Security and Trust in a Networked Immersed World: from Components to Systems and Beyond

John S. Baras
Lockheed Martin Chair in Systems Engineering
The Institute for Systems Research,
Electrical and Computer Engineering Department,
Fischell Bioengineering Department,
Mechanical Engineering Department, and
Applied Mathematics, Statistics and Scientific Computation Program
University of Maryland College Park, USA

and

Tage Erlander *Guest Professor*
School of Electrical Engineering
and ACCESS Linnaeus Centre
Royal Institute of Technology (KTH), SWEDEN

The tremendous explosion of wireless devices and services have created unprecedented advances and are impacting every aspect of life and work. However, many of these advances and resulting expanding markets are critically endangered by weaknesses in security, integrity and trust. We first describe several of these emerging systems and markets in areas ranging from aerospace and automotive to healthcare and e-commerce to social networks over the Web. We then describe various physical layer (e.g. hardware and signal processing) techniques that can be successfully utilized to significantly strengthen the security of wireless devices and networked systems. We argue for the need of a "trusted core" in wireless networks and for the allocation of part of the security functionality to the physical layer. We next turn into the subject of trust in large networks and describe a new framework using multiple partially ordered semirings for analyzing reputation and trust dynamics and composite trust. Next we describe our work based on constrained coalitional games towards understanding the role of trust in collaboration and social networks. We describe several specific applications of these methods in securing distributed inference systems, SCADA sensor networks for power grids, wireless network routing protocols, LTE paging systems, wireless handheld devices for healthcare and e-payment systems. We close by describing the need for rigorous frameworks and theories for composable security and outline future research challenges and directions.