以保证用户不能随意发送并非正常批准的文档,所发的文档也会被系统记录下来[4,5]。

3 动态安全保护系统的关键技术

动态安全保护既要能够适应大型和多网络环境下的协同工作特点,又要能够保护电子文档,避免电子文档/技术资料可能从各种非法途径流失并为竞争对手有效使用的潜在风险,充分保护企业的核心技术机密。因此,我们采用 3 个主要的关键技术来实现动态安全保护系统。

3.1 与用户无关的文件实时透明加解密技术

该项技术基于 Windows 内核层实现。所有新建、拷贝甚至通过网络传输获得的文档强制透明加密。对于安全规则运行的应用程序和文档,则可以透明在内存中解密供用户使用。

3.2 用户终端与管理中心之间的通讯认证技术

为了保证安全产品的自身安全性,系统还通过提取用户机器的一系列硬件指纹,结合当前用户 SID 等信息演算后得到硬件机器码,并以此为服务器/用户端的通讯认证凭据。

3.3 稳定高效的加解密算法

系统使用 AES 加密技术对内部信息进行加密。AES 是美国国家标准与技术研究所用于加密电子数据的规范。它已经能成为人们公认的加密包括金融、电信和政府数字信息的方法[6]。

4 动态安全保护系统的特性

动态安全保护系统能够有效地保护内部信息，具有较好的保护特性。

4.1 全程保障

文档保护的过程是从文档创建、传递直至销毁全过程完全控制。

4.2 介质无关

无论是通过存储(USB、光盘、软驱、ZIP盘等)或网络(Email、FTP、红外、蓝牙等)，均在保护范畴(介质无关的特性能够使用户不必为新的存储介质和传输协议/方式而被迫升级系统)

4.3 集中控制

通过集中控制台对每个客户端进行轮询和管理，有效保证电子文档既受保护，又能够灵活使用。

4.4 用户透明

客户端无界面、无进程、无端口，使用者完全无需更改原有电子文档使用习惯。这样可以使用户对产品在部署和安装的时候的抵触情绪降到最低[5]。

5 结束语

现在国内的内网信息安全产品主要有三类电子文档保护安全产品。第一类强调封堵各种可能的泄漏途径并作好监控，就像堵漏水桶一样哪里有可能泄漏的就对那里进行封堵，但封堵的效果总是有限的，且事后对违规行为的追查往往为时已晚，损失已经造成。这个以中软Water Box防水墙为代表。第二类强调对放入特定文件夹/位置的文件进行加密和保护，但是产品功效的发挥基于相关操作人员的诚实可靠，并自觉执行所有的规定。该类产品依然不能解决合法用户的无意识的错误操作或故意犯错的给企业带来的危害。这个以山丽防水墙数据防泄漏系统、亿赛通Cobra DocGuard为代表。第三类是防渗墙"Infoguard"系统，它的重点在于，在企业内部进行集中的安全域的管理和维护。系统在安全域内的成员在经过严格的身份认证后，无条件的对符合安全保护规则的文档进行动态加解密，同时将数据的保护实现了文件级的保护，从源头上就实现安全保护的基础。我们开发设计的动态安全保护系统从大规模多网络环境的特点出发，采用动态安全保护技术，实现电子文档全过程的保护。避免电子文档/技术资料可能从各种非法途径流失并为竞争对手有效使用的潜在风险，充分保护了企业的核心技术机密。

本系统在广西柳工机械股份有限公司及其子公司已经投入使用，并取得明显的效果，可以推广使用。

参考文献：

[1] CSI/FBI. Computer crime and security survey [EB/OL]. [2007-08-10]. http://duecare.biz/download/FBI2005.pdf.

[2] 黄志晖. 计算机网络管理与维护全攻略[M]. 西安：西安电子科技大学出版社，2004.

[3] SEAN CONVERY. 网络安全体系结构[M]. 北京：人民邮电出版社，2005.

[4] STEVEN SPLAINE. Web安全测试[M]. 北京：机械工业出版社，2003.

[5] 萨师煊. 中文版SQL Server 2000开发与管理应用实例[M]. 北京：高等教育出版社，2002.

[6] ATUL KAHATE. 密码学与网络安全[M]. 北京：清华大学出版社，2005.

(责任编辑：邓大玉)

美国物理学家研制出电离天线

当电流在金属内部激荡时，一根金属天线便会发射无线电波。对于军事和其他用途而言，这一具有百年历史的"老"技术存在体积大、易暴露、易受到干扰或抑制3个缺点。美国诺克斯维尔市田纳西大学的物理学家Igor Alexeff报告说，他们研制出一种新型天线。这种天线能够抗干扰，并且只消耗很少的电量，所需能量只为普通金属天线的1/1000。同时能够以很小的体积在各种频率下工作。这种装置用一种充满电离气体的管子代替传统金属实现无线电波的吸收和播送功能。Alexeff表示，这种新型天线非常适合军事用途，并且在移动电话网络中也将大显身手。

Alexeff的合作者Theodore Anderson解释说，这种天线与金属天线的工作原理一致，唯一区别在于电流是在电离气体中移动。Anderson指出，这种装置只会对等于或低于工作频率的信号作出响应，因此通常用来实施干扰的所谓高频信号很难对其产生影响。这种天线同时还能够被内置于其他天线中，进而在多种无线电频率下工作而不会互相干扰。而在关闭等离子体天线后，它们并不会反射雷达信号，从而保证其在军事应用中不被暴露。

(据科学网)