一种分布式网站安全防护系统①

薛　辉[1]，邓　军[2]，叶柏龙[3,4]

[1](湖南涉外经济学院，长沙 410205)
[2](湖南科技职业学院，长沙 410004)
[3](中南大学，长沙 410083)
[4](湖南创博龙智信息科技股份有限公司，长沙 410205)

摘　要：为了及时、高效地阻止黑客对网页文件的篡改，并对被篡改的页面文件进行及时修复还原，提出了一种分布式“过滤驱动技术＋事件触发技术+核心内嵌技术”架构的网站安全防护系统。事件触发技术负责自动实时监测，若有网页被篡改，通过过滤驱动技术和核心内嵌技术立即删除被篡改网页，停止 Web 服务。与传统的网页防篡改产品相比，系统可以对网页的非法篡改做出更为敏捷快速的反应，对系统资源占用更少。同时兼容其他安全产品，形成深度防护体系，最大限度地保障受保护网站的安全。

关键词：事件触发；核心内嵌；过滤驱动；密码水印；网页篡改

Distributed Site Security Protection System

XUE Hui[1], DENG Jun[2], YE Bai-Long[3,4]

[1](Hunan International Economics University, Changsha 410205, China)
[2](Hunan Vocational College of Science and Technology, Changsha 410004, China)
[3](Central South University, Changsha 410083, China)
[4](Hunan BLRise Information Technology Co. Ltd, Changsha 410205, China)

Abstact: In order to timely and efficient manner to prevent tampering hacking of web documents, and tampering of documents and timely repair to restore the page, a distributed " filter driver technology + event trigger technology + core embedded technology " the website security protection system.Events responsible for triggering automatic real-time monitoring, if the page is altered, by filtering the core drive technology and embedded technology has been tampered page deleted immediately, stop the Web service. Tamper with the traditional web products, the system can make a web of illegal tampering more agile rapid reaction, taking up less system resources. Compatible with other security products, the formation of the depth of protection system to maximize the protection of the safety of the protected sites.

Key words: event trigger; core embedded; filter driver; password watermark; pages tampering

1　引言

目前随着互联网的迅速发展和广泛应用，网站在我国已经渗透到了各个角落，根据中国互联网络信息中心（CNNIC）调查报告显示，截至 2011 年 6 月底，中国大陆网民人数高达 4.85 亿，已大幅超越美国跃居世界第一位[1]。庞大的网民数量和网站群为互联网应用的快速发展奠定了良好的基础。但是网络安全问题仍然很严重，网络攻击现象尤为普遍。已经成为危害最为严重的网络安全问题。经过调查发现：目前，传统的大多数企事业网站通常采用防火墙、入侵检测/漏洞扫描等技术作为网站边界的防护，但是这些主要是针对链路层、网络层信息进行威胁识别，防范效果不甚理想，无法全面对网络入侵攻击事件进行阻断、记录、统计、分析。

为了及时、高效地阻止黑客对网页文件的篡改，并对被篡改的页面文件进行及时修复还原，本文采用

① 收稿时间:2011-08-08;收到修改稿时间:2011-09-08

业界领先的第三代文件过滤驱动技术＋事件触发技术并利用核心内嵌技术。具有实时自动恢复被篡改网页、不增加网站主机负载的特点。

2 系统分析

2.1 原理分析

目前新兴的网页防篡改技术不断出现，目前比较有代表性的技术主要有三个：一是外挂轮询技术，利用一个网页检测程序,以轮询方式读出要监控的网页,与真实网页相比较,来判断网页内容的完整性,对被篡改的网页进行报警和恢复，但该技术无法阻止公众访问到被篡改网页，它只能在被篡改后一段时间发现和进行恢复，因此公众有很大可能访问到被篡改网页。二是核心内嵌技术，将篡改检测模块内嵌在 WEB 服务器软件里,它在每一个网页流出时都进行完整性检查,对于篡改网页进行实时访问阻断,并予以报警和恢复。三是事件触发技术，利用操作系统的文件系统接口,在网页文件被修改时进行合法性检查,对于非法操作进行报警和恢复[2]。

本文采用的文件过滤驱动技术最初应用于军方和保密系统，作为文件保护技术和各类审计技术,在网页防篡改技术革新历程中,与事件触发技术结合,形成了今天的第三代网页防篡改技术。

