French-Japanese cooperation on cybersecurity
https://project.inria.fr/FranceJapanICST

Intermediate online workshop
February 25 and 26, 2021

February 25 (Thursday), 9:30-12:30 CET and 17:30-20:30 JST
Main session program

CET France	JST Japan	

09:30-09:45	17:30-17:45	- Opening: Claude Kirchner, Hélène Kirchner, Koji Nakao, Mitsuhiro Okada, Kavé Salamatian
		- Welcome openings:
		  - Cécile Vigouroux (Inria)
		  - Sandrine Maximilien (French embassy)
		- Welcome address:
		  - Jun Murai (Keio University)

09:45-10:15	17:45-18:15	Trustworthy Machine Learning in Cyber Security Practices Yufei Han (Inria, Rennes)
10:15-10:45	18:15-18:45	Introduction of Japanese Government Current Policy for Cybersecurity Research and Development Ueda (NISC)
10:45-11:00	18:45-19:00	Discussion (Chair: Claude Kirchner and Koji Nakao)
11:00-11:10	19:00-19:10	Break
11:10-12:30	19:10-20:30	**Breakout sessions for WGs** (detailed program below) **WG3** — Chairs, Dai Inoue and Jean-Yves Marion **WG5** — Chairs, Hiroaki Kikuchi and Sébastien Gambs **WG8** — Chairs, Didier Danet, Kavé Salamatian and Motohito Tsuchiya

February 25 (Thursday),
Working groups programs 11:10-12:30 CET and 19:10-20:30 JST

CET France	JST Japan	WG3 Events and Malware Analysis
11:10-11:30	19:10-19:30	Tracing and Analyzing Web Access Paths Based on User-Side Data Collection: How Do Users Reach Malicious URLs? Takeshi Takahashi (Research manager of Cybersecurity Laboratory, NICT)
11:30 11:50	19:30-19:50	Compiler and optimization-level recognition using graph neural network Sébastien Bardin (CEA List), Tristan Benoit, Jean-Yves Marion (Université de Lorraine, Loria)
11:50-12:10	19:50-20:10	Real-time Detection of Malware Activities on Darknet by Estimating Anomalous Synchronization Chan-su Han (Researcher of Cybersecurity Laboratory, NICT)
12:10-12:30	20:10-20:30	Data flow analysis in order to construct control flow graphs of obfuscated x86 binary codes Jean-Yves Marion (Université de Lorraine, Loria) and Sylvain Cecchetto (Cyber-Detect)

CET France	JST Japan	WG5 Privacy
11:10-11:40	19:10-19:40	Contact tracing current proposals and evaluations Hiroshi Nakagawa (RIKEN AIP)
11:40-12:10	19:40-20:10	DARC : Data Anonymization and Re-identification Challenge Antoine Boutet (INSA Lyon / Inria).
12:10-12:30	20:10-20:30	Discussion

CET France	JST Japan	WG8 Cooperation and Conflicts in Cyberspace
11:10-11:20	19:10-19:20	Introduction
11:20 11:50	19:20-19:50	A Geopolitical Overview of China’s Digital Silk Road : Implications and Challenges in Central & South Asia Nowmay Opalinsk (IFG and Montaigne Institute)
11:50-12:30	19:50-20:30	Discussion

February 26 (Friday), 9:30-12:30 CET and 17:30-20:30 JST
Main session program

CET France	JST Japan	
09:30-09:35	17:30-17:35	Opening: Claude Kirchner and Koji Nakao
09:35-11:00	17:35-19:00	**Breakout sessions for WGs** (detailed program below) **WG1** — Chairs, Mitsuhiro Okada, Catuscia Palamidessi and Kostas Chatzikokolakis **WG4** — Chair, Shinsaku Kiyomoto **WG7** — Chairs, Gregory Blanc, Silverston Thomas
11:00-11:10	19;00-19:10	Break
11:10-11:40	19:10-19:40	Data Driven Cybersecurity Research Dai Inoue (NICT)
11:40-12:10	19:40-20:10	Canadian and Québec approaches to contact tracing Sébastien Gambs (UQAM, Montreal)
12:10-12:30	20:10-20:30	Discussion and final wrap up Chair: Claude Kirchner and Koji Nakao

February 26 (Friday),
Working groups programs 09:35-11:00 CET and 17:35-19:00 JST

