Information Security Laboratory

Conference
for INCS-CoE

Nov. 1st , 2016

Introduction of Security Study in Tokyo Denki University

Professor, Tokyo Denki University
Ryoichi Sasaki
sasaki@im.dendai.ac.jp

University Overview

- Tokyo Denki University(TDU) is a private university for future engineers located mainly in Adachi, Tokyo, Japan.
- Our founding spirit is “Respect for Practical Studies” .
- The predecessor of the school was founded in 1907. It was chartered as a university in 1949.

TDU and Security

Tokyo Denki University(TDU) has been making much of study and education of the security.

President of TDU
Dr. Hiroshi Yasuda

Overview of Security Education

- Tokyo Denki University launched a cyber-security education course named CySec in 2015.
- CySec is a course for Security workers and Master course students.
- It is supported by the Ministry of Education, Culture, Sports, Science and Technology (MEXT)

CySec Topics

1PF: Cyber Security Infrastructure

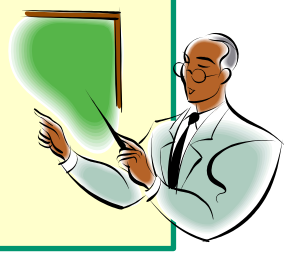
2CD: Cyber Defense Actual Exercise

3IN: Security Intelligence, Psychology, Ethics and Law

4DF: Digital Forensics

5MG: Information Security Management and Governance

6DD: Secure System Design and Development



Education Status

1. In 2015, the course was attended by 54 security field workers and 16 Master course students.
2. Security field workers were sent from police departments, financial services agencies, etc.
3. Based on post-course questionnaire results, students were highly satisfied with our lectures.

Structure of University

Tokyo Denki University

- (1) School of Engineering
- (2) School of Science and Engineering
- (3)School of Information Environment
- (4) School of Science and Technology for Future Life

Research Institute for Science and Technology

Cyber Security Institute

From September, 2013
Director : Ryoichi Sasaki

Main Security Researchers in TDU

Tokyo Denki University

President Dr. H. Yasuda

- (1) School of Engineering
  Prof. T.Saito
- (2) School of Science and Engineering
  Assistant Prof. M.Inamura
- (3)School of Information Environment
  Prof. H. Kobayashi, N. Miyaho, S. Suzuki, Y.Ueno, H.Yamaki
- (4) School of Science and Technology for Future Life
  Prof. A.Inomata, R.Sasaki, Assistant Prof. Y. Kakizaki

Research Institute for Science and Technology

Cyber Security Institute

From September, 2013
Director : Ryoichi Sasaki

Candidates of Collaborative Work

1. IT Risk management based on Risk Communication

2. Network Forensics using Artificial Intelligence

3. Disaster Recovery Technology

4. Novel Measure against Cyber Crimes and Cyber Wars

Candidates of Collaborative Work and Related Researches in TDU

1. IT Risk management based on Risk Communication
   No.1 MRC Project (Prof. R. Sasaki)*
2. Network Forensics using Artificial Intelligence
   No.2 LIFT Project (Prof. R. Sasaki, H. Yamaki)*
3. Disaster Recovery Technology
   No.3 DRT Project (Prof. N. Miyaho)*
4. Novel Measure against Cyber Crimes and Cyber Wars
   No.4 AIS Project (Prof. H. Kobayashi)

* Research at Cyber Security Institute of TDU

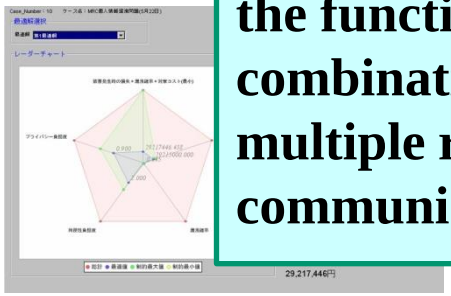
No.1 MRC Project

MRC: Multiple Risk Communicator for IT systems

Back-ground

It is difficult to select proper measures from many proposed ones.

Measure to decrease the risk creates new risks



We developed the MRC system having the function to obtain the satisfactory combination of measures considering multiple risks based on the risk communication between stakeholders.

Present

MRC was applied many actual systems. Many prizes were given to the research.

