

Basic Threat Modeling and Risk Assessment

Fotios (Fotis) Chantzis
(@ithilgore)


Principal Information Security Engineer
Clinical Information Security - Resiliency
Mayo Clinic



whoami

@ithilgore

- <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> , XMPP zombie scan)
- Nmap contributor & Google Summer of Code Mentor
- Ncrack author - <https://nmap.org/ncrack>
- Mastering Nmap video course - <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

65 UK
hospitals
in one
day



Do you recognize this?

The background image is a blurred, futuristic scene. It appears to be a high-tech laboratory or a control room. There are several computer monitors displaying various data and graphs. The lighting is predominantly blue and white, creating a cool, technological atmosphere. In the foreground, a person is lying down, possibly on a medical bed or a specialized workstation, with their arm extended. The overall impression is one of advanced technology and scientific research.

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





zero downtime
24/7



limitations on
additional
software



"behind-the-perimeter-
firewall" mentality



clinical workflow
issues

Medical Device Security Problems



(re-)approval
takes long time



patient safety requires
special handling



lack of Software
Development Lifecycle



AV, anti-malware
limitations

[illegible]

Hardcoded Credentials

User Name

admin

Password

Default Passwords



no/weak/**custom**
encryption

Common Types of Vulnerabilities



Unsupported
Operating
System



Lack of Patch Management



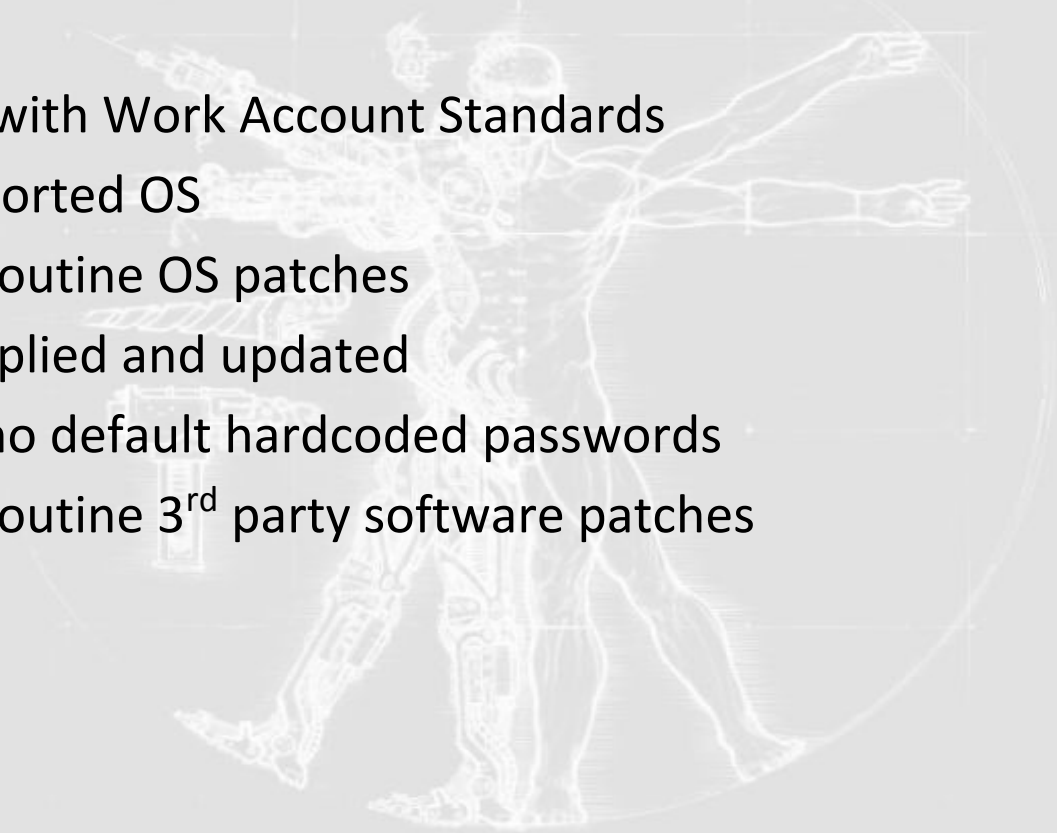
Insecure configuration



Web app injections

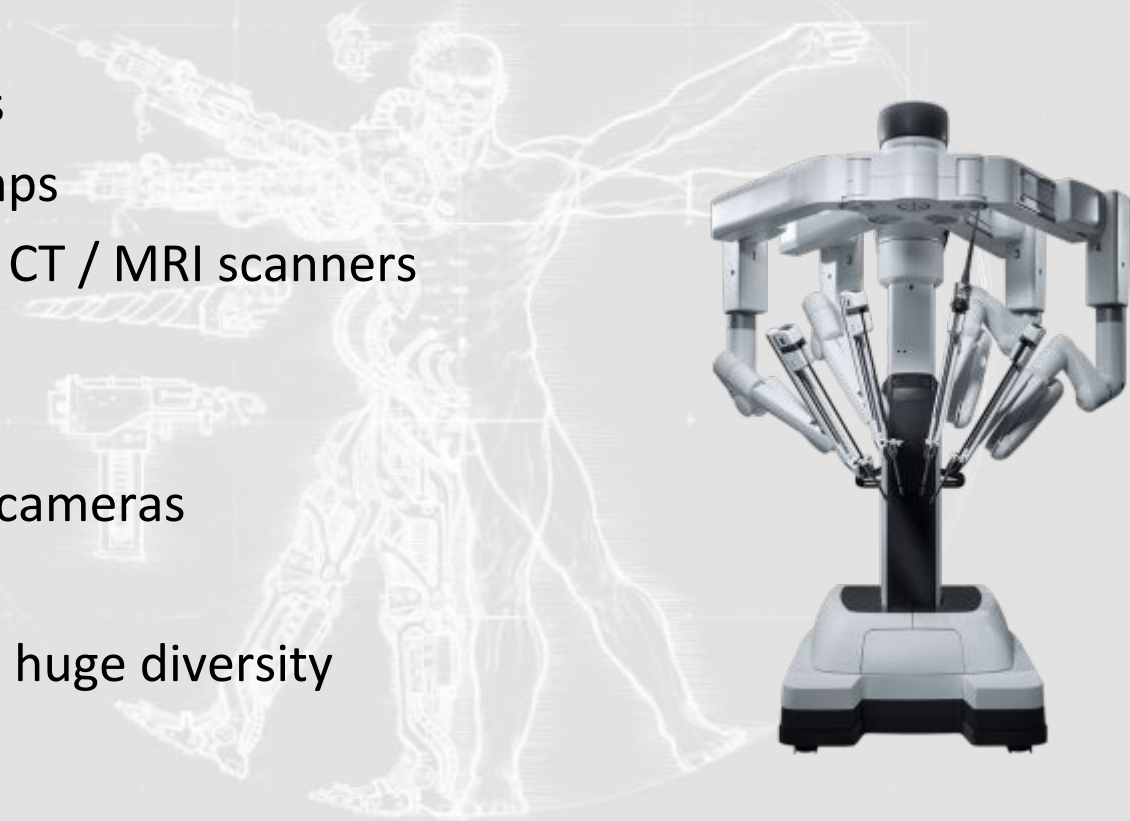