系统原理是：将篡改监测核心程序通过微软文件底层驱动技术应用到 Web 服务器中,通过事件触发方式进行自动监测,对文件夹的所有文件内容,经过内置单项散列快速算法生成文件属性,对照其底层文件属性,进行实时监测，若发现文件属性变更，即有网页被篡改，立即删除被篡改网页,停止 Web 服务,同时通过非协议方和纯文件安全拷贝将备份路径文件夹内容拷贝到监测文件夹相应文件位置;通过底层文件驱动技术,整个文件复制过程为毫秒级，使得公众无法看到被篡改页面，其运行性能和监测实时性都达到极高的标准[3]。网页防篡改模块采用 Web 服务器底层文件过滤驱动保护技术,与操作系统紧密结合。这样做不仅完全可以杜绝轮询扫描式网页防篡改技术在扫描间隔中篡改内容被用户访问的可能,其所消耗的内存和 CPU 占用率也远远低于文件轮询扫描技术和核心内嵌式技术，可以说是一种简单、高效、安全性极高的一种网页防篡改技术。

采用文件过滤驱动和事件触发技术不仅可以实时地监测网页属性的变动情况,而且还能够对被篡改网页文件进行及时的删除,同时进行修复还原,还可以对 Web 访问者实施访问过滤监测,以实现 Web 服务器网页内容正常的更新管理和对其他异常事件的处理。从而对系统服务器实施自动监测网页、及时处理事故、安全管理操作，提高系统的防护能力。

2.2 系统关键技术分析

(1) 实时阻断技术，本系统采用实时阻断技术，特点在于可用阻断对受保护网页的非法操作，有效甄别合法进程和非法进程，阻断非法进程对网页的篡改，将非法进程直接挡于门外。

(2) 事件触发技术，安全防护系统具备触发式篡改检验引擎，针对受保护网站文件的增删改操作，一触即发，能校验修改的合法性，瞬间清除被非法篡改的网页，实时恢复正确网页[3]。事件触发技术一个最突出的特点就是确保任何时候网站文件的合法性。

(3) 密码水印技术，即核心内嵌技术，安全防护系统内嵌式篡改检测引擎运行于 Web 服务器内部，与 Web 服务器无缝结合。安全防护系统检测每一个 Web 请求访问的页面，一旦有黑客程序绕过操作系统级别，对网页文件进行了修改，系统控制网页的发布，当用户请求访问网页文件，系统将网页文件的水印与中心数据库文件的水印进行比较，如发现不能匹配，即中止响应，并恢复被篡改的文件[4]。

(4) 系统级的文件驱动技术，主要用来控制网页文件的文件目录,一旦文件目录下的文件发生非法进程进行新建、修改、删除，系统立即进行保护，禁止非法进程操作文件目录及文件[5]。

所以，可以说本系统是第三代文件过滤驱动技术＋事件触发技术和核心内嵌技术的综合利用，取长补短，具有较高的创新性和实用性。

3 系统实现

从系统实现的角度来看，本系统采用 3 个层次、3 个核心模块来实现，系统体系架构如图 1 所示，下面分别进行论述。

从层次结构上看，本系统分为 3 个层次来实现：

(1) 系统监控层

是本系统的核心层，该层设计一个监控模块，其实可以说是一个子系统，该层主要负责实时监测，完全杜绝被篡改内容被外界浏览。

(2) 数据存储层

该层设计中心数据库和中心服务器以及 Web 服务器 3 类，主要用于保存电子水印、加密数据、网页文件及文件目录，对系统监控层提供依据和凭证，对更新发布层负责保存生成电子水印，并对其采用加密方式后通过 TCP/IP 协议传输到中心数据库。

