Contribution ID: **27** Type: **Poster Presentation**

Certification Mechanism to Assure Software Reliability with Digital Signature

Internet of Things (IoT) platforms are widely deployed both in scientific and social e-infrastructures. Security is one of crucial issues to assure secure data collections and analyses on the platforms. For example, the vulnerability of software running on an IoT device may give opportunity attackers to insert malicious processes in the software (or code) such as data leakage and falsification. Code developers, system administrators and users of an IoT platform need to confirm that codes, including applications, middleware and operating systems, used in the platform is reliable to avoid security incidents.

Code signing is commonly used to prove the reliability of codes. The code developer signs the code and publishes it with his/her digital signature, so that the user of the code can verify the integrity of the code and the code developer. However, the digital signature here does not assure that the code does not include vulnerability. Vulnerability scanning tools are also used to detect vulnerability in a code. The tools verify if the scanned code includes known vulnerability. For example, Docker Scan enables the code developer or the user to verify vulnerabilities included in container images. While these tools assure the reliability of the code at the moment of scanning, they do not verify the reliability of the code after scanning. If a new vulnerability is found after the user run the scanned code, the tools do not have means to stop the code.

In this presentation, we propose a software certification mechanism to provide an assurance of software reliability with digital signature. We assume that the code is reliable, if the integrity and the developer of the code are proved, and if the code has passed vulnerability scanning. The proposed architecture is organized by a code developer, a code user, a code validator and a certificate authority. The code developer signs the code and submit it to the code validator. The code validator is a third-party organization that provides a code verification service. The service scans the code submitted by the code developer and sign the code if it confirms that the code does not include known vulnerability. The code user can confirm the reliability of the code by verifying the digital signature of the code, and the user runs the reliable code on IoT devices or servers. The certificate authority issues digital certificates for code signing and clients (a code developer and a code validator). A new vulnerability may be found after scanning, or at the moment of the code validator signed the code. Once the new vulnerability is found, the certificate authority revokes the digital certificate used for signing the vulnerable code and notifies the code user, so that the user can immediately make decision, e.g., stopping the running code or applying the workaround.

We present the detailed architecture of the proposed mechanism and discuss its operational issues: Which entity (an application source codes, library codes, OS packages) should the code validator sign? How does the certificate authority immediately notify certificate revocations to users?

This work is supported by JST, CREST Grant Number JPMJCR21M3.

Primary authors: SHIMIZU, Sayako (National Institute of Informatics); SAKANE, Eisaku (National Institute of Informatics); NISHIMURA, Takeshi (National Institute of Informatics); AIDA, Kento (National Institute of Informatics); Mrs TAKEFUSA, Atsuko (National Institute of Informatics)

Presenter: SHIMIZU, Sayako (National Institute of Informatics)

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