SCADA Security

NLANR/Internet2 Joint Techs Meeting
Columbus OH, July 21, 2004

Joe St Sauver, Ph.D.
University of Oregon Computing Center
joe@uoregon.edu

http://darkwing.uoregon.edu/~joe/scada/

I. Introduction

My Interest In SCADA; This Talk

- I grew up around industrial facilities (for example, my Dad was a stationary engineer who helped run an industrial steam facility for a major airline)
- My terminal degree is in Production and Operations
- SCADA-related incidents have continued to pop up in the news, sustaining my interest over time
- One note: The technical level of this talk has been tailored to insure that it doesn't provided a detailed "cookbook" that can be used by the bad guys to attack SCADA systems, while still providing sufficient technical detail/evidence to highlight some of the issues that need to be addressed.
- Given the venue, we're not going to talk about policy stuff today (but security policies are important).

So What the Heck *IS* "SCADA?"

- SCADA is "Supervisory Control and Data Acquisition" – realtime industrial process control systems used to centrally monitor and control remote or local industrial equipment such as motors, valves, pumps, relays, etc.
- SCADA is used to control chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, water purification and distribution infrastructure, etc.
- Industrial plant-scale SCADA is often referred to as a "Distributed Control System" or DCS
- SCADA nuzzles up to embedded system issues, too.

Think of SCADA As…

- … the computer equivalent of George, the guy in the hard hat, going around reading gauges and recording values on a clip board, or opening valve #173 and turning on pump #8 at 10:15AM on July 24th when the schedule says it is time to make another batch of product <foo>.
- Of course, because we're talking about computerized systems, we'll typically be talking about complex systems with hundreds, thousands or tens of thousands of remotely managed control points. At that volume, it is not surprising that SCADA is often "event driven" (e.g., "signal an alarm, something's out of spec")

II. Wow. That Sounds About As Exciting As Watching Paint Dry….

Actually, SCADA Can Be Frighteningly "Exciting"…

- SCADA insecurity may have contributed to the end of the Cold War*
- SCADA may be of substantial interest to major terrorists
- SCADA systems may suffer sabotage by disgruntled insiders, acting individually
- SCADA may have "big" technical failures
- … but we'd really prefer it to be VERY dull!

*SCADA's role in bringing an end to the Cold War needs to balanced against activities elsewhere, as described, for example, in George Crille's book "Charlie Wilson's War," (Grove Press, 2003, 0-8021-4124-2)

“The Most Monumental Non-Nuclear Explosion and Fire Ever Seen From Space."

- Thomas C. Reed, Ronald Regan’s Secretary of the Air Force, described in his book At The Abyss (Ballantine, 2004, ISBN 0-89141-821-0) how the United States arranged for the Soviets to receive intentionally flawed ***process control software*** for use in conjunction with the USSR's natural gas pipelines, pipelines which were to generate critically needed hard currency for the USSR.

  Reed stated that "The pipeline software that was to run the pumps, turbines, and values was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

  The result? A three-kiloton blast in a remote area of Siberia in 1982, which, only by some miracle, apparently didn't result in any deaths. (For context, the Halifax Fire Museum lists the massive 1917 Mont Blanc ship explosion in the Halifax Harbor at a force of 2.9 kilotons.) (but also see www.themoscowtimes.ru/stories/2004/03/18/014.html)

Nation-States Aren't the Only Ones Interested in SCADA Security

- 'A forensic summary of the investigation, prepared in the Defense Department, said the bureau found "multiple casings of sites" nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities.

  'Some of the probes suggested planning for a conventional attack, U.S. officials said. But others homed in on a class of digital devices that allow remote control of services such as fire dispatch and of equipment such as pipelines. More information about those devices -- and how to program them -- turned up on al Qaeda computers seized this year, according to law enforcement and national security officials.'

  "Cyber-Attacks by Al Qaeda Feared"
  http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26
  [See also: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html]

Sabotage By Insiders May Also Pose A Risk to SCADA Systems

- [Apologies to those of you with queasy stomachs] In 2000, in Maroochy Shire, Queensland, Vitek Boden released millions of liters of untreated sewage using a wireless laptop, apparently taking revenge against former employers. He was arrested, convicted and jailed.

  -- http://www.news.com.au/common/story_page/0,4057,3161206%255E1702,00.html

  -- http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

The Boden Incident Wasn't Unusual… Wireless Network Porosity Is Common

- 'Paul Blomgren […] measures control system vulnerabilities. Last year, his company assessed a large southwestern utility that serves about four million customers." Our people drove to a remote substation," he recalled. "Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords. […] Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports.' http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html

The ($50B) 9/14/2003 U.S. Blackout

- "Starting around 14:14, FE [FirstEnergy] control room operators lost the alarm function that provided audible and visual indications when a significant piece of equipment changed from an acceptable to problematic status. **Analysis of the alarm problem performed by FE after the blackout suggests that the alarm processor essentially "stalled" while processing an alarm event. With the software unable to complete that alarm event and move to the next one, the alarm processor buffer filled and eventually overflowed**. After 14:14, the FE control computer displays did not receive any further alarms, nor were any alarms being printed or posted on the EMS's alarm logging facilities.

  "FE operators relied heavily on the alarm processor for situational awareness, since they did not have any other large-scale visualization tool such as a dynamic map board. The operators would have been only partially handicapped without the alarm processor, had they known it had failed. However, by not knowing that they were operating without an alarm processor, the operators did not recognize system conditions were changing and were not receptive to information received later from MISO and neighboring systems. **The operators were unaware that in this situation they needed to manually, and more closely, monitor and interpret the SCADA information they were receiving."**
  ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf [emphasis added]

Mundane Attacks Could Target SCADA Network Fiber As Easily as Powerlines

- SCADA systems are often physically distributed over large areas, making physical security a challenge. Simple vandalism is a real/well known risk:
  -- “[…] vandals shot out approximately 80 individual insulators on the BPA Cougar-Thurston 115,000 volt transmission line causing it to go out of service at that time. The vandalism occurred near Cougar Dam, which is approximately 25 miles east of Eugene. BPA crews replaced the damaged insulators at an estimated cost of $6,000. Even though no electrical service to EWEB and Lane Electric Cooperative customers was disrupted by the vandalism, Eugene Water and Electric had to purchase additional power to serve its customers during the 13 hours that it took to repair the damaged line.” http://www.bpa.gov/corporate/BPAnews/archive/2002/NewsRelease.cfm?ReleaseNo=297
  -- ‘A Washington man who admitted to tampering with more than 20 high-voltage transmission towers in four Western states said yesterday he was trying to point out the power system's vulnerabilities. "I intended to loosen the bolts and by doing so illustrate the vulnerabilities of these towers," Poulin told the judge. Poulin said in a telephone interview before his arrest that he considered his actions necessary to point out that he was able to damage the towers despite being "62 years old, overweight, arthritic, diabetic, half-blind and a cancer patient living on a minimum of 12 medication pills a day.“’ seattletimes.nwsource.com/html/localnews/2001796373_transmission20m.html

And In The Interest of Balance, A Dissenting Opinion

- “Despite tantalising accounts of Al Qaeda interest in targeting SCADA networks and other critical infrastructure, there actually appears to be little interest among the hacker community in developing tools and exploits against PLC or industrial protocols such as Modbus/TCP or Ethernet/IP. Unlike IT products, tools for automatically "hacking " PLCs, remote IO devices, robots, or Ethernet-based sensors are not readily available.

  “Bedroom hackers with little or no knowledge of automation systems are, in reality, unlikely to cause deliberate harm.”

  ethernet.industrial-networking.com/articles/i15security.asp

Still Not Clear What the Official Position Is On The Urgency of SCADA Security

- -- “Senator Edwards Introduces Cyberterrorism Legislation” http://www.senate.gov/~edwards/press/2002/jan28-pr.html (see the text of the Cyberterrorism Preparedness Act of 2002 at http://www.fas.org/irp/congress/2002_cr/s1900.html)
  -- Homeland Security Presidential Directive/HSPD-7 (Critical Infrastructure Identification, Prioritization, and Protection) http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
  -- **“**Industrial control systems seen as 'undeniably vulnerable:' Congress is focusing on securing the nation's critical infrastructure” http://www.computerworld.com/securitytopics/security/story/0,10801,91790,00.html (March 31, 2004)
- **BUT…** “Cybercrime becomes DHS priority” “Cybercrime, emerging as the leading public and private sector IT threat, now ranks above cyberterrorism on the DHS radar screen, said Amit Yoran, Homeland Security Department cybersecurity chief.” www.washingtontechnology.com/news/19_6/datastream/23784-1.html (June 21, 2004, emphasis added).

III. Say What You Will, The Security of SCADA Systems **IS** Often Poor

SCADA Security Today : Where Enterprise Security Was 5-10 Years Ago

- "The present state of security for SCADA is not commensurate with the threat or potential consequences. The industry has generated a large base of relatively insecure systems, with chronic and pervasive vulnerabilities that have been observed during security assessments. Arbitrary applications of technology, informal security, and the fluid vulnerability environment lead to unacceptable risk. […] **Security for SCADA is typically five to ten years behind typical information technology (IT) systems** because of its historically isolated stovepipe organization."

  Federal Technical Support Working Group (TSWG)'s
  "Sustainable Security for Infrastructure SCADA"
  http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf
  (emphasis added)

The “Hidden Half” of the Network

- Traditionally network and security folks have focused virtually all our attention on the “enterprise” side of the network, ignoring the parallel “hidden” half of the network associated with process control systems and embedded systems.
- Process control systems and embedded systems use different protocols, different jargon, and no one ever really mentioned them. They were out of sight and out of mind, and “handled” by hardware guys.

Unfortunately, “Hidden” Does Not Always Equal Physically Separated

- In the old days, process control systems used proprietary protocols and ran with serial communications (e.g., modems) or on physically separated (“air gapped”) private dedicated networks, but that’s no longer always the case.
- These days, process control systems often run using MODBUS/TCP on the enterprise LAN and over the Internet; process control traffic may be commingled with web pages, email, P2P traffic, VoIP traffic, etc.

But Don't Take My Word For It…

- **'MISCONCEPTION #1** – *"The SCADA system resides on a physically separate, standalone network."*

  *'*Most SCADA systems were originally built before and often separate from other corporate networks. As a result, IT managers typically operate on the assumption that these systems cannot be accessed through corporate networks or from remote access points. Unfortunately, this belief is usually fallacious.'

  "Understanding SCADA System Security Vulnerabilities" http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf (RIPTECH, Inc., January 2001)

Serious Consequences of SCADA-Related Compromises

- While enterprise network security is undeniably important, unlike enterprise network security, SCADA compromises can have real world life safety impacts.
- Enterprise network security breach: financial consequences, customer privacy is compromised, systems need to be rebuilt, spam gets sent, etc., but life goes on.
- SCADA security breach? Property can be destroyed and people can be hurt or killed.

Simple Protocols

- Because SCADA devices with embedded controllers tend to have limited computational power, and were historically connected via low speed serial lines, SCADA protocols tend to be quite simple, with little or no protection against spoofing, replay attacks, or a variety of denial of service attacks.
- ‘In a demonstration at a recent security conference, [Jeff Dagle, a PNNL EE] hacked into his testbed system and tripped an electrical breaker. The breaker then signaled the SCADA software that it had opened. But the SCADA controller did not respond because it had not instructed the breaker to open. It was a classic denial-of-service attack. "We were demonstrating a weakness at the protocol level itself," said Dagle.’ http://memagazine.org/backissues/dec02/features/scadavs/scadavs.html

Long Life Cycle Devices

- Industrial plants, and the instrumentation they include, tend to be long life cycle projects – ten, fifteen or twenty year project lives are by no means uncommon. As a result, the devices that may be deployed as part of that construction may be virtual antiques by the time the facility is finally decommissioned, and there's no provision for refreshing those devices the way you might upgrade out of date PCs in some office.
- '"Anti-virus software doesn't work on these SCADA systems," said Robert Childs, information security analyst at the Public Service Company of New Mexico, who spoke at NetSec about the challenges in working with SCADA vendors to get them to comply with the new rules. "Many of these systems are based on old Intel 8088 processors, and security options are limited to us."' http://napps.nwfusion.com/news/2004/062104secwrap.html

Windows-Based Control Stations

- SCADA devices are often controlled from central monitoring stations (MTUs, or “master terminal units”). Historically those were Unix-based systems, but many contemporary MTUs are now Microsoft Windows based.
- “The end-of-life for Windows NT is having a big impact on manufacturers.” http://www.digitalbond.com/SCADA_Blog/2004_07_01_archive.html

Hard-to-Upgrade Remote Devices

- Remote devices (RTUs and PLCs) also tend to be hard to upgrade :
  -- the device may use an OS and application that was burned to ROM, and which is not rewritable ("upgrade" == replacing ROMs)
  -- the device may be physically sealed and not upgradeable, or be located in a difficult location, or have no removable media
  --- the vendor may no longer be in business, or may not be producing upgrades, or the vendor may not be allowing upgrades

Certifying Patches

- An example from the embedded system world: “Health care IT professionals say medical device makers prohibit them from changing the systems and even from running anti-virus software in some cases. These IT administrators say manufacturers often are slow to supply software patch updates and routinely claim the Food and Drug Administration (FDA) requires approval of patch-base changes. However the FDA says it has no such rules…” http://www.nwfusion.com/news/2004/070504hospitalpatch.html

Need For Positive Control ==> Simple Known/Shared Passwords

- Because of the need for positive access and control, there is a trend toward simple, known, and shared passwords. Users like to avoid situations such as: “Do you know the password to turn off the nuclear reactor before it melts down? I forgot mine today…”
- But there’s hope: people in the SCADA community are beginning to talk about strong auth systems: http://www.digitalbond.com/dale_peterson/ISA%20July%20Event.ppt

Common Passwords Across Multiple Devices

- There's also the sheer issue of managing passwords for thousands of devices – passwords will tend to be common across devices as a practical matter (this is much like SNMP community strings)
- And of course those passwords aren't changed very often (if at all), even when staff transitions occur or years have gone by…

Access Control Granularity and Accountability

- Related to the problem of shared, simple passwords is the issue of poor access control granularity; again, like SNMP, in most cases access control is “read” (everything) or “read/write” (everything).
- Accountability with common passwords is poor/non-existent, which may be one reason that transaction logging also may be limited. (Any bets how long it will take to get something like syslog-ng or SDSC Secure Syslog for SCADA systems?)

Plain Text (Unencrypted) Traffic

- These days, few of us would be willing to send our passwords over plain text transmissions paths (as we would when using telnet), yet plain text transmissions are still very common in the SCADA world.
- One notable exception: the AGA/GTI SCADA Encryption initiative… http://www.gtiservices.org/security/
- In the realtime world, encryption overhead and jitter may be the crucial problems to overcome…

All Traffic Is On Just One Port

- In many cases, SCADA traffic will be on just one port such as 502/tcp (e.g., Modbus/TCP). This is both good and bad.
- The use of a single port (or just a couple of ports) makes it easy to track that traffic, or to poke a hole in firewalls to allow that traffic to pass, but it also makes it easy for the bad guys to scan for connected devices, and it makes it impossible to do port-based selective filtering.

Few Firewall Options

- Speaking of firewalls, SCADA-protocol aware firewall choices are pretty limited out there right now; I'm aware of: http://modbusfw.sourceforge.net/ and that's about it.
- Where are the commercial SCADA-protocol-aware firewall vendors? I'd love to find out that there are dozens out there that are available which I've missed…

Critical Control Traffic on a Best Effort Network

- In some cases, SCADA systems may be impacted incidentally, as a side effect of a more general problem (e.g., frame relay network congestion and outages associated with the Slammer worm). See for example “Slammer worm crashed Ohio nuke plant network,” in http://www.securityfocus.com/news/6767/ citing http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf

IV. What Needs to Be Done?

Hard-won Lessons From Enterprise IT Need to Be Tech Transferred to SCADA Networks and Systems

- Much of what's being faced in the SCADA world has already been hashed through and fixed in the enterprise IT world. Those solutions, where suitable, need to be "thrown over the wall" to SCADA networks and systems so SCADA folks don't "reinvent the wheel." We need to visit with our process control brethren.

Secure Your Own SCADA Infrastructure

- While admittedly many SCADA issues are national in scope, there are undoubtedly SCADA control systems on your campus. Are those local SCADA systems secure?
- Do you see local port 502/tcp traffic on your campus backbone or transit links? Should it be there?
- Are you seeing probes targeting SCADA facilities from offsite? Are you reporting or blocking those probes?

Run a SCADA Honeypot?

- One familiar technique from enterprise network security is the “honeypot,” or a system that *looks* vulnerable/exploitable, but which is actually well instrumented and being run solely to capture evidence of miscreant misbehavior.
- There’s one SCADA honeypot project: http://scadahoneynet.sourceforge.net/ but how many folks are actually deploying SCADA honeypots? Not very many, I suspect… Maybe deploy one?

Update Intrusion Detection Systems

- Work has just recently begun on a DHS-funded research projected focused on developing Snort signatures for MODBUS/TCP; see: http://www.digitalbond.com/SCADA_Blog/2004_05_01_archive.html
- The excellent open source protocol analyzer Ethereal (www.ethereal.com) and a number of other common protocol analyzers also support Modbus protocols.

Add SCADA Security to Your Network Security Syllabus

- If you teach network security courses, either for university credit or as part of a professional training program, make sure SCADA security becomes part of that syllabus.
- Besides the topics covered already in this talk, some additional areas which may be worth consideration include…

Embedded Real Time Operating Systems (RTOS)

- We all know some version of Unix and/or Windows, but quick check: how many of you are also familiar with embedded RTOS's like:
  -- Integrity from http://www.ghs.com/
  -- LynxOS or BlueCat from http://www.lynuxworks.com/
  -- QNX Neutrino http://www.qnx.com/
  -- RTOS-32 from http://www.on-time.com/
  -- TinyOS from http://www.tinyos.net/
- What are their respective security strengths and weaknesses? SHOULD you know?

How About Hardware Topics, Such as Programmable Logic Controllers?

- Unless you're an electrical engineer, you probably haven't had a chance to learn about PLCs, even though there's excellent support for educational use of programmable microcontrollers such as Basic STAMPs from www.parallax.com
  or more traditional ladder-logic programming PLCs such as Toshiba's T1 (see http://xtronics.com/toshiba/plcnf.htm and http://xtronics.com/toshiba/Ladder_logic.htm

SCADA Security Research Opportunities

- Because of strong federal interest in homeland security and the relatively primitive state of SCADA security right now, there are substantial opportunities to successfully seek research support, particularly in conjunction with industry.
- There are also some remote-device-control-related activities already under way, such as the NSF Grid-related Instrument Middleware Project: http://www.instrument-middleware.org/

Vendors Are Ramping Up, Too

- Cisco deserves a big “atta boy” for its Critical Infrastructure Assurance Group: http://www.cisco.com/security_services/ciag/
- You may also want to check out the Cyber Security Industry Alliance (CSIA) at https://www.csialliance.org/ whose members include over a dozen leading security-related vendors.
- Make sure vendors know what SCADA security products YOU need them to be making!

Thanks for the Chance to Talk Today!

- Are there any questions?

Some References

- “SCADA and Industrial Automation Security,” http://www.scadasec.net/
- “SCADA Security Blog” http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm
- “SCADA Gospel Archives (edited archives of the SCADA mailing list)” “http://members.iinet.net.au/~ianw/archive/book1.htm
- “21 Steps to Improve the Cyber Security of SCADA Networks,” http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf
- “Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems” http://www.gao.gov/new.items/d04354.pdf
- “Myths and Facts Behind Cyber Security of Industrial Controls” http://www.pimaweb.org/conferences/april2003/MythsAndFactsBehindCyberSecurity.pdf
- Cisco’s “Integrating IT and Control System Security” http://www.scadasec.net/local/37
- modbus.org