# Security Correlation Analysis System for Insider Threat Detection of Industrial Control System

Young-jun Heo[1], Seon-gyoung Sohn[1], Jung-chan Na[1] and Beom-hwan Chang[2]
[1]Electronics and Telecommunications Research Institute
218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea
[2]Div. of Cyber Investigation Police, Howon University
727 Howondae-gil, impi-myeon, Gunsan-city, Jeonbuk
yjheo@etri.re.kr

## ABSTRACT

The security accident is increasing in industrial infrastructure. The security of industrial control system is caused not only by deliberate acts of external attacker but also by sometimes inadvertent threats of legitimate inner operator. The latter can ultimately have more devastating consequences. Industrial control system works deterministic and restrictive operation. The anomaly communication patterns may be relevant to attack activities or misconfiguration of operator. To detect these threats in industrial control system, we propose security data objects that describe operation and state of system and security correlation analysis system that collects and analyzes these objects and detects intrusion or anomaly state of system. Our approach may provide complementary detection ability for protecting internal threat of industrial infrastructure.

## KEYWORDS

ICS security data object Correlation analysis; internal threat detection; industrial control system;

## 1 INTRODUCTION

Industrial control system (ICS) infrastructures, such as gas/oil pipeline, power generation and water/wastewater distribution, are large facilities that are distributed over large areas. The ICS system continuously monitors these infrastructure facilities in order to guarantee accurate operation and safety of these components. They must perform under strict conditions and use proprietary protocols to communicate control and data between devices. They have been use digital system to improve efficiency. And, there is an increasing trend toward the usage of common IP protocols and the interconnection with other networks and even the Internet, and software and hardware. Also, ICS infrastructure is vulnerable that they were not designed with security and safety in mind. Recently, security accident is considerably increasing and an accident has extreme consequences to human life.

Conventionally, organizations have focused their security management efforts on mitigating threat beginning from outside the ICS infrastructure boundary. However, organizations have come to realize that advertent and inadvertent insider threats can result in significant losses in social and economic property if the organization fails to mitigate insider threat. In a recent survey of information security professionals, 52% cited that they we most concerned about the magnitude of the damage that can result from trusted insider actions of ICS [1]. An insider threat can pose a threat to an organization in a variety of ways: [2]

- Malicious or inappropriate use of authorized credentials
- The authorized user may not be an employee of the organization
- Insider threats can appear in numerous forms
- Inappropriate use of access

The increased awareness of the insider threat has led to significant interest in techniques which can effectively detect malicious or non-malicious insiders in ICS [3]. Many ICS organizations remain vulnerable to insider threats. Event and Site Security (ESG)'s research illustrates a portentous situation—organizations are vulnerable to a myriad of insider attack vectors and finding it increasingly difficult to detect these incidents [4]. Unfortunately, the techniques for mitigating the insider threat are relatively immature and have not gained wide acceptance or use. This is despite research which indicated that the application of best practices including policy and training improvements, creating behavioral models to detect malicious behavior, and very basic network monitoring and analysis would have mitigated many of the insider threats studied [5,6]. Valdes A. et al. present a work to demonstrate that anomaly detection, and specifically methods based on adaptive learning, can provide a useful intrusion detection capability in ICS [7].

ICS security is non-trivial since the ICS infrastructure has different control process and very complex, so they perform their process under strict conditions and individual different environment. Also, they use dedicated networks running proprietary protocols. Zhu etc. discusses past work on classification and characteristics of attacks and ICS specific Intrusion Detection System (IDS) attempts [8].

In this paper, we propose ICS security data object to detect internal threat and manage performance and reliability management of the ICS information infrastructure. Also we discuss our correlation analysis approach focused on the detection insider threat and unusual situation of ICS infrastructure. Our approach has collecting and correlating industrial network monitoring and intrusion detection objects.

## 2 ICS SYSTEM and NETWORKS

The ICS infrastructure consists of sensors,

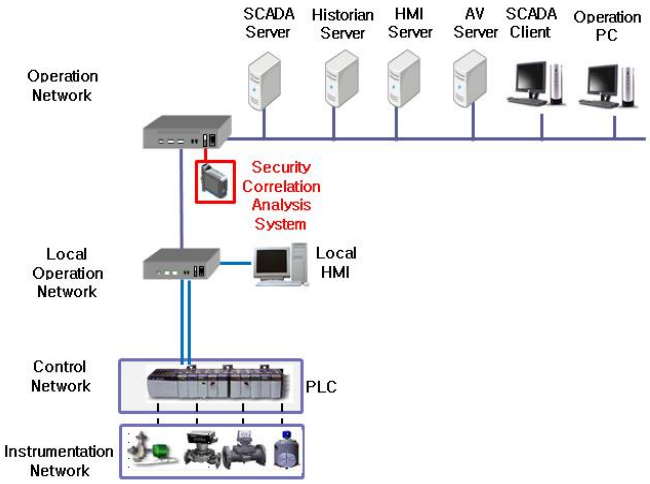


**Figure 1.** ICS infrastructure and security correlation analysis system

Remote Terminal Units (RTUs), control systems, workstations, ICS Servers, Historian Servers, Human-Machine Interfaces (HMIs), and network devices as shown in figure 1. The ICS infrastructure operations are increasingly reliant on information infrastructures, including communication networks, and self-defining communication protocols. The HMI allows human operators to monitor the state of a control process and issue commands to change the control objective. ICS systems operate widely dispersed control systems and acquire system data for monitoring and control at the central server.

The characteristic of ICS networks is much different to those of IT networks. This is due to a number of reasons [9]. The ICS infrastructure is often characterized fairly deterministic communication patterns between master and slave units, and a fairly static address space. These are expected to be more stable over time. From this point of view, we monitor connection patterns between systems, connection dispersion, and traffic content. The ICS infrastructure is static, both in the sense of network topology and the tasks performed on the network, so. Servers and networking systems are infrequently added to a system once it goes live; they also serve one single purpose, which is running ICS software [10]. A

ISBN: 978-1-941968-03-1 ©2014 SDIWC

qualitative measure of the potential loss incurred by unauthorized access to network link requires knowledge of the services available on the link and the actions that a motivated attacker could perform by manipulating the available services to execute malicious software on a target device.

## 3 ICS SECURITY DATA OBJECTS

To provide the necessary high levels of security and reliability in power system operations, IEC defines IEC 62351-7 Network and System Management (NSM) data object models [11]. IEC 62351-7 NSM data object models have 3 types category: Communications Health, End System Health, and Intrusion Detection. End System objects are not appropriate to ICS system monitoring because the collection of some data objects in ICS is not suitable for computing power and environment of PLC. So we modify IEC 62351-7 data object models to ICS security data object models for the internal threat detection and the performance and reliability management of the ICS information infrastructure. The ICS security data object models have communication health and intrusion detection health as shown in table 1.
Communication health defines communication information objects such as network configuration monitoring, network communication monitoring, communication protocol monitoring, and network traffic monitoring. Specially, we add network traffic monitoring to monitor network session information that used to abnormal network situation detection. Intrusion detection includes intrusion detection information such as unauthorized access, buffer overflow, and invalid network access. Each group consists of configuration setting, alarm, and values. The user sets values to device by using configuration setting. ICS security data object management get information of their alarms and values object from ICS facilities and delivery this information to security correlation analysis.

TABLE I. ICS SECURITY DATA OBJECT

| *Category* | | | *Object* |
|---|---|---|---|
| Communications Health | Network Configuration Monitoring | Configuration Settings | EndLst<br>ACLLst |
| | | Alarm | EndDct |
| | Network Communication Monitoring | Configuration Settings | ConnFailTmms<br>ConnRtryCnt<br>ConnRtryTmms<br>ConnFailRtryCnt<br>ConnFailRtryTmms |
| | | Values | RsTmms<br>ConnFailTot<br>ConnTotTmms<br>ConnCurTmms<br>ConnAvTmms<br>ConnRej |
| | Communication Protocol Monitoring | Configuration Settings | ProtId, ProtVer |
| | | Alarms | ProtMisAlm<br>ProtAcsAlm |
| | Network Traffic Monitoring | Configuration Settings | ConnCnt<br>ConnSimCnt |
| | | Alarms | ConnAlm<br>ConnFailAlm<br>ConnExcAlm<br>ConnExcSimAlm<br>IdlTmmsMinAlm<br>IdlTmmsMaxAlm<br>sessionInfoAlm |
| | | Values | protoID<br>srcIpAddr<br>srcPortNum<br>dstIpAddr<br>dstPortNum<br>ssnStatus<br>firstTime<br>lastTime<br>msgSentCnt<br>msgSentByt<br>msgRcvdCnt<br>msgRcvdByt |
| Intrusion Detection | Unauthorized Access | Configuration Settings | AuthUsrLst |
| | | Alarms | UnAuthAlm |
| | | Values | UnAuthUsrId<br>UnAuthUsrCnt<br>UnAuthRte |
| | Buffer Overflow | Alarms | BufOvAlm<br>BufUnAlm |
| | | Values | BufOvCnt<br>BufUnCnt<br>BufUsrId |
| | Invalid Network Access | Configuration Settings | TrfFrqSet<br>TrfVolmSet |
| | | Alarms | TfrFrqAlm<br>TrfVolmAlm |
| | | Values | TfrFrq<br>FrfVolm |

ISBN: 978-1-941968-03-1 ©2014 SDIWC

## 4 SECURITY CORRELATION ANALYSIS SYSTEM

To detect internal threat in ICS system, we propose security correlation analysis system (SCAS). This system collects and correlates ICS security data objects. The SCAS system detects unusual event or state such as unauthorized access, buffer overflow attack, invalid network access, and unauthorized protocol usage may be relevant to attacker or operator's misconfiguration.

The SCAS consists of data collection module (DCM) and correlation analysis module (CAM) as shown in figure 2. The DCM collects network packets from ICS infrastructure, creates alarm and value objects of communication health and intrusion detection, and sends these data to CAM. The DCM manages flows information with similar traffic feature by destination address, destination port, and source IP address, and creates alarms with a simple comparison between configuration settings and values.

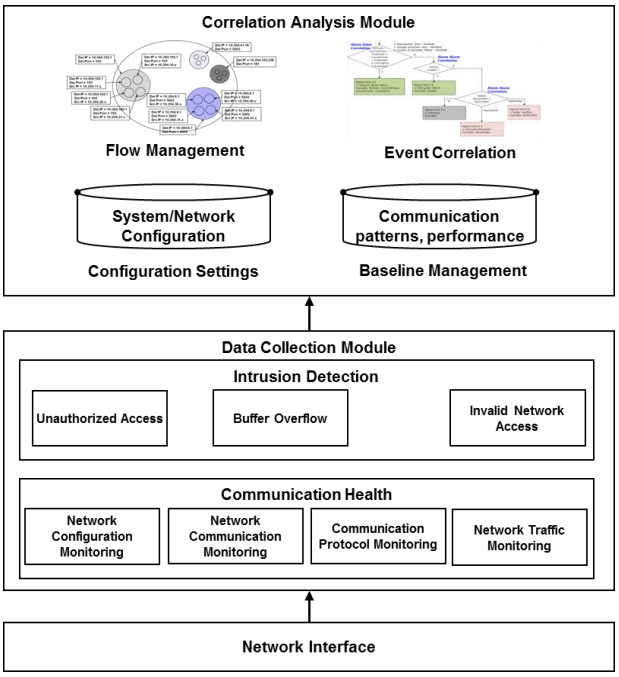


**Figure 2. Security correlation analysis system architecture**

The CAM receives security data objects from DCM, correlates these objects, and detects unusual situations in ICS infrastructure. To detect attack or anomaly state, the CAM analyzes ICS security data objects and compute connection patterns between systems, connection dispersion, and traffic content. This has 4 mechanisms; flow management, event correlation, baseline management and configuration settings. The user set threshold value to detect intrusion through configuration settings.

The baseline management treats communication pattern and performance of hosts. We establish baselines by understanding communication performance and usage patterns of ICS infrastructure. The connection patterns include network connectivity, number of peers, number of source ports, and number of destination ports. The connection dispersion is ratio of source IP and destination IP. The traffic content includes the mean number of packets per flow, percentage of small-size and large-size packets, and distribution of medium sized packets. The SCAS system detects anomaly communication patterns and unauthorized access that may be relevant to attack activities or misconfiguration of operator.

The flow management deal with session information between hosts and classifies same operation of hosts to same group. Due to the nature of the SCADA system, systems of same group work the same operation to perform same function. The number of generated group is determined by service or operation. So the system in the same group make same message that has same message size, message interval, protocol. The flow management detects anomaly system behavior through comparison between same group systems. The flow management detects abnormal behavior of system through comparison between systems of the same groups.

The event correlation correlates intrusion detection objects and communication health objects to detect anomaly situation of ICS infrastructure. We design 40 algorithms to

detect denial of service attack, unauthorized access, invalid data, configuration error, and software fault. Figure 3 shows a SCAS user interface that is designed to display security event and correlation result.

**Figure 3. SCAS user interface**

## 5 CONCLUSION

In this paper, we propose ICS security data objects and security correlation analysis system. This system collects and analyzes security data objects. Our approach may provide complementary detection ability for protecting internal threat of ICS infrastructure. The SCAS has flow management, event correlation, baseline management and configuration settings. We will extend our research to develop an ICS Security Information and Event Management (SIEM) solution.

## 6 ACKNOWLEDGEMENT

This work was supported by the IT R&D program of MISP/IITP. [10041560, A development of anomaly detection and a mult-layered response technology to protect an intranet of a control system for the availability of pipeline facilities]

## 7 REFERENCES

[1] Hall, S. 2008. Turbulent Economy Adds to Risk of Insider Threat, IT Business Edge, December 22, 2008,http://www.itbusinessedge.com/cm/community /features/articles/blog/ turbulent- economy-adds-to-risk-of-insider-threat/?cs=23208

[2] EY, Authorized access: uncovering insider threats within oil and gas companies, http://www.ey.com/Publication/vwLUAssets/EY_Our_experience_will_enable_you_to_detect_and_respond_to_the/$FILE/EY-Authorized_access_uncovering_insider_threats_within_ oil_and_gas_companies.pdf, 2013

[3] Wilson, T. 2009. State of Security: What Keeps Infosec Pros Awake at Night? Information Week Analytics and Dark Reading, February 2009, http://www.stateofsecurity. informationweek.com/.

[4] Jon Oltsik, 2013 Vormetric/ESG Insider Threats Survey, The Ominous State of Insider Threats, September, 2013

[5] Carnegie Mellon University. 2007. Over-Confidence is Pervasive Amongst Security Professionals. E-watch Crime Survey.

[6] Myers, J., Grimaila, M.R., and Mills, R.F., "Towards Insider Threat Detection using Web Server Logs," Proceedings of the Cyber Security and Information Intelligence Research Workshop (CSIIRW 2009), Oak Ridge National Laboratory, Oak Ridge, TN, April 13-15, 2009.

[7] A. Valdes, S. Cheung, Communication Pattern Anomaly Detection in Process Control Systems

[8] B. Zhu and S. Sastry, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy", In proceedings the First Workshop on Secure Control Systems (SCS'10), 2010.

[9] S. Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, Alfonso Valdes, "Using Model-based Intrusion Detection for SCADA Networks", SCADA Security Scientific Symposium, 2007

[10] R. Rafael, B. Regis, S. Ramin, P. Aiko, "A First Look into SCADA Network Traffic", IEEE NOMS, 2012.

[11] IEC 62351-7 TS Ed.1: Power systems management and associated information exchange –Data and communication security –Part 7: Network and system management (NSM) data object models