

SCADA and Process Control System Security

Presented by Patrick C Miller, CISSP SSCP IAM
IEEE Power Engineering Society – Portland, OR
January 21st, 2004

BREAKWATER
BREAKWATER
SAFE HARBOR FOR YOUR BUSINESS

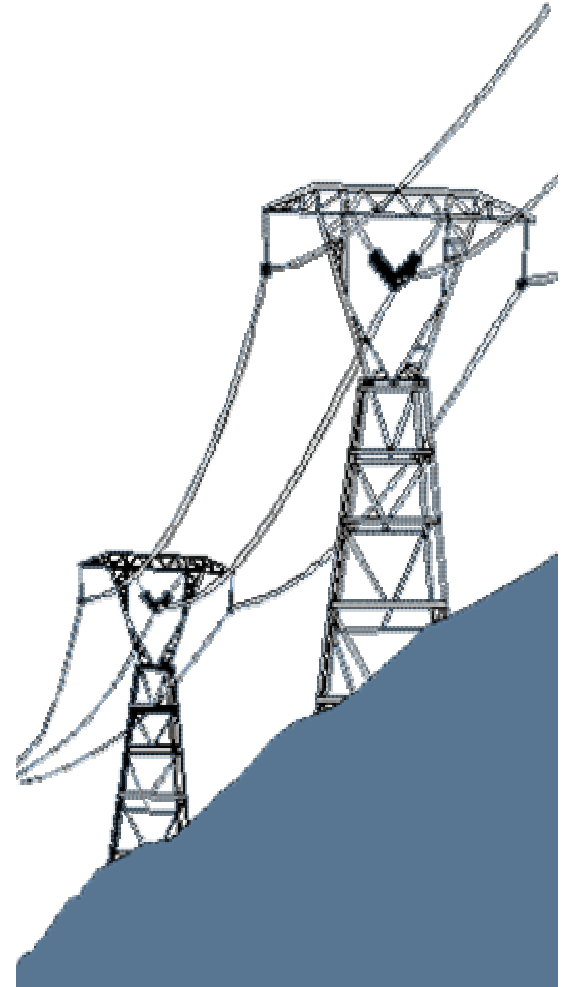


Information security

is a dynamic, constantly evolving, living system. Breakwater keeps ahead of the curve and anticipates threats to provide clients with highly responsive protection.

Presentation Overview

- **Breakwater Security Associates Profile**
- **Current and future SCADA Security**
- **Relevant industry regulations**
- **Secure Process Control System architectures and models**
- **Partnerships and participation**





Breakwater Security Associates

Information Security and Risk Management Services Firm since 1996.

A few of the things BSA does well...

- **Security Program Development**
 - Risk, Security and Vulnerability Assessments
 - Regulatory Compliance Gap Analysis
 - Policy Development and Auditing
 - Security Strategy

- **Managed Security Services**
 - Device Management
 - Event Correlation (Security Risk Management)
 - Monitoring



SCADA Security – History...

- Legacy devices/systems were built for reliability and performance, not security
- Terrorism was not a consideration
- No Internet...
 - No Internet connectivity to SCADA
 - Less connectivity, in-general
 - No Internet information access
- Obscure systems with obscure documentation
- Minimal interoperability with proprietary protocols
- Large degree of software customization
- SCADA hacks were rare, if ever reported



SCADA Security – Today...

- Devices/systems are still built for reliability and [arguably] performance, not security
- Terrorism *is* a consideration
- The Internet...
 - SCADA networks **are** connected
 - Large amounts of information very easy to obtain in a short amount of time
- The “Obscurity Factor” is no longer a reality
- More interoperable with public protocols, but IT security still won’t work entirely
- Less software customization necessary, but still too much; patching is difficult
- SCADA hacks are reported and becoming more regular



SCADA Security – Today (cont)...

- Coordinated Physical and Cyber attack still considered to be greatest threat...
 - Confusion is not to be underestimated (August 14th)
 - Resource availability and backup
 - Critical spares
 - Interconnectivity points
- Observed Cyber-attacks...
 - External (remote) console access, usually via modem
 - High/low trigger values; Breakers/valves modified
 - Network sniffing and “replay” attacks
 - Even switched environments aren’t safe anymore (ettercap)
 - Christmas Tree packets



SCADA Security – Tomorrow...

- Devices/systems will be built with security technologies; expect growing pains
- Terrorism will probably still exist
- The Internet (or similar) will probably still exist
 - SCADA will be “air-gapped” by regulation
 - Bandwidth will increase exponentially
 - All information will be near-instantaneous access
- Obscurity will be extraordinarily rare
- High degree of interoperability and security
- Minimal software customization; easy patching
- SCADA hacks could become frequent

Regulations and Directives

- **FERC Standard Market Design (SMD)**
- **NERC 1200 Urgent Action Cyber Security Standard**
- **NERC Security Standard**
- **DHS Critical Infrastructure Info (CII) Directive**





FERC SMD

- FERC Standard Market Design (SMD)
 - Federal entity with Federal process; slow
 - Plan is very large, complex and hard to push
 - Entire document was over 800 pages
 - Security language located within Appendix G
 - Politics are involved; important opposition
 - Lost steam and security focus was redirected to NERC 1200...
 - Gaining momentum again!
 - Appendix G is gone, now referencing the NERC 1200 standard in Section M



NERC 1200 Urgent Action Std

- NERC 1200 Urgent Action Cyber Security Standard
 - Started as Appendix G of the SMD
 - Had to set the “low bar”
 - Really attempting to get attention and assess state
 - No *real* punishment other than reprimanding letter
 - Requires extensive documentation
 - Requires classification of all critical systems
 - Process Control Systems are explicitly excluded
 - EMS/DCS and other related systems included
 - Typically 1, but maximum 2 year life span



NERC Security Standard

- NERC Security Standard
 - Permanently replaces the NERC 1200 Urgent Action Cyber Security Standard
 - Should be more refined with better procedures
 - “Higher bar” this time around...
 - Sanctions or punishments are still unclear
 - Still very information/documentation-centric
 - Process Control Systems included

***For more info, see Joe Weiss at the NW NERC 1200 Forum
Friday at 1:00PM on Jan 23rd - WTC2 (PGE), Portland, OR***



DHS CII Directive

- DHS Critical Infrastructure Info (CII) Directive
 - Easy to remember title: *6 CFR, Part 29*
 - Offers some protection from FOIA; get legal advice
 - Defines Critical Infrastructure Information (CII)
 - Requires certain protection of CII
 - Still in draft; Notice of Public Rule-Making (NOPR)



Why all the new regulations?

- 9-11 and terrorism/disaster resiliency
- August 14th Blackout
- Corporate accountability scandals...
- GAO Testimony; “Critical Infrastructure Protection – Challenges in Securing Control Systems” *gao-04-140t*
- Results from assessments indicate a clear lack of security in many areas
 - RAM-D; RAM-T
 - DHS OEA VAP (was DOE OEA VAP)
 - ISO/IEC
 - NIST
 - Independent consulting firms



What can be done?

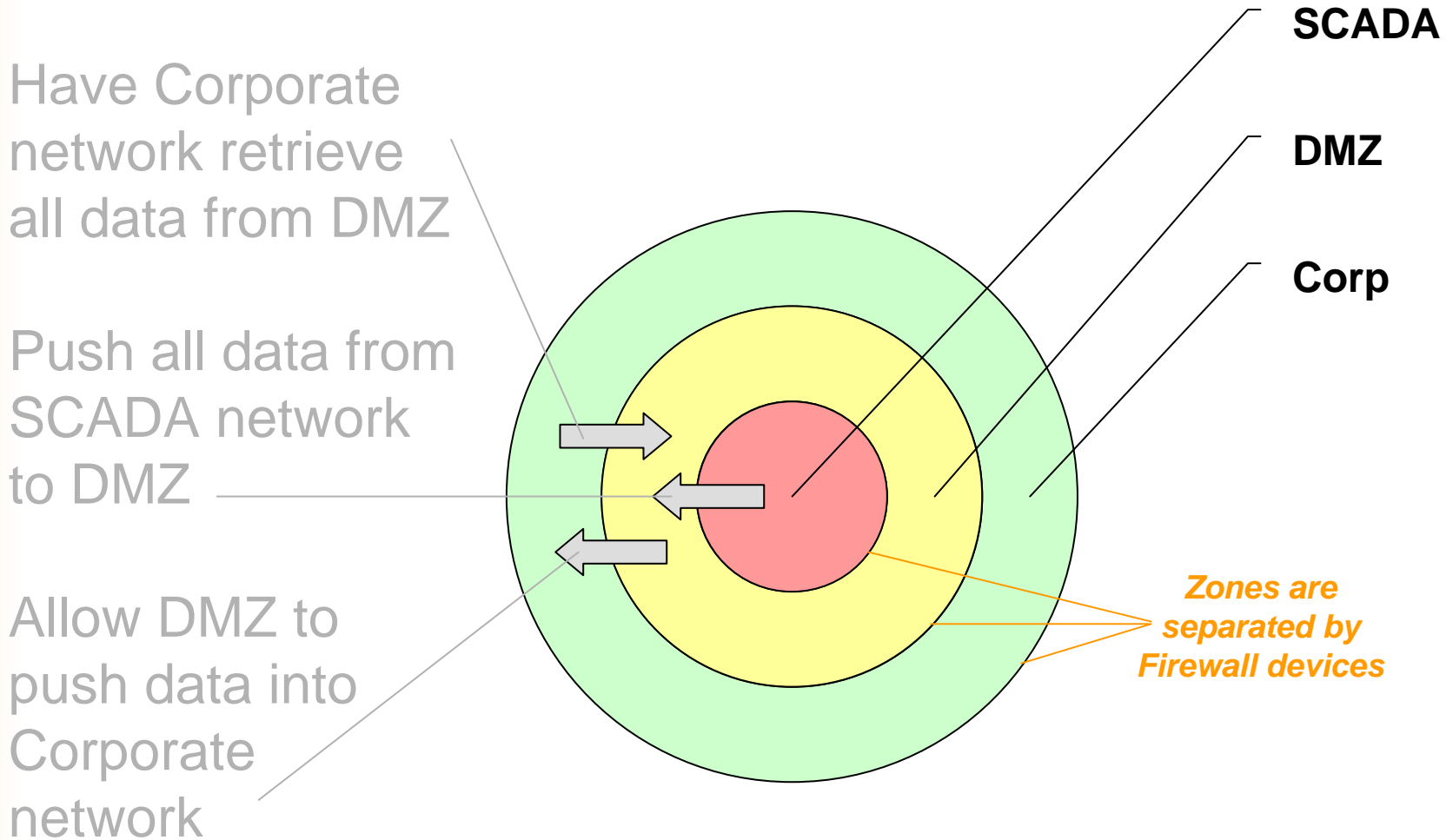
- Security can be implemented now, with low impact
- Don't rush out to buy new equipment; *re-architect*
- **Get management attention**
- Assess and report the situation; increase awareness
- Get the necessary resources to fix the holes
 - Budget/Strategy
 - Hardware
 - Software
 - Staff
 - Training and Consulting
- Start one step at a time...

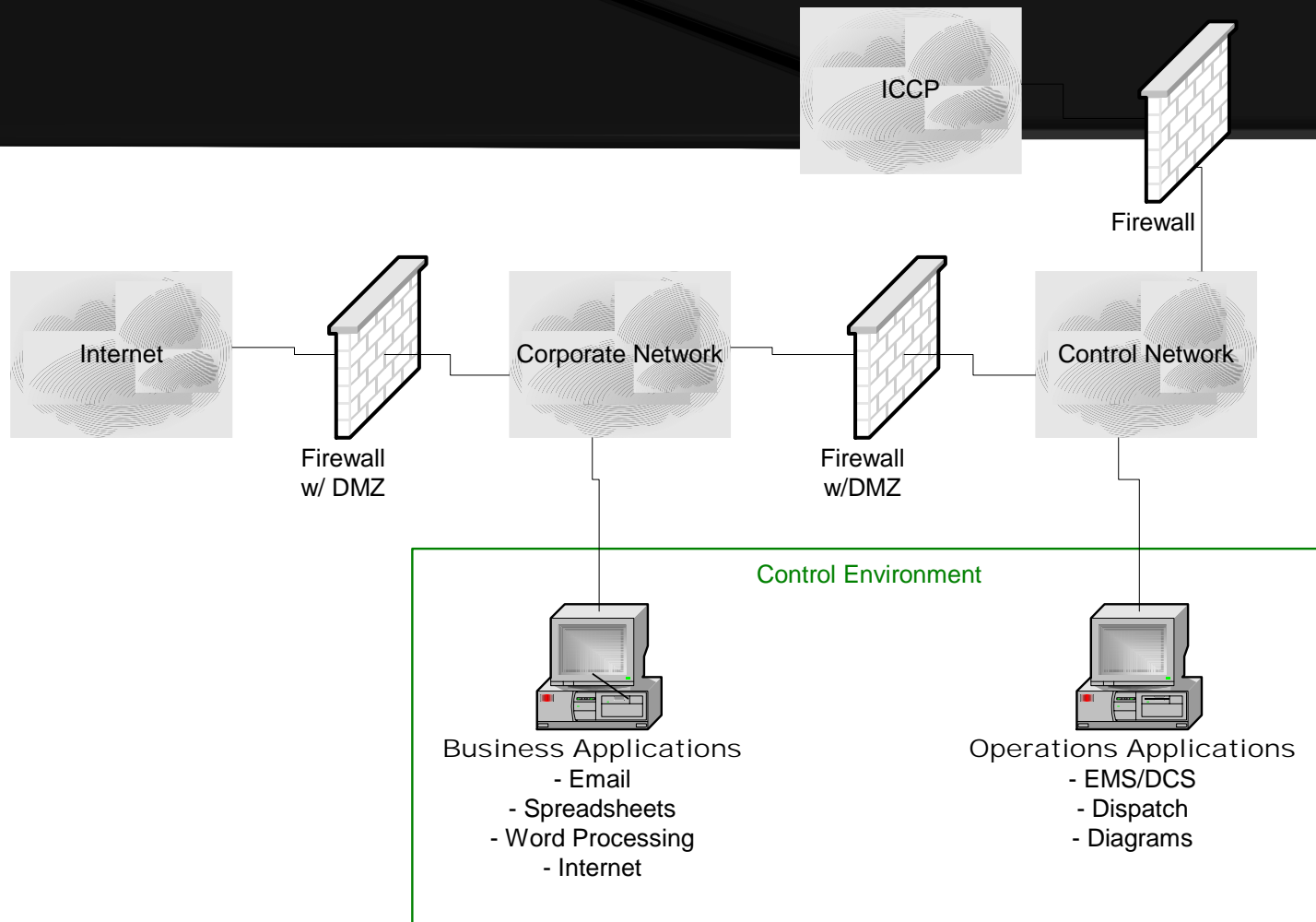


One simple rule...

- **Keep the networks separate and private**
 - Never connect control networks to the Internet
 - Don't mix business and engineering; keep business traffic away from the process control network
 - Use strong control devices such as firewalls at **all** ingress/egress points
 - Consider employing security technology at gateway
 - Intrusion Detection Systems (IDS); Host and/or Network
 - Integrity Assurance solutions
 - Event Correlation
 - Use a DMZ model to “publish” all data to the business network
 - Use VPNs over RF and “public/private” networks

SCADA Network Model







General SCADA Security

- Passwords
 - First of all, having one would be a start!
 - Stronger passwords
 - Password change cycles
- Well-refined account management procedures
 - The “Insider Threat”
- No insecure services with credentials “on the wire”
 - Move away from telnet, ftp, tftp, VNC, etc...
 - Move toward VPN, ssh, sftp, scp, MSTTS, etc...
- Modems
 - Dial-back
 - Hardware/software keys
- Security Awareness and Training
- Pressure your vendors for more secure products



SCADA Security “Don’ts”

- Don’t run vulnerability scanners or other network mapping software in control networks without extreme caution and extraordinary care
- Don’t trust ICCP (and other protocols) yet...
 - Get involved w/ IEC TC57 WG15
- Don’t trust wireless (802.11x) or RF yet...
- Don’t rely on “security through obscurity”
- Don’t connect anything to the Internet
- Don’t connect control networks and business networks unless through a firewall w/ a DMZ



Partnering with IT

Partnering with IT can have long-term benefits...

- Better and faster support of IT systems and network infrastructure; even dedicated staff
- Access to diverse development staff
- Access to stronger procurement channels
- Increased profitability to the organization as a whole through a better understanding of control data
- Increased control over all corporate information
- Increased visibility to organization = more funding
- Access to shared-budget projects



Participate in the effort...

- ISA Conferences
- UTC SCADA Conferences
- KEMA/PCSCS SCADA Security Conferences
- CBI Electric Industry Security Conferences
- IEC TC57 WG15 and WG16
- Process Control Systems Security Requirements Forum (PCSSRF)
- INEEL SCADA Test Bed
- NERC Security Workshops
- NERC CIPAG and CIPIS
- NERC PCSTF (PCS Task Force)



Summary

- SCADA is now considered “insecure” by *many*
- SCADA is connected to the Internet, wireless and insecure RF
- Traditional IT Security measures may impact SCADA and control environments
- SCADA can be secured, with minimal/no impact
- Start with a secure SCADA architecture
- Never connect control networks to the Internet
- Use remote access security (modems, passwords)
- Classify and document *everything* for Regulations
- Participate in Energy-Industry Security effort



Questions?

Patrick C Miller, CISSP SSCP IAM

Senior Security Consultant;

Energy and Utility Practice Principal

pmiller@breakwatersecurity.com

503.517.3407 (desk)

503.312.0703 (mobile)