Workshop: Cybersecurity for Connected and Autonomous Cars

Monday, December 12, 2022 | 9:15 - 16:30
Télécom Paris, 19 place Marguerite Perey, 91120 Palaiseau, France

09:15 – 09:30	Welcome
09:30 – 10:10	**Introduction to the connected vehicles cybersecurity** **Loubna Ghammam,** ITK Engineering GmbH (Bosch), Germany Loubna is a researcher in cryptography and cyber security expert. She has conducted her PhD study at University of Rennes 1 between 2013 and 2016. From 2016 to 2019, Loubna worked as a research engineer in University of Caen and in Ecole des Mines de Saint Etienne. In 2019, Loubna joined ITK Engineering GmbH (Bosch) in Germany. Loubna's research interests cover several aspects of cryptography such as elliptic curve cryptography, pairings calculation, side-channel attacks on pairings, protection of biometric data and recently security in the automotive domain including post-quantum cryptography.
10:10 – 10:50	**Misbehaviour detection in the TAM project** **Francesca Bassi,** IRT SystemX, Palaiseau, France Francesca Bassi was born in Cremona, Italy. She received the Master of Science degree in telecommunications engineering from the University of Bologna, Bologna, Italy, in 2006, and the Ph.D. degree from University Paris-Sud, Orsay, France, and from the University of Bologna, in 2010. In 2007 and 2009, she has been a visiting Ph.D. student at the University of Bologna. From 2006 to 2010, she was with Laboratoire des Signaux et des Systèmes, Gif-sur-Yvette, France. Between 2011 and 2012, she was a Postdoctoral Researcher at the University of Michigan, Ann Arbor, MI, USA. Between 2012 and 2019 she has been an Assistant Professor at ESME-Sudria, Ivry-sur-Seine, France, and an Associate Researcher with the Laboratoire des Signaux et des Systèmes. She is now a researcher at IRT SystemX, Palaiseau, France, and an associate member of the LINCS lab.
10:50 – 11:10	Coffee Break
11:10 – 11:50	**Securing V2X communication in the context of 5G** **Lyes Khoukhi,** Professor at ENSICAEN, Normandie University, France Lyes Khoukhi is Full Professor at ENSICAEN, Normandie University, with GREYC CNRS laboratory, Caen, France. He received the Ph.D degree at the University of Sherbrooke, Canada, in 2006. Between 2007 and 2008, he was a researcher at the University of Montreal in collaboration with Bell-Canada. In 2008, he also worked for Dialexia Corporation-Montreal. His research interests

include attacks detection and mitigation in V2X/IoT/5G, and privacy. He has several projects related to connected cars. He has participated as a General chair or program chair in many conferences, like IEEE LCN, IEEE ICC, IEEE Globecom, etc.

11:50 – 12:30 **Poster Session**

- **Cooperative Trust and Misbehavior Detection for Platooning**
  Emma Braiteh, PhD student, Télécom Paris, Institut Polytechnique de Paris, France
- **Towards a centralized security architecture for SOME/IP automotive services**
  Hamza Khemissa, PhD student, Télécom Paris, Institut Polytechnique de Paris, France
- **Denial of service impact in V2I**
  Ayoub Wehbe, PhD student, Télécom Paris, Institut Polytechnique de Paris, France
- **A Secure routing scheme for V2V**.
  Fadlallah Chbib, PhD student, Télécom Paris, Institut Polytechnique de Paris, France
- **Lightweight Cryptography algorithms benchmarking in connected vehicles environment**
  Abdessamad Fazzat, , PhD student, Télécom Paris, Institut Polytechnique de Paris, France

12:30 – 14:00 Lunch Break

14:00 – 14:40 **Intrusion Detection with Deep Learning for In-Vehicle Networks**

Natasha Alkhatib, PhD student, Chair C3S, Télécom Paris, Institut Polytechnique de Paris, France

Due to the rising number of sophisticated customer functionalities, electronic control units (ECUs) are increasingly integrated into modern automotive systems. However, the high connectivity between the in-vehicle and the external networks paves the way for hackers who could exploit the in-vehicle network protocols' vulnerabilities. Among these protocols, the Controller Area Network (CAN) and the Automotive Ethernet, both considered as the most widely used in- vehicle networking technology, lack security mechanisms, making the communications delivered by distributed ECUs insecure. Through her work, Natasha Alkhatib will show how to leverage deep learning based intrusion detection systems to detect novel and known in-vehicle network attacks with high accuracy.

Natasha is currently a third year PhD student at IPP under the supervision of Drs Jean-Luc Danger, Hadi Ghauch and Maria Mushtaq. Her main research contributions lie in the generation of datasets that contain diverse and sophisticated automotive cyberattacks, the adoption of unsupervised learning techniques for attack detection, and the development of novel neural network architectures, which are customized for intrusion detection.

14:40 – 15:20 **Unsupervised Learning Algorithms for Denial of Service Detection in Connected Vehicles**

Ali El Attar, Researcher, INDID Project, Télécom Paris, Institut Polytechnique de Paris, France

15:20 - 15:35 Coffee Break

15:35 – 16:15 **An overview of automotive perception security**.

Jean-Philippe Monteuuis, Qualcomm, Boston, Massachusetts, United States

Jean-Philippe is currently a senior engineer at Qualcomm. He received his Ph.D. from Institut Polytechnique de Paris (Telecom ParisTech) in 2020.

His research interests include threat analysis and anomalies detection in the context of Intelligent Transportation System (ITS) and automotive perception.

16:15 – 16:30	Conclusion