ON THE CONTEMPORARY CYBERSECURITY THREATS

Assistant Prof. Linko G. Nikolov, PhD[1]; Assistant Prof. Krasimir O. Slavyanov, PhD[2]
„Artillery, Air Defense and CIS“ Faculty – Shumen, National Military University „Vasil Levski“, Bulgaria[1,2]
linko.nikolov@aadcf.nvu.bg[1], k.o.slavyanov@gmail.com[2]

Abstract: *Cybersecurity is one of the most commented areas in IT nowadays. Plenty of network and application attacks are possessed worldwide. Security becomes serious issue for corporations and governmental computer networks as functionality of applications rises in technological aspect. Most affective and widely used network attacks and application vulnerabilities are commented in this reviewing paper. Primary solutions for network security are proposed.*

Keywords: CYBERSECURITY, NETWORK ATTACKS, APPLICATION VULNERABILITIES, SQL INJECTION

1. Alert for networks and computers

The information era is an old word already. Contemporary Internet users have known instantaneous access to web-applications and live video-calling a long time ago. The computer network infrastructures of governments and corporations grew bigger and are deploying worldwide. Internet access and web-site front end seems inevitable since commercialism and publicity is the target direction. Artificial Intelligence (AI), Internet-of-Things (IoT) and even Internet-of-Everything (IoE) play the main role in the world's communication scene nowadays.

One decade ago the situation was narrow availability of attacker tools, script kiddies and platform homogeneity. Challenges were client-side attacks and many alerts and logs for network administrators to review. Nevertheless, Threat Management and Security Operations Centers were the armors against hackers. After 2010, attacker ecosystems and tools matured, challenges changed to lateral movements and persistent targeted attacks. Focus on security is Risk Management and independency of CIS Officer functions.

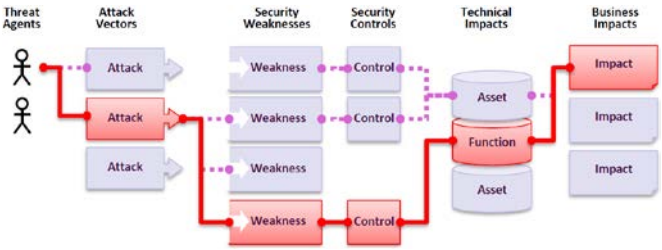

Fig. 1 *Attackers' paths representing cybersecurity risk [7]*

On Figure 1 a variant of paths for conducting a network and web application attack is depicted according to [7]. What web developers and network administrators should have in mind is that these paths are sometimes trivial to find, but sometimes are distributed in code and difficult to recognize. Technical and business impact estimation in combination with evaluation of threat agent, attack vector and security weakness helps determining the risk of the organization.

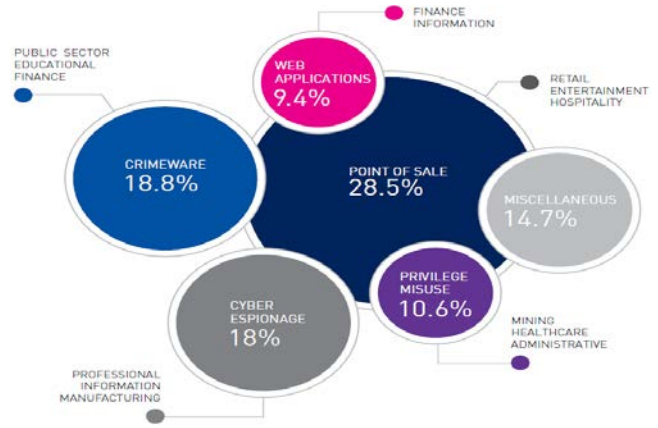

Fig. 2 *Attack vectors for industry [4]*

Having those evolutional processes in communication and computer systems brings the issue of security. Company rivalry, cyber war and database access appetite are one of the vast number of motivations for attacking the network and systems inside. With the Internet connectivity and widely deployed Wireless networks, physical access is no more a breakpoint for attackers.

2. Network attacks and the impact

A network attack can be described as passive or active. Active attack aims system resources altering or affecting their operation. Passive attack tries to learn or make use of system information but does not affect resources (e.g., wiretapping). An attack can be perpetrated by an insider or from outside the organization. An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"). An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments. In the common literature on network security, main network attacks are as follows:

- Denial-of-Service;
- Man-in-the-middle;
- ARP poisoning;
- Ping flood;
- Ping of death;
- Smurf attack, and more.

The most famous network attack is the Distributed Denial-of-Service – DDoS. Its purpose is providing network malfunction by different ways: buffer overflow, TCP SYN flood and etc. Another well-known network attack is the Man-in-the-Middle attack. It is achieved by the means of ARP Spoofing and ARP Snooping. Its main purpose is data sniffing, stealing and if possible – offline data traffic decrypting including private cryptographic keys.

In a continuous live network attack monitoring from Norse Corporation [8] the most interested countries for network attacks are the United States, followed by United Arab Emirates, Spain and Philippines (table 1).

Table 1: *Report from monitored attack sensors [8].*

№	Top 10 attack origins	Top 10 attack targets	Attack type
1	United States	United States	smtp
2	China	United Arab Emirates	telnet
3	Netherlands	Spain	http-alt
4	Ukraine	Italy	rfb
5	Czech Republic	France	ms-wbt-server
6	South Korea	Singapore	microsoft-ds
7	Germany	Norway	xsan-filesystem
8	Pakistan	Saudi Arabia	netis-router
9	India	Belgium	netbios-dgm
10	Spain	Thailand	mysql

Most DDoS attacks are divided into three categories targeting the network infrastructure. Measured in [Mbps] Volume based attacks saturate a site's bandwidth, which blocks client's access.

OSI Model layers protocol attacks compromise servers and intermediate communication equipment in order to tie up enough of these resources to lead to denial of service. This is measured in packets per second. The third category is application layer attacks, which are measured in requests per second. These types of attacks crash web-servers by means of flooding requests that appear legitimate. Sometimes the victims of a DDoS attack may not realize they were targeted. Hackers' motivations may have political intentions, business competition, use it as a means of stealing money, or just distracting victims while performing another malicious activity. One example is the Mirai botnet used for targeting Internet of Things (IoT) devices acquiring massive scale. It brings the next top cyber threat: IoT [3].

From the American research and advisory firm "Gartner" it is estimated that by 2020, consumers and businesses will be using more than 20 billion IoT devices. We are to expect more attacks in 2018 on smart devices, often incompatibly monitored or secured. IoT security fall is the leverage that a malicious hacker could prevail over a large healthcare organization if manages to gain access to the amount of electronic protected health information stored on the organization's network of medical devices. Vulnerable networked video cameras and camera enabled smart devices provide criminals access to sensitive recorded audio and visual information behind closed doors at target organizations.

IoT typically includes webcams, smart TVs, and even internet-connected refrigerators. IoT actually comprises a broad range of products – electronics, sensors, actuators and software soon to be built into everything from car-vehicles to homes: technology to unlock the gate and switch on the lights when entering home; technology allowing cars to talk to other cars and traffic lights to prevent accidents; technology to regulate breathe air quality, manage energy distribution, and control water supply all in real-time, each with thousands of sensors, all communicating through a city-wide network [4]. Implants for heart monitoring, pathogen monitoring for food, environmental waste monitoring, feedback sensors for firefighters in search and rescue and much, much more are in the potential of IoT. According to the CEO of Cisco, Chuck Robbins, the IoT industry is expected to be worth $US19 trillion globally by 2020 [9].

As for the classification of network attacks, Wi-Fi traffic is also a subject of attack having the air interface open. Linux commands like *airodump-ng*; *aireplay-ng* and *aircrack-ng* define Wireless Network Interface Cards (NICs) as an attacking hardware tool which by the means of the operating system can crack access passwords. This imposes the risk of unauthorized network access and Wi-Fi network de-authentication processes, leading to air-interface network malfunction and later - unauthorized access.

3. Major computer systems and application attacks

Computer systems are being protected against viruses, worms and Trojan horses by antivirus software [1], but having in power some programming skills, attacks could be successful. Common host attacks are:

- Buffer overflow;
- Heap overflow;
- Stack overflow;
- Format string attack, and more.

Computer systems execute codes of applications. Most common application vulnerabilities and attacks are:

- Backdoor;
- Denial-of-service attack;
- Direct-access attacks;
- Eavesdropping;
- Spoofing;
- Tampering;
- Privilege escalation;
- Phishing;
- Clickjacking;
- Social engineering, and more.

As is shown in Table 2 injection tries are the most used in web applications. Typical example is SQL Injection where attacker can "inject" unwanted code in the field of username and password (see Fig. 3). The methodology of injection is as follows: from the web-browser the front end of the site is accessed (most of the times via protocol HTTPS); the user sends "request" queries and data to the web server; and then the scripting language connects to database (such as SQL) storing values to it or retrieving data from it. The front end is usually coded in JavaScript, **.**NET or PHP scripting languages. The database stores tables in the backend of the site by MySQL, SQL Server, Oracle or other. With the commands shown in fig 3 an injection can be executed.

Table 2: *Top 10 web app security risks [7].*

№	Type of risk	Year
1	Injection	2017
2	Broken Authentication and Session Management	2017
3	Sensitive Data Exposure	2017
4	XML External Entity (XXE) (new risk)	2017
5	Broken Access Control	2017
6	Security Misconfiguration	2017
7	Cross-Site Scripting (XSS)	2017
8	Insecure Deserialization (new risk)	2017
9	Using Components with Known Vulnerabilities	2017
10	Insufficient Logging and Monitoring (new risk)	2017

A found vulnerability in the JavaScript scripting language is here exploited. In another explanation, "SQL Injection" can be defined as subset of unverified/unsanitized user input vulnerability. The idea here is to convince the victim's application to run SQL code that is actually not intended (see fig. 3). Should the application create SQL strings naively on the fly and then running them, no later real surprises will be on the go.

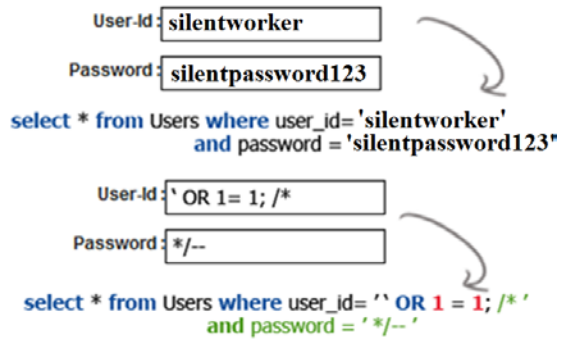

Fig. 3 *Example of SQL injection script*

The best goal achieved by SQLi is username and password stealing. This would break the authentication barrier. Broken authentication is the second most important security risk which leads to sensitive data being compromised. In this type of risk attackers have in power millions of usernames and passwords, default administrative account lists as well as advanced cracking tools which use lots of calculating power including Graphic Processing Units (GPU).

Another famous attack nowadays is the Cross-site scripting (XSS). It is a code injection attack that allows a hacker to execute malicious JavaScript in victim's web-browser, for example - in a blank text field of a blogger website. The path for running this malicious activity is injecting the code into a page, downloaded from a web-site and surfed by the victim. Cross-site scripting aims cookie stealing, which contain sensitive information, even though it is in an encrypted form. Decrypting mechanisms would extract passwords and usernames if dictionary or brute force attacks are successful. There are two main types of XSS: Persistent and Reflected. In persistent XSS malicious strings originate from the

website's database, while in reflected XSS the malicious string originates from victim's HTTP GET request.

The future impact will be on network Confidentiality (e.g. Wikileaks, Doxxing, etc.). Impact will also affect data integrity - malware such as Ransomware. And last but not least - Availability (Bricking Firmware, MBR Wiper, etc.).

4. The social engineering phenomenon

Social Engineering as a cyberattack underlies on end-users low-level security awareness. It is an information gathering methodology. An attacker can gain access by fooling an authorized user by means of e-mails that lead to clicking or opening an external web-link or a file, whose masquerade is actually a hidden virus or a malware executing malicious function. Such activities are called E-mail scam and phishing. Actual example of a real e-mail scam is shown of Fig. 4:

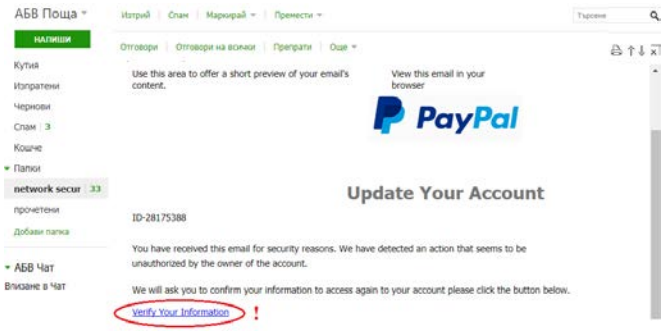

Fig. 4 *Example of existing real e-mail scam letter*

The red color ellipse is pointing out the link to be open from the "fooled" user and if done, malicious software would execute. Such an e-mail can be constructed easily from the "SET" tool in KALI Linux operating system [10].

