Cyber-Physical Systems (CPS) are becoming pervasive and changing our lives. Smart cyber-physical devices can be used in many different fields, such as connected vehicles, smart homes, mobile social networks and Internet of People, and Industrial Cyber-Physical Systems.
CPS devices usually leverage on Machine-to-Machine (M2M) communication. This allows these devices to operate in interconnected groups, enabling them to autonomously perform critical operations, take decisions, or perform tasks that single devices cannot do.
As we move towards an era of "automation", interconnected CPS certainly make their existence as a panacea to address several issues in the smart world, but also are an attractive target for attackers, which can operate on single devices or on the whole network. In fact, these devices are usually resource constrained and unable to defend themselves against security threats. Even a single compromised node in a group of cooperating devices can pose a serious security threat, e.g., by either disrupting communications (and thus the coordination) within the group, or sharing critical information to unauthorized external parties. Attackers can use devices as a vector to other targets, as in the case of Denial of Service (DoS) attacks, interfere with the normal functionality of the network in order to force abnormal behaviours, or simply infere private information through compromised devices. As such, security and privacy are a major concern, to guarantee both the correct operational capabilities of devices and prevent data thefts and/or privacy violations.

This Special Issue provides significant contributions for the improvement of different interconnected Cyber-Physical Systems in several fields with the goal of improving their security and/or privacy.

We start our special issue with two papers focusing on smart home security.
Kafle et al. provide a systematic security analysis of Google Nest and Philips Hue, two widely popular data store-based smart home platforms. In "*Security in Centralized Data Store-based Home AutomationPlatforms: A Systematic Analysis of Nest and Hue*", authors evaluate the security of the two platforms, identify vulnerabilities in them, and propose solutions for their mitigations.
In "*Canopy: A Verifiable Privacy-Preserving Token Ring based Communication Protocol for Smart Homes*", Panwar et al. propose a protocol that prevents privacy breaches in smart homes that can arise from the analysis of the traffic generated by smart devices. The protocol is based on a cryptographically secure token circulation in a ring network to which smart home devices are connected.

We then continue with two papers whose subject is the network of connected people.
Azad et al. in "*Privacy-preserving Crowd-sensed trust aggregation in the User-centric Internet of People Networks*" propose a protocol that uses homomorphic cryptosystem in a decentralized way to assess the trustworthiness of content and content providers in the connected Internet of People, while preserving the privacy of individual ratings.
Privacy is also demanding in location-based services offered by social networks making use of mobile devices. A protocol that protects the physical position of users and other related information is proposed in "*Preserving Secrecy in Mobile Social Networks*" by Suntaxi et al.

An emerging field where CPS plays a relevant role is the connected vehicle scenario where autonomous and timely decisions can improve drivers and passengers safety.
In "*TangleCV: A Distributed Ledger Technique for Secure Message Sharing in Connected Vehicles*", Rathore et al. present a protocol, TangleCV, that leverages a directed acyclic graph-based distributed ledger technique to address data tampering threats in connected vehicular networks.

To guarantee security in the automotive domain, Rawat et al. in "*Decentralized Firmware Attestation for In-Vehicle Networks*" design and evaluate two decentralized firmware attestation schemes where each electronic control unit (ECU) attests other ECUs on which it depends on, in order to verify the status of the smart vehicle.

Smart resource distribution platforms are large-scale interconnected Cyber-Physical Systems where security and privacy plays an important role.
In "*Safe and Private Forward-Trading Platform for Transactive Microgrids*", Eisele et al. propose TRANSAX, a platform enabling participants to trade in an energy market that improves efficiency by finding feasible matches for energy trades, guarantee privacy by anonymizing participant trading activity, and limit trading activity based on safety requirements.
Palleti et al. presents an experimental study in "*Can Replay Attacks Designed to StealWater from Water Distribution Systems Remain Undetected?*" that shows how replay attacks can be used to steal water from an operational water distribution plant. Authors investigate the conditions under which such attacks can be detected by a protocol based on a Linear Time-Invariant system model of the physical system.

Abdelaziz et al. focus on industrial Cyber-Physical Systems (ICPS) by proposing a fully automatic framework that assesses the security of the system. The framework proposed in "*Assessing the Severity of Smart Attacks in Industrial Cyber Physical Systems*" assesses the severity of attacks by modeling the architecture, its components and the attacks the ICPS can be subjected to, analyzing the effects of the attacks to the model, and mitigating the attacks with appropriate countermeasures to be deployed.

We conclude with a paper whose content can provide a significant contribution to all the interconnected Cyber-Physical Systems. Ardagna et al. in "*From Trustworthy Data to Trustworthy IoT: A Data Collection Methodology Based on Blockchain*" boost trustworthiness in IoT by defining a methodology for data collection based on blockchain and smart contracts that, through syntactic and semantic rules, identifies and filters untrusted data.

Moreno Ambrosin
Mauro Conti
Riccardo Lazzeretti
Chia-Mu Yu