CET France	JST Japan	WG1 Privacy by Formal Methods
09:35-10:00	17:35-18:00	Locality Sensitive Hashing with Extended Differential Privacy Natasha Fernandes (speaker), Yusuke Kawamoto and Takao Murakami 20 min talk + 5 min questions
10:00-10:20	18:00-18:20	Information Leakage Games: Exploring Information as a Utility Function Yusuke kawamoto (speaker), Mario Alvim, Konstantinos Chatzikokolakis and Catuscia Palamidessi 15 min talk + 5 min questions
10:20-10:45	18:20-18:45	An hybrid model for differential privacy Catuscia Palamidessi (speaker), Konstantinos Chatzikokolakis and Ehab ElSalamouny 20 min talk + 5 min questions
10:45-11:00	18:45-19:00	Report from the logic-formal method group of Japan Mitsuhiro Okada (speaker) 10 min talk + 5 min questions

CET France	JST Japan	WG4 Hardware Security
09:35-09:40	17:35-17:40	Introduction
09:40-10:10	17:40-18:10	Introduction of AVIM project for hardware trojan detection Kazuhide Fukushima
10:10-10:40	18:10-18:40	Machine learning based hardware trojan detection using electromagnetic emanation Sylvain Guilley
10:40-11:00	18:40-19:00	Discussion

CET France	JST Japan	WG7 Network, network security, measurement
09:35-	17:35-	Automation of Threat Mitigation for Cyberdefense Elkin Aguas (Orange Labs)
		IoT Malware Analysis Igor Santos (Mondragon University)
		GRIFIN: Cognitive and Programmable Security for Resilient Next-Generation Networks Gregory Blanc (Télécom SudParis), Thomas Silverston (Shibaura Institute of Technology)
11:00	19:00	TBD (related to IoTPot) TBD (Yokohama National University)

Abstracts of plenary talks

Speaker: Yufei Han (Inria, Rennes, France)
Title: Trustworthy Machine Learning in Cyber Security Practices
Abstract: Machine Learning-as-a-Service (MLaaS) has been deployed to overcome the day-to-day challenges of Security Operation Centers (SOCs) in recent years. It is thus essential that we trust the output of these AI systems to inform our decisions for cyber-security services, such as intrusion detection and malware classification. Trustworthy Machine Learning research aims to achieve trustable, privacy protection and human-in-the-loop collaboration in Machine Learning system architectures. In this talk, I will share my past research on trustworthy machine learning for predictive security data analysis, which sets up a bridge between emerging requirements of real-world security practices and Machine Learning techniques. Especially, I am interested in how to build robust machine learning algorithms to echo dirty raw data, strict privacy protocols, and adversarial threats in intelligent security services.

Speaker: Mitsuyuki Ueda (NISC, Tokyo, Japan)
Title: Introduction of Japanese Government Current Policy for Cybersecurity Research and Development
Abstract: The Basic Act on Cybersecurity enacted in 2014 stipulates that the national government is to provide necessary measures related to promotion of research and development. In this talk, I will introduce the outline of the current policy, based on the Cybersecurity Strategy of 2018, a following initiative policy, and a current initiative of an expert Working Group on the promotion of cybersecurity research and industry-academia collaboration.

Speaker: Sébastien Gambs (UQAM, Montreal, Canada)
Title: Canadian and Québec approaches to contact tracing
Abstract: Contact tracing applications have been deployed in many countries as a complementary measure to fight Covid-19 by enabling to automatically notify individuals who have been in contact with infected persons. However, the choice of the design of a particular application is not innocent as it has a direct impact on its security as well as on the privacy of its user. In this talk, I will review the proposition of contact tracing applications that have emerged in the last months in Canada and Québec, comparing in particular their security and privacy properties. Finally, I will conclude by discussing some ethical issues raised by the deployment of these applications.

Speaker: Dai Inoue (NICT)
Title: Data Driven Cybersecurity Research in NICT
Abstract: Data is the most crucial asset for Cybersecurity research. As Japan's sole national R&D agency specializing in the field of ICT, NICT has been conducting data driven Cybersecurity research for more than 15 years. In this talk, we present NICT's Cybersecurity research including NICTER, DAEDALUS, NIRVANA KAI, WarpDrive, STARDUST, CURE, and introduce a new project for establishing a Cybersecurity data platform in Japan.