SCADA Cyber Attack Alert Tool (CAAT)

Raytheon
Network Centric Systems

- Sponsored by Technical Support Working Group (TSWG) on behalf of DHS National Cyber Security Division (NCSD)
- Raytheon contacts
  - Principal investigator: Simon Hennin, 508-490-2088, simon_j_hennin@raytheon.com
  - Program manager: Teh-Kuang Lung, 508-490-3908, teh-kuang_lung@raytheon.com
- Phase 1 period of performance: 5/21/07 – 5/21/08

Enhance our ability to respond effectively to cyber attacks on nation's critical infrastructure systems

SCADA CAAT - Project Vision

Raytheon
Network Centric Systems

The problem

- Increasing commonality of control system technology
- Inter-dependency between systems in different critical infrastructure sectors
- Common cyber threats and vulnerabilities
- Potential for widespread coordinated cyber attack by hostile parties

Enhance our ability to respond effectively to cyber attacks on nation's critical infrastructure systems

SCADA CAAT - Project Vision (continued)

Raytheon
Network Centric Systems

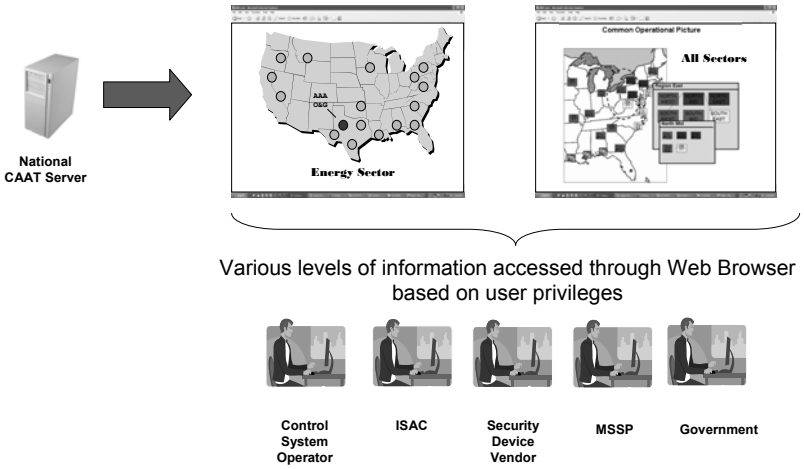
The CAAT part of the solution

- Create network of control system sites across multiple sectors contributing cyber event information
- Provide situational awareness of control system cyber events at sector, regional & national levels
- Disseminate threat and advisory information from monitoring centers (SOCs, ISACs, Government etc) on potential and escalating cyber attacks
- Timely cyber event information sharing with robust information assurance provisions

Enhance our ability to respond effectively to cyber attacks on nation's critical infrastructure systems

SCADA CAAT - Project Vision (continued)

Raytheon
Network Centric Systems



Enhance our ability to respond effectively to cyber attacks on nation's critical infrastructure systems

SCADA CAAT

Raytheon
Network Centric Systems

Initial project goal

- In conjunction with Industry Advisory Group (IAG), define draft industry standard protocol and data schema for control system cyber incident information sharing
- As follow-on options, develop and test proof-of-concept prototype (extending project through 2008)

Engage industry to define protocol standard

SCADA CAAT

Raytheon
Network Centric Systems

Project approach

- Involve industry and government stakeholders in advisory capacity
  - 10+ industry participants in IAG meetings to date
  - IAG meeting held as part of PCSF meeting 1/15/08
- Build from prior control system cyber security work, e.g. LOGIIC, and existing information sharing mechanisms and protocols
- Explore relationships with other projects, e.g. recently announced DoE sponsored projects

Contact us about involvement in the CAAT IAG