Panel:
Safety-Critical, High-Assurance Software Systems

Ken Birman, Cornell
Assaf Kfoury, Boston University
Engin Kirda, Northeastern University
Rami Melhem, University of Pittsburgh
Overview of Panel

• This panel is on safety-critical, high-assurance systems
  – I am a systems security person – hence, this is not necessarily my main area of research ;)
  – However, the security of critical systems is increasingly gaining focus and attention
  – There have been documented, high-profile attacks against critical systems (e.g., Stuxnet)

• This panel aims to discuss
  – Promising research directions
  – Current research challenges
  – How we can foster more collaboration
Background: Critical Systems

- Critical systems control public resources such as electricity, water, telecommunications, banks, etc.

- The consequences of any disruption of service are severe and may result in loss of human life.

- Such systems must often consider different types of constraints compared with regular computer systems (e.g., real time).

- Interdependencies between subsystems may lead to cascading effects that are difficult to foresee.

- There is an emphasis on safety and less understanding of computer security in this domain (and vice versa).

Safety-Critical, High-Assurance Systems
Examples of Critical Systems

• “Traditional” critical infrastructures
  – electricity, water, telecommunications, etc.

• SCADA systems
  – Used in almost all critical infrastructures
  – Efforts are already ongoing to protect such systems

• Financial systems are critical infrastructures
  – Many access points
  – Availability to many and diverse users
“Emerging” Critical Systems

- **Data centers** are becoming common and these can be seen as CIs in that they provide data necessary for more traditional CIs.

- **In-vehicle automation** with remote diagnostics and software updates for vehicles:
  - Embedded (automobile) systems connected to open networks.
  - Some of the problems related to any embedded system are also valid for the *connected car*.
Safety takes priority over security

• **Problem:** In the domain of critical systems, both safety and security are important, but in certain scenarios, safety takes priority
  • If the underlying process is about to become critical, security should not block or delay appropriate remedies or counteractions

• We need an integrated view on safety and security, since a breach in security could provoke a breach in safety
Unforeseen cascading effects

- **Problem:** Interconnected systems are difficult to model properly, and interdependencies between the subsystems, can lead to cascading effects that are difficult to foresee

- We need to develop appropriate models for the domain, and an overall better architecture with a security baseline
Use of new technology

- **Problem:** Critical systems also use new types of technology to add functionality
  - e.g., wireless communication for remote sites and internal enterprise communication. Critical control communication will be wireless within 10 years

- There is a tradeoff between the advantages gained with a technology versus the security risk
  - This trade-off must be carefully modeled and analyzed
The Human Factor

• **Problem:** The human is probably the weakest point in a critical system
  – The roles include operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development
  **Adversarial problem:** Insiders with experience of and knowledge about the system

• **Important issues:**
  – Education and training, raising awareness of security risks; sound and evolving security policy; modeling the user (“cognitive modeling”) and user-interface properties.
  Effective strategies for discovering an “insider” is an open research question.
The Next Challenge: Cyberwar

- Stuxnet, Duqu, Flame
  - Government-sponsored malware attacks against other nations
  - How can we secure existing critical systems?