TrustED 2016 Chairs' Welcome

The 6th International Workshop on Trustworthy Embedded Devices (TrustED 2016) was held October 28th, 2016 in Hofburg Palace, Vienna, Austria, and has been co-located with the 23rd ACM Conference on Computer and Communications Security (CCS 2016). 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 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 resource-constrained smart embedded devices in IoT systems as well as the inherent complexity of IoT system architectures have posed new challenges for designing and implementing security and privacy mechanisms for protecting emerging IoT applications. Given the above, major themes of TrustED 2016 include security and privacy aspects of the Internet of Things and in particular of embedded devices as parts of cyber physical systems and their environments. It aims 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 in this field.

This year, twelve papers have been submitted. Each paper received at least three reviews, which were followed by an online discussion to decide on the program. Papers co-authored by one PC chair were exclusively handled by the other. The program committee accepted six papers that cover a variety of topics, including Physical Unclonable Functions, side-channel attacks, physical layer security, hardware security, and system security. In addition to the technical program, the workshop featured three internationally highly renowned speakers: Aurélien Francillon, Marcel Medwed, and David Oswald.

We would like to thank the program committee, which consisted of fifteen world-renowned experts, both from academia and industry. Although the review period was comparatively short and fell into the common vacation period, the committee has put in a substantial effort reviewing the papers and providing feedback to the authors. Likewise we want to thank the external reviewers who provided expert opinions that helped guide the program selection. We want to thank Mathias Payer and Stefan Mangard, the ACM CCS Workshop Co-Chairs, as well as Edgar Weippl and Stefan Katzenbeisser, the ACM CCS General Chair, for their help with the organization of the workshop. Our acknowledgements also go to Jorge Guajardo Merchan from the Bosch Research and Technology Center North America for his great help and support during the preparation of the workshop. Finally, we would like to thank ACM SIGSAC for sponsoring the CCS workshops and the Bosch Research and Technology Center North America for supporting TrustED.

We hope that you will find this program interesting and thought-provoking and that the workshop will provide you with opportunities to share ideas with other researchers and practitioners.

Xinxin Fan
Bosch Research and Technology Center, USA

Tim Güneysu
University of Bremen & DFKI, Germany