Critical Infrastructure Security: The Emerging Smart Grid

Cyber Security Lecture 5:
Assurance, Evaluation, and Compliance
Carl Hauser & Adam Hahn
Overview

• Evaluation
  – Common Criteria
  – Security Testing Approaches
  – Software Testing
  – Formal Methods

• Standards and Compliance
  – NERC CIP
    • System Classification
    • Requirements
    • Assessment
Terminology

• Why?
  – Need to ensure system security mechanisms operating as designed

• Assurance
  – “our estimate of the likelihood that a system will fail in a particular way”

• Evaluation
  – “the process of assembling evidence that a system meets, or fails to meet, a prescribed assurance target”
Most security tools are “dual purpose”
Attackers also use these techniques to find & exploit weaknesses
Network Monitoring (Passive)

1) Access physical network (e.g., WiFi)

2) Sniff traffic to collect packets (Wireshark)

Target Network/Systems

Search for useful information
- software banners (products/versions)
- authentication data (users, passwords, etc)
- other sensitive information (email, http traffic)
System/Port Scanning

System Scanning
- search for all systems on a network
- Ping sweep

1) ICMP Echo Req. 1.1.1.1
   ICMP Echo Req. 1.1.1.2
   . . .
   ICMP Echo Req. 1.1.1.254

2) Target Network
   1.1.1.0/24
   If system exists:
   - send “ICMP Echo Response”
   Else
   - send “ICMP Dst. Host Unreachable”

3) ICMP Echo Resp. 1.1.1.1
   ICMP Echo Resp. 1.1.1.2
   . . .
   ICMP Dst. Host Unreachable. 1.1.1.254

4) List of systems on network

Port Scanning
- search system for open ports (services)
- TCP Syn Scan

1) TCP Syn Port 0
   TCP Syn Port 1
   . . .
   TCP Syn Port 65535

2) Target System
   1.1.1.2
   If TCP port listening:
   - send “TCP Syn/Ack”
   Else
   - send “TCP Reset”

3) TCP RST Port 0
   TCP Syn/Ack Port 1
   . . .
   TCP RST Port 65535

4) List of open ports And system properties (e.g., operating system)
Vulnerability Scanning

**Vulnerability Scanner**
- Database of vulnerability indicators, including:
  - Configurations (e.g., TLS)
  - Software versions
  - Vulnerabilities

**Example List of Vulnerabilities:**
- SSL v2
- Apache 2.2
- Shellshock

1) Openssl connect -sslv2 Port 443
2) TCP Connect Port 443
3) Inject Shellshock vuln.

1) Connection Success
2) “Apache 2.2” Banner
3) Shellshock response?
Security Assessment Concerns

- Many of the assessment techniques may cause issues when run on real system
  - Consume network bandwidth
  - Create connections to running services and send disruptive information
- Examples:
  - Ping sweep of SCADA systems in integrated circuits plant caused robotic arm to swing 180 degrees and destroy $50,000 of wafers
  - Security test of natural gas utility caused lockup of SCADA system, shutting down pipeline for 4 hours
- Need non-intrusive security testing methods for online systems

Continuous Monitoring

- Need to frequently monitor the security of systems & networks
  - Many previously discussed tools based on
    - Provide incomplete information
    - Maybe intrusive when used to real networks

- SCAP – Security Content Automation Protocol
  - “suite of specifications that standardize the format and nomenclature by which security software products communicate security content, particularly software flaw and security configuration information”

- Core Technologies
  - OVAL – Open Vulnerability and Assessment Language
    - XML based language to communicate
  - CVE – Common Vulnerabilities and Exposures
  - CVSS – Common Vulnerability Scoring System
  - CPE, CCE, XCCDF

- Major initiative in Federal Govt

Network Policy Review

• Network security policy is enforced by many firewalls and routers
  – Each has its own ruleset and access control list
  – Need to identify potential policy violations, misconfigurations.

• Analysis techniques
  – Offline review of firewall rulesets
  – Online probing of network to infer configurations

• Tools: NetAPT, Firemon
Software Testing
Static vs Dynamic Analysis

• **Static Analysis**
  - Analyzes source code for vulnerabilities without actually executing
  - More “complete” than “sound”
    - Evaluates/analyzes many possible execution paths
    - High “false-positive” rates
  - Tools: Fortify, Covertiy, Splint

• **Dynamic Analysis**
  - Analyzes code by monitoring its execution
  - Can identify errors at runtime
  - More “sound” than “complete”
    - Actually executes each path
    - Low false positive rates
  - Tools: Valgrind, Purify
Fuzz Testing

• Randomized fault injection
  – Repeated inject invalid/random data into program to find fault
  – Crash of the program usually signify some sort of memory error (e.g., buffer overflow)
  – Don’t perform on live/operational system
• Inputs crossing trust boundary
  – Network Packets
  – File formats
  – Shared memory
• Weaknesses:
  – Usually poor “code coverage”
• Tools: JBroFuzz, SPIKE
  – Some commercial tools for smart grid protocols (e.g., DNP3, IEC 61850)
Common Criteria

• Protection profiles
  – Security requirements for the system
    • operating systems, access control systems, boundary control devices, intrusion detection systems, smartcards, key management systems, VPN client

• Evaluation Assurance Levels (EALs)
  – The extent to which testing was performed:
    – EAL1 – Functionally Tested
    – EAL4 – Methodically Designed, Tested, and Reviewed
      • Red Hat Enterprise Linux, Windows 7, Windows Server 2008
    – EAL6 – Semiformally Verified Design and Tested
      • Green Hills OS
    – EAL7 – Formally Verified Design and Tested
Compliance
NERC CIP Standards

• CIP – Critical Infrastructure Protection
  – Compliance requirements for electric power grid
    • Specifically the Bulk Electric System (BES)

• Proposed by NERC, signed by Federal Energy Regulatory Commission (FERC)

• NERC can issue fine of $1 million/day for non-compliant
  – Based on periodic assessments of a utility’s security

• Versions
  • v3 – Current
  • v5 - Effective 4/1/16
BES Cyber Asset Classification

• What systems does NERC CIP apply to?
• v3 – standards applied to “Critical Cyber Assets”
  – Generating units (and control centers) above 1500MW
  – Transmissions facilities (and control centers)
    • operated over 500kV
    • 300kV and interconnected with 3 or more other substations
  – FACTS systems, if identified as critical by Interconnection Reliability Operating Limits (IROLs)
  – Special Protection Systems (SPS), if identified as critical by Interconnection Reliability Operating Limits (IROLs)

• v5 - “Bright Line Criteria” to classify cyber assets based on violation risk factor (VRF)
  – High
    • Most control centers for reliability coordinators, balancing authorities, generator operator
  – Medium
    • Transmissions facilities over 500kV, or 200-499kV with interconnection with >2 lines
    • Special protection systems
  – Low – all other control systems
NERC CIP: Key Requirements

- **From v3**
- **CIP-003-3 Security Management Controls**
  - R5.2 “at least annually the access privileges to protected information to confirm that access privileges are correct”
- **CIP-005-2a Electronic Security Perimeters**
  - R2.1 “use an access control model that denies access by default”
  - R2.2 “enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic”
  - R2.3 “maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)”
- **CIP-007-2a System Security Management**
  - R1.1 “create, implement, and maintain cyber security test procedures”
  - R2 “implement process to ensure that only those ports and services required for normal emergency operations are enabled”
  - R3.1 “assessment of security patches and security upgrades for applicability within thirty calendar days of availability”
  - R4.2 “implement a process for the update of anti-virus and malware prevention signatures. The process must address testing and installing the signatures.”
  - R5 “establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity”
  - R5.1.3 “review, at least annually, user accounts to verify access privileges”
  - R5.3 “require and user passwords, subject to the following”, “six characters”, “combination of alpha, numeric and special characters” and “changed at least annually”
  - R6.3 “maintain logs of system events related to cyber security”
  - R6.4 “retain all logs specified in Requirement R6 for ninety calendar days”
  - R8.3 “review of controls for default accounts”