Chapter 14

ASSESSING THE IMPACT OF CYBER ATTACKS ON WIRELESS SENSOR NODES THAT MONITOR INTERDEPENDENT PHYSICAL SYSTEMS

Valerio Formicola, Antonio Di Pietro, Abdullah Alsubaie, Salvatore D'Antonio, and Jose Marti

Abstract This paper describes a next-generation security information and event management (SIEM) platform that performs real-time impact assessment of cyber attacks that target monitoring and control systems in interdependent critical infrastructures. To assess the effects of cyber attacks on the services provided by critical infrastructures, the platform combines security analysis with simulations produced by the Infrastructure Interdependencies Simulator (i2Sim). The approach is based on the mixed holistic reductionist (MHR) methodology that models the relationships between functional components of critical infrastructures and the provided services. The effectiveness of the approach is demonstrated using a scenario involving a dam that feeds a hydroelectric power plant. The scenario considers an attack on a legacy SCADA system and wireless sensor network that reduces electricity production and degrades the services provided by the interdependent systems. The results demonstrate that the attack is detected in a timely manner, risk assessment is performed effectively and service level variations can be predicted. The paper also shows how the impact of attacks on services can be estimated when limits are imposed on information sharing.

Keywords: Cyber attacks, wireless sensor networks, attack impact

1. Introduction

Cyber attacks against supervisory control and data acquisition (SCADA) systems [22] have shown that security violations can compromise the proper functioning of critical infrastructures. The Stuxnet worm [13] exploited vulnerabilities in the information and communications technology layer (primarily

J. Butts and S. Shenoi (Eds.): Critical Infrastructure Protection VIII, IFIP AICT 441, pp. 213–229, 2014.

deficient security policies and bugs in special purpose systems), ultimately affecting the operation of programmable logic controllers and the uranium hexafluoride centrifuges they controlled. Cyber attacks typically induce faults in sensors and actuators, and alter supervisory mechanisms and notification systems. Once activated, the faults become errors and result in improper operations. These can cause failures in critical infrastructures and eventually affect services, facilities, people and the environment.

Sophisticated wireless sensor networks [5] are increasingly used to monitor critical infrastructure assets, including dams and pipelines [4, 18]. In fact, sensor networks are rapidly being integrated in SCADA environments. Wireless sensor networks are often deployed in hydroelectric power plants and dams to monitor feed water supply, power generation, structural stability, environmental conditions and pollution levels. A single dam can have a thousand sensors, with additional sensors deployed in areas surrounding the water reservoir. Wireless sensor networks expose SCADA systems to new threats introduced by the information and communications technology layer. Unlike traditional sensor systems, wireless sensor networks are also vulnerable to signal eavesdropping and physical tampering, along with new ways of compromising data confidentiality, integrity and availability. The effects of cyber attacks against a dam include: (i) anomalous variations in seepage channel flows; (ii) uncontrolled gate opening; (iii) excessive turbine and infrastructure vibrations; (iv) structural instability; and (v) reservoir level variations.

Despite the adoption of security policies and the implementation of countermeasures, SCADA systems and wireless sensor networks continue to be vulnerable [2, 17]. SCADA systems are generally unable to cope with cyber attacks primarily because they were not designed with security in mind. Protection from cyber attacks has to be provided by additional security mechanisms that must be integrated with existing SCADA systems in a seamless manner. Logical security is commonly provided by security information and event management (SIEM) systems, which are specifically designed to manage and operate information and communications technology applications.

This paper presents a next-generation SIEM platform that performs real-time impact assessment of cyber attacks against monitoring and control systems in interdependent critical infrastructures. Run-time service level analysis is performed in the SIEM workflow. This is enabled by three novel contributions: (i) enhanced security event collectors (probes) that perform advanced semantic analysis of non-IP domains (e.g., wireless sensor networks) in the SIEM framework; (ii) impact assessment based on interdependency simulation; and (iii) transformation of SIEM risk assessment metrics to critical infrastructure operational levels (i.e., levels of services provided by the attacked systems). The approach also helps predict service level variations when limits are imposed on information sharing among different critical infrastructures.

Romano, *et al.* [23] have proposed the use of an enhanced SIEM system to monitor the security level of a traditional dam that incorporates legacy control systems and wireless sensor networks; the system was designed to collect data

from physical devices (sensors) and correlate physical events with events generated at the logical layer. This paper further enhances the SIEM system to assess the impact of cyber attacks against a dam that exhibits interdependencies with other critical infrastructures. The goal is to improve risk analyses performed by SIEM systems with qualitative and quantitative analysis of service level variations. This ultimately reduces the time required for decision making and improves decision outcomes in the presence of impending failures. The impact assessment module of the SIEM system relies on i2Sim [16], an infrastructure interdependency simulator that models resource flows between critical infrastructures and assesses how the output of one critical infrastructure is affected by the availability of resources provided by other critical infrastructures.

2. Related Work

This section discusses related work on next-generation SIEM systems for service level monitoring and models for evaluating critical infrastructure interdependencies.

