KAUNAS UNIVERSITY OF TECHNOLOGY

TAUTVYDAS BAKŠYS

DEVELOPMENT OF EARLY STAGED CYBER ATTACK DETECTION METHOD FOR IT&T NETWORKS

Summary of Doctoral Dissertation
Technological Sciences, Electrical and Electronics Engineering (T 001)

2019, Kaunas

This doctoral dissertation was prepared at Kaunas University of Technology, Faculty of Electrical and Electronics Engineering, Department of Electronics engineering during the period of 2014 – 2018.

Scientific Supervisor:
Assoc. Prof. Dr. Saulius JAPERTAS (Kaunas University of Technology, Technological Sciences, Electrical and Electronics Engineering, T 001).

Editor: Dr. Armandas Rumšas (Publishing Office "Technologija")

Dissertation Defence Board of Electrical and Electronics Engineering Science Field:
Prof. Dr. Arminas RAGAUSKAS (Kaunas University of Technology, Technological Sciences, Electrical and Electronics Engineering, T 001) – **chairman**;
Prof. Dr. Raimundas MATULEVIČIUS (University of Tartu, Technological Sciences, Informatics Engineering, T 007);
Prof. Dr. Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronics Engineering, T 001);
Prof. Dr. Dangirutis NAVIKAS (Kaunas University of Technology, Technological Sciences, Electrical and Electronics Engineering, T 001).
Prof. Dr. Jevgenijus TOLDINAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering, T 007).

The official defence of the dissertation will be held at 1 p.m. on 29th of August, 2019 at the public meeting of Dissertation Defence Board of Electrical and Electronics Engineering Science Field in Rectorate Hall at Kaunas University of Technology.

Address: K. Donelaičio St. 73-402, 44249 Kaunas, Lithuania.
Tel. no. (+370) 37 300 042; fax. (+370) 37 324 144; e-mail doktorantura@ktu.lt.

Summary of doctoral dissertation was sent on 29th of July, 2019.
The doctoral dissertation is available on the internet http://ktu.edu and at the library of Kaunas University of Technology (K. Donelaičio St. 20, 44239 Kaunas, Lithuania).

KAUNO TECHNOLOGIJOS UNIVERSITETAS

TAUTVYDAS BAKŠYS

ANKSTYVŲJŲ STADIJŲ KIBERNETINIŲ ATAKŲ KOMPIUTERIŲ IR TELEKOMUNIKACIJŲ TINKLUOSE APTIKIMO METODAS

Daktaro disertacijos santrauka
Technologijos mokslai, Elektros ir elektronikos inžinerija (T 001)

2019, Kaunas

Disertacija rengta 2014 – 2018 metais Kauno technologijos universiteto Elektros ir elektronikos fakulteto Elektronikos katedroje.

Mokslinis vadovas:
doc. dr. Saulius JAPERTAS (Kauno technologijos universitetas, Technologijos mokslai, Elektros ir elektronikos inžinerija, T 001).

Redagavo: dr. Armandas Rumšas (Leidykla „Technologija“)

Elektros ir elektronikos inžinerijos mokslo krypties disertacijos gynimo taryba:
prof. dr. Arminas RAGAUSKAS (Kauno technologijos universitetas, Technologijos mokslai, Elektros ir elektronikos inžinerija, T 001) – **pirmininkas**;
prof. dr. Raimundas MATULEVIČIUS (Tartu universitetas, Technologijos mokslai, Informatikos inžinerija, T 007);
prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, Technologijos mokslai, Elektros ir elektronikos inžinerija, T 001);
prof. dr. Dangirutis NAVIKAS (Kauno technologijos universitetas, Technologijos mokslai, Elektros ir elektronikos inžinerija, T 001);
prof. dr. Jevgenijus TOLDINAS (Kauno technologijos universitetas, Technologijos mokslai, Informatikos inžinerija, T 007).

Disertacija bus ginama viešame elektros ir elektronikos inžinerijos mokslo krypties disertacijos gynimo tarybos posėdyje 2019 m. rugpjūčio 29 d. 13.00 val. Kauno technologijos universiteto Rektorato salėje.

Adresas: K. Donelaičio g. 73-402 44249 Kaunas, Lietuva.
Tel. (370) 37 300 042; faks. (370) 37 324 144; el. paštas doktorantura@ktu.lt.

Disertacijos santrauka išsiųsta 2019 m. liepos 29 d.
Su disertacija galima susipažinti internetinėje svetainėje http://ktu.edu ir Kauno technologijos universiteto bibliotekoje (K. Donelaičio g. 20, 44239 Kaunas).

INTRODUCTION

Research object

The object of the dissertation research is the detection of intelligent cyber-attack techniques allowing early detection of cyber attack parameters and their specific characteristics from complex IT systems and the telecommunication network behavioural pathway and ensuring the detection of cyber attacks in the early (1–3) stages.

Relevance of the topic

Intelligent cyber attacks cause the most significant damage in Information and Telecommunications systems. Such attacks can take a very long time, require considerable financial and human resources, and, therefore, they can only be organized by large interest groups. Furthermore, the current Intrusion detection systems, Intrusion prevention systems and Intrusion response systems used to protect against cyber attacks suffer from several shortcomings. Such systems respond only to the attack itself when it is too late to take preventive action, and they are not suitable for detecting an attack in its early stages when it is still possible to block the attack and minimize the losses. Early detection requires detailed monitoring of network and system parameters to be able to accurately identify the early stages of the attack when it is still possible to 'kill the attack chain'. The early-staged cyber attack detection method based on the attack chain analysis while using logical filter system is suggested. This method requires limited computing resources; therefore, it can be implemented in mobile devices, as well.

Objective and tasks

The aim of this work is to develop and examine a method that would enable the detection of early-stage cyber attacks based on parametric logic filter analysis, identifying early attack traits from attack-forming complex factors isolated from cached network traffic and system performance data.

The work intends to perform the following tasks:

1. Perform analysis of the main stages of attacks and their detection methods;
2. Analyze network and system monitoring data by indicating parameters and regularities that enable early detection;
3. Create a system and algorithms capable of determining the necessary detection features for monitoring data streams;
4. Create a method that will enable detection of attacks at early moments by using the collected set of parameters;
5. Experimentally test the created system by collecting monitoring data, obtaining the attacks parameters from the complex traffic and detecting cyber attacks in their early stages.

Scientific novelty

Following the theoretical and experimental research, the following new results for electrical and electronics engineering were obtained:

1. Obtained features of cyber attacks vector characteristic of early stages (stages 1–3), which can be used to detect attacks at earlier moments.
2. A methodology has been developed to enable early cyber-attack stages to be extracted from the intelligent cyber attacks vector based on system behavior and network path parameters.
3. A model has been evaluated by theoretical and practical research enabling attacks to be detected at early moments under realistic conditions.

Statements presented for defence

1. By obtaining the features of cyber vectors, it is possible to detect attacks at early moments;
2. By using a logical filter system, cyber attacks can be detected at earlier moments;
3. The logic filter system can be used to analyze system and network parameters.

Practical relevance

The following practical results were obtained during the preparation of the dissertation:

1. In this work we propose cyber attack scenarios, identify early traits and characteristics of attacks, develop a method of detecting cyber attacks in their early stages and provide proof of the concept software implementation of the method;
2. The early stages of cyber attacks detected by the cyber attacks vector allow the attacking of attacks in the early moments and minimizing the damage they cause;
3. The designed practical system allows the proposed model to be applied in practical environment.

Approbation of the research results

The main results of the dissertation were published in 2 periodical scientific journal (ISI Web of Science) and in 4 issues of international conference proceedings.

Structure and volume of the dissertation

The dissertation consists of an introduction, 4 main chapters, conclusions, a list of the author's publications, and a summary in English. The total volume of the dissertation consists of 108 pages; the thesis includes 49 images, 29 tables, 17 formulas and is based on 91 references.

1. REVIEW OF CYBER ATTACK DETECTION METHODS

The most dangerous cyber attacks are those that are planned in advance [1–3], and they can be planned by both state structures and terrorist organizations. The planned cyber attacks consist of a variety of different stages. Different authors describe the different number of the stages and parameters of such cyber attacks. *Symantec* designates five stages: Reconnaissance, Incursion, Discovery, Capture, and Exfiltration [4]. The same number of stages, but with different names, is proposed in [5]: Reconnaissance, Intrusion, Taking control, Collecting and leaking information, Eliminating traces. Meanwhile, Yadav and Rao [6] suggest seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Act on Objective. More works [6–9] can be found where the number of stages varies between three and eight. Different stages use different means and equipment to organize the attack. It can be assumed that certain actions in the early stages of the attack can prevent serious harmful effects [7, 8]. However, it is necessary to determine the 'early' stages and the 'late' stages when the damage created by an attack is essentially unavoidable. Therefore, it is necessary to distinguish the various stages of an attack in order to provide the means and methods for preventing the consequences of such attacks. Yadav and Rao [6] suggested that the early stages include Reconnaissance, Weaponization, Delivery, and Part Exploitation Stages (Figure 1), in which, if an attack is observed, its effects can be eliminated.

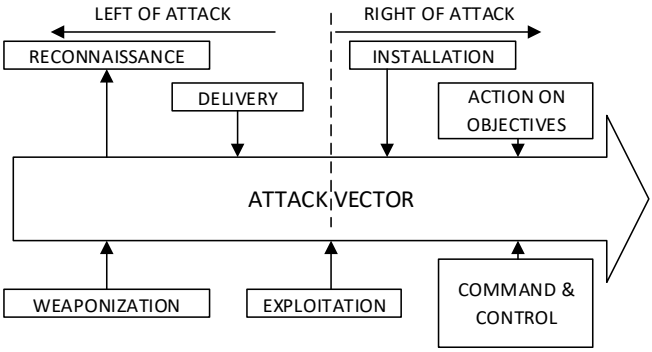

Figure 1. Typical cyber-attack vector formed against IT and Telecommunication systems [6]

Currently, information and telecommunication networks are protected from cyber attacks by using various tools and methods. All these tools and methods can be divided into three groups: intrusion detection system (IDS), intrusion prevention system (IPS), and intrusion response system (IRS). Unfortunately, despite the constant development of such tools and methods, they remain imperfect and cannot protect themselves from well-prepared attacks.

There are currently some attempts to detect cyber-attacks in early stages. Siddique *et al*. [9] presented promising experimental results of the attack detection using IDS. Yan and Zhang [10] offered structured intrusion detection (SID) based on behavioral semantics. However, it is not entirely clear how the 'early stage' is understood and what the opportunities are to process large flows of information. Vincent *et al*. [11] highlighted the importance of early detection and offered some solutions for detecting Trojan viruses. However, it should be noted that Vincent *et al*. [11] did not provide a detection algorithm. Chen *et al*. [12] proposed a model that integrates and correlates multiple logs to identify the early phase of targeted attacks. The state-based hidden Markov model is used to detect joint attacks. However, this model is based on the IDS system, which, as noted above, has a number of shortcomings and, mostly, is designed to detect distributed denial-of-service (DDoS) attacks. Moreover, an idea of provided attack detection is vaguely presented. There are more investigations that are dedicated to the specific type of the attacks [13], [14]. Bhattacharya and Selvakumar [13] suggested a multi-measure multi-weight ranking approach for the identification of the network features for the detection of denial of service (DoS) and probe attacks. This approach combines the filter and wrapper feature selection methods and clustering methods to assign multiple weights to each feature. Cheng *et al*. [14] proposed a DDoS detection method for socially aware networking based on the time-series autoregressive integrated moving average model. The model describes a multi-protocol-fusion feature to characterize normal network flows.

The nature of cyber attacks against IT and Telecommunications systems and networks is different and variable [19]. The system-based attacks are as follows: system insider attacks, user to root attacks, attacks on a virtual machine (VM) or hypervisor. The network-based attacks are as follows: flooding attacks, port scanning, backdoor channel attacks.

As it was mentioned earlier, for detecting cyber attacks, IDSs are used; intrusion detection techniques vary and are categorized as follows [20]:

1. Signature-based Detection (SD);
2. Anomaly-based Detection (AD);
3. Stateful Protocol Analysis (SPA).

The features of these techniques are analyzed in papers [20–23] and are based on various detection algorithms and models:

1. Statistical methods;
2. Data Mining Based Methods;
3. Rule-based systems;
4. Genetic algorithms;
5. State transition-based;
6. Expert-based;
7. Petri Nets;

8. Machine learning methods.

These methods are briefly described in papers [24–27]. Hybrid detection methods are also used [19], [28] that combine several attack detection methods.
One of the desirable features of IDS is being a real-time system. An adaptive intrusion detection system that can detect unknown attacks in real-time network traffic is a major concern. Conventional adaptive intrusion detection systems are computationally expensive in terms of computer resources and time because these systems have to be retrained with known and unknown attacks. Rathore *et al*. [29] proposed a real-time intrusion detection system for ultra-high-speed big data environment using Hadoop implementation. The proposed system is based on four-layered IDS architecture that consists of the capturing layer, the filtration and load balancing layer, the processing or Hadoop layer, and the decision-making layer. Al-Yaseen *et al*. [30] suggested a method that is based on a multi-agent system to allow the intrusion detection system to adapt to unknown attacks in real time. The detection model uses multi-level hybrid support vector machines and extreme learning techniques.
Despite the widespread use of IDS systems, they have a number of weaknesses. Major deficiencies in the network intrusion detection systems (NIDS) include the inability to analyze encrypted traffic, late updates, time delay between the attack start and the warning, and the difficulty of processing data on a redundant network. Hybrid intrusion detection systems (HIDS) deficiencies are identified as the failure to recognize network scans, and inefficiencies in DoS attacks [28], [31]. Some IDSs can be relatively easily avoided (e.g., anomaly-based or signature-based) [32], [33]. Werlinger *et al*. [34] states that the result of using IDS is not always clear. It is also of interest that virtually the same imperfections have existed for many years [6], [25], [35], and even the new methods [33] do not help to avoid them. IPS is a newer approach than the IDS to fight against the cyber security threat. The IPS combines the technique of firewall with the IDS [36]. The use of traditional IPSs for IT and Telecommunications systems is problematic for several reasons [37]:
1. Latency: in-bound IPS requires inspection and blocking action on each network packet, which consumes cloud system resources and increases the detection latency;
2. Resource Consumption: running the intrusion detection and prevention systems (IDPS) services usually consumes significant resources;
3. Inflexible Network Reconfigurations: traditional IPS does not have network configuration features to reconfigure the virtual networking system and provide scrutinized traffic inspection and control.

IRSs are used for responding to attackers' actions. There are two types of an IRS: passive and active IRS, depending on the type of response. If a system

automatically takes measures leading to a response, this system is called an active IRS; if it takes place in a notification or forms a response in the manual way, this system is called a passive IRS [38, 39]. The Audit expert system is currently widely used [39]. In support of Audit expert systems, Moon *et al*. [40] presented *Multi Layer Defense System* (MLDS) which applies a reinforced defense system by collecting and analyzing log information and various information from network infrastructure. Heo *et al*. [41] suggested a system design that helps to maintain a certain level of quality of service (QoS) and quality of security service (QoSS) in threatening environments. Nevertheless, despite all the advantages provided by such systems, they still have many deficiencies that are fully disclosed in papers [34–39].

One of the most significant deficiencies noted by the experts is that such systems are susceptible to violations because they are relatively static (especially for the associative-based IRS). Other major deficiencies are the activation of such systems only when an incident has been detected [38], and also the high number of false alarms, which directly depends on the quality of IDS [39]. There are more deficiencies, but they are related not to the attack itself but rather to the healthy state of the system which can be affected by the use or non-use of the IRS [38] or the use of the appropriate hardware.

One of the reasons for such an ineffective fight is the fact that usually systems (IDS, IPS, and IRS) begin functioning only when the attack is already happening or even has happened. Further reasons for relatively ineffective protection systems are the delay of the software updates and the ability to bypass or negatively impact protection systems functionality by exploiting their own vulnerabilities.

The aim of this dissertation is to suggest a method to determine the possibility of a cyber attack against IT and Telecommunications systems at its earliest stages when the cyber attack can still be effectively stopped.

2. Early Stages of a Cyber Attack

The most dangerous cyber attacks are those that are planned in advance. The preparation of such attacks and their initial stages can last quite long – for months or even years. The attacker can assess all of the victim's weaknesses, and the consequences of the attack could be extremely harmful. The main purpose of these attackers is to get the user's access to the system, so their attack vectors are directed to obtain the user rights in the system by exploiting system software vulnerabilities. At their late stages, such attacks normally cannot be terminated without causing losses. Such prepared cyber attacks are difficult to detect because of their well-planned steps, but if they occur and enter the late stage sector, their consequences are the greatest comparing to other types of attacks. It would be advisable to distinguish two types of attacks: the classic attack and the intelligent attack.

The first type of attack is characterized by the fact that it has virtually no individual stages, or, in some cases, it is possible to distinguish one or two stages: exploration and attack. Such attacks are relatively fast, often without a well-defined target, they are poorly organized and coordinated. The tools used in such attacks are intended to create rugged effects, i.e., launching DoS and DDoS attacks, various viruses (untargeted), malware, and similar ones. Such attacks cause losses, but usually these losses relate to a single entity or an individual object, the effects of such attacks are relatively easily recoverable, and the attackers are easily detectable. Attackers creating such attacks are normally represented in relatively low-impact output groups, i.e., hackers, crackers, phreakers, or vandals. Normally, these groups are formed from a small number of members, and, in most cases, just one member forms a group.

The second type of attacks (intelligent attacks) are denoted by the following characteristics: detailed planning, multiple stages, and slow progress. Attackers have a well-defined target and a well-defined goal. Attacks use malware specifically designed for the target and deep self-disguise. The effects of such attacks are extremely damaging, and requiring a lot of effort to eliminate the consequences of the attacks. Such attackers are in large groups and well-organized, with sufficient financial resources from criminal groups, terrorist organizations or state structures. The general classification of cyber attacks is given in Table 1.

Table 1. General classification of cyber attacks

Attacks parameters	**Classic**	**Intelligent**
Number of Stages	1–2	> 3
Speed of Attack	Fast	Slow
Attack types	DoS, DDoS, malware, virus	Classic and custom made software tools, purposefully delivered to a certain target and specifically adapted to the victim's network and system configuration
Attacker types	Individual person or small groups	Criminal and terrorist groups, state structures
Target of an attack	Separate object or subject	Object groups, state institutions, economic branches, wide social groups
Attackers financial resources	Relatively small	Wide financial resources, in some cases, unlimited
Consequences	Relatively small, easily recovered	Heavy losses, hardly recoverable

For intelligent attacks, it is necessary to firstly define their possible stages. As stated in the introduction, the elaboration of those stages is an important factor in

enabling the most accurate estimation of the initial stages of the attack which has not yet done any harm and which can still be described as 'chain killing'. Yadav and Rao [6] proposed a vector for intelligent attacks that is formed out of seven stages. Although Yadav and Rao [6] clearly distinguished two groups of stages (early stages and late stages), our suggestion is to extend the number of groups into three:

1. Early stages;
2. Transitional stages;
3. Late stages.

The early stages include processes for data collection, target tracking and attack infrastructure. In the transitional stages, information from the early stages is used, and actions are taken to weaken the victim's system (e.g., implementing a malicious code or process against the system, exploiting its vulnerabilities). This enables access to the system. Thereafter, the late stage attack processes follow: direct system take-over, specific data capture, or infrastructure removal procedures.

Based on the literature analysis and own experience, an extension of the number of stages proposed in [6] to nine was suggested by adding the stage of social engineering and incorporating the stage of evasion (Fig. 2).

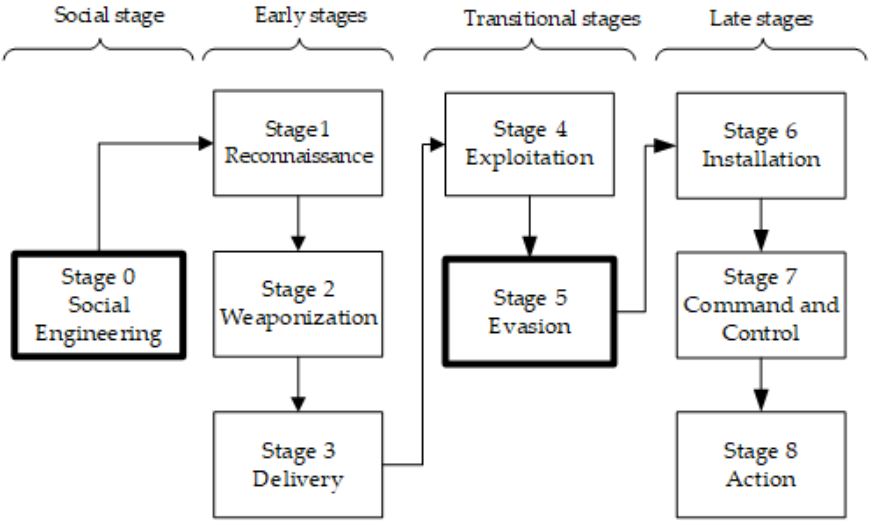

Figure 2. Offered attack vector with additional stages

In the social engineering phase (Stage 0), there is an attempt to extract certain information about the future cyber attack target (an entity or an object) with some

information that would facilitate a cyber attack by using the psychological effects of human beings. Experts say that the impact of social engineering is almost impossible to avoid. Therefore, this is a good way to extract certain primary data. In this paper, this stage will not be discussed further because it is the information collection step that involves various social and psychological manipulation techniques. However, to the extent that it aims to obtain data for planning a cyber attack, social engineering should be considered as the initial stage of a cyber attack.

It is supposed that an attack can be withheld if it was detected in the preliminary stages 1–3, i.e., reconnaissance, weaponization and delivery, since an attack detection during these stages allows killing or blocking the attack. In Fig. 3, a summary of all the stages is presented with the steps that are taken at each stage by the attacker. Because of the continuing attack vector, tangible damage starts with directly interfering with the system and network work. It is necessary to detect these processes before they reach the 4^{th} stage (stage 4 – exploitation).

The first stage of the attack (reconnaissance) is formed of three actions: port scan, host scan and system version scan. Port scan involves scanning network ports by using a SYN request. Host scan is a scan of nodes in the system and obtaining their IP addresses. Version scan is the obtaining of the service version of the system.

The second stage (weaponization) includes two factors: system & services version scan and service stress test.

The third stage (delivery) is the stage when the first part of the malicious code is delivered to victim's infrastructure to be executed at a certain time, and it begins harmful processes against the targeted system.

The third stage consists of two actions: version check and spoofing. Each of these factors has its own activities. For example, the spoofing factor includes actions such as modifying network packets and programs with malicious code infiltration; the action of services stress tests performs the over-loaded system processes remotely.

Processes and actions which are executed by an adversary can be registered by monitoring the network stack and system behavior. The monitoring results enable distinguishing the features inherent in these ongoing processes and their application for the detection of system anomalies and recognition of the beginning of an attack.

Attacks in the different stages are denoted by a number of characteristics that identify the attack process. In this dissertation, we distinguish among three characteristic groups that allow characterizing the ongoing processes: physical network stack parameters, logical parameters of the system being attacked, network stack flags.

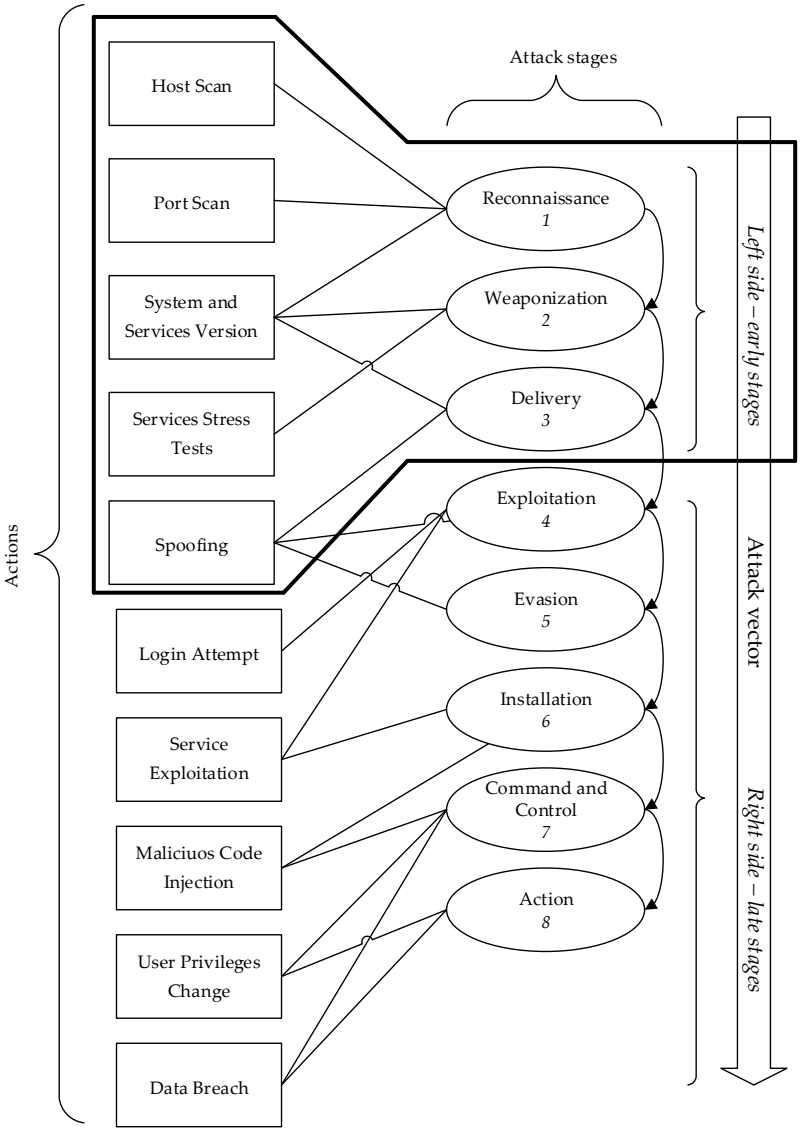

Figure 3. Action impact of the attack stages

3. Method to Detect the Early Stages of a Cyber Attack

The essence of the proposed method is to use the appropriate logical filters in order to classify the certain parameters of the traffic. For this purpose, the total analyzed data (information) flow is considered to consist of two parts: the normal flow (i.e., the flow that is not harmful), and the attacker's flow (malicious flow). A generic filter structure is shown in Figure 4.

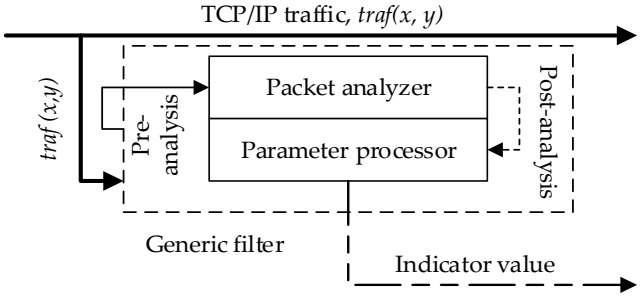

Figure 4. Structure of a Generic Filter

The generic filter consists of two blocks: a packet analysis block and a parameter processor. The *traf(x, y)* input into the filter is analyzed on the packet level, which results in a packet parameter (e.g., DST IP). The obtained parameter is passed to the internal parameter processor that forms an indicator value according to the provided conditions.

A schematic view of the activities of the detection method is shown in Fig. 5. In the proposed method, traffic *traf(x, y)* is unmodified because there is need to maintain the traffic of the system without affecting the system services reliability. It is shown as a separate line ("Unmodified traffic *x* and system status *y*"). The detection method consists of three parts: the filter part, the evaluation block, and the action block. The filters are implemented in two blocks: consolidated network filtering and system monitoring (CNFSM) and parameter preprocessing (PP). In the CNFSM block, the filters are grouped into three groups: filtering of network parameters (NF), filtering of system parameters (SF), filtering of network stack flags (LF). The evaluation block consists of three logical circuits that are connected at the outputs of the corresponding filter groups. The purpose of the filters is to register parameters and, if their values exceed some predefined values, indicate the malicious activity. The purpose of the evaluation block is to collect binary parameters and process them for the indication of the possible attack action. The purpose of the action block is to decide which stage of the attack is being observed.

By using this principle, it is possible to analyze network traffic and system behavior adaptively by adjusting filters for analysis according to the need

(available resources, depth of analysis, speed and tolerances of the created system or network delays).

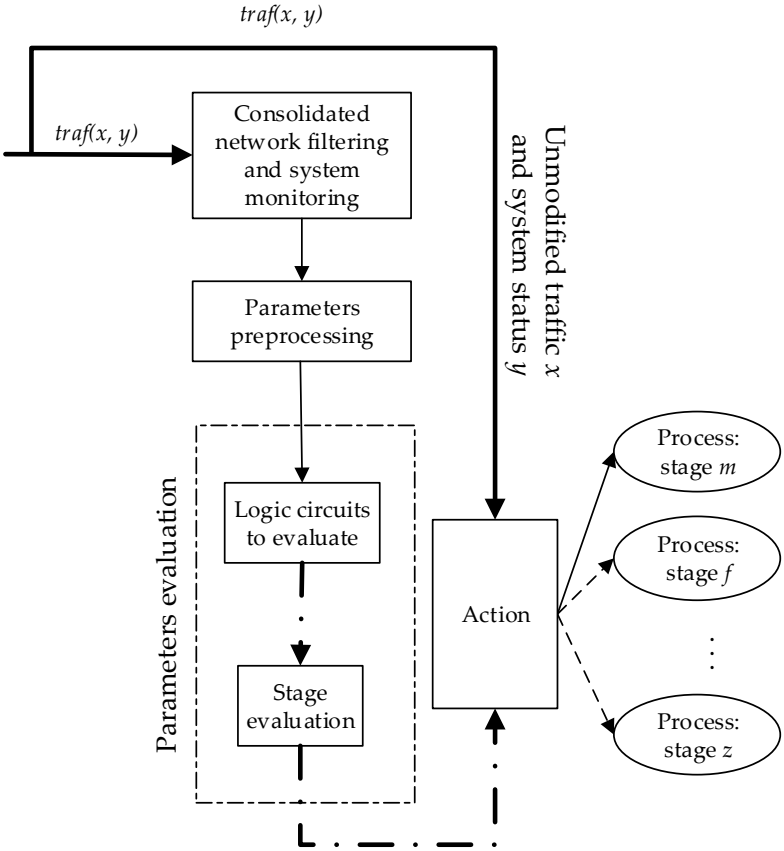

Figure 5. Schematic view of the detection method

The detailed schematic view containing filters is shown in Fig. 6. To ensure early detection, different types of filters are used: network parameters NF (shown in circles); system parameters SF (depicted in rectangles); network stack flags LF (shown in hexagons). The three filter groups in total include 31 different filters: 12 filters belong to the NF group, 6 filters belong to the SF group and the remaining 13 filters belong to the LF group. These filters are consolidated, i.e., they perform the collection of the parameters and their analysis.

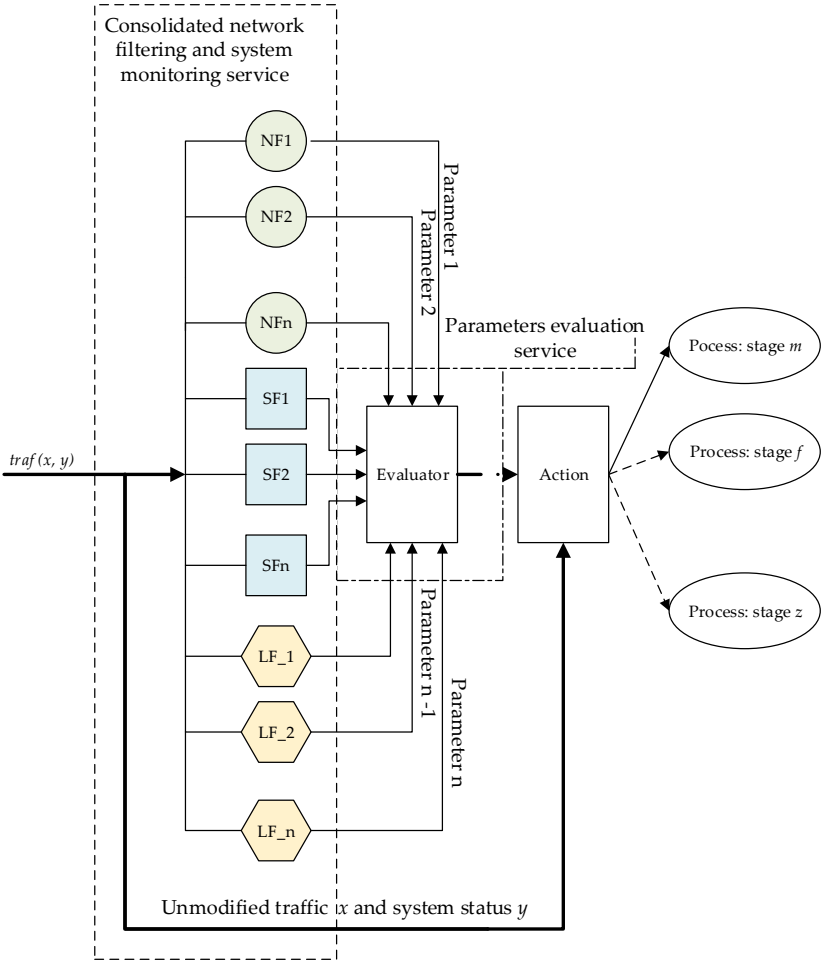

Figure 6. Detailed schematic view of the filters

The filters of network parameters are numerated from 1 to 12 (NF1 ... NF12 and the outputs of the filters which form inputs to the logical circuit are labeled as x1 ... x12). The filters of the system behavior are labeled from SF1 to SF6. The outputs of the filters are labeled as x13 ... x18. The filters of network stack flags are labeled from LF1 to LF13. The outputs of the filters are labeled as x19 ... x31. All the filters and their functions are enumerated in Table 2.

The data collected from all the types of logical filters is sent to the parameter preprocessing block, in which, according to filtered parameters, sets of attack parameters are further processed. If the value of the filtered parameter exceeds the

predefined value, then this parameter is assigned the binary value 1 (anomaly value), otherwise – the binary value 0 (normal value).

Table 2. Functions of attack filters

No.	Filter name	Filtering parameter	Filter description
1	NF1	IP	Attacker's IP address
2	NF2	IP COUNT	IP address repetition
3	NF3	PORT NUMBER	Port number to which the information is sent
4	NF4	PORT DISTRIB.	Distribution of ports according to the token information
5	NF5	PACKET COUNT	The number of packets in the network tract
6	NF6	STACK BYTES	Amount of data transferred in the session
7	NF7	PACKETS A-> B	Number of packets sent from the attacker to the victim
8	NF8	PACKETS B->A	Number of packets sent from the victim to the attacker
9	NF9	BYTES A->B	Amount of data transferred from the attacker to the victim
10	NF10	BYTES B->A	Amount of data transmitted from the victim to the attacker
11	NF11	DURATION	Duration of the active single session between the attacker and the victim
12	NF12	ABSOLUTE TIME	Absolute start time for the session
13	SF1	PERIPHERAL STATUS	Whether the peripheral device has changed
14	SF2	UNLISTED PROCESS	What processes in the system are in the list
15	SF3	FLAWLESS USER LOGIN	Whether an unexpected user connection was attempted or a password or unconnected connection was attempted
16	SF4	SUSPICIUOS TIME	System clock times whose average significantly deviates from the standard user connection time
17	SF5	DISK ACTIVITY	Increased activity of the disk array is detected by comparing with the average value
18	SF6	PORT BINDING	Whether the port is bound to port
19	LF_FIN	FIN FLAG	Packet's FIN flag
20	LF_SYN	SYN FLAG	Packet's SYN flag
21	LF_TCP_CONN()	TCP_CONN() FLAG	TCP Connection request
22	LF_NULL	NULL FLAG	NULL flag
23	LF_PING	ICMP FLAG	ICMP request
24	LF_VERSION_DETECTION	VER FLAG	VERSION flag
25	LF_UDP_SCAN	UDP FLAG	UDP request
26	LF_BULK_SCAN	BULK FLAG	Random request
27	LF_WINDOWS_SCAN	WIN_SCAN FLAG	Versions of Windows query
28	LF_RPC_SCAN	RPC FLAG	Identification of the RPC protocol
29	LF_LIST_SCAN	LST FLAG	A query that results in a list of the previous query vector
30	LF_IDLE_SCAN	IDL FLAG	An IDLE process request
31	LF_FTP_BOUNCE	BOUNCE FLAG	FTP service request

The algorithm of this process is shown in Fig. 7. The algorithm indicates that, upon receiving the TCP/IP packet, packet structure analysis is executed, in which, the existing packet fields are read, and parameter search is performed, numerical estimates are generated which are compared to the limit values. According to the result of this process, seven attack actions can be distinguished that fall into the three early attack stages. The actions are as follows:

1. HS – Host Scan;
2. PS – Port Scan;
3. SSV – System and Services Version;
4. SST – Services Stress Tests;
5. SP – Spoofing;
6. LA – Login Attempt;
7. SE – Service Exploitation.

The processed session parameter sets are sent to the evaluation block of logical circuits. The evaluation block consists of three independent logic circuits: the first logical circuit performs analysis of the evaluated parameters of NF, the second logical circuit evaluates the analyzed SF parameters, and the third logical circuit performs analysis of filtered LF parameters. The configuration of these filters allows creating a setup of detection whose result is determined by logical circuits. Logical circuits operate on sets of binary parameters. Seven types of the possible attack actions were determined, therefore, the logical circuits were designed which had seven primary outputs. In such a way, every primary output indicates the presence of the different attack action. A logical circuit of NF analysis uses primary inputs x1 ... x12 and produces seven primary outputs labeled as F21 ... F27. A logical circuit of SF analysis uses primary inputs x13 ... x18 and produces seven primary outputs labeled as F35 ... F41. A logical circuit of LF analysis uses primary inputs x19 ... x31 and produces seven primary outputs labeled as F42 ... F48. Subsequently, the primary outputs of all the logical circuits are combined at the final point in the evaluator block. The algorithm to decide the possible attack action is presented in Fig. 8.

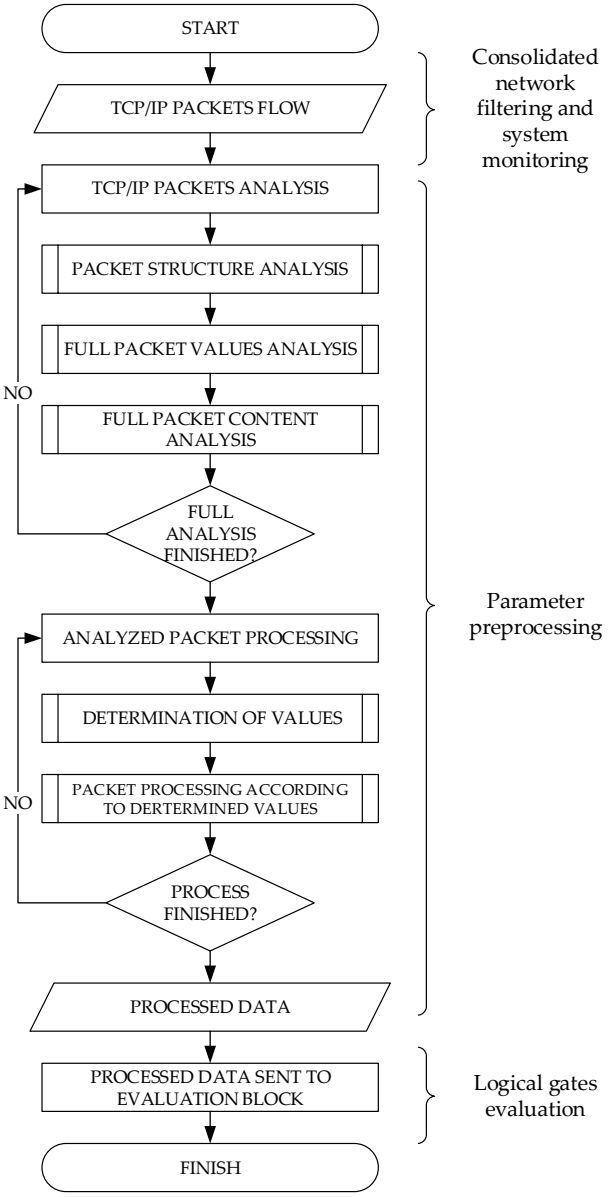

Figure 7. Algorithm of filtered data preparation for logical analysis

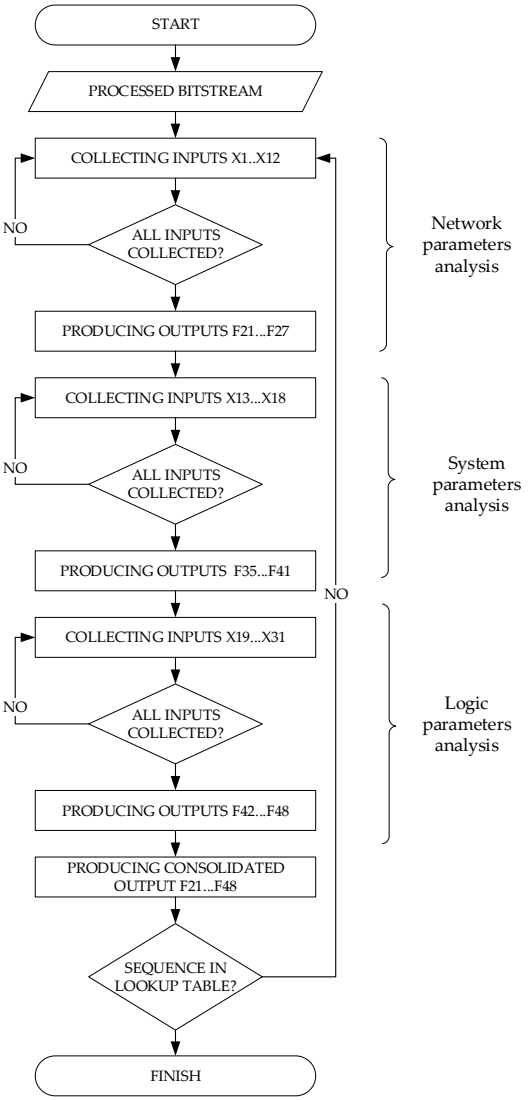

Figure 8. Algorithm of logical analysis

The bit stream which arrives at the inputs of the evaluation block is divided into three parts and supplied into three independent logical circuits. Every circuit is dedicated and produces seven bits. The values at the primary outputs of all the

three logical circuits are joined into a single vector. Only the values of the combined vector can implicate the presence of the attack action. The presence of the values of the final vector in the lookup table indicates the early stage of a cyber attack.

The analytical form of the logical circuit of the NF analysis is shown in (1). Member xA, where $A \in \{1 \ ... \ 12\}$, corresponds to the binary 1, and member $\overline{xA}$, where $A \in \{1 \ ... \ 12\}$, corresponds to the binary 0. This form contains output logical functions which consist of inputs $x1$ ... $x12$, and Output 1 is a vector of F21 ... F27 values.

$$OUTPUT\ 1 = \begin{Bmatrix} F21 \\ F22 \\ F23 \\ F24 \\ F25 \\ F26 \\ F27 \end{Bmatrix} = \cdot \begin{Bmatrix} x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot \overline{x5} \cdot \overline{x6} \cdot \overline{x7} \cdot \overline{x8} \cdot \overline{x9} \cdot \overline{x10} \cdot \overline{x11} \cdot \overline{x12} \\ x1 \cdot x2 \cdot x3 \cdot x4 \cdot \overline{x5} \cdot \overline{x6} \cdot \overline{x7} \cdot \overline{x8} \cdot x9 \cdot x10 \cdot \overline{x11} \cdot \overline{x12} \\ x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot x5 \cdot \overline{x6} \cdot \overline{x7} \cdot \overline{x8} \cdot \overline{x9} \cdot \overline{x10} \cdot \overline{x11} \cdot \overline{x12} \\ x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot \overline{x5} \cdot x6 \cdot x7 \cdot x8 \cdot \overline{x9} \cdot \overline{x10} \cdot \overline{x11} \cdot \overline{x12} \\ x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot x5 \cdot \overline{x6} \cdot \overline{x7} \cdot \overline{x8} \cdot \overline{x9} \cdot \overline{x10} \cdot x11 \cdot x12 \\ x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot x5 \cdot \overline{x6} \cdot \overline{x7} \cdot \overline{x8} \cdot \overline{x9} \cdot \overline{x10} \cdot x11 \cdot x12 \\ x1 \cdot x2 \cdot \overline{x3} \cdot \overline{x4} \cdot x5 \cdot x6 \cdot \overline{x7} \cdot \overline{x8} \cdot \overline{x9} \cdot \overline{x10} \cdot \overline{x11} \cdot \overline{x12} \end{Bmatrix} \quad (1)$$

Table 3 shows the attack actions that make up the attack vector. The values in the column under the name 'Action' have the attribute 'part' because the single circuit on its own cannot fully define the action of an attack. The action of an attack can be defined only when the results of the all the three circuits are combined.

Table 3. Lookup table of $x1 \ldots x12$ parameter set and NF output values

No.	ACTION	INPUTS												OUTPUTS						
		x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12	F21	F22	F23	F24	F25	F26	F27
1	HS part	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
2	PS part	1	1	1	1	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0
3	SSV part	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0
4	STT part	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	1	0	0	0
5	SP part	1	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0
6	LA part	1	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	1	0
7	SE part	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1

The logical circuit of NF analysis is presented in Fig. 9. On the left side of the picture, it marks binary processed NF parameter inputs; these parameters are obtained directly from the network driver.

The logical circuit uses 23 logical gates. Primary outputs F25 and F26 are identical due to the identity of the analyzed parameter values (the analyzed parameters of the SP Part and LA part are identical in this analysis, so the generated response is the same, but the outputs are different).

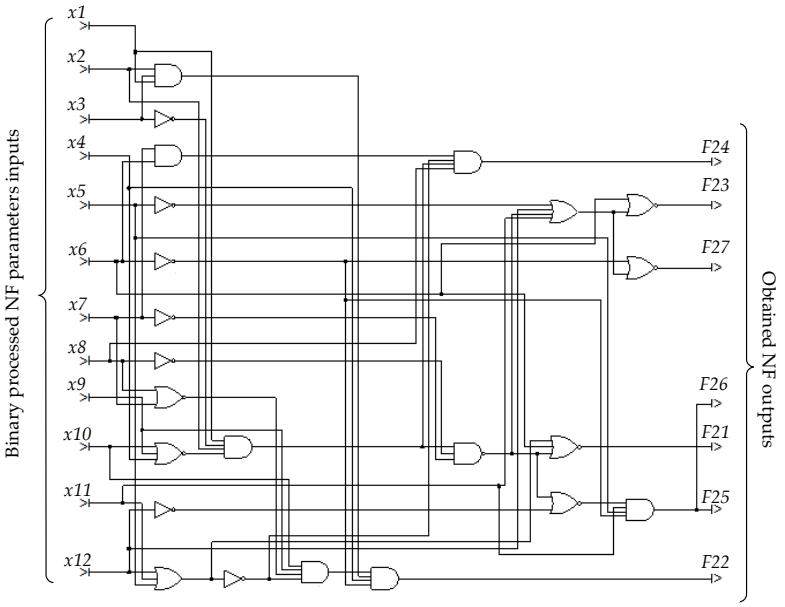

Figure 9. Logic circuit of x1…x12 bit stream parameters

For example, the values on the primary inputs indicating the HS action part of the attack are as follows: $x1 = 1$, $x2 = 1$, $x3 = 0$, $x4 = 0$, $x5$ ... $x12 = 0$, and the primary output is F21 = 1, the remaining primary outputs are F22 ... F27 = 0. In this case, the HS action part of the attack will be detected when parameter $x1$ 'IP address' and parameter $x2$ 'IP repetition' exceed their predefined values; meanwhile, the predefined values of the remaining NF filter parameters $x3$ ... $x12$ will not be exceeded. In this case, the entire output vector will have a value of 1000000. Such an assessment is only part of the overall assessment of the HS action process, and other parts of the assessment are performed at SF and LF logical circuits, respectively.

Output 1 is the first part of the logical analysis results, and further results are obtained from SF and LF analysis named as Output 2 (SF) and Output 3 (LF), respectively.

The analytical form of SF analysis Output 2 is shown in (2). Analogically to the case of Output 1, member $xA, A \in \{13 \ ... \ 18\}$ corresponds to the binary 1, and member $\overline{xA}, A \in \{13 \ ... \ 18\}$ corresponds to the binary 0.

Output 2 result consists of F35 ... F41 primary outputs. The obtained result is the second part of the analysis which is combined with Output 1.

$$OUTPUT\ 2 = \begin{Bmatrix} F35 \\ F36 \\ F37 \\ F38 \\ F39 \\ F40 \\ F41 \end{Bmatrix} = \begin{Bmatrix} \overline{x13} \cdot \overline{x14} \cdot \overline{x15} \cdot \overline{x16} \cdot \overline{x17} \cdot \overline{x18} \\ \overline{x13} \cdot \overline{x14} \cdot \overline{x15} \cdot \overline{x16} \cdot \overline{x17} \cdot \overline{x18} \\ \overline{x13} \cdot \overline{x14} \cdot \overline{x15} \cdot \overline{x16} \cdot \overline{x17} \cdot x18 \\ \overline{x13} \cdot x14 \cdot x15 \cdot x16 \cdot x17 \cdot x18 \\ \overline{x13} \cdot \overline{x14} \cdot \overline{x15} \cdot \overline{x16} \cdot \overline{x17} \cdot x18 \\ \overline{x13} \cdot \overline{x14} \cdot x15 \cdot x16 \cdot \overline{x17} \cdot x18 \\ \overline{x13} \cdot x14 \cdot x15 \cdot x16 \cdot x17 \cdot x18 \end{Bmatrix} \tag{2}$$

Table 4 shows the attack actions that make up the attack vector of the SF analysis. In this case, the attack action HS part and the attack action PS part describe the values on the primary inputs *x*13 ... *x*18 as zeroes. This is because the SF analysis parameters *x*13 ... *x*18 do not take part in forming HS and PS actions. However, this result is important, and outputs F35 and F36 are assigned the appropriate values.

Table 4. Lookup table of x13…x18 parameter and SF output values

No.	ACTION	INPUTS						OUTPUTS						
		x13	x14	x15	x16	x17	x18	F35	F36	F37	F38	F39	F40	F41
1	HS part	0	0	0	0	0	0	1	0	0	0	0	0	0
2	PS part	0	0	0	0	0	0	0	1	0	0	0	0	0
3	SSV part	0	0	0	0	0	1	0	0	1	0	0	0	0
4	STT part	0	1	1	1	1	1	0	0	0	1	0	0	0
5	SP part	0	0	0	0	0	1	0	0	0	0	1	0	0
6	LA part	0	0	1	1	0	1	0	0	0	0	0	1	0
7	SE part	0	1	1	1	1	1	0	0	0	0	0	0	1

The logical circuit used for SF analysis is shown in Fig. 10. The analysis is based on six criteria, so there are six primary inputs and, as previously mentioned, seven primary outputs to identify the action of an attack.
In the logical circuit of SF analysis, 12 logical gates are used. As in the case of the NF circuit, there are input sequences that are identical, therefore, primary outputs F35 and F36, primary outputs F37 and F39, and primary outputs F38 and F41 are connected in parallel. Despite the fact that some input vectors for the SF circuit are the same, their combination with the input vectors of the NF circuit makes the unique input vector and produces a different final output result.

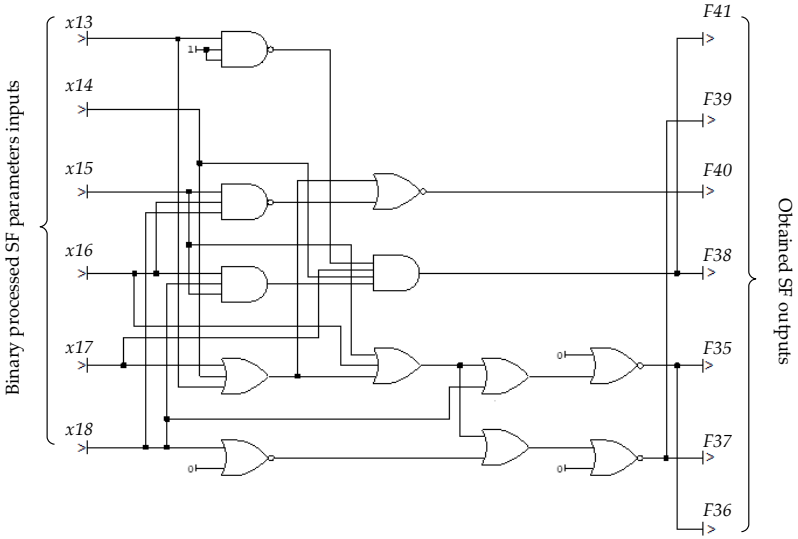

Figure 10. Logical circuit of $x13 \ldots x18$ bit stream parameters

The analytical approach to LF Analysis Output 3 result is shown in (3). Analogically to the Output 1 and Output 2 forms, member xA, $A \in \{19 \ldots 31\}$ corresponds to the binary 1, and member $\overline{xA}$, $A \in \{19 \ldots 31\}$ corresponds to the binary 0. Output 3 is the last component of the logical gate analysis characterizing the flag states in the network stack.

$$OUTPUT\ 3 = \begin{Bmatrix} F42 \\ F43 \\ F44 \\ F45 \\ F46 \\ F47 \\ F48 \end{Bmatrix} = \begin{Bmatrix} \overline{x19} \cdot \overline{x20} \cdot x21 \cdot \overline{x22} \cdot x23 \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \\ x19 \cdot x20 \cdot \overline{x21} \cdot \overline{x22} \cdot \overline{x23} \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \\ \overline{x19} \cdot \overline{x20} \cdot x21 \cdot x22 \cdot \overline{x23} \cdot x24 \cdot x25 \cdot x26 \cdot x27 \\ \overline{x19} \cdot \overline{x20} \cdot x21 \cdot \overline{x22} \cdot x23 \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \\ \overline{x19} \cdot \overline{x20} \cdot x21 \cdot x22 \cdot \overline{x23} \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \\ \overline{x19} \cdot \overline{x20} \cdot x21 \cdot \overline{x22} \cdot x23 \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \\ \overline{x19} \cdot \overline{x20} \cdot x21 \cdot x22 \cdot x23 \cdot \overline{x24} \cdot \overline{x25} \cdot \overline{x26} \cdot \overline{x27} \end{Bmatrix} \cdot \begin{Bmatrix} \overline{x28} \cdot \overline{x29} \cdot x30 \cdot \overline{x31} \\ \overline{x28} \cdot \overline{x29} \cdot \overline{x30} \cdot \overline{x31} \\ x28 \cdot x29 \cdot \overline{x30} \cdot \overline{x31} \\ \overline{x28} \cdot \overline{x29} \cdot \overline{x30} \cdot x31 \\ \overline{x28} \cdot \overline{x29} \cdot \overline{x30} \cdot \overline{x31} \\ \overline{x28} \cdot \overline{x29} \cdot \overline{x30} \cdot \overline{x31} \\ \overline{x28} \cdot \overline{x29} \cdot x30 \cdot x31 \end{Bmatrix}. \quad (3)$$

The values on the primary outputs of the logical circuits are combined, and the attack factors are determined according to the obtained result.

Table 5 shows the attack actions that make up the attack vector of the LF analysis. In this case, the primary inputs x19 ... x31 and the primary outputs F42 ... F48 are used. Differently from NF and SF analysis, there are no duplicate output cases. All the primary outputs are activated with unique combinations on the primary inputs.

Table 5. Lookup table of *x*18…*x*31 parameter set and LF output values

No.	ACTIONS	INPUTS													OUTPUTS						
		x19	x20	x21	x22	x23	x24	x25	x26	x27	x28	x29	x30	x31	F42	F43	F44	F45	F46	F47	F48
1	HS part	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0
2	PS part	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
3	SSV part	0	0	1	1	0	1	1	1	1	1	1	0	0	0	0	1	0	0	0	0
4	STT part	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0
5	SP part	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
6	LA part	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
7	SE part	0	0	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1

The logical circuit used for LF analysis is shown in Fig. 11. For the analysis, 13 criteria are used, and 13 primary inputs x19 ... x31 correspond to them. The seven primary outputs F42 ... F48 for identifying attack actions are used. The logical circuit consists of 26 logical gates. In this circuit, unlike NF and SF cases, there are no identical value combinations on the primary inputs.

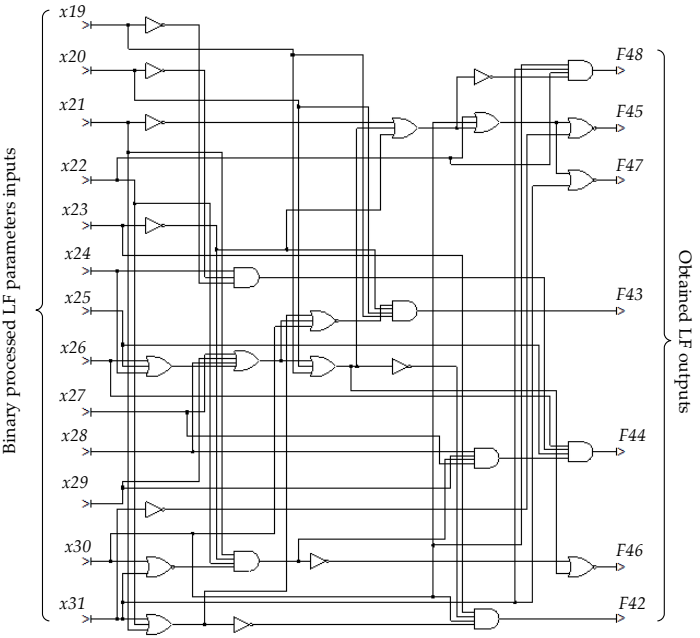

Figure 11. Logical circuit of *x19*…x31 bit stream parameters

The analytical aggregated expression combining the previously presented separate results is presented in (4). Formula (4) combines output vectors of Output 1, Output 2, and Output 3 into a single vector for cyber attack detection.

$$OUTPUT\ ACTION\ FULL\ (OAF) = OUTPUT1 + OUTPUT2 + OUTPUT3 \quad (4)$$

An accumulated description of the attack actions is presented in Table 6.

Table 6. Lookup table for definition of attack actions

No.	ACTIONS	NF OUTPUTS							SF OUTPUTS							LF OUTPUTS						
		F21	F22	F23	F24	F25	F26	F27	F35	F36	F37	F38	F39	F40	F41	F42	F43	F44	F45	F46	F47	F48
1	HS	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
2	PS	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
3	SSV	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
4	STT	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
5	SP	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
6	LA	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
7	SE	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1

For example, HS denotes that attack action Host Scan is fully characterized by code HS = 10000010000001000000 consisting of a set of NF = {F21 ... 27}, SF = {F35 ... 41} and LF = {F42 ... F48} filters. It is possible to determine the early stage of the attack according to the values in Table 6.

4. Early Detection Results

To determine the detection capabilities of the proposed method, we generated an array of 100352 events which were analyzed by the proposed logical circuits. The proposed early detection method consists of three filters: network filter (NF), system filter (SF), and network flags filter (LF). The generated array was analyzed by these filters separately, and the obtained results were combined to determine the attack action formed out of events. The generated 100352 events consist of 100053 randomly generated events and 299 events that have the parameters of known attacks. NF, SF and LF filters identification values are shown in Table 7. Eight parameters are shown in the table of the filters: seven parameters that indicate the detection of an attack: HS, LA, PS, SE, SP, SST, SSV, and parameter 0 that corresponds to non-malicious traffic.

As it was possible to predict, the largest values are for non-malicious traffic which are shown in the last row of Table 7. The values 0% in this row show the very

important obtained result that all the deterministically generated events were detected as malicious.

Table 7. NF, SF and LF filters attack identification values

Actions	Filter NF			Filter SF			Filter LF		
	No. of events	Randomly generated events	Deterministically generated events	No. of events	Randomly generated events	Deterministically generated events	No. of events	Randomly generated events	Deterministically generated events
HS	6242	95%	5%	7632	96%	4%	3728	92%	8%
LA	1790	83%	17%	2133	86%	14%	4068	93%	7%
PS	438	32%	68%	7632	96%	4%	2979	90%	10%
SE	944	68%	32%	888	66%	34%	621	52%	48%
SP	1790	83%	17%	6997	96%	4%	3535	92%	8%
SST	616	51%	49%	888	66%	34%	2162	86%	14%
SSV	1802	83%	17%	6997	96%	4%	349	14%	86%
0	86730	100%	0%	67185	100%	0%	82910	100%	0%

The biggest number of detected events in the filter NF was HS, and the lowest number was for PS. HS actions also had a high detection ratio in filter SF. The most noticeable difference between the filters SF and NF was that PS action in filter SF had a high detection ratio of randomly generated events. Filter LF showed a substantially lower number of events in comparison with filters NF and SF for action HS. Such differences in the action detection ratios among filters show the specificity of methods.

In Table 8, an aggregated form out of the three filters for actions HS, LA, and PS is shown, which indicates the detection of the first stage – Reconnaissance. The obtained result confirms that the proposed method is able to detect all the deterministically on purpose generated events. The proposed method has also detected a number of randomly generated events, which varies depending on the action.

Table 8. Aggregated form of three filters

Name	**HS**	**LA**	**PS**
Detected events	1154	305	316
Detected randomly generated events	855	6	17
Detected deterministically generated events	299	299	299
Deterministically/TOTAL %	26%	98%	95%

For the second part of the experimental set, we generated an array of randomly selected 100352 events. The objective of this part of the experiment is to evaluate the possibility to create an attack randomly. The results of the three filters NF, SF and LF and accumulation results $A = NF \,\&\, SF \,\&\, LF$ are shown in Table 9.

Table 9. Results of filters NF, SF, LF and accumulated detection

Action	Filter *NF*		Filter *SF*		Filter *LF*		Accumulated detection	
	No. of detected events	% of total events	No. of detected events	% of total events	No. of detected events	% of total events	No. of detected events	% of total events
HS	6424	6%	7616	8%	3790	4%	1181	1%
LA	1784	2%	2165	2%	4107	4%	301	0.3%
PS	466	0%	7616	8%	2922	3%	312	0.3%
SE	967	1%	874	1%	609	1%	289	0.3%
SP	1784	2%	6653	7%	3495	3%	310	0.3%
SST	621	1%	874	1%	2148	2%	270	0.3%
SSV	1803	2%	6653	7%	320	0%	2	0%
'0'	86503	86%	67901	68%	82961	83%	97687	97.6%

The main part of the traffic is generated randomly for both parts of the experiment. Therefore, we can compare detection of malicious actions in the random traffic in Table 7 and in Table 9. The main stream of the randomly generated traffic is non-malicious (see the last rows of Table 7 and Table 9). Moreover, the obtained numbers of the non-malicious traffic are quite similar in both tables, e.g., filter NF showed 86,730 events for action HS in Table 7, and filter NF showed 86,503 events for action HS in Table 9. The same is true for detection of malicious events, as well. For example, filter SF showed 2,133 events for action LA in Table 7 and filter SF showed 2,165 events for action LA in Table 9.

This confirmed that the proposed method is capable to detect the early stages of the cyber attack in the network traffic. The method showed that the randomly generated traffic consists of 1.6% events indicating the Reconnaissance stage (the first stage), 0.3% events indicating the Weaponization stage (the second stage), and 0.3 % events indicating the Delivery stage (the third stage).

The proposed method is a part of a large work that is oriented to near-real-time cyber attack detection.

