Proceedings of the 5th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'19)
Lisbon, Portugal – August, 2019
Paper No. EEE 117
DOI: 10.11159/EEE19.117

Direction of Security Monitoring for Substation Automation Systems

Sugwon Hong, Jae-Myeong Lee
Department of Computer Engineering and Next-Generation Power Technology Center, Myongji University
116 Myongji-ro, Cheoin-gu, Yongin, Gyeonggi-do, S. Korea
swhong@mju.ac.kr; ljm9317kr@gmail.com

Abstract - All security measures which have been proposed ultimately come under three security strategies: network separation, communication message security, and security monitoring. However, considering the recent sophisticated attacks against SCADA/ICS systems, these security strategies cannot provide sufficient security measures. These attacks try to hijack or take control of host systems, control servers and eventually control devices, once they penetrate the networks in one way or another. Their attack vectors are the vulnerabilities of the software underlying the host systems. The attack was realized by injecting malicious codes into legitimate process memory and executing the malicious codes in the context of a legitimate process, and eventually cause malfunction of field devices. In this respect, we need a security measure running on host systems which can provide the process and file protection related to legitimate usage of memory ranges and file paths. The measure can provide a holistic security strategy for SCADA systems including substation automation systems.

***Keywords*:** Security, Substation, SCADA, Host IPS, IDS, Monitoring.

1. Introduction

All security measures which have been considered and published for substation automation systems can be classified into three categories: *physical/logical network separation, communication message security, and monitoring*.[1] These strategies are based on the concept of Defence in Depth.[2,3] The logical separation is to separate a SCADA network into several segmented zones or domains depending on criticality or functionality.[4] Firewall and intrusion prevention systems (IPS) are common equipment used for this purpose, and virtual Private network (VPN) is a common network design technique used for deploying dedicated networks. The network separation is the major security strategy which the current SCADA/ICS systems depend on, and it will keep on being so in the foreseeable future. The communication message security aims at providing authenticity, integrity, and/or confidentiality of messages exchanged in the systems. IEC 62351 standards specify the security measures for this purpose.[5] This will raise security class a notch if installed in the substation automation system. As an another security strategy, the security monitoring in the SCADA is still in its infancy. It is hardly installed yet in the current SCADA/ICS systems. However, the network IDS/IPS is gaining interests as an efficient security approach in the SCADA/ICS because SCADA networks have very predictable traffic patterns compared to IT networks, and IDS/IPS can be easily adapted without any major configuration change of SCADA systems. [6]

Even though these three strategies give us a holistic approach to SCADA security, recent attacks on SCADA/ICS systems such as Stuxnet, Black Energy, Trisis, and Crashoverride make us recognize that these strategies are necessary but not sufficient. [7-14] The nature of these attacks is that once attackers penetrate the network, it takes control of host systems by process manipulation, whether they are control servers or local device controllers. Thus, either communication message security measures or security monitoring base on the network IDS/IPS cannot detect malfunctions committed by these attacks, much less prevent them. For this reason, we need an additional measure to detect these sophisticated attacks, which can be acting as a special purpose host IPS.[15] In the following two sections, we briefly explain the communication message security and network monitoring methods. And then in section 4 we explain the substantive nature of these attacks and propose a measure to prevent them.

2. Communication Message Security

While physical network separation is the first line of defence, security at the level of communication messages can be regarded as the last line of defence from the viewpoints of substations. Any intruder's final attack goal is to impair the

functions of primary field devices in substations and ultimately disrupt proper operations of substations. The goals of message security are to guarantee message integrity, message authentication, and/or message confidentiality. That is, message security prevents intruders from manipulating messages by modifying message contents, injecting false messages, reusing old messages. So, this security strategy can raise substation security capability at the same level as online banking or online transaction in the IT network.

In substation automation systems there are three kinds of message exchanges: between control devices such as IEDs inside a substation, between different substations, between substations and control centers. The IEC 61850 standards define the communication protocols for information exchange in the substations. The IEC 62351 standards aim at developing security solutions for specific IEC 61850 communication protocols. Unlike other SCADA-related security standards, these standards specify the technical details of security measures.

The IEC 62351 standards adopt the common IT security algorithms and protocols to derive security measures, such as crypto algorithms, keyed-hash message authentication code (HMAC), digital signature, and Transport Layer Security (TLS). There are two factors to be considered to choose proper security solutions. One is the underlining network stacks. TLS is commonly used in every application running over the TCP/IP in the current IT network, thus choose TLS as the security protocol for client-server application running over the TCP/IP stacks, since TLS provides all the flavors required for message security.[16] The other factor to select proper security solutions is to meet the performance criteria for each application. The time-critical application based on the bare Ethernet communication may choose any message authentication protocols such as HMAC, digital signature, or others, avoiding heavy computing loads involving in encryption/decryption.[17] For a practical reason, HMAC is preferable over digital signature which requires the public key crypto computation.

3. Intrusion Detection System(IDS) for SCADA systems

Network security monitoring (NSM) is to do the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. NSM is a way of finding intruders on the network and do something about them before they damage the system. In a nutshell, monitoring is involved in detecting and reporting any illegal behaviour in the system, consequently providing the necessary high-level of security and reliability in the SCADA system.

The intrusion detection system (IDS) is a main tool to do security monitoring. The techniques of IDS in which we are interested for the SCADA security monitoring is the anomaly-based detection. The anomaly detection is the process to determine which observed events are to be identified as abnormal because it has significant deviation from normal behavior which is called profile. As always, the difficult part is how to decide or derive profiles which reflect all characteristics of the system. Thus, the main task to do security monitoring is to design domain-specific IDS which is conscious of the target domain semantics. In the framework of the anomaly-base intrusion detection, the learning procedure to derive profiles is part and parcel of the process. Analyzing the inputs during the learning procedure derives profiles or normal behavior which is otherwise called whitelists, rules, or models in other literatures. We classify the currently proposed SCADA-specific IDS into four categories: network features, application protocols, device characteristics, and other domain-specific normal activities. [6]

First, inputs to be utilized to derive profiles is the information about target network features. SCADA networks have very predictable patterns compared to the IT network.[18] In the IT network, it is not possible to completely predict a list of allowable communication paths. A large portion of the traffic occurring in the IT network is involved in human actions, leading to dynamic traffic patterns. On the contrary, the SCADA network configuration is stable and has the fixed communication paths and IP addressing schemes. Unless there is any abrupt change in the system configuration, intentional or unintentional, communication paths are deterministic since data exchanges take place between fixed nodes such as IEDs, servers, and other devices, which is mostly machine-to-machine communication.

Secondly, the application protocol header information is used as input for learning. In this case, the semantics of each fields of the header in the application protocol data unit (PDU) can be used to verify the validity of the incoming packets. Any correlated rules between different fields of the same packet or between the fields of subsequent packets are also utilized as effective criteria to decide whether incoming packets obey the logic of the application protocols. For example, if the sequence number field exits in the header, the sequence numbers of all packets should be in order, and the following packet's number should be incremented by one. Time stamp field is also useful to check the correctness of a series of arriving packets. In this way, the extracted header information of incoming packets is compared with profiles by simple matching or sometimes checking rules between headers or between a sequence of packets. The paper [6] explains the various protocols to derive the profiles.

The effectiveness of IDS will increase as we can derive profiles which are more aware of semantics of the target system. If we can find out features of field devices to help to monitor traffic, we can enhance the performance of IDS. The paper [19] shows the way of monitoring the status information of PLC. PLCs exchange comprehensive status information with the ICS server on a regular basis, and in turn the HMI issues control commands to the PLCs to initiate process changes. Both activities can be reflected at the network level in the form of requests and replies that report and manipulate PLC process variables, encoded in their corresponding network representation. So, they can catch the network features to reflect PLC status information. Another possible way of deriving profile is to use machine learning techniques, and we expect that more researches will be carried out on machine learning methods.

4. Canary in the Host System

The security strategies as explained in the previous sections may be potent bullets, though not silver bullets, to encounter the current and upcoming threats to the substations. However, considering the substance of the recent sophisticated attacks we have gone through, these strategies miss the target. The attacks that shocked the people in SCADA/ICS system tried to hijack or take control of host systems, control servers and eventually control devices, once they penetrate the networks in one way or another. Their attack vectors are the vulnerabilities of the software underlying the host systems. In this respect, we need to pay attention to the supply chain management and precaution for managed servers and/or outsourcing. But if we want to find any security solutions on top of vendor-independent platforms, we need to take special notice of the attack patterns which have been revealed in the recent incidents.

First, the shortcoming of the communication message security is that the attacks did not take place via the standardized and defined communication messages. Rather, the attacks were accomplished by virtue of taking over central servers and local device controllers. As shown in the Stuxnet, the attack was realized by injecting malicious codes -DLL files in the case of Stuxnet- into legitimate process memory and executing the malicious codes in the context of a legitimate process. Once a code is injected into the target process, it has full access to the process memory and can manipulate code and data blocks of programmable logic controllers (PLS), and eventually cause malfunction of field devices. For this reason, the authenticity and integrity check of the messages which are exchanged between control servers and local device controllers as defined in the IEC 61850 standards cannot detect these kinds of attacks.

Secondly, the network IDS which is currently proposed in the context of substation automation systems is intended to detect anomaly behavior based on traffic patterns or contextual mismatch of message contents which are specified in the standard protocols such as IEC 61850. However, this approach cannot detect these kinds of attack which is mainly related to process manipulation in host systems.

In order to detect and prevent such attacks, we need security measures to detect any process manipulation which is involved in memory range protection, file paths, and file handling. The following pseudocode shows a high-level description of one possible technique.

host process set: $P=\{P_1, P_2,\ldots, P_m\}$
memory range set: $M_i=\{M_{i1}, M_{i2},\ldots, M_{in}\}$ for each process i
file path set: $F_i=\{F_{i1}, F_{i2},\ldots, F_{in}\}$ for each process i

derive allowable process executable pairs: $S=\{P_i, (M_{ij}, F_{ik})\}$
while (executing process)
  if illegal file modification, alert
  record Mi, Fi for current Pi
  if (Pi, Mi, Fi)) $\notin$ S then alert

5. Conclusion

Together with network separation which is currently used in the SCADA security, communication message security and security monitoring are expected to enhance SCADA security level. However, considering the recent attacks against SCADA/ICS systems, these security strategies do not provide sufficient measures to detect and prevent these sophisticated attacks. The nature of these attacks performs process manipulation by injecting malicious codes into legitimate process memory and executing the malicious codes in the context of a legitimate process. Thus, we need a security measure running

on host systems which can provide process and file protection which are related to legitimate usage of memory range and file path. The measure can provide a holistic security strategy for substations, furthermore SCADA/ICS systems.

Acknowledgements

This work was supported by "Human Resources Program in Energy Technology" of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea. (*No. 20174030201790*) And this research was also supported by Korea Electric Power Corporation. (Grant number: R18XA01)

References

[1] S. Hong, "Cyber Security Strategies and their Implications for Substation Automation Systems," in *proceeding of 15th Korea-China Joint Seminar on Power Systems Protection & Automation Technologies*, Yongin, Korea, Oct. 2018.

[2] *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. DHS ICS-CERT. September 2016.

[3] *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Rev.2, May 2015.

[4] *Industrial Communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. IEC TS 62443-1-1. 2009.

[5] F. Cleveland, "IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure," IEC, June 2012.

[6] S. Hong, "Monitoring and Network Management for SCADA Security and Its Implications," in proceeding of ICNSET, Sapporo, Jan. 2019**,**

[7] N. Falliere et al., "W32.Stuxnet Dossier version 1.4," Symantec, Feb. 2011.

[8] *Trisis Malware: Analysis of Safety System Targeted Malware Ver.1*, Dragos Inc., Dec. 2017.

[9] *Security Report: Black Energy*, ThreatSTOP, Feb. 2016.

[10] *Crashoverride: Analysis of the Threat to Electric Grid Operations*, Dragos Inc., June 2017.

[12] *ICS Defense Use Case No. 6: Modular ICS Malware*, I-ISAC, August 2017.

[13] TRISIS Malware Analysis of Safety System Targeted Malware, DRAGOS, December 2017.

[14] J. Weiss, "Control system cyber attacks have become more stealthy and dangerous – and less detectable," April 2019, https://www.controlglobal.com/blogs/unfettered.

[15] J. Chee, *Host Intrusion Prevention Systems and Beyond*, SANS Institute, 2008.

[16] *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security – Profiles including TCP/IP*, IEC TC57 WG15, IEC 61850-3, 2014

[17] *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850*, IEC TC57 WG15, IEC 61850-5, 2007

[18] A. Lemay., J. Rochon, and J. Fernandez, "A Practical flow white list approach for SCADA systems," *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research*, 2016.

[19] D. Hadziosmanovic, R. Sommer, and E. Zambon, "Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems," 2013.