I.J. Wireless and Microwave Technologies, 2012, 3, 16-20
Published Online June 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815//ijwmt.2012.03.03

Available online at http://www.mecs-press.net/ijwmt

The Research and Application of Webpage Temper-proofing System

Wu Beihua[a], Wang Yongquan[b]

[a]*Informatization Office, East China University of Political Science and Law, Shanghai, China*
[b]*Department of Information Science and Technology, Criminal Justice School, East China University of Political Science and Law, Shanghai, China*

Abstract

With the sharp increase of hacking attacks over the last couple of years, web application security has become a key concern. The attack to websites, especially the explosion of webpage interpolating incidents has become one of the most serious problems of it. In this paper, the system adopts Web server core embedded technology to imbed tamper detection module and application protection module into the Web server, define corresponding strategies for temper-proofing, and realize the real-time monitoring and protection of web pages and the dynamic content in databases.

Index Terms: Network security; temper-proofing; core embedded technology

1. Introduction

Along with the unceasing development of information technology, the Internet has become the important means of information dissemination, circulation, exchange and store. Meanwhile, network security has drawn more and more attention. In the first half of 2010, CNCERT (Computer Network Emergency Response Technical Team) received 4,780 reports of network incidents, which were increased by about 105% compared with that of last year respectively. The attack to websites, especially the explosion of webpage interpolating incidents has become one of the most serious problems of it [1]. Therefore how to completely solve the problem of interpolating pages has become a key concern. In this paper, the webpage tamper-proofing system adopts Web server core embedded technology to imbed tamper detection module and application protection module into the Web server, define corresponding strategies for temper-proofing, and realize the real-time monitoring and protection of web pages and the dynamic content in databases. Therefore it is helpful not only to improve the security of websites, but also to provide clues and proofs for the investigation of safety accidents.

This work was supported by National Social Science Foundation of China (No. 06BFX051), National Natural Science Foundation of China (No. 60775038) and Judicial Expertise Construction Project of 5th Key Discipline of Shanghai Education Committee (No. J51102).

* Corresponding author.
E-mail address: [a]wubeihua@ecupl.edu.cn; [b]wangyongquan@ecupl.edu.cn

2. Statement of Problem

It's well known that network firewalls are capable of providing network layer access control and attack protection services. The firewalls are deployed in network border and the front end of Web server for necessary protection against network attacks. However, some important protocols (such as HTTP/HTTPS) must access Web applications without the restriction of network firewall rules. In other words, the firewalls have to completely open application HTTP/HTTPS port to the outside network. If user input, which is embedded in SQL statements, is incorrectly filtered for escape characters, attackers will take advantage of the present vulnerability. Network firewalls have no capability to protect against such attacks at this time [2].

It is the same with IDS/IPS (intrusion detection system / intrusion prevention system). The intrusion detection technology is limited in understanding and reacting application protocols and even unable to process complicated HTTP conversations and protocols. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to the system. Therefore, IDS/IPS is not always available to react in real-time to new attacks.

3. The Architecture of Webpage Temper-proofing System

The webpage temper-proofing system adopts Web server core embedded technology to imbed tamper detection module and application protection module into the Web server, define corresponding strategies for temper-proofing, and realize the real-time monitoring and protection of web pages and the dynamic content in databases. The architecture of webpage temper-proofing system can refer to Fig. 1.

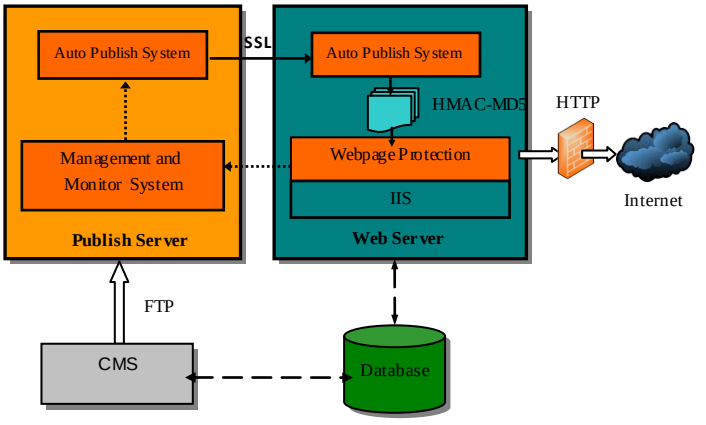

Fig.1 The architecture of webpage temper-proofing system

As shown in Figure 1, when user uploads web pages to Publish Server by FTP, Management and Monitor System can monitor the change of directory structure and file system. The Automatic Publishing Program uses secure hash function HMAC-MD5 to generate a unique irreversible digital webpage watermark, and then make identification on the Web Server. After detecting webpage contents have been changed, Automatic Publish Server use SSL security protocol to transfer the webpage and digital watermark to Web Server. The digital watermark associated with webpage contents can be stored in secure database and webpage update is completed.

In addition, Application Protection Module will have a security check on each user's request. All the request contents will be compared with the features of attack feature store. If the comparison is successful, that is to say,

the content is in accordance with certain attack mode, this request will be immediately suspended and the warning alarm will start. If attack code is not found, Tamper Detection Module will have an immediate integrate check on each page to be sent out. It will use secure hash function HMAC-MD5 to calculate the watermark of the page, and compare the watermark with that in the security database. If no watermark is found in the secure database or the comparison fails, the webpage will be judged as an illegal page. Then, the system will use Management System to recover the page automatically and meanwhile report the alarm to monitoring logs. Otherwise Web contents will be viewed by the public.

4. Application Strategies of Webpage Temper-Proofing System

4.1. Web Server Core Embedded Module

Web server core embedded technology means to embed security module into Web server software (IIS/Apache/ Weblogic/Websphere and etc.), for different Web server software this module is embedded with corresponding different core embedding technology [3]. In this paper, URLScan is deployed on IIS to improve the security of Web server. URLScan is a security tool that restricts the types of HTTP requests that IIS will process. By blocking specific HTTP requests, URLScan helps to prevent potentially harmful requests from being processed by web applications on the server.

All configuration of URLScan is performed through the URLScan.ini file, which is located in the %WINDIR%\ System32\Inetsrv\URLscan folder. Define the *AllowVerbs* section as *get*, *post*, *head*. And permit the requests that use the verbs which are listed in the *AllowVerbs* section. Furthermore, configure URLScan to reject requests for *.exe*, *.asa*, *.bat*, *.log*, *.shtml*, *.printer* files to prevent Web users from executing applications on the system. In addition, we configure it to block requests that contain certain sequences of characters in the URL, Such as '..', './', '\', ':', '%', '&'. It is seen that URLScan includes the ability to filter based on query strings, which can help reduce the effect of network hacker attacks [4][5].

The Security Module is embedded in Web server software and fully integrated with Web server software. It is helpful to improve Web services operation process with a high efficiency, stability and strong compatibility. In the meanwhile, there is no separate security module running process, so the invaders can not find security module and stop the module running [6].

4.2. Self-defined Strategies for Temper-proofing

Tamper Detection Module and Application Protection Module are embedded in the Web server. Application Protection Module will analyze the request from client and check whether there is illegal or not. It is imperative that we should define certain tamper-proofing strategies, use a standard input validation mechanism to validate all input data for length, type, syntax and business rules before accepting the data to be displayed or stored. For example, we construct the filtering rules for vulnerable characters as fallows:

```
<Rule id="70101" phase="2" log= "Restrict date parameter" severity= "critical" name="Restrict date
parameter">
<Item id="7010101" variables= "REQUEST_HEADERS:Host" transforms= "urlDecodeUni|lowercase"
method= "begin" pattern="url" action="next, pass" />
<Item id="7010102" variables="ARGS: id|ARGS: pagenumber" transforms= "none" method="rx"
pattern="!^\\d+$" action="deny,pass" />
</Rule>
```

It is seen that IIS will send a default error message to the browser when nonnumeric characters are detected in the parameter *id* or *pagenumber*.

