



Information Sciences Institute

Understanding Trust and Security in SCADA Systems

Clifford Neuman

USC Center for Computer Systems Security



USC Viterbi
School of Engineering



SCADA systems should not be monolithic

Many SCADA systems today are monolithic

- The system is often protected from the outside, but the functions of the systems are not protected from one another.
- We should design SCADA systems with internal boundaries
 - Critical functions protected from interference by less critical functions. Critical functions in different parts of the system protected from one another.
- The first step is to understand the system itself
 - Understand which functions are critical.
 - Understand intrinsic system boundaries.





Providing Isolation within SCADA Systems

Apply principle of least privilege.

- Design system so non-critical functions can not interfere with critical functions.
- Design system so critical functions in one part of the system can be isolated from critical functions in other regions.
- Understand any key points of failure such as management functions.
- **Simplify the policy enforced within the system.**
 - Core isolation should be based on membership in coarse-grained regions.
 - Any fine grained controls should be managed within each function, and not by the primary isolation methods.
- **Utilize Trusted Computing technologies**
 - Such as SNAIR architecture to provide necessary isolation.





Roadmap

Information Sciences Institute

- **Short term - Understand the SCADA system**
 - Model internal dependencies as well as interdependencies across SCADA systems.
 - Develop isolation mechanisms within network and system architectures.
 - Work on understandability of the management of the protection mechanisms used to provide such isolation.
- **Longer term - redeployment and advanced management.**
 - Begin to redeploy SCADA systems using the new architectures.
 - Understand issues of safe/constrained reconfiguration of such systems to recover from partial failure.

