Security Technologies for Industrial Control System

Toshiki Hirata

Keywords Application security, Static analysis, Digital signature, Communication restriction, Communication secrecy

Abstract

There are many cases in which industrial control systems are used by connecting with a local network system as such system is mission-critical for society. With the progress of recent cloud-computing technologies, it is expected that industrial control systems need to work with external IT network systems.

When an industrial control system is connected with an external IT system, IT security risks increase. This underscores the importance of having security measures in place for industrial control systems.

The technology covered in this paper is presented as a security technology in order to cope with alterations on control system software and system configurations. Our security measures protect systems from unauthorized use and unintended misuse and it also ensures the completeness of applications in order to configure control system confidentiality during communication.

1 Preface

IT security-related incidents of industrial control systems increase year after year. In the case of the Stuxnet incident in 2010, it attracted the world's attention as a target type of attack against industrial control systems. Due to the development of cloud-computing technologies, there are many situations where industrial control systems work with external IT network systems. As a result, these industrial control systems are built on general-purpose Operating Systems software or protocols. For these reasons, the importance of having security measures on industrial control systems is increasing.

Taking NIST Special Publication 800-82[(1)] as our reference, we are promoting our R&D programs into security technologies as measures against any security-breaching incident in the future.

This paper introduces our security technologies developed mainly to cope with falsification on control system software and system configuration.

2 Outlined Security Technologies

The newly developed security technologies are composed of the following five elements.

2.1 Code Verification Tool

This tool is used for the static analysis of application codes and libraries. In static analysis, any available list of functions defined for each application is used. The role of static analysis is to call up any OS function that leads to the vulnerability of software or restriction of a library function call. The code verification tool is devised to use only the functions that are limited to applications so that they do not involve any vulnerability.

2.2 Deployable Application Bundle

The deployable application bundle is an assembly of various policies, authentication information, and setup data. It is a model of the only application that can be started up within a control system where this expertise is used.

The deployable application is established by inserting the application codes and libraries into the system configuration tool together with specifications related to the system setup.

Fig. 1 shows the procedure for creating the deployable application. For creating the application, a system configuration tool is used. This system configuration tool is used in 3 stages of work. In the first stage (Fig. 1 ①), system configuration specifications are incorporated. In the second stage (Fig. 1 ②), deployment specifications are incorporated. In

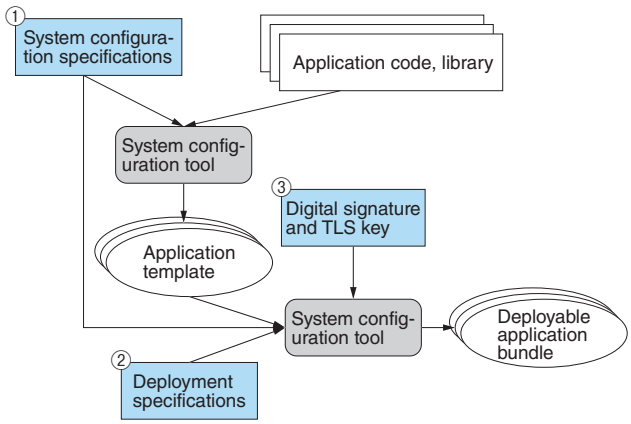

Fig. 1 Deployable Application Bundle Creation Procedure

A procedure for deployable application bundle creation by using the system configuration tool is shown.

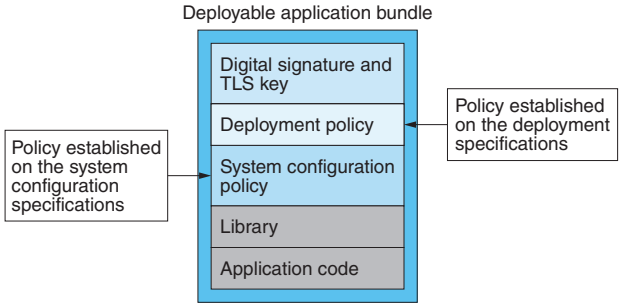

Fig. 2 Deployable Application Bundle Configuration

Configuration of a deployable application bundle established by using the system configuration tool is shown.

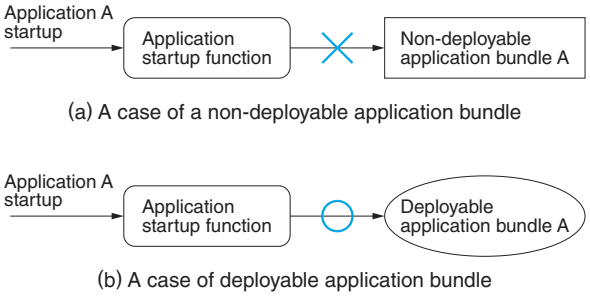

Fig. 3 Outline of Application Startup Function

Roles of an application startup function are shown.

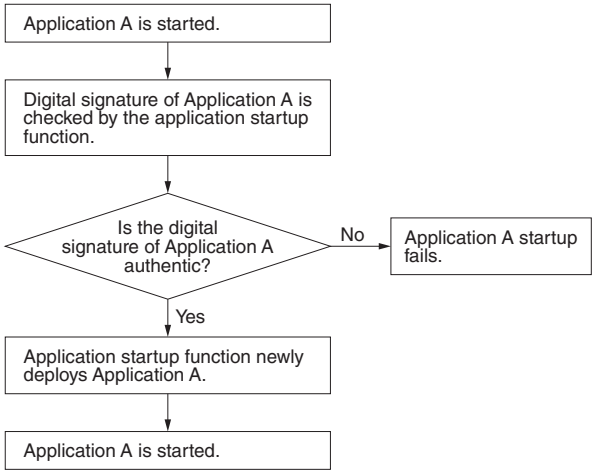

Fig. 4 Flowchart of Application Startup Function

State transition diagram of the application startup function is shown.

the third stage (Fig. 1 ③), a digital signature and digital key needed for Transport Layer Security (TLS) communication are incorporated in the application. The system configuration specifications involve various critical information such as definition information and network classification attributes to the transmission destination of the application. The deployment specifications involve concrete host setup data to be required at the time of deployment of applications to the production environment.

Fig. 2 shows the deployable application configuration. Security policies established on the system configuration specifications and deployment specifications are incorporated in the application. The digital signature is incorporated to check for no falsification of deployable application bundles.

2.3 Application Startup Function

Fig. 3 shows the outline of the application startup function. The application startup function is used to start a deployable application bundle. All applications begin with the invoking of the application startup function. There is no action for the application startup where no system configuration tool is used.

Fig. 4 shows a flowchart of the application startup function. When the application startup function is used, a digital signature incorporated in the deployable application bundle is verified to confirm that no content of the application is altered. After the verification of the digital signature, the application startup function newly deploys any deployable application bundles and creates a condition to start up the application.

2.4 Communication Restriction of Applications

Fig. 5 shows an outline of the diagram explanation for the communication restriction on applications. This function is intended to limit communication so that this communication can be maintained only with the destinations specified for the applica-

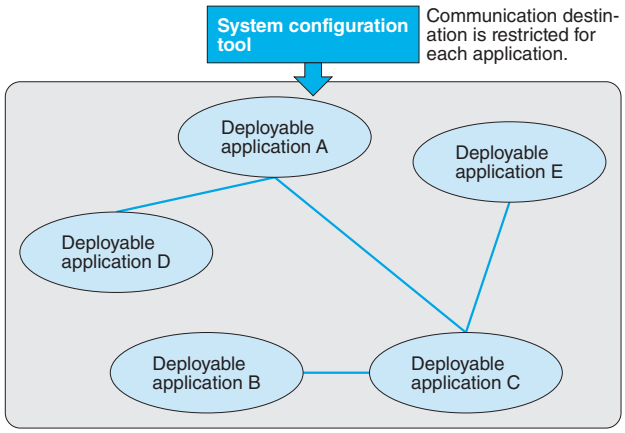

Fig. 5 Outline of Communication Restriction on Applications

The outline of a communication restriction on applications by the system configuration tool is shown.

tion. The deployable application bundle includes definition information about the communication destinations. When communication for an application is initiated, a series of confirmation process is carried out to examine whether the communication destination and the communication type registered in the definition information are authenticated. Definition information in regard to communication destinations for applications also contains access restriction information to such communication destinations as databases and files.

2.5 Communication Secrecy for Applications

All application communications are encrypted by the TLS.

3 Features of Our Security Technologies

Table 1 shows an IT security threat to be controlled by our security methods.

Our technologies provide security measures through an effective combination of the aforementioned five elements.

(1) Using the code verification tool, applications are developed without allowing the introduction of vulnerability.

(2) Using the system configuration tool, a highly reliable application can be created for the deployable application bundles.

(3) Using the application startup function, it can start up a deployable application. Regarding the startup state application, by the authentication of the digital signature by the application startup function, it can ensure that there is no alternation on the application contents from the state of using the system configuration tool.

(4) When an application starts a communication, the authentication of the communication destination will be carried out. The application is only allowed to perform communication under the control specified by the definition information in the specifications.

(5) The application exchanges TLS-encrypted data with permitted communication destinations.

Table 1 Application Range of Security Technologies

This table shows the elements of IT security risks and the measures taken by our security technologies.

Security threat	Mitigations
Session hijacking: Takeover of one end of a live communication channel by unauthorized party	Use endpoint authentication TLS 1.2
Man-In-The-Middle (MITM) attacks : Communication relaying and interference intended for eavesdropping and tampering	Communication integrity according to TLS 1.2
Messaging attacks: Transmission of unauthorized or invalid requests or responses	Relief of the attacks in communication by TLS 1.2
Exfiltration: In a network without any restrictions, data may be illegally transmitted by application.	Conduct static analysis on application codes and library and taking measures in order not to create any vulnerability.
Substituted application codes: Execution of an unverified application	Due to digital signature authentication by the application startup function, no unauthorized falsification application is executed.
Code injection attacks: Injection of malicious codes in applications	In order to avoid the creation of vulnerability, conduct static analysis in order to relieve code injection risks.

4 Postscript

This paper introduces our security-related technologies developed to cope with the falsification on control system software and system configurations. Going forward, we will continue to work on the required security technology development at the application layer level so that our customers can use control systems in a highly secure manner.

《**Reference**》

(1) NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," 2011, (http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf) (December 2, 2014 reading)