Endpoint Security for Industrial Control System

Hiroshi Itakura [*1] *Toshihiro Hatakeyama* [*1]
Kentaro Hayashi [*1] *Kumiko Takayashiki* [*1]

In the office automation environment, security measures are implemented, as a matter of course, in endpoints such as PC servers and terminal devices. However, many human machine interface (HMI) terminals and server systems in industrial control systems are left without any security measures. Since 2010, many incidents have been reported in which malware (malicious software, a kind of computer virus) invades and proliferates inside control systems, and then makes HMI terminals inoperable, leading to plant shutdowns. Many such incidents could have been prevented if security measures had been implemented at proper endpoints.

In this paper, security measures for endpoints including HMI terminals and PC servers are shown as a comprehensive security measure for control systems.

INTRODUCTION

According to a survey by a security software vendor, more than 80 million pieces of malware (malicious software, a kind of computer virus) were made in a single year, 2013. This means that more than two viruses are created every second. The number of new malware was of the order of one million until around 2007, but since then it has been rapidly increasing. In particular, many security incidents in control systems caused by malware infection occurred between 2010 and 2012. Recently, its occurrence has been slightly decreasing owing to improvement of user awareness for security. However, security incidents are still being reported, and users and vendors need to repeat investigation and recovery actions for every incident. On the basis of the experience in responding to major security incidents in 2009 and 2010, Yokogawa launched the endpoint security service (EPS) mainly for the CENTUM integrated production control system as a preventive security solution, immediately producing effective results. Since then, Yokogawa has been adding EPS measures and expanding their coverage to offer multiple solutions. This paper outlines the features and technologies of the EPS.

BACKGROUND AND ROUTES OF MALWARE INFECTION

Figure 1 shows security risks in control systems.

When the control system is infected with malware, many of the causes are removable media such as USB storage devices. They are often used during routine work on a daily basis to collect trend data or Excel worksheets from terminal devices.

*1 Business Planning & Development Dept., Global Service Center, Solution Service Business Headquarters

USB storage devices are inexpensive, easy-to-use, and convenient for copying and moving data files. However, some recent malware spreads via such removable media. Without their proper management, they can be malware carriers. These days, managing and limiting the use of USB storage devices is increasing and the controlling effect of the incidents is recognized. There are still many other devices that require attention.

One example is a smartphone. Batteries of smartphones are sometimes charged via USB ports of the terminals in control systems such as HMI because of its convenience. The connected smartphone is recognized as a memory device such as a USB storage devices. Therefore, if it is contaminated with malware, it may intrude into the control system. Yokogawa's survey found that one HMI had been connected with multiple smartphones. Careless connection of smartphones with PCs in control systems must be avoided, even only for battery charging.

If the network of a control system is not completely closed, infection through networks must be paid attention to. These days, plural control systems are connected to upper networks such as for OA or production management. Usually, communication traffic is restricted to only the necessary ones through gateways or firewalls at each connection point. However, if the setting for the restriction is not proper, control systems cannot be protected against infection from upper networks, and it may even cause the provision of an entrance for malware to intrude into control systems. In addition, if any other network domain is infected with malware, the damage may spread.

ENDPOINT SECURITY MEASURES

Considering the situation described above, Yokogawa has enhanced EPS measures for HMI terminals and servers in control systems since 2010.

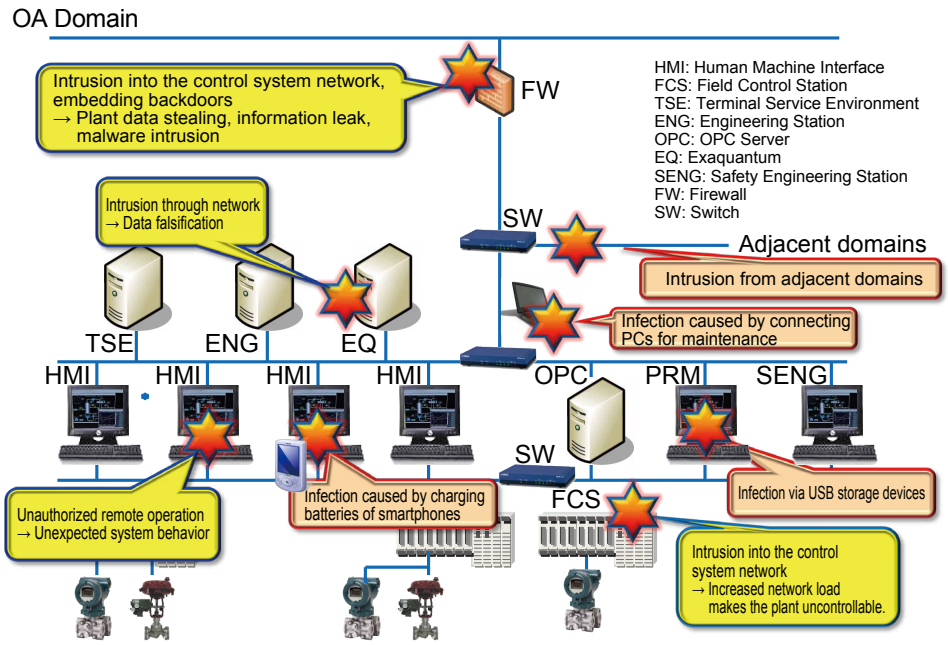

Figure 1 Security risks in control systems

The same set of measures cannot satisfy all needs in actual systems. This is because operating systems (OS), installed application software and system operation differ from system to system, and advanced security policies are applied in some user environments. Meanwhile, Yokogawa's EPS is effective for any needs by preparing multiple measures and applying them solely or comprehensively. Major EPS services are described below.

Security Update Programs Implementation Service

Microsoft Corporation releases security update programs (MS patches) every month. They include basic security measures for preventing malware intrusion, suppressing its execution and protecting from cyber-attacks via networks, and thus they are recommended to be timely applied.

However, in the case of control systems, the possibility of applying patches must be confirmed, and the behavior after their application must be verified in advance so that the patches do not affect the system operation. Moreover, because applications of MS patches require reboots, the timing to apply them must be carefully considered, such as between the system operation or during shutdown. Yokogawa is verifying that the applications of MS patches do not affect the system operation at the security competence laboratory (SCL) described later. After the verification, the introduction timings are planned with customers and then service engineers apply the MS patches.

Blacklisting Approach Implementation Service

Anti-virus software [Note 1)] is often installed in OA systems and home PCs as a blacklisting-approach security measure. Meanwhile, measures by this approach for control systems have been practically avoided because there is the possibility of lowering the system performance and affecting their operation. Anti-virus software keeps information on malware to block as blacklists in pattern files (also called signatures). These pattern files need to be kept updated, but most control systems are not connected to the Internet, causing a problem that the update cannot be performed automatically.

The performance degradation is no longer a serious problem thanks to performance improvement in PCs and the establishment of a tuning method not affecting control systems.

In the case where control systems are not connected to the Internet, two methods are available to update the pattern files. One is to manually update the pattern files one by one, and the other is to use a distribution server described below. By considering the possible risks and required costs, the update method will be selected. Yokogawa has provided anti-virus software dedicated for Yokogawa products, taking these performance and automatic update issues into account. This can be installed with best-suited tuning for each control system, and is one of the key software components for providing security measures.

Whitelisting Approach Implementation Service

Control systems need to continuously operate for a long period when they have started up once. Their lifetime is 5 to 10 years, or even longer. In some cases, software support is terminated before the end of its use and satisfactory security measures are no longer available.

For this reason, new technology for a whitelisting approach is attracting attention. In this approach, only

Note 1) In this paper, "malware" is used as a name of software that is made maliciously, and "virus" is expressed as a name used in services and products for security.

programs registered in the list are allowed to run in the system, and other unfavorable programs including malware cannot run. Although this approach makes it difficult to modify the system through introducing new programs or other means, it can maintain the state of the system as it is. This is effective when the system uses an obsolete OS for which MS patches are no longer provided. Control systems seldom require installing new programs after the start up, and their lifetime is long. Therefore, many control system users prefer this approach. In this approach, only programs allowed to run are registered in the whitelist. Some application programs create daughter programs and if the daughter programs are not registered in the list, this causes a problem in the system because they cannot run. Thus, by combining control system products and whitelisting technology, Yokogawa provided whitelisting software dedicated for Yokogawa products. This software can be installed with the parameter tuning best suited for each control system.

The whitelisting approach prevents malware from running but not its infection. If malware has already intruded into a PC, the malware may start running just after the whitelist software is stopped. Therefore, the combination of whitelisting and blacklisting approaches will be more effective and safer. Table 1 compares the blacklisting approach usually used in anti-virus software and the whitelisting approach used in the whitelisting software described above.

Virus Scan Service without Installing Antivirus Software

When some abnormality is observed in a control system and malware infection is suspected to be the cause, there is a case where the cause of the abnormality cannot be identified if no security measures are taken for the system. Thus, Yokogawa offers a means that can perform a virus scan on control systems without installing antivirus software in them. If any malware is found by the scan, the procedure for responding to a security incident described below is applied.

This service is also used for a periodical virus scan during preventive maintenance work for control systems with no anti-virus software installed.

Entire HDD Contents Backup Service

When a PC or a server is infected with malware, its OS settings might be overwritten or its startup files might be deleted depending on the impact of the malware. In such a case, the HDD must be initialized and all the application software and data must be restored. Yokogawa offers dedicated software to back up the entire HDD contents of PCs and servers in control systems preparing for contingencies. This can significantly reduce the time required for recovery from the infection, because the required action for the recovery is only the reloading of the backup data. This is also effective for shortening the recovery time in the case of a PC or server failure. The necessity of the backup has increased from the viewpoint of the business continuity plan (BCP).

MS patches & Pattern Files Distribution Server

The MS patches and the pattern files for anti-virus software, as described above, need to be periodically updated and applied. When many PCs and servers are installed in a system, a distribution server might be added to the system for efficient updates. The distribution server can timely update them according to the planned schedule and manage the update situation of all the PCs and servers. In addition, the server can gather information of malware detected by anti-virus software at each PC and server, and can report it to outside. This enables early detection of infected PCs or servers that are not displayed on the screen.

Table 1 Comparison between blacklisting approach and whitelisting approach

	Blacklisting Approach	Whitelisting Approach
Advantages	· A widely used and effective approach against malware This approach is widely used and very effective. Yokogawa applies this approach as a standard, and is verifying measures based on this approach in its SCL, combining it with its control systems. · Detects and removes malware Detected malware is isolated and removed before it infects, preventing the spread of infection. · Detect malware intrusions When malware is detected, an alarm is issued before it infects, reporting that malware will be isolated and removed.	· Requires no updates while there is no change Periodic maintenance such as updating pattern files is not required. · Effective even for OSs for which support is terminated Attacks on vulnerabilities in the OS are mitigated. · Lighter load compared with the blacklisting approach Periodic scans are not required unlike in the case of anti-virus software. · Effective for unknown threats Because programs not registered in the list are not allowed to run, this approach is effective even for unknown threats.
Notice	· Needs to update pattern files Pattern files supplied by vendors needs to be periodically updated. If they are not applied, new viruses cannot be protected from them.	· High risks when disabled If malware has already intruded into a PC or server, it starts causing problems the moment the whitelist is disabled. Virus scans are indispensable before the whitelist is disabled. · Does not isolate or remove malware Unlike anti-virus software, malware is not isolated or removed. Even its intrusion is not detected. · Requires re-setting on hardware or software update For some system modification work, whitelisting-approach software needs to be disabled prior to the work, and needs to be enabled after updating the whitelist.

FRAMEWORKS TO SUPPORT ENDPOINT SECURITY SERVICES

Operation Validation Environment

Although most measures provided by the EPS are usually applied in a common OA environment, the introduction of these applications has been slow in control systems because of the possibility of system performance degradation or malfunctions. If such concerns are allayed, appropriate applications can be applied to the control systems. For this reason, Yokogawa has set up the security competence laboratory (SCL) shown in Figure 2, and is continuously conducting operation verification on Yokogawa's control system products in combination with MS patches and Yokogawa's dedicated anti-virus software. Yokogawa constructed a system in which EPS can be used with ease for customers after it is confirmed that there are no problems.

Figure 2 Security competence laboratory (SCL)

Responding to Security Incidents

Unlike usual malfunctions, security incidents such as malware infection require users to decide upon a means for preventing the spread of infection and a means for recovery on a case-by-case basis. Therefore, it is essential to study features of malware including its behavior and impact. Especially for network infectious malware, a recovery procedure must be prepared before implementing respective measures, because the spread of infection must be prevented, and simply removing it cannot prevent its reinfection. Yokogawa offers a framework in case of security incidents in which security experts including SCL staff will work closely with on-site operators to achieve a quick recovery.

CONCLUSION

Some users are strengthening security for control systems while most users are unsure about security measures and are still adopting a wait-and-see approach. The malware threat is increasing and quick action is urgently required for preventive maintenance. In particular for companies and organizations that manage critical infrastructures, security measures are indispensable to protect them from cyberterrorism. Security measures must be taken from various viewpoints. Yokogawa's EPS has produced a lot of positive results as a security measures solution with immediate effect, and has contributed to user's safe and secure operation. Yokogawa will advance the strengthening of its services in this area.