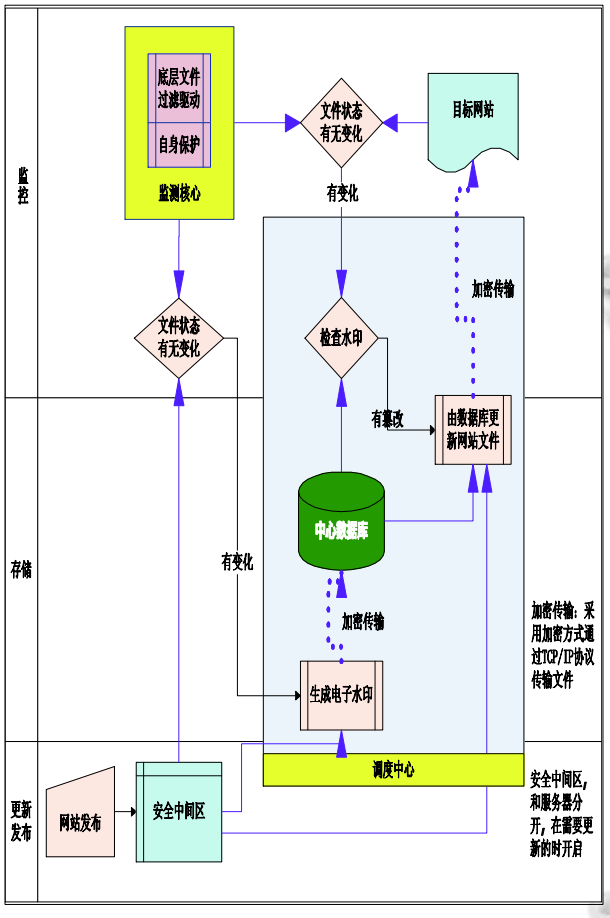

图 1　网站安全防护体系架构图

3.1 系统层次架构实现

(3) 系统发布层

该层属于事后恢复，当用户请求访问网页文件，系统将网页文件的水印与中心数据库文件的水印进行比较，如发现不能匹配，即中止响应，并恢复被篡改的文件。

3.2 系统模块实现

从模块结构来看，3 个核心模块可实现本系统的主体功能，这些模块根据层次的划分而分解为多个子模块，每个子模块根据其特点划分到系统的不同层次，3 个核心模块的功能如下：

(1) 系统防篡改监测核心模块

是系统的核心模块，该模块通过微软文件底层驱动技术应用到 Web 服务器中，通过事件触发方式进行自动监测，对文件夹的所有文件内容，对照其底层文件属性，经过内置散列快速算法，实时进行监测，若发现文件的状态属性发生变更，通过非协议方式，纯文件安全拷贝方式将备份路径文件夹内容拷贝到监测文件夹相应文件位置，通过底层文件驱动技术，整个文件复制过程毫秒级，使得公众无法看到被篡改页面，其运行性能和检测实时性都达到较高的水准。此外，该模块采用 Web 服务器底层文件过滤驱动级保护技术，与操作系统紧密结合，所监测的文件类型不限，可以是一个 html 文件也可以是一段动态代码，执行准确率高。这样做不仅完全杜绝了轮询扫描式页面防篡改软件的扫描间隔中被篡改内容被用户访问的可能，其所消耗的内存和 CPU 占用率也远远低于文件轮询扫描式或核心内嵌式的同类软件。可以说是一种简单、高效、安全性又极高的一种防篡改技术。

(2) 中心调度模块

本模块主要设计中心数据库和中心服务器以及 Web 服务器 3 类，中心服务器是网页防篡改控制中心，各种防护技术和机制都部署在其中，负责网站的实时检测、文件及文件夹防篡改的保护等。支持多级目录文件夹内容篡改保护；支持异地文件同步功能，异地目录保护恢复功能等。与中心数据库结合，支持备份可信端安全保护和大规模虚拟机、热备网站系统部署。在每台 Web 服务器上安装网页防篡改代理控制端，且在内网中架设一台网页防篡改服务器用于安装网页防篡改控制中心及同步备份系统， 这样对网站的更新、维护仅通过 Web 服务器来完成。亦可参看系统部署如图 2。

(3) 系统更新发布模块

位于系统发布层，由发布服务器负责电子水印的生成，经过加密传输到中心数据库，同时判断系统检测模块文件的变化状态，为中心服务器提供决策支持。中心服务器根据电子水印查验是否有篡改行为，立即中止响应，并恢复被篡改的文件。发布服务器置于安全中间区，和中心服务器分开，在需要更新是开启。

