French-Japanese cooperation on cybersecurity

Intermediate online workshop
February 25 and 26, 2021
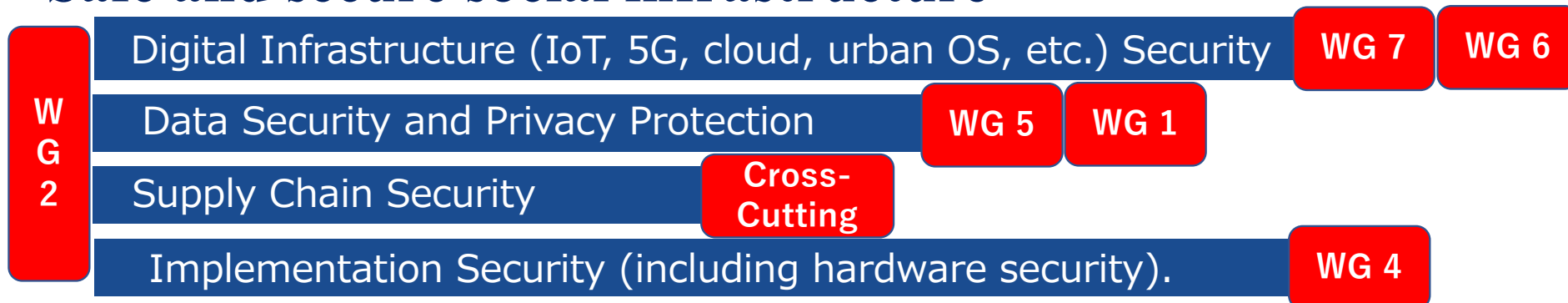
Wrap-up session

Feb. 26, 2021

In this workshop, we did have 4 wonderful invited talks in the plenary session. These PL talks can be recognized as a set of good references in this workshop for promoting our future direction of our collaborative research activities between F/J. 4 PL talks are below.

- Trustworthy Machine Learning in Cyber Security Practices

    Dr. Yufei Han (Inria, Rennes)

- Introduction of Japanese Government Current Policy for Cybersecurity Research and Development

    Mr. Mitsuyuki Ueda (NISC)

- Data Driven Cybersecurity Research

    Dr. Dai Inoue (NICT)

- Canadian and Québec approaches to contact tracing

    Prof. Sébastien Gambs (UQAM, Montreal)
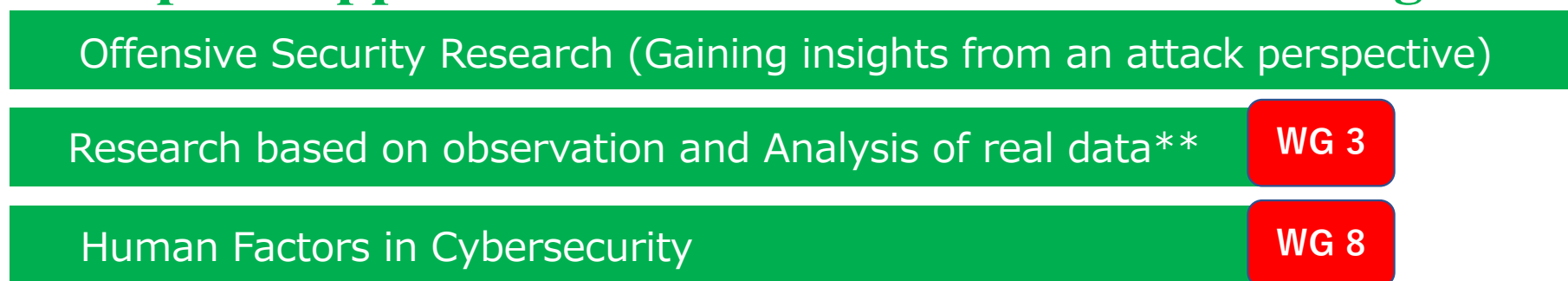
Mapping between NISC Research strategy and our WGs

Safe and secure social infrastructure

WG 2

Digital Infrastructure (IoT, 5G, cloud, urban OS, etc.) Security — **WG 7** **WG 6**

Data Security and Privacy Protection — **WG 5** **WG 1**

Supply Chain Security — **Cross-Cutting**

Implementation Security (including hardware security). — **WG 4**

Areas to be addressed for the future

AI Security — **Cross-Cutting**

Automotive Cybersecurity → Society 5.0 — **WG 6**

Pre-emptive approach to overturn attackers' advantage

Offensive Security Research (Gaining insights from an attack perspective)

Research based on observation and Analysis of real data** — **WG 3**

Human Factors in Cybersecurity — **WG 8**

Issues obtained from this workshop

➢ **Ensure Trustworthiness:**

  Security, Privacy, Safety, Resilience and Reliability

➢ **Fundamental Technologies (Crypto, Protocol Verification…)**

➢ **Threat detection, Classification, Prediction, Automation**

➢ **Utilizing AI algorithms**

➢ **How to construct a common data set/tool/system for our security/privacy research**

➢ **How to realize human resource exchanges between F/J**
  Seeking international possibility of industry-academia-public sector collaborate including how to invite experts from industry sectors

Wrap-up (1)

1. **Summary of WGs activity : WG1, 3, 4, 5, 7, 8**
   Leaders of WGs are asked to send a short report to Claude and Koji

2. **Plan to hold the next 7th F/J Cybersecurity workshop (for 3 days in hybrid mode between F2F and virtual) in France (Bordeaux). Dates for the workshop may be in September or October 2021. It was decided to invite Germany experts to the next workshop as we did in the previous workshop.**

3. **If possible, it is recommended to hold WG virtual meetings before the next 7th workshop especially for WG2 and WG6 to make appropriate preparations for the next workshop.**

Wrap-up (2)

The following issues were highlighted at the wrap-up session to be continuously considered toward the next 7th workshop:

◆In order to effectively conduct joint research between F/J, how to construct a common data set/tool/system to be used in the WG should be considered;

◆To strengthen joint research between F/J, it is recommended to promote human experts/students exchanges between F/J;

◆The following research topics should be also focused for the workshop:
- Ethical issues
- Human security (already addressed by WG8)
- Digital security for people life and society: security at home, for work, education, social interaction and culture
- Policy layer
- Education regarding Cyber Geopolitics including Geopolitical analysis

Attachment

Steering committee

Japan
- Nakao Koji <ko-nakao@nict.go.jp>
- Okada Mitsu <mitsu@abelard.flet.keio.ac.jp>
- Murai Jun <jun@wide.ad.jp>

France
- Cappé Olivier <olivier.cappe@cnrs-dir.fr>
- Kirchner Claude <claude.kirchner@inria.fr>
- Kirchner Hélène <helene.kirchner@inria.fr>
- Nguyen Phong <phong.nguyen@ens.fr>
- Salamatian Kavé <kave.salamatian@univ-savoie.fr>

Structure of WGs

- **WG1** Cryptographic Protocol Verification/Privacy by Formal Methods
- **WG2** Lattice-based cryptography / Post-quantum cryptography
- **WG3** Events collection by sensor technologies and exchange for joint analysis of attack events with malware
- **WG4** Countermeasure against Side Channel Attacks (it was "System Security and IoT)
- **WG5** Technologies on Sanitization, Generalization and Data Mining for privacy preservation
- **WG6** Secure IoT systems for critical services (ICS/ITS)
- **WG7** <Network, network security, measurement> Virtualization, SDN security, including measurement of security performance and effectiveness
- **WG8** (cyber-norms and international cooperations on cybersecurity)
- Any other WGs