MODEL OF THREATS IN INFORMATION NETWORKS

***Robbins, J. G.*[1*], *Rolf Jergman*[2]**

1The City University of New York, Kingsborough, USA
2University of Sfax, Tunisia
** Corresponding author: serchre43an@gmail.com*

Abstract

In years based on a fairly detailed analysis of many possible threats [4-9], an example and method of building their model is given, which is a step in determining the set of necessary means of protecting information objects of the corresponding distributed computer network (ROM) and building protection systems. However, the model proposed in [3] does not answer the question of the mechanisms of implementation of each of the many possible threats, and therefore does not specify the composition of such protection systems. Therefore, a more advanced version of the threat model is proposed below. In this model, as in [3], the security features of information objects that may be violated are defined - confidentiality (k), integrity (c), accessibility (e) and qualitative assessment of the probability of threats and levels of damage (harm) to each of the types of violations.

Kewords:

Possible threats, computer, network, mechanisms, model .

Introduction

As in previous materials, the method of developing such a model is that in one of the columns of the table is entered as complete a list of types of threats; in the given example such list is given in column 2. Further for each of possible threats by their analysis (possibly also by a method of expert estimations) it is necessary to define:

1 . The likelihood of such threats. Qualitative estimates can be used as the first step in determining such a probability. The table can provide qualitative estimates

of their probability unacceptably high, very high, high, significant, medium, low, neglected low (column 3);

2. Violation of which functional properties of information security (column 4) it is aimed at (violation of confidentiality k, integrity ts, accessibility d);

3. Possible (expected) level of damage (column 5). An example of this assessment is also given on a qualitative scale (absent, low, medium, high, unacceptably high). The presence of such assessments, even on a qualitative scale, allows to justify the need to provide means of protection of each of the security features of information;

4. Mechanisms of realization (possible ways of realization) of threats (column 6).

Threat model in ROM

№	Type of threats	Probability	What breaks	The level of damage	Implementation mechanism
1	2	3	4	5	6
Network monitoring (intelligence)					
1	Intelligence, traffic analysis	high	k, c, d	from the essence	Interception of information transmitted in unencrypted form in a broadcast medium, the lack of a dedicated communication channel between ROM objects.
Unauthorized access to information resources with ROM					
1	Substitution (imitation) of a trusted object or subject of ROM with forgery of network	high	k, c, d	average	Falsification (forgery of IP network addresses, replay of messages in the

Threat model in ROM

№	Type of threats	Probability	What breaks	The level of damage	Implementation mechanism
1	2	3	4	5	6
	addresses of those objects that attack				absence of a virtual channel, insufficient identification and authentication in the presence of a virtual channel
2	Change routing	Let's not get high	k, c, d	low	Changing routing settings and the content of transmitted information due to lack of control over the route of messages or lack of filtering of packets with the wrong address
3	Selection of information flow and its preservation	high	k, c, d	high	Using the shortcomings of remote search algorithms by introducing erroneous objects into a distributed computing system ("man in the middle" attacks).

Threat model in ROM

№	Type of threats	Probability	What breaks	The level of damage	Implementation mechanism
1	2	3	4	5	6
4	Overcoming access administration systems to workstations, local networks and secure information object based on attributes of workstations or means of access control and routing (masking) of relevant networks - (firewalls, proxy servers, routers, etc.).	high	k, c, d	high	Using the shortcomings of identification and authentication systems based on user attributes (identifiers, passwords, biometric data, etc.). Insufficient identification and authentication of ROM objects, in particular sender addresses
Specific threats to information objects					
1	Overcoming the cryptographic security of intercepted information objects	low	To	high	Use of leaks through technical channels, removal from the network and specific virus attacks by implementing spyware with the disclosure of key sets
2	Overcoming the cryptographic security	low	To	high	Unauthorized access to information

Threat model in ROM

№	Type of threats	Probability	What breaks	The level of damage	Implementation mechanism
1	2	3	4	5	6
	of information objects of workstations				objects using the shortcomings of identification and authentication systems based on user attributes (identifiers, passwords, biometric data, etc.) with the disclosure of key sets
3	Modification of transmitted data, data or program code stored in the elements of computer systems.	high	c, d	high	Modification or substitution of information objects (program codes) or their parts by implementing destructive software or changing the logic of the program file using special types of virus attacks that can commit a violation of integrity
					Distortion of a certain number of symbols of an

Threat model in ROM

№	Type of threats	Probability	What breaks	The level of damage	Implementation mechanism
1	2	3	4	5	6
					information object with the use of special effects on information by technical channels in the local network or in the elements of the distributed network
4	Service blocking or overloading of access control system requests (denial of service)	high	d	high	Use of "Syn Flood" attacks, transmission of incorrect, specially selected requests to the attacked object
					Use of anonymous (or modified address) service requests (spam) or virus attacks of a special type

The availability of such information allows to build a more substantive general model of the protection system; assess the value of residual risk as a function of security for each of the functional properties of security; determine the structure of the protection system and its main components.

It should be noted that the estimates of the probability and magnitude of possible damage to each of the threats in this example of a threat model are

illustrative. For cases of specific ROM, these values must be determined by specialists of the protection service of the enterprise according to separate methods.

Thus , the analysis of many possible remote threats in distributed networks and mechanisms of their implementation proposed in the article make it possible to determine the components of security policy of information objects of the relevant ROM and the set of necessary means of protection against information objects from possible threats from the ROM environment.

References

1. Matov O.Ya., Vasylenko VS, Budko MM Estimation of security in local area networks. // Kyiv: News of the Academy of Engineering Sciences of Ukraine. 2005, № 2, pp. 59 – 73.
2. MaximumSecurity: AHacker's Guide to Protecting Your Internet Site and Network (http://zaphod. Redwave.net/books/hackg/index.htm).
3. TCP under sight (http: //www.hackzone. Ru / articles / tcp.html);
4. Some FTP problems (http://www.hackzone.ru/articles/ftp.html);
5. The attack on the DNS or Mr. ichnyy Nightmare network administrator (http://www.hackzone.ru/articles/dn-poison.html s)
6. . Medvedovsky ID Semyanov PV Leonov DG "Attack on the Internet" M .: PEC Publishing House 1999;
7. Sobolev KI Security Research with Windows NT 4.0 HackZone: Hacking Area. № 1-2-1998;
8. Buffer overflow in WIN32 (http://www.void.ru/stat/9907/20.html);
9. EXPLOIT buffer overflow on PERL (http: //www.void. Ru / stat / 0102 / 02.html).
10. Morgan, P. A. (2013). Shaping an Ethical Workplace Culture. In *SHRM Foundation's Effective Practice Guidlines Series* (pp. 1-44). USA.
11. National Business Ethics Survey - Ethics Resource Centre. (2011). *SCCE'S Social Network.* Retrieved 05 03, 2021, from https://community.corporatecompliance.o
12. rg/

13. Offorbike, S. A., NNADI, C. S., & AGU, J. C. (2018). Effect of Managing Employee Attitudes for Improved. *International Journal of Academic Research in Economics and Management Sciences*, 7(4), 64-77.