Approach for determination of cyber-attack goals based on the ontology of security metrics

E Doynikova¹ and I Kotenko²

¹ Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia
² Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia

E-mail: doynikova@comsec.spb.ru

Abstract. The research aims to determine cyber-attack goals in the information systems of various types for the further selection of the optimal countermeasures. We propose an approach based on the ontology of security metrics to achieve the research goal. The developed ontology provides the features for the determination of attack goals using neuro-fuzzy network. The paper describes the proposed ontology combining security components, classes of security metrics, various data sources, and relations between them. The concept of using the security metrics as features for training neuro-fuzzy network is given. Application of the approach is shown on the case study.

1. Introduction

Determination of cyber-attack goals is an essential step to an efficient responding to them. This means prevention of their negative consequences and revealing of their sources to avoid the cyber-attacks in the future. To achieve this goal we previously used attack graphs and risk level metrics [1]. Attack graphs incorporate all possible attack sequences in the analyzed information system. Thus, the set of possible attack goals in the system were specified considering possibilities of attacks implementation. This set includes all end nodes of the possible attack sequences. We apply risk level metric to select the goals (or end nodes of the attack sequences) that should be prevented. The risk level is calculated for each node of an attack graph as the combination of a node compromise probability and an impact in case of its successful compromise. The nodes with a risk level that exceeds the predefined threshold were selected for the countermeasures implementation. This approach has shown good results for preventing propagation of the attacks in the information system. But it has some limitations related to selection of the optimal response solution because it uses rather rough indicator.

In this study we try to overcome existing limitations to enhance the approach to attack goal determination using neuro-fuzzy networks. We introduce an ontological model of the attack goals specified by the set of interconnected features. The motivation of the research is that more accurate determination of attack goals will allow more efficient and less costly responding to cyber-attacks. We also believe that this will allow preventing of the cyber-attacks in future.

The developed approach includes two stages: determination of possible classes of attack goals and determination of goal of an ongoing attack. We propose to use the set of features specified using security metrics to determine possible classes of cyber-attack goals. The set of security metrics and their relations with different classes of goals depends on the input security data and their interrelations.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd
We specify all these relations using an ontology of security metrics. On the second stage we propose to use neuro-fuzzy networks to determine the goals of ongoing attacks. Selection of features of attack goals and determination of membership functions for different sets of features corresponding to different classes of goals is rather challenging task. Thus, in this paper only the first stage is considered.

The paper is organized as follows. Section 2 reviews main related works. Section 3 describes a common idea of the proposed approach. Section 4 shows application of the approach on the case study. The paper ends with conclusion and plans for future research.

2. Related works

Existing studies provide various classifications of cyber-attack goals. For example, in [2] the following attack goals are outlined: root privilege gain; user privilege gain; denial of service; loss of integrity, confidentiality, availability; others. Such allocation of goals is typical for the researches based on the attack graphs [3], including our previous research [4]. But this classification is not enough to accurately determine an attack type and depending correct response [5]. In [6] a broader classification is proposed. It incorporates the following cyber-attack types: challenge, status, thrill; political gain; financial gain; damage. This classification is basis for the current study. Cyber-attack objectives depend on the specificity of the analyzed information system (e.g. information system of commercial organization, information system of public institution, etc.) and attacker class. In [2] the classification of attackers based on the complexity of the vulnerabilities they exploit is introduced: script kiddies; hackers; botnet owners. In [7] the following classes of attackers are specified: criminals, hackers and liberals. While in [6] the following classes of attackers are outlined: hackers, spies, terrorists, corporate raiders, professional criminals, vandals, voyeurs. The latest classification of attackers is used in this study. For example, an information system of state institution is target for the attacks with political gain objective. It would rather be interesting for the professional criminals, spies and terrorists. While an information system of commercial organization is a target for the attacks with financial gain objective. It can be attacked by the professional criminals and hackers.

