ASEAN-Wide Cyber-Security Research Testbed
[LAN Security Monitoring Device Technical Talks and Workshop]
Report Form

I. Organizer:

Name:	Dr.Kuljaree Tantayakul
Position:	Lecturer
Institution:	Prince of Songkla University

II. Program:

Date: 16 - 18 February 2022
Venue: Thepsatri Rajabhap University (TRU), Lopburi Province, Thailand

Program Agenda:

Day 0: Workshop preparation and setup
Day 1: 08.30-10.30 Technical talk (ASEAN IVO Project team) (1.5 hours)
Day 1: 10.30-16.00 Hand-on workshop (6.5 hours)

Schedule of the ECTI CARD 2022 workshop
"LAN Security Monitoring Device Technical Talks and Workshop"
17 February 2022

Time	Topic
08.45 - 09.15	Registration & ATK Testing
09.15 - 09.25	Opening Ceremony Assoc.Prof.Dr.Sinchai Kamolphiwong College of Computing, Prince of Songkla University
09.25 - 10.25	LAN Security Monitoring Device Assoc.Prof.Dr.Hideya Ochiai Graduate School of Information Science and Technology, The University of Tokyo, Japan
10.25 – 10.40	Practical Part - Basic Configuration of Raspberry PI - Configure Raspberry Pi for LAN security monitoring
10.45 – 11.00	Coffee/Tea Break
11.00 - 12.30	Practical Part - Basic Configuration of Raspberry PI - Configure Raspberry Pi for LAN security monitoring

12.30 - 13.30	Lunch Break
13.30 – 15.30	Practical Part - Setup a honeypot
15.30 – 15.45	Coffee/Tea Break
15.45 – 18.00	Practical Part - Setup a honeypot - Q & A

III. Participants:

No.	Name	Organization
1	Assoc.Prof.Dr.Sinchai Kamolphiwong (Organizer - Online from PSU Hatyai)	Prince of Songkla University (PSU)
2	Assoc.Prof.Dr.Hideya Ochiai (Organizer - Online from Japan)	Graduate School of Information Science and Technology, The University of Tok yo, Japan
3	Asst. Prof. Touchai Angchuan (Organizer)	Prince of Songkla University (PSU)
4	Dr. Kuljaree Tantayakul (Organizer)	Prince of Songkla University (PSU)
5	Dr.Norrathep Rattanavipanon (Organizer)	Prince of Songkla University (PSU)
6	Jirameth Puapermpoolsiri (Participant)	King Mongkut's Institute of Technology Ladkrabang
7	Jeerapat Chotsangthong (Participant)	King Mongkut's Institute of Technology Ladkrabang
8	Prateep Boonwong (Participant)	Chiang Rai Rajabhat University
9	Mr. Nattanan Yimsin (Participant)	Thepsatri Rajabhat University, Lopburi
10	Isriya Saengmuangyang (Participant)	Thepsatri Rajabhat University, Lopburi
11	Monlada Sitkham (Participant)	Thepsatri Rajabhat University, Lopburi
12	Mr. Sorawit Mitnum (Participant)	Thepsatri Rajabhat University, Lopburi
13	Mr. Raksit Cherdsawan (Participant)	Thepsatri Rajabhat University, Lopburi
14	Mr. Pongthep Thepkan (Participant)	Thepsatri Rajabhat University, Lopburi

15	Mr. Thanawat Tubtimthong (Participant)	Lopburi Technical College (LBTECH)
16	Ms. Jutatip Boonkerd (Participant)	Lopburi Technical College (LBTECH)
17	Mr. Thitipong Phuprasert (Participant)	Lopburi Technical College (LBTECH)
18	Mr. Thanakorn Phiboonphaet (Participant)	Lopburi Technical College (LBTECH)
19	Witsava Seusuwan (Participant)	Nakhon Pathom Rajabhat University
20	Mr. Asadawut (Participant: online)	Valaya Alongkorn Rajabhat University under the Royal Patronage
21	Mr. Thanakorn Chaikaew (Participant: online)	Valaya Alongkorn Rajabhat University under the Royal Patronage
22	Therdsak Mon-in (Participant: online)	Valaya Alongkorn Rajabhat University under the Royal Patronage

