Development Approach to the Attack Modeling for the Needs of Cyber Security Education

Blaž Ivanc
Laboratory for Open Systems and Networks
Jožef Stefan Institute
Ljubljana, Slovenia
blaz.ivanc@ijs.si

Borka Jerman Blažič
Laboratory for Open Systems and Networks
Jožef Stefan Institute
Ljubljana, Slovenia
borka@e5.ijs.si

***Abstract*— Critical infrastructure faces changed landscape of threats which requires progress in the understanding of highly sophisticated attacks. A reflection of this awareness is the upcoming technical documentation of umbrella organizations in critical infrastructure. The attack modeling is an important approach in the design stage of the system. The attack tree is a structural technique for attack modeling. In terms of graphic presentation, attack trees are not complex and can be designed manually, also, they are an important tool in recognizing threats and evaluating risks. The absence of the presentation of comprehensive and systematic approaches to the attack modeling is often reflected in rather generalized and inconsistent presentations of the attack modeling as well as in difficult transfer of attack modeling techniques into practice. The current absence of the agreement and lack of consistency in the development approach of structural attack models limits the transfer of concepts in the field of cyber-attacks to educational environments. The purpose of the paper is to present, in clear practical example, a proposal for the development approach to the attack modeling. Thus, we want to contribute to the implementation of attack modeling into practice, especially in the field of cyber security education.**

Keywords*— *attack modeling, awareness, critical infrastructure, cyber security education, interdisciplinary approach, structural techniques.

I. Introduction

Critical infrastructure faces changed landscape of threats which requires progress in the understanding of highly sophisticated attacks. A reflection of this awareness is the upcoming technical documentation of umbrella organizations in critical infrastructure, such as the IAEA, which stresses the demonstration of possible attack scenarios [1]. It is important, in this respect, to recognize potentially related attacks, which can be done with the consideration of indicators, such as exploited vulnerabilities, used technologies, sources of effected attacks, focus on the targets and others [2]. These characteristics in practice allow narrowing of the range of potential attack agents. Attack modeling significantly contributes to the recognition of vital areas, which can be sabotaged in their operational functioning [3].

The attack tree is a structural technique for attack modeling providing formal, methodological approach to the planning and documentation of the steps carried out by the attackers on a particular system. Attack trees represent a basis for the development of attack scenarios and are focused on the presentation of the individual steps within the attack execution. In terms of graphic presentation, attack trees are not complex and can be designed manually, also, they are an important tool in recognizing threats and evaluating risks.

Security assessments on the basis of attack trees are analytical processes of deduction and decomposition [4]. Such assessments are particularly desirable when the system is in the process of development and it is still possible to affect the primary design. The attack modeling is also an important approach in the design stage of the system. At the same time, the attack trees are a frequently used technique for the assessment and they are based on the actual implementation of the information attacks on computer systems and networks.

The absence of the presentation of comprehensive and systematic approaches to the attack modeling is often reflected in rather generalized and inconsistent presentations of the attack modeling as well as in difficult transfer of attack modeling techniques into practice. The purpose of the paper is to present, in clear practical example, a proposal for the development approach to the attack modeling. Thus, we want to contribute to the implementation of attack modeling into practice, especially in the field of cyber security education.

The paper is further composed as follows: the second section presents the importance of the graphic representations. The third section focuses on the proposal for the development approach in attack modeling. It consists of two subsections presenting an example of attack model with the analysis of the levels of nodes. The forth section is the discussion. The fifth one is the conclusion.

II. Graphic representations of cyber-attacks

Graphic representation techniques with its associated models help to impart knowledge in the form of graphic representations (trees, graphs, etc.) and thus enable the understanding of large amounts of data in a short time [5]. Abstract data, acquired from different sources, have to be converted into a coherent structure, which is achieved by visualization techniques. That is how a wide range of information is presented in a compact and useful way [3]. If we correctly take and optimize the set of necessary information, the graphic representation will be more suitable for human's cognitive system [6]. The attack modeling in the area of

ISBN: 978-1-4673-9379-9 ©2016 IEEE

network security promotes a security awareness. Consequently, models help in the design or layout of the defense measures within potential threats. In the field of graphic representations and formation of the attack graphs, it is worth focusing on the need for rapid identification of key nodes causing great risk to network security and it should be fundamental subject of the application of defense approaches [7]. At the same time, it is not easy to be truly familiar with a set of relevant attributes and to determine their value [8].

The Enhanced structured model (ESM) was presented in the past in order to provide a better understanding of the implementation of cyber-attacks while increasing the flexibility of structural models to generate scenarios [9]. With the model, shown in Figure 1, we mainly wanted to improve certain restrictions faced by analysts when using the attack modeling. The main characteristics of the ESM are the use of additional information items in the form of attack vectors and exploited vulnerabilities, the display of countermeasures, an increased set of possible nodes and a visible segmentation of individual subtree structures.

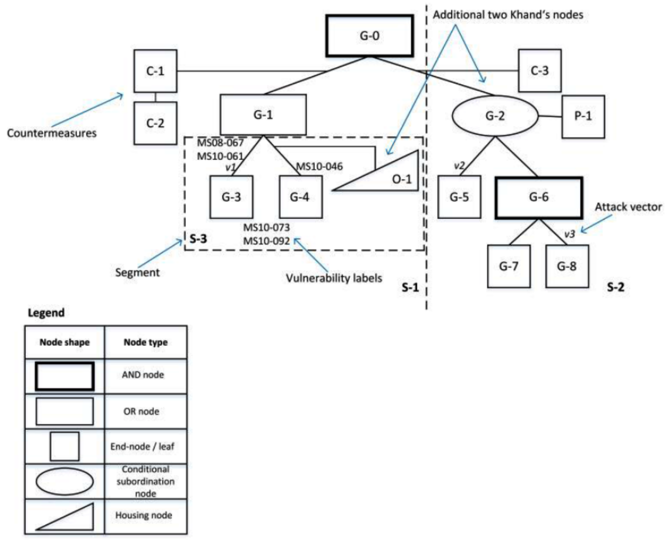

Fig. 1. A display of the Enhanced structured model example with its main characteristics

Later, we also showed the quantification of the ESM [10], based on a set of three attributes: cost, impact and complexity. For AND, OR and CSUB nodes we designed rules for calculating the value with the bottom-up algorithm and showed potential designated points for an initial assignment of the attribute values.

III. Proposal of the development approach to attack modeling

Cyber-attacks are often presented in a form which is not user-friendly and offers a limited ability to display details. All this makes the understanding of cyber-attacks difficult. The authors in [11] say that it is imperative to present cyber-attacks to security analyst and experts, to explain targets of the attack, the attacked system sources and attack methods that were used. The mentioned authors present a general four-step procedure, which is a bridge between top down approach for attack modeling and a standard bottom up approach. The top down approach is used for the first two steps in the procedure and it is applied to main attack goal and other attack subgoals. The standard bottom up approach is used for the last two steps and it is applied to attack methods that could be employed to achieve the attack goal and to specify the logical relationships between different attack methods. The authors in [12] present an iterative procedure focused on the selection of the attributes and the assignment of their values. The first step of the presented case study process includes model creation, which is an iterative process. The next steps in the process are attribute decoration, attribute value preparation and attribute value calculation.

The individual nodes in the structural model in a general agreement in the field of attack modeling present different goals and activities in the course of the attack. The root of the tree is the main object of the attack, presented by the model. The intermediate nodes present only partial goals that can be individual goals of a certain subtree structure, if only we isolate it from the model. The end nodes or leaves present direct activities in the attack. The consequences of such agreement are too generalized presentations of different models at the level of attack trees. Therefore, such presented models frequently have no useful value.

The following subsection describes the model of the attack focused on the Internet of Things (IoT) smart home device, followed by the reading of the model and the analysis based on the level of the nodes in the model. The next subsection presents a proposal of the development approach to the attack modeling based on the displayed model.

A. *The example of attack model with the breakdown of nodes on different levels in the model*

This section presents our proposal to the attack modeling with structural graphic techniques based on the practical example. The example is shown on the basis of attack surface in the field of the internet of things. It often turns out that security aspect of IoT devices is insufficiently dealt with. The devices frequently do not support or require strong passwords, the use of mutual authentication and protection from brute-force attacks [13]. There are still examples of the absence of encrypted communication with the cloud, also, a set of IoT technologies involves many common vulnerabilities.

Figure 2 shows a structural attack model or attack tree, which involves certain characteristics of the ESM model. Thus, the vector mark is located on the connections from the node G-12 to the nodes G-16 and G-17, as the additional information item. The node G-15 represents a conditional subordination node, which behaves like a conventional AND-node dominated by the XOR operation. In practice, this means that you can opt for an alternative attack, presented by a subtree structure with the P-1 goal. Since this demonstration is not needed in the paper, the model does not contain a display of countermeasures or exploited vulnerabilities, which are all otherwise the characteristics of the ESM attack model. Table 1 shows a description of the nodes and Table 2 a description of the attack vectors. Furthermore, there is a reading of the model and an overview of the nodes according to the individual level.

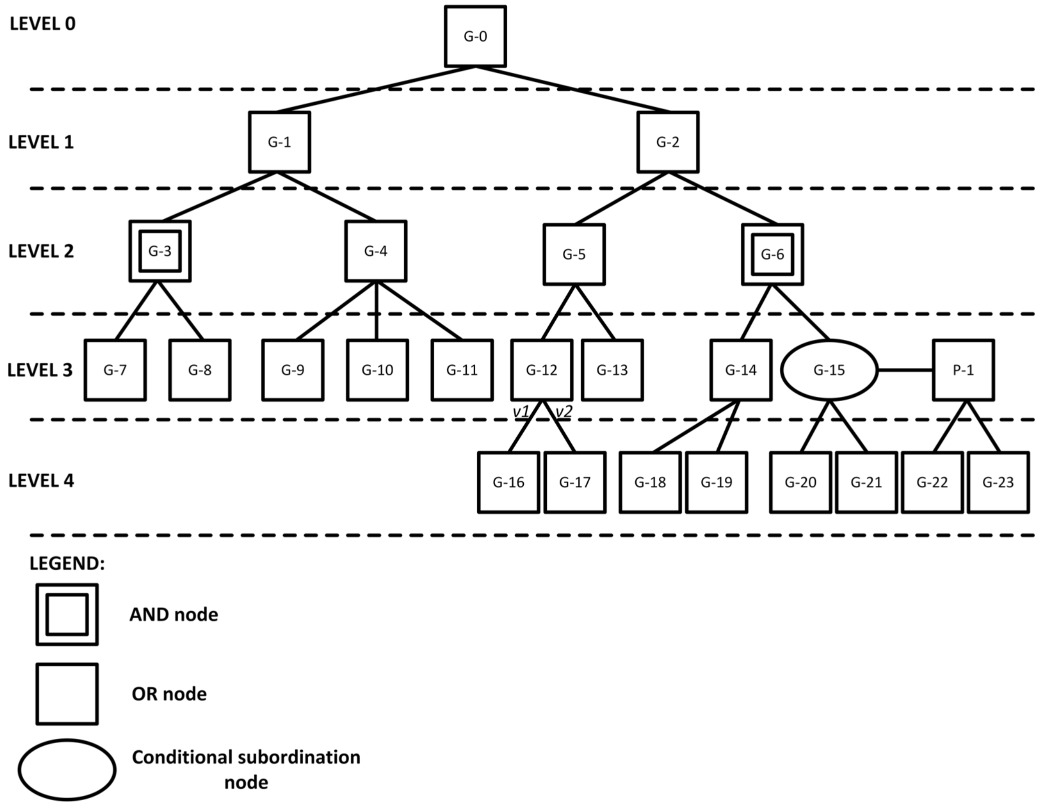

Fig. 2. Display of structural attack model on the IoT smart hub

TABLE I
DESCRIPTION OF THE NODES IN THE ATTACK MODEL

Node	Description
G-0	IoT Smart Hub attack
G-1	Physical access
G-2	Local attacks
G-3	Supply chain hack
G-4	Alter configuration settings
G-5	Cloud polling
G-6	Direct connection
G-7	Compromise supplier company's network
G-8	Trojanized software updates
G-9	New device pairing request
G-10	Resetting device to factory settings
G-11	Installing custom SSL certificate
G-12	Man-in-the-Middle (MitM) attacks
G-13	Other combined local attacks
G-14	Locate IoT devices
G-15	Exploit interface vulnerabilities
G-16	DNS spoofing
G-17	Session hijacking
G-18	IP Address/Port probing
G-19	Use of SSDP/UPnP
G-20	Results-based command injection attack
G-21	File-based blind command injection attack
G-22	Cross-site scripting attack
G-23	Cross-site request forgery
P-1	Exploit basic vulnerabilities

TABLE II
DESCRIPTION OF THE ATTACK VECTORS

Vector	Description
v1	ARP cache poisoning
v2	HTTPS stripping

Reading of the model:

The main goal of the attack, presented by the root node labelled G-0, is to attack Smart Hub device as a key modern component of the concept called the internet of things. In accordance with the displayed model, the attack can be carried out at the level of physical access (node G-1) or with an attack via a local network (node G-2). At the level of physical attack, we can choose between supply chain hack or alter configuration settings. Supply chain hack represents the AND-node G-3, which means that we first have to carry out activities in the node G-7 and then in the G-8. Such attack therefore provides compromise of the network and the use of trojanized software updates. When changing configuration settings, there are three mutually independent offensive activities predicted in accordance with the model: G-9, G-10, G-11. These can also be read from Table 1, which contains a description of the nodes.

Local attacks, presented by subtree structures with the top goal of G-2, can be carried out by attacks linked to the way in which the device operates; this is cloud polling (G-5) or direct connection (G-6). In the attacks focused on the cloud polling, the offensive approach is further better estimated and it uses man-in-the middle mechanism. Specifically, this subtree structure anticipates two mutually independent attack techniques: DNS spoofing (G-16) and session hijacking (G-17). The links to these nodes also locate codes of the attack vectors (v1 and v2), which in a form of additional information point to the supplementary use of the offensive techniques of those present in the execution of the offensive attacks (Table 2). A subtree structure which anticipates the attacks focused on the direct connection mode (node G-6) is more complex. Here, it is first necessary to locate the IoT device, which can be achieved by the application of techniques in the node G-18 or G-19. This is followed by the exploitation of the interface vulnerabilities, which is presented by the CSUB-node G-15. The latter, in addition to the techniques presented by the nodes G-20 and G-21, provides an alternative possibility of attack execution, presented by node P-1. This node continues to offer two possible techniques presented by the nodes G-22 and G-23.

An overview of nodes on individual levels:

Given the model and its reading, it is possible to perform a breakdown of the nodes at different levels in the structure of the model. The example of the attack model on the IoT smart home devices further shows that lower-level nodes move from abstract descriptions of the attacks to the increasingly sophisticated offensive approaches. The analysis of breakdown of nodes and their importance shows that it is possible to attribute the focus and the importance of individual nodes in the model according to the level at which they are located. Table 3 shows the mapping of individual level of the model and the level of the breakdown of nodes which shows different goals and activities in the attack.

TABLE III
MAPPING OF INDIVIDUAL LEVEL OF THE MODEL AND THE LEVEL OF BREAKDOWN OF NODES

Level of the model	Proposed level of the breakdown of nodes	Nodes
LEVEL 0	Abstract attack goal presented by a root node.	G-0
LEVEL 1	Display of attack surface.	G-1, G-2
LEVEL 2	Display of approaches for individual attack surface.	G-3, G-4, G-5, G-6
LEVEL 3	Concretization of attack methods.	G-7, G-8, G-9, G-10, G-11, G-12, G-13, G-14, G-15, P-1
LEVEL 4	Breakdown of attack methods in a range of attack techniques.	G-16, G-17, G-18, G-19, G-20, G-21, G-22, G-23

B. Proposal to the development approach to attack modeling

In attack modeling, it is important to comply with four opposing objectives [12]: reusability, simplicity, time and accuracy. Big time investment is also linked to the cost effect of the modeling. Consequently, it is reasonable to expect that a major time investment will result in increased reusability or better accuracy. It is necessary to know that greater accuracy of the model reduces its reusability. Simplicity is the main advantage of structural models. If we want to keep it, it is recommended to also include non-experts in the process of attack modeling. Certainly, such an approach can also have an impact on accuracy.

This paper proposes an approach based on the importance of individual nodes according to the level in the attack model. The advantages of structural models are that they enable a modular design, which allows:

- Simultaneous work of experts in various areas of the development of attack model.
- Integration of previously already designed subtree structures for specific attacks.
- Simple improvement of the model according to new or modified intelligence data entry.

Our proposal is based on the fact that the nodes at each level in the model need to have a logical substantive performance. At the same time, nodes at the deeper levels move from the general discussion of offensive approaches to more technically specific activities within the attack.

TABLE IV
PROPOSAL OF THE DEVELOPMENT APPROACH TO THE ATTACK MODELING

Step	Development approach or task	Additional recommendations and guidelines
1	Determining main attack goal, that is the contents of the root of structural attack model.	A reasonable selection of the main attack goal of the model is advisable considering the purpose and the area studied. Thus, a later aggregation of content-related models into the so-called attack forest is made possible.
2	Recognition and display of the attack surfaces with nodes at the level 1.	In this stage, it is important to include a wide range of different experts, those from the attack modeling field as well as others, such as system administrators, etc.
3	Specification of the offensive approaches with nodes at the level 2 in relation to each element of the attack surface presented by a node-predecessor.	In this step, it is already possible to divide individual subtree structures of the model into working groups formed based on field knowledge and expertise.
4	Actual display of attack methods with nodes at the level 3.	Displays at this level already involve more definite offensive approaches. It is recommended to introduce the use of the catalogue of attack techniques, tactics and procedures that has to be regularly updated.

5	Concretization of attack methods with a description of attack techniques with nodes at the level 4.	It is expected that this step already presents content of suitable technical nature. This content is already appropriate to produce so-called attack patterns or libraries.
6	Nodes in each subsequent level represent further concretizations of performance of attack techniques, which are already highly target-specific.	Nodes in each subsequent level in the model include specific approaches related to system characteristics of the target. It is recommended that modeling is based on simultaneous work in the mirror laboratory environment.

Table 4 shows a clearly demonstrated proposal of the approach to attack modeling in individual steps. Each step includes a description of functions and additional explanation. The latter leads the reader to potential input information for the model development as well as to interdisciplinary reflection. It also needs to be said that the proposed approach is primarily intended to assist in the implementation of the cyber-attack modeling in educational processes.

IV. Discussion

Concepts aimed at the proposals of development processes are poorly present and limited in the field of attack modeling. Consequently, the nodes in numerous model presentations are content-wise rather simple and lacking technical improvement. The current absence of the agreement and lack of consistency in the development approach of structural attack models limits the transfer of concepts in the field of cyber-attacks to educational environments.

Our proposal is otherwise based on a qualitative approach, which does not lead the reader to the assessment of scenarios within the model, although the quantification of the ESM model was already previously presented. However, we believe that the proposal of the development approach to attack modeling with simultaneous presentation of the work so far will contribute to the much needed shift in the field of cyber security education in terms of attack modeling.

We should not overlook the need for the excellence in the design of the development process with the application of the attack modeling methods. The development process has to be focused on the user, practical approaches have to be stressed, procedures suitably structured and logically arranged, the model itself has to be presented clearly, comprehensibly and unambiguously [14]. In practice, the aforementioned characteristics are hard to find in a single proposal for the model that would further serve as a universal tool for the design and analysis of information attacks.

V. Conclusion

This paper presents a proposal of development approach to attack modeling based on the breakdown of nodes and their importance in relation to the node-level within the tree structure of the model. This approach takes advantage of modular design offered by structural techniques for attack modeling. Logical content breakdown of nodes according to the level in the model structure will be especially welcome in educational processes in the cyber-security field and practical self-analysis of the attacks by students. A transition from abstract descriptions to technical implementations of the attacks provides a good interdisciplinary approach.

In the future, we intend to develop a structural attack model based on the technical analysis of the malicious software code. The purpose of such an approach would be to further work in the development process in the attack modeling focused on the production of libraries with patterns of individual attacks.

References

[1] P.N. Sema, P. Zavarsky, and R. Ruhl, “A critical review of attack scenarios on the IAEA Technical Guidance NSS 17 Computer Security at Nuclear Facilities,” World Congress on Internet Security (WorldCIS), pp. 87 – 90, 2014.

[2] A. Razzaqa, Z. Anwara, H. F. Ahmada, K. Latifa, and F. Munira, “Ontology for attack detection: An intelligent approach to web application security,” Computers & Security 45, pp. 124 – 146, 2014.

[3] T. Malachova, J. Malach, and Z. Vintr, “Threat characterization in vital area identification process,” 47th International Carnahan Conference on Security Technology (ICCST), pp. 1 – 6, 2013.

[4] Z. Gan, J. Tang, P. Wu, and V.A. Varadharajan, “Novel Security Risk Evaluation for Information Systems,” Japan-China Joint Workshop on Frontier of Computer Science and Technology, pp. 67 – 73, 2007.

[5] C. Maple and V.A. Viduto, “Visualisation Technique for the Identification of Security Threats in Networked Systems”, 14th International Conference Information Visualisation (IV), pp. 551 – 556, 2010.

[6] G.B. Varnado and D.W. Whitehead, “Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants”, SAND2008-5644, 2008.

[7] S. Yi, Y. Peng, Q. Xiong, and T. Wang, “Overview on attack graph generation and visualization technology,” IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID), pp. 1 – 6, 2013.

[8] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, “Attack–defense trees,” Journal of Logic and Computation 24, pp. 55 – 87, 2014.

[9] B. Ivanc and T. Klobučar, “ESM: an enhanced attack tree model for critical infrastructure,” Journal of Control Engineering and Applied Informatics 17(4), pp. 102 – 113, 2015.

[10] B. Ivanc and T. Klobučar, “Analysis of advanced cyber attacks with quantified ESM,” Cloud computing and security : First International Conference, revised selected papers, (Lecture notes in computer science, ISSN 0302-9743, vol. 9483), pp. 230 – 243, 2015.

[11] M.S. Idrees, Y. Roudier, and L. Apvrille, “Model the System from Adversary Viewpoint: Threats Identification and Modeling,” EPTCS 165, pp. 45 – 58, 2014.

[12] A. Bagnato, B. Kordy, P.H. Meland, and P. Schweitzer, “Attribute Decoration of AttackDefense Trees,” International Journal of Secure Software Engineering 3(2), pp. 1 – 35, 2012.

[13] M.B. Barcena and C. Wueest, “Insecurity in the Internet of Things,” Security response, Symantec, 2015.

[14] N.R. Prasad, “Threat Model Framework and Methodology for Personal Networks (PNs),” 2nd International Conference on Communication Systems Software and Middleware, COMSWARE 2007, pp. 1 – 6, 2007.