The connections between separate security concepts that specify dependencies among attack classes, attacker classes and attack objective classes, and specify their distinctive features, can be represented as ontology. An ontological approach is used in various research works to represent security knowledge [8], to process complex events and detect their sources [9], to represent information for the security monitoring systems, for the logical inference in the response decisions support area [10], to generate security data storage [11]. We first introduced an ontology of security metrics in [12]. In this study the previously developed ontology is revised and extended for the task of attack goal determination.

Recently the neuro-fuzzy networks are widely used. There are different examples of their implementation including ANFIS, FALCON, GARIC, NEFCON and FUN [13]. Selection of neuro-fuzzy network technology for the denoted task of determination of attack goals is due to the fact that on the one hand it allows using fuzzy logic for the decision making. It is necessary in case of the uncertain input data for an attack forecasting. On the other hand, it allows using the computing capabilities of neural networks to set parameters of fuzzy sets membership functions and their learning ability to enhance forecasting mechanisms. In this research we plan to apply neuro-fuzzy network implementation based on ANFIS [13], [14] because of its efficiency in obtaining conclusions.

An accuracy of forecasting of attack objectives and resulting efficiency of countermeasure selection depend on the selected parameters and their values, and on the accuracy of their classification by the different attack goals. From our point of view an ontology of security metrics, their interconnections, input data for their calculation, and cyber-attack objectives can provide required quality of input data, while an apparatus of neuro-fuzzy networks can provide sufficient accuracy of classification of features by attack objectives. As soon as currently there is no such ontology in the analyzed researches, we develop it in this study and generate proposals for its application to the determination of attack goals.

2
3. Common approach to prediction of attack goals

The proposed approach includes two stages: determination of possible classes of cyber-attack goals and determination of goal of an ongoing attack. In this paper we mainly consider the first stage. We suggest using the set of features specified using security metrics to determine possible classes of cyber-attacks and their goals. The set of security metrics and their relations to different classes depends on the input security data and their interrelations. We specify them as an ontology of security metrics. The ontology allows us to express complex relations between entities using description logic.

The proposed ontology is partially based on the ontology of security metrics [12] and ontology of security data [11], that we developed previously. Let us to describe the set of concepts first. These are the objects that participate in the attack goals forecasting process, their features, possible values of the features, and connections between objects considering their relations and interaction.

The set of concepts of the developed ontology incorporates three main groups of objects for forecasting cyber-attack goals. These groups are as following: the main objects of cyber-attack domain; input data sources; features of objects (metrics).

We include in the ontology the following basic entities: “system”, “target”, “attacker”, “weakness”, “attack”, “vulnerability”, “countermeasure”, “incident”, “attack objective”, “attack tool”, “event”, “attack action”. In Figure 1 the listed concepts determining basic objects that are involved in a cyber-attack are incorporated by the entity “Thing”. We add subclasses proposed in [6] to classes “attacker”, “objective” and “system” to the ontology to determine attack goal. These subclasses were described above. Some subclasses are represented in figure 1 (appropriate ovals are colored). Other subclasses are omitted so as not to overload the figure. The allocated subclasses can be detailed further if necessary. Thus, for the “political gain” class the following subclasses can be specified: “protests against political actions”, “protests against laws or public documents”, “outrage against acts related to physical violence” [15].

![Figure 1. Ontology fragment with top-level concepts.](image-url)
The group of concepts that correspond to the input data sources is described in [11]. It incorporates open security databases, such as the weaknesses database CWE, the attack patterns database CAPEC, the database of vulnerabilities CVE and NVD, the database of exploits ExploitDB, and others. In Figure 1 these concepts are joined by the entity “Source”.

The entity “Source” is connected with the entity “Thing” because it determines the specific data for the concepts of “Thing” group. Besides, the concepts of the “Source” group provide input data for another group of objects of the ontology. This group incorporates the features of objects and we name it “Metrics”. We introduce this concept to determine class of a cyber-attack objective using features and their values inherent in each class. In scope of the concept “Metrics” we outline different classes of metrics to evaluate different objects. In [4] we determined the following classes of metrics: system metrics, attack metrics, attacker metrics, event metrics, response metrics and integral metrics.

