A SHORT NOTE ON RELIABILITY OF SECURITY SYSTEMS

Jóźwiak Ireneusz J., Laskowski Wojciech

Wroclaw University of Technology,
Wroclaw, Poland

Keywords

computer security, reliability, computer incidents

Abstract

Telecommunication systems become a key component of critical infrastructure. One of the main elements of such systems is computer system. The organizations which can be involved in crisis management (e.g. government agencies, etc.) need to know results of security drawbacks in their systems. Moreover, they should have a tool for analysing the results of decision made in security context. And often the following question is raised: why do security systems fail? To answer it in this paper the aspects of reliability are discussed. From this point of view the security systems are analysed. We hope that thanks to such approach we will be able to reach some characteristics of security incidents occurrence. Moreover, we hope to use our results to build security attributes metrics. In addition, we present thesis that predictions of occurrence of incidents is impossible, so we should focus on registration of incidents type. On such a foundation we can formulate conclusions about drawbacks in configurations or administration of information systems. In our research we have observed that in case of some class of information systems, the availability incidents are the most dangerous. And we conclude that only using technologies with good reliability characteristics can lead to solving this problem.

1. Introduction

The problem of reliability of security systems were discussed by Anderson in several publications e.g. [1] or [2]. Another example is paper [11] where system reliability is viewed from game theoretical perspective and this work can be easily applied to security domain. One of the most popularised practical models of security systems is so called 'defence-in-depth' model [3]. Taking into consideration such a model it can direct our attention into basic models of system reliability: serial or parallel systems [4], [7]. Many components of security systems can be characterized by one of the above-mentioned structures. For example, access control subsystem, firewall, IDS and antivirus software can be considered as a mixed structure (*Figure 1*) with three serial elements and one element parallel to this structure.

Using reliability techniques influence security systems. A good example is a problem of placing IDS in redundant networks [10]. Another example is operating systems. Very large number of modules, software

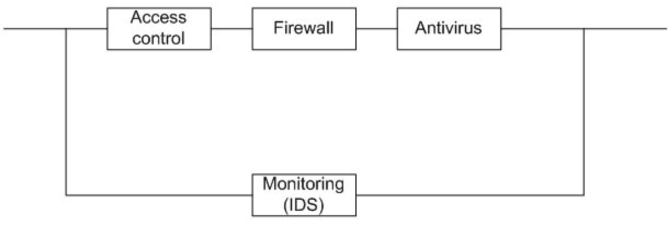

Figure 1. The scheme of a typical security system – an example

applications or services induce many security problems. There are many areas when security vulnerabilities are present, e.g. authorization subsystem, remote services etc. There is a set of security holes, which can be viewed as a serial or parallel structure (in basic reliability models sense). In this paper we present some empirical data from our research connected with analysing incidents connected with security of information systems.

2. Security incidents

In some period of the time (approximately 2 years) we have focused on observation of tree kinds of security systems. These systems (the models are presented in fig. 2) can be characterized as follows:

1. System A – a stand-alone system, not connected to any network, an access to this system is limited to a small number of users.
2. System B – specialized networked system, separated from public networks (several workstations)
3. System C – system networked, connected to public operators network (dozen workstations)

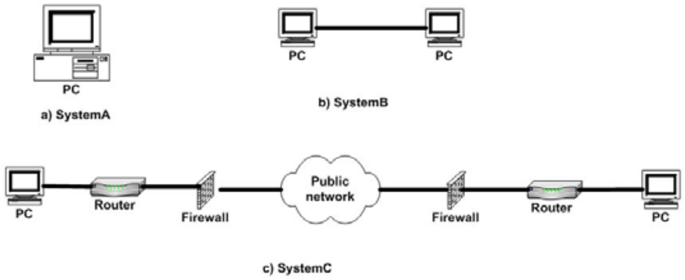

Figure 2. The models of observed information systems

The physical structures of these systems are less important for our research. Moreover, the size, role and localization of these systems are intended not to be mentioned at this time. Taking into consideration of three attributes of information: confidentiality, integrity and availability these systems were observed in order to notice specific incidents: virus incidents in System A and System C and availability incidents in case of System B. The availability incidents we understand as the breaks in proper working the system, e.g. lack of communications or servicing the elements of network infrastructure. The preliminary results are presented in *Table 1.*

Table 1. The number of observed incidents

Type of system	Number of virus incidents	Number of availability incidents	Period of observations
System A	2	----	1 year
System B	----	137	2 years
System C	41	----	1,5 year

In case of System A we noticed two different kinds of macro viruses [12]. The virus incidents in System C were connected with worms (mainly from Sasser 'family'), trojans or loggers [12]. The most interesting observations are connected with System B. Over 130 incidents were noticed. So some kind of reliability analysing methodology was used in order to describe the characteristics of events in this system. We are interested in mean time between incidents and frequencies of incidents.

