

## **Note 1:**

1. The number of slides should be around 12 total.
2. The size of your PowerPoint PDF is no more than 10MB.
3. Please follow the format starting from the next slide.
4. Please delete the first slide (this slide) and upload to website.

## **Note 2:**

1. You may submit three additional supporting files for a maximum of four files total.
2. Each additional file is no more than 130MB.
3. Any supporting materials you submit must be saved as PDFs, where possible. This includes PowerPoint presentations, Word documents and Excel spreadsheets. Any audio you submit should be in mp3 format and any video you submit should be in mp4 or mov format.

## **Note 3:**

1. A website for “Registration” is already open from September 11, 2020.  
(<https://naivo.org/> )
2. the website for uploading presentation files will close on October 25, 2020.

**Background :**

According to Microsoft Security Intelligence Report 2019, **Malware Encounter Rate in ASEAN region is very high.**

Cyber-Space does not have country borders. It is necessary to eliminate this situation in order to make the cyber-space safe.

**Targets:**

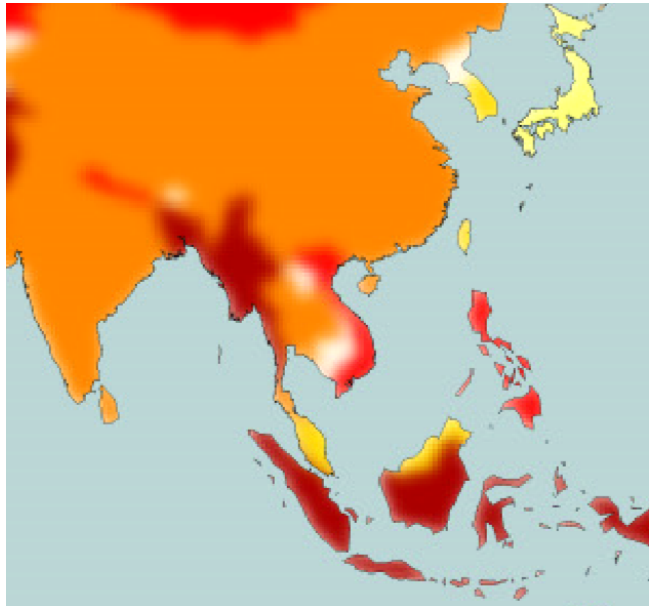
We target the security of the Local Area Networks (LAN)  
Enhance the functions of LAN-security monitoring devices and programs, which are currently provided as an open source by LAN-Security Monitoring Project.

Enhancement :

- Anonymization of captured LAN data
- Visualization of data for useful security operation
- Statistical analysis of data
- Improvement of detection algorithms (with ML)  
(\* ) such as federated learning (proposed by Google)

**Speaker:**

Assoc.Prof. Sinchai Kamolphiwong (PSU), Assoc. Prof. Hideya Ochiai (UT)



Average Monthly Malware Encounter Rate, 2018  
(Microsoft, Security Intelligence Report, 2019)



# Project Title: ASEAN-Wide Cyber-Security Research Testbed

## Project Members :

Full Name	Institution, Country	Email Address
Sinchai Kamolphiwong	Prince of Songkla University, Thailand	ksinchai@coe.psu.ac.th
Achmad Basuki	Universitas Brawijaya, Indonesia	abazh@ub.ac.id
Mie Mie Su Thwin	University of Computer Studies Yangon, Myanmar	drmiemiesuthwin@ucsy.edu.mm
Aung Htein Maw	University of Information Technology, Myanmar	ahmaw@uit.edu.mm
Hideya Ochiai	The University of Tokyo, Japan	ochiai@elab.ic.i.u-tokyo.ac.jp

## Project Duration :

2 Years: 2020-2022

## Project Budget:

2020-2021: 33,050 USD,  
2021-2022: 12,345 USD

## Project Activities: (Max. 3 slides)

Please write a brief introduction of your project activities from the following points of view:

1. Scientific
2. Technological development
3. Experiments including field testing
4. Budget plan in detail
5. etc.

**Note: please write what your project members did.**

According to survey study, malware encounter rates in ASEAN region are very high. In order to make it a real-world public testbed for cyber-security studies, this project is going to enhance the functions of the monitoring devices provided by LAN-security monitoring project by installing around hundred newly-developed security devices across ASEAN countries. To that end, we are going to develop (i) vulnerability assessment of remote local-area networks, (ii) visualization of data for useful security operation, (iii) improvement of detection algorithms and statistical analysis including the application of federated learning, and (iv) anonymization of captured data for publicizing the data.

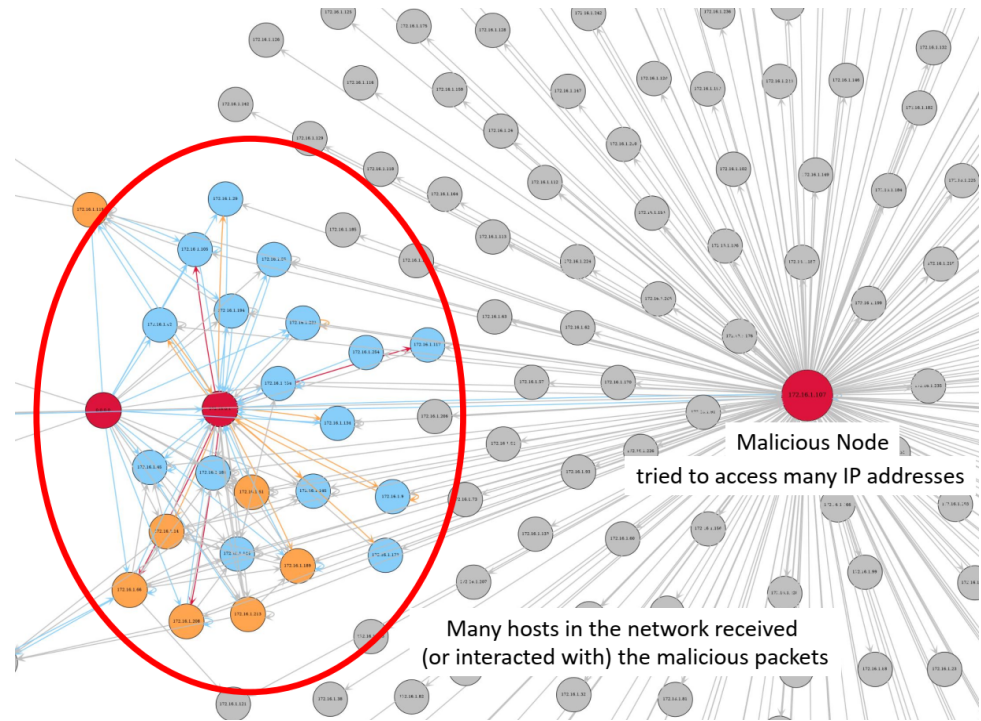
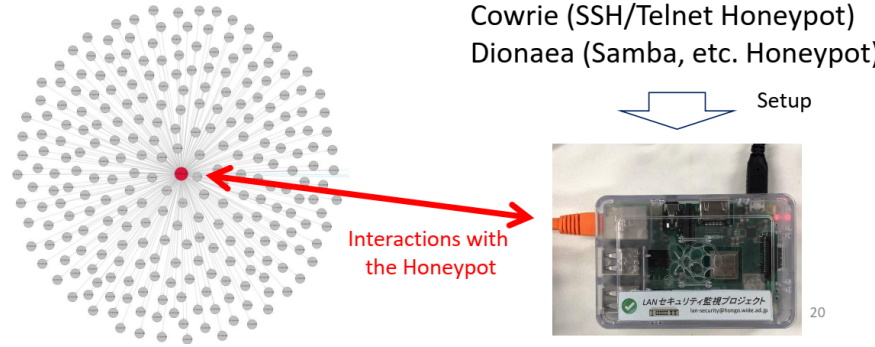


Fig 1. Visualized connection graph of a LAN. In this case, it is easier to read the node's IP addresses. However, sometimes it become too complex to read them.



Fig. 2: Monitoring node of LAN-security monitoring project



# Project Activities: On-line workshop: Preparation of Monitoring Node Deployment

*July 9<sup>th</sup>, 2020*

1. We developed a manual of installing LAN security monitoring device for ASEAN IVO Project.

## LAN-Security Monitoring Device

How to Setup for ASEAN IVO Project

Create: 2020-06-24  
Update: 2020-07-09

### Part I : Preliminary Setup

#### 1. Raspberry PI OS (Raspbian) Installation

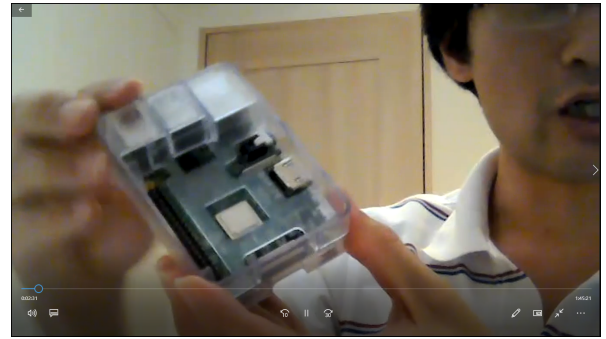
Insert microSD card into your PC.  
Download Raspberry PI Imager from <https://www.raspberrypi.org/downloads/> into your PC, and execute it for installing Raspberry PI OS into your microSD card.

Choose **Raspberry Pi OS Lite (32-bit)** - A port of Debian with **no desktop environment**



**Raspberry Pi OS Lite (32-bit)**  
A port of Debian with no desktop environment  
Released: 2020-05-27  
Online - 0.4 GB download

- 2. We setup a data collection server in June.
- 3. We had an online workshop for installation of monitoring device.




July 9<sup>th</sup>, 2020

10 pages

# Sensor nodes installation

**\* Myanmar-UIT  
(20 Nodes)**



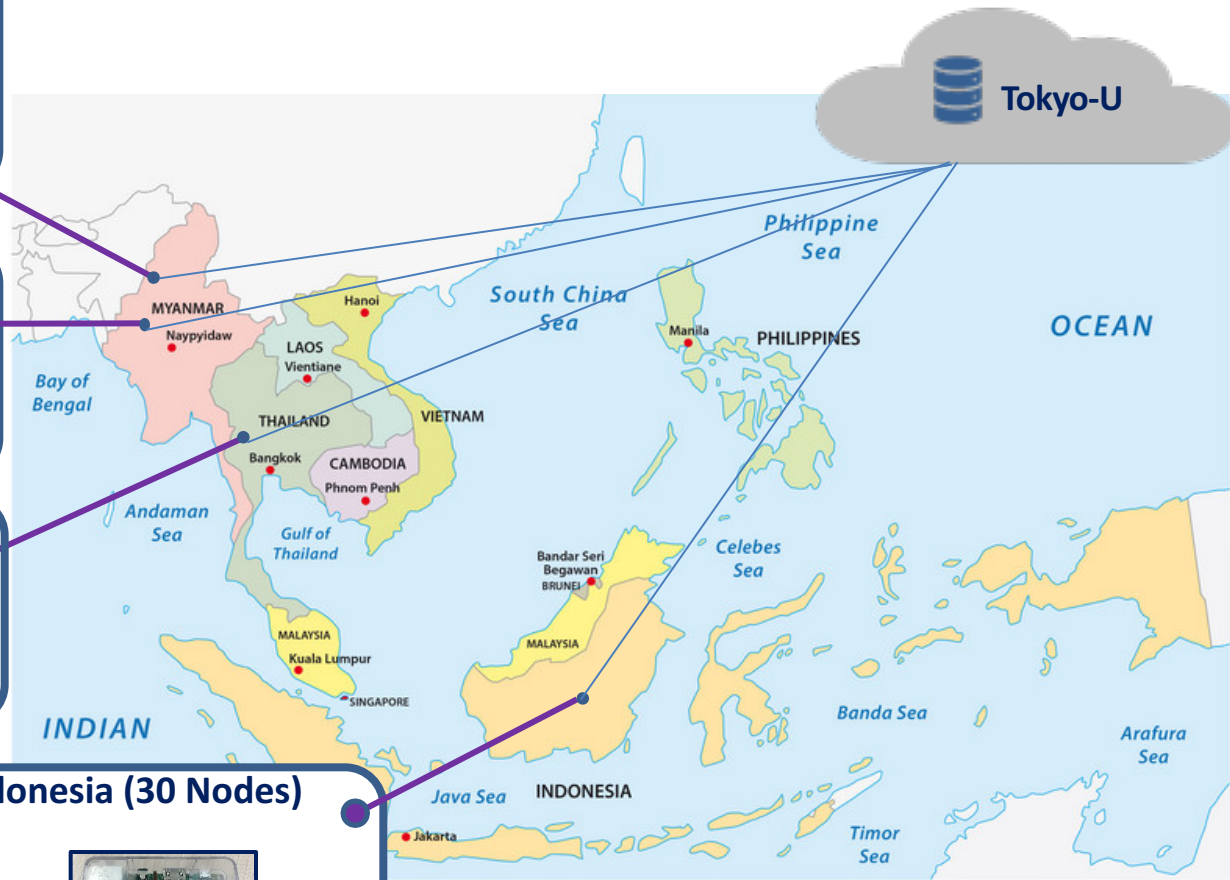
**\* Myanmar-UCSY  
(30 Nodes)**



**Thailand-PSU  
(40 Nodes)**



**Indonesia (30 Nodes)**

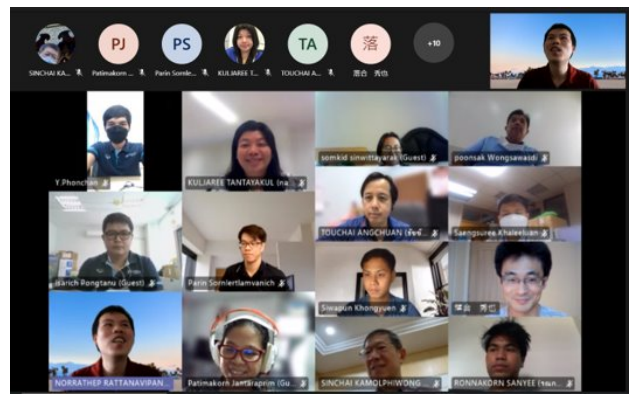


