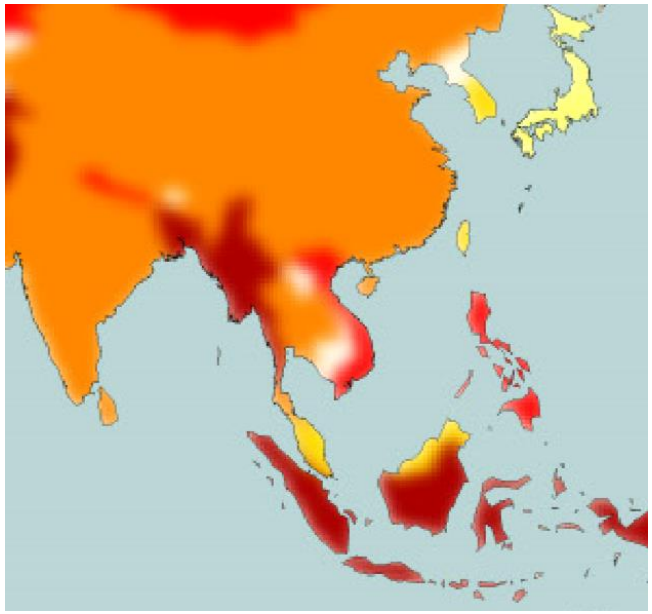
Project Title: ASEAN-Wide Cyber-Security Research Testbed

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.



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

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)

Project Title:

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
Khiev Samnang		Institute of Technology of Cambodia, Cambodia	khsam@itc.edu.kh
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: 40,000 USD

Project Title: ASEAN-Wide Cyber-Security Research Testbed

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.

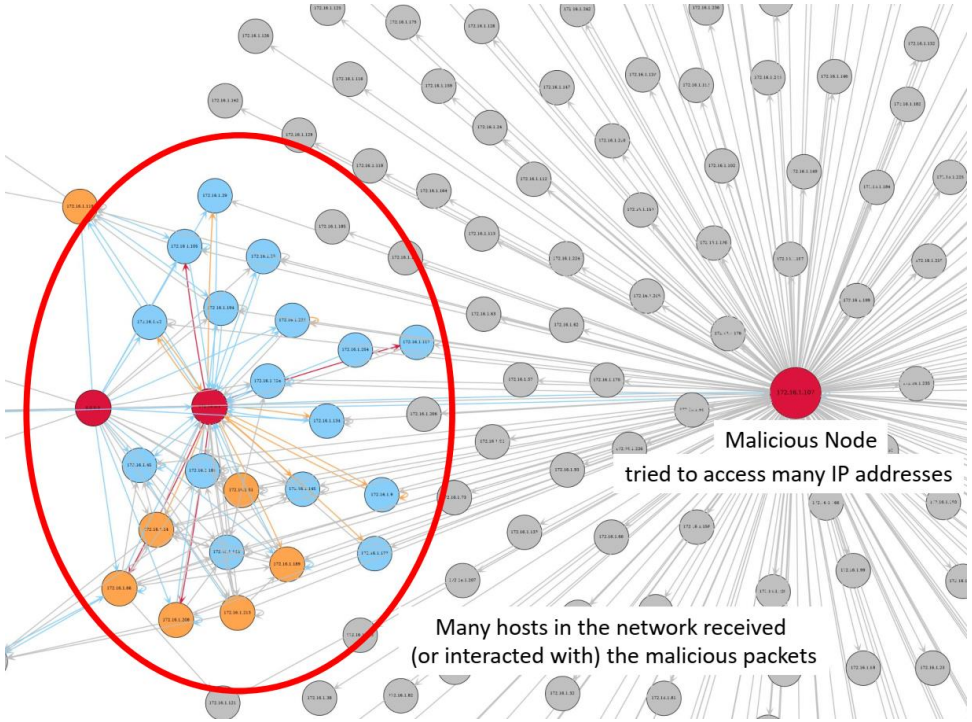
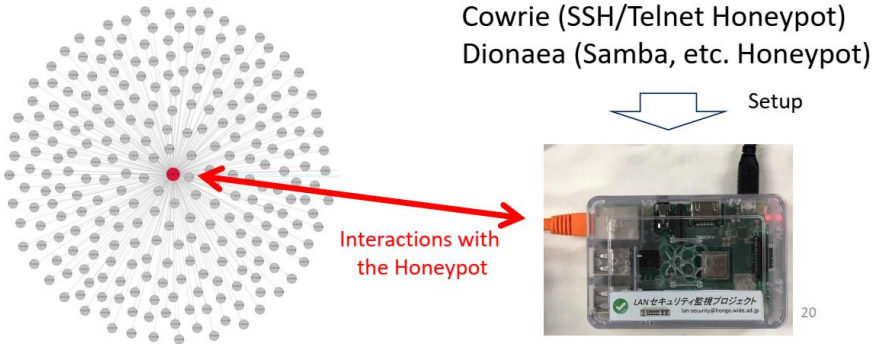


Fig 1.Visualized connection graph of a LAN. In this case, it is easier to read the node's IP addresses. However, sometimes it become too complex to read them.

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



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

July 9th, 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

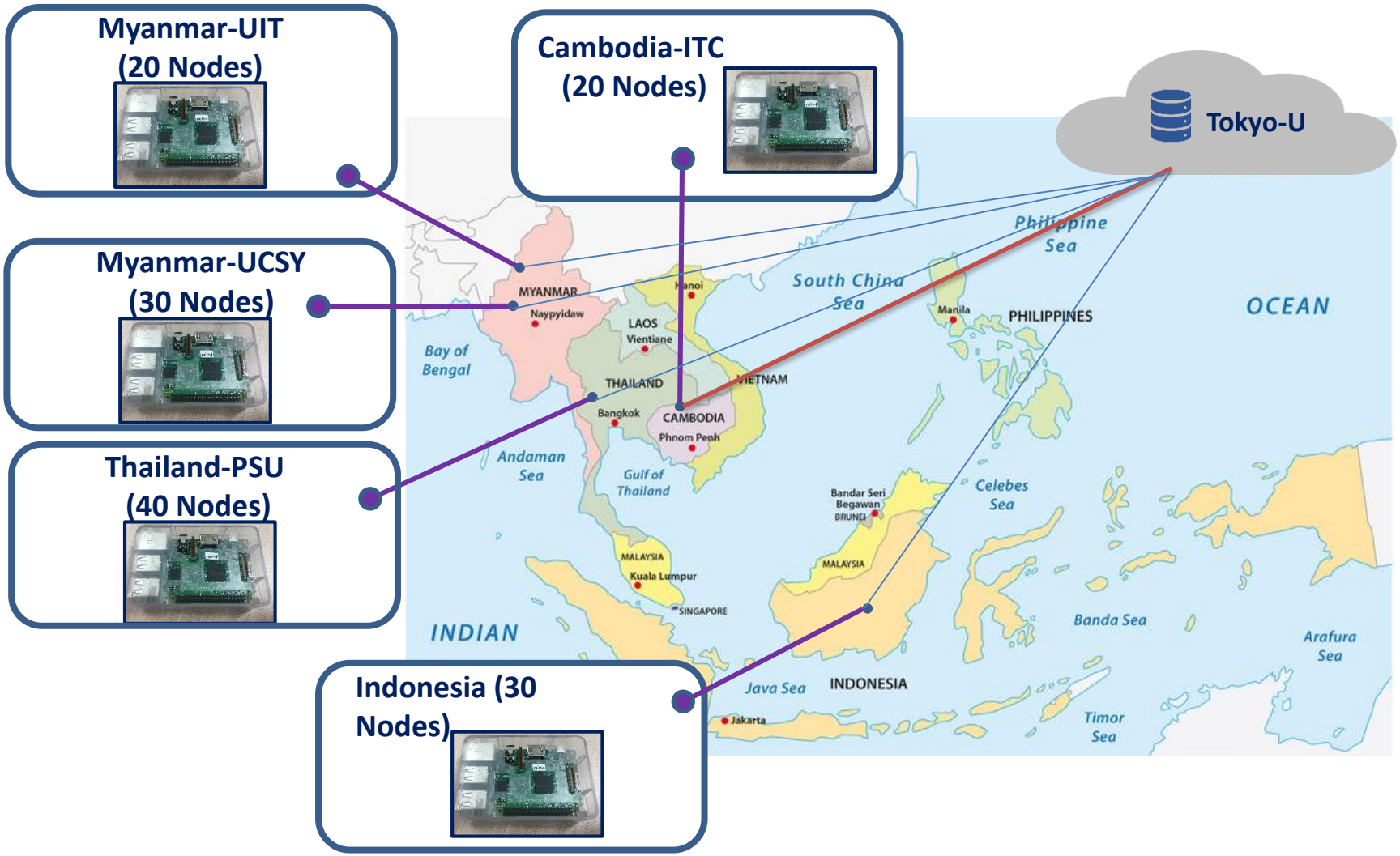
10 pages

2. We setup a data collection server in June.

3. We had an online workshop for installation of monitoring device.

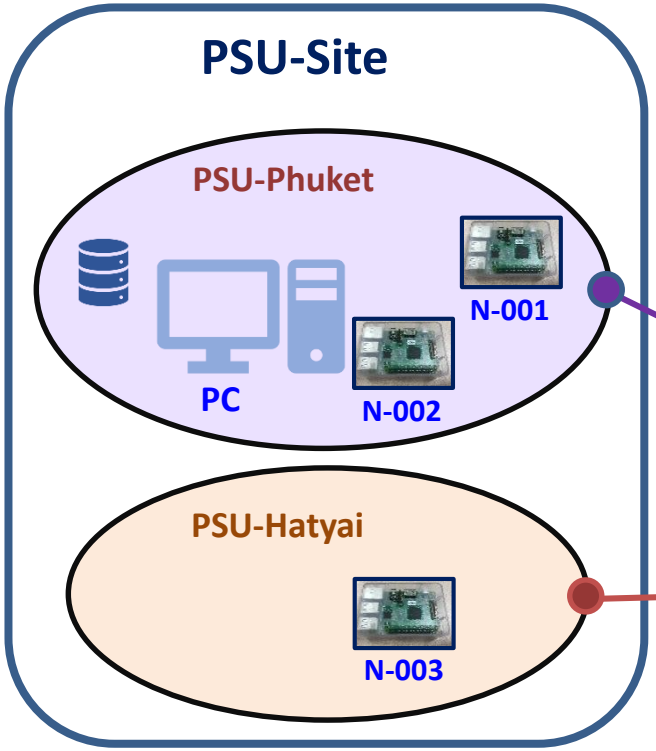
July 9th, 2020

Sensor nodes installation

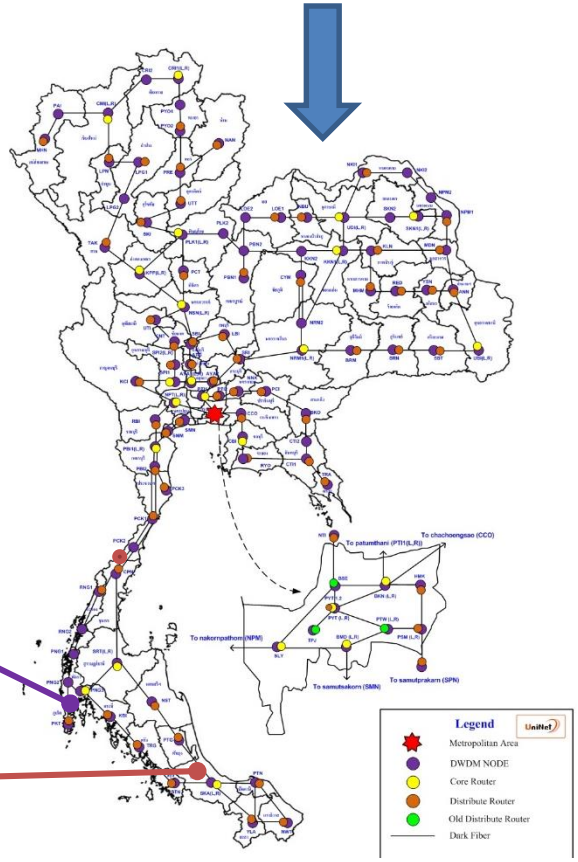


Sensor nodes installation

Sensor nodes installation in
20 Thai Universities



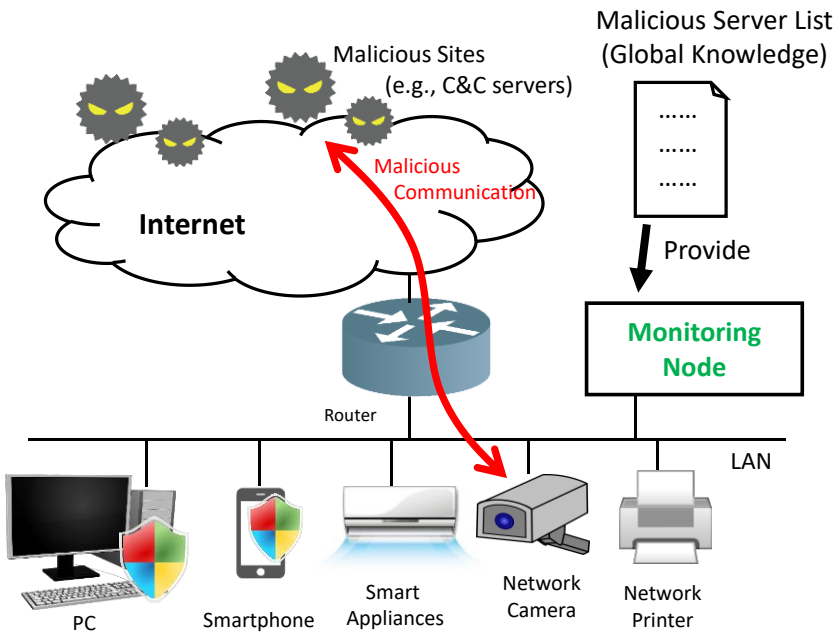
Thai UniNet Network

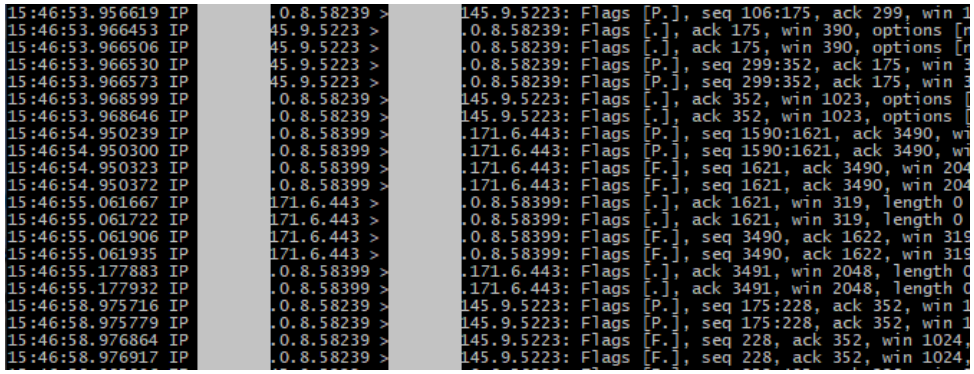


Further Analysis of Suspicious Behavior

(*) This study was made as a basic study – not conducted in the real network.

When a monitoring node detected a suspicious behavior in the local area network, this mechanism sends redirection requests to capture the main traffic from the suspicious host. By being able to capture the main traffic, the monitoring node will be able to verify that if the host is connecting to C&C servers on the Internet or not, or it can even block further communication from the suspicious host in order to mitigate the cyber-attack disasters.





```
15:46:53.956619 IP        .0.8.58239 >        145.9.5223: Flags [P.], seq 106:175, ack 299, win 1
15:46:53.966453 IP        45.9.5223 >         .0.8.58239: Flags [.], ack 175, win 390, options [n
15:46:53.966506 IP        45.9.5223 >         .0.8.58239: Flags [.], ack 175, win 390, options [n
15:46:53.966530 IP        45.9.5223 >         .0.8.58239: Flags [P.], seq 299:352, ack 175, win 3
15:46:53.966573 IP        45.9.5223 >         .0.8.58239: Flags [P.], seq 299:352, ack 175, win 3
15:46:53.968599 IP        .0.8.58239 >        145.9.5223: Flags [.], ack 352, win 1023, options [
15:46:53.968646 IP        .0.8.58239 >        145.9.5223: Flags [.], ack 352, win 1023, options [
15:46:54.950239 IP        .0.8.58399 >        .171.6.443: Flags [P.], seq 1590:1621, ack 3490, wi
15:46:54.950300 IP        .0.8.58399 >        .171.6.443: Flags [P.], seq 1590:1621, ack 3490, wi
