

8th Franco-Japanese Cybersecurity Workshop

November 29th – December 1st, 2023

Bordeaux / Talence, in presence

Registration, free and mandatory before 12:00 CET, November 23, 2023:

<https://fj-cybersec2023.sciencesconf.org>

Venue

ENSC

École Nationale Supérieure de Cognitique, <https://ensc.bordeaux-inp.fr>

(Graduate School of Cognitics, <https://www.bordeaux-inp.fr/en>)

109 avenue Roul, 33405 Talence, France

<https://www.openstreetmap.org/?mlat=44.8060&mlon=-0.5994#map=12/44.8060/-0.5993>

With the support of

La région Nouvelle-Aquitaine, ENSC, Inria

Web site of the Joint collaboration between France and Japan on
Cybersecurity Research:

<https://project.inria.fr/FranceJapanICST>

PROGRAM

CET	Wednesday afternoon, November 29th, 2023 Main room: O-108
13:30 14:00	<i>Opening and Welcome address</i> Benoit Le Blanc , Director of ENSC Nicolas Roussel , Director of the Inria research center of Bordeaux university Shiho Moriai , Director General Cybersecurity Research Institute, NICT Cécile Vigouroux , Inria's director of international relations Koji Nakao , NICT Ludovic Mé , Inria's deputy scientific director in charge of cybersecurity Claude Kirchner , Inria and French national ethics committee (CCNE)
14:00 15:30	Keynotes
	Junji Shikata (Yokohama National University, Professor and Vice-President), <i>Introduction of JP Research Project on New Generation Cryptography for secure wireless communications (Tentative)</i> Hervé Debar (IMT, Télécom SudParis), <i>Quantifying and qualifying cybersecurity information - a (more) structured approach to CTI</i>
15:30 16:00	Break

CET	Wednesday afternoon, November 29th, 2023
16:00 18:00	Parallel working groups session
	<p>WG1 Formal Method: Main room: O-108 Chairs: Mitsuhiro Okada and Catuscia Palamidessi Carlos Pinzon (École Polytechnique & Inria), <i>Longitudinal data collection based on local hashing for local differential privacy</i> Gangsoo Zeong (École Polytechnique & Inria), <i>Advancing Personalized Federated Learning: Group Privacy, Fairness, and Beyond</i> Karima Makhlouf (École Polytechnique & Inria), <i>On the impact of local differential privacy on fairness: A formal approach</i> Tetsuya Sato (Tokyo Institute of Technology), <i>Towards formal verification of differential privacy in Isabelle/HOL</i> Yusuke Kawamoto (AIST), <i>A logic-based approach to explaining causality and fairness</i> Mitsuhiro Okada (Keio University), <i>On social awareness issues of cybersecurity</i></p> <p>WG2 Cryptography: Room N-201 Chair: Shiho Moriai Damien Robert (Inria), <i>Recent advance in isogeny-based cryptography</i> Olivier Ruatta (Université de Limoges), <i>Code-based cryptography with rank metric: an efficient post-quantum alternative</i> André Schrottenloher (Inria), <i>Security Analysis of Rocca-S</i> Junji Shikata (Yokohama National University) and Naoto Yanai (Osaka Univ), <i>Information for joint project from JP crypto project team</i> Shintaro Narisada (KDDI Research, Inc.), <i>Research Activities in KDDI Research on Post-quantum Cryptography</i></p> <p>WG3 Events and Malware Analysis: Room N-208 Chairs: Jean-Yves Marion and Daisuke Inoue Takayuki Sasaki (Yokohama National University), <i>Measurement and notification for securing IoT devices</i> Ryoichi Isawa (NICT), <i>Hardware trojan detection in FPGA</i> Misato Matsuda (NICT), <i>Typification and analysis of posts on social media leading to online fraud and crime</i> Yufei Han (Inria-Irisa), <i>AI-driven malware classification</i> Gabriel Sauger (Lorraine University-Loria), <i>Model-agnostic adversarial examples against ML-driven binary functions classifiers</i></p>
18:00	End of Wednesday sessions

CET	Thursday Morning, November 30th, 2023
	Main room: O-108
08:45 10:15	Keynotes
	Tatsuya Mori (Waseda University), <i>The Intriguing Aspects and Trends of Research on Security for Autonomous Vehicles</i> Kavé Salamatian (University of Savoie), <i>Internet connectivity and the situation of cables in the China Sea</i>
10:15 10:45	Break
10:45 11:15	Guy Flament (Cybercampus Nouvelle-Aquitaine), <i>The national and regional cybercampuses</i>
11:15 12:45	Industrial session
	Laurent Oudot (Tehtris), <i>Nomadic honeypots: how to create actionable cyber threat intelligence?</i> Kazuki Takada (Secure Brain), <i>Developing Remote and Automatic IoT Malware Disabling Technology and technology for Reduction of Phishing Scam</i> Hugues Thiebeauld (Eshard), <i>Anticipating the Post Quantum cryptography: don't think it is simple</i> Yuka Miyatake (Trend Micro), <i>Usage of Generative AI. Perspective of both "Cybercriminals" and "Cyber Security Defense"</i>
12:45	Lunch buffet: Room N-208

CET	Thursday afternoon, November 30th, 2023
	Main room: O-108
14:00 15:30	ICS/ITS security
	<p>Masaki Umejima (IEC System Committee Smart Energy), <i>IEC System Committee Smart Energy</i></p> <p>Tatsuya Mori (Waseda University), <i>Discussion related to the keynote</i></p> <p>Stéphane Mocanu (Inria), <i>Industrial Control Systems security: some results and ongoing research</i></p> <p>Thomas Marchioro (CEA), <i>Learning from past attacks to discover new threats</i></p>
15:30 16:30	Network security
	<p>Toshiro Sawamoto and Mio Suzuki (NICT 5G team), <i>Introduction of 5G security research activities at NICT Cybersecurity Laboratory</i></p> <p>Abdelkader Lahmadi (Lorraine University-Loria), <i>An Experimental Study of Denial-of-Service Attacks on a 5G COTS Server</i></p> <p>Philippe Owezarski (CNRS, LAAS), <i>From tracing in the cloud to 5G cybersecurity</i></p>
16:30	Break
17:00 19:00	Cybersecurity strategies
	<p>Jun Murai (Keio University), <i>Cybersecurity impacts by network infrastructure design</i></p> <p>Florent Kirchner (SGPI), <i>The France 2030 plan and the French cybersecurity strategy</i></p> <p>Shiho Moriai (NICT), <i>Cybersecurity strategy in NICT (tentative)</i></p> <p>Discussion chaired by Ludovic Mé (Inria) and Koji Nakao (NICT)</p>
20:00	<p>Workshop dinner</p> <p>Le Café du Port, https://www.lecafeduport.com</p>

CET	Friday, December 1st, 2023
	Main room : O-108
09:00 10:30	Human factor security
	<p>Akira Fujita (NICT), <i>ISPs' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT</i></p> <p>Valeria Loscri (Inria Lille), <i>Emerging Communication Technologies, Social Aspects and Legal Factors for evolved cybersecurity solutions</i></p> <p>Mitsuaki Akiyama (NTT Social Informatics Laboratories), <i>Systematizing Knowledge of Cybersecurity Research Ethics</i></p> <p>Panel (30mn): Moderator: Catuscia Palamidessi Panelists: Mitsuaki Akiyama, Akira Fujita, Valeria Loscri</p>
10:30 11:00	Break
11:00 12:30	AI and security
	<p>Yinminn Papa (Yokohama National University), <i>The Dark Side of AI in Cybersecurity</i></p> <p>Naoto Yanai (Osaka Univ), <i>Recent Approach for Attacks on Machine Learning Models</i></p> <p>Yufei Han (Inria), <i>Which AI is wanted? Towards AI-driven Security Incident Detection and Prediction</i></p> <p>Panel (30mn): Moderator: Koji Nakao Panelists: Yufei Han, Yinminn Papa, Naoto Yanai</p>
12:30 14:00	Lunch buffet: Room N-208
14:00 15:30	<p>Cooperation organization, general conclusion and future plans</p> <p>General discussion chaired by Ludovic Mé and Koji Nakao</p>
15:30 16:00	Final conclusions
16:00	Farewell drinks