Introduction to "Security and Critical Infrastructure for Cloud, IoT and Decentralized Trust" minitrack

William J. Yeager
Retired
Formerly of Stanford University and Sun Microsystems, Inc.
byeager@fastmail.fm

Jean-Henry Morin
Institute of Information Service Science
University of Geneva, CUI, Switzerland
Jean-Henry.Morin@unige.ch

This minitrack has evolved over a decade initially starting with peer-to-peer distributed systems, covering ubiquitous computing, the rise of cloud computing and Internet of Things. Security has always been a central concern in this evolution, originally centered on users, it has now become a critical matter of global public safety as Internet of Things and Cloud Services have entered our most intimate areas such as homes, health, work and personal interactions.

Consequently, there is an urgent need to recognize such systems and services as part of Critical Infrastructure, alongside commonly recognized infrastructure such as water, electricity, transportation systems, etc. It will be only if this is properly addressed, from a security standpoint, that we will be able to consider a sustainable and responsible digital society.

In this context, recent evolution in the area of decentralized trust has shown promising results with, for example, the use of distributed ledgers such as blockchain technology. The key properties of transparency and immutability of such approaches offer great opportunities to implement more secure and resilient systems and services. The growing interest in this area suggests these technologies may be reaching a level of maturity allowing for their use in many situations requiring a much needed security level to be trustworthy.

In this minitrack we represent the very beginnings of the current research on securing IoT as well as the opportunities IoT enables. To this end we have the following two papers:

The first paper, "On Software Standards and Solutions for a Trusted Internet of Things" by David Maher of Intertrust Technologies proposes a high-level model for software applications and services that can support a minimal set of human-centric trust management capabilities. In this context, the role of standards is discussed alongside a set of solutions for trust management including blockchain to record trust and policy graphs.

The second paper, "Drivers vs. Inhibitors - What Clinches Continuous Service Certification Adoption by Cloud Service Providers?" by Heiner Teigeler, Sebastian Lins, and Ali Sunyaev, of University of Kassel report on a study analyzing factors influencing adoption of Continuous Service Certification (CSC) by cloud service providers. The study is very timely as services are increasingly provided as commodities in the cloud. And, consequently, so is the growing importance of compliance and monitoring.

URI: http://hdl.handle.net/10125/50598
ISBN: 978-0-9981331-1-9
(CC BY-NC-ND 4.0)