APT Attack Analysis in SCADA Systems

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

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

Abstract. SCADA (Supervisory Control and Data Acquisition) systems play a significant role in ICS (Industrial Control System). Safety, security and stable operation is crucial to the SCADA system. However, SCADA system currently faces many security threats, of which the most harmful is the APT attack. This paper analyzes the attack surface and its own vulnerabilities of SCADA system, and analyzes the characteristics of APT attack comprehensively. Then the paper dissects the cases of real APT attack thoroughly and gives measures of SCADA security protection.

1 Introduction

With the continuous integration of industrialization and informationization, more and more information technologies have infiltrated into the industrial production environment, which have greatly enhanced the efficiency of industrial production and reduced the cost of cables for communications. However, while enjoying the convenience brought by information technology, it has also introduced the security issues that have never before been encountered in the industrial field.

The "isolated island of information" in the original industrial production no longer exists and more and more systems are integrated into one large system. Coupled with the growing knowledge of attackers for industrial processes, industrial control systems are also becoming one of the targets of attacks by attackers. Iran's Natanz nuclear power plant suffered Stuxnet^[1] virus attacks in 2010, breaking the myth of absolute security of closed and isolated system, causing about one-fifth of centrifuges in nuclear power plants to be scrapped, greatly postponing Iran's nuclear program. Much like Stuxnet, the duqu Trojans^[2] appeared in 2011. The Duqu attack targets mainly industrial control systems to steal private information. In 2014, Finnish information security vendor F-secure exposed Havex^[3], a malicious software designed specifically for ICS / SCADA systems. It has the ability to disable hydroelectric dams and overload nuclear power plants. Some hackers have used it to attack European and American energy industries Industrial control system. On 23 December 2015, the Ukrainian power sector was attacked by malicious code^[4]. The Ukrainian news media TSN reported on the 24th: "At least three power zones were attacked and caused several hours at around 15:00 local time blackouts "; attackers invaded the surveillance

management system, and more than half of the area and a few hours after the Ivano-Frankivsk area was powered down".

To sum up, the SCADA system has become more complex and increasingly an important target for attacks. The technology used by attackers are becoming increasingly sophisticated, and attacks evolve toward APT.

The paper structure is as follows: Section 2 depicts the architecture of SCADA system and its vulnerabilities. After presenting APT technological features in detail in Section 3, we analyze APT attack cases in Section 4. SCADA Network Security defense measures are given in Section 5. We make our conclusion in Section 6, and give a discussion of our work in Section 7. Finally, we make acknowledgements in Section 8.

2 SCADA system model 7

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

2.1. SCADA system structure

A typical industrial network^[5] shown in Figure 1:

* Corresponding author: author@e-mail.org

Fig. 1. The architecture of SCADA system.

The industrial control system includes four main components: business network, monitoring network, control system and field system. The business network includes business services such as web server and mail server. The monitoring network mainly includes Supervisory Control and Data Acquisition (SCADA) systems, history records and historical databases. The control system mainly includes Human Machine Interface (HMI), Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED), etc. The HMI is an operation control panel of PLC / RTU / IED. Its function is to provide operators / engineers with a view of real-time on-site system status. Field system is the bottom of the entire industrial control system, mainly used to execute the control commands issued by the operating system, including the implementation of the main equipment PLC / RTU / IED. Moreover, PLCs are often used in industrial control systems as an alternative to RTUs and IEDs.

2.2 Attack surface analysis

That one system is isolated or closed does not mean there is no information security risks, not to mention that it is impossible to be completely isolated. Even if the industrial system is closed, Wi-fi, USB and other means can still provide a lot of points of entry, a USB device equipped with a wifi-modem can even provide available access to public network. And most industrial systems generally do not have the corresponding account and password management measures, where administrator account is left public, account permissions are not assigned properly, the account is not deleted in time after the expired, the password is weak and remains unchanged or too simple and so on. This provides a convenient door for intrusion. Relevant statistics show that only 20% of data breaches are done by outsiders, while 80% are from inside, including operational errors, vandalism and lack of knowledge.

Attack surface is a collection of software system vulnerabilities that can be exploited. The more attack surface a system has, the lower the security. Taking the

smart grid SCADA system as an example, radiation from the central power generation equipment to the smart grid terminal node shows an exponential growth in the attack surface^[5]. As shown in Figure 2.

Business networks generally provide information to policy-makers and are also the easiest to attack as business networks are inevitably connected to the Internet. Moreover, business networks generally provide many services, which increase the attack surface.

Monitoring networks, as a bridge between business networks and control systems, are vital to their safety. If the business network is compromised by the attacker, then the monitoring network can not be spared. Moreover, the fragility of the monitoring network itself includes weak passwords in historical databases, weak firewall rules, unmanaged assets, and more.

The control system directly controls the field devices and, if compromised, can often cause serious physical damage or even loss of life. The attack surface generally includes insecure protocols, unsafe wireless transmissions, weak firewall rules, unencrypted data transmission, and more. The attack entry points^[6] are shown in Figure 3.

Fig. 2. The attack surface of smart grid.

Fig. 3. The attack entry point of SCADA system.

3 APT technical analysis

In this chapter, we will take a deep analysis

3.1. Attack technology features

(1) Attack Form

APT has evolved from viruses, trojans and worms to combinations that combine multiple traits. It is not a mere virus but a collection of viruses. Moreover, APT leverages a large number of known or unknown system vulnerabilities in order to achieve code execution or elevation of privilege.

(2) Attack Mode

APT attacks use a variety of attack methods to penetrate and analyze targets, especially in large applications of social engineering. Through extensive collection of information such as social relations, hobbies, and internet habits of target people, a full set of well-designed websites are set up to entice target people to visit malicious sites and download programs or files with attack codes so as to infiltrate and utilize attack codes.

(3) Attack Object

The goal of APT attacks is primarily the country's critical infrastructure, designed to create chaos, achieve political intent, and even be used in cyberwarfare. The purpose of APT is strong, which is a threat to the security of key infrastructure and even the whole country.

3.2 APT attack technical complexity

(1) The technical means used are complicated

APT uses more 0day vulnerabilities to attack and continuously expands in the attack depth. The communication content is continuously monitored and has a long latency period. More and more social engineering tools are used in propagation.

(2) Multi-domain cross-collaboration

APT employs many fields of knowledge, such as psychology, social engineering, computer science, game theory and other fields. APT is no longer confined to the field of computer information, but a complex system that integrates multiple disciplines.

(3) Less cases can be referred to

APT attacks are not only changeable, but also make more use of 0day vulnerability. General APT attacks will only be used once, and will develop new attack tools in the next attack. Moreover, the number of APT attacks is relatively small. To make things worse is that APT samples are difficult to collect.

4 APT attack cases analysis

Below we have a detailed analysis of three typical SCADA system attacks, trying to find out their commonality, so as to take the appropriate safety precautions.

4.1. Stuxnet

Stuxnet, which is a complicated worm specially designed to infect Siemens SIMATIC WinCC and S7 PLC products. Its target is S7 series PLCs. The Stuxnet worm (the super-factory virus) is the world's first destructive

virus written specifically for industrial control systems to exploit seven vulnerabilities in the windows system and the Siemens SIMATIC WinCC system. Especially for SIMATIC WinCC monitoring and data acquisition (SCADA) system against Siemens, the system is widely used in many important industries in our country to be used for human-computer interaction in important industries such as steel, power, energy and chemical industry with monitoring. Route of transmission: The virus is mainly spread through U disk and LAN.

Stuxnet is by far the most sophisticated threat not only because it leverages the "fun" anti-virus circumvention technology and sophisticated process injection code, but also exploits the latest vulnerabilities in virus design including utilizing four separate zero-day vulnerabilities. And the first ever rootkit ever to target a programmable controller system. Figure 4 depicts the spreading process of Stuxnet^[7].

Fig. 4. Stuxnet attack Graph.

4.2 Havex

Havex is considered a malware targeted for different industry sectors and in the initial report the malware was of particular interest to the energy industry. An attacker first infected the Trojan with the software used by the ICS /SCADA manufacturer's website for download by the user, enabling the user to be infected when the user downloads the software and installs it. With a large sample analysis, we found that attackers can take advantage of one of these components to steal data from a machine used in an ICS / SCADA system. This means that attackers are not only interested in the target company's network, but also motivated to control the ICS / SCADA systems of these companies.

Havex RAT spread through the following channels:

- (1) Spam
- (2) Exploit tools
- (3) The software installation package that is provided to the user on the main website of the compromised manufacturer contains the Trojan.

Fig. 5. Havex attack route.

4.3. Flame

Flame virus was first discovered by Kaspersky in May 2012. Its structure is very complex and harmful. It can be spread in many ways through USB storage and network copy and can accept Commands from multiple servers around the world, making it one of the most complex and dangerous viruses in the world. The Flame virus is not only smarter than the Stuxnet virus that attacked the Iranian nuclear program's computer system, but also made a big difference in attack targets and code composition. Flame viruses have a more sophisticated attack mechanism and target specific geographic locations, which may indicate that the Flame virus's behind-the-scenes team is likely to be manipulated by government agencies. The earliest possible occurrence of the Flame virus dates back to 2007, and it is speculated that the attacker may be released (attacking business intelligence of the Iranian oil sector) in March 2010 but

due to its structural complexity and selective targeting, anti-virus software has not found it.

