ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2012. No. 4(120)
ELEKTRONIKA IR ELEKTROTECHNIKA

T 120 SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Survivability Modelling of Lithuanian Government Information System

N. Paulauskas, E. Garsva, L. Gulbinovic, A. Stankevicius, D. Poviliauskas
Department of Computer Engineering, Vilnius Gediminas Technical University,
Naugarduko g. 41, LT – 2600 Vilnius, Lithuania, phone +370 5 2744767, fax +370 5 2627730,
e-mails: nerijus.paulauskas@el.vgtu.lt, eimantas.garsva@el.vgtu.lt, gulbinovic@gmail.com,
arvydas.stankevicius@el.vgtu.lt, darius.poviliauskas@gmail.com

crossref http://dx.doi.org/10.5755/j01.eee.120.4.1463

Introduction

Information systems provide critical services in nearly all the areas of life. Services must be provided in a secure and reliable manner. The targeted security and availability characteristics are defined in security policy or the formal regulations. The main part of the information system is a computer system which is addressed in this research.

Survivability characteristic is suitable for the information system security evaluation [1–4] and will be used in this research. Stochastic computer system model was composed and investigated using Möbius tool. The information systems of different category were simulated and the obtained results were analyzed.

Computer system security regulation

Lithuanian government information systems are well regulated and will be addressed in this research. According to orders of the Minister of Interior of the Republic of Lithuania information systems are categorised based on their vitality for the state [5] and the requirements to the system recovery time and accessibility are set [6]. These requirements are summarised in Table 1.

Table 1. Requirements to the Lithuanian government system accessibility and recovery time

Category	System recovery time	System accessibility	Number of subsystems
I	15 min	99%	7
II	1 h	96%	5
III	8 **wh**	90% **wd**	3
IV	16 **wh**	70% **wd**	2

Note: ***wh*** *– working hours,* ***wd*** *– working days*

The requirements for first and second system categories are very high and system recovery time should be no longer than 15 minutes for first category and 1 hour for second category. The system accessibility is set to 99 percent for first and 96 percent for second category. The requirements for third and fourth system categories are set only for working hours and working days. Also each category has no less than a specified number of subsystems (Table 1). Requirements to major security mechanisms, which must be implemented for each category, are different. Every higher category system must have additional security mechanisms alongside security mechanisms which are specified for lower category systems.

Four information system models were composed according to the requirements presented in Table 1. The creation of models and simulation results are presented in the following sections.

Simulation model

This simulation addresses one aspect of information security – computer network risks rising from the outer perimeter of the computer system.

Structure of computer system model is presented in Fig. 1. Incidents are grouped by the threats to confidentiality, integrity and availability and have different severity levels (j) – high ($j = 1$), medium ($j = 2$) and low ($j = 3$).

Incidents are independent and occur by exponential law targeting the specific module (m) (subsystem) of the modelled computer system considering its rate of use, which is expressed as module usage probability ($P_M(m)$).

All the system modules are protected by the security mechanisms (N_m) regulated by the law [6]. Computer system modules have different importance which is represented by its weight ($w(m)$). After the incident, computer system's module is compromised or not, by that affecting the state of the whole system.

Probability that the systems degradation will be detected at zero time is very small, but when the period of time after the system was compromised is getting longer the incident detection probability rises. We made an assumption, that incident detection probability is linear and

distributed according to triangular law. In this case, the time, when one of the system modules is compromised but incident is not detected, may vary from zero to upper bound of triangular distribution. This time corresponds to the situation, when compromised module is accessible and may provide inadequate service for the system's users. Therefore it is important to minimise incident detection time as much as possible.

According to the same assumptions, triangular distribution for system recovery time is used, i.e. module recovery probability rises, when time period after incident detection is getting longer. During recovery time compromised module is not accessible by the users. The average system recovery time must satisfy the requirements presented in Table 1.

