Eimantas GARŠVA

MODELLING OF COMPUTER SYSTEM SECURITY

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

1333

LEIDYKLA
Vilnius TECHNIKA **2006**

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Eimantas GARŠVA

MODELLING OF COMPUTER SYSTEM SECURITY

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

VGTU
LEIDYKLA
Vilnius TECHNIKA 2006

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2002–2006

Scientific Supervisor

Prof Dr Habil Julius SKUDUTIS (Vilnius Gediminas Technical University, Technological Sciences, Electrical Engineering and Electronics – 01T)

The Dissertation is being defended at the Council of Scientific Field of Electrical Engineering and Electronics at Vilnius Gediminas Technical University:

Chairman

Assoc Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical Engineering and Electronics – 01T)

Members:

Prof Dr Habil Gintautas DZEMYDA (Institute of Mathematics and Informatics, Technological Sciences, Informatics Engineering – 07T)

Prof Dr Habil Romanas MARTAVIČIUS (Vilnius Gediminas Technical University, Technological Sciences, Electrical Engineering and Electronics – 01T)

Prof Dr Habil Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T)

Assoc Prof Dr Šarūnas PAULIKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical Engineering and Electronics – 01T)

Opponents:

Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T)

Assoc Prof Dr Algirdas BAŠKYS (Semiconductor Physics Institute, Technological Sciences, Electrical Engineering and Electronics – 01T)

The dissertation will be defended at the public meeting of the Council of Scientific Field of Electrical Engineering and Electronics in the Senate Hall of Vilnius Gediminas Technical University at 10 a. m. on 5 January 2007.

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.vtu.lt

The summary of the doctoral dissertation was distributed on 5 December 2006.

A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, Vilnius, Lithuania).

© Eimantas Garšva, 2006

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Eimantas GARŠVA

KOMPIUTERIŲ SISTEMŲ SAUGUMO MODELIAVIMAS

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

VGTU
LEIDYKLA
Vilnius TECHNIKA 2006

Disertacija rengta 2002–2006 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
doc. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).
Nariai:
prof. habil. dr. Gintautas DZEMYDA (Matematikos ir informatikos institutas, technologijos mokslai, informatikos inžinerija – 07T),
prof. habil. dr. Romanas MARTAVIČIUS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),
prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T),
doc. dr. Šarūnas PAULIKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Oponentai:
habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),
doc. dr. Algirdas BAŠKYS (Puslaidininkių fizikos institutas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Disertacija bus ginama viešame Elektros ir elektronikos inžinerijos mokslo krypties tarybos posėdyje 2007 m. sausio 5 d. 10 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.
Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: +370 5 274 4952, +370 5 274 4956; faksas +370 5 270 0112;
el. paštas doktor@adm.vtu.lt

Disertacijos santrauka išsiuntinėta 2006 m. gruodžio 5 d.
Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, Vilnius, Lietuva)
VGTU leidyklos „Technika“ 1333 mokslo literatūros knyga

© Eimantas Garšva, 2006

1. General Characteristic of the Dissertation

Topicality of the problem. Computer systems are interconnected and distributed in respect of each other. Requirements to the computer security increase because organisations highly depend on their computer network. The number of potential threats increases because of the computer system integration more potential intruders get access to other systems. The computer system security increase does not allow reaching total security, therefore widening of the computer system security attitude and striving for system functioning despite of possible attacks are needed.

In order to achieve a higher computer system security, the evaluation of all influencing aspects is needed because the computer system is as secure as its weakest element is. The computer system security modelling allows evaluating the system in the design phase or forecasting security changes. The computer system security comprises security description, existing influence on the system, security mechanisms, ability to evaluate the level of the system security and possible changes.

The prosperity of the organisation or individual depends on the computer system provided services. The number of everyday services provided by the computer system increases constantly: tax payment, planning, telephony, etc. The more valuable the computer system providing crucial services becomes, the more serious threat arises to its security. The importance of the computer system security increased drastically over the last decade, and it increases further.

Aim and tasks of the work are to create principles of the incident tolerant computer system security evaluation, to examine the survivability of the modelled computer system examining its dependence on the security mechanism strength using the composed model.

The tasks for achieving this aim are:

- to analyse the computer system security standards and security models;
- to compose the computer system attack classification which incorporates all the main features of the attack;
- to model typical threats to the computer system using graph theory;
- to perform the experimental study on the computer system security incidents;
- to analyse security mechanisms evaluating the modelling abilities;
- to compose a model of the computer system survivability;
- to examine the modelled computer system survivability dependence on the security mechanism strength.

Scientific novelty

- The computer system security modelling methodology was suggested;
- The model for examination of the modelled computer system survivability dependence on the security mechanism strength examination was created;
- The universal computer system attack classification was suggested.

Methodology of research includes the usage of analytical and probability methods. Graph theory was used to model typical attacks.

Experiments were performed with the aim to study the security incident distribution and the security mechanism features. Experiment results were used in further modelling.

Stochastic Activity Network formalism was used for the computer system security modelling. To realise a model and calculate modelling results, Mobius software package was used.

Practical value. The suggested computer system security simulation model, with collected additional empirical data on the computer system design can be used to compare different computer system designs, to evaluate the efficiency of possible computer system modifications and to forecast possible security incidents. The computer system security evaluation software can be produced using the suggested computer system security modelling methodology after the collection and verification of a larger number of the statistical security incident data.

The suggested universal computer system attack classification and numerical incident severity evaluation have wide application abilities for incident correlation and analysis.

Defended propositions

- The methodology of the computer system security evaluation modelling.
- The computer system attack classification and numerical incident severity evaluation.
- The experimental statistical data analysis results on security incidents affecting different computer systems.
- The results of the computer system security simulation.