We organized an online workshop for distribution and installation of the LAN security monitoring nodes.

The screenshot shows a PowerPoint slide with the following content:

- LAN-Security Monitoring Project**
- Associate Prof. Ph.D., Hideya Ochiai (UTokyo, Japan)
- Prince of Songkla University & The University of Tokyo
- ASEAN-WIDE Cyber Security Research Testbed (NICT)
- October 1<sup>st</sup>, 2021

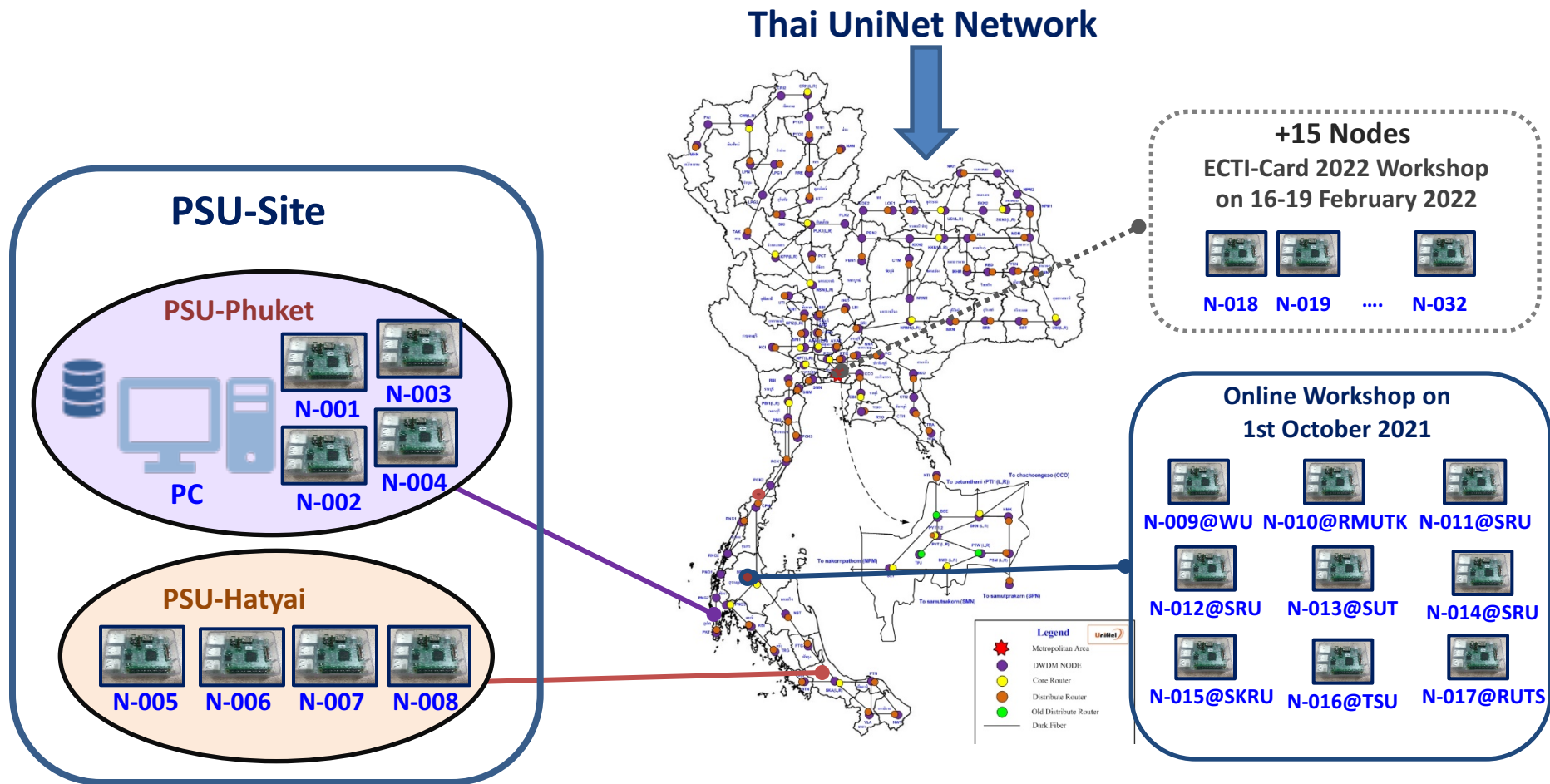
The slide features a network diagram with nodes and connections. A sidebar on the left contains a table of contents with 5 items. The bottom of the slide has a 'ノートを入力' (Enter notes) field.



10 pages



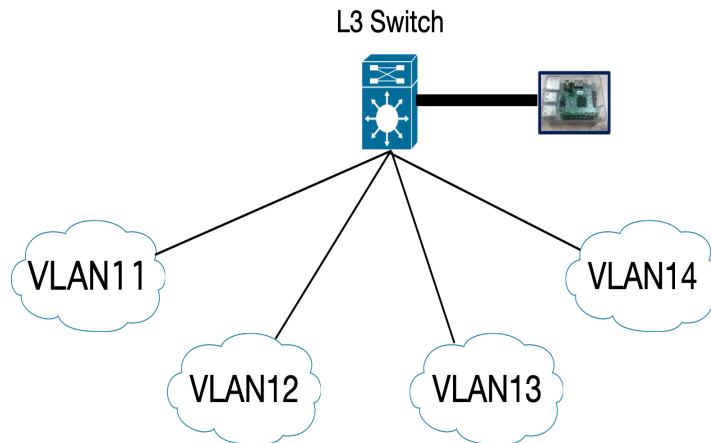
## Sensor nodes installation in 17 nodes in 9 Thai Universities



# Sensor nodes installation in Campus Network (multiple VLAN)

In order to deploy one LAN security monitoring node per one network in VLAN environment. This work propose a solution that use only one node connected to L3 switch through VLAN trunk.

Network configuration file (/etc/network/iface.d/eth0 in AIVO-node can be shown as:



```

auto lo inet loopback
iface lo inet loopback

#management vlan
auto eth0
iface eth0 inet static
    address 172.30.80.8
    netmask 255.255.255.0
    gateway 172.30.80.1

auto eth0.11
iface eth0.11 inet manual
    vlan-raw-device eth0
    address 172.30.11.8
    netmask 255.255.255.0
    
```

```

auto eth0.12
iface eth0.12 inet manual
    vlan-raw-device eth0
    address 172.30.12.8
    netmask 255.255.255.0

auto eth0.13
iface eth0.13 inet manual
    vlan-raw-device eth0
    address 172.30.13.8
    netmask 255.255.255.0

auto eth0.14
iface eth0.14 inet manual
    vlan-raw-device eth0
    address 172.30.14.8
    netmask 255.255.255.0
    
```

Please describe the R&D results in detail for your project activities from the following points of view:

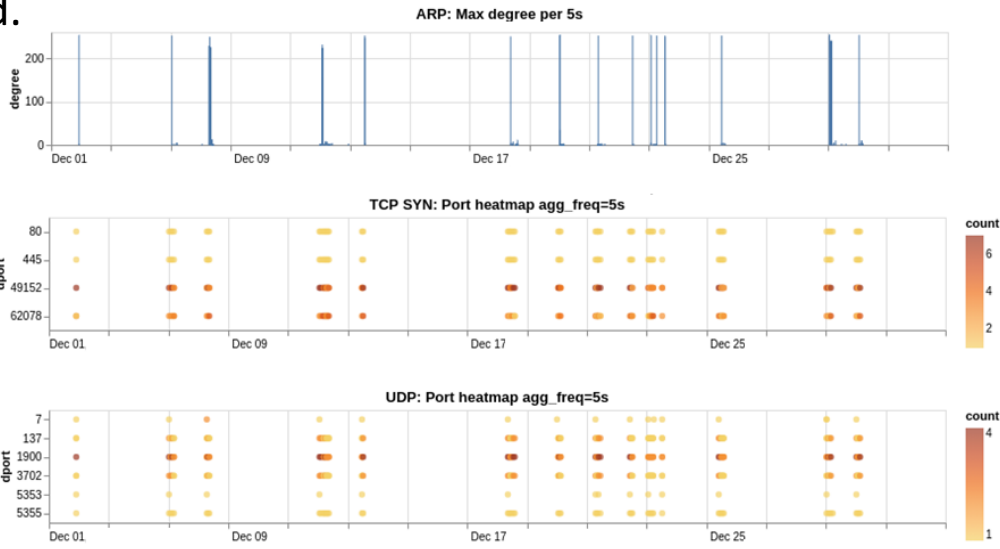
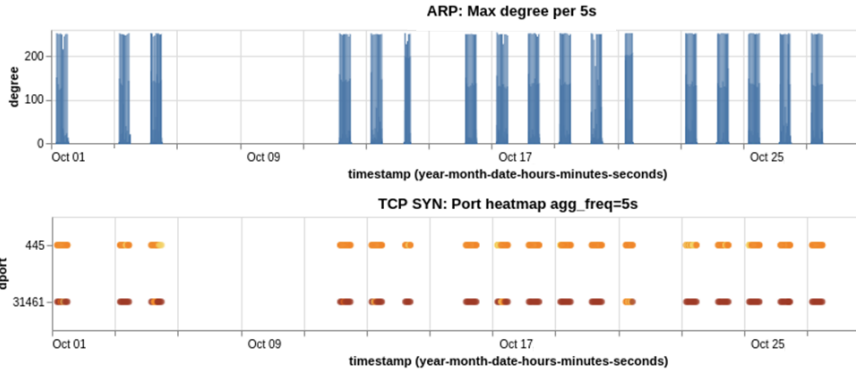
1. Scientific and technological
2. Application (or system) development
3. Experiments including field testing
4. etc.

**Note: please write what your project members did.**

# (1) Visualization of Suspicious Behavior of a Local Area Network

As the LAN's traffic is complex for normal network system operators and IoT system operators, suspicious behavior is usually invisible. We have designed a dashboard that visualizes host activities, especially suspicious cases based on the packet capture at the monitoring node. It shows how it made ARP scan, and how it accessed the monitoring node with TCP/UDPs by heat map. Through this user-interface, the system operators can check suspicious behavior and make security actions such as isolation of the node from the network if necessary. The network researchers can make further categorization using the signatures created on the dashboard.

## Suspicious Access Patterns with ARP scan and TCP port access.



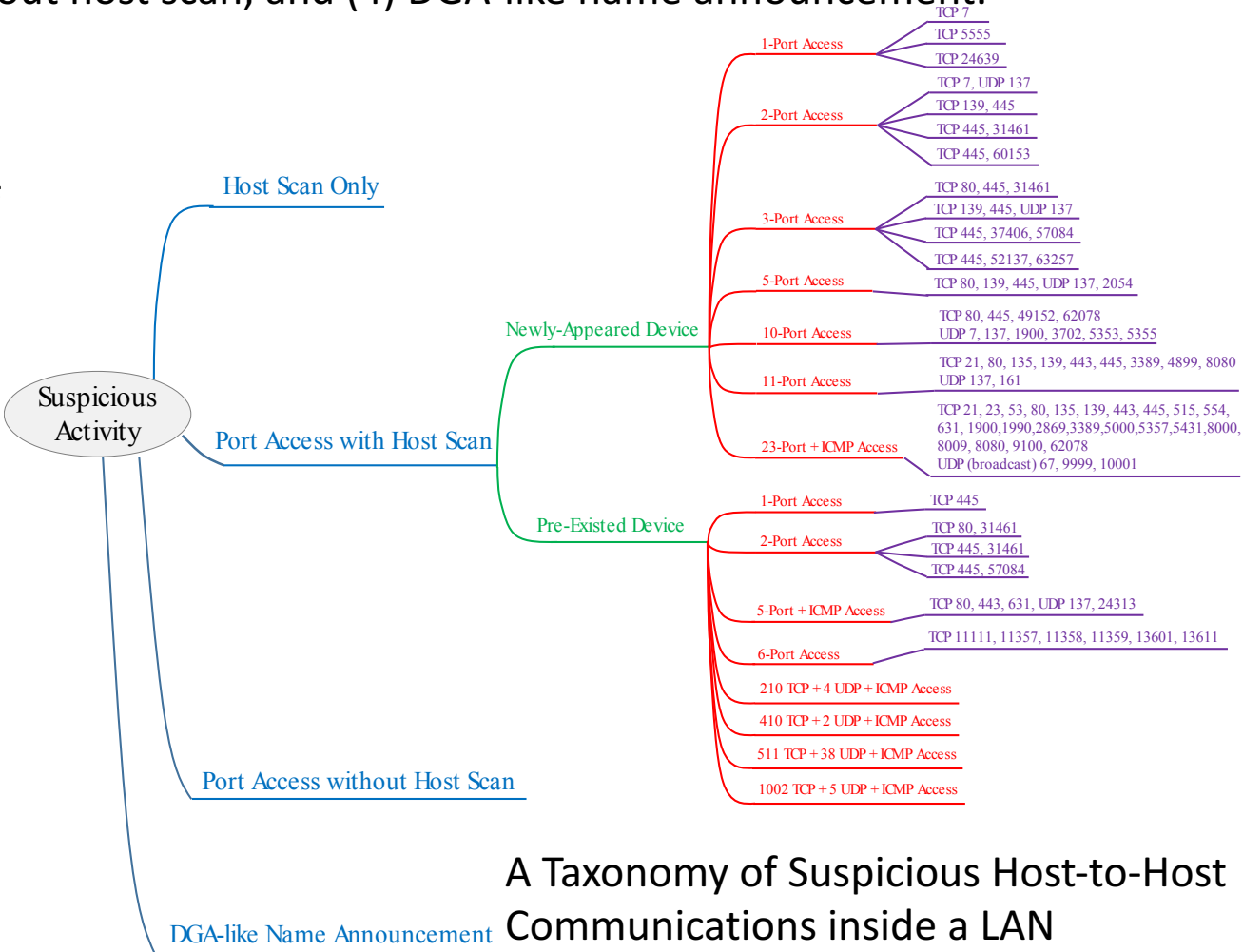
## Suspicious Access Patterns with ARP scan and TCP/UDP port access.

