Design and Implementation of Automatic Defensive Websites Tamper-Resistant System

Jiuyuan Huo*
Modern Information Technology and Education Center, Lanzhou Jiaotong University, Lanzhou, China
Email: huojy@lzb.ac.cn

Hong Qu
Modern Information Technology and Education Center, Lanzhou Jiaotong University, Lanzhou, China
Email: quh@mail.lzjtu.cn

Liqun Liu
College of Information Science and Technology, Gansu Agricultural University, Lanzhou, China
Email: liulq@gsau.edu.cn

***Abstract*—Webpages tampering attack has become one of the most serious hazards to network security. Security measures of Website system were limited to install network layer protection devices, thus they could not provide effective monitoring and protection for illegal page tampering attack which making use of vulnerabilities of operating system. In this paper, we analyzed the research development of domestic and international Webpages tamper-resistant technologies, presented Website tamper-resistant technology system architecture of combining the third-generation anti-tampering technology with hardware device. We also established an integrated anti-tampering system that could actively detect attacks and dynamically defend tampering attack for Websites. Test results showed that the system could effectively prevent Webpages to be tampered, and could recovery real time in the event of tampering and alert administrators. It was proved that the deployment of this system would not result in a performance loss of Web server environment.**

***Index Terms*—Webpages Tamper-Resistant, Automatic Defensive, File Filter Driver, Event-Driven, Security**

I. INTRODUCTION

In recent years, Internet sites have been playing an increasingly important role in people's daily life for its convenience, effectiveness, and broadness. But, they are also in a relatively open environment and easy to become targets of criminals and hostile forces [1-3]. In various attacks, webpage-tampering is one of the most serious hazards of network security. If the page has been tampered, altered pages will be spread rapidly and broadly, and seriously effect public image and dignity of governments and enterprises, and even cause major losses in politics and economy and adverse social impact.

According to incomplete statistics, more than 98% Web sites in China have been subjected to different levels of hacking. CERT published the distribution of a number of Websites have been tampered in mainland China, and the total number of tampered Websites from January to August in 2010 is about 20041 [1].

Main reasons of Web page tampering are the following: the relatively weak security sense of administrators; systems and applications are vulnerable or refer some open source code; the attacker was skilled and use sophisticated tools. Most security measures for Website are limited to purchase Firewalls, IDS (Intrusion Detection System), Anti-Virus systems and so on, but complexity and diversity of operating systems and Web application systems will lead to the endless web vulnerabilities, and illegal tampering attacks exploit these vulnerabilities in the application layer, therefore, these network layer protection products could not monitor and prevent these Webpages tampering attacks.

Given the importance of Website information security and the above situation, we studied and developed a web tamper-resistant system of fast response, accurate determine and flexible deployment Web Security Guard (WebDefender). Through deployment of this system, files and directories in Website will be real-time monitored to ensure the contents of Web will not be tampered with attackers.

II. RELATED WORK

The formally presentation of "Web Anti-tampering" concept was in 2000 or so, then systematic research and development works have been carried out [2, 3]. At present, technology development of web anti-tampering has experienced about three generations that are Round-robin detection technology, Web server embedded technology, file filter driver technology and event-triggering technology. The development process was shown in Fig 1.

(l) The starting point - Artificial Contrast Detection

At earliest stage, page anti-tampering using an artificial contrast detection method that is designating an

Corresponding author: Jiuyuan Huo, Modern information Technology and Education Center, Lanzhou Jiaotong University, Lanzhou, China, 730070

doi:10.4304/jsw.7.10.2379-2386

administrator to manually monitor Websites. If tampered pages have been found, then he should manually restore the modified pages. It is an original and inefficient method.

(2) The first generation - Round-robin Detection Technology

This technology reads the monitored Webpages in a round-robin way, and then compares them with the original Webpages to determine the integrity by a detection application. If a tampered page was found, it would recover the page and launch an alarm. But during the detection interval, hackers can attack the system and lead the users access the tampered Webpages. It also occupies large system resources and only suitable for small Websites.

(3) The Second-generation - Web Server Embedded Technology

This technology modifies the original architecture of Web server, non-symmetric encrypts and stores certain attributes of Webpages such as file size, creation time. As a user visits the site, server encrypts the requested page and compares the value with the stored value. If the verification was consistent, server shows the page, or not. It greatly improves security, but it will take a lot of server resources, and lower the system efficiency.

