ICS SCADA Operations
Joe Klein, CISSP ...
Internet of Things (IoT)

ICS SCADA
Why is ICS SCADA Important?
Definitions

ICS - Industrial Control Systems
• Command and control networks and systems designed to support industrial processes

SCADA - Supervisory Control and Data Acquisition Systems
• The largest subgroup of ICS
Primary Functions

- Data Acquisition
- Data Communications
- Data Presentation
- Control
Equipment

- Sensors & Controls
- SCADA RTU’s
- SCADA Master
- Communications
ICS SCADA Network

https://www.youtube.com/watch?v=fJyWngDco3g
ICS Vulnerabilities

Problems
- Wired
- Wireless
- No trust models
- No data isolation
- No security model
- Physical Access
- No Anti-Malware
- Security Monitoring
- Redundancy
Key Flaws in the System

- Protocol Design
- System Design
- System Implementation
- Procurement & Supply Chain
- System Maintenance & Operation
Figure 1: Vulnerabilities 2013

- Authentication, 58 (33%)
- Denial of Service, 25 (14%)
- Buffer Overflow, 17 (10%)
- Memory Corruption, 16 (9%)
- Directory Traversal, 12 (7%)
- Protocol Vulnerability, 12 (7%)
- Privilege Escalation, 8 (4%)
- Cross Site Scripting, 7 (4%)
- Use After Free, 1 (3%)
- Heap Corruption, 1
- Stack Overflow, 1
- Integer Overflow, 3 (2%)
- SQL Injection, 5
- Remote Code Execution, 5 (3%)
- Multiple, 6
Resources

- DHS ICS-CERT
- NIST SP 800-82
- SCADA Hacker Library
- Digital Bond – S4 Conference & podcast
- International Symposium for ICS & SCADA Cyber Security Research