Innovative technology in the research of implementation dynamics of network attacks on the digital educational resources

O I Bokova¹, I G Drovnikova², E S Ovchinnikova² and S V Rodin²

¹ Kaskad Ltd, 2, Ferganskaya str., Moscow, 109444, Russian Federation
² Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots ave., Voronezh, 394065, Russian Federation

E-mail: idrovnikova@mail.ru

Abstract. Based on the analysis of the verbal models for implementing some of the most dangerous and typical network attacks on the modern digital educational resources as well as of the formal models of their functioning developed using Petri-Markov networks, graph models are developed in the article and simulation modeling of dynamics of the implementation of these network attacks in the CPN Tools software environment is carried out, too. Simulation results are presented as the quantitative values of probability-time characteristics of the network attack types under examination. Using the obtained results as initial data when assessing the threats of network attack implementation, developing a model of relevant attacks for a specific educational environment and forming quantitative requirements to the information resource protection systems will increase the real protection of both the existing digital educational environment and the one under development.

1. Introduction
One of the most important negative factors affecting the efficiency and reliability of the modern digital educational environment (DEE) [1] is the remote unauthorized access (UA) [2] of an attacker to its information resources, implemented through network attacks, which directly affects the environment protection level. The use by modern attackers of increasingly sophisticated methods of social engineering, OSINT (Open Source INTelligence) of searching, collecting and analyzing information about the DEE structure, other intelligence methods allows to successfully implement the network impact that damages its information resources, depending on the intention of the attacker. The current situation necessitates to anticipate the possible threats of network attacks implementation at the initial stages of DEE development [1, 3]. Therefore, the scientific studies dedicated to the threat assessment of the implementation of network attacks on the information resources of a protected educational environment are very important.

Review of published sources, international and industry standards of the Russian Federation, dedicated to the problem of information security (IS) of automated systems (AS) [3-8], demonstrated that the issues related to the quantitative assessment of the threats of implementing network attacks on the digital educational resources, especially to their analysis in a dynamic (timed) mode by means of determining the probability-time characteristics (PTC) (obtaining quantitative characteristics of the attack implementation time), are not explored enough. These characteristics are necessary: when
developing a model of relevant attacks, with respect to the performance features of the given DEE types; when developing their protected version; when developing the regulatory documents required for certification of systems of information protection from unauthorized access (ISS (information security systems)) in the protected AS, used in the educational environment applications; when elaborating requirements to the means and systems of educational environment IS ensuring.

The technology development for the research of implementation dynamics of network attacks on the digital educational resources by means of determining their PTC includes the following steps:

- Construction of graph functional models of destabilizing actions using Petri-Markov networks, on the basis of verbal (descriptive) models for implementing the most dangerous and currently typical network attacks on the digital educational resources.
- Simulation of the implementation process of each network attack on the digital educational resources using the CPN Tools simulation software environment.
- Presentation in tabular format of the simulation results in the form of PTC values of network attacks on the digital educational resources.

2. Materials and methods

The implementation of network attacks on the information resources of the modern educational environment is a complex dynamic process, that includes many interdependent parallel processes. Therefore, to study the network attacks implementation process, it is preferable to use models built on Petri-Markov networks [9, 10], which are based on theories of Petri networks and on Markov (semi-Markov) processes, which allows us to study the behavior of parallel processes with the determination of temporal and statistical characteristics [10].

One of the methods for determining the quantitative parameters of the given characteristics is a full-scale experiment. Without considering the DEE variety, the article presents a general methodology for solving the task assigned for DEE variant, implemented on the basis of AS with the file server most popular in use, which can be integrated into more enlarged DEE models with already different time characteristics for penetrating the used security tools. To test the methodology, a laboratory bench was deployed, consisting of a file server and three client workstations, one of which works under the Kali Linux operating system (OS) in order to implement a destructive action. Since the practical implementation of the full-scale experiment will be much more complicated in the case of a short time of network attack implementation, in order to overcome this drawback we used the CPN Tools simulation software environment – a powerful tool for modeling and analyzing networks of various complexity, where Petri-Markov networks can also be included, which is available for OS of the Windows and Linux family [11]. Simulation in CPN Tools is process-based, that is, it supposes an instantaneous state transition of the Petri-Markov network. In the CPN Tools environment, it is possible to program in the Unified Modeling Language (UML). The CPN Tools software product allows to generate, analyze the state space of a model under construction and to receive various kinds of reports in the form of non-timed and timed (time interval is used to evaluate a specific value) statistics [11].

An analysis of 217 threats currently presented in the IS threats databank developed by the Federal Service for Technical and Expert Control (FSTEC) of Russia (bdu.fstec.ru) [12], of operational features of modern protected AS used in the educational environment applications, of the results of interviewing IS experts allowed to identify eight types of the most dangerous and frequently implemented nowadays network attacks on the digital educational resources, taking into account their sources, targeted objects and possible consequences of their implementation (damage caused). The generated list includes the following main types of attacks: 1) network traffic analysis, 2) network scanning, 3) “password” attack, 4) spoofing of a trusted network entity, 5) imposing a false route, 6) installing decoys into the network (ARP-spoofing), 7) service denial (SYN-flood), 8) remote application launch (IP-hijacking) [13].