Conclusions

1. Scientific and technical literature analysis and good practice show that the current system of response to cyber threats using IDS, IPS and IRS systems is denoted by a number of shortcomings, and the main problem is that they start up only when a cyber attack is taking place, i.e., such a system does not play the preventive role. Intelligent cyber attacks are characterized by using certain stages. In order to determine the precautionary state, when preventive measures can 'kill the chain', the identification of those stages has to be as complete as possible. In this dissertation, we considered an attack chain of nine steps to describe the cyber attack vector.
2. The dissertation proposes a method to detect an intelligent cyber attack which takes several preparation steps and which is the most dangerous one, as it takes place in the early stages of the cyber attack. The method is based on the use of several logical filters. To ensure early detection, different types of filters were proposed: network parameters NF filter; system parameters SF filter; network stack flags LF filter. These three filter groups in total include 31 different filters: 12 filters belong to the NF group, 6 filters belong to the SF group, and the remaining 13 filters belong to the LF group. These filters are consolidated, i.e., they perform the collection of the parameters and their analysis. These filter sets allow obtaining attack parameters in early stages (stage 1–3). Analytical aggregated expressions have been built for the detection of threats caused by the early stages of the cyber attacks.
3. Experiments to test the ideas implemented in the proposed method were carried out. The essence of the experiments was to evaluate the reliability of the suggested method. All the values which were generated deterministically for the attack were identified as malicious ones. The proposed method was able to detect many real simple and complex cyber attacks at their early stages thus giving the accumulated detection rate of 97.6%. In practical use, the proposed method was able to detect cyber attacks – the best results for classical attacks detection were obtained for Syn Flodd (92%) and Ack Flood (91%). Wannacry (80%) and Cryptolocker (90%) were analyzed for intelligent attacks. It can be proposed that such a result shows a good base for further work in increasing the sensitivity of the method to other forms of cyber-attacks.
4. The mode to detect the early stages of a cyber attack may be appropriate for both standard information systems and small-sized mobile devices since the suggested method is suitable for processing data on devices with a limited memory and computing power.

References

1. Weiman, G. Cyberterrorism How Real Is the Threat? United States Institute of Peace Special Report 2004, 119, 1-12. Available online: https://www.usip.org/sites/default/files/sr119.pdf. (accessed on 30 November 2017).
2. Wade, M.; Maljevic, A. A war on terrorism? The European stance on a new threat, changing laws and human rights implications. Springer, 2010, 51-78.
3. Ashmore, W. C. Impact of Alleged Russian Cyber Attacks. School of Advanced Military Studies, USA, 2009.
4. Symantec. Preparing of a Cyber Attack, 2013. Available online: http://symc.ly/1PHHl3n (accessed on 02 December 2017).
5. Kearney, A. T. GmbH. Information Security: Preparing for the Next Hack Attack, 2013. Available online: http://bit.ly/2vtIwkM (accessed on 30 11 2017).
6. Yadav, T.; Rao, A. M. Technical Aspects of Cyber Kill Chain. Proc. of Security in Computing and Communications: Third International Symposium on Security in Computing and Communication, Kochi, India, 2015, 438-452. doi: 10.1007/978-3-319-22915-7_40.
7. Husak, M. Early detection and mitigation of multi-stage network attacks. PhD thesis, Masarykova Univerzita Fakulta Informatiky, Brno, Czech, 2015.
8. Morinaga, M.; Nomura, Y.; Furukawa, K.; Temma, S. Cyber Attack Countermeasure Technologies Using Analysis of Communication and Logs in Internal Network. Fujitsu Scientific and Technical Journal, 2016, 52- 3, 66-71.
9. Siddique, K.; Akhtar Z.; Lee H.; Kim W.; Kim Y. Toward Bulk Synchronous Parallel-Based Machine Learning Techniques for Anomaly Detection in High-Speed Big Data Networks. Symmetry. 2017, 9(9), 197; doi:10.3390/sym9090197.
10. Yan, X.; Zhang, J. Y. Early Detection of Cyber Security Threats using Structured Behavior Modeling. ACM Transactions on Information and System Security. 2013. Available online: http://www.cs.cmu.edu/~xiaohuay/papers/draft_TISSEC.pdf (accessed on 05 January 2017).
11. Vincent, H.; Wells, L.; Tarazaga, P.; Camelio, J. Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems. Procedia Manufacturing. 2015. 1, 77-85, doi: 10.1016/j.promfg.2015.09.065.
12. Chen, M. C.; Yang, P. Y.; Ou, Y. H.; Hsiao, H. W. Targeted Attack Prevention at Early Stage. Proc. 28th International Conference on Advanced Information Networking and Applications Workshops. 2014, Victoria, BC, Canada, 866-870. doi: 10.1109/WAINA.2014.134.

13. Bhattacharya, S., Selvakumar, S. (2016) Multi-Measure Multi-Weight Ranking Approach for the Identification of the Network Features for the Detection of DoS and Probe Attacks. The Computer Journal, 59 (6), 923–943.
14. Cheng, J., Zhou, J., Liu, Q., Tang, X., Guo Y. (2018) A DDoS Detection Method for Socially Aware Networking Based on Forecasting Fusion Feature Sequence. The Computer Journal, 61 (7), 959–970.
15. Xu, X.; Sun, Y.; Huang, Z. Defending DDoS Attacks Using Hidden Markov Models and Cooperative Reinforcement Learning. Proc. Pacific Asia conference on Intelligence and security informatics. 2007. Chengdu, China, 196-207. doi: 10.1007/978-3-540-71549-8_17.
16. Abaid, Z.; Sarkar, D.; Kaafar, M. A.; Jha S. The Early Bird Gets the Botnet: A Markov Chain Based Early Warning System for Botnet Attacks. Proc. 41st Conference on Local Computer Networks (LCN). 2016. Dubai, United Arab Emirates, 61-68. doi: 10.1109/LCN.2016.17.
17. Li, X. Detection on Hidden Markov Model and Intention Prediction Techniques. Journal of Chemical and Pharmaceutical Research. 2016. 8-6, 433-437.
18. Rashid, T.; Agrafiotis, I.; Nurse, J. R. C. A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models. Proc. 8th ACM CCS International Workshop on Managing Insider Security Threats. 2016. Vienna, Austria, 47-56. doi: 10.1145/2995959.2995964.
19. Sharifi, A. A.; Noorollahi, B. A.; Farokhmanesh, F. Intrusion Detection and Prevention Systems (IDPS) and Security Issues. International Journal of Computer Science and Network Security. 2014. 14-11, 80-84.
20. Strasburg, C. R; Stakhanova, N.; Basu, S.; Wong, J. S. The Methodology for Evaluating Response Cost for Intrusion Response Systems. Iowa State University. 2008. Available online: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1204&context=cs_techreports (accessed on 20 March 2018).
21. Inayat, Z.; Gani, A.; Anuar, N. B.; Khan, M. K.; Anwar, S. Intrusion response systems: Foundations, design, and challenges. Journal of Network and Computer Applications. 2016. 62-C, 53-74, doi: 10.1016/j.jnca.2015.12.006.
22. Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions. Algorithms. 2017. 10-39, 1-24, doi:10.3390/a10020039.
23. Houmansadr, A.; Zonouz, S.A.; Berthier, R. A Cloud-based Intrusion Detection and Response System for Mobile Phones. Proc. 41st International Conference on Dependable Systems and Networks Workshops (DSN-W). 2011. Hong Kong, China, 31-32. doi: 10.1109/DSNW.2011.5958860.

24. Gbolahan, I. A.; Enikoumehinand, O.; Olasanoye, S. Intrusion Response Systems: An Overview. Asian Journal of Information Technology. 2011. 10-5, 192-200, doi: 10.3923/ajit.2011.192.200.
25. Lo, C.H.; Ansari, N. Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid. IEEE Transactions on Emerging Topics in Computing. 2013. 1-1, 33-44. Available online: https://doi.org/10.1109/TETC.2013.2274043 (accessed on: 22 February 2018).
26. Karim, I., Vien, Q.-T., Le, T. A. and Mapp, G. (2017) A comparative experimental design and performance analysis of Snort-based Intrusion Detection System in practical computer networks. Computers, 6 (1), 1-15.
27. Shen Y., Zheng K., Wu C., Zhang M., Niu X., Yang Y. (2018) An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection. The Computer Journal, 61 (4), 526–538.
28. SANS Institute InfoSec Reading Room. (2002) IDS - Today and Tomorrow. Available online: https://www.sans.org/reading-room/whitepapers/detection/ids-today-tomorrow-351, accessed on 22 February 2018.
29. Rathore, M.M., Ahmad, A., Paul, A. (2016) Real time intrusion detection system for ultra-high-speed big data environments. J Supercomput, 72, 3489-3510.
30. Al-Yaseen W. L., Othman A. L., M. Z. A. (2017) Real-time multi-agent system for an adaptive intrusion detection system. Pattern Recognition Letters, 85, 56–64.
31. Rajan, S. S.; Cherukuri, V. K. An Overview of Intrusion Detection Systems (Presented Conference Paper style). Proc. IDT Workshop on Interesting Results in Computer Science and Engineering (IRCSE). 2009. 18, 1-8.
32. Cho, S. M. Intrusion detection systems vs. Intrusion Prevention Systems (Report style). Technical Report ACC. 2010. 626.
33. Kashyap, S.; Agrawal, P.; Pandey, V. C.; Keshri, S. P. Importance of Intrusion Detection System with its Different approaches. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2013. 2- 5, 1902-1908.
34. Werlinger, R.; Hawkey, K.; Muldner, K.; Jaferian, P.; Beznosov, K. The Challenges of Using an Intrusion Detection System: Is It Worth the Effort? Proc. of ACM Symposium on Usable Privacy and Security (SOUPS). 2008. 107-118. Available online: https://doi.org/10.1145/1408664.1408679 (accessed on 15 January 2018).
35. Singh, K.; Tamrakar, S. A Review of Intrusion-Detection System- Clustering and classification using RBF and SOM Networks. International Journal of Emerging Technology and Advanced Engineering. 2015. 5- 7, 502-505.

36. Chi, Y., Jiang, T., Li, X., Gao C. (2017) Design and Implementation of Cloud Platform Intrusion Prevention System based on SDN. Proc. 2nd IEEE International Conference on Big Data Analysis (ICBDA), Beijing, Peoples R China, March 10-12, pp. 847-852, IEEE.
37. Xing, T.; Huang, D.; Xiong, Z.; Medhi, D. SDNIPS: Enabling Software-Defined Networking based intrusion prevention system in clouds. Proc. of International Conference on Network and Service Management (CNSM). 2014. 308-311. Available online: https://doi.org/10.1109/CNSM.2014.7014181 (accessed on 11 February 2018).
38. Ragsdale, D. J.; Carver, C. A.; Humphries, J. W.; Pooch, U. W. Adaptation techniques for intrusion detection and intrusion response systems. Proc. of the IEEE International Conference on Systems, Man, and Cybernetics. 2000. 2344–2349.
39. Shameli-Sendi, A.; Cheriet, M.; Hamou-Lhadj, A. Taxonomy of intrusion risk assessment and response system. Computers and Security. 2014. 45, 1–16. Available online: https://doi.org/10.1016/j.cose.2014.04.009 (accessed on: 25 February 2018).
40. Moon, D.; Im, H.; Lee, J. D.; Park, J. H. MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats. Symmetry. 2014. 6-4, 997-1010. doi:10.3390/sym6040997.
41. Heo, S.; Lee, S.; Doo, S.; Yoon, H. Design of a Secure System Considering Quality of Service. Symmetry. 2014, 6-4, 938-953. doi:10.3390/sym6040938.

LIST OF PUBLICATIONS ON THE THEME OF THE DISSERTATION

Articles in journals from the list of Institute of Scientific Information (ISI) Web os Science database

1. Japertas, S.; Bakšys, T. „Method of Early Staged Cyber Attacks Detection in IT and Telecommunication Networks.“ *Elektronika ir Elektrotechnika,* ISSN:1392-1215. **2016**. Kaunas, Lithuania;
2. Jusas, V., Japertas, S., Bakšys T. “Logical Filter Approach for Early Staged Cyber Attack Detection”. *„Computer Science and Information Systems“,* ISSN: 1820-0214. **2019**. Serbia. (In proceedings).

Articles in conference proceedings

1. European Commision organized Eastern Partnership Electronic Communications Regulators Network (EaPeReg) conference on Network and Information Security. “*Early Staged Cyber Incidents Identification”*. 2015. Vilnius, Lithuania;
2. NATO Energy Security Center of Excellence conference “Critical Energy Infrastructure Protection (CEIP) 2016”. *“Early Staged Cyber Incidents Identification”*. 2016. Vilnius, Lithuania;
3. First international conference 2018 “Challenges to National Defence in Contemporary Geopolitical Situation” (CNDCGS-2018). *“High Efficiency Logical Filters Approach in Early-staged Cyber Attacks Detection”.* 2018. Vilnius, Lithuania;
4. The 22nd International Conference ELECTRONICS 2018. *“Method of Early Staged Cyber Attacks Detection in IT and Telecommunication Networks”*. 2018. Palanga, Lithuania.

ANKSTYVŲJŲ STADIJŲ KIBERNETINIŲ ATAKŲ KOMPIUTERIŲ IR TELEKOMUNIKACIJŲ TINKLUOSE APTIKIMO METODAS

REZIUMĖ

Didelis informacijos skaitmeninimas kartu su nauda sukėlė daug problemų, susijusių su uždaviniais kibernetinėje erdvėje. Dėl nuolatinio kibernetinių atakų didėjimo, nuostoliai telekomunikacijų ir IT paslaugų sektoriuose auga. CERT ir kibernetinius incidentus tiriančių institucijų ataskaitos parodė, kad per pastaruosius dešimt metų situacija kibernetinėje erdvėje itin paaštrėjo – pagausėjo pavojingų atakų, kurios yra iš anksto suplanuotos, gerai parengtos ir vykdomos teroristinių grupių kurias kontroliuoja vyriausybė. Iš anksto suplanuotos kibernetinės atakos pasižymi tam tikrais etapais ir fazėmis, kurios leidžia atakas atpažinti ankstyvose stadijose, kai jų poveikis nesukelia didelės žalos duomenims ar informacijai.

Intelektualios kibernetinės atakos sukelia didžiausią žalą informacinėse ir telekomunikacijų sistemose.

Tokie išpuoliai gali užtrukti ilgai, reikalauti didelių finansinių ir žmogiškųjų išteklių, todėl juos gali organizuoti tik didelės interesų grupės. Be to, dabartinės įsilaužimo aptikimo sistemos, įsilaužimo prevencijos sistemos ir įsilaužimo atsako sistemos, naudojamos apsaugoti nuo kibernetinių išpuolių, turi keletą trūkumų.

Esamos kibernetinių atakų detekcijos sistemos ir metodai identifikuoja tik vykstančią ar jau įvykusią ataką, kai jau yra per vėlu imtis prevencinių veiksmų. Naujausi moksliniai šaltiniai kibernetinio saugumo tema tegia, kad itin svarbu nustatyti ataką ankstyvosiose stadijose, kai galima atlikti jos užkardymą ir sumažinti potencialius nuostolius. Ankstyva atakų detekcija įmanoma tik atliekant išsamią tinklo ir sistemos parametrų stebėseną, to pasekoje tiksliai nustatant ankstyvą atakos stadiją ir nutraukiant atakos grandį.

Šiame darbe nagrinėjami kibernetinių atakų bruožai ir charakteristikos, leidžiančios išskirti ankstyvąsias atakų stadijas. Ankstyvųjų atakų bruožų detekcija vykdoma panaudojant loginius indikacinius filtrus, kurie išskiria tinklo ir sistemos charakteristikas ir nustato galimas anomalijas. Šios anomalijos formuoja veiksnius, iš kurių susideda kibernetinės atakos. Metodui indikavus galimas sistemos anomalijas, srautas toliau analizuojamas, informacija apdorojama loginiais grandynais, gaunami binariniai vektoriai, charakterizuojantys atakas.

Darbe pasiūlyta tinklo analizės struktūra, loginio filtro konfigūracija ir atakos detekcijos algoritmai, leidžiantys iš tinklo srauto ir sistemos parametrų nustatyti galimus ankstyvųjų stadijų atakų vektorius.

Siūlomas metodas nereikalauja daug skaičiavimo išteklių, todėl jį taip pat galima įdiegti mobiliuosiuose įrenginiuose.

Tyrimo objektas

Disertacijos tyrimų objektas yra intelektualiųjų kibernetinių atakų detekcijos metodai, leidžiantys iš kompleksinio IT sistemų ir telekomunikacinio tinklo elgsenos trakto išskirti ankstyvuosius kibernetinių atakų bruožus ir specifines jų charakteristikas, užtikrinant kibernetinių atakų detekciją ankstyvose (1 – 3) stadijose.

Darbo aktualumas

Pažangios kibernetinės atakos labiausiai kenkia informacinėms ir telekomunikacijų sistemoms. Tokie išpuoliai gali užtrukti labai ilgai, reikalauti didelių finansinių ir žmogiškųjų išteklių, todėl juos gali organizuoti tik didelės interesų grupės. Be to, dabartinės įsibrovimo aptikimo sistemos, įsibrovimo prevencijos sistemos ir įsibrovimo atsako sistemos, naudojamos apsaugoti nuo kibernetinių atakų, turi tam tikrų trūkumų. Tokios sistemos reaguoja tik į pačią ataką, kai per vėlu imtis prevencinių veiksmų ir jie netinka aptikti ataką ankstyvosiose stadijose, kai galima užblokuoti ataką ir sumažinti nuostolius. Ankstyvas aptikimas reikalauja išsamaus tinklo ir sistemos parametrų stebėjimo, kad būtų galima tiksliai nustatyti ankstyvus atakos etapus, kai vis dar įmanoma „sustabdyti atakos grandinę“. Siūlomas ankstyvas kibernetinės atakos aptikimo metodas, pagrįstas atakos vektoriaus analize, naudojant loginę filtravimo sistemą. Šis metodas reikalauja ribotų skaičiavimo išteklių, todėl jis taip pat gali būti tinkamas vykdyti ankstyvųjų kibernetinių atakų prevenciją mobiliose sistemose.

Darbo tikslas ir uždaviniai

Šio darbo tikslas yra sukurti ir ištirti metodą, kuris įgalintų ankstyvųjų stadijų kibernetinių atakų aptikimą remiantis parametrinių loginių filtrų analize, ankstyvuosius atakų bruožus nustatant iš atakas formuojančių kompleksinių faktorių, išskirtų iš sukauptų tinklo srauto ir sistemų veiklos duomenų.

Darbe numatyta išspręsti šiuos uždavinius:

1. Atlikti atakų pagrindinių etapų ir detekcijos metodų analizę;
2. Atlikti tinklo ir sistemos stebėsenos duomenų analizę, indikuojant parametrus bei dėsningumus, įgalinančius ankstyvąją detekciją;
3. Sukurti sistemą ir algoritmus, gebančius išskirti reikalingus detekcijai bruožus stebėsenos duomenų srautuose;
4. Sukurti metodą, kuris naudodamas ankščiau iškirtus parametrų rinkinius įgalins detektuoti atakas galimai ankstesniais momentais;
5. Eksperimentiškai patikrinti sukurtą sistemą atliekant stebėsenos duomenų kaupimą, ankstyvųjų bruožų detekciją ir atakos nustatymą ankstyvojoje stadijoje.

Mokslinė hipotezė
Remiantis surinktomis tinklo srauto ir sistemos registracijos žurnalų charakteristikomis ir atlikus šių duomenų apdorojimą parametriniais filtrais, kibernetines atakas galima aptikti ankstyvoje stadijoje prieš joms sukeliant neatstatomą žalą.

Mokslinis naujumas
Atlikus teorinius ir eksperimentinius tyrimus buvo gauti šie elektros ir elektornikos inžinerijos mokslui nauji rezultatai:

1. Išskirti kibernetinių atakų vektoriaus bruožai, būdingi ankstyvosioms stadijoms (1 – 3 stad.), kuriais remiantis galima aptikti atakas ankstesniais momentais.
2. Parengta metodika, įgalinanti remiantis sistemos elgsenos ir tinklo trakto parametrais iš intelektualių kibernetinių atakų vektoriaus išskirti ankstyvąsias kibernetinių atakų stadijas.
3. Sudarytas ir teoriniais bei praktiniais tyrimais įvertintas modelis, įgalinantis atakas aptikti ankstyvaisais momentais realiomis sąlygomis.

Praktinė vertė
Rengiant disertaciją gauti šie praktiniai rezultatai:

1. Sudaryti atakų scenarijai, nustatyti ankstyvieji atakų bruožai ir charakteristikos, parengti metodai jų detekcijai, katalizuojami analizės procesai, atlikta programinė metodų realizacija;
2. Iš kibernetinių atakų vektoriaus išskirti ankstyvųjų atakų stadijų bruožai kibernetinių atakų detekcijai leidžia aptikti atakas anstyvaisiais momentais ir sumažinti jų kuriamą žalą;
3. Suprojektuota praktinio pobūdžio sistema leidžia pasiūlytą modelį taikyti praktinėje terpėje.

Dalyvavimas moksliniuose projektuose

1. Lietuvos mokslo taryba. Reikminių tyrimų projektas Nr. REP-15115, tema „Ankstyvoji kibernetinių incidentų identifikacija kritinėse infrastruktūrose“.
2. Lietuvos verslo paramos agentūra. Kompleksinė ankstyvųjų stadijų kibernetinių atakų prevencijos sistema Nr. J05-LVPA-K-01-0286.

Ginamieji teiginiai

1. Išskiriant kibernetinių vektorių sudarančius bruožus yra galimybė nustatyti atakas ankstesniais momentais;
2. Panaudojant loginių filtrų sistemą, galima nustatyti kibernetines atakas ankstesniais momentais;

3. Loginių filtrų sistemą galima taikyti analizuojant sisteminius ir tinklo trakto parametrus.

Disertacijos struktūra

Disertaciją sudaro įvadas, 4 skyriai, bendrosios išvados, šaltinių ir literatūros sąrašas, autoriaus mokslinių publikacijų diserатacijos tema sąrašas ir santrauka anglų kalba. Disertacijos apimtis – 108 puslapiai. Disertacijoje yra 49 paveikslai, 29 lentelės ir 17 numeruotų formulių, disertacijoje panaudotas 91 literatūros šaltinis.

UDK 004.056 (043.3)

SL344. 2019-06-17, 2,5 leidyb. apsk. l. Tiražas 50 egz.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas