
**Nerijus PAULAUSKAS**

# ANALYSIS OF COMPUTER SYSTEM INCIDENTS AND SECURITY LEVEL EVALUATION

**Summary of Doctoral Dissertation**
**Technological Sciences,**
**Electrical and Electronic Engineering (01T)**

**1617-M**

**Vilnius** VGTU LEIDYKLA TECHNIKA **2009**

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

**Nerijus PAULAUSKAS**

# ANALYSIS OF COMPUTER SYSTEM INCIDENTS AND SECURITY LEVEL EVALUATION

Summary of Doctoral Dissertation
Technological Sciences,
Electrical and Electronic Engineering (01T)

Vilnius LEIDYKLA TECHNIKA 2009

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2005–2009.
Scientific Supervisor
**Prof Dr Habil Julius SKUDUTIS** (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T).
**The dissertation is being defended at the Council of Scientific Field of Electrical and Electronic Engineering at Vilnius Gediminas Technical University:**
Chairman
**Prof Dr Habil Romanas MARTAVIČIUS** (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T).
Members:
**Prof Dr Habil Antanas ČENYS** (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),
**Assoc Prof Dr Šarūnas PAULIKAS** (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T),
**Assoc Prof Dr Rimantas PUPEIKIS** (Institute of Mathematics and Informatics, Physical Sciences, Informatics – 09P),
**Prof Dr Habil Stanislavas SAKALAUSKAS** (Vilnius University, Technological Sciences, Electrical and Electronic Engineering – 01T).
Opponents:
**Prof Dr Dalius NAVAKAUSKAS** (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T),
**Prof Dr Habil Rimantas ŠEINAUSKAS** (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Electrical and Electronic Engineering in the Senate Hall of Vilnius Gediminas Technical University at 1 p. m. on 2 June 2009.
Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4952, +370 5 274 4956; fax +370 5 270 0112;
e-mail: doktor@adm.vgtu.lt
The summary of the doctoral dissertation was distributed on 30 April 2009.
A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania).

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

**Nerijus PAULAUSKAS**

# INCIDENTŲ KOMPIUTERIŲ SISTEMOSE TYRIMAS IR SAUGUMO LYGIO ĮVERTINIMAS

Daktaro disertacijos santrauka
Technologijos mokslai,
elektros ir elektronikos inžinerija (01T)

Vilnius LEIDYKLA TECHNIKA 2009

Disertacija rengta 2005–2009 metais Vilniaus Gedimino technikos universitete.
Mokslinis vadovas
**prof. habil. dr. Julius SKUDUTIS** (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).
**Disertacija ginama Vilniaus Gedimino technikos universiteto Elektros ir elektronikos inžinerijos mokslo krypties taryboje:**
Pirmininkas
**prof. habil. dr. Romanas MARTAVIČIUS** (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).
Nariai:
**prof. habil. dr. Antanas ČENYS** (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),
**doc. dr. Šarūnas PAULIKAS** (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),
**doc. dr. Rimantas PUPEIKIS** (Matematikos ir informatikos institutas, fiziniai mokslai, informatika – 09P),
**prof. habil. dr. Stanislavas SAKALAUSKAS** (Vilniaus universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).
Oponentai:
**prof. dr. Dalius NAVAKAUSKAS** (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),
**prof. habil. dr. Rimantas ŠEINAUSKAS** (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija bus ginama viešame Elektros ir elektronikos inžinerijos mokslo krypties tarybos posėdyje 2009 m. birželio 2 d. 13 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.
Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4952, (8 5) 274 4956; faksas (8 5) 270 0112;
el. paštas doktor@adm.vgtu.lt
Disertacijos santrauka išsiuntinėta 2009 m. balandžio 30 d.
Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva).
VGTU leidyklos „Technika“ 1617-M mokslo literatūros knyga.

## Introduction

***Topicality of the problem***

The importance of information systems survivability and information availability in computer networks as well as the ever-increasing dependence of activity of various organizations on the computer systems providing services had a major influence on the increase in the computer intrusions and their complexity.

After the Internet having become the space of financial operations, the aims of attackers also change. If earlier the main aim of attackers was to become famous, to try one's abilities or to do harm in some other way, at present the financial gain becomes their main objective. Attackers more frequently overcome protection systems installed in banks or companies intended to restrict the access to the computer network resources of the organization.

General purpose applied programs, the security of which is not always ensured, vulnerabilities allowing realization of security threats are constantly detected. Moreover, during operation of computer systems their functions and the composition of the applied programs constantly change. Therefore, the information security insurance is not a single action but a constant process.

The appearance of attack and the system response to it are random variables, therefore in order to determine the impact of attackers on the computer system, the probabilistic models should be used.

For the evaluation of the computer system security and its increase, it is necessary to know the ways of impact on this system, their typical features and the possible influence on the system. The stochastic assumptions are irreplaceable when modeling and simulating systems which are not implemented yet or evaluating possible vulnerabilities which are not discovered yet. Stochastic values should be used to describe the vulnerability occurrence and discovery, the attacker's behavior and system response.

Seeking to reduce the risk and possible consequences it is very important to identify the intrusions at the initial stage of their realization and to react to them properly. For this purpose the intrusion detection system (IDS) can be applied. The performance of IDS strongly depends on its configuration for the particular computer system. The intrusion detection system effectively detects known attacks, but it generates a large number of false positive about attacks and it cannot detect new, not known yet attacks. Therefore, it is necessary to improve the available methods of the intrusion detection and to develop new methods.

***Research object***

- the incidents of computer networks;
- impact of incidents on the computer systems;
- intrusion detection systems;
- network scanning types.

***The aim of the work***

The aim of the dissertation is the investigation of the intrusions in the computer network and evaluation of the computer system security level.

***Tasks of the work***

To achieve the aim of the work these tasks have to be solved:

1. To classify the attacks according to their main features and to suggest the numerical evaluation of the attack severity level based on the impact on the computer system.
2. To develop the methodology of quantitative evaluation of the computer system security level according to the system vulnerabilities and the attacker's skill level.
3. To investigate the dependence of the computer system performance and availability on the attacks affecting the system and defense mechanisms used in it.
4. To develop the model simulating the computer network horizontal (hosts) and vertical (ports) scanning and to determine the influence of the method applied to the computer network scanning detection on the scanning detection efficiency.
5. To investigate the dependence of the system *Snort 2.8.0* performance on the chosen hardware.

***Applied methods***

In the work for the computer system security evaluation the probabilistic and statistical analysis techniques were used. Stochastic activity networks (SANs) were used for describing the system random behavior. SAN models were created by the stochastic activity network modeling tool *Möbius*. The intrusion detection system *Snort* has been used for the incident analysis in the computer networks.

***Scientific novelty***

The scientific novelty of this dissertation is the following:

1. Computer attacks were classified and the numerical evaluation of the attack severity level was suggested.

2. The distribution of the attacker‘s skill level was introduced in the computer system security evaluation by the Mean Time-to-Compromise criterion.
3. New stochastic activity network models for the computer system performance, availability of provided services and network scanning techniques investigation were developed.
4. The dependence of the system *Snort 2.8.0* efficiency on the chosen hardware by analyzing different speed network traffic has been investigated.

***Practical value***

The created computer network scanning model allows evaluation of the influence of simulated computer system parameters on the scan detection efficiency.

The suggested model of the computer system performance and availability simulation could be used to investigate the performance and availability of the real systems and forecast the necessity to increase the quality of systems defense mechanisms.

The improved methodology of the computer system security evaluation, by using Mean time-to-Compromise criterion, additionally allows evaluating the attacker’s skill level distribution when various security environments and solutions of computer systems are compared.

The suggested computer attack classification and attack severity numerical evaluation could be used for the incidents analysis and investigation.

***Defended propositions***

1. According to suggested original computer attack classification, is rational to evaluate the attack severity by five numerical levels.
2. The probabilistic distribution should be used for the Mean Time-to-Compromise evaluation in the attacker skill level group instead of top attacker’s skill level values.
3. To evaluate the impact of attacks on the computer system, to investigate the scan detection efficiency and to find intrusion detection system correct configuration parameters values, is rational to use stochastic activity networks.
4. Based on the experimental results of the intrusion detection system *Snort 2.8.0* efficiency investigations, the reasonable hardware can be chosen for the particular load network for the *Snort* system implementation, and the system can be configured properly.

***The scope of the scientific work***

The dissertation is written in Lithuanian. The total scope of the dissertation is 136 pages. The work contains 25 mathematical expressions, 39 figures and 6 tables, cites 117 references. The thesis consists of introduction, five chapters, general conclusions and one appendix.

## 1. Analytical Survey of Computer System Incidents Detection Methods and Security Level Evaluation Methods

Chapter 1 covers the analysis of existing publications related to the problems of the thesis. The survey of technologies of the intrusion detection and intrusion prevention systems is presented and methods of the intrusion detection are analyzed. The currently existing techniques of the attack classification are considered. Much attention is paid to the methods of the computer system security level evaluation, computer network scanning techniques and scanning detection methods. At the end of the chapter conclusions are drawn and tasks of the thesis are formulated.

## 2. Investigation of Computer System Incidents

The currently available computer system attack classifications are intended for a certain purpose or for some aspect of the attack. Very often not full information is known about the attack, thus it is very useful when all features of the attack are described. Thus, only having a wide classification we can combine different statistical data.

The composed computer system attack classification is based on the known attack classification analysis and includes all attack specific features and is suitable for experimental data analysis and assessment.

Computer system attacks are classified according to:

1. the attack objective;
2. the effect type;
3. the ISO/OSI model level;
4. the type of the operating system;
5. the location of the attack subject;
6. the type of the object location;
7. the service attacked;
8. the attack concentration;
9. the feedback;
10. the attack execution initial conditions;
11. the impact type;
12. the attack automation;
13. the attack source;
14. the connection quantity.

The objective achievement is most important for the attacker, therefore, it is advisable to compare all the attack classification items with it. The total computer system control is usually the final objective of the intruders. The effect type most depends on the intruder's objective as well as the subject and object location. The ISO/OSI model can characterize all computer system processes. The application level is most suitable because of its potentiality and complexity to perform attacks. There is a variety of operating systems OS in the global network, specific OS families have common vulnerabilities which attract OS specific attacks. Location of the attack subject affects the effect type and the probability of attack object achievements. Attack technology and possible threats are affected by the type of the object location and attacked service. The attack can be concentrated in one packet or can be fragmented to several packets. Feedback is not necessary for all attacks. In order to avoid detection or for better efficiency on the system attackers can choose different initial execution conditions, the impact type or automation level. According to the attack objective and the effect type the number of attack sources and connection quantity may differ.

The suggested attack classification is open for expansion. New effect types, operating systems, object locations and services are most possible.

The computer system security modeling needs a numerical attack severity evaluation. It is shown that it is rational to use the 5 levels attack severity numerical evaluation based on the attack objective.

The security incident statistical data were collected in the public institution, home network and academic organization. Data were analyzed, classified and compared. After the security incident statistical analysis it was found that the number of most severe incidents is the least. Threats to confidentiality and availability are targeted most; security policy enforcement and management require special attention.

## 3. Evaluation of Computer System Security Level

The computer system security is usually evaluated using qualitative criteria and later the recommendations for the successful attack outcome possibility decrease are provided.

The computer system security can be evaluated using Mean Time-to-Compromise (MTTC) criterion. Mean Time-to-Compromise is the amount of time needed for an attacker with a certain skill level to compromise the computer system. The success of the attack depends on the attacker's skill level. A target network or device must be capable of surviving an attack for some minimally acceptable time period (MTTC). As the time-to-compromise is

increased, the likelihood of successful attack, and therefore risk, tends to decrease.

Most attackers will use a limited set of tools based on their experience and knowledge, therefore the attackers can be divided into groups according to readily available exploits, knowledge and skills, i.e. beginner, intermediate and expert. Beginners are only capable of using existing code, tools, and attacks to exploit known vulnerabilities, intermediate attackers are able to modify the exploit code and exploit known vulnerabilities. The experts' skill level is the highest. They can create new exploits and find and exploit new vulnerabilities.

The attacker skills in MTTC evaluation are usually considered to be the top value of the skills group, but the skill level of an individual attacker in the group is different. It is suggested using the attacker skill values from the attacker group interval, where attacker's skills are distributed normally. As the attackers skills are distributed according to the normal distribution law, the time needed to compromise the system will be distributed according to the same law.

In order to define normal distribution every group MTTC mean and variance values must be calculated. For this purpose the MTTC value of every group using top values is calculated. Further we assume that MTTC of every attacker group equals the interval mean value with 0.8 probability and interval end values with 0.1, respectively. Under these assumptions the mean and variance describing normal distribution are calculated.

In order to evaluate how the MTTC value depends on these assumptions, modeling tool *Möbius* using the Stochastic Activity Network (SAN) formalism was used and the SAN model was composed (Fig. 1).

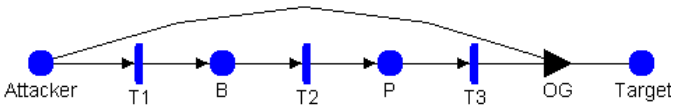



**Fig. 1.** MTTC stochastic activity network model

Circles represent states, arrows – transitions, and rectangles represent transition activities with different time distributions. In the model states represent the attack path to the target. Transition from one state to another means the compromise of some component of the system. In this case transition from state *Attacker* to state *B* (*breach*) corresponds to compromise of computer 1 from the Internet by overcoming the perimeter protection device (e.g., firewall). Transition from state *B* to state *P* (*penetration*) corresponds to compromise of computer 2 directly from computer 1, i.e. when computers are not separated by the perimeter protection device. Transition from state *P* to state

*Target* corresponds to penetration of the target computer. The computer system is affected by one attacker at a time; this is assured by output gate (*OG*). Activities (*T1*, *T2* and *T3*) represent transition time from one attack stage to another.

The results of a small hypothetical organization computer network modeling show that the MTTC value increases when the attacker skill level interval is used. The largest change in the MTTC value is when the attacker is a beginner, because the beginner's skill level interval is the widest.

## 4. Modeling of Computer System Performance, Availability and Network Scanning

### 4.1. Modeling of Computer System Performance and Availability

The appearance of attack and the system response to it are random variables, therefore in order to determine the impact of attackers on the computer system stochastic models should be used. For this purpose the computer system stochastic activity network model was developed. The model allows evaluation of the dependence of the system performance and availability, one of the system security components, on the rate of attacks affecting the system and the defense mechanisms used in the system.

The modeled computer system is composed of the following components: the client, firewall and the server. The client is a program, such as a web browser, that establishes connections to the service system in order to process user requests. The firewall monitors incoming requests and filters known attacks. The server processes the incoming client requests.

Two measures were defined in the study:

*System performance* is the measure which characterizes the number of requests that the server replies to correctly per time unit. The server replies correctly to the requests if it is not compromised. The mean value of this measure in a time interval was determined.

*System unavailability* is the measure which characterizes the fraction of time the service is improper or service is offline in the given time interval, i.e. server is in a corruption undetected state or server is offline for repair.

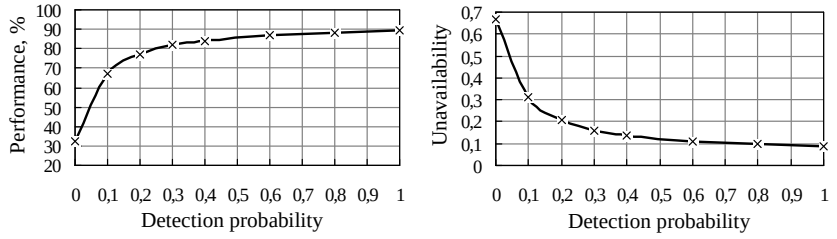
In the modeled system the following input parameters were varied: the quality of the detection mechanism being used, the attack rate, the probability of the attack success and the rate at which the server is repaired.

The quality of detection is the probability with which an intrusion detection system can ascertain that a system has been compromised. To determine the effect of the probability of detection on the performance and

availability of the system, the detection probability from 0.0 (no intrusion detection) to 1.0 (perfect intrusion detection) was varied.

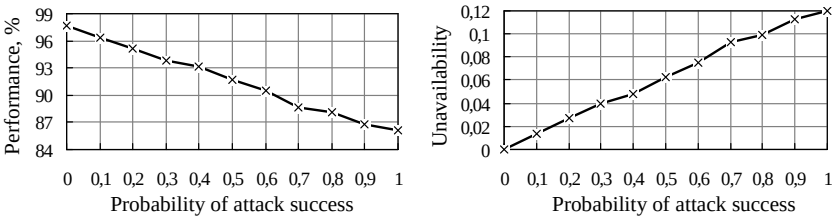
As we can see in Figure 2, in the absence of an intrusion detection mechanism the server performance and unavailability depend primarily on the system defense against intrusion attempts. When the probability of detection increases the server unavailability decreases and the server becomes more available. The performance also increases. A trend that is observed in Figure 2 shows that beyond a certain detection probability (approximately 0.3) the performance does not show an appreciable increase because the performance depends primarily on the system total service capacity and the query arrival rate which were kept constant in the model.

Figure 3 shows the effect of varying the probability of attack success on the performance and unavailability of the server. The probability of attack success is the probability that firewall will not stop the attack and this attack will compromise the server. The probability of attack success was varied from 0 to 1 when the rate of attack was constant and equal to 0.2 (12 attacks per hour).




(a) Performance (b) Unavailability

**Fig. 2.** Dependences of the system performance and unavailability on the detection probability




(a) Performance (b) Unavailability

**Fig. 3.** Dependences of the system performance and unavailability on the probability of attack success

As we can see in Figure 3, the performance and availability of the server directly depend on the probability of attack success. When the probability of attack success increases the server performance decreases. The system performance can be increased by decreasing the probability of attack success. This can be done by increasing the quality of defense mechanisms used in the server.

### 4.2. Modeling of Computer Network Scanning

The port scanning is most often related to the malicious activity trying to detect the target network vulnerabilities and to use them by causing a major damage. Therefore, there appears a demand to create effective scan detection methods allowing determination of sources of a possible attack and to prevent the attacker from further network scanning.

The model for simulation of different network scanning types (horizontal and vertical) is proposed. The developed model allows evaluation of the influence of simulated computer system parameters on the scan detection efficiency and proper configuration of the intrusion detection system.

The simulated computer system is described by the set of server destination addresses and open ports. The computer system model consists of the packet generator and the scanning detection system. In the packet generator output the packet sequence is obtained, part of which consists of scanning packets. The scanning detection system is connected so that the whole network packet flow can be monitored. It determines the number of unique scanners $C_{\text{scanner}}$ and the number of scanning $C_{\text{scan}}$ cases. The model was created using Stochastic Activity Networks and its modeling tool *Möbius*.

The horizontal and vertical scan of a small business hypothetical company network was modeled. Computer system has 14 routable IP addresses (192.168.0.0/28) and four servers: web, email, domain controller and database. Authorized users using the services provided by the servers access not to all open system ports, but only to part of them, thus in the model the number of authorized access ports is lower than the number of all open ports in the system. The number of scanners is lower than that of authorized system users. For the malicious scanner of the supposed victim the network not all hosts are interesting, but only a particular network or a subnet and not all possible ports, but only the most frequently used ones and those used by vulnerable services.

The model was calibrated and effective intervals of the detection parameters were detected. Dependences of the number of horizontal and vertical scans and the number of malicious scanners on the threshold value,

scanning packet appearance probability and detector counters reset interval were obtained.

Dependences of the number of horizontal scans $C_{\text{hscan}}$ and the number of malicious scanners $C_{\text{scanners}}$ on the threshold value $W_{\text{h}}$ are presented in Figure 4. When the threshold value is equal to 2 (it means that all IP addresses from which two or more network hosts were accessed are detected), the number of scans and scanners is the highest. This is due to the fact that at this threshold value, good network users are mistaken for scanners and false positive detection occurs. A further increase of the threshold value lowers the number of scans and scanners and both curves reach the breaking point. The breaking point appears at the threshold value at which good network users are not recognized as scanners. Since the model foresees that good network users can connect only to the services providing computers, which in this case are 4, at the threshold value equal to 5 they are not recognized as scanners.

By adjusting the scan detector and seeking to reduce the number of false positives, the threshold value higher than the number of servers in the network should be chosen or the access to open ports of these servers should not be logged when detecting scans. It can be seen from Figure 4 that a further increase of the threshold value reduces the number of detected scans and scanners. The reason is that when the threshold value is too high the attempts of scanning are not detected. This is called false negative.

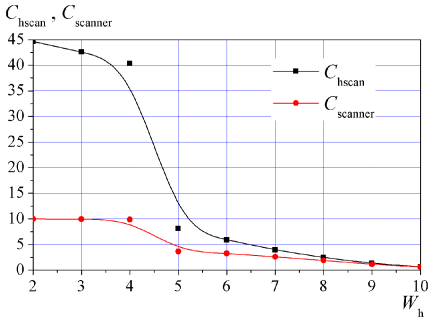



**Fig. 4.** Dependences of the number of horizontal scans $C_{\text{hscan}}$ and the number of malicious scanners $C_{\text{scanners}}$ on the threshold value $W_{\text{h}}$

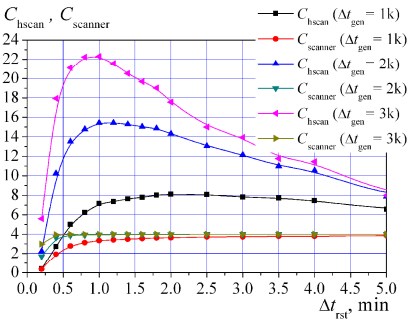



**Fig. 5.** Dependence of horizontal scans $C_{\text{hscan}}$ and scanners $C_{\text{scanners}}$ on detector counters reset interval $\Delta t_{\text{rst}}$

The dependence of horizontal scans $C_{\text{hscan}}$ and scanners $C_{\text{scanners}}$ on the detector counters reset interval $\Delta t_{\text{rst}}$ is presented in Figure 5. When the scan detector counters reset interval $\Delta t_{\text{rst}} < 0.5$ (counters are resetting more

frequently than half a minute) the number of detected scans and scanners is the lowest because of the model packet generation rate and scan detection threshold. Increasing the reset interval $\Delta t_{rst}$ makes the number of scans $C_{hscan}$ and scanners $C_{scanners}$ high. The number of scans $C_{hscan}$ increases further because the same scanner can scan more than once. As we can see in Figure 5, the number of scanners $C_{scanners}$ is the highest (in this case 4) when $\Delta t_{rst} = 4$ and the packet generation rate is $\Delta t_{gen} = 1000$ pckt/min. The scanners appearance time decreases when the packet generation rate increases. When $\Delta t_{gen} > 2000$ pckt/min the number of scanners reaches its highest value much earlier. Besides, it can be seen in Figure 5 that the number of scans $C_{hscan}$ in the interval $\Delta t_{rst} = [0.75–2]$ is the highest. Later the number of scans $C_{hscan}$ decreases when the reset interval $\Delta t_{rst}$ increases as the scan detection system upon the scanner detection does not detect other scans from the specific source until the counters are not cleared.

Therefore, we can draw a conclusion that in this computer network using the attack detection systems, in which one of the parameters used for the scan detection is the scan detection time window, it is recommended to determine the value of this parameter shorter than 2 minutes because in the range of this interval up to 90% of all scanners appear.

The model allows evaluating the impact of all modeled computer system parameters on the scan detection efficiency. The threshold value and the detector reset interval are the main parameters having influence on the efficiency of the scan detection.

## 5. Investigation of the Intrusion Detection System *Snort* Performance

By implementing the network intrusion detection system (IDS), one of the essential system parameters is the total IDS system performance. In this case, the system performance is understood as its capability to process all packets transmitted over the network. It is important to ensure that the intrusion detection system should process all packets transmitted over the network irrespective of the network usage, i.e. it is necessary to reduce the number of dropped packets to the minimum. Otherwise, part of intrusions can be skipped and important data capable of having influence on the investigation of incidents in computer networks can be unregistered.

The dependence of the *Snort 2.8.0* efficiency on the chosen hardware by analyzing different speed network traffic has been investigated experimentally.

During the investigation two computers interconnected by the twisted pair cable were used. One of the computers was intended to send the network traffic, while in the other computer the intrusion detection system *Snort 2.8.0* was

implemented. The aim was to investigate the performance of the network intrusion detection system *Snort 2.8.0,* its dependence on the hardware (CPU, RAM, NIC) and the chosen logging way of alerts: 1 – directly to MySQL, 2 – MySQL+*Barnyard 0.2.0*.