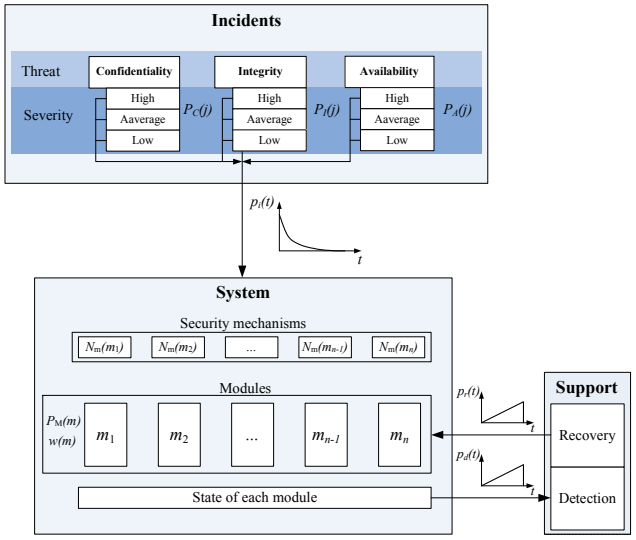


Fig. 1. Structure of computer system model

Four computer system simulation models (one model per system category) were composed using Stochastic Activity Network (SAN) formalism. Simulation models are organised using Möbius tool [7], where models design repeats the block diagram presented in Fig. 1. The detailed SAN model description can be found in our previous work [8], where one system category was presented using SAN model and model parameter values were determined by risk analysis. In this work a new approach is presented. It allows to find the system compromise probabilities and apply them to simulate computer system survivability. Each model has different number of modules (subsystems): first category has 7 modules; second category has 5 modules, third category has 3 modules and fourth category has 2 modules.

System compromise probabilities

To simulate system survivability we need to know system compromise probabilities, i.e. the probabilities that particular incident will compromise a system. These probabilities depend on incident severity and the amount of implemented security mechanisms. The best way to do this is to collect an accurate statistical data about incidents during some tangible time period. But in many cases this statistical data is not available, e.g. system is in development stage or is just implemented. We suggest to use some theoretical characteristics of the system compromise probability for this purpose.

Fig. 2 shows the characteristics which represent how the system compromise probabilities depend on the amount of implemented security mechanisms. There are three characteristics, each for different incident severity level. First one is most severe. That means, that compromise probability is higher when incidents are more severe.

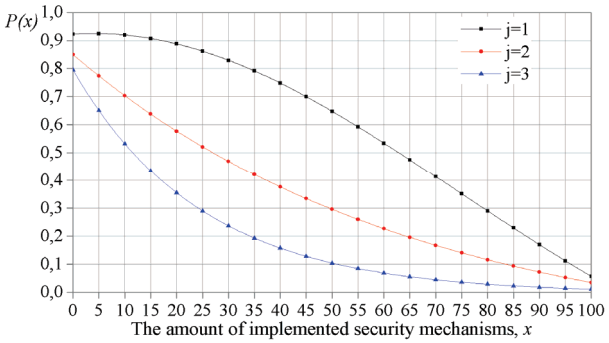


Fig. 2. The dependence of computer system compromise probability ($P(x)$) characteristics on the amount of implemented security mechanisms (x)

Compromise probability curves were drawn based on these hypotheses:

- The amount of basic security mechanisms must be higher to withstand the most severe incidents;
- If incidents are less severe, then less of security mechanisms are enough;
- When little or no mechanisms are used, the influence of all severity incidents are almost the same, as even least sever incident will compromise the system;
- When all possible security mechanisms are implemented, the influence of all severity incidents are almost the same, as even the most sever incidents will be repelled.

