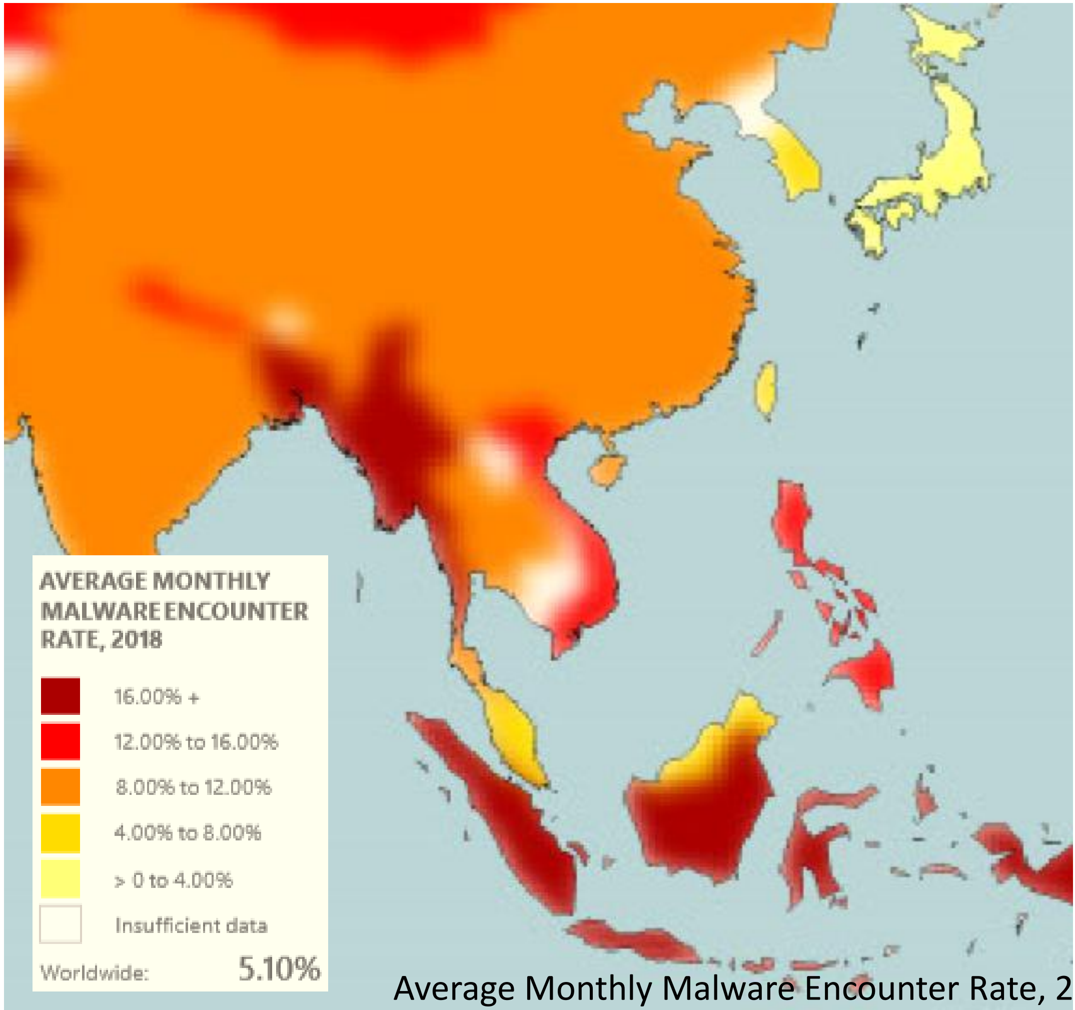
Development of LAN Monitoring Platform for Cyber-Security Data Analysis and Management

Sinchai Kamolphiwong	Achmad Basuki	Khiev Samnang	Aung Htein Maw	Hideya Ochiai
Prince of Songkla University (Thailand)	University Brawijaya (Indonesia)	Institute of Technology (Cambodia)	University of Information Technology (Myanmar)	University of Tokyo (Japan)

Development of LAN Monitoring Platform for Cyber-Security Data Analysis and Management (1/2)

Background :

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



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

Myanmar and Indonesia are ranked in the worst 5 countries in the world.
Cambodia and Laos are out of rank
(because of statistically no enough data)

Cyber-Space does not have country borders.

