

Flexible Web Monitoring System (FWMS) for Web Connection Information

A-Ra Jo^{1,2}, Beom-Hwan Chang², Chi-Yoon Jeong², Jung-Chan Na^{1,2},

¹ Division of Information Security, University of Science and Technology, Daejeon, Korea.

² Managed Security Research Team, Knowledge-based Information Security & Safety Research Division, ETRI, Daejeon, Korea.
{joara11, bchang, iamready, njc}@etri.re.kr

Abstract. We study the mechanism that extracts the information of web clients. Web monitoring system based on ActiveX is executed on Internet Explorer. The need for mechanism not based on ActiveX has increased due to rise in other web browsers usage. Thus, the mechanism based on ActionScript becomes alternative mechanism. However, the information of web clients through ActionScript is not enough to identify real intruder. Therefore, this paper provides Flexible Web Monitoring System (FWMS) mechanisms. FWMS can use both of mechanisms according to environment for web browsing.

Keywords: Web Tracer; web monitoring system; web connection information.

1 Introduction

Recently, as the population of the Internet users grows rapidly, various hacking and the cyber crime on the Internet have increased. If there are illegal activities or criminal acts that can be done online due to the accessibility of the Internet, we should be aware of real criminal location. Without criminal's information, we cannot prove any illegal activities. Extracted information through monitoring system utilize as legal evidences.

A study of technologies that extract the information of web clients increases to procure legal evidences. A lot of systems are developed in various ways like using real time access log [1] and plug-in. However, information of mechanisms based on real time access log and plug-in are not enough whereas former mechanisms can acquire only web connection information.

Therefore we propose Flexible Web Monitoring System (FWMS) to obtain information of web connection and web client host. FWMS consists of FWMS based on ActiveX controls (FWMS-AX) and FWMS based on ActionScript (FWMS-AS). As we use combined FWMS-AX with FWMS-AS, we acquire both of benefits. FWMS-AX extracts information from web client host directly and gains more detail information than monitoring system based on plug-in and FWMS-AS. The various information from FWMS-AX such as host name, mac address, operating system information, host network interface, host user id, proxy information are used as legal evidences. However, FWMS-AS is executed more various web-based browser environments than FWMS-AX's.

This work was supported by the IT R&D program of MKE/IITA.

[2007-S022-03, The Development of Smart Monitoring and Tracing System against Cyber-attack in All-IP Network]

This paper is organized as follows: Related Work of FWMS is described in Section 2. In section 3, we present a proposed FWMS. We provide overview of FWMS and future works in Section 4 conclusion.

2 Related Work

2.1 FWMS-AX

Approximately 70% of Internet users consume Microsoft Internet Explorer [2]. Microsoft's ActiveX technology [3] supports Windows COM component to be downloaded and executed within web pages. The ActiveX controls that are provided with Internet Explorer are installed automatically when the user installs Internet Explorer 3.0 or higher. Once installed, ActiveX controls run automatically when a web page containing them is displayed. The ActiveX consists of codes that extract information of web clients.

[Figure.1] presents flowchart of FWMS-AX. When a web client joins web page included ActiveX controls, a web client downloads ActiveX controls. After executing ActiveX in web client's host, data from ActiveX are delivered to monitoring server.

Monitoring server analyzes the message from ActiveX. Received message is composed of user ID, Mac address, host name, operating system information, host network interface and proxy IP address. Real IP address of host is sent when ActiveX is activated. Monitoring server obtains geographic information of host IP address and proxy IP address through GeoIP database [4].

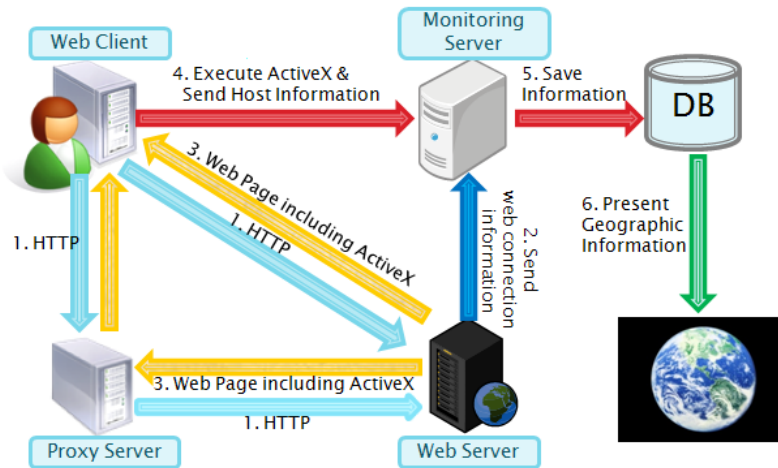


Figure. 1. Flowchart of FWMS-AX

2.2 FWMS-AS

Flash Players that support ActionScript implement a full virtual machine in which ActionScript code is verified and run. Flash Player [5] is the world's most pervasive software platform, used by over 2 million professionals and reaching 99.0% of Internet-enabled desktops in mature markets as well as a wide range of devices. Moreover, flash players free from operating system environment and web-based browser environment.

[Figure.2] indicates flowchart of FWMS-AS [6]. If a web client using proxy server or not makes connection with web server, web server requires a web client to approve performing ActionScript. For FWMS-AS, web clients need a Flash Player. When a web client arrives the web page being monitored, ActionScript is executed and then sends information such as real IP address of a web client, latest passed proxy IP address, current URL address and IP address of web server to monitoring server.

Monitoring server analyze received information of a web client via ActionScript. Using analyzed information, geographic information of IP addresses (real IP address, latest passed proxy IP address) are determined through GeoIP database.

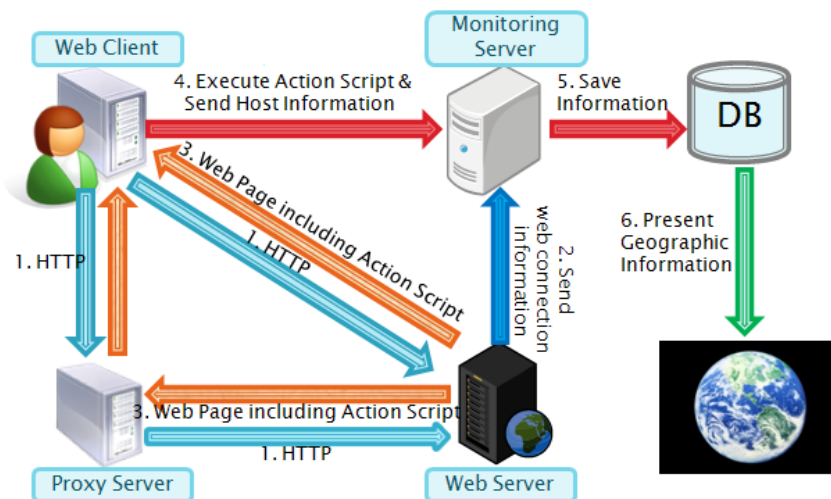


Figure. 2. Flowchart of FWMS- AS

The vulnerabilities of FWMS-AX are that it is executed only on Internet Explorer and needs agreement of a web client. The manager can set options like no execution of web page without agreement, however it is too unpractical. On the other hand, the problem of FWMS-AS is lack of information. The information from ActionScript is only web connection information. But we need more detail information such as host information of a web client, because this information is used as legal evidences. To solve these problems, we proposed flexible monitoring system named FWMS.

3 Architecture of FWMS

Comparing [Figure.1] with [Figure.2], we recognize that FWMS-AX and FWMS-AS have almost same structure. However, there exist differences. The largest difference is that each technology is executed in different web-based browser environments. FWMS-AX can be supported only in Internet Explorer, on the other hand, FWMS-AS can be supported in various web-based browser environments.

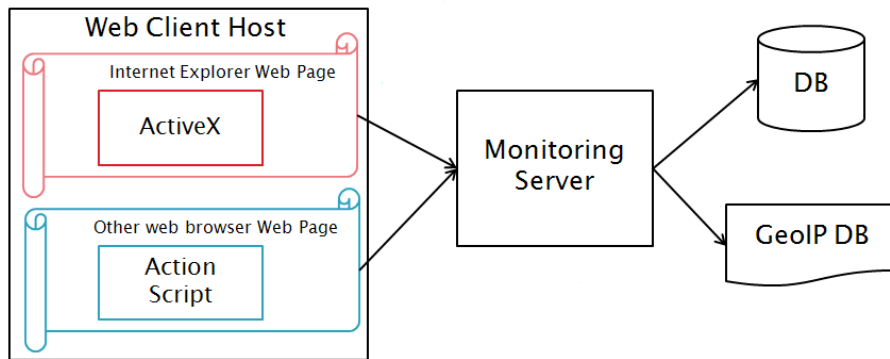


Figure. 3. Structure of FWMS

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE="JavaScript" type="text/javascript">
<!--
    function getParam() {
        var bIE = new RegExp(/MSIE/).test(navigator.userAgent);

        var ip = location.host;
        var current_url = document.URL;

        if (bIE) {
            // Execute ActiveX
        } else {
            // Execute ActionScript
        }
    }
//-->
</script>
</HEAD>

