ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

UDK 004.056

RASIM MAHAMMAD OGLU ALGULIEV, IRADA YAVAR KIZI ALAKBAROVA

Institute of Information Technologies of ANAS

COMPARATIVE ANALYSIS OF INFORMATION ATTACKS IN INTERNET

Аннотация: В статье перечислены средства информационного оружия, осуществлены анализ и классификация информационных атак. Также рассмотрены самые распространенные информационно-сетевые атаки, такие как CSS атака, "расщепление" HTTP-запроса, SQL инъекция, утечка информации и т.д. А также осуществлен сравнительный анализ уязвимостей веб-приложений.

Ключевые слова: информационные атаки, информационное оружие, логические атаки, DoS атака, подделка DNS, внутренняя атака, CSS атака, SQL инъекция, утечка информации, SSI инъекция, веб-приложение.

Abstract: The article describes the tools of information weapons, the analysis and classification of information attacks are conducted. Also, most common information network attacks such as Cross-site Scripting, HTTP Response Splitting, SQL Injection, Information Leakage and others are examined, comparative analysis of vulnerabilities of Web Applications is carried out.

Key words: information attacks, information weapons, logical attacks, denial of service attack, DNS spoofing, insider attack, CSS attacks, SQL injections, information leakage, SSI injection, web-application.

Introduction

Currently, information warfare, conducted using computer networks, as well as global computer network Internet are gaining a critical character. At the moment, information warfare can be defined as a purposeful activity from any party towards state governmental body, masses of people or a single person using information technologies and resources [1].

Information warfare – is a war conducted for the purpose of seizure of primary, energetic, human resources of one country using highest levels (ideological, chronological, and methodological) of common facilities of society control [2]. Information warfare is a natural result of development of worldwide scientific-technical mind and improvement of computer and information technologies create prerequisites for development and application of information weapons. Possession of effective information weapon and protection means from it, are becoming one of the main conditions of provision of homeland security of the government in XXI century [3].

Information warfare is directed to obtaining capital and power. A necessity of protection of national informational resources and preservation of confidentiality of informational exchange at World Wide Web occurs, because of possible emergence of political and economical confrontations of governments, new crisis' in international relations on this basis [4]. Thus, informational security, information warfare and information weapon are currently in the center of the spotlight.

Relevance

The world is undergoing global changes at the moment: technologies revolution related to development of information technologies and telecommunications, creation of new markets, financial revolutions carried out through globalization of capital flows and savings management. Under these new terms, the society has become more vulnerable – as on governmental level, as well as on the level of individual enterprises, for which informational risk has become number one risk.

Necessity of research of given topic is caused by the fact that currently intergovernmental, international conflicts are increasingly carried out in information sphere, mainly in Internet. Diversity of information weapon and information attacks, specifics of occurrence and application has generated complex protection tasks from them.

Objective

Objective of the article is general analysis and classification of information attacks on Internet, as well as statistical analysis of vulnerabilities of web-applications.

Tasks

The main of the article is:

1. analysis and classification of information attacks based on their impact characteristics;
2. analysis of detected vulnerabilities of web-applications. Comparison of vulnerabilities of web-applications during four years.

Only vulnerabilities of web-applications are considered in conducted statistics. Such widespread deficiencies such as absence of relevant refreshments of OC security and erroneous setting of Web-server are not taken into consideration.

Information Weapons

Currently, information warfare is carried out in several forms. Information warfare in Internet is spread from network security breaches, financial fraud, intervention in personal life and theft of personal data till virus infection and spam distribution.

Information warfare is carried out using special means called information weapons. Information weapons – is a composite of program and technical means, intended to control the information resources of the target object and intervention into operation of its information systems [5]. Information weapon is distinguished from warfare weapon by low expenses and high application effectiveness. It doesn't destroy the opponent, development of complex structures and particularly trained specialist are not required for it, and there's not necessity to cross the borders [6].

