第 33 卷 第 12 期 计 算 机 工 程 2007 年 6 月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0166—03 文献标识码：A 中图分类号：TP393

Linux 平台下动态网页保护系统的设计与实现

袁 丹，张玉清
(中国科学院研究生院国家计算机网络入侵防范中心，北京 100043)

摘 要：在 Linux 平台下设计并开发了一种基于 MySQL 数据库的动态网页保护系统。该系统对动态网站中的网页脚本文件和后端数据库进行有效监控和保护，并采用异机备份机制，可及时恢复受损网页文件和数据库。动态网页保护系统为动态网站安全提供了重要的保障。
关键词：动态网页保护；MySQL 数据库；网页脚本文件保护；备份与恢复

Design and Implementation of Dynamic Webpage Protection System Based on Linux Platform

YUAN Dan, ZHANG Yuqing
(National Computer Network Intrusion Protection Center, Graduate School of Chinese Academy of Sciences, Beijing 100043)

【Abstract】 A dynamic Webpage protection system based on MySQL is designed and implemented. Both the Webpage files and the databases can be monitored and protected effectively, and the mechanism of different-machine backup makes sure that they can be restored in real time once they are juggled illegally. So the system can be applied to ensure the security of dynamic websites.
【Key words】 Dynamic Web page protection; MySQL database; Script files protection; Backup and restore

网络安全是现今社会的一个严重问题，根据国家应急相应中心(CNCERT/CC)事件处理 2005 年 10 月统计报表显示，网页篡改事件居网络安全事件之首。同时，随着人们对网站功能需求的不断扩大，各种动态网页已经在Web应用中占有支配地位，而对动态网页保护技术的研究还较少[1]。在如此严峻的形势下，建立一套安全的动态网页保护系统显得尤为迫切和重要。

动态网页包括网页脚本文件和数据库，其中对网页脚本文件的修改主要归因于服务器自身的安全缺陷；对数据库(这里使用 MySQL)的修改主要是因为 MySQL 数据库的安全配置较差以及程序漏洞导致被溢出等原因。通过安全评估、防火墙、入侵检测等工具配合可以在一定程度上保护网站的安全，但是黑客一旦突破这些屏障而对网页数据进行篡改，上述策略就无能为力了。作为网站的最后一道防护关卡，动态网页保护系统的主要作用就是及时进行灾难拯救，使动态网站具有可生存性。因此，动态网页保护系统可从功能上描述为及时发现对网页脚本文件和数据库的非法篡改并在第一时间做出合理响应。

目前多数动态网页保护研究所针对的数据库多为Windows平台下的SQL Server[2]，因此，如何保证Linux平台下Web网站内容的完整性、正确性和合法性，是本文所要研究的内容。基于此目的，本文以MySQL为基本构架，设计并实现一个能够对动态网站进行有效保护的相对安全的动态网页保护系统。

1 动态网页保护总体设计与实现

本系统中采用 3 层的 B/S 结构，这样用户只要装有普通的浏览器就可以实现远程监控；并且 B/S 模式在客户机和服务器之间增加了一层 Web 服务器，使两者不再相连，可有效地防止用户的非法入侵。

1.1 系统结构

动态网页保护系统的系统结构如图 1 所示。

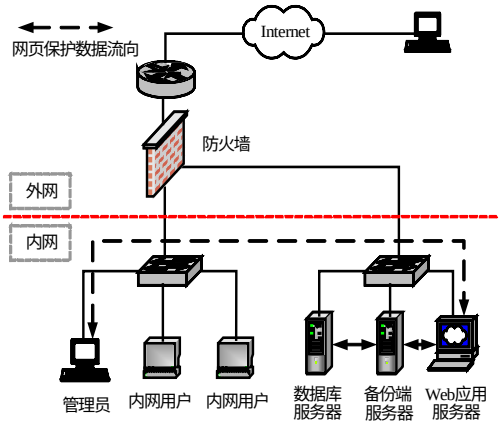


图 1 动态网页保护系统结构

(1)Web 应用服务器接收 Web 服务器委托的用户请求，执行相应的应用程序与数据库进行连接，并将处理结果提交给 Web 服务器。动态网页保护系统安装在被保护的 Web 应用服务器上，用户可通过浏览器在本机或远程访问控制端进行监控。

(2)数据库服务器用来提供数据库服务，在 Web 应用服务器控制下向外界提供数据服务，同时，在监控工具控制下向备份端提供数据库的定时备份和接受从备份端传来的恢复数

基金项目：国家自然科学基金资助项目(60373040, 60573048)；中国科学院研究生院科研启动经费基金资助项目
作者简介：袁 丹(1982－)，女，硕士生，主研方向：信息安全；张玉清，副研究员
收稿日期：2006-08-10 **E-mail：**yuand@nipc.org.cn

据等。

(3)备份服务器主要用来保存网页脚本文件及数据库的备份，在监控工具的控制下实现数据的备份和恢复。备份服务器与 Web 应用服务器的分离为备份服务器的安全提供了保障，也为系统的灾难恢复提供了资料保证。

1.2 系统功能模块构成

3 层 B/S 模式的动态网页保护系统分为系统管理模块、网页脚本文件保护模块、数据库保护模块、自动与手动备份恢复数据库模块、Web 网站更新模块。功能模块构成及相互之间的关系如图 2 所示。

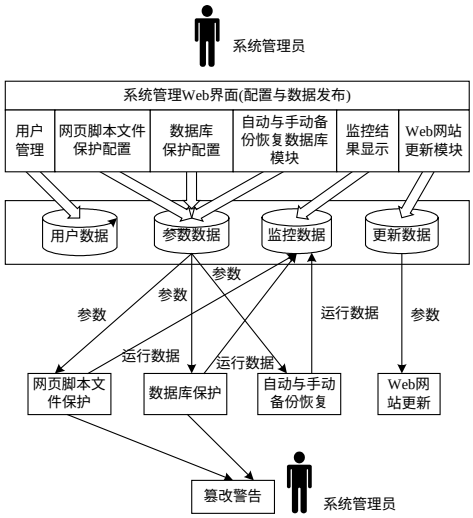


图 2 动态网页保护系统功能模块的构成

(1)系统管理模块是系统的控制端，主要完成对系统的配置工作。通过人机交互的方式完成用户身份验证、用户管理、网页脚本文件保护配置、数据库保护配置、自动与手动备份恢复数据库配置以及给系统管理员一个接口，使得合法用户可以对 Web 网站进行更新。

(2)网页脚本文件保护和数据库保护模块是实现网页保护系统的核心，它们都以系统服务形式运行，实现对网页脚本文件和 MySQL 数据库的检测和恢复；协调备份服务器与 Web 服务器、数据库服务器之间的通信和数据交换；发出警报和实现日志记录，并将这些信息返回给系统管理模块等。

(3)自动与手动备份恢复数据库模块主要负责定时备份数据库，在有故障发生的时候提供手动恢复的功能。

(4)Web 网站更新模块为系统管理员提供了一个管理 Web 站点的功能，包括上传新的网页文件以及在线编辑已经存在的网页文件等。

其中，网页脚本文件保护和数据库保护模块在 Linux 平台下采用标准 C 编程实现，其余模块采用 Linux+PHP+Apache+MySQL 进行 Web 程序开发。

1.3 网页脚本文件保护

所有的网页脚本文件都具有一个共同特点：如果管理员没有修改这些文件，他们应该是稳定的，即文件内容和状态信息不会发生变化。因此，如果文件内容或者状态信息发生变化，则可以判定其被非法篡改。

(1) HTTP 触发监控与实时监控

根据不同 Web 站点的特点，提供了两种监控策略供选择。

1)针对访问流量不大，但准确性要求较高的 Web 站点，系统提供 HTTP 触发监控方式。这种监控方式通过直接捕获浏览器客户端发出的 HTTP 请求，获知用户请求的页面，然后启动监控程序检查所要访问的页面是否被篡改，若页面遭到篡改，则启动自动恢复措施还原被保护的页面，并向浏览器返回正确的 Web 页面。这种监控方式将监控模块整合在 Web 服务器软件里，因此不可能有网页绕过检测机制。即使在黑客中断了 Web 服务器和备份网页服务器连接的情况下，也可以阻止被篡改网页的流出，真正做到万无一失。

2)针对访问流量很大，但准确性的要求相对较低的 Web 站点，系统提供实时监控方式。这种监控方式对所有需要保护的网页文件进行实时扫描，如果发现网页文件被篡改，立即对其进行恢复，因此可以保证所有网页文件一直处于监控之中。

(2)完整性检查

该系统通过对网页脚本文件消息摘要比较的方式来判定网页脚本文件的完整性。每次检查时，系统重新计算网页脚本文件的消息摘要并将之与数据库中的值相比较：若相同，则网页脚本文件未发生变化；若不同，则网页脚本文件已被篡改。

(3)备份恢复

该系统对所有施加保护的网页脚本文件在备份端进行完整的备份。当监控工具发现 Web 站点上的网页脚本文件被破坏或非法篡改后：先将该网页脚本文件删除，以保证用户不会浏览到错误的信息；然后迅速从备份端恢复被破坏或篡改的网页脚本文件。本系统采用 FTP 方式对网页脚本文件进行备份与恢复，同时为了提高整个系统的安全性，将备份端与 Web 服务器端隔离，并在传输过程中以安全套接层协议(SSL)进行加密传输。

1.4 动态网页数据库保护

动态保护网页除了要保护其网页脚本文件外，还要保护其后端的数据。动态网页中的数据大部分是以数据表形式保存在专用的数据库中的，因此对于动态网页中数据的保护，变成了对其所使用数据库的保护。各个数据库均有其自身特点，本文仅针对目前在动态网页中应用较广泛的 MySQL 数据库进行说明。

MySQL 本身提供了各种安全措施，动态网页保护系统对数据库的保护应该在此功能之上进行扩展，充分发挥数据库本身提供的各种安全功能，同时又要保证当数据库的安全措施被破坏之后，动态网页保护系统的及时响应。

(1)MySQL 数据库的安全性

MySQL 内部安全性关心的是文件系统级的问题，可以使用文件系统本身提供的设置文件和目录属主的工具来对相应文件进行设置。

MySQL 外部安全性关心的是从外部通过网络连接服务器的客户的问题。这就必须设置 MySQL 授权表，使各级用户有明确的权限。虽然数据库管理机制为各用户分配了比较明确的权限，但用户的权限仍然可能找到各种攻击方法得到“非法”提升，从而使某些敏感数据处于危险之中。这里对数据库的篡改主要是指用户权限的非法提升。

为防止用户权限的非法提升，动态网页保护系统为各个数据库用户分配安全的权限，然后对授权表文件进行备份，系统启动后就采用实时监控机制对 MySQL 的授权表文件进行监控。当发现授权表文件被非法改动时，立即将其恢复，从而防止了任何数据库用户权限的任何改动。授权表的恢复可以通过调用系统命令的方式实现，具体操作步骤如下：

1)以正常方式停止服务器运行[3]：

```
system("service mysql.server stop");
```

2)修改 MySQL 安装的数据目录，然后删除 MySQL 文件夹：

```
system("rm –rf mysql_path/data/mysql");
```

3)然后将备份的文件恢复

```
system("cp –R backup_path/mysql /usr/local/mysql/data/mysql");
```

4)重新启动数据库

```
system("service mysql.service restart");
```

这样，各用户的权限就恢复到篡改之前了。

(2)MySQL 数据库的备份与恢复

mysqldump 转储程序是将数据库表的内容写入到文本文件中。这些文件可用于备份数据库、移动数据库到另一个服务器中，或基于已有数据库的内容建立测试数据库等。系统利用该工具对相应数据库进行备份，通过启动选项-T path or -tab = path 来创建两个文件：1)包含 DDL 语句或者表创建语句；2)包含数据。DDL 文件被命名为 table_name.sql,数据文件被命名为 table_name.txt。

mysqlimport 是一个非常有效的载入数据工具。利用该工具可以实现数据库的恢复。只要将 table_name.txt 文件作为 mysqlimport 的输入即可以恢复相应数据表。如果数据表已经破坏，则可利用 table_name.sql 文件来重建数据库。

