Contribution ID: **57** Type: **Oral Presentation**

A Study of Certificate Management Mechanism Suitable for Virtual Machine with Arbitrary Lifecycle

Thursday, 4 April 2019 15:00 (30 minutes)

Virtual machine can flexibly meet user's demands for computing resources and be freely created and deleted. The virtual machine validation and secure communication as network entity are required as well as a physical machine. This paper investigates an X.509 certificate issuing mechanism to virtual machine with arbitrary lifetime.

Let us consider a service that offers virtual machines as computing resources. The provisioning service can create a virtual machine immediately according to the demands of users and boot up it. If user requires an X.509 certificate for secure communication over TLS in the Internet, the service will not be able to arrange the certificate issued by an ordinary certificate authority unless the service prepares the certificate in advance. It is necessary to carry out procedure for certificate issuance separately. When the virtual machine shut down, certificate revocation will be needed unless the user plan to reuse it. The quick revocation must be needed even if the period of use is very shorter than the validity of the certificate. Thus, because of the flexibility of lifetime of virtual machine, certificate management following the ordinary certificate authority does not often fit the lifetime of virtual machine. Therefore it is worthwhile to investigate certificate management mechanism suitable for the flexibility of virtual machine.

In this paper, we consider a mechanism for restrictedly issuing a kind of intermediate CA certificate. The subject possessing the certificate does not act as an ordinary certificate authority and shall issue server certificates only to virtual machines managed by itself. By means of the mechanism an organization that offers virtual machines can issue certificates suitable for the flexible lifetime of the virtual machines. Moreover it is able to manage the certificate lifecycle based on the lifecycle of virtual machine. We also discuss the proposed mechanism, comparing with Let's encrypt approach that can be considered as another solution to the issues.

Primary author: Dr SAKANE, Eisaku (National Institute of Informatics)

Co-author: Prof. AIDA, Kento (National Institute of Informatics)

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

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations