

# Understanding Vulnerabilities in SCADA and Control Systems

APPLIED RESEARCH AT BCIT



## Understanding Vulnerabilities in SCADA and Control Systems

Eric Byres, P. Eng.  
British Columbia Institute of Technology  
eric\_byres@bcit.ca



[www.tc.bcit.ca](http://www.tc.bcit.ca)




## Why Study Vulnerabilities in SCADA and Control Protocols?

- Windows and Linux vulnerabilities are generally well known and understood.
- SCADA/Control vulnerabilities are not understood.
- Need to discover these flaws before:
  - Critical devices containing them are deployed in the field (where they are expensive to fix).
  - The hackers discover them and begin to exploit them.

7

# Understanding Vulnerabilities in SCADA and Control Systems



## Why Study Vulnerabilities in SCADA and Control Protocols?

- Once we understand our vulnerabilities we can either:
  - Fix the flaw.
  - Design mitigation strategies to reduce their impact.
- Until we know our weaknesses we can do little to protect ourselves.

8

APPLIED RESEARCH AT BCIT




## Understanding The Origins of Vulnerabilities



[www.tc.bcit.ca](http://www.tc.bcit.ca)


# Understanding Vulnerabilities in SCADA and Control Systems



## Why Vulnerabilities Exist?

- SCADA and control protocols were designed when the control network was an isolated system.
- Design assumed a trusted environment.
- The closed trust model no longer applies, yet the protocols haven't changed.

10




## Why Vulnerabilities Exist?

- Lots of market pressure to offer a number of communications options.
- Typically based on multiple commercial or industrial specifications:
  - Ethernet, IP, TCP, UDP, HTTP, SNMP, etc.
  - MODBUS, ProfiNet, EtherNET/IP, etc.
- Supporting many specs results in very complex systems.

11


# Understanding Vulnerabilities in SCADA and Control Systems



## Why Vulnerabilities Exist?

- Modern controllers are typically based on a commercially available embedded systems platforms that are well known to some hackers.
- Primary focus of device is control functionality.
- CPU and memory limitations limit security options.
- Products are shipped and deployed without knowledge of possible flaws.

12




## Classes of Vulnerabilities

- Vulnerabilities can be divided into two general classes:
  - Inherent Protocol Vulnerabilities
  - Implementation Vulnerabilities

13


# Understanding Vulnerabilities in SCADA and Control Systems


APPLIED RESEARCH AT BCIT



RESEARCH • DEVELOPMENT • SOLUTIONS

## Inherent Protocol Vulnerabilities

  
BRITISH COLUMBIA  
INSTITUTE OF TECHNOLOGY  
A POLYTECHNIC INSTITUTION  
[www.tc.bcit.ca](http://www.tc.bcit.ca)




RESEARCH • DEVELOPMENT • SOLUTIONS

## What are Inherent Protocol Vulnerabilities?

- Security weaknesses that are built into the protocol specification.
- Not the result of programming or design errors.
- Likely to effect an entire class of devices on the market.

15


# Understanding Vulnerabilities in SCADA and Control Systems



## Example: Lack of Command Authentication in SCADA Protocols

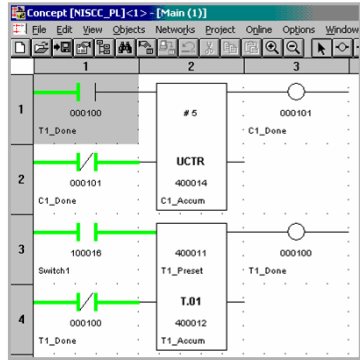
- Most control devices require no authentication from a device issuing a command proving it is allowed to do so.
- Blindly accept any command from any device.

16




## Demo: Attacking PLCs with Standard Tools

- A sample program was loaded onto the PLC unit to flash the lights in sequence (the legitimate program).
- This program simulates any program controlling devices on a SCADA or control network, such as a pipeline pumping station.



17


# Understanding Vulnerabilities in SCADA and Control Systems



RESEARCH • DEVELOPMENT • SOLUTIONS

## Demo: Using SuperScan to Attack a PLC

- Free Windows tool from FoundStone.
- One of the more useful Win32 scanners available.
- No where near the sophistication as the Linux utility nmap.
- Can be modified to attack PLCs!



SuperScan 4.0  
Scan | Host and Service Discovery | Scan Options | Tools | Windows Emu

Hostname/IP: 142.232.22.160 Start IP: 142.232.22.160  
Start IP: 142.232.22.160 End IP: 142.232.22.160  
Read IPs from file

Live hosts this batch: 1  
142.232.22.160  
Hostname: [Unknown]  
TCP ports (3): 21,80,802

Total live hosts discovered: 1  
Total open TCP ports: 3  
Total open UDP ports: 0

Performing banner grabs...  
TCP banner grabbing (0 ports)  
UDP banner grabbing (0 ports)  
Reporting scan results...  
----- Scan done -----  
Discovery scan finished: 01/22/04 13:44:56

View HTML Results

00:41 Saved log file Live: 1 TCP open: 3 UDP

18

APPLIED RESEARCH AT BCIT



RESEARCH • DEVELOPMENT • SOLUTIONS

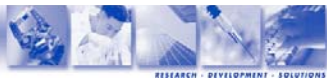
## Implementation Vulnerabilities



BCIT  
BRITISH COLUMBIA  
INSTITUTE OF TECHNOLOGY  
A POLYTECHNIC INSTITUTION

[www.tc.bcit.ca](http://www.tc.bcit.ca)

# Understanding Vulnerabilities in SCADA and Control Systems



## What are Implementation Vulnerabilities?

- Security weaknesses resulting from errors in the product development (design flaws).
- Can be single release or across entire product lines.
- In the IT world, these are what hackers or worms typically like to exploit.

20



## Some Statistics

- Commercial average defect density is 0.6 defects per thousand lines of code (KLOC).
- At least 100 KLOC in a modern embedded controller.
- 8% of defects are exploitable.
- 5 exploitable defects per device.

21

# Understanding Vulnerabilities in SCADA and Control Systems



## Where Do Implementation Vulnerabilities Come From?

- Classic software mistakes are also made on embedded systems:
  - Input validation
  - Format strings
  - Buffer overflows
  - Cross Site Scripting
- Limited resources lead to removal of sanity checks.

22



## Where Do Implementation Vulnerabilities Come From?

- Undocumented functionality:
  - Developer backdoors;
  - Auto-something features;
  - Legacy functions.
- Uncontrolled increase of complexity:
  - New subsystems;
  - New access methods with inconsistent restrictions.
- Ignored standards.

23

# Understanding Vulnerabilities in SCADA and Control Systems



## Example SCADA and PLC Implementation Vulnerabilities

- SCADA systems were designed for performance, not security:
  - Certain PLCs fail while being scanned, indicating a serious TCP/IP implementation issue;
  - Many PLCs have legacy commands still deployed that are very dangerous;
  - Most embedded HTTP daemons are vulnerable.

24



## A Published Vulnerability

- **ISS Security Advisory –  
ICMP Redirects Against Embedded Controllers**  
\*\*\*\*\* WARNING \*\*\*\*\* This advisory pertains to an indeterminant class of networked embedded controllers found in a wide variety of automation equipment ...  
**Synopsis:** The OS-9 operating system, popular for use in intelligent embedded controllers or PLCs (Programmed Logic Controllers), may have network protocol stacks which are vulnerable to certain classes of ICMP Redirect attacks. Vulnerable controllers are prone to hang or shutdown shortly after receiving the attacking packets.

25

# Understanding Vulnerabilities in SCADA and Control Systems


APPLIED RESEARCH AT BCIT



RESEARCH • DEVELOPMENT • SOLUTIONS

## Sniffing out the Flaws

  
BRITISH COLUMBIA  
INSTITUTE OF TECHNOLOGY  
A POLYTECHNIC INSTITUTION  
[www.tc.bcit.ca](http://www.tc.bcit.ca)




RESEARCH • DEVELOPMENT • SOLUTIONS

## Finding the Flaws Before the Bad Guys

- Inherent protocol vulnerabilities can be discovered by:
  - Rigorous analysis of specifications.
- Implementation vulnerabilities can be discovered by:
  - Analysis of device source code;
  - In-depth device testing.

27

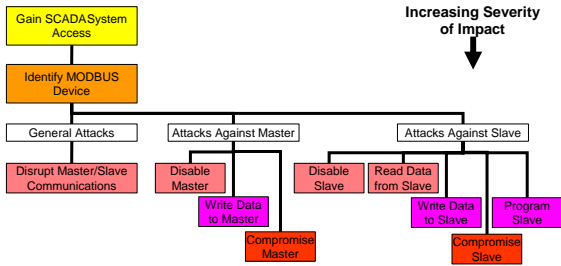
# Understanding Vulnerabilities in SCADA and Control Systems



RESEARCH · DEVELOPMENT · SOLUTIONS


## Protocol Vulnerability Analysis Methodology

- Develop a methodology to analyze SCADA protocols to determine the potential vulnerabilities inherent in the specification and likely implementation issues.



Increasing Severity of Impact

```
graph TD; A[Gain SCADA System Access] --> B[Identify MODBUS Device]; B --> C[General Attacks]; B --> D[Attacks Against Master]; B --> E[Attacks Against Slave]; C --> C1[Disrupt Master/Slave Communications]; D --> D1[Disable Master]; D --> D2[Write Data to Master]; D2 --> D2a[Compromise Master]; E --> E1[Disable Slave]; E --> E2[Read Data from Slave]; E --> E3[Write Data to Slave]; E3 --> E3a[Compromise Slave]; E --> E4[Program Slave];
```




RESEARCH · DEVELOPMENT · SOLUTIONS

## Attack Tree Modeling

- A methodology is needed to:
  - Organize attack possibilities,
  - Understand their inter-relationships
  - Rank them according to risk.
- “*Attack Tree Modeling*” was selected.

29


# Understanding Vulnerabilities in SCADA and Control Systems



## Attack Tree Modeling

- Defines a series of attacker goals.
- Determines possible means to achieve that goal.
- Assigns a risk indicator to each possible means of attack.
- Highlights the “weak links” in the system.

30




## Attack Tree Modeling Example

- **Goal: Gain unauthorized physical access to building**  
OR
  1. Unlock door with key
  2. Pick lock
  3. Break window
  4. Follow authorized individual into building

31


# Understanding Vulnerabilities in SCADA and Control Systems



## Attack Tree Modeling Example

- **Goal: Gain unauthorized physical access to building**
  - OR
    - 1. Unlock door with key
      - OR 1.1. Steal Key
      - 1.2. Social Engineering
        - OR 1.2.1. Borrow key
        - 1.2.2. Convince locksmith to unlock door
    - 2. Pick lock
    - 3. Break window
    - 4. Follow authorized individual into building
      - AND 4.1 Wear appropriate clothing for the location
        - OR 4.2.1. Act like you belong and follow someone else
        - 4.2.2. Befriend someone authorized outside building
        - 4.2.3. Appear in need of assistance (e.g. carry a large box)

32




## Assigning Risk

- Risk is influenced using a number of interrelated indicators including:
  - Technical Difficulty
  - Probability of Apprehension
  - Cost of Attack
  - Likelihood of Attack Success
  - Site Conditions
  - Installed Countermeasures

33

# Understanding Vulnerabilities in SCADA and Control Systems

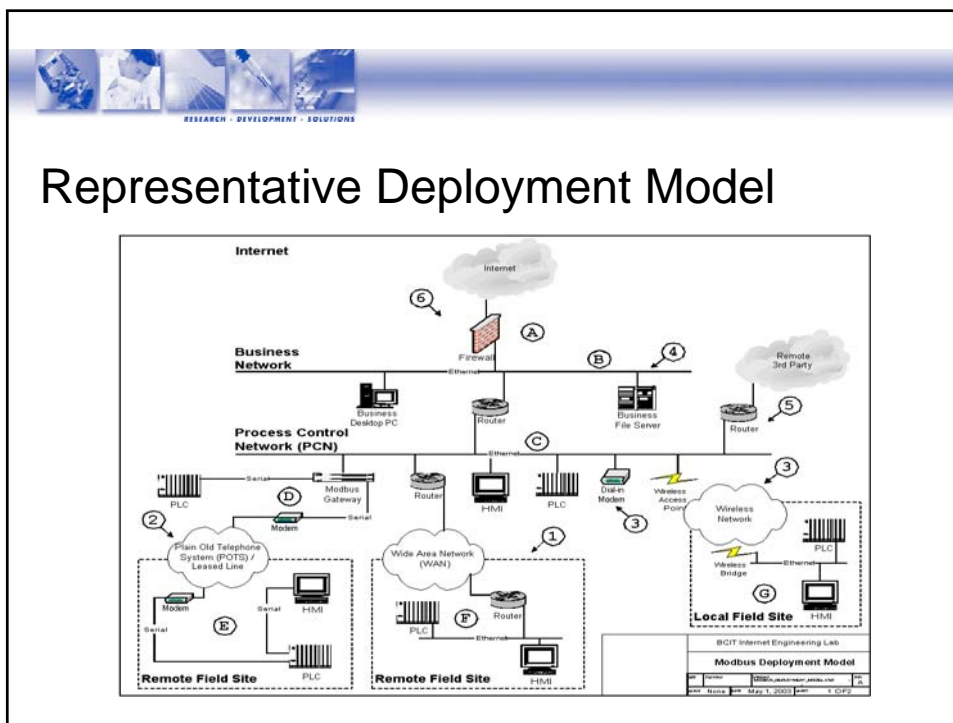


RESEARCH · DEVELOPMENT · SOLUTIONS


## Assigning Risk

- For cyber attacks technical difficulty of an attack is the most critical indicator of possible attack success.
- Four point scale used:
  - **Trivial:** Little technical skill required
  - **Moderate:** Average cyber hacking skills required
  - **Difficult:** Demands a high degree of technical expertise
  - **Unlikely:** Beyond known capability of today's hackers

34



# Understanding Vulnerabilities in SCADA and Control Systems

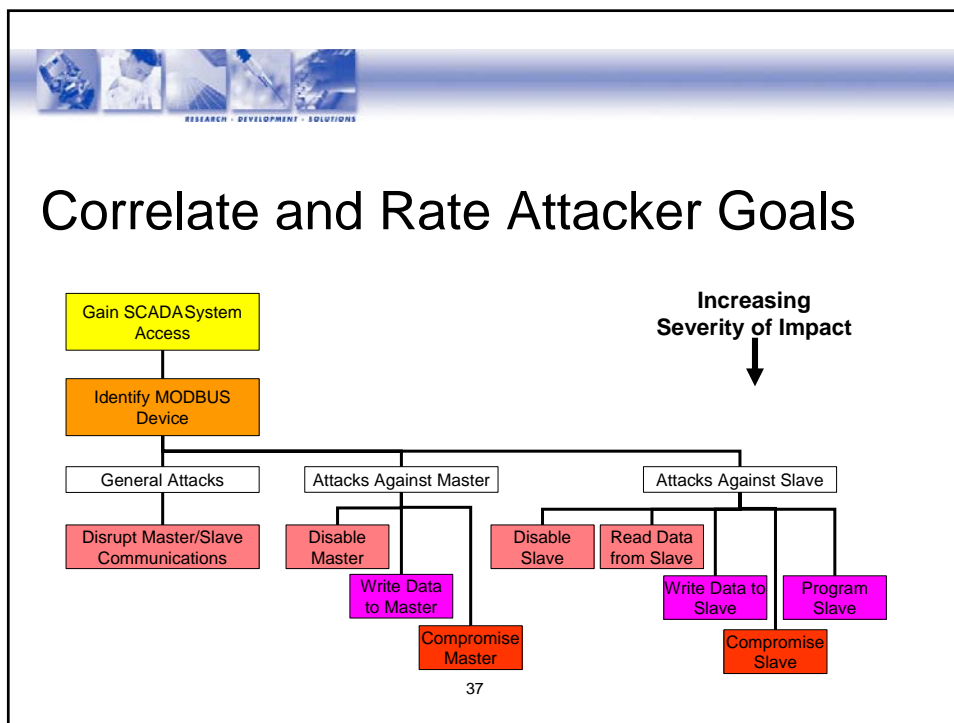


## Possible Attacker Goals


■ Determined 11 possible attacker goals:

1. Gain SCADA System Access
2. Identify Modbus Device
3. Disrupt Master/Slave Comms
4. Read Data from Slave
5. Write Data to Slave
6. Disable Slave
7. Program Slave
8. Compromise Slave
9. Write Data to Master
10. Disable Master
11. Compromise Master

36



# Understanding Vulnerabilities in SCADA and Control Systems




## Attack: Identify SCADA Device

OR

1. Social Engineering (e.g. pretend to be PLC manufacture's service engineer) 2
2. TCP/UDP Port Scan for Port 502 2
  - AND
  - 2.1. Gain local PCN network access (non-blind) 2
  - 2.2. Deploy TCP/UDP scanning tool 1
3. MODBUS Message Scan (only against slave) 2
  - AND
  - 3.1. Gain access to remote site or SCADA transmission system 2
    - 3.1.1. Deploy MODBUS Message Scanning Tool 2
    - 3.1.2. Gain access to remote site or SCADA transmission system 2
    - 3.1.3. Install packet capture util. 2
  - 3.2. Sniff via intercepted SCADA media 2
    - AND
    - 3.2.1. Gain access to SCADA link media 2
    - 3.2.2. Install protocol capture tool 1

38



## Summarize Attack Characteristics

Attacker Goal	Technical Difficulty	Severity of Impact	Prob. of Detection	Underlying Critical Vulnerabilities	Comments
Gain SCADA System Access	1-3	Very Low	Low	<ul style="list-style-type: none"> <li>• Wireless PCN</li> <li>• 3<sup>rd</sup> party access</li> <li>• Remote field sites</li> <li>• SCADA transmission media</li> </ul>	<ul style="list-style-type: none"> <li>• Critical precursor for all other attack goals</li> <li>• Difficulty highly dependant on point of access and security measures in place</li> </ul>
Identify MODBUS Device	2	Very Low	Low	<ul style="list-style-type: none"> <li>• Lack of Confidentiality</li> </ul>	<ul style="list-style-type: none"> <li>• Critical precursor for other goals</li> </ul>
Disrupt Master-Slave Communications	2	Moderate	High	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> <li>• Simplistic Framing Tech.</li> </ul>	
Disable Slave	3	Moderate	High	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> <li>• Simplistic Framing Tech.</li> </ul>	
Read Data from Slave	2	Moderate	Very Low	<ul style="list-style-type: none"> <li>• Lack of Confidentiality</li> <li>• Lack of Authentication</li> </ul>	
Write Data to Slave	2	High	Very Low	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> <li>• Lack of Integrity</li> </ul>	
Program Slave	2	High	Low	<ul style="list-style-type: none"> <li>• Possible Lack of Authentication</li> <li>• Lack of Session Structure</li> <li>• Lack of Integrity</li> </ul>	
Compromise Slave	3	Very High	Low	<ul style="list-style-type: none"> <li>• Lack of Integrity</li> <li>• Possible Lack of Authentication</li> </ul>	
Disable Master	2	Moderate	High	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> </ul>	
Write Data to Master	3	High	Low	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> </ul>	
Compromise Master	2	Extreme	Low	<ul style="list-style-type: none"> <li>• Lack of Authentication</li> <li>• Lack of Session Structure</li> </ul>	<ul style="list-style-type: none"> <li>• Very useful precursor to other attack goals</li> </ul>

39

# Understanding Vulnerabilities in SCADA and Control Systems



## Conclusions - Lack of Common Security Mechanisms

- **Authentication** – There is no authentication evident in most SCADA protocols. If you can reach the device you can control it.
- **Confidentiality** - SCADA protocols are transmitted in clear text across transmission media.
- **Integrity** - No integrity checks built into most protocols - they depend on lower-layer protocols to preserve integrity.

40



## Conclusions - Lack of Robustness

- The mapping of serial SCADA protocols into TCP/IP has exposed a number of serious robustness issues:
  - Simplistic Framing Technique
  - Lack of Session Structure
  - Lack of Command & Confirm
  - Numerous Legacy Commands
- These make attacks very simple.

41

# Understanding Vulnerabilities in SCADA and Control Systems



## Next Steps for SCADA Vulnerability Research

- Additional high level SCADA Analysis, particularly attacks against masters.
- Work with standards orgs to improve specification.
- Find secure method for dissemination of SCADA Security Vulnerability Information.
- Develop recommendations and best practises for securing currently flawed SCADA devices.

42