Following means are called information weapons:

- limitation of access to information of legal users;
- highly-precise determination of location of equipment radiating in electromagnetic spectrum and its fire damage;
- overcoming of security systems;
- impact on components of radio electronic equipment;
- means of impact on program resources of electronic control modules;
- destruction or deterioration of information systems, theft of information masses;
- Attack with an objective of disorganization of operation of computer systems, technical means.
- Effect on information transfer process;
- Propaganda and disinformation;
- Psychotropic weapon.

Information weapon gives the maximum effect only when it's applied on the most vulnerable parts of the information systems. Systems that are most sensitive to input information – decision making, control systems have the highest informational vulnerability.

Classification of information attacks

Actions with application of information weapons are called information attacks. During information attacks, means which allow carrying out planned actions [7] with transferred, processed, created, destroyed and perceived information are used as information weapons. The main objective of any classification of information attack consists of proposal of such classification factors, which allow accurate description classified occurrences or objects.

Information attacks of remote character can be classified by their impact objective [8]:

- Violation of privacy of information or resources of the system
- Violation of information integrity;
- Violation of system accessibility.

This classification feature is the direct projection of three main types of threats: disclosure, integrity and service denial.

The main objective of practically any attack – is to obtain unauthorized access to information. There are two principal possibilities of access to information: interception and distortion. Possibility of interception means gaining access to it, but impossibility of its modification. Consequently, interception of information leads to violation of its confidentiality. Possibility of distortion of information means either full control of information flow among system objects, or possibility of transfer of messages on behalf of another object. Thus, obviously, distortion of information leads to violation of its integrity. Another principally different objective of an attack is obtaining of unauthorized access to information by the attacker.

Another objective of an attack is violation of accessibility of the system. In this case, the attacker is not supposed to obtain unauthorized access to information. His main objective is – to achieve that access to the resources of the attacked target would be impossible.

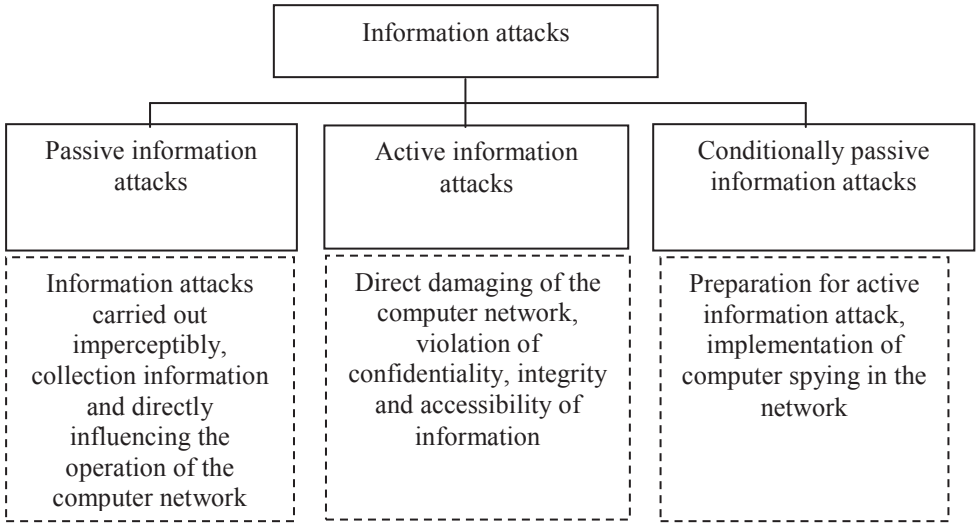
Based on abovementioned, it is obvious, that information-network attacks can be classified by their impact characteristics: passive, active, conditional-passive (pic1).

Servers and workstations are main components of any information network. The task of the server is storage of information and provision of access to information and some kinds of services. Consequently, all possible objectives of information attacks can be classified as following:

- Obtaining access to information
- Obtaining unauthorized access to services
- Attempt of making a defined class of services inoperable
- Attempt of changing information or services, as an auxiliary stage of a larger attack.

Information- network attacks in Internet environment

«Internet Security Threat Report» report of Symantec Company demonstrates that, up to 70 percent of vulnerabilities used by intruders fall on web-applications.
Wide-spread vulnerabilities of web-applications are divided in six classes:
1. Authentication.
2. Authorization.
3. Client-side Attacks.
4. Command Execution.
5. Information Disclosure.
6. Logical Attacks.



Pic. 1. Classification of information attached by their impact characteristics

There are several varieties of attacks in each class. Information-network attacks are as diverse, as the systems against which they are directed. Some attacks are distinguished by complexity. Others can be carried out by an ordinary operator, without even presuming what subsequences his actions might have. For evaluation of attack types it is necessary to know some limitations, initially inherent to TPC/IP protocol.

Different information-network attacks are used for these purposes. These include:

– DoS attack (Denial of Service Attack) – Denial of service attack, sending the server a large number of requests, artificially created by the attacking party, as well as sending a large number of TCP-, UDP- or UMP-packages, incorrectly fragmented UMP-packages etc. Typical examples of DoS attacks – automatic blocking of unsuccessful registration attempts, especially when mechanism of automatic unblocking mechanism is not supported.
– DNS spoofing – spoofing of identifiers of computer network, replacement of DNS replies with fake ones.
– Insider attack – attack from within the protected network,
– IP spacing/hijacking, session stealing – attacking the access channel,
– IP spoofing – spoofing of approved external and internal IP-addresses of the system,
– (Brute-force attack – attack on ciphertext or electronic digital signature, using direct search of all possible cipher key options.
– CSS attack (Cross-Site Scripting, XSS) – attacks during which a foreign code is intruded into loaded web page. Specifics, of the given attacks consist of that fact that, instead of direct attack of the server, they use a vulnerable server as a mean of attack on the client.
– SQL Injection – attack used to exploit web-sites, forming SQL requests from the user input data flow.
– Content Spoofing – attack for deception of confidence of the user that the certain content presented on the web-site is authentic, is not derived from an external source.
– Information Leakage – different types of information leakage. Attacks of given class are directed at obtaining additional information on web-application. Location of temporary files or reserve copies can be contained in the leaked information.
– HTTP Response Splitting- It can be used for implementation of intersite attacks.
– XPath injection – attack for exploitation of web-sites, creating XPath requests from the user input data flow,
– SSI Injection) – attack allowing the intruder to send a code in web-application, which will be executed by the web-server locally.
– etc.

Analysis of the attacks and vulnerabilities of web-applications

Simplicity of HTTP protocol allows developing effective methods of automatic analysis of web-applications and detection of their vulnerabilities. This allows the attacker to detect a large number of vulnerable web-sites, in order to execute an attack on them. Possibility of using web-applications as an attack platform to work stations makes these applications an attractive target for intruders. During preparation of an attack on information infrastructure of the company, the intruder researches its web-application at first instance.

Positive Technologies Company, during the process of evaluation of network safety in 2007, 2008, 2009 yrs obtained statistical data on vulnerability of web-applications. Main direction of company operation – is protection of computer networks from unauthorized access. Data was based on results of automated scanning of hosts of public hosting-provider and manual analysis of safety of web-applications [8].

Detected vulnerabilities were classified in accordance with Web Application Security Consortium Web Security Threat Classification (WASC WSTCv2). Criticality of vulnerability was evaluated in accordance with CVSSv2 (Common Vulnerability Scoring System version 2) with further mapping to risk levels of PCI DSS (Payment Card Industry Data Security Standard) information security standard.

Statistics demonstrated that, during last four years, (Cross-Site Scripting, XSS) is the most wide-spread vulnerability class. This average level of risk can be used for execution of an arbitrary code in the browser of the clients on script language (for example JavaScript) for the purpose of theft of identification data, replacement of screen content, execution of "phishing" type attacks etc. Given error was detected in all analyzed applications. Analysis demonstrated that practically three-quarters of all sites contain a similar error [9].

In 2009, SQL Injection was the second most popular vulnerability class. Using given vulnerability, intruders obtain capability to read and modify information in the data base used by the web-application. In some cases, exploitation of SQL Injection can be resulted in obtaining full control on the server. Therefore, vulnerability of given type is classified as high level risk.

Predictable Resource Location was the third popular vulnerability class. Underestimation of the risk, available from Internet, which can affect the vulnerability of web-applications, is possibly the main reason of the low level of security of their majority.

Analysis of vulnerabilities of web-applications in 2009 demonstrated that practically half of analyzed systems contained vulnerabilities. As a result of conduction of 6239 automatic scans and detailed analysis of 77 web-applications, data on 5560 web-applications was collected in statistics. In total, 13434 errors of different risk levels were detected in all applications, 1412 samples of malicious code contained on the pages of vulnerable systems were recorded. The ratio of compromised sites distributing malicious software comprised 1,7%.Each of such sites contained vulnerabilities allowing execution of commands on the server, which confirms possibility of use of these vulnerabilities for discredit of the system (tab.1).

Information Leakage class attack, which was one of the most dangerous and frequently detected attacks in 2006, 2007, 2008 years, was replaced by SQL Injection in 2009 (pic. 2). Different vulnerabilities, leading to leakage of important information from the server pertain to information leakage. Inaccurate access limitation to web-resources, storage of confidential data in publicly-accessible, but "hidden" folders, reserve copies of scripts are typical examples of such errors.

As demonstrated in the analysis of attacks and based on the experience of Positive Technologies company in conduction of tests in entry and audit of information security – vulnerability in web-applications are of the most wide-spread deficiencies of network security provision.

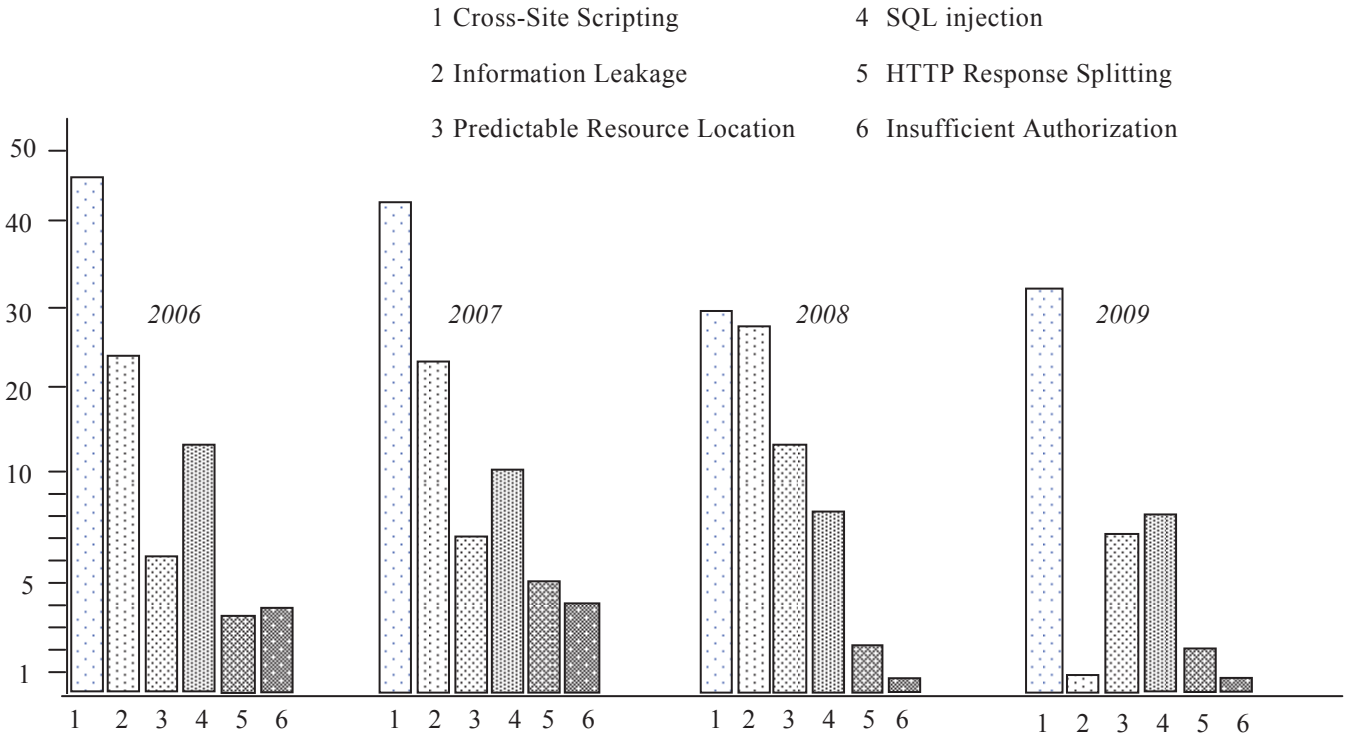
Following conclusions can be made based on comparative data analysis:

- Cross-site Scripting, different types of Information leakage, SQL Injection, HTTP Response Splitting are the most wide-spread vulnerabilities during last 4 years;
- In accordance with results of the researches, situation with security level in web-applications has improved in the year of 2009 in comparison with previous four years;
- In comparison with 2006 and 2007 years, number of sites containing widespread vulnerabilities as Injection and Cross-site Scripting has reduced, however number of sites containing different types of information leakage has increased;
- In comparison with 2006, 2007 and 2008 years, number of sites containing different types of information leakage has reduced in several times in 2009;
- The number of new attacks to be researched has increased in 2009.

Possibility of detection of critical error in web-application by an automatic scanner consists of 35% and reaches 80% at detailed expert analysis. This fact demonstrates low level security of modern web-applications not only from attacks from qualified intruders, but also from actions of attackers armed with ready-made utilities for "automatic hacking".

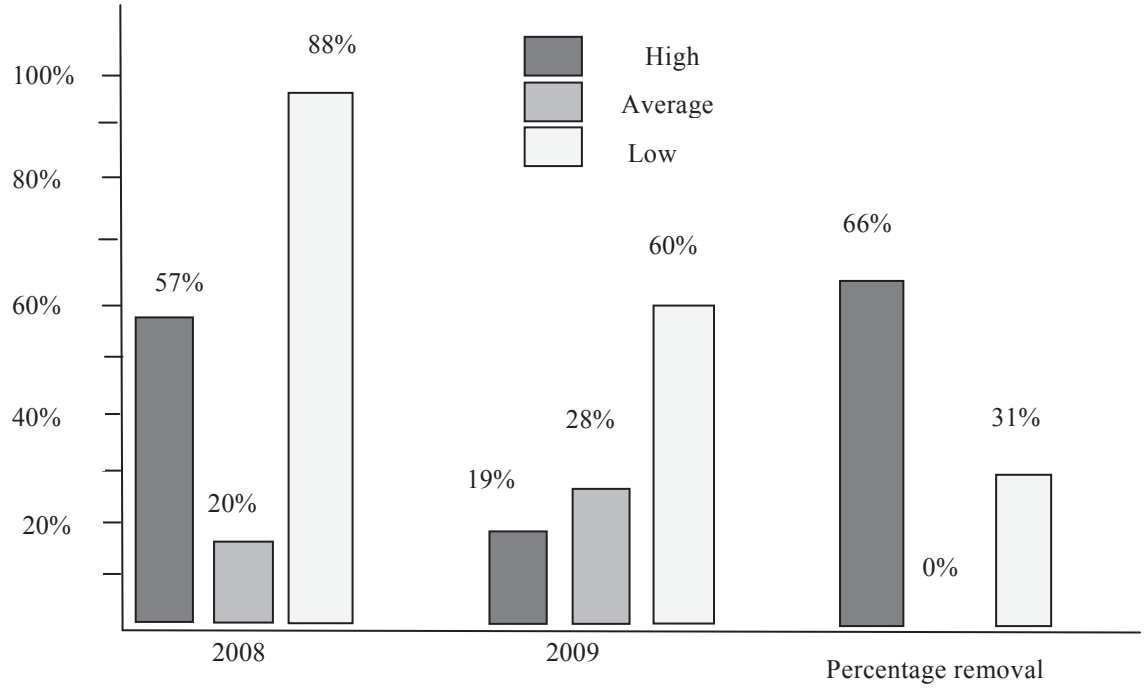
Table 1. Statistics of vulnerabilities of web-applications in years.

№	Vulnerabilities class	% Vulnerabilities 2006	% Vulnerabilities 2007	% Vulnerabilities 2008	% Vulnerabilities 2009
1	Cross-Site Scripting	44,8	43,4	30,1	33,6
2	Information Leakage	21,2	21	29,8	0,6
3	Predictable Resource Location	5,4	6,9	11,8	7,0
4	SQL injection	10,1	9,8	7,95	7,7
5	HTTP Response Splitting	3,5	3,9	0,8	1,5
6	Insufficient Authorization	3,3	2,7	0,02	0,01
7	Directory Indexing	3	2,7	0,01	0,01
8	Insufficient Anti-automation	1,6	1,8	5	6,4
9	Path Traversal	1,4	1,5	3	0,3
10	Insufficient Authentication	1,1	1,0	1,0	1,0
11	Insufficient Process Validation	1,1	1,0	1,0	1,0
12	Bruteforce	0,8	1,7	0,01	0,01
13	SSI Injection	0,3	1,0	0,4	0,6
14	other	0,18	1,6	9,11	40,27



Picture.2. Comparison of vulnerabilities of web-applications in four years

Conducting analysis of elimination of detected vulnerabilities in 2009, based on the scanning results of 2008, it was detected that total percent of elimination of all detected vulnerabilities comprise approximately 20% (pic. 3)



Pic.3. Sites with different risk level vulnerabilities (in percents).

Conclusion

As actually all network levels contain vulnerabilities, malicious hackers have an abundance of possibilities for carrying out different attacks. Without development of relevant security, any part of any network can become vulnerable to attacks or other unauthorized actions. Reading this article, one may fall under impression that global network has been affected by an incurable epidemic, which sooner or later will lead to total consequences. In reality, that is not the case. As demand creates supply, threat causes response security reaction. During the last years, information security industry has developed several sufficiently effective technologies of struggle with different types of information attacks.

However, necessary information security can be achieved only in society with high scientific-technical and industrial potential, and sufficient cultural-educational level of different layers of populations of different countries. We must also note that, only most developed and relevantly prepared countries in information technologies and telecommunications field can enter global information space.

Analysis and classification of information attacks create a possibility for selection of effective means for provision of information security and execution of relevant reaction to the intruders in Internet environment, as well as in general information exchange network.

Generally, regular analysis of web-application security and tuned process of elimination of detected deficiencies allow reducing the number of vulnerable sites in average in three times during a year.

Literature

1. Павлютенкова М. Ю., Информационная война: реальная угроза или современный миф? // "Власть", М., 2001, стр.19-23
2. Libicki M., What is Information Warfare? // National Defense University. ACIS, 1995, pp. 3
3. Dorothy Denning, Information Warfare and Security // Addison–Wesley, 1999, pp. 9-19
4. Colonel Alan D., Douglas H., Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Hardcover) // Afcea Intl. Pr., 2000, pp. 309
5. Прокофьев В.Ф., Тайное оружие информационной войны: Атака на подсознание // - М: СИНТЕГ, 2003, 408 с.
6. Szafranski R. A Theory of information warfare. Preparing for 2020 // Airpower Journal, Spring 1995
7. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet // НПО "Мир и семья-95", 1997 г., 250 с.
8. Гриняев С.Н., Интеллектуальное противодействие информационному оружию, М. СИНТЕГ, 1999, 232 с.

9. Статистика уязвимостей web-приложений за 2008 год // http://www.securitylab.ru/analytics/386759.php.
10. Статистика уязвимостей веб-приложений за 2009 год // http://www.securitylab.ru/analytics/394205.php

Стаття надійшла до редакції 15.09.2010.

About the Authors

Rasim Mahammad oglu Alguliev, doctor of Technical sciences, Professor, Corresponding member of ANAS, Institute of Information Technologies of ANAS, str. F.Agaev 9, Baku, Azerbaijan, Az1141, E-mail: director@iit.ab.az , rasim@science.az

Alakbarova Irada yavar kizi, Sector Chief of the institute, Institute of Information Technologies of ANAS, str. F.Agaev 9, Baku, Azerbaijan, Az1141, E-mail: depart17@iit.ab.az, airada.09@gmail.com