The formulas which satisfy the curves in the Fig. 2 (where $\beta_{Th} = 0$ and $\alpha_{mi} = 0$) are:

$$P(x)_{j=1} = \left(\frac{25}{7\sqrt{2\pi}} \cdot e^{-\frac{\left(x-4+\alpha_{m_i}\right)^2}{9800}} \right) - 0.5 + \beta_{Th}, \qquad (1)$$

$$P(x)_{j=2} = \left(1.05 \cdot e^{-0.015 \cdot \left(x+\alpha_{m_i}\right)} \right) - 0.2 + \beta_{Th}, \qquad (2)$$

$$P(x)_{j=3} = \left(0.8 \cdot e^{-0.04 \cdot \left(x+\alpha_{m_i}\right)} \right) - 0.004 + \beta_{Th}, \qquad (3)$$

here x – the amount of implemented security mechanisms [0–100]; β_{Th} – coefficients for assessing the threat type (β_C – confidentiality, β_A – availability, β_I – integrity); α_{mi} – coefficients for assessing modules ability to withstand incidents.

These formulas were used in simulation to find out the exact values of compromise probabilities. Threat type is evaluated using β_{Th} coefficients. These coefficients

represent the security mechanism ability to deal with specific threat and may have positive or negative values. For example, if particular security mechanism is more suitable to secure module from confidentiality threats than integrity threats, when β_C coefficient will have negative value (lower compromise probability) and β_I coefficient will have positive value (higher compromise probability).

The system modules ability to withstand incident is different from module to module. This difference is evaluated using the α_{mi} coefficients, which also may have positive or negative values. If module is more important to whole system (this is represented by module weight *w(m)*) when implemented security mechanisms are adjusted more accurate, this means that α_{mi} coefficient for this particular module will be positive, i.e. the system compromise probability will be lower. Proposed formulas allow adopt system compromise probabilities based on threat type, incident severity and security mechanisms set. Also these formulas can be easily modified to fit the needs of real computer system.

Simulation Results

Survivability is the quantitative security characteristic of computer system. Survivability is the degree to which a system has been able to withstand an attack or attacks, and is still able to provide services at a certain level in its new state after attack.

When service or the system survives in the maximal functional state b_1 (where b_2, b_3,…, b_n other states, when one, two or more system's modules are compromised) during the system usage time Δt_{all}, then such characteristic can be called maximal survivability S_{max}

$$S_{max} = \frac{\Delta t_{b1}}{\Delta t_{all}}. \quad (4)$$

Namely the maximum system survivability was addressed in this research. Survivability characteristics were found by averaging time which system's modules spend in not compromised state.

Different services or modules providing these services represent different importance to the mission of the system, this must be considered. When survivability of the system *S* can be described as:

$$S = \sum_m w(m)S(m), \quad 0 \le S(m) \le 1, \quad (5)$$

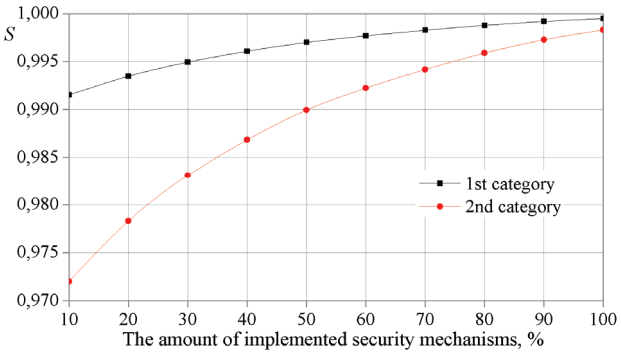
$$\sum w(m) = 1, \quad 0 \le w(m) \le 1, \quad (6)$$

here *S(m)* is the survivability of computer system module *m*, and *w(m)* is the weight of the module.

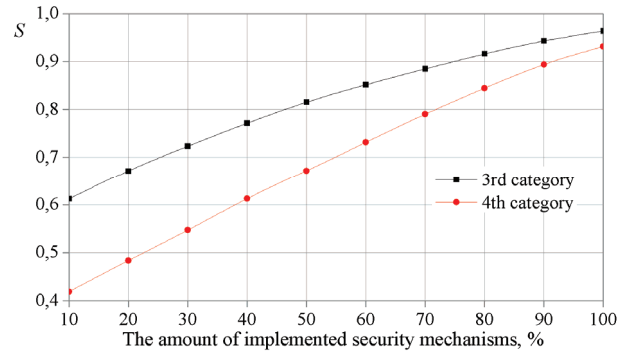
The main parameter values used in simulation are provided below:

- The simulation time period is 365 days, i.e. 1 year.
- Computer system faces 3 incidents per day. Incidents are independent and distributed exponentially.
- Incidents appearance probabilities:
  - *Confidentiality* – P_C(j=1)=0.04, P_C(j=2)=0.1, P_C(j=3)=0.2;
  - *Integrity* – P_I(j=1)=0.01, P_I(j=2)=0.05, P_I(j=3)=0.1;
  - *Availability* – P_A(j=1)=0.1, P_A(j=2)=0.1, P_A(j=3)=0.3.

$\sum P_C(j) + \sum P_I(j) + \sum P_A(j) = 1$. These values are hypothetical and were chosen only for simulation purposes. Incidents appearance probability values were chosen based on the following considerations. Attack on the computer system data integrity is most complicated one, because the attacker must gain access to the system, elevate access rights, find needed data, perform manipulations and hide the tracks. Therefore, appearance probability values of integrity incidents are the lowest ones. Finding confidential information is easier, the information also can be leaked accidentally. Those two types of the attacks require the knowledge and the experience of the attacker. To perform denial of service attack disturbing computer system availability is the least complicated as the Botnets for the attack can be leased, scripts and tools to perform such attack are widely available. Therefore, availability incident appearance probabilities are the highest.



a)



b)

Fig. 3. The dependence of computer system survivability characteristics on the amount of implemented security mechanisms: a) 1st and 2nd system categories, b) 3th and 4th system categories

The computer systems of the 1st and 2nd category were designed with higher accessibility requirements, therefore survivability characteristics (Fig. 3a) obtained by simulation are higher and less depend on the amount of implemented security mechanisms.

The influence of security mechanisms is small for a 1st category system, but if we express the survivability

value in days we will see that the difference is 2.9 days between the least and the most security mechanisms installed. As we know the requirements of information accessibility for 1st category system is 99 percent. So 2.9 days is a tangible value. This small difference can be explained considering model characteristics. The system recovery time during simulation was kept constant. Even when the amount of implemented security mechanisms was small, the system recovery time remained high. The next our step will be to implement the relation between security mechanisms and system recovery time.

We cannot compare 1st and 2nd category systems with 3rd and 4th category systems because there are different requirements. The information accessibility requirements of 3rd and 4th category systems are only for working days, therefore the information accessibility requirements for 1st and 2nd category systems are for all days a year. Fig. (Fig. 3b) shows the survivability simulation results of 3rd and 4th category systems. We can see that survivability characteristics of these category systems are more linear than survivability characteristics of 1st and 2nd categories. It means that survivability of 3rd and 4th category systems are more depend on implemented security mechanism.

Conclusions

1. The suggested model allows us evaluating system survivability based on threat type, incident severity and the amount of implemented security mechanisms. The model is flexible, expandable and can be adapted to other computer systems.

2. The computer systems of the 1st and 2nd category were designed with higher accessibility requirements, therefore, survivability characteristics obtained using simulation depend less on the security mechanisms and are better.

3. Simulation shows that the difference between the least and the most security mechanisms installed is: for 1st category system – 2.9 days, 2nd category system – 9.5 days, 3rd category system – 128 working days, 4th category system – 187 working days.

4. The results of simulation show that compromise detection period depends on the amount of implemented security mechanisms. Existence of zero day exploits suggests that there is a probability that when such exploit is available even best protected system can be compromised. This will be evaluated in the future research.

