Security Technologies for Control Systems

Satoshi Doki

Keywords IoT, Security, Tamper resistance

Abstract

With the rapid spread of the Internet of Things (IoT) in recent years, security threats to control systems increase every year. Although security measures are taken for the IT devices connected to the Internet, there are still many security challenges to be resolved for closed networks.

Security measures in control systems, which operate on networks with a high level of security, have not been advanced. Cortex-M, a Central Processing Unit (CPU) for IoT devices provided by ARM Ltd., has an optional security function called the TrustZone as a security technology that can be applied to the end devices of control systems where low cost and low power consumption are more important than preferred over performance. TrustZone provides a function to divide the system into a secure state※1 and a non-secure state※2 with a single CPU at a low cost. Placing confidential data and processing in the secure state makes it impossible to access the system from a common area, thus preventing security attacks on IoT devices from networks controlled in a normal state. In addition, by using cryptographic accelerators, we can support cryptographic communication with a performance that can be applied to control devices.

1 Preface

Stimulated by the recent advent of Internet of Things (IoT), control equipment formerly used in a closed network and field network equipment can be connected to a public network. At the same time, however, the improvement of tamper resistance is required. Tamper resistance is a capability to prevent reading and rewriting of internal data by means of an irregular method. Even though communication data are encrypted, such data can be stolen or damaged if the terminal equipment is attacked and a secret key or authentication data used for cryptographic communication are leaked. This paper introduces the secure processing of an application for cryptographic communication where security technologies developed for IoT equipment are employed.

2 Central Processing Unit (CPU) with Tamper Resistance Function

2.1 Cortex-A Series

Like the CPU for mobile phones, the Cortex-A designed by ARM Ltd. is widely adopted. Cortex-A is provided with a security function called the TrustZone. For the TrustZone, the system is divided into the secure state and the non-secure state and both states can be separated by an exclusive instruction. Since the secure and non-secure states are not separated physically, the security function can be realized with a low cost and any specific development environment is not required. The TrustZone assures the tamper resistance property by which access can be controlled from non-secure to secure state. In the case of a mobile phone for example, the secure state manages confidential data like electronic money, secrecy treatments like authentication and cryptographic processing, and hardware functions like fingerprint sensing.

Table 1 Comparison of TrustZone

Comparison of the TrustZone is shown between Cortex-A and Cortex-M.

Item	Cortex-A	Cortex-M
Switchover processing	Software control	Hardware control
Switchover level	OS	Function
Switchover time	Slow	Fast
Memory separation	Memory space separated	Memory regions

2.2 Cortex-M23/M33

As a CPU for IoT equipment where low cost and low power consumption are more valued than performance, ARM Ltd. offers the Cortex-M. The Cortex-M23/M33 released in 2016 is provided with the TrustZone, which has specifications that are different from the Cortex-A, so that even a low-power Cortex-M can function effectively. Table 1 shows a comparison of the TrustZone.

In the Cortex-M TrustZone, security conditions are switched over to hardware control. Such a feature simplifies switchover processes and increases the processing speed. Since the security condition switchover is conducted at the function level and a distinction of memory is performed at the address level according to the state of security, the programing volume necessary for security processing is greatly saved.

3 Secure Processing Actions

3.1 Environment of Development

Secure processing with the use of the Cortex-M TrustZone is applied to the communication application in order to confirm the tamper resistance property and investigate the resultant influence upon secure processing performance. Table 2 shows the development environment of Cortex-M.

3.2 Secure Processing

Essential points are described below when an existing application is used for secure processing with the TrustZone.

(1) Separation of project

In the integrated development environment, applications are administered by projects. An existing project is used to deal with processing in the non-secure state. The new project is used to manage processing in the secure state. The secure project includes cryptographic processing and processes to access crypto and authentic data.

Table 2 Development Environment of Cortex-M

The developed board and development environment of Cortex-M are shown.

Function	Specifications
Developed board	ARM Cortex-M Prototyping System (MPS2+) Cortex-M33 20 MHz
Integrated development environment	ARM Keil MDK Professional
Compiler	ARM Compiler v6 (Clang/LLVM)
Debugger	µVision v5.26.0
RTOS	CMSIS-RTOS2 RTX5
Middleware	IPv4, mbedTLS, Paho MQTT

(2) Initialization process for secure project

A process for initialization of the TrustZone function is added. This refers to the process of segmentation where the memory regions are divided into segments (address ranges).

(3) Registration of a call enabling function

A function of the secure state is registered to enable calling from the non-secure state. Any call with the use of a function not registered is regarded as an unauthorized access.

(4) Call of non-secure state function

Function pointers in a non-secure state are registered to call up the secure state.

(5) Thread attribute setup

Thread attribute setup is conducted by a non-secure project. When a thread (a unit of process in real-time OS) is established to call up a function in the secure state, the TrustZone attribute is set up.

3.3 Communication Application

As an applicable object for secure processing, a communication application conforming to the Message Queuing Telemetry Transport (MQTT) protocol is adopted. It supports the Secure Socket Layer (SSL), a quasi-standard crypto communication protocol. Table 3 shows the cipher suite that is used for crypto communication.

In addition, treatments for secure processing have been carried out with the use of the TrustZone. Table 4 shows distribution of processes and data in a secure and non-secure state. Revisions needed, other than user applications, are the points where cryptographic processes are called inside the MQTT library.

3.4 Evaluation

From the serial port of the non-secure state,

Table 3 Cipher Suite

Combination of cyphers used for crypto communication is shown. The adopted cipher suite has sufficient cryptographic strength.

Function	Specifications
Protocol	Transport Layer Security (TLS) v1.2
Key exchange	ECDHE
Public key cryptography	RSA 2048 bit
Common key cryptography	AES256-GCM
Hash function	SHA2-384
Public key certificate	X.509 certificate

Table 4 Distribution of Processes and Data

Processes and data in the secure state cannot be accessed from the non-secure state.

Process/data	Secure state	Non-secure state
RTOS		○
Network processing		○
Cryptographic processing	○	
Secret key of cipher	○	
Cipher certificate	○	
Transmission data before encryption	○	
Reception data after decryption	○	
Encrypted transmission/reception data	○	○

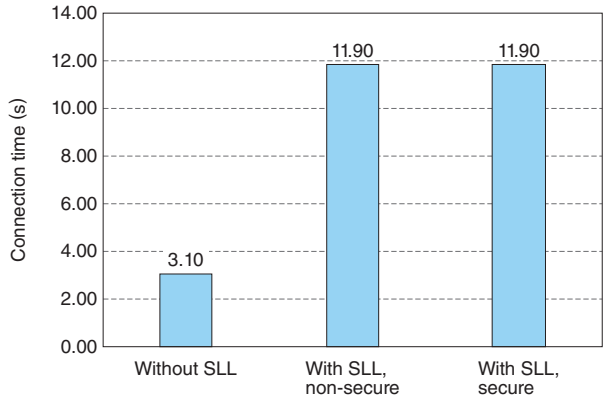

Fig. 1 MQTT Connection Time

Consumed time is shown to complete a connection with the server. As a result of encryption (SSL made effective), connection time is extended considerably. Influence by secure processing is kept minimal.

we tried to gain access to the crypto data in the secure state but failed in reading out any data. At that time, we confirmed a sign of detection of an unauthorized access.

Fig. 1 shows MQTT connection time and Fig. 2 shows MQTT transmission time. By making cryptographic communication (SSL made effective), connection time can be extended considerably. At the same time, it is apparent that the effect of secure processing by the TrustZone is minimal in terms of processing time.

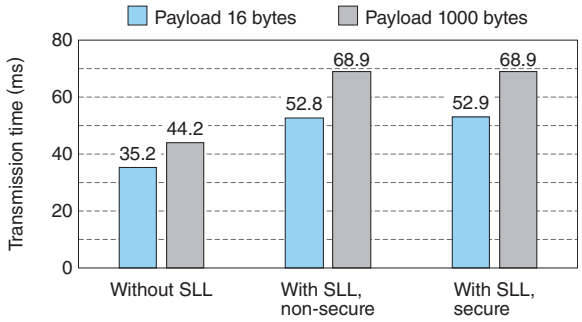

Fig. 2 MQTT Transmission Time

Transmission time for each payload (transmission size) is shown. As a result of encryption (SSL made effective), transmission time is increased by about 50%. Influence by secure processing is minimal.

Table 5 Development Environment of Cortex-A

The developed board and development environment of Cortex-A are shown.

Function	Specifications
Developed board	Xilinx Zynq UltraScale+MPSoC (ZCU102) Cortex-A53 1.5 GHz
Crypto accelerator	Xilinx Configuration Security Unit (CSU) AES-GCM256, RSA 2048/4096 bit, SHA3-384
Integrated development environment	Xilinx SDK 2018.1
Compiler	GCC 7.2.0
Library	Xilinx XilSecure (H/W), ARM mbedTLS (S/W)

4 Cryptographic Accelerator

There is a cryptographic accelerator (“crypto accelerator” hereafter) that performs encryption in hardware. We examined the effect of the crypto accelerator with the aid of a developed board for Cortex-A. Table 5 shows the development environment of Cortex-A.

Fig. 3 shows the processing time of a common key number and Fig. 4 shows the processing time of the Hash function. In any case, performance is enhanced by tens of times that of software processing when a crypto accelerator is employed.

Any CPU adopting the Cortex-M23/M33 is equipped with a crypto accelerator so that high-speed cryptographic processing and reduction of power consumption can be realized.

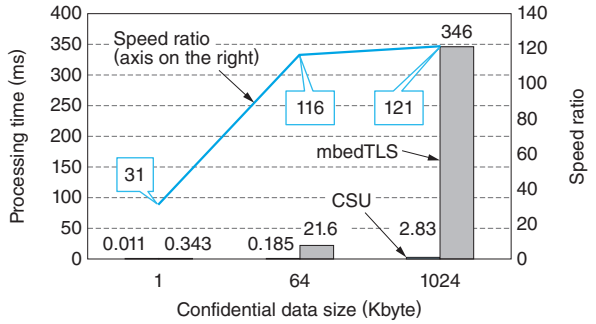

Fig. 3 Processing Time of Common Key Number

Comparison of processing time is shown between the crypto accelerator (hardware processing) and common key cryptography by software processing (AES-GCM256). The effect of the crypto accelerator is prominent.

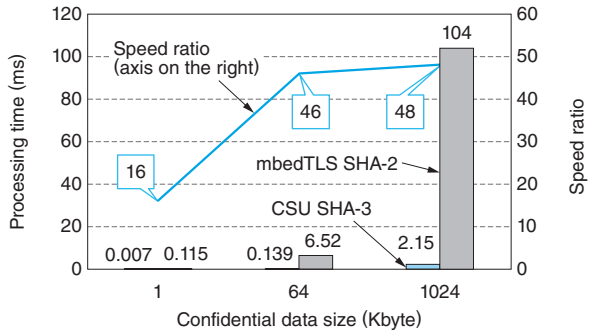

Fig. 4 Processing Time of Hash Function

Comparison of processing time is shown between crypto accelerator (hardware processing) and Hash function by software processing (AES-GCM256). Although the opposing algorithms are different, the security strength is equivalent to each other.

5 Postscript

This paper introduced security-related technologies applied to terminal equipment of control systems. For the Cortex-M23/M33 based on the TrustZone, we confirmed that crypto communication and tamper resistance performance applicable to control equipment can be secured by using CPUs equipped with crypto accelerators.

(Notes)

※1. Memory state where security is assured
※2. Memory state where security is not assured