"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 6, No. 4, pp. 135–138
P-ISSN: 2069-0932, E-ISSN: 2066-1061
© 2014 Pro Universitaria
www.orizonturi.ucdc.ro

# INFORMATION SECURITY FOR WEB SERVICES – PROACTIVE AND REACTIVE SECURITY TECHNIQUES

**Nicoleta Magdalena IACOB[1], Costinela-Luminiţa DEFTA[2]**

[1] *Faculty of Finance, Banking and Accounting, "Dimitrie Cantemir" Christian University, Bucharest, Romania, E-mail: nicoleta.iacob_2007@yahoo.com*
[2] *Faculty of Tourism and Commercial Management, "Dimitrie Cantemir" Christian University, Bucharest, Romania, E-mail: lumi.defta@yahoo.com*

***Abstract*** *Over the past years, e-learning portals helped teachers to streamline learning process, users to decrease associated costs involved in traditional learning process and in this way customer satisfaction was increased and the impact of this teaching method increased worldwide. Web servers are a fundamental component for almost every e-learning application. In this paper we will categorize the most frequent security threats associated with web and SQL services and present the ways to mitigate security threats such as distributed denial of services attacks on web services using the capabilities of a network device from a recognized leader in network security.*

**Key words:**
Distributed databases, E-learning, Security, Web Services, Distributed denial of service
**JEL Codes:**
L86

## 1. Introduction

E-learning platforms have drastically improved the way people learn today. Users can easily access the learning application on their personal devices at any time, flexibility being one of the main advantages of such an application. Additionally, each user is able to learn according to his preferred strategy and in his own pace and so everyone can benefit from the value added learning process that the platform offers and enjoy learning. In this way, these types of online platforms help increase the productivity of the students and help them find a learning style that suits their needs.

Such an e-learning application model based on Oracle Application Express web platform and Oracle distributed databases was developed in thesis "*Distributed databases. A dynamic model fully decentralized and automated"* (Ciobanu-Iacob, 2014). But this model requires networks that support big data traffic, and these networks must be scalable to support increasing numbers of users to address the need for greater capacity and performance. As networks grow and support more and more services and applications, they become more vulnerable to security threats. To combat those threats and ensure that electronic applications are not hacked, security techniques (Ciobanu-Defta, 2012; Ciobanu-Defta and Ciobanu-Iacob, 2012) must play a fundamental role in any type of environment.

## 2. Web and SQL Servers Security Threats

Web applications are exposed to some specific vulnerability due to their method of access (web browsers) and integration with databases in backend. The actual web servers configurations commonly presents to users multiple web applications running on a single server and available through some standard network ports (80 and 443), giving attackers a big area to compromise.

There are many common attacks that can occur against different applications servers and they depend on the installed applications (for example Web, SQL, ERP etc.), operating system running on the server (for example Windows or Linux), and environment (network where the server is running). In this section we will briefly describe some of the generic attacks that can compromise the server (Boyles, 2010).

- Denial of service (DoS) is an attack in which one system attacks another with the intent of consuming all the resources on the system (such as bandwidth or processor cycles), leaving nothing to use for other legitimate requests from normal clients. This is accomplished by increasing traffic on web site so much that the victim's server becomes unresponsive.
- Distributed denial of service (DDoS) is an attack similar with DoS, but at a larger scale, because the attack is orchestrated from multiple systems from many countries around the globe.

The most common DDoS attacks are:

- Port scanning attack. A port scanning attack is performed by systematic scanning of a host using some programs. For example, an attacker can scan a Web server with the intention of finding exposed services or other vulnerabilities that can be further exploited.

- Ping flooding attack. A ping flooding is a classical type of attack where the attacker send sends ICMP echo requests packets as fast as possible without waiting for replies.
- SYN flooding. This attack requires knowledge of the TCP/ IP protocol suite because this is a network protocol targeted type of attack. In SYN flood the attacker sends a SYN packet to target host which then respond with SYN acknowledgement. In the end of communication, the attacker does not send any ACK packet back to the target host and this causes the connection to remain in half open state. TCP connection established to the attacker host is not ending, waiting for the session to expire. The attacker continue sending new SYN packets until TCP SYN queue is filled and cannot accept any new connections.
- IP packet fragmentation attack. In this attack, an attacker change the TCP/IP protocol behavior to break packets up into smaller pieces, or fragments, that bypass most intrusion-detection systems.