(4) The third generation - File Filter Driver Technology and Event Triggering Technology

As file's attribute changes, the operating system will generate the appropriate system messages. Anti-tampering system captures these messages of the protected files, and starts recovery mechanism to restore the tampered files by event-triggering technology, and sends an alarm to notify the administrator. The entire procedures of attack detection and recovery files are all in seconds. The consumed memory and CPU utilization rate is far lower than previous techniques.

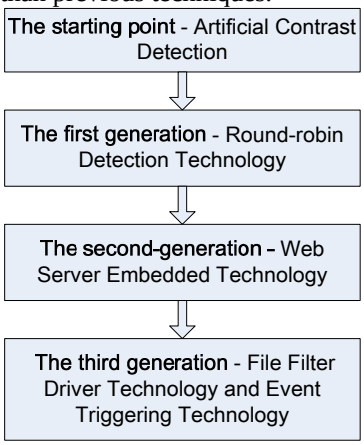

Figure 1. The development process of Website Tamper-Resistant technologies

Through the upper comparison, we can concluded that the third generation of Web anti-tampering technology is a simple, efficient, safe Web anti-tampering technology and advanced in aspects of performance, cost and deployment.

Domestic and international researches of Webpages tamper-resistant technologies and products have following major issues: Webpages tamper-resistant products are mainly developed based on software [4-17]. Once the hacker gets the operating system's administrator privileges, destruction and illegal tampering will cannot be prevented. In order to improve integrated security capabilities of Websites, we adopted the advanced file filtering technology and event-driven technology with a hardware security device, and build an automatic defense and integrated web security anti-tampering system that could initiatively detect all types of malicious tampering attacks and make operations of shutting off net of Web server and send alarms.

III. SYSTEM ARCHITECTURE

A. System Requirements

Main functions of Web anti-tampering system needs to achieve can be summarized as follows:

(1) Publishing function: publish the update files via tools such as FTP software to backup directory of publishing server, then the publishing server will automatically synchronize the files to the Web server;

(2) Detection function: automatically detect Website on the Web server through file filter driver technology to monitor whether the pages have been altered;

(3) Recovery function: as Webpages modified by hackers, the synchronization recovery mechanism will be started immediately to restore the tampered files in real time;

(4) Automatic alarm function: send alarms for the tampering events to notify administrators via SMS or E-mail.

B. System Topology

According to the physical composition of the anti-tampering system, we divided the system into three hardware parts: Web server, Publishing server, Hardware security subsystem. The publishing server is deployed in inner network, and responsible for synchronization normal updating files to Web server and recovery the tampered files. Web server is deployed in the DMZ zone of a Firewall, and responsible for displaying Web contents to users, requesting the publishing server to launch the recovery progress in a tampering event, and releasing alarm information to the hardware security subsystem. Hardware security subsystem connected a Web server through serial port and can accept commands from administrators to remote control the web server. The system hardware topology was showed in Fig 2.

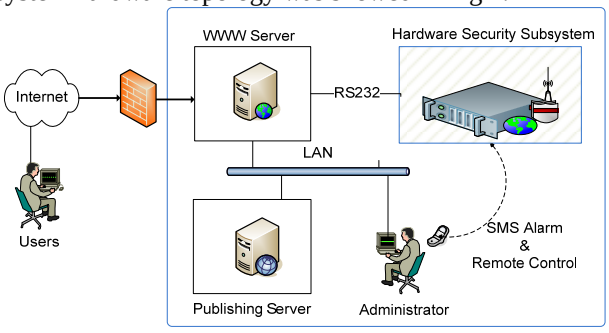

Figure 2. System hardware topology

C. System Workflow

System workflow was showed in Fig 3. It could be described as follows steps:

(1) First, set protected files or directories, and then start the protection services;

(2) Then intercept all the system calls to modify the monitored files through event-triggering technology, real-time block the illegal modifying act and recovers in time. The modified files will be compressed to archive for the future check, and the alarm notification will be sent administrator at the same time.

(3) Web server sent the correct Web page to users' browser.

