Protection in Cyber-Physical Systems (PCPS)

Cyber-Physical Systems (CPS) are defined as the integrations of ICT and physical processes. The Internet-of-Things (IoT), smart grid, critical infrastructures, autonomous and connected vehicles, industrial control systems, smart homes and cities, and medical monitoring systems are all parts and examples of cyber physical systems. Today, the operations of many critical services for businesses, government agencies and individuals rely on cyber-physical systems for many daily activities. This dependency means that any attack can have devastating results. The sophistication of some of the already seen attacks and the sponsorship of some nation-states for actors and cyber criminals mean that the protection of cyber-physical systems is of an utmost importance.

The workshop on Protection in Cyber-Physical Systems (PCPS) focuses on the threats and countermeasures related to cyber-physical systems. Authors are invited to submit high-quality research papers related to the theory or practice of all aspects of cyber-physical systems. All submitted papers must not have been previously published nor currently under review by another conference, journal or publishing venues. Topics include, but not limited to:

- Cryptographic mechanisms
- Resilience
- Accountability
- Trustworthy devices and systems
- Intrusion prevention, detection and recovery mechanisms
- Wired and wireless communication security
- Authentication
- Secure architectures
- Security policies
- Usable security
- Privacy
- Forensic
- Hardware security
- Embedded systems security

Contact Session Chair: Prof. Khalil El-Khatib, Email: Khalil.El-Khatib@uoit.ca