Introduction and Welcome Message From “IPA” and “INSTAC”

26 September 2005

Tsutomu Matsumoto

Yokohama National University

What is “IPA”

CRYPTREC (Cryptography Evaluation and Research Committees)

– CRYPTREC Cryptographic Module Committee*

is aiming at **the creation of evaluation criteria and test requirements for cryptographic modules to prepare for a domestic CMVP compliant to the international standard**.

* Chair: Matsumoto

Secretariat consists of the members from

1. METI (Ministry of Economy, Trade and Industry)
   - **IPA (Information-Technology Promotion Agency, Japan) --- is planning to establish “Japanese CMVP”**
2. MIC (Ministry of Internal Affairs and Communication)
   - NICT (National Institute of Information and Communications Technology)

What is “INSTAC”

TSRC (Tamper-resistance Standardization Research Committee)*

was established in 2003 in

INSTAC (Information Technology Research and Standardization Center), which is a department of

JSA (Japanese Standardization Association).

* Chair: Matsumoto

Circumstances (1)

- It was in the year 2003 that Security Requirement for Cryptographic Modules became a New Work Item in ISO/IEC JTC1 SC27.
- This was one of the events that triggered TSRC to start.
- On the other hand, there were pressing domestic demands for secure implementation of cryptographic functions for government use as well as commercial use.

Circumstances (2)

- With these backgrounds, TSRC has been focusing on technical study of future items for standardization.
- Its scope is a little different from that of the CRYPTREC cryptographic module committee, another activity in Japan, which is aiming at the creation of evaluation criteria and test requirements for cryptographic modules to prepare for a domestic CMVP compliant to the international standard.

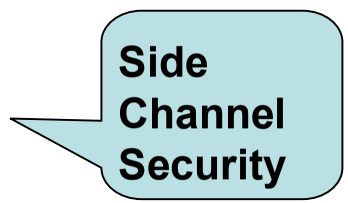
Purpose of INSTAC/TSRC

– The purpose of TSRC is to establish the foundations of secure implementation of information technologies from a point of view of standardization by carrying out the following study and research items:

1. Systematic study of various tampering techniques
2. Developing the method to describe requirements to tamper-resistance
3. Contributing to the international standardization with respect to tamper-resistance

Activities of INSTAC/TSRC

- TSRC is a three-year-term committee and its plan is as follows:
- It was established in September 2003 and decided its direction and started building **platforms** for experiments.
- In FY2004, it studied tamper-resistance deeply, based on theoretical and experimental analysis.
- It also discussed **how to describe requirements to tamper-resistance**.
- In FY2005, it is attempting to contribute to tamper-resistance standardization, including FIPS140 series.



Enjoy Discussion!