

Creating a SCADA-Aware Distributed Firewall

APPLIED RESEARCH AT BCIT



Creating a SCADA-Aware Distributed Firewall

Eric Byres, John Karsch, Joel Carter,
Darren Lissimore and Khai Lee

British Columbia Institute of Technology
eric_byres@bcit.ca



Waiting for the Attack?

- Most attacks against the business information systems exploit vulnerabilities in the communications protocols and their implementations.
- SCADA protocols have similar vulnerabilities.
- It is only a matter of time before network hackers begin to take advantage of these flaws to attack SCADA systems.

2



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.

3



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 entire classes of devices on the market.

4



What are Implementation Vulnerabilities?

- Security weaknesses resulting from errors in the product development (design flaws).
- Can be single release or across entire product lines.

5



Where Do Vulnerabilities Come From?

- Undocumented functionality:
 - Developer backdoors;
 - Auto-something features;
 - Legacy functions.
- Ignored standards.

6



Where Do Vulnerabilities Come From?

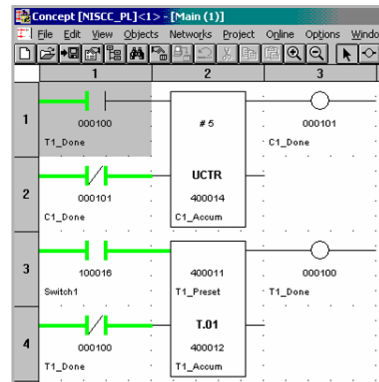
- Classic IT programming mistakes are also made on control systems software:
 - Input validation
 - Format strings
 - Buffer overflows
- Limited resources in small devices lead to removal of sanity checks.

7



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 network, such as oil pipeline.



8



Demo: Using SuperScan to Attack a PLC Protocol

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



9



Some SCADA/PLC Vulnerabilities to Worry About...

- Known malformed packets that crash PLCs.
- Insecure HTTP or SNMP services you don't want but can't close down.
- Valid commands you don't want sent to your PLC under normal operations (like firmware upgrade).
- Lack of authentication on SCADA/PLC protocols.
- Lack of encryption on SCADA/PLC systems.

10

APPLIED RESEARCH AT BCIT



Plugging the Holes



www.tc.bcit.ca



Dealing with Control System Vulnerabilities

- Once we discover vulnerabilities we can either:
 - Fix the flaw.
 - Design mitigation strategies to reduce their impact.
- The best solution is to fix the vulnerability.
- If you have legacy systems (or the vendor isn't cooperative) fixing might not be possible.
- Need to do something to reduce risk or impact.

12



The Solution in the IT World

- If your desktop has flaws you add security software:
 - Patches
 - Personal Firewalls (like Blacklce or ZoneAlarm)
 - Anti-Virus Software
 - Encryption (VPN Client or PGP)
- But you can't add software to your PLC or RTU...

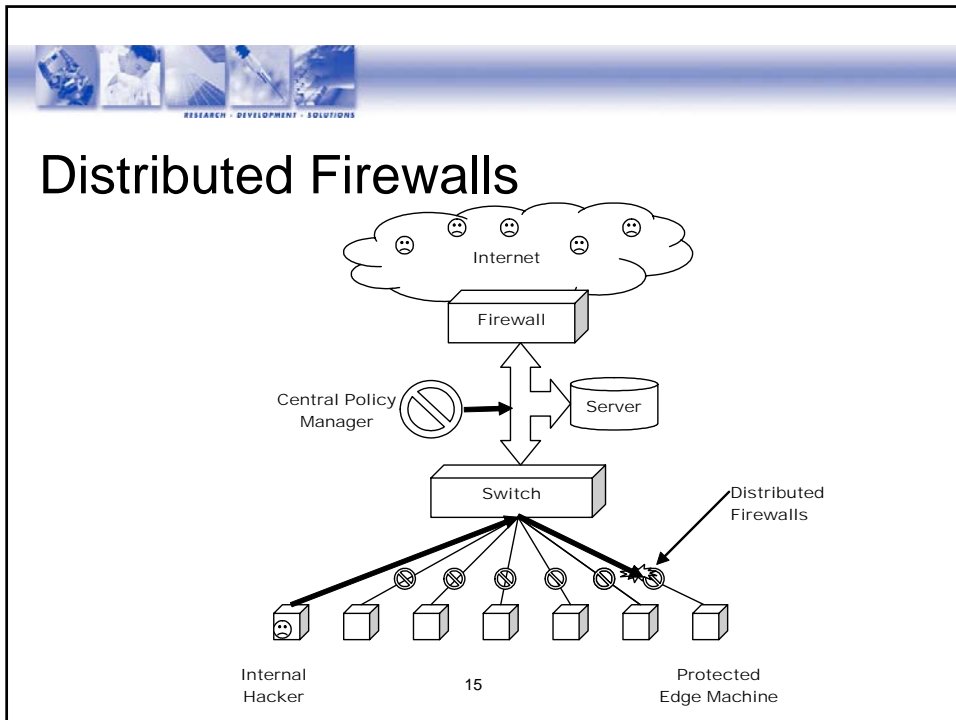
13



Distributed Firewalls

- Add hardware instead - a micro-firewall designed to be placed in front of individual PLC devices.
- Protects the device from any unauthorized contact, probing, commands, etc.

14



Why Not Use a COTS Personal Firewall?

- Not industrially packaged or hardened.
- Doesn't understand controls protocols so it can't selectively filter commands.
- Not extensible to SCADA requirements (AGA-12?).
- Not easy for maintenance staff to configure.
- Difficult to manage hundreds of personal firewalls from a central administration point.



What is Required in a Industrial Micro-Firewall

- **Form Factor and Robustness** – the security device must fit in a standard-sized industrial encasement.
- **Functionality** – the security device must understand the SCADA protocols, and act as a barrier to prevent all unauthorized network access to the PLC devices while in no way obstructing valid PLC control commands.

17



What is Required in a Industrial Micro-Firewall

- **Security** – the security device must provide a high level of encryption for all communications, and present no new security issues.
- **Extensible** – the security device should act as a platform where any type of security software may be deployed – i.e. intrusion detection, network statistics gathering, encryption, etc.

18



What is Required in a Industrial Micro-Firewall?

- **Deployment** – must support a “zero configuration deployment model” – i.e. a service technician need do no more than simply plug it in.
- **Administration** – the security device must be able to be configured, monitored and administrated from a remote location.
- **Global Management** - Should not require individual logins to check device status.

19



What is Required in a Industrial Micro-Firewall?

- Anything else?

20

APPLIED RESEARCH AT BCIT



Easy to Ask for, But How Do We Do All That?



Form Factor and Robustness

- Use single board computer (SBC) that will mount into standard PLC Modules.
- Allow either mounting on DIN-Rails or in PLC chassis.



Functionality –Understand SCADA Protocols and Filter Intelligently

- Use MODBUS PLC command filter Firewall developed by Matt Franz at Cisco CIAG.
- Allows user to specify what MODBUS functions are allowable.
- Example: Drop packet whenever the function code is 16 (Write Multiple Registers).

```
# iptables -A INPUT -p tcp -m modbus --funccode 16 --allowtcp 1 -j DROP
```

23



Extensible to allow Any Security Software to be Deployed

- A “module” can be any software that can run under Linux:
 - Intrusion detection,
 - network statistics gathering,
 - encryption,
 - virus scanner, etc.
- Security applications and policy SECURLY pushed out from a central security mgmt server.

24



Secure Communications Between Management and Firewall

- All communications encrypted using SSL.
- Authentication using client and server certificate pairs.
- Certificates can be upgraded in the F/W from the management server.
- Firewall is very stealthy - has no IP address and doesn't respond to port scans.

25



Zero Configuration Deployment Model

- Layer-2 firewall that requires no IP address.
- Doesn't require address/gateway changes in PLC.
- Learns IP address of the PLC to be protected.
- Management server automatically pushes appropriate configuration to firewall.
- Service technician need do no more than simply plug the firewall in.

26



Administration and Global Management

- Firewall reports with encrypted heartbeat (like a fieldbus) to report status and events.
- One management station can monitor and manage thousands of firewalls, deployed in remote locations.

27



Monitoring the Firewall's Health

Node ID	Firewall	IDS	Heart Beat
AMD2			
Time Stamps	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004
ER			
Time Stamps	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004
SK1	MIA	MIA	MIA
Time Stamps	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004
test			
Time Stamps	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004	Fri Oct 1 13:45:39 2004



Next Steps

- Locate industry partner to move forward.
- Improve GUI to be more industrial-engineer friendly.
- Secure web front end for management of server.
- Add Radius for authentication.
- Add more protocols (Ethernet/IP, ProfiNet)
- Add more extensions (AGA-12 module?)

29