However, it is unavailable to set the filtering rules too tight. So define exception for webpage in particular is essential. Consider the following code:

```
<Ignore_rule rule_id="11103" ignore_all="0" >
<Ignore_rule_url url="/save.asp" />
</Ignore_rule>
```

The above code represents the filtering rule numbered 11103 is not applied to the Web page *save.asp*.

4.3. Incident Triggered Detection Mechanism

The webpage temper-proofing system also includes an enhanced incident triggered detection module, which stays in the core operating system to protect the dynamic website content against the Web attacks and interpolating. Tamper Detection Module will have an integrate check on each page to be released. If the check result is normal the page will be sent out. Once a page is found having been illegally modified, an automatic recovery in accordance with certain strategy will be done. The Webpage Temper-proofing Module is closely integrated with the Web Server. It not only completely eliminates user's possible visit to interpolating contents which always happens in the polling scan interval and events trigger process, but also reduces the network bandwidth occupation and CPU utilization [7][8].

5. Conclusion

Scanning the Web site with Acunetix WVS6.5, three low-severity vulnerabilities have been discovered by the scanner. The result is given in Table 1. It is seen that possible sensitive directories have been found, and these directories are not directly linked from the Web site. To fix the vulnerabilities, we restrict access to these directories. For instance, admin directory is confined to access only for appointed IP address, and deny write access to cms and data directory.

Table 1 Web Vulnerability Scanning Report With Acunetix WVS6.5

Severity level	Quantity	Vulnerability description	Detail
High	0		
Medium	0		
Low	3	possible sensitive directory	/admin /cms /data

With the sharp increase of hacking attacks over the last couple of years, web application security has become a key concern. The webpage temper-proofing system adopts Web server core embedded technology to imbed tamper detection module and application protection module into the Web server, define corresponding strategies for temper-proofing, and realize the real-time monitoring and protection of web pages and the dynamic content in databases.

In the end, we must emphasize that each prevention technique cannot provide complete protection against various network attacks, but a combination of the pretection mechanisms will cover a wide range of these attacks.

Acknowledgment

This work was supported by National Social Science Foundation of China (No. 06BFX051), National Natural Science Foundation of China (No. 60775038) and Judicial Expertise Construction Project of 5th Key Discipline of Shanghai Education Committee (No. J51102).

References

[1] CNCERT/CC, "China Internet network security report in the first half of 2010," http://www.cert.org.cn/articles/docs/common/ 2010092925138.shtml.
[2] "Introduction to intrusion detection systems," http://netsecurity. about.com/ cs/hackertools/a/aa030504.htm.
[3] Zhang Lei, Wang Lina, Wang Dejun, "Model of webpage tamper-proof system," J.Wuhan Univ. (Nat.Sci.Ed.), Vol.55, No.1, pp.121–124 (in Chinese).
[4] Wu Beihua, "SQL injection defense mechanisms for iis+asp+mssql web applications," J. China Communications, vol. 7, No.6, pp.145–147
[5] "How to configure the URLScan tool, " http://support.microsoft.com/ kb/326444/en-us.
[6] "Core embedded technology," http://www.tcxa.com.cn/technology/ technology_embeddinwebserver.htm (in Chinese).
[7] Fan Jianhua, Song Yunbo, "Web page tamper-resistant mechanism based on file-filtering driver and event-triggering", J. Chongqing Institute of Technology (Natural Science), Vol.23, No.12, pp.65–70 (in Chinese).
[8] Zhang Jianhua, Li Tao, Zhang Nan, "Mechanism of anti-modification and anti-replacement on web pages", J. Computer Applications, 2006, 26(2), pp.327-331(in Chinese).