The scope of the scientific work. The scientific work consists of the general characteristic of the dissertation, 4 chapters, conclusions, list of tables, list of pictures, list of abbreviations, list of literature and list of publications. The total scope of the dissertation is 125 pages, 44 pictures, 17 tables and 198 references.

2. Modelling of Computer System Security

2.1. The Study of Security Models of the Computer System and the Information Protection Means

Security standards and models describe the computer system security and define aims in securing the system. Security models are useful when modelling the impact on the system and permits binding of the modelled computer system states with a real operational computer system. In order to do that description of a real computer system, the policy definition formally presented by the security model is needed.

It is necessary to define computer system boundaries and the security perimeter with gathered most valuable elements and information.

An attack is realisation of the threat, the harmful action aiming to find and exploit the system vulnerability. A successful attack causes intrusion. Vulnerability is some poor characteristic of the system establishing conditions for the threat to arise. The computer system is affected by the active element – a subject (a user or a process) that initiates the query for the object (resource) access and usage. The access is interaction between the subject and the object during which they exchange information. An incident consists of the attack and the response of the computer system to it. An attack can fail to achieve the intended objective for some reasons, but even then there exists possibility that the system becomes more vulnerable.

There are three main types of threats arising to the system: confidentiality, integrity and availability (or Denial of Service). The threat to policy violation must be also considered.

Security evaluation standards describing secure system requirements evolved from Trusted Computer System Evaluation Criteria TCSEC to Common Criteria CC. The first laid the foundation and the second is widely used nowadays.

The documentation and system design management is addressed mostly in Common Criteria and consists of the security profile and evaluation. Secure products and computer systems are classified using seven Evaluation Assurance Levels.

Security models (formal security policy definitions) can be grouped into access control (confidentiality), integrity and Denial of Service. In order to compose a model addressing all threats these models should be combined.

Composing the universal, all computer system security features incorporating model is too complicated, that is why it is effective to use the model where separate features are modelled using different models.

Threat realisations can be modelled using graph theory with the non-formal security policy defined. The computer system security level dependence on the incident severity and security mechanism strength modelling using stochastic formal methods can be performed after threat and security mechanism research.

The total computer system security can not be achieved even with all security requirement compliance defined in security policy and formally analysed using security models. Because of that the survivability paradigm should be used in evaluating the security of the computer system tolerant to the possible security violations.

2.2. The Study of Threats to the Computer System

Knowledge of the impact on the computer system is essential for security modelling. Only malicious impact is considered, it is caused by attacks – threat realisations. The analysis of computer system attack classifications and taxonomies was performed. Finding a widely used universal computer attack classification with severity evaluation was not successful, so the universal computer system attack classification, which includes all features of the attack, was composed using known classifications.

Attack severity numerical values are essential for modelling. Using numbers, which represent the attack, it is possible to group, generate and compare attacks as well as their distributions in different computer systems. The method to group incidents according to composed attack classification was suggested.

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

Computer system attacks are classified according to:

1. the objective;
2. the effect type;
3. the ISO/OSI model layer;
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.

Objective achievement is most important for the attacker (1), therefore the attack severity numerical evaluation is based on it. The effect type (2) most depends on the intruder's objective as well as the subject and object location. ISO/OSI model can characterise all computer system processes. The application layer (3.7) is most popular 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 (4) attacks. Location of the attack subject (5) affects the effect type and the probability of attack object achievements. Attack technology and possible threats are affected by the type of object location (6) and attacked service (7). The attack can be concentrated (8) in one packet, and then the attack is called atomic or can be fragmented to several packets. Feedback (9) is not necessary for all attacks, e.g. sniffing. In order to avoid detection or for better efficiency on the system attackers can choose different initial execution conditions (10), the impact type (11) or automation level. According to the attack objective and the effect type the number of attack sources (13) and connection quantity (14) may differ.

Technology evolution will uncover new attacks and new aspects. The suggested classification is open for expansion. New effect types (2), operating systems (4), object locations (6) and services (7) are most possible. The suggested classification is expandable.

The computer system security modelling needs a numerical attack severity evaluation. It is rational to use the 5 level attack severity numerical evaluation based on the attack objective.

Evaluation of threat topicality using the suggested computer system attack classification is also possible.

Attacks usually are targeted to reach same or similar objectives and can be grouped into typical threat realisations. Typical threat realisations were evaluated using the composed attack classification. Hypothetical network topology was designed and modelled using graphs in order to evaluate topology changes caused by the typical attacks.

There are such typical threat realisations with common features: network traffic analysis, replacement of trusted subject or object in the distributed computer system, injection of the false object and causing the Denial of Service.

The computer system graph model provides the ability to present computer system attack mechanisms in the visual and efficient way. Channel and network

OSI model layers are presented in a graph model, other layer presentations are ineffective.

The security incident statistical data were collected in the public institution, home network and academic organisation. Data were analysed, classified and compared.

When the computer system security incident number is evaluated among the research time other computer system parameters, such as the amount of users, incident source bandwidth, must be taken into account. The average incident number INC_{vid} is lower when investments and attention paid to the system security are higher.

After the security incident statistical analysis it was found that the number of most severe incidents is the least (Fig 1.). Threats to confidentiality and availability are targeted most; security policy enforcement and management require special attention.

The largest part of attacks was performed using TCP, the smallest – UDP.

The amount of incidents where ICMP is used is the highest because of policy violation and DoS attack automation.