# (2) A Taxonomy of Suspicious Host-to-Host Communications

From the observations of port access patterns and ARP features, we drafted a taxonomy of suspicious host-to-host communications inside a local area network. We discovered that the suspicious behavior can be categorized as (1) Host Scan Only, (2) Port access with host scan, (3) Port access without host scan, and (4) DGA-like name announcement.

These suspicious behaviors can be further divided into sub categories. The edge of the categories can identify the pattern of combination accesses, which may come from the same malware.

While developing this taxonomy, we also found same suspicious activities are appeared in many local area networks.

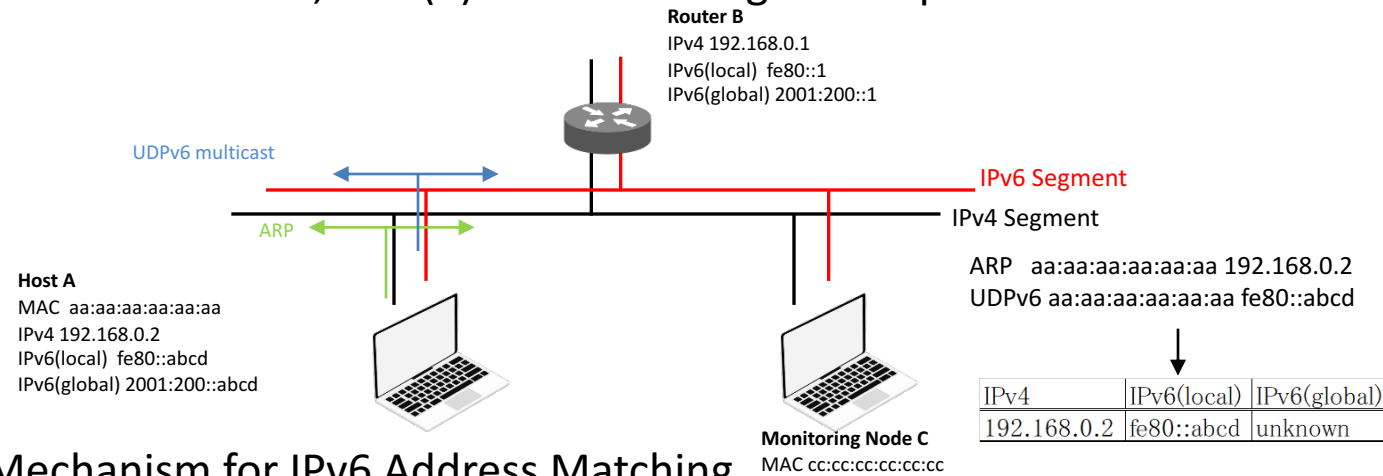


A Taxonomy of Suspicious Host-to-Host Communications inside a LAN

### (3) Traffic Redirection of IPv6 Segment for Further Analysis

In a Local Area Network, even without IPv6 network configurations, hosts joined in a LAN automatically have IPv6 link-local addresses and can make interactions between them as a peer-to-peer manner. As IPv6 channel can be a security hole (even in IPv4 only network), we have developed a traffic redirection method (1) for identifying suspicious hosts in IPv6 address domain, and (2) for monitoring the suspicious traffic.

