Device Security Challenges for Military and Defense

Sameer Dixit - Sr. Director Spirent Security Labs
Agenda

- Current State of Connected Devices
- Connected Devices Security Snap Shot
- Connected Devices Attack Surface
- Top 10 Vulnerabilities
- What to Test?
- How to Test?
Connected Devices - It’s Huge Already!

![Projected New Adoption of Connected Technology by Consumers](image)

- **In the next year**
- **Five years from now**
- **More than five years from now**
- **Total expected adoption**

**Percentage of customers expected to purchase device:**
- Smart thermostat
- Connected security system
- Smart refrigerator
- Wearable fitness device
- Smart watch
- Self-driving vacuum cleaner
- Wearable heads up display
- Smart clothing
IoT Coverage Continues to Expand

- Military and Defense
  - Security sensors
  - Wearables
  - Unmanned Vehicles
  - Heath and Safety Devices
  - Automotive Real-time Diagnostics
  - HVAC
  - Bodycams
  - Control Systems
  - Robotic Systems

A more connected military means new battlefield glitches, too
Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Internet Of Things' Hacking Attack Led To Widespread Outage Of Popular Websites

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Insurgents 'hack into video feeds from drones'

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

New Windows Trojan Spreads MIRAI Malware To Hack More IoT Devices
Top Connected Device Security Concerns

- IoT & Web application security vulnerabilities: 37%
- Privacy & data exposure: 32.1%
- Data exposure associated with collection & analysis: 27.3%
- Lack of encryption: 26%
- Ease of applying software, firmware updates: 24.3%
Connected Device Security Attack Surface

- **Network** - Services, firewall
- **Application** - Authentication, Authorization, Input Validation
- **Device Hardware** - Physical security, Encryption, Local Data Storage
- **Interface** - Client Data Storage, Data Transport, API
- **Cloud** - Backend Server, Authorization, Update security
<table>
<thead>
<tr>
<th>Rank</th>
<th>Title</th>
<th>Connected Device Attack Surface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insecure Web Interface</td>
<td>Application</td>
</tr>
<tr>
<td>2</td>
<td>Insufficient Authentication/Authorization</td>
<td>Application, Network, Mobile &amp; Cloud</td>
</tr>
<tr>
<td>3</td>
<td>Insecure Network Services</td>
<td>Network</td>
</tr>
<tr>
<td>4</td>
<td>Lack of Transport Encryption/Integrity Verification</td>
<td>Application, Network, Mobile &amp; Cloud</td>
</tr>
<tr>
<td>5</td>
<td>Privacy Concerns</td>
<td>Application, Network, Mobile &amp; Cloud</td>
</tr>
<tr>
<td>6</td>
<td>Insecure Cloud Interface</td>
<td>Cloud</td>
</tr>
<tr>
<td>7</td>
<td>Insecure Mobile Interface</td>
<td>Mobile</td>
</tr>
<tr>
<td>8</td>
<td>Insufficient Security Configurability</td>
<td>Application, Mobile &amp; Cloud</td>
</tr>
<tr>
<td>9</td>
<td>Insecure Software/Firmware</td>
<td>Device &amp; Cloud</td>
</tr>
<tr>
<td>10</td>
<td>Poor Physical Security</td>
<td>Device</td>
</tr>
</tbody>
</table>
What to Test?

- Device
  - Application & Cloud
    - Insecure Server Configuration
    - Default System Passwords
    - Unpatched systems
    - Known Vulnerabilities & Exploits
    - Insecure Firewall Configuration
    - Information Leakage
    - Improper Error Handling
    - Weak cryptographic keys
    - Vulnerable Ciphers and Protocols
    - Data Exfiltration
  - Device Interface
    - Device End Security
      - Sensitive information stored in cache
      - Unencrypted Data Storage
      - Files inspection
      - Excess Permissions and Privileges
      - Device Lockout policy
    - Dynamic Analysis
    - Authentication
    - Authorization
    - Encryption usage
- Device Interface
  - Device Firmware Analysis
  - Binary Code Analysis
  - Spoofing
  - JTAG/UART Review
  - Fuzzing
  - Underlying Software & application evaluation
  - Unencrypted Communication
- Device Network
  - Device Hardware
    - Device End Security
      - Sensitive information stored in cache
      - Unencrypted Data Storage
      - Files inspection
      - Excess Permissions and Privileges
      - Device Lockout policy
    - Dynamic Analysis
    - Authentication
    - Authorization
    - Encryption usage
Best Practice – Stack Hardening

- What is tested?
  - New network devices, anything that has a protocol stack
  - Gateways, proxies, end servers

- How is it tested?
  - Fuzz testing

- Why is it Critical?
  - Most attacks focus on finite state machine bugs or corner case conditions. Fuzzing automatically checks the “Hardness” of the stack, identifying a possible weak point in the design

- What can make this fail?
  - Fuzzing is a “weakest link” event, if you do not test all the protocols, a failure or exposed vulnerability may be found

- Fuzzing Value
  - SmartMutation fuzzing will quickly zones in on problems and test those area more deeply as opposed to random generation of patterns.
Best Practice – Blended Volumetric Attack Testing

- **What is tested?**
  - Ability to mix multiple DDoS attacks in an orchestrated fashion

- **Why is it Critical?**
  - Test each attack with high realism under high volume load

- **What can make this fail?**
  - Not testing critical combinations of attacks

- **Value**
  - Be able to mix and match valid and DDoS Traffic
  - Very high load
  - Ensure test emulate users traffic under elastic conditions
Managed Vulnerability Scanning

- Managed vulnerability scanning of IoT device to uncover vulnerabilities regarding Insecure Server Configuration, Default System Passwords, Insecure Firewall Configuration, Insecure Communications, Information Leakage and Improper Error Handling.

Manual Penetration Testing

- **IoT Device Penetration Test**: The penetration test will assess the IoT device firmware, binary code, related web services and http(s) communication for exploitable vulnerabilities, discover and exploit underlying web application for security weaknesses such as authentication bypass, authorization boundary, SQL injection & XSS in Embedded Web Application Servers and many others.

We Can Help!

Spirent SecurityLabs Service Levels for Connected Device
<table>
<thead>
<tr>
<th>Security Issue</th>
<th>Managed Automated Testing</th>
<th>Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining unauthorized access to sensitive data</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Code injection</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Denial of service attack</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Service crashes</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Input validation weaknesses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Man in the Middle attacks</td>
<td>Partial</td>
<td>✓</td>
</tr>
<tr>
<td>Make unauthorized changes to data or program</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Bypass authentication and authorization mechanism</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Elevation of privilege</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Memory leaks</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Serialization issues</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Our SecurityLabs services follow testing methodology that are structured to deliver consistent, high impact results with minimal impact on the client organization.

**Project planning**
Spirent consultants identify key characteristics of the customer’s asset and construct guidelines for remote or onsite assessment.

**Assessment and analysis**
Using Spirent’s proprietary testing solutions and manual penetration testing techniques; Consultants will identify critical vulnerabilities that could lead to a potential compromise, misuse of the functionality and create a potential security risk.

**Presentation and final report review**
Spirent Consultants will present the final report that summarizes the assessment process, identified vulnerabilities, risk analysis, potential attack scenario(s) and suggested remediation.
Spirent SecurityLabs Credentials

<table>
<thead>
<tr>
<th>Certified &amp; Experienced Security Consultants</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CREST</strong> (Global Certified Ethical Security Testers)</td>
</tr>
<tr>
<td><strong>OSCP</strong> (Offensive Security Certified Professional)</td>
</tr>
<tr>
<td><strong>CEH</strong> (Certified Ethical Hacker)</td>
</tr>
<tr>
<td><strong>CISSP</strong> (Certified Information Systems Security Professional)</td>
</tr>
<tr>
<td><strong>GXPN</strong> (GIAC Certified exploit researcher and advanced penetration tester)</td>
</tr>
<tr>
<td><strong>GPEN</strong> (GIAC Penetration Tester)</td>
</tr>
<tr>
<td><strong>GICSP</strong> (Global Industrial Cyber Security Professional)</td>
</tr>
<tr>
<td><strong>NSA ISAM</strong> (NSA InfoSec Assessment Methodology Certification)</td>
</tr>
<tr>
<td><strong>CCENT</strong> (Cisco Certified Entry Networking Technician)</td>
</tr>
<tr>
<td><strong>Security+</strong>, <strong>Server+</strong></td>
</tr>
<tr>
<td><strong>UCP</strong> (Unix Certified Programmer)</td>
</tr>
</tbody>
</table>
Questions?

Come visit us at - PLEXNET Booth #18
Thank You

SecurityLabs@spirent.com
sameer.dixit@spirent.com