https://doi.org/10.53656/math2022-2-7-ame

Educational Issues
Въпроси на преподаването

A METAGRAPH MODEL OF CYBER PROTECTION OF AN INFORMATION SYSTEM

Dr. Emiliya Koleva, Assist. Prof., Dr. Evgeni Andreev, Assist. Prof., Dr. Mariya Nikolova, Assoc. Prof.
Nikola Vaptsarov Naval Academy – Varna (Bulgaria)

Abstract. The aim of this article is to present a developed metagraph model which serves to verify the minimum requirements for cyber security in web-based student information management systems. The model presents the correlation between cyber attacks and cyber defense of the system. The protection is based on a created model for cybersecurity 3-12 and is divided into 3 categories – software, server and information system users. The most common 9 cyber attacks on automated information systems have been selected. Twelve countermeasures to these attacks have been selected. The application of the metagraph model is used to check whether the system meets the requirements of the model 3-12. The developed information system has been tested in foreign language training of students at Nikola Vaptsarov Naval Academy. The developed metagraph model can be applied to other information systems.

Keywords: metagraph; cyber security; cyberattacks; information system

1. Introduction

Student information management systems are complex electronic resources with multi-user access and sensitive information. This makes them subject to a large number of cyberattacks in order to gain access to the system, to the information stored in it, to disrupt its availability or to destroy the information stored in it (Sivkov & Andreev 2019) This requires the use of technological solutions and software implementations (Spasova 2018) in order to increase cyber security, which leads to a reduction in the number of administrators (Petrova 2019; Petrova 2021).

The cyber attack of the information system can be identified by several models. They can be represented graphically using the graph theory – simple graphs and digraphs. The problem with such data structure is that they usually associate individual information elements and not sets of elements. However, in many cases, it is necessary to associate sets of elements, such as multiple attributes in data relations, multiple variables in decision models, multiple logical variables in decision rules, and multiple documents in workflow systems. (Basu & Blanning 2007). In recent years, a new type of data structure has been developed that overcomes these limitations – the metagraph. It allows representation and analysis of more complex systems (Gapanyuk 2019).

The goal of this article is to present a metagraph model of cyber security of an information system.

2. Cyber security of an information system

The most common types of cyberattacks in information systems are directed against[1), 2), 3)] (Melnick 2018):

1. User profiles in the information system;
2. The server on which the system is running;
3. The software platform used to build the system.

At Nikola Vaptsarov Naval Academy an automated information system for monitoring student status has been developed. The system has been tested in the process of training foreign students. The system protection is based on the specially developed model 3-12, published in (Sivkov & Andreev 2019). Its development is a process of implementation of best practices, modifying and combining the widely used models of cyber protections based on the experience of implementing information systems (Petrova 2019). Three basic levels of cybersecurity are differentiated (Figure 1). They are related to system users, the server on which the system is being executed, and the software product, used to build the system. Based on these three cybersecurity levels, twelve mandatory security requirements have been selected.

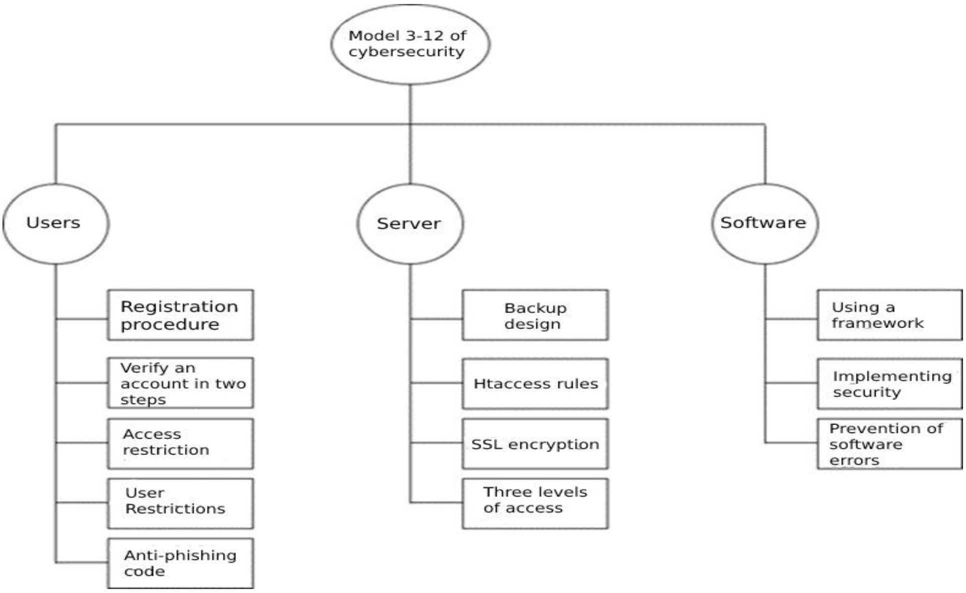

Figure 1. Model 3-12 for cyber defense (Sivkov & Andreev 2019)

