The Emerging Threat: AI-Powered Cybersecurity Risks to Medical Equipment

Presenters: Benjamin Larson Ph.D

MDEXPO
New England • October 8-10, 2024

Who am I, and why should you listen to me?

1994-2002: US Army trained Bio-Med (Fitzsimmons)

2000: Bio-med Technician Atlantic Health System

2005-2017: Informatics Specialist Atlantic Health System

- **BS** Information Management - University of Phoenix
- **MS** in Analytics - Villanova University
- **Ph.D** in Decision Sciences – Capitol Technology University

2017-Current: Senior Mgr Data Science supporting CISO (Cyber Information Security Officer)

2021-Current: AI and Healthcare Technology Chair and researcher at Capitol

2021-Current: Adjunct Professor – Computer Science and Data Science- Raritan Valley Community College /SNHU

Quick Introduction to Cybersecurity

The practice of protecting networks and connected devices from cyber threats

In order to properly protect a network, we first need to understand the threat landscape.

In this presentation, we will cover the following topics:

- Threat Actors
- Attack Vectors
- Quick intro to AI
- AI Enhanced Cyber Threats
- Unique Problems Facing Medical Devices
- Suggestions to reduce exposure and harden the network

Quick Introduction to Cybersecurity

What are the threat actors:

A Threat Actor is a person or group intent on causing harm to a network and devices on the network.

- Individuals
- Groups
- State Sponsored Entities

What are attack vectors:

A method that cybercriminals use to gain access to network and resources

- Social Engineering
- Malware
- Ransomware
- DDoS
- Drive-by/Sideloaded downloads
- APT

Quick Introduction to Cybersecurity

Who are the threat actors:

Script Kiddies: Usually new to hacking. They use existing code and tools available online to attempt to attack a network vulnerability.
Usually motivated by the thrill.

Insiders/Former Employees: Can be especially dangerous.

- Inside knowledge as to network and assets
- May have advanced credentials
- Profit/Revenge motivated

Quick Introduction to Cybersecurity

Hacktivist: Usually politically motivated.

Anonymous is probably most well known

Examples of attacks:

Oil/Energy Companies

Ukraine/Russian

Political Campaigns

Quick Introduction to Cybersecurity

Cybercrime Syndicates: Driven by monetary gain. Operate much like organized crime syndicates. Operate out of countries known to turn blind eye to financial crimes (Eastern Europe, Africa)

Example: **Scattered Spyder**

Ransomware
Data Theft
Account Theft

Quick Introduction to Cybersecurity

State Sponsored Groups:
These groups are well funded and well trained. They specialize in Intelligence gathering, sabotage, political destabilization
(China, North Korea, Russia, Iran, Ukraine)

DDoS
Ransomware
Malware
APT

Quick Introduction to Cybersecurity

What are threat vectors?

Method or mechanisms used by attacker to:

- Steal Information
- Launch malware/ransomware attacks
- Damage or completely take down systems
- Take control of a system.

Quick Introduction to Cybersecurity

Drive-By attack methods:

No User Interaction: User visits a compromised page and the malware download/install starts without any user interaction.

With User Interaction:

- Pop up ads may use a false X or Close button that really triggers a download
- A legitimate looking link on a website/app/ or email is compromised
- Email attachments that look legitimate may include hidden malware

Quick Introduction to Cybersecurity

Social Engineering: tactics and techniques designed to trick a user into giving away sensitive information or performing actions for the attacker.

Common Examples:

Phishing – attacker sends out emails disguised as though they are from a legitimate source in an attempt to lure user into believing the email is real

Smishing – Utilizing SMS messaging services (text messages) to trick users

Vishing – Attacks using voice over phone lines. Becoming more concerning as Deepfakes are improving

Qishing – altering QR codes to redirect victims to a malicious website without their knowledge.

Quick Introduction to Cybersecurity

APT (advanced persistent threats):

This attack exists when a threat actor manages to gain control of a network and remains undetected for a long period of time.

These are the most sophisticated attacks.

Require highly skilled attacks with lots of resources.

Often these attacks are pulled off by state sponsored groups.

Quick Introduction to Cybersecurity

What are some common attacks:

Malware
Ransomware
DDoS
Man-in-the-middle

Quick Introduction to Cybersecurity

What are some common attacks:

Malware: Malicious Software designed to disrupt, damage or gain control of computer system.

Ransomware: software that hijacks a system, making it unusable. A common method is to encrypt data found in the system. The data can only be decrypted after a ransom is paid by the victim.

Quick Introduction to Cybersecurity

What are some common attacks:

DDoS: Distributed Denial of Service attacks is the use of hundreds or thousands of Devices (often zombie devices) to overwhelm a target server or system with an assault of network requests. The server quickly becomes unusable as it cannot reply to all the coordinated requests.

Man-in-the-Middle: the bad actor positions themselves between the user and the system/application. Sometimes they simply listen in and collect information, other times they will interact with the user, pretending to either be part of the application or a member of IT staff.

Quick Introduction to Artificial Intelligence

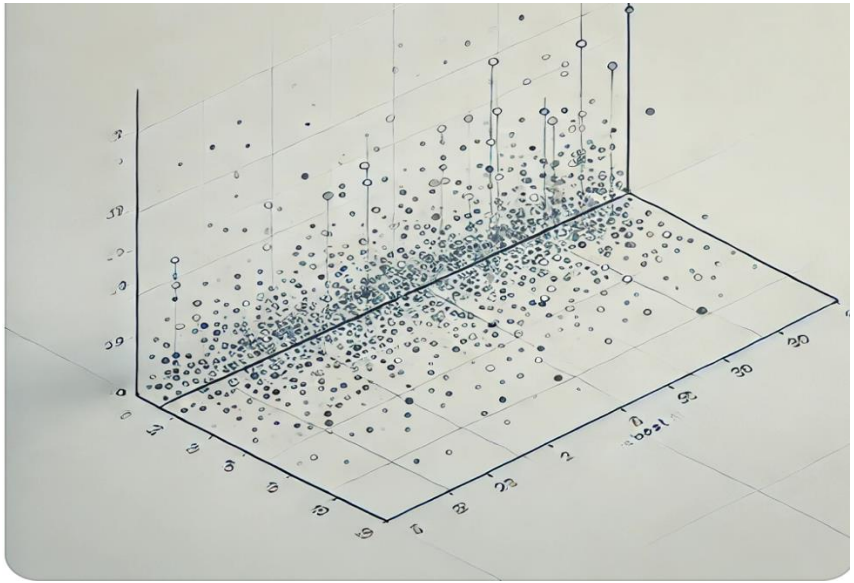
Machine Learning/Data Mining
Deep Learning
Narrow AI vs AGI (artificial general intelligence – doesn't exist yet)
Generative AI
Computer Vision
Deep Fakes

Machine Learning/Data Mining: Machine learning is the use of algorithms that can train themselves using data.

Supervised Machine Learning: Uses labeled datasets to find patterns in data that will aid in creation of a predictive model.

Examples: **Regression Models** – look to return a continuous value (price of house, salary)

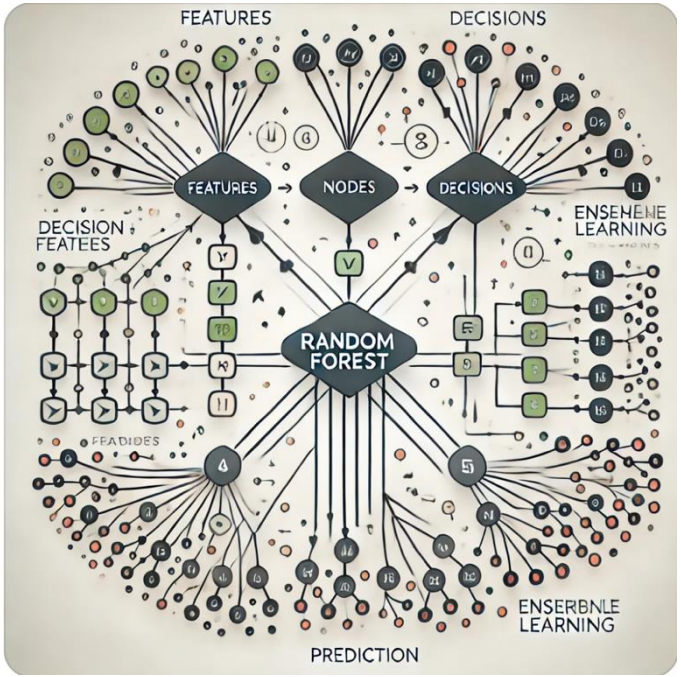
- Linear Regression
- Lasso Regression
- Bayesian Regression
- Regression Trees



MDEXPO
New England • October 8-10, 2024

Machine Learning/Data Mining: Machine learning is the use of algorithms that can train themselves using data.

Supervised Machine Learning: Uses labeled datasets to find patterns in data that will aid in the creation of a predictive model.



