PRECYSE: Cyber-attack Detection and Response for Industrial Control Systems

Kieran McLaughlin, Sakir Sezer
Centre for Secure Information Technologies (CSIT)
Queen's University Belfast
Belfast, UK
firstname.lastname@qub.ac.uk

Paul Smith, Zhendong Ma, and Florian Skopik
Safety and Security Department
AIT Austrian Institute of Technology
Vienna, Austria
firstname.lastname@ait.ac.at

In this short paper, we present an integrated approach to detecting and mitigating cyber-attacks to modern interconnected industrial control systems. One of the primary goals of this approach is that it is cost-effective, and thus whenever possible it builds on open-source security technologies and open standards, which are complemented with novel security solutions that address the specific challenges of securing critical infrastructures.

Detection, Response, Cyber-attacks, Security Architectures

1. INTRODUCTION

When examining cyber and operational risk mitigation strategies, it is understandable that technologists tend to focus more on the technology side than the business side. However, the original decisions to modernise and deploy SCADA systems within national infrastructures were based on business assessments, which determined that the required investments were justified based on quantifiable financial benefits and non-quantifiable benefits, such as improved level of service and customer satisfaction (Ehrenreich (2005)). Similarly, current and future investment decisions in cyber-security will be based on a business case examining the financial implications and other intangible risks and benefits.

Infrastructure operators will thus make decisions on their cyber-security posture based ultimately on a business assessment. Arguably, the emergence of sophisticated targeted attacks, such as Stuxnet, Duqu and Flame, or the effectiveness of bleeding edge technologies that attempt to detect such advanced persistent threats (APTs), will play only a small part in the decision process for most small-to-medium size operators. Why? Because, as discussed by Cardenas et al. (2009), not only will an all powerful adversary usually defeat security mechanisms, but the cost of defence will be prohibitively high. In practice, the risk for a small-to-medium size operator of being directly targeted by a truly APT, such as Stuxnet, is quite low. Therefore, given (a) the very low probability, and (b) the low chance of resisting such an attack, there is not a strong business case for implementing costly APT risk mitigation strategies.

Consequently, the scope of this presented work is to explore a cyber-security approach that meets the business needs of small-to-medium sized operators of industrial controls systems that support national infrastructure, in terms of both cost and satisfactory cyber-risk mitigation. The architecture described herein was developed in the context of the EU-funded PRECYSE project[1], which includes such critical infrastructure operators. Primary requirements from these operators include that security measures should not disrupt operational systems and be implementable at a reasonable cost. To address the first requirement the implementation of the architecture takes an *overlay-based* approach, requiring a minimal number of monitoring interfaces to the operational infrastructure. The second requirement is addressed by, wherever possible, integrating open-source solutions with necessary novel security technologies, via the use of open standards.

The approach proposed in this paper can be used to by operators to detect cyber-threats in the different domains (or *enclaves*) that are associated with their infrastructure, and supports the execution of appropriate response strategies.

[1]The PRECYSE project https://www.precyse.eu

Submitted to ICS-CSR for review

2. RELATED WORK

There is a great deal of related work in the area of detecting and responding to cyber-attacks; here we provide a brief summary. The canonical network intrusion detection system (IDS) is the open-source Snort IDS[2] tool. Snort makes use of *signatures* – descriptions of malicious behaviour – to detect attacks. Similarly, commercial systems from Cisco[3] and others make use of signatures to detect attacks. The PRECYSE approach builds on these systems, and adds capabilities, regarding the detection of the misuse of SCADA protocols (as discussed in Section 3.2). Complementing signature-based detection, there has been significant research interest and deployment of systems that aim to identify deviations from normal traffic behaviour – *anomalies* – that are indicative of an attack (Chandola et al. (2009)). PRECYSE implements a flexible open standards-based approach to integrating such detection systems, and uses novel systems to detect anomalies in system behaviour.

In a similar way, Security Information and Event Management (SIEM) solutions aim to correlate and visualise detection events from IDSs, in order to develop situation awareness. Perhaps the best known SIEM solution is the Open Source Security Information Management (OSSIM)[4] system. Using OSSIM, so-called *directives* can be used to correlate *alerts* from IDSs and, using a risk-based approach, generate *alarms* that an operator can act on. Commercial products from companies, such as RSA[5], offer similar solutions to OSSIM, and make use of *big data* to implement security analytics tasks (Cybenko and Landwehr (2012)). To the best of our knowledge, these systems are not able to readily integrate data from both the ICT and ICS domain of a critical information infrastructure, as we propose.

As part of an overall approach to network resilience (Sterbenz et al. (2010)), Schaeffer-Filho et al. (2012) have developed a resilience management framework. The management framework realises a control loop, which takes *detection* events from a network infrastructure and, based on policies, determines a suitable *remediation* action to implement. This is similar to the approach proposed by PRECYSE. However, evaluation of the management framework has largely been simulation-based – in contrast, PRECYSE is developing a prototype implementation – and their work focuses on threats to large ICT networks.

[2]Snort IDS http://www.snort.org/
[3]Cisco Intrusion Prevention System http://www.cisco.com/go/ips
[4]The OSSIM SIEM solution http://www.alienvault.com/open-threat-exchange
[5]http://www.emc.com/security/security-analytics/security-analytics.htm

3. THE PRECYSE APPROACH: DETECTION AND COUNTERMEASURE

Although past evidence[6] is limited, it suggests attacks on operators of small-to-medium sized infrastructure often begin with successful intrusion through exterior defences, in order to execute further activities. A basic cyber-security strategy that focuses mainly on preventing attacks from penetrating the exterior will quite probably not detect malicious activities once the intruder is inside. Therefore, in order to improve upon such a basic cyber-security stance, and taking into account the primary requirements identified by the operators in PRECYSE, an approach to detecting and mitigating cyber-attacks is proposed that adopts several key features for improving cyber-protection for small-to-medium sized operators: *(i)* the use of *security enclaves*; *(ii)* perimeter defence and interior anomaly detection; *(iii)* an event correlation framework; *(iv)* countermeasure management system; and *(v)* an open source and standards based approach.

A security enclave is a group of systems with common security policies, in order to minimize the attack surface and the impact of a security breach (FORCE (2013)). Enclaves may be defined by logic function, role or physical location. Figure 1 shows how an operator's infrastructure can be divided into Process network, SCADA network, Office Network and Central System enclaves.

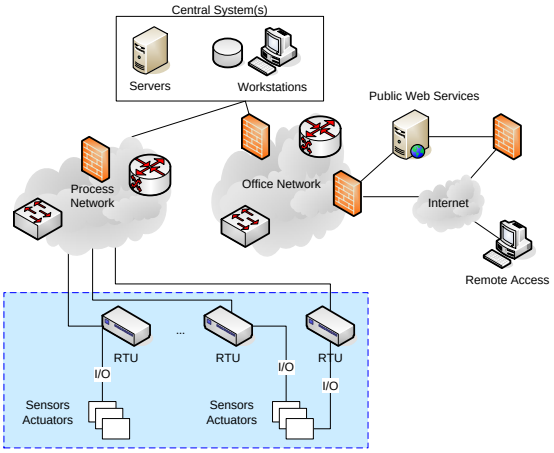

Figure 1: *Overview of the PRECYSE network enclaves*

The proposed approach is that enclaves are monitored by a comprehensive set of tools in order to protect all classes of ICT and ICS assets. For enclaves that include specialised SCADA operations, customised tools can be adopted to enhance security monitoring capabilities. For example, a security client may check for compliance to protocols in the

[6]"Hackers darkened cities, CIA says" http://www.securityfocus.com/brief/666

SCADA communications, while another assesses the wider network communications for anomalous patterns. Each security tool provides local security, attack detection and log management, while a central system provides decision making across enclaves, regarding attack mitigation and the issuance of countermeasures during attacks.

3.1. Architecture Implementation

We are currently developing a first prototype of the approach described above. Where possible, the implementation makes use of existing open-source tools and open standards, as a way of managing implementation costs and the integration of new technologies. Reflecting our end-user requirements, the implementation requires minimal disruption to the existing infrastructure – monitoring of the infrastructure is realised using network taps and via the analysis of operational log files.

Furthermore, the approach is deployed as an *overlay* to the target infrastructure enclaves, using virtualised networks (VLANs) and systems. The various detection systems communicate via an Enterprise Service Bus (ESB), allowing the flexible integration of new security services. The various detection systems generate alerts in the Intrusion Detection Message Exchange Format (IDMEF) (Debar et al. (2007)). As necessary, adaptors have been developed that can generate and consume IDMEF messages, in the Web services SOAP format, for each of the systems in the architecture.

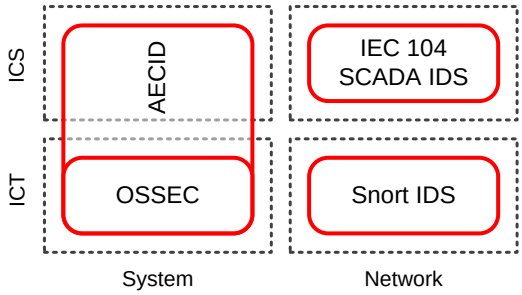

Figure 2: *The detection technologies that are applied to the ICS and ICT enclaves, from a system and network perspective*

To ensure coverage of the different enclaves of a critical infrastructure, we make use of a range of detection capabilities, which are summarised in Figure 2. In what follows, we provide a brief introduction to each of these technologies.

3.2. Intrusion Detection for IEC 60870-5-104

The IEC 60870-5-104 SCADA protocol is widely used for telecontrol communications for water, gas and electricity systems, and is of specific interest to end-users within PRECYSE. In the project, we have developed a SCADA IDS toolset for the IEC 104 protocol, based on deep-packet inspection of SCADA packets at the application layer. This enables protocol verification and data correlation approaches to be deployed. In one approach, custom rules for IEC 104 have been derived that are compatible with the Snort IDS (Yang et al. (2013)). In a second approach, this is enhanced with stateful analysis of the protocol across the packet flow to enable a more sophisticated analysis of the IEC 104 communications (Yang et al. (2014)). The aim is to monitor the SCADA communications at the application layer, in comparison to standard tools that only examine the TCP/IP layers. Although IEC 104 is the focus here, we propose that similar IDS tools can be used to secure different SCADA network enclaves, which use protocols such as IEC 61850.

3.3. AECID: Correlating Anomalous Behaviour

As part of the operational management of the ICT and industrial control systems in a critical information infrastructure, logging data is produced to report events, internal state changes, and committed actions. This data is used by the Automatic Event Correlation for Incident Detection (AECID) system to detect anomalous behaviour, which could be indicative of an attack (Skopik et al. (2014)). AECID collects log files from systems in the ICT and ICS domain, maintaining the temporal order of log messages, and creates search patterns from single log lines. The aim of AECID is to correlate the different events, expressed in log lines, including their relative position to each other. For that purpose, it creates hypotheses about causes and effects. If a hypothesis can be confirmed as valid, it becomes a part of a model of the system. An ongoing statistical analysis of correlation results allows the system to infer the degree of deviation of “if-then” hypotheses related to events, and therefore determine a degree of anomalous behaviour.

3.4. Integrated ICT Security Solutions

As discussed, we target the use of open-source tools where possible, and we have integrated and deployed just such a toolset to provide monitoring capabilities across a broad spectrum of network data, including configuration, topology and traffic. A common data model is used for all processing of data in order to provide interoperability. The open-source toolset comprises: a set of tools (Snort, Barnyard, PRADS, netsniff-ng) observing the network traffic; a firewall system for the enforcement of traffic blocking countermeasure actions, based on Netfilter and Shorewall; a host-based IDS, based on OSSEC; and a user interface that is used within an enclave, based on Sguil, Squert and MySQL.

3.5. Issuing Countermeasures

The alerts from the aforementioned systems are subjected to a correlation phase – for the first version of the implementation, we propose to leverage the solution provided by OSSIM. A challenge associated with this approach is the specification of suitable correlation directives; future work will seek to develop machine learning approaches to support this process, in a similar manner to the AECID system. After the correlation phase, an alarm is presented to an operator that can be used as a basis for issuing a countermeasure to the attack, e.g., block network traffic or isolating systems. In previous work, we have developed the concept of *management patterns* that describe best-practices for addressing specific threats, using a number of remedial systems. These were focused on the description of remediation strategies for challenges to ICT networks. Moving forward, we plan to express these management patterns for the other enclaves of a critical information infrastructure, building on the Common Remediation Enumeration (CRE) format[7].

4. CONCLUSION AND FUTURE WORK

We have presented a cyber-security approach for securing small-to-medium sized ICS infrastructures, which meets the requirements of users in the PRECYSE project. The most significant feature of this work is that the approach is sufficient to provide comprehensive monitoring of ICS and ICT domains, while also meeting budgetary constraints through the adoption of open-source methods, where possible. Additionally, novel security tools have been developed and integrated to provide further tailored monitoring of SCADA protocols and for behavioural anomaly detection. The flexible approach allows the toolset to be tailored to enclaves with differing security polices, and for the integration of further tools where necessary. In PRECYSE, we have implemented a first version of the approach at two ICS demo sites, where verification via a comprehensive range of cyber-attack use cases is ongoing.

ACKNOWLEDGEMENTS

The research presented in this paper has been supported by the PRECYSE project, funded by the European Commission with contract FP7-SEC-2012-1-285181 (www.precyse.eu). The authors are grateful to the members of the PRECYSE consortium, whose research has contributed to the outcomes described in this paper.

[7]http://scap.nist.gov/specifications/cre/

REFERENCES

Cardenas, A. A., T. Roosta, and S. Sastry (2009). Rethinking security properties, threat models, and the design space in sensor networks: A case study in scada systems. *Ad Hoc Networks 7*(8), 1434–1447.

Chandola, V., A. Banerjee, and V. Kumar (2009, July). Anomaly detection: A survey. *ACM Comput. Surv. 41*(3), 15:1–15:58.

Cybenko, G. and C. Landwehr (2012). Security analytics and measurements. *IEEE Security Privacy 10*(3), 5–8.

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

Ehrenreich, D. (2005). Operating benefits achieved with scada for water distribution. *BCWWA Conference*.

FORCE, J. T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication 800*, 53.

Schaeffer-Filho, A., P. Smith, A. Mauthe, D. Hutchison, Y. Yu, and M. Fry (2012, April). A framework for the design and evaluation of network resilience management. In *Proceedings of the 13th IEEE/IFIP Network Operations and Management Symposium (NOMS 2012)*, Maui, Hawaii, USA, pp. 401–408. IEEE Computer Society.

Skopik, F., I. Friedberg, and R. Fiedler (2014, February). Dealing with Advanced Persistent Threats in Smart Grid ICT Networks. In *5th IEEE Innovative Smart Grid Technologies Conference*, Washington DC, USA.

Sterbenz, J. P. G., D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith (2010, June). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET) 54*(8), 1245–1265.

Yang, Y., K. McLaughlin, T. Littler, S. Sezer, and H. Wang (2013). Rule-based intrusion detection system for scada networks. In *Renewable Power Generation Conference (RPG 2013), 2nd IET*, pp. 1–4. IET.

Yang, Y., K. McLaughlin, S. Sezer, Y. Yuan, and H. W (2014). Stateful intrusion detection for iec 60870-5-104 scada security. In *IEEE PES General Meeting*. IEEE.