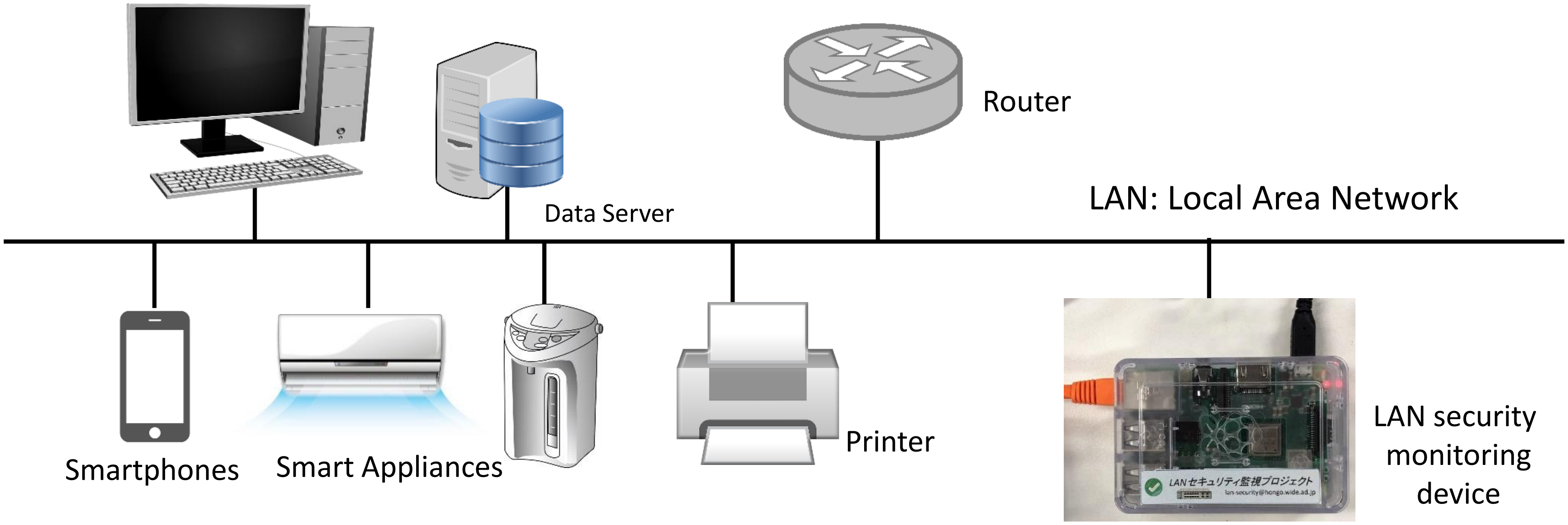
It is necessary to eliminate this situation in order to make the cyber-space safe.

Development of LAN Monitoring Platform for Cyber-Security Data Analysis and Management (1/2)

Targets: We target the security of the Local Area Networks (LAN)

Malware Intrusion into LANs :
- Malware Distribution by Phishing E-mails
- Connection of Malware-Infected Smartphones via Wi-Fi

Many Vulnerabilities in LANs :
- Smart-home devices can be easily accessed directly without authentication.
- Support-expired operating systems (Windows XP/7) are working without patches.
- Routers/Network cameras are deployed with default username/password.



Data Server

Router

LAN: Local Area Network

Smartphones

Smart Appliances

Printer

LAN security monitoring device

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

Proposed Method 1: Enhancement of Monitoring Nodes

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

Enhance the functions of LAN-security monitoring devices and programs, which are currently provided as an open source by LAN-Security Monitoring Project of the University of Tokyo.

https://www.lan-security.net/

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)

Proposed Method 2: Deployment with Network Operator Communities

Thai UniNet – Thailand Universities' Network connects 1000 academic institutions.

In January 2020, PSU will organize a workshop with UTokyo in WUNCA 40th (Forum of UniNet) for LAN-security monitoring.

Through this kind of activity, we distribute the security monitoring platform to all over ASEAN.

The data collected to the server will be anonymized and can be shared for academic research purposes as a common and open platform (if the collaborator agrees).

Impact:

This project shall explore the study of LAN-security regarding to its behavior, detection of malware, application of federated learning, anonymization of data, visualization of LAN, statistical analysis of LAN.

This project shall give opportunity for ASEAN-wide university network administrators to consider about their network security situations.

This will also give another impact to the education of university or college students. They will have a chance to learn “cyber-security consciousness”.

The anonymized data, which is allowed to share for academic purposes, can be used not only in ASEAN region, but also in all over the world including NICT, Japan – which will give great impact.

Output/Outcome:

LAN monitoring data will be anonymized and can be shared for public use if we got agree from collaborators.

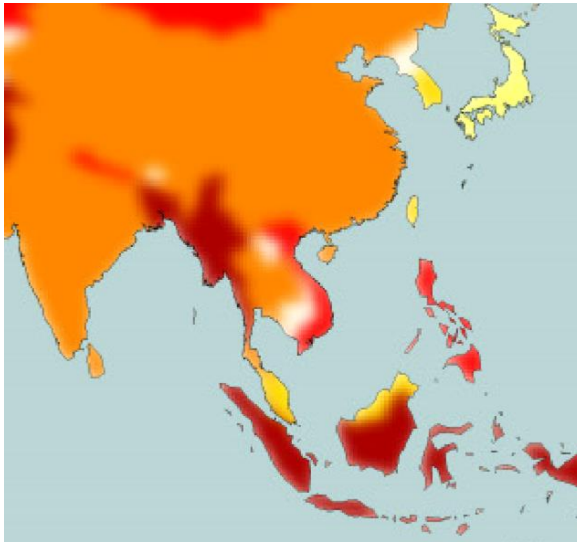
For that, we will create a good anonymization technique to get approval from them – which means useful anonymization technique.

We will give an architecture of application of federated learning for LAN-security management.

We will give a statistical overview of security situations in the universities of ASEAN region from the collected dataset.

This project will re-unite “Network Researchers and Operators” across ASEAN regions, which was actually united a decade ago.

Conclusion:



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

LANセキュリティ監視プロジェクト
lan-security@hongo.wide.ad.jp

As not a few LAN in ASEAN region have malware these days, this project target the security of the local area networks.

By enhancing the monitoring device and program provided by LAN-security monitoring project, this project will enable anonymization of monitored data, also studying the application of federated learning for malware detection.

This project will talk to many academic network operators. Through the installation of the monitoring node, they will have opportunities to consider about LAN-security.

The anonymized data, which is allowed to share for academic purposes, can be used not only in ASEAN region, but also in all over the world including NICT, Japan – which will give great impact.