Sixth International Workshop on Trustworthy Embedded Devices (TrustED 2016)

Xinxin Fan
Bosch Research and Technology Center, USA
Xinxin.Fan@us.bosch.com

Tim Güneysu
University of Bremen & DFKI, Germany
tim.gueneysu@uni-bremen.de

ABSTRACT

The Internet of Things (IoT) is expected to become a global information and communication infrastructure for cyber physical systems and to bring numerous value-added services for modern society. However, the integration of heterogeneous devices and service models into a cohesive system significantly increases the complexity of design and deployment and introduces the new challenges for the security of systems and processed as well as the privacy of the collected data. The Workshop on Trustworthy Embedded Devices (TrustED) addresses all aspects of security and privacy related to embedded systems and the IoT. TrustED 2016 is a continuation of previous workshops in this series, which were held in conjunction with ESORICS 2011, IEEE Security & Privacy 2012, ACM CCS 2013, ACM CCS 2014, and ACM CCS 2015 (see http://www.trusted-workshop.de for details). The goal of this workshop is to bring together experts from academia and research institutes, industry, and government in the field of security and privacy in cyber physical systems to discuss and investigate the problems, challenges, and recent scientific and technological developments.

CCS Concepts

•Security and privacy → Tamper-proof and tamper-resistant designs; Embedded systems security; Hardware security implementation; Hardware attacks and countermeasures; Distributed systems security; Security protocols;

Keywords

TrustED, Security, Embedded Devices, Cryptography

1. BACKGROUND AND MOTIVATION

The fast and steady developments in sensor technologies, micro-electromechanical systems (MEMS), Internet infrastructure and communication standards have given rise to a new disruptive technology: the Internet of Things (IoT). As a key enabler for building a connected world, IoT allows people and objects in the physical world to interact with each other and create various smart environments in an autonomous manner. It has been estimated that the IoT ecosystem will bring over 28 billion connected autonomous things by 2020.

As IoT continues to gain traction and more connected devices come to market, security and privacy will become major concerns. The smart embedded devices in IoT systems, unlike full-fledged computers, are generally constrained in terms of speed, memory and power consumption, due to their low cost and high volume characteristics, which has posed new challenges for designing and implementing security solutions for protecting those resource-constrained devices. Furthermore, the inherent complexity of IoT, which comes from heterogenous devices and service models, also significantly increases the difficulty for realizing efficient, scalable and interoperable security mechanisms. In addition, some IoT applications handle sensitive information about people such as their locations, movements, health status, etc. Ensuring strong data security and privacy in these applications is of paramount importance.

Given the above, there is an increasing demand for design, analysis and implementation of new security and privacy solutions for ensuring the confidentiality, integrity and availablity of IoT applciations. In particular, protecting billions of embedded smart devices from a wide range of attacks and making good trade-offs bewteen security and performance is both a challenge and a requirement to ensure the confidence in and acceptance of the IoT.

2. SCOPE AND OBJECTIVES

TrustED 2016 will address range of problems related to security and privacy in embedded systems and the IoT. Of particular interest are security and privacy topics that are unique to the IoT. Contributions may present and solve existing IoT security challenges, introduce new threat models and attack methods to IoT devices and architectures, design novel security and privacy-enhancing mechanisms for IoT applications, and focus on performance evaluation and comparison with existing solutions and standards. Submissions exploring innovative and multidisciplinary methods and techniques to solve IoT security challenges are strongly encouraged.

The workshop topics include, but are not limited to, the following:

- Trustworthy and secure embedded systems

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.

DOI: http://dx.doi.org/10.1145/2976749.2990489

- Novel constructions, implementations and applications with physical security primitives (e.g., PUFs, PhySec)
- Hardware entangled cryptography
- Novel security architectures for the IoTs
- Frameworks and tools to design, validate and test trustworthy embedded systems
- Secure execution environments (e.g., TrustZone, TPMs) on mobile devices
- Remote attestation and integrity validation
- Privacy aspects of embedded systems (e.g., medical devices, electronic IDs)
- Physical and logical convergence (e.g., secure and privacy-preserving facility management)
- Novel paradigms to established trust in large distributed environments

3. PROGRAM COMMITTEE

We are thankful to the members of our program committee for their work during the review process:

- Mark Aagaard (University of Waterloo, CA)
- Lejla Batina (Radboud University Nijmegen, NL)
- Guido Bertoni (STMicroelectronics, IT)
- Marten van Dijk (University of Connecticut, US)
- Thomas Eisenbarth (Worcester Polytechnic Institute, US)
- Junfeng Fan (Open Security Research, CN)
- Wieland Fischer (Infineon Technologies, DE)
- Aurélien Francillon (EURECOM, FR)
- Shalabh Jain (Robert Bosch LLC, US)
- Sandeep Kumar (Philips Research Europe, NL)
- Hui Li (Xidian University, CN)
- Stefan Mangard (IAIK TU Graz, AT)
- Matthias Schunter (Intel, DE)
- André Weimerskirch (University of Michigan, US)
- Attila Yavuz (Oregon State University, US)

4. PC CHAIRS

Xinxin Fan is a senior scientist at the Robert Bosch Research and Technology Center (RTC) in Pittsburgh, USA, where he conducts research on security and privacy for cloud computing and Internet of Things (IoT) systems. Prior to joining Bosch RTC, Xinxin was a research associate and project manager at University of Waterloo, Canada, where he conducted theoretical and applied research on lightweight cryptography and security and privacy for RFID systems and machine-to-machine (M2M) communications. He also managed the 5-year, $1.7M Ontario Research Fund – Research Excellence (ORF-RE) Program sponsored project for the development of next generation security and privacy solutions for mobile ad-hoc communications and embedded systems. During his scientific career he has authored over 40 scientific publications in refereed conferences, workshops and journals, several patents and patent applications, and served in the program committee of over 10 conferences in communication system security. He also regularly acts as a reviewer for journals such as IEEE Transactions on Computers, IEEE Transactions on VLSI, and the IEEE on Dependable and Secure Computing among others. Xinxin holds a B.Sc degree in applied mathematics and M.S. in Information Systems and Telecommunications Engineering from Xidian University, China and a Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Canada.

Tim Güneysu is associate professor and head of the research group for Computer Engineering and IT-Security (CEITS) at University of Bremen that was established under the Excellence initiative in corporation with the German Research Center for Artificial Intelligence (DFKI). Tim's primary research topics are the secure design and implementation of embedded and hardware-based systems, including aspects such as long-term secure cryptography, lightweight and hardware-entangled cryptography. Prior to his current position, Tim was appointed as assistant professor and leader of the Hardware Security Group at Ruhr-University Bochum since 2011. From 2000 to 2006 he worked for IBM Germany and was visiting researcher at IBM Almaden Researcher Center. He stayed as senior researcher and visiting professor with UMass Amherst and the Hubert Curien Lab in Saint-Etienne in 2009 and 2011, respectively. Tim published and contributed to more than 70 peer-reviewed journal and conference publications in the area of reconfigurable devices, IT-security and cryptography. He served as Program Co-Chair of CHES, LightSec, TrustED and as Track Chair of the A5 track *Secure Systems* of the Design, Automation and Test Conference (DATE) for the years 2015-2017.