

## ORGANIZING COMMITTEE

### Workshop Co-Chairs

**Kewei Sha**  
University of Houston – Clear Lake,  
USA

**Xiaohui Liang**  
University of Massachusetts Boston,  
USA

### Technical Program Committee (tentative)

**Keke Chen**  
Wright State University, USA

**Songqing Chen**  
George Mason University, USA

**Mauro Conti**  
University of Padua, Italy

**Gul Khan**  
Ryerson University, Canada

**Hongwei Li**  
University of Electronic Science and  
Technology of China, China

**Wenjia Li**  
New York Institute of Technology, USA

**Xiaodong Lin**  
University of Ontario Institute of  
Technology, USA

**Rongxing Lu**  
Nanyang Technological University,  
Singapore

**Mohamed Mahmoud**  
Tennessee Technological University,  
USA

**Shrirang Mare**  
Dartmouth College, USA

**Chia-Ho Ou**  
National Pingtung University

**Tim Pierson**  
Dartmouth College, USA

**Jun Shao**  
Zhejiang Gongshang University, China

**Sheng Bo**  
University of Massachusetts Boston,  
USA

**Dongwan Shin**  
New Mexico Tech, USA

**Weichao Wang**  
University of North Carolina at  
Charlotte, USA

**Zhiwei Wang**  
Nanjing University of Posts and  
Telecommunications, China

**Wei Wei**  
University of Houston – Clear Lake,  
USA

**Yafei Yang**  
Qualcomm. LLC, USA

**Sherali Zeadally**  
University of Kentucky, USA

**Kuan Zhang**  
University of Waterloo, Canada

**Haojin Zhu**  
Shanghai Jiao Tong University, China

# The First International Workshop on SECURITY, PRIVACY, and TRUSTWORTHINESS IN MEDICAL CYBER PHYSICAL SYSTEM (MedSPT 2016)

Washington DC, USA, June 27-29, 2016

Medical Cyber Physical Systems (MCPS) are life-critical, context-aware, and networked systems of medical devices that provide tight integration and coordination between the cyber world of computing and communications and the physical world. Recent advances in mobile and wearable healthcare, communication, and Cloud computing technologies are making MCPS a promising platform for scientific advancement and development of new tools that may improve patients' health and wellbeing. Coming along with the potential social economic and personal healthcare benefits are significant security, privacy, and trustworthiness challenges in MCPS, due to unreliable embedded software controlling medical devices, weak computing and networking capabilities of medical devices, and adaptive privacy requirements introduced by complicated physiological dynamics of patient bodies. So far, the security, privacy, and trustworthiness initiatives for MCPS are still at an early stage. On one hand, more and more concerns have been raised in the fields and many security, privacy, and trustworthiness-enhancing techniques have been proposed to resolve these concerns. On the other hand, the emerging mobile and wearable technologies revolutionize the entire MCPS as well as its models of security, privacy, and trustworthiness. It is still not clear that these proposed techniques are useful and effective in practice and how quickly or even possibly they are going to be adopted.

This workshop aims to bring together the technologists and researchers who share interest in the area of security, privacy and trustworthiness in medical cyber physical systems, as well as explore new venues of collaboration. The main purpose is to promote discussions of research and relevant activities in the design of secure, privacy, or trustworthiness architectures, protocols, algorithms, services, and applications on medical cyber physical systems. It also aims at increasing the synergy between academic and industry professionals working in this area. We plan to seek papers that address theoretical, experimental research, and work in-progress for security, privacy and trustworthiness related issues in the context of medical cyber physical system.

### Topic of Interest

- Mobile Healthcare Security
- Smartphone Security for Healthcare
- Wearable Device Security
- Medical Device Security
- Security and Privacy on Implantable Medical Sensors
- Biometrics
- Wireless Communication Security
- Security and Privacy for Wireless Body Area Networks
- Secure RFID technology in MCPS
- Software Defined Networks (SDN)
- Security in Virtualized Health Systems
- Security Risk Assessment
- Secure Cloud Health System
- Big Health Data Security
- Differential Privacy on Health Data
- Secure Machine Learning on Health Data
- Privacy Preserving Big Health Data Analysis
- Novel Threats and Attack Models
- Novel Trust Models
- Security Detection and Evaluation
- Key Management
- Cryptography for Health Systems
- Security Management (administration and training) in Health Systems
- Security and Privacy Policies in Health Systems
- Security in Electronic Health Record Systems
- Access Control for Medical Systems

### Instructions for Authors

Submitted papers must be neither previously published nor under review by another workshop, conference or journal. Only electronic submissions in PDF will be accepted. Submitted papers must be written in English, must be formatted in a standard IEEE camera ready format, must be no longer than 8 pages in double-column and 10-point font (\$100 for the extra 8<sup>th</sup> page), must render without error using standard PDF viewing tools, must print on US-Letter-sized paper, and must include the author names and affiliations on the first page. Note that at least one of the authors of each paper accepted for presentation in MedSPT 2016 must be registered. All papers presented at the workshop will be published in formal workshop proceedings and will be part of the IEEE Digital Library. Please submit your paper to the EDAS system <http://edas.info/newPaper.php?c=21967>.

### Review and Publication of Manuscripts

Submitted papers will be reviewed by the workshop Program Committee and judged on originality, technical correctness, relevance, and quality of presentation and the comments will be provided to the authors. If any accepted paper is not registered, the paper will be removed from the workshop program and the proceedings.

Outstanding papers will be invited to extend to full version for a prestigious journal (SCI(E)-indexed), currently under contacting and

### TIMELINE

March-14, 2016  
March 25, 2016  
Paper submission due

April 18, 2016  
Acceptance Notification

May 15, 2016  
Camera ready versions due