ECyTeCC 2020

Workshop on Emerging Cybersecurity Technologies for Cooperative, Connected and Automated Mobility

Ryerson University

Toronto, Canada, May 6-8, 2020

(http://widecomconference.org/)

SCOPE:

Most current Cooperative Connected and Automated Mobility (CCAM) applications do not take automated actions based on data from external sensors. This fact severely limits the potential performance gains of cooperative applications. Having a secure vehicular communication sub-system is thus mandatory to extend situational awareness beyond the limits of the onboard sensors and to design truly cooperative automated mobility applications. Over the last decade there has been a vast amount of work on security for vehicular applications, leading to the standardization of several security protocols and Public Key Infrastructure (PKI) architectures, being the most relevant the IEEE 1609.2 and ETSI ITS Security Standards. These security architectures are relatively complex and have a central management authority, with public and private stakeholders. However, it has been reported that some aspects of these standards are insecure and are not at a quantum-safe cryptography level. Furthermore, traceability is also an issue, made possible by sniffing network traffic and compare it with static information. Recently, several promising research lines have been proposed to overcome the limitations of existing security architectures for CCAM, notably the ones based on blockchain, self-sovereign identity, hybrid security schemes, and physical-layer security.

In this context, the 1st International Workshop on Emerging Cybersecurity Technologies for Cooperative, Connected and Automated Mobility aims to provide researchers and practitioners a forum for presenting and discussing research challenges addressing security technologies for CCAM systems and applications. In the last few years, with the onset of autonomous driving, cooperation among intelligent vehicles has been gaining increasing attention from car manufacturers, communication equipment producers, and mobile operators as a way to offer new services and improve the overall traffic performance while enhancing road users' safety. However, the increased complexity and information sharing bring higher security risks and an extended exposure to attacks, which might compromise anonymity and safety.

Original, high quality contributions that are not yet published, submitted or not currently under review by journals or peer-reviewed conferences are sought. These can be of two types, full paper with up to **12 pages** and short communication with up to **6 pages**, both in Springer conference format.

TOPICS OF INTEREST:

- Autonomous vehicle security
- CCAM security architectures
- Privacy-enhancing technologies
- Hybrid network security
- Vehicular 5G security
- Vehicular security through artificial intelligence
- Security performance and impact on vehicular communications
- Lightweight security and its applications
- Modelling of cybersecurity threats
- Applications of distributed ledger technologies for vehicular security
- Key management schemes

- Secure over-the-air updates
- Quantum safe security
- In-vehicle sensing, infotainment or network security
- V2X security
- Security testbed construction, validation and assessment
- User privacy in CCAM application

IMPORTANT DATES:
Submission deadline: September 20, 2019
Notification of acceptance: October 20, 2019
Deadline for camera-ready version: November 20, 2019
Workshop Date: May 6-8, 2020

PAPER SUBMISSION:
Authors should prepare a PDF version of their paper formatting according to Springer Word or LaTex template available at https://www.springer.com/us/authors-editors/book-authors-editors/manuscript-preparation/5636

Short papers should be up to 6 pages maximum including references AND regular papers should be up to 12 pages maximum including references.

The submission page for ECyTeCC 2020 through EasyChair system is: https://easychair.org/conferences/?conf=ecytecc2020

In order to submit your paper, you must first create an EasyChair account if you do not have one already, using https://www.easychair.org/account/signup.The EasyChair system will then email you your password, which you can then use.

All accepted papers will be included in Springer Series: Lecture Notes on Data Engineering and Communications Technologies. Proceedings will be sent by Springer for indexing in MetaPress, ISI Proceedings, Springerlink, and DBLP. Authors of accepted papers will be given instructions for submission of camera-ready and copyright form. All authors of accepted papers will have access to the electronic version of the proceedings.

Extended versions of selected papers at Widecom 2020 will be considered for publication in Special Issues of Internet of Things Journal, Elsevier and The International Journal of Space-Based and Situated Computing (IJSSC), Inderscience.

For any additional query, please email the conference organizers using: jjcf@ua.pt

ORGANIZING COMMITTEE:
Joaquim Ferreira (jjcf@ua.pt) (Main organizer)
Arunita Jaekel (arunita@uwindsor.ca),
Sherif Saad (shsaad@uwindsor.ca)
Paulo C. Bartolomeu (bartolomeu@ua.pt)

VENUE:
The conference will be held in Ryerson University, Toronto, Canada.

CONTACT:
All questions about submissions should be emailed to Joaquim Ferreira (jjcf@ua.pt)