3.3 系统部署

系统部署如图 2 所示，系统分为发布和防篡改监控两部分。

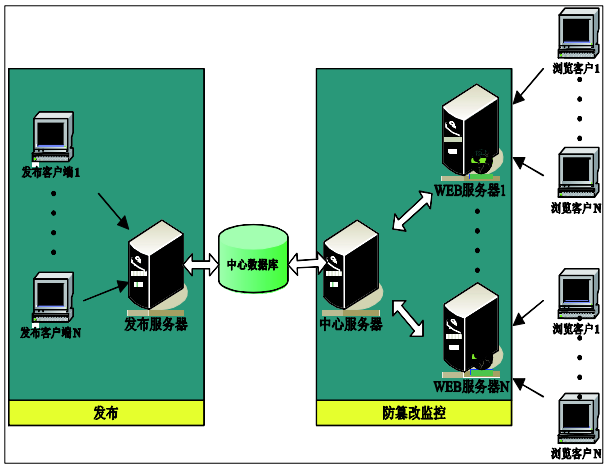

图 2 系统部署图

防篡改监控：这部分属于实时阻断，部署在中心服务器，一旦部署网页文件的文件目录或文件有非法进程进行更改，系统立即进行阻止。

发布: 这部分属于事后恢复，部署在发布服务器，当用户请求访问网页文件，系统将网页文件的水印与中心数据库文件的水印进行比较，如发现不能匹配，即中止响应，并恢复被篡改的文件。

通过对系统的层次、模块和部署三个维度的分析和设计形成了本系统的完整实现思路，本系统作为一种在线部署的产品，其目标不仅仅在于能够精确识别各种网页篡改方式，而且在不影响正常业务流量的前提下，使得公众无法看到被篡改页面，实施实时阻断，其运行性能和检测实时性都达到较高的水准，为用户提供较全面的安全检测与防御。

4 结语

本系统是在响应国家“信息安全”产品产业化专项基金的要求下，旨在研发出一种能自动采取行动阻止非法篡改和入侵。通过部署该防护系统，同时与防火墙、入侵检测等方式，形成深度防御体系。与传统的网页防篡改产品相比，本系统可以对网页的非法篡改做出更全面、更敏捷快速的反应，同时对系统资源占用更少的特点，最大限度地保护企业和组织的网络安全。目前本系统已经通过国家发改委验收，并成功在 PowerSEC 高性能监控一体化网络安全平台上，实践证明该系统具有极大的研究价值、开发价值和市场前景。然而，网站防护现在还处于不断完善的过程，“三分技术、七分管理”，在管理上还需要加强对技术设备的日常管理以及制定出网站安全的相关安全管理制度，并在日常工作中加以培训、落实，从思想真正提高重视，这样才能够有效地做好网站安全的防护工作。

参考文献

1 CNCERT/CC.中国互联网网络安全报告(2011 上半年)北京:国家计算机网络应急技术处理协调中心,2011.
2 张岸,张毅东.政府网站安全防护解决方案研究.情报探索,2010,(11):84–86.
3 范建华,宋云波.基于文件过滤驱动和事件触发的网页防篡改机制.重庆工学院学报,2009,23(12):65–70.
4 张迎春.基于三层过滤的分布式网页防篡改系统.济南:山东大学,2007.
5 符广全,王海峰.基于文件过滤驱动的内核病毒防火墙技术.计算机应用与软件,2006,(7):21–23.

（上接第 150 页）

应用.软件学报,2001,12(1):117–125.
3 石波,卢秀山,陈允芳.基于 kd-tree 的建筑物散乱点云平面分割.测绘科学,2008,33(1):135–136.
4 王世东,陈杨,张本福,孙光灵,黄晓梅.八叉树在三维建模中的应用.安徽建筑工业学院学报(自然科学版),2006,14(6):96–98.
5 胡斌,江南,邹志强,邵华,王鹏.大规模室外动态场景调度机制研究.地球信息科学,2007,9(5):8–13.
6 郭景,雷鸣.3DS MAX 模型在 OPENGL 中的读取与重现.计算机应用,2002,(5):46–49.
7 Lewiner T, Mello V, Peixoto A, Pesco S, Lopes H. Fast Generation of Pointerless Octree Duals. Computer Graphics Forum, 2010,29(5):1661–1669.
8 刘琪,迟贤书.OpenGL 与 OpenGL ES 在开发过程中的异同.辽宁工程技术大学学报,2008,27(2):261–262.
9 Astle D, Durnil D. OpenGL ES Game Development. Course Technology PTR, 2004:35–45.