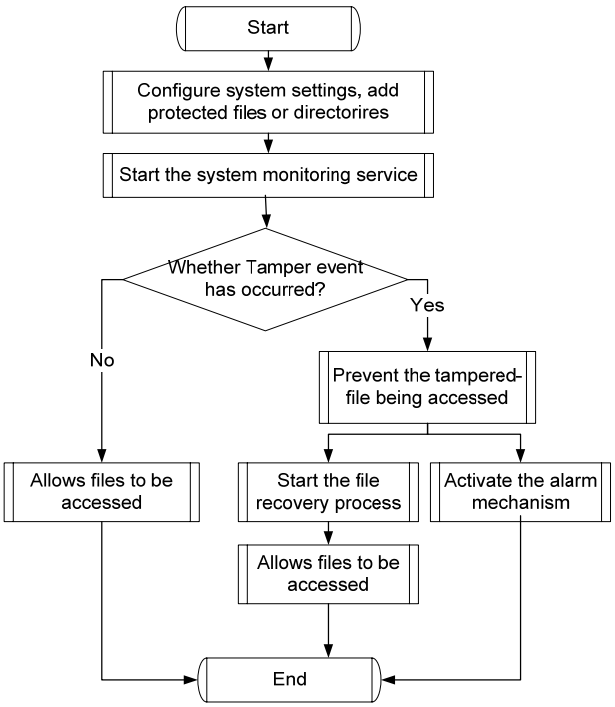

Figure 3. System workflow diagram

D. System Components and Deployment

According to the logic responsibilities and deployment, the system was divided into four relatively independent subsystems:

Monitoring subsystem (MoSS): Deployed in Website server, and responsible for real-time monitoring and protection of Webpages, sending recovery request as finding tampering attacks and immediately sending alarm message.

Synchronization subsystem (SySS): Divided into server side and client side. Server side is deployed on Web server and the client side is deployed on publishing server. It is responsible for real-time monitoring the changes on the backup files and receiving the recovery request submitted by Monitoring subsystem to implement the files synchronization.

Management Subsystem (MaSS): Deployed in publishing server to act as the interface between users and system. It is responsible for conveying operating instructions to Monitoring subsystem, Synchronization subsystem and Hardware security subsystem and responsible for real-time receiving various alarm information from Web server and promptly notifying the administrator.

Hardware Security Sub System (HaSS): It is an independent hardware device. It is responsible for regular communication with critical services such as monitoring subsystem, receiving alarms from management subsystem to notify administrators via SMS messages, receiving SMS commands from administrators to carry out operations such as shutting off the Web server's network.

The deployment structure of system components was showed in Fig 4.

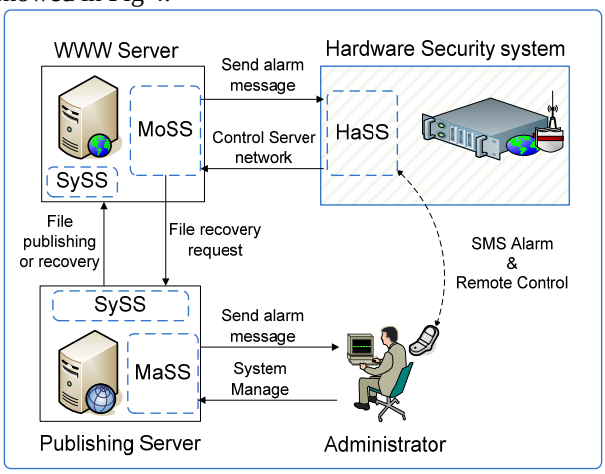

Figure 4. The overall system components deployment diagram

E. System Design

Monitor Sub System (MoSS) was deployed in Website server and responsible for real-time monitoring and protection of Webpages, sending recovery request as finding tampering attacks and immediately sends an alarm message.

1) Technical Solution

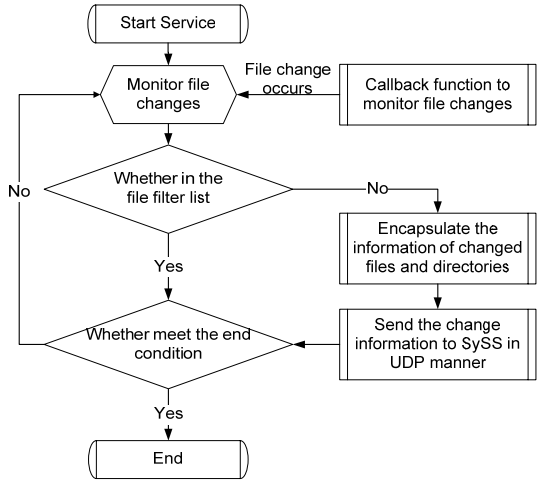

Figure 5. The flow chart of Monitoring Sub-System (MoSS)

Monitoring subsystem realizes real-time monitoring of file system by utilizing Windows or Linux file filter driver technology. According to real-time protection requirements of Website, any operation to add, modify, delete on monitored files and directories will be detected

immediately. To improve performance and reliability, file monitoring subsystem (MoSS) only performs function of monitoring files and directories on Web server and function of sending alarms, and will not perform other control functions. The implementation process of monitoring subsystem was showed in Fig 5.