Top 6 Mayo Clinic Baseline Requirements

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

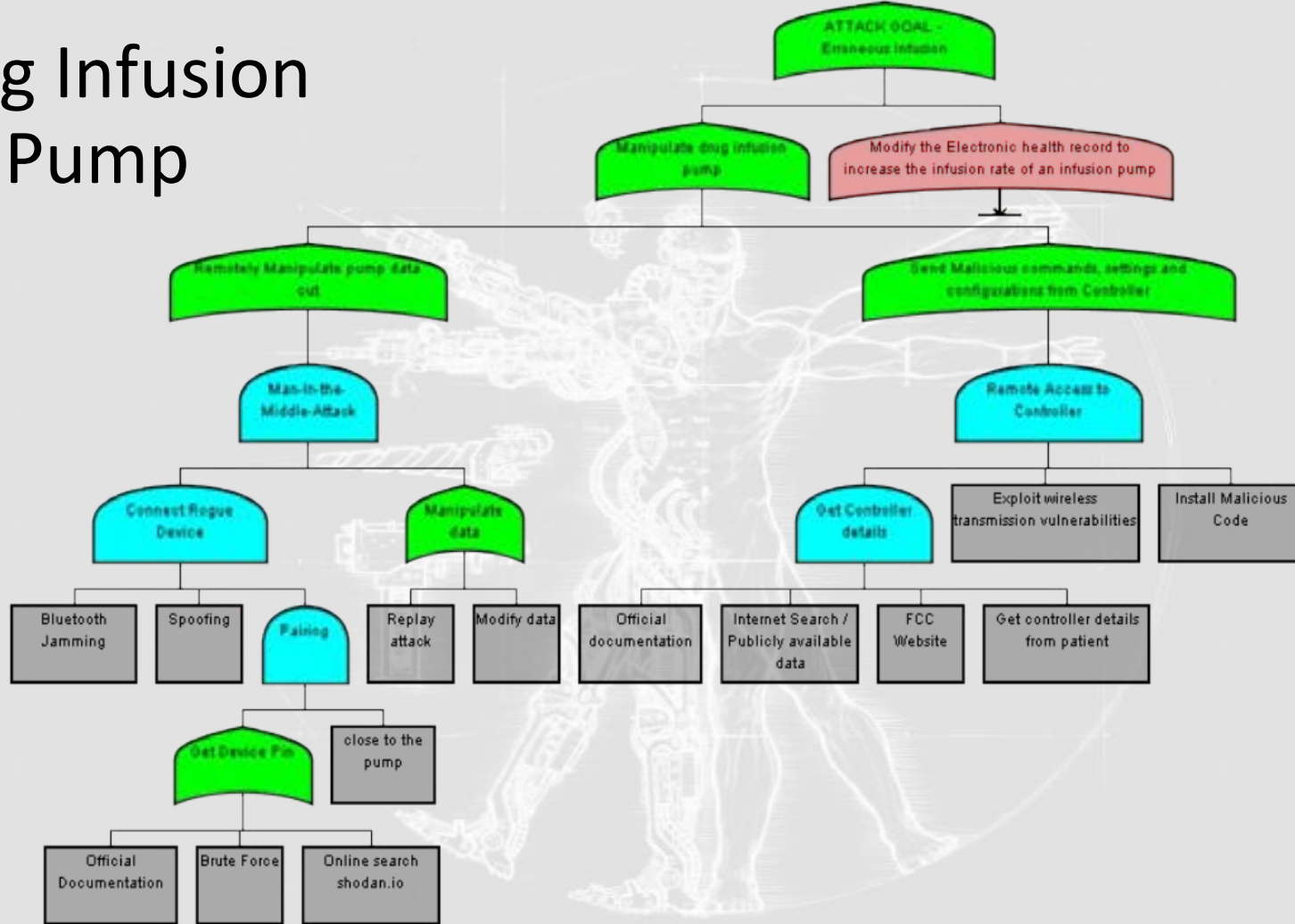


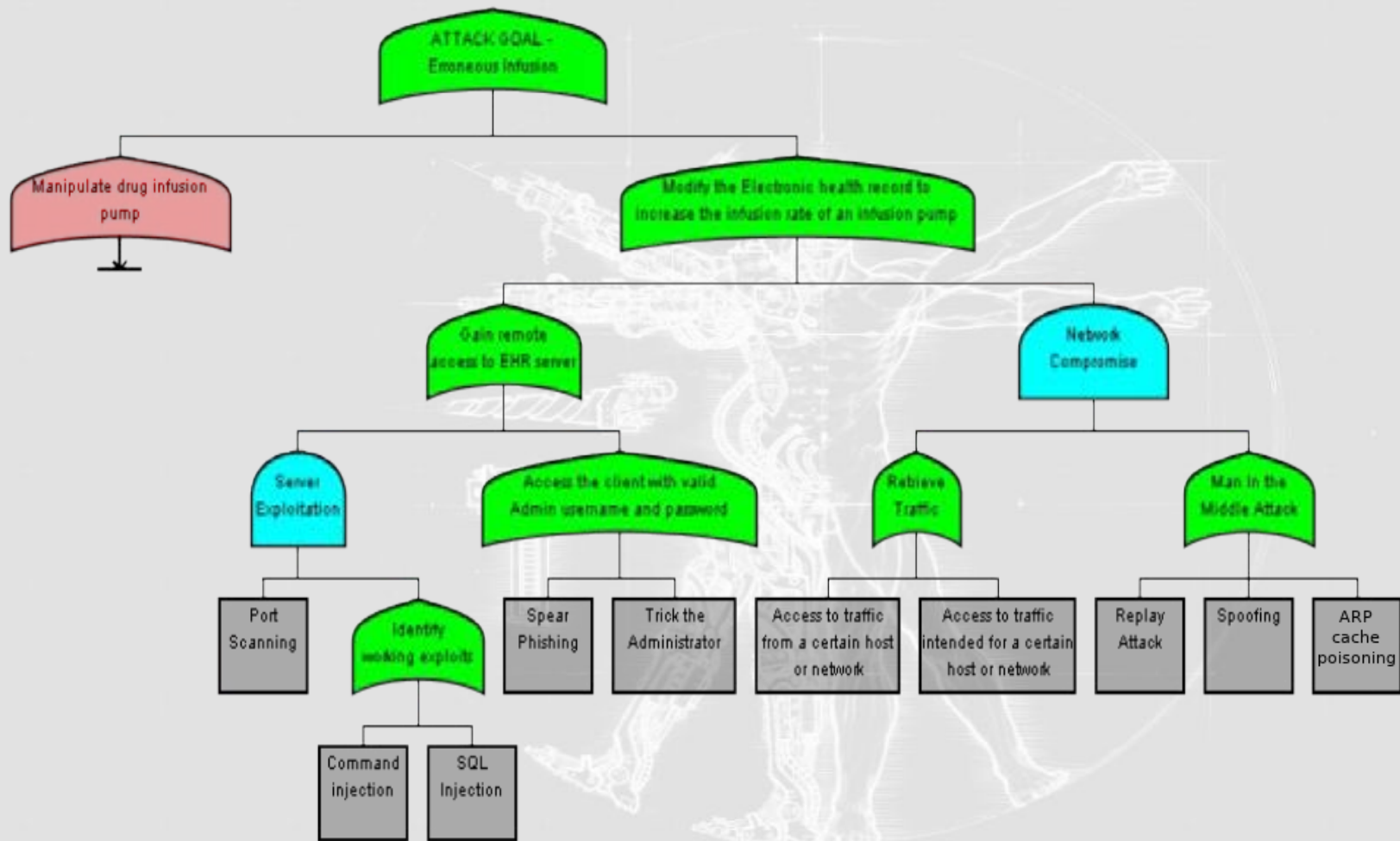
Attack Trees

- Conceptual diagram
- Focused on attackers (vs threats)
- Logical operators (AND, OR)



Drug Infusion Pump





Saltzer and Schroeder design principles



Open design	Assume the attackers have the sources and the specs.
Fail-safe defaults	Fail closed; no single point of failure.
Least privilege	No more privileges than what is needed.
Economy of mechanism	Keep it simple, stupid.
Separation of privileges	Don't permit an operation based on a single condition.
Total mediation	Check everything, every time.
Least common mechanism	Beware of shared resources.
Psychological acceptability	Will they use it?

Security Properties

Confidentiality	Data is only available to the people intended to access it.
Integrity	Data and system resources are only changed in appropriate ways by appropriate people.
Availability	Systems are ready when needed and perform acceptably.
Authentication	The identity of users is established
Authorization	Users are explicitly allowed or denied access to resources.
Nonrepudiation	Users can't perform an action and later deny performing it.

Threats and Security Properties (STRIDE)



Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Threat Rating (DREAD)

Damage potential	If a threat exploit occurs, how much damage will be caused?
Reproducibility	How easy is it to reproduce the threat exploit?
Exploitability	What is needed to exploit this threat?
Affected users	How many users will be affected?
Discoverability	How easy is it to discover this threat?

