Report of Cybersecurity cooperation between France and Japan

Intermediate workshop: November 4 and 5, 2019
Venue: CEA Leti, Grenoble, France

This intermediate workshop of the Japanese-French cooperation on cybersecurity held at CEA Leti in Grenoble. It has been organized by Assia Tria with the support of CEA Leti and has been attended by 25 scientists from France and Japan.
This report summarizes its main contents and outcomes.

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. In between the annual meetings, we have started to organize an intermediate workshop for two days for the purpose of rapidly sharing the latest Cybersecurity Research topics by using "invited talks" and deeply discussing specific WG's topics;
- ✓ In this intermediate workshop at Grenoble, we decided to concentrate in the discussion of WGs in more depth, together with invited talks. Unfortunately, we did not hold all WGs meeting, but WG3, WG6 and WG7 could hold the specific meeting and discussion (see Section 3).
- ✓ 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. Invited talks and Demonstration from CEA

During this intermediate workshop, the following presentations as invited talks and demonstrations from CEA were made. All Invited talks 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 list of invited talks and a demonstration are:

A) Cross-Organizational Activity for Facilitating Ethical Cybersecurity Research in Japan: Lessons from the Case Studies (Dr. Akiyama (NTTlab))
B) One Probe, Several Indicators (Pr. Jean-Louis Lanet (Inria))
C) Demonstration and visit of CEA sylver eco and smartgrid platform.
D) Environmental sensitive and evasive malware -Past and future in the IoT era- (Prof. Yoshioka (Yokohama National University))

E) A restrospective look at the issues of Huawei and cybersecurity. A cyberstrategy of large scale infrastructures (Kavé Salamatian (Université de Savoie))

3. Specific WG(s) activities (WG3, WG6 and WG7)

3.1 WG3-Events and Malware Analysis

Based on the agenda of WG3, the following presentations were made with Q&A:

- ✓ Daisuke Inoue (NICT), "Latest activities in NICTER project"
- ✓ Ryoichi Isawa (NICT), "AI and Cybersecurity"
- ✓ Mathilde Ollivier (CEA LIST), " Code obfuscation: protecting against advanced program analysis methods"
- ✓ Sylvain Cecchetto (Loria), "BOA : a CFG builder (by Basic blOck Analysis) based on system state prediction"
- ✓ Yu Tsuda (NICT), "STARDUST: a large-scale deception framework"

Summary of discussion for future activities:

- NICTER Sensor installation
  - ➢ In Inria/ Loria- Done, keep collecting events through installed NICTER sensors;
  - ➢ Telecom Sud Paris- Ongoing needs to fix installation schedule.
- IoT malware samples can be shared from Yokohama National University;
  (contact: Prof. Yoshioka (yoshioka@ynu.ac.jp))
- Promote for comparing multiple results of behavior analysis among IoT sandboxes of several research institutes (e.g. Yokohama National University and Loria);
- Researcher (student) Exchange can be encouraged for long stay in NICT headquarter in Tokyo.

3.2 WG6-Secure IoT systems for critical services

There was no specific agenda for WG6, however the following presentations were made and discussed:

- ✓ Securing IIOT and communications (Maxime Puys, CEA-Leti)
- ✓ Cyber Physical Security Framework (CPSF) by METI (Koji Nakao, NICT)
- ✓ Cybersecurity on Automotive related to IoT and 5G (submission) (Koji Nakao, NICT)
- ✓ Collaboration activity between Virtual Power Plant (VPP) initiative in Japan and F/J Cybersecurity Workshop (Prof. Umejima, Keio Univ.)

Summary of discussion for future activities:

- IIOT, ICS- share a presentation from CEA with AIST etc in Japan and get feedback or comments from them for future collaboration;
- Virtual Powerplant:

- consider cybersecurity guideline on VPP between France and Japan;
- collect latest guidelines of VPP and provide us comments mainly from France side.

- Automotive security- candidate of topic for the next workshop
- 5G (WG7)- NICT will be able to share some results of assessments of methodology in 5G environment testbed for the next workshop.