As from the Security experts: humans are the biggest cybersecurity vulnerability leading to intentional and also unintentional network breaches. Often are the results of employee's carelessness; a disgruntled employee seeking revenge, or the victimization of an employee by a sophisticated hacker. "Social engineering" said in another words is "tricking" a user into opening sensitive information. Most employees assume they can identify a spam e-mail meant to scam the recipient out of money. What they don't assimilate is that attacks are becoming much more sophisticated. Hackers' tactics that rely on social engineering, like spear phishing, succeed because the attacker has an intimate understanding of an employee's motivations and role within an organization so that these can be precisely exploited. Black hat hackers gain enough information about the personal and professional lives of their victims, then effectively impersonate someone the victim trusts or craft an email or popup window that looks legitimate to someone without sufficient security knowledge. Human errors leave networks open to opportunistic cyber criminals. Poor password hygiene is due to a struggle to remember strong passwords for multiple devices of most consumers and employees. Busy high volume businesses like healthcare organizations may have difficulty managing privileged users effectively, leading to inappropriate access. Human beings increasingly rely on technology to make their lives easier and achieve aims that they could not reach using people power alone. But there has yet to be technology developed to make humans infallible, and they will continue to be the biggest cybersecurity threat in 2018 and beyond [3].

5. Attack countermeasures assuring cyber security

During Internet evolution, security had ever-increasing role. The evolution of cybersecurity was as stated in [2]:

Identify → Protect → Detect → Respond

In 2020 the trend will be "Improving the ability to recover", also called "Age of Resiliency".

Improving resiliency includes User Education and Awareness. Lessons such as: "Don't open suspicious e-mails even from friends and colleagues, and moreover – the included files or links inside!" are essential for the future cybersecurity.

Another point assuring cybersecurity is proper planning and preparation – a network with enough resources and predicted situations can be a key to less stress of systems and of the monitoring personnel.

Having in mind that hacker attacks are unpredictable by nature, detection and recovery is the first aid. It includes deployed IDS/IPS systems and also Incident response teams educated for the company/organization. And the most famous advice of security devices providers: Firewall, OS and Antivirus - all patched regularly! As for countermeasures against the highest risk nowadays – Structured Query Language injection (SQLi):

- Prepared Statements (with Parameterized Queries);
- Sanitizing and validating the input field;
- Check the web server & DB configuration (some offer built-in features);
- Strong passwords for SA and Administrator accounts;
- Apply least privilege rule to run the application that access database;
- Use a properly configured WAF, and more.

Against Cross-Site Scripting (XSS) the countermeasures proposed are:

- Validation of input data;
- Encrypting;
- Cookie flag *HTTPOnly* to be available for all languages;
- Content Security Policy implementation;
- Usage of Auto-Escaping Template System;
- Usage of X-XSS-Protection Response Header – already available in most browsers.

The Web-Application Firewall is the most effective technical solution to achieve web app protection. Basically it's an application filter for HTTP applications. It applies a set of rules to an HTTP conversation, which protect against attacks such as XSS, SQLi, etc.

Useful advices are to conduct regular penetration testings and vulnerability assessments. Furthermore, advantage of threat intelligence should be taken in order to determine who is targeting an industry branch, what approaches the hackers employ, and whether your institution is likely to be targeted. A remediation strategy should be developed allowing vulnerability or compromise resolution with a minimum disruption of business processes, of hardware control and of customers or users application experience.

References:

[1] – Kizza, J. M., „Guide to Computer Network Security" – 4th ed., Springer, ISBN 978-3-319-55605-5
[2] - Sounil Yu, SVP, RSA Conference, San Francisco, feb. 2017
[3] – The Top Cyber security Threats of 2017, NopSec whitepaper, url: https://www.nopsec.com/blog/top-5-cybersecurity-threats-for-2017
[4] – „Cybersecurity – Threats, Challenges, Opportunities", ACS, url: www.acs.org.au
[5] – Muckin, M.; Fitch, S. „A Threat-Driven Approach to Cyber Security", Lockheed Martin Corporation
[6] – Biggest cybersecurity threats in 2016, url: https://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html
[7] – OWASP Top 10 2017 "The Ten Most Critical Web Application Security Risks", url: https://owasp.org
[8] – Norse Corporation, 333 Hatch Drive Foster City, CA 94404, 29 nov 2017 14:30, url: http://map.norsecorp.com/#/
[9] - Cisco CEO Pegs, "Internet of Things as $19 Trillion Market", Bloomberg Technology, January 2014, url: www.bloomberg.com/news/articles/2014-01-08/cisco-ceo-pegs-internet-of-thingsas-19-trillion-market
[10] – David Kennedy, url: https://tools.kali.org/information-gathering/set