A Security Framework for IoT Networks

Objectives of this Research

• Developing a new comprehensive security framework for IoT Network.

• Building a Testbed for Monitoring/Detection/Visualization, Secure Communication for IoT devices. Case-study with a WSN.

• Creating an open collaboration between researchers of Japan and other ASEAN-IVO members (joint seminars, workshops, common paper publication).

Assoc. Prof. Dr.Hab. Dr.Ing HOANG Dang Hai
Hanoi, 24.11.2016
• IoT = World of interconnected things (~50 billion devices by 2020)

• IoT = pervasive & ubiquitous network that enables monitoring/controlling physical environment by collecting, processing, analyzing data generated by sensors/smart objects

• IoT enables advanced applications like smart cities, smart society,...

• IoT is everywhere !
Security in IoT

• IoT has common security issues as in traditional networks:
  - All of the same issues we have with:
    - Malware, malicious applications, DoS/DDoS attacks, Hijacking, etc.
    - Access control, vulnerability management, patching, monitoring, etc.
    - Security of the Cloud, Fog, etc.

• Increasing growth of IP-based devices/applications

• IoT opens a completely new dimension to security:
  - Attacks move from digital to physical world, from manipulating information to controlling actuation.
  - Issues: Physical tampering, Data Confidentiality & Data Authentication, Entity Authentication, Entity Confidentiality (Privacy), Availability (Resist Denial-of-Service), Insecure communication channel, Identity, Trust, etc.

• Other considerations: limited resources, processing, etc.

Smarter security systems for IoT needed!
A comprehensive security framework for IoT
What we need?

- Secure infrastructure (secure Fog)
- Effective device monitoring/attack detection system (visualization), network traffic anomaly detection
- Identity management, Trust authentication, secure data acquisition
- Lightweight encryption protocol
- Secure communication and data transport channels
- Etc.

Fig. (Source: Cisco)
A Security Monitoring System for IoT Networks

**Building Components:** (some our previous research results)

- Traffic data capture
- Network traffic anomaly detection
- Anomaly data processing & visualization

**New approaches for IoT**

**Building a Testbed for Monitoring / Detection / Visualization, Secure Communication for IoT devices.** (some our previous research results. Experiences/Expertises from NICTER/DAEDALUS system)

**Further development for IoT**

**Developing a dataset for attack detection on IoT networks**

(some our previous research results. Experiences/Expertise from Kyoto Honeynet Project)
Our previous researches:

- Application of WSN for smart city: Traffic-generated pollution monitoring in Hanoi City
- Pollution data collection
- Data transfer / forwarding
- Data processing (calibration, clustering, etc.)
- Data visualizing based on google map services

Further study:

- Sensor identity management
- Secure data transfer
- Privacy & trust
Expected Collaboration

- **NICT from Japan:**
  Experiences/Expertises from NICTER/DAEDALUS system

- **Other institutions in Vietnam:**
  HUST-SoICT, HUST-FET, etc.

- **Other institutions from ASEAN-IVO member states:**
  NECTEC (Thailand), MTI (Indonesia), CSYU (Myanmar), etc.

Thank your!