Workshop on
Research Directions for Security and Networking in Critical Real-Time and Embedded Systems

http://moss.csc.ncsu.edu/~mueller/crtes06
April 4, 2006, San Jose, California, USA
In conjunction with RTAS'06
CFP as PDF and text

The objective of this workshop is to identify research problems related to security and networking of real-time/embedded systems deployed as control systems for critical infrastructure and as mission-critical systems.

Scientific principles, disciplined engineering methodologies, and well-defined formulations on system problems have helped the IT industry to produce some of the most celebrated technologies in the past two decades. As we see various technologies penetrate into every aspect of our daily life, new issues and ever greater challenges begin to emerge. Cybersecurity and networking are on top of the list of grand technology challenges that will have profound impact on the quality of information services to be delivered to the whole society. In particular, embedded systems and real-time systems are widely used in today's society. Critical infrastructure, such as the power grid, power plants, telephone and the Internet itself, rely on such systems, just as safety-critical systems (planes, cars) and mission-critical systems (e.g., UAVs) do. Such control systems are increasingly being connected to the Internet to facilitate maintenance and reduce the cost of monitoring. Another trend is to increasingly rely on sensor networks to provide input to these control systems via wireless communication. However, the increasing connectivity of these real-time/embedded systems to general computing services poses a significant threat as they become exposed to potentially harmful attacks. Cybersecurity and networking concerns must be considered to counter these risks.

This workshop aims to identify these risks at a technical level. Its objective is to determine the needs of current and future critical systems and their integration into existing computing infrastructure. The forum's purpose is to bring together researchers, practitioners and partners from funding agencies to identify grand challenges in this domain. Its intent is to initiate medium to long-term projects addressing fundamentally novel approaches instead of short-term, retrofitted solutions. The workshop results will be compiled in a document to support agencies in their task to request funds for research in this area.

Problems of interest (topics) for this workshop include, but are not limited to:

- Security threats to critical real-time and embedded systems, specifically
    - SCADA (supervisory control and data acquisition) systems
    - PCS (process-control systems)
- New challenges introduced by networking embedded systems
    - Network connectivity of critical infrastructure
    - Wireless data acquisition and sensor networks
    - Real-time computing techniques for network security measures
    - Real-time constraints on security provisions
- Trustworthiness of real-time embedded systems and networks

Submission:

Authors are invited to submit position papers describing grand challenges (not their solutions) and new research directions to crtes06@csc.ncsu.edu. Submissions are restricted to 2 pages. A selection of these submissions will be considered for presentation during the workshop. Electronic submissions are mandatory. Submissions should be e-mailed to one of the workshop organizers. Preferred formats are PDF or PostScript.

Important Dates:

Submission Deadline: Feb 24, 2006 at midnight EDT
Notification: Mar 13, 2006
Camera-ready: Mar 20, 2006

Organizers:

Frank Mueller (NC State University)
Peng Ning (NC State University)
Kevin Jeffay (UNC Chapel Hill)

Keynote Speakers:

Helen Gill (NSF)
More TBA

Advisory Committee:

Cathy Gebotys (Waterloo)
Al Mok (UT Austin)
Adrian Perrig (CMU)
Radha Poovendran (UW)
Raj Rajkumar (CMU)
Kang Shin (Michigan)
Sang Son (UVA)
Eugene Spafford (Purdue)
John Stankovic (UVA)
Janos Sztipanovits (Vanderbilt)
Gene Tsudik (UC Irvine)
Wayne Wolf (Princeton)
More TBA