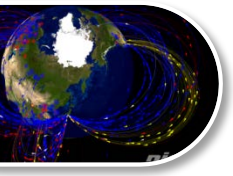
Enhancing cybersecurity with visualization, automation, and machine learning techniques

Takeshi Takahashi
Cybersecurity Laboratory
Cybersecurity Research Institute
National Institute of Information and Communications Technology (NICT)

Agenda

1. Next-gen cybersecurity empowered by visualization
2. Machine learning for automating operations
3. Adjacent topics

Research Map of Cybersecurity Laboratory in NICT



Network Incident analysis Center for Tactical Emergency Response

NICTER 1

Direct Alert Environment for Darknet And Livenet Unified Security

DAEDALUS 2

Passive

NICTER Real-network Visual ANAlyzer KAI

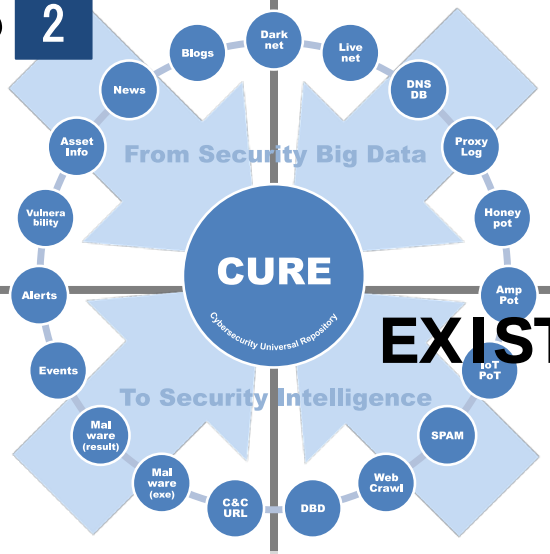
NIRVANA 改

NICTER Real-network Visual ANAlyzer KAI-II

NIRVANA 改弐

Global (indiscriminate attack)

