Minutes from the 3rd EUNITY Workshop

Introduction

Youki Kadobayashi (NAIST, coordinator of associated partners) and Gregory Blanc (IMT, coordinator of EUNITY project) welcomed the attendees and introduced the agenda of the day.

Session 1: EUNITY Project Results

The session was chaired by Gregory Blanc (IMT) and focused on delivering the outcomes of the EUNITY project with respect to research analysis, privacy and legal analysis, as well as some recommendations for jointly tackling future challenges.

Cybersecurity Research Analysis Report for the two regions

Marek Janiszewski (NASK) presented the methodology and the results of the cybersecurity research analysis between the two regions. The outcomes of this analysis has been published as Deliverable 3.1, and its revised version, Deliverable 3.2 will be released by the end of the project. The document details the results of the analysis of corpora of documents related to funding the research, to legal and policy frameworks, as well as strategy documents, to industry associations and research programmes. It highlights the most visible similarities and differences between the two regions, and serves as a basis for other deliverables of the project.

As the presentation highlighted the lack of a global cybersecurity player in Europe, NICT was concerned on how to build such a company.
EUNITY partners indicated that as desirable it may be to have a leading force in the European economy to produce homegrown security products, it may take time before a global-size company would emerge.

Cybersecurity and privacy legislation

Stefano Fantin (KUL) presented an analysis of the main differences between the European and the Japanese legal and privacy frameworks. He introduced a number of regulations from European laws that are quite specific, including the widely discussed GDPR, but also more peculiar provisions such as the adequacy decision, which seeks to find a balance between Europe and another region for exchanging private information. He also detailed a number of policy blockers that would need to be resolved for advancing the dialogue between the two regions.

The CRIC CSF was quite concerned that legal and policy staff would not be competent to make informed decisions if they were not trained about cyber crimes and privacy infringements.
An emerging issue is artificial intelligence (AI) and how justice in Europe would consider the use of algorithms. Are threats to AI integrated into cybersecurity? Are issues to AI only considered from an ethics perspective?

NAIST reinforced the argument that legal staff and policy makers should have a certain degree of knowledge about AI, so as to understand what AI can achieve and how it can lead to some threats, including possible bias in processing information.

With respect to collaboration, NICT was concerned on how they could leverage data from EU partners in the future. The EUNITY partners pointed out the adequacy decision was such tool to enable it.

Analysis of challenges and opportunities for EU-Japan cooperation

Gregory Blanc presented slides prepared by José Francisco Ruiz (ATOS) on the results of the analysis of the gaps identified between the two regions, and the recommendations of the EUNITY project to overcome the challenges identified in the two regions. At the end, the presentaton features early ideas to constitute a strategic R&I agenda for the future cooperation between Europe and Japan.

CRIC CSF was concerned that although cybersecurity awareness is gaining importance, some company CEOs are still unaware of the cybersecurity threats, in order for them to orient more investment towards cybersecurity. Europe could take example from CRIC CSF high-level conference for CEOs to alert CEOs about cybersecurity threats.

Session 2: R&D

The session was chaired by Stefano Fantin (KUL) and illustratd recent research and innovation initatives in both regions.

Towards a European Cybersecurity Competence Network: Overview of the selected pilots

Gregory Blanc (IMT) presented the 4 pilots selected for Horizon 2020 call ICT-03 to build a European Cybersecurity Competence Network. He presented in details how this Network is actually constituted with a Competence Centre as a hub and a Community to support it. He then introduced the 4 pilots.

NAIST is concerned that funding 4 pilots is money overspent if the outcomes are the same. The EUNITY partners indicated that the philosophy behind each proposal is quite different but they are indeed attempting to achieve similar goals as described in the call for proposals.
NAIST was also wondering whether there will be a single Competence Centre and Network in the end, and if some of the pilots will be merged. The EUNITY partners highlighted the fact that the 4 projects are pilots, and that a subset will be chosen by the European Commission to embody the Competence Centre at the end of a trial period.

ECSO WG6 SRIA on cybersecurity, AI and robotics

The slides prepared by Fabio Martinelli (ECSO) were presented by Christophe Kiennert (IMT). They describe the organisation and operation of the European Cyber Security Organisation (ECSO) and focused on its working group 6 that develops a strategic research and innovation agenda (SRIA) with recent interests in many emerging technologies of growing importance, such as blockchain, AI, IoT, Industry 4.0, or robotics.

The Challenges of Assisting Threats Detection, Analysis, and Response by Data-Mining Technology

Yuji Sekiya (University of Tokyo) presented the Network Muscle Learning (NML) project, funded by JST CREST, which attempts to facilitate decision making in Security Operation Centers (SOCs). The project has two main goals, one is to leverage natural language processing analysis of social data to predict threats and the other is to leverage machine learning to detect malicious behaviors and decide the first action to take to mitigate these. The project resuls were demonstrated at INTEROP Tokyo 2018.

Attendees were quite excited about the results and asked access to the datasets, which will be made available.

Enhancing cybersecurity with visualization, automation, and machine learning techniques

Takeshi Takahashi (NICT) presented a corpus of projects at NICT to enhance cybersecurity situational awareness through the analysis of data they collect. In particular, they leverage visualization to explore data and increase awareness, and machine learning to automate a number of security operations, including:

- prioritizing alerts: to replace static filter rules and manual verification;
- idenfying Android malware by using Doc2Vec and CBOW for feature reduction and then MLP for learning how to Android applications;
- detecting early and predicting cyber threats by estimating the cooperativeness of hosts sending packets to a darnet using unsupervised ML.
  He introduced CURE, a cybersecurity universal repository accumulating data from NICTER (darknet), Nirvana-kai (real network analysis), etc; and EXIST, an external information aggregation system against cyber threats.
  He also introduced the NOTICE program (National Operation Towards IoT Clean Environment) which identifies weak IoT devices by scanning them on the Japanese internet and attempting log-in with default credentials. The program then notifies the service providers that host these devices which will in turn notify the end users. The NOTICE program also provides customer support to the victims in order to secure their devices.

With respect to WarpDrive which relies on distributed agents, i.e., browser plug-ins which collect users' history, IMT raised concerns about the sensitivity of such tool on the users' privacy, and its possible lack of acceptation. NICT replied that privacy concerns were covered by a consent form, and that they designed a character to enhance the engagement of the users.

About the NOTICE program, attendees, in particular from Europe, were concerned about the legality of unauthorized access to IoT devices, even if they were not properly secured. It seems that NICT is protected by a specific law that gives them a special waiver over 5 years to conduct specific cybersecurity studies.

Since NICT is tackling similar goals by detecting malicious behaviors using ML, UT was interested in knowing the timeline between attack discovery and mitigation. In particular, it seemed that little time was available to counter the threats. NICT is conscous about the short time to react and feels that it is not possible for now. But in the future where computers will be responsible for the reaction, the time constraint will be satisfied.

Session 3: Capacity building

The session was chaired by Anna Felkner (NASK) and features presentations on topics related to education and awareness raising of different populations.

Capacity and awareness building

Anna Felkner started to introduce NASK and other European agencies' capacity and awareness building around Europe, including ENISA exercies such as Cyber Europe, CTFs such as the European Cyber Security Challenge or summer schools. She also detailed NASK invovlement with Internet providers for CSIRT operation, the participation to the Locked Shields challenge with NATO CCDCOE, CSIRT trainings at FIRST and other awareness building initiatives.

SecNumEdu: light assessment framework for cybersecurity trainings in France

Christophe Kiennert (IMT) presente the SecNumEdu initiative which aims at building a uniform yet lightweight framework to assess and label cybersecurity training programs in France. The presentation also covered trainings delivered by ANSSI itself, including the ESSI diploma and the short programs.

The Japanese audience was quite interested in knowing more about SecNumEdu and asked several questions. For example, UT wanted to know what aspects were taught in ANSSI's training (ESSI) that were not technical. IMT replied that the scope of the program was indeed broad encompassing legal, system, administration aspects among others. ESSI trainees get to acquire a broad knowledge since cybersecurity is quite a horizontal topic, promting ANSSI's training to provide courses in many domains so that trainess can connect all these aspects.

Some Japanese attendees were concerned about the ratio between theoretical and practical training, and what practical may mean as SecNumEdu may require up to 70% of practice. IMT found that the description of practical may not be so clear

in the framework but SecNumEdu does require necessary hands-on and practical exercises of security. Discussion followed on what could be the best ratio.
The training being quite broad, the Japanese attendees wondered how many people were in the teaching staff. IMT replied that outside the 6 core teachers, many other experts, both internal to ANSSI and external were sollicited to give classes.

BASE Alliance: Academic Community and Education on Blockchain

Shigeya Suzuki (Keio University) inroduced the BASE Alliance, an open discussion on blockchain's R&D, testbeds and community. It is linked to the BSafe network which focuses on testbeds. He also presented a number of challenges both in class and outside class (research projects) proposed to students from bachelor and master levels.

Attendees were impressed by the level of literacy and expertise gained by the young students involved in the program, and some suggested that policy makers could follow such programs to get up to pace with emerging technologies.

ICS-CoE training program for ICS Cybersecurity

Youki Kadobayashi (NAIST) presented the ICS-CoE training, which is a one-year full training program that aims at upbringing the next generation of CISOs in critical infrastructure operating companies. He also presented some facilities built in downtown Tokyo to emulate real critical infrastructure control systems that will put trainees in realistic conditions for incident response exercises.

NICT was amazed by the quality of the program and was interested of its cost for companies sending trainees to the program. NAIST replied that the cost for one trainee is 3 million yens to the company, which is quite cheap all things considered.

NICT was interested in running CTFs on the emulated control systems but NAIST was concerned that the goal of such competitions was divergent from ICS-CoE's. In particular, it is well known that these systems are vulnerable, so such vulnerabilities should not be easily disclosed outside.

Session 4: Future collaborations

The 3rd EUNITY workshop was concluded by a session on future collaborations where EUNITY partners, their associated Japanese partners, and attendees from industry, government and academia were all invited to discuss topics of future collaborations. In particular, Gregory Blanc (IMT) proposed a number of topics with respect to resarch and innovation and capacity building.

Among these, were discussed:

- an Erasmus Mundus Joint Master Degree on Cybersecurity between Europe and Japan, with IMT leading the effort. NAIST, JAIST and possibly UT expressed interest.
- a Marie Sklodowska-Curie Action R&I Staff Exchange was proposed by IMT on the topic of IoT cybersecurity. Proposal lengths are 40 pages long but it needs a lot of preparation ahead of time to establish how the project goals will be fulfilled through the secondments. JAIST expressed interest. NICT also proposed to extend the NOTICE program through such framework. NAIST indicated that Third Countries (TCs) benefitting from such framework could be in Asia outside Japan and in Africa, as many students of NAIST are from these countries.
- JAIST proposed that EUNITY be pursued beyond the end of the project as an independent body, as the form was not known yet. The dialogue should be continued in one form or another, at least by maintaining the mailing-list and opening it to other partners.
- DRS02 call was presented by IMT on developing technologies for first responders. This call actually involves TCs from the Forum for First Responders. Japanese partners could be funded in this call. UT expressed interest in developing secure user interfaces for first responders.
- NAIST proposed that EUNITY partners and their Japanese associated partners continue their analysis work and inform policy makers on AI and cybersecurity. Critical reviews could be written on emerging technologies, their limitations, and pitfalls. Topics such as AI, or the blockchain could be treated to make policy makers understand their adequacy or appropriateness. EUNITY could evolve into a sanity dialogue.
- Some attendees suggested that Olympic games related topics could involve both French (and European) and Japanese partners with the transition from Tokyo 2020 to Paris 2024.