Basic Threat Modeling and Risk Assessment

Fotios (Fotis) Chantzis (@ithilgore)
Principal Information Security Engineer
Clinical Information Security - Resiliency
Mayo Clinic
whoami

- [https://sock-raw.org](https://sock-raw.org)
- Vulnerability Assessments on medical devices (Mayo Clinic)
- Network security research (e.g. TCP Persist Timer exploitation - [http://phrack.org/issues/66/9.html](http://phrack.org/issues/66/9.html), XMPP zombie scan)
- Nmap contributor & Google Summer of Code Mentor
- Ncrack author - [https://nmap.org/ncrack](https://nmap.org/ncrack)
- Mastering Nmap video course - [https://www.udemy.com/mastering-nmap/](https://www.udemy.com/mastering-nmap/)
- OSCP, OSCE, M.Eng., PhD candidate on IoT & medical device security
The healthcare industry was the victim of 88% of all ransomware attacks in U.S. industries last year. (source: Solutionary)

89% of studied healthcare organizations have experienced a data breach, which involved patient data being stolen or lost, over the past two years. (source: Ponemon Institute)

27% of all reported breaches are in the Healthcare industry (Source: Gemalto 1st Half Findings from 2016 Breach Level Index Data)

Healthcare organizations experience more than twice the number of attacks on average as compared to other vertical market categories  (FortiGuard Labs)
1. Patient harm
2. PHI / PII theft
3. Medical research IP theft
4. Disruption
5. Profit

Do you recognize this?

65 UK hospitals in one day
With great connectivity comes great responsibility
Previously on...
Previously on...

the Defcon 26 Biohacking Village

http://villageb.io/#s4
DVMD
Damn Vulnerable Medical Device

Emulates IV pump
- BOF
- Insecure network protocol

Server component
- SQLi
- Serialization bug
- PACS DICOM
Medical Device Security Problems

(re-)approval takes long time

zero downtime 24/7

"behind-the-perimeter-firewall" mentality

临床工作流问题

FD FDA

AV, anti-malware limitations

患者安全需要特殊处理

缺乏软件开发生命周期

限于额外软件
Common Types of Vulnerabilities

- Hardcoded Credentials
- Default Passwords
- Unsupported Operating System
- Lack of Patch Management
- Insecure configuration
- Web app injections
- No/weak/custom encryption
Top 6 Mayo Clinic Baseline Requirements

1. Complies with Work Account Standards
2. Runs supported OS
3. Receives routine OS patches
4. Has AV applied and updated
5. Contains no default hardcoded passwords
6. Receives routine 3rd party software patches
Common systems in healthcare environments

- PACS Servers
- Infusion pumps
- Ultrasound / CT / MRI scanners
- Pacemakers
- Pagers
- Surveillance cameras
- EHR systems
- Many more - huge diversity
Attack Trees

- Conceptual diagram
- Focused on attackers (vs threats)
- Logical operators (AND, OR)
Drug Infusion Pump
ATTACK GOAL - Emuneous Infusion

Manipulate drug infusion pump

Modify the Electronic health record to increase the infusion rate of an infusion pump

Gain remote access to EHR server

Nebook Compromise

Server Exploitation

Access the client with valid Admin username and password

Retrieve Traffic

Man in the Middle Attack

Port Scanning

Identify phishing exploits

Spear Phishing

Trick the Administrator

Access to traffic from a certain host or network

Access to traffic intended for a certain host or network

Replay Attack

Spoofing

ARP cache poisoning
<table>
<thead>
<tr>
<th>Saltzer and Schroeder design principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open design</strong></td>
</tr>
<tr>
<td><strong>Fail-safe defaults</strong></td>
</tr>
<tr>
<td><strong>Least privilege</strong></td>
</tr>
<tr>
<td><strong>Economy of mechanism</strong></td>
</tr>
<tr>
<td><strong>Separation of privileges</strong></td>
</tr>
<tr>
<td><strong>Total mediation</strong></td>
</tr>
<tr>
<td><strong>Least common mechanism</strong></td>
</tr>
<tr>
<td><strong>Psychological acceptability</strong></td>
</tr>
</tbody>
</table>
## Security Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Data is only available to the people intended to access it.</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Data and system resources are only changed in appropriate ways by appropriate people.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Systems are ready when needed and perform acceptably.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The identity of users is established</td>
</tr>
<tr>
<td><strong>Authorization</strong></td>
<td>Users are explicitly allowed or denied access to resources.</td>
</tr>
<tr>
<td><strong>Nonrepudiation</strong></td>
<td>Users can’t perform an action and later deny performing it.</td>
</tr>
</tbody>
</table>
## Threats and Security Properties (STRIDE)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Security Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non-repudiation</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Availability</td>
</tr>
<tr>
<td>Elevation of privilege</td>
<td>Authorization</td>
</tr>
</tbody>
</table>
# Threat Rating (DREAD)

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage potential</td>
<td>If a threat exploit occurs, how much damage will be caused?</td>
</tr>
<tr>
<td>Reproducibility</td>
<td>How easy is it to reproduce the threat exploit?</td>
</tr>
<tr>
<td>Exploitability</td>
<td>What is needed to exploit this threat?</td>
</tr>
<tr>
<td>Affected users</td>
<td>How many users will be affected?</td>
</tr>
<tr>
<td>Discoverability</td>
<td>How easy is it to discover this threat?</td>
</tr>
</tbody>
</table>

Rating DREAD = (Damage potential + Reproducibility + Exploitability + Affected Users + Discoverability) / 5

**High:** 8 - 10  
**Medium:** 5 - 7  
**Low:** 1 - 4
Threat Modeling Steps

1. Identify the assets of the system
2. Decompose the system
3. Analyze each component for threats
4. Rate threats
5. Mitigate threats
Scenario: Infusion Pump

<table>
<thead>
<tr>
<th></th>
<th>Assets - Ax</th>
<th>Threats - Tx</th>
<th>Controls - Cx</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wireless creds</td>
<td>S, I</td>
<td>WPA2</td>
</tr>
<tr>
<td>2</td>
<td>User creds</td>
<td>S, I, E</td>
<td>MD5</td>
</tr>
<tr>
<td>3</td>
<td>Drug Settings</td>
<td>S, T, R, I</td>
<td>HTTP</td>
</tr>
<tr>
<td>4</td>
<td>EHR record</td>
<td>S, T, R, I</td>
<td>AV, Auditing</td>
</tr>
<tr>
<td>5</td>
<td>IV pump</td>
<td>S, T, R, I, D, E</td>
<td>Telnet</td>
</tr>
<tr>
<td>6</td>
<td>Drug Settings</td>
<td>S, T, R, I</td>
<td>Bluetooth</td>
</tr>
</tbody>
</table>
**Scenario: Infusion Pump**

<table>
<thead>
<tr>
<th>ID</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Access IV pump network</td>
</tr>
<tr>
<td>Description</td>
<td>Bypass wireless auth and gain access to network by using KRACK</td>
</tr>
<tr>
<td>Controls</td>
<td>WPA2</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Disable EAPOL-Key frame re-transmission during key installation</td>
</tr>
<tr>
<td>Entry Point</td>
<td>Wireless AP</td>
</tr>
<tr>
<td>Assets</td>
<td>Wireless credentials, IV pump</td>
</tr>
<tr>
<td>Rating</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Diagram:**
- **IV pump**
  - ID 1
  - Name: Access IV pump network
  - Description: Bypass wireless auth and gain access to network by using KRACK
  - Controls: WPA2
  - Mitigation: Disable EAPOL-Key frame re-transmission during key installation
  - Entry Point: Wireless AP
  - Assets: Wireless credentials, IV pump
  - Rating: Medium
Scenario: Infusion Pump

<table>
<thead>
<tr>
<th>ID</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Recover user credentials</td>
</tr>
<tr>
<td>Description</td>
<td>Crack the MD5-hashed credentials</td>
</tr>
<tr>
<td>Controls</td>
<td>MD5</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Use stronger hashing (e.g. SHA2)</td>
</tr>
<tr>
<td>Entry Point</td>
<td>EHR server</td>
</tr>
<tr>
<td>Assets</td>
<td>User credentials</td>
</tr>
<tr>
<td>Rating</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Scenario: Infusion Pump

<table>
<thead>
<tr>
<th>ID</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Change drug library settings</td>
</tr>
<tr>
<td>Description</td>
<td>Perform mitm and modify drug library settings in transit</td>
</tr>
<tr>
<td>Controls</td>
<td>HTTP</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Use HTTPS</td>
</tr>
<tr>
<td>Entry Point</td>
<td>Wireless AP</td>
</tr>
<tr>
<td>Assets</td>
<td>IV pump</td>
</tr>
<tr>
<td>Rating</td>
<td>High</td>
</tr>
</tbody>
</table>
Scenario: Infusion Pump

IV pump

EHR

Server

Wireless
AP

A1, C1, T1

A2, C2, T2

A3, C3, T3

A4, C4, T4

A5, C5, T5

ID | 4
---|---
Name | Modify EHR record
Description | Perform SQL injection in web app of EHR server
Controls | AV, auditing
Mitigation | Sanitize all input from web app.
Entry Point | EHR server
Assets | EHR record
Rating | High
**Scenario: Infusion Pump**

<table>
<thead>
<tr>
<th>ID</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Gain administrative access on IV pump</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Use default telnet credentials</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td>Telnet</td>
</tr>
<tr>
<td><strong>Mitigation</strong></td>
<td>Disable telnet. Change credentials</td>
</tr>
<tr>
<td><strong>Entry Point</strong></td>
<td>IV pump</td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td>IV pump</td>
</tr>
<tr>
<td><strong>Rating</strong></td>
<td>High</td>
</tr>
</tbody>
</table>
### Scenario: Infusion Pump

**ID**: 6

**Name**: Change drug library settings

**Description**: Perform bluetooth pairing, then mitm and modify drug library settings in transit

**Controls**: Bluetooth

**Mitigation**: Disable bluetooth

**Entry Point**: Bluetooth, physical presence

**Assets**: IV pump

**Rating**: High
Attack Chain

Example scenario:
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 OS in server
5. Gain access to medical device by exploiting trust between server and device
Scenario 1: Gain access to MRI scanner

Step 1.
Gain access to intranet
**Scenario 1: Gain access to MRI scanner**

Step 1.
Gain access to intranet

Vulnerabilities exploited:
- Network perimeter devices have insufficient email filtering

Hacking tools:
- exe packers, custom payloads

Attacker sends malicious email attachment

*Bob*
Scenario 1: Gain access to MRI scanner

Step 1.
Gain access to intranet

Vulnerabilities exploited:
• User ignorance

Bob is duped into opening the malicious attachment

Hacking tools:
social engineering, patience
Scenario 1: Gain access to MRI scanner

Step 1.
Gain access to intranet

Vulnerabilities exploited:
- Insufficient Endpoint Protection
- Weak perimeter firewall / IDS security

Hacking tools:
reverse shell (msfvenom)

Attacker’s malware is installed in Bob’s machine and calls back to attacker’s machine.
**Scenario 1: Gain access to MRI scanner**

Step 2. Gain access to web server

Vulnerabilities exploited:
- Lack of Network Segmentation

**Hacking tools:**
- Nmap, nikto, web browser

Attacker pivots to attacking the web server that manages the MRI device.
**Scenario 1: Gain access to MRI scanner**

Step 2.
Gain access to web server

Vulnerabilities exploited:
• Weak Password Policy
• Lack of Brute-force Protection
• Default Passwords

Attacker gains access to the *web application* that manages the MRI scanner by:
- Brute-forcing / guessing or
- consulting the device manual

**Hacking tools:**
Ncrack
**Scenario 1: Gain access to MRI scanner**

Step 3.
Elevate privileges on web server

Vulnerabilities exploited:
- Web server running with excessive privileges
- Unpatched web application

*Hacking tools:*
web browser, metasploit

Attacker gains shell on medical device server by exploiting the web application. Runs remote code in the context of the web application user (elevated privileges).
**Scenario 1: Gain access to MRI scanner**

Step 4.
Gain access to MRI scanner

Vulnerabilities exploited:
- Unsupported Outdated Operating System
- Insecure Firewall Configuration

Attacker gains Administrator access to the MRI scanner by exploiting known vulnerabilities (such as MS17-010)

**Hacking tools:**
metasploit
Scenario 2: Gain access to infusion pump

Step 1.
Experiment with similar or older version of medical device

Vulnerabilities exploited:
• Hardcoded Credentials

Hacking tools:
Reverse engineering tools, time

Threat actor purchases medical device from eBay or other marketplace. They then search for hardcoded credentials.
Threat actor discovers hardcoded credentials that have been placed by vendor for backdoor access. Then they leak them online.

Scenario 2: Gain access to infusion pump

Step 2. (optional)
Leak discovered hardcoded credentials

Vulnerabilities exploited:
• Hardcoded Credentials

Hacking tools:
Reverse engineering tools, time

deep web

online forums

by vendor for backdoor access. Then they leak them online.
**Scenario 2: Gain access to infusion pump**

Step 3a.
Gain access to infusion pump

Vulnerabilities exploited:
• Hardcoded Credentials

Threat actor uses Dave’s computer to pivot his attack to the infusion pump. Directly gains access using the hardcoded credentials.

(access to intranet same as before - phishing)

**Hacking tools:**
proxychains, telnet, ftp clients
**Scenario 2: Gain access to infusion pump**

Step 3b-i. *(alternative way)*
Analyze communication between server and pump

Vulnerabilities exploited:
• ARP Spoofing (Lack of Static ARP)
• Insecure Communication Channel (Lack of TLS)

**Hacking tools:**

dSniff, Wireshark, Python
Scenario 2: Gain access to infusion pump

Step 3b-ii. (alternative way)
Remotely install rogue drug library

Vulnerabilities exploited:
- Lack of mutual authentication

Attacker masquerades as server and replays maliciously modified versions of captured packets that push the rogue drug library to the pump.

Hacking tools:
dSniff, Wireshark, Python
Attacker plants XSS in healthcare portal which will be visited by healthcare practitioner from inside the hospital intranet.

**Scenario 3: Gain access to Ultrasound scanner**

Step 1. Plant XSS in publicly accessible healthcare portal

Vulnerabilities exploited:
- Stored XSS

Hacking tools:
- Web browser
- PACS Server

*Charlie*

**Portal**

*Hacking tools:*
Web browser
Scenario 3: Gain access to Ultrasound scanner

Step 2.
Redirect victim to attacker controlled system (through XSS) and leverage RCE browser exploit

Vulnerabilities exploited:
• Unpatched browser (IE - CVE-2017-8618, MS14-064)

Access to intranet is gained.

Hacking tools:
- metasploit

After being redirected to the malicious machine, their system gets compromised through a client-side attack (browser exploit). Access to intranet is gained.
**Scenario 3: Gain access to Ultrasound scanner**

Step 3.
Hijack victim’s PACS Server session

Vulnerabilities exploited:
• Insufficient Endpoint Protection

Hacking tools:
Javascript, browser

Having a shell in victim’s computer through the RCE exploit, the victim’s active PACS web session is hijacked using a man-in-the-browser attack.
Scenario 3: Gain access to Ultrasound scanner

Step 4.
Start exfiltrating data from PACS through encrypted tunnel

Vulnerabilities exploited:
• Weak DLP implementation

Data exfiltration from PACS Server is taking place using tunnel over HTTPS – this will bypass many DLP solutions.

Hacking tools: stunnel

PACS Server

DICOM

attacker-controlled machine

portal

Charlie

Portal

attacker-controlled machine
Scenario 3: Gain access to Ultrasound scanner

Step 5.
Gain access to Ultrasound system by exploiting DICOM service

Vulnerabilities exploited:
• Buffer Overflow in DICOM service

Hacking tools: debugger

PACS Server

attacker-controlled machine

portal

The US system regularly communicates with PACS through DICOM. Attacker gains foothold by exploiting (inherently) broken DICOM toolkit.
Bonus Scenario

1. Infiltrate vendor network that provides remote support to HDO
2. Access the remote support software
3. Pivot to hospital network through remote support connection
4. ???
5. PROFIT

*third parties implicated in 63% of all data breaches (Trustwave - 2013)*
Vulnerability Assessment Methodology

- Conduction of manual web application assessments
- Analysis of custom protocols
- Reverse engineering of binary executable files
- Assessment of cryptographic aspects of application
- Manual host configuration reviews
- **Hardware hacking**
- Remote scan of services for vulnerabilities
- Interview vendor staff
Hardware Hacking

Lots of patience ^ 2

Multimeter, Logic Analyzer (Saleae), Bus Pirate, FT2232H (Bus Blaster / Shikra), JTAGulator, Flash Programmers, Raspberry PI IO pins, Arduino / Teensy / … boards, FPGA, OpenOCD, Binwalk, Ida Pro / Binary Ninja / radare2, HackRF, RFcat, BladeRF, GNU Radio

really looks like our CIS lab
<table>
<thead>
<tr>
<th>Component</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardcoded Credentials</td>
<td>Reverse engineering of binary executable files</td>
</tr>
<tr>
<td>Default Passwords</td>
<td>Analysis of custom protocols</td>
</tr>
<tr>
<td>no/weak/custom encryption</td>
<td>Assessment of cryptographic aspects of application</td>
</tr>
<tr>
<td>Unsupported Operating System</td>
<td>Manual web application assessments</td>
</tr>
<tr>
<td>Lack of Patch Management</td>
<td>Manual host configuration reviews</td>
</tr>
<tr>
<td>Insecure configuration</td>
<td>Interview vendor staff</td>
</tr>
<tr>
<td>Web app injections</td>
<td>Remote scan of services for vulnerabilities</td>
</tr>
</tbody>
</table>
Lessons Learned

• Medical Device Security is **hard**
• Vulnerabilities are similar to those affecting mainstream systems
• No easy solution for legacy devices
• Holistic Vulnerability Assessment approach is necessary
• Healthcare is a highly targeted industry
• **Vendors should integrate security in the development lifecycle**
• Incorporating security in the procurement phase is important
Resources

- Vulnerability Assessment book (plus VA checklist) inside the vendor book -
  https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647
- FDA Premarket Submissions for Management of Cybersecurity in Medical Devices -
- FDA Postmarket Management of Cybersecurity in Medical Devices -
- OWASP Secure Medical Device Deployment Standard -