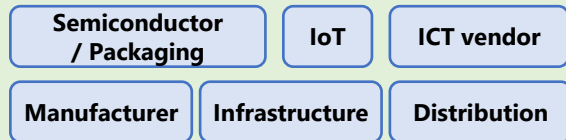


Development of Security Assurance Scheme for SCU which can be embedded to low-cost IoT devices

Electronic Commerce Security Technology Research Association
 • National Institute of Advanced Industrial Science and Technology (AIST)

Application Area



Systematic threat analysis clarifies security requirements and finds good tradeoffs between security evaluation rigor and development man-hour.

Technical Features

■ Security level classification

Ensuring the validity of how to classify the level of certainty of security implementation and of how to show security for the low-cost IoT nodes.

■ Security assurance schemes

Building security assurance schemes (security evaluation technology and certification framework) optimal for devices using hardware roots of trust.

Effects·Use Case·Technical Details

■ Effects

Third party security evaluation and certification of IoT devices equipped with SCU, which is the root of trust, is possible.

■ Use Case

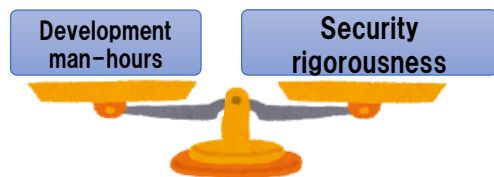
By applying this technology to devices equipped with SCU, it is possible to develop highly reliable equipment at a reasonable cost.

■ Technical Details

Evaluate the resistance of SCU-equipped chips to all relevant attacks in a rigorous evaluation in accordance with the international standard ISO/IEC 15408.

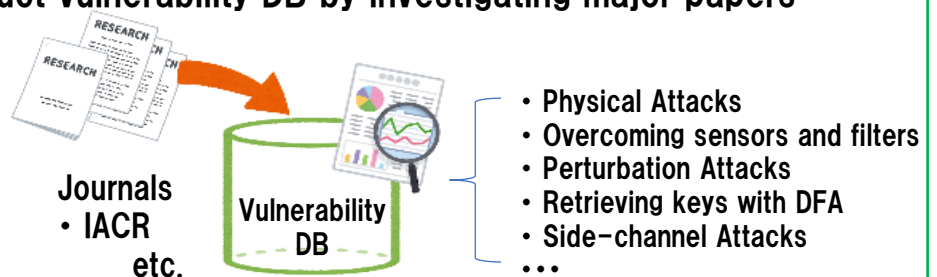
Security assurance of SCU-used IoT devices

Based on cryptographic hardware roots of trust, develop highly reliable devices at reasonable cost



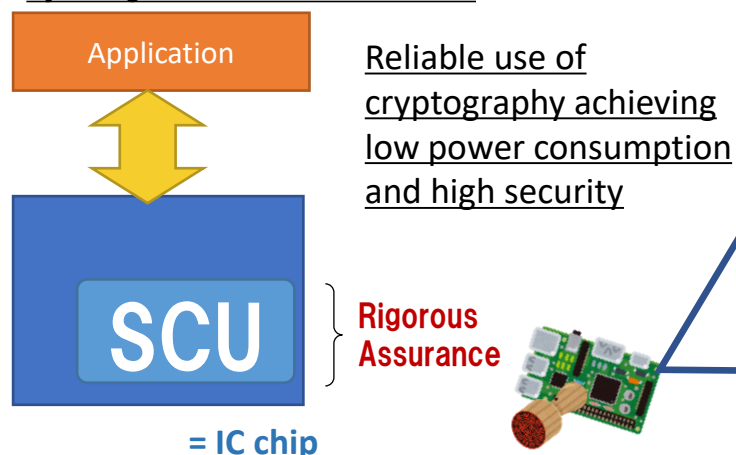
Systematic aggregation of attack methods for IoT devices

Construct vulnerability DB by investigating major papers



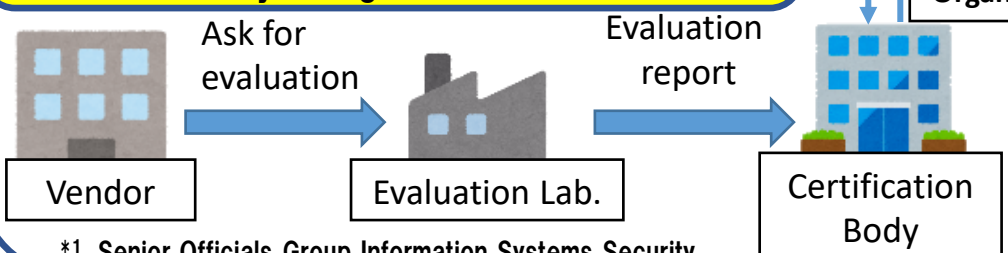
Building security assurance schemes for roots of trust

Ensuring security of an IoT device by using an SCU as root of trust



Building security assurance schemes for SCUs

Examine how to assure the security of SCU-equipped devices, based on discussion trends such as evaluation guarantee level and vulnerability rating in SOGIS*1



*1 Senior Officials Group Information Systems Security