To simulate the implementation process of the above network attacks using the Petri-Markov network, we introduce the following designation for network elements: $S_i$ – positions, $t_j$ – transitions.

When simulating the implementation process of each of the network attacks on the digital educational resources, the dynamics of the implementation process is determined by the initial marking of the Petri-Markov network. The final result of the simulation is a table of PTC values for each network attack on the digital educational resources.
resources in the form of a directed graph and obtaining quantitative values of their PTC (average time spent in one of the states of the graph model formally describing the attack implementation in the system) in the CPN Tools simulation software environment, in order to ensure the correspondence of linear models we set the number of runs on the network $N \geq 100$.

Since the time in CPN Tools is represented as a whole number, to obtain timed statistics of the implementation process of a network attack, we establish the following relationship between the simulation time (computed machine time) and the real time: $1$ unit $= 1$ s [9].

Timed statistics when marker hits all positions is presented in the form of tables having the following fields: Name – position name; Count – counter of passages in the graph, starting from $0$; Sum – total number of hits of a marker in a specific position, Avrg – average value in the context of a given simulation task (average number of markers in a position); Min – the minimum number of markers in a position; Max – the maximum number of markers in a position; Time Avrg – the average time spent in one of the states of graph models formally describing the implementation process of network attacks on the digital educational resources.

3. Results and discussion

Let's simulate the implementation process four of the above types of network attacks.

A graph model simulating the main stages of the implementation process of the “Network traffic analysis” attack (packet sniffing) on the digital educational resources is shown in figure 1, where $S_1$ – attacked hosts are ready; $S_2$ – the attacker's host is physically ready to traffic interception; $t_1$ – packet transfer between the attacked hosts, packet capture; $S_3$ – packet captured; $t_2$ – packet analysis, extraction of necessary data (password, username); $S_4$ – essential data are extracted from the packet.

![Figure 1. A graph model of the implementation process of the “Network traffic analysis” attack.](image)

Table 1 shows the results of simulation (timed statistics) of the implementation process of the given network attack in the CPN Tools software environment.

**Table 1.** Timed statistics of the implementation process of the “Network traffic analysis” attack.

| Name                                      | Count | Sum    | Avrg     | Min | Max | Time Avrg |
|-------------------------------------------|-------|--------|----------|-----|-----|-----------|
| Marking_size_Network_traffic_analysis'S1_1 | 104   | 904    | 8.695652 | 0   | 100 | 2         |
| Marking_size_Network_traffic_analysis'S2_1 | 104   | 904    | 8.695652 | 0   | 100 | 2         |
| Marking_size_Network_traffic_analysis'S3_1 | 154   | 14061  | 91.304348| 0   | 100 | 21        |
| Marking_size_Network_traffic_analysis'S4_1 | 54    | 0      | 0.000000 | 0   | 100 | 57        |

A graph model simulating the main stages of the implementation process of the “Network scanning” attack on the digital educational resources is shown in figure 2, where $S_1$ – the attacker's host is ready, the program is configured and running; $t_1$ – definition of active network hosts using an ICMP request; $S_2$ – active hosts are defined; $t_2$ – definition of OS types of active network hosts; $S_3$ – OS types are defined; $t_3$ – scanning services on the active network hosts; $S_4$ – active services are defined.
Figure 2. A graph model of the “Network scanning” attack implementation process.

Table 2 presents the simulation results (timed statistics) of the implementation process of the given network attack in the CPN Tools software environment.

Table 2. Timed statistics of the implementation process of the “Network scanning” attack.

| Name                        | Count | Sum   | Avg    | Min | Max | Time Avrg |
|-----------------------------|-------|-------|--------|-----|-----|-----------|
| Marking_size_Network_scan/S1_1 | 107   | 563   | 5.263158 | 0   | 100 | 1         |
| Marking_size_Network_scan/S2_1 | 207   | 16342 | 78.947368 | 0   | 100 | 15        |
| Marking_size_Network_scan/S3_1 | 207   | 3268  | 15.789474 | 0   | 100 | 3         |
| Marking_size_Network_scan/S4_1 | 107   | 0     | 0.000000 | 0   | 100 | 1         |

Figure 3 shows a graph model that simulates the main stages of the implementation process of a “Password” network attack on the digital educational resources, where S1 – the attacker’s host is ready, connected to the shared network; t1 – the attacked host requests a password; S2 – the password request is completed by the attacked host; S3 – the host of the attacker, not knowing the password, decided to guess it using a special dictionary or by direct enumeration; t2 – guessing password by use of the dictionary; t3 – guessing password by direct enumeration; S4 – password guessing result; t4, t5 – intermediate pseudo hops; S5 – the password is correctly guessed, the unauthorized access to the attacked host has been completed; S6 – the password is guessed incorrectly, the attack is thwarted.

Since this model, in contrast to the linear models of other typical network attacks under consideration, is non-linear, to simulate a “Password” network attack with adequate output characteristics, the required number of runs on the Petri-Markov network (N≈14937) is defined on the basis of the method described in [9].

The simulation results (timed statistics) of the implementation process of the considered network attack in the CPN Tools software environment are presented in table 3.
Table 3. Timed statistics of the implementation process of the “Password” network attack.

| Name                          | Count | Sum   | Avrg  | Min  | Max  | Time Avrg |
|-------------------------------|-------|-------|-------|------|------|-----------|
| Marking_size_Password’S1_1    | 103   | 0     | 0.000000 | 100 | 1    |           |
| Marking_size_Password’S2_1    | 138   | 53    | 0.384615 | 35  | 5    |           |
| Marking_size_Password’S3_1    | 167   | 117   | 0.703297 | 64  | 5    |           |
| Marking_size_Password’S4_1    | 131   | 7831  | 59.780220 | 64  | 450  |           |
| Marking_size_Password’S5_1    | 102   | 3777  | 37.032967 | 95  | 300  |           |
| Marking_size_Password’S6_1    | 102   | 527   | 5.164835 | 7   | 0    |           |

A graph model simulating the main stages of the “Service denial” network attack (SYN flood, also known as a “TCP flood attack”) on the digital educational resources is shown in Figure 4, and the simulation results (timed statistics) of the process of its implementation in the CPN Tools software environment are presented in Table 4. Here \( S_1 \) – attacker’s host is ready; \( t_1 \) – launch and configuration of the program for SYN-flood; \( S_2 \) – the attacked host is ready to allocate the SYN packets with an unroutable address in the queue of unopened connections; \( S_3 \) – the program is running and configured; \( t_2 \) – sending SYN packets and queuing them to the attacked host; \( S_4 \) – requests are allocated in the queue of expected connections to the attacked host; \( t_3 \) – queue overflow on the attacked host; \( S_5 \) – the attacked host is not able to handle other requests.

Figure 4. A graph model of the implementation process of the “Service denial” attack.

Table 4. Timed statistics of the implementation process of the “Service denial” network attack.

| Name                          | Count | Sum   | Avrg  | Min  | Max  | Time Avrg |
|-------------------------------|-------|-------|-------|------|------|-----------|
| Marking_size_SYN_flood’S1_1   | 107   | 4968  | 46.428571 | 100 | 1    |           |
| Marking_size_SYN_flood’S2_1   | 107   | 382   | 3.571429 | 100 | 1    |           |
| Marking_size_SYN_flood’S3_1   | 207   | 8871  | 42.857143 | 100 | 12   |           |
| Marking_size_SYN_flood’S4_1   | 207   | 11089 | 53.571429 | 100 | 15   |           |
| Marking_size_SYN_flood’S5_1   | 107   | 0     | 0.000000 | 100 | 52   |           |

4. Conclusion
The innovative technology proposed in the article for the research of implementation dynamics of network attacks on the digital educational resources in the CPN Tools software environment can be used to evaluate the threat of network attack implementation in order to develop a model of relevant attacks and to formulate quantitative requirements to ISS in AS used in the educational environment applications. Potentials of using the obtained results are associated with an increase of the real protection of both the existing DEE and the one under development.

References
[1] Ponomareva M N 2019 Digital educational environment of a professional educational organization: directions of development Innovative development of professional education
Batskikh A V, Drovnikova I G, Ovchinnikova E S and Rogozin E A 2020 Analysis and classification of the main threats to information security of automated systems at the objects of Informatization of internal Affairs Security of information technologies = IT Security 1(27) 40-50

GOST R 51583-2014 2014 Algorithm for creation of automated systems in protected performance (Moscow, Standartinform) p 27

Drovnikova I G, Ovchinnikova E S and Rogozin E A 2019 Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal Affairs bodies and aspects of their improvement Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia 4 51-63

ISO/IEC 15408 2012 Common Criteria for Information Technology Security Evaluation (CC 3.1) 93

Oliver M 2011 Technological determinism in educational technology research: some alternative ways of thinking about the relationship between learning and technology Journal of Computer Assisted Learning 27(5) 373-84

Rebovich G and White B 2011 Enterprise Systems Engineering: Advances in the Theory and Practice (Boca Raton, CRC Press) p 459

Dordevic N 2017 Software quality standards Vojnotehnicki Glasnik Military Technical Courier 65(1) 102-4

Sinegubov S V 2016 Modeling telecommunication systems and networks (Voronezh, VI MIA) p 336

Akinshin R N 2014 Use of mathematical apparatus of the Petri-Markov’s networks for definition of temporary and probabilistic characteristics of the control system by the high-loaded web portals with the increased fault tolerance Scientific Bulletin of MSTU GA 210 90-7

Zaitsev D A and Shmeleva T R 2016 Simulating Telecommunication Systems with CPN Tools (Odessa, ONAT) p 60

IS Threats Data Bank of FSTEC of Russia http://bdu.fstec.ru/threat

Drovnikova I G, Ovchinnikova E S and Konobeyevskikh V V 2020 Analysis of typical network attacks on automated systems of internal affairs departments Bulletin of the Dagestan State Technical University. Engineering sciences 1(47) 85-92