



Fifth Workshop on
Embedded Systems Security (WESS'2010)
A Workshop of the Embedded Systems Week (ESWEEK'10)
October 24, 2010
Scottsdale, AZ, USA
<http://www.wess-workshop.org/>

General Chairs

Catherine Gebotys (U Waterloo)
Marilyn Wolf (Georgia Tech)

Program Chairs

Raj Rajagopalan (HP)
Patrick Schaumont (VT)

Program Committee

Frederik Armknecht (U Mannheim)
Lejla Batina (Radboud U)
Levente Buttyan (UTE)
Reouven Elbaz (Intel)
Junfeng Fan (KUL)
Guy Gogniat (U Bretagne Sud)
Leyla Nazhandali (Virginia Tech)
Sri Parameswaran (UNSW)
Axel Poschmann (Nanyang TU)
Kazuo Sakiyama (UEC)
Zhujie Shi (U Connecticut)
Stefan Tillich (U Bristol)
Ingrid Verbauwhede (UCLA)
Ning Weng (SIUC)
Tilman Wolf (UMass Amherst)
Chuck Yoo (Korea U)

Steering Committee

Catherine Gebotys (U Waterloo)
Dimitrios Serpanos (U Patras)
Marilyn Wolf (Georgia Tech)

Embedded computing systems are widely found in application areas ranging from safety-critical systems to vital information management. This introduces a large number of security issues. Embedded systems are vulnerable to remote intrusion, local intrusion, fault-based and power/timing-based attacks, intellectual-property theft, subversion, hijacking and more. Due to their strong link to software engineering and hardware engineering, these security issues are different from the traditional security problems found on personal computers. For example, embedded devices are resource-constrained in power and performance, which requires them to use computationally efficient solutions. They have a very weak physical trust boundary, which enables many different implementation-oriented attacks. They use an intimate connection between hardware and software, often without the shielding of an operating system. This workshop provides a forum for researchers to present novel ideas on addressing security issues that arise in the design, the operation, and the testing of secure embedded systems. Of particular interest are security topics that are unique to embedded systems.

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
- 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 codesign for secure embedded systems
- Specialized hardware support for security protocols

Abstract Registration:	26 July 2010
Submission Deadline:	2 August 2010
Notification:	30 August 2010
Copyright Forms Due:	3 September 2010
Camera Ready Papers:	13 September 2010

SUBMISSION: Please refer to <http://www.wess-workshop.org>