2) Synchronization subsystem (SySS)

Synchronization subsystem is divided into server side and client side. Server side is deployed on Web server and the client side is deployed on publishing server. Client side is responsible for real-time monitoring of changes in backup files on the publishing server, and restore request submitted by monitoring subsystem, and upon the request to synchronize files to Web server. The flow chart of file Synchronization subsystem was showed in Fig 6.

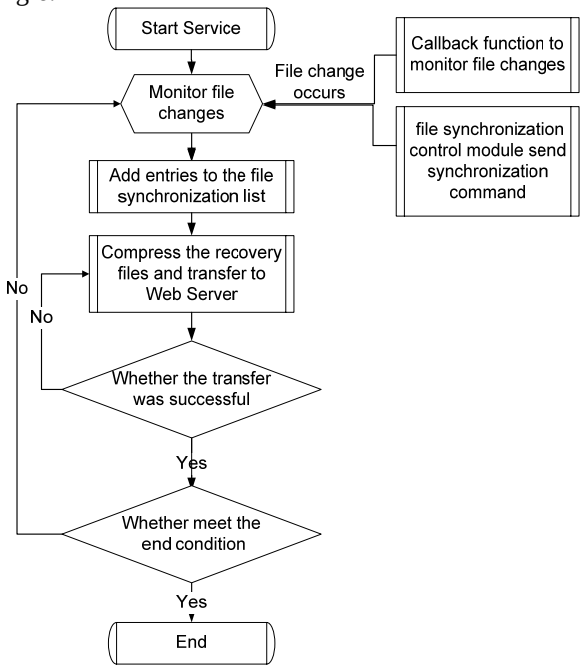

Figure 6. The flow chart of File synchronization subsystem

3) Management subsystem (MaSS)

Management subsystem is deployed in publishing server to act as the Web management interface between users and system. It is responsible for conveying operating instructions to Monitoring subsystem, Synchronization subsystem and Hardware security subsystem and responsible for real-time receiving various alarm information from Web server and promptly notifying the administrator. Web-based management platform includes the following functions:

a) User Management

System administrators can add, delete, and modify administrator's account and set administrator's email account, mobile phone number and other information.

b) System Settings

There are two fault and alarm notification: SMS and email. Before using the SMS alarm, the correct serial port which connects Web server with hardware security subsystem must be firstly set up. In email alarm, the parameters of mail server and mail accounts should be set up. The notification types of alarm messages were described in Table 1.

c) Log Management

Administrators can view and maintain the system log records. There are mainly two types of logs: one type log is recorded by system monitoring service and Web management subsystem; the other one is file tampering alarm log recorded by monitoring subsystem that is illegal creation, deletion, modification of protected files and directories.

TABLE I.
NOTIFICATION TTYPES OF AALARM MMESSAGES

ALARM CONTENT	REMARKS
File monitor service status invalid	File monitoring service has problems, administrator should check the server.
CPU usage >80%	CPU utilization is greater than 80%.
Mem usage >80%	Memory utilization is greater than 80%.
File monitor report error	File monitoring subsystem reports files are in illegally tampering event.

d) Monitoring Settings

In the "Monitoring Settings", administrators should set parameters relevant the monitored Website.

1. Monitoring directory and backup directory settings. Configuration rule is monitoring directory should be correspond with the backup directory one to one. In normal file update progress, synchronization is updating from backup directory to monitoring directory. As in the tampering attacks, the tampered files will be recovered from backup directory to monitoring directory automatically in real-time.

2. Filter directories or files list

Some files or directories in Website were often needed to be dynamically modified such as counters file, log file, Microsoft access database files. To prevent these files being wrong synchronization, they should be added to the filter file list.

e) Service Management

In "service management" interface, status of system-related services and system resources usage such as memory and CPU were listed. Administrators can view the current status of each service and control them such as stop or restart service.

4) Hardware security subsystem (HaSS)

Hardware Security Sub System (HaSS) is an independent hardware device. It is responsible for regular communication with critical services such as monitoring subsystem, receiving alarms from management subsystem to notify administrators via SMS messages. Once the server under attack, it can receive SMS commands from administrators to carry out operations such as shutting off the server's network to minimize the adverse effects.

a) Technical Solution based on GSM network

GSM mobile communication system is a more sophisticated and the most widely used mobile system. GSM has an incomparable advantage in coverage of wireless networks and its data transfer function of short message (SMS) also helps to make applications to rapidly

growing popularity. Hardware security subsystem is using GSM technology for wireless communication, and it integrated technologies of computer, communications, automation and other technologies to achieve real-time monitoring and management system for Website. The subsystem could free the operation and maintenance personnel from lots of tedious work and greatly reduce the adverse effects of malicious attacks. The subsystem adopted Atmel Company's ATMGEA 162 single-chip and ZTE Company's GSM module ME3000 to realize the sending warning messages to administrators' mobile, and receives SMS commands from administrator to remote control system for emergent operations.

b) Hardware and software structure of Hardware security subsystem

Hardware design of hardware security subsystem was showed in Fig 7, and there are five modules, namely, single-chip system and its peripheral circuits, GSM module and its external circuit, power supply module, the serial communication module that single-chip communicates with monitoring subsystem and GSM module, and network interface control module.

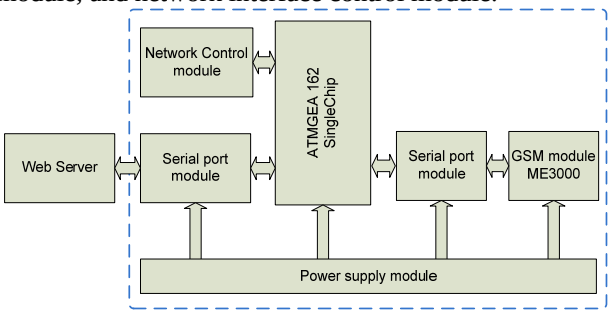

Figure 7. Hardware structure of hardware security subsystem

Software design of hardware security subsystem includes system initialization, interrupt management, data communication, network interrupt control functions and so on. The flow chart of Hardware security subsystem was showed in Fig 8. Before system operating, single-chip's serial port initially set should be done at first. Atmega 162 has two programmable serial ports, serial port 1 is connected with the Web server through level conversion; serial port 2 can be directly connected to GPRS module ME3000 for they have the same level. In this initialization process, serial communication parameters such as data bit, stop bit, parity bit and baud rate needed to be set.

Receiving mean of data communication adopts serial port interrupt. Information sent from serial front-end could be received and responded in any case. This soft design ensures the smooth flow of communication, and saves the processing time of data communication. Data flow can be received in the form of single byte and then be concentrated analyzed in communication program, thus communication program was more in line with requirement of modular design.

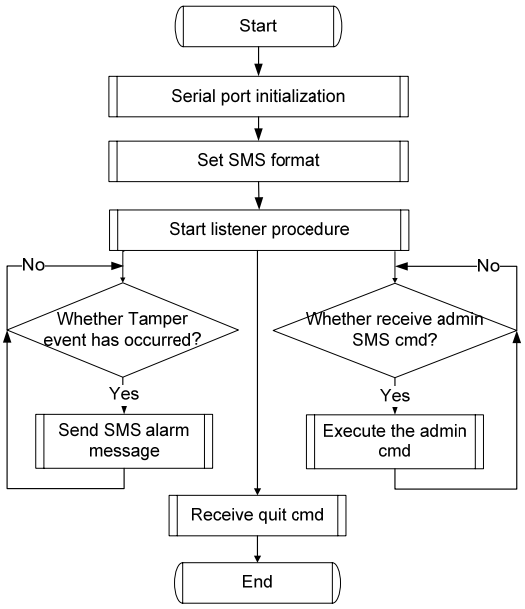

Figure 8. The flow chart of Hardware Security Subsystem

c) Hardware circuit design

(1) Hardware circuit design of single-chip

The subsystems adopted Atmel Company's ATMGEA 162 single-chip to perform the operation of communicating with Monitoring subsystem in Web Server, sending warning messages to administrators' mobile, and receive SMS commands. Due to the enhanced RISC 8-bit CPU with FLASH memory in a single chip, ATMEGA 162 is a powerful microcontroller for embedded control applications in a flexible and cost-effective technical solution. The basic circuit diagram was showed in Fig 9.

(2) Circuit design of serial interface with single-chip

MAX232 was adopted as the level converter circuit of serial communication to realize the function of serial communication with Monitoring subsystem.

(3) Circuit design of network interface control

Electronic switching-off Max312 was adopted to achieve control of network on and off. After GSM module receiving the network off command from administrator and transmit it to single-chip, single-chip control the network interface off through operating max312.

d) GPRS module ME3000

ZTE Company's GSM module ME3000 was adopted for sending alarm information submitted by single-chip to the administrator's mobile phone, and receiving remote control commands from administrator and transmitting them to single-chip for processing. ME3000 is an industrial level GSM module, and it supports for packet data service and short message service.

F. Own Security Design of System

Multiple security measures were taken to protect anti-tampering system itself:

(1) Management subsystem has strong authentication and authorization module;

(2) Heartbeat messages were used for modules to perceive each other's existence to ensure that each service was operating well;

(3) If heartbeat messages could not be received during three heartbeat intervals, alarm messages will be sent to inform administrator;

(4) Mutual protection was established between the service daemons. If one side of service monitored that the other side service is not started, it will try to start the other one.

This system meets the security requirements of web page tampering resistant, while it has an adequate security measures to protect itself to avoid hackers tampering system and better ensure the integrity of files from illegal tampering.

IV. System Performance Aanalysis and Function Test

A. Test Samples

There are 7, 029 files and 221 directories in test Website of which approximately 80% of files are html pages and 20% are gif/jpg image files. The total amount is about 70M bytes and the home page is index.html.

B. Performance Test

This section is mainly concerned with the impact on Web access speed in the case of before and after deployment of tamper-resistant system.

Test tools: Apache Bench (ab) 2.2. It is a small tool in Apache software packages and designed for Apache HTTP server benchmarking testing tool that can simultaneously simulate multiple concurrent requests.

Test procedure: Using Apache Bench to fulfill simulation access tests to Web server. Each test cycle consists of 3000 Web page requests; the test speed is 200 requests per time. There were a total of six test cycles, three times test on non-loaded tamper-resistant system and three times on loaded anti-tampering system.

As shown in table II, there are three types of testing result data that respectively are Request per second (mean) is the average number of transactions per second; Time per request/ms (mean) is the average transaction response time and the unit is ms; Time Per request/ms (mean, across all concurrent) is the average of the actual run-time of each request across all concurrent, the unit is ms.

As a result of adopting advanced file filtering technology and event-triggering technology, loading this tamper-resistant system will only cause a small impact on system performance. The impact of loading tamper system on transaction throughput and response time of Web server is about 2% to 5%. Thus, the performance impact on Website could be almost negligible.

C. Function Test

Function test is to test the correctness of system functionality of each module to ensure the correctness of modules, and no logical errors exist in modules. Function test are mainly include publishing function test, detect function test, recovery function test and automatic alarm function test.

Test tools: Notepad is a text editor in Windows system which could be used to edit the page file for simulating Web file tampered with attacks.

FlashFXP is a batch file upload tool which could be used to simulate the CMS (Content Management System) to generate large quantities of Web pages for automatically triggering the test of publishing function. Table 3 describes test case of publishing function.

Since the monitoring function, recovery function, and automatic alarm function are interact with each other, we designed a test case in Table 4 to test these features.

D. Test Results

Through the function test of system, system modules meet the design requirements, and user's interface to system is convenient. System could prevent illegal tampering website, send the alarm information and automatically recovery the tampered file. The impact on transaction throughput and response time of Web server could be negligible.