3. Analysis of incidents

The preliminary results are presented in *Table 2* and in the *Figures 3,4,5*.

These pictures present number of incidents and its length and time periods between incidents. In case of System B we are focused on general number of incidents and time between incidents (*Figure*.)

Table 2. A comparison of mean values and standard deviations of data about incidents

Type of system	Mean time between incidents [day]	Standard dev.of time between incidents [day]	Mean time of incident [min]	Standard dev.of time of incident [min]
System B	5,25	7,30	129,48	184,77
System C	11,90	16,54	---	---

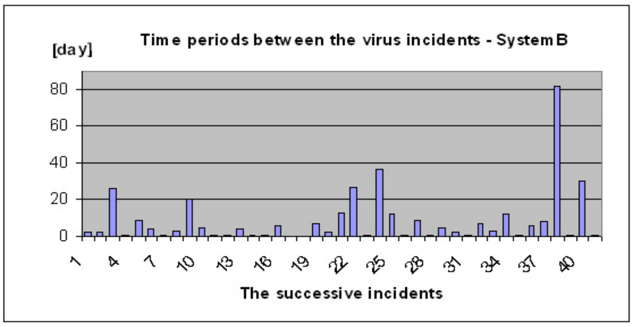

Figure 3. Graphical representation of observed length of time periods between incidents. System C.

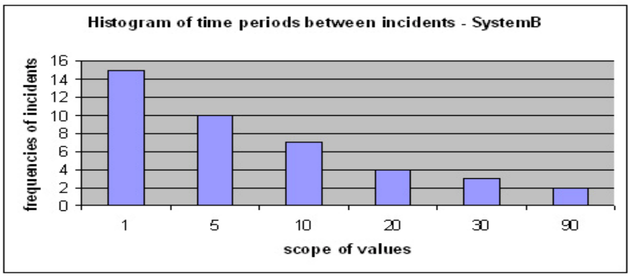

Figure 4. Histogram of observed time between the virus incidents. System C.

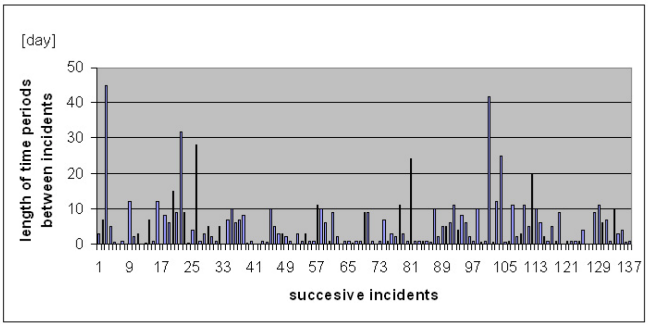

Figure 5. Graphical representation of observed length of time periods between incidents. System B.

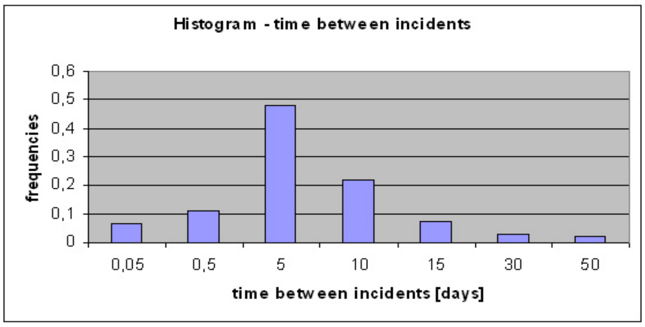

Figure 6. Histogram of observed time between the availability incidents. System B.

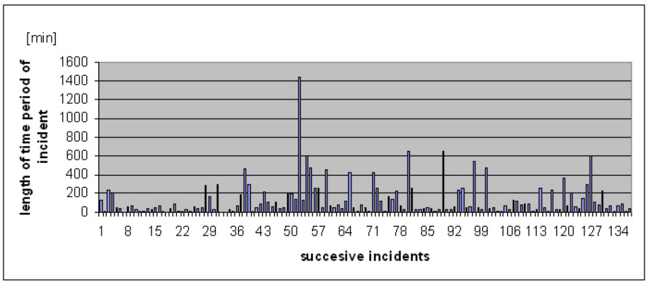

Figure 7. Graphical representation of observed length of time periods of availability incidents. System B.

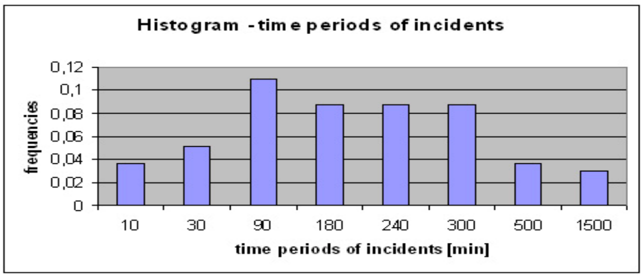

Figure 8. Histogram of observed time periods of availability incidents. System B.

The basic statistical analyses were done in order to notice the frequencies of incidents and derive empirical distributions.

In case of SystemB and virus incidents, the occurring the events has characteristic presented in figure 4.

In case of System C and availability incidents, the characteristics presented in fig. 6 and 7 were derived.

4. Reliability of security systems

When security of information systems is considered it is needed to analyse three attributes: confidentiality, availability and integrity. According to reliability theory, one of the key measures is probability of failures or time between failures. When it comes to security systems there is a lack of such metrics. In general security can be seen as a subjective category. So it is very difficult to find adequate metrics or measures of security attributes. But it seems that reliability context and analogies should be helpful. Another problem is if such metrics can be helpful in decision taking during ensuring security process. It seems that measuring security is impossible or at least possible in very limited scope. In authors' opinion every techniques which can be utilized to limit uncertainty during decision taking (in computer security domain) is worth considering.

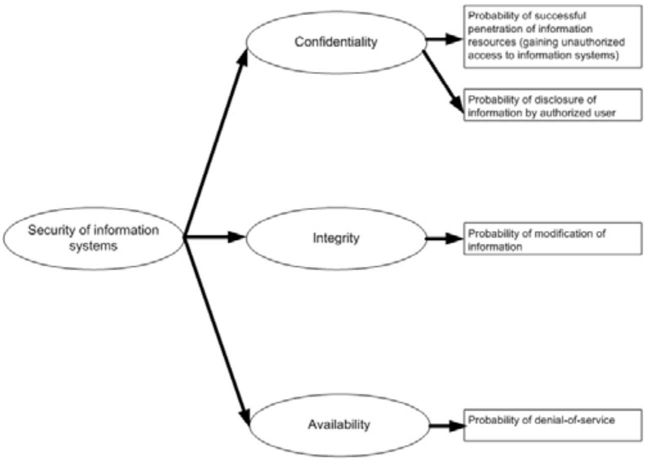
Security of information systems
Confidentiality
Integrity
Availability
Probability of successful penetration of information resources (gaining unauthorized access to information systems)
Probability of disclosure of information by authorized user
Probability of modification of information
Probability of denial-of-service

Figure 9 . Metrics for security attributes analysing

The observation done by authors can be helpful in analysing first of all aspects of availability. Looking for the distribution of probability of occurring incidents we can observe shape the distribution presented in *Figure 10* and *Figure 11*.

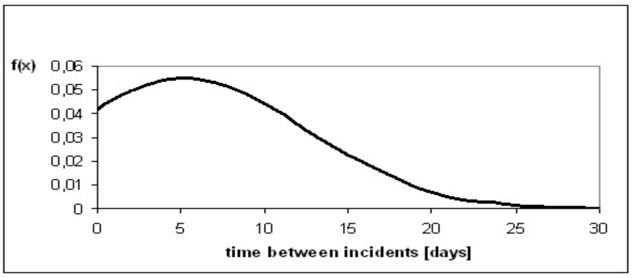

Figure 10. Probability distribution of observed time between the availability incidents. System B.

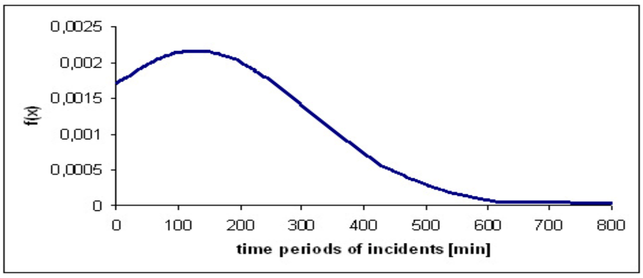

Figure 11. Probability distribution of observed time periods of availability incidents. System B.

The main conclusion from this preliminary analysis is that the most probable time between incidents is from range 0,01 to 1 day. It means that in the case of this system, the attention of operators should be focused first of all on control transmission links and devices. When it comes to virus incidents our observation proves that supervising the system should be done every day (the shape of characteristic in

Figure 4 shows that occurrence of incidents more often than one incident per 5 days period is possible with high probability).

The availability incidents' distributions were presented in fig. 10 and *Figure 11*. Expected time period of availability incidents is approximately 2 hours.

The reliability of security systems is connected with proper implementation of software and hardware components of security systems. The flexible and easy in realization reconfigurable hardware elements can be used. This problem was discussed and presented e.g. in [8] or [6]. Using reconfigurable hardware can significantly increase reliability e.g. cryptographic systems. What is more the speed of transmitting data are very important parameters. For example, the results of implementation of cryptographic device CRYPTON [12] is presented in *Table 3*.

5. Conclusion

Our observations proof the thesis that collecting data for analysing security is a very complex practical problem.

Table 3. The chosen parameters of reconfigurable device CRYPTON [12]

Device	Reconfigurable device CRYPTON
Clock period [ns]	52
Frequency [MHz]	19,2
Encryption (decryption) speed [Mb/s]	203,2
Time to encrypt (decrypt) one data block [ns]	630
Number of encryption (decryption) per second	1 587 301

What is more, the analysing of these data needs new more accurate methods. This is a general problem of IDS systems. Many methods of artificial intelligence are used in this domain, e.g. machine learning, data mining or neural networks. Exploring the data for discovering dependencies connected with incidents is a real and still open problem. We face some kind of paradox: we either a huge number of data and have problems with its exploring or we suffer from lack of accurate data. This problem can be noticed when a need for a fast assessing of security incidents takes place. In such a situation very often fast decision is needed: is this an incident or not? We still do researches connected with developing a new method for security assessment. Our method is based on preliminary preparation of data for scaling early intrusion detection systems using simulation. And in this method we need some characteristic connected with frequencies of incidents presented in the paper. In many elements our analysis is very similar to reliability analysis. We are focused on answering the questions: why do the security systems fail? And this is the key direction of constructing our method: finding the cause – effect dependencies in incident analysis in order to induce the rules for IDS systems. The first element of these observations is to notice how often the incidents take place.

As far as reliability of security system is concerned it is worth underline the wide spectrum of threads, which should be considered. One of these subjects is implementing hardware devices using high speed and characterized by good reliability characteristic technology.

The occurrence of computer incidents is rather unpredictable. It is very hard to reach characteristics like probability distributions. Institutions do not publish data about incidents. We can only collect own data or gather data from other sources, like CERT (Computer Emergency Response Team). Other solution is preparing data using simulation.

To conclude we can say that only implementing heterogeneous environments with combination of software and hardware, commercial and open source components can lead to ensuring a good level of reliability. And consequently in such a way we can increase level of security of information systems.

References

[1] Anderson, R. (1993). Why Cryptosystems Fail. *1st Conference on Computer and Communication Security*. VA, USA.

[2] Anderson, R. (2001). Security engineering. *A Guide to Building Dependable Distributed Systems.* John Wiley & Sons Inc.

[3] Hazlewood, V. (2007). Defense-in-depth. An Information Assurance Strategy for the Enterprise, San Diego 2006, (http://security.sdsc.edu/DefenseInDepthWhitePaper.pdf, February 2007)

[4] Jóźwiak, I.J. (1992). The reliability and functional model of computer network with branched structure. *Microelectronics and Reliabilit.* Vol. 32, nr 3, 345-349.

[5] Jóźwiak, I.J. (1996). The failure time random variable modeling. *Microelectronics and Reliability*. vol. 36, 10, 1525-1529.

[6] Jóźwiak, I. & Laskowski, W. (2003). Reconfigurable hardware and safety and reliability of computer systems. *Risk Decision and Policy Journal*. Philadelphia.

[7] Kołowrocki, K. (2004). *Reliability of Large Systems.* Amsterdam-Boston-Heidelberg-London-New York-Oxford-Paris-San Diego-San Francisco-Singapore-Sydney-Tokyo, Elsevier.

[8] Laskowski, W. (2001). Układy programowalne jako narzędzia wspomagające kryptograficzną ochronę danych. *Przegląd Telekomunikacyjny* 3, 178-183.

[9] Liderman, K. (2003). *A guide for security administrators.* Warszawa (in Polish).

[10] SANS Institute, Intrusion detection FAQ. (2007). (on line: http://www.sans.org/resources/idfaq).

[11] Varian, H. (2002). *System reliability and free riding*. Workshops on Economics and Information Security. Berkeley, (on line: http://citeseer.ist.psu.edu/527418.html).

Virus Encyclopedia, CA. (2007). (http://www3.ca.com/securityadvisor/virusinfo/browse.aspx).