COT 4930/5930 Security for infrastructure systems

Critical infrastructure are the systems that support our everyday life and the Dept. of Homeland Security has identified 14 areas of concern including agriculture, information and telecommunications, food, energy, water, transportation, public health, and finance. We need to protect the information necessary to control and coordinate these systems without which our normal life is not possible. This information is embodied in a process control system (PCS) with its corresponding information system. A PCS typically includes a supervisory, control, and data acquisition (SCADA) system, which monitors and controls switches, valves, and physical quantities (temperature, pressure) and collects and logs field data. SCADA systems are distributed systems, including workstations, wired and wireless sensors, and application software. Databases contain the necessary information. SCADA requirements include 24/7 availability, real-time operation, survivability, safety, and remote control. Their protection includes security and reliability concerns, including authentication, authorization, intrusion detection as well as fault tolerance and survivability measures.

Instructor: Dr. E.B.Fernandez
http://www.cse.fau.edu/~ed,
ed@cse.fau.edu

Textbook: Class notes, papers

Goals: To provide a perspective of the problems involved in protecting the critical infrastructure of a country. Understanding of how to coordinate hardware and software to provide data and network protection against internal and external attacks as well as accidental errors. How to define safety assertions. Modeling of the systems involved through the use of object-oriented patterns and formal models.

Prerequisite by topic: General concepts of computer system architectures. Some knowledge of object-oriented concepts, in particular UML modeling.

Outline:

1. **Context and motivation**. Importance of infrastructure. Possible attacks, failures, and hazards. Security, reliability, and safety objectives. Complex systems. Review of UML and patterns. Security and reliability patterns.

2. **Critical Infrastructure.** Features and requirements. Standards. Requirements. Process control systems, information systems, and sensor networks.

3. **Security and reliability objectives**. Systematic analysis of attacks against the infrastructure. Misuse patterns. Overview of defenses (countermeasures). Effect of errors. Protection against errors. Hazards and safety assertions.

4. **Countermeasures I.** Authentication. Access control models. Physical access control. Comparison and voting for hardware fault tolerance. Diversity.

5. **Countermeasures II.** Cryptography. Network security. Viruses and worms. Firewalls and IDS. Web services and agents. Cloud computing. Redundancy to protect against denial of service.

6. **Systems security and availability**. Middleware and database security. Reinforced systems for high security and fault tolerance. Survivable systems.

7. **Dependable architectures for infrastructure systems**. Effect of system architecture on security, safety, and reliability. Secure and reliable development process.

Grading: Take-home exam (70 %). Three assignments (30%).