Collections of events occurring in network systems enable the SIEM framework to assess the security level of network domains. A common way to store this information is to save it in logs generated by security probes and logical sensors. Since logs have heterogeneous formats (semantics and syntax), it is necessary to convert log data into a common representation. The overall process encompasses data gathering, parsing, field normalization and format conversion. Mostly, this process is executed by SIEM agents that collect data from several sources. In order to use SIEM systems to protect critical infrastructures, obtain a holistic view of security and enable impact analysis of cyber attacks on service levels, it is necessary to incorporate enhanced data collectors [6]. Specifically, enhanced data processing has to be introduced at the edge of the SIEM architecture to perform multi-level data aggregation and to manage data processing in the organizational domain [6].

Two widely-used data collectors, OSSIM-Agents [1] for the Open Source Security Information Management (OSSIM) SIEM platform and Prelude-LML for the Prelude OSS SIEM system [19], collect data using transport protocols (e.g., Syslog, Snare, FTP and SNMP) and produce OSSIM and IDMEF [8] messages, respectively. Both types of collectors execute format translation tasks, but do not perform content analysis and advanced data manipulation such as aggregation, filtering, correlation, anonymization and content-based encryption. Coppolino, *et al.* [7] have demonstrated that the OSSIM SIEM system can be used to protect critical infrastructures in a non-intrusive manner (i.e., without modifying SIEM framework components). They also show how to process physical layer data on the OSSIM server. Specifically, the server is configured to analyze environmental and physical measurements to detect physical anomalies in the SCADA workflow of a dam infrastructure. The introduction of SIEM technology in a dam protection system enables a massive number of messages to be sent from data sources (measurement collection points) located in the field towards the core of the OSSIM architecture (OSSIM server).

In the area of interdependency models, researchers have adopted a variety of techniques (e.g., agent-based systems, input-output inoperability, system reliability theory, nonlinear dynamics and graph theory) to model different types of interdependency phenomena [9, 21]. Satumitra, *et al.* [24] have demonstrated that it is possible to distinguish between physical, social, logical, geographical and cyber interdependencies. Ghorbani, *et al.* [14] have presented a classification and comparison of agent-based interdependency modeling and simulation tools. The work described in this paper is based on i2Sim [16], a simulation environment that models critical infrastructure interdependencies based on resource requirements and distribution. Using specific components called production cells, i2Sim is able to model the high-level behavior of a critical infrastructure by specifying the level of input resources that the critical infrastructure needs in order to provide a certain quantity of output. i2Sim also makes it possible to model the reduction of output quantity due to a reduction of input resources or an internal failure (e.g., due to a physical or cyber event).

Although SIEM systems can be enhanced to provide a multilayer view of system events and cope with sophisticated cyber attacks against service infrastructures, they do not use infrastructure interdependency models to evaluate real-time cascading effects [11]. The approach described in this paper incorporates an infrastructure interdependency model in a SIEM system in order to evaluate how cyber attacks against wireless sensor nodes impact interdependent systems. The proposed methodology is effective in current information sharing contexts where only limited amounts of information can be exchanged between interdependent infrastructures. Theoharidou, *et al.* [25] discuss related work on risk and impact assessment, but they neither consider security-related risks and technologies nor information sharing constraints.

3. Cyber Attack Impact Assessment

The proposed SIEM platform analyzes data from diverse sources and assesses the impact of cyber attacks on the services provided by interdependent critical infrastructures. The SIEM platform implements a novel level of intelligence (with respect to state-of-the-art commercial solutions), enabling a holistic view of security. The solution also supports the introduction of sophisticated detection mechanisms to discover attacks in non-IP networks (e.g., wireless sensor networks) and in the business layer. This feature is key to enhancing SIEM system intelligence and assessing the impact of attacks on critical infrastructure services.

Figure 1 shows the architecture of the enhanced SIEM platform. The platform incorporates the following main components:

- **SIEM Collector:** This component collects data from the monitored infrastructures to provide a multilayer view of system events and cross-correlate data in the proximity of the collection points. The modules responsible for data aggregation are called security probes. The security probes observe data related to specific services and detect anomalous

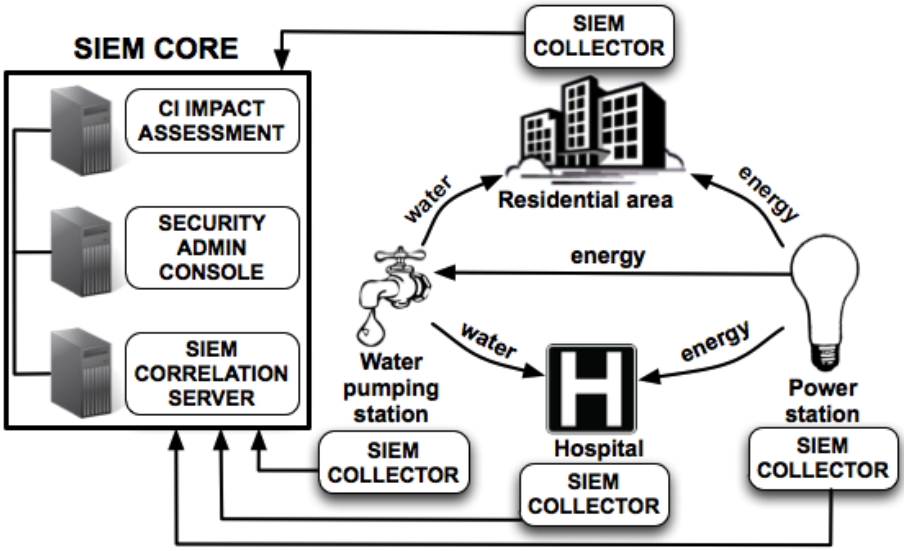

Figure 1. Enhanced SIEM platform architecture.

behavior. Information expressed in the resulting alarms is valuable for security risk assessment as well as service level impact assessment.

- **SIEM Correlation Server:** This component correlates events from security probes located in the proximity of critical infrastructure field systems. The SIEM server generates high-level alarms when cyber attacks against the monitored critical infrastructures are detected. The alarms contain a risk metric and information about the targeted assets. This information is used to assess the impact of attacks on critical infrastructure services. In this work, the SIEM correlation server is the OSSIM server.

- **Critical Infrastructure Impact Assessment:** This component assesses the impact on the services provided by interdependent critical infrastructures, some of which may be victims of cyber attacks. First, a mapping is performed between the alarms triggered by the SIEM correlation server and the operability levels provided by i2Sim. Next, an i2Sim simulation is executed to assess how the services provided by other critical infrastructures are affected by the new operability levels given the existing interdependencies. The alarms are weighted based on the relevance of the targeted assets to other critical infrastructures. The weighted alarms are sent to human experts or to decision support systems (DSSs) to identify the appropriate countermeasures.

3.1 Enhanced Collection

The SIEM collector is called the generic event translation (GET) framework [23]. It comprises modules that gather, parse, filter, anonymize, normalize, translate, aggregate and correlate low-level events (micro-events) across different layers. This workflow generates semantically-rich messages (macro-events) and dramatically reduces the volume of data generated by the sensors and directed to the SIEM server. Moreover, the GET framework confines the processing of private data within the domain boundaries of the collection points (e.g., company and organization networks). The GET framework operates as a data parser (i.e., it preprocesses data and translates content representation) and also correlates and analyzes data. A useful tool for producing pattern detectors is the State Machine Compiler [20], which facilitates the deployment of complex state machines represented as state charts. Each security probe receives messages from a subset of parsers and uses the information to provide input to the state machines.

3.2 Central Correlation

The SIEM correlation server is responsible for analyzing all the events collected by the GET framework. As shown in Figure 1, the SIEM correlation server receives data from event sources installed in the critical infrastructures (e.g., intrusion detection systems, firewalls, and servers running different operating systems) and from security probes in the GET framework.

The correlation engine is typically configured using detection patterns stored in rule databases. In order to assess the security level of the overall system, the SIEM correlation server operates in a centralized manner. By correlating events and security information, the SIEM server reduces the volume of alerts that reach the higher security event analysis layers (e.g., security administrators and, in our case, the critical infrastructure impact assessment module). Indeed, the SIEM server essentially reduces the number of false positives. For instance, consider the deployment of Linux servers and network intrusion detection systems that generate alerts due to malicious packets that target Windows Servers; the alerts are correlated with the current software characteristics (i.e., Linux operating systems) and no alarms are generated. Also, by correlating events from distributed security sources, the SIEM server can reveal malicious activities that are perpetrated in a distributed manner.

Correlation servers differ from each other in the correlation logic (logical tree, complex event processor, etc.). Their main task is to assess the risk posed by the events that occur. Outputs are reported as concise and meaningful alarms containing indicators of the risk levels reached by the events composing an attack sequence. Indicators are expressed as numerical values or qualitative indices. For instance, OSSIM SIEM uses numerical risk values in the range zero (lower risk) to ten (higher risk). Prelude OSS generates alarms with an assessment ("severity" in the IDMEF standard) expressed as *info*, *low*, *medium* *high* along with a flag that states if the attack was successful. In this work,

risk (and severity) are important to calculate the impacts of the cyber attacks that are detected.

The impact assessment process can be described as follows:

- Each event e is normalized by the GET framework in order to have a standard structure and appear as an information vector of the monitored activity $e(x_1, ..., x_N)$ where N is the number of fields that comprise the normalized event format.

- The SIEM server stores all the information that can help improve the accuracy of detection by the organization that hosts the SIEM system. This information includes the real vulnerabilities that affect a targeted host (e.g., known bugs) and the relevance of the target as a company asset. This information is referred to as "context information" or simply "the context" and is expressed as a vector of the additional data $a(s_1, \ldots, s_m)$. It is worth noting that this information is known only to the organization in charge of the targeted asset, (e.g., a company that manages the infrastructure) because it includes very sensitive information such as hardware characteristics, IP addresses, software versions and business relevance. This information cannot be shared with other infrastructures.

