Title:
Security/Privacy Models for "Internet of things": What should be studied from RFID-schemes?

Authors: Daisuke Moriyama and Shin'ichiro Matsuo (NICT)

Emerging technology space: Internet of Things
Class of cryptographic requirements: Security/Privacy model

Abstract:
We would like to discuss the security/privacy models toward "Internet of Things". One of the important technologies to enhance Internet of Things is security/privacy protection for low-power devices. Related researches are intensively conducted for low-power devices like RFID-tags from early 2000's. Their prime contributions are on designing secure encryption/authentication schemes and defining security/privacy model. However, they are still developing.

Several cryptographic security models for RFID-tags had been proposed from 2005, they do not entirely cover real-life security/privacy problems caused from Internet of Things. For example, authentication is confused with identification in the proposed models/schemes for RFID-tags, but it should be separated to construct higher protocols for Internet of Things.

The difficulty to build security/privacy model is in the limited computing environment. It is hard to implement expensive operations like asymmetric key cryptography in the current RFID-tag. On the other hand, potential scale of privacy issues is unknown for Internet of Things.
Thus, we should build security/privacy models which meet such balance of resource constraints and real-life security/privacy issues.

Here, we discuss way to formalize the applicable security/privacy from the existing cryptographic primitives and provide formal security proof.
When we consider real-life usage, we also should take care of life cycle, key management problem and reusability to accomplish Internet of Things. For example, RFID tags are only used to show identity to someone in present, however, one can imagine that cheap low-power devices extensively communicate with other one.

In this talk, we show a direction toward the security/privacy model:
(1)the difference from the existing security/privacy and key-management model for RFID-tags, (2)organizing real-life security/privacy requirements, and (3)their relationship for Internet of Things.