SCADA (in)Security: Hacking Critical Infrastructures

Raoul Chiesa  
raoul@mediaservice.net

Alessio L.R. Pennasilico  
mayhem@alba.st

CONfidence ’08 – May 16th -17th 2008, Krakow (Poland)
UN consultant on cybercrime issues at UNICRI agency

OPST, OPSA, Key Contributor for OSSTMM (1.5, 2.0, 2.1, 3.0)

Board of Directors of:
CLUSIT, ISECOM OWASP-Italy, Telecom Security Task Force

CrISTAL, Project Manager for Hacker’s Profiling Project

http://cristal.recursiva.org/
What is SCADA?
Going commercial...

Terroristic video spot about SCADA security
“Supervisory Control And Data Acquisition”.

It’s the monitoring branch of an automated infrastructure that decides “what to do” on the basis of “what is happening” (event driven).
Managing pumps...

[Image of a computer screen displaying a SCADA system interface for managing pumps and leachate collection.]
Industrial Automation

It is reality since many years

But market is migrating infrastructures:

from proprietary, obscure and isolated systems towards standard, documented and connected ones
Critical Infrastructures

Many SCADA infrastructures are responsible for:

Power and Nuclear plants, Gas, Oil, Water distribution, Transports

but true life taught us that lack of communications created more panic than huge incidents..
# Critical National Infrastructures

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sample Target Sub-sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy and Utilities</td>
<td><em>Electrical power (generation, transmission, nuclear)</em></td>
</tr>
<tr>
<td></td>
<td><em>Natural gas</em></td>
</tr>
<tr>
<td></td>
<td><em>Oil production and transmission systems</em></td>
</tr>
<tr>
<td>Communications and Information Technology</td>
<td><em>Telecommunications (phone, fax, cable, satellites)</em></td>
</tr>
<tr>
<td></td>
<td><em>Broadcasting systems</em></td>
</tr>
<tr>
<td></td>
<td><em>Software</em></td>
</tr>
<tr>
<td></td>
<td><em>Hardware</em></td>
</tr>
<tr>
<td></td>
<td><em>Networks (Internet)</em></td>
</tr>
<tr>
<td>Finance</td>
<td><em>Banking</em></td>
</tr>
<tr>
<td></td>
<td><em>Securities</em></td>
</tr>
<tr>
<td></td>
<td><em>Investment</em></td>
</tr>
<tr>
<td>Health Care</td>
<td><em>Hospitals</em></td>
</tr>
<tr>
<td></td>
<td><em>Health-care facilities</em></td>
</tr>
<tr>
<td></td>
<td><em>Blood-supply facilities</em></td>
</tr>
<tr>
<td></td>
<td><em>Laboratories</em></td>
</tr>
<tr>
<td></td>
<td><em>Pharmaceuticals</em></td>
</tr>
</tbody>
</table>

SCADA (in)Security

http://cristal.recursiva.org/
## Critical National Infrastructures

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sample Target Sub-sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food</td>
<td>Food safety</td>
</tr>
<tr>
<td></td>
<td>Agriculture and food industry</td>
</tr>
<tr>
<td></td>
<td>Food distribution</td>
</tr>
<tr>
<td>Water</td>
<td>Drinking water</td>
</tr>
<tr>
<td></td>
<td>Wastewater management</td>
</tr>
<tr>
<td>Transportation</td>
<td>Air</td>
</tr>
<tr>
<td></td>
<td>Rail</td>
</tr>
<tr>
<td></td>
<td>Marine</td>
</tr>
<tr>
<td></td>
<td>Surface</td>
</tr>
<tr>
<td>Safety</td>
<td>Chemical, biological, radiological, and nuclear safety</td>
</tr>
<tr>
<td></td>
<td>Hazardous materials</td>
</tr>
<tr>
<td></td>
<td>Search and rescue</td>
</tr>
<tr>
<td></td>
<td>Emergency services (police, fire, ambulance and others)</td>
</tr>
<tr>
<td></td>
<td>Dams</td>
</tr>
</tbody>
</table>
## Critical National Infrastructures

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sample Target Sub-sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>Government facilities</td>
</tr>
<tr>
<td></td>
<td>Government services <em>(for example meteorological services)</em></td>
</tr>
<tr>
<td></td>
<td>Government information networks</td>
</tr>
<tr>
<td></td>
<td>Government assets</td>
</tr>
<tr>
<td></td>
<td>Key national symbols <em>(cultural institutions and national sites and monuments)</em></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Chemical industry</td>
</tr>
<tr>
<td></td>
<td>Defence industrial base</td>
</tr>
</tbody>
</table>
Parts of SCADA systems

Human Machine Interface (HMI)

Remote Terminal Unit (RTU)

Programmable Logic Controller (PLC)

Communication infrastructure
A complex infrastructure: Enel

Enel is the biggest power distributor in Italy

SCADA (in)Security

http://cristal.recursiva.org/
SCADA Issues
Hackers know about it! :)

A lot of presentations by SCADA people talk about

* DefCon, BlackHats and similar events
* on-line password and vulnerability databases
* legacy IT tools implementing SCADA scanning/testing/assessing features...

It seems that the outside world is really worried about hackers :)
Problems caused by...

- Vendors
- People
- Technology
- Incidents
- Customers

SCADA (in)Security

http://cristal.recursiva.org/
Incidents
“Shit happens!”

“About 3:28 p.m., Pacific daylight time, on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1.5 hours after the rupture, the gasoline ignited and burned approximately 1.5 miles along the creek. Two 10-year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham’s water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least $45 million.”
“The Olympic Pipeline SCADA system consisted of Teledyne Brown Engineering 20 SCADA Vector software, version 3.6.1., running on two Digital Equipment Corporation (DEC) VAX Model 4000-300 computers with VMS operating system Version 7.1. In addition to the two main SCADA computers (OLY01 and 02), a similarly configured DEC Alpha 300 computer running Alpha/VMS was used as a host for the separate Modisette Associates, Inc., pipeline leak detection system software package.”
“5. If the supervisory control and data acquisition (SCADA) system computers had remained responsive to the commands of the Olympic controllers, the controller operating the accident pipeline probably would have been able to initiate actions that would have prevented the pressure increase that ruptured the pipeline.”

Technical problems
SCADA systems need **real-time** performance.

Antivirus would **degrade** performances enough to make the system useless or dangerous.

Although SCADA systems are **vulnerable** to viruses!
“In August 2003 Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours.”

NIST, Guide to SCADA
Patching systems is a known **problem** in the IT world

Changing anything is a **nightmare** in the SCADA world.
“Our service contractor provides us patches once a year.”

*CSO of a power distribution company*
PenTesting old, small, very simple, projected-to-be-isolated devices may lead to service disruption.

The market is trying to provide a useful, but mainly “assured” method to assess SCADA networks security.

Although periodical security testing is a need, and cannot be simply ignored.
“While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated.”

NIST, Guide to SCADA
Because of all these reasons, SCADA networks must be strongly protected from a perimeter point of view: VLANs, DMZs, filtering, content filtering, IDS...
Vendors
Vendor Live witness
Insecure by default?

Traffic in clear text
No data encryption
No authentication
No accounting
Customers
Customer live witness
(no disclosure agreement)
Mr. Rossi, CIO in a Power Distribution Company

The last project has been a hard work:
Common mistakes

Merged IT and SCADA network
(no physical or logical separation)
RAS/VPNs provide too much simple remote access
Default configurations
No backups at all
No tested disaster recovery plan
People...
...were used to ...
...but now have to work with...
“The power plant monitoring system was unresponsive. When emergency services arrived, they found the operator watching a DVD on the HMI system”.

CSO of a power distribution company
Vitek Boden, in 2000, was arrested, convicted and jailed because he released millions of liters of untreated sewage using his wireless laptop. It happened in Maroochy Shire, Queensland, may be as a revenge against his last former employer.

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
Thomas C. Reed, Ronald Regan’s Secretary, described in his book “At the abyss” how the U.S. arranged for the Soviets to receive intentionally flawed SCADA software to manage their natural gas pipelines.

"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."

A 3 kiloton explosion was the result, in 1982 in Siberia.

http://www.themoscowtimes.ru/stories/2004/03/18/014.html
“Russian authorities revealed this week that Gazprom, a state-run gas utility, came under the control of malicious hackers last year. […] The report said hackers used a trojan horse program, which stashes lines of harmful computer code in a benign-looking program.”

http://findarticles.com/p/articles/mi_qa3739/is_200403/ai_n9360106
Lagos, Nigeria - “At least 40 people died because of fire injuries coming from a pipeline they were trying to open to steal petroleum.”

[…] “One year ago more than 250 people died in the same circumstances near Lagos.”

http://news.bbc.co.uk/2/hi/africa/6209845.stm
“On August 2007 Anti Imperialist Team placed a complex and powerful home-made bomb at the pipeline in Vicenza, North of Italy, the one that take kerosene from the NATO base in Aviano to the Vicenza’s one”.

http://www.ansa.it/opencms/export/site/notizie/rubriche/daassociare/visualizza_new.html_127962764.html
DON'T PANIC!
Security Standards
“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.”

SCADA security **evolution** is at the same point IT security was 5 years ago.

**Differences** are to be understood, and a similar approach and security path has to be done.

Does **exists** any SCADA Security Standard?
SCADA Security Standards

BS7799-ISO27000 Information sec. management systems – Specification with guidance for use

ISO/IEC 17799:2005 Information Technology – Code of practice for information sec. management

ANSI/ISA S.99.1 Security for Manufacturing and Control Systems

ANSI/ISA SP99 TR2 Integrating Electronic Sec. into Manufacturing and Control Systems Env.

ISO/IEC 15408 Common Criteria

NIST System Protection Profile for Industrial Control Systems (SPP-ICS)

CIDX Chemical Industry Data Exchange - Vulnerability Assessment Methodology (VAM) Guidance

ISPE/GAMP4 – Good Automated Manufacturing Practices

PCSF Process Control System Forum ; NERC standards ; AGA standards ; NISCC Guidelines
ISO27000 vs. ISA-99.00.01

Traditional IT systems

- Confidentiality
- Integrity
- Availability

Manufacturing and Control System

- Availability
- Integrity
- Confidentiality

Different Priorities
The CrISTAL Project
Critical Infrastructures Security Test & Analysis Lab was born in 2007 from some everyday-working-on-security and often-working-on-scada professionals, to inform the world about SCADA issues.

http://cristal.recursiva.org/
Project Objectives

- talk with people, as many people as possible
- exchanging experiences related to SCADA security
- perform more technical research
- measure the SCADA’s market real security level
- write documents / white papers
- write necessary tools
- create a FDL methodology to pentest SCADA
<table>
<thead>
<tr>
<th>Technical</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Measurement</td>
</tr>
<tr>
<td>Security Testing</td>
<td>Education</td>
</tr>
<tr>
<td>Hardening</td>
<td>Ergonomics</td>
</tr>
</tbody>
</table>
First Steps

✓ released a paper for CLUSIT
✓ workshops at different events in Italy and Europe
✓ workshops for students at universities
✓ a first public case history, chosen among our available references and research partner companies
Companies

Airliquide.com (Cryogenics, Industrial and Medical Gas Distribution)
Mil Mil (Healthcare)
Mirato (Healthcare)
Sovema (Manufacturing)
Multiutility (Power & Gas)
Sant Luis (Manufacturing)
Others (NDA signed)

written DA required
Sovema case history video
“... is the world leader committed with the manufacturing of battery making equipment ...”

Established 38 years ago

average 30 MLN US Dollars sales/year

Italy: about 100 employees, 10,000 sq

Offices in Europe, Asia and U.S.A.
Sovema always used SIEMENS Profibus technologies then some customers demanded for Ethernet and they implemented a new solution...
Infrastructure details

A new internal test-bed
A PLC with expansion card
An operator panel
Visual alert about PLC operations
The Testbed


# Rockwell Encapsulation
# Rockwell Encapsulation
Brian Batke - bbatke@ra.rockwell.com

SCADA (in)Security

http://cristal.recursiva.org/
Tools

brain - always needed!
nmap - let’s meet ...
nessus - just to be sure about stupid things :)
wireshark - do you feel the net inside yourself? :)
custom scripts/commands/hacks/test/experience
# rockwell-encap (44818/tcp)
# http (80/tcp)
# snmp (161/udp)
# rockwell-csp2 (2222/udp)
# rockwell-encap (44818/udp)

No access to PLC functions trough HTTP or SNMP /
No parameters can be changed trough HTTP /
No HTTP authentication / Remote monitor via CIP
# rockwell-encap (44818/tcp)
# streetperfect (1330/tcp)
# intersan (1331/tcp)
# netbios-ns (137/udp)

Managed through the display / Monitored via CIP by a HMI / Honours the source-route option / File server available
The page at http://192.168.1.160 says:

HITB!
Clear Text Traffic

EtherNet/IP (Industrial Protocol), Session: 0xA020100, Send Unit Data

- Command: Send Unit Data (0x0070)
- Length: 28
- Session Handle: 0xA020100
- Status: Success (0x00000000)
- Sender Context: 0000000000000000
- Options: 0x00000000

Command Specific Data
- Interface Handle: CIP (0x00000000)
- Timeout: 0
  - Item Count: 2

Common Industrial Protocol

- Service: Get Attribute All (Request)
  - 0... .... = Request/Response: Request (0x00)
  - .00 0001 = Service: Get Attribute All (0x01)
- Request Path Size: 2 (words)
- Request Path: Identity Object, Instance: 0x01
- 8-Bit Logical Class Segment (0x20)
  - Class: Identity Object (0x01)
- 8-Bit Logical Instance Segment (0x24)

```plaintext
04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05 00 00 00 00 02 00 a1 00 04 00 c1 00 3c 00 b1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06 08 00 01 00 01 02 20 01 24 01
```

SCADA (in)Security

http://cristal.recursiva.org/
DoS

- nmap -sV / -O
- ping -f
- ping -s > 56200
- Traffic > 10 Mb/s

All conditions that make both devices unresponsive
**Results**

**DoS:**
- ping -f, ping -s 56200, nmap -sV/-O

**WEBugs2.0:**
- xss, no auth, but no parameters to change

**Protocol:**
- cleartext, easily forgeable
- snmp, but useless on SCADA, only IP
Considerations

Very simple device (both HW&SW), very tailored:

- very simple to DoS
- some “silliness”, but nothing terrible
- no huge bugs
- emerged the need for specific tools ...
Todo

- involve more people
- release a periodic bulletin about market status
- write more tech&org articles/white papers
- create a larger pool of public case histories
- write some tools (i.e. CIP injector)
- release a PenTesting methodology under FDL
Conclusions
Best Practices

- Split into VLANs/DMZs
- Firewall / Content Filtering / IDS
- Implement device redundancy
- Take care about physical security
- Update and verify documentation
- ... and apply policies
✓ Disable unused services
✓ Adopt AAA solutions
✓ Use encryption (i.e. VPN)
✓ Implement Quality of Service
✓ Use test-bed for simulations/security tests
✓ periodically run security tests (with a declared and common methodology)
http://cansecwest.com/slides06/csw06-byres.pdf
http://www.mayhem.hk/docs/scada_univr.pdf
http://darkwing.uoregon.edu/~joe/scada/
http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=206
http://www.apogeonline.com/libri/88-503-1042-0/ebook/libro
http://www.sans.org/reading_room/whitepapers/warfare/1644.php
http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm
http://www.visionautomation.it/modules/AMS/article.php?storyid=32
http://www.iscom.istsupcti.it/index.php?option=com_content&task=view&id=16&Itemid=1
http://books.google.it/books?id=xL3Ye3ZORbgC
I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions.

These slides are written by Alessio L.R. PenzaSilico aka mayhem. They are subjected to Creative Commons Attribution-ShareAlike 2.5 version; you can copy, modify, or sell them. “Please” cite your source and use the same licence :/
The CrySTAL Project
Critical Infrastructures Security Testing & Analysis LAB

Thank You!

Raoul Chiesa
raoul@mediaservice.net

Alessio L.R. Pennasilico
mayhem@alba.st

CONfidence ’08 – May 16th -17th 2008, Krakow (Poland)