Conference Program

Monday, 24 November 2024

13:30 - 17:00: Workshop “Women in cybersecurity”

Tuesday, 25th November

9:00 – 9:30	Registration and coffee
9:30 – 9:50	Opening remarks
9:50 – 10:50	**Keynote 1**: Guillaume Prigent (Diateam)
10:50 – 11:15	Coffee Break
11:15 – 12:30	Session 1
12:30 – 13:45	Lunch
13:45 – 15:20	Session 2
15:20 – 15:45	Coffee Break
15:45 – 17:45	Session 3
18:45 – 20:45	Cocktail

Wednesday, 26th November

9:00 – 10:00	**Keynote 2:** Kave Salamatian (Savoie University)
10:00 – 10:30	Coffee Break
10:30 – 12:30	Session 4
12:30 – 13:45	Lunch
13:45 – 15h40	Session 5 : **Industrial Track**
15:40 – 15:55	Coffee Break
15:55 – 17 :45	Session 6
18:45 – 22:00	Social Event

Thursday, 27th November

9:00 – 11:00	Session 7
11:00 – 11:30	Coffee Break
11:30 – 12:30	**Keynote 3** : Raphael Khoury (University of Quebec in Outaouais - UQO)
12:30 – 13:45	Lunch
13:45 – 15:50	Session 8
15:50 – 16:15	Closing remarks

Details about sessions :

Tuesday, 25th November

11:15 – 12:30

Session 1 : Security, Privacy, and Trust in Blockchain & Emerging Distributed Systems

Session Chair : Yvon Kermarrec

Time	Authors	Title
11:15-11:35	**Pierre Saha Fobougong**, Mohamed Mejri and Kamel Adi	Towards A Pragmatic Selection Of Self-Sovereign Identity Security Measures : Exploiting Mitre Att&ck Graph And Multi-criteria Optimization
11:35-11:55	Petr Dzurenda, **Minh Tran**, Mubashar Iqbal, Sara Ricci, Vaclav Stupka, Raimundas Matulevicius and Lukas Malina	ForensicChain: Blockchain-based Secure Digital Forensic Investigations
11:55-12:15	**Jan Ariel Ocampo**, Lejla Islami and Mina Alishahi	Privacy-Preserving Federated Learning for IoT Intrusion Detection in 6G Networks
12:15-12:30	**Remi Barbier**, Francoise Sailhan, Alexandre Reiffers-Masson and Loic Machado	Scaling Blockchains with zk-Rollups: State of the Art and Implementation

13:45 – 15:20

Session 2 : Cyber Resilience and Risk Management in Enterprise Architectures

Session Chair : Reda Yaich

Time	Authors	Title
13:45-14:05	**Francis Wanko Naa**, Nora Boulahia-Cuppens and Frederic Cuppens	Eliciting metrics and evaluating cyber resilience of a capability in multilayer enterprise architecture
14:05-14:25	**Arslane Fawzi Halilou** and Natalia Stakhanova	Predicting IoT Security Vulnerabilities from Device Specifications
14:25-14:45	N'Famoussa Kounon Nanamou, Neda Baghalizadeh-Moghadam, Kéren A Saint-Hilaire, Thibault Leblanc, Nora Cuppens, **Frédéric Cuppens** and Anis Bkakria	Real-Time Insider Threat Hunting Based on Dynamic Risk Indicators
14:45-15:05	**Babacar Mbaye** and Mohamed Mejri	Optimizing Resilience in IT Architectures : A Multi-Objective Ontology-Based Approach
15:05-15:20	Barbara Carminati, Elena Ferrari, Christian Rondanini, **Azhar Muhammad Shahid** and Luca Clementi	COBRA-Z: Collaborative Blockchain Risk Assessment for Zero Trust Architecture

