ELEKTROTEHNIŠKI VESTNIK 81(5): 285-292, 2014
ORIGINAL SCIENTIFIC PAPER

Attack Modeling in the Critical Infrastructure

Blaž Ivanc, Tomaž Klobučar

Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana, Slovenija
E-mail: blaz.ivanc@determinanta.si

Abstract. The development and connection of information and communication technologies with industrial control systems in the so-called critical infrastructure have contributed to the emergence of new complex threats. The critical infrastructure has become a target of sophisticated cyber attacks which exploit numerous known as well as unknown vulnerabilities in one course of an attack. The paper proposes an attack modeling method enabling us to determine the vulnerabilities and riskful exposure of the systems. Organizational changes to ensure the cyber defense of the critical infrastructure are also proposed.

Keywords: attack analysis, attack model, attack tree, enhanced structural model, incident

Modeliranje napadov v kritični infrastrukturi

Razvoj in povezanost informacijskih in komunikacijskih tehnologij z industrijskimi nadzornimi sistemi v tako imenovani kritični infrastrukturi sta pripomogla k nastanku novih kompleksnih groženj. Kritična infrastruktura je postala tarča dovršenih kibernetskih napadov, ki izkoriščajo številne, tudi neznane ranljivosti v enem poteku napada. Članek predstavlja metodo modeliranja napadov, ki nam omogoča ugotavljanje ranljivosti in izpostavljenosti sistemov. Predlagane so tudi organizacijske spremembe za zagotavljanje kibernetske varnosti kritične infrastrukture.

1 INTRODUCTION

The development and connection of information and communication technologies with industrial control systems in the so-called critical infrastructure have contributed to the emergence of new complex threats. Not long ago, the question of the industrial control system security referred to the physical security, while the main concern in terms of the information security triad, i.e. availability, confidentiality and integrity, is in particular the latter. Due to new threats and attacks, now more than ever a focus on the cyber threat and attack modeling in the critical infrastructure is necessary. The critical infrastructure may become a more frequent target of sophisticated attacks which exploit several unknown vulnerabilities in one course of the attack, including less known and completely new types of attacks. Therefore, due to the impact which can be achieved with computer-network operations, the cyber security is equally important as the physical security.

There are several definitions of the critical infrastructure. [19] describes the critical infrastructure of national importance as follows: 'The critical infrastructure of national importance in the Republic of Slovenia includes the capacities and services which are of key importance for the state and whose interruption or destruction would significantly influence and have serious consequences for the national security, economy, key social roles, health, safety and protection, and social well-being."

Before we continue, let us define a few other basic notions, such as vulnerability, threat and threat agent. [18] describes vulnerability as: "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.", and threat as: "A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm." In professional and broader terms, the entity representing a threat to the system is called a threat agent. In a malicious act, i.e. attack, the threat agent exploits the vulnerabilities of the system.

The incidents connected to control systems are divided into intentional targeted attacks, unintentional incidents and unintentional internal security events [17]. Unintentional incidents include indirect damage with unpredictable effects caused by a malicious code, for example the so-called Slammer worm, which entered the computer network of the Davis-Besse nuclear power plant in January 2003 through the unsecured network of one of the power plant's contractors. Unintentional internal security events include a variety of production malfunctions and downtimes as a result of irregularities and complications during security testing. Intentional targeted attacks include the Stuxnet malicious code detected in June 2010, which was the subject of numerous analyses and discussions in 2010 and 2011 [22]. The target of this complex malicious code spreading through a local network and removable storage devices are industrial control systems.

In addition to the increased connectivity, system complexity and interdependence, the vulnerability of systems is increased by greater information availability

Received 17 July 2014
Accepted 15 November 2014

and less knowledge required for the execution of an attack.

The aim of this paper is to present the use of an attack modeling method in a critical infrastructure. In model categorization, the paper focuses on the attack trees as a highly useful method which has been the subject of numerous studies and consequently improvements or derivatives of the original model.

The sections cover the following topics. Section 2 gives a brief overview of the critical infrastructure elements. Section 3 discusses the attack modeling methods, in particular the attack tree and the novel Enhanced structural model. Section 4 contains a practical example of an attack tree based on the Stuxnet malicious code presented with the Enhanced structural model. Section 5 includes an overview of the attack tree use in connection with the critical infrastructure and smart energy networks. Section 6 contains a discussion, while Section 7 gives a conclusion and highlights the future work.

2 CRITICAL INFRASTRUCTURE ELEMENTS

A critical infrastructure, such as electricity production, contains information systems as well as industrial control systems. The latter include:

- Supervisory control and data acquisition systems (SCADA): they are used for the dispersed asset control through a centralized supervisory control and data acquisition. The systems are referred to as the central nervous system of a wide-area control network. The development of these systems has raised fundamental questions related to the cyber security in the critical infrastructure, e.g. security assurance in the conditions of an increased connection and integration with the standard information infrastructure.
- Distributed control systems: they are part of the system control on one integral location. They represent a combination of supervising, control and data acquisition systems and programmable logic systems.
- Programmable logic controllers: they are used in the control of specific applications, most frequently in the machine control in the production process.

The control elements are a key part of one or several control sub-systems. In addition to the abovementioned programmable logic controller, we can often come across the following elements: Remote Terminal Unit (RTU), Master Terminal Unit, Human-Machine Interface, Intelligence Electronic Device, while control servers, information process bases and other control information infrastructures are also classified in this group.

The systems for the supervisory control present the upgrade of the control systems on the level of the process. They enable operators to influence the control. The distributed control systems have the following characteristics [16]:

- a large number of the process control stations,
- a control room with workstations for operators, which is also the centre for the supervisory control,
- local operating stations with a redundancy function, which is very useful in the event of a failure in the control room,
- the processes and operator stations communicate via a communication network.

The industrial control systems are of key importance in the critical infrastructure processes. The development of information and communication technologies has triggered the adjustment of protocols in terms of interoperability. As opposed to the standard information systems, the industrial control systems are time-critical and do not allow high delays. Due to the required availability, all system interventions are planned, and the attention to the possible subsequent errors is a key element of extensive system testing prior to the regular use. After setup, the abovementioned systems are rather static, have a relatively long service life and are characterized by a difficult access to individual components. This means that the system setup and maintenance require a specialized knowledge. This particularly applies to protection from the cyber attacks, where due to the specific nature of the system, prior experience and direct cooperation with the manufacturers are necessary.

[21] presents findings regarding the current situation of the security of control systems which can be divided in five groups:

- Control systems – the findings are as follows: the use of the default accounts and passwords, available visitor accounts, inadequate use of services and the presence of unnecessary services and software, uncontrolled dynamic ARP tables, allowed direct virtual private network to the control systems.
- Switches and routers – it has been found that the state of the devices is the same as at the time of the equipment installation. Furthermore, a lack of an appropriate security knowledge and experience by the operators has been found as well.
- Firewalls – in general, insufficient, inadequate and too simple rules as well as the absence of recording have been found.
- Intrusion detection systems – they represent a novelty in the control system environment. Consequently, fewer signatures as well as insufficient means and support for adequate staff training are available.

- Intrusion prevention systems – they are relatively new and difficult to set up, particularly in more demanding environments. In general, their characteristics are similar to those of the intrusion detection systems.

The control system attack risks are increased by the control system configurations accessible via the Internet, vulnerabilities and tools for exploitation of vulnerabilities, and an increase in interest and activities for the execution of control system attacks.

3 ATTACK MODELING TECHNIQUES

The attack modeling techniques mostly serve as a tool for the security analysts and support the components of practically every security risk analysis. [4] claims that information systems security engineering for security testing follows two approaches: the flaw hypothesis and the attack trees. [1] states that two prominent approaches have been developed in attack modeling: the attack trees and stochastic models. [9] presents the history of the formal graphic security models and categorizes the models as follows:

- Static or structured models, which are defined by a lack of the time dimension. These include the attack trees and Bayesian networks.
- Dynamic or behavioral models with a time dimension. This category has been divided in two parts:
    - Low-threshold models which in most cases contain different status graphs and machine-oriented representations. These include stohastic space-state models.
    - High-threshold models which are characterized by a compact representation adapted for human interpretation. These include the Petri networks and dynamic Bayesian networks.

[2] finds that the graph-based attack models can be divided in two groups, namely: a) the Petri-network-based models; b) the attack tree models. The latter are most often used to describe the course of the attack and are presented in continuation. The Petri networks represent a tool for the modeling of different systems and are represented by the so-called Petri graph.

By using different models and techniques an expert can model the past and future cyber attacks and thus develop a sense for the manner of the attack implementation and improve the ability of countermeasure management. Modeling of potential attacks facilitates the selection of appropriate security technologies and is preferable already at the design of the information systems.

The skills of the analysts – the subject-matter experts who model the attacks – are of key importance in the attack modeling. Therefore constant work on the following inter-related points is important:

- Consideration of the security issues from the threat agent's point of view.
- Monitoring of new attack techniques.
- Analysis of the attack methods.

Attack modeling is one of the most important methods for detecting weak points of the information systems and networks. It raises the security awareness and helps us to prepare for possible scenarios which we would like to avoid in practice. If we prepare ourselves for the potential security incidents, we can adequately protect the corporate environment and make sure the incidents do not occur.

3.1 Attack Tree

The attack tree is one of the static or structured model types, along with the Bayesian networks. The model has the structure of a tree and represents a formal method of attack modeling [10]. The main goal of the attack is represented in the root of the tree, while the intermediate nodes represent the obligatory or non-obligatory subgoals which need to be reached on the way to the main goal. The end nodes or leaves of the tree represent actions. After setting up the model, the nodes can be assigned the quantitative or qualitative values. The attack tree is a practical model for setting up the attack scenario. It is primarily used for the evaluation of the existing security mechanisms, but it is particularly useful in the evaluation of the security mechanisms during the system design. The attack trees require a significant practical experience and expert knowledge from the analyst, which in practice means that several analysts, who are specialized in different subgoals of an offensive nature, work on one tree.

Figure 1 shows the attack tree in the graphical and textual form. The graphical form, whose weakness is that transparency is lost with the growing scope of the attack representation, has two possible representations: in the first one, the condition to reach the goal is written in words, while in the second, graphically presented model, the execution of the condition is represented by the shape of the node, which is explained in the legend under the tree.

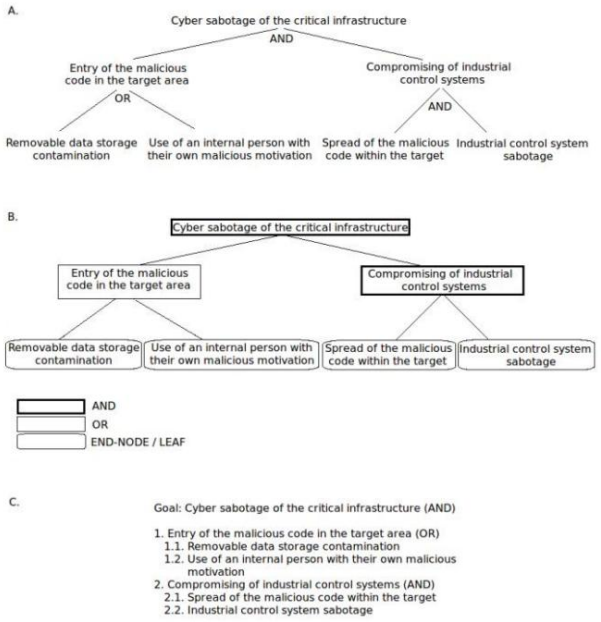

Figure 1. Same attack tree represented in two graphic variations (A. and B.), and the attack tree in a textual form (C.).

As opposed to the fault tree, the attack tree has nodes which require the execution of one or all of the descendants of the node. This means that the nodes, but not the leaves, have two Boolean operations: conjunction (AND) and disjunction (OR). With this, the author of the model has achieved his objective: to represent different attacks which the attacker can use to compromise the target. The graphic representations of attack trees use different node port identifiers. Thus, an OR-port node may have a different shape than an AND-port node; nevertheless, the nodes may also be the same, and the operation written under the node in words or with an agreed identifier.

[12] introduces the following additional nodes in the attack tree with the aim of increasing the applicability of this model in security modeling: Priority-AND, K-out-of-n (k/n), Conditional subordination (CSUB), Sequence enforcing (SEQ), and Housing node. The additional nodes facilitate the representation of the different possibilities of attack execution in relation to the diversity and changes in the system status.

The attack tree represents the basis for the protection tree and the defense tree. As opposed to the attack tree, the protection tree defines the main goal and the subgoals with a protective measure, while at the same time, it changes the node port. Thus, an AND-port node becomes an OR-port node, and an OR-port node in the attack tree becomes an AND-port node in the protection tree [11]. The attack tree presented in [13] adds one or more countermeasures to the end nodes of the attack tree.

3.2 Enhanced Structural Model

In an effort to improve the attack modeling in a critical infrastructure and remedy certain weaknesses of the existing models, we developed a model called the Enhanced Structural Model (ESM) [7].

The models, such as the ESM, are based on a modular approach which allows the expert analysts of different disciplines to work on the development of the model at the same time. The development of the model is relatively fast; however, reading can be more transparent than with some other models. The attack modeling using ESM enables better understanding of the implementation of the attacks, identification of the security weaknesses and analysis of the existing security policy. The model eliminates certain limitations that are present in the attack modeling. These are: high abstract demonstration of the attacks and low flexibility of the course of the operation to a particular target.

The attack modeling is most recommended in the design phase of the system or operations. In this way it can provide better operational safety. The attack modeling is also useful when an incident has already happened. It enables a better assessment and decision-making in relation to the handling in the next hours and days and also a subsequent analysis of the events.

Figure 2 displays an example of ESM. Its main characteristics are:

- **Use of two additional Khand's nodes to illustrate the course of the attacks**
  - Using the Khand's conditional subordination node, the internal enemy can be considered as a threat agent during the course of the attack. The use of the housing node allows us to demonstrate different time stages of the attack execution.
- **Use of labels for the exploitable vulnerabilities**
  - The vulnerability labels help us recognize the vulnerable target computer systems or software. In addition to describing the software, which is the target of exploiting vulnerabilities, the labels provide information on the complexity of a given set of attacks. Subject to the expected result of the exploited vulnerability, they also give a sense of the position for each part of the attack within the framework of the entire operation.
- **Use of labels for the attack vectors**
  - The attack vector indicates a particular method or a path for compromising the computer systems.
- **Demonstration of the countermeasures**
  - The Countermeasures in ESM appear as a set of countermeasures, the elements of which are individual security countermeasures. The aim of a set of the security countermeasures in ESM is to demonstrate what type of the

countermeasures is encountered in the implementation of the attack.

- **Segmental distribution of the model structure**
  - A segment is a logically labelled collection of the nodes that form a certain comprehensively completed sub-tree structure. Each analyst involved in assembling the model can use the dotted lines to isolate a specific part of the model and thus indicate a certain characteristic of this segment.

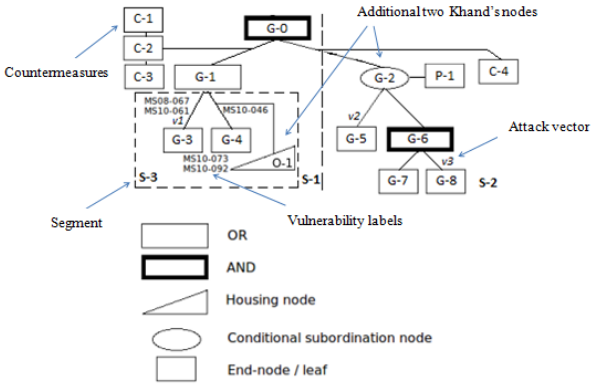

Figure 2. Example of ESM intended for information attack modeling [7].

Based on the previous work and evaluation of our model [15][7], we believe that ESM is a suitable tool for attack analysis.

4 ILLUSTRATION OF AN EXAMPLE

This section contains a representation of an attack tree whose main goal is the 'cyber sabotage of the critical infrastructure' and which is based on the known functionality of the Stuxnet malicious code. In addition to the AND and OR nodes, it also contains a conditional subordination node and a housing node. The additional nodes allow an easier modeling of the specific attacks appropriate for execution in the critical infrastructure. These are mainly the attacks that include malicious actions of employees and contractors of the critical infrastructure operator, and execution of attacks in different operating regimes.

Stuxnet is a malicious code discovered in June 2010. It is a complex and definitely the most sophisticated malicious code publically presented so far. The use of the new techniques and digital signatures enabled long-term covert operation of Stuxnet. It can be deduced from the analysis in [22] that the main target as well as ground zero of the infection with the self-replicating code were the nuclear sector facilities in Iran. Despite the numerous analyses by renowned sources, reports on this malicious code are contradictory in specific details. Furthermore, the public has still not been fully informed of the analyzed Stuxnet operation.

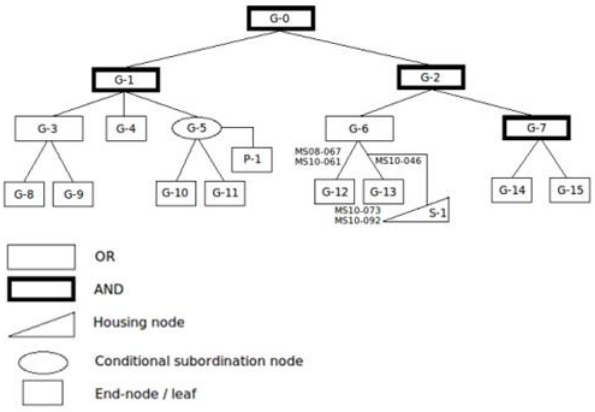

Figure 3. Attack tree with the main G-0 goal "cyber sabotage of the critical infrastructure".

Table 1: Individual node descriptions.

Node	Description
G-0	Cyber sabotage of the critical infrastructure
G-1	Malicious code infection of the target systems
G-2	Compromising of industrial control systems
G-3	Familiarization with the target systems
G-4	Development of a malicious code in a set-up image environment
G-5	Entry of the malicious code in the target area
G-6	Spread of the malicious code within the target
G-7	Industrial control system sabotage
G-8	Theft of the documentation containing system descriptions
G-9	Use of the reconnaissance malicious code
G-10	Identification of the network of persons connected to the target
G-11	Removable data storage contamination
G-12	Spreading over the local network
G-13	Spreading over a removable data storage
G-14	Compromising the computer containing the target software
G-15	Modifying the code on the programmable logic controller
P-1	Use of internal persons with their own malicious motivation
S-1	Industrial computer connected to the local network

Below, the course of the attacks with the aim of achieving both subgoals of the first level of the attack tree is described and the countermeasures are presented:

- **G-1 Malicious code infection of the target systems:** the G-1 node may be treated separately as a subtree in which the node becomes the main goal. In order to achieve this goal, all the subgoals of the node must be executed, i.e. G-3, G-4 and G-5. In accordance with the methodology, we begin with the left G-3 node. The Stuxnet design required an extensive preparation and knowledge of the target systems. The attackers achieved this by stealing the documentation or by a previously prepared malicious code which was used for familiarization with the systems - or both. Then, the G-4 subgoal must be executed where

the attackers had to set up an image environment for research and development as well as for obtaining the missing elements. The image environment is a result of the analysis of the data acquired by achieving the G-3 subgoal. The G-5 node is a conditional subordination node that represents the entry of the malicious code in the target area. This node is connected to the actuator P-1 node which anticipates an internal enemy. In this case this is a person who, due to his/her own interest or convictions, has used the access to otherwise secure systems to enter the malicious code in the target.

- **G-2 Compromising of industrial control systems:** Stuxnet spread within the target in different ways. In order to achieve the goal, it also exploited unknown vulnerabilities. According to the published analysis reports, Stuxnet exploited as many as five vulnerabilities unknown at the time of the attack. Four of them were based on the Windows operation system. Two of these were used for the malicious code reproduction, while the other two were used for the elevation of privileges on the systems. The connections between G-6 through G-12 and G-6 through G-13 contain the Microsoft update identifiers used to identify the vulnerabilities exploited during the reproduction within the target via the local network or removable data storage. Thereby, the Stuxnet designers anticipated various possibilities which ensured a higher probability of achieving the goal. Under the G-12 and G-13 nodes, there are identifiers for identifying the vulnerabilities exploited in order to elevate the privileges. The exploitation of these vulnerabilities depends on the operation system installed, which in any case is one of the anticipated Windows systems. A housing node is linked to the connection to the G-13 node. This allows simulation of the violation of the isolation rules and connection of the industrial computer to the local network through which the infection is spreading, which can thus reach the industrial computer. If the computer is isolated from the local network through which the malicious code is spreading, the transfer of the malicious code must be carried out using removable data storage. In general, spreading through the local network by using various techniques is necessary since it enables the transfer of the malicious code into the heart of the target systems.

  Stuxnet achieves the sabotage of the industrial control system, which represents the target of the G-7 node, with a modification of the code on the programmable logic controller presented in the G-15 end node. Compromising the system in the G-14 end node, which is achieved by replacing the .dll file, enables the monitoring of writing and reading, infection, and concealment of the infection of a specific programmable logic controller.

- **Countermeasures**: the use of the attack tree model enables a correct cyber defense layout, which includes [20]: a computer system and network analyses, defense-in-depth strategies, security controls, inclusion of the cyber security programs in the physical security program, and implementation of security policies and procedures.

Today, the cyber defense requires keeping up-to-date with the published research in the field of information operations, and continuous feedforward, concurrent, and feedback control. All this requires establishment of dedicated departments and hiring a specialized staff, separate from the informatics sector. This will prevent the rapidly growing number of the vulnerabilities and exposures of the information technology in the critical infrastructure.

5 RELATED WORK

Due to its characteristics, using the attack tree in attack modeling is practical and is therefore used in studies for modeling attacks on the critical infrastructure. In [3], the authors present a method used for the energy meters. The method offers the possibility of tracking the critical path of attack.

In [6], the authors present the attack tree in connection with a methodology to identify the entry points in a power system control network and evaluate the network vulnerabilities. They propose a new research in the field of sophisticated modeling techniques which would include the dynamics of the attacker and the system behavior on one hand and modeling focused on the loss of functionality and economic damage on the other. In [8], the authors introduce a framework for modeling the cyber exposure of a smart energy network. They briefly describe the attack tree, attack graph and access graph. They claim that the implementation of the smart energy networks introduces unknown risks in the existing design of a specific network. Consequently, due to numerous unknown vulnerabilities, it is difficult to truly present the final implementations of the aforementioned models.

The need to build a system which will be safe from the real-world attacks constituted the guidance for the development of the MORDA methodology ('Mission-Oriented Risk and Design Analysis') in [5]. For the purpose of analysis, the methodology uses the attack tree built on the basis of the data acquired during several

initial processes. The results of the attack tree analysis represent the basis for risk assessment. In [14], the authors introduce a supplemented attack tree in connection with the distributed denial of service. They present a path for modeling the abovementioned attack and an attack detection algorithm. The attack is based on a supplemented attack tree method.

6 DISCUSSION

The attack tree has proven to be a highly useful model since it enables a simultaneous work of the analysts of different specialties on the same tree. With a teamwork and brainstorming method, the basic model is developed relatively quickly, which is particularly suitable for the incident response, security weakness detection, and quick attack scenario design. All this speaks in favor of the use of the model in critical infrastructure attack modeling.

In the recent years, the model has been subject to numerous improvements and upgrades. New nodes have been introduced, new derivatives of the original model defined, and the nodes have been equipped with numerous attributes. The model itself is still used in relatively simplified forms and in relatively narrow fields, although its potential for being used in other scientific areas, with the need for planning different activities and responses to these activities, can be seen. Numerous discrepancies can be found in specific details, though, such as execution of actions of the specific nodes, and defining the origin of the model and its formal methodology.

Due to the interconnection of the industrial and business systems, the critical infrastructure is subject to numerous vulnerabilities. At the same time, the low commitment to weakness detection on one hand and high emphasis on the interleaving of technologies on the other, is also a cause for concern. The available properties of the critical infrastructure support systems, which are a result of the continuous system integration of new components, cause security exposure of the critical infrastructure, which is exactly the opposite of what would be desired. Every system is theoretically vulnerable, however, on the basis of the facts presented, it can be concluded that the critical infrastructure is becoming more and more exposed and vulnerable to the cyberspace threats.

Thus, the critical infrastructure attack modeling is a necessity, since it enables a timely response to the emerging threats. This requires a more extensive and in-depth presentation of the model improvements by the researchers, and identification of the already executed attacks as well as those likely to occur in the future. This will enable a faster transfer of the related knowledge to practice and a wider use of the attack modeling, and thus a greater security of the critical infrastructure.

7 CONCLUSION AND FUTURE WORK

The attack tree is a model contributing to the security weakness identification and security mechanism integration already during the system design phase. The model represents a fundamental tool for setting up attack scenarios and analyses, however, it requires experienced analysts. Fortunately, the model enables a modular approach. Due to the complexity of the coordinated attack capture, the use of the widely spread model methods and teamwork are recommended.

In view of the topic discussed, the critical infrastructure operators are advised to establish cyber defense departments which will review the security issues in terms of the threat agents. The informatics sector cannot be in charge of the cyber security; however, cooperation is necessary since it offers a different type of service. The argument supporting this are also the sophisticated critical infrastructure attack analyses showing that the attacks executing a discrete covert channel are a relatively evenly distributed combination of a physical and cyber attack backed-up by extensive intelligence efforts. Therefore, the use of the models requiring the designers to think like attackers should be encouraged.

The graphic representation of the attack tree model with the numerous nodes and attributes may become difficult to read. The solution is the textual representation which, however, lacks an agreed manner of representation of the improvements of the model in the recent years, which were primarily based on the limited graphic presentations. Thus, the current textual model representation is still on the same level as it was during popularization of the model, and represents only the tree levels and execution with the AND and OR condition.

Despite integration of the different systems in the critical infrastructure, the methods of the cyber attack protection are the same as in the standard business systems. This is also reflected in the attack modeling methods. This paper clearly demonstrates that the critical infrastructure is becoming an increasingly frequent target of attacks which are more sophisticated than the attacks on the business systems and whose goal is to cause damage in the physical environment. In most cases, these are targeted, deliberate, multi-stage attacks. Therefore, we wish to introduce an advanced methodology able to represent the dynamics of the attacks and system response, which means that it will be more suitable for use by the critical infrastructure operators.

REFERENCES

[1] Chang, Y.H.; Jirutitijaroen, P.; Ten, C.W. A Simulation Model of Cyber Threats for Energy Metering Devices in a Secondary Distribution Network. In: *5th International Conference on Critical Infrastructure*. 1–7 (Beijing, 2010).

[2] Fovino, I.N.; Masera, M.; De Cian A. Integrating cyber attacks within fault trees. In: *Reliability Engineering & System Safety 9* 1394–1402 (2009).
[3] Li, W.; Huang, J.; You W. Attack Modeling for Electric Power Information Networks. In: International Conference on Power System Technology. 1–5 (Hangzhou, 2010).
[4] Yan, J.; He, M.; Li, T.; A Petri-net Model of Network Security Testing. In: *IEEE International Conference on Computer Science and Automation Engineering*. 188–192 (Shanghai, 2011).
[5] Evans, S.; Heinbuch, D.; Kyule, E.; Piorkowski, J.; Wallner, J.; Risk-based systems security engineering: stopping attacks with intention. In: IEEE Security and Privacy **6** 59–62 (2004).
[6] Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. In: *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 4 853–865 (2010).
[7] Ivanc, B.; Modelling of Information Attacks on Critical Infrastructure by Using the Enhanced Structural Model, *Jožef Stefan IPS*, Ljubljana, M.Sc, thesis (2013).
[8] Hahn, A.; Govindarasu, M.; Smart Grid Cybersecurity Exposure Analysis and Evalution Framework. In: *IEEE Power and Energy Society General Meeting*. 1–6 (Minneapolis, 2010).
[9] Ludovic, P.C.; Bouissou , M. Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP). In: *European Dependable Computing Conference*. 199 –208. (Valencia, 2010).
[10] Camtepe, A.; Bulent, Y. Modeling and Detection of Complex Attacks. In: *Third International Conference on Security and Privacy in Communications Networks and the Workshops*. 234–243 (Nice, 2007).
[11] Edge, K. The Use of Attack and Protection Trees to Analyze Security for an Online Banking System. In: *Proceedings of the 40th Hawaii International Conference on System Sciences*. 144b–144b (Waikoloa, 2007).
[12] Khand, P.A. System level Security modeling using Attack trees. *2nd International Conference on Computer, Control and Communication*. 1–7 (Karachi, 2009).
[13] Bistarelli, S.; Fioravanti, F.; Peretti, P. Defense trees for economic evaluation of security investments. In: The First International Conference on Availability, Reliability and Security. 416 – 423 (2006).
[14] Wang, J.; Phan, R.C.; Whitley, J.N.; Parish, D.J. Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method. In: *10th International Conference on Computer and Information Technology*. 1009 – 1014 (Bradford, 2010).
[15] Ivanc, B.; Techniques and procedures of cyber attacks on critical infrastructure. In: *Management of corporate security: new approaches and future challenges*. 161–171 (2013).
[16] Groover, M. P.; Automation, Production Systems, and Computer-Integrated Manufacturing, New Jersey: Prentice Hall (2008).
[17] NIST. Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. (Gaithersburg, 2011).
[18] Shirey, R. Internet Security Glossary, Version 2 (RFC4949, 2007).
[19] Uredba o evropski kritični infrastrukturi. In: *Uradni List RS, št. 35/2011*. 4783 – 4788 (2011).
[20] NRC Regulatory guide 5.71. Cyber security programs for nuclear facilities. U.S. Nuclear Regulatory Commission. (Washington, D.C, 2010).
[21] U.S. Department for homeland security. Strategy for securing control systems. (2009).
[22] Falliere, N.; Murchu, L.O.; Chien, E. W32.Stuxnet Dossier. Symantec Security Response. (2011).

Blaž Ivanc is a researcher at the Jožef Stefan Institute. He was the professional head of the 1st International Academic Conference in the field of intelligence and security that took place in Slovenia. He is a regular lecturer at various conferences and conducts trainings in the area of information security for the key staff in corporations.

Tomaž Klobučar For the past 20 years Tomaž Klobučar has been a researcher, developer, teacher and project manager in the areas of information security and technology enhanced learning. Most of his research and development results were produced within EU Framework Programme and eContentplus R&D projects. He has authored or co-authored 80 scientific journal papers, conference papers, books and book chapters.