AN INDUSTRY-ACADEMIC WORKSHOP

Standards Challenges and Cybersecurity: Implications for Distributed Systems (Business Infrastructure, Cloud Computing, Smart Grid/Smart Cities) and User Privacy

Hosted by the University of Pittsburgh
Sponsored by the National Institute of Standards and Technology (NIST)

Workshop Design by University of Pittsburgh, Energetics, and Northwestern University

November 20-21, 2014

WORKSHOP GOALS

The US industry is facing new opportunities and new threats that challenge technology operations and strategic, technology and innovation decisions including, particularly, concerns for safety and security. The increased prominence of the internet, exemplified by the emergence of smart grid/smart cities and cloud computing requires increased attention to the underlying role of standards and how emerging systems interoperate. Companies, operation managers, and strategic and cyber security professionals need to appreciate the competitive implications of how standards develop domestically and internationally and the value of participation in the standardization process. Attention to standards and standardization in cyber security planning and operations in business and engineering courses is called for but may be challenging to faculty.

This program looks at standardization in cyber security and emerging technologies and applications to complex "systems of systems". It is intended to support faculty in increasing coverage of standards. Action-oriented, it includes exercises and emphasizes discussion with presentations by both industry and academic experts on the contextual areas and potential teaching models.

The workshop, with active industry involvement throughout, has two interrelated components:

- Day 1 includes an overview leading into presentations by industry stakeholders with standards experts adding commentary and perspective; and,
- Day 2 (half-day) targets workforce education and training, related curricula and pedagogy and offers an experiential standards negotiation exercise (with content modified to fit targeted domain concerns) to enhance workshop participant' appreciation of subtle issues and suggest potential class approaches.

Both days feature breakouts with day 1 stressing discussion of industry challenges, requirements and implications for teaching and day 2 delving deeper into pedagogy and curricula/course challenges and approaches.

The program builds on workshops conducted in March and June 2013 at Northwestern University and UCLA, respectively. These focused on *smart systems* including smart grid, cloud, smart manufacturing and related supply chain issues and each drew some 45 very actively engaged participants from multiple units of 14 schools, 11 companies and 3 industry associations.

This workshop is being hosted by the University of Pittsburgh. The overall program is supported by the National Institute of Standards and Technology (NIST).

<u>Intended Workshop Outcomes</u>

- Identification of standardization issues within the identified domains;
- Actions by participants to more fully incorporate standards and standardization issues in their courses and training. This will be supported by dissemination of materials and discussion of adaptation for varying course settings;
- Movement, advanced through breakout discussion, toward an ongoing industry-university support community.

RELEVANT DOMAIN BACKGROUND

Cyber Security

The private and public sectors increasingly operate through complex, large-scale, highly distributed and highly interconnected systems. Though emerging technologies allow continuous monitoring and powerful analytic tools help to rapidly identify, assess and even predict threats, threats are increasing and evolving. Even major companies with robust internal risk management processes, appropriate and timely information exchange and mission critical functions find it difficult. It is a challenge to maintain confidentiality and privacy. While standards have been developed to insure adequate encryption and digital signatures, students educated in the business, engineering, and technical fields are often ignorant of existing and potential new standards and best practices for security in the system they build and manage.

Distributed Systems

Smart Grid (SG) responds to the pressing need for enhanced energy grid reliability, improved precision of monitoring and control, greater flexibility in energy sources, and allocation, ability to manage energy use more dynamically and overall reduction in energy cost. There are numerous stakeholders with varying perspectives and demands, and optimization of the overall grid may conflict with requirements of user segments. SG is highly complex and dynamic and must be continually reconfigured as new technology is developed and incorporated. A broader concept, ***Smart Cities (SC)*** varies in definition but generally refers to the use of innovative technologies, particularly information and communication technologies, to manage complex urban and resources and physical, cyber and knowledge infrastructures in a sustainable and growth-enabling way. As in smart grid initiatives smart cities require standards that respond to these characteristics and support interoperability and agility.

Collaborative Cloud Computing services, loosely defined, provide ubiquitous, virtual on-demand internet/network-based access to digitized information, storage, servers, software and applications. Smart Grid/Smart Cities (SG/SC) apply collaborative clouds that not only share facility and software resources but also share data and information for business and societal purposes. This is the case for individual businesses, municipalities and utilities. They have the potential to reduce capital expenditures significantly and the need for in-house expertise with increased flexibility in terms of media, work location and collaboration. But there are lingering concerns over migration paths, participation and choice, security, intellectual property, implied interoperability and portability across varying global infrastructure and regulatory frameworks. Related investment planning with changing technologies and inherent supply chain coordination issues further calls for carefully designed standards***.***

THE WORKSHOP EMPHASIS

Standards are important and support innovation, product development, etc. Standards can support innovation by giving confidence that new products, technologies and processes will be compatible with legacy systems, infrastructure and vendor capabilities, and will be accepted in the market. Standards development and selection will be influential in determining which technologies and approaches lead. Standards are especially important for new technology areas and challenges, such as those that exist in the cyber security realm. The increased prominence of the internet, exemplified by the emergence of smart grids, smart cities, and cloud computing, requires increased attention to the role of standards and how the emerging net-enabled systems interoperate. Not only do companies and industry need to appreciate the competitive implications of cyber security standards, so does the U.S. higher education system. Engineering and business schools at the undergraduate and graduate level teaching in the targeted domains need to understand the significance of standards, their technical aspects as well implications for operations and planning, but also strategic challenges of appropriate participation in their development.

AGENDA

Day 1 (9:00am – 5:15pm)

(8:30 doors open; coffee)

9:00 **Welcome**
Ronald Larsen, Dean and Professor, School of Information Science, University of Pittsburgh

9:10 **Laying out the challenges, why are we here**
Gordon Gillerman, Acting Director, Standards Coordination Office, National Institute of Standards and Technology (NIST)

9:25 **Overview of agenda**
Jeffrey Strauss, Acting Director, Northwestern BCICS CTIM

9:35 **Keynote: Call to Action**
Carl Cargill, Standards Principal at Adobe Systems / Advanced Technology Labs, previously Senior Director, Corporate Standards at Sun Microsystems

10:10 BREAK

10:20 **Industry/government stakeholder panel (domain and standards issues) Challenge to Education**

- NIST Smart Grid, Smart Cities and Cyber Security initiatives and frameworks
  Victoria Yan Pillitteri, Advisor for Information Systems Security, NIST; Chair, Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC)
- Distributed Systems Industry perspectives
  Heather Kreger, Distinguished Engineer, CTO International Standards, IBM
  Jeffery Stutzman, President, Wapack Labs Corporation

Discussion/Q&A
Facilitator: **Michael Spring**, Associate Professor, Information Science, University of Pittsburgh and NIST curricula development grantee

Noon Lunch

1:00 **Academic Perspectives**

- **David Tipper**, Chair, Telecommunications Program & Associate Professor, Information Science, University of Pittsburgh
- **David Thaw**, Asst. Professor, Law, and Information Science, University of Pittsburgh

2:00 **Breakouts (incl. break at participant discretion): industry challenges and implications for teaching**
2:00-2:15 Introductions and expectations – discussion will continue in day 2 breakouts
2:15-4:15 **Focal Questions**

- *What are key cybersecurity challenges facing industry in distributed systems that have standards underpinnings; how will standards impact?*

- *What are related implications/requirements for education? What needs to be covered in courses?*
- *What specific knowledge and skills will professionals need to support the target domains and related standardization?*
- ***Identify breakout group spokesperson and populate PowerPoint template slides***

4:15 **Reports, open discussion**

4:40 **Summary of day 1 lessons learned**
Linda Garcia, Professor, Communication, Culture and Technology, Georgetown University, former Project Director, Office of Technology Assessment, US Congress

5:00 **Lead into Day 2**
Jeff Strauss

5:15 **ADJOURN; OPEN DISCUSSION**

Day 2 (8:15am – 2:30pm)

(8:00 doors open, coffee)

8:15 **Exercise:** Cross-country/cross agenda Standards negotiation (**Jeff Strauss**)

9:45 BREAK

10:00 **Reports, Discussion of exercise, value and potential use/further adaptation in different courses/ institutional contexts**

10:40 **International and US standards education initiatives competition and models (links provided to US materials)**
Erik Puskar, Group Leader, Global Standards & Information, Standards Coordination Office, National Institute of Standards & Technology (NIST)

11:00 **Breakouts (same groups as in day 1): Pedagogy challenges and approaches - Focal questions:**

- *What are challenges to related teaching (materials, faculty knowledge, course content, etc.)? How can these be overcome?*
- *How might standards content be incorporated into the curricula (fit)? Consider business, engineering and other possible "homes" and specific courses; what are course/discipline specific issues and how can they be addressed?*
- ***Identify breakout group spokesperson and populate PowerPoint template slides***

Other questions for consideration

- *What specific knowledge and skills will professionals need to support the target domains and related standardization?*
- *How does this enhance or detract from course/curricula goals and university mission?*
- *What types of support and assistance could help better enable the integration of education standards in cybersecurity related curriculum?*

- *What are specific initiatives and actions that universities and educators can do immediately to promote educational standards in cybersecurity curriculum?*
- *What will each of you do individually following this workshop?*

12:30 **Lunch**

Patrick Gallagher, Chancellor, University of Pittsburgh, former Deputy Secretary of the U.S. Department of Commerce and Director of the National Institute of Standards and Technology (NIST); Introduced by Michael Spring

1:30 **Break out reports, discussion**

2:00 **Wrap-up discussion: Next Steps** (Moderator: **Jeff Strauss)**

2:30 **ADJOURN**