15:45 – 17:45

Session 3 : Formal Methods and Automated Analysis for Secure Software Systems

Session Chair : Kassem KALLAS

Time	Authors	Title
15:45-16:05	**Yekatierina Churakova**, Mathias Ekstedt and Larissa Schmid	Vexed by VEX Tools: Consistency Evaluation of Container Vulnerability Scanners
16:05-16:25	**Alberto Tacchella**, Jurij Mihelič, David Cerdeira, José Martins, Sandro Pinto, Bruno Crispo and Marco Roveri	Towards a formal verification of the Bao Hypervisor
16:25-16:45	**Luis Soeiro**, Thomas Robert and Stefano Zacchiroli	Finding Software Supply Chain Attack Paths with Logical Attack Graphs
16:45-17:05	**Rémi Garcia**, Paolo Modesti and Leo Freitas	From provable models to provable implementations: translating Alice & Bob security protocols to F*
17:05-17:25	**Quentin Goux** and Nadira Lammari	Automatic Attack Script Generation: a MDA Approach
17:25-17:45	Ludjina Benoit, **Rim Ben Salem**, Nora Boulahia-Cuppens and Frédéric Cuppens	Mining Reliable ABAC Policies: A Specificity and Confidence-Aware Extension of Rhapsody

Wednesday, 26th November

10:30 – 12:30

Session 4 : ML and Intelligent Systems for Attack Detection and Trust Evaluation

Session Chair : Frédéric Cuppens

Time	Authors	Title
10:30-10:50	Antoine Rebstock, Yann Busnel and **Romaric Ludinard**	A Grammar-Driven Approach to Model and Detect APT Attack Sequences
10:50-11:10	**Bastien Vuillod**, Pierre-Alain Moellic and Jean-Max Dutertre	Watch Out for the Lifespan: Evaluating Backdoor Attacks Against Federated Model Adaptation
11:10-11:30	**Seán Óg Murphy**, Utz Roedig and Cormac Sreenan	Systematic Security Context Weighting for Trust Algorithms via AI/ML Model Performance Analysis
11:30-11:50	Kobra Khanmohammadi, Pooria Roy, **Raphael Khoury**, Abdelwahab Hamou-Lhadj and Wilfried Patrick Konan	WildCode: An Empirical Analysis of Code Generated by ChatGPT
11:50:12:10	**Miguel Silva**, Daniela Pinto, João Vitorino, Eva Maia, Isabel Praça, Ivone Amorim and Maria Viamonte	Binary and Multiclass Cyberattack Classification on GeNIS Dataset
12:10-12:30	**Bassirou Badiane**, Valerie Viet Triem Tong and Yufei Han	Towards Automated Botnet Threat Intelligence with Knowledge-Guided Large Language Models

13:45 – 15:40

Session 5 : Industrial Track

Session Chair : David Espes

Time	Authors	Title
13:45-14:05	**Pierre Mahieux**, Mouhamadou Bamba Sakho, Gouenou Coatrieux and Reda Bellafqira	An Improved Paillier-Based Reversible Watermarking Scheme for 3D Models with Reduced Complexity
14:05-14:25	**Yeoh Wei Zhu**, Shaltiel Eloul, Yash Satsangi, Imran Bashir and Sudhir Upadhyay	Towards adoption of private distributed ledgers for capital markets
14:25-14:40	**Florence Sèdes** and Brice Chellet	Dynamic Multilayer Information System Cartography for Cybersecurity, Compliance and Industrial Governance
14:40-15:00	**Francesco Ferazza** and **Konstantinos Mersinas**	Socio-Technical Friction: An Emergent Grounded Theory of DevSecOps Challenges
15:00-15:20	**Tanja Pavleska**, Giovanni Paolo Sellitto, Helder Aranha and Massimiliano Masi	Secure-by-Design Architectures for Cooperative Intelligent Transport Systems
15:20-15:40	**Leonie Wolf**, Samson Umezulike, Gurur Öndarö, Sebastian Schinzel and Fabian Ising	Practical Evaluation of the Crypto-Agility Maturity Model

