SCADA Security Testing

APPLIED RESEARCH AT BCIT

RESEARCH - DEVELOPMENT - SOLUTIONS

Who Turned Out The Lights?

Security Testing for SCADA and Control Systems

Eric Byres, P.Eng. ebyres@wurldtech.com
Darren Lissimore darren.lissimore@gmail.com
Nate Kube nkube@wurldtech.com

Wurldtech analytics

BCIT
www.tc.bcit.ca

APPLIED RESEARCH AT BCIT

What are Critical Infrastructures?

- "Infrastructure systems for which continuity is so important that loss, significant interruption or degradation of service would have grave social consequences."

Source : National Infrastructure Security Coordination Centre, UK

APPLIED RESEARCH AT BCIT

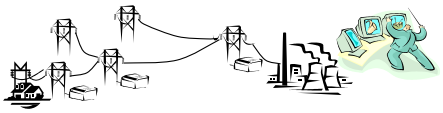
What are Critical Infrastructures?

- Power generation and distribution
- Oil and gas refining and distribution
- Water and waste systems
- Chemical processing and transport
- Manufacturing
- Telecommunications
- Banking

APPLIED RESEARCH AT BCIT

Running The Show

- Most critical infrastructures are controlled by a web of dedicated computers.
- Typically known as Supervisory Control And Data Acquisition (SCADA) systems.



APPLIED RESEARCH AT BCIT

Also Known As…

- Process Control Systems
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)
- Intelligent Electronic Device (IED)

APPLIED RESEARCH AT BCIT

Ethylene Oxide Explosion at Sterigenics International

- http://www.chemsafety.gov/index.cfm?folder=news_releases&page=news&NEWS_ID=286

BCIT

SCADA Security Testing

Security Through Obscurity

- For many years SCADA systems were proprietary, isolated systems.
- Typical industry view…

  "Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge."

  "Debunking the Threat to Water Utilities", CIO Magazine, March 15, 2002

Why is Internet Security Linked to Critical Infrastructure Protection?

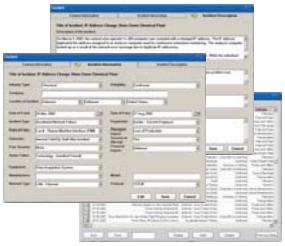
- Today industry is experiencing massive changes as new network technologies are used:
  - Windows-based operator stations
  - Web technologies in control equipment
  - Ethernet and TCP/IP networks
  - Wireless networking

Separating Fact from Fiction

- We need a realistic assessment of the risks to our critical control systems:
  - What is fact & what is urban myth?
  - How urgent is the security risk?
  - What vulnerabilities are exploited?
  - What are the threat sources?
  - How serious are the consequences?

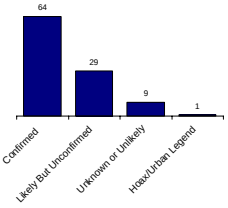
What is Industrial Security Incident Database (ISID)?

- ISID tracks network cyber incidents that directly impact industrial and SCADA operations.
- Both malicious and accidental incidents are tracked.

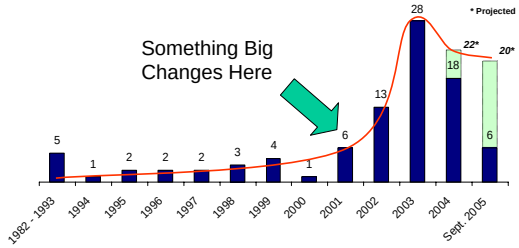


September 2005 ISID Status

- 103 Incidents (26 Pending)
- 17 Contributor companies from:
  - USA, Canada, UK, France and Australia
  - Oil/Gas, Chemical, Power, Food, Water…



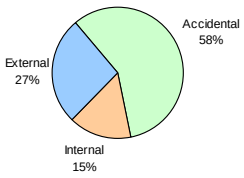
Incident Trends 1982 -2005



SCADA Security Testing

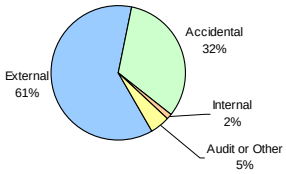
Types of Incidents 1982 -2001

- Incidents are primarily internally driven:
  - Accidental
  - Inappropriate employee activity
  - Disgruntled employees



Types of Incidents 2002 - 2005

- Most incidents are externally driven:
  - Virus/Trojan/Worm
  - System Penetration
  - Denial of Service
  - Sabotage



External Attacks on the Rise/ Accidental Incidents Steady

- External Incidents have grown by an order of magnitude.
- There are a worrying number of accidental incidents, many of which have significant cost implications. Most are due to:
  - *Poor design of products*
  - *Poor design of systems*

Worlds in Collision

- Why is PCN/SCADA Security a Challenge?
- Five Key Differences between IT and IC

Wurldtech analytics

BCIT

www.tc.bcit.ca

Why is PCN/SCADA Security A Challenge?

"Why not just apply the already developed practices and technologies from existing Information Technology security to plant floor security - isn't that good enough to solve the problem?"

Researcher at Security Conference

No Problem?

- *"None of this would be a problem if those plant floor people just used proper security policies – what's wrong with them?*

IT Manager after a Security Incident

Five Important Differences

- Key differences between IT and IC worlds:
  - #1 - Differing Performance Requirements
  - #2 - Differing Reliability Requirements
  - #3 - "Unusual" Operating Systems and Applications
  - #4 - Differing Security Architectures
  - #5 - Differing Risk Management Goals
- Problems occur because assumptions that are valid in the IT world may not be on the plant floor.

Example: The IT Approach to Vulnerability Management

- In the IT world we can scan for vulnerabilities on the network.
- Then we patch…

Let's Scan for Vulnerabilities #1

- Ping sweep was being performed on network that controlled 9-foot robotic arms.
- One arm became active and swung 180 degrees.
- The controller for the arm was in standby mode before the ping sweep was initiated.
- Luckily, the person in the room was outside the reach of the arm.

Let's Scan for Vulnerabilities #2

- An ISS scan was performed on a food manufacturer's network. Some packets made it onto PLC network.
- Caused all PLCs controlling the cookie manufacturing to hang.
- Destruction of $1M worth of product.

Let's Scan for Vulnerabilities #3

- A gas utility hired a security company to conduct penetration testing on their corporate IT network.
- Consultant ventured into the SCADA network.
- Penetration tool locked up the SCADA system.
- Gas utility was not able to send gas through its pipelines for four hours.

And Then We Patch…

- PLC/DCS/RTU patching can be done but…
  - Controllers often run for years without shutdown (long intervals between patches).
  - Patching may require "Return-to-vendor".
  - Patching may require re-certification of the entire system.

SCADA Security Testing

The Reality: Limited Resources in a Small Box

- Modern controllers are typically based on a commercially available embedded systems platforms.
- CPU and memory limitations.
- Primary focus is control functionality.

The Reality: Market Pressure

- Lots of market pressure to offer a number of communications requirements.
- Typically based on commercial or industrial specifications:
  - Ethernet, IP, TCP, UDP, HTTP, SNMP, etc.
  - MODBUS, ProfiNet, EtherNET/IP, etc.

The Reality: SCADA Device Testing

- Testing is compliance based.
- Send the device under test (DUT) a number of known valid messages:
  - DUT Responds correctly – **Pass**
  - DUT Responds incorrectly – **Fail**
- DUT response to malformed or invalid messages is rarely tested.

The Result - Vulnerabilities

- Products are shipped and deployed without knowledge of possible flaws:
  - PLCs fail while being scanned, indicating TCP/IP implementation issues;
  - RTUs violate basic TCP standards;
  - PLCs have dangerous legacy commands;
  - Nearly all PLC/DCS have no authentication.

APPLIED RESEARCH AT BCIT

RESEARCH · DEVELOPMENT · SOLUTIONS

Security Quality Assurance Testing

Wurldtech analytics

BCIT

www.tc.bcit.ca

Security Quality Assurance Testing

- Industry needs a way to find vulnerabilities before control devices are deployed.
- Need tests for a basic security level of assurance:
  - What does the device really do?
  - Is the device stable under typical DoS attacks?
  - Is the device secure for buffer overflows, etc.?

SCADA Security Testing

A Multi-pronged Approach

- **Profiling Tools:** Fingerprinting control devices and determining possible vulnerable services.
- **Known Flaw Testing:** Check for well-known flaws.
- **Resource Starvation Testing:** Check what happens if bombarded with traffic or requests.
- **Specification Testing:** Detecting boundary values and flaws based on specifications.
- **Fuzz Testing:** Directed pseudo-randomly created data sets to detect unexpected behaviour.

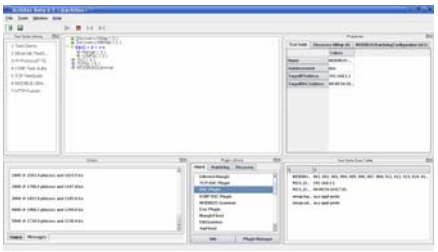
Too Many Tools

- In 2001 BCIT tried to do this for a major oil company:
  - Needed 30 - 40 different tools to test a device.
  - Most are command line based with complex syntax.
  - Difficult to coordinate and report results.

Achilles Vulnerability Test Platform

- GUI platform to coordinate multiple testing tools (open-source or custom).
- Each security tool is a “plug-in”.
- Parameter files coordinate options, execution and reporting.
- ‘Watchdogs’ check device health during tests.

Achilles Demo



Typical Test Results

- Testing against three major brands of PLC, two ESD and two DCS has uncovered:
  - 9 critical vulnerabilities;
  - 42 warning notices;
  - 7 informational notices.
- Two of these vulnerabilities hard-faulted the PLC application logic.

Into the Future: Security Standards for Industry

- Create and promote control system security best practises and standards.
- Develop recommendations for securing vulnerable control systems.
- Get security QA standards developed.

Wurldtech analytics

BCIT British Columbia Institute of Technology A Polytechnic Institution

www.tc.bcit.ca