Protecting the WSN Zones of a Critical Infrastructure via Enhanced SIEM Technology

Luigi Romano[1], Salvatore D'Antonio[1], Valerio Formicola[1], and Luigi Coppolino[2]

[1] University of Naples "Parthenope", Department of Technology, Naples, Italy
{luigi.romano,salvatore.dantonio,
valerio.formicola}@uniparthenope.it
[2] Epsilon S.r.l., Naples, Italy
luigi.coppolino@epsilonline.com

Abstract. Attacks on Critical Infrastructures are increasing and becoming more sophisticated. In addition to security issues of Supervisory Control And Data Acquisition systems, new threats come from the recent adoption of Wireless Sensor Network (WSN) technologies. Traditional security solutions for solely Information Technology (IT) based infrastructures, such as the Security Information and Events Management (SIEM) systems, can be strongly enchanced to address such issues. In this paper we analyze limits of current SIEMs to protect CIs and propose a framework developed in the MASSIF Project to enhance services for data treatment. We present the Generic Event Translation and introduce the Resilient Storage modules to collect data from heterogeneous sources, improve the intelligence of the SIEM periphery, reliably store information of security breaches. Particularly, by focusing on the first two features, we illustrate how they can improve the detection of attacks targeting the WSN of a dam monitoring and control system.

Keywords: Security Information and Event Management (SIEM), Supervisory Control and Data Acquisition (SCADA), Wireless Sensor Networks.

1 Rationale and Contribution

Coordinated and targeted cyber-attacks to Critical Infrastructures (CIs) are increasing and becoming more sophisticated [1][2]. Mostly, such infrastructures rely on legacy Supervisory Control And Data Acquisition (SCADA) systems that have been designed without having security in mind, as they were originally isolated and based on proprietary protocols. Moreover, the recent and increasing trend of critical infrastructure monitoring is based on Wireless Sensor Network (WSN) technology, which introduces new security threats in addition to a number of advantages, such as dramatically reduction of deployment costs, possibility for deploying a proper level of redundancy, effective monitoring in several scenarios [3][4][5].

According to the National Institute of Standards and Technology (NIST) [6], securing a Critical Infrastructure is very different from protecting solely Information Technology-based infrastructures, hence traditional solutions, such as the Security

F. Ortmeier and P. Daniel (Eds.): SAFECOMP 2012 Workshops, LNCS 7613, pp. 222–234, 2012.

Information and Event Management (SIEM) systems are often ineffective for CIs protection. In order to overcome such issues, the European Commission funded project MASSIF [7] proposes an enhanced SIEM for the protection of Critical Infrastructures. In this paper we analyze the main limits of current SIEM solutions when applied to protecting CIs and design and implement a framework to overcome the identified limits by enhancing data collection and storage services of a SIEM. The solution is composed of several modules that we named Generic Event Translation (GET) and Resilient Storage (RS) which allow to: i) increase the heterogeneity and number of data sources; ii) move part of the data processing toward the edge of the distributed IT system managing the CI; iii) provide post-accidental support allowing a precise and reliable reconstruction of the happening of a security breach and forensic evidence of such a circumstance. A final contribution of this paper is the application of the proposed solution to protect a real CI, namely a dam, monitored by means of WSN technology. To the best of our knowledge, no works in literature discuss the adoption of SIEM technology to protect the WSN zones of a CI. Most of the related work faces security issues in WSN technology by means of Intrusion Detection Systems (IDS) and improved routing protocols. For instance, in [8] a reputation based approach combined with clustering algorithms is used to detect attacks to the WSN routing protocols. In [9] an hybrid agent based IDS detects routing protocol attacks, such as sinkhole and sleep deprivation. In [10] intrusion detection algorithm based on neighbor nodes' power is applied to WSN with static nodes.

In Section 2, the paper discusses the main limits of current SIEM technologies when applied to protect Critical Infrastructures and excerpts a list of features for an enhanced SIEM for CIs. Section 3 introduces the data service components in the context of the MASSIF framework. Section 4 presents the implementation of such solutions and their usage to protect a dam monitoring and control system. Section 5 closes the paper with final remarks and an overview of future plans.

2 Enhanced SIEMs for CIs

MASSIF project has analyzed four real world scenarios and has identified the main limits of current State of the Art (SotA) technology [8] when deployed to protect CIs. Such limits may invalidate the effectiveness of SIEM operation, which, primarily, has to avoid security-induced safety issues impacting society and environment. In Table 1 we shortly summarize them and excerpt a list of features for an enhanced SIEM for CIs.

Besides such capabilities, MASSIF project has identified additional services which can be offered on the top of the SIEM (e.g. attack modeling and simulation, decision support and reaction/countermeasure systems, advanced visualization, etc.); however, these topics are out of the scope of this paper. In the following we will present our solution to address issues presented in Table 1, with the exception of resilient data dissemination, faced in MASSIF and partially discussed in [17]. Moreover the RS module is briefly introduced, but no more details are provided in this work.

Table 1. Features for an enhanced SIEM for Critical Infrastructures

Enhanced SIEM capability	Rationale
Data collectors should be able to integrate legacy and novel information sources in an effective and flexible way, by interpreting multi-layer and multi-domain data formats, typically characterized by heterogeneous syntax and semantics.	Traditionally, SIEMs focus on IT infrastructure events [12][13][14][15], but some security occurrences may not produce evidence at this level. Enhanced SIEMs should have a more comprehensive view of security-aware processes.
SIEMs should limit the consumption of shared resources as much as possible (e.g. bandwidth, central server processing).	SCADA and SIEMs are deployed together in the same environment, thus they compete for the same resources, which are often very constrained.
SIEM should provide mechanisms to treat and pre-correlate data at the edge of the (SIEM) architecture, very close to the field devices.	i)Correlation may be more effectively operated when the security information is contextualized, detailed data can be retrieved on-demand and analysis can exploit knowledge of the specific application domain. ii)Traditional SIEMs disseminate information through intermediate communication nodes and towards remote correlation servers, by exposing sensitive data to third parties.
SIEMs should be capable of high data volume performance at the edge of the network, specifically in data treatment components, such as data collectors, data parsers and event correlators.	Field devices are even more capable to generate massive physical data and perform very complex operations. This may result in overwhelming the SIEM for CIs with huge amounts of security related patterns and alerts.
SIEM storage systems should provide high capabilities in terms of: data authenticity of event sources; fault and intrusion tolerance; control of data access by authorized parties. Forensic events, and only such events, must be kept, while unnecessary details must be deleted or made anonymous (“least persistence principle”).	CIs are very attractive to malicious actions, so security events may be used for forensic purposes. In order to use SIEM reports as forensic proof, digital evidence (e-evidence) properties like Authentication, Admissibility and Best-evidence should be granted [16].
SIEM should be able to disseminate events in a reliable manner by means of resilient architectures.	Data channels of SIEMs are vulnerable to faults and malicious activities which may impact correct and timely dissemination of events from data sources to central engines and may invalidate SIEM analysis.

3 Data Treatment Framework of MASSIF SIEM

MASSIF project proposes a SIEM with enhanced capabilities such as those exposed above. Specifically, the SIEM is deployed as a logical overlay on the monitored infrastructure. The GET is the MASSIF module that collects data from the "Payload Machinery" of the CI, which is typically composed of heterogeneous and multi-layer event sources - legacy IT and SCADA components, security applications and appliances – and performs preliminary security analysis of the data at the edge side of the SIEM architecture. The Resilient Storage (RS) implements a set of techniques which allow to reliably store data containing information of relevant security breaches.

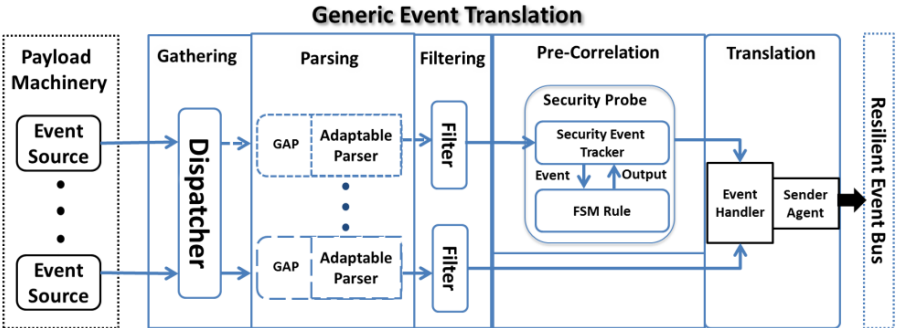


Fig. 1. Architecture of Generic Event Translation (GET) module

Cross-layer Data Collection

The GET is the module of the SIEM in charge of cross-layer event collection, which in turns requires gathering, parsing, filtering and translating data generated by the Payload Machinery. GET is made of several components located at the edge-side of the MASSIF SIEM architecture. Each one is assigned to a single subtask. Moreover, the GET can be interfaced very closely to the field systems and can sign information as soon as it is generated. Follows a list of the GET components, shown in Fig 1.

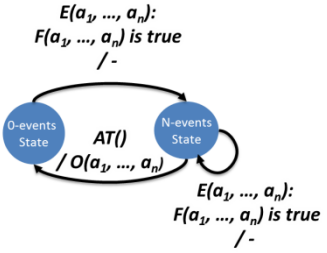
Dispatcher gathers raw data from event sources by means of textual based protocols, such as Syslog [18], which is by far the most widely used transport protocol to send event logs. *Adaptable Parsers (APs)* extracts information from the flow of raw data (e.g., a stream of characters) previously collected (*parsing)*. APs adopt Compiler-compiler technology to automatically manipulate formally specified documents [19]. This approach retains a number of associated advantages including: a very large degree of expressiveness, the availability of well-known tools for the automatic processing of grammar-based artifacts, a high level of generality and technology-independence, which decouples the format definition from the underlying technology used for data processing. Each AP is joined to the *GET Access Point (GAP)*, which supports the Dispatcher by associating a data source stream with the related parser. *Event Filters* selectively discard events generated by the event sources to avoid the propagation of useless data to SIEM analysis. *Event Handler (EH)* translates the

message format into a common and generic event format, in order to be effectively processed by SIEM core engines. *Sender Agent* sends SIEM-formatted events to the dissemination layer of the enhanced SIEM, namely the Resilient Event Bus of MASSIF.

Edge-Side Data Analysis

The part of the GET in charge of cross-layer event correlation, aggregation and abstraction is the Security Probe (SP). The SP introduces a novel level of intelligence into SIEM analysis and contextualizes it to the specific application domain. Particularly, SP is a Finite State Machine (FSM)-based event pattern detector which reduces the burden of processing the whole data at the core of the SIEM. Specifically, SPs are based on State Machine Compiler (SMC) [20] technology, which gives the possibility to separate the description of the FSM from its actual implementation, thus allowing the analyst to concentrate his/her attention on the correlation logic (and rule) instead of the implementation details. Security Probes operate with event sources belonging to very different layers: in order to make FSMs "evolve", Adaptable Parsers feed the SPs with proper information. The Security Event Tracker is part of the SP in charge of getting input events, identifying the FSM instance to evolve, receiving the feedback from the machine (e.g. an alert) and sending the FSM output to the EH; the FSM logic (states, transitions, …) is maintained in the Finite State Machine Rule.

An SP which aggregates input events and related schema in shown in Fig. 2.



Function/ Parameter	Meaning
$a_1, \ldots, a_n$	(parsed) data fields of the input event
$E(a_1, \ldots, a_n)$	input event with n data fields
O(x)	output event computed from x
AT()	aggregation trigger which activates the output: e.g. timer, counter, threshold *(Output Condition)*
$F(a_1, \ldots, a_n)$	boolean condition to evolve the machine *(Aggregation Condition)*

Fig. 2. Security Probe: aggregation schema

a_1: timestamp variable; T: first event timestamp; K: time window
$a_2 \ldots a_j$: new input fields $\quad \underline{a_2} \ldots \underline{a_j}$: first event input fields
a_i: field to be summed
$F(a_1, a_2, \ldots, a_j, \ldots, a_n)$: $(T < a_1 < T + K)$ AND $(a_2 \ldots a_j == \underline{a_2} \ldots \underline{a_j})$
AT:(counter >= N) OR (timer >= t)
$O(a_1, \ldots, a_n)$: $E(T, a_2 \ldots a_j, sum(a_i))$

Fig. 3. Time based aggregation on input data

For instance, consider a time-reference based aggregation, which consolidates a certain number of events sharing same values of the first event arrived (or part of it) and generated in the same time window. Given the formalism expressed above, we can configure the FSM as follows:

The schema in Fig. 3 generates an aggregate output if the number of events arrived overcomes the threshold N or the timer associated with the Aggregator expires. The output message creates a new event, which contains: the Timestamp of the first message, the invariant of data fields, a new data field obtained by summing the events aggregated. Overcoming this example, we prefigure the possibility to create aggregated events by providing several operations on data fields: for instance we could disseminate the first and the last timestamps in order to identify the time window extent of aggregated events, or link the identity fields of aggregated events.

As GET framework functionalities are distributed among several (edge-side) components, load distribution policies and mechanisms, such as load balancing, can be implemented: this would allow handling load peaks in different phases of the edge-side data processing and reconfiguring the usage of computational resources. Moreover, SotA security technologies have been adopted to protect data channels among GET components, such as SSL/TLS protocols. Indeed, in this way, as new data arrive at the Dispatcher, they are signed and encrypted.

Data Storage for Forensic Purposes

The Resilient Storage (RS) is the MASSIF module in charge of supporting reliable storage of information related to security incidents. Key mechanism adopted to design the RS is the threshold cryptography [21] combined to diversity and replication techniques and hardened with Write-Once-Read-Many (WORM) storage devices [22]. RS is particularly useful to criminal/civil prosecution of attackers in the post-security breach stage: in this case the main component feeding the RS is the SIEM Correlation/Rule Engine at core-side.

4 Protecting the WSN Zones of a Dam Infrastructure

In the following we present our solution applied to the case study of a dam monitoring and control system which adopts the WSN technology. Dams are complex infrastructures conceived for a multitude of purposes and, typically, a huge number of physical parameters are monitored to guarantee safety and security. Monitoring and control systems are based on geotechnical instrumentation combined with SCADA systems. Such systems are increasingly becoming automated and remotely controlled and this fact paves the way for a new class of security induced safety issues that is for the possibility that cyber-attacks against the IT layer of the dam, ultimately result in damage to people and environment.

Case Study. In our case study we consider a dam feeding a hydroelectric power station, as depicted in Fig. 4. The *Intake* Gate of the dam is controlled to release the basin water and activate the Turbine in the power plant. Normally, water flow in the

Penstock is controlled to not exceed an alert threshold. Indeed, high turbine speed may result in electric overload and in power plant facility failure due to excessive vibrations. The deployment of our case study is based on three water flow sensors placed at different points of the penstock (WF1, WF2, WF3). Moreover, other sensors are placed in the seepage channels under the dam wall. Indeed, parameters of seepage waters (turbidity, water levels, etc.) are continuously monitored to foresee dangerous events such as erosion and piping phenomena (sensors WL1 and WL2). A Tilt sensor is placed on the dam gate and measures gate opening levels (inclination). A Vibration sensor is placed on the Turbine. All the sensors constitute the nodes of a WSN and, at regular intervals, send their measurements to a WSN Base Station (BS) located at the dam surveillance office. The BS acts as a wireless Remote Terminal Unit (RTU), which forwards the measurements to the Remote SCADA server. Finally, opening commands are issued by the remote SCADA facility toward the gate actuator. The SCADA allows to open the gate only if safety conditions are verified in the turbine, i.e. if the penstock water flow is under the safety threshold.

The IT security deployment of our case study includes a Network-based Intrusion Detection System (N-IDS) in the remote SCADA server facility, a Host-based Intrusion Detection System (H-IDS) in the dam local facility, a SIEM with the correlation engine located in a remote warehouse.

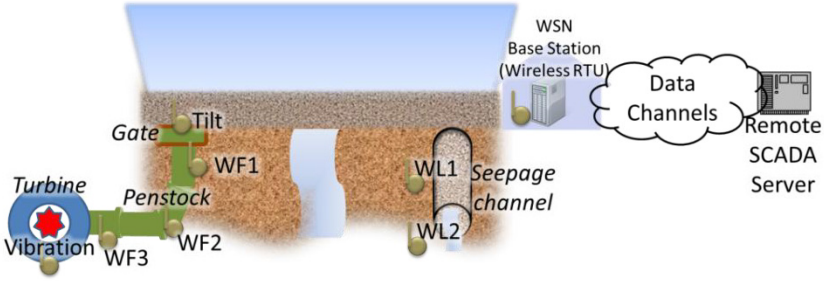


Fig. 4. WSN-based monitoring of a dam

In order to extend the analysis of the SIEM from a multi-layer security perspective, we feed the SIEM correlation engine with the evidence of physical incoherencies in the parameters measured by the WSN nodes. This is only possible if we have specific knowledge of the critical infrastructure under control. It's worth noting that to do this with a traditional SIEM, we should disseminate physical data to the central correlation engines, resulting in several issues, such as: difficulty in gathering and translating physical data from sensor devices into the SIEM format; unsuitability of SIEM correlation engines to describe and detect physical anomalies; wasting of computational and bandwidth resources to propagate and elaborate data into the SIEM correlation engine.

Misuse Case. In order to present the effectiveness of our framework, we considered a storyboard that closely mimics Stuxnet behavior [23]. The attack target is the failure

of the turbine facility. The attacker alters the water flow measurements to hide their actual values and solicit excessive gate opening. Precondition to the attack is that the attacker has access to some hosts in remote station and can execute tools to hack the SCADA machines and the BS host (e.g. by plugging a USB device in). The attack is perpetrated in a chain of malicious activities, which we summarize as follows: usage of malicious software to locate and exploit SCADA server vulnerabilities; creation of a backdoor on the SCADA server; gathering of information about RTU devices and facilities (i.e. IP address of BS host); scanning and violation of the BS host; access to the BS host and execution of a malicious Over-The-Air (OTA) programming with a rogue code. In particular, we point out that the attacker can install the rogue code both as privileged user of the BS device or by executing a WSN injection tool, such as those indicated in [24] [25]: for instance he/she can perform a sinkhole attack by violating one of the seepage channel sensors or manually reprogramming the routes of the wireless data paths. Finally, the gate command is issued by the attacker self (e.g. by the compromised SCADA host) or is further executed by the authorized personnel.

Security Probes for WSN Zones

In the following we describe the Security Probes deployed for our case study. They will be used to support the detection of the misuse case presented above. The state machines are depicted in Fig. 5.

Triple Modular Redundancy. As the three water flow sensors are related to the same physical event (water discharge), physical values outside the same range can be highlighted and reported to the SIEM. In order to do so, we designed a Security Probe implementing a Triple Modular Redundancy (TMR) system. TMRs generate a single output from several independent processes by adopting majority voting decision (Fig. 5(a)). The TMR SP aggregates the three measurements and reports the number of sensors falling in the same physical range. Disagreeing sensors are indicated in the output. Sample logs are reported in Fig. 6 (TMR SP).

Gate command-Water Flow Incoherence. This SP generates warnings if low water flow levels are measured after a gate opening command has been issued.

Gate command-Gate Tilt Incoherence. This SP (Fig. 5 (b)) generates warnings if the Tilt sensor doesn't reveal variations after a gate opening command.

Gate command-Turbine Vibration Incoherence. This SP generates warnings if the Vibration sensor doesn't reveal variations after a gate opening command.

Experimental Set-Up

In order to test our solution we deployed an experimental testbed composed of: 1) an application configured for monitoring of dams, namely DaMon (Dam Monitor) - developed by Epsilon R&D department together with the University of Naples Parthenope FITNESS research group - realized by using a powerful web-based, AJAX enabled framework for SCADA design, namely Mango [26]; 2) a set of WSN Libelium Waspmote ZigBee devices with Digimesh communication protocol to measure

Tilt, Vibration, Water Levels, Water Flows [27]; 3) a Linux-based BS host; 4) an RTU (based on Datataker DT85G) communicating via Modbus protocol. The Gate actuator is controlled by the DaMon HMI through the RTU.

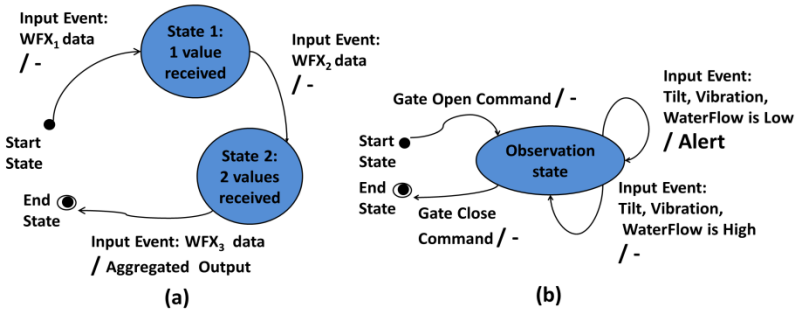


Fig. 5. WSN Security Probes: TMR (a) – Gate-Sensors Incoherence (b)

```
<directive id="500001" name="WSN zone warning" priority="5">
            <rule type="detector" name="Snort Portscan" reliability="2"
                  occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
                  plugin_id="1100" plugin_sid="21">
                  <rules>
                        <rule type="detector" name="Last log"
                              reliability="3" occurrence="1"
                              from="1:DST_IP" to="10.0.0.1"
                              port_from="ANY" time_out="100000" port_to="ANY"
                              plugin_id="1010" plugin_sid="1" userdata1="!reboot"/>
                        <rule type="detector" name="TMR Security Probe"
                              reliability="2" occurrence="2"
                              from="ANY" to="ANY"
                              port_from="ANY" time_out="100000" port_to="ANY"
                              plugin_id="1011" plugin_sid="1"/>
                        <rule type="detector" name="Gate-Tilt incoherence"
                              reliability="1" occurrence="1"
                              from="ANY" to="ANY"
                              port_from="ANY" time_out="100000" port_to="ANY"
                              plugin_id="1012" plugin_sid="1"/>
                        <rule type="detector" name="Gate-Vibration incoherence"
                              reliability="1" occurrence="1"
                              from="ANY" to="ANY"
                              port_from="ANY" time_out="100000" port_to="ANY"
                              plugin_id="1012" plugin_sid="2"/>
                        <rule type="detector" name="Gate-Flow incoherence"
                              reliability="1" occurrence="1"
                              from="ANY" to="ANY"
                              port_from="ANY" time_out="100000" port_to="ANY"
                              plugin_id="1012" plugin_sid="3"/>
                  </rules>
            </rule>
</directive>
```

Fig. 6. OSSIM directive of a WSN attack

Security tools installed are: Snort NIDS [28], Linux shell monitor (Last), the OSSIM SIEM by AlienVault [29] integrated with the GET modules and the RS system.

The attack has been performed by executing an OTA code on the Seepage Channel sensors. The OTA forces the routes from the penstock sensors to pass through the seepage channel sensors (destination address and maximum hops are reprogrammed). The seepage sensors alter the water flow values transiting through them.

The warning events generated by the system are: i) a network scan by Snort; ii) a shell activity in the Linux BS host; iii) a TMR warning; iv) a number of warnings from the Gate-Tilt/Vibration/Flow Security Probes.

The misuse case model presented above is used to configure an OSSIM *Directive* as in Fig. 6. The rule triggers alerts with a total reliability (i.e. alert confidence) of 10. Actually, observe that the Vibration and Tilt warnings are not necessarily generated (this only happens if the violated node of the WSN modifies all the data through it). Even if the Directive may generate lower level alerts – in case of few physical evidence – we may identify additional conditions related to other physical parameters.

The GET modules are able to gather, parse and process the data format shown in Fig. 7, such as Libeium Waspmote data, Gate commands reported by DaMon HMI (text based reports) and Syslog reports by Snort and "Last" utility. The SPs show three capabilities: they treat physical data from a security perspective; they place SIEM intelligence at the periphery and avoid irrelevant data to be propagated to the central system; they exploit specific knowledge of the application domain (redundancy and physical incoherence).

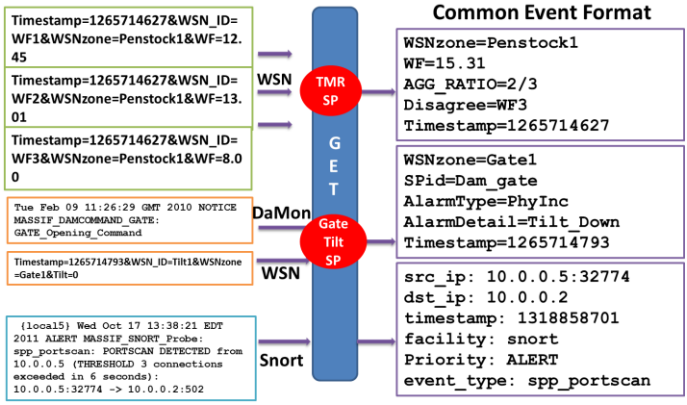


Fig. 7. GET processing at the edge of MASSIF SIEM

Fig. 8 shows DaMon interface and in particular the gate monitoring and control mimics. This interface allows users to change the gate openess levels; each actuator command generates notification messages, such as in Fig. 7.

Fig. 9 shows an OSSIM Alarms, which includes the events that generated the alerts (Fig. 8).

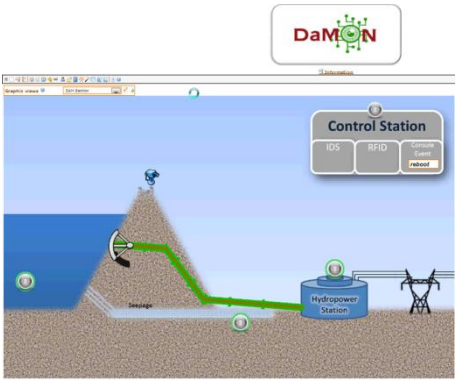


Fig. 8. DaMon interface showing gate and penstock details

#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	15	WSN zone warning	6	2011-03-30 14:01:15	ANY	ANY	6
		Alarm Summary [Total Events: 6 - Unique Dst IPAddr: 2 - Unique Types: 2 - Unique Dst Ports: 1]					
1	15	Gate-Flow Incohe	1	2011-03-30 13:59:29	ANY	ANY	6
2	14	Gate-Vibration In	1	2011-03-30 13:59:26	ANY	ANY	5
3	12	Gate-Tilt Incohe	1	2011-03-30 13:59:25	ANY	ANY	4
4	8	TMR Security Probe	1	2011-03-30 13:59:24	ANY	ANY	3
5	5	Last log	1	2011-03-30 13:54:12	ANY	ANY	2
6	2	Snort Portscan	1	2011-03-30 13:49:10	ANY	ANY	1

Fig. 9. OSSIM alarm and related events (addresses are obfuscated)

5 Conclusions and Future Work

In this paper we have discussed main limits of current SIEM technology when deployed to secure CIs. We have described the main features of the enhanced SIEM for CIs developed in the EC-funded project MASSIF [7], mainly focusing on the framework of the system assigned to data collection and storage, namely the Generic Event Translation (GET) and the Resilient Storage (RS). We have proposed them in the challenging case study of a dam monitoring and control system which uses WSN technologies. We have presented an attack model aimed at tampering the WSN data from a remote facility and have indicated how to support SIEM detection of the attack with a number of Security Probes triggering warning revealing physical incoherence in the measurements. In the future we plan to produce quantitative evidence of the benefits due to the adoption of the enhanced SIEM, against traditional solutions.

Acknowledgments. The research leading to these results has received funding from the European Commission within the context of the Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 257644 (MAnagement of Security information and events in Service Infrastructures, MASSIF Project).