Cyber security in the software product includes the following elements:

1. Fault prevention. It is a stage to identify all potential areas where a fault can occur and to close those gaps. The incomplete business rules and requirements will give rise to a heap of defects during development. Any team should be aware of how and by what rules the project will be developed. Depending on the number of people in the team, the most appropriate development methodology can be selected. During the individual development of the automated information system, it is envisaged that the system will be maintained by a small, expert team size of three to nine developers.
2. Deployment security. It includes security verification milestones. It is a fully automated process. When choosing a version control system, it must be predicted how the information will be sent to the server. Each project must have two parts, located in two different logical places for users and developers. It is a good practice to use two different domains to access them. In the version that is available to users, administrators often forget to turn off server errors. In this way, they are displayed when loading the automated information system. This information can be used to search for vulnerabilities. For better protection, an approach to exploiting the latest stable version of automated information system is used.
3. Use framework – To prevent multiple vulnerabilities a good approach is to use a ready-made framework for automated information system development. Framework developments are developed and tested by many people and thus security is achieved. Examples of open source frameworks are: Secure Software Development Framework (SSDF) (Souppaya, Scarfone & Dodson 2022) CodeIgniter, Symfony, Laravel and others.

The cyber security of the server includes the following elements:

1. Three-level access restriction – Access control is a process in which users request access to resources or data supported by a system, and the system determines whether the request should be granted or rejected. First, a list of IP addresses that can be accessed by the server through a virtual machine is used. Second, a username and a password to access the automated information system must be required. The third step requires a username and a password to access the virtual machine itself.
2. Backup design 3-2-1 – The basic concept is that three copies are made of the data to be protected – one copy and two backup copies. The information must be stored on two different types of storage media and one copy of the data is sent to an independent cloud-based server.
3. Htaccess rules – htaccess and regex rules (Bowen 2006) are used to increase the security of MVC software design. The functionality of these rules limits the ability to guess and access unauthorized files and folders.

4. SSL encryption – It is recommended to use an SSL certificate to encrypt the entire communication from the client to the server. This reduces the likelihood of reading data transmitted over the network.

Cybersecurity for users includes the following elements:

1. User registration procedure – users cannot register on their own, administrators have the responsibility and obligation to register them.
2. Double account confirmation – when activating user's account at the first entering into the system is required a confirmation on the e-mail stated in the registration;
3. Access restriction – the automated information system is available only to registered users.
4. Account restriction – Users have different levels of access to the automated information system depending on the rank they have.
5. Anti-phishing code – Add code to each business letter that verifies the sender of the e-mail to provide protection against phishing attacks.

Table 1 shows the relations between Cyber attack, Levels and security elements of model 3-12.

Table 1. Correlation between cyber attack, levels and model 3-12

Cyber attack	Levels	Security elements of model 3-12
SQL injection	Software	Prevention of program errors
		Implementing security
		Using a framework
XSS	Software	Prevention of program errors
		Implementing security
	Server	Htaccess rules
		Three levels of access restriction
	Users	Access restrictions
		User Restrictions
Password attack	Software	Prevention of program errors
		Implementing security
	Server	Htaccess rules
		Three levels of access restriction
		SSL encryption
	Users	Verify an account in two steps
		Access restrictions
Man in the middle	Server and Users	SSL encryption
Phishing	Users	Antifishing code

Drive-by attack	Software	Prevention of program errors
		Implementing security
	Server	Backup design
		Htaccess rules
	Users	Three levels of access restriction
		User Restrictions
Eavesdropping attack	Server and Users	SSL encryption
Zero-day exploit	Software	Prevention of program errors
		Implementing security
DDoS	Server	-

4. A metagraph model of cyber protection of an information system

The article uses a metagraph for a formalized description of the cyber security model 3-12. This kind of graph offers the possibility for more details, gives more clarity about the structure of the modeled object, as well as possibilities for modeling the hierarchy, as is the model 3-12. The metagraph is a graphical representation of a description of a subject area in which all objects can be divided into several groups, for example: visual programming languages, databases (Chernenkiy, Gapanyuk, Kaganov, Dunin, Lyaskovsky & Larionov 2018), computer networks (Novokhrestov & Konev 2016), Data Mining, information systems (Chernenkiy, Gapanyuk, Kaganov, Dunin, Lyaskovsky & Larionov 2018) and others. The foundational works on the theory of metagraphs are summarized in the monograph (Basu & Blanning 2007).

