Report of Cybersecurity cooperation between France and Japan

Intermediate workshop: October 29 and 30, 2018

&

Satellite Meeting: October 31st
Venue: Keio University, Tokyo

1. Purpose of the Intermediate workshop

- ✓ The annual meeting of the Japanese-French cooperation on cybersecurity is held at springtime alternatively in France and in Japan. This 2 days intermediate workshop has for purpose to rapidly share and organize our cooperation on the two specific topics of cybersecurity of IoT and AI;
- ✓ In addition to the 2 days intermediate workshop, a satellite meeting (tutorials and discussions) on new issues on technology and algorithmic ethics/privacy/fairness, related to Digital/AI/ML was held on Oct. 31;
- ✓ Presentations made during the intermediate workshop can also be shared with the members who were not participating in the workshop in order to seek future topics and issues on the specific WGs.

2. Key Note Presentations

In the 2 days intermediate workshop, the following Key Note Presentations were made. All Key Note presentations interestingly provided us broader issues related to Cybersecurity with deep insights and every WGs should take them into consideration for improving the existing topics and investigating the new ideas in WGs.

A) Evolution of IoT and Cybersecurity Research in NICT (Prof. Tokuda (NICT))
B) Cybersecurity for Industry 4.0, Security Issues and Mitigation in Ethernet POWERLINK (Prof. Hervé Debar (IMT))
C) Internet Civilization (Prof. Jun Murai (Keio University))
D) A retrospective on almost 20 year of Artificial Intelligence and machine learning in Internet measurement research (Prof. Kavé Salamatian (University Annecy & Inria)).

3. Presentations related to specific WG(s)

After the Key Note presentations, several presentations were made according to the program. Presentations in the first day were basically related to IoT security and privacy and those in the second day were related to AI and Cybersecurity. The following allocation of presentations is a suggestion for WGs to further investigate new ideas or improve

existing topics presented in these talks.
It is also recommended to WGs to review all presentations.

WG1) Cryptographic Protocol Verification/Privacy by Formal Methods

- Formal Fairness in Machine Learning / Data Mining (Dr. Kamishima (AIST))

Presentation on the second day and tutorial on the third day (Algorithmic Ethics/Fairness/Privacy). This should lead to further discussions and researches on algorithmic-informatics ethics in the French and in the Japanese Groups (Claude Kirchner, Kavé Salamatian, and Mitsuhiro Okada).

WG2) Lattice-based cryptography / Post-quantum cryptography

- Towards Low Energy Ciphers for IoT (Prof. Takanori Isobe (Univ. of Hyogo))
- Towards Future-Proof, Secure IoT with Open Source Code and RIOT (Emmanuel Baccelli (Inria)) (parts related to Cryptographic primitives for IoT environment)

WG3) Events collection by sensor technologies and exchange for joint analysis of attack events with malware

- Toward the automation of cybersecurity operations using machine learning techniques (Takeshi Takahashi (NICT)) – (including how to share the captured data by NICT)
- Predicting Impending Exposure to Malicious Content by Learning User Behavior (Ayumu Kubota (KDDI Lab))
- Ransomware detection with learning techniques (David Lubicz (DGA))

NOTE

It should be noted that how to share the events and malware should be carefully considered.
It is recommended to start for sharing the small parts of sample data from both sides (F/J).
It is also recommended to start discussion on ransomware between DGA, Inria and NICT.

WG4) Countermeasure against Side Channel Attacks

- Defensive and offensive AI for embedded security (Thomas Perianin (Secure-IC))

WG5) Technologies on Sanitization, Generalization and Data Mining for privacy preservation

- A retrospective on almost 20 year of Artificial Intelligence and machine learning in Internet measurement research (Prof. Kavé Salamatian (University Annecy & Inria))

WG6) Secure IoT systems for critical services (ICS/ITS)

- Towards Future-Proof, Secure IoT with Open Source Code and RIOT (Emmanuel Baccelli (Inria))
- IoT Marketplace in Japan (Mr. Kosuke Ito (CCDS))

- VPP (Virtual Power Plant) system and IoT (Prof. Masaki Umejima (Keio Univ.))
- Introduction on systemic risks of IoT (Prof. Kavé Salamatian (University Annecy & Inria))
- 5G IoT convergence (Dr. Satoshi Konishi (KDDI))

NOTE

This WG should target secure IoT systems and we need to assign active leaders on this WG.

WG7) Virtualization, SDN security, including measurement of security performance and effectiveness

- 5G IoT convergence (Dr. Satoshi Konishi (KDDI))
- WG6 Network cybersecurity interim update: focus on IoT (Thomas Silverston (Shibaura Institute of Technology))
- Predicting Impending Exposure to Malicious Content by Learning User Behavior (Ayumu Kubota (KDDI Lab))

WG8) Cyber-norms and international cooperation on cybersecurity

The topics of this newly installed WG are in relation with the topics discussed in the third day:

- A comparative analysis of governmental AI strategies: from narrative, to utopia passing by ethics (Kavé Salamatian (University Annecy & Inria))
- Sovereignty and global risks (Stéphane Grumbach (Inria))
- Ethics and sovereignties in our digital societies (Claude Kirchner (Inria, CERNA and CCNE)) 1- Citizen consultation on Bioethics in France: The 2018 experience. 2- Recommendations of CCNE on digital and health

4. Actions for WGs and SC

Each WG is invited to consider the presentations listed in the above assignment through correspondence (emails) and/or WG conferences (virtual or F2F) and is requested to send feed back about the topics suggestions to the members of SC.

The SC should plan and draft an agenda (program) for the next F/J cybersecurity workshop.

WG leaders are invited to send propositions for talks and invited people.

5. Next F/J cybersecurity workshop (annual) : Save the date!

✧ **Dates: 2019 April 23 – 25 (for three days)**

✧ **Venue: Kyoto (Japan) (tentative- need to be confirmed)**