ELEKTROTEHNIŠKI VESTNIK 79(4): 193-196, 2012
ERK 2012 CONFERENCE ISSUE

Critical Infrastructure Attack Modeling

Blaž Ivanc[1], Tomaž Klobučar[2]

[1]Jožef Stefan International Postgraduate School
[2] Jožef Stefan Institute
E-pošta: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 several, also 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 cyber defense of the critical infrastructure are also proposed.

1 Introduction

Not long ago, the question of industrial control system security referred to physical security, while the main concern in terms of the information security triad, i.e. availability, confidentiality and integrity, was in particular the latter. Due to new threats and attacks, now more than ever a focus on 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, also unknown, vulnerabilities in one course of attack, including less known and completely new types of attacks. Therefore, due to the impact which can be achieved with computer-network operations, cyber security is equally important as physical security.

There are several definitions of critical infrastructure. [9] 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 national security, economy, key social roles, health, safety and protection, and social well-being.”

The incidents connected to control systems are divided into intentional targeted attacks, unintentional incidents and unintentional internal security events [10]. Unintentional incidents include indirect damage with unpredictable effects caused by 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. The target of this complex malicious code spreading through a local network and removable storage devices is industrial control systems.

The aim of this article is to present the attack modeling method in relation to the critical infrastructure. In model categorization, the article focuses on attack trees as a highly useful method, which has been the subject of numerous scientific studies and consequently improvements or derivatives of the original model. The article is based on an overview of studies, the existing literature and processes, with an additional comment and the presentation of the use of the abstraction and concretization method.

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

2 Critical infrastructure elements

A critical infrastructure, such as electricity production, contains information systems as well as industrial control systems including SCADA systems, distributed control systems and programmable logic controllers.

Industrial control systems are of key importance in the critical infrastructure processes. [11] presents the findings regarding the current situation of the security of control systems which can be divided in five groups:

- Control systems – the use of default accounts and passwords, available visitor accounts, inadequate use of services and the presence of unnecessary services and software, uncontrolled dynamic ARP tables and allowed direct virtual private network to control systems.
- Switches and routers – it has been established that the state of devices is the same as at the time of equipment installation. Furthermore, a lack of appropriate security knowledge and experience by the operators has been established as well.

- Firewalls – in general, insufficient, inadequate and too simple rules as well as the absence of recording have been established.
- 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 intrusion detection systems.

[12] warns that control system attacks risks are increased by control system configurations accessible via the Internet, vulnerabilities and tools for the exploitation of vulnerabilities, and an increase in interest and activities for the execution of control system attacks. The source stresses the increase in easily accessible tools for known vulnerability exploits. In addition, it detects an increase in the interest in attacks on control systems by hacktivist groups which use the aforementioned tools to attack critical infrastructure assets without practically any specialized knowledge.

3 Attack modeling techniques

Attack modeling techniques mostly serve as a tool for security analysts and support the components of practically every security risk analysis. [1] states that two prominent approaches have been developed in attack modeling: attack trees and stochastic models. [6] presents the history of formal graphic security models and thus categorizes the models as follows:

- Static or structured models, which are defined by a lack of the time dimension. These include attack trees and Bayesian networks.
- Dynamic or behavioral models with a time dimension. This category has been divided into two parts:

  - Low-threshold models which in most cases contain different status graphs and machine-oriented representations. These include stochastic space-state models.

  - High-threshold models which are characterized by a compact representation adapted for human interpretation. These include Petri networks and dynamic Bayesian networks.

The attack tree is one of the static or structured model types, along with Bayesian networks. The model has the structure of a tree and represents a formal method of attack modeling. The main goal of 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, nodes can be assigned 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 security mechanisms during system design. Attack trees require 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. The model proves to be extremely useful since it enables modular tree design.

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. 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, nodes may also be the same, and the operation written under the node in words or with an agreed identifier. [7] 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.

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 AND and OR nodes, it also contains a conditional subordination node and a housing node. The additional nodes allow easier modeling of specific attacks appropriate for execution in the critical infrastructure. These are mainly attacks that include malicious actions of employees and contractors of the critical infrastructure operator, and the 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 new techniques and digital signatures enabled long-term covert operation of Stuxnet. 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.

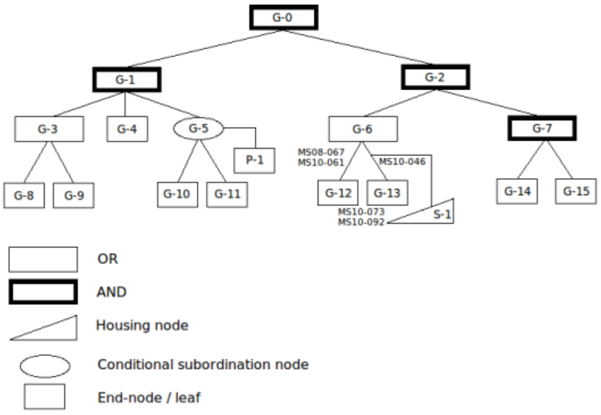
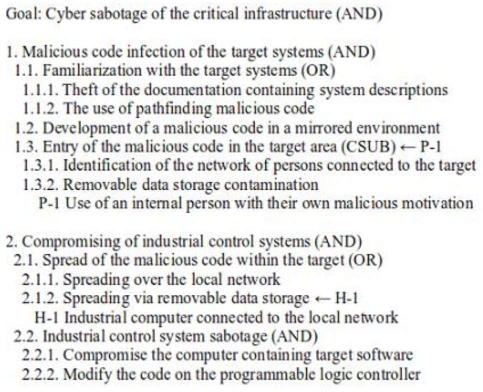


Figure 1. The attack tree with the main goal G-0 'cyber sabotage of the critical infrastructure'.

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 mirrored 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	The use of 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 via removable data storage
G-14	Compromise the computer containing target software
G-15	Modify the code on the programmable logic controller
P-1	Use of an internal person with their own malicious motivation
S-1	Industrial computer connected to the local network


Goal: Cyber sabotage of the critical infrastructure (AND)

1. Malicious code infection of the target systems (AND)
 1.1. Familiarization with the target systems (OR)
  1.1.1. Theft of the documentation containing system descriptions
  1.1.2. The use of pathfinding malicious code
 1.2. Development of a malicious code in a mirrored environment
 1.3. Entry of the malicious code in the target area (CSUB) ← P-1
  1.3.1. Identification of the network of persons connected to the target
  1.3.2. Removable data storage contamination
   P-1 Use of an internal person with their own malicious motivation

2. Compromising of industrial control systems (AND)
 2.1. Spread of the malicious code within the target (OR)
  2.1.1. Spreading over the local network
  2.1.2. Spreading via removable data storage ← H-1
   H-1 Industrial computer connected to the local network
 2.2. Industrial control system sabotage (AND)
  2.2.1. Compromise the computer containing target software
  2.2.2. Modify the code on the programmable logic controller

Figure 2. Attack tree from Figure 1 in textual form.

Below, the course of 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. G-5 is a conditional subordination node that represents the entry of the malicious code in the target area. This node is connected to the actuator node P-1, which anticipates an internal enemy, in this case a person who, due to their own interest or convictions, has used the access to otherwise secure systems to enter the malicious code in the target.

- G-2 Compromising industrial control systems: Stuxnet spread within the target in different ways. In order to achieve the goal, it also exploited unknown vulnerabilities. The connections between G-6 through G-12 and G-6 through G-13 contain Microsoft update identifiers, which are used to identify the vulnerabilities that have been exploited during the reproduction within the target via the local network or removable data storage. Under the G-12 and G-13 nodes, there are identifiers for identifying the vulnerabilities exploited in order to elevate the privileges. A housing node is linked to the connection to the G-13 node. This allows the simulation of the violation of isolation rules and the connection of the industrial computer to the local network through which the infection is spreading, which can thus reach the industrial computer.

- Countermeasures: Today, cyber defense requires keeping up-to-date with the published research in the field of information operations, and continuous feedforward, concurrent, and feedback control. The use of the attack tree model enables the correct cyber defense layout.

5 Related work

Due to its characteristics, the use of the attack tree in attack modeling is practical and therefore used in studies for modeling attacks on the critical infrastructure. In their study, [2] present the method in connection with energy meters. According to the authors, the model offers the possibility of tracking the critical path of attack.

[4] present the attack tree in connection with the methodology whose purpose is to identify the entry points in the power system control network, and evaluate network vulnerabilities. They propose new research in the field of sophisticated modeling techniques, which would include the dynamics of the attacker's and the system behavior on the one hand, and modeling focused on the loss of functionality and economic damage on the other. [5] introduce the framework for the modeling of cyber exposure of a smart energy network. They briefly describe the attack

tree, attack graph and access graph. The authors claim that the implementation of smart energy networks introduces unknown risks in the existing design of a specific network. Consequently, due to all the 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 [3]. For the purpose of analysis, the methodology uses the attack tree built on the basis of data acquired during several initial processes. The results of the attack tree analysis represent the basis for risk assessment. [8] introduce a supplemented attack tree in connection with the distributed denial of service. In their work, the authors present the path for modeling the aforementioned attack and the attack detection algorithm. The attack is based on the supplemented attack tree method.

6 Discussion

The attack tree enables the simultaneous work of analysts of different specialties on the same tree. With teamwork and the brainstorming method, the basic model is developed relatively quickly, which is particularly suitable for incident response, security weakness detection, and quick attack scenario design.

Due to the interconnection of the industrial and business systems, the critical infrastructure is subject to numerous vulnerabilities. The available features of the critical infrastructure 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. This is logical since 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 cyberspace threats.

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

7 Conclusion and future work

The attack tree is a model contributing to security weakness identification and security mechanism integration already during system design. The model represents a fundamental tool for setting up attack scenarios and analyses; however, it requires experienced analysts. The graphic representation of the attack tree model with 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 limited graphic presentations. Therefore, in the future, we wish to introduce our own attack tree model presentation in a more in-depth, useful and textual form which will allow the representation of all nodes and the connections between them.

In view of the topic discussed, critical infrastructure operators are advised to establish cyber defense departments which will review security issues in terms of threat agents. Therefore, the use of models requiring designers to think like attackers should be encouraged.

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] Li, W., Huang, J., You W. *Attack Modeling for Electric Power Information Networks.* In: International Conference on Power System Technology. 1–5 (Hangzhou, 2010).

[3] 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).

[4] 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).

[5] Hahn, A., Govindarasu, M. *Smart Grid Cybersecurity Exposure Analysis and Evaluation Framework.* In: IEEE Power and Energy Society General Meeting. 1–6 (Minneapolis, 2010).

[6] 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).

[7] Khand, P.A. *System level Security modeling using Attack trees.* In: 2nd International Conference on Computer, Control and Communication. 1–7 (Karachi, 2009).

[8] 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 (2010).

[9] Uredba o evropski kritični infrastrukturi. In: Uradni List RS, št. 35/2011. 4783 – 4788 (2011).

[10] National Institute of Standards and Technology. *Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security.* (Gaithersburg, 2011).

[11] U.S. Department for homeland security. *Strategy for securing control systems.* (2009).

[12] ICS-CERT. ICS-ALERT-12-046-01 - *Increasing threat to industrial control systems.* (2012).