3.3 WG7-Network, network security, measurement

Summary of discussion

- VarIoT-seeking collaboration with US and Japan
- PHC Sakura-5G oriented funding-candidate of collaboration

4. Next F/J Cybersecurity Workshop and future schedule

The next workshop:

- **Dates: 2020.04.27(Mon)-29(Wed)**
- **Venue: Bordeaux [Confirmed now (December 2019)]**

During the wrap-up session, the following issues were discussed and agreed:

a) For the next F/J Cybersecurity Workshop, we should try to prepare and organize the workshop much earlier than the previous workshops so that we will be able to select appropriate topics and decide necessary actions for each WG discussion;
b) By the end of this year, we need to fix the draft program (skeleton) for the next F/J workshop;
c) WG3, WG6 and WG7 should prepare the detailed actions/topics for the next workshop based on the intermediate workshop. Leaders of other WGs should be asked for the initial proposed actions/topics for the next workshop;
d) Prepare the detailed actions based on the above input (c) to fix the program by the end of Feb. 2020 (hopefully);
e) Regarding participation of German experts to the next F/J workshop, the participants felt positive to invite them;
f) Ethical issues can be discussed at the next workshop as a single session including further re-construction of WGs.

5. Group Photo at the dinner in the first day

Appendix

Program of the Intermediate French-Japanese workshop on Cybersecurity

LETI, Grenoble France
November 4 and 5, 2019

Monday, 4th November

08:45 – 09:00 : Entry procedures
09:00 – 10:00 : Visit of the CEA-LETI Showroom
10:15 – 10:30: Welcome by **Bruno Charrat**, director of security department, Claude Kirchner and Koji Nakao
10:30 – 11:15: Key Note Talk by **Mitsuaki Akiyama (NTT)**
Cross-Organizational Activity for Facilitating Ethical Cybersecurity Research in Japan: Lessons from the Case Studies
11:30 – 12:15: Key Note Talk by **Jean-Louis Lanet (Inria)**
One Probe, Several Indicators

12:15 – 13:30: Lunch

13:30 – 15:30: Demonstration and visit of CEA sylver eco and smartgrid platform. (by Assia) (for all WGs members)
15:30 – 16:00: Coffee Break
16:00 – 17:45: WGs session (1) WG3 and WG6

Dinner: details provided on site

Tuesday, 5th November

09:30 – 10:15: Key Note Talk by **Katsunari Yoshioka (Yokohama National University)**
Environmental sensitive and evasive malware -Past and future in the IoT era.
10:15 – 11:00: Key Note Talk by **Kavé Salamatian (Université de Savoie)**
A retrospective look at the issues of Huawei and cybersecurity. A cyberstrategy of large scale infrastructures
11:00 – 12:00: WGs session (2) (WG3 together with WG7)

12:00 – 13:30: Lunch

13:30 – 15:30: WGs session (3) (WG3, WG6)
15:30 – 16:00: Coffee Break
16:00 – 16:30 Wrap-up of WGs sessions and discussion for future directions

Abstracts

Jean-Louis Lanet: One Probe, Several Indicators

Abstract: Ransomware is a class of malware designed to limit or deny users from accessing their data unless a ransom is paid. Notable attacks spread since 2012, starting with Revetons ransomware attack and lately in 2017 WannaCry, Petya and Bad Rabbit cyberattacks.

The ransomware remains a widespread problem for computer users. Research papers often focus on one characteristic to detect such an activity or they propose multiple detectors using several probes. In fact, the usability of a solution depends largely on the performance of the probes. Few papers point out the cost of the solution. We present here a probe that collects information for several detectors increasing the coverage capacity of the solution.

Statistical estimators show also their limits when the ciphering process is smart.

Keywords: Software security and malware, Ransomware, Intrusion Detection System, LSA, Machine Learning

Kavé Salamatian: A restrospective look at the issues of Huawei and cybersecurity. A cyberstrategy of large scale infrastructures

Abstract: During the past two years we have seen the emergence of major political concern about the use of Huawei as a provider of 5G technology. These concerns were fuelled by US/China trade war and more globally by the geopolitical struggle that is building up between these two major actors of the XXI century. While we can consider that a large part of the controversy is more of political issues that strictly security issues, the main question that is raised there is how countries and global actors should define their strategy in a globalized world where whatever constructor you choose the supply chain and the software quality insurance is the weakest point. This talk will make a retrospective view about the position of the different actors related to Huawei controversy, it will also discuss about the existing evidence that we have, but it would more generally discuss some more strategic questions about supply chain cybersecurity.