References

1. Seung, H.K., Qiu-Hong, W., Johannes, B.U.: A comparative study of cyberattacks. Commun. ACM 55(3), 66–73 (2012), doi:10.1145/2093548.2093568
2. Symantec ® Applied Research: Symantec 2010 Critical Infrastructure Protection Study (Global Results) (October 2010)
3. Buttyan, L., Gessner, D., Hessler, A., Langendoerfer, P.: Application of wireless sensor networks in critical infrastructure protection: challenges and design options. Security and Privacy in Emerging Wireless Networks. IEEE Wireless Communications 17(5), 44–49 (2010), doi:10.1109/MWC.2010.5601957
4. Bai, X., Meng, X., Du, Z., Gong, M., Hu, Z.: Design of Wireless Sensor Network in SCADA System for Wind Power Plant. In: Proceedings of the IEEE International Conference on Automation and Logistics, Qingdao, China (2008)
5. Minteos DamWatch (2011), `http://www.minteos.com/wp-content/uploads/2011/02/Microsoft-Word-minteos-damwatch_ita.pdf`
6. Stouffer, K., Falco, J., Scarfone, K.: Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology (NIST), SP 800-82 (2011)
7. MASSIF project, `http://www.massif-project.eu/`
8. Bankovic, Z., Vallejo, J.C., Malagon, P., Araujo, I., Moya, J.M.: Eliminating routing protocol anomalies in wireless sensor networks using AI techniques. In: Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security (AISec 2010), pp. 8–13. ACM, New York (2010), doi:10.1145/1866423.1866426
9. Coppolino, L., D'Antonio, S., Romano, L., Spagnuolo, G.: An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies. In: 5th International Conference on Critical Infrastructure (CRIS), pp. 1–8 (2010)
10. Wang, Q., Wang, S., Meng, Z.: Applying an Intrusion Detection Algorithm to Wireless Sensor Networks. In: Second International Workshop on Knowledge Discovery and Data Mining, WKDD 2009, pp. 284–287 (2009)
11. MASSIF project. Scenario requirements Deliverable D2.1.1, Project MASSIF (April 2011)
12. RSA™ Security: RSA enVision™ Universal Device Support Guide (2008)
13. AlienVault™: Available OSSIM Plugin List (2010)
14. ArcSight™: ArcSight™ Smartconnector (2009)
15. Q1Labs™: Supported devices, `http://q1labs.com/products/supported-devices.aspx`
16. The Committee on the Judiciary House of Representatives: Federal Rules of Evidence (December 2010), `http://judiciary.house.gov/hearings/printers/111th/evid2010.pdf`
17. Sousa, P., Bessani, A., Correia, M., Neves, N., Verissimo, P.: Highly available intrusion-tolerant services with proactive-reactive recovery. IEEE Transactions on Parallel and Distributed Systems 21(4) (2010)
18. BSD Syslog Protocol, RFC 3164, `http://www.ietf.org/rfc/rfc3164.txt`
19. Campanile, F., Cilardo, A., Coppolino, L., Romano, L.: Adaptable Parsing of Real-Time Data Streams. In: Proceedings of the 15th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2007), pp. 412–418. IEEE Computer Society, Washington, DC (2007), doi:10.1109/PDP.2007.16
20. Home of SMC: the State Machine Compiler, `http://smc.sourceforge.net/`

21. Shoup, V.: Practical Threshold Signatures. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 207–220. Springer, Heidelberg (2000)
22. Zhu, Q., Hsu, W.W.: Fossilized Index: The Linchpin of Trustworthy Non-Alterable Electronic Records. In: Proceedings of the ACM International Conference on Management of Data, Baltimore, Maryland, pp. 395–406 (June 2005)
23. Langner, R.: Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security and Privacy 9(3), 49–51 (2011), doi:10.1109/MSP.2011.67
24. Parthasarathy, R., Peterson, N., Song, W.Z., Hurson, A., Behrooz Shirazi, A.: Over the Air Programming on Imote2-Based Sensor Networks. In: 43rd Hawaii International Conference on System Sciences, pp. 1–9 (2010)
25. McNabb, J.: Vulnerabilities of Wireless Water Meter Networks. In: DEF.CON Hacking Conference (2011)
26. Mango, Open Surce M2M, `http://mango.serotoninsoftware.com/`
27. Libelium™ Waspmote, `http://www.libelium.com/products/waspmote`
28. Snort™, Network IDS/IPS, `http://www.snort.org/`
29. OSSIM AlienVault™, `http://www.alienvault.com/`