International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:12, 2007

A Novel Security Framework for the Web System

J. P. Dubois, and P. G. Jreije

***Abstract*—**In this paper, a framework is presented trying to make the most secure web system out of the available generic and web security technology which can be used as a guideline for organizations building their web sites. The framework is designed to provide necessary security services, to address the known security threats, and to provide some cover to other security problems especially unknown threats. The requirements for the design are discussed which guided us to the design of secure web system. The designed security framework is then simulated and various quality of service (QoS) metrics are calculated to measure the performance of this system.

***Keywords*—**Web Security, Internet Voting, Firewall, QoS, Latency, Utilization, Throughput.

I. Introduction

THE World Wide Web has been the main driving force of the internet. There is about 60 million website reported to be on the internet as for February 2005, according to Netcraft survey [1]. Together with number of general websites, the number of websites for e-commerce purpose is also increasing. Web sites have been since the honey spots for attackers. Web attacks have been a major problem of information security recently, and are at the top of the 2005 incidents, according to SecurityFocus analysis [2]. As web systems become more and more important, the cost related to security incidents also raised exponentially as reported by CSI/FBI [3] as well as AusCERT [4].

Thus, the main question is how to try to make web system more secure. In order to answer such a question, we need to review all of the current security measures then look for a possible improvement of available security technologies and put them together to build a secure web system that can be used as a guideline for organizations building their web sites. There are relatively little research about web security and web system architecture. However, most of the works concentrates in web service only, not web systems. Some industrial vendors define the security framework with some security coverage such as Microsoft DNA [5], Oracle EcoStructure [6], and IBM WebSphere [7]. It is common that in these designs the web server and/or database servers are usually put into the same location. One notable exception is Oracle EcoStructure with a very complex integrated design of Cisco router, switches, and firewalls. Since the access requirements for the web servers and database server are different, they should be put in different zones with different access policies.

The main strategy when designing the web security architecture is to separate the network into multiple security zones with multiple levels of protection where each component joining the network is as secure as possible.Defense can be at all levels from physical access to network, transport level or secure applications. Security strategies such as in [8] are taken into account namely least privilege, defense in depth, choke point, weakest link, fail-safe stance, simplicity, and security through observation.

Manuscript received July 15, 2005.

J. P. Dubois and P. Jreije are with the University of Balamand, Koura, Lebanon (phone: 961-3-841472; fax: 961-6-930250; e-mail: jeanpierre_dubois@ hotmail.com).

II. System Design

The design is illustrated in Fig. 1. Such design has to consider all the possible attacks. While many web specific attacks can be prevented by careful application development, no developer can declare perfect software. Buffer overflows and denial of service attacks are extremely difficult to prevent. Configuration errors are common. A security protocol considered safe today can be broken tomorrow. Thus the design should be prepared for the worst case.

The design separates network into security zones: public servers, production network, and corporate network. There are three main traffic flows: between remote users and public servers, between web server and application/database servers, and between local users and application/database server. In addition, traffic flow that results from local users trying to access resources on the internet should be taken in consideration. There are two firewalls installed to separate the security zones and to enforce traffic flows. The public servers are put in the DMZ zone of the first firewalls.

First, all hosts are hardened following guidelines at [9] and [10]. Physical access is controlled and switches are used instead of hubs to reduce the packet sniffing threats.

The first traffic flow represents the flow of traffic between remote users and web servers. Due to the fact that the communication environments and the organization have little control over remote client software protocol, security services should be provided at higher layer protocols. The SSL, secure socket layer protocol provides excellent confidentiality and integrity service. The authentication service is currently not supported, however, server to client authentication is widely used. There are reasons that client to server authentication is

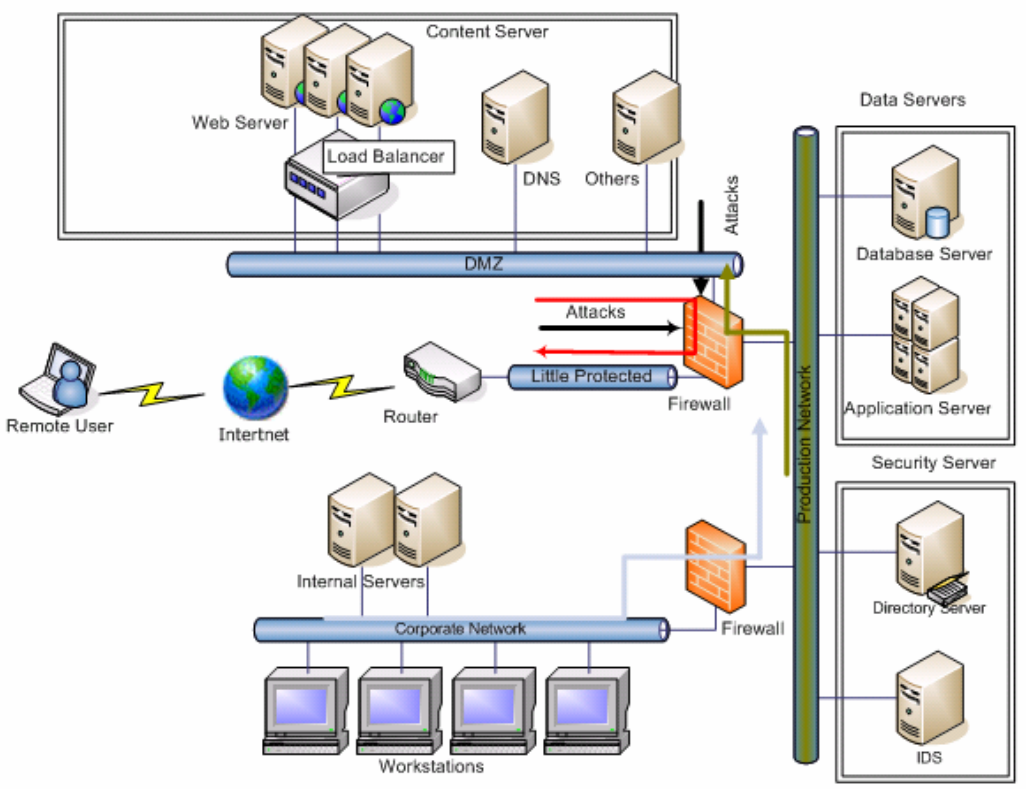


Fig. 1 Security framework design for the web system

used as discussed in [11] - [15], and [16] - [18] suggest improvement for web authentication. Further research might find a solution for this problem, but the current solution is username and password using HTML form and HTTP POST. There is currently no other solution for session control, which in turn supports access control development, other than creating session token using secure cookies. The selected access control model is RBAC, role based access control, as discussed in [19] and [20]. In this traffic flow, the web server and the web application are the weak points. By selectively controlling traffic on the firewall, the weak point can be reduced to only HTTP based attacks. Conforming secure application development guidelines at [21] and [22] further reduces the problems. Giving the web application limited privileges on the web server reduces the chances that the server is taken as a base for further attacks. There is still very little chance of the servers in the public network is broken.

The second traffic flow represents the flow of traffic between the web servers and database/application servers. The communication of the traffic flow is in a totally controlled environment. Physical access can be controlled, as well as higher access levels. Data integrity and confidentiality might not be required in such communication environment. This also exhibits benefits in term of performance. Database arguably provides enough access control for most applications Username and password authentication should be enough; however, there is still a very small chance that the web server has been broken into. This requires that the credentials to access the database server not be stored in the web server. There is a solution for this requirement: directly pass user credential to database server, which checks against stored credential in the security server. If the web application is designed with authentication protocol that can prevent man-in-middle attacks, then the system is still safe even in the case web server is broken into.

The third traffic flow represents the flow of traffic between local users and database/application servers. It seems that the networking environments here are secured. However, there is quite a number of staff doing different jobs. The situation should be considered. The organization owns the infrastructure, thus it is possible to implement some lower level security here. The solution is VPN with the IPSec protocol providing all necessary security services for authorized person without having to modify applications. It is possible that applications can provide some services as additional measures. This is not, however, required. Most, if not all insider attacks, should be prevented by the combination of the host hardening, the second firewalls and the VPN protocol.

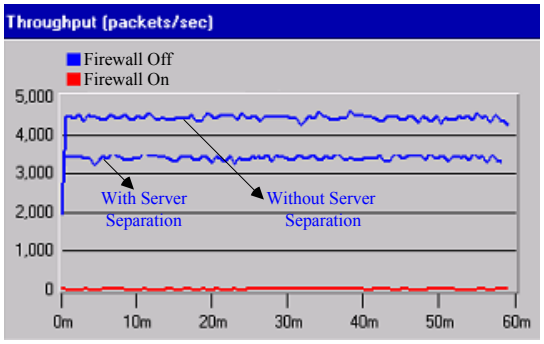
The fourth traffic flow represents the flow of traffic between local users and the internet. This traffic flow might not directly relate to web system security but the threats of virus and worms should be seriously considered.

While most security threats can be fixed by securing configuration, application development, & applying patches,

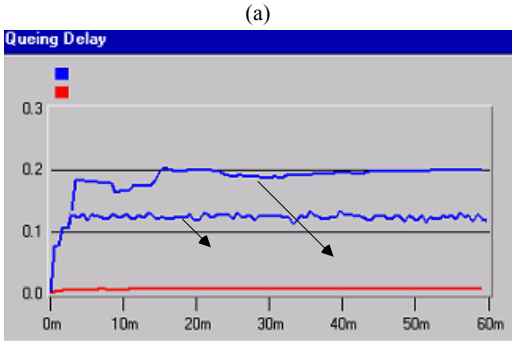
the unknown bugs and error have been considered. To be able to get into databases, the attacker has to pass several levels of protections provided that the attacker exploits the multiple security holes at the same time. Additional intrusion detection system might help detect the attack in case.