15:46:54.950323 IP        .0.8.58399 >        .171.6.443: Flags [F.], seq 1621, ack 3490, win 204
15:46:54.950372 IP        .0.8.58399 >        .171.6.443: Flags [F.], seq 1621, ack 3490, win 204
15:46:55.061667 IP        171.6.443 >         .0.8.58399: Flags [.], ack 1621, win 319, length 0
15:46:55.061722 IP        171.6.443 >         .0.8.58399: Flags [.], ack 1621, win 319, length 0
15:46:55.061906 IP        171.6.443 >         .0.8.58399: Flags [F.], seq 3490, ack 1622, win 319
15:46:55.061935 IP        171.6.443 >         .0.8.58399: Flags [F.], seq 3490, ack 1622, win 319
15:46:55.177883 IP        .0.8.58399 >        .171.6.443: Flags [.], ack 3491, win 2048, length 0
15:46:55.177932 IP        .0.8.58399 >        .171.6.443: Flags [.], ack 3491, win 2048, length 0
15:46:58.975716 IP        .0.8.58239 >        145.9.5223: Flags [P.], seq 175:228, ack 352, win 1
15:46:58.975779 IP        .0.8.58239 >        145.9.5223: Flags [P.], seq 175:228, ack 352, win 1
15:46:58.976864 IP        .0.8.58239 >        145.9.5223: Flags [F.], seq 228, ack 352, win 1024,
15:46:58.976917 IP        .0.8.58239 >        145.9.5223: Flags [F.], seq 228, ack 352, win 1024,
```

Confirmation of the capability of traffic redirection

Societal Impact:

How does our project create the social impacts:

1) We will do hand on workshop 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 will share our research experiment results and experiences to academic forums, e.g. Thai UniNet, Indonesia IdREN (normally around some hundreds people joining these events)
3) We will organize a special session on Cyber Security in IEEE Conference (18th ECTI-CON 2021), expect to have around 10 papers presented in this session.
4) We expect to publish 2 technical journals, and 4-5 conference papers, and
5) anonymization of captured data for publicizing the data.

Conclusion:

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

Future works:

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. Experiment including field testing:

   (i) Around 140 sensor nodes installation in 4 countries,

   (ii) anonymization of captured data for publicizing the data

Future Work: Conference Special Session

Expect to submit some papers

Special Session on Cyber Security

Session Chair:

Hideya Ochiai The University of Tokyo, Japan ochiai@elab.ic.i.u-tokyo.ac.jp

Co-chair:

Kuljaree Tantayakul Prince of Songkla University,Thailand kuljaree.t@phuket.psu.ac.th

Technical Committee:

Norrathep Rattanavipanon Prince of Songkla University,Thailand,
Achmad Basuki Universitas Brawijaya, Indonesia abazh@ub.ac.id
Mie Mie Su Thwin University of Computer Studies Yangon, Myanmar, miemiesuthwinster@gmail.com
Khiev Samnang Institute of Technology of Cambodia, Cambodia, khsam@itc.edu.kh
Aung Htein Maw University of Information Technology, Myanmar ahmaw@uit.edu.mm
Touchai Angchuan Prince of Songkla University,Thailand, touch@coe.psu.ac.th

Future Work: Technical Workshop

In June 2021, ***Technical Talk session,***
Hand-on Technical Workshop@WUNCA 41st

One full day hand-on technical workshop

Chair:
Sinchai Kamolphiwong Prince of Songkla University,Thailand, Sinchai.k@psu.ac.th
Co-chair:
Kuljaree Tantayakul Prince of Songkla University,Thailand kuljaree.t@phuket.psu.ac.th
Technical Committee:
Hideya Ochiai The University of Tokyo, Japan ochiai@elab.ic.i.u-tokyo.ac.jp
Norrathep Prince of Songkla University,Thailand,
Achmad BasukRattanavipanon i Universitas Brawijaya, Indonesia abazh@ub.ac.id
Mie Mie Su Thwin University of Computer Studies Yangon, Myanmar, miemiesuthwinster@gmail.com
Khiev Samnang Institute of Technology of Cambodia, Cambodia, khsam@itc.edu.kh
Aung Htein Maw University of Information Technology, Myanmar ahmaw@uit.edu.mm
Touchai Angchuan Prince of Songkla University,Thailand, touch@coe.psu.ac.th

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: November 2021

Venue: Universitas Brawijaya, Indonesia