(targeted attack) Local



EXIST

Honeypot for Amplification Attack

AmpPOT#

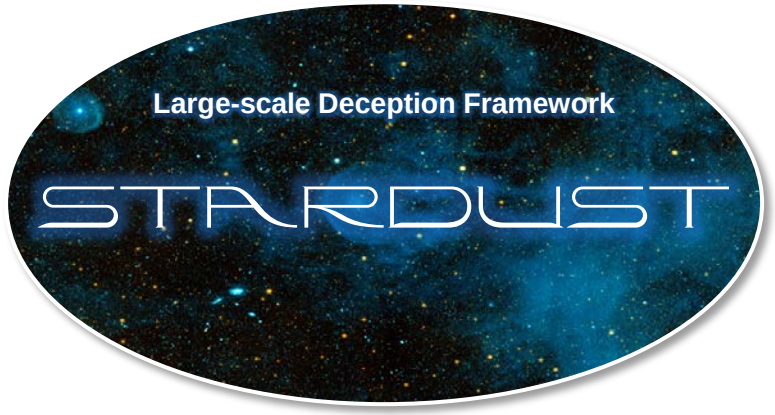
Honeypot for IoT Malware

IoTPOT#

3

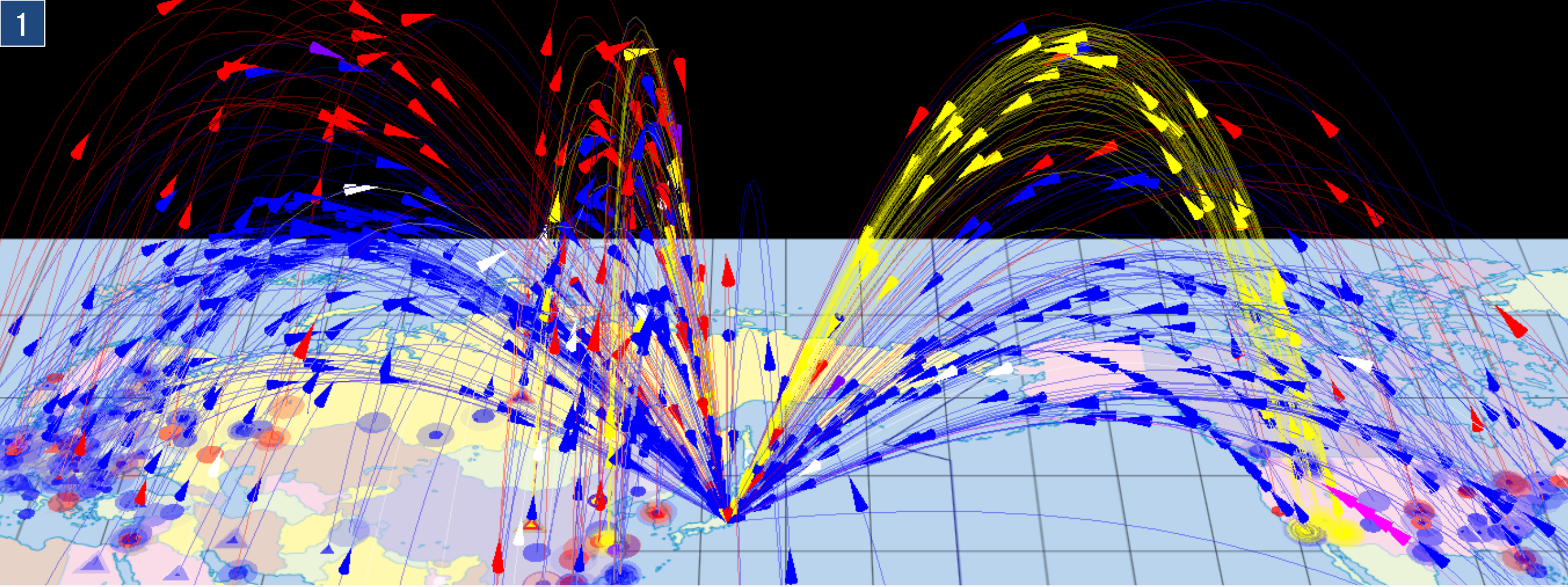
Cybersecurity Universal REpository

CURE



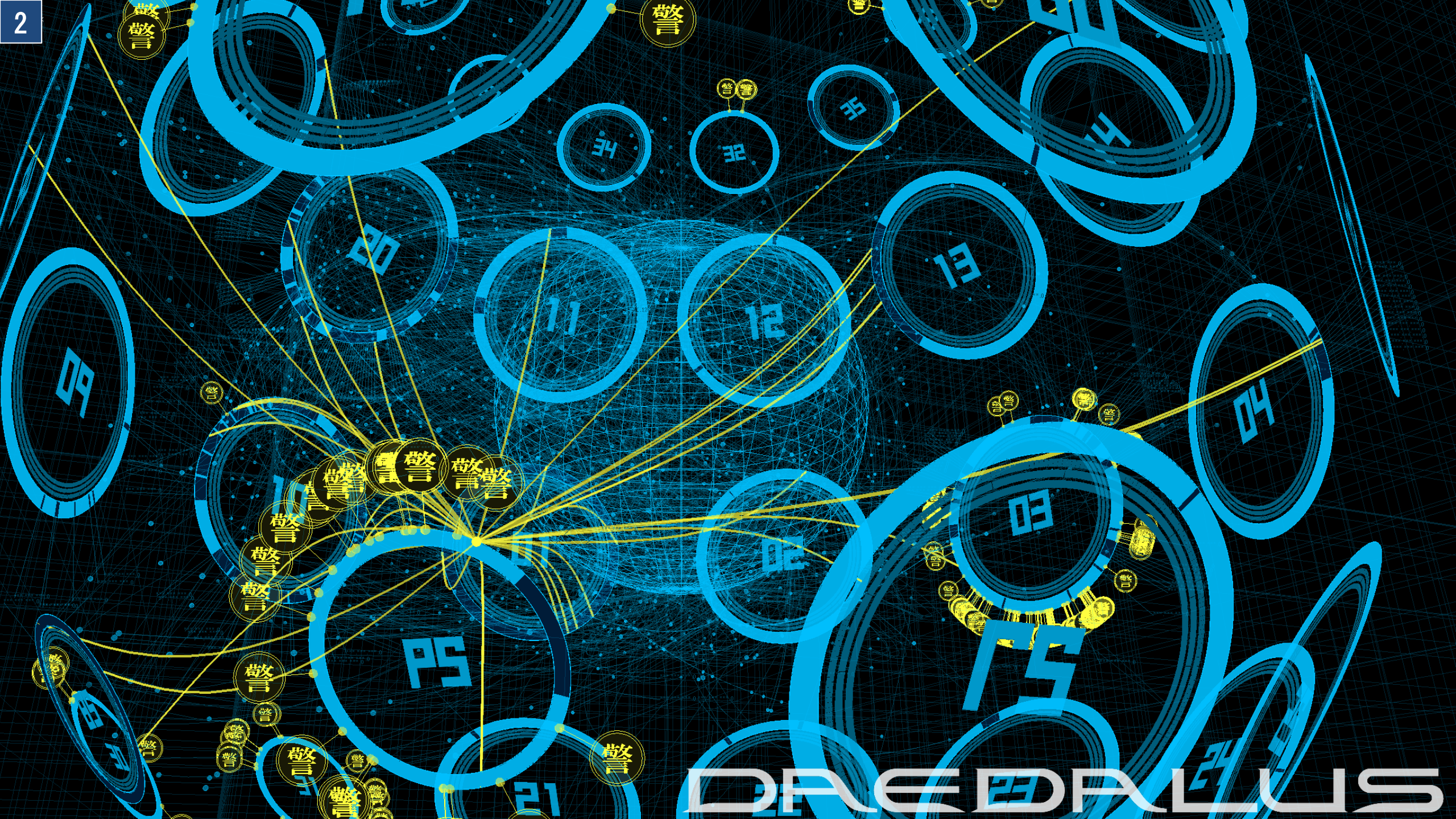
Active

Collaborative research with Yokohama National Univ. and Saarland Univ.



NICTER

- is an **integrated security system** for countering indiscriminate cyberattacks
- based on a large-scale **darknet monitoring**, an automated **malware analysis** and their **correlation**


2
DAEDALUS

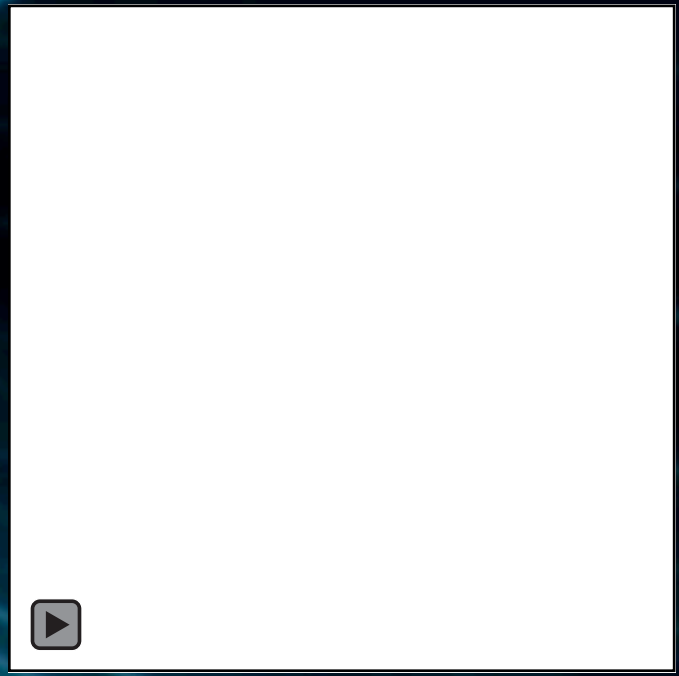
WarpDrive

Web-based Attack Response with Practical and Deployable Research InitiatiVE

- To cope with drive-by download attack, we implemented a sensor on browsers, called Tachikoma. A **Tachikoma** is a fictional walker with artificial intelligence (AI) from the Ghost in the Shell universe (Wikipedia, Jun 18, 2018)