The investigation results of *Snort 2.8.0* implemented in the system with the *PentiumD* (3.2 GHz) processor and 2 GB RAM show that by sending network packets at a rate not higher than 50 Mbps, the system manages to process all packets transmitted over the network irrespective of the used network interface card (NIC). Differences appear when packets are transmitted at the rate higher than 50 Mbps. Better results are obtained by logging data in a second way (using *Barnyard 0.2.0* tool). In this case, the system detects almost all attacks and the number of dropped packets does not exceed 0.08%.

*Snort 2.8.0* system with the *PentiumIV* (1.8 GHz) processor and 256 MB RAM starts dropping packets much earlier, i.e. reaching the traffic transmission rate of 30 Mbps. The difference between the number of dropped packets using different network interface cards appears when the traffic is transmitted at the rate higher than 70 Mbps. Meanwhile, the difference of detected incidents using different network cards does not exceed 3.8% of the value in the investigated range of the traffic sending rate.

The investigation results of the intrusion detection system *Snort 2.8.0* with the *PentiumIII* processor show that when the traffic sending rate reaches 45 Mbps, the system drops more than 50% of all packets transmitted over the network. Even after changing the network interface cards and the pattern-matching algorithm, the results did not improve.

**General Conclusions**

The main results are the following:

1. Computer attacks were classified and the numerical evaluation of the attack severity level was suggested. It is shown that it is rational to use the 5 levels attack severity numerical evaluation based on the attack objective. The main advantage of the suggested classifications is its universality; it can be expanded and supplemented with new attacks, attributing them to a certain severity level.
2. The methodology of the computer system security level evaluation by applying the mean time-to-compromise criterion and evaluating the attacker skill level distribution was developed. The distribution of attacker‘s skill level was introduced in the computer system security level evaluation by the Mean Time-to-Compromise criterion. The probabilistic distribution should be used for Mean Time-to-Compromise evaluation in the attacker skill level group instead of top attacker’s skill level values.

3. The computer system stochastic activity network model intended for the investigation of the system performance and availability of provided services was created. The investigation results of the created model show that:
   3.1. At the beginning by increasing the quality of defense mechanisms the system performance and availability increase considerably, but later, after reaching the saturation point, the growth becomes slower. This shows that a sufficient system performance and availability can be obtained by using even standard additional system protection mechanisms.
   3.2. In the case of successful attack, the system performance and availability depends on the incident detection and compromised system repair time. When the system repair time is less than mean time between successful attacks, the service could be provided despite of successful attacks.
4. The model for simulation of the network scanning using the stochastic activity network was developed. The model allows evaluating the impact of all modeled computer system parameters on the scan detection efficiency. The threshold value $W$ and the detector reset interval $\Delta t_{\text{rst}}$ are the main parameters having influence on the efficiency of the scan detection.
5. Scanning is detected most effectively when the threshold value $W_{\text{h}}$ is higher than the number of hosts in the network, which are accessed most frequently (higher than the number of active servers). By adjusting the scan detector and seeking to reduce the number of false positives, the threshold value higher than the number of active computers in the network should be chosen or the access to active ports of these computers should not be logged when detecting scans.
6. The investigation results have shown that hardware and alerts logging technique are the main factors having impact on the intrusion detection system *Snort 2.8.0* performance.
7. When the network traffic rate does not exceed 50 Mbps, the *Snort 2.8.0* system with the *PentiumD* (3.2 GHz) processor manages to process practically all packets transmitted over the network irrespective of the chosen network interface card or logging alerts technique. The number of dropped packets in the whole investigated rate range (up to 100 Mbps) was $\leq$0.7%, and when alerts were logged in a database using *Barnyard 0.2.0* it was $\leq$0.1%.
8. The intrusion detection system *Snort 2.8.0* with the *PentiumIV* (1.8 GHz) processor begins to drop packets already at the transmission rate of 30 Mbps. The network interface card and the pattern-matching algorithm have influence on the number of dropped packets in this system only when

the traffic rate exceeds 70 Mbps. When *Barnyard 0.2.0* is used to log alerts in the database, the number of dropped packets is ≤1.1%.

**List of Published Works on the Topic of the Dissertation**

**In the reviewed scientific periodical publications**


1. Paulauskas, N.; Garsva, E.; Skudutis, J. 2009. Network Scan Detection Simulation, *Electronics and Electrical Engineering* 2(90): 43–46. ISSN 1392-1215. (Thomson ISI Web of Science).
2. Paulauskas, N.; Skudutis, J. 2008a. Investigation of the Intrusion detection system *Snort* performance, *Electronics and Electrical Engineering* 7(87): 15–18. ISSN 1392-1215. (Thomson ISI Web of Science).
3. Paulauskas, N.; Garsva, E. 2006a. Computer System Attack Classification, *Electronics and Electrical Engineering* 2(66): 84–87. ISSN 1392-1215. (INSPEC).
4. Paulauskas, N.; Garsva, E. 2006b. The analysis of threats to academic computer system, *Инженерный вестник* 1(21)/1: 73–76.


**In the other editions**


5. Paulauskas, N.; Garsva, E. 2008b. Attacker Skill Level Distribution Estimation in the System Mean Time-to-Compromise, in *Proceedings of 1st International Conference on Information Technology*, Gdanks, 19–21 May, 2008, 463–466. ISBN 978-1-4244-2244-9. (Thomson ISI Proceedings).
6. Paulauskas, N.; Garsva, E. 2006c. Computer System Security Incident Analysis, in *Seventh International Baltic Conference on Databases and Information Systems*. Communications Materials of Doctoral Consortium, 336–339. ISBN 9955-28-013-1. (Thomson ISI Proceedings).
7. Paulauskas, N.; Garsva, E. 2008c. Host Scan Detection Simulation. *Information Systems Architecture and Technology*. *Information Systems and Computer Communication Networks*, Wroclaw, 151–161. ISBN 978-83-7493-416-9.
8. Paulauskas, N. 2008d. Kompiuterių sistemos modeliavimas stochastiniais veiklos tinklais, iš *11-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“, įvykusios Vilniuje 2008 m. kovo 14 d., teminės konferencijos „Elektronika ir elektrotechnika“ straipsnių rinkinys*. Vilnius: Technika, 84–96. ISBN 978-9955-28-373-7.
9. Paulauskas, N. 2007. TCP ir UDP prievadų žvalgos būdai, iš *10-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“, įvykusios Vilniuje 2007 m. kovo 16 d., medžiaga: Elektronika ir elektrotechnika*. Vilnius: Technika, 37–52. ISBN 978-9955-28-184-9.

10. Paulauskas, N.; Garšva, E. 2006d. Kompiuterinių grėsmių, kylančių skirtingų tipų organizacijoms, apžvalga, iš *LKMA 20-ojo suvažiavimo darbai*. Vilnius: M. Romerio universitetas, 441–452. ISSN 1392-0499.

**About the author**

Nerijus Paulauskas was born in Klaipėda, on 28 of May 1980.

He was granted the Bachelor's degree in Electrical Engineering and Electronics at the Faculty of Electronics of Vilnius Gediminas Technical University in 2002 and the Master's degree in Electrical Engineering and Electronics at the Faculty of Electronics of Vilnius Gediminas Technical University in 2004. In 2001–2004 he worked as laboratory assistant in the Department of Radio Engineering. In 2004–2005 N. Paulauskas worked as junior scientific officer in Department of Computer Engineering. In 2005–2009 he was a PhD student of Vilnius Gediminas Technical University.

# INCIDENTŲ KOMPIUTERIŲ SISTEMOSE TYRIMAS IR SAUGUMO LYGIO ĮVERTINIMAS

***Mokslo problemos aktualumas***

Informacinių sistemų išliekamumo ir informacijos pasiekiamumo moderniuose kompiuterių tinkluose svarba ir didėjanti įvairių organizacijų veiklos priklausomybė nuo ryšio paslaugas teikiančių kompiuterinių sistemų ženkliai įtakojo kompiuterinių įsilaužimų įvairovės ir jų sudėtingumo augimą.

Internetui tapus finansinių operacijų erdve, keičiasi ir piktavalių vykdomų atakų tikslai. Jeigu anksčiau pagrindinis piktavalių tikslas buvo išgarsėti, išbandyti savo sugebėjimus ar kitaip kam nors pakenkti, tai šiuo metu pagrindiniu jų tikslu tampa finansinė nauda. Vis dažniau piktavaliai įveikia įmonėse ar bankuose įdiegtus informacijos apsaugos mechanizmus, skirtus riboti prieigą prie kompiuterių tinklo resursų.

Kompiuterių sistemose dažniausiai funkcionuoja bendrosios paskirties taikomosios programos, kurių saugumas ne visuomet garantuotas, nuolat aptinkamos spragos, kurios leidžia realizuoti saugumo grėsmes. Be to, kompiuterių sistemos darbo metu nuolat keičiasi jos vykdomos funkcijos ir taikomųjų programų sudėtis. Todėl, informacijos saugumo užtikrinimas yra ne vienkartinis veiksmas, o nuolatinis procesas.

Atakos atsiradimas ir sistemos atsakas į ją yra atsitiktiniai dydžiai, todėl, norint nustatyti piktavalių atakų poveikį kompiuterių sistemai, tenka naudoti tikimybinius modelius.

Kompiuterių sistemos saugumo įvertinimui ir jo didinimui, būtina žinoti poveikio šiai sistemai būdus, jiems būdingus požymius ir galimą įtaką sistemai.

Stochastinės prielaidos yra būtinos aprašant dar neįdiegtas sistemas ir sistemas, kurių pažeidžiamumai dar nėra žinomi. Šiais atvejais yra būtina padaryti stochastines prielaidas apie pažeidžiamumų atsiradimą, jų atradimą, puolančiojo ir pačios sistemos elgseną.

Siekiant sumažinti grėsmių keliamą riziką ir galimas pasekmes, labai svarbu identifikuoti atakas pradiniame jų realizavimo etape, laiku ir atitinkamai į jas reaguoti. Vienas iš būdų leidžiančių tai atlikti yra atakų atpažinimo sistema (angl. *Intrusion Detection System* – IDS). IDS darbo efektyvumas labai priklauso nuo jos sukonfigūravimo konkrečiai kompiuterių sistemai. Atakų atpažinimo sistema efektyviai aptinka žinomas atakas, tačiau pasižymi dideliu klaidingų pranešimų apie atakas skaičiumi ir negali aptikti naujų dar nežinomų atakų. Todėl yra būtina tobulinti jau esamus arba kurti naujus atakų atpažinimo metodus.

***Tyrimų objektas***

Darbo tyrimų objektai yra:

- incidentai kompiuterių tinkluose;
- incidentų poveikis kompiuterių sistemoms;
- atakų atpažinimo sistemos;
- kompiuterių tinklo žvalgos būdai.

***Darbo tikslas***

Šio darbo tikslas yra incidentų kompiuterių tinkluose tyrimas ir kompiuterių sistemų saugumo lygio įvertinimas.

***Darbo uždaviniai***

Darbo tikslui pasiekti reikia išspręsti šiuos uždavinius:

1. Suklasifikuoti atakas pagal įvairius jų požymius ir pasiūlyti atakų sunkumo lygio skaitinį įvertinimą pagal galimą įtaką kompiuterių sistemai.
2. Sudaryti kompiuterių sistemų saugumo lygio kiekybinio įvertinimo metodiką, pagal sistemos pažeidžiamumus ir atakuojančiųjų kvalifikaciją.
3. Ištirti kompiuterių sistemos našumo ir pasiekiamumo priklausomybę nuo sistemą veikiančių atakų ir joje naudojamų apsaugos mechanizmų.
4. Sukurti kompiuterių tinklo žvalgos modelį, imituojantį horizontalią (mazgų) ir vertikalią (prievadų) žvalgą ir ištirti žvalgos atpažinimui taikomo metodo įtaką žvalgos atpažinimo efektyvumui.
5. Eksperimentiškai ištirti atakų atpažinimo sistemos *Snort*, įdiegtos skirtingo našumo kompiuteriuose, efektyvumą ir įtaką jos našumui.

***Tyrimų metodika***

Darbe kiekybiniam kompiuterių sistemos saugumo įvertinimui taikomi tikimybiniai ir statistinės analizės metodai. Atsitiktiniams įvykiams kompiuterių sistemose modeliuoti naudojami stochastiniai veiklos tinklai (angl. *Stochastic Activity Networks* – SAN). SAN modeliai sudaryti panaudojant stochastinių veiklos tinklų modeliavimo įrankį *Möbius*. Incidentams kompiuterių tinkluose rinkti ir analizuoti naudota atakų atpažinimo sistema *Snort*.

***Darbo mokslinis naujumas***

Rengiant disertaciją buvo gauti šie elektros ir elektronikos inžinerijos mokslui nauji rezultatai:

1. Sudaryta originali kompiuterių atakų klasifikacija ir pasiūlytas atakų sunkumo lygio skaitinis įvertinimas.
2. Kompiuterių sistemos saugumo lygį vertinant vidutinio laiko iki sukompromitavimo kriterijumi, įvertintas atakuojančiųjų sugebėjimų lygio pasiskirstymas.
3. Kompiuterių sistemos našumui, jos teikiamų paslaugų pasiekiamumui ir kompiuterių tinklo žvalgos būdams tirti, sudaryti nauji stochastinių veiklos tinklų modeliai.
4. Eksperimentiškai ištirtas atakų atpažinimo sistemos *Snort* efektyvumas apdorojant įvairios spartos duomenų srautą skirtingo našumo aparatine įranga.

***Darbo rezultatų praktinė reikšmė***

Sukurtas kompiuterių tinklo žvalgos modelis, leidžiantis įvertinti modeliuojamos kompiuterių sistemos parametrų įtaką horizontalios ir vertikalios žvalgos atpažinimo efektyvumui.

Sudarytas kompiuterių sistemos našumo ir pasiekiamumo tyrimo modelis leidžia tirti realių kompiuterių sistemų našumą ir pasiekiamumą, o taip pat nustatyti, ar tolimesnis apsaugos mechanizmų kokybės didinimas duos laukiamų rezultatų.

Patobulinta kompiuterių sistemos saugumo lygio kiekybinio įvertinimo vidutinio laiko iki sukompromitavimo kriterijumi metodika leidžia papildomai įvertinti atakuojančiųjų sugebėjimų lygio pasiskirstymą, lyginant tarpusavyje įvairių kompiuterių sistemų saugumą.

Pasiūlyta originali atakų klasifikacija ir atakos sunkumo lygio įvertinimas skaitine verte gali būti taikomi incidentų tyrimui ir analizei.

***Ginamieji teiginiai***

1. Sudaryta originali kompiuterių atakų klasifikacija, pagal kurią atakų sunkumą tikslinga vertinti penkiais sunkumo lygiais.
2. Sistemos saugumo lygį siūloma vertinti vidutinio laiko iki sukompromitavimo kriterijumi ir naudoti ne kraštines atakuojančiųjų sugebėjimų lygio vertes, o intervalą, kuriame skirtingo lygio atakuojantieji yra pasiskirstę pagal tikimybinį dėsnį.
3. Atakų poveikiui sistemoms tirti, žvalgos atpažinimo efektyvumui įvertinti ir atakų atpažinimo sistemų konfigūravimo parametrų reikšmių suradimui tikslinga naudoti stochastinius veiklos tinklus.
4. Remiantis eksperimentiniais atakų atpažinimo sistemos *Snort 2.8* efektyvumo tyrimo rezultatais, konkretaus apkrovimo tinklui galima parinkti tinkamą aparatinę įrangą *Snort* sistemos diegimui ir tinkamai sukonfigūruoti atakų atpažinimo sistemą.

***Disertacijos struktūra***

Disertaciją sudaro įvadas, penki skyriai, bendrosios išvados ir 1 priedas. Darbo apimtis yra 136 puslapiai, tekste panaudotos 25 numeruotos formulės, 39 paveikslai ir 6 lentelės. Rašant disertaciją buvo panaudota 117 literatūros šaltinių.

Pirmasis skyrius skirtas literatūros apžvalgai. Jame apžvelgiamos atakų atpažinimo ir atakų prevencijos sistemų technologijos, analizuojami atakų atpažinimo metodai. Nagrinėjami atakų klasifikavimo būdai. Didelis dėmesys skiriamas kompiuterių sistemos saugumo lygio įvertinimo metodams, kompiuterių prievadų žvalgos būdams ir žvalgos atpažinimo metodams. Skyriaus pabaigoje formuluojamos išvados ir konkretizuojami disertacijos uždaviniai.

Antrajame skyriuje pateikta sudaryta atakų nukreiptų į kompiuterių sistemą klasifikacija, atakų sunkumo lygio skaitinis įvertinimas. Analizuojama trijose skirtingų veiklos sferų organizacijose surinkta duomenų apie incidentus statistika.

Trečiajame skyriuje pateiktas sistemos saugumo lygio įvertinimo metodas vidutinio laiko iki sukompromitavimo kriterijumi.

Ketvirtajame skyriuje pateiktas sudarytas kompiuterių sistemos modelis, įgalinantis įvertinti sistemos našumo ir vieno iš sistemos saugumo komponentų – pasiekiamumo priklausomybę nuo sistemą veikiančių atakų dažnio ir sistemoje naudojamų apsaugos mechanizmų. Skyriuje taip pat yra pateikiamas sukurtas kompiuterių tinklo žvalgos modelis, leidžiantis ištirti įvairius žvalgos tipus ir žvalgos atpažinimui taikomo metodo įtaką žvalgos atpažinimo efektyvumui. Modeliai sudaryti naudojant stochastinius veiklos tinklus.

Penktajame skyriuje nagrinėjamos atakų atpažinimo sistemos *Snort* galimybės ir jos efektyvų darbą sąlygojantys veiksniai. Yra pateikiami *Snort 2.8.0* sistemos našumo priklausomybės nuo pasirinktos aparatinės įrangos ir duomenų apie atakas registravimo būdo tyrimo rezultatai. Taip pat aptarti sistemos našumą įtakojantys pagrindiniai veiksniai ir pateiktos rekomendacijos, kaip pagerinti atakų atpažinimo sistemos *Snort* našumą.

***Bendrosios išvados***

Darbo metu gauti šie rezultatai:

1. Sudaryta originali kompiuterių atakų klasifikacija ir pasiūlytas atakų sunkumo lygio skaitinis įvertinimas. Parodyta, kad tikslinga skirstyti atakas į 5 sunkumo lygius, kurie tiesiogiai priklauso nuo atakos tikslo. Pagrindinis pasiūlytos klasifikacijos privalumas – universalumas; ją galima išplėsti ir papildyti naujomis atakomis priskiriant jas tam tikram sunkumo lygiui.
2. Sudaryta kompiuterių sistemų saugumo lygio įvertinimo metodika, taikant vidutinio laiko iki sukompromitavimo kriterijų ir įvertinant atakuojančiųjų sugebėjimų lygio pasiskirstymą. Skaičiuojant sistemos vidutinį laiką iki sukompromitavimo, pasiūlyta naudoti ne kraštines atakuojančiųjų sugebėjimų lygio vertes, o intervalą, kuriame skirtingo lygio atakuojantieji yra pasiskirstę pagal tikimybinio skirstinio dėsnį.
3. Sudarytas kompiuterių sistemos stochastinių veiklos tinklų modelis, skirtas sistemos našumui ir jos teikiamų paslaugų pasiekiamumui tirti. Sudaryto modelio tyrimo rezultatai parodė, kad:
   3.1. Didinant apsaugos mechanizmų kokybę, pradžioje sistemos našumas ir pasiekiamumas auga ženkliai, tačiau vėliau, pasiekus įsisotinimo tašką, augimas sulėtėja. Tai parodo, kad pakankamą sistemos našumą ir pasiekiamumą galima gauti, naudojant net ir standartinius sistemos apsaugos mechanizmus.
   3.2. Sėkmingos atakos atveju, sistemos našumas ir pasiekiamumas priklauso nuo incidento aptikimo ir sukompromituotos sistemos atstatymo į veiksnumo būseną laiko. Tuo atveju, kai sistemos atstatymui reikalingas laikas yra trumpesnis už vidutinį laiko intervalą tarp sėkmingų atakų, paslauga gali būti teikiama net ir esant sėkmingoms atakoms.
4. Panaudojant stochastinius veiklos tinklus sukurtas kompiuterių tinklo žvalgą imituojantis modelis. Šis modelis leidžia įvertinti visų modeliuojamos kompiuterių sistemos parametrų įtaką žvalgos atpažinimo efektyvumui. Slenkstinė vertė $W$ ir žvalgos atpažinimo detektoriaus

skaitiklių išvalymo laiko intervalas $\Delta t_{rst}$ yra pagrindiniai parametrai, įtakojantys atpažinimo efektyvumą.

5. Žvalga atpažįstama efektyviausiai, kai slenkstinė vertė $W_h$ yra didesnė nei mazgų skaičius tinkle, į kuriuos kreipiamasi dažniausiai (didesnė nei paslaugas teikiančių tarnybinių stočių skaičius). Todėl derinant IDS ir siekiant sumažinti klaidingų atpažinimų skaičių, slenkstinė vertė $W_h$ tūrėtų būti parenkama didesnė nei tinkle esančių aktyvių kompiuterių skaičius arba, atpažįstant žvalgą, kreipimasis į šių kompiuterių aktyvius prievadus netūrėtų būti fiksuojamas.
6. Atakų atpažinimo sistemos efektyvumo tyrimo rezultatai parodė, kad aparatinė įranga ir duomenų apie atakas registravimo būdas yra pagrindiniai veiksniai, įtakojantys atakų atpažinimo sistemos *Snort 2.8.0* našumą.
7. Kai tinklo paketų srauto greitis neviršija 50 Mbps, atakų atpažinimo sistema *Snort* su *PentiumD* procesoriumi dirba efektyviai, spėja apdoroti visus tinklu perduodamus paketus, nepriklausomai nuo to, kokia tinklo plokštė ar duomenų apie atakas registravimo būdas yra pasirinktas. Pamestų paketų skaičius visame tirtame greičių ruože (iki 100 Mbps) neviršija 0,7 %, o jeigu duomenys apie atakas į duomenų bazę įrašomi naudojant *Barnyard 0.2.0*, pamestų paketų skaičius ≤0,1 %.
8. Atakų atpažinimo sistema *Snort 2.8.0* su *PentiumIV* procesoriumi, paketus pradeda pamesti jau esant 30 Mbps perdavimo greičio. Tinklo plokštė ir paieškos pagal šabloną algoritmas įtakoja pamestų paketų skaičių šioje sistemoje tik tada, kai tinklo paketų srauto greitis viršija 70 Mbps. Kai duomenims apie atakas į duomenų bazę įrašyti naudojamas *Barnyard 0.2.0*, pamestų paketų skaičius ≤1,1 %.

**Trumpos žinios apie autorių**

Nerijus Paulauskas gimė 1980 m. gegužės 28 d. Klaipėdoje.

2002 m. įgijo elektros ir elektronikos inžinerijos bakalauro laipsnį Vilniaus Gedimino technikos universiteto Elektronikos fakultete. 2004 m. įgijo elektros ir elektronikos inžinerijos mokslo magistro laipsnį Vilniaus Gedimino technikos universiteto Elektronikos fakultete. 2001–2004 m. dirbo Radijo aparatūros katedros laborantu. 2004–2005 m. dirbo jaunesniuoju mokslo darbuotoju Kompiuterių inžinerijos katedroje. 2005–2009 m. – Vilniaus Gedimino technikos universiteto Kompiuterių inžinerijos katedros doktorantas.

**Nerijus Paulauskas**

**ANALYSIS OF COMPUTER SYSTEM INCIDENTS AND SECURITY LEVEL EVALUATION**

**Summary of Doctoral Dissertation**
**Technological Sciences**
**Electrical and Electronic Engineering (01T)**

**INCIDENTŲ KOMPIUTERIŲ SISTEMOSE TYRIMAS IR SAUGUMO LYGIO ĮVERTINIMAS**

**Daktaro disertacijos santrauka**
**Technologijos mokslai**
**Elektros ir elektronikos inžinerija (01T)**

2009 04 21. 1,5 sp. l. Tiražas 60 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“, Saulėtekio al. 11, LT-10223 Vilnius
*http://leidykla.vgtu.lt*
Spausdino UAB „Biznio mašinų kompanija“,
J. Jasinskio g. 16A, LT-01112 Vilnius