Contribution ID: **30** Type: **Oral Presentation**

A Design of Automatic Certificate Management for a Zero Trust IoT system

Friday, 21 March 2025 09:40 (20 minutes)

In IoT (Internet of Things) systems consisting of IoT devices, edges, and cloud servers, it is expected that various sensor data obtained from IoT devices will be collected, accumulated, and utilized to solve various social issues using Artificial Intelligence. However, due to the sophistication and intensification of cyber attacks, security measures for IoT systems consisting of a large number of IoT devices deployed remotely have become an issue. The idea of "zero trust" has attracted attention as a security measure method, and we are considering applying the idea of zero trust to IoT systems. In zero trust, it is necessary to identify resources such as computers and data that need to be protected, monitor and analyze access to them, and take measures to prevent the spread of damage when a security infringement is discovered. In applying zero trust to IoT systems, we monitor the software execution status and communication status of many IoT devices, and aim to prevent the spread of damage to other IoT devices and servers by revoking the host certificate of an IoT device where a problem has occurred. Issuing host certificates to IoT devices needs to be done without human intervention, and it is essential to implement automatic issuance and automatic revocation of certificates in cooperation with a certificate authority.

In this paper, we consider the application of the ACME (Automatic Certificate Management Environment) protocol to certificate lifecycle management in IoT systems. A model in which the certificate subscriber requests the revocation cannot be applied directly to IoT scenarios. Therefore, it is necessary to identify and authenticate entities that have the authority to revoke the host certificate of an IoT device and to revoke it on behalf of the device. We consider several designs that meet this requirement, particularly the use of the ACME protocol, and discuss how the proposed system solves the issues and its feasibility in the zero trust IoT system.

Primary authors: Prof. TAKEFUSA, Atsuko (National Institute of Informatics); Dr SAKANE, Eisaku (National Institute of Informatics)

Presenter: Dr SAKANE, Eisaku (National Institute of Informatics)

Session Classification: Network, Security, Infrastructure & Operation -III

Track Classification: Track 7: Network, Security, Infrastructure & Operations