- The correlation process operates on sequences of events ($e(k)$) and additional data vectors (a). At the end of the process, alarms may be triggered if the security thresholds are exceeded. The SIEM server applies a risk assessment function R to calculate the risk associated with a sequence of events e in conjunction with the a information, i.e., $R(e, a)$.

For example, consider the implementation of risk assessment as provided by OSSIM SIEM. The OSSIM rules are called directives. When a directive is fired, the following function is applied:

$$Risk = (Priority \times Reliability \times Asset)/25 \tag{1}$$

In OSSIM, the Priority range is zero to five, the Reliability range is zero to ten and the Asset range is zero to five. Thus, Risk ranges from zero to ten. Priority and Asset are assigned through an offline analysis of host vulnerabilities, the typology of the attack and the relevance of the targeted asset to the organization; these constitute the context vector in the model above. Reliability is computed by observing the e sequence and by summing the Reliability of each event. In OSSIM, Reliability is taken to be the probability that an attack is real, given current events observed in the system. Note that lower Risk values (e.g., zero) are not dangerous because they mean that one of the assessment parameters has very low security relevance.

3.3 Critical Infrastructure Impact Assessment

The core function of the critical infrastructure impact assessment module is provided by i2Sim, which is an event-driven, time-domain simulator that is

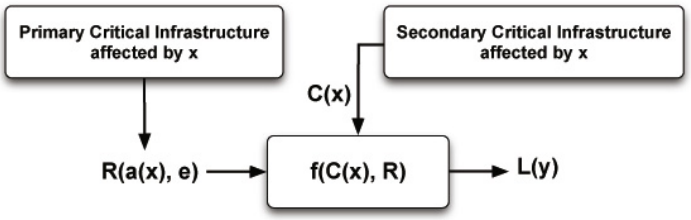

Figure 2. Metric transformation function.

used to model infrastructure interdependencies. i2Sim uses a cell-channel approach, which provides a multi-system representation at multiple hierarchical levels (e.g., local, municipal and provincial/state) and can be used in real time to assess the effects of resource allocation decisions during disasters. In addition, i2Sim provides a dynamic simulation environment that integrates different systems in a common simulation platform [3]. i2Sim determines the output of a critical infrastructure using two measures: resource mode (RM) and physical mode (PM). RM is determined by the availability of input resources from other critical infrastructures whereas PM is determined by the internal conditions of the critical infrastructure itself (e.g., level of physical damage to a building). Therefore, the output of a critical infrastructure modeled in i2Sim is a function of the availability of input resources and its physical integrity.

3.4 Metric Transformation

In order to relate alarms resulting from SIEM analysis to physical modes of each i2Sim cell, the risk assessment value (R) is combined with the service criticality metric (C). Criticality considers the relationships between the attacked nodes (e.g., sensors and actuators) and services (e.g., electric power and water supply). The mixed holistic reductionist (MHR) approach [9, 10] is used to define service criticality. The approach considers interdependency phenomena using three-layers: (i) a holistic layer that considers the evaluation of an event within a critical infrastructure; (ii) a service layer that specifies the services delivered to end users; and (iii) a reductionist layer that models the functional interdependences among different critical infrastructures. The reductionist layer evaluates the impact on a critical infrastructure. i2Sim translates this impact to the impacts on physical resource flows between infrastructures.

Figure 2 shows the transformation function. The transformation function f is factorized and the parameters are used to adapt the OSSIM risk values to i2Sim (x is the sensor and y is the secondary critical infrastructure). There is a subtle, but substantial, difference between the concepts of context and criticality. Context embraces the relevance of an asset (e.g., sensor) to the primary infrastructure, namely the relevance of an asset to the business of the infrastructure providing a service. Criticality refers to the relevance of an

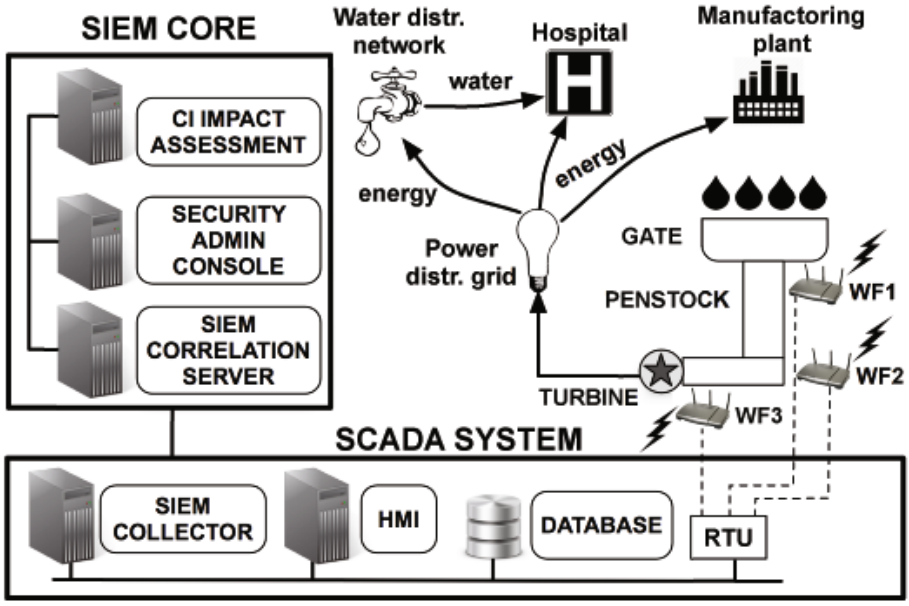

Figure 3. Sample scenario.

asset to the infrastructure that uses a service. Thus, criticality is not a unique parameter, but is strictly dependent on the infrastructure that consumes the service; it is computed by the provider based on information shared with the consumer. Indeed, criticality focuses on the need as indicated by the consumer infrastructure, which is not aware of the systems in the provider infrastructure. Given the information supplied by the consumer, the provider calculates a criticality value for each asset that is involved.

4. Example Scenario

The example scenario uses an attack on wireless sensor network nodes to demonstrate how the enhanced SIEM system can help evaluate the impact of an attack on infrastructure services. Figure 3 shows the scenario involving a dam that feeds a hydroelectric power station, which feeds a power distribution substation through a transmission network (not modeled for simplicity). Arrows in the figure indicate functional dependencies between critical infrastructures.

The dam provides water to the hydroelectric power station through a gate that is remotely controlled to release basin water and activate the power plant turbine. The dam and hydroelectric power station are controlled by a SCADA system that utilizes a wireless sensor network. Water fed to the hydroelectric power station is conveyed through pipes called penstocks. It is important to guarantee that the water flow values in the penstocks are within the operational

Table 1. Electricity demands of the critical infrastructures.

Critical Infrastructure	Electricity Demand
Hospital	13.47 MW
Water Distribution Station	52.5 MW
Manufacturing Plant	9.47 MW

range. Lower values can result in low power generation while higher values can lead to excessive turbine rotational speed and turbine vibration, which can result in physical damage to the infrastructure [15].

A hospital, water distribution station and manufacturing plant receive electricity from the power distribution substation. All the dependencies are modeled using i2Sim. A cyber attack is launched against the wireless sensor network that monitors the dam; the objective is to measure the impact on the operability level of the hospital, which requires electricity and water. Table 1 shows the electrical demands of the critical infrastructures in the scenario.

The wireless sensor network enables the SCADA system to monitor physical parameters. Four types of sensors are used: (i) three water flow sensors placed in the penstocks (WF1, WF2, WF3); (ii) two water level sensors that monitor erosion and piping phenomena under the dam wall (WL1 and WL2); (iii) a tilt sensor placed on the dam gate to measure the gate opening level (inclination); and (iv) a vibration sensor placed on the turbine. The sensors, which correspond to nodes in the wireless sensor network, send their measurements at regular intervals to the wireless sensor network base station (BS). The base station acts as wireless remote terminal unit (RTU) that forwards measurements to the remote SCADA server. Opening commands are issued by the remote SCADA facility to the gate actuator. The information and communications technology components deployed include a network-based intrusion detection system (N-IDS) installed in the remote SCADA server facility, a host-based intrusion detection system (H-IDS) positioned in the dam facility and a SIEM platform with a correlation engine located in a remote office. Figure 4 shows the results of applying the MHR approach, which models the services and equipment that are relevant to the critical infrastructure impact assessment module of the SIEM platform.

4.1 i2Sim Model

The i2Sim model provides a high-level abstraction of the physical components. In the i2Sim ontology, physical infrastructure entities are modeled as cells connected through channels that transport resources (e.g., electricity and water). The implemented model includes five cells that are used to represent the dependent infrastructures: hydroelectric power station, power distribution substation, water distribution station, manufacturing plant and hospital. The hydroelectric power station cell represents both the dam and the turbine. Alarms

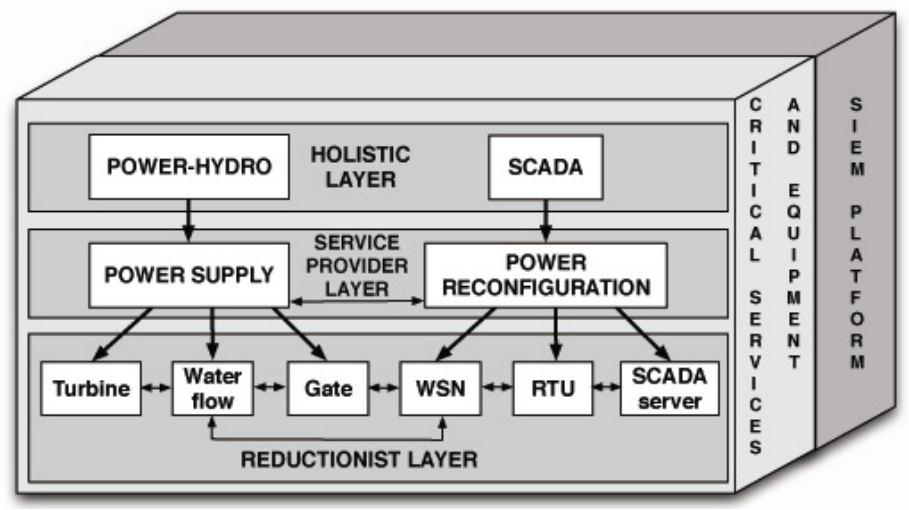

Figure 4. MHR model of the example scenario.

generated by the SIEM correlator are mapped to physical modes of the considered critical infrastructures. Changes to the physical modes of i2Sim result in changes to the RMs of the affected cells that measure their operability levels.

4.2 Attack Execution and Identification

The scenario considers an attack targeting the wireless sensor network nodes that involves several steps. At the end of the attack, the physical measurements collected by the wireless sensor network nodes are altered to induce incorrect situational awareness about the SCADA system. The SIEM framework detects this complex attack by correlating security events generated by the security tools installed in the dam facility, specifically the intrusion detection systems and GET security probes.

The assumption is that the attacker is a dam employee who can physically access wireless sensor network zones and connect to the network that hosts the SCADA server. The attacker has limited administrator rights and is not responsible for the cyber security of deployed systems (e.g., not responsible for security configuration policies and does not know the credentials needed to change the configuration or the cryptographic keys used for wireless sensor network communications).

The attack is performed in two phases. In the first phase, the attacker steals the wireless sensor network cryptographic key (e.g., via a side-channel attack as described in [12]). In the second phase, the attacker targets the SCADA server since he can access a host that monitors the dam (e.g., a human-machine interface (HMI) or engineering station). The attacker exploits a SCADA server

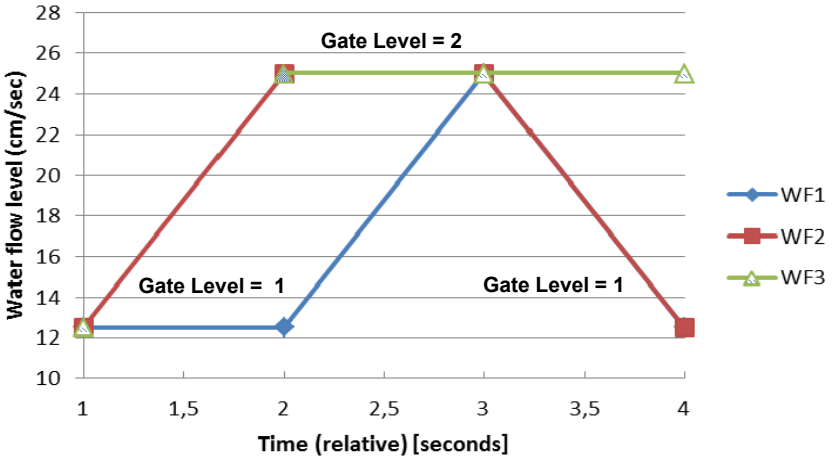

Figure 5. Water flow measurements forged by a malicious sensor.

vulnerability via malware that is installed by inserting a USB device into a SCADA network machine (as in the case of the Stuxnet worm [13]).

After the SCADA server is compromised, the attacker connects to the wireless sensor network RTU host. Having gained access to the wireless sensor network master node, the attacker reprograms the wireless sensor network nodes (e.g., via over-the-air programming). The new program is configured with the cryptographic key obtained during the previous phase. The new malicious code executes the routing protocol by altering the data forwarded from the water flow sensors to the master RTU. Water flow measurement data is altered in order to exceed the control threshold by adding a constant offset to the measured values. In this way, the gate is forced to limit water release and ultimately cause low turbine rotation. The final effect of the attack is a reduction in the electricity supplied to the power grid.

In order to detect the attack, we consider events generated by the security probes that oversee the wireless sensors. These security probes detect physical inconsistencies in the sensor data and generate alarms that are processed by the SIEM server: seepage channel sensors should report similar values of water levels; water flow sensors should measure values in the same range; and the gate opening sensor should report a value that is consistent with the water flow in the penstocks. The security probes aggregate the sensor data and verify their consistency.

Figure 5 shows the trends in the wireless sensor network data collected by the security probes (measurements). The SCADA server regulates the gate opening level (level 1 is low and level 2 is medium) based on the average water flow level provided by the three sensors. When the gate opening is at level 2, the water flow level is 12.5 cm/sec. The attack compromises the sensors so that they indicate a water flow level of 25.0 cm/sec. This causes the SCADA system to set the gate opening to level 1 to reduce the water flow below the

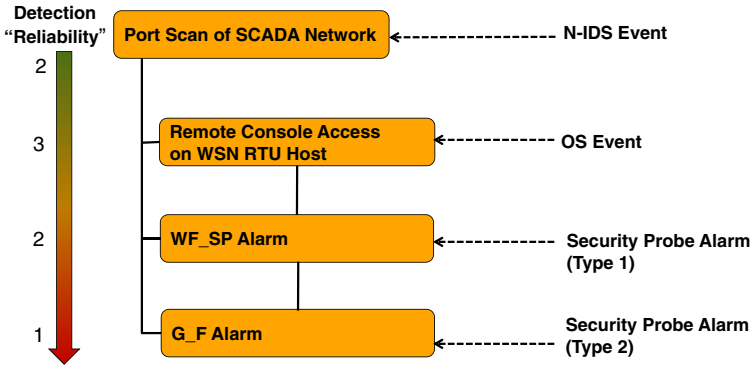

Figure 6. OSSIM rule.

control threshold. The result of the attack is that the gate opening moves to level 1 although measurements indicate that the gate opening is at level 2 (last measurements in the sequence in Figure 5).

The anomaly is revealed by two security probes: the first (WF_SP) reveals an inconsistency in the water flows and the second (G_F) reveals a gate opening level inconsistency for all three sensors. Note that another security probe that monitors the water level in the seepage does not show any inconsistency for WL1 and WL2. The alarms from the security probes are correlated by the SIEM platform according to the rule shown in Figure 6. The rule takes into account the two events from the H-IDS and N-IDS due to the worm activities and access to the wireless sensor network RTU host. The final alarm generated by the SIEM server contains evidence that the wireless sensors exhibit anomalies. In particular, the security probes indicate that WFx in the Penstock1 zone exhibits anomalous conditions. Such parameters, despite being irrelevant to the rule, are crucial to understand the impact of the attack (i.e., reduction in the power supplied by the hydroelectric power station). The parameters are used by i2Sim to evaluate the impact of the attack. In the rule, the Priority is highest (5), Reliability is 8 (sum of single event reliabilities) and Asset has the highest value (5). Thus, the Risk is $(5 \times 8 \times 5)/25 = 8$. This value must be associated with the service criticality of the wireless sensors with respect to the power production service in the critical infrastructure impact assessment module.

4.3 Critical Infrastructure Impact Assessment

Using the MHR approach, services and equipment that exhibit high event criticality can be identified. The graph in Figure 7 shows the estimated rate of treated patients depending on the hospital operability level following the cyber attack on the water flow sensors. As far the scenario is concerned, the flow sensors placed at different points in the penstocks (WF1, WF2 and WF3) exhibit high service criticality because, if attacked, they may alter the water

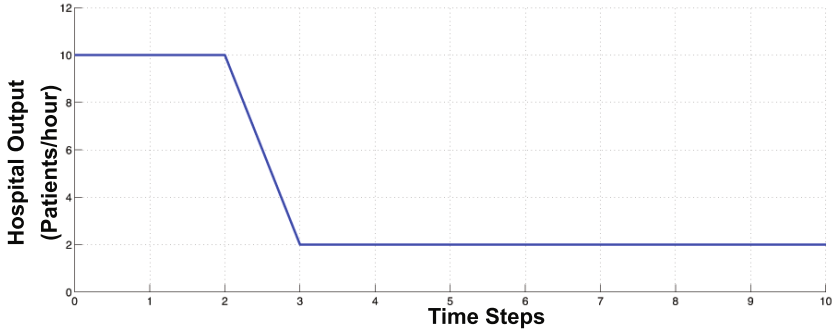

Figure 7. i2Sim results.

flow measurements and lead to low or over energy production, thus impacting the dependent critical infrastructures.

In this scenario, the Risk (R) of the attack is 8 while the event criticality (C) is in the range 0 to 0.5 (0 is not critical and 0.5 is highly critical). Given that the energy production is affected by the wireless sensor network measurements by a factor of 0.5, the resulting impact is PM $= R \times C = 8 \times 0.5 = 4$. The physical mode (PM) value is the physical mode in i2Sim where a value of one corresponds to fully operational and a value of five corresponds to not operational. Specifically, PM = 4 indicates that the cyber attack moves the physical mode functionality down to its lowest energy production level. The 0.5 factor was chosen because the wireless sensor network affects the total productivity of the power plant. Figure 7 shows a scenario where a cyber attack against the water flow sensors is detected. Due to the existing interdependency phenomena, the cyber attack degrades the operability level of the hospital.

5. Conclusions

The next-generation SIEM platform described in this paper is designed to support the real-time impact assessment of cyber attacks that affect interdependent critical infrastructures. The platform can detect cyber attacks against wireless sensor network nodes and can conduct real-time assessments of the impact of the attacks on the services provided by the wireless sensor nodes as well as the potential cascading effects involving other critical infrastructures. As demonstrated in the scenario, the i2Sim tool can be used to model the physical layer and services of an interdependent system (i.e., a dam and hydroelectric power plant) in order to analyze the impact of service degradation. The scenario helps understand how the interdependent system reacts to an attack that impacts water flow from the dam. The resulting functioning levels of the hydroelectric power plant and the effects on other critical infrastructures can be provided as inputs to an operator dashboard to help make decisions about appropriate mitigation strategies. Our future research will continue this line of

inquiry, in particular, validating the approach and the SIEM platform using a realistic testbed that incorporates a dam equipped with sensors and actuators.

Acknowledgement

This research was supported by the Seventh Framework Programme of the European Commission (FP7/2007-2013) under Grant Agreement No. 313034 (Situation Aware Security Operations Center (SAWSOC) Project). The research was also supported by the TENACE PRIN Project (No. 20103P34XC) funded by the Italian Ministry of Education, University and Research.

References

[1] AlienVault, OSSIM Sensor (`www.alienvault.com/wiki/doku.php?id=documentation:agent`).

[2] C. Alcaraz and J. Lopez, A security analysis for wireless sensor mesh networks in highly critical systems, *IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews*, vol. 40(4), pp. 419–428, 2010.

[3] A. Alsubaie, A. Di Pietro, J. Marti, P. Kini, T. Lin, S. Palmieri and A. Tofani, A platform for disaster response planning with interdependency simulation functionality, in *Critical Infrastructure Protection VII*, J. Butts and S. Shenoi (Eds.), Heidelberg, Germany, pp. 183–197, 2013.

[4] X. Bai, X. Meng, Z. Du, M. Gong and Z. Hu, Design of wireless sensor network in SCADA system for wind power plant, *Proceedings of the IEEE International Conference on Automation and Logistics*, pp. 3023–3027, 2008.

[5] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta and Y. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, *Computer Communications*, vol. 30(7), pp. 1655–1695, 2007.

[6] L. Coppolino, S. D'Antonio, V. Formicola and L. Romano, Enhancing SIEM technology to protect critical infrastructures, *Proceedings of the Seventh International Workshop on Critical Information Infrastructure Security*, pp. 10–21, 2010.

[7] L. Coppolino, S. D'Antonio, V. Formicola and L. Romano, Integration of a system for critical infrastructure protection with the OSSIM SIEM platform: A dam case study, *Proceedings of the Thirtieth International Conference on Computer Safety, Reliability and Security*, pp. 199–212, 2011.

[8] H. Debar, D. Curry and B. Feinstein, The Intrusion Detection Message Exchange Format (IDMEF), RFC 4765, 2007.

[9] 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.

[10] A. Di Pietro, C. Foglietta, S. Palmieri and S. Panzieri, Assessing the impact of cyber attacks on interdependent physical systems, in *Critical Infrastructure Protection VII*, J. Butts and S. Shenoi (Eds.), Heidelberg, Germany, pp. 215–227, 2013.

[11] A. Di Pietro and S. Panzieri, Taxonomy of SCADA systems security testbeds, to appear in *International Journal of Critical Infrastructures*.

[12] Z. Dyka and P. Langendorfer, Improving the security of wireless sensor networks by protecting the sensor nodes against side channel attacks, in *Wireless Networks and Security*, S. Khan and A. Pathan (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 303–328, 2013.

[13] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.

[14] 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.

[15] J. Hasler, Investigating Russia's biggest dam explosion: What went wrong, *Popular Mechanics* (`www.popularmechanics.com/technology/engineering/gonzo/4344681`), February 2, 2010.

[16] J. Marti, Multisystem simulation: Analysis of critical infrastructures for disaster response, in *Networks of Networks: The Last Frontier of Complexity*, G. D'Agostino and A. Scala (Eds.), Springer International Publishing, Cham, Switzerland, pp. 255–277, 2014.

[17] D. Martins and H. Guyennet, Wireless sensor network attacks and security mechanisms: A short survey, *Proceedings of the Thirteenth International Conference on Network-Based Systems*, pp. 313–320, 2010.

[18] K. Poulsen, Slammer worm crashed Ohio nuke plant network, *Security Focus* (`www.securityfocus.com/news/6767`), August 19, 2003.

[19] Prelude-IDS, Prelude LML (`www.prelude-ids.org/wiki/prelude/PreludeLml`), 2013.

[20] C. Rapp, Home of SMC: The State Machine Compiler (`smc.sourceforge.net`), 2013.

[21] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[22] R. Roman, C. Alcaraz and J. Lopez, The role of wireless sensor networks in the area of critical information infrastructure protection, *Information Security Technical Report*, vol. 12(1), pp. 24–31, 2007.

[23] L. Romano, S. D'Antonio, V. Formicola and L. Coppolino, Protecting the WSN zones of a critical infrastructure via enhanced SIEM technology, *Proceedings of the Thirty-First International Conference on Computer Safety, Reliability and Security*, pp. 222–234, 2012.

[24] G. Satumitra and L. Duenas-Osorio, Synthesis of modeling and simulation methods in critical infrastructure interdependencies research, in *Sustainable and Resilient Critical Infrastructure Systems*, K. Gopalakrishnan and S. Peeta (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 1–51, 2010.

[25] M. Theoharidou, P. Kotzanikolaou and D. Gritzalis, A multi-layer criticality assessment methodology based on interdependencies, *Computers and Security*, vol. 29(6), pp. 643–658, 2010.