IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Vulnerabilities in Power Systems, Critical Infrastructure and Mitigation Techniques

Michael Milvich

IOActive

Overview

- How we do an assessment and penetration tests
- The two types of vulnerabilities we see
- How they compare to each other
- How to mitigate them

Assessment Methodology

- Reconnaissance
  - Discover Public Information
  - Discover Intranet Information
  - Map DMZ Boundaries
- Assessment
  - Inspect Firewall Rules
  - Ascertain Effectiveness of Procedures
  - Understand Points of Interoperability
  - IDS/IPS Deployment
- Penetration Testing
  - Penetrate DMZ Services
  - Engineer Workstations
  - Shared Resources (Citrix cluster, patch server, etc…)
  - Perform Invasive Tests on Development/Test/Training Systems

Two Types of Vulnerabilities

- Typical IT Vulnerabilities
  - Vulnerabilities Common with Corporate Networks
- SCADA Specific Vulnerabilities
  - Targets SCADA Specific Software
  - Targets SCADA Specific Network Configurations

Typical IT Vulnerabilities

- Vulnerabilities
  - Operating System Vulnerabilities
  - Patch Management
  - Password Management
  - Remote Access (VPN, RDesktop, Citrix, etc…)
  - Web Services
  - Databases
  - Network Backup Systems
  - Poor Firewall Configurations
- Characteristics
  - Research for Vulnerabilities
  - Download and Run Existing Tools
  - Limited Need for Custom Exploitation

SCADA Specific Vulnerabilities

- SCADA Specific Threats
  - Historians
  - SCADA Specific Vulnerabilities
  - Fragile Systems
  - Substation Connections
  - Neighbor Communications
  - Dial-Up Communications
  - Backup Site
  - Physical Security
  - Vendor Connections
- Characteristics
  - Some Public Information
  - Custom Exploits Needed
  - Need a Testing Environment

Typical IT vs SCADA Vulnerabilities

	Typical IT	SCADA Specific
Difficulty of Exploitation	Easier, public tools and knowledge.	Harder, generally requires custom tools.
Likelihood of Exploitation	Higher, easier availability of tools.	Lower, needs custom tools.
How we Compromise SCADA Networks	Usually, easier than finding a SCADA specific vulnerability.	Occasionally, when it is not possible through typical IT vulnerabilities.

What to do about Typical IT Vulnerabilities

- End Users
  - Deploy Security Products
    - Firewalls, IDS, Anti-Virus, etc…
  - Patch Systems
  - Use Good Passwords
  - Perform Penetration Tests
    - Use Multiple Companies
    - Perform Yearly Tests
  - Foster IT and SCADA Relationships
  - The same actions you do on the corporate network
- SCADA Vendors
  - Make it easy for end users to follow best practices and apply patches
  - Integrate with IT solutions

What to do about SCADA Vulnerabilities

- End Users
  - Apply patches as vendors release them
  - Encourage and ask for security
  - Deploy SCADA systems securely
  - Isolate Vulnerable Systems
- SCADA Vendors
  - Train developers in secure development
  - Create a Security Culture
  - Perform Security Assessments
  - Patch Vulnerabilities
  - Notify Users of Patches

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Questions?