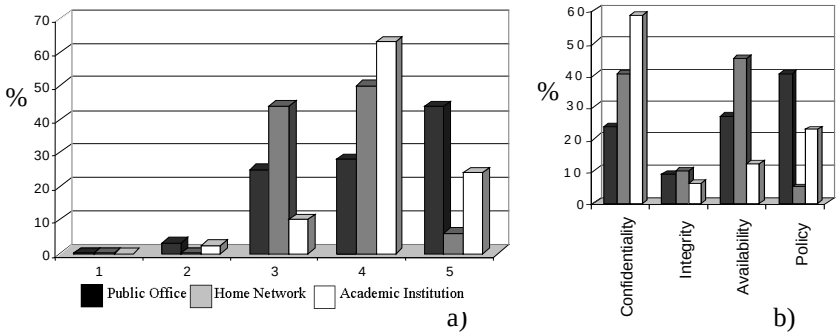

Fig 1. Incident distribution in different network type organisations, according to: a) incident severity level and b) threat realisation

2.3. The Study of Information Security Means Efficiency in the Computer System

Information security assurance means were classified and analysed. Analysis showed the security mechanism installation priority. In the computer system design phase the aspects of using secure protocols, secure design principles and cryptography mechanisms must be addressed.

In order to assure optimal security level in the computer system the combination of all security mechanisms must be used and security must be

already addressed in the design phase. There are such means to secure the network:

- Information protection equipment (RAID, UPS and other);
- Secure network operating systems;
- Antiviral systems;
- Firewalls;
- Software and hardware network traffic scramblers and secure network cryptoprotocols;
- Advanced access control;
- Intrusion detection and prevention systems;
- Security analysis tools;
- Strong authentication and identification systems;
- Organisational means.

Securing the computer system without the secure (configured properly and updated according to the manufacturer requirements) network operating system is impossible. Virus occurrence probability is the highest, so the next step should be antiviral system implementation. Firewall is necessary and effective mean to secure the network perimeter. Network traffic scramblers are necessary to transmit data through the insecure media. The advanced access control is effective at preventing insider threats by precise definition and limitations to the user or a group. Intrusion Detection Systems detect intrusion targeted attacks, and IPSes are able to block them. The security analysis tool does security evaluation and vulnerability discovery. Strong authentication and identification system using certificates or biometric means are more secure than passwords. The computer system security is usually considered to be a technical problem, but the attitude must change in order for security to be an organisational problem, only then maximal security can be achieved. Computer system security is considered to be an organisational problem and security policy is prepared, threat analysis performed and all security mechanisms needed in order to implement security policy are installed.

The attention to the secure mechanism positioning must be paid when designing the computer system. OSI application layer is the most suitable for security mechanism deployment, but in that case they are dependent on the services provided. Channel, network and transport layer security mechanisms do not depend on services provided. Transport layer security mechanisms are most effective at securing information transition through insecure media, and channel ones securing access.

The study showed that at present there is no universal and effective security assuring the computer system design. Different secure system designs are incompatible: ISO 9478-2 is based on OSI model and addresses

communication security, SDNS suggests the design and protocols additional to TCP/IP protocol stack and ECMA addresses security in the distributed computer systems.

Part of the researchers considers the threat management and antiviral system to be unable to use the present-day security standards because they emerged as the Internet itself without the plan and administration. Secure network design expectations are bounded with the new projects (Internet-2) and new protocols (e.g.: IPv6) implementation in the global network.

The intrusion Detection System Snort with initial configuration correctly detects more than 70 % of all incidents. The largest part of false positives was detected when ICMP was used (43 %). BASE front end was found most suitable for the incident analysis.

Checkpoint NGX firewall restrained 64 % of all incidents, application gateway component was most effective at blocking service (WEB, SMTP, others) targeted incidents, because of that TCP incident restraint was most effective (90 %). Most severe incidents were blocked most efficiently (92 %). Defence from threat to confidentiality was best (87 %) (Fig 2.).

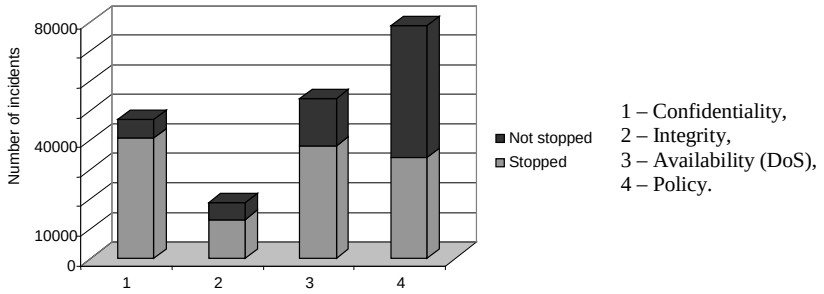

Fig 2. Firewall efficiency dependence on the treat realisation

2.4. Computer System Security Evaluation

The computer system modelling is valuable when the computer systems in the design phase are evaluated or the forecasting of the computer system parameter change influence on its security is performed.

Set, graph and probability theories can be used in describing the computer system.

Computer system security can be evaluated procedurally, economically and using statistical characteristics. Statistical security evaluation is most suitable for the modelling.

Survivability is the computer system ability to resist attacks and to keep functioning at some level after the incident. To achieve that, the system reaction to and evaluation of occurring incidents are needed: to detect incidents, resist to attacks, and keep functionality if compromised. The computer system survivability comprises such areas as reliability, security and interference resistance. A new state of the computer system after the incident *s*, in common case, is compromised, and the system functions and waits to be restored to full functionality. Survivability can be computed for every computer system service. If service does not change, then the survivability value is equal to 1, if service is stopped, then it equals to 0, other values are distributed between them.

The computer system is a distributed computer network with boundaries defined. The computer system provides service *k* with some operational grade defined by the system states *{S}:* normal (s=1), attacked (s=2), compromised (s=3), recoverable (s=4) and non-functional (s=5). The service operational grade in a specific system state and the number of states depend on the system analysed. The initial state of the computer system is normal (r=1). The security of the computer system is assured by using security mechanisms, which are defined by their strength *m*. In this case *m* is linearly associated with the cost *C(m).* The computer system security mechanism cost *C(m)* varies from 0, when no security mechanisms are used, to 100, when all the best possible security mechanisms are used.

It is likely that a system with correct configuration and resistant design will not be impacted by less severe incidents, although defence mechanisms will not be used. Correct configuration is minimal, designed according to the creator recommendations and updated minimal service collection, needed for the systems mission. The inter incident time is generally longer than a month and recovery time is a lot shorter, so it is likely that the system before the next serious incident will be in the normal initial state r=1. The computer system design resistance is defined by the parameters: π_1, π_3, χ_1 and χ_3. These parameters are the functions depending on the characteristics of an incident (j) and the system (s).

Incident arrival is a stochastic point process. Incidents arrive at random moments of time t_n and incident type $j \in \{j\}$ is the incident parameter, and incident probability is *P(j)*. Incidents occur at every random rate *a*, which obeys the Poisson distribution. The Poisson distribution was chosen because of its simplicity and modelling ability; despite attack motivation relationships with political or technical issues, the occurrence of incidents is approximately Poisson. The incident type describes the severity of incident and probability that there are several incidents at the same time. Incident is most severe when its type j=1 and least severe when j=5.

The computer system state transitions happen with such logic: probability of getting to a much worse state is lower than getting to a slightly worse state, probability of staying normal is higher if the incident is less severe and the security mechanisms are stronger, and the system must end up in some state.

Statistical data show that the mean time to failure T_{MTTF} is much longer than the system recovery time T_R: ($T_{MTTF} > T_R$), therefore that we can consider that the initial state of the system is always normal (r=1). When incident occurs, the next state of the system can be one out of the system state space {S}, but because of the resistive computer system design, the probability that the computer system stays in the normal state P*(1,1)* after the incident is higher.

Stochastic characteristics of the computer system security depend on the system event times, time spent in each system state and the service level in each state (Fig 3.). The computer system is brought into production at time $t_{0i}=t_{r(i-1)}$ and is affected by some incident i at time $t_{inci.}$ It is possible that after some impact period T_{imi}, which depends on the computer system response to the attack, the system state change will occur at $t_{sci,}$ and that will possibly cause a failure at time t_{fi} and bring the system to non-functional state (s=5). After some recovery period T_{ri}, which depends on the fault discovery time and the system repair time, the computer system will be recovered to the fully functional state. These events will occur repeatedly and usage of the system will end at time t_{all}. T_{all} is the time during which simulation is performed in the computer system security model.

Modelling results show that the computer system with a proper initial configuration and secure design will not be affected by mild incidents even without additional security mechanisms.

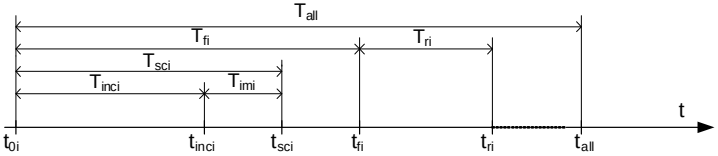

Fig 3. Computer system events that impact on the computer system security characteristics

Survivability dependence on the conditional security mechanism strength was found using the composed model. Dependence curves show that survivability is better if attacks are less severe, and in the beginning the dependence is stronger. Maximal survivability S_{max} is more dependent on the

security mechanism strength and is best to evaluate a homogeneous system, and the system survivability *S* – a complex one.

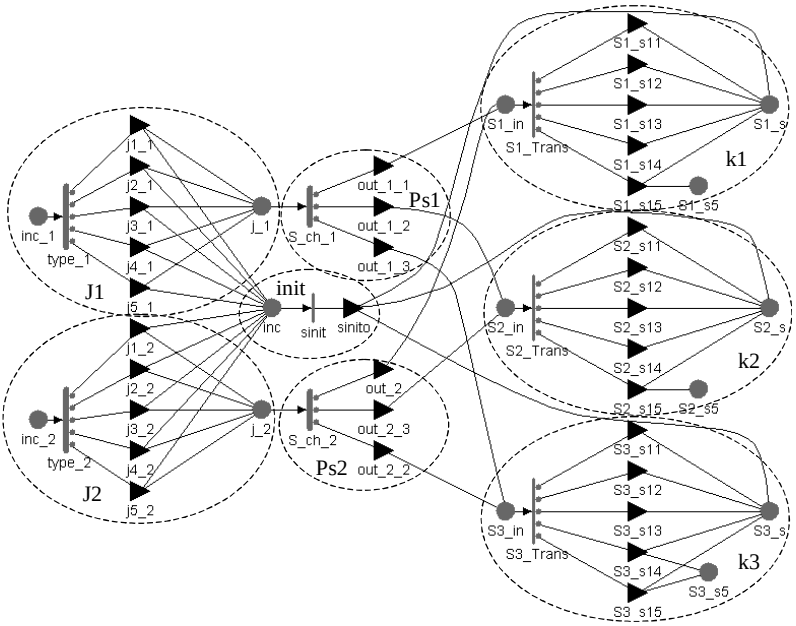

Fig 4. Computer system security simulation model

Let us model a computer system, which has two connections to outer systems: Internet (*J1*) and Intranet (*J2*), and provides three services: windows sharing (*k1*), SMTP (*k2*) and HTTP (*k3*) (Fig 4.). These all three services are used by some human resource planning application. These attack severity and service attack probabilities were aggregated from the global sources and experiments, and adapted to the modelled system.

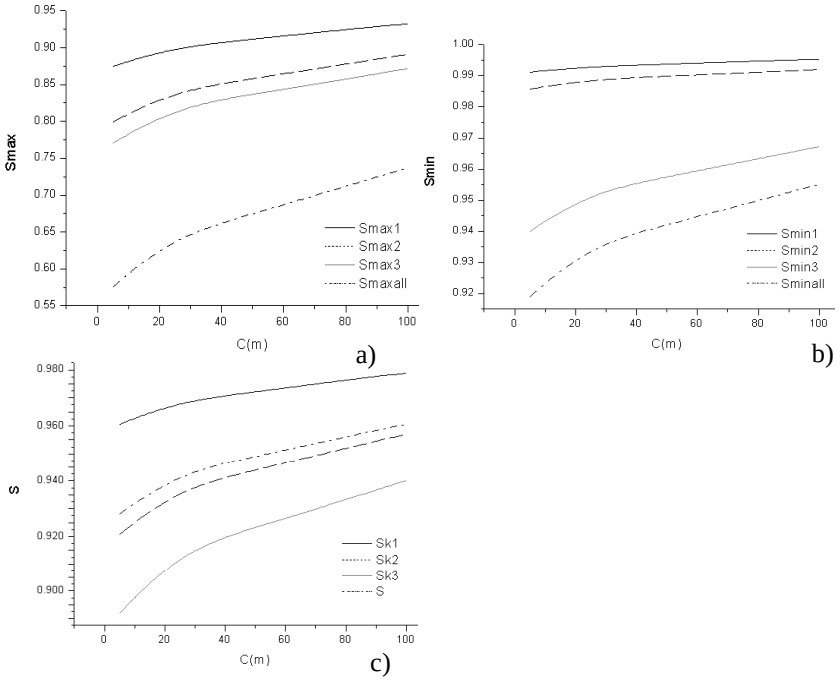

Fig 5. Survivability characteristics: a) maximal S_{max}, b) minimal S_{min} and c) the system survivability *S(s)*

Incidents occur faster from the Intranet (*J1*) than from the Internet (*J2*) because some security measures are implemented by the provider. Generated incidents by "type_2" and "type_1" activities, with appropriate types at the set rate arrive to the system via places "j_1" and "j_2". PS1 and PS2 decide which service is attacked. Activities "S_ch_1" and "S_ch_2" choose the attacked service at the rate equal to the fastest incident occurrence rate and output gates transfer attack type *j* to the specific service *k1*, *k2* or *k3*. The initialisation unit "init" assures that services are recovered to the normal state *s=1* before the incident enters the system. Architecture parameters defining the initial service strength (π_1, π_3, χ_1 and χ_3) are the same for all services. Service weights *w(k)* as well as levels at which service *k* is provided in different system states *φ(s,k)* differ. Maximal survivability S_{max} characteristics for all the services (Fig 5. a), and the common maximal survivability S_{maxall}, representing the probability that all the services will be in the normal state *s=1*, were calculated. Minimal

survivability S_{min} characteristics for all the services (Fig 5. b), and one common, presenting the probability that all the services will be provided at some states, except non-functional, were calculated. Then the survivability of all the services, according to the levels that service survives in the specific state, was calculated and one value common to the whole system survivability *S(s)* (Fig 5. c) was found.

As it is seen from the graphs (Fig 5.) the survivability curves have similar shapes to the basic computer system simulation ones. Because of more distributed incident types they are more flat. Common survivability characteristics S_{maxall} and S_{minall} have lower values because they represent the worst case in the system. The system survivability *S(s)* has average values, which depend on the state in which the services have survived and their weight.

3. General Conclusions

1. The suggested computer system attack classification is suitable for experimental data classification and is intended to incorporate every feature of the attack. The suggested classification is open for expansion when technology evolution will uncover new attacks and new aspects. New effect types, operating systems, object locations and services are most possible. The computer system attack severity numerical evaluation, needed for security modelling, is possible using suggested attack classification according to the objective. Evaluation of threat topicality is also possible. The computer system graph model provides the ability to present computer system attack mechanisms in the visual and efficient way.

2. When the computer system security incident number is evaluated over the research time, other computer system parameters such as the amount of users and the incident source bandwidth must be taken into account. The analysis of the security incidents at three different organization networks showed that the average incident number INC_{vid} is lower when investments and attention paid to the systems security are higher. After the deeper analysis it was found that: the number of most severe incidents is the least; threats to confidentiality and availability are targeted most; the security policy enforcement and management require special attention; the largest part of attacks were performed using TCP, the smallest – UDP; the amount of incidents where ICMP is used is the highest because of policy violation and DoS attack automation.

3. In order to assure an optimal security level in the computer system the combination of all security mechanisms must be used and security must be already addressed in the design phase. The maximal computer system security

level can be achieved only when security is considered to be an organisational problem and threat analysis performed, security policy is prepared and all security mechanisms needed in order to implement security policy are installed. OSI application layer is the most suitable for the security mechanism deployment. Transport layer security mechanisms are most effective at securing information transition through insecure media, and channel ones at securing access.

4. The intrusion detection system Snort with initial configuration correctly detects more than 70 % of all incidents. The largest part of false positives was detected when ICMP was used (43 %). BASE front end was found most suitable for incident analysis.

5. Checkpoint NGX firewall restrained 64 % of all incidents, application gateway component was most effective at blocking service (WEB, SMTP, others) targeted incidents, therefore the TCP incident restraint was most effective (90 %). Most severe incidents were blocked most efficiently (92 %). Defence from threat to confidentiality was best (87 %).

6. The computer system security can be evaluated procedurally, economically and using statistical characteristics. Statistical security evaluation is most suitable for modelling. The suggested methodology of the computer system security evaluation consists of the impact analysis, the system model construction, the simulation using SAN model and the survivability characteristics' analysis. Modelling results show that the computer system with a proper initial configuration and secure design will not be affected by mild incidents even without additional security mechanisms.

