УДК 681.3.06

V. KHARCHENKO, A. FURMANOV, A. GORBENKO

National Aerospace University «KhAI», Ukraine

INTRUSION TOLERANCE OF WEB-SYSTEMS: IMEA-ANALYSIS AND MULTIVERSION ARCHITECTURE

The kinds of network attacks are considered, their classification is carried out and the IMEA-table (Intrusion Modes and Effect Analysis) is designed. The multiversion variant of Web-system architecture tolerated to some kinds of network attacks resist is proposed. On the suggested architecture basis the taxonomy of diversity levels is proposed. Compatibility matrixes of the modern Web-systems components are analyzed. Result of work is the variants of the Web-systems graph, which allows choosing a configuration of the future system for achievement of a maximum level of the system diversity.

fault tolerance, intrusion tolerance, multiversion approach, web-service architectures

Introduction

The high level of modern technologies development is caused by many factors, but recently one of basic is a factor of the information streams increasing. High speed of the information distribution is one of the consequences of Internet globalization and the increasing prevalence of the Web-applications which plays main role in access to this information. Consequence of impetuous distribution of Web-applications also is the problem of the network attacks increasing. This fact is connected with the network technologies imperfections which have been not designed for their malicious use [1, 2].

The Web Service architecture [3] is rapidly becoming the de-facto standard technology for achieving interoperability between different software applications running on a variety of platforms. This architecture supports development and deployment of systems in which component system integration can be postponed until the systems are executed. Individual components (i.e. Web Services – WSs) advertise their services via a registry (typically developed using the UDDI standard [4]).

The WS architecture is in effect a further step in the evolution of the well-known component-based system development with off-the-shelf (OTS) components.The main advances enabling this architecture have been made by the standardisation of the integration process (a set of interrelated standards such as SOAP [5], WSDL, etc.).

There are various ways of Web-applications stability maintenance from network attacks: from the administrative company rules up to firewalls and hardware systems of attacks detection [6].

However, even the advanced protection means not always cope with a problem of maintenance of system stability [7].

Hence, the problem of the Web-systems advanced architecture design with the purpose of maintenance of higher parameters of fault tolerance and stability from network attacks is up-to-date. One of the useful decisions is a diversity principle using at architecture of system construction. The purpose of this paper is development of intrusion tolerance analysis technique and multiversion intrusion tolerant Web-system architecture.

Classification and the analysis of attack kinds

The set of network attacks (fig. 1) can be classified by the following attributes: character of influence, purpose of influence, attack start condition, feedback presence with attacking object, target location and level of ISO/OCI model on which influence is carried out, etc.

The basic attack kinds are following.

1. The network traffic analysis is the typical remote influence consisting in listening of an information channel. Such influence is distributed computing systems

© V. Kharchenko, A. Furmanov, A. Gorbenko

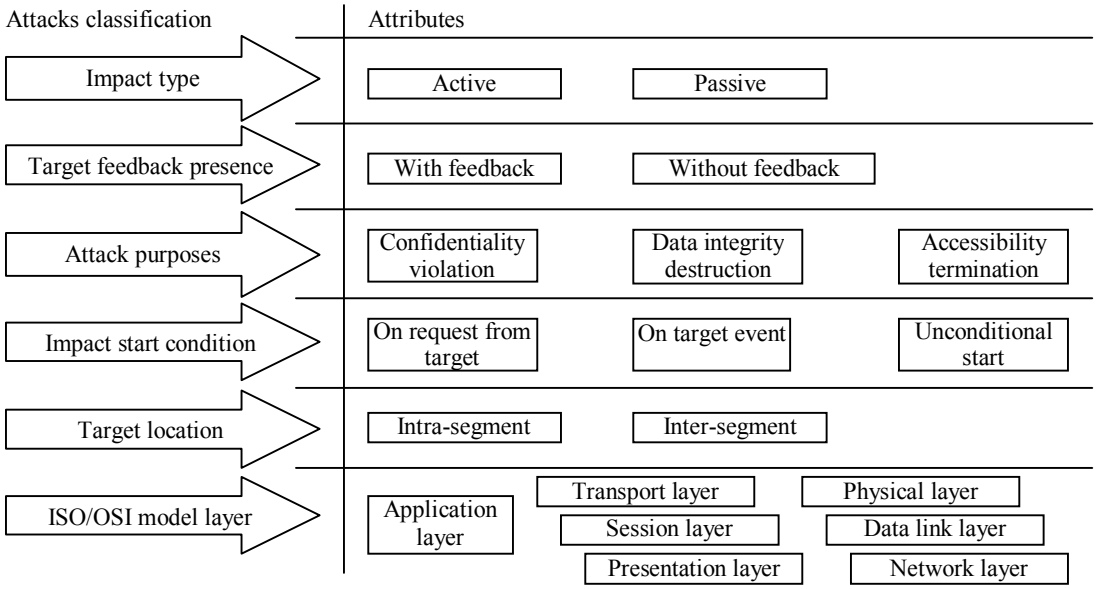

Fig. 1. Network attacks taxonomy

(DCS) specific. The network traffic analysis allows studying logic of DCS work. It's achieved by exchange packages interception and the analysis at a channel level. The knowledge of DCS work logic allows modeling and carrying out the typical remote attacks in practice.

2. Denial of Service (DoS-attack) – remote service availability infringement on the attacked object (remote access exchange impossibility from other DCS objects).

3. Trusted object substitution – is possible when DCS uses unstable remote objects identification algorithms (for example, only the IP-address). This is the message transfer on network channels from the any DCS object.

4. Trusted object embedding (lacks of the remote search algorithms) – in DCS often is necessary to receive addresses of remote objects. For this purpose the search query (ARP-, DNS-) is formed and the answer with the remote object address inside is expected. There is a probability of the false answer production that will lead to false object addressing. All further information streams will pass through fake DCS object.

5. Trusted object embedding (false route obtrusion) - a variant of false object embedding in DCS. This method consists in periodic transfer of beforehand prepared false answer to attacked object without receiving of search results. Thus attacking object can provoke attacked object to transfer of search query and then its false answer will be immediately to achieve a success.

Let's carry out the analysis of attacks kinds in an angle of modes and intrusion effects. Result of such analysis is the IMEA-table (Intrusion Modes and Effects Analysis) (tabl. 1).

From this table we can see that the most often attacks belong to "Denial of Service" class. The reason of this fact is carrying out simplicity of such attack type which needs a minimum of knowledge and skills.

Attacks of "Denial of Service" class differ from attacks of other types. They are not aimed to take over of access to a network or on receiving any information from this network. Attack of "Denial of Service" class makes the network inaccessible to use at the expense of the network, operation system or the application allowable functional limits exceeding.

In the process of "Denial of Service" class attacks usual Internet-protocols, such as TCP and ICMP (Internet Control Message Protocol) can be used. The majority of this class attacks bases not on program mistakes or gaps in system safety, and on the common system architecture weaknesses. Some attacks reduce to zero productivity of a network by overflowing it with the undesirable and unnecessary packages or by informing false information about the network resources current status.

This attacks type is difficult for preventing because it needs coordination with the Internet service provider (ISP). If the traffic intended for your network overflowing cannot be stopped on the ISP-side then it's impossible to stop it on the network input because all bandwidth will be taken.

Table 1

IMEA-table

Kinds of remote attacks	Modes					Intrusion effects		
	Character of influence	Condition of attack beginning	Feedback presence	Target location	ISO/OSI level	Attack results	Attack probability	Attack criticality
Network traffic analysis (Sniffing)	Passive	Unconditional attack	Without feedback	Intra-segment	Channel	Confidentiality violation	Average	Low
Denial of Service (DoS-attack)	Active			Intra- & inter-segment	All but the physical	Accessibility violation	High	Average
Trusted object substitution		On target event	Any		Network	Confidentiality & data integrity violation	Average	High
Trusted object embedding (lacks of remote search algorithms)		On request from target or unconditional attack	With feedback		Network, transport		Low	
Trusted object embedding (false route imposing)		Unconditional attack	Any		Channel, network, transport	All possible	Average	

Compatibility analysis

There is a wide range of various components for construction of Web-systems. For a components choosing it's necessary to construct compatibility matrixes of Web-servers with OS (tabl. 2), application-servers with OS (tabl. 3), and also application-servers with Web-servers (tabl. 4). Sign "+" corresponds to pairs of compatible components.

Overwhelming application-servers majority uses Java technology at which using JDBC (Java Database Connectivity) technology becomes available for accessing to databases. There are JDBC-drivers for data accessing to all industrial databases. Since Java technology is cross-platform (independent from a hardware platform, operation system, etc.) the problem of application-servers compatibility with databases servers does not exists.

Using compatibility matrixes we shall construct graph of multiversion system variants (fig. 2) which will allow us picking up channels optimally, depending on the requirements which are declared to the system.

Nodes of this graph correspond to the multiversion variants at the each diversity levels whereas arcs assign compatibility features. As a result, all possible diverse system configurations can be identified. Different types of arcs shading show which components are compatible and which of them can be selected to a whole configuration. For example: we can compose a multiversion architecture of two channels, i.e. the system will contain two selected variants of system configuration from the graph.

Table 2

Compatibility matrix (Web-servers/OS's)

Web-server\ OS	Win2K	WinXP	Mac OS X Server	Solaris 9	HP-UX 11	Linux	AIX
Apache	+	+	+	+	+	+	+
Internet Information Server	+	+					
Lotus Domino Go WebServer	+			+	+	+	+
Sun ONE Web Server	+	+		+	+	+	

Table 3

Compatibility matrix (Application-servers/OS's)

Application-server\ OS	Win2K	WinXP	Mac OS X Server	Solaris 9,10	HP-UX 11	Linux	AIX
Apache Tomcat	+	+	+	+	+	+	+
BEA WebLogic	+	+		+	+	+	
Caucho Resin	+			+		+	
IBM WebSphere	+			+	+	+	+
JBoss	+			+	+	+	
Oracle Application Server 10g	+			+	+	+	+
Sun Java System Application Server	+	+		+		+	

Table 4

Compatibility matrix (Application-servers/Web-servers)

Web-server \ Application-server	Built-in Web-server included	Apache	IIS	Lotus Domino Go WebServer	Sun ONE Web Server
Apache Tomcat	+	+			
BEA WebLogic	+	+	+		+
Caucho Resin	+	+	+		
IBM WebSphere	+	+	+	+	
JBoss	Apache Tomcat				
Oracle Application Server 10g	Apache				
Sun Java System Application Server	+				

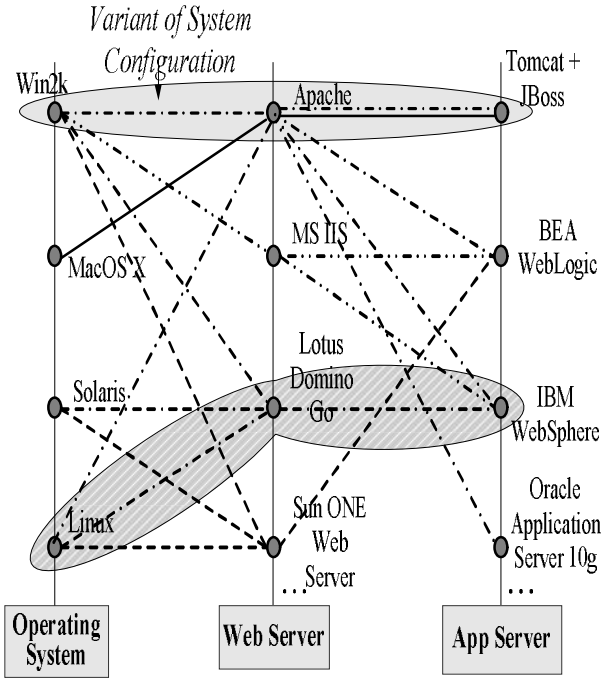

Fig. 2. Graph of multiversion systems variants

Multiversion architecture

The majority of "Denial of Service" class attacks are caused by architectural lacks of modern systems. Hence, using a diversity principle at the architecture level can increase system tolerance to these attacks.

In such architecture (fig. 3) it's possible to distinguish various levels of diversity, such as: hardware level, operation systems (OS) level, Web-server level, application-server level and database management system (DBMS) level. It's obvious that not all application-servers are compatible with various Web-servers as, in its turn, not all of Web-servers are compatible with various operation systems. Therefore the basic criterion for choosing diverse variants at various levels of system construction is compatibility.

