TOSHIBA
Leading Innovation

Cybersecurity Topics and Vulnerability Management - ICS and IT security -

Part1:

The Latest Research Subjects about ICS Cyber Security

Corporate R&D Center, Toshiba Corporation

TOSHIBA eco style

Toshiba Group contributes to
the sustainable future of planet Earth.

Research Territory

We focused on the latest research subjects about

- **Requirements specific to ICS, e.g. Smart Grids**

and

- **Defensive technologies highly effective for ICS**

rather than many different matters of common IT security.

(※) ＩＣＳ：Industrial Control System

1. Privacy Protection in Metering Data

Subject :

Meter

Metering Data

Server

Consumers

Want to avoid leakage of privacy information from metering data

Conflicting requirement

Operators

Need statistics of metering data for accounting and stabilization

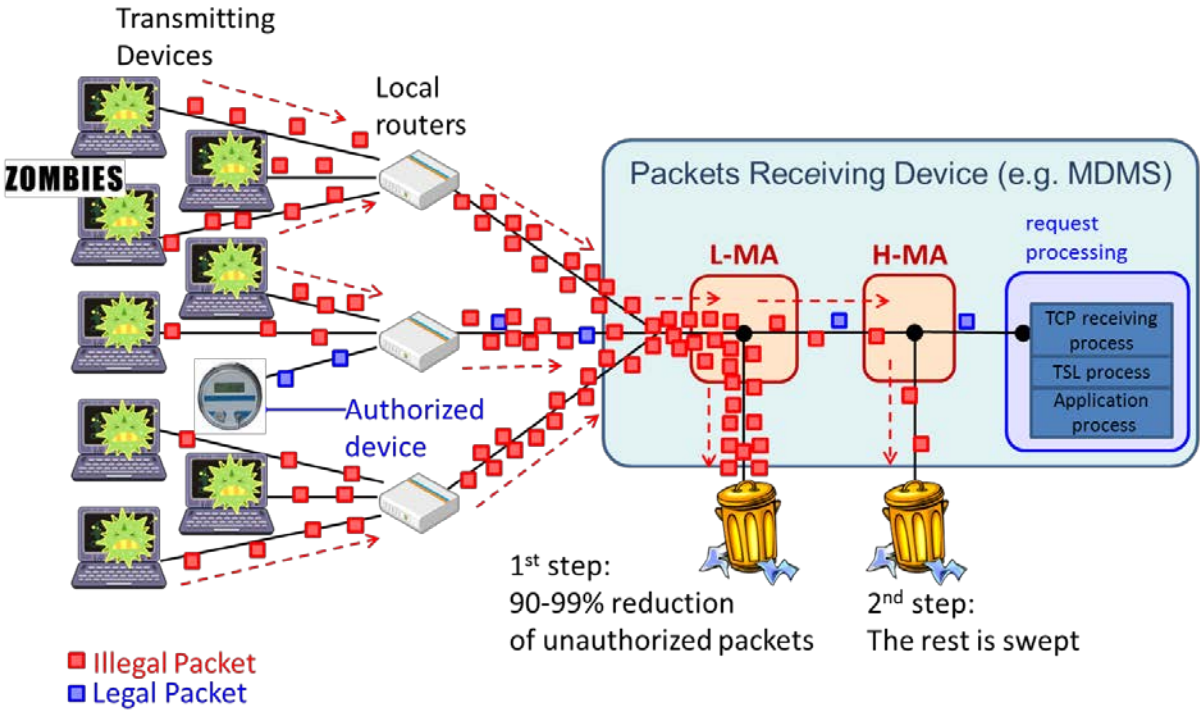
Contribution : Both sides requirements are solved

- ✓Monthly amount is visible / current value is invisible
- ✓Regional current amount is visible / personal is invisible

➥ We developed privacy protection schemes with "secret sharing" and "homomorphic encryption“ and experimentally proved them, respectively.

2. Device authentication protocol against DDoS attacks

Contribution : We proposed a multi-layer authentication scheme using a combination of L-MA (speed-oriented very Light Message Authentication) **and H-MA** (security-oriented relatively Heavy Message Authentication) **parts, that enables pre-authorized proprietary communication devices to run continuously against unexpected DDoS and zero-day attacks.**



3. Key management scheme in AMI networks

Subject : **Metering application data and control messages are hard to keep systematically secure without a re-key function.**

Contribution : **We developed and validated a key management scheme with a re-key function by integrating a standard network access authentication protocol (RFC 5191) and metering protocols (ANSI C12.22/C12.19).**