



**Homeland
Security**

**Science & Technology Directorate, US DHS
National Cyber Security Division, US DHS
Office of the Secretary of Defense, US DOD
National Institute of Standards and Technology
US Department of Energy**

**Operations, Plans & Requirements (A3/5), HQ USAF
Logistics, Installations, & Mission Support (A4/7), HQ USAF
*In Collaboration with the following states: Delaware, District of
Columbia, Maryland, New Jersey, New York, Pennsylvania, Virginia,
West Virginia (members of the All Hazards Consortium)***

**Workshop on
Future Directions in Cyber-physical Systems Security
July 22-24, 2009
Gateway Hilton Newark Penn Station
Gateway Center, Newark, NJ 07102**

Overview

Cyber-physical systems (CPS) are characterized by the tight coupling and coordination among sensing, communications, computational and physical resources and are exhibited in many application areas including industrial control systems (ICS). ICS encompass several types of control systems including: supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). CPS are prevalent in almost every critical infrastructure sector such as: electricity, water, gas, transportation, chemical, and healthcare. Interconnections of cyber-physical systems form complex systems with interdependencies within a given sector as well as across sectors. For example, the electric power grid of today forms one of the largest and most complex systems of power generation, transmission, and distribution systems at local, regional, and national level. It is envisioned that the complexity of the cyber-physical systems of the future will far exceed that of today's. Such a complexity poses several research challenges related to resiliency, vulnerability, threat, and recovery assessment. There is a need for models, theories, methods, and tools to address the security of cyber-physical systems taking into account the cyber and physical components of a system in an Integrated and unified way and realizing the discrete and continuous aspects of the system.

Program Committee

- **Nabil R. Adam, DHS-S&T (Program Chair) nabil.adam@dhs.gov**
- Michael Aimone, U.S. Air Force
- S. Massoud Amin, U of Minnesota
- Elisa Bertino, Purdue U
- Alvaro Cardenas, UC Berkeley
- Peter Chen, Louisiana State U
- Lydia Duckworth, The MITRE Corporation
- Ronda Dunfee, U.S. DOE
- George Gross, UIUC
- Mark Hadley, Pacific Northwest NL
- Steve Hawkins, Raytheon Intelligence and Information Systems
- Clas A. Jacobson, United Technologies
- Sushil Jajodia, GMU
- Antwane Johnson, Office of the Secretary of Defense
- Bruce Larson, American Water Works, Inc. and Water Sector Coordinating Council
- Insup Lee, U of Pennsylvania
- Chung-Sheng Li, IBM
- Marija D. Ilic, CMU
- Sean P. McGurk, National Cyber Security Division, DHS
- Frank Mueller, NCSU
- Raj Rajkumar, CMU
- Riley Repko, US Air Force
- William H. Sanders, UIUC
- Ronald M. Sega, Colorado State U
- Kang G. Shin, The Univ. of Michigan
- Lawrence Skelly, DHS-S&T (General Chair)
- James A. St. Pierre, NIST
- John A. Stankovic, U of Virginia
- Kevin Sullivan, Microsoft
- Bhavani Thuraisingham, U Texas at Dallas
- Bill Woodward, DHS/TSA
- Yelena Yesha, UMBC

Workshop Goals and Objectives

The objective of the workshop is to provide a forum for

- i) representatives from various government agencies to briefly present their strategic vision of securing the cyber-physical systems as it relates to the nation's critical infrastructures;
- ii) researchers from academia, industry and national laboratories to assess the state of the art, identify related R&D challenges, and propose solutions to address these challenges;
- iii) subject matter experts, practitioners and state and local representatives to discuss their perspectives on the current state of the security of cyber-physical systems; where should the technology and science be in 5-10 years from now; why we are not there now - What are some of the challenges that are in the way of to be there now?; and why do we need to be there? That is, what legitimate case can be made to justify the needed R&D investments?

The results of the workshop will help DHS-S&T formulate near and long term investment decisions as well as research strategies, plans and objectives for cyber-physical systems security.

Classification

The workshop will be conducted as **Unclassified**.

Workshop Structure and Format

Format for the workshop:

- Keynote Speakers
- Presentations, Panels, posters – The presentations and panels will be discussing background useful for the breakout sessions
- Breakout sessions and reports

Submission Requirements

Presentations at the workshop will be by invitation. If interested, please submit 3-page position paper (excluding references).

Papers not selected for presentations at the workshop will be considered for a poster session.

Workshop discussions will focus on identifying detailed research challenges and promising avenues for satisfying the unique security needs in cyber-physical systems. Infrastructure sectors of special interest include Electricity, Chemical, Transportation, Drinking Water/Wastewater, and Healthcare.

A position paper should address one or more of the following questions. Authors should feel free to add more questions as they see fit.

- What makes CPS security different from traditional IT security?
- What is the current state-of-the-art in CPS security?
- What are some grand challenges for CPS security?
- Can different degrees of security be applied to CPS?
- Can security and hard real-time constraints co-exist?
- What physical properties of CPS influence security/cryptography and vice-versa?
- How does network infrastructure need to change in order to support security in large-scale distributed CPS?



Homeland Security

- What new scientific foundations (e.g. temporal security, dynamics-based cryptography, location-based encryption/decryption) need to be explored for security in CPS?
- Does the distributed nature of ICS and critical infrastructure help or hinder security? How can any hindrances be removed?
- What are good architectures and programming paradigms for secure CPS?
- What new operating systems, components and services are suited for securing CPS?
- What human factors challenges that are unique to CPS security?
- What are possible appropriate analytical frameworks for the assessment of CPS reliability, security, and risk?
- What are the viable approaches for addressing economics of security measures so as to justify related expenditures?
- How can we address the formulation of appropriate policy for security measures?

Poster Submission

Inviting one page submission for Posters. The deadline for submitting the poster description is July 6, 2009. Please email a pdf copy of the description to Basit Shafiq at basit@andromeda.rutgers.edu

For more information, please visit <http://cimic.rutgers.edu/>

Paper Submission

Submission site: <http://www.easychair.org/conferences/?conf=cpssw09>

Important Dates

- **July 6, 2009** – Deadline for submitting poster description.
- ~~June 1, 2009~~ **Extended** Deadline for Position paper submission: **June 8, 2009**
- **June 29, 2009**- Author notification
- **July 22-24, 2009**- Workshop

Travel and Lodging Support for Students

PhD students are encouraged to apply for Travel & Lodging support - the first 6 students will receive such a support. To apply for travel & lodging support, Please send a copy of your resume including a description of your research work to "Mr. Ron Bilbrey" at Ron.Bilbrey@associates.dhs.gov. Also copy Dr. Nabil Adam (Nabil.Adam@dhs.gov) in the email. For more information, please visit <http://cimic.rutgers.edu/>

Registration

Workshop attendance is open subject to space availability, with July 10 as the cut-off date. Workshop registration is free. For registration detail and for an up-to-date copy of this workshop write up, please visit:

<http://cimic.rutgers.edu/>

or

<http://www.enstg.com/signup/passthru.cfm?ConferenceCode=WOR89068>

Workshop Venue

This workshop is scheduled for July 22-24, 2009 at the Hilton Newark Penn Station, Newark, NJ

Hotel Accommodation



Hilton Newark Penn Station

Gateway Center - Raymond Blvd, Newark, New Jersey, United States 07102-5107

Tel: 1-973-622-5000 Fax: 1-973-824-2188. The hotel offers a block of rooms at the government rate of \$133.00 per night, with July 6 as the cut –off date.

Travel

1. Flying

i. Newark International Airport

Distance from hotel: 5 mi.

Drive time: 15 min.

Directions to Hilton Gateway:

Car - From airport, take route 9 to route 21. It will turn into McCarter Highway. Proceed down route 21 North for 2.5 miles. Make right hand turn onto Market Street. At next light turn left onto Raymond Plaza West. Hotel is on left.

Shuttle – Courtesy Bus HRLY-Call for PU 11PM-6AM

Taxi- Approx. 15.00 USD from airport

Train – Take AirTrain Newark to the Newark Liberty International Airport Station and purchase a ticket for a NJ TRANSIT to Newark Penn Station. Hilton Gateway is across the street from Newark Penn Station.

ii. John F. Kennedy International Airport

Distance from hotel: 24 mi.

Drive time: 1 hr.

Directions to Hilton Gateway:

Car - From airport, take the Van Wyck expressway to Belt Parkway to over the Verrazano-Narrows Bridge. Follow the signs for Goethals Bridge to the New Jersey turnpike north to Exit 15. Raymond Boulevard go west for 2.5 miles. Hotel on left.

Taxi- Approx. 60.00+ USD from airport

iii. La Guardia Airport

Distance from hotel: 22 mi.

Drive time: 40 min.

Directions to Hilton Gateway:

Car - Follow signs for BQE/278W. Take Exit 35 and follow signs for the Queens Midtown Tunnel. After tunnel, follow signs for Lincoln Tunnel. NJ Tpke South to Exit 15W (280W). Exit 15A (RT 21 S). Left onto Raymond Blvd., hotel on right.

2. Trains from Washington/Boston Area – Coming from Washington or Boston Area, take an Amtrak Train to Newark Penn Station. Hilton Gateway is across the street from Newark Penn Station.



**Workshop on Future Directions in Cyber-physical Systems Security
AGENDA
Wednesday July 22, 2009**

12:00-1:00 pm	Registration (Outside Garden State Ball Room)
1:00-1:10 pm	Workshop Kickoff Nabil Adam , DHS-Science and Technology Directorate (Garden State Ball Room)
1:10-1:25 pm	Welcome Address by Christopher Doyle , DHS-Science and Technology Directorate (Garden State Ball Room)
1:25-1:55 pm	DHS Perspective Speaker- Philip Reiting , Deputy Undersecretary of National Protection & Programs Directorate, DHS (Garden State Ball Room)
1:55-2:25 pm	NSF Perspective Speaker- Jeannette Wing , Asst. Director, National Science Foundation (Garden State Ball Room)
2:25-2:40 pm	Break
2:40-3:10 pm	DOE Perspective Speaker- Thomas Malec , Department of Energy (Garden State Ball Room)
3:10-3:40 pm	NIST Perspective, Speaker- George Arnold , National Coordinator for Smart Grid Interoperability (Garden State Ball Room)
3:40-4:00 pm	NJHSP Perspective, Speaker- Richard L. Cañas , NJ Office of Homeland Security and Preparedness (Garden State Ball Room)
4:00-4:15 pm	Break
	Owners/Operators and State Representatives Panel (Garden State Ball Room)
4:15-5:45 pm	Speaker—Representatives from Valero, Verizon, Bank of America and American Water State Representatives: K. Wood (MD), S. Popat (DC), R. Dixon (WV), R. Keener , M. McAllister (VA), J. Conrey (NJ), TBA (NY), TBA (PA), and E. Starkey (DE). (members of the All Hazards Consortium) Chair – Joe Conrey
6:00-7:30 pm	Reception (Essex Room)



Workshop on Future Directions in Cyber-physical Systems Security

AGENDA

Thursday July 23, 2009

7:00-8:00 am	Continental Breakfast (Bergen Room)		
8:00-8:10 am	Welcome Back Christopher Doyle , DHS-Science and Technology Directorate (Garden State Ball Room)		
8:10-8:30 am	Welcome Remarks by Mildred Crump , City Council President, Newark, NJ (Garden State Ball Room)		
8:30-9:00 am	DOD Perspective Speaker- Robert F. Lentz , Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance, DOD (Garden State Ball Room)		
9:00-10:30 am	Industry Panel (Garden State Ball Room)		
	Microsoft (Kevin Sullivan), IBM (Chung-Sheng Li) Raytheon (Steve Hawkins), United Technologies (Clas Jacobson), Cisco Systems (Dave Dalva), Siemens (Yan Lu) Chair – Riley Repko, USAF		
10:30-10:45 am	Break		
10:45-12:15 pm	Position Paper Sessions (parallel sessions) See below for list of papers in each session		
	Session 1 Chair – Raj Rajkumar (Monmouth Room)	Session 2 Chair – Peter Chen (Seth Boyden Room)	Session 3 Chair – Insup Lee (Menlo Park Room)
12:15-1:15 pm	Lunch (on your own)		
1:15-2:45 pm	Sectors Panel (Garden State Ball Room)		
	Lydia Duckworth (Healthcare); Walter Heimerdinger (Process Control); Scott Lintelman (Air Transportation); Paul Myrda (Electricity) Chair – Dr. William Sanders, UIUC		
2:45 – 3:00 pm	Break		
3:00-4:15 pm	Breakout Sessions (Working Groups 1 – 3)		
	WG1.1 Chair– Riley Repko Co-chairs– Lydia Duckworth; Scott Lintelman; (Monmouth Room)	WG2.1 Chair– James St. Pierre Co-chairs– Stephen Curren; Mark Hadley; Cherrie Black (Seth Boyden Room)	WG3.1 Chair– Norman Fosmire Co-chairs– Richard Andres; Michael Mason; Cal Jaeger (Menlo Park Room)
4:15-4:30 pm	Break		
4:30-5:30 pm	Breakout Reports (Garden State Ball Room)		
	WG1.1 Report, Speaker: Riley Repko ; WG2.1 Report, Speaker: James St. Pierre ; WG3.1 Report, Speaker: Norman Fosmire ;		
5:30-6:45 pm	Poster Session (Garden State Ball Room)		



**Workshop on Future Directions in Cyber-physical Systems Security
AGENDA
Friday July 24, 2009**

6:45-7:45 am	Continental Breakfast (Bergen Room)		
7:45-8:30 am	Venture Capital Firms Panel (Garden State Ball Room)		
	Speaker – Jack Biddle, Novak Biddle Elad Yoran, Security Growth Partners LLC Edward Merrill, Granite Gate Corp. Chair – Riley Repko, USAF		
8:30-9:15 am	Position Paper (Garden State Ball Room) See below for list of papers in this session		
	Session 4 Chair – Yelena Yesha		
9:15-10:30 am	NSF/NITRD Panel (Garden State Ball Room)		
	Ty Znati (NSF) Helen Gill (NSF) Lenore Zuck (NSF) Frankie King (NITRD) Chair – Raj Rajkumar (CMU)		
10:30-10:45 am	Break		
10:45-12:00 pm	Breakout Sessions (Working Groups 1 – 3)		
	WG 1.2 Chair– George Gross Co-chairs– Craig Rieger; Clas Jacobson (Monmouth Room)	WG 2.2 Chair– Raj Rajkumar Co-chairs– Cal Jaeger; Dave Dalva (Seth Boyden Room)	WG 3.2 Chair– Peter Chen Co-chairs– Steven Fernandez; Walter Heimerdinger (Menlo Park Room)
12:00-1:00 pm	Breakout Reports (Garden State Ball Room)		
	WG1.2 Report, Speakers: George Gross WG2.2 Report, Speakers: Raj Rajkumar WG3.2 Report, Speakers: Peter Chen		
1:00 – 1:10 pm	Closing Remarks by Nabil Adam (Garden State Ball Room)		
1:10 pm	Adjourn		

Position Paper Session 1

Thursday July 23, 2009

11:00am – 12:30pm

Location: Monmouth Room**Session Chair:** Raj Rajkumar

1. Frank Mueller and Subhashish Bhattacharya. Cyber Security for Power Grids. (**Power Grid Security**)
2. Blake Boyer, Mohsen Jafari and Dong Wei. Cyber-related Risk Assessment and Critical Asset Identification within The Power Grid. (**Power Grid Security**)
3. Art Conklin. Security in Cyber-Physical Systems. (**CPS Security Challenges/Issues – General**)
4. Indrakshi Ray and Indrajit Ray. Access Control Challenges for Cyber-Physical Systems. (**Security Policies/Trust**)
5. Sam Clements, Mark Hadley and Thomas Edgar. NACIO Non-obtrusive Authentication of Critical Infrastructure Operators. (**Methodology/Technique**)
6. Adrian Chavez. Protecting Process Control Systems Against Lifecycle Attacks Using Trust Anchors. (**Methodology/Technique**)
7. David Dittrich. Visualizing Secure Cyber-Physical Systems. (**CPS Security Challenges/Issues – General**)

Position Paper Session 2

Thursday July 23, 2009

11:00am – 12:30pm

Location: Seth Boyden Room**Session Chair:** Peter Chen

1. Kevin Sullivan. Information Security Practices for Industrial Control Systems. (**Security Practices/Policies/Trust**)
2. Partha Pal, Rick Schantz, Kurt Rohloff and Joseph Loyall. Cyber-physical Systems Security - Challenges and Research Ideas. (**CPS Security Challenges/Issues – General**)
3. Chris Codella, Arun Hampapur, Chung-Sheng Li, Dimitrios Pendarakis and Josuyla Rao. Continuous Assurance for Cyber Physical System Security. (**CPS Security Challenges/Issues – General**)
4. Michael McDonald and Bryan Richardson. Position Paper: Modeling and Simulation for Process Control System Cyber Security Research, Development and Applications. (**Modeling/simulation; Methodology/Technique**)
5. Mukesh Singhal and Yelena Yesha. Protecting Water Bodies and Systems Against Waterborne Biochemical Warfare. (**Water Distribution Infrastructure Security**).
6. Michael Kirkpatrick, Elisa Bertino and Frederick Sheldon. Restricted Authentication and Encryption for Cyber-physical Systems. (**Methodology/Technique**)
7. Vineela Muppavarapu and Soon Chung. Role-Based Access Control for Cyber-Physical Systems Using Shibboleth. (**Methodology/Technique**)

Position Paper Session 3

Thursday July 23, 2009

11:00am – 12:30pm

Location: Menlo Park Room

Session Chair: Insup Lee

1. Anupam Joshi, Tim Finin, Yelena Yesha, Wenjia Li and Palanivel Kodeswaran. A Policy and Trust Driven Framework for Securing Cyber Physical Systems. (**Security Policies/Trust**)
2. Mu Sun, Sibin Mohan, Lui Sha and Carl Gunter. Addressing Safety and Security Contradictions in Cyber-Physical Systems. (**CPS Security Challenges/Issues – General**)
3. Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig and Shankar Sastry. Challenges for the Security of Cyber Physical Systems. (**CPS Security Challenges/Issues – General**)
4. Anthony Wood, Vijay Srinivasan and John Stankovic. Autonomous Defenses for Security Attacks in Pervasive CPS Infrastructure. (**Methodology/Technique**)
5. Gordon Skelton. Cyber-Physical Security for Wireless Sensor Networks: Position Paper. (**Wireless Sensor Network/General**)
6. Aloysius Mok. Position paper for Future Directions in Cyber-physical Systems Security (**CPS Security Challenges/Issues – General**)
7. Steven Fernandez and Waseem Naqvi. Cyber Physical Systems Requirements to Mitigate Stress Points by Introduction of Distributed Energy Resources into Scalable Grid Environment. (**Power Grid Security**)
8. Damian Watkins. Towards an Evolvable Cyber Security Protection Profile for Electronic Medical Records to Ensure Privacy and Security. (**Healthcare sector**).

Position Paper Session 4

Friday July 24, 2009

8:15am – 9:00pm

Location: Garden State Ball Room

Session Chair: Yelena Yesha

1. Clifford Neuman. Challenges in Security for Cyber-Physical Systems. (**General issues/CPS challenges**).
2. Dong Wei, Yan Lu and Paul Skare. Power Infrastructure Security: Fundamental Insights of Potential Cyber Attacks and Their Impacts on the Power Grid. (**Power Grid Security**).
3. Bhavani Thuraisingham, I-Ling Yen, Sajal Das, Yonghe Liu, Elisa Bertino, and Lorenzo Martino. Secure Semantic Service Oriented Information Grid for Cyber-Physical Applications. (**Security Policies/Trust/Practices; Information Grid**).