RESEARCH ARTICLE | OCTOBER 13 2016

Mathematical model of threats to information systems

Aleksey Novokhrestov; Anton Konev

AIP Conf. Proc. 1772, 060015 (2016)
https://doi.org/10.1063/1.4964595

Mathematical Model of Threats to Information Systems

Aleksey Novokhrestov[a] and Anton Konev[b]

Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Avenue, Tomsk 634050 Russian Federation

[a]corresponding author: nak1@keva.tusur.ru
[b]kaa1@keva.tusur.ru

Abstract. Existence of the need to assess the quality of computer networks security requires the development of a formalized evaluation method. One of the elements of such method is the model of threats to information system. In the article it is described a model of threats to integrity of information system exposed as a 3-level attributed metagraph. Threat model includes the threats on software, operating system and network layers. The model is used as part of the methodology for assessing the quality of computer network security.

INTRODUCTION

Currently, there is a necessity to assess the quality of both existing and emerging security systems. Quality of system security from threats is a measure of information security system to neutralize the threats to the information system and processed information [1]. The problem is that there is not a formalized method for the objective evaluation of the quality of the information systems security, and the result of evaluation depends largely on the subjective opinion and professional level of an expert [2] and also on the probability factor [3]. The review of some methods of security assessment and risk control (CRAMM, Risk Advisor) is given in [4].

The purpose of work is to create a formalized method of information systems security quality assessment. Creating of such method needs to rely on some models [5]:

- a model of an information system;
- a model of a security system;
- a model of threats to an information, an information system and means of information security.

In this paper we propose a model of threats to the integrity of information system (computer network).

EXPERIMENTAL PART

As a model of system we use a multi-level model based on attributive metagraphs. The interaction between objects in the model of information system described ac-cording to the rules of interaction of objects in the OSI reference model. This approach is described in [6].

Attributive metagraph nesting 3 is represented as an ordered six:

$$G = \left(X_1, X_2, X_3, E_1, E_2, E_3,\right),$$

where G – attributive metagraph nesting 3;

$X_1 = \{x_1^k\}, k = \overline{1,q}$ – a set of software;

$X_2 = \{x_2^l\}, l = \overline{1,r}$ – a set of operating systems (OS), $x_2^l \subset X_1$;

$X_3 = \{x_3^m\}, m = \overline{1,s}$ – a set of networks, $x_3^m \subset X_2$;

$E_1 = \{e_1^n\}, n = \overline{1,t}$ – a set of links between software, defined on set X_1;

Prospects of Fundamental Sciences Development (PFSD-2016)
AIP Conf. Proc. 1772, 060015-1–060015-4; doi: 10.1063/1.4964595
Published by AIP Publishing. 978-0-7354-1430-3/$30.00

$E_2 = \{e_2^o\}, o = \overline{1,u}$ – a set of links between OS, defined on set X_2;
$E_3 = \{e_3^p\}, p = \overline{1,v}$ – a set of links between networks, defined on set X_3.

Moreover, there are functions:

$$f_1^w : g_1^w(x_1^k, e_1^n) \to x_2^l,$$

where x_1^k – an element of software set;
e_1^n – an element of link set;
x_2^l – an element of OS set.

$$f_2^y : g_2^y(x_2^l, e_2^o) \to x_3^m,$$

where x_2^l – an element of software set;
e_2^o – an element of link set;
x_3^m – an element of OS set.

A node is characterized by set of attributes:

$$x_i^b = \{atr_a\},$$

where $i = \overline{1,3}$ – nesting level of node;
b – a number of node on corresponding layer i;
atr_a – a node attributes (numeric, string, and others).

An edge is characterized by set of attributes:

$$e_j^h = \langle x_i^c, x_i^d \rangle = \{atr_z\},$$

where x_i^c – initial node of the edge;
x_i^d – end node of the edge;
$j = \overline{1,3}$ – nesting level of edge;
atr_z – a node attributes (numeric, string, and others);
c, d – numbers of nodes on corresponding layer i;
h – a number of edge on corresponding layer j.

The suggested model of threats is an evolution of approach described in [5]. The type of attack for each of the sets of node attributes is the changing of link parameters (node attributes).

Types of attacks for each set of nodes:
1. replacement of an element (node);
2. removal of an element (node);
3. addition of an element (node).

Types of attacks for each set of edges:
1. replacement of a link (edge);
2. removal of a link (edge);
3. addition of a link (edge).

The link parameters are set in the attributes of nodes. The link parameters for the elements of the software set is the port number, which for the set of operating systems is the ip-address, what is used by the corresponding OS. In turn, link parameters for the network set are ip-address and a network routing table.

Almost every information system consists of a network, workstations and software. The main elements of the network interested for the attackers are workstations with the operating systems, the software included in the corresponding operating systems and protocols with which software interacts. On the workstation the main elements are the operating system and the software installed within operating system and api-functions enabling interaction between the software in the appropriate operating system.

Threats to the sets of nodes, node attributes and edges of graph G are given in Table 1.

TABLE 1. Threats to the integrity of information system

Set	Threats
X_3 (set of networks)	1. replacement of network 2. removal of network 3. addition of network
X_2 (set of OS)	1. replacement of OS 2. removal of OS 3. addition of OS
X_1 (set of software)	1. replacement of software 2. removal of software 3. addition of software
$\{atr_a\} \in x_3^m$ (set of network attributes)	Changing the routing table or the network ip-address
$\{atr_a\} \in x_2^l$ (set of OS attributes)	Changing the ip-address, which is used by the OS
$\{atr_a\} \in x_1^k$ (set of software attributes)	Changing the port number that is used by the software
E_3 (set of links between networks)	1. replacement of protocol running on the network level 2. removal of protocol running on the network level 3. addition of protocol running on the network level
E_2 (set of links between OS)	1. replacement of protocol running on the OS level 2. removal of protocol running on the OS level 3. addition of protocol running on the OS level
E_1 (set of links between software)	1. replacement of protocol running on the software level 2. removal of protocol running on the software level 3. addition of protocol running on the software level

RESULTS

As an example we consider the threats on operating systems layer. The threat of replacement of OS is characterized by deleting a node x_2^l from the set X_2 of the graph G and adding to the set X_2 a new node x_2^{r+1}, where *r* is an amount of nodes in X_2:

$$G' = \left(X_1, X_2 \backslash x_2^l, X_3, E_{1,} E_{2,} E_{3,}\right),$$
$$G'' = \left(X_1, X_2 \cup x_2^{r+1}, X_3, E_{1,} E_{2,} E_{3,}\right).$$

The threat of removal of OS is characterized by deleting a node x_2^l from the set X_2 of the graph *G*:

$$G' = \left(X_1, X_2 \backslash x_2^l, X_3, E_{1,} E_{2,} E_{3,}\right).$$

The threat of addition of OS is described by the by adding to the set X_2 of the graph *G* a new node x_2^{r+1}, where *r* is an amount of nodes in X_2:

$$G' = \left(X_1, X_2 \cup x_2^{r+1}, X_3, E_{1,} E_{2,} E_{3,}\right).$$

The threat of replacement of protocol running on the OS level is determined by deleting an edge e_2^o from the set E_2 of the graph G and adding a new edge e_2^{u+1} to E_2, where u is an amount of edges in E_2:

$$G' = (X_1, X_2, X_3, E_1, E_2 \backslash e_2^o, E_{3,}),$$
$$G'' = (X_1, X_2, X_3, E_1, E_2 \cup e_2^{u+1}, E_{3,}).$$

The threat of removal of protocol running on the OS level is characterized by deleting an edge e_2^o from the set E_2 of the graph G:

$$G' = (X_1, X_2, X_3, E_1, E_2 \backslash e_2^o, E_{3,}).$$

The threat of addition of protocol running on the OS level is described by the by adding to the set E_2 of the graph G a new edge e_2^{u+1}, where u is an amount of edges in E_2:

$$G' = (X_1, X_2, X_3, E_1, E_2 \cup e_2^{u+1}, E_{3,}).$$

The threat of changing ip-address, which is used by the operating system is described by changing of attribute atr_a of node x_2^l in the graph G. Attribute atr_a contains ip-address:

$$atr_a := atr_a'.$$

SUMMARY

In the work it was suggested a model of threats to integrity for a model of information system based on attributive metagraph nesting 3. This threat model includes the threats on software, operating system and network layers.

The model can be used as part of the methodology for assessing the quality of computer network security and can be successfully implemented to develop model of system and model of threats of automatic system for commercial accounting of power consumption.

ACKNOWLEDGMENTS

This work is financially supported by the Ministry of Science and Education of Russian Federation, contract no. 02.G25.31.0107.

REFERENCES

1. J. Yuill, F. Wu, J. Settle and F. Gong, Computer Networks, **34**, 671–697 (2000).
2. A.K. Novokhrestov and A.A. Konev, Dynamics of Systems, Mechanisms and Machines, **4**, 85–87 (2014) available at http://dinamika.omgtu.ru/images/stories/content2/Dinamika_tom4.pdf.
3. S. Jha, R. Linger, T. Longstaff and J. Wing, Survivability Analysis of Network Specifications, see http://www.cs.cmu.edu/~wing/publications/Jha-Longstaff00.pdf.
4. N.A. Staroverova and Z. Fadkhal, Bulletin of the Technological University, **9**, 282-287 (2013) available at http://elibrary.ru/item.asp?id=19101049.
5. A.A. Konev and E.M. Davydova, Proceedings of TUSUR, **2(28)**, 107–111 (2013) available at https://journal.tusur.ru/ru/arhiv/2-2013.
6. A.K. Novokhrestov and A.A. Konev, Electronic Equipment and Control Systems, **2**, 184-188 (2015) available at https://storage.tusur.ru/files/43177/2015-2.pdf.