59th International Scientific Conference on Information, Communication and Energy Systems and Technologies, Sozopol, Bulgaria, July 1 – 3, 2024

Simulation of Cookie Poisoning network attacks

Aleksandar Hristov[1]

Abstract – **The purpose of the paper is to develop a simulation model of cookie poisoning network attacks. A review of the current state of the problem is done, as well as some known solutions. The stages of cookie poisoning attack are described and research methods that can be used for developing a simulation model for cookie poisoning network attacks are proposed. Some results are achieved by conducting numerical experiment.**

Keywords – **network attacks, cybersecurity, cookie poisoning, simulation model, GPSS.**

I. INTRODUCTION

The emergence of today's information society is connected with the introduction of new computer and telecommunication technologies, which leads to new forms of information transmission and usage in the of economic, public and social life spheres. The implementation of distributed processing by computer networks and various information technologies allow to quickly and efficiently spread knowledge, experience and information in many fields of science, technology, medicine, education, etc. The number of malicious impacts is constantly growing, and the development of cybersecurity systems does not always keep pace with the development of cyberattack methods [1]. Well-known patterns of cyberattacks are often complex and require knowledge of the specifics of a particular attack and its intensity. One of the biggest threats for the network traffic is using cookies [6]. They do not contain executable code, but they contain sensitive information for the client and could be accessed by another site trough malicious script or ActiveX code. A lot of sites are using this mechanism for identifying of user session.

The literature review showed that many of the proposed models involve a large amount of heterogeneous input data, many of which are difficult to specify with acceptable accuracy [1] or require configuration and usage of artificial intelligence methods and tools [6 and its references]. This affects the computation time and the accuracy of the final results [5]. An automated process control system includes programmable logic controllers (PLCs), workstations, a server, and a communication equipment connecting them in an IIoT network [4].

Determining the time it takes for cyberattack to be successful is very important. In [5] is proposed restart if the SecureCore before the time needed for a successful cyberattack. The average time needed for conducting a successful cyberattack can be used to estimate the required response time of cybersecurity systems and can also be used in embedded information security tools. If the response time of the cybersecurity system added to the time for taking the necessary measures is less than the average time to carry out a cyberattack, then, as a rule, the probability conducting a successful attack is significantly reduced.

The purpose of this paper is to develop a simulation model of cookie poisoning network attacks.

This section presents the current state of the problem, as well as some known solutions. The next two sections are dedicated to the research methods that can be used for developing a simulation model for cookie poisoning network attacks.

II. RESEARCH METHODS FOR CYBERATTACKS

Studying and evaluating the characteristics of network protocols and their corresponding cyberattacks is an important and difficult problem to solve. The aim of this section is to analyze the known methods and tools for investigating network protocols and their corresponding attacks, emphasizing their inherent problems, advantages, and disadvantages.

Experimental research methodology is a set of approaches, ways and methods for conducting a complex scientific research, including processing and analysis of the results. The main elements of experimental research methodology are given below:

- Defining the goals and objectives of the study;
- Determination of the input and output parameters that affect the studied object, their interconnection and the conditions under which the experiment is conducted;
- Preparation for the implementation of the experiment;
- Determination of the number of observations (number of investigated objects) needed, total duration and the sequence of individual stages;
- Processing of the experiment results.

In the analytical approach, the first results of the analysis of wired and wireless networks were obtained using the mathematical apparatus of discrete Markov chains or the queuing system theory. The drawbacks of the analytical approach for studying computer networks (taking into consideration the presence of relatively complex protocols) are that the models are often very complex with a huge number of changing states and are based on various nonlinear dependencies that further complicate the analytical models.

Simulation modeling is a flexible tool for studying complex network protocols and cyberattacks. It is also possible to detect an important feature of a given protocol or cyberattack with variable accuracy through simulation modeling.

[1]Aleksandar Hristov is with Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia, Bulgaria, 1000, E-mail: ahristov@tu-sofia.bg

979-8-3503-8619-6/24/$31.00 ©2024 IEEE

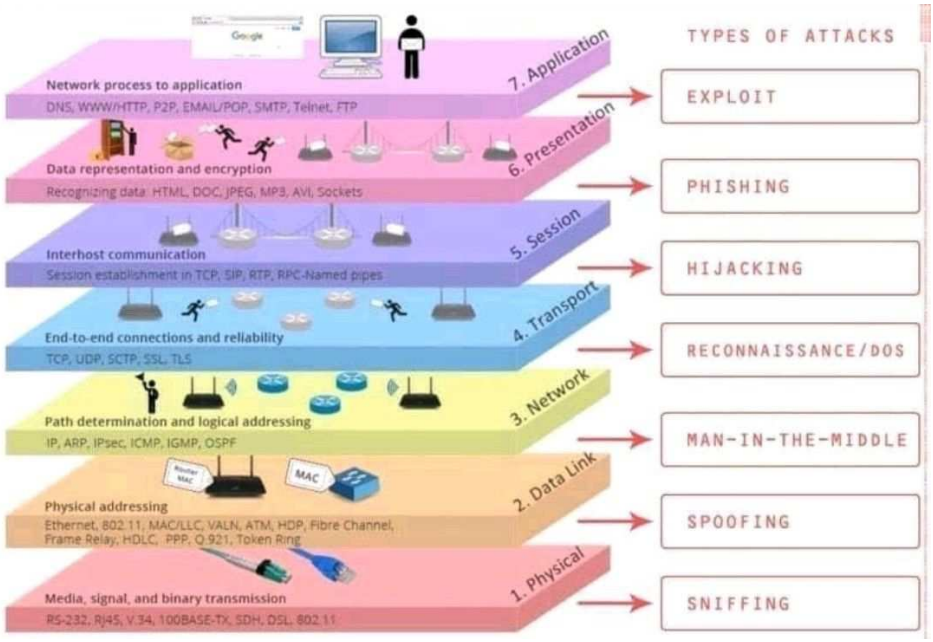

Fig. 1. Internet Architecture and Taxonomy of cyberattacks [6]

Due to the high complexity of such models, respectively the high resource consumption of model operation, general purpose simulators such as Arena, Simula, etc. are used. The General Purpose Simulation System - GPSS is one of the most powerful and flexible simulators for describing the dynamics of functioning of queuing systems. The version of the language used in this paper is GPSS World Student Version (Windows application).

III. Simulation of Cookie Poisoning Network Attacks

A. Types of network attacks and computer network research methods

In recent years, the Internet has grown faster than any other network, resulting in an exponential increase in the number of subscribers and traffic. The Internet is a global computer network made up of thousands of interconnected subnets, where each subnet uses the TCP/IP protocol for control and data transmission, and sharing a common address structure. Each subnet can be an Ethernet LAN, 802.11 wireless LAN, 5G, or 6G. These subnets, interconnected directly or through access points, constitute the structure of an IP network.

The architecture of Internet and also taxonomy of cyberattacks is shown on Fig. 1.

Web developers often use HTTP cookies, or packets of information sent from a web server to an Internet browser, and then returned by the browser when it accesses that server. Cookies contain random information chosen by the server and are used to maintain the state of HTTP transactions that are otherwise "stateless". They are used for user authentication, maintaining a "shopping cart", personalizing a site (presenting different pages to different users), tracking access to a given site, etc. Cookies contain information relevant to a given context (user, computer, web browser, domain, etc.) and are used for cross-site scripting attacks and cookie hijacking attacks by hackers.

Cookie poisoning is another threat for the user, because it allows bypassing the trust protection mechanism. Using cookie poisoning, a hacker can inject malicious code by modifying cookies and conduct persistent cyberattacks.

Fig. 2 shows the steps of performing a cookie poisoning attack, using a pseudo Petri net.

B. Cookie poisoning attack stages

The steps for performing a cookie poisoning attack are as follows:

0 – initial state of the process, the intruder is ready to perform a script injection attack. The attacked host sends a HTTP request to web server;

1 – the web server receives the request and prepares a cookie file for transmission to the host;

2 – the cookie file is intercepted by a network sniffer tool and transmitted to the intruder;

3 – a malicious script is embedded in the cookie file for transmission to the attacked host;

4 – the cookie file is received and opened by the web browser of the attacked host, launching the malicious script;

5 – the target user file is found on the attacked host with probability p_{SEARCH}. Then the file is copied and prepared for transmission over the network;

6 – the cookie manager program is launched and the malicious script is detected with probability p_{DETECT};

7 – a command is sent to execute the malicious script;

8 – the target user file is copied and transferred to a host with a network address defined by the intruder.

The transitions between the states for conducting the attack are as follows:

c_{01} – a request for an Internet resource is sent from the attacked host to the web server;

c_{12} – cookie file is sent from the web server to the host;

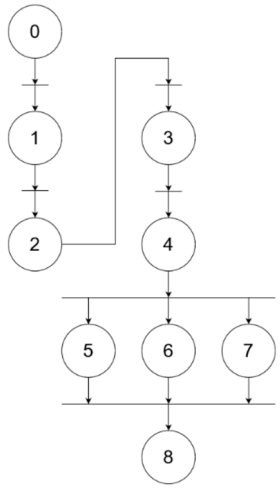

Fig. 2. Steps for performing a cookie poisoning attack

c_{23} – the cookie file is intercepted from the intruder's sniffer tool, embedding the malicious script in the cookie file and sending it to the host;

c_{34} – the cookie file with the embedded malicious script is received from the attacked host;

c_{45} – the malicious script is started;

c_{5x} – a logical transition (i=5,6,7) is triggered, fulfilling:

a) the malicious script is started;

b) the targeted user file is copied;

c) the cookie manager program has not detected the malicious script. The result of the transition is the transfer of targeted user file to an intruder host.

The probability of successful completion of a process P_j of step j (j=6,7) can be set according to specific threat models or, as in [1] can take values in the interval [0.7, 1] with a given step.

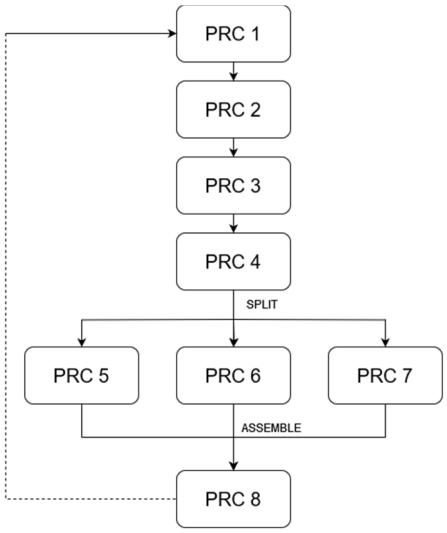

Fig. 3. Steps of cookie poisoning attack

Below, conducting a cyberattack in an automated process control system is investigated. The model (Fig. 3) is based a queuing system theory and allows estimation of the average time for a successful cyberattack as well as the distribution function of the time for conducting the attack.

The model is a closed queueing system in which the elements PROC[j] j={1,2,..,8} corresponding to the processes from the steps above are sequentially connected.

Figure 4 shows the Q-scheme and its corresponding segment of GPSS code for process PROC[j] i.e. one of the processes discussed above. The process PROC[j] has an input connection with the previous PROC[j-1], and an output connection with the next PROC[j+1].

In PROC[4], the output connection to the following processes PROC[5], PROC[6] and PROC[7] is implemented by SPLIT blocks, in which the transaction from PROC[4] is multiplied, then each of the resulting 3 transactions is directed to PROC[5], PROC[6] and PROC[7] respectively.

It is assumed that processes PROC[6] and PROC[7] are implemented with the corresponding probability to conditions b) or c) of the logical transition c_{5x}, raising the flags Fl_j, j=6,7 respectively (See in the GPSS model [2] following fragment TRANFER (1-PROBj),,LABi; LOGIC S Flj; LABi ASSEMBLE 3;). As can be seen on Fig. 3 the transactions from processes PROC[5], PROC[6] and PROC[7] are transferred to an ASSEMBLE block in which those transactions are synchronized and thus the resulting single transaction is an input to the process PROC[8].

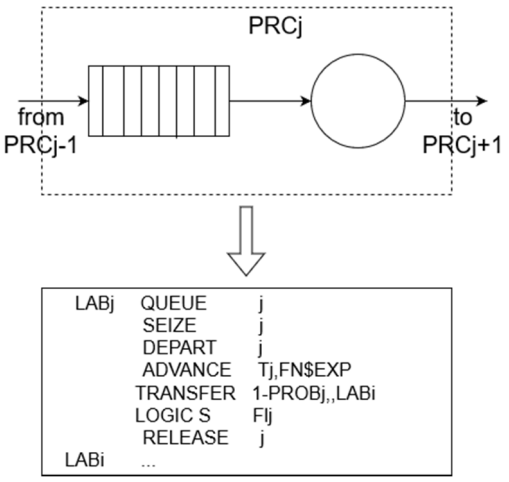

Fig. 4. Q-scheme and its corresponding GPSS code

After the transaction is serviced by the process PROC[8], it is transferred to the input of the process PROC[1], since the model is a closed queuing system. Note that only if the conditions of transition c_{5x} are met (See TEST NE (Fl6&Fl7),1,EEE; TABULATE XTIME; EEE TRANSFER ,BGN;), the time for which the cyberattack is conducted in the system is tabulated (using GPSS blocks MARK and TABULATE). An example histogram retrieved from the model is given in Fig. 5.

The last step in order to prepare the GPSS model for conducting experiments is to set the model parameters for the

time delay of each process T_j (j = 1,2...8) and the probabilities P_2 and P_5.

IV. Experimental results

The proposed simulator is online available in github [2]. Below are given the numerical results from the experiments conducted with the created simulation model, using GPSS World Student Version [3].

The time delay of each process (1-8) is chosen as follows: $T_1 = T_2 = T_3 = T_4 = T_5 = T_6 = T_7 = T_8 = T = \{5, 10, 15, 20, 30, 40, 50, 60\}$ s. with exponential distribution. The described processes are performed on digital equipment and they are more likely to complete in a short time period than in a long time period, hence all durations for the successful completion of the processes in steps (1-8) are chosen to have exponential distribution as in [1]:

$$y = 1 - e^{-\lambda t} \quad (1)$$

, where λ is parameter (constant) of the distribution and t is the time.

Note that for the given model in [2], the time delay for each process can be chosen individually. Also, the chosen time delay distribution is exponential, but the model is invariant about these distributions (determined, uniform, exponential, etc.).

It is also assumed that the probabilities P_2 and P_5 take values in the interval [0.6, 0.99] with a step of 0.1 ($P = P_2 = P_5$). The obtained numerical results for the mean times for a successful attack are shown in Table I, i. e. the average time vs. T and P. First column of this table $t_{mean}(T,P)$ contains the time delays, T and the first row contains set of values of the probability, P.

Table I
Mean times for successful cyberattack

T/P	0.6	0.7	0.8	0.9	0.99
5	34.3	34.3	34.3	34.3	34.3
10	68.8	68.8	68.8	68.9	68.7
15	103	103.1	103.3	103.3	102.9
20	136.7	137.4	137.8	137.7	137.2
30	203.7	205.2	206	206	205.5
40	271.3	273.7	274.9	275.1	274.5
50	337.7	341.9	344.5	344.5	344.1
60	406.9	413.5	415	414.6	413.2

The resulting histogram for T = 20 and P = 0.8 is given in Fig. 5. For the other values of the probability (see table 1 for T=20) the type of histograms are similar and due to the limited volume of the paper, they are not applied here.

If it is assumed that the distribution of time for a successful attack is exponential, then the probability for success of the attack as a function of time P(t) can be determined using (1).

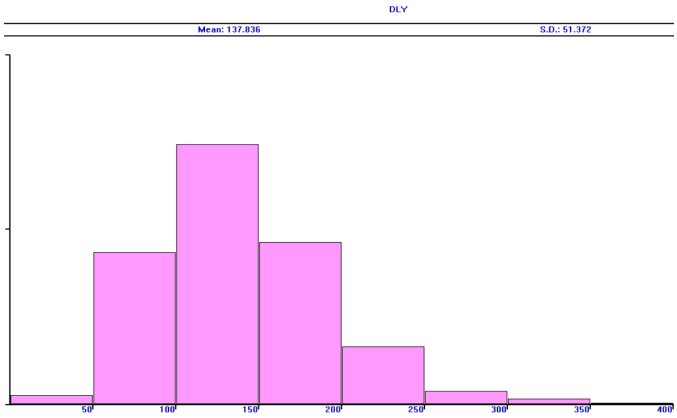

Fig. 5. A histogram of the times distribution for successful attack

In Eq. 1, the intensity λ is inversely proportional to the time for a successful attack (see Table I), i.e. $\lambda = 1/t_{mean}$.

V. Conclusion

In this paper is developed a simulation model of cookie poisoning network attacks. For this purpose, a review of the current state of the problem as well as a review of types of network attacks is done. The stages of Cookie poisoning attack are described and research methods that can be used for developing a simulation model for cookie poisoning network attacks are proposed. Using the proposed GPSS simulator, some results are achieved by conducting numerical experiment.

Acknowledgement

The presented research is funded by National Science Fund under the Ministry of Education and Science in Bulgaria with contract КП-06-Н 47/7 entitled “Possibility Investigation of Increasing the Cybersecurity of the Systems in Industry 4.0 using Artificial Intelligence”.

References

[1] Богер, Ал. Математическая модель вектора DDOS-атаки на сетевую инфраструктуру АСУ ТП с использованием метода топологического преобразования стохастических сетей, ВКС 4/2023, с. 72-77, DOI:10.21681/2311-3456-2023-4-72-79

[2] https://github.com/sashkinaaa/CookiePoisoningGPSS

[3] https://gpss-world-student-version.software.informer.com/download/

[4] Hristov A. et al. Developing and experimenting simulation model of DDoS attacks in IIoT networks using Python, Proceedings of the 31st scientific conference "TELECOM 2023", IEEE Conference, Rec # 59629, 16 – 17 November 2023, Sofia, Bulgaria

[5] Chien-Ying Chen et al. Securing Real-Time Internet-of-Things, J. Sensors 2018, 18, 4356; doi:10.3390/s18124355

[6] R. Trifonov, E.Sabev, G. Pavlova, K. Raynova; Analysis of deep learning methods for cybersecurity in industry 4.0. AIP Conf. Proc. 16 February 2024; 3084 (1): 060003. https://doi.org/10.1063/5.0193712