References

1. **Moitra S. D., Konda S. L.** A Simulation Model for Managing Survivability of Networked Information Systems. – 2000. Online: www.cert.org/research/00tr020.pdf.
2. **Moore A. P., Ellison R. J., Linger R. C.** Attack Modeling for Information Security and Survivability. – 2001. Online: www.cert.org/archive/pdf/01tn001.pdf.
3. **Garšva E.** Computer system survivability modeling // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 1(65). – P. 48–51.
4. **Garšva E.** Computer System Survivability Modelling by Using Stochastic Activity Network // SAFECOMP'06, 2006. – Vol. 4166. – P. 71–84.
5. **Clasification Guidelines for Goverment Institution and Office Information Systems according to the Processed Electronic Information.** Order of the Minister of Interior of the Republic of Lithuania. 2007–07–11. – No. 1V–247. – Official Gazette, 2007. – No. 78–3160.
6. **Requirements to Technical Security of Goverment Institution and Office Information Systems.** Order of the Minister of Interior of the Republic of Lithuania. 2008–10–27. – No. 1V–384. – Official Gazette, 2008. – No. 127–4866.
7. **Sanders W. H.** Möbius: model–based environment for validation of system reliability, availability, security, and performance. – Möbius Manual Version 2.3.1, 2010. Online: https://www.mobius.illinois.edu/manual/MobiusManual.pdf.
8. **Garšva E., Paulauskas N., Gulbinovič L., Stankevičius, A.** Computer System Survivability Evaluation Based on Risk Analysis // Information Systems Architecture and Technology. – Web Information Systems Engineering, Knowledge Discovery and Hybrid Computing Networks. – Wroclaw, 2011. – P. 291–301.

Received 2011 11 15
Accepted after revision 2012 01 24

N. Paulauskas, E. Garsva, L. Gulbinovic, A. Stankevicius, D. Poviliauskas. Survivability Modelling of Lithuanian Government Information System // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 4(120). – P. 95–98.

This paper presents a new approach which allows us to find the system compromise probabilities and applying them to simulate computer system survivability. Also, four computer system survivability simulation models were composed and according to requirements for recovery time and accessibility of Lithuanian government information systems computer system survivability simulations were performed. Simulation models were composed using Stochastic Activity Network (SAN) formalism. Presented model allows evaluating system survivability based on threat type, incident severity and the amount of implemented security mechanisms. The model is flexible, expandable and can be adapted to other computer systems. Ill. 3, bibl. 8, tabl. 1 (in English; abstracts in English and Lithuanian).

N. Paulauskas, E. Garšva, L. Gulbinovič, A. Stankevičius, D. Poviliauskas. Lietuvos valstybės institucijų ir įstaigų informacinių sistemų išliekamumo modeliavimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 4(120). – P. 95–98.

Straipsnyje aprašomas naujas metodas, leidžiantis rasti kompiuterių sistemos sukompromitavimo tikimybes ir panaudoti jas kompiuterių sistemos išliekamumui modeliuoti. Tuo tikslu yra sudaryti keturi kompiuterių sistemų išliekamumo imitaciniai modeliai, įvertinantys Lietuvos valstybės institucijų ir įstaigų informacinių sistemų atkūrimo trukmės ir prieinamumo reikalavimus, ir atlikti imitaciniai šių sistemų išliekamumo skaičiavimai. Imitaciniai modeliai buvo sudaryti naudojant stochastinių veiklos tinklų (angl. *Stochastic Activity Network* – SAN) formalizmą. Pasiūlytas metodas leidžia įvertinti kompiuterių sistemų išliekamumą pagal grėsmių tipą, incidentų sunkumo laipsnį ir įdiegtų apsaugos mechanizmų skaičių. Metodas yra lankstus, lengvai plečiamas ir pritaikomas įvairių kompiuterių sistemų išliekamumui modeliuoti. Il. 3, bibl. 8, lent. 1 (anglų kalba; santraukos anglų ir lietuvių k.).