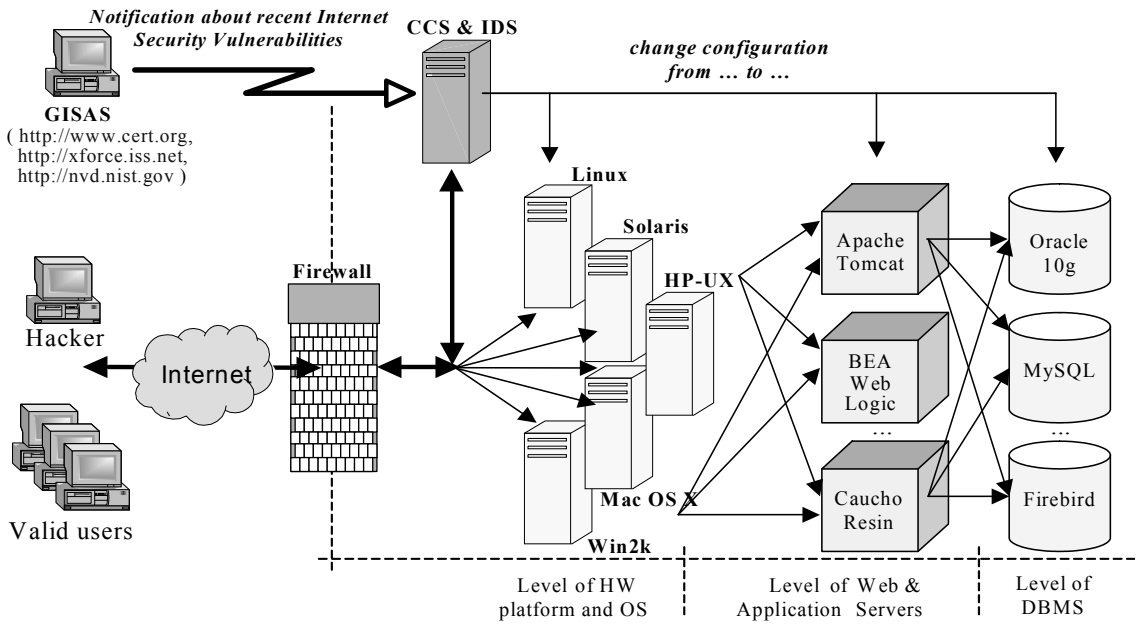

Fig. 3. Web service multiversion architecture

Conclusion

Proposed approach has the following advantages:

a) guarantees the reliable decision of system fault tolerance and tolerance to network attacks of "Denial of Service" class;

b) increases system availability, i.e. the idle time of system is reduced that is especially important for some commercial systems (payment, bank, etc.);

c) general system's productivity grows at the expense of several reserve channels simultaneous use (the equivalent circuit with a hot reserve).

This approach has also a number of limitations:

a) complexity of system as a whole and its cost grows accordingly;

b) reduction of the data confidentiality (it's enough to crack one of channels for the data integrity infringement of all system).

In the future researches it's necessary to develop fuller graph of components compatibility, to construct mathematical model for evaluation of variants weight by various criteria, to increase diversity system's protection from penetration of malefactors with the purpose of the data integrity infringement.

References

1. Scoudis E. Counter Hack. – PH, 2001. – 512 p.

2. W3C Working Group, Web Services Architecture. – [Электрон. ресурс]. – Режим доступа: http:// www.w3c.org/TR/2004/NOTE-ws-arch-20040211.

3. Gorbenko A., Kharchenko V., Tarasyuk O. FMEA technique of Web Services Analysis and Dependability Ensuring // Proc. Workshop on Rigorous Eng. of Fault-Tolerant Systems (REFT' 2005). Newcastle, 2005.

4. Веб-сайт "Oazis-Uddi". – [Электрон. ресурс]. – Режим доступа: http://www.uddi.org.

5. SOAP Version 1.2. – [Электрон. ресурс]. – Режим доступа: http://www.w3.org/TR/soap12-part0.

6. Kader M. Network attack types. – [Электрон. ресурс]. – Режим доступа: http://www.cnews.ru/reviews/ free/oldcom/security/cisco_attacks.shtml.

7. Харченко В.С., Фурманов А.А. Обеспечение отказоустойчивости и устойчивости WEB-приложений от сетевых атак за счет использования диверсного подхода // Мат. II наук. конф. ХУ ПС, 15-16.02.2006. – Х.: ХУ ПС, 2006. – С. 87.

Поступила 15.03.2006

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.