III. Simulation and Discussions

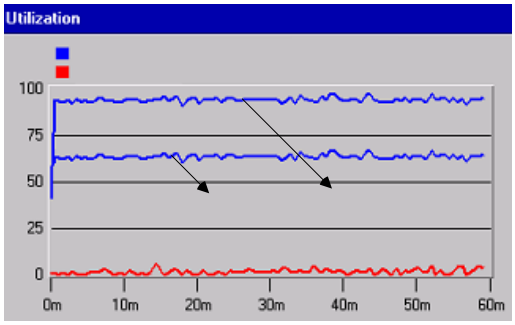
Without loss of generality, the proposed design is simulated using OPNET IT GURU for the cases with server separation and without server separation, when the firewall is turned on and off. The results are illustrated in Fig. 2 (a) – (c) and show that the proposed design had a significant improvement in the Web, Data, and Security Servers. The throughput, queueing delay, and utilization graphs show significant reduction in the network utilization due to the firewall policy and servers separations, thereby improving the application performance and reducing the unwanted traffic diminishing the chance where the system is broken.



(a)



(b)



(c)

Fig. 2 QoS performance metrics in terms of: (a) throughpout, (b) queueing delay or latency, (c) utilization

IV. Conclusion

In this paper, we presented a security design with the goal of obtaining the most secure web system out of the available generic and web security technologies. The security framework was designed to provide necessary security services, to address the known security threats, and to provide some cover to other security problems especially unknown threats. The proposed solution was simple and secure since there were only three security zones and four traffic flows. It was also practical using available technologies. Although most of the security threats have been addressed, this approach does not completely fix the problems. However, it does significantly lower the probability that the system is broken where most of the security requirements are provided.

A number of applications can benefit from this work. Most notably, internet voting systems have been increasingly becoming a feasible option for political as well as non political ballots. The main restriction on the implementation of such systems is the security issue. We expect research such as ours, to help reduce the security issues and make internet voting an effective and viable means of achieving "electronic" democracy.

References

[1] Netcraft, "Netcraft Web Server Survey," 2005. Available http://www.netcraft.com/survey
[2] D. Hanson, "ARIS Top Ten 2005 Threats," Security Focus, 2005. Available http://www.securityfocus.com/corporate/research.
[3] R. Power, "CSI/FBI Computer Crime and Security Survey," Computer Security Issues & Trends, vol. 8, no.1, 2002.
[4] AusCERT, "Australian Computer Crime and Security Survey," 2002. Available http://www.auscert.org.au.
[5] Microsoft, "E-Commerce Security," 2000. Available microsoft.com/technet/itsolutions/ecommerce/maintain/operate/ecomsec.asp
[6] L. Ganci, "Firewall and Network Configuration," Websphere Commerce V5.4 Handbook, Architecture and Integration Guide, Appendix A, IBM Redbooks, 2002, p. 790.
[7] Oracle, "Deploying CRM Applications on the ECO Structure Architecture," 2001. Available http://www.eecostructure.com/crmwp.pdf
[8] R. Zalenski, "Firewall Technologies," IEEE Potentials, vol. 21, no. 1, 2002, pp. 24-29.
[9] AusCERT, Windows NT Configuration Guidelines, 2002. Available http://www.auscert.org.au/render.html?it=1970&cid=1920.
[10] AusCERT, UNIX Security Checklist, v2.0, 2001. Available http://www.auscert.org.au/render.html?it=1935&cid=1920.
[11] R. Sandhu and S. Samarati, "Authentication, Access Control, and Audit," ACM Computing Surveys, vol. 28, no. 1, 1996, pp. 241-243.
[12] J. Ellis and T. Speed, The Internet Security Guidebook: from Planning to Deployment. San Diego: Academic Press, 2001.
[13] R. Duncan, "An Overview of Different Authentication Methods and Protocols", 2001, unpublished. Available http://rr.sans.org/authentic/overview.php
[14] E. Spafford, "Observing Reusable Password Choices," UNIX Security Symposium III Proceedings, 1992.
[15] J. Franks, "RFC-2617 HTTP Authentication: Basic and Digest Access Authentication," 1999, unpublished.
[16] K. Fu, "Dos and Don'ts of Client Authentication on the Web," Proceedings of the 10th USENIX Security Symposium, 2001.
[17] S. Hada and H. Maruyama, "Session Authentication Protocol for Web Services," Proceedings Symposium on Applications and the Internet Workshops, Nara, Japan, 2002.
[18] T. Verschure, "Smart Access: Strong Authentication on the Web, Computer Networks and ISDN Systems, vol. 30, 1998, pp. 1511-1519.

[19] J. Joshi, "Security Models for Web-Based Applications," Communications of the ACM, vol. 44, no.2, 2001, pp. 38-44.
[20] J. Park, R. Sandhu, and A. Joon, "Role-Based Access Control on the Web," ACM Transactions on Information and Systems Security, vol. 4, no. 1, 2001, pp. 37-71.
[21] Publications and Web Services OWASP, A Guide to Building Secure Web Applications, 2001. Available http://www.owasp.org/
[22] R. Peteanu, Best Practices for Secure Development, 2001. Available http://members.rogers.com/razvan.peteanu