



CERT

Coordination of Control System Vulnerabilities

Jeff Gennari

Overview

Brief overview of control systems

Vulnerabilities in control systems

Coordination process for control system vulnerabilities

Work to date and next steps

What are control systems?

Computer-based control of physical processes

- Open valve, lower voltage, monitor pressure
- Sound alarm if safety thresholds are surpassed
- Utility companies
 - Electric, gas, water treatment
- Manufacturing
 - Pharmaceutical, automotive

Distributed Control Systems (DCS)

- Management and control of distributed, physical processes
- Human intervention may not be needed

Supervisory Control And Data Acquisition (SCADA)

- Monitoring and limited control
- SCADA systems may make limited decisions without human intervention
 - Humans are still in the control loop

Control systems historically used specialized, proprietary technologies

- MODBUS, EIA-232, serial protocols

Characteristics of Control Systems

There is little, if any, downtime

- System availability is critical

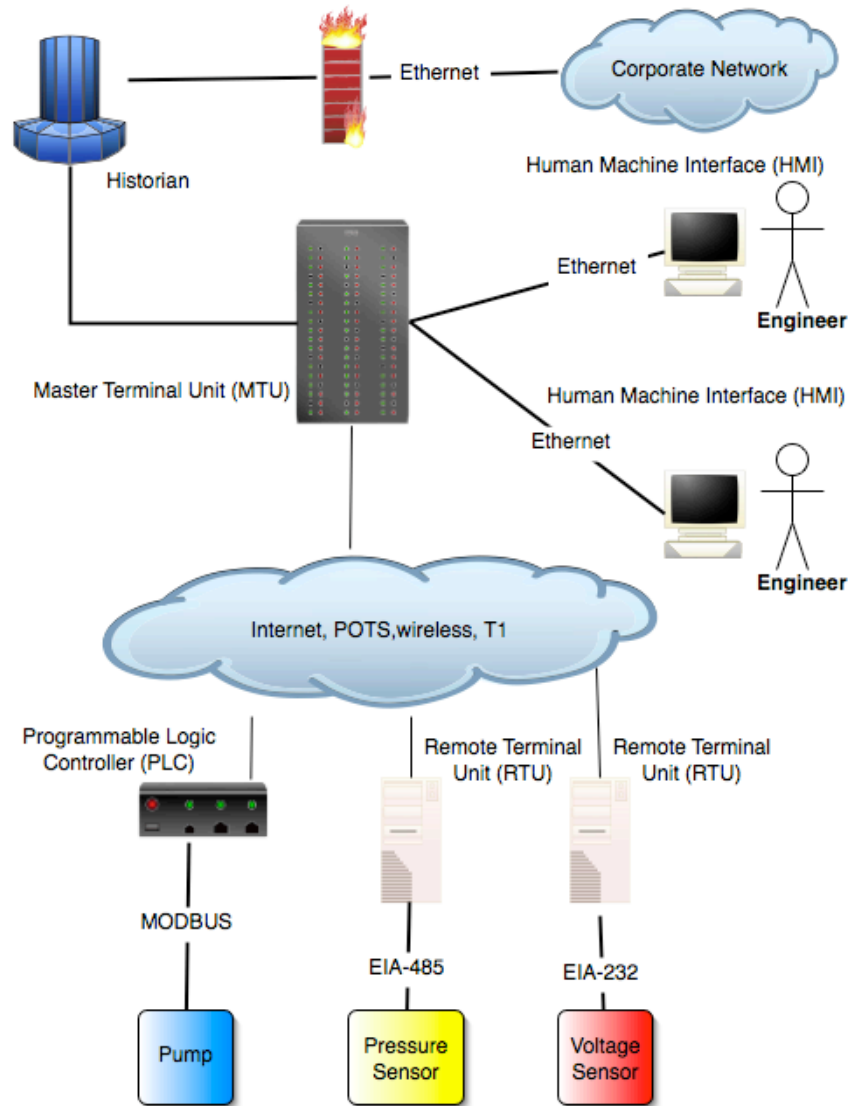
Considerations for real-time systems

- Latency is damaging
 - Data estimation errors

The consequences of tampering with a control system could be significant

- Power failures
- Damage to the economy
- Loss of human life

Example Control System Architecture



Trend Towards Open Technology

Control systems are using more standardized, open, and understood technologies

- Reduces costs
- Increases functionality
- Increases operating efficiency
- Deregulation of utilities
 - Communication between utilities is a necessity
 - U.S. specific?

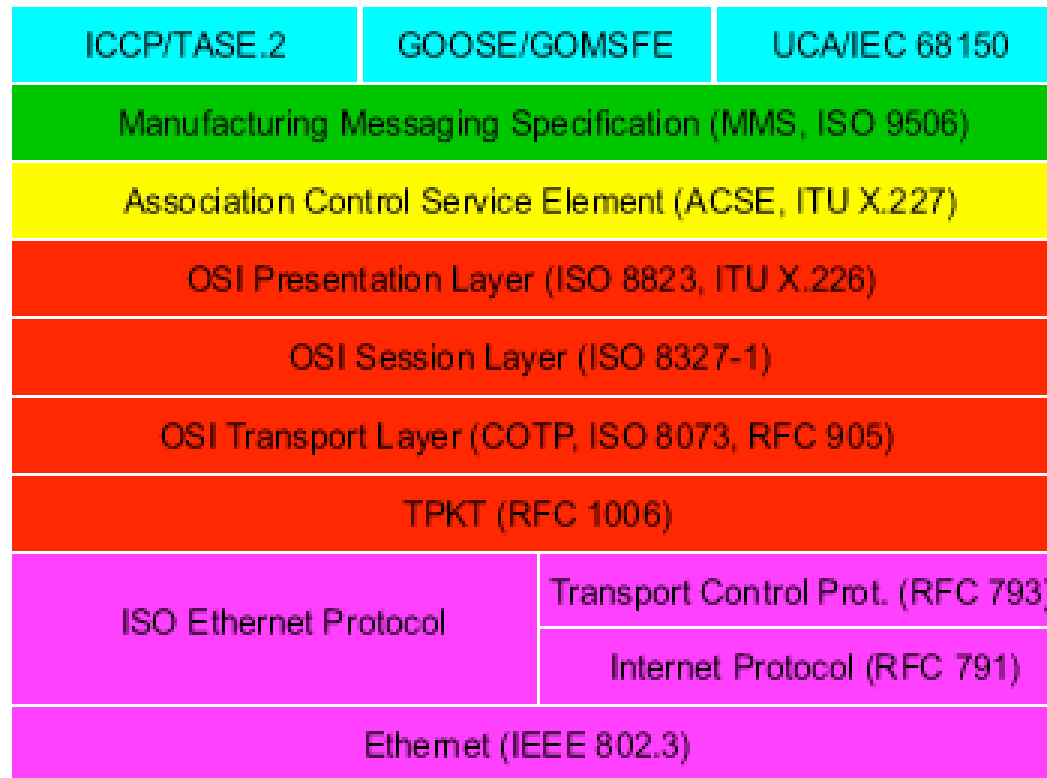
Control systems are using COTS platforms, Internet protocols, and becoming interconnected

- OS platforms (UNIX, Windows, Solaris)
- Embedded OS (Wind River, QNX, Windows)
- Internet technologies
 - ActiveX, COM, Java
- TCP/IP, Ethernet, wireless

Standardized, open protocols are increasingly used in control systems

- ICCP, MMS, TPKT, OSI

Example Protocol Stack (ICCP)



Source: Digital Bond Consulting <http://www.digitalbond.com>

Effects of Open, Standardized Technologies on Control Systems

Control systems are increasingly exposed to the same security issues that affect Internet systems

- Security through obscurity not longer works
- Patches for COTS applications must also be applied to control systems
 - Remember, no downtime!

Legacy platforms and difficulty upgrading

- Lifetime of control system may be decades
- Upgrades (including security fixes) not supported, certified, or properly tested
- May not be possible to upgrade software
 - Hardware restrictions
- Asset owners may have to pay for security fixes

Increased Visibility and Interest

Increased connectivity, the implementation of well documented, standardized technologies, and a historical lack of good network security practices make control systems vulnerable to attack

Control systems are not invisible

- Internet researchers will be (are) interested
 - Toorcon 2005 rootwar contest

If the Internet is a model, security researchers will find vulnerabilities

- What will researchers do?

Control Systems Security Program (CSSP)

CSSP includes CERT/CC, US-CERT, and U.S. National Labs

- U.S. Department of Homeland Security (DHS) formed CSSP to improve security in control systems
 - Including vulnerability analysis and remediation
- CERT/CC supports US-CERT via CSSP to provide coordination and analysis of control system vulnerabilities

Coordination Process

Goal: Responsible coordination and dissemination of vulnerability information to all affected parties

Premise: An security researcher discovers a vulnerability in control system software, what do they do?

- Nothing
 - Delays the inevitable
- Report to vendor
 - What if the vendor is unresponsive?
- Go public
 - Public release before vendors are notified is usually bad

The coordination process handles these types of reports

Roles

CERT Coordination Center

- Lead analysis and coordination effort
 - Receive, catalog, and analyze reports
 - Distribute vulnerability information to affected vendors
 - Publish documents describing the vulnerability

US-CERT

- Facilitate communication
- Respond to incidents in control systems
- Also accept reports (forward to CERT/CC)

U.S. National Laboratories

- Technical expertise and test facilities
- Industry experience

Vulnerability Analysis

CERT/CC has experience analyzing and coordinating vulnerabilities

- Focus on general purpose/Internet systems
 - OS vulnerabilities
 - Common Internet protocols and applications
 - End-user applications

Within CSSP CERT/CC coordinates vulnerabilities in control systems software

Coordination Process

Report is submitted to CERT/CC

- Encourage encrypted mail (PGP)

CERT/CC handles the report accordingly

- Acknowledge the reporter
- Analyze the vulnerability
 - May ask for help from U.S. national labs
- Notify Vendor(s)
 - Provide them technical information
- Notify resellers, repackagers, OEMs
- Notify asset owners (customers)
- Publish document to describe the vulnerability

Publication

Vulnerability Notes

- Public document
- Assures all potentially affected parties are informed

Knowledgebase

- Non-public, restricted access
- Sponsors and trusted collaborators

Is there a need for a new forum in which to disclose control systems vulnerabilities?

- Modification of Knowledgebase?
 - Specialized Knowledgebase for control system vendors and operators
- Who should have access to what information, and when?

To Date ...

Sisco ICCP vulnerability

- Nessus scan crashed ICCP stack
 - Implementation defect in TPKT layer of ICCP stack
- Not handled by CERT/CC or CSSP

LiveData ICCP Server vulnerability

- Common TCP/IP network scanner crashed ICCP stack
 - Implementation defect in TPKT layer of ICCP stack

Several other reports in process

The model of public disclosure has been debated in the control system community

- Is it necessary, given the closed nature of this community?
- Do the risks of public disclosure outweigh the benefits?

Next steps

Continue applying “Internet” experience to control systems

- Vulnerability analysis, coordination, and disclosure
- How should the “Internet” model change?

Learn about process control systems

- Technologies and protocols
- Real system architecture and deployment
 - Difficult to understand actual risks involved
 - What are the consequences of exploitation
- Business models and relationships
 - Resellers, distributors, OEMs, integrators
 - Vertical organization

International Aspects

How are control system technologies used?

- Different technologies
 - The same technology may be used differently in different countries
 - Additional complexity
- Different regulations
- Different business models
 - Free market, nationalized, etc.

What are the needs of CSIRTs regarding control system vulnerability information?

- How should this information be shared?
 - What information do CSIRTs need?
 - Who are the right contacts?
 - How should information be distributed?

Parting Thoughts

Are you responsible for control systems?

What capabilities are in place to handle control system vulnerabilities?

What control system technologies are used?

How are control system technologies used?