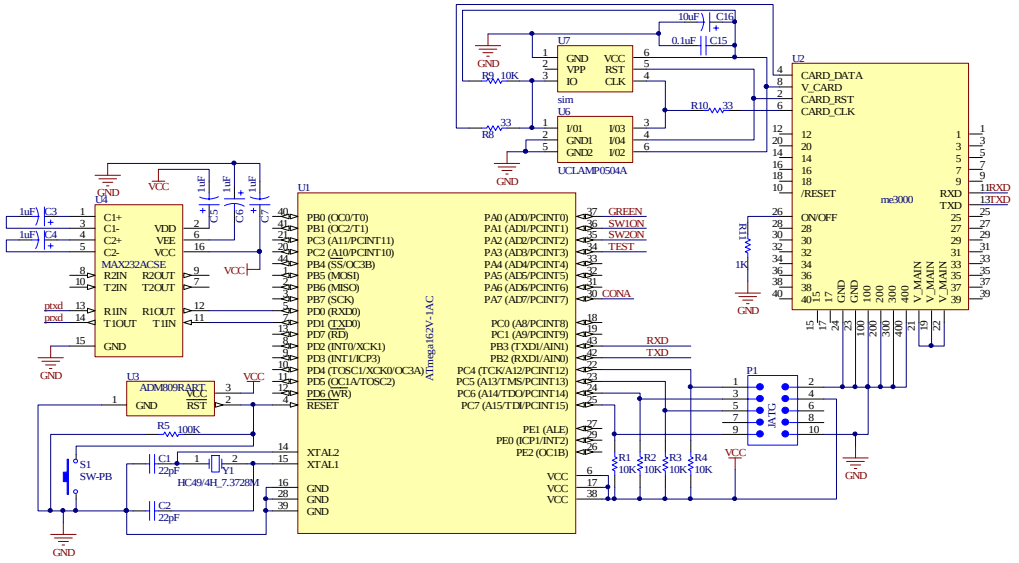

Figure 9. The basic circuit design chart of ATMEGA 162 Single-chip

TABLE II.
COMPARISON WEBPAGES TAMPER-RESISTANT SYSTEM PERFORMANCE TEST DATA

Test project	Non-loaded tamper-resistant system				Loaded anti-tampering system				Impact
	First	Second	Third	Average	First	Second	Third	Average	
Requests per Second (mean)	45.03	46.52	45.35	45.63	44.30	44.77	43.82	44.30	-2.91%
Time per Request/ms (mean)	4471.04	4464.58	4654.17	4406.60	4528.13	4497.71	4802.92	4609.59	4.61%
Time per Request/ms (mean, across all concurrent)	22.21	21.50	22.05	21.92	22.57	22.34	22.82	22.58	3.01%

TABLE III.
FUNCTION TEST CASE 1

Test content	Verification of publishing Webpages
Description	It can provide real-time Web page publishing function, that is it could automatically publish Web page files that generated by CMS and real-time synchronize to Web server without the user's manual operation.
Test project	Test operation: Running high CPU load program on Web server to make its CPU utilization reaching about 80%, then using FlashFXP to copy Website files to backup area of publishing server for simulating the Web file generation process of CMS. Test times: 10 times. Test results: all the files were published to the Web server successfully.
Test results	Web pages publishing function is effective.

TABLE IV.
FUNCTION TEST CASE 2

Test content	Verification of monitoring, recovery and automatic alarm functions
Description	As system real-time monitored the unauthorized file modification (tampering) to Web server, it immediately startup file synchronization recovery progress from publishing server and notify the administrator.
Test project	Test operation: Running high CPU load program on Web server to make its CPU utilization reaching about 80%, then using Notepad to open home page file, modify the contents of the file and close. Test times: 10 times. Test result: Files were restored, alarm information was sent to administrator and external visitors can access the normal Web page.
Test results	Monitoring, recovery and automatic alarm functions are effective.

V. CONCLUSIONS AND FUTURE WORK

In order to effectively prevent tampering attack to Websites and ensure integrity security of Web pages, we presented a Website tamper-resistant system of combination of third-generation Web anti-tampering technology with hardware device that could actively detect attacks and dynamically defend tampering attacks in this paper. Test results showed that the system could effectively prevent web pages from tampering, and deployment would not result in performance loss of Web server environment.

Although tamper-resistant system could further enhance the security of Website, but there are still some deficiencies. The system is mainly designed for static Web pages and the framework of dynamic pages, but it is powerless to database used by dynamic pages. In future work, we will focus on study of dynamic data protection for database of Websites.

ACKNOWLEDGMENT

This work is supported by Lanzhou Science and Technology Development Project, "Security Public Information Service System of Web" (Grant number: 2009-1-111) and Gansu Science and Technology Support Program, "A Security WEB Information Query System of Automatic Defense" (Grant number: 0804GKCA040).

REFERENCES

[1] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), http: //www.cert.org.cn/

[2] Waldman. M., Rubin. A.D., Cranor. L.F, “The architecture of robust publishing systems, ” *ACM Trans*. Internet Technology, vol. 1, pp. 199-230, 2001

[3] Waldman. M., Rubin. A.D., Cranor. L.F, “Publius: a robust, tamper-evident, censor-ship-resistant web publishing system.” *Proceedings of the 9th conference on USENIX Security Symposium*, vol. 9, pp. 5-12, 2000

[4] Lee. J., Kim. H., Yoon. H., “Tamper Resistant Software by Integrity-Based Encryption, ” *Parallel and Distributed Computing: Applications and Technologies*, vol. 3320, pp. 608-612, Springer, Heidelberg, 2006

[5] Jin. H., Lotspiech. J, “Proactive Software Tampering Detection, ” *Information Security*, vol. 2851, pp. 352-365, Springer, Heidelberg, 2003

[6] Jin. H., Myles. G., Lotspiech. J., “Towards Better Software Tamper Resistance, ” *Information Security*, vol. 3650, pp. 417-430, Springer, Heidelberg, 2005

[7] Blietz. B., TyagI. A., “Software Tamper Resistance Through Dynamic Program Monitoring, ” *Digital Rights Management. Technologies, Issues, Challenges and Systems*, vol. 3919, pp. 146-154, Springer, Heidelberg, 2006

[8] Horne. B., Matheson. L., Sheehan. C., Tarjan. R., “Dynamic Self-Checking Techniques for Improved Tamper Resistance, ” *Security and Privacy in Digital*

Rights Management, vol. 2320, pp.77-85, Springer, Heidelberg, 2002

[9] Ghosh. S., Hiser. J., Davidson. J., "A Secure and Robust Approach to Software Tamper Re-sistance, " *Information Hiding*, vol. 6387, pp. 33-41, Springer, Heidelberg, 2010

[10] Wu Hsien-Chu, Chang Chin-Chen, "Detection and restoration of tampered JPEG compressed images", *Journal of Systems and Software*, Vol. 64, pp. 151-161, 2002

[11] Saggesea G.P., Romanoa L., Mazzoccab N., Mazzeoa A., "A tamper-resistant hardware accelerator for RSA cryptographic applications", *Journal of Systems Architecture*, Vol. 50, pp. 711-727, 2004

[12] Chen Tzung-Her, Horng Gwoboa, "A lightweight and anonymous copyright-protection protocol", *Computer Standards & Interfaces*, Vol. 29, pp. 229-237, 2007

[13] Nighat M., Sayed A.H., "Secure web-based communication", *Procedia Computer Science*, Vol. 3, pp. 556-562, 2011

[14] Markus J., Philip D.M., Julien P.S., "Secure and lightweight advertising on the Web", *Computer Networks*, Vol. 31, pp. 1101-1109, 1999

[15] Shuchih E.C., Boris M., "The implementation of a secure and pervasive multimodal Web system architecture", *Information and Software Technology*, Vol. 48, pp. 424-432, 2006

[16] Carminati B., Ferrari E., Thuraisingham B., "Access Control for Web Data: Models and Policy Languages", *Annals of Telecommunications*, Vol. 61, pp. 245-266, 2006

[17] Elena F., Bhavani T., "Security and Privacy for Web Databases and Services", *Lecture Notes in Computer Science*, Vol. 2992, pp. 17-28, 2004.

Jiuyuan Huo received his B.S degree in 2000 from Computer major, Lanzhou Jiaotong university, and received Master Scholar degree in computer science from Lanzhou University in 2007. Now he is currently a Ph.D. candidate in Cold and Arid Regions Environmental and Engineering Research Institute (CAREERI), CAS. He is also senior engineer in Lanzhou Jiaotong University. His technical interest includes Wireless Sensor Network, and Grid Computing.

Hong Qu is a senior engineer and the Dean of Modern Information Technology and Education Center in Lanzhou Jiaotong University. His current research interests include Network Security, Network Computing, and Embedded Systems.

Liqun Liu received Master Scholar degree in computer science from Lanzhou University in 2007. Now she is a lecturer in College of Information Science and Technology, Gansu Agricultural University, Lanzhou, China. Her research interests include Information Security, WLAN Security, and Network Computing.