Medical Device Attack Scenario

Sarah Jopp, BS, MBA, CISSP
Senior Analyst, Clinical Information Security – Resiliency
Mayo Clinic
Challenges to Securing Medical Devices

- Zero downtime 24/7
- Clinical workflow issues
- (Re-)approval takes long time
- Patient safety requires special handling
- Lack of Software Development Lifecycle
- "behind-the-perimeter-firewall" mentality
- AV, anti-malware limitations
- Limitations on adding security software
- Patient safety requires special handling
Common Types of Vulnerabilities

Hardcoded Credentials

Default Passwords

Unsupported Operating System

Lack of Patch Management

Insecure configuration

Web app injections

User Name
admin

Password
**********

no/weak/custom encryption

Microsoft Windows XP
Attack Chain

Series of vulnerabilities an attacker will exploit to gain complete access to a critical asset - starting from zero access (*not to be confused with the cyber kill chain)*
Example Scenario: *Gain Unauthorized Access to MRI scanner*

1. Gain access to intranet by exploiting *user ignorance* (phishing) and weak email filtering
2. Install and maintain backdoor access to victim’s system by exploiting *weak perimeter and endpoint security*
3. Pivot to medical device server by exploiting web application *default password*
4. Elevate privileges by exploiting *unpatched server OS*
5. Gain access to medical device by exploiting *trust between server and device*
Step 1: Gain access to intranet

Vulnerability Exploited:
Network perimeter devices have insufficient email filtering

Attacker sends malicious email attachment

**Hacking Tools:** exe packers, custom payloads
Step 1: Gain access to intranet

Vulnerability Exploited:
User ignorance

_Hacking Tools:_ social engineering, patience
Step 1: Gain access to intranet

**Vulnerability Exploited:**
- Insufficient Endpoint Protection
- Weak perimeter firewall / IDS

**Attacker’s malware is installed on Bob’s machine and calls back to attacker’s machine**

**Hacking Tools:** reverse shell (msfvenom)
Step 2: Gain access to web server

Vulnerability Exploited:
Lack of Network Segmentation

Attacker pivots to attack the web server managing the MRI

*Hacking Tools:* Nmap, nikto, web browser
Step 2: Gain access to web server

Vulnerability Exploited:
Weak Password Policy
Lack of Brute-force Protection
Default Passwords

Attacker gains access to the web application managing the MRI by: Brute-force, guessing or consulting the device manual

Hacking Tools: Ncrack
Step 3: Elevate privileges on web server

Vulnerability Exploited:
Web server running with excessive privileges
Unpatched web application

Attacker gains shell on server by exploiting web app and running remote code as a web application user (elevated privileges).

Hacking Tools: web browser, metasploit
Step 4: Gain access to MRI scanner

**Vulnerability Exploited:**
- Unsupported/Outdated OS
- Insecure Firewall Configuration

Attacker gains Administrator access to the MRI by exploiting known vulnerabilities (i.e. MS17-010)

**Hacking Tools:** metasploit
## Testing Methods for Common Vulnerabilities

<table>
<thead>
<tr>
<th>Method</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse engineering of binary executable files</td>
<td>Hardcoded Credentials</td>
</tr>
<tr>
<td>Assessment of cryptographic aspects of application</td>
<td>Default Passwords</td>
</tr>
<tr>
<td>Analysis of custom protocols</td>
<td>no/weak/custom encryption</td>
</tr>
<tr>
<td>Manual web application assessments</td>
<td>Unsupported OS</td>
</tr>
<tr>
<td></td>
<td>Lack of Patch Mgmt.</td>
</tr>
<tr>
<td></td>
<td>Insecure config.</td>
</tr>
<tr>
<td></td>
<td>Web app injections</td>
</tr>
</tbody>
</table>

### Manual Web Application Assessments
- Testing Methods for Common Vulnerabilities
- Assessment of cryptographic aspects of application
- Analysis of custom protocols
- Manual web application assessments
# Testing Methods for Common Vulnerabilities

<table>
<thead>
<tr>
<th>Method</th>
<th>Hardcoded Credentials</th>
<th>Default Passwords</th>
<th>no/weak/custom encryption</th>
<th>Unsupported OS</th>
<th>Lack of Patch Mgmt.</th>
<th>Insecure config.</th>
<th>Web app injections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual host Configuration reviews</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interview vendor staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote scan of services for vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions