SCADA Past, Present and Future

Dale Rowe PhD
Asst. Professor, Information Technology & Cyber Security
Jordan Sheen BSc
Research Assistant, Cyber Security Research Lab
Overview

• Introductions
• Overview of SCADA
• The problem
• History of SCADA Security
• IAS – Strengths and Failings
• Research
Dale Rowe PhD, CISSP, GXPN, CITP MBCS, MCP

- Background in secure systems architecture
- Moved to Utah in 2010
- Teach the security emphasis of the IT Program
  - Information Assurance and Security
  - Digital Forensics
  - Systems Administration
  - Cyber Security & Penetration Testing
- Co-Director of the Cyber Security Research Lab
- Married, 5 Children. Live in PG
- dale_rowe@byu.edu
• Jordan Sheen
  – Background in enterprise virtualization
  – BSc in Information Technology at BYU
    • Emphasis in Cyber Security
  – Currently researching SCADA Security & Forensics for a Masters degree in IT
  – Working for BYU’s Office of IT
  – Married, 4 Children, Living in Provo
  – jordan_sheen@byu.edu
Overview of SCADA

• Stands for
  – Supervisory Control and Data Acquisition
• Used to
  – Monitor and control a plant or equipment
• Used in
  – Telecommunications, water, waste control, energy, oil and gas refinement, transportation…
Components of a SCADA System

- Programmable Logic Controller (PLC)
- Remote Transmission Unit (RTU)
- Supervisory Computer System
- Human-Machine Interface (HMI)
- Communications Infrastructure
- Instrumentation
Putting it all together

The SCADA system reads the measured flow and level data, and sends the setpoints to the PLC.

- PLC1 compares the measured flow to the setpoint and adjusts the pump speed as required.
- PLC2 compares the measured level to the setpoint and adjusts the flow through the valve as required.

http://www.technologyuk.net/telecommunications/industrial_networks/scada.shtml
Security Problems

• Many proprietary technologies and protocols
  – What is the security review process?
  – How do we detect an attack?
  – Legacy hardware/software

• Security through obscurity

• No Secure Development Lifecycle for SCADA

• No authentication protocol
  – Minimum protocol set
  – If you can send it a packet, you can control it

• What happens if we connect all of this to the Internet?
Security Problems - Quote

• ‘One of the best security measures is to select a controller that utilizes an embedded operating system not popularly used by the consumer public. This helps keep the PLC from being vulnerable to attackers using known exploits to the operating system because the knowledge base is much smaller.’
• ‘a properly configured router can provide effective protection for the control network from potential attacks.’
• For increased protection, a virtual private network (VPN) can be setup to increase the security by encrypting the data transmission when traveling over a public network - such as the Internet.
  – White Paper: Connecting to the PLC from a Remote Location, WAGO Corporation.
Categories of SCADA Attacks

• Intentional, targeted attacks
  – Clever bad guy
• Unintentional consequences from malware or failure
  – Stupid bad guy
• Unintentional consequences caused by internal personnel or mechanisms
  – Just plain stupid
History 101

• Referring to the Nov 8 2011 Houston Water SCADA Attack:
  – “Everybody keeps asking how come you don’t see attacks on SCADA systems? Well, here it is guys,” (Joe Weiss)

• We’re not scared of one guy with a laptop…
  – White House spokesman Robert Gibbs
History

• Siberian Pipeline Explosion (1982)
  – SCADA Trojan caused an explosion equivalent to 3 kilotons of TNT
• Chevron Emergency System (1992)
  – Disgruntled employee sabotaged the emergency system in over 22 states
• Roosevelt Dam (1994)
  – Hacker breaks into SCADA floodgate systems
• Worcester Airport, Massachusetts (1997)
  – Teenager broke into communication system and shutoff comms for 6 hours (including runway lights)
• EU Main Gas Pipeline
  – Hackers used Trojan to control pipelines
• Bellingham, Washington Gasoline Pipeline (1999)
  – Pipeline ruptured leaking gasoline into creeks before igniting and killing three, injuring 8.
• Russian Natural Gas Pipeline (2000)
  – SCADA system hacked to gain control. Not known if physical damage was caused.
History

- Maroochy Shire Sewage Spill (2000)
  - After control system was installed, series of problems including ‘random’ valves opening. After months of logging discovered spoofed controllers being run by disgruntled employee. 264,000 gallons of raw sewage flooded into hotel, park and river.

- Venezuela Port (2002)
  - Hackers disabled PLC components during strike disabling the country’s main port

- Slammer (2003)
  - SQL Server Worm infected an Ohio nuclear power plant disabling safety monitoring for 5 hours. Airlines also crippled.

  - 50 million people in midwest, northeast US and Ontario affected by blackouts. Estimated to cost between $4 billion and $10 billion USD.

- Sobig Virus (2003)
  - E-Mail attachment worm caused shutdown of CSX Train Signalling System.
History

- Israel Electric Corporation (2003)
  - DoS attack from Iranian addresses attempted to shutdown IEC Systems
- Zotob Worm (2005)
  - Windows PnP buffer overflow crashed 13 of DaimlerChrysler automobile manufacturing plants.
  - Malware infected HMI systems disabled emergency stop of equipment in adverse weather.
- Middle East Sea Port (2005)
  - Intrusion test gone wrong – ARP spoofing shut down port signalling system
- California Canal System (2007)
  - Former employee installed unauthorized software to divert water from the Sacramento river.
  - Emergency shutdown due to software update. Business network and SCADA networks were connected.
  - Insider attack
History

- **STUXNET (2010)**
  - Malware leveraging 3 zero-day attacks to sabotage Iranian nuclear enrichment facilities. Misreported data to HMI.

- **DUQU (2011)**
  - Recon malware (preparatory to further attacks?). Shared code with Stuxnet – could be from reverse engineering or same authors

- **Illinois Water Pumps (2011)**
  - Pump burned out

- **Houston Water Pumps (2011)**
  - Weak (3 letter) passwords led to unauthorized pump control

  - Coding error or hacker?
Current Issues

- Hardcoded default passwords
- Services that cannot be disabled:
  - Telnet
  - FTP
  - Windriver Debug
- No authentication/encryption
  - Eavesdropping
  - Replay attacks
- Railway SCADA running over GSM-R
  - More secure than GSM, but keys delivered on USB sticks...
- SCADA Malware SDK’s
- NSA Director states that capability to control US Power Grid could be within grasp for groups like anonymous within 1-2 years
- Jailbreak – Prison ICS
Simulated Attack on Power Infrastructure

- http://www.youtube.com/watch?v=fJyWngDco3g
Changing Landscapes

- 1975 Frequency Allocation Chart
- 2007 Frequency Allocation Chart
Changing Landscapes

• Everything connected in cyberspace
• Evolving definitions
  – System of systems
  – What is a system?
    • Computers?
    • Networks?
    • Users?
    • Critical Infrastructure?
Changing Threat Levels

• Under certain conditions, an attack against infrastructure presents a greater danger than an attack against information
  – This is particularly true in SCADA environments
  – Can directly cause injury, loss of human life, physical damage
Limitations of IAS

• Information Assurance and Security was designed to protect and secure the confidentiality, integrity and availability of information
  – Scope creep?
  – Does cybersecurity = IAS?
  – Cybersecurity comprises IAS + ?
The Future

• What is needed?
  – Increased collaboration between SCADA developers and security professionals
  – Risk assessment
  – Secure architecture
  – Defence in depth
  – Secure (Embedded) Software Development Lifecycle
  – Effective threat detection
SCADA Research

• What has been done
• What is happening now
• Where the research is headed
Previous SCADA Research

• Lots of variety in what was done previously
• Research covering all kinds of areas including security strategy, architecture to support security, and proof of vulnerabilities.
Previous SCADA Research

• Eric Byres
  – Tofino Security

• Joe Weiss
  – One of the main advocates of not only SCADA security, but industrial control in general.

• Maynor and Graham
  – BlackHat 2006 Federal, “We’re Not Crying Wolf!”
  – Showed what could be done.

• Other research…
Previous SCADA Research

- Next Generation SCADA Security (Bowen, CL 2005)
- Improving Security for SCADA Control Systems (Hentea, M. 2008)
- Challenges for Securing SCADA Systems (Cardenas, A. 2009)
- The list goes on…
Current Research

• Research effort trotted along, then exploded after Stuxnet.
• Why?
  – Stuxnet validated what people like Byres, Weiss, and others said.
  – People learned to live with the vulnerabilities, because there weren’t risks.
  – Security is really bad when, “This required almost no skill and could be reproduced by a two year old with a basic knowledge of Simatic.” (Pr0f pastebin post on South Houston break-in)
Now there is research looking at a variety of problems and solutions relating to SCADA systems
Current Research

- Trust Systems
- Intrusion Detection/Prevention
- Honeypots
- Forensics
- Education
- More?
Trust Systems

- Why?
  - C.I.A

- Want the protocol to be confidential
- Want the communication to have integrity
- Want the information to be authentic
Trust Systems

• What challenges exist in this area?
  – Bandwidth
    • If you’re trying to do authentication over a serial link, on a real-time system, you need that authentication to be fast
  – Keysize
    • Big key sizes aren’t acceptable
  – Computing power of the Programmable Logic Controllers and Human Machine Interfaces
    • Not built for this kind of workload, especially the older stuff.
Trust Systems

• Research
  – What kind of trust system can be used?
  – Should we use symmetric over asymmetric?
  – How do we manage keys?
  – Can we modify it to support a broader range of protocols?
    • Not just UDP, but TCP as well
    • Add support for multicast (ASKMA+)
Intrusion Detection

- Why
  - Placement
  - Effective, when you have a signature
- What about zero-day attacks?
Intrusion Detection

• Anomaly based IDS fits very well in the SCADA space
• Published research using different methods of analyzing SCADA networks, and looking for anomalies.
• A good way to protect against Zero-Days because you have a defined space indicating what your traffic should be doing.
Honeypots

• SCADA Honeynet Project
  – Custom scripts created and used with Honeyd to model modbus PLCs.
• At one point used by CERN in Switzerland, and Northrup Grumman.
• Problem is making something like honeyd high fidelity.
There’s an issue of determining what happened on a SCADA network in the event of a suspected attack.

Can be very difficult to do for a lot of reasons:

- Live forensics seem to be out of the question
- Not enough historical information to compare
Forensics

• Challenges in Live Forensics
  – Automation
  – Volatility of Data
    • Registers, cache
    • Routing table, ARP, kernel stats, memory
    • Temp FS
    • Disk
    • Remote Logging
    • Physical Config
    • Network Topology
  – Powercycle a PLC and a lot of volatile information is gone
Forensics

- Live analysis is an area without a lot of research
- An area that needs more research in order to gather the rich data available.
• Challenges in Post-Mortem Forensics
• First problem is the fact that the architecture doesn’t support forensic analysis
• Second, aftermarket modifications to Windows and Linux make each solution unique.
• Research has been done showing how the architecture could be changed to support forensics, but it’s good for other problems
Note:
All three networks are comprised in two switches using VLANs for lab simplicity and portability. For the same reasons, the OPC Server software is actually installed on the same machine as the SCADA Server.
Forensics

- Most research in forensics supports the idea of integrating a “historian”
- INL Recommendation understanding the requirements of your environment, and then creating capabilities for that environment to support a forensic process.
- Future research will face the challenge of dealing with encryption in control system environments
• Joe Weiss:

• “This is where I've been pushing. Industry hasn't created an educated control system cybersecurity workforce... Industry needs to develop and train the workforce, so not only can they work with it but develop the appropriate technologies to deal with it.” (CNET Interview, May 10 2010)

• Could start even before people enter the industrial workforce
Education

- Simulation Environments
- Give good learning experience by presenting an environment that looks like a SCADA system
- Most research where a testbed or lab was created use the lab to test DOS attacks, specially crafted malware, etc.
- Getting more people who know how to deal with is.
Research Summary

- Research in SCADA security is continually growing
- Some of the research has a while before it can be implemented
- There is a lot of information that if you look at right now, you can apply.
- Good things to come.
Conclusion

• SCADA Systems security is growing
• We have to believe there will be more attacks
• We also need to take efforts to understand the new security solutions, and how to use them.