本系统中通过编程调用 mysqldump 和 mysqlimport 来实现数据库的备份与恢复。

1.5 监控流程

综合以上分析，可以得出动态网页保护系统监控的流程，如图 3 所示。

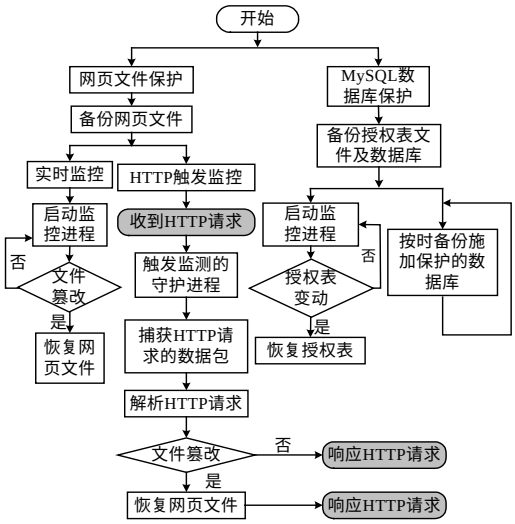


图 3 动态网页保护系统监控流程

2 相关技术

2.1 多线程技术

网页脚本文件保护模块和数据库保护模块都将完成备份、监控、报警、恢复、日志记录等多个任务，为了使各个任务可以并行处理，将采用多线程编程技术。

2.2 安全设计

(1)利用PHP和MySQL进行身份验证[4]，保障只有合法用户能够运行本系统；

(2)由于控制端、Web 应用服务器、数据库服务器和备份服务器之间传输的是较敏感的数据，因此整个系统的传输机制以 SSL 协议作为基础，在通信双方建立一条安全的、可信任的通信通道，确保了信息的保密性和完整性；

(3)系统采用将服务器和备份端分离的方式，有效提高了备份库的安全性，同时，在系统启动后，将对备份库采取独占模式，防止外界对备份库的破坏操作；

(4)系统监控运行采用开启服务方式，避免了程序运行时容易遭受非法关闭进程的攻击(KILL)，从而加强了系统自身的安全性。

2.3 数据库的定时备份

在 Linux 环境下，实现数据库自动备份的方法是借助于 MySQL 数据库提供的转储程序 mysqldump，结合 Linux 操作系统提供的 cron 定时服务共同实现，并对其用 PHP 程序进行包装，使其更面向用户，符合用户的需求，具体步骤如下：

(1)将系统管理传递的定时备份参数构造成定时备份的命令，并将它们以文本文件的形式存放，命名为 auto_backup.cron，备份命令形式如下：

```
0 1 * * 6 /usr/local/mysql/bin/mysqldump -uusername -ppassword
--add-drop-table –opt | mysql –h backup_host –uname –ppass db_name
```

(2)修改 auto_backup.cron 文件的权限，防止其他用户读取到该密码：

```
chmod("auto_backup.cron",600);
```

这样将文件 auto_backup.cron 的权限设置为仅文件属主可读写。

(3)将定时执行文件 auto_backup.cron 投入运行。利用系统命令执行如下 crontab 命令：

```
system("crontab auto_backup.cron")
```

2.4 Web 站点安全配置

(1)给 apache 装上 mod-security 模块，他有请求过滤、日志审计等功能，可以有效防止 SQL 注射和跨站脚本攻击；

(2)打开 PHP 的安全模式，即设置 safe_mode = On 这样 PHP 文件只能访问所有者和 PHP 文件所有者一样的文件，即使在 chroot 环境下也无法访问 jail 中属主不一样的文件；

(3)使 mysqld 进程运行于一个独立的用户/用户组下，此用户和用户组没有根目录，没有 shell，也不能用于其它程序；修改 MySQL 的 root 账号，并使用一个复杂的密码；保证连接 MySQL 的 nobody 账号登录被禁止；

(4)把 LAMP(Linux+Apache+MySQL+PHP)放置在一个 chroot jail 环境中以增进系统的安全性。

3 动态网页保护系统运行结果及评测

3.1 运行结果

动态网页保护系统的各项功能一旦被启用，动态 Web 网站就处在保护之中。系统运行过程中若发现网页脚本文件被非法篡改或者数据库用户权限非法提升，便将这种篡改还原，并发出报警信息，显示篡改目标和处理结果等。结果形式如图 4 所示。

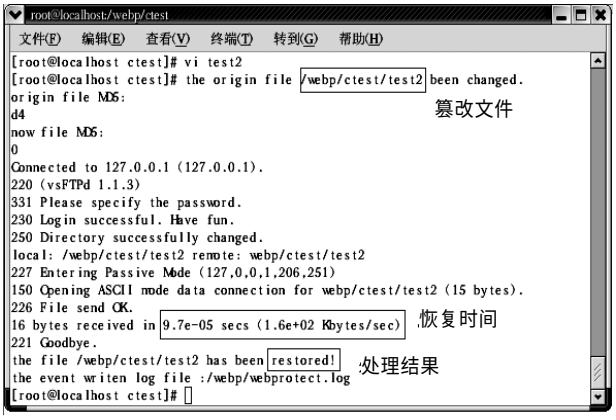


图 4 网页脚本文件被篡改后的报警信息

(下转第 171 页)