7. The survivability dependence on the conditional security mechanism strength was found using the composed model. Dependence curves show that the survivability is better if attacks are less severe, and in the beginning the dependence is stronger. The maximal survivability S_{max} is more dependent on the security mechanism strength and is best to evaluate a homogeneous system, and the system survivability S – a complex one.

Published papers on the topic of the dissertation

In the peer-reviewed journals

1. GARŠVA, E. Computer System Survivability Modelling. *Elektronika ir elektrotechnika*. ISSN 1392-1215. Kaunas: Technologija, 2006, No 1 (65), p. 48–51 (in Lithuanian).
2. PAULAUSKAS, N.; GARŠVA, E. Computer System Attack Classification. *Elektronika ir elektrotechnika*. ISSN 1392-1215. Kaunas: Technologija, 2006, No 2(66), p. 84–87.

3. GARŠVA, E. Computer System Survivability Modelling by Using Stochastic Activity Network. In Proceedings of the 25th International Conference on Computer Safety, Reliability and Security (SAFECOMP`06). Volume 4166 of LNCS Berlin Heidelberg Springer-Verlag, 2006.
4. GARŠVA, E.; SKUDUTIS, J. Secure Computer System Design. *Elektronika ir elektrotechnika*. Kaunas: Technologija, 2004, No 6(55), p. 43–48 (in Lithuanian).
5. GARŠVA, E.; SKUDUTIS, J. Security mechanism position in the network model. *Izvestija Beloruskoj inzenernoj akademiji*. Minsk, 2004, No 1 (17)/3, p. 101–103.
6. GARŠVA, E. Survivability modeling with Petri nets. *Izvestija Beloruskoj inzenernoj akademiji*. Minsk, 2005, NO 1 (19)/1, P. 211–214.
7. PAULAUSKAS, N.; GARŠVA, E. Computer System Security Incident Analysis. In Seventh International Baltic Conference on Datbases and Information Systems / Communications Materials of Doctoral Consortium, 2006, p. 336–339.

In the other publications

8. GARŠVA, E. Computer System Security Evaluation with Survivability. Iš Šeštosios Lietuvos jaunųjų mokslininkų konferencijos „Lietuva be moks lo – Lietuva be ateities“ medžiaga: Elektronika ir elektrotechnika. Vilnius: Technika, 2004, p. 64–69 (in Lithuanian).
9. GARŠVA, E. Attack Modelling Using Computer System Graph Model. Iš Penktosios Lietuvos jaunųjų mokslininkų konferencijos „Lietuva be mokslo – Lietuva be ateities“ medžiaga: Elektronika ir elektrotechnika. Vilnius: Technika, 2002, p. 57–63 (in Lithuanian).

About the author

Eimantas Garšva was born in Vilnius, on 23 of October 1977.

He was granted the Bachelor’s degree in Electrical Engineering and Electronics at Faculty of Electronics of Vilnius Gediminas Technical University in 1999 and the Master’s degree in Electrical Engineering and Engineering at Faculty of Electronics of Vilnius Gediminas Technical University in 2001. In 2002–2006 E. Garšva was a PhD student of Vilnius Gediminas Technical University. At present he is Assistant at Computer Engineering Department of Vilnius Gediminas Technical University.

KOMPIUTERIŲ SISTEMŲ SAUGUMO MODELIAVIMAS

Mokslo problemos aktualumas. Šių dienų kompiuterių sistemos yra sujungtos tarpusavyje ir vienos kitų atžvilgiu yra nutolusios. Reikalavimai saugumui didėja, nes organizacijos yra labai priklausomos nuo savo kompiuterių tinklo. Kompiuterių sistemų pažeidžiamumas savo ruožtu taip pat neišvengiamai didėja, nes dėl sistemų apjungimo daugiau potencialių įsibrovėlių turi kitų sistemų pasiekimą. Patirtis rodo, kad kompiuterių sistemos saugumo didinimas negali pilnai užtikrinti nepažeidžiamumo, todėl būtina praplėsti požiūrį į kompiuterių sistemos saugumą ir siekti, kad sistema išliktų darbinga nepaisant galimų atakų.

Siekiant didesnio kompiuterių sistemų saugumo tenka įvertinti visus galinčius ją įtakoti aspektus, nes sistema yra saugi tiek, kiek yra saugus jos silpniausias elementas. Kompiuterių sistemos saugumo modeliavimas leidžia vertinti dar kuriamą sistemą ar prognozuoti galimus saugumo pokyčius. Kompiuterių sistemos saugumas susideda iš saugumo aprašymo, esančio poveikio sistemai, saugumo užtikrinimo priemonių ir gebėjimo įvertinti saugumo lygį, bei jo pokyčius.

Nuo kompiuterių sistemų atliekamų funkcijų yra priklausoma konkrečios organizacijos ar individo gerovė. Vis daugiau įvairių įprastų operacijų ir paslaugų patikima kompiuterių sistemoms, pvz.: abonentiniai mokesčiai, planavimas, telefonija ir kt. Kuo sistema, dėl teikiamų kritinių paslaugų, tampa vertingesnė, tuo didesnė grėsmė kyla jos saugumui. Pastarąjį dešimtmetį kompiuterių sistemų saugumo svarba ženkliai išaugo ir domėjimasis nepaliaujamai didėja.

Darbo tikslas ir uždaviniai – sukurti kompiuterių sistemų saugumo įvertinimo principus, besiremiančius tolerancija kylantiems incidentams, naudojant sudarytą modelį ištirti modeliuojamos kompiuterių sistemos išliekamumo priklausomybę nuo apsaugos mechanizmų stiprumo.