<BODY onLoad="getParam();">
<!--
    BODY EXECUTE
//-->
</body>
</html>
```

Figure. 4. Main function of FWMS's web page

As ActiveX controls that are provided with Internet Explorer are installed automatically, the population of the ActiveX grows. Many security software is using by ActiveX control, so Internet Explorer users have no reluctance to download ActiveX controls. However, for other web-based browsers, we propose flexible FWMS in each web browser environment. [Figure.3] describes whole structure of FWMS. As shown in [Figure.4], according to a type of user's web browser FWMS chooses between FWMS-AX and FWMS-AS automatically. FWMS consumes same monitoring server whether FWMS-AX or FWMS-AS. Monitoring server is stored information of web client in database along with geographic information extracted through GeoIP database.

Nevertheless, both of FWMS-AX and FWMS-AS use same database. Information of FWMS-AX and FWMS-AS is same like [Figure.5] and [Figure.6]. The information describes as follows:

Web Client. This field presents real IP address of web client.

IP. This field presents the latest passed Proxy IP address.

Webserver. This field presents IP address of web server.

URL. This field presents URL address of web server.

{countryCode, countryName, latitude, longitude, ISP}. First set presents geographic information of real IP address. Second set presents geographic information of proxy IP address.

{MAC Address, User ID, User OS, IFF Name}. This set presents information of web client host.

OWNER. This field presents what kind of FWMS is. (FWMS-AX or FWMS-AS)

```

=====
Web Client      : 125.248.82.129
=====
IP              : 125.248.82.129
Webserver      : 129.254.242.205
URL            : http://129.254.242.205/index.html
=====
countryCode    : KR
countryName    : Korea, Republic of
latitude       : 37.566406
longitude      : 126.999695
ISP            : DACOM-PUBNETPLUS
=====
countryCode    : NO PROXY
countryName    : NO PROXY
latitude       : NO PROXY
longitude      : NO PROXY
ISP            : NO PROXY
=====
MAC Address    : No Information
User ID       : No Information
User OS       : No Information
IFF Name      : No Information
OWNER         : ActionScript
=====
Connection released .....

```

Figure. 5. Saved data using no proxy server

```

=====
Web Client      : 125.248.82.129
=====
IP              : 213.41.71.164
Webserver      : 129.254.242.205
URL            : http://129.254.242.205/index.html
=====
countryCode    : KR
countryName    : Korea, Republic of
latitude       : 37.566406
longitude      : 126.999695
ISP            : DACOM-PUBNETPLUS
=====
countryCode    : FR
countryName    : France
latitude       : 48.899994
longitude      : 2.399994
ISP            : COLT Telecom GmbH
=====
MAC Address    : 0A-06-E3-21-B9-13
User ID       : simpson
User OS       : Windows XP SP2
IFF Name      : Intel (R)
OWNER        : ActiveX
=====
Connection released .....

```

Figure.6. Saved data using proxy server

[Figure.4] is the case that information from FWMS-AS indicates data of web client without proxy. As shown in same Web Client field and IP field, we can recognize that a web client did not use proxy. Conversely, as shown in Web Client field and IP field of [Figure.5], we can discover that web client joins web page through proxy server. Whether high anonymous proxy or no proxy, FWMS accumulates both of real IP address and proxy IP address of web clients.

Table 1. Comparison proposed mechanism with existing mechanism.

	FWMS-AX	FWMS-AS	Web log	Plug-in
Memory requirements	Low	Low	High	Low
Information diversity	High	Low	Low	Low
Isolated by security settings	Yes	No	N/A	Yes (according to conditions)

Differences between our proposed mechanism and existing mechanism are given in Table 1. Not only information diversity, memory requirement of FWMS is lower than a mechanism using real time access log (web log). FWMS-AX might be isolated by Internet security settings. If FWMS-AX is restricted by a web client, the web client loses connection.

4 Conclusion

In this paper, we introduced FWMS for gaining web connection information. FWMS-AX can gain more information than web monitoring system based on plug-in. FWMS-AS can be applicable in various web-based browser environments and executed without agreement of a web client. Therefore, FWMS extracted information which let the manager know who real user is.

A proposed system improves flexibility as gather benefits of FWMS-AX and FWMS-AS. The manager of FWMS can choose FWMS/FWMS-AX/FWMS-AS according to their environments. In the future, we supplement FWMS based on various ways like signed java applets. All-combined FWMS will be more flexible and comfortable. The manager can use considering each benefit and limitation.

References

1. Kug, K., Lee, S.: Design and Implementation of a Real Time Access Log for TCP/IP Protocol Weakness Attack Detection (Korean version), KCC 2001, (2001)
2. Internet Explorer 8, <http://www.microsoft.com/windows/internet-explorer/default.aspx>
3. MSDN: Microsoft Developer Network, [http://msdn.microsoft.com/en-us/library/aa268948\(VS.60\).aspx](http://msdn.microsoft.com/en-us/library/aa268948(VS.60).aspx)
4. Maxmind, Ltd. Geop database, <http://www.maxmind.com>.
5. Millward Brown survey, "Flash Player Penetration", www.adobe.com/products/player_census/flashplayer/
6. Jo, A., Jeong, C., Chang, B., Na J.: Monitoring Environment Design for Web Connection Information (Korean version), KIPS conference, (2009,4)
7. Lim, C.: Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis, FIRST Conference on Computer Security Incident Handling & Response. (1999)
8. Schnackenberg, D., Djagandary, K., Strene, D.: Cooperative Intrusion Traceback and Response Architecture(CITRA), Proceedings of the 2nd DARPA Information Survivability Conference and Exposition(DISCEX II), (2001,6)