Committees

Program Chairs

S. Koubias (Univ. of Patras)
T. Sauter (Donau University Krems)

Program Committee

D. Arora (Intel, USA)
I.C. Bertolotti (PolitecnicoTorino, Italy)
A. Bogdanov (KU Leuven, Belgium)
B. Carbunar (FIU, USA)
K. Dietrich (NXP Semiconductors, Austria)
M. van Dijk (U. Connecticut, USA)
D. Forte (U. Connecticut, USA)
J. Groszschaedl (U. Luxemburg, Luxemburg)
W. Kastner (TU Wien, Austria)
F. Praus (FH Technikum Wien, Austria)
S. Rajagopalan (Honeywell, USA)
P. Schwabe (Radboud U. Nijmegen, Netherlands)
N. Sklavos (TEI Epirus, Greece)
M. Taha (Assiut U., Egypt)
A. Treytl (Donau U. Krems, Austria)
Y. Wang (I2R A*STAR, Singapore)
T. Yu (Qatar Computing Research Institute)

Steering Committee

C. Gebotys (U. Waterloo)
D. Serpanos (QCRI)
M. Wolf (Georgia Tech)

About WESS

Embedded computing systems are continuously adopted in a wide range of application areas and importantly, they are responsible for a large number of safety-critical systems as well as for the management of critical information. The advent of the Internet-of-Things introduces a large number of security issues: the Internet can be used to attack embedded systems and embedded systems can be used to attack the Internet. Furthermore, embedded systems are vulnerable to many attacks not relevant to servers because they are physically accessible. Inadvertent threats due to bugs, improper system use, etc. can also have effects that are indistinguishable from malicious attacks.

This workshop will address the range of problems related to embedded system security. Of particular interest are security topics that are unique to embedded systems. The workshop will provide proceedings to the participants and will encourage discussion and debate about embedded systems security.

Topics of Interest

- Trust models for secure embedded hardware and software
- Isolation techniques for secure embedded hardware, hyperware and software
- System architectures for secure embedded systems
- Hardware security
- Metrics for secure design of embedded hardware and software
- Security concerns for medical and other applications of embedded systems
- Support for intellectual property protection and anti-counterfeiting
- Specialized components for authentication, key storage and key generation
- Support for secure debugging and troubleshooting
- Implementation attacks and countermeasures
- Design tools for secure embedded hardware and software
- Hardware/software co-design for secure embedded systems
- Specialized hardware support for security protocols
- Efficient and secure implementation of cryptographic primitives

Submission Instructions

The proceedings of the workshop will be published by the ACM. Papers must be submitted in PDF form through the **EASYCHAIR** system. Submitted papers should present original research that is unpublished and not submitted elsewhere. Papers should be no more than 10 pages 2-column in ACM format. Templates for the submission of papers can be found at the **ACM website.** To submit a paper refer to **http://www.wess-workshop.org**

Important Dates

Paper submission deadline:	July 3, 2015
Author notification:	August 18, 2015
Camera ready papers due:	September 1, 2015
Copyright forms due:	September 1, 2015
Workshop date:	October 8, 2015