Interconnections between the classes of metrics and the concepts of ontology corresponding to different objects are represented in figure 2. Each top-level class of metrics include the set of characteristics that define the class of the appropriate object. We select metrics considering the goals of security assessment, parameters of object, and its connections with other objects. Thus, for an attacker the following parameters can be used: attacker skill level and attacker knowledge on system.

“Attacker skill level” is an integral metric that considers metrics that are calculated based on the metrics of other objects. These metrics are “tools complexity”, “attack steps complexity”, “steps success rate”, “trace coverage rate”. All these metrics are calculated using the connection between an attacker and his attack steps. An attack is defined by the following metrics: “attack probability” and “attack impact”. “Attack probability” is calculated on the basis of complexity of attack implementation and an attack depth (number of attack steps). The latest metrics are calculated considering steps of a multi-step attack.

An ontology fragment that describes main metrics of attacker and attacks is provided in figure 3. It should be noted that two described concepts – “attack” and “attacker” – are not enough to determine attack goal and attacker goal, accordingly. The features of concept “target” should also be considered. They allow definition of an attack impact. Besides, an attack goal highly depends on a target type (e.g. an information system of state organization, an information system of state organization, etc.). In the future work we plan further extension and detailing of the proposed ontology of metrics. For this goal existing classifications of attacks, vulnerabilities and weaknesses can be used.

**Figure 2.** Ontology fragment with top-level classes of metrics.

**Figure 3.** Ontology fragment with attacker and attack metrics.

In the first rough approximation, the following correspondence between the specified objectives of attacks and qualitative features of attacks, attackers and attack targets can be defined. In case of the objective “political gain”, the attack targets cover services, computers and web sites of state...
institutions and politicians, of financial centers, banking districts, and multinational corporate power bases. For this type of objectives a serious damage for information integrity, availability and/or confidentiality is typical. Usual executors of such attacks are organized professional cyber criminals. Because these attacks are characterized by the high cost and complexity of the used tools, complexity of the implemented actions, organized steps, high success rate of steps, and high trace coverage. Besides, executors of attacks with “political gain” objective often take responsibility for the conducted attack (if it is “protests against political actions”, “protests against laws or public documents”, or “outrage against acts related to physical violence”).

To determine the goals of specific cyber-attacks it is necessary to determine a set of parameter values that uniquely determine the class of attack objective. We propose to use neuro-fuzzy networks for this goal. In this research we plan to use an implementation of neuro-fuzzy network on the basis of ANFIS [13], [14]. An essential stage when we use the technology of neural networks is generation of the training sample. We plan to analyze known political, economic and social-cultural attacks of the last decades [15], and data in the open security databases to gather the input data set. An implementation of neuro-fuzzy network for determination of cyber-attack goals and the process of generation and resulting composition of the training sample will be described in details in the future research.

4. Case study
As a case study we analyze an attack that aims to steal user accounts of a web resource. The fragment of network configuration used for the case study incorporates the following components: a remote computer of attacker, a web server with web application, and an authentication server that is used for the remote authentication. The attack consists of the following steps.

1. An analysis of behavior and code of the web application (attack pattern CAPEC-580 “Application Footprinting” in accordance with the attack patterns database). This step requires low level skills.
2. Exploitation of OGNL Injection in ApacheStruts2 framework to launch processes on the web server remotely.
3. Internal reconnaissance on the web server (attack pattern CAPEC-529 “Malware-Directed Internal Reconnaissance”). This step requires skills of medium level. The reconnaissance revealed the vulnerability of the JBoss Application Platform.
4. Application of the vulnerability detected on step 4. The step resulted in the partial access to the confidential data on the web server.
5. Further reconnaissance of the internal network (attack pattern CAPEC-300 “Port Scanning”). This step requires low level skills. The reconnaissance shown that tcp/ldaps (636) port is opened. This port is used for the NetIQ eDirect authentication server.
6. Application of the zero day vulnerability of NetIQ eDirect server. It is resulted in root access to the authentication server and the theft of user accounts. This latest step requires high skills.