15:55 – 17:45

Session 6 : Advances in Privacy-Preserving Cryptography and Secure Computation

Session Chair : Nora Cuppens Boulahia

Time	Authors	Title
15:55-16:15	**Yuan Liang**, Giovanni Di Crescenzo and Haining Wang	Sender-Efficient Identity-Based Encryption with Reduced Server Trust in the Key Curator Model **(Online)**
16:15-16:35	**Shohei Kaneko**, Yang Li, Kazuo Sakiyama and Daiki Miyahara	Counterfeit Coin Problem Can Be Extended to Secure Multiparty Computation
16:35-16:55	El Hadji Mamadou Dia, **Walid Arabi**, Anis Bkakria and Reda Yaich	StrawHat: Private Non-Interactive Gradient Boosting Decision Tree Evaluation Based on Homomorphic Encryption
16:55-17:15	**Nicolas Quero**, Renaud Sirdey, Aymen Boudguiga, David Pointcheval, Quentin Sinh and Nadir Karam	Scalable privacy-preserving database queries with FHE and PEKS
17:15-17:30	**Marc Damie**, Mihai Pop and Merijn Posthuma	Energy Consumption of TLS, Searchable Encryption and Fully Homomorphic Encryption
17:30-17:45	**Augustin P. Sarr**	An Embarrassingly Parallel Cryptanalysis of EC(H)MQV

Thursday, 27th November

09:00 – 11:00

Session 7 : Secure and Intelligent Network Architectures for Next-Generation Communications

Session Chair : Omar Mawloud

Time	Authors	Title
9:00-9:20	**Alex Pierron**, Michel Barbeau, Luca De Cicco, Jose Manuel Rubio Hernan and Joaquin Garcia-Alfaro	A Fairness-Aware Strategy for B5G Physical-layer Security Leveraging Reconfigurable Intelligent Surfaces
9:20-9:40	**Lucas Schrass**, Yu Shen and Stefanie Roos	APADV: Anonymous Proactive Distance Vector Routing in Connectivity-Restricted Environments
9:40-10:00	**Andrea Fulgence Ndreveloarisoa**, Frédéric Guidec and Mawloud Omar	A secure lightweight system based on device-to-device communication for objects sharing in local communities
10:00-10:20	Matthew Bush, **Dave McKay** and Atefeh Mashatan	Consumer Zero Trust: Towards a Principled Adaptation of Zero Trust for Consumer Networks
10:20-10:40	**João Vitorino**, Daniela Pinto, Eva Maia, Ivone Amorim and Isabel Praça	Revisiting Network Traffic Analysis: Compatible Network Flows for ML Models
10:40-11:00	**Hocine Attoumi**, Etienne Gael Tajeuna and Mohand Said Allili	Causal Graph Modeling of Network Traffic for Early Cyberattack Prediction

13:45 – 15:50

Session 8 : Secure, Explainable, and Efficient Machine Learning in Cybersecurity

Session Chair : Ranwa Al Mallah

Time	Authors	Title
13:45-14:00	**Ananta Raha**, Junaeid Ahmed, Md Shohrab Hossain and Suryadipta Majumdar	Defending Model Inversion Attack Using an Improved Filter-Based Approach
14:00-14:20	Muhammed Tahir Akdeniz, Zeynep Yesilkaya, Ibrahim Enes Kose, Ismail Ulas Unal and **Sevil Sen**	VOLTRON: Detecting Unknown Malware Using Graph-Based Zero-Shot Learning
14:20-14:40	**Alexandre Dohin**, Karim Zkik, Omar Mawloud and Abdellah Akilal	Deep Learning-Driven Energy Auditing for Smart Grid Cyberattack Detection
14:40-14:55	**Saba Kasrelou**, Samuel Pierre and Ranwa Al-Mallah	Verifiability of Unlearning Schemes Through Local Explanation
14:55-15:10	**Myria Bouhaddi**, Feriel Sadoun and Kamel Adi	Anomaly-Aware Aggregation for Robust Peer-to-Peer Machine Learning
15:10-15:30	Shuaishuai Liu, **Gergely Acs** and Gergely Biczók	Interdependent Privacy in Smart Homes: Hunting for Bystanders in Privacy Policies
15:30-15:50	**Daphnee Chabal**, Dolly Sapra, Cees de Laat and Zoltan Mann	QUOKKA: Faster Secure Neural Network Inference with Early-Exit Technology

Contact: fps-registration@imt-atlantique.fr

Website: https://hub.imt-atlantique.fr/fps2025/