With this method, we could find 103 IPv4-IPv6 address pairs for 155 hosts.



#### Mechanism for IPv6 Address Matching

```

MAC address      Assigned IPv4, IPv6 Addresses
a8: [redacted] :0c ['192.168. [redacted].230', 'fe80:: [redacted]:a203']
a8: [redacted] :67 ['192.168. [redacted].142', 'fe80:: [redacted]:ab15']
50: [redacted] :07 ['192.168. [redacted].48']
00: [redacted] :89 ['192.168. [redacted].157']
98: [redacted] :cb ['192.168. [redacted].203']
a0: [redacted] :25 ['192.168. [redacted].37']
b4: [redacted] :df ['192.168. [redacted].166', 'fe80:: [redacted]:71c6']
00: [redacted] :82 ['192.168. [redacted].167', 'fe80:: [redacted]:d650']
84: [redacted] :d9 ['fe80:: [redacted]:66d9']
  
```

} IPv4-IPv6 address pairs found  
 } IPv4-only hosts found  
 ← An IPv6-only host found

#### Discovered IPv4-IPv6 Pairs

# Scientific Contribution:

Please fill in the following table if your members gave presentations at an international conference or published papers in scientific journals.

**Presentations at International Conferences:**

No:	Paper title:	Author names	Affiliation	Conference name:	The date of the conference	The venue of the conference
1	Releasing ARP Data with Differential Privacy Guarantees For LAN Anomaly Detection	Norrathep Rattanavipanon, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan, Sinchai Kamolphiwong	Prince of Songkla University, Chiang Mai University, The University of Tokyo	International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)	19/05/2021	Virtual

# Scientific Contribution:

Please fill in the following table if your members gave presentations at an international conference or published papers in scientific journals.

**Published Journal Papers:**

No:	Paper title:	Author names	Affiliation	Journal name:	The publisher of the Journal	The volume number and Pages
1	Detecting Anomalous LAN Activities under Differential Privacy	Norrathep Rattana- vipano n, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan, Sinchai Kamolphiwong	Prince of Songkla University, Chiang Mai University, The University of Tokyo	Security and Communication Networks	Hindwawi	Under submission



How does our project create the social impacts:

1) We are doing hand on workshops to train and share our knowledge to people in academic networks, expect to be around a hundred of them,

We hope that our network will be expanded

2) We expect to publish 1 technical journals (submitted) by early of next year, and

3) anonymization of captured data for publicizing the data.

The finding of our project will be:

- (i) vulnerability assessment of remote local-area networks,
- (ii) visualization of data for useful security operation,
- (iii) improvement of detection algorithms and statistical analysis including the application of federated learning, and
- (iv) anonymization of captured data for publicizing the data

### 1. Scientific and Technological:

- (i) vulnerability assessment of remote local-area networks,
- (ii) improvement of detection algorithms and statistical analysis including the application of federated learning, and
- (iii) some publications and knowledge sharing

### 2. Application development

visualization of data for useful security operation,

3. We will organize a technical hand-on workshop at the ECTI CARD 2022 (<http://ecticard2022.ecticard.org>), expect to have around 15 universities participating in this workshop.



**February 17, 2022, Technical Talk session,  
Hand-on Technical Workshop@ECTI CARD 2022**

One full day hand-on technical workshop

**Chair:**

Sinchai Kamolphiwong Prince of Songkla University,Thailand, [Sinchai.k@psu.ac.th](mailto:Sinchai.k@psu.ac.th)

**Co-chair:**

Kuljaree Tantayakul Prince of Songkla University,Thailand [kuljaree.t@phuket.psu.ac.th](mailto:kuljaree.t@phuket.psu.ac.th)

**Technical Committee:**

Hideya Ochiai The University of Tokyo, Japan [ochiai@elab.ic.i.u-tokyo.ac.jp](mailto:ochiai@elab.ic.i.u-tokyo.ac.jp)

Norrathep Rattanavipanon Prince of Songkla University,Thailand,

Touchai Angchuan Prince of Songkla University,Thailand, [touch@coe.psu.ac.th](mailto:touch@coe.psu.ac.th)

Achmad Basuk i Universitas Brawijaya, Indonesia [abazh@ub.ac.id](mailto:abazh@ub.ac.id)

## *IdREN Network, Indonesia*

### **Objective:**

- To organize a technical hand-on workshop to whom will install the security device,
- To present and promote ASEAN IVO project to IdREN Network

Date: January 2022

Venue: Universitas Brawijaya, Indonesia