While performing some attacking actions, the monitoring system issued alerts, but the incident was not generated.

As it was described in section 3 using the ontology, an attack goal is determined by the parameters of an attack, attacker and attack target. All these objects – an attacker, an attack, an attack target and an objective – are connected in scope of the security events and incidents. These events and incidents provide initial dynamic data for the analysis. An attack class, in its turn, depends on the complexity of used tools, complexity of attack steps, security properties impact and costs of target. In the analyzed attack the zero-day vulnerability was exploited. It is a complex action (“attack steps complexity” = “High”). An attacker was not detected in a system till the objective was achieved (the events shown the small deviations but were not correlated into an incident, i.e. “trace coverage rate” = “High”). The system itself is characterized by the high cost of user data (“target” = “data on DB server”, “cost” = “High”). And, finally, on each step an attacker tried to get the highest privileges (“unauthorized result” = “Increased access”). All this is typical for the objective “financial gain” and it is consistent with the real goal of the analyzed attack.
It should be noted that the provided case study is very abstract and should only demonstrate an applicability of the ontology to determine the goals of cyber-attacks. In future work the metrics and their values will be specified and more specific experiments will be conducted.

5. Conclusion
The paper describes the common idea of approach for determination of cyber-attack goals based on the ontology of security metrics and neuro-fuzzy networks. The basic ontology of object and appropriate security metrics for determination of cyber-attack goals is proposed. The case study that shows applicability of the developed ontology for the stated purpose is provided. In the future work we plan to extend the proposed ontology in terms of the used metrics, to specify their possible values, and to introduce a mechanism of application of neuro-fuzzy network to determine different classes of cyber-attack goals.

References
[1] Doynikova E and Kotenko I 2017 CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection Proc. of the 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing
[2] Aliyev V 2010 Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network
[3] Idika N and Bhargava B 2012 Extending attack graph-based security metrics and aggregating their application IEEE Trans. Dependable Secur. Comput. 9(1) 75-85
[4] Kotenko I and Doynikova E 2015 Countermeasure selection in SIEM systems based on the integrated complex of security metrics Proc. of the 23rd Euromicro Int. Conf. on Parallel, Distributed, and Network-Based Processing
[5] Kanoun W Cuppens-Boulahia N Cuppens F and Araujo J 2008 Automated reaction based on risk analysis and attackers skills in intrusion detection systems Proc. of the Third Int. Conf. on Risks and Security of Internet and Systems
[6] Howard J D and Longstaff T A 1998 A common language for computer security incidents
[7] Dantu R, Kolan P and Cangussu J 2009 Network risk management using attacker profiling Secur. Commun. Networks
[8] Herzog A, Shahmehri N and Duma C 2007 An ontology of information security LIISP 1 1-23
[9] Taylor K and Leidinger L 2011 Ontology-driven complex event processing in heterogeneous sensor networks Semant. Web Res. Appl. 6644 LNCS 285-99
[10] Granadillo G G, Mustapha Y B, Hachem N and Debar H 2012 An ontology-based model for SIEM environments Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering
[11] Kotenko I, Doynikova E, Fedorchenko A and Chechulin A 2018 An ontology-based hybrid storage of security information Inf. Technol. Control
[12] Kotenko I, Polubelova O, Saenko I and Doynikova E 2013 The ontology of metrics for security evaluation and decision support in SIEM systems Proc. of the Int. Conf. on Availability, Reliability and Security
[13] Branitskiy A 2017 Hierarchical hybridization of binary classifiers for detecting anomalous network connections SPIIRAS Proc. 52(3) 204-33
[14] Jang J S R 1993 ANFIS: Adaptive-Network-Based Fuzzy Inference System IEEE Trans. Syst. Man Cybern.
[15] Gandhi R, Sharma A, Mahoney W, Sousan W, Zhu Q and Laplante P 2011 Dimensions of cyber-attacks: Cultural, social, economic, and political IEEE Technol. Soc. Mag. 30(1) 28-38