Kill Chain for Industrial Control System

Xiaojun Zhou[1,2], Zhen Xu[1], Liming Wang[1], Kai Chen[1], Cong Chen[1,2], Wei Zhang[1,2]

[1]State Key Laboratory of Information Security, Institute of Information Engineering,Chinese Academy of Sciences, 100195 E-park C1 Norh, 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. Attacks in industrial control systems vary widely and are influenced by many factors, including the intent of the attacker, the capabilities of the attacker, the sophistication of the attacking techniques, and his familiarity with the industrial control systems and industrial processes. Attacks against industrial control systems are not a simple network intrusion, but are accomplished through a series of activities to achieve precise attack. This article expands the cyber kill chain model to improve it so that it can be applied to industrial control systems to ensure that defenders in industrial control can understand the attackers' attack activities so as to reasonably allocate limited security resources, take effective security measures and make well-informed risk management decision.

1 Introduction

With the deepening of the integration of industrialization and informationization, the links between the industrial field control, on-site production process and decision-making management are getting closer to the Internet. The industrial control system was originally closed but now the isolated environment was broken. Viruses, Trojans, hackers, etc. , which are the security threats of traditional Internet, are increasingly spreading to the field of industrial control. The security of industrial control systems has become increasingly prominent. Industrial control systems are widely used in industries and fields related to national economy and the people's livelihood such as chemical industry, energy, transportation and municipal administration. They have become an important part of the country's critical infrastructure. Once attacked, the industrial control system will likely paralyze industrial production and cause huge economic losses, even causing environmental disasters and casualties, endangering the public's normal life and national security.

Researchers have made a great deal of in-depth study on the security of industrial control systems. The security of industrial control systems has been improved to a certain extent. And governments of various countries have also released security protection guidelines for industrial control systems. However, it is now mainly based on isolated industrial security precautions that it is difficult to effectively deal with the new security issues brought about by the rapid development of industrial control systems.

This paper starts with the intrusion campaign of attackers, deeply analyzes the difference between the attacker's invasion of industrial control system and the traditional IT system, and expands and improves the traditional kill chain model so that it can meet the special attributes of industrial control system. The structure of the article is as follows: In Chapter 2, the difference between industrial control system and traditional IT system is analyzed in combination with Purdue reference model, and the security risk of industrial control system is pointed out. Chapter 3 first introduces the traditional kill chain model and then analyzes its deficiencies. Chapter 4 presents a kill chain model for industrial control systems, including an external kill chain, an internal kill chain, and an industrial kill chain. Chapter 5 analyzes the proposed kill chain based on the actual attack cases (Havex). The 6th Chapter gives the discussion and 7th chapter gives the future research work. Finally, we make our acknowledgement in chapter 8.

2 Introduction of ICS system

In this chapter, we will give a brief introduction of ICS system.

2.1. ICS model

* Corresponding author: author@e-mail.org

The following is a Purdue Reference Model[1] to illustrate the architecture of industrial control system.

Fig. 1. The Purdue Reference model of ICS.

As can be seen from the figure, the industrial control system mainly includes five layers. The bottom three layers successively are the process layer, the basic control layer, and area control layer, all these three layers constitute the Cell/Area Zone. Level 3 is the Manufacturing Zone that is primarily responsible for the operations and control of the manufacturing process. Following is DMZ, where some security equipment is placed. The top two layers are the enterprise network and the site-business planning and logistics network that the two together make up the Enterprise Zone. Level 3 and below are composed of on-site control equipment, including HMI (human machine interface), PLC (programmable logic controller), RTU (remote terminal unit), IED (intelligent electronic devices) and so on. Above level 3 generally utilizes the traditional PC (personal computer), and usually connected with the Internet.

2.2. Difference between traditional IT system and ICS

Due to their different construction goals, industrial control systems and traditional IT systems still have considerable differences in terms of technology, management and service[6]. Some typical differences are shown in the Table 1.

Table 1. Difference between traditional IT system and ICS

Item	IT System	ICS
operating system	Common Operating System (window, UNIX, linux, etc.), the function is relatively powerful.	Extensive use of embedded operating systems such as VxWorks, uCLinux, WinCE, etc., and may have functional reduction or customization based on the actual industrial need
Data exchange protocol	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
Real-time requirements	Low real-time system requirements , allowing information transmission delay, accept shut down and restart.	High real-time requirements on system transmission and dealing with information, must not stop and restart.
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
System upgrade difficulty	Universal system, good compatibility, easier hardware and software upgrades, and more frequent software system upgrades	Proprietary system, poor compatibility, hardware and software upgrades are difficult, generally rarely upgrade the system, may need to upgrade the entire system when it has to.

3 Traditional Kill Chain

In this chapter, we will analyze the traditional Kill Chain [4] and point out its shortbacks when being used in industrial control system.

3.1. Introduction of Cyber Kill Chain

Kill chain was originally derived from K (kill) in the military C5KISR system. Then Lockheed-Martin proposed a seven-step cyber-security chain model[2]. The attack chain divides one attack into seven stages, which can quickly help us understand how to effectively defend against an attack, as shown in the following figure.

First, the reconnaissance stage. The reconnaissance phase is the process by which an attacker attempts to detect, identify and determine the target in order to achieve the goal. At this stage, various target-related intelligences such as corporate / institutional websites, press releases, public notices of tenders, social media networks for staff, and membership lists can be collected online.

Second, the weaponization phase. Weaponization phase refers to the preparation of network weapons after the phase of reconnaissance has determined the target. Networked weapons can be created directly by attackers or made byusing automated tools.

Third, the delivery stage. The delivery stage refers to delivering the created network weapons to the target. According to Lockheed Martin Network Security Assurance Team, the most frequently used means of delivery between 2004 and 2010 are email attachment, websites, USB (Universal Serial Bus) and so on.

Fourth, the exploitation phase. Exploitation phase is to initiate the malicious code after the delivery phase. In most cases, applications and operating system vulnerabilities and defects are often being exploited.

Fifth, the installation stage. Installation stage refers to the attacker setting Trojan horse, back door in the target system, to create an active environment within a certain period of time.

Sixth, command and control stage. This stage refers to the attacker to establish attack path in the target system. In most cases, a cyberattack is not a purely automated attack, but rather an attacker involved campaign. Once the attack path is established, attackers will be able to freely access the target system.

Seventh, Actions on Objective. This stage refers to the attacker to achieve the desired attack goal. The targets of attack are diversified, so the attack goals vary: scouting, gathering sensitive information, destroying the integrity of data, destroying systems and so on.

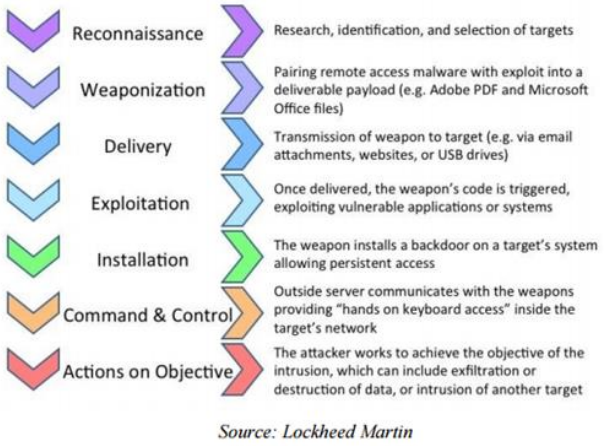

Fig. 2. The whole steps of Cyber Kill Chain.

3.2. The drawbacks of traditional Kill Chain

The traditional kill chain has played a role in security defense, but its disadvantages are also obvious[5]:

(1) Leading defenders to focus on perimeter-based security;

(2) It doesn't work well for insider threats;

(3) At present, every cyber attacker can be potential considered as insider.

4 Kill Chain for industrial control system

We extend and improve the traditional kill chain model, making it suitable for industrial control systems, including three kill chain, including external kill chain, internal kill chain and ICS kill chain.

The relationship of the three kill chain is illustrated in Figure 3.

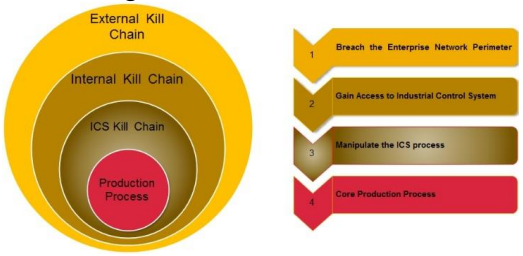

Fig. 3. The telationship of the three-layer Kill Chain.

External kill chain is used to invade the corporate network, the internal kill chain is used to gain access to industrial control systems and ICS kill chain is used to implement the final attack of a specialized production process.

Let's discuss these three kill chain in detail, as shown in Figure 4.

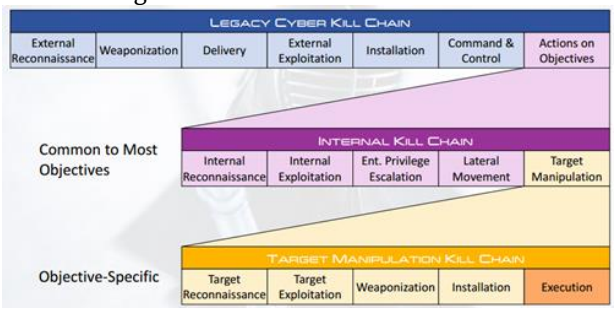

Fig. 4. Three-layer Kill Chain in detail

Specifically, the external kill chain is the original kill chain, but we have extended it.

Internal kill chain includes 5 steps, introduced as follows:

(1) Internal Reconnaissance. Get intranet-related intelligence information and vulnerability information.

(2) Internal Exploitation. Exploit information and vulnerabilities within the intranet system.

(3) Internal Privilege Escalation. Leverage the compromised intranet account and trusted certificate, to gain a high level of privilege.

(4) Lateral Movement. Access to the restricted area of the compromised system.

(5) Target Manipulation. Attack against specific objectives.

Among them, the last step of the internal kill chain is the ICS kill chain, including the following five steps:

(1) ICS Reconnaissance. Identify specific industrial control systems and control software.

(2) ICS Exploitation. Exploit-specific vulnerability information of the target ICS.

(3) ICS Weaponization. Develop specific attack tools based on ICS-specific vulnerability information.

(4) ICS installation. Install well-developed tools such as malware or Trojans into the target ICS.

(5) Execution. Launch attack on a specific production process.

5 Analysis of Havex

Havex malware[5] is used to gather ICS sensitive data and network infrastructure information from thousands of industrial control systems. It is a remote trojan used for general purpose espionage. According to publicly available information, Havex has been lurking in industrial control systems for many years. Havex uses a variety of ways to intrude industrial control systems, three commonly used methods are listed below:

(1) by phishing mail, attachments are malicious files;

(2) Employment of malware to infect the ICS provider's website, and intervene in ICS when an operator visits the infected website.

(3) Providing trojanized version of ICS software installers, invade ICS when operators download or install infected ICS software.

Havex malware is used to gather ICS sensitive data and network infrastructure information from thousands of industrial control systems. It is a remote trojan used for general purpose espionage. According to publicly available information, Havex has been lurking in industrial control systems for many years. Havex uses a variety of ways to intrude industrial control systems, three commonly used methods are listed below:

(1) by phishing mail, attachments are malicious files;

(2) use of malware to infect the ICS provider's website, and take the opportunity to invade ICS when an operator visits an infected website.

(3) To provide ICS software with Trojan malware, operators need to download or install infected IPC software.

The first method of intrusion, by phishing mail. The attacker first implemented an external kill chain. The attackers conduct reconnaissance to determine the target of the attack and tailor the phishing email to determine who will receive the phishing email. Then weaponization is the phishing mail attachment file. Mail itself is a delivery mechanism, and when a victim opens the mail attachment, it begins to exploit the system and install Havex malware. Next, Havex tries to communicate with the C2 server. Then, the attacker implements the internal kill chain. Havex scans the entire system to find specific ICS components, identify vulnerabilities of the component, elevate his privileges, and send the collected information to the C2 server. If Havex is going to attack production process, it is ICS KILL CHAIN.

The second method of intrusion, by infecting the vendors' website. In particular, we should note that infected vendors' sites is a kill chain, it belongs to the external kill chain. Once the operator has visited the infected website, the attacker begins to implement the internal kill chain. The internal kill chain needs firstly reconnaissance to determine which vendor's website may be probably visited. At this point, the vendor's website itself is weaponization. As long as the ICS through the supplier's site, other steps will be the same as the first intrusion method.

The third method of intrusion, through the Trojan infected ICS software. reconnaissance includes determining which ICs are generally used by ICS and the software itself is weaponization. Then the next steps are of the same with the first intrusion method.

Through the analysis we found that the improved kill chain model is suitable for analysis of APT attacks such as Havex, and can effectively help defenders to be aware of attackers' campaign and the attack route.

6 Conclusion

In this paper, the traditional kill chain has been extended and improved. It proposes three levels of kill chain, including external kill chain, internal kill chain and ICS kill chain. Moreover, combined with the real Havex attacks, analysis of the three kill chain is performed. After analysis, we found that the improved kill chain can well model the attacks in industrial control systems, so that defenders can understand attackers' steps and attack paths and take timely measures.

7 Future network

Future work and research directions are as follows:

1). Kill Chain quantification. We will establish a quantitative kill chain model to quantify and analyze attacker's steps.

2). A quantitative description of the defense in depth system[6]. Establishing a quantitative analysis model for defense in depth in industrial control systems enables better allocation of limited security resources.

3). Quantitative analysis of the key nodes. We will utilize quantitative analysis to find the key nodes that need to be focused of protection.

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. Hutchins E M, Cloppert M J, Amin R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare & Security Research, 2011, 1(1): 80.
3. Langner R. To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve[J]. Online: http://www. langner. com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge. pdf, 2013.
4. HENTUNEN D T. A: Havex Hunts for ICS/SCADA Systems [on-line][J]. 2014.
5. Assante M J, Lee R M. The industrial control system cyber kill chain[J]. SANS Institute InfoSec Reading Room, 2015, 1.
6. Kuipers D, Fabro M. Control systems cyber security: Defense in depth strategies[R]. Idaho National Laboratory (INL), 2006.