Designed-in Cybersecurity for Smart Cities: A Discussion of Unifying Architectures, Standards, Lessons Learned and R&D Strategies

May 27-28, 2015

Red Auditorium, NIST Campus, Gaithersburg, Maryland

Draft Agenda

May 27

7:30 AM	**Registration**	
8:30 AM	**Welcome**	
8:40 AM	**Keynote Address**	
9:05 AM	**Keynote Address**	
9:30 AM	**Workshop Overview**	
9:40 AM	**BREAK**	
	Breakout Sessions	
10:00 AM	**Session 1: Reference Framework for CPS, Cybersecurity Framework (CSF) and Smart Cities** The Cyber Physical Systems Public Working Group (CPS PWG) has been working on a Reference Framework for CPS. Leaders for this working group will brief the participants on the CPS Framework which includes the identification of foundational goals, characteristics, common roles and features, actors, and interfaces, across CPS domains. The discussion will consider how designed-in cybersecurity and privacy in Smart Cities can be further facilitated by the NIST Cybersecurity Framework (CSF). The session will identify components of CPS framework and CSF risk analysis that are immediately applicable to Smart Cities and identify gaps in coverage specific for this context.	**Session 2: Standards Space: Analyzing Standards for Smart Cities** Participants will review relevant standards and identify gaps where new standards are needed. The review will include both specific and general purpose standards relevant to Smart Cities and produced by a variety of standards bodies. The objective of the session is to provide a high level environment scan for standards, identify gaps, and provide recommendations for optimization of standardization approaches.
11:30 AM	**LUNCH**	
12:30 PM	**Session 3: Understanding Smart Cities Context: Modeling Techniques** The size and complexity of smart cities poses a major challenge for thinking about	**Session 4: Economic Incentives for Safer & Privacy Friendly Smart Cities** Participants will discuss the economic and business issues surrounding

	cybersecurity in smart cities. What approaches might be useful in modeling the big picture? How might they be used to identify cybersecurity vulnerabilities, design in more comprehensive defenses, and understand complex interactions between layers? This session will include two ontology case studies for discussion. Attendees will identify key requirements and possible approaches to understanding cybersecurity on a macro scale.	designed-in cybersecurity & privacy for smart cities. Participants will consider foundations and principles that could enable us to design economic incentives for Smart Cities that will promote security and privacy. Questions may include: What are the returns for investing in cybersecurity for Smart City deployments? What are the economic incentives (and disincentives)? What are the mandatory obligations in city planning that transcend economic incentives?
2:00 PM	**BREAK**	
2:20 PM	**Session 5: Beyond Architecture and Technology: Other Elements Necessary for Success** There is more to designed-in cybersecurity for Smart Cities than the development of a particular architecture and advances in a certain technology space. Too often we only consider the technology in architecting and designing a system and don't take into consideration the motivations and culture surrounding the need for the new system. In this session, we will discuss additional considerations surrounding cybersecurity architectures and privacy enhancing technologies for Smart Cities that need to be addressed, including broader organizational context such as organizational culture, adoption framework, governance, usability, process improvement, finances or chargebacks, SLA's, etc. Taking a full enterprise viewpoint we may find usability benefits resulting in increased user adoption. Discussions will bring out areas where additional research is needed and possible products that need development.	**Session 6: An Interdisciplinary Approach to Cybersecurity for Smart Cities** The highly interconnected nature, extensive and integrated scope of Smart Cities indicates the need for broad perspectives in cybersecurity research. In this session, we look at two such perspectives: First, when and how do cybersecurity challenges motivate an interdisciplinary approach that is distinct from traditional lines of cybersecurity research? What new approaches or combinations of disciplines should be considered to effectively conduct research within this domain? Second, what new and unexplored challenges need to be addressed by researchers within this context?
3:50 PM	**Day 1 Wrap Up**	
5: 00 PM	**Reception & Networking (Sponsored by CSRA)**	

May 28

7:30 AM	**Registration**	
8:30 AM	**Welcome to Day 2 and Overview of Workshop**	
8:40 AM	**Keynote Address**	
9:05 AM	**Keynote Address**	
9:30 AM	**BREAK**	
	Breakout Sessions	
9:50 AM	**Session 7: Extant Architectures and Cybersecurity for Smart Cities** Participants will discuss planned Smart City deployments and their architectures, with the objective of identifying the "best fit" approaches for cybersecurity and privacy and risk analysis techniques in this area.	**Session 8: Privacy in Smart Cities** Smart City deployments necessitate examination of diverse scenarios that require consideration of users' privacy and personal data protection. Numerous use cases fall into this group, in such different areas as citizen-government interactions, transportation services, energy, or education. In this session, we discuss privacy engineering and general privacy principles for Smart Cities. What kind of privacy architecture would support the processing of information about individuals yet mitigate risks to their privacy? Participants will discuss challenges, processes, regulations, and technologies associated with privacy.
11:30 AM	**LUNCH**	
12:30 PM	**Session 9: Modular Architectures and Open Sensor Web** Modular architectures are an approach to design that divides a system into small subsystems that may be re-used in other deployments and that may promote interoperability. The system architecture is the combination of architecture modules that together scale to produce a system that meets the requirements. New solutions may be "plugged into" an existing modular system to produce a new solution without affecting the existing system. Open Sensor Web is one such modular architecture. Such sensors may be used to create applications for Smart Cities, such as flood gauges, traffic monitors, and stress gauges on bridges. Participants will discuss the methodology and suggest new uses for	**Session 10: Cryptography: Role and Implementation in Smart Cities** Cryptography provides mechanisms to protect sensitive information, devices, communications, and infrastructure in Smart City deployments. The session will study technologies, identify technology gaps, focus on current and emerging research issues, and highlight specific problems associated with enabling cybersecurity in smart city context. The session will be based on the evaluation of representative use cases illustrating the needs, concerns, and challenges of supporting confidentiality, integrity, and privacy with the help of novel encryption techniques in smart cities.

	modular architectures in conjunction with their own Smart City efforts.	
2:00 PM	**BREAK**	
2:40 PM	**Session 11: Research Priorities and Collaboration Models for Cybersecurity and Privacy in Smart Cities** In this session, we identify research priorities for cybersecurity and privacy in smart cities and adjacent issues as well as need for new approaches that could anticipate issues in this complex environment. We will also discuss collaboration and funding models, approaches, and processes to fill the gaps in such a dynamic and diverse environment as a Smart City.	**Session 12: Key Technologies for Smart Cities** The ambitious vision of smart cities challenges us to think more comprehensively about cyber security requirements, including security and privacy in key technologies. Recent advances in network technology, data management, device security, and other areas crucial for smart cities will be discussed in this session.
3:35 PM	**Day 2 Wrap Up**	
4:35 PM	**Workshop Closing, Comments, Feedback**	
5:05 PM	**Workshop End**	