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

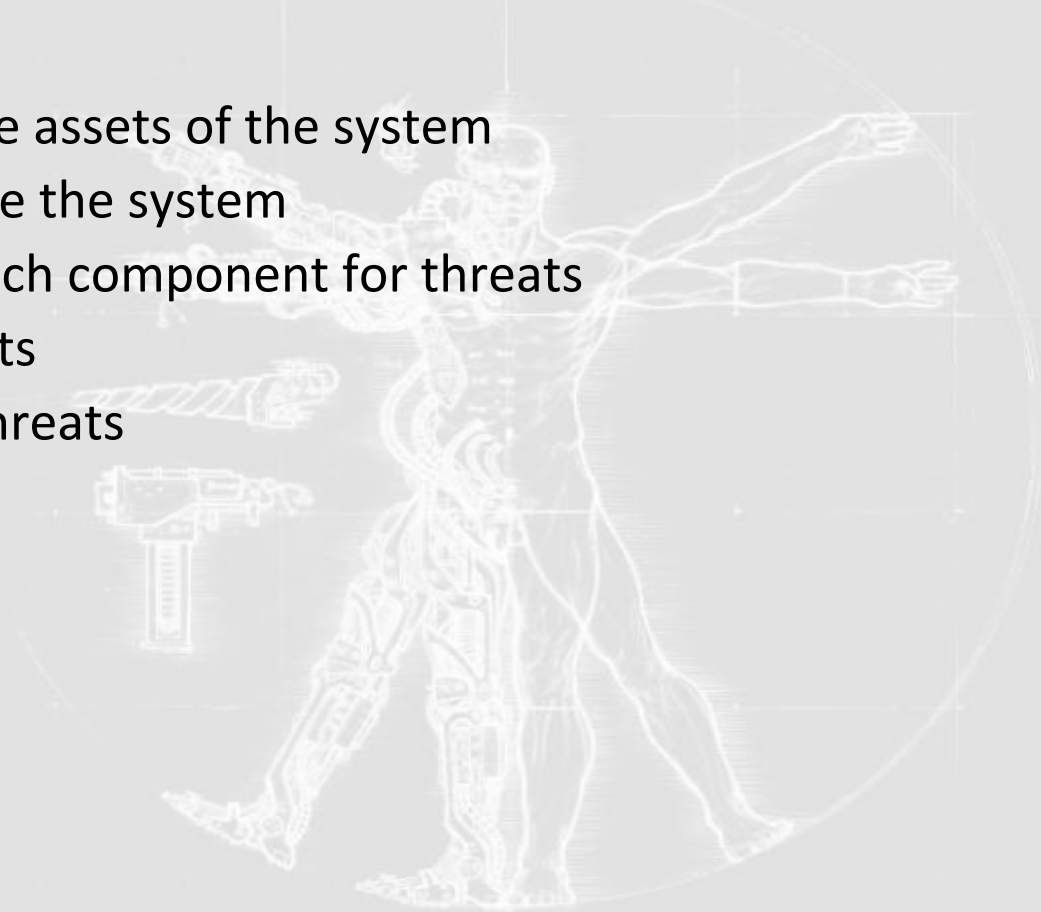
High: 8 - 10

Medium: 5 - 7

Low: 1 - 4

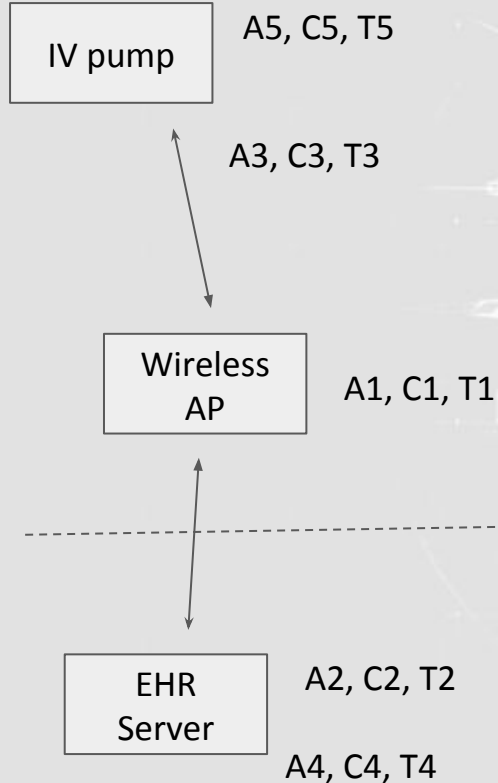
Threat Modeling Steps

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

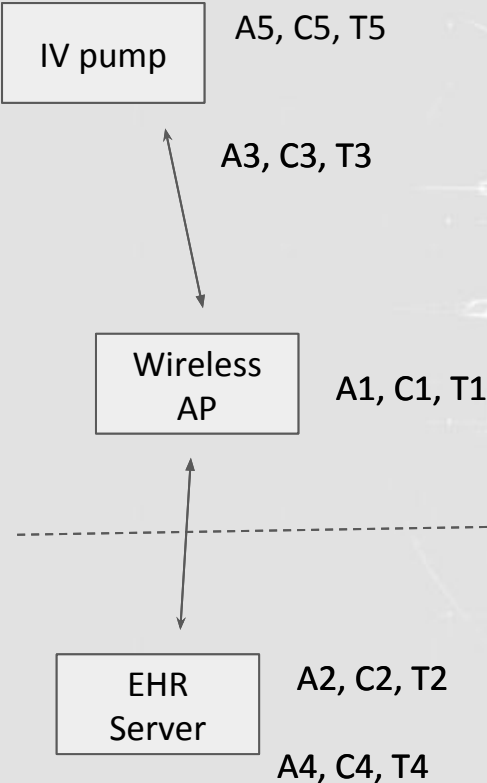
A6, C6, T6



	Assets - Ax	Threats - Tx	Controls - Cx
1	Wireless creds	S, I	WPA2
2	User creds	S, I, E	MD5
3	Drug Settings	S, T, R, I	HTTP
4	EHR record	S, T, R, I	AV, Auditing
5	IV pump	S, T, R, I, D, E	Telnet
6	Drug Settings	S, T, R, I	Bluetooth

Scenario: Infusion Pump

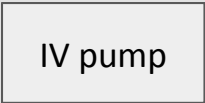
A6, C6, T6



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

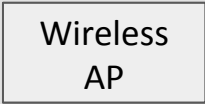
Scenario: Infusion Pump

A6, C6, T6



A5, C5, T5

A3, C3, T3



A1, C1, T1



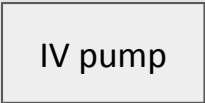
A2, C2, T2

A4, C4, T4

ID	2
Name	Recover user credentials
Description	Crack the MD5-hashed credentials
Controls	MD5
Mitigation	Use stronger hashing (e.g. SHA2)
Entry Point	EHR server
Assets	User credentials
Rating	Medium

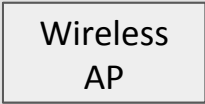
Scenario: Infusion Pump

A6, C6, T6



A5, C5, T5

A3, C3, T3



A1, C1, T1



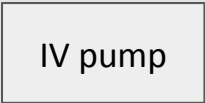
A2, C2, T2

A4, C4, T4

ID	3
Name	Change drug library settings
Description	Perform mitm and modify drug library settings in transit
Controls	HTTP
Mitigation	Use HTTPS
Entry Point	Wireless AP
Assets	IV pump
Rating	High

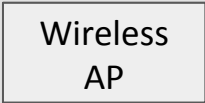
Scenario: Infusion Pump

A6, C6, T6

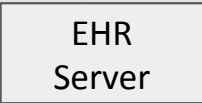


A5, C5, T5

A3, C3, T3



A1, C1, T1



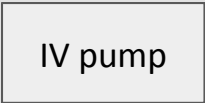
A2, C2, T2

A4, C4, T4

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

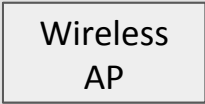
Scenario: Infusion Pump

A6, C6, T6

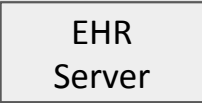


A5, C5, T5

A3, C3, T3



A1, C1, T1



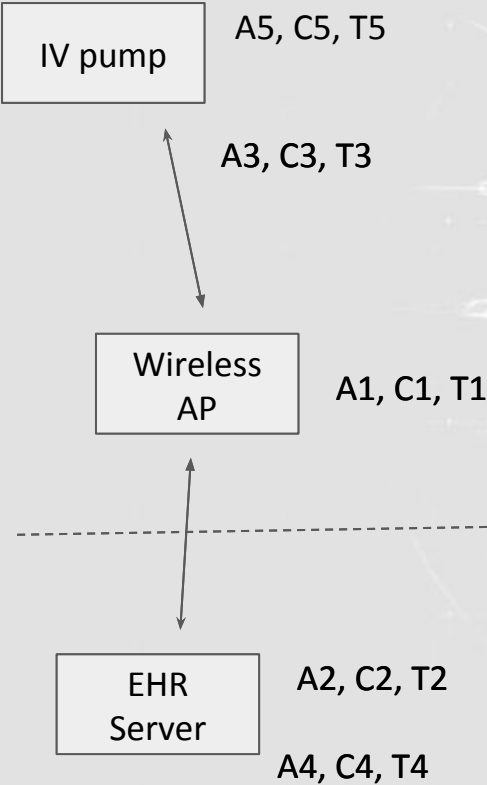
A2, C2, T2

A4, C4, T4

ID	5
Name	Gain administrative access on IV pump
Description	Use default telnet credentials
Controls	Telnet
Mitigation	Disable telnet. Change credentials
Entry Point	IV pump
Assets	IV pump
Rating	High

Scenario: Infusion Pump

A6, C6, T6



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

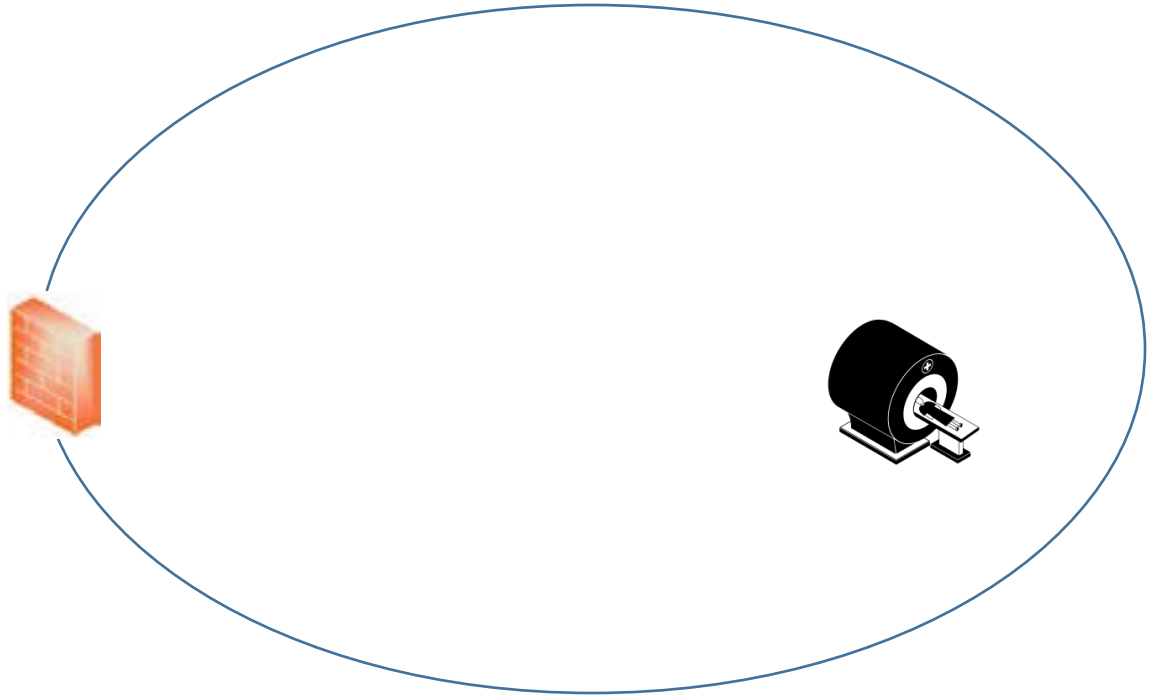
Example scenario:

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

Attacker sends malicious email attachment



Bob



Hacking tools:

exe packers, custom payloads

Scenario 1: Gain access to MRI scanner

Step 1.

Gain access to intranet

Bob is duped into opening the
malicious attachment

Vulnerabilities exploited:

- User ignorance



Bob



Hacking tools:

social engineering, **patience**

Scenario 1: Gain access to MRI scanner

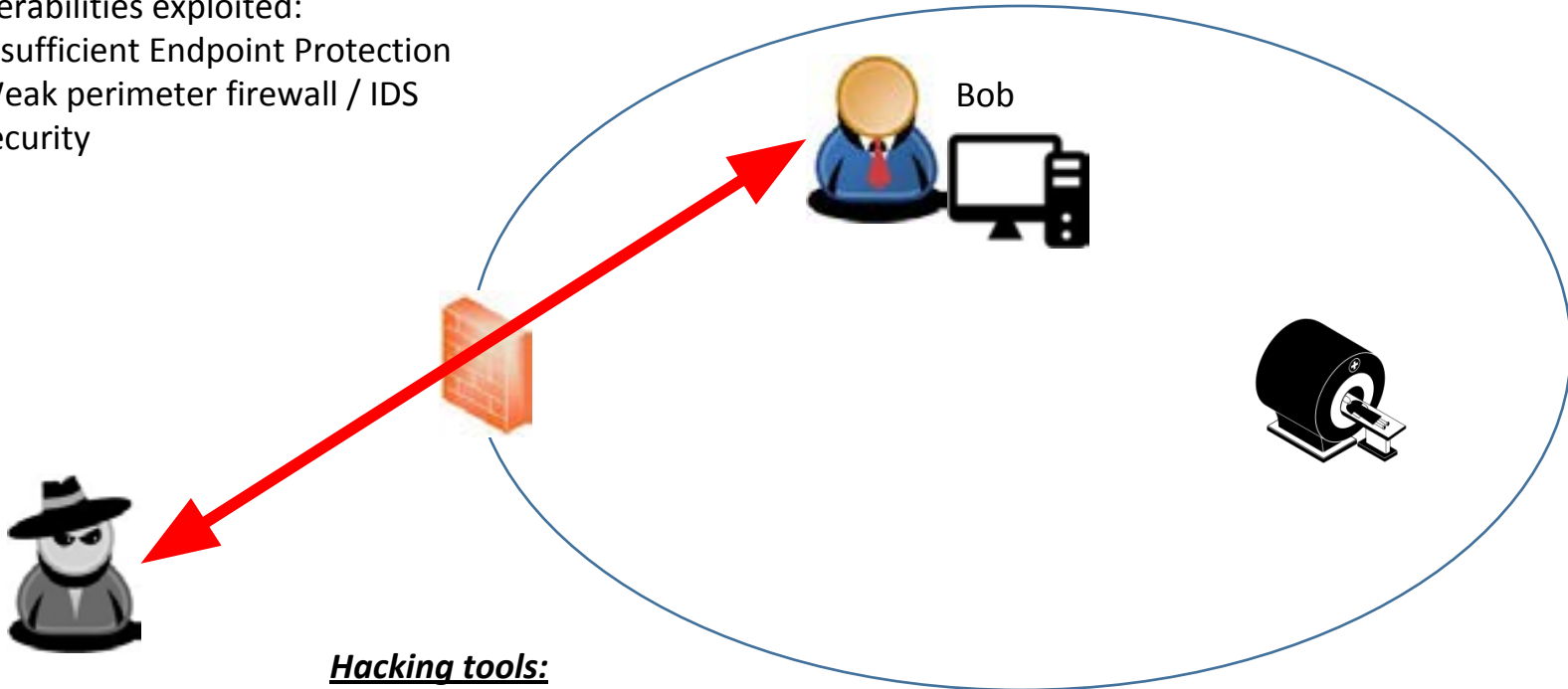
Step 1.

Gain access to intranet

Vulnerabilities exploited:

- Insufficient Endpoint Protection
- Weak perimeter firewall / IDS security

Attacker's malware is installed in Bob's machine and calls back to attacker's machine



Hacking tools:

reverse shell (msfvenom)

Scenario 1: Gain access to MRI scanner

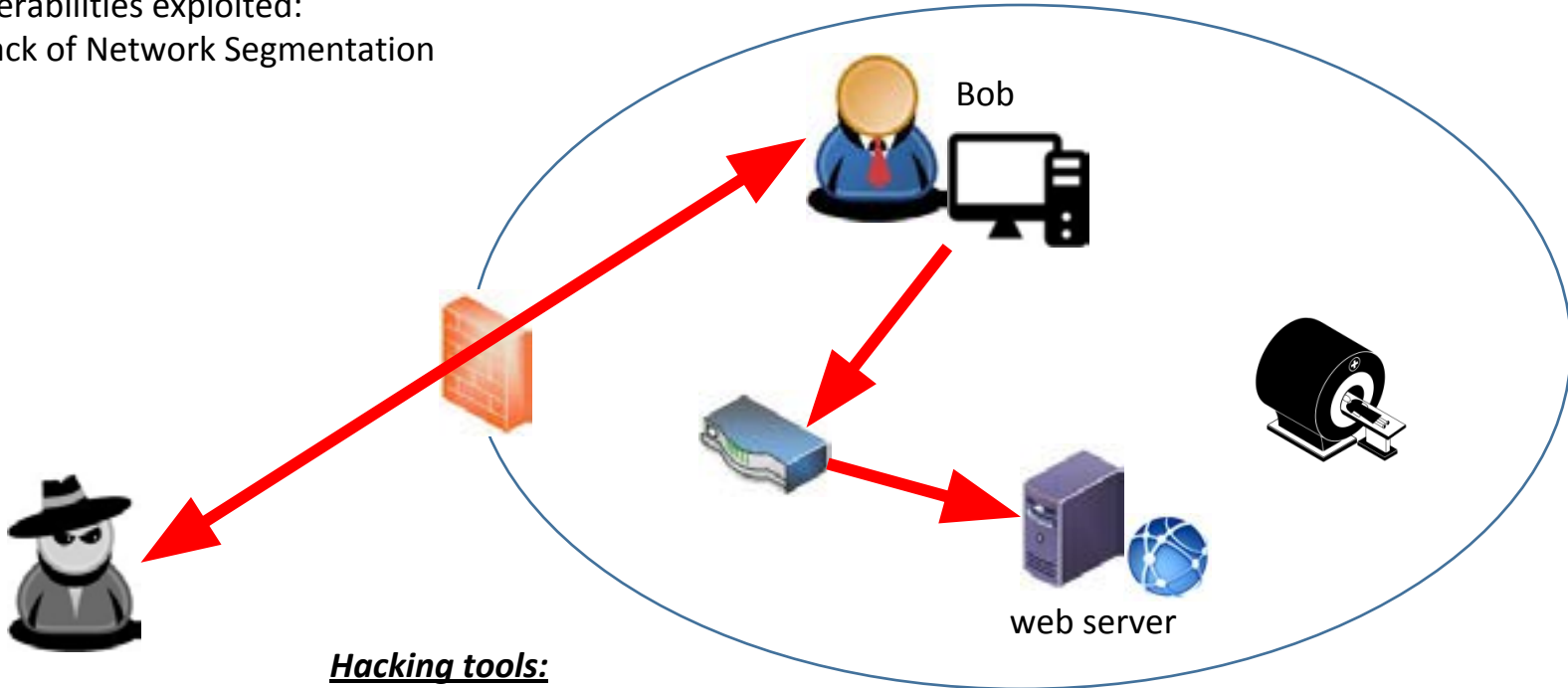
Step 2.

Gain access to web server

Vulnerabilities exploited:

- Lack of Network Segmentation

Attacker pivots to attacking the
web server that manages the MRI
device



Hacking tools:

Nmap, nikto, web browser

Scenario 1: Gain access to MRI scanner

Step 2.

Gain access to web server

Vulnerabilities exploited:

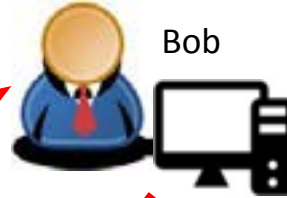
- Weak Password Policy
- Lack of Brute-force Protection
- Default Passwords

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

User Name

admin

Password



Bob

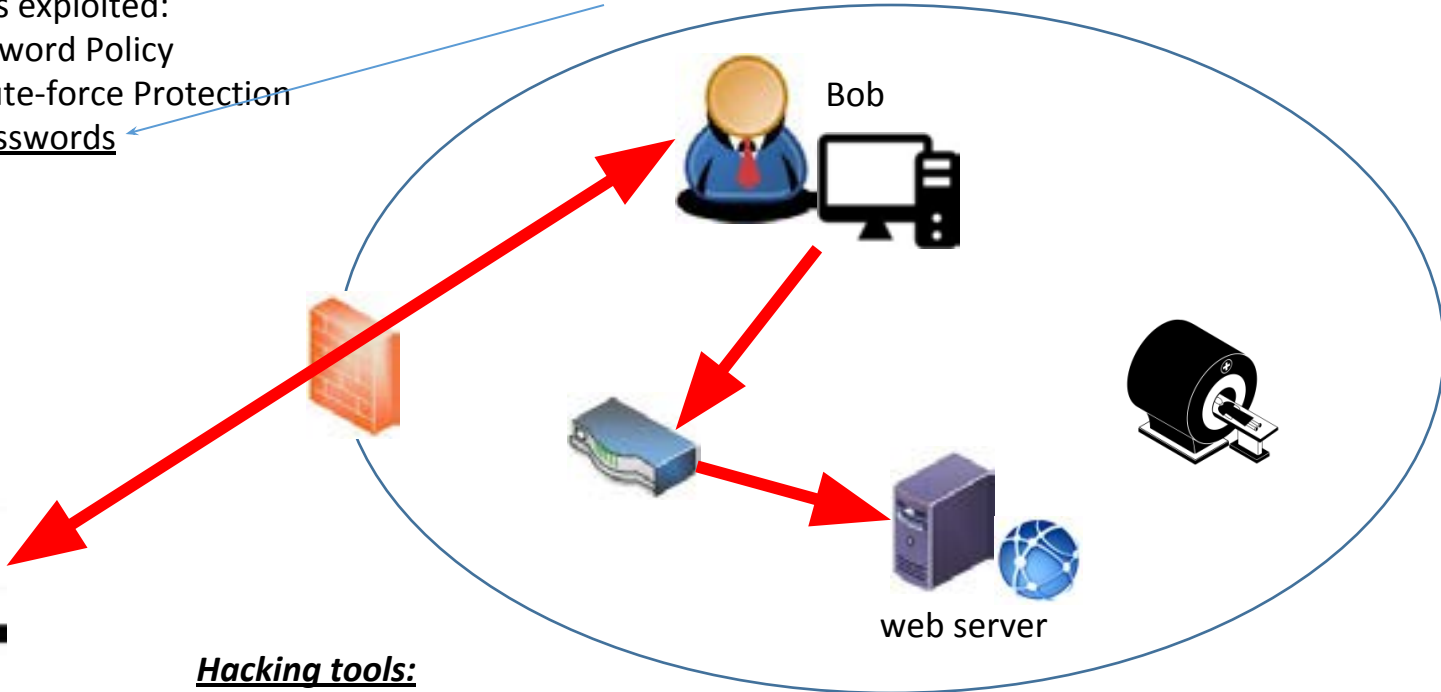


web server



Hacking tools:

Ncrack



Scenario 1: Gain access to MRI scanner

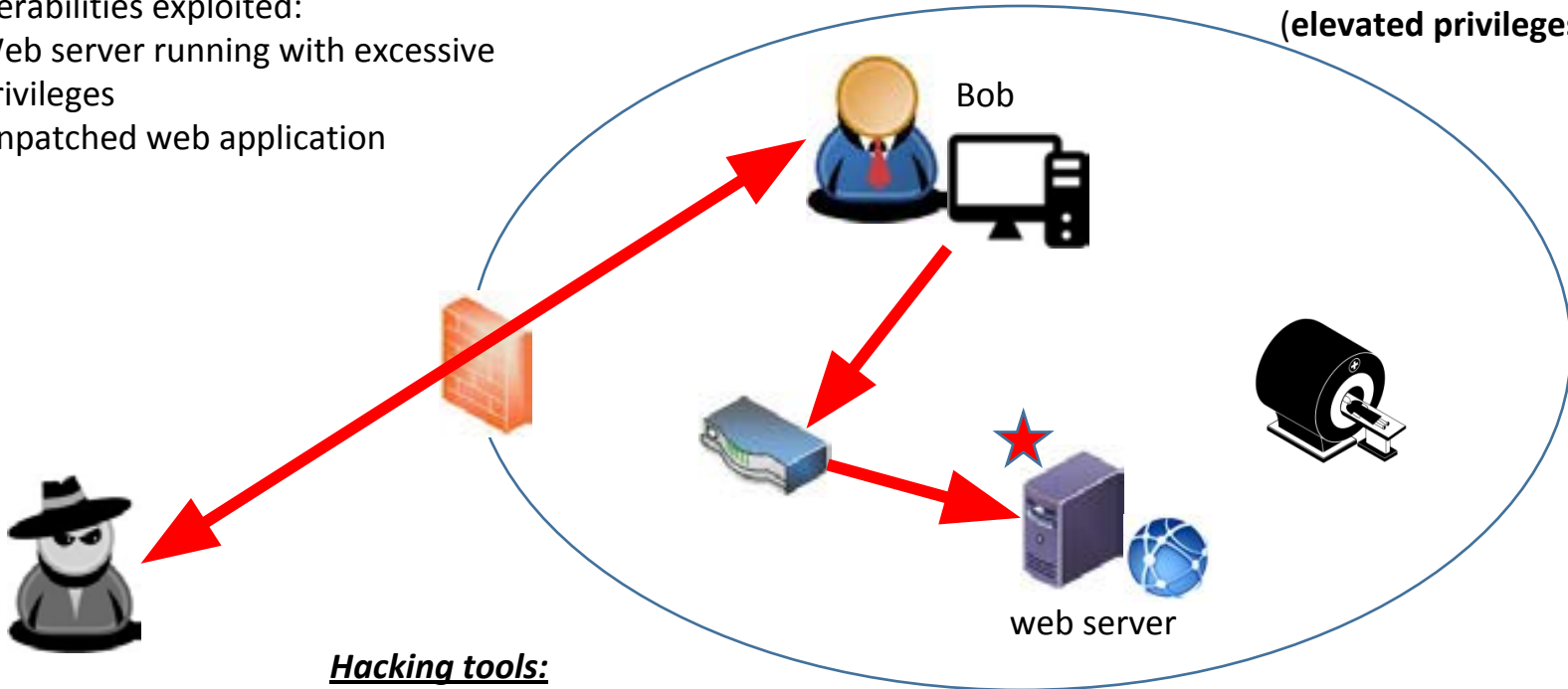
Step 3.

Elevate privileges on web server

Vulnerabilities exploited:

- Web server running with excessive privileges
- Unpatched web application

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**).



Hacking tools:

web browser, metasploit

Scenario 1: Gain access to MRI scanner

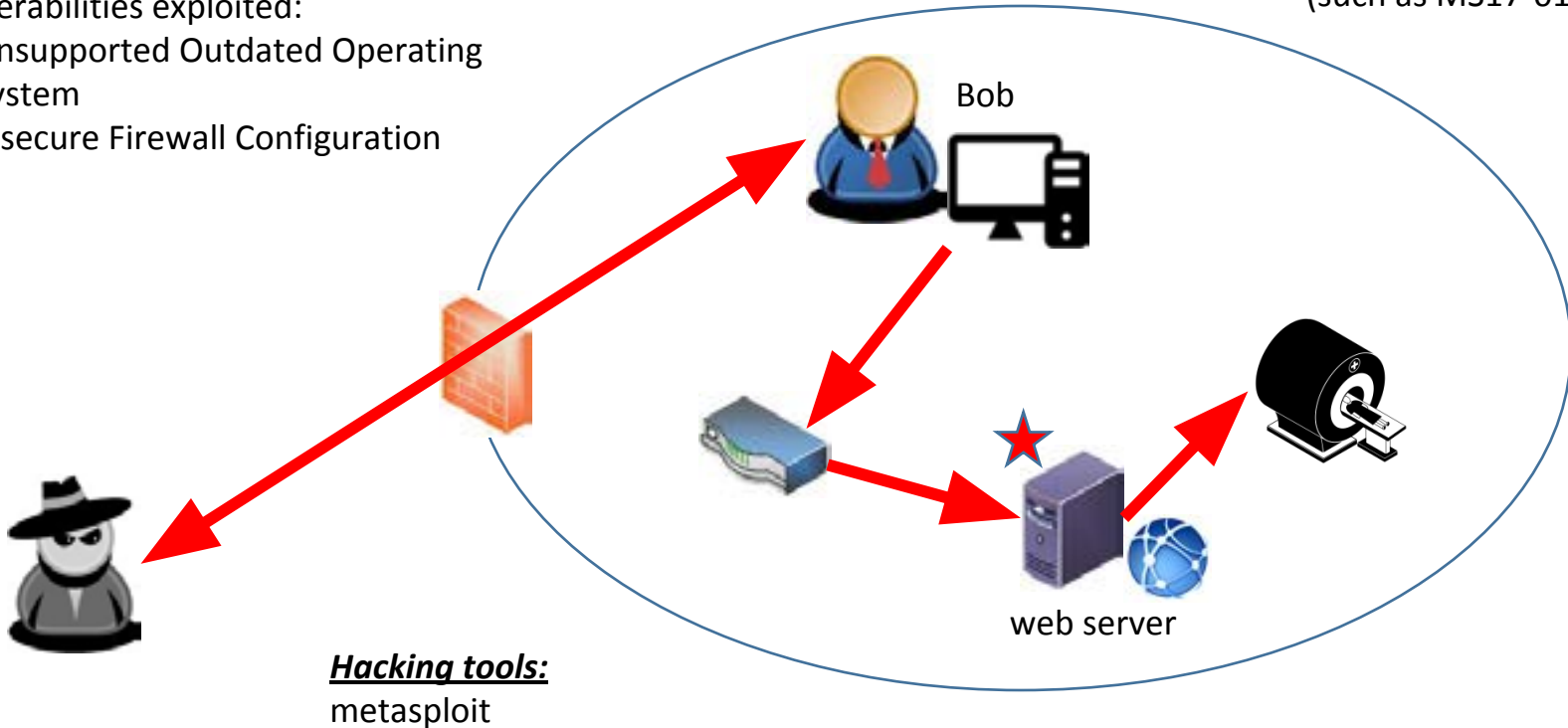
Step 4.

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)



Scenario 2: Gain access to infusion pump

Step 1.

Experiment with similar or older version of medical device

Vulnerabilities exploited:

- Hardcoded Credentials

Threat actor purchases medical device from eBay or other marketplace. They then search for hardcoded credentials.



Hacking tools:

Reverse engineering tools, **time**

Scenario 2: Gain access to infusion pump

Step 2. (optional)

Leak discovered hardcoded credentials

Vulnerabilities exploited:

- Hardcoded Credentials



online forums



Threat actor discovers
hardcoded credentials
that have been placed
**by vendor for backdoor
access**. Then they leak
them online.



deep web



Tor network

Hacking tools:

Reverse engineering tools, **time**

Scenario 2: Gain access to infusion pump

Step 3a.

Gain access to infusion pump

Vulnerabilities exploited:

- Hardcoded Credentials

(access to intranet
same as before -
phishing)

Hacking tools:

proxychains, telnet, ftp clients



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



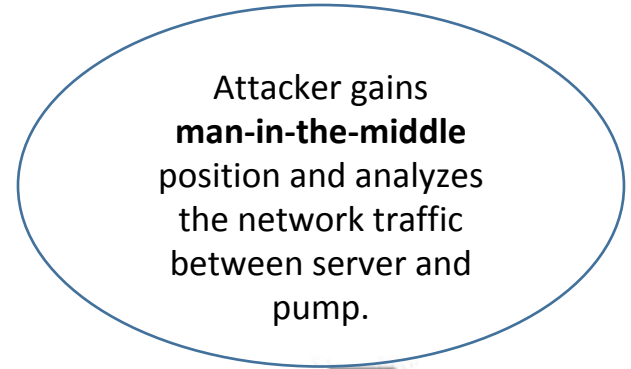
Scenario 2: Gain access to infusion pump

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



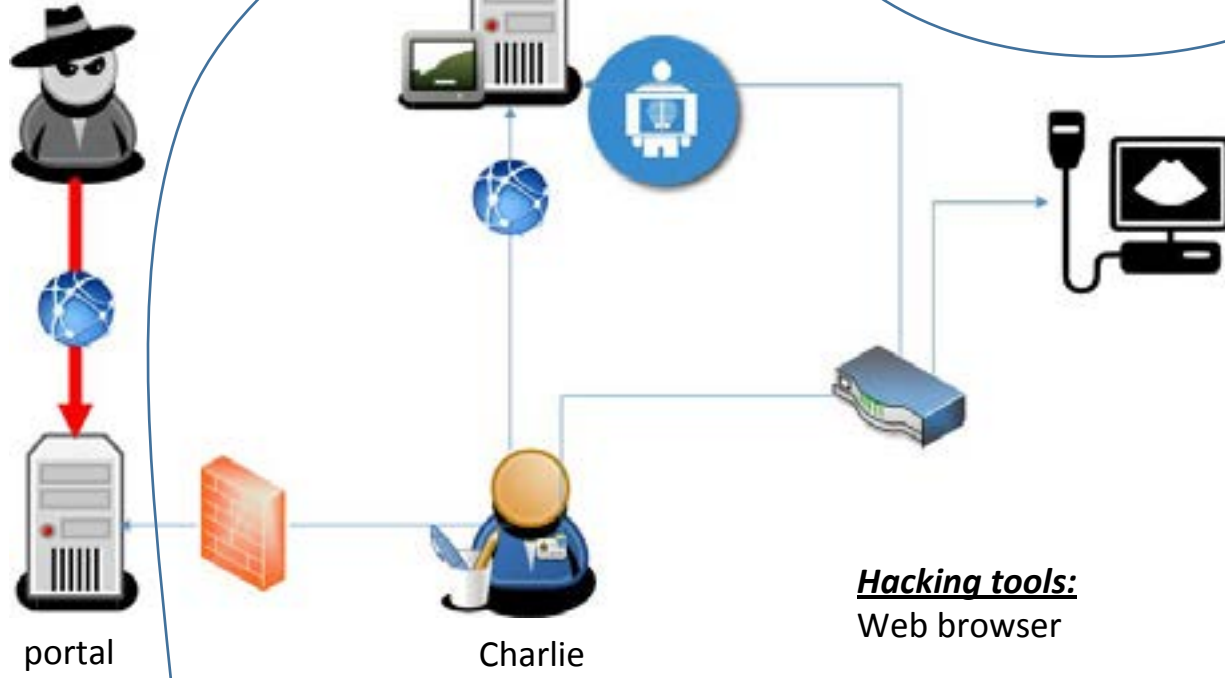
Scenario 3: Gain access to Ultrasound scanner

Step 1.

Plant XSS in publicly accessible healthcare portal

Vulnerabilities exploited:

- Stored XSS



Hacking tools:
Web browser

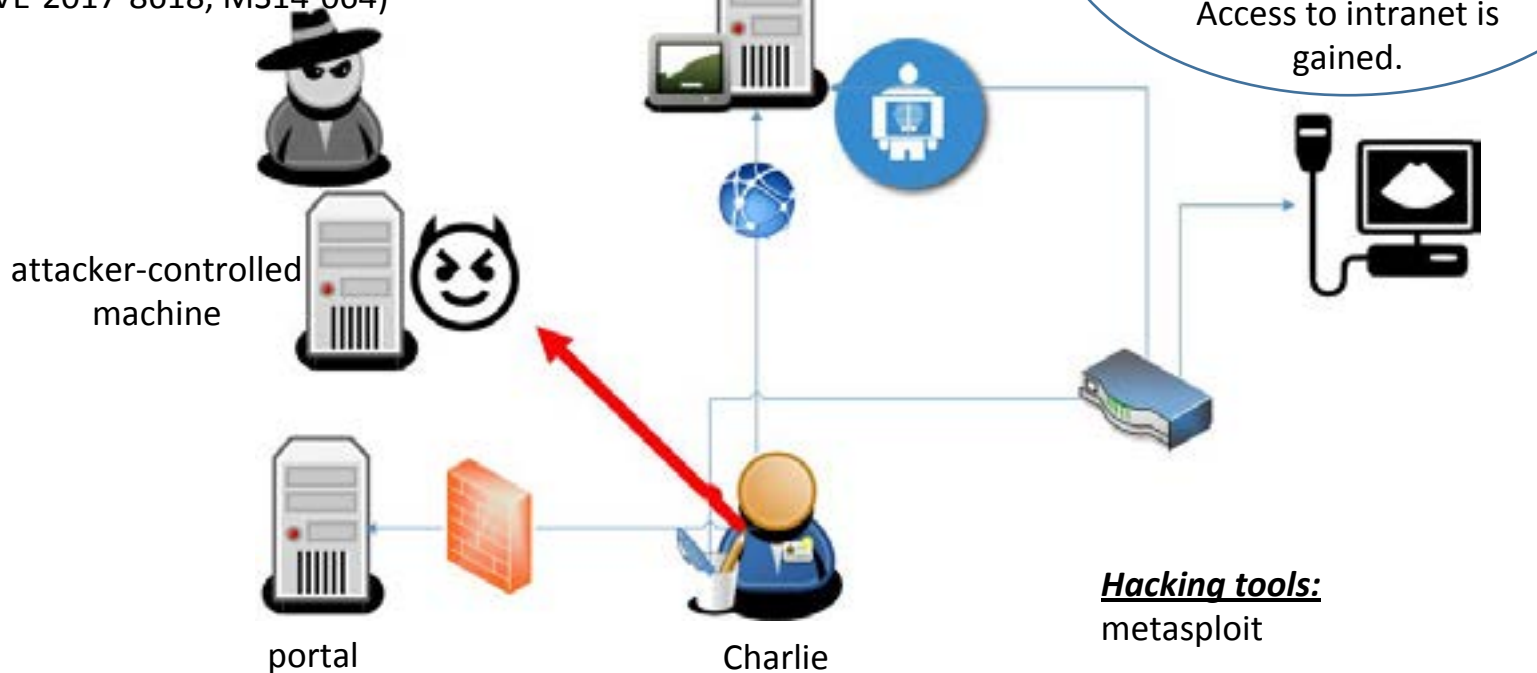
Scenario 3: Gain access to Ultrasound scanner

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)



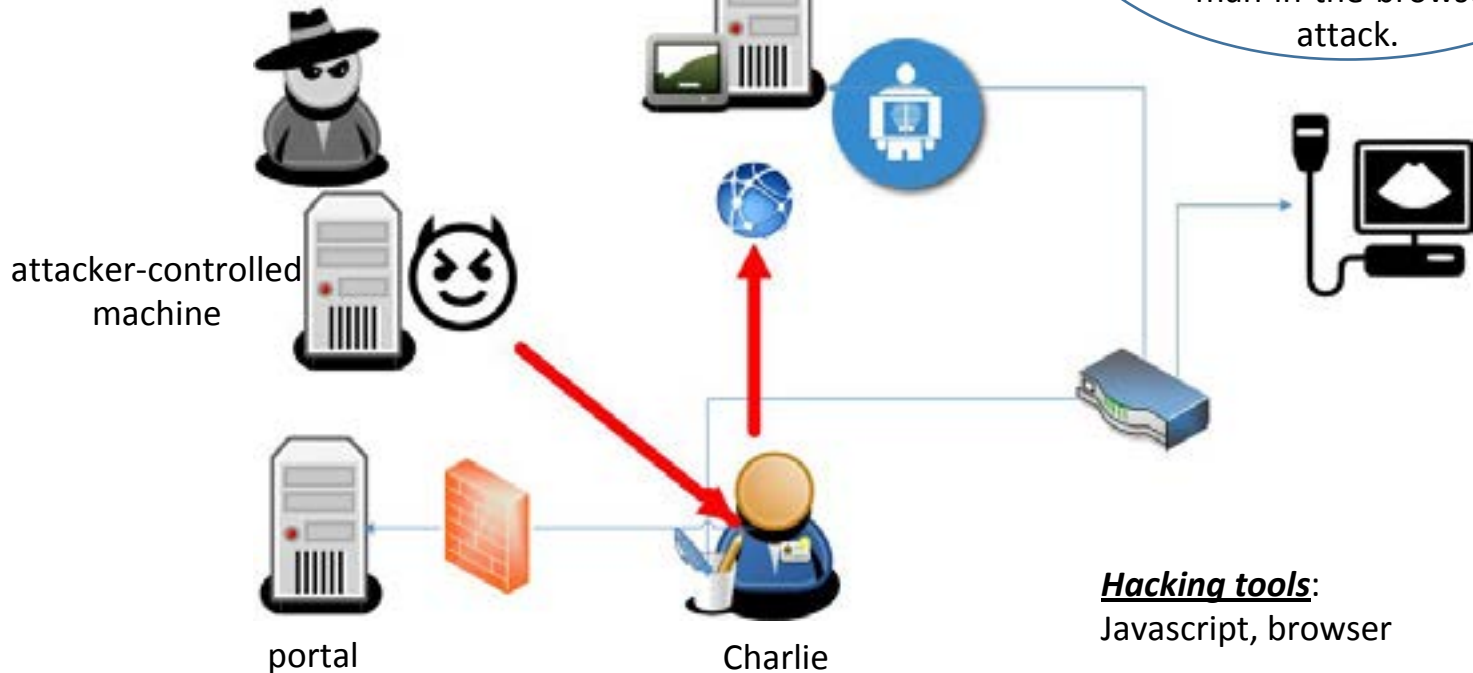
Scenario 3: Gain access to Ultrasound scanner

Step 3.

Hijack victim's PACS Server session

Vulnerabilities exploited:

- Insufficient Endpoint Protection



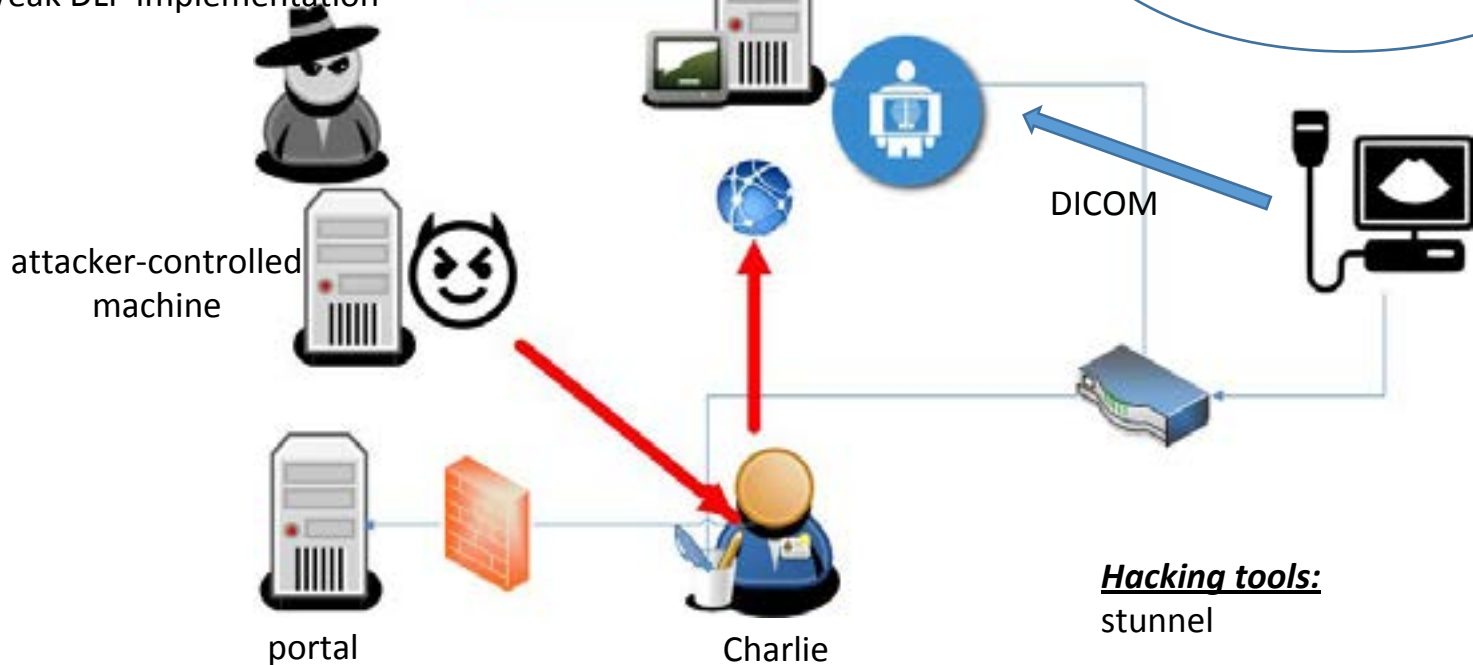
Scenario 3: Gain access to Ultrasound scanner

Step 4.

Start exfiltrating data from PACS through encrypted tunnel

Vulnerabilities exploited:

- Weak DLP implementation



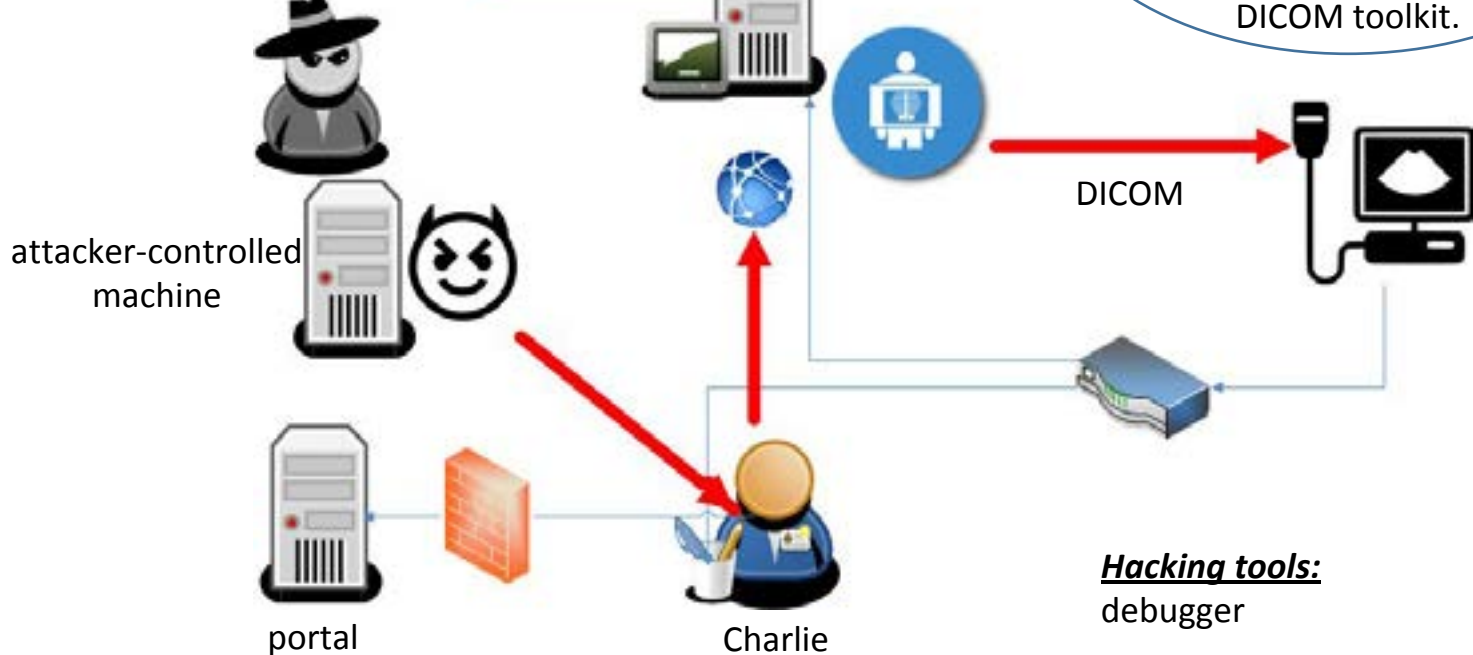
Scenario 3: Gain access to Ultrasound scanner

Step 5.

Gain access to Ultrasound system
by exploiting DICOM service

Vulnerabilities exploited:

- Buffer Overflow in DICOM service



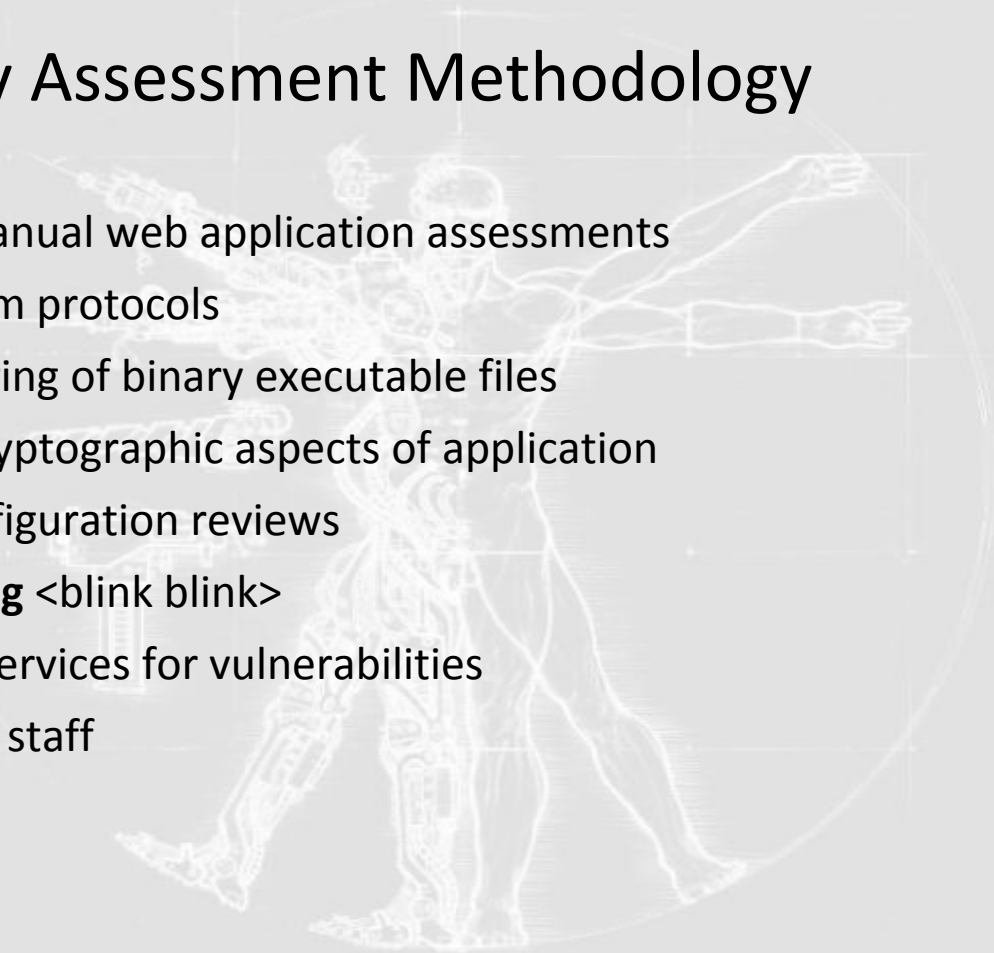
Bonus Scenario

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** <blink blink>
- 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



Hardcoded
Credentials

User Name
admin

Password

Default
Passwords



no/weak/custom
encryption



Unsupported
Operating
System



Lack of Patch
Management



Insecure
configuration



Web app
injections

Reverse engineering
of binary executable files



Assessment of cryptographic
aspects of application



Analysis of custom protocols



Manual web application
assessments



Manual host configuration
reviews



Interview vendor staff

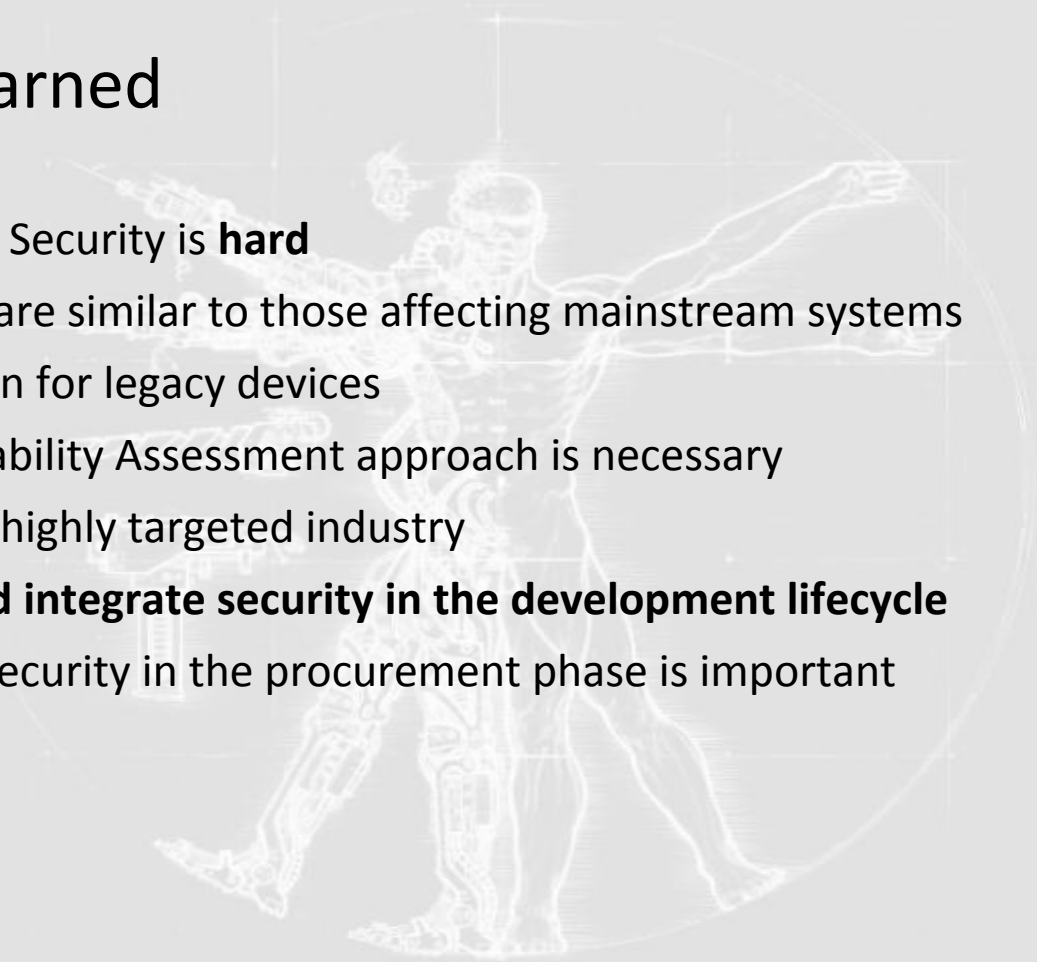


Remote scan of services
for vulnerabilities



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 - <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf>
- FDA Postmarket Management of Cybersecurity in Medical Devices - <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>
- OWASP Secure Medical Device Deployment Standard - https://www.owasp.org/images/9/95/OWASP_Secure_Medical_Devices_Deployment_Standard_7.18.18.pdf