International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

The importance of self-management mechanisms to ensure Software safety

Tamilla Bayramova

Institute of Information Technology of ANAS, Baku, Azerbaijan

---

Abstract - ***The paper analyzes the threats arisen from the increasing number of software hacker attacks. In order to prevent the threats, the paper studies the automated threat detection tools, the development of software self-management mechanisms, and the certification of developed applications.***

Key words: *software reliability; malware; application safety; Self-Management; Self-Configuring; Self-healing; Self-protecting Self-adaptiveness*

I. INTRODUCTION

The efficiency of using information technology (IT) is chiefly depends on its quality and the confidence of the users in the applications. Expansion of application fields of IT has led to the lack the quality of software products, and the errors, as the result of which the damages cost much more than the revenue of the application.

Information security is one of the key factors for the typical functioning of any company. Today, most companies are using the Internet as the main businesses element more and more. As a result of which the role of hardware and software in the secure functioning of the internal applications of the company's IT structure, and in the security policy of the companies, in general, is growing constantly. In addition, in most cases, the measurement of economic efficiency of the application of security tools is relatively more difficult than the measurement of the efficiency of the enterprise management systems and the use of office applications.

Information security tools can be divided into three groups: antivirus tools, firewalls and attack detection tools. The first two categories of tools are used widely enough. Although some firewall products include attack detection tools, the latter group is more recent. The paper considers the necessary measures to be taken for the prevention of the most common attacks, and analyzes self-management mechanisms.

II. HACKER ATTACKS WITH THE USE OF APPLICATION CODE VULNERABILITIES

It is known that, the attacks are aimed at the illegal use of corporate resources, and at getting administrator rights to realize certain processes. The attacks can be both internal and external. However, regardless of its source, the vulnerabilities in the application code should be found first to get administrator rights. Unfortunately, most of these vulnerabilities are available in software products. The list of the attacks with the use of such software product vulnerabilities is quite extensive. It includes setting passwords, attacking Web servers, as well as, adding the objects of codes executed in Web pages. The most common ones are as follows:

- buffer overflow - unregistered users send a large number of surveys to the attack target, as a result of these attacks the application is not capable to functions. Although, this type of attack has been known for a long time, the applications with such vulnerabilities are still being developed;

- using standard passwords - while attacking, it is supposed that network or database administrator does not change the password specified in the documentation, however the password is known;

- Using malicious software (malware) - allows to monitor the network without permission, to identify vulnerabilities, and to set passwords. The notions of “malicious software” or “malicious software code” include undesirable activities, such as viruses, Trojan applications, phishing, network attack tools, spam distribution and so on. [1];

- Sending viruses – the viruses are the software aimed at data destruction, and network termination, which have self-growth features. In some cases, viruses are used to get the control over the network, and unauthorized resource access;

- denial of service (DoS - DDoS) - is one of the most common network attacks. The simplest way of the attack is to response to a legitimate request, since all the network (or functioning software) resources serve to a large number of requests received from other sources. Note that, such attacks are used not only for network attacks, but also for attacking the networks other companies.

Qrator Labs[2] and Wallarm [3], which are specialized in the prevention of DDoS attacks and focused on web-program safety, developed a report on cyber-threats, which is of great importance for the companies this year.
Hackers' activity was phenomenal in 2014, they studied the Attack Amplification Method very well by using the vulnerabilities in DNS, NTP, SSDP, SNMP, and other server configurations, Qrator Labs Director Alexander Lyamin says. By providing massive fake IP addresses in sent packets they are forcing thousands of other servers to attack the targeted server. The threats for Internet applications and web projects are increasing, Wallarm Director Ivan Novikov reports. 2014 was marked by Heartbleed, Shellshock and Poodle attacks affecting the Internet safety.

Heart bleed vulnerability was detected in the OpenSSL library (OpenSSL includes functions realizing cryptographic protocols SSL and TLS, that is the majority of modern systems are developed on the SSL protocol for secure data transfer). Heartbleed put millions of servers and devices under threat. With the help of Heartbleed the hackers got a chance to read the data of remote servers by accessing the Internet resources and stole registration records, payments and other confidential information. Even though the vulnerability of Heartbleed was found, the attacks still go on. Since the update of some facilities is a very complex and expensive process.

The second and more dangerous vulnerability was discovered in the Bash command shell, which is widely used in Shellshock Linux and Unix. It allows the generation of an environment of variables within the Bash interpreter and enables malicious code to run in the system. Shellshock is a source of danger not only for the Internet servers and work stations, but also for smart phones, tablets and laptops, which are more widely used in everyday life.

Poodle attacks (Padding Oracle on Downgraded Legacy Encryption) detected vulnerability in the SSL protocol.

In early 2015, two more dangerous vulnerabilities - Freak and Ghost were found. Although the first one was not as dangerous as Shellshock, in some cases, it allows hackers to execute hazardous code in Linux servers, as well. The second one was included to the list of threats for SSL channels. A number of patches (a small program written to replace a specific part of a program) were released to prevent the majority of these threats. Oracle released 128 patches for its programs within last three months [4].

III. DEVELOPMENT PROSPECTS OF THE PROGRAM CODE ATTACKS

This year the number of cyber threats may increase. According to the forecasts, in 2015, the attacks will be more aggressive, and this will be realized not only for revenue, but also to demonstrate the strength of the attackers. The conflicts between the governments, organizations and individuals will shift to the cyber space. Shellshock and Heart bleed attacks to network equipments will go on, and more new vulnerabilities associated with SSL and NoSQL databases will be revealed.

According to Kaspersky Lab experts, if such attacks are financed by the state the era of "cold cyberwarfare" will begin. To create an effective information security system, today, this area should be invested by 25% more, they note [5].

The wide range of cloud services will be used for storage and distribution of hazardous applications, in this regard, this area attracts the criminals. A large volume of confidential data is stored on their servers, as the result of successful attack it can be available for cybercriminals. Nevertheless, the cloud infrastructure is usually protected from the threats in rather reliable and professional way. Gartner (the world's leading IT analyst company (US)) forecasts that 80% of security incidents will be due to the system administrators' faults and the mistakes made by cloud service users [6].

The data stored in the clouds can be accessed via mobile devices, as well, since they are not protected by the network as reliable as common network points. The risks are even greater when the mobile device is used for personal purposes, as well as to solve business problems.
In recent years, the number of malicious mobile software has increased sharply. More than 90% of them are targeted at Android-based devices [7]. According to the statistics, one out of three companies does not use the tools against malicious software fully.

IV. THREAT DETECTION TOOLS

Analytic studies show that 10% of enterprises experiences security system in the application phase of software, 20% of them in documentation phase, and 70% waits for the system to be exploited [8]. It is due to the fact that the programmers hope that their programs will not be attacked.

Threat detection tools are developed to identify the incidents assessed as an attempt to attack and to notify the IT administrator. These tools are divided into two categories, depending on the activity:

- the tools analyzing whole network traffic (in this case, the software called agent is installed at the network workstations);
- the tools analyzing the traffic of a specific computer (for example, corporate Web-server traffic).

Attack detection tools can be developed in the form of software and hardware as firewalls, but also created in the form of - complex. These tools should be set so accurate to detect true attack attempts and to minimize the risk of false signals. Cisco Systems, Internet Security Systems, Enterasys Networks and Symantec, including Computer Associates and Entercept Security Technology are the dominating companies in the development of attack detection tools.

Microsoft SDL Threat Modeling Tool 3.0 (Security Development Lifecycle (SDL) - a secure software development method, which can be applied at all stages of the life cycle of the program) is an analytical tool, which implements the structural analysis of the project and detects potential drawbacks to provide security. The tool can be used to verify both new and existing applications running on Windows or other platforms. The application itself runs on Windows.

Threat Modeling Tool defines the special points during the development of software components. The vulnerable points should be predefined to be sure of the software tolerance to the attacks. A special attention should be paid to the inclusion of the data, authentication and encryption of confidential data.

V. MODERN SECURITY TECHNOLOGY AGAINST THE THREATS

The need for modern security technology against the threats is occurred for objective and subjective reasons. The objective reasons are the rapidly changing threats. Therefore, developed software should be flexible and effective against the new type of threats, and the price must be suitable for users. As to the subjective requirements, the level of access to any confidential information should be control surely.

Internal complexity and dynamic changes of modern and large volume application code causes a lot of problems. In 2001, vice president of IBM reported that the software complexity would be the main obstacle for the development of IT [9]. The more complex the software, the more number of vulnerabilities is. Even after the software trial, all the problems in the system, which consists of millions of lines of codes, can't be detected. Besides, the cyber attacks are inevitable. Existing methods to protect the integrity and availability of the software are not enough anymore.

By analyzing the requirements (adaptive, free, prompt response to new threats, etc.), it is obvious that there is a need to develop the systems which is based on artificial intelligence can work independently and adapt to new conditions quickly. These systems adapt to changing conditions continuously and increase their knowledge, and the most important point is that they can do all of these freely without the involvement of a human [10]. Thus, the notion of software self-management was born. It includes the features as self-adaptive, self-protected, self-treatment and so on.