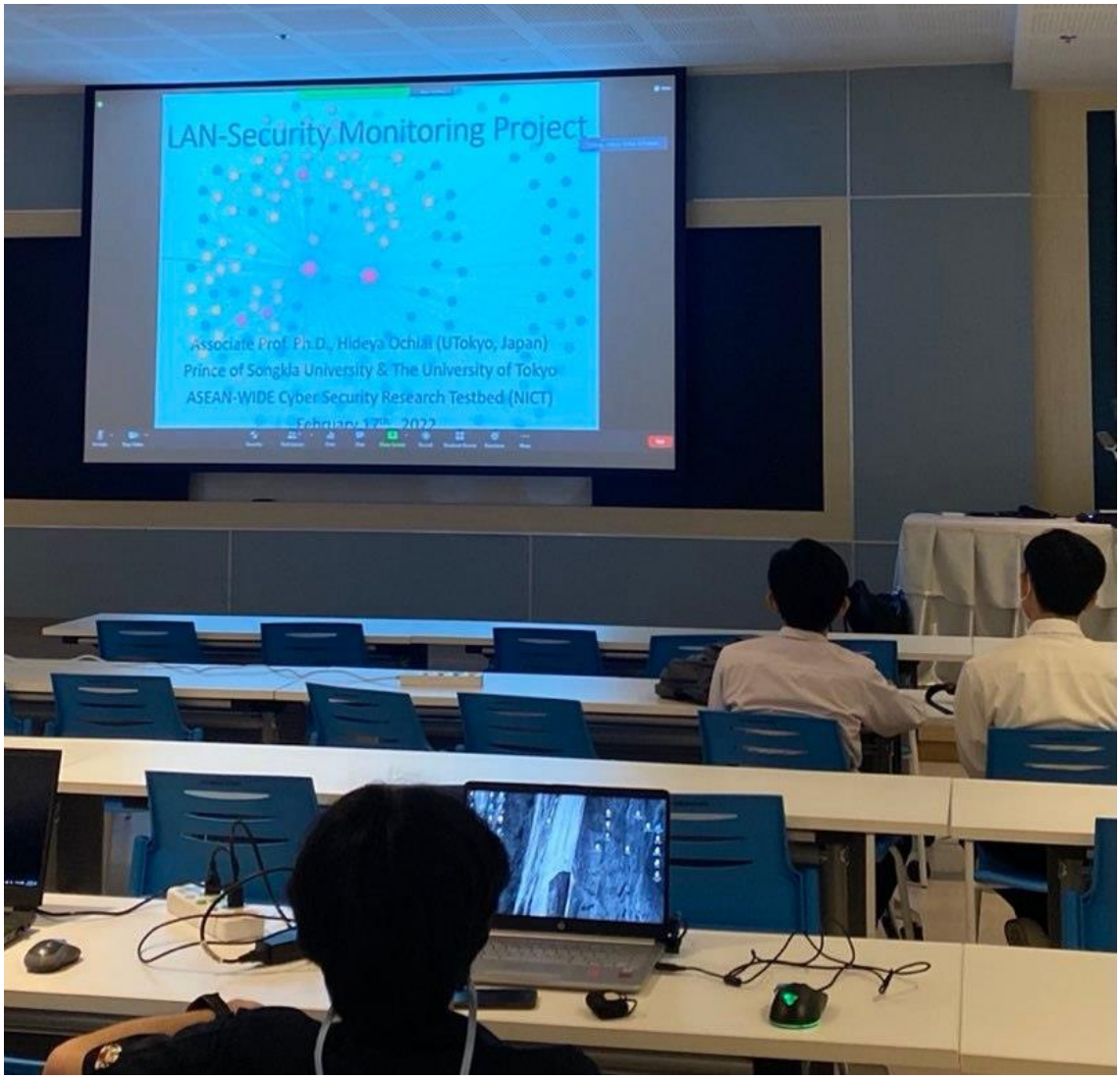
IV. Summary of the activities corresponding to the objectives

