Starting Food for Thought

Cybersecurity of Buildings Workshop
National Institute of Building Sciences

John Saunders, PhD, Professor and Director, Center for Cybersecurity, National Defense University

The views expressed herein are those of the presenter and do not reflect the official policy or position of the National Defense University, The Department of Defense, or the U.S. Government.
Attacking & Defending Building Control System Networks
Intelligence Surveillance Reconnaissance

- C4ISR - What is this?
- Setting Objectives, The Battle Plan
- Conducting Offensive Maneuvers
  - Demo 1 - Overt Short Term Denial of Service
  - Demo 2 - Covert Malware Implant
- Setting up a Defense

STRATEGY
Who What Where When How

ACTION
Probing

RESULTS
The Goodies

![Image of a whiteboard with a diagram and notes]

![Image of a meeting room with a group of people]

![Image of a whiteboard with ASCII art and codes]
Command, Control, Computers, Communication (C4)
Intelligence, Surveillance, Reconnaissance (ISR)
Discovery & Pre-positioning in Cyber & ICS Networks

Open Source for whatever might be available about the organization & its IT & control system(s); Vulnerabilities of those networks / devices; Processes

HUMINT & OPS to scope out people, facility, physical characteristics, locate/ID sensors, actuators, PLC & RTU vendors, 3rd party Engr, Maint. for trusted access

SIGINT & OPS to scope out & verify connectivity, RF, hardware geo-location; network(s) scan to create or locate info on structures & equipment, OS, applications, search for information on network [vendors, network diagrams, etc]; identify vulnerabilities; exploit /place malware; monitor for changes / connectivity (maintain persistence)
Battle Plan /Objectives

• Offensive Strategy
  – Purpose
    • Short term
      – Show Face, Damage
      – In-out Asset Capture
    • Long term
      – Espionage
      – Hide, random Lie in wait for signal to do damage
  – Tools Techniques Processes (TTPs)

• Defensive Strategy
  – Kill Chain
  – Defense In Depth
  – Continuous Monitoring / Risk Management
Offensive Campaign

Plan
Prepare
Maneuver
Capture - Foothold
Morph
Entry Points – Building Control System

- **SCADA CONSOLE**
- **Web serv, Pgs: Netcraft, W3af, ZAP**
- **OS, Updates, DNS**
- **Maint & Engineering**
- **OPC tunnel**
- **VPN**
- **Phishing; SET**
- **SQLMap**
- **Open Source; Shodan; Nslookup nmap**
- **Aircrack**
- **VLAN hopping**
- **War dialer/remote tap**
Actual Building Control System

N1: TCP&UDP/IP, Modbus over IP

N2: RS-485 protocol, BACNet, LonWorks, Modbus
Demonstration 1
Short Term Denial of Service on PLC

iCollege SCADA/ICS Lab Network

Trusted party

Spoof Trusted Party IP
Demonstration 1
Low Orbit Ion Cannon
Demonstration 2
Malware Dropper

STUXNET Replaced valid copy of dynamic link library (.dll) complied statement list (STL) with malware
Demonstration 2
Standalone USB Device Attack

- **CVE-2009-0243 TA09-020A** Summary: Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutoRun registry values, which allows physically proximate attackers to execute arbitrary code by (1) inserting CD-ROM media, (2) inserting DVD media, (3) connecting a USB device, and (4) connecting a Firewire device; (5) allows user-assisted remote attackers to execute arbitrary code by mapping a network drive; and allows user-assisted attackers to execute arbitrary code by clicking on (6) an icon under My Computer\Devices with Removable Storage and (7) an option in an AutoPlay dialog, related to the Autorun.inf file. NOTE: vectors 1 and 3 on Vista are already covered by CVE-2008-0951. Published: 01/21/2009 CVSS Severity: **7.2** (HIGH)

- **CVE-2008-0951 VU#889747** Summary: Microsoft Windows Vista does not properly enforce the NoDriveTypeAutoRun registry value, which allows user-assisted remote attackers, and possibly physically proximate attackers, to execute arbitrary code by inserting a (1) CD-ROM device or (2) U3-enabled USB device containing a filesystem with an Autorun.inf file, and possibly other vectors related to (a) AutoRun and (b) AutoPlay actions. Published: 03/24/2008 CVSS Severity: **9.3** (HIGH)
Direct Countermeasures

• Wireless Denial Of Service
  – No Radio Frequency Devices
  – Strong Access Point Encryption
  – Perimeter Device DOS Deflection

• USB/Flash Drive Malware Dropper
  – Limit Outside Media
  – Media Scan Upon Insertion
  – Integrity Checker (e.g. Tripwire)
Strategy
The Kill Chain

Initial Entry
Memory Exploitation
Instruction Pointer Control

Arbitrary Code Exploitation

Exploit Mitigation Kill Chain.ppt

DEFENSIVE
DEFENSIVE

Strategy
Defense in Depth

Configuration Management
PKI
Logging Checks
Wireless Lockdown
Incident Handling Procedures

Social Engineering Checks
Physical Security
Training
ID Management
HD Encryption

Background Checks
Firewalls
Update Service
Intrusion Prevention

Device STIG
Penetration Testing
Validated Equipment
Device Authentication

PKI
Comm Encryption

Validation

NIST 800-53 – Recommended Security Controls for Federal Information Systems and Organizations revision 4 has approximately 850 controls
Strategy

CM/RM (Risk Management/Continuous Monitoring)

• Risk = (Threat * Vulnerability * Impact)

Countermeasures

• Continuous Monitoring
  – People: 24 hour cyber watch desk
  – Process: check logs, incident response, backup,
  – Technology: IDPS, AV, EMET, updating
Final Food for Thought

SOURCE: http://www.youtube.com/watch?v=QvUXkchVTjc
Thank You!

Dr. John Saunders

\texttt{saunders@ndu.edu}

\texttt{(202) 685-2078}

\texttt{http://www.ndu.edu}

iLabs, iCollege, National Defense University