- Password attacks. Password attacks can be implemented using different methods, including brute-force attacks and packet sniffers. Although packet sniffers can reveal user accounts and passwords, from network packet captures where an attacker can see in clear or decrypt some passwords, password attacks usually refer to specific attempts to identify a user account, password, or both. A brute-force attack is performed using some programs that run across the network and attempt to log in to the attacked server using various users and passwords. When a user account is compromised and if this account has enough privileges, the attacker can gain access to the system.
- Cross-site scripting or XSS is a technique that makes use of vulnerabilities in web applications. In a cross-site scripting attack, data is entered into an application which is later written back to another user. If the application is not coded is such a way to validate the data correctly, it may simply echo the input back allowing the insertion of malicious code into the web page.
- SQL injection type of attack search for a vulnerability in the database associated with a web application. The malicious code is inserted into strings that are later passed to the SQL server, parsed, and executed.
- Malware is a malicious software. It consist of viruses, bots, spyware, worms, trojans, rootkits, and any other software intended to disrupt normal user activity and collect personal data.

## 3. E-Learning Platforms Security

In the diagram below (Figure 1), we figured a typical network and systems architecture for an e-learning platform (Baron et al, 2014), consisting of a database server and a web server to serve client requests. We choose an Adaptive Security Appliance from Cisco to defend servers from various security threats. Cisco ASA provide an end to end security solution, offering protection from OSI (Open Systems Interconnection model) layer 2 to 7. The built in IPS (Intrusion Prevention System) enhance firewall protection by looking deeper into the packets to provide real-time ip protection against worms, trojans, and exploits against application and operating systems vulnerabilities (Iacob, 2014).

We will present two types of security techniques related to two types of web services attacks:

1) Proactive technique (we threat a problem before it become an issue) used against distributed denial of service attacks on web services using tcp syn type of attack;
2) Reactive technique (we threat the problem as it arrives) used against distributed denial of service attacks using http applications resource exhaustion.

1) TCP SYN attack is a type of DoS attack in which a sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, in this way denying service to legitimate TCP users.

When a normal TCP connection starts, a destination host receives a SYN packet from a source host and sends back a synchronize acknowledge (SYN ACK). The destination host must then hear an ACK of the SYN ACK before the connection is established. This is referred to as the TCP three-way handshake. In this type of attack the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as web services) to legitimate users.

A proactive approach for this type of attack means to configure the Adaptive Security Appliance to be ready to mitigate tcp syn attack before this will happen.

In order to identify the traffic, we will create a policy map that will match http type of traffic (to protect internal web server) and define the necessary connection limits. The policy map will be applied to the outside interface:

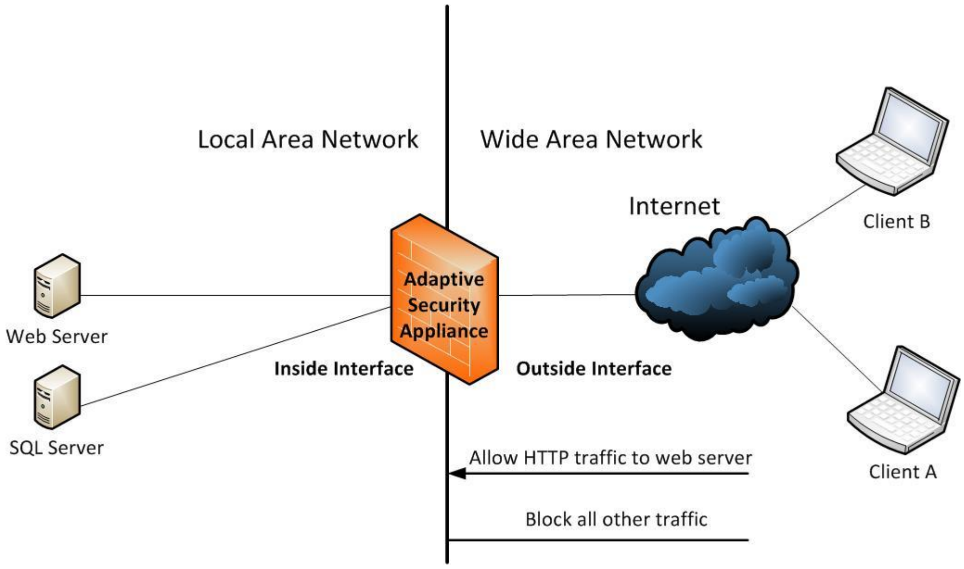

*Figure 1.* Typical network and systems architecture

class-map *web_protect*
match port tcp eq 80 //match http type of traffic – port 80
policy-map *synattack*
class *web_protect*
set connection conn-max 100
*// maximum number of simultaneous connections*
set connection embryonic-conn-max 500
*// maximum number of simultaneous embryonic connections*
set connection per-client-embryonic-max 100
*// maximum number of simultaneous embryonic connections allowed per client*
set connection per-client-max 5
*// maximum number of simultaneous connections allowed per client*
service-policy *synattack* interface outside
*// policy is applied on outside interface of security device*

An embryonic connection is a TCP connection request that has not finished the necessary handshake between source and destination. When embryonic connections are configured on ASA, the security appliance intercepts the initial SYN from going to the backend server and forwards the connection only when the 3-way handshake is complete.

2) As a basic security measure, we configured an access list on appliance that permits to enter in local area network only http traffic destined for the web server and have applied this access list on outside interface (the interface facing Internet). All other traffic will be dropped at the outside interface by the security appliance. By using such an inbound ip packet filter, the sql server is not exposed to the internet and web server is exposed only on port 80 (required to server http requests to students using e-learning web platform). If a packet is denied by the access list, the security appliance discards the packet and generates a syslog message indicating that such an event has occurred.

access-list *WEBTRAFFIC* extended permit tcp any host 4.4.4.4 eq www *//where 4.4.4.4 is the ip address of the web server*

But this type of access list does not help us to deal with application resource exhaustion Dos attack, which means that the attacking servers/botnets create thousands of application requests (http requests) to our web server, thus consuming the application resources. Http application attacks usually have a pattern or string which may help distinguish the attacking http requests from other legitimate requests. Analyzing http attacking packets, we might find such a common parameter or string, which can be for example a common POST or GET URI request. With the ASA HTTP inspection feature we can match on this common pattern in the HTTP packet and in this way we can filter the attacking packets and drop them.

We will use the access list WEBTRAFFIC that match all traffic destined to our webserver and add to this http inspection:

regex *malicious* dfr9xd *//define malicious string found in all requests implied in attack*
class-map *WEBTRAFFIC*
match access-list *WEBTRAFFIC*
*//packet classification that match the access list for web traffic*
policy-map type inspect http *DOS* *//HTTP inspection policy to match on the malicious string*

```
        parameters
        match request uri regex malicious
                drop-connection
        match request args regex malicious
                drop-connection
    policy-map BLOCKATTACK
        class webtraffic
                inspect http DOS
     service-policy BLOCKATTACK interface outside
                //  policy is applied on outside
                interface of security device
```

## 4. Conclusions

Securing any type of server that run in a network environment is not an easy task. Web and sql servers are one of the most critical type of servers, because of the sensitive data they usually host. Appropriate security practices are essential to operating and maintaining a secure server, because security practices help ensure the confidentiality, integrity and availability of information system resources. All the security techniques described in this article help assure a very good protection for information systems and are the baseline for searching the perfect protection.

### References

Baron, C., Șerb, A., Iacob, N.M. and Defta, C.L. (2014): “IT Infrastructure Model Used for Implementing an E-learning Platform Based on Distributed Databases”, *Quality-Access to Success,* Vol. 15 / S2 / 2014, pp. 195-201.

Boyles, T. (2010): “CCNA Security Study Guide”, Wiley Publishing.

Ciobanu (Defta), C.L. (2012): „Wireless LAN Security - WPA2-PSK Case Study”, *Global Journal on Technology since*, Vol. 1 / 2012, pp. 62-67.

Ciobanu (Defta), C.L. and Ciobanu (Iacob), N.M. (2012): “Methods for Securing Routing Protocols in Ad-Hoc Networks”, *SYNASC 2012 - 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, September 26-29, 2012, Timișoara, Romania, *IEEE post-proceedings* 2013, pp. 341-348.

Ciobanu (Iacob), N.M. (2014): “*Distributed databases. A dynamic model fully decentralized and automated/ Baze de date distribuite. Un model dinamic complet descentralizat și automatizat”*, Editura Pro Universitaria, București, 2014, ISBN 978-606-26-0095-2.

Iacob, N.M. (2014): “Information security for web and SQL services”, *Proceedings of the 9th International Conference on Virtual Learning 2014. Models & Methodologies, Technologies, Software Solutions*, University of Bucharest, Faculty of Psychology and Educational Sciences, Siveco Romania, October 24-25, 2014, pp. 408-412.

Tracy, M., Jansen, W., Scarfone, K. and Winograd, T. (2007): “Guidelines on securing public web servers”, Nationals institutes of standards and technologies, September 2007.

www.cisco.com, ASA configuration guides, accesed 2014.