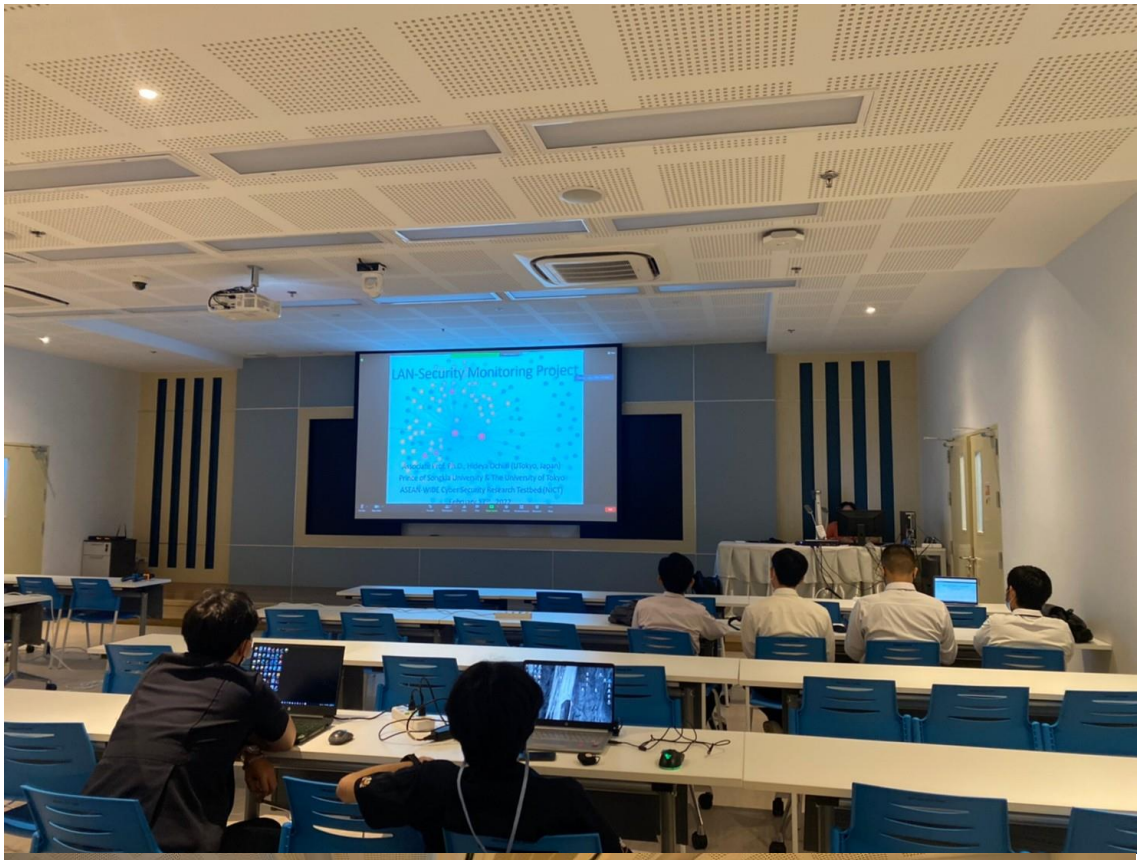
The objective of this workshop is to teach participants how to setup and install a LAN monitoring security device on Raspberry PI. We expect to have around 20 participants in this workshop and hopefully many of them will continue to use and deploy the monitoring device configured through this workshop to one of the LANs in their organizations.

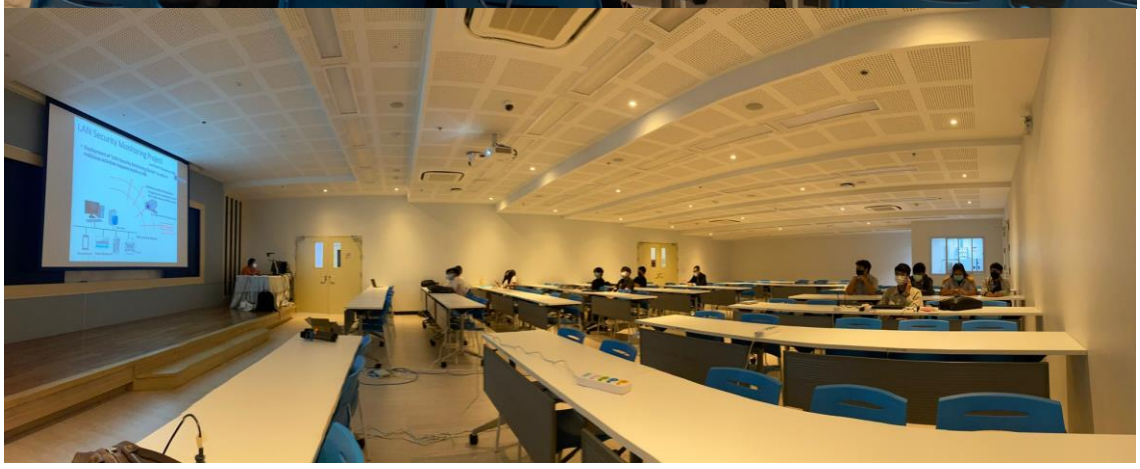
The workshop is organized in a hybrid that consists of two parts. The first part is the technical talks, given by Assoc. Prof. Sinchai Kamolphiwong and Assoc. Prof. Hideya Ochiai. It highlighted the importance of our ASEANIVO project and discussed the current status of the project. The second part – a hands-on workshop – took place at Thepsatri Rajabhat University (TRU) and online via ZOOM. It is organized and supervised by Asst. Prof. Touchai Angchuan, Dr. Kuljaree Tantayakul, and Dr. Norrathep Rattanavipanon. The second part is to teach participants how to setup and install a LAN monitoring device. In particular, we taught how to configure Raspberry PI for LAN security monitoring, how to set up a honeypot, how to utilize the captured data from the installed LAN monitoring device. Finally, we distributed the LAN security node to each participant of the institute. There are five institutes preferred to receive the LAN security node to install in their institute. Node “PSU023”, “PSU024”, “PSU026”, “PSU028”, and “PSU029” are distributed to Chiang Rai Rajabhat University, King Mongkut's Institute of Technology Ladkrabang, Lopburi Technical College (LBTECH), Thepsatri Rajabhat University Lopburi, and TOT Public Company Limited (Lopburi branch) respectively.