Self-management means the ability to change its characteristics to improve its activities and functional capacity, as well as the reliability of the system automatically and dynamically without the intervention of the system administrator. Self-management mechanisms of the software can be classified as follows, depending on its functions(adaptive, supporting the requirements to control operating modes):

- mechanisms changing the system structure in general (Self-Configuring) and affecting its separate components (Self-Organizing);
- mechanisms controlling internal (Self-healing) and external (Self-adaptiveness) changes (environmental change) of the system;
- mechanisms supporting security requirements of software systems (Self-protecting) and quality mechanisms (Self-optimizing).

Self-healing can include the followings:

- Clear View system was developed at Massachusetts Technological University (US) in order to increase the resistance of the application against failures and attacks. When an engineer-programmer detects the vulnerability he develops a patch to fix it, which takes a month. The program works without a human intervention; the instructions on the proper functioning of the software are included here. As soon as the system discovers the attack it defines the changed parameters, and develops the patch for the software recovery, afterwards, it checks whether the adjustment problems were eliminated.
- Hewlett-Packard (HP) has developed "smart BIOS" application to prevent attacks to the device itself. As

mentioned above, the majority of hacker attacks is directed to the operating systems and gets the administrator right by changing in BIOS. In the new application a copy of BIOS is installed to the equipment and compared to the application, which is usually loaded. If the difference is detected, the computer reloads the initial BIOS version.

-

VI. CONCLUSION

Various projects ensuring the safety and reliability of the software have been developed recently. department for Advanced Research Projects of US National Investigation Agency accept new proposals for Machine Intelligence from Intelligence Cortical Networks (MICrONS) software project. The project aims at the development of new generation of adaptive algorithms based on the model similar to a human brain microstructure, in order to solve complex problems as human [11]. These algorithms shall be able to change and update the data, which is received basing on the learning rules owned by the brain. Compatibility of the architecture, hardware and software of complex information systems can be achieved through the standardization of software and hardware in accordance with international standards. In this regard, the tools, processes and services should be certified.

Depending on the scope of IT and the purpose of software and database, the certification may be mandatory (hard) and optional (soft). Mandatory certification is essential for information systems implementing important functions. Low quality, errors and denials can cause foremost damage or pose a threat to life and health of the people. Certification of information technology in such systems reduces the risk arising from their application and increases required level of security.

Optional certification is applied to enhance the competitiveness of IT in order to guarantee its quality, to expand the scope of application, and to achieve additional economic advantages in the market. Operating systems components and applied software packages are exposed to such certification trials. Certification expenditures are justified with the price raise, reduction of user claims, increase in sales circulation, and so on.

$(ISC)^2$ (International Information Systems Security Certification Consortium) deals with the certification of the professionals in the field of computer security. From this year two more certificates are expected to be provided [12]. One of them is designed to define the qualification of the programmers to develop and apply the methods to ensure the safety of the applications. In order to get the CSSLP certificate (Certified Secure Software Lifecycle Professional) a professional takes an exam in the program life cycle, vulnerabilities, risks and information security fundamentals. Another certificate is CCSP (Certified Cloud Security Professional) which is provided by $(ISC)^2$ and the Cloud Security Alliance (CSA) will jointly.

Some software self-management methods are analyzed to improve the reliability of the programs and to be protected from hacker attacks. Practical application of the methods will increase the software interactivity, flexibility and tolerance. It may also address the issue of creating complete stand-alone system. Therefore, one of the main goals of IT industry is the development of the self-restoring software to ensure the safety and reliability of the applications. Though, the first steps have been taken in this field, the problem is still relevant.

REFERENCES

[1] Julian Evans. “Mobile Malware – the new cyber threat” / HAKIN9, 2010, Vol. 5, No. 8, P. 46-49.
[2] www.qrator.net/ru/company/news/qrator-labs-i-wallarm-proanalizirovali-rynok-kiberugroz-v-runete
[3] www.wallarm.com
[4] www.pcworld.com/article/2034729/oracle-shipping-128-patches-for-apps-database-and-middleware.html
[5] www.blog.kaspersky.ru/ksb2014-predictions/6381/ www.osp.ru/lan/2013/01/13033558/
[6] www.gartner.com
[7] www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security (Access date: 26.02.2009).
[8] www.osp.ru/news/articles/2008/37/5439424/
[9] Horn P. “Autonomic computing: IBM’s perspective on the state of information technology”, IBM, October 2001.
[10] Bailey C., Montrieux L., De Lemos R., Yu Y., Wermelinger M. “Run-Time Generation, Transformation, and Verification of Access Control Models for Self-Protection” / Proc. of 9th International Symposium on Software Engineering for Adaptive and Self – Managing Systems. Hyderabad, India. 2-3 June 2014, p135-144.
[11] www.iarpa.gov/research-proqrams/microus/
[12] www/isc2/org

BIOGRAPHIES

Bayramova Tamilla senior researcher at the Institute of Information Technologies of ANAS. Her research interest include software engineering.

