Construction and Evaluation of Defense-in-Depth architecture in SCADA System

Xiaojun Zhou^{1,2}, Zhen Xu¹, Liming Wang¹, Kai Chen¹, Cong Chen^{1,2}, Wei Zhang^{1,2}

¹State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, 100195 E-park C1 North, No. 80 Xingshikou Road, Haidian District, Beijing, China

² School of Cyber Security, University of Chinese Academy of Sciences, 100049 No.19(A) Yuquan Road, Shijingshan District, Beijing, P.R.China

Abstract. The increasing use of common computer technologies in SCADA systems has brought convenience and at the same time introduced unprecedented security threats. SCADA system is becoming an attacker's target day by day. As attackers gain more understanding of industrial control systems, attacker's attack methods are more and more sophisticated, and the attack intensity is also increasing day by day. Faced with many security threats and risks, traditional security precautions cannot be effectively implemented. Therefore, this paper proposes an improved SCADA defense system, and evaluates it by using a variety of attacks. Experiments show that the defense-in-depth model we proposed is very effective against a variety of attacks.

1 Introduction

SCADA system is the core of industrial control system. The integration of physical space and cyberspace has deepened, bringing great convenience to SCADA system operation, saving costs, but also introducing new security threats and security challenges. In order to achieve the integration of management and control in SCADA system, engineers introduce the MES(Manufacturing Execution System), for management of network and control data exchange between networks and system integration, it is not an isolated system, but connected with management systems, control systems and even the Internet, introducing an unprecedented risk of attack. Moreover, SCADA system, its own problems are also very prominent^[1].

(1) Control equipment often cannot be updated and patch in time, exacerbating the SCADA system security risks.

(2) SCADA system lack of security design, the operating system, system architecture, communication protocol used do not consider data integrity, encryption, identity verification and other security functions;

(3) Staff security awareness is weak. SCADA system present a large number of misuse and abuse, and internal attacks are also gradually increased.

(4) There is no well-demarcated security zone.

(5) The IT department is responsible for security, the automation department is responsible for safety, and the two departments do not have a good communication with each other.

Therefore, we propose a deep defense mechanism for industrial control systems to alleviate the current serious security situation of SCADA system.

2 SCADA system model

Firstly, we conduct a comprehensive analysis of the SCADA system and analyze its attack surface in detail.

2.1. SCADA system structure

First, we conduct a comprehensive analysis of the SCADA system and point out its vulnerability and attack surface based on its own characteristics.

A typical SCADA system architecture^[4] is shown below (Figure 1). The control center has a SCADA server (MTU) and a communication router. Other control center components include the HMI (Human Machine Interface), engineer workstations, and historical database, all these are connected via a local area network. The control center collects and records the information collected by the stations, displays the information on the HMI, and may generate action based on the detected events.

* Corresponding author: author@e-mail.org

Fig. 1. The Architecture of SCADA system.

The control center is also responsible for central alerting, trend analysis and reporting. Field site is responsible for the local control of the actuator and for the monitoring of the sensor. Field sites are often equipped with remote access capabilities that allow field operators to perform remote diagnostics and repairs on a single dial-up modem or WAN connection. Standard and proprietary communication protocols running on serial links are used to transfer information between control centers and field sites through telemetry technologies such as telephone lines, cables, optical fibers, radio frequencies such as radio, microwave and satellite.

The original ICS has little similarity to traditional information technology (IT) systems because ICS was a stand-alone system that used proprietary hardware and software to run proprietary control protocols. Now widespread employment of low-cost Internet Protocol (IP) devices is replacing proprietary solutions, increasing the likelihood of cyber security vulnerabilities and accidents. Because ICS employs IT solutions to enhance the connectivity and remote access capabilities of enterprise business systems and is designed to use industry-standard computers, operating systems (OSs), and networking protocols, they have begun to resemble IT systems. This integration supports new IT capabilities, but it offers significantly less isolation for ICS than the original system, creating additional security needs.

2.2 Attack Model

Next, let us take Stuxnet as an example to analyze the attack entry point of SCADA system, namely attack surface.

Based on an in-depth analysis of Stuxnet^[2], we found that Stuxnet has at least seven paths of propagation, rather than the general belief that it is propagated through only USB sticks (Figure 2).

We can see that the attack points include modems, print/copy/fax machines, package vendors, infected office network, unauthorized connections, infected laptops/PCs and so on. In other words, SCADA systems in industrial systems face a very large attack

surface, not just a single point of defense can hold (Figure 3).

Therefore, we need to learn from the defense strategy described in "Control Systems Cyber Security: Defense in Depth Strategies" released by Idaho National Laboratory, from the United States.

3 Defense in depth model

Prior to obtaining other effective protection methods, defense-in-depth model^[3] is the most effective SCADA system security measures.

3.1. Traditional defense in depth model

The traditional defense in depth model^[3] is illustrated in Figure 4. According to the theory of defense-in-depth, the defense measures were grouped according to their objective into 7 categories. They are: Data, Application, Host, Internal Network, Perimeter, Physical, and Management (policies, procedures, awareness).

Fig. 2. The Attack paths of stuxnet.

Fig. 3. Possible attack entry points.

However, in SCADA system, the goal is different. For the most important thing in SCADA is the production process rather than data. As a result, we propose an architecture of defense in depth specially for SCADA system.

Fig. 4. Traditional defense in depth model.

3.2. Defense in depth model suitable for SCADA

The most essential difference between industrial control systems and IT systems lies in: in terms of system characteristics, industrial control systems belong to the cyber-physical integration system. The logic implementation of ICS directly affects the physical world. While the IT system usually only belongs to cyber system, and information only spreads in the cyber space. Other difference are shown in Table 1 in detail.

Table 1. Difference between IT system and SCADA system.

Items	IT System	SCADA System
Security Priority	Security Priority	Availability, Integrity, Confidentiality;
System real-time Requirements	Real-time system requirements are not high, allowing information transmission	System transmission, dealing with real-time information requirements, cannot stop and restart.

	delay, can be shut down and restart.	
Processing capacity	Requiring high throughput, high latency and jitter is acceptable.	Moderate throughput is acceptable, high latency or jitter is unacceptable
Protocols	TCP / IP protocol stack (application layer protocol: HTTP, FTP, SMTP, etc.)	Proprietary communication protocols (OPC, Modbus, DNP3, etc.), being used directly or as an application layer of the TCP / IP protocol
Operating System	Common operating system (window, UNIX, Linux, etc.), whose function is relatively powerful.	Extensive use of embedded operating systems VxWorks, uCLinux, WinCE, etc., and may have functional reduction or customization based on actual need.
Component lifetime	3-5 years;	15-20 years
Software Upgrade	Universal system, better compatibility, easier hardware and software upgrades, and more frequent software system upgrades	Proprietary system whose compatibility is poor, hardware and software upgrades are difficult, generally rarely upgrade the system
System fault response	Unforeseen interruptions can cause loss of mission, and system failure response levels depend on IT system requirements	Unforeseen interruptions can result in economic loss or disaster and failures must be handled urgently

The most important thing in industrial control system is not the confidentiality of data, but the production process is not tampered with. In combination with Purdue ICS model, we construct a defense-in-depth model suitable for SCADA system. Defense-in-depth model is divided into five layers: physical protection, perimeter security, intranet, control system, production process

Of course, we also need to formulate safety protection strategies, enhance staff training and raise the security awareness of all employees.

4 Implementation

The most important thing in industrial control system is not the confidentiality of data, but the production process is not tampered with. In combination with

Purdue ICS model, we construct a defense-in-depth model suitable for SCADA system. Defense-in-depth model is divided into five layers: physical protection, perimeter security, intranet, control system, production process. Of course, we also need to formulate safety protection strategies, enhance staff training and raise the security awareness of all employees^[5].

The establishment of defense in depth. The meaning of defense in depth is to provide a deeper level of protection on the basis of layer defense and increase network security. It creates a multi-layered barrier between attackers and the enterprise's information resources, and the deeper they want to penetrate the system, the more difficulty attackers will face. These barriers prevent attackers from attacking important resources of the system and also prevent attackers from reconnaissance of the network system. In addition, defense-in-depth strategies provide a natural area for the implementation of intrusion detection systems (IDSs).

To achieve defense in depth strategy, industrial control network need an overall architecture design. The first is the design of the security zone, such as remote access zone, local operating zone, automation equipment zone, and so on (Figure 5). Then the design of security mechanisms within the zone, such as authentication, intrusion detection, incidents response and so on. Next, the design of security mechanisms, including logging and event management, for example using SIEM technology for centralized management of logs and events. Finally, redundant design. Redundancy technology also plays an important role in defense-in-depth strategy, enabling industrial control network in the event of an information security incident to recover in time, such as the firewall hot standby. After the overall design, a variety of security measures such as firewall and intrusion detection are deployed in the industrial control network to form the overall protection capability.

Fig. 5. Defense in Depth Implementation.

According to Purdue industrial control system reference model, the industrial control network can be

divided into different security zones. The external network is divided into a security zone, called the external zone; the enterprise layer is divided into a security zone, called the corporate zone; the control center is divided into a single zone, called the control zone, the field production process is divided into field zone. According to the division of the above security zones, the industrial defense network architecture is designed to control the network defense and the firewalls and intrusion detection devices are deployed at the boundaries of the security zones. In the corporate zone, an enterprise-class firewall with DMZ is used to protect the entire enterprise from security threats from external networks. In the control zone, an industrial control-level firewall with DMZ is used to protect the entire control system.

5 Evaluation

Next, we utilize simulated attacks to verify the proposed defense in depth model.

(1) System penetration. If we utilize the defense in depth model, we can find that, the attacker can only gain access to the external but cannot get connected with the internal network.

(2) Data tampering. In the past, it was possible to communicate directly with the control equipment in a SCADA system and tamper with the data packets, causing a system failure. Now after setting the DMZ between different zones, attackers cannot directly tamper with the packet.

In summary, the use of defense-in-depth techniques can increase the challenge and difficulty of an attack and thus protect the production process. Moreover, defenders can discover attacks in time and take the necessary security measures.

6 Conclusion

This paper analyzes the SCADA system architecture and its characteristics, and builds and analyzes the attack model. According to the original defense-in-depth model, an improved five-layer defense architecture is proposed and simulated using multiple attacks. Experiments show that the defense-in-depth model we proposed can increase the attack difficulties and effectively resist attacks such as system infiltration and data tampering.

7 Future network

Future research mainly focuses on the following aspects:

1. A quantitative model of the defense-in-depth architecture. In order to assess the effectiveness of the defense-in-depth system, we will utilize the establishment of a variety of quantitative indicators to analyze the attackers' capacity and system security.

2. Using SCADA system model, combined with SCADA system control features to find the key nodes, to achieve the reasonable allocation of limited resources.

3. Construction an extended kill chain that is suitable for industrial control system.

Acknowledgements

We thank our shepherds—Zhen Xu, Liming Wang in our research group, for providing insightful feedback of the draft that helped improve the final paper. We would also like to thank Kai Chen, Zelong Chen and Zhenbo Yan for their help in early discussions and providing insightful comments. This work was supported by Software Defined Networking (Sdn) Scale Testing and Validation for Multiservice Convergence Program, Institute of Information Engineering, Chinese Academy of Sciences, under grant No. 2015AA016106, for which we are grateful.

References

1. CIM Reference Model Committee. Purdue University. A reference model of computer integrated manufacturing from the viewpoint of industrial automation[J]. *Int J Computer integrated manufacturing*, 1989, 2(2): 114-127.
2. Byres E, Ginter A, Langill J. How Stuxnet spreads—A study of infection paths in best practice systems[J]. *Tofino Security*, white paper, 2011.
3. Kuipers D, Fabro M. Control systems cyber security: Defense in depth strategies[R]. Idaho National Laboratory (INL), 2006.
4. Stouffer K, Falco J, Kent K. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security[J]. NIST Special Publication SP800-82 (draft), USA, 2006..
5. Knapp E D, Langill J T. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems[M]. Syngress, 2014.