The workshop is started late 15 minutes for waiting for the results of the ATK test of participants. Due to Covid 19 pandemic situation, the ECTI-CARD conference’s policy requires all participants are test ATK before attending the workshop. Three participants from Valaya Alongkorn Rajabhat University under the Royal Patronage cannot join the physical workshop but can join via Zoom.

V. Others

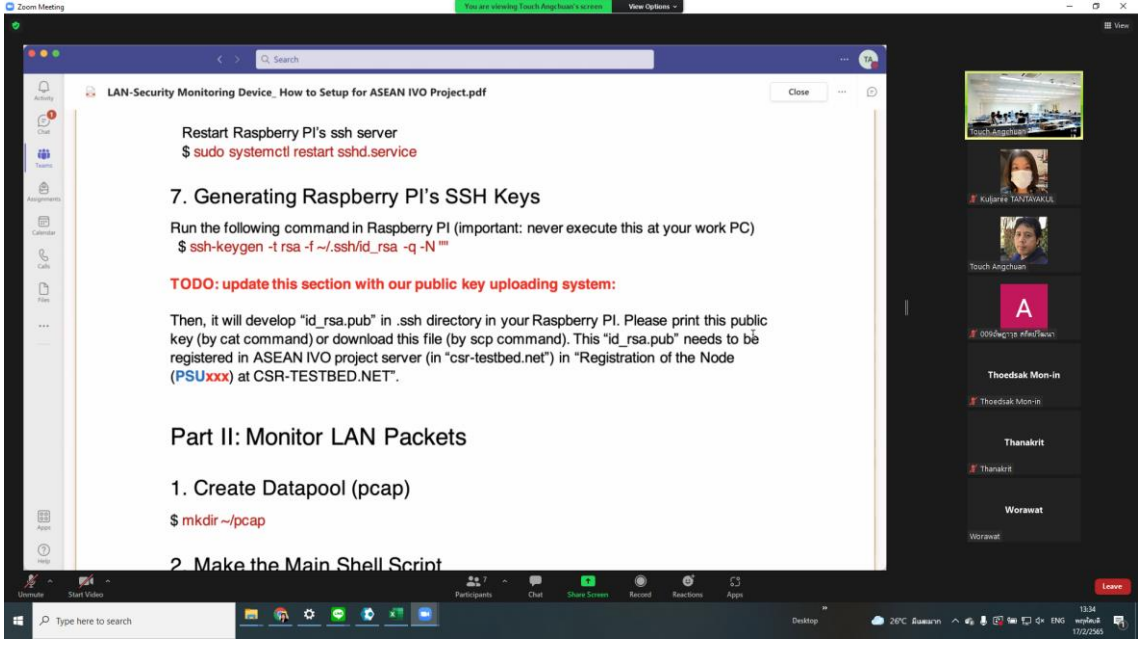

LAN-Security Monitoring Project
Associate Prof. Ph.D., Hideya Ochiai (UTokyo, Japan)
Prince of Songkla University & The University of Tokyo
ASEAN-WIDE Cyber Security Research Testbed (NICT)


LAN-Security Monitoring Project



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

ASEAN-Wide Cyber-Security Research Testbed


LAN-Security Monitoring Device_ How to Setup for ASEAN IVO Project.pdf
Restart Raspberry PI's ssh server
$ sudo systemctl restart sshd.service
7. Generating Raspberry PI's SSH Keys
Run the following command in Raspberry PI (important: never execute this at your work PC)
$ ssh-keygen -t rsa -f ~/.ssh/id_rsa -q -N ""
TODO: update this section with our public key uploading system:
Then, it will develop "id_rsa.pub" in .ssh directory in your Raspberry PI. Please print this public key (by cat command) or download this file (by scp command). This "id_rsa.pub" needs to be registered in ASEAN IVO project server (in "csr-testbed.net") in "Registration of the Node (PSUxxx) at CSR-TESTBED.NET".
Part II: Monitor LAN Packets
1. Create Datapool (pcap)
$ mkdir ~/pcap
2. Make the Main Shell Script
Thoedsak Mon-in
Thanakrit
Worawat