ICT Virtual Organization of ASEAN Institutes and NICT
ASEAN IVO Forum 2016
Call for Presentations

Submission and Registration Form

I. Title—Title of presentation:
The Development of an Internet of Things (IoT) Monitoring and Detecting System based on NICTER/DAEDALUS

II. Author(s)—Full name (First name family name):
1. Dr. Chalee Vorakulpipat
2. Mr. Ekkachan Rattanalerdnusorn
3. Mr. Visut Savangsuk
4. Ms. Sineenat Tienkouw

III. Organization(s):
National Electronics and Computer Technology Center (NECTEC), Thailand

IV. Topic selection:
Cyber-Security and its applications

IV. Abstract:
Project objectives

1. The general objective of this project is to formalize the collaboration of domain experts in information security research in Japan and Thailand, create strong and sustainable links between partners through exchange of researchers, and cultivate international industry academic partnerships.
2. The scientific goal of the project is to develop an applied research study for monitoring and detecting attacks and threats in Internet of Things devices, based on the NICTER/DAEDALUS system developed by Cybersecurity Laboratory of the National Institute of Information and Communications Technology (NICT), Japan. The different and complementary approaches developed by partners in Japan and Thailand will allow the project to develop innovative solutions to the challenging and fundamental issue of IoT security, which cannot be achieved by any single group.
3. The outcomes of the project will include joint publications, workshops and new project proposals in this emerging area. The expertise and industry connections of partners in Japan and Thailand will provide a great leverage for understanding the

user requirements in diverse countries, for better dissemination of research results and for potential commercialization.

Motivations, Use cases and System requirements

Network security has become a critical issue in recent years. A drastic increase of device usage for accessing to corporate networks could expose the systems to major security risks. While the use of personal computers moves to mobile devices and IoT devices, it is highly desirable to gain more services and more accessible channels to the corporate information. This leads to an increase in the number of attacks and threats from hackers, thus the need for advanced security solutions is growing rapidly. One of the widely-accepted solutions is a preventive action including a system for monitoring and detecting attacks and threats in computer systems within an organization or across organizations. Since the use of IoT device drastically increases and security practices in most IoT devices are not yet in place, the monitoring and detecting system should also emphasize attacks and threats between and among IoT devices. The system requirements can be illustrated by the following use scenario:

Scenario 1

A humid sensor is connected to a smartphone. Data from the humid sensor is sent out via the smartphone to a computer server within an organization. A temperature sensor, another Iot device attacks the humid sensor via another smartphone through another corporate network. Our system detects the attacks at the attacked IoT device (humid sensor), and then sends alert messages to the attacking IoT device (temperature sensor) and the system administrator.

Scenario 2

A humid sensor is infected by DDOS. A hacker uses the humid sensor to attack three other IoT devices within three different corporate networks. Our system detects the attacks at the three attacked IoT devices. Then, our system sends alert messages to the DDOS victim at the humid sensor.

Actually similar requirements applied for monitoring and detecting attacks and threats in corporate networks can be found on a system called NICTER/DAEDALUS system developed by NICT, Japan. In this proposal, we aim to focus on an application that monitors and detects attacks and threats between or among IoT devices, based on NICTER/DAEDALUS. IoT devices used for experiments in this project will be developed based on an IoT platform, developed by NECTEC .

Requirement analysis, research approaches and work plan

In order to enable the IoT monitoring and detecting system, there are key challenges which need to be addressed.

1. What are the additional requirements in monitoring and detecting attacks and threats in IoT devices to these in computers?
2. What is the root cause of IoT attacks and threats?

Apparently, a preventive mechanism related to IoT security presented above needs to be explored and validated. Fortunately, project partners have developed in-depth expertise in cybersecurity. NICT has built the NICTER/DAEDALUS system. NECTEC has been developing IoT security monitoring and detecting solutions and has had an IoT platform. The background of the partners provide a great opportunity for developing a mechanism which supports monitoring and detecting attacks and threats between and among IoT devices.

The expected outcomes of the project are:

1. A demonstrator which is evaluated in different network settings.
2. Technical solution for monitoring and detecting attacks and threats in IoT.
3. Publications and new international research project proposals.
4. Organizing joint seminars and workshops

<< Project planning is presented next page >>

The project is planned for a period of one year. The table below describes the schedule of the project.

Action	Activities/ Deliverables	Month											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Kick-off meeting												
2	Report on requirements, use cases												
3	Report on system design												
4	System installation												
5	Development, experiment and evaluation												
6	Report on results												
7	Close meeting, workshop, lesson learnt												

V. Speaker information:

Full name: Dr. Chalee Vorakulpipat
Institute: National Electronics and Computer Technology Center (NECTEC)
Address: 112 Thailand Science Park, Paholyothin Rd., Klong 1, Klong Luang, Pathumthani, 12120 Thailand
Telephone: (66) 25646900 ext 2551
E-mail: chalee.vorakulpipat@nectec.or.th

VI. Support for speaker—circle or underline any that you wish to request:

- Round trip fare at discount economy class
- Accommodation