- WarpDrive project makes Tachikoma as…
  1. **Sensor** in the browser
  2. **Actuator** to block web-based attacks
  3. **Communicator** with users

- How to motivate people to keep using the plug-in was a tough issue, but Tachikoma overcame this issue



Source: https://warpdrive-project.jp/

Agenda

1. Next-gen cybersecurity empowered by visualization
2. Machine learning for automating operations
3. Adjacent topics

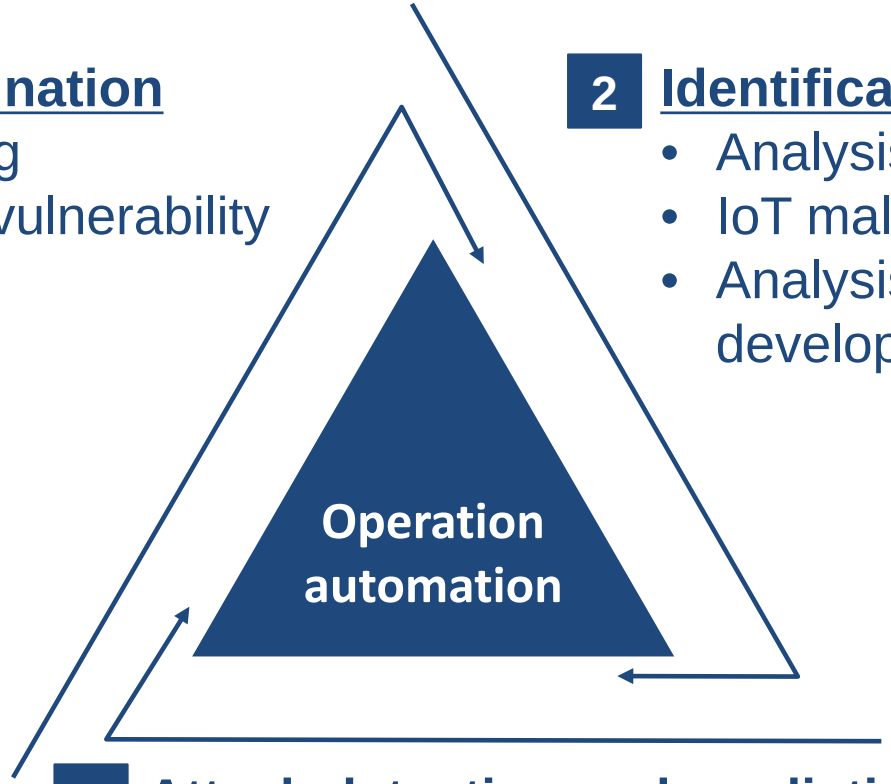
Our Research Focus

1 **Priority determination**

- Alert screening
- Evaluation of vulnerability severity

2 **Identification of malware functions**

- Analysis of Android apps and markets
- IoT malware analysis
- Analysis automation tool development



3 **Attack detection and prediction**

- Darknet analysis
- Threat estimation and prediction
- Encrypted traffic analysis

Alert Screening and Prioritization

Current process for identifying important security alert

Security/SIEM appliances

lastline

cisco

JUNIPER NETWORKS

AlaxalA

PFU a Fujitsu company

FFRI

A10

Alerts/hints
>= 800M/day

static rule filter

Some alerts may have been missed

Suspicious Alerts
~ 100/day

Manual verification filter

One expert is working for 4 ca. dedicated hours for this tedious work

True Alerts
~ 5 /day

We ***replace and streamline*** the above 2-stage filtering process (static rule + manual verification) ***with machine learning techniques.***

