Cybersecurity of Control System Networks

Robin Gandhi, William Mahoney, Ken Dick

University of Nebraska at Omaha (UNO)
College of Information Science and Technology (IS&T)
Nebraska University Centre on Information Assurance (NUCIA)
rgandhi@unomaha.edu, wmahoney@unomaha.edu, kdick@unomaha.edu
Who am I?

• Job
  – Assistant Professor of Information Assurance at IS&T since Fall 2008

• Research highlights
  – Regulatory Requirements driven Risk Assessment
    – Using the semantic web to bridge the gap from high-level regulations to low-level technical evidence (Domain: SCADA)
  – Software Assurance in the Development Lifecycle
    – Building semantic templates for the most egregious software flaws
  – Cyber attack modeling and forecasting (CyCast)
    – Exploring disturbances in the human network to predict cyber attacks

• Teaching
  – Software Assurance (seniors/grad) New!
  – Foundations of Information Assurance (seniors/grad)
  – Introduction to Information Assurance (Freshmen) New!
  – Introduction to Computer Science II (Freshmen/Sophomore)
Agenda

• Terminology (Very Quick Overview)
  – What is that new alphabet soup?
• Why do control system need cybersecurity?
• Control system requirements and standards
  – NIST, NERC, DOE regulations....
• Our current research and solutions
• Summary
Terminology
Terminology

• **Industrial (process) Control Systems (ICS) includes:**
  – **Supervisory Control and Data Acquisition (SCADA)**
  – **Distributed Control Systems (DCS)**

• **SCADA systems** provide supervisory control for distributed assets using centralized data acquisition
  – Essentially, it is a computer system that controls and monitors a process, **all remotely**!

Source: NIST 800-82: Guide to ICS Security
What does SCADA control?

- Water distribution
- Wastewater collection systems
- Oil and Natural Gas pipelines
- Electrical power grids
- Railway transportation systems
- Refineries
- Chemical plants
- Telecom
- Building environment control systems
And worst of all...

SCADA controls all sorts of things, such as winery systems, and ...

... such as the **Budweiser Plant** in St. Louis, Missouri!
What’s so special about SCADA?

• Highly **distributed systems**
  – Control **geographically dispersed assets**, often scattered over thousands of square kilometers

• **Control and monitoring data** transmitted over long-distance communications networks

• Process control has been automated to an significant extent
Supervision, Data Acquisition End

- HMI: Human Machine Interface
- Workstations
- Historian/Logging
- Control Server (MTU)
- Routers & Firewalls

Internal/Private network

External/Public network
Remote End

- Protocol Translator
- Ethernet Gateway
- Interoperability
- Modems/Network Cards
- PLC – Prog. Logic Controller
- RTU – Remote Terminal Units
- Actuators
- Sensors
- Environment/Process
- External/Public networks
- Internal/Private network
Communications (Middle)

- Telephone, Power Lines
- Radio (VHF/UHF), Microwave, Cellular
- Satellite
- WAN/LAN
The SCADA Context

• SCADA is different from IT systems:
  – SCADA computations and logic have a direct affect on the **physical world**
  – **Safety, efficiency, maintainability** sometimes conflict with cyber security of control systems

• Ordered list of security expectations from SCADA
  1. Availability
  2. Integrity
  3. Confidentiality

The Empire State Building and midtown New York City are shown during the 2003 blackout. (AP Photo)
SCADA Evolution

15 to 20 years prior
- Proprietary Devices and OS
- Vendor defined protocols
- No standards
- Push button panels
- Isolation from public networks

Today
- COTS, Microsoft, Linux OS
- Internet Protocol, Ethernet, Wireless
- Open Standards
- Remote setup and configuration
- Share public networks
SCADA systems (1\textsuperscript{st} gen.)

Source: NCS TIB 04-1
SCADA systems (2nd gen.)
SCADA systems (now)

Source: NIST 800-82: Guide to ICS Security
Source: NIST 800-82: Guide to ICS Security
Source: NIST 800-82: Guide to ICS Security
What caused the Evolution?

• Widely available, low-cost Internet Protocol (IP) devices are replacing proprietary solutions

• Corporate networks are being connected to SCADA systems as part of business processes

• Bottom-line:
  – They are starting to represent traditional IT systems!
Problems
Trust me, it’s a problem…
Proprietary protocol is a Myth

• Long system lifecycles do tend to make SCADA systems obscure

• Attackers are dedicated and persistent
  – Will spend significant effort to study and understand available applications and protocols

• While the systems may not be available for examination
  – The vendors have datasheets and protocol documents openly available for examination
Who are the cyber attackers?

• Vandals
  – Disgruntled employee, ego, pride, awareness, personal beliefs, revolt

• Cyber Mercenaries
  – Money

• Nation States
  – Information operations
  – Espionage
  – Cyber warfare
What does it take to cause damage to SCADA?

• Blocked or delayed flow of information
• Unauthorized changes to instructions, commands, or alarm thresholds
• Inaccurate information sent to system operators
• SCADA software infected with malware
• Interference with the operation of safety systems, which could endanger human life

Source: NIST 800-82: Guide to ICS Security
Attack Scenarios?

• Advanced persistent threats in the corporate network reach the master control network
  – Giving up keys to the kingdom

• Remote sites are directly contacted
  – Disable controls
  – Subvert system to insert time and logic bombs
  – Spying, identifying sensitive installations

• Communication networks are used for passive monitoring of operations
  – Man in the middle attacks
    • Spoofing messages, dropping messages, eavesdropping
Real Case 1

Gas refineries at Defcon 1 as SCADA exploit goes wild
At least they should be
By Dan Goodin in San Francisco
Posted in Security, 8th September 2008 18:32 GMT

Gasoline refineries, manufacturing plants and other critical facilities that rely on computerized control systems just became more vulnerable to tampering or sabotage with the release of attack code that exploits a security flaw in a widely used piece of software.

The exploit code, published over the weekend as a module to the Metasploit penetration testing tool kit, attacks a vulnerability that resides in CitectSCADA, software used to manage industrial control mechanisms known as SCADA, or Supervisory Control And Data Acquisition, systems. In June, the manufacturer of the program, Australia-based Citect, and Computer Emergency Response Teams (CERTs) in the US, Argentina and Australia warned the flawed software could put companies in the aerospace, manufacturing and petroleum industries at risk from outsiders or disgruntled employees.
'Cyber Attack' Aimed At Texas Electricity Provider
By Robert Arnold
POSTED: Saturday, April 3, 2010
UPDATED: 9:54 am CDT April 5, 2010

HOUSTON -- Local 2 Investigates has uncovered details about a so-called "cyber attack" on one of Texas' largest electricity providers, KPRC Local 2 reported Saturday.

A confidential e-mail obtained by Local 2 explains a "single IP address in China" tried 4,800 times to log in to the Lower Colorado River Authority's computer system. In the e-mail, the Electricity Reliability Council of Texas reports all login attempts failed and went on to term the incident a "suspected sabotage event." The e-mail explained the FBI had been notified.

Real Cases 3 and 4

• April 2000, Vitek Boden, a former contractor, took control of the SCADA system controlling the sewage and water treatment system in Australia
  – Using a wireless connection and a stolen computer, Boden released millions of gallons of raw sewage and sludge into creeks, parks and a nearby hotel.

• In late 2006, a foreign hacker penetrated security at a water filtering plant near Harrisburg, Pennsylvania
  – Planted malicious software capable of affecting the plant’s water treatment operations.
Real Cases 5 and 6

• In January 2008, a teenage (14 year old) boy who hacked into a Polish tram system used it like “a giant train set,” causing chaos and derailing four vehicles.

• In 2007, the “Aurora Generator Test” was conducted by the US Department of Homeland Security (DHS) and involved the remote accessing of a generator control station by a foreign hacker.
  – It resulted in the partial destruction of a $1 million large diesel-electric generator.
Attacks close to home

- Let the games (err... attacks) begin!
"Last May we had an incident where one of our web pages was exploited through an SQL injection flaw," Kerber said. "It was a wake-up call that we had vulnerabilities people could find out about."
Mitigations/Solutions
NERC top ten vulnerabilities

• Inadequate policies, procedures and a security culture to govern control systems
• Incomplete design of control network security architecture
• Remote access without appropriate access control
• Applications used in control system are not appropriately tested for security
• Inadequately secured wireless communications
NERC top ten vulnerabilities

• Use of non-dedicated communications channel for command and control
• Insufficient mechanisms to report anomalous system activity
• Unauthorized or inappropriate applications or devices on the control network
• Command and data source not authenticated
• Inadequately managed support infrastructure
SCADA Security Challenges

• Common security technologies can be hard to deploy on low powered devices
• Authentication is shared or often non-existent
• Long lifetime
• Vulnerability and patch management is difficult
  – No maintenance downtime available
• Limited auditing (only when something breaks)
• Most focus only on boundary controls (Firewalls)
The Standards and Best Practices Labyrinth

• The good thing is that
  – There’s plenty to choose from!
• NIST Special publications
  – Enhancement to 800-53
  – 800-82
• NERC
  – In Hindi it means “Hell”, what a coincidence!
  – Cyber protection CIP augmentations, Being enforced since July 2009
• ISO / IEC standards
• DHS CS\textsuperscript{2}SAT self assessment tool
CS²SAT
CONTROL SYSTEM CYBER SECURITY SELF-ASSESSMENT TOOL

THE DEPARTMENT OF HOMELAND SECURITY

National Cyber Security Division
Control Systems Security Program

Ver 2.0
1. Select the standards to be included in this assessment.

- NERC CIP-002 through CIP-009
- NIST SP800-53 Rev. 0
- NIST SP800-53 Rev. 1
- NIST SP800-53 Rev. 2
- ISO/IEC 15408 (Common Criteria)
- DoDI 8500.2
- SANS Top 20
- Components (Control System Diagram)
Critical Cyber Assets

1. Has a risk-based assessment methodology been documented to identify critical assets?

2. Is the risk-based assessment documentation, procedures, and evaluation criteria maintained as required?

3. Does the risk-based assessment consider the required assets (see HELP for required assets)?
Overlaps are typical among standards

• NERC-CIP-7-R-2.2.1:
  – The Responsible Entity shall enable only those ports and services required for normal and emergency operations

• NIST 800-53 CM-7 LEAST FUNCTIONALITY
  – ......provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services

• NIST 800-82 Guidance, pg 70
  – Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis.
Significant Overlaps among the Standards

- Why not have them all relate to each other?

NERC-CIP-7-R-2.2.1
NIST 800-53 CM-7 LEAST FUNCTIONALITY
NIST 800-82 Guidance, pg 70
Ports and Services
A SCADA Domain Model

Service

- **Name**: string
- **Status**: boolean
- **Port-Number**: integer

Service Instance on PLC 80082

- **Name**: FTP service
- **Status**: true
- **Port-Number**: 20
Our Research
Our Approach

• Make an explicit relationship between the high level policies to concrete system attributes monitored for anomalous behavior detected in near-real time

**Policy:**
The system shall not...
A Component Based Anomaly View

• Write executable “Policy Monitors” that watch for anomaly or compliance violation for each critical SCADA component
  – Divide and Conquer

• What is divided must also be put back together
  – A domain model facilitates this task at a higher level of abstraction
The Domain Divide

- SCADA domain experts are NOT security experts

- Their primary concern is safety and functional availability of the infrastructure services

- Industry adoption can be inversely proportional to the complexity of a solution and the changes required
The Always Block

• Inspired by “Verilog”, a hardware description language, for Digital Logic Chips
  – “always” is a parallel execution statement that triggers every time the events are detected

```plaintext
always @(Gotham Port?,
             Gotham Service?)
```

48
1. ACA Model of water-supply SCADA system

2. Monitoring the metrics and measures from the simulation

3. Malicious Fault Injection point

4. Summary of XML based Messages sent out from the simulation

Examination of tank water levels over a period of time.
Machine-understandable Model of the SCADA system
Summary

• We now know....
  – What SCADA means
  – Why is it’s cybersecurity a concern
  – What are the top ten vulnerabilities in control systems
  – What are the SCADA regulations and best practices
  – What is the cool new research going on at UNO
Acknowledgement

• This research is funded in part by Department of Defense (DoD)/Air Force Office of Scientific Research (AFOSR), NSF Award Number FA9550-07-1-0499, under the title “High Assurance Software”
Conclusions / Questions