Future

Introduction of Dynamic Risk
Risk Communication including president etc.

Primary Project Members
Prof. R. Sasaki

(1) Best Paper Award of DICOMO 2010 held in Japan
(2) Best Paper Award of InfoSEC 2014 held in Malaysia, 2014 etc.

Ryoichi Sasaki," Consideration on Risk Communication for IT Systems and Development of Support Systems" (Invited Paper)Journal of Information ProcessingVo.20(2012)-4, pp814-822

Key Technology : Risk Communication, Risk Analysis, Combinatorial Optimization

Candidates of Collaborative Work and Related Researches in TDU

1. IT Risk management based on Risk Communication
   No.1 MRC Project (Prof. R. Sasaki)*
2. Network Forensics using Artificial Intelligence
   No.2 LIFT Project (Prof. R. Sasaki, H. Yamaki)*
3. Disaster Recovery Technology
   No.3 DRT Project (Prof. N. Miyaho)*
4. Novel Measure against Cyber Crimes and Cyber Wars
   No.4 AIS Project (Prof. H. Kobayashi)

* Research at Cyber Security Institute of TDU

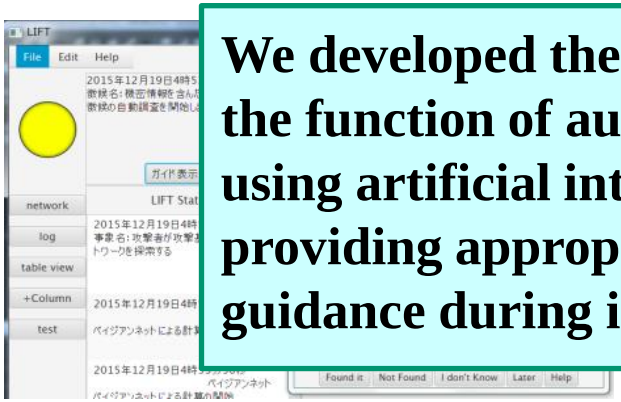
No.2 LIFT Project

LIFT: Live and Intelligent network Forensic Technologies

Back-ground

Increase of severe targeted attack

Lack of excellent operators



We developed the LIFT system having the function of automatic operation using artificial intelligence(AI) and providing appropriate actions response guidance during incidents

Present

LIFT proto program could estimate the events in all cases which occurred past

Future

We would like to estimate new type events also. ⟹ **Multi Agent Approach**

Primary Project Members
Prof. R. Sasaki
Prof. H. Yamaki
Prof. T.Uehara (Ritsumeikan University)

F. Suzuki, Young Researcher Prize in Dicomo2016

K. Hashimoto et al. "Development of intellectual networks forensic system LIFT against targeted attacks" CyberSec 2015

Key Technology : Network Forensics Bayesian Network, Multi Agent

Candidates of Collaborative Work and Related Researches in TDU

1. IT Risk management based on Risk Communication
   No.1 MRC Project (Prof. R. Sasaki)*
2. Network Forensics using Artificial Intelligence
   No.2 LIFT Project (Prof. R. Sasaki, H. Yamaki)*
3. Disaster Recovery Technology
   No.3 DRT Project (Prof. N. Miyaho)*
4. Novel Measure against Cyber Crimes and Cyber Wars
   No.4 AIS Project (Prof. H. Kobayashi)

* Research at Cyber Security Institute of TDU

No.3 Disaster Recovery Technology Project

Background

Importance of electric data storage in cyber society increases.

Objectives

- Security of private information
- Business continuity in case of a disaster occurrence

Government, Hospitals, Municipal offices, Insurance companies, Banks, etc.

Disaster

- natural disaster
- cyber terrorism
- electronic tapping (organization level)

To find out solution

How to recover the important data in the safest and in addition, economical way?

Key Technologies

Combination of (1) spatial scrambling after file data encryption, (2) fragmentation/rearrangement, and (3) distribution in random order to many clouds' resources.

Primary Project Members

Professor Dr. N. Miyaho

Professor Dr. S. Suzuki

Professor Dr. Y. Ueno

ICSNC2009, 2010 International Conference (Best paper awards)

(1) "Performance Evaluation of a Disaster Recovery System and Practical Network", IARIA Journals, vol.4, pp.130-137, Sep., 2011.

(2) "Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications", IARIA Journals, vol.3,pp.266-278, Sep., 2010.

mail to: miyaho@mail.dendai.ac.jp

Graduate School of Information Environment Technology

Candidates of Collaborative Work and Related Researches in TDU

1. IT Risk management based on Risk Communication
   No.1 MRC Project (Prof. R. Sasaki)*
2. Network Forensics using Artificial Intelligence
   No.2 LIFT Project (Prof. R. Sasaki, H. Yamaki)*
3. Disaster Recovery Technology
   No.3 DRT Project (Prof. N. Miyaho)*
4. Novel Measure against Cyber Crimes and Cyber Wars
   No.4 AIS Project (Prof. H. Kobayashi)

* Research at Cyber Security Institute of TDU

AIS Research Project for Global Cyber Security

Hiroshi KOBAYASHI, *Hirofumi* YAMAKI, *Naoki* YONEZAKI, *Hiroyuki* KIMIYAMA, *Yoichiro* UENO, *Ryoichi* SASAKI

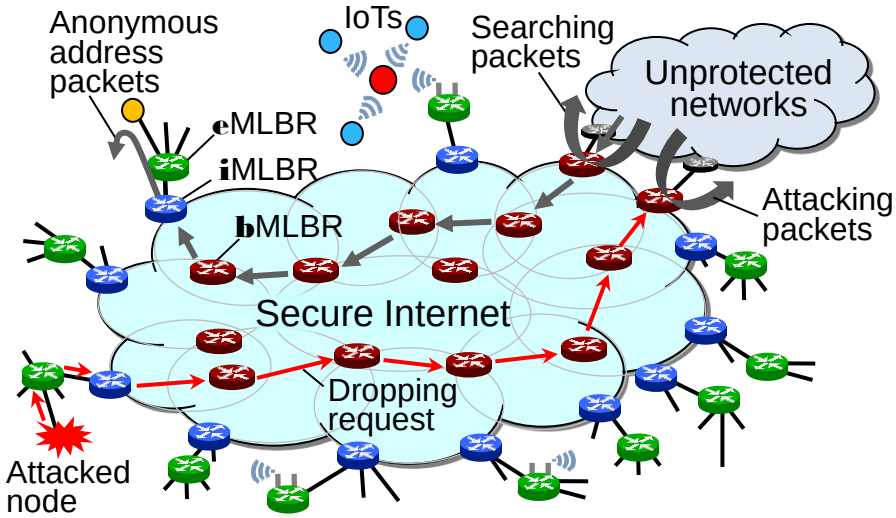
Autonomous distributed Internet security infrastructure provides the following features;

- A security infrastructure, functioning as an adaptive firewall, is constituted by our MLB (multi-layer binding) routers on user networks, at user-side edges of ISP networks and at boundaries between ISP networks.
- Spoofed packets, not listed in MLB table, are filtered so as to confine malicious packets to the reverse path.
- Malicious packets are blocked at the nearest MLBR to the source address of them by sending a dropping request to the reverse path from an attacked node.
- Security rating of every packet is performed by soft-state based authentication, quarantine and other means, and the result is stored in TOS field. Judgement of whether to receive packets is left to receivers.

As a result, the Internet involving a large amount of IoT devices will become secure against cyber crimes and cyber wars. This implies to contribute the peace of the world by non-military technologies.

Current status and future plans

- Some experiments to block attacks were performed on our security infrastructure testbed adopting OpenFlow-based MLBRs.
- Looking for R&D partners for responding to urgent needs.
- Adopt machine learning technologies for detecting malicious traffic.
- Developing wire-speed MLBRs and related appliances with highly trustable function adopting TPM.
- Apply incentive mechanism design so that ISPs and users deploy the infrastructure on their own initiative.
- Planning experiment on R&E networks such as Internet2 and SINET within two years.



mailto: hirokoba@mail.dendai.ac.jp
Graduate School of Information Environment

Candidates of Collaborative Work

1. IT Risk management based on Risk Communication
2. Network Forensics using Artificial Intelligence
3. Disaster Recovery Technology
4. Novel Measure against Cyber Crimes and Cyber Wars

We hope we can start the collaborative works.

Thank you for your attention