Field-level Situational Awareness: Challenges and Solutions

Mauricio Papa

Associate Professor of Computer Science

I3P Institute for Information Infrastructure Protection

SANS Process Control & SCADA Summit 2009

Lake Buena Vista, FL – February 3rd, 2009

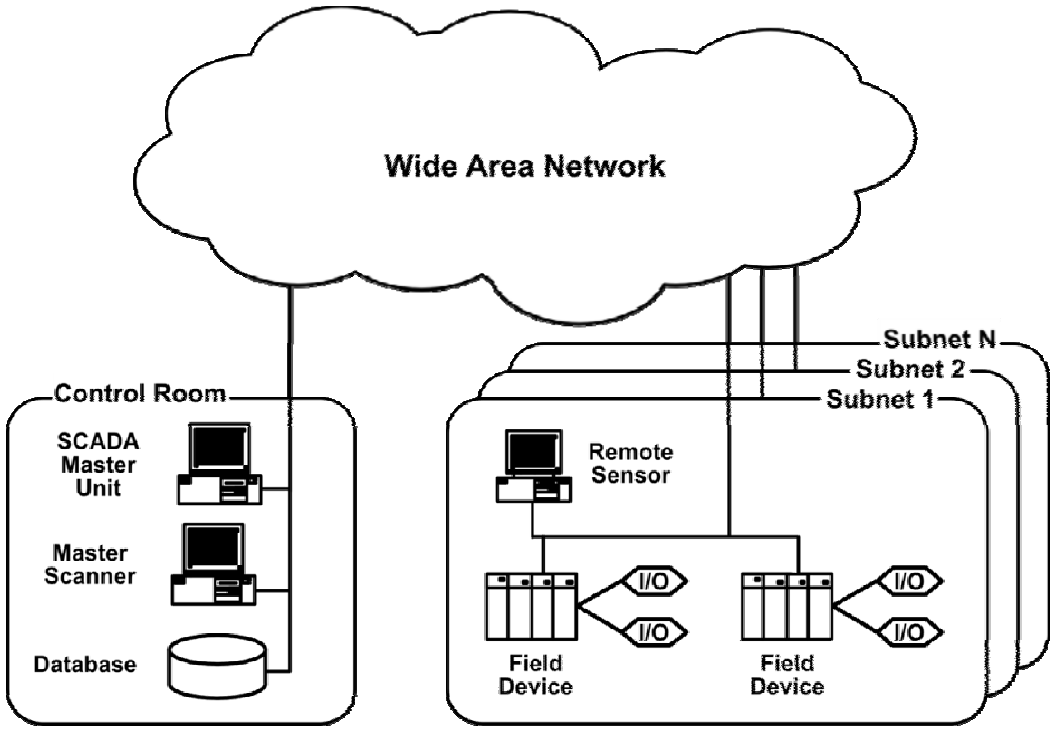
Concept and relevance

- Definition
  - Observe and understand what is happening on your network
  - Operation, communication, topology
- Why do you need it?
  - Monitor network, IDS, Filtering devices
  - Detect intrusion, communicate with filtering device
  - Detect changes, verify/evaluate, policy enforcement
  - Pass messages to higher-level apps
  - Reduce risk of RTUs that do not respond well to certain TCP/IP messages
  - Real-time traffic analysis
  - Central command and storage

Challenges

- SCADA and IT networks are different
  - Security Principles
    - SCADA – Availability, IT – Confidentiality
  - Protocol Isolation
    - SCADA – Protocols from both, IT – Only IT protocols
  - Protocol Variations
    - SCADA – Multiple, IT – Standard Protocols
  - Traffic Uniformity
    - SCADA – Routine and predictable, IT – User-generated
  - Traffic Volume
    - SCADA – Light, IT – Massive
- Solution requirements
  - Scalable, distributed, low impact on production system

Solutions



Methodology
- Leverage previous results and tools
- Collaboration with industry partners from oil & gas and security services
- Testing and development facility
- Showcase results to other entities
- Technology transfer

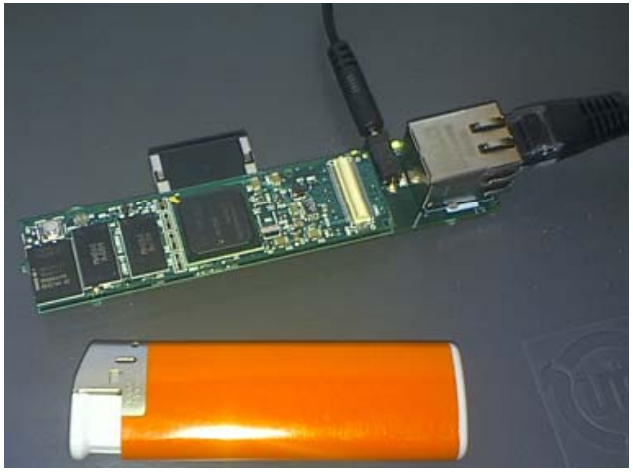
Master scanner, remote sensors, DB

Solutions – Current Capabilities

- MODBUS implementation
  - Demo presented at I3P Conference in 2008
  - Ability to profile MODBUS communications and identify malicious activity
    - Denial of Service, Spoofed IP/MAC, Unexpected MODBUS commands, Unauthorized systems on network
  - Visualization GUI
- Full situational awareness of SCADA network
- Fisher ROC module is in development

Solutions – Technology transfer

- Gumstix
  - Full processing capability
- Cost less than $200



- Open source
- Light weight, power conserving, reliable

Future Work & Research Directions

- PCS/SCADA Forensics
  - Post-mortem
  - Dynamic analysis to enable pro-active solutions (live forensics)
  - Current solutions applicable only to IT world
- Failure-oblivious computing
  - Detect certain flaws as software runs and act to mitigate
- State estimation
  - Use models to estimate/predict system state faster than real-time
- Demo
  - 5th Annual I3P Process Control Security Workshop
  - Houston, April 28, 2009