Android Application Vetting

- We detect malware among Android APKs (recall =99.52)
  - Features: API calls, permission requests, and app categories
  - Doc2Vec with DBoW (not CBoW) in step 2
  - Multi-layer perceptrion (MLP) in step 3

Step 1: Collect, extract, and encode features

Step 2: Reduce the feature dimension

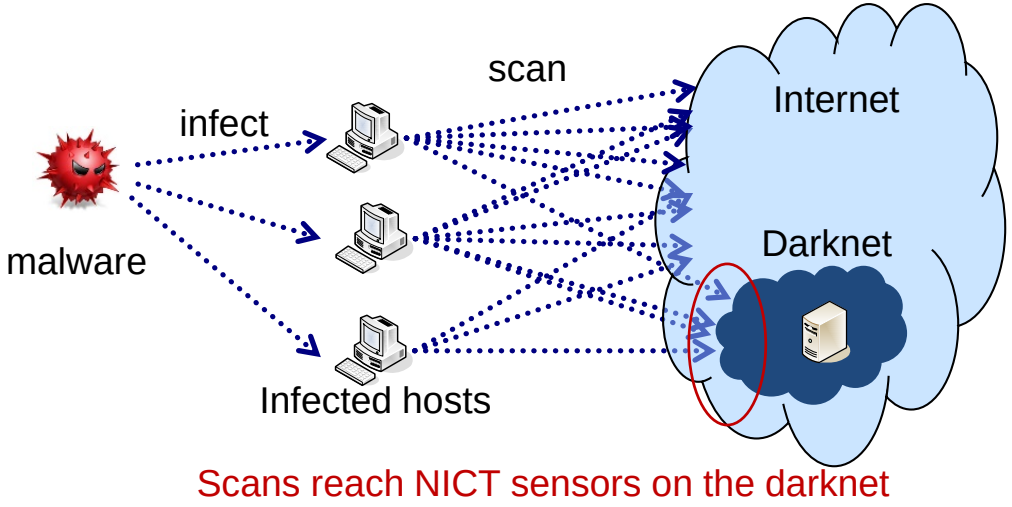
Step 3: Classify benign /malicious apps

Feature Dimension	Accuracy	Precision	Recall
500	99.7%	99.2%	99.47%
100	99.73%	99.18%	99.54%
50	99.79%	99.47%	99.52%

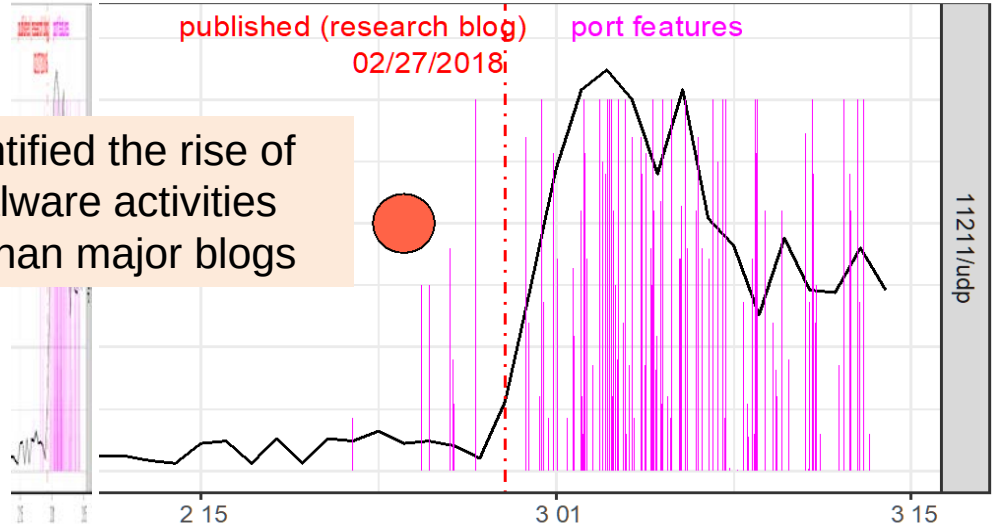
Source: B.Sun, et al., "A Scalable and Accurate Feature Representation Method for Identifying Malicious Mobile Applications," ACM SAC, 2019.

Early detection of malware activities

Objective	• Detect the rise of new (or reactivated) malware scan activities in real time, especially those that are hard to manually detect
Approaches	• Estimate the cooperativeness of the hosts sending packets to our darknet by analyzing the packets with unsupervised machine learning techniques



Scans reach NICT sensors on the darknet



A sample case of a coordinated scan detection
(x: date/time, y: number of sources)

Source: H.Kanehara et al., "Real-Time Botnet Detection Using Nonnegative Tucker Decomposition," ACM SAC, 2019.

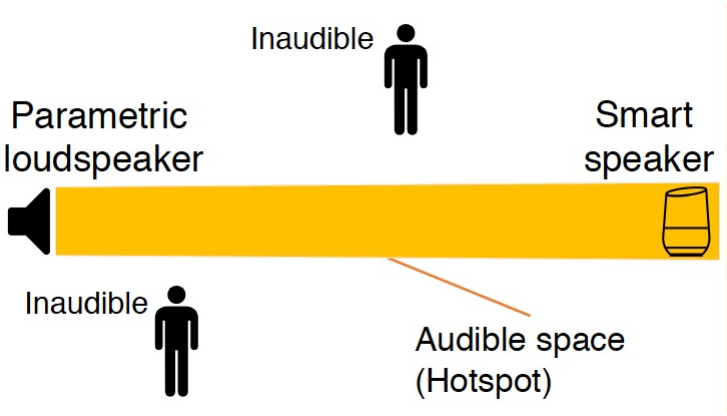
Agenda

1. Next-gen cybersecurity empowered by visualization
2. Machine learning for automating operations
3. Adjacent topics

Voice command security

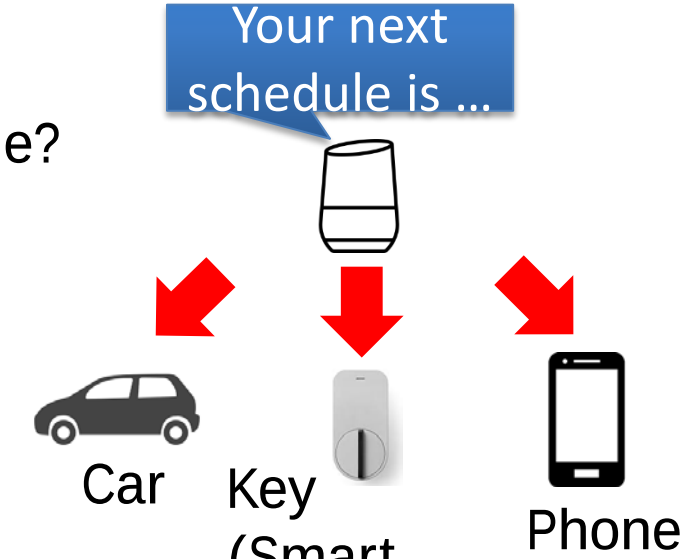
Audio Hotspot Attack

- A voice assistance system can be manipulated by illegitimate attacker without being noticed by anybody else
- We inject malicious voice commands using directional sound beams.
- Parametric loudspeaker can generate directional sound beams.



1. Privacy concerns
   ex) What's my schedule?
2. manipulating other connected devices

ex) Open the key.
Call to [someone]



Countermeasure

We made a new classifier that detects various voice attacks using 2D convolutional neural network (2DCNN).

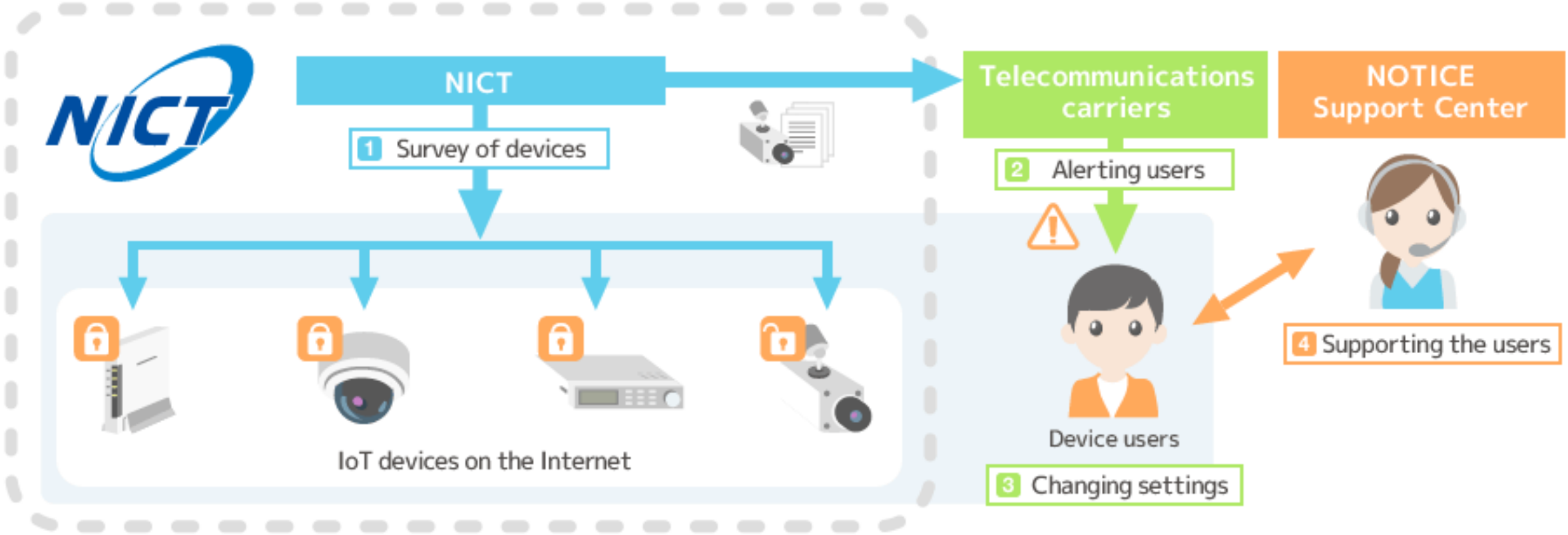
Source: R.Iijima et al., "Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams," ACM CCS poster, 2018.

Advancing current&next-gen cryptographic researches

Functional Cryptographic Technologies	Security Evaluation of Cryptographic Technologies	Privacy Enhancing Technologies
✓ Homomorphic Encryption ✓ Searchable Encryption ✓ Structure Preserving Cryptography ✓ Lightweight Cryptography ✓ IoT Security	Security Evaluation of ✓ RSA, ECC, … ✓ Pairing-based Cryptography ✓ Post-quantum Cryptography	✓ Privacy-preserving Data Analytics ✓ Risk Assessment of data anonymization ✓ Fair Privacy Policy Agreement

NOTICE (This project is outside of our institute)

- NOTICE: National Operation Towards IoT Clean Environment



The survey is to check whether the password setting in each IoT device is easily guessed, and the survey will not intrude into the device or acquire information other than that required for the survey.

Source: https://notice.go.jp/en/

Future Works

- **Next generation active monitoring**
  - ✓ Passive monitoring -> **Active monitoring**
  - ✓ **New sensor technologies** (e.g., IoTPoT and Tachikoma sensor)

- **Cybersecurity Universal Repository**
  - ✓ **Gathering and sharing** security big data
  - ✓ **Correlation** among heterogeneous data
  - ✓ Based on **international collaborations!**

- **ML/DL technologies for Cybersecurity**
  - ✓ Data mining and machine learning for security big data
  - ✓ **Automation** for monitoring, analysis and response