Chapter 15

ASSESSING THE IMPACT OF CYBER ATTACKS ON INTERDEPENDENT PHYSICAL SYSTEMS

Antonio Di Pietro, Chiara Foglietta, Simone Palmieri and Stefano Panzieri

Abstract Considerable research has focused on securing SCADA systems and the physical processes they control, but an effective framework for the real-time impact assessment of cyber attacks on SCADA systems is not yet available. This paper attempts to address the problem by proposing an innovative framework based on the mixed holistic reductionist methodology. The framework supports real-time impact assessments that take into account the interdependencies existing between critical infrastructures that are supervised and controlled by SCADA systems. Holistic and reductionist approaches are complementary approaches that support situation assessment and evaluations of the risk and consequences arising from infrastructure interdependencies. The application of the framework to a sample scenario on a realistic testbed demonstrates the effectiveness of the framework for risk and impact assessments.

Keywords: Cyber attacks, SCADA systems, impact assessment, testbed

1. Introduction

The risk of cyber attacks that can compromise the operation of critical infrastructures such as electricity and water distribution systems has increased due to network connectivity and convergence, strong attacker motivation and expertise, and the use of general-purpose and open communication protocols for communications and control. Evaluating the impact of cyber attacks is a complex task due to intra-system interactions and interdependencies. Moreover, interactions between infrastructure components and the infrastructures themselves lead to cascading effects are difficult to model and evaluate.

Supervisory control and data acquisition (SCADA) systems are employed widely in the critical infrastructure to control physical processes. However,

J. Butts and S. Shenoi (Eds.): Critical Infrastructure Protection VII, IFIP AICT 417, pp. 215–227, 2013.
© IFIP International Federation for Information Processing 2013

SCADA systems rely heavily on information and communications technologies (ICTs); these technologies exhibit numerous vulnerabilities that can be exploited by cyber attacks, especially those involving malware such as viruses and worms. The often-cited Stuxnet worm [7] that targeted SCADA systems was able to alter the behavior of programmable logic controllers (PLCs). Indeed, despite the adoption of security policies, firewalls and intrusion detection systems across the critical infrastructure, SCADA systems and their networks remain vulnerable as a result on their ICT layer. For these reasons, all impact assessments of faults should also consider cyber attacks [5].

Several research efforts have focused on developing simulation environments that evaluate the impact of malware on critical infrastructure systems. The possibility of modeling and performing cyber attacks in a controlled simulation environment allows SCADA operators to develop and test security standards with the aim of preventing and/or reducing the impact of attacks on physical processes. Due to the difficulty – and danger – involved in performing security tests on real-world SCADA systems [16], SCADA security researchers typically employ hybrid simulation environments that integrate commercial software used in real SCADA systems and simulated components that emulate SCADA networks and devices (e.g., routers and PLCs).

However, most SCADA security testbeds are incapable of modeling and simulating critical infrastructure interdependencies [8]. This paper attempts to overcome this limitation. It describes a SCADA security testbed that engages infrastructure interdependency models in performing impact assessments. The approach seeks to provide SCADA operators with qualitative and quantitative measurements of (near-term) future risk to reduce the decision-making time and effort, and to improve the outcome. The approach is based on the mixed holistic reductionist (MHR) model [2, 3], a general formalism that can describe large, complex systems like critical infrastructures and with their interdependencies and the impact of faults. MHR employs CISIA [4], an agent-based system for modeling and simulating interdependencies. CISIA models each physical component as an agent that exhibits: (i) an operative level, which is defined as the ability to perform the required task; (ii) a set of resources needed by the component to operate; and (iii) a set of faults that can affect the component. The MHR approach has been validated by research conducted under the EU FP7 MICIE Project [20]. It is currently being used in the EU FP7 CockpitCI Project [18] to investigate the real-time impact of cyber attacks on the quality of service (QoS) delivered by targeted critical infrastructure assets.

2. Related Work

This section discusses research efforts related to SCADA security testbeds and models for analyzing critical infrastructure interdependencies.

Queiroz, *et al.* [16] have designed a testbed for investigating attacks that affect system functionality. The testbed, which is based on a real SCADA network, incorporates a human-machine interface (HMI), remote terminal units (RTUs), and sensors and actuators connected to a corporate network over the

Internet. McDonald, *et al.* [14] have developed a testbed based on a customized simulation framework for analyzing the interactions between a physical process, control devices and a SCADA network. Genge, *et al.* [10] have developed a network emulator environment, which simulates the cyber layer of a SCADA system (e.g. RTUs and process control software) that controls a simplified water purification plant modeled using Matlab. The environment allows the evaluation of the consequences of cyber attacks on the physical process.

In the area of interdependency modeling, Ghorbani, *et al.* [11] have presented a classification and comparison of interdependency modeling and simulation tools for critical infrastructures. The Interdependency Infrastructure Simulator (I2Sim) [17] provides a power simulation environment that models interdependencies between critical infrastructures based on resource requirements and distribution. The core component of I2Sim is a production cell, a functional unit that needs a certain quantity of one or more input resources to produce an output resource. The production cell is associated with a matrix called the human readable table, which encapsulates the behavior of the modeled component by associating input quantities with output quantities. Hierarchical holographic modeling (HHM) [13] facilitates the modeling of complex systems at different levels, including the physical, organizational and managerial levels. HHM has been applied to SCADA systems to evaluate the risk of cyber attacks on controlled critical infrastructures [6].

Agent-based models developed for analyzing complex systems can be applied to critical infrastructure protection. These include NetLogo [21], a multi-agent programming language and modeling framework used to analyze natural and social science phenomena. Another framework is RePast [1], which uses genetic algorithms and neural networks to model the behavior of concurrent agents. Yet another is SimJADE [12], a multi-agent framework based on discrete event simulation that supports generic interaction protocols for agent communications.

Existing SCADA security testbeds have been employed to study the impact of cyber attacks on physical processes, but they do not employ infrastructure interdependency models to evaluate the real-time cascading effects. In contrast, our testbed specifically incorporates interdependency models. This helps evaluate how cyber attacks on SCADA systems can induce cascading effects on interdependent physical processes (e.g., physical and cyber [15]).

This work has been undertaken under the FP7 CockpitCI Project [18]. The project seeks to improve the dependability and resilience of critical infrastructures by providing operators with efficient tools that help prevent cyber attacks and implement consequence containment strategies in the event of attacks. The CockpitCI Project is a follow-up to the MICIE Project [20] that focused on the creation of a distributed alert system for the early detection of cascading physical faults. The alert system to be developed under the CockpitCI Project will: (i) incorporate smart detection agents that monitor potential cyber threats in various networks (e.g., SCADA and IP networks); (ii) identify in real-time the critical infrastructure functionality that is impacted by cyber attacks and assess the degradation of the delivered services; (iii) broadcast alert messages to other

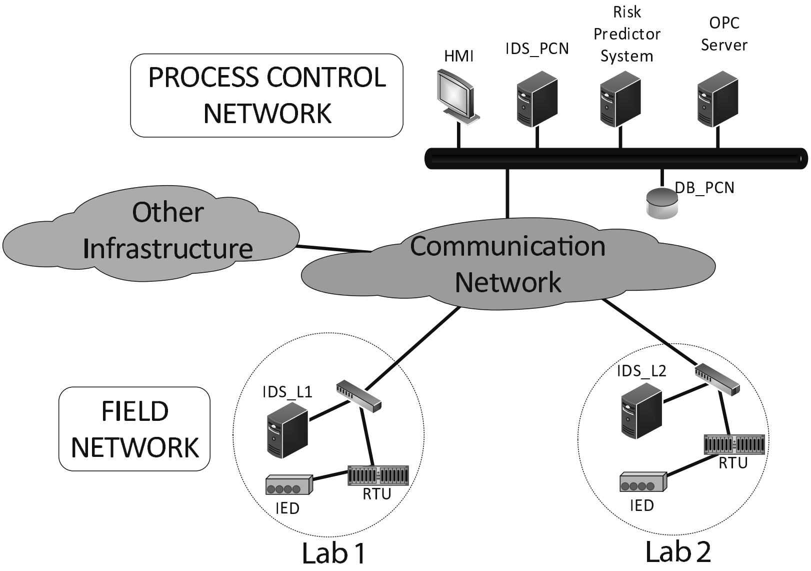


Figure 1. SCADA testbed architecture.

critical infrastructures at different security levels; and (iv) support containment strategies that address the consequences of cyber attacks in the short, medium and long terms.

3. SCADA Testbed Architecture

The SCADA security testbed engages a typical client-server SCADA network architecture, which incorporates PLCs, RTUs, intelligent electrical devices (IEDs) and an HMI. Two key components are an integrated risk predictor system (IRP) and a set of intrusion detection systems (IDSs). These two components support the evaluation of the impact of cyber attacks on the physical components controlled by the SCADA system. The SCADA network spans two laboratories, one located at the University of Roma Tre and the other at ENEA, also in Rome, Italy. The distribution of SCADA network nodes over the Internet helps model the large geographic scale of real-world SCADA systems.

Figure 1 shows the reference architecture of the SCADA security testbed. The architecture incorporates the following components:

- **Process Control Network:** This network serves as the connection layer for the SCADA equipment. A database (DB_PCN) stores information about field equipment. An HMI provides operators with a facility for visualizing data and information. The data and information can be accessed by other operators via an open platform communications (OPC) server as well as by the IRP, which performs a situation assessment by computing the risk level associated with the state of the considered critical

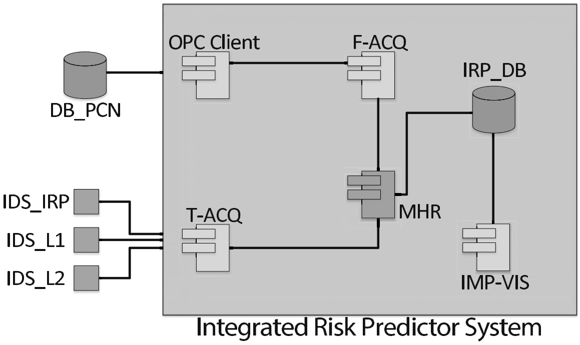


Figure 2. Integrated risk predictor architecture.

infrastructure and evaluating the impact of cyber attacks. Cyber attacks are detected using IDSs associated with the critical infrastructures and relayed to the network (IDS_PCN) whose output is merged into the IRP.

- **Field Network:** This network includes sensors, actuators (IEDs) and RTUs, and supports the acquisition of process field data and the execution of control actions. Two IDSs (IDS_L1 and IDS_L2), one at each laboratory, monitor traffic directed at the RTUs, perform local cyber attack detection and notify the IRP about possible malicious activity to enable it to support global risk assessments. An attacker is assumed to be located in this network and can launch attacks that compromise SCADA system functionality.

- **Communication Networks:** This network uses the Internet to connect the process control and field networks.

4. Integrated Risk Predictor Architecture

Figure 2 presents the modular structure of the IRP. The IRP has six main components: (i) mixed holistic reductionist (MHR) unit; (ii) failure acquisition (F-ACQ) unit; (iii) threats acquisition (T-ACQ) unit; (iv) OPC client; (v) impact visualization (IMP-VIS) interface; and (vi) IRP database (DB_IRP).

- **Mixed Holistic Reductionist Unit:** This unit performs the real-time impact analysis of faults and cyber attacks on a set of critical infrastructures through the execution of an agent-based model. The model represents a network of heterogeneous systems that exhibit interdependencies. The MHR model captures critical infrastructures at different hierarchical levels: holistic, reductionist and service layers. For each critical infrastructure, agents are used to model the production, supply and transportation (or consumption) of tangible or intangible resources: goods, policies, operative conditions, etc. The capability of each agent to provide the required resources depends on its operative condition, which is based on the availability of the resources that it requires and on the severity of the failures that affect it. The F-ACQ and T-ACQ units provide the MHR model with real-time information about failures and attacks, respectively.

- **Failure Acquisition Unit:** This unit extracts information about physical device failures from the real-time data provided by the SCADA database. The set of failures and the measurement values are input to the MHR unit to help conduct real-time impact assessments of the considered critical infrastructures. The F-ACQ unit translates the data into an appropriate format for input to the MHR unit.

- **Threats Acquisition Unit:** This unit collects real-time data from the set of IDSs that provide local and global cyber attack detection assessments. The data includes log data and alert messages produced when malicious attacks are detected. This unit, like the F-ACQ unit, translates data into an appropriate format for input to the MHR unit. Communications between the T-ACQ unit and the IDSs are handled using web service technology: each IDS hosts a web service that accepts requests from web clients hosted by the T-ACQ unit.

- **OPC Client:** The OPC client queries real-time data from the SCADA database (DB_PCN) at a fixed rate. This data, which includes equipment faults and failures and measurement values, is passed to the F-ACQ unit.

- **Impact Visualization Interface:** This unit provides the operator with a graphical user interface (GUI) that shows the real-time status and the predicted impact of failures and attacks on the considered critical infrastructures.

- **IRP Database:** This unit stores the results of MHR model executions. The MySQL database incorporates a historian that maintains all the data for offline analyses.

5. MHR Modeling

The mixed holistic reductionist (MHR) approach supports the modeling and evaluation of interdependencies existing between critical infrastructures. Interdependency identification relies on the interaction of two different approaches, holistic and reductionist methods.

Holistic models focus on a single critical infrastructure and the evolution of an event within the critical infrastructure, ignoring events in other infrastructures. These models are usually created in collaboration with sector experts and embed complex dynamics related to the single infrastructure (e.g., transient behavior of a power grid when a breaker is opened). In contrast, reductionist models capture elements of multiple critical infrastructures in order to model interdependencies existing between the infrastructures.

Figure 3 shows the MHR modeling technique. The upper boxes represent the holistic approach for two interdependent infrastructures. A situation as-

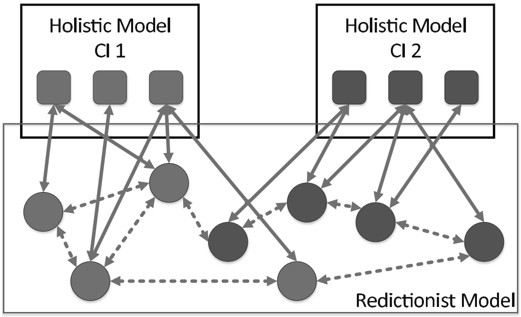


Figure 3. Mixed holistic reductionist modeling technique.

sessment at this level of abstraction is realized by considering several technological and organizational aspects and using techniques and methods specific to each infrastructure. In this context, important services directed towards customers are defined along with the possible impacts due to endogenous faults and threats. An example is the detection of possible cyber attacks on a telecommunications network and the evaluation of the effects on the network. The lower boxes model the reductionist approach, which evaluates interdependencies and propagates faults. At this level, the evaluation of cyber attacks on real equipment is considered, including the equipment responsible for interdependencies such as remote-controlled circuit breakers and switches in a power grid.

6. Attack Scenario

This section focuses on a scenario involving a cyber attack on the reconfiguration service of a power grid, which is controlled by a SCADA system. The scenario incorporates three infrastructures: a medium voltage power grid controlled by a SCADA system via a telecommunications network that connects the control center with the RTUs. Each RTU incorporates a modem connected to a switch; it receives and transmits data in order to open or close the switch. The Modbus/TCP protocol is used for RTU communications. Control actions are implemented by a PLC connected to the HMI. Figure 4 shows the data workflow starting from an attack occurrence to attack impact assessment.

The impact evaluation focuses on the effects of faults and cyber attacks on the services provided by the coupled infrastructures. Note that the services include those supplied to customers (e.g., electricity) as well as those that enable each critical infrastructure to be reconfigured.

6.1 Attack Execution

The scenario involves a man-in-the-middle attack by an attacker located in the process control network or at one of the two laboratories connected to the field devices (see Figure 1). The attacker can eavesdrop on the messages between the two hosts as well as modify messages to send fake data to a host.

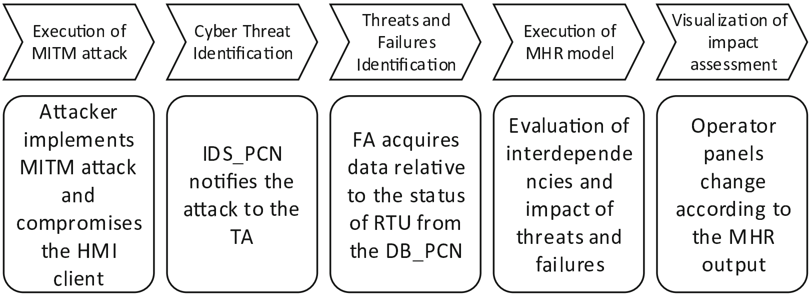

Execution of MITM attack
Cyber Threat Identification
Threats and Failures Identification
Execution of MHR model
Visualization of impact assessment
Attacker implements MITM attack and compromises the HMI client
IDS_PCN notifies the attack to the TA
FA acquires data relative to the status of RTU from the DB_PCN
Evaluation of interdependencies and impact of threats and failures
Operator panels change according to the MHR output

Figure 4. Attack scenario data workflow.

The man-in-the-middle attack exploits a vulnerability in the address resolution protocol (ARP). The attack is commonly referred to as ARP poisoning (spoofing). The attack was performed using Ettercap [19], a packet injector that manipulates ARP tables, enabling the attacker to compromise an RTU (e.g., by manipulating a message or sending fake commands to the RTU).

6.2 Attack Identification

The TCP layer of the Modbus/TCP protocol provides a sequence number that is unique for each session. However, as described in [9], Modbus only accepts the first response received and discards additional responses.

We used Snort as an IDS to detect ARP attacks, unicast ARP requests and inconsistent Ethernet-IP address mappings. In particular, Snort was configured to detect changes in the mappings between valid MAC addresses and IP addresses in order to detect ARP poisoning attacks originating from the SCADA network.

The T-ACQ unit acquires data from the IDSs while the F-ACQ unit acquires data from the real equipment (e.g., HMI). Web service technology is used for connections between the T-ACQ unit and the IDSs: each IDS represents a server and the T-ACQ unit is the client that "polls" the servers to obtain updated information. The connections between the F-ACQ and the real equipment are realized using the OPC client/server architecture.

The T-ACQ and F-ACQ outputs are passed to the MHR model (Figure 5). The outputs of the two units are in the form of XML files with the same structure for both units. A specific XML element specifies the attack type and another element represents the severity of the attack.

6.3 MHR Model Execution

The MHR model was realized using the CISIA agent-based software [4]. The CISIA software models every element (equipment, service, policy or entity) as an agent using a common representation. Each agent is described by its inputs and outputs. Agents exchange resources, such as telecommunication packets, power flows and service levels. Agent behavior is affected by faults

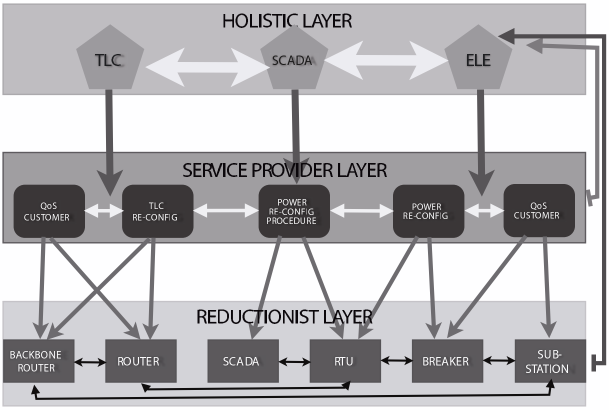


Figure 5. Infrastructure interdependency model.

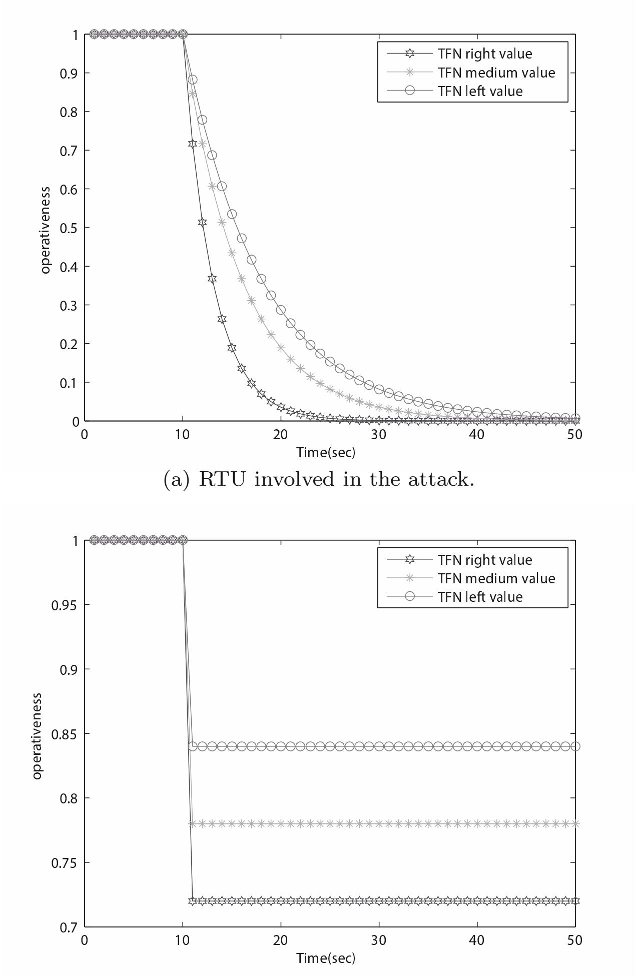
and failures. The internal representations of agents may be heterogeneous; however, the coupling of the agents with several internal models is achieved using a common exposed interface. Each agent is represented by its operative level or operativeness, the ability of the agent to produce goods and services.

The CISIA simulator uses triangular fuzzy numbers to handle uncertainty. A triangular fuzzy number is expressed using four (crisp) numbers: left, middle, right and height values.

Figure 5 shows the principal agents in the MHR model implementation. Three holistic nodes are shown, one for each critical infrastructure. The services are shown as purple boxes: the quality of service for customers of the telecommunications network and power grid, the automatic telecommunications reconfiguration procedure, and the reconfiguration of the power grid related to the SCADA network and the power reconfiguration topology. The reconfiguration of the power grid needs the SCADA network and the telecommunications network in order to send and receive messages to and from switches via the RTUs. The reconfigured topology of the electric grid is determined based on the ability of each line to feed customers after a power fault. The main objects in the reductionist layer are the telecommunications network routers, the SCADA control center and RTUs, and the switches, breakers and substations in the power grid. To simplify the presentation, Figure 5 does not show the other elements and agents.

6.4 Impact Evaluation

A man-in-the-middle attack can have several outcomes. Surveillance attacks collect information about the SCADA system and RTUs and the messages they exchange, or they read requests issued by the HMI to RTUs. More serious attacks modify reply messages (e.g., randomly or using a “NOT” operator, which would close a circuit breaker instead of opening it). Other attacks change messages transmitted between the HMI and RTUs. These attacks can compromise



(a) RTU involved in the attack.

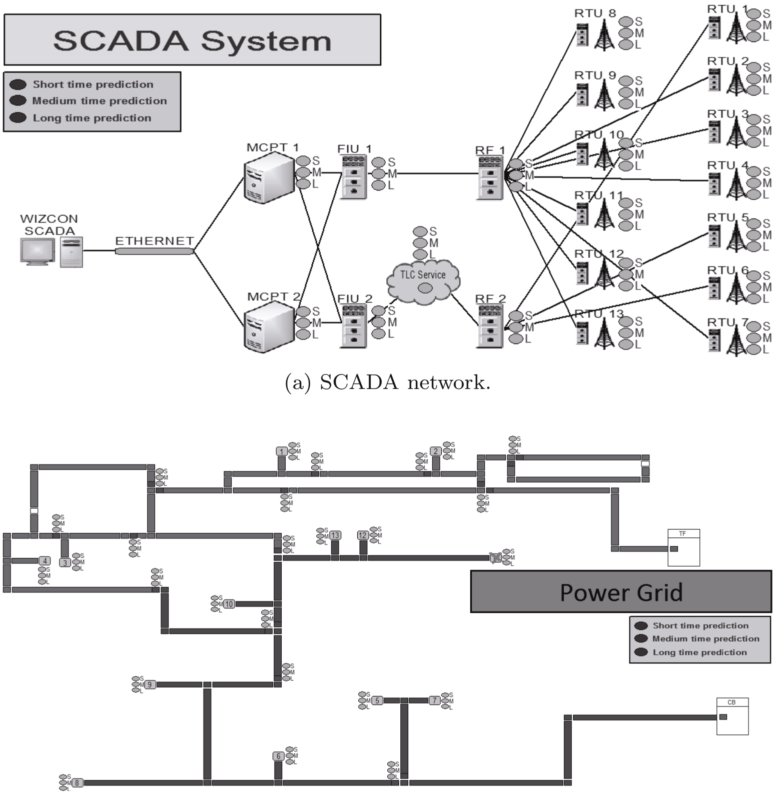
(b) Reconfiguration service in the power grid.

Figure 6. CISIA operative levels.

the functionality of the SCADA system by altering the control strategy and ultimately affecting the physical system.

The implemented attack changes the values of messages sent from the HMI to the RTUs, which are connected to circuit breakers and switches. Figure 6(a) shows the behavior of an RTU under attack (computed using CISIA). The behavior exhibits an exponentially-decreasing trend starting at the attack start time ($t = 10$). Note that the RTU should execute commands from the HMI only in the event of a fault in the power grid.

The reconfiguration service in the power grid involves operator-initiated procedures that change the topology of the power grid after a fault has occurred.



(a) SCADA network.

(b) Power grid.

Figure 7. Operator panels for the SCADA network and power grid.

These procedures are implemented by the HMI sending commands to selected RTUs to open or close switches. The reconfiguration procedures cannot be executed if one or more RTUs are affected by the attack. Figure 6(b) shows the operative level of the power grid reconfiguration service. Note that in Figures 6(a) and 6(b), three values (i.e., left, middle and right values) are used to represent triangular fuzzy numbers. The y-axis values are between 0.7 and 1.0; the height values are not shown because these values are always equal to 1.0.

Figure 7 shows the operator panels, which present the system behavior to operators in a simple and effective manner. The panels show system snapshots with the possible impact in the near future using colored circles to express the severity of equipment faults.

The operative level of each element is specified using a red cross if the element is not working (e.g., a load in Figure 7(b)). A circle near an element denotes the prediction of its operative level during the next iteration. Note that S denotes a small time prediction (during the next step), M a medium time prediction (during two time steps) and L a large time prediction (during three time steps).

7. Conclusions

The experimental testbed described in this paper supports real-time impact assessments of cyber attacks on interdependent critical infrastructures. The sample scenario focused on the evaluation of the impact on services provided by a SCADA system that controls a power grid. The physical layer and the services provided by the two infrastructures were modeled using the CISIA agent-based tool. The experimental results involving a man-in-the-middle attack on a SCADA RTU demonstrate the utility and effectiveness of the testbed as a means for providing infrastructure operators with the current status as well as the predicted impact on key infrastructure components and services.

Our future research will continue to refine the testbed and the modeling framework. Also, it will investigate more complex attacks on interdependent critical infrastructures, including stealth attacks that modify packet content in SCADA-RTU communications.

Acknowledgement

This research was partially supported by EU Project Cockpit-CI FP7-SEC-285647/2012.

References

[1] N. Collier, RePast: An extensible framework for agent simulation, *Natural Resources and Environmental Issues*, vol. 8(1), article no. 4, 2001.

[2] S. De Porcellinis, G. Oliva, S. Panzieri and R. Setola, A holistic-reductionistic approach for modeling interdependencies, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 215–227, 2009.

[3] S. De Porcellinis, S. Panzieri and R. Setola, Modeling critical infrastructure via a mixed holistic reductionistic approach, *International Journal of Critical Infrastructures*, vol. 5(1/2), pp. 86–99, 2009.

[4] S. De Porcellinis, S. Panzieri, R. Setola and G. Ulivi, Simulation of heterogeneous and interdependent critical infrastructures, *International Journal of Critical Infrastructures*, vol. 4(1/2), pp. 110–128, 2008.

[5] G. Digioia, C. Foglietta, S. Panzieri and A. Falleni, Mixed holistic reductionistic approach for impact assessment of cyber attacks, *Proceedings of the European Intelligence and Security Informatics Conference*, pp. 123–130, 2012.

[6] B. Ezell, Y. Haimes and J. Lambert, Risks of cyber attack to water utility supervisory control and data acquisition (SCADA) systems, *Military Operations Research*, vol. 6(2), pp. 23–33, 2001.

[7] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Symantec, Mountain View, California, 2011.

[8] C. Foglietta, G. Oliva and S. Panzieri, Online distributed evaluation of interdependent critical infrastructures, in *Nonlinear Estimation and Applications to Industrial Systems Control*, G. Rigatos (Ed.), Nova Science, New York, pp. 89–120, 2012.

[9] W. Gao, T. Morris, B. Reaves and D. Richey, On SCADA control system command and response injection and intrusion detection, *Proceedings of the eCrime Researchers Summit*, 2010.

[10] B. Genge, I. Nai Fovino, C. Siaterlis and M. Masera, Analyzing cyber-physical attacks on networked industrial control systems, in *Critical Infrastructure Protection V*, J. Butts and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 167–183, 2011.

[11] A. Ghorbani and E. Bagheri, The state of the art in critical infrastructure protection: A framework for convergence, *International Journal of Critical Infrastructures*, vol. 4(3), pp. 215–244, 2008.

[12] D. Gianni, Bringing discrete event simulation concepts into multi-agent systems, *Proceedings of the Tenth International Conference on Computer Modeling and Simulation*, pp. 186–191, 2008.

[13] Y. Haimes and D. Li, A hierarchical-multiobjective framework for risk management, *Automatica*, vol. 27(3), pp. 579–584, 1991.

[14] M. McDonald, G. Conrad, T. Service and R. Cassidy, Cyber Effects Analysis Using VCSE, Promoting Control System Reliability, Sandia Report SAND2008-5954, Sandia National Laboratories, Albuquerque, New Mexico, 2008.

[15] A. Nieuwenhuijs, E. Luiijf and M. Klaver, Modeling dependencies in critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Boston, Massachusetts, pp. 205–213, 2008.

[16] C. Queiroz, A. Mahmood, J. Hu, Z. Tari and X. Yu, Building a SCADA security testbed, *Proceedings of the Third International Conference on Network and System Security*, pp. 357–364, 2009.

[17] H. Rahman, M. Armstrong, D. Mao and J. Marti, I2Sim: A matrix-partition based framework for critical infrastructure interdependencies simulation, *Proceedings of the Electric Power and Energy Conference*, 2008.

[18] The CockpitCI Project, CockpitCI, Selex Systems Integration, Rome, Italy (`www.cockpitci.eu`).

[19] The Ettercap Project, Ettercap (`ettercap.github.io/ettercap`).

[20] The MICIE Project, MICIE, Selex Communications, Rome, Italy (`www.micie.eu`).

[21] S. Tisue and Wilensky, Netlogo: A simple environment for modeling complexity, presented at the *International Conference on Complex Systems*, 2004.