Various types of metagraph definitions could be found in different sources, which differ in small details depending on the application of the metagraph in the respective subject area. In (Basu & Blanning 2007), (Basu & Blanning 1994) the concept of "attribute metagraph" MGA is introduced, in which to each vertex and edge can be assigned any number of attributes. They could be numerical, string, etc. The article will use a formalized definition of metagraph (Samokhvalov, Revunkov & Gapanyuk 2015; Chernenkiy, Gapanyuk, Kaganov, Dunin, Lyaskovsky & Larionov 2018), which is adapted to describe the semantics of the information systems.

Let MG (1) be a metagraph represented by an ordered triple set:

$$MG = \langle MG^V, MG^{MV}, MG^E \rangle, \qquad (1)$$

where:

MG^V – is a set of all the vertices of the metagraph;

MG^{MV} – is a set of all the metavertices of the metagraph;

MG^E – is a set of edges of the metagraph.

The metavertex may include several vertices of the metagraph together with the edges between them.

The vertex of the metagraph is described by several attributes:

$v_i = \{atr_k\}, v_i \in MG^v$, where v_i – vertex of the metagraph; atr_k – attribute.

The edge of the metagraph e_i is described as a set of attributes, start and end vertices, and a direction flag:

$e_i = \langle v_S, v_E, eo, \{atr_{\iota}\}\rangle, e_i \in MG^E, eo = true|false$. where e_i – edge of the metagraph; v_S – initial vertex of the edge (metavertex); v_E – final vertex of the edge (metavertex); eo – flag direction of the edge ($eo = true$ – directed edge (arc), $eo = false$ – undirected edge); atr_k – attributes.

Based on the proposed model 3-12 (Figure 1) and Table 1, a metagraph model for cyber defense of an automated student status system has been developed. Its graphical model is presented in Figure 2.

The metagraph on Figure 2 includes the following elements:

1) $The\ set\ MG^V = \cup X_i$ за $i = \overline{1,4}$, where:

$X_1 = \{x_{11}, x_{12}, x_{13}, x_{14}, x_{15}\}$ – includes various cyber protections at the user level;

$X_2 = \{x_{21}, x_{22}, x_{23}, x_{24}\}$ – includes server-level types of cyber security;

$X_3 = \{x_{31}, x_{32}, x_{33}\}$ – includes various cyber security at the software level;

$X_4 = \{x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}\}$ – includes the various cyber attacks from the first column of Table 1.

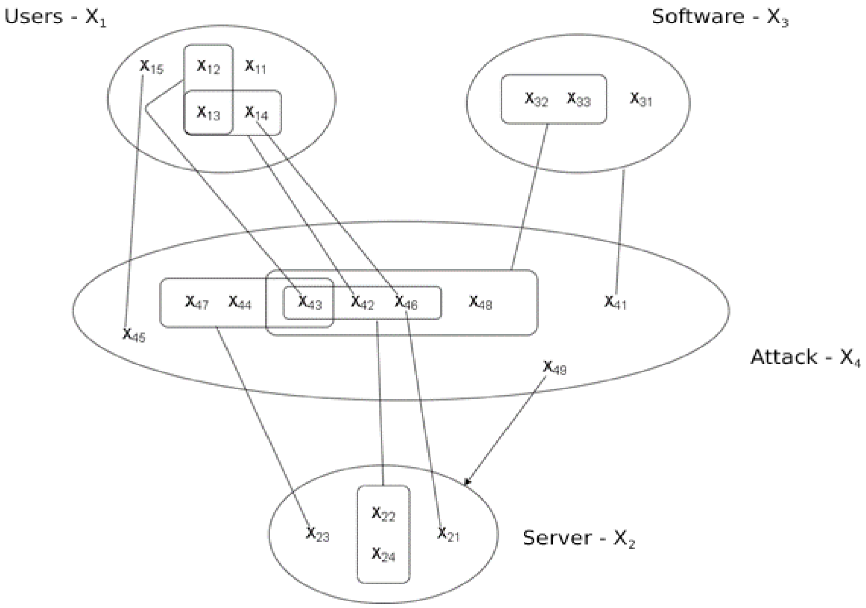

Figure 2. Model for cyber protection of an information system, presented through a metagraph

The elements of $X_i, i = \overline{1,4}$ are shown in the Table 2:

Table 2. Elements of the sets $\mathrm{X_i, i} = \overline{1,4}$

Elements of the sets $\boldsymbol{X_i, i = \overline{1,4}}$	**Relation with model 3-12**
$x_{11} \in X_1$	Registration procedure
$x_{12} \in X_1$	Verify an account in two steps
$x_{13} \in X_1$	Access restrictions
$x_{14} \in X_1$	User Restrictions
$x_{15} \in X_1$	Antiphishing code
$x_{21} \in X_2$	Backup design
$x_{22} \in X_2$	Htaccess rules
$x_{23} \in X_2$	SSL encryption

Elements of the sets $X_i, i = \overline{1,4}$	**Relation with model 3-12**
$x_{24} \in X_2$	Three levels of access restriction
$x_{31} \in X_3$	Using a framework
$x_{32} \in X_3$	Implementing security
$x_{33} \in X_3$	Prevention of program errors
$x_{41} \in X_4$	SQL injection attack
$x_{42} \in X_4$	XSS attack
$x_{43} \in X_4$	Password attack
$x_{44} \in X_4$	Man in the middle attack
$x_{45} \in X_4$	Phishing attack
$x_{46} \in X_4$	Drive-by attack
$x_{47} \in X_4$	Eavesdropping attack
$x_{48} \in X_4$	Zero-day exploit attack
$x_{49} \in X_4$	DDoS attack

2) The set $MG^{MV} = \cup\, v_i$ for $i = \overline{1,9}$, where v_i are metavertices of the metagraph MG:

$v_1 = \{x_{12}, x_{13}\} \subset X_1$

$v_2 = \{x_{13}, x_{14}\} \subset X_1$

$v_3 = \{x_{22}, x_{24}\} \subset X_2$

$v_4 = \{x_{32}, x_{33}\} \subset X_3$

$v_5 = \{x_{42}, x_{43}, x_{46}\} \subset X_4$

$v_6 = v_5 \cup \{x_{48}\} \subset X_4$

$v_7 = \{x_{43}, x_{44}, x_{47}\} \subset X_4$

$v_8 = X_2$

$v_9 = X_3$

$MG^E = \cup\ e_i$ for $i = \overline{1,10}$

Each of the MG edges is described as an ordered quadruple: $e_i = (u_e, u_m, atr_i, eo)$, where:

$e_i \in MG^E, i = \overline{1,10}$

u_e- initial vertex (metavertex), $u_e \in MG^V \cup MG^{MV}$

u_m- final vertex (metavertex), $u_m \in MG^V \cup MG^{MV}$

$atr_i \in \{0,1\}, i = \overline{1,10}$

$eo = true|false$ – directed | undirected edge.

Initially $atr_i = 0$ for $\forall i = \overline{1,10}$. In the presence of a cyber attack of the corresponding type, the given attribute is assigned a value of 1.

If $eo = \text{“}true\text{”}$ for a given edge, then the edge is directed. Otherwise, ie. $eo = \text{“}false\text{”}$ the edge is undirected.

For the presented metagraph model (Figure 2), the edges are as follows:

$e_1 = (x_{41}, v_9, 0, false)$

$e_2 = (v_6, v_4, 0, false)$

$e_3 = (v_5, v_3, 0, false)$

$e_4 = (x_{46}, x_{14}, 0, false)$

$e_5 = (x_{46}, x_{21}, 0, false)$

$e_6 = (x_{42}, v_2, 0, false)$

$e_7 = (x_{43}, v_1, 0, false)$

$e_8 = (v_7, x_{23}, 0, false)$

$e_9 = (x_{45}, x_{15}, 0, false)$

$e_{10} = (x_{49}, v_8, 0, true)$

The proposed metagraph is a graphical representation of the main components of the model 3-12 for cyber protection of the information system.

Conclusion

Metagraphs represent a more complex data structure than ordinary graphs, but allow the possibility for the presentation and analysis of more complex systems. The proposed metagraphic approach allows presenting the main components of the model for cyber defense of the automated system for student status and the connections between them. The presented metagraph is a graph-theoretic construct that captures relationships between the different types of cyber attacks, as well as cyber defenses at different levels (user, server, software). The interaction between objects in the model is described by attributes and relations between metavertices, which are one of the main features of metagraphs. In addition, the graphical visualization of the model 3-12 is a tool with which most common problems faced by the designers and users can be addressed by using the properties of metagraphs.

The 3-12 model is a set of rules based on good practices in protecting web-based information systems. The rules include the allowable minimum cyber security of web-based systems and therefore the metagraph model can be used as part of the methodology for quality assessment of cyber security of the automated student status system.

NOTES

1. CWE Top 25 Most Dangerous Software Weaknesses, 2021, https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html.
2. Web Applications Attacks – Common Types of Web Based Attacks, https://www.trustnetinc.com/web-application-attacks/.
3. What Are the Most Common Cyber Attacks?, 2021, CISCO, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work.
4. What are web threats and online Internet threats? https://www.kaspersky.com/resource-center/threats/web.

REFERENCES

BOWEN, R., 2006. Access Control. *In: The Definitive Guide to Apache mod_rewrite.* New York City: Apress Media LLC, 89 – 97. Available from: doi.org/10.1007/978-1-4302-0122-9_9.

BASU, A. & BLANNING, R., 2007. *Metagraphs and their applications.* New York City: Springer US. Available from: doi.org /10.1007/978-0-387-37234-1.

BASU, A. & BLANNING, R., 1994. Model Integration Using Metagraphs, *Information Systems Research*, **5**(3). Available from: doi.org /10.1287/isre.5.3.195.

CHERNENKIY, V., GAPANYUK, Y., KAGANOV, Y., DUNIN, I., LYASKOVSKY, M. & LARIONOV, V., 2018. Storing Metagraph Model in Relational, Document-Oriented, and Graph Databases, *DAMDID/RCDL'2018*, **2277**(1), 82 – 89.

GAPANYUK, Y., 2019. Metagraph Approach to the Information-Analytical Systems Development, *CEUR WORKSHOP PROCEEDINGS/ APSSE 2019*, **2514**(1), 428 – 439.

MELNICK, J., 2018. *Top 10 Most Common Types of Cyber Attacks.* https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.

NOVOKHRESTOV, A. & KONEV, A., 2016, *Mathematical model of threats to information systems.* Maryland: AIP Publishing. Available from: doi.org /10.1063/1.4964595.

SAMOKHVALOV, E., REVUNKOV, G. & GAPANYUK, Y., 2015. Metagraphs for Information Systems Semantics and Pragmatics Definition. *Newspaper Bauman Moscow State Technical University*. Available from: doi.org /10.18698/0236-3933-2015-1-83-99.

SIVKOV, Y. & ANDREEV, E., 2019. 3-12 model of Cybersecurity in the Implementation of a Student Information Management System., *Proceedings of the Doctoral Scientific Conference*. Varna: Nicola Vaptsarov Naval Academy, 11 – 18.

SOUPPAYA, M., SCARFONE, K. &DODSON, D., 2022. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, *NIST Special Publication*, 800-218.

PETROVA V., 2019. Using the Analytic Hierarchy Process for LMS selection. *CompSysTech '19: 20th International Conference on Computer Systems and Technologies - Ruse, Bulgaria*, 332 – 336, ISBN: 978-1-4503-7149-0.

PETROVA, V., 2021. The Hierarchical Decision Model of cybersecurity risk assessment. *12th National Conference with International Participation "Electronica 2021",* 18 – 21, ISBN 978-1-6654-4060.

SPASOVA, V., 2018. Savremenni tendencii v razvitieto na informacionnite sistemi, podpomagashti vzemaneto na resheniya v upravlenieto, Varna: *e-Journal VFU*, **5**, https://ejournal.vfu.bg/bg/it.html [In Bulgarian].

✉ **Dr. Emiliya Koleva, Assist. Prof.**
ORCID ID: 0000-0003-1902-2042
Faculty of Engineering
N. Y. Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: e.koleva@nvna.eu

✉ **Dr. Evgeni Andreev, Assist. Prof.**
ORCID ID: 0000-0001-5211-4307
Web of Science Researcher ID: AAB-5612-2019
Faculty of Engineering
N. Y. Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: e.andreev@naval-acad.bg

✉ **Dr. Mariya Nikolova, Assoc. Prof.**
ORCID ID: 0000-0002-2640-093X
Web of Science Researcher ID: E-2923-2012
Faculty of Engineering
N. Y. Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: m.nikolova@naval-acad.bg