Uždaviniai šiam tikslui pasiekti:

- Išanalizuoti kompiuterių sistemų saugumą reglamentuojančius standartus ir saugumo modelius;
- Sudaryti atakų klasifikaciją apimančią visus pagrindinius atakos kompiuterių sistemai bruožus;
- Modeliuoti tipines grėsmes kompiuterių sistemai, naudojant grafų teoriją;
- Eksperimentiškai ištirti skirtingų kompiuterių sistemų incidentus;

- Išanalizuoti apsaugos mechanizmus, vertinant jų modeliavimo galimybes;
- Sudaryti kompiuterių sistemos išliekamumo modelį;
- Ištirti kompiuterių sistemos išliekamumo priklausomybę nuo apsaugos mechanizmų stiprumo.

Mokslinis naujumas

- Sudaryta kompiuterių sistemos saugumo modeliavimo metodika.
- Sudarytas modelis leidžiantis įvertinti kompiuterių sistemos saugumo priklausomybę nuo apsaugos mechanizmų stiprumo.
- Pasiūlyta universali atakų kompiuterių sistemai klasifikacija.

Tyrimų metodika apima analitinių ir tikimybinių metodų naudojimą. Tipinių atakų realizacijų tyrimui buvo naudota grafų teorija.

Eksperimentiškai tirtas saugumo incidentų pasiskirstymas ir apsaugos mechanizmų savybės. Eksperimentų rezultatai panaudoti tolesniame modeliavime.

Kompiuterių sistemos saugumo modeliavimui naudotas stochastinių veiklos tinklų SAN formalizmas. Modelio realizavimui ir modeliavimo rezultatų skaičiavimui naudotas Mobius programinis paketas.

Praktinė vertė. Pasiūlytas kompiuterių sistemos saugumo modelis surinkus papildomus empirinius duomenis apie kompiuterių sistemos architektūrą gali būti naudojamas kelioms galimoms kompiuterių sistemos architektūros realizacijoms palyginti, veikiančios kompiuterių sistemos galimų modifikavimų efektyvumui įvertinti ir galimiems saugumo pažeidimams prognozuoti. Surinkus ir patikrinus didesnį kiekį statistikos apie incidentus įvairioms kompiuterių sistemoms, pagal aprašytą metodiką būtų galima sukurti kompiuterių sistemos saugumą vertinančia programinę įrangą. Tai būtų vertinga kuriant, atnaujinant ar vertinant kompiuterių sistemą. Pasiūlyta atakų klasifikacija ir atakos sunkumo įvertinimas skaitine verte turi platų pritaikymą incidentų koreliacijai ir analizei.

Ginamieji teiginiai

- Kompiuterių sistemos saugumo įvertinimo modeliavimo metodika;
- Atakų kompiuterių sistemai klasifikacija ir incidentų sunkumo skaitinis įvertinimas;
- Eksperimento metu surinkti ir apdoroti statistiniai duomenys apie saugumo incidentus, tenkančius skirtingoms kompiuterių sistemoms;
- Kompiuterių sistemos saugumo modeliavimo rezultatai.

Darbo apimtis. Darbą sudaro bendra darbo charakteristika, 4 skyriai, išvados, iliustracijų sąrašas, lentelių sąrašas, santrumpų sąrašas, simbolių ir kintamųjų sąrašas, literatūros sąrašas ir publikacijų sąrašas. Disertacijos teksto apimtis – 125 puslapiai, 44 iliustracijos, 17 lentelių ir 198 bibliografiniai šaltiniai.

Pirmajame skyriuje pateikta tirtų saugumą aprašančių standartų ir saugumo modelių analizė leido suformuoti darbo uždavinius.

Antrajame skyriuje, įvertinant poveikį buvo suklasifikuos atakos, naudojant grafų teoriją analizuotos tipinės atakos, surinkta ir apdorota saugumo incidentų statistika.

Trečiajame skyriuje tirtos egzistuojančios kompiuterių sistemų apsaugos priemonės bei saugios architektūros. Eksperimentiškai tirtas naudotų saugumo mechanizmų efektyvumas.

Ketvirtajame skyriuje naudojant gautus rezultatus buvo atliekamas kompiuterių sistemos saugumo įvertinimas. Kaip parodė atlikta analizė absoliutus kompiuterių sistemos saugumas nėra įmanomas, kompiuterių sistema turi dirbti toleruodama saugumo pažeidimus, todėl saugumo įvertinimui labiausiai tinkama yra statistinė išliekamumo charakteristika. Parinkus tinkamą formalų metodą buvo atliktas kompiuterių sistemos išliekamumo modeliavimas.

Galutinės išvados

1. Darbe pasiūlyta kompiuterių sistemos atakų klasifikacija tinka eksperimentinių duomenų klasifikavimui. Ja siekiama apimti visus kompiuterių sistemos atakai būdingus bruožus. Klasifikacija gali būti lengvai plečiama ir leidžia įvertinti naujus atakų bruožus, kurie atsiras ateityje. Labiausiai tikėtinas naujų poveikio tipų, naujų operacinių sistemų, objekto aplinkų ir paslaugų atsiradimas. Kompiuterių sistemos saugumo modeliavimui reikalingą atakų sunkumo įvertinimą galima atlikti naudojantis pasiūlyta atakų klasifikacija pagal poveikio tikslą. Taip pat galima įvertinti, kuri grėsmė kompiuterių sistemos saugumui yra aktualiausia. Grafų teorija modeliuojant kompiuterių sistemą galima vaizdžiai ir efektyviai atvaizduoti ir analizuoti atakų mechanizmus.
2. Vertinant incidentų skaičių, tenkantį kompiuterių sistemai, tikslinga įvertinti ne tik tyrimo laiką, bet ir kitus kompiuterių sistemos parametrus: vartotojų skaičių bei ryšio kanalo su incidentų šaltiniu pralaidą. Išanalizavus incidentus, tenkančius trijų skirtingų organizacijų kompiuterių tinklams, pastebėta, kad vidutinis incidentų skaičius INC_{vid} yra tuo mažesnis, kuo didesnis dėmesys ir investicijos, skiriamos kompiuterių sistemos apsaugai. Tolesnė

incidentų analizė parodė, kad sunkiausių incidentų kiekis yra mažiausias; daugiausia siekiama realizuoti grėsmes, kylančias konfidencialumui ir pateikiamumui; daugiausia skirtingų atakų vyksta TCP protokolu, mažiausia – UDP protokolu; ICMP protokolu vykstančių incidentų kiekis yra didelis, kadangi, siekiant apeiti saugumo politiką ir sukelti atsisakymą aptarnauti, paplitę automatizuotos atakos.

3. Norimo lygio saugumo užtikrinimas kompiuterių sistemoje galimas tik įdiegus visą apsaugos priemonių kompleksą ir jau sistemos kūrimo metu įvertinant jos funkcionavimo niuansus, susijusius su saugumu. Išanalizavus egzistuojančias kompiuterių sistemų apsaugos priemones pastebėta, kad maksimalus saugumo lygis gali būti pasiekiamas tik tada, kai saugumas laikomas organizacine problema ir imamasi organizacinių priemonių: atliekama grėsmių analizė, sudaroma saugumo politika ir įdiegiami visi saugumo politikos įgyvendinimui reikalingi saugumo mechanizmai. Saugumo mechanizmus išdėstyti daugiausia galimybių yra programiniame OSI lygmenyje. Transporto lygmenyje saugumo mechanizmai efektyviausi apsaugant informacijos srautą per nesaugią terpę, o kanalo lygmenyje – apsaugant prieigą.

4. Atakų atpažinimo sistemos „Snort“ tyrimas parodė, kad ji, naudodama pradinę konfigūraciją, teisingai atpažįsta daugiau nei 70 % visų incidentų. Daugiausia neteisingų atpažinimų buvo dėl incidentų, vykusių ICMP protokolu (43 %). Iš tirtų grafinių aplinkų incidentų analizei tinkamiausia yra „BASE“ aplinka.

5. Naudotas „Checkpoint NGX“ tarpsegmentinis ekranas sulaikė 64 % visų incidentų. Efektyviausias buvo programinio lygmens tarpinio šliuzo komponentas, blokavęs incidentus, nukreiptus į žiniatinklio, SMTP ar kitas konkrečias tinklo paslaugas, dėl to TCP protokolu vykusių incidentų sulaikymas buvo geriausias (90 %). Tirtas TE sunkiausius incidentus blokavo efektyviausiai (92 %). Šiuo atveju apsauga nuo grėsmės konfidencialumui buvo geriausia (87 %).

6. Kompiuterių sistemų saugumą galima vertinti procedūriškai, ekonominiu požiūriu ar pagal jų statistines charakteristikas. Modeliavimui tinkamiausias yra statistinis įvertinimas. Pasiūlyta kompiuterių sistemų saugumo įvertinimo metodika susideda iš poveikio analizės, sistemos modelio sudarymo, modeliavimo naudojant SAN modelį ir gautų išliekamumo charakteristikų analizės. Modeliavimo metu gauti rezultatai rodo, kad teisingos pradinės konfigūracijos ir atsparios architektūros sistemos lengvi incidentai nepaveiks net tada, jei ji neturės apsaugos mechanizmų.

7. Pagal pasiūlytą saugumo įvertinimo metodiką gauta išliekamumo priklausomybė nuo apsaugos mechanizmų stiprumo, kuris nurodomas sąlygine jų kaina. Iš kompiuterių sistemos išliekamumo priklausomybės matyti, kad

išliekamumas tuo geresnis, kuo lengvesnės atakos. Apsaugos mechanizmų kainai didėjant išliekamumas pradžioje auga sparčiau. Maksimalus išliekamumas I_{max} labiausiai priklauso nuo apsaugos mechanizmų kainos ir tinka vertinti vienalytę sistemą, o sistemos išliekamumas I – sudėtingą sistemą.

Trumpos žinios apie autorių

Eimantas Garšva gimė 1977 m. rugpjūčio 23 d. Vilniuje.

1999 m. įgijo elektros ir elektronikos inžinerijos bakalauro laipsnį Vilniaus Gedimino technikos universiteto Elektronikos fakultete. 2001 m. įgijo elektronikos inžinerijos mokslo magistro laipsnį Vilniaus Gedimino technikos universiteto Elektronikos fakultete. 2002–2006 m. – Vilniaus Gedimino technikos universiteto doktorantas. Šiuo metu dirba asistentu Vilniaus Gedimino technikos universiteto Kompiuterių inžinerijos katedroje.

Eimantas Garšva

MODELLING OF COMPUTER SYSTEM SECURITY
Summary of Doctoral Dissertation
Technological Sciences, Electronics and Electrical Engineering (01T)

Eimantas Gašva

KOMPIUTERIŲ SISTEMŲ SAUGUMO MODELIAVIMAS
Daktaro disertacijos santrauka
Technologijos mokslai, elektros ir elektronikos inžinerija (01T)

2006-11-29. 1,5 sp. l. Tiražas 100 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“, Saulėtekio al. 11, 10223 Vilnius
Spausdino UAB „Biznio mašinų kompanija“,
J. Jasinskio g. 16 A, 01112 Vilnius