Once infected with the Flame virus and activating the component, it collects information using all possible conditions, including keyboards, screens, microphones, removable storage, networking, WIFI, Bluetooth, USB and system processes, communication calls, account passwords and even keyboard input records, or even use Bluetooth to steal the infected computer connected to the smart phone, tablet PC files sent to the remote control of the virus server. In addition, even if the connection with the server is cut off, attackers can still close the infected computer with Bluetooth signals. From a functional point of view the virus is very powerful, you can call it "super thief", covering all the user input and output of the computer interface.

Fig. 6. Flame spread route.

5 SCADA network security defense measures

In this chapter, we will discuss SCADA network security defense measures.

5.1. Industrial firewall

Industrial firewalls designed specifically for SCADA systems can identify industrial control protocols.

5.2 Anomaly detection

Build a normal model for the entire SCADA system and establish baselines, abnormal traffic in a timely manner, and anomalous behavior.

5.3. Full flow audit

Audit traffic in the SCADA system and discover unknown threats based on traffic information.

Of course, there are other methods of protection, such as whitelisting based mechanisms, sandbox detection mechanisms, and more. However, it is still under exploration and there is no very effective method of security protection.

6 Conclusion

Through in-depth analysis of SCADA system, combined with the actual APT attack cases, we find that the attack surface of SCADA system is broader than that of common IT system, and that SCADA system has more vulnerabilities. Moreover, the APT attack faced is also more complicated, more advanced and more difficult to defend. However, the current security measures is not very effective and far from satisfactory. We need to develop a comprehensive security program, combining the SCADA system's own characteristics, and against the techniques of APT attacks, to create a targeted defensive measures, rather than copying the defense means of traditional IT systems^[8].

7 Discussion and future network

This paper first introduces the structure of SCADA system, analyzes its vulnerability, and gives the attack surface of SCADA system. Then it analyzes the technical characteristics of APT attack, and then analyzes the attack process of APT with the real case. Finally, it gives the security measures of APT attack. Through the analysis we found that APT attacks are more complicated security threats, which take more manpower and resources to defend.

Future work we will focus on the following research directions:

(1). Behavior-based anomaly detection model construction. Through the machine learning method, a normal behavior model is constructed from multiple dimensions, including the normal behavior model of historical, peer and communication partners, so that the abnormal behavior in the SCADA system can be found accurately and efficiently.

(2). To establish a suitable depth of defense system^[9] for industrial control system. According to the characteristics of industrial control system, the depth defense system will be improved so that it can be better applied to the security of industrial control systems.

(3). Establish a kill-chain model specially for industrial security. The current kill chain model is rough, ignoring a lot of details of attack. We intend to create a

kill chain model that is specific to industrial control systems.

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 Research on Core Technologies of national key infrastructure security supervision platform. Beijing Municipal Science & Technology Commission of China under grant No.Z161100002616032, for which we are grateful.

References

1. Langner R. Stuxnet: Dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.
2. Bencsáth B, Pék G, Buttyán L, et al. Duqu: A Stuxnet-like malware found in the wild[J]. CrySyS Lab Technical Report, 2011, 14: 1-60.
3. HENTUNEN D T. A: Havex Hunts for ICS/SCADA Systems [on-line][J]. 2014.
4. Case D U. Analysis of the cyber attack on the Ukrainian power grid[J]. Electricity Information Sharing and Analysis Center (E-ISAC), 2016..
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.
6. Fielder A, Li T, Hankin C. Defense-in-depth vs. critical component defense for industrial control systems [J]. 2016.
7. Byres E, Ginter A, Langill J. How Stuxnet spreads—A study of infection paths in best practice systems[J]. Tofino Security, white paper, 2011.
8. Ness J. Flame malware collision attack explained[R]. Tech. Rep., Jun. 2012.[Online]. Available: <http://blogs.technet.com/b/srd/archive/2012/06/06/more-informationabout-the-digital-certificates-used-to-sign-the-flame-malware.aspx>, 2012.
9. Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security[J]. NIST special publication, 2011, 800(82): 16-16.
10. Kuipers D, Fabro M. Control systems cyber security: Defense in depth strategies[R]. Idaho National Laboratory (INL), 2006.