Workshop Proposal to INFOCOM 2016

1 Workshop Title, Scope and Topics

Title
IEEE International Workshop on Cross-Layer Cyber-Physical Systems Security (CPSS)

Scope
The research of Cyber-Physical Systems (CPS) security addresses the security issues among close interactions and feedback loop between the embedded cyber components for computing and control and the dynamic physical components that involve mechanical components, human activities and surrounding environment. Example CPS systems include automotive and transportation systems, smart home, building and community, smart battery and energy systems, surveillance systems, cyber-physical biochip, and wearable devices. The recent advances of manufacturing technologies, system integrations and software platforms bring enormous challenges and opportunities for CPS design and implementation. However, the increasing complexity of networked computing systems makes modern network systems vulnerable to various attacks against their resources, infrastructure, and operability. The purpose of this workshop is to bring together researchers from a broad community, presenting state-of-the-art security solutions crossing software and hardware layers towards trustworthy CPS development and to motivate new research topics and directions in this interdisciplinary area.

Topics
The topics of interests to this workshop include (but are not limited to):
1. Cross-layer cyber system modeling and optimization for CPS Security
2. Real-time embedded system design and scheduling for CPS Security
3. Resilient and robust network system design for CPS Security
4. User privacy in CPS
5. Sustainability for CPS
6. Security in emerging applications such as automotive and transportation system, smart energy system, internet of things, biomedical system and smart health
7. Cross-layer solutions for CPS protection
8. Hardware Trojans detection in embedded hardware platforms
9. Hardware root-of-trust
10. Cross-layer hardware/software attacks and protections
11. Hardware-supported trustworthy CPS platforms
12. Topographic and data flow modeling for cyber physical system security
13. Countermeasures for backdoors and in the software-hardware interface
14. Formal verification for CPS Security

2. The Workshop Organization Team

Mark Tehranipoor, University of Florida, tehranipoor@ece.ufl.edu
Shiyan Hu, Michigan Technological University, shiyan@mtu.edu
Xin Li, Carnegie Mellon University, xinli@cmu.edu
Yier Jin, University of Central Florida, yier.jin@eecs.ucf.edu

The workshop organization team is composed by researchers who have significant experience in conference organization and have been working in various CPS- and cybersecurity-related areas for years. The biographies of organizers are attached in this proposal.

3. Rationale

INFOCOM is the leading conference in which the publications describe significant and innovative research contributions to the field of computer and data communication networks. The research topics of CPS Security have a significant overlap with the INFOCOM themes and there are mutual benefits between the INFOCOM and the proposed CPS Security workshop. Network level research outcomes will help construct more efficient and secure CPS network and the CPS provides the network research an important application driver. However, there are also some major differences between the workshop and INFOCOM regarding the paper submissions. While INFOCOM may solicit papers from a broad aspect covering different areas of computer and data communication networks. The proposed workshop only focuses on the CPS Security-related research either from a theoretical aspect or from a practical angle.

Researchers from government, industry and academia have recently understood the importance of CPS Security and started to realize the gap between the existing solutions/research and the industrial requirements. This fact has recently attracted many researchers of different background to join this area to develop interdisciplinary solutions to solve challenges in CPS Security and related area. The development of CPS Security not only impacts our daily life but also directly links to national security. The continuing trend of replacing existing isolated industrial controlling system with network supported CPS imposes an urgent request for CPS-oriented forums where researchers can share their findings, discuss new solutions, and come up with collaborative groups for new breakthroughs.

Given the importance of CPS Security, a community is emerging with members from cybersecurity, CPS, and hardware security areas. The lack of a CPS Security dedicated forum hampers with the growth of this community such that many CPS Security papers have been submitted to conferences with a broad audience. The impact of these submissions is thus lowered while interested audience has to go through many different conferences to find the relevant work. However, the proposed CPS Security workshop, for the first time, provides CPS Security researchers a forum dedicated for CPS Security related work. The reviewers will be invited from related areas so that all submissions will be rated objectively. Being the first CPS Security related workshop and considering the large CPS Security community, we are confident that this workshop will attract a significant number of high quality submissions.

As we mentioned above, there are no similar workshop or conferences dedicated for CPS Security research. The proposal of this workshop will fill the gap so that CPS Security researchers will have their dedicated forum for sharing their work. Some top network and embedded system conferences, including INFOCOM, have already put CPS Security as one topic of interest. However, being listed as one topic of interest prevents audience from realizing the importance of research in this area. While the impact of CPS Security is at a national level, we strongly believe that a CPS Security dedicated workshop is a necessity.

4. Workshop Committee

Workshop Co-Chairs:
 Mark Tehranipoor, University of Florida
 Shiyan Hu, Michigan Technological University
 Xin Li, Carnegie Mellon University
 Yier Jin, University of Central Florida

Wenye Wang, North Carolina State University
Min Song, Michigan Technological University
Nei Kato, Tohoku University, Japan
Yingying Chen, Stevens Institute of Technology
David Du, University of Minnesota
Yi Qian, University of Nebraska
Peter Mueller, IBM Zurich Research Lab, Switzerland
Mario Gerla, University of California at Los Angeles
Tommaso Melodia, Northeastern University

5. Workshop Tentative Schedule

Submission Deadline: Friday, December 18, 2015
Review Deadline: Friday, January 22, 2016
Notification of Acceptance: Friday, February 5, 2016
Camera-Ready Version: Friday, February 19, 2016
Program Ready: Friday, March 4, 2016

6. Workshop Format

The workshop will last one day, consisting of the following components:

1. *Keynote speech*: We plan to invite a well-established expert to deliver a keynote speech. The keynote will last 60 minutes. It is expected to focus on an emerging area of CPS Security.
2. *Invited talk*: About four 30-minute talks will be invited from both industry and academia. These talks will cover the state-of-the-art research and development activities in the area of CPS Security.
3. *Regular talk*: Oral presentations will be solicited by broadly distributing a CFP. About six regular talks will be selected by the workshop TPC. Each regular talk will be 15 minutes.
4. *Panel discussion*: About five senior persons in the CPS Security community will be invited to form a panel and discuss the challenges and opportunities for CPS Security. The panelists will be carefully chosen from both academia and industry to carry the opinions from both worlds.
5. *Poster session*: We expect to solicit 15+ posters to further motivate interactive discussions and boost workshop attendance.

7. Previous Workshop

This is the first time that we propose the INFOCOM CPS Security workshop and hence there is no past workshop in history.

Biographies of Organizers

Dr. Mark M. Tehranipoor is currently the Intel Charles E. Young Professor in Cybersecurity at the Department of Electrical and Computer Engineering, the University of Florida. His current research projects include: hardware security and trust, electronics supply chain security, counterfeit IC detection and prevention, and reliable and testable VLSI design. Prof. Tehranipoor has published over 250 journal articles and refereed conference papers and has given more than 150 invited talks and keynote addresses since 2006. In addition, he has published six books and ten book chapters. His projects are sponsored by both the industry (Semiconductor Research Corporation (SRC), Texas Instruments, Freescale, Comcast, Honeywell, LSI, Mentor Graphics, Juniper, R3Logic, Cisco, Qualcomm, MediaTeck, etc.) and the Government (NSF, ARO, MDA, DOD, AFOSR, DOE, etc.). He is a recipient of several best paper awards, the 2009 NSF CAREER award, the 2014 MURI award, the 2008 IEEE

Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2010 IEEE CS Most Successful Technical Event for co-founding and chairing HOST Symposium, the 2009 and 2014 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award.

Mark serves on the program committee of more than a dozen leading conferences and workshops. Prof. Tehranipoor served as the guest editor for JETTA, IEEE Design and Test of Computers, and IEEE Computer Society Computing Now. He served as Program Chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T-2009 and DFTS-2009, and Vice-general Chair for NATW-2011. He served as associate Editor-in-Chief (EIC) for IEEE Design and Test of Computers from 2012-2014. He is currently serving as an Associate Editor for IEEE Design and Test of Computers, an Associate Editor for JETTA, an Associate Editor for Journal of Low Power Electronics (JOLPE), an Associate Editor for ACM Transactions for Design Automation of Electronic Systems (TODAES). He has served as an IEEE Distinguished Speaker and an ACM Distinguished Speaker from 2010-2013. Prof. Tehranipoor is a Senior Member of the IEEE, Golden Core Member of IEEE Computer Society, and Member of ACM and ACM SIGDA.

Dr. Shiyan Hu received his Ph.D. in Computer Engineering from Texas A&M University in 2008. He is currently an Associate Professor in the Department of Electrical and Computer Engineering at Michigan Technological University, where he is Director of the Michigan Tech Cyber-Physical System Research Group, Co-Director of Michigan Tech Institute of Computing and Cybersystems, and Director of the Michigan Tech VLSI CAD Research Lab. He was a Visiting Professor at IBM Research (Austin) during summer 2010, and he is a Visiting Associate Professor at Stanford University starting August 2015.

Shiyan is the Founding Chair for IEEE Technical Committee on Cybernetics for Cyber-Physical Systems. His research interests include Computer-Aided Design of VLSI Circuits, Embedded Systems, Cyber-Physical Systems and Cybersecurity, where he has published about 100 refereed papers, including 20+ in the premier IEEE Transactions. He is an ACM Distinguished Speaker, a recipient of ACM SIGDA Richard Newton DAC Scholarship (as the faculty advisor), a recipient of Faculty Invitation Fellowship from Japan Society for the Promotion of Science (JSPS), and a recipient of the National Science Foundation (NSF) CAREER Award. His papers have been nominated for IEEE/ACM ICCAD William J. McCalla Best Paper Award in 2009 and IBM Pat Goldberg Best Paper Award in 2008 and 2010. Dr. Hu is an Associate Editor/Guest Editor for 5 IEEE/ACM Transactions including IEEE Transactions on Circuits and Systems, IEEE Transactions on Computers, IEEE Transactions on CAD, IEEE Transactions on Industrial Informatics and ACM Transactions on Embedded Computing Systems. He has served as General Chair, Technical Program Committee (TPC) Chair, TPC Subcommittee Chair, Session Chair, and TPC Member for various conferences for more than 70 times, which include the TPC Subcommittee Chair for IEEE/ACM Design Automation Conference (DAC) in 2014 and 2015, and IEEE/ACM International Conference on Computer Aided Design (ICCAD) in 2011. He is a Senior Member of IEEE.

Dr. Xin Li Xin Li received the Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA in 2005, and the M.S. and B.S. degrees in Electronics Engineering from Fudan University, Shanghai, China in 2001 and 1998, respectively.

He is currently an Associate Professor in the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA. In 2005, he co-founded Xigmix Inc. to commercialize his PhD research, and served as the Chief Technical Officer until the company was acquired by Extreme DA in 2007. In 2011, Extreme DA was further acquired by Synopsis (Nasdaq: SNPS). From 2009 to 2012, he was the Assistant Director for FCRP Focus Research Center for Circuit & System Solutions (C2S2), a national consortium of 13 research universities (CMU, MIT, Stanford, Berkeley, UIUC, UMich, Columbia, UCLA, among others) chartered by the U.S. semiconductor industry and U.S. Department of Defense to work on next-generation integrated circuit design challenges. From 2014 to 2015, he was the Assistant Director for the Center for Silicon System Implementation

(CSSI), a CMU research center with 20 faculty members working on integrated circuits and systems. His research interests include integrated circuit and signal processing.

Dr. Xin Li has been an Associate Editor of IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems (TCAD), ACM Trans. on Design Automation of Electronic Systems (TODAES), IEEE Design & Test (D&T), and Journal of Low Power Electronics (JOLPE). He served on the Executive Committee of ACM SIGDA, the IEEE Systems, Man, and Cybernetics Society Technical Committee on Cybernetics for Cyber-Physical Systems, the IEEE Computer Society Technical Committee on VLSI, the ACM/SIGDA Outstanding PhD Dissertation Award Selection Committee, the IEEE Outstanding Young Author Award Selection Committee, the Technical Program Committee of Design Automation Conference (DAC), and the Technical Program Committee of International Conference on Computer-Aided Design (ICCAD). He received the NSF Faculty Early Career Development Award (CAREER) in 2012, the IEEE Donald O. Pederson Best Paper Award in 2013, a Best Paper Award from Design Automation Conference (DAC) in 2010, two IEEE/ACM William J. McCalla ICCAD Best Paper Awards in 2004 and 2011, and a Best Paper Award from International Symposium on Integrated Circuits (ISIC) in 2014.

Dr. Yier Jin is currently an assistant professor in the EECS Department at the University of Central Florida. He received his PhD degree in Electrical Engineering in 2012 from Yale University after he got the B.S. and M.S. degrees in Electrical Engineering from Zhejiang University, China, in 2005 and 2007, respectively. His research focuses on the areas of trusted embedded systems, trusted hardware intellectual property (IP) cores and hardware-software co-protection on computer systems. He proposed various approaches in the area of hardware security, including the hardware Trojan detection methodology relying on local side-channel information, the post-deployment hardware trust assessment framework, and the proof-carrying hardware IP protection scheme. He is also interested in the security analysis on Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era.

Dr. Jin is the guest editor of IEEE Transactions on Multi-Scale Computing Systems. Special Issue/Section on Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing. He is also the associate editor of IEEE SMC Society Technical Committee on CCPS Newsletter. He serves and has served on the Organizing Committees and Technical Program Committees of many Conferences and Workshops including DAC, ICCAD, ASP-DAC, HOST, ISVLSI, ATS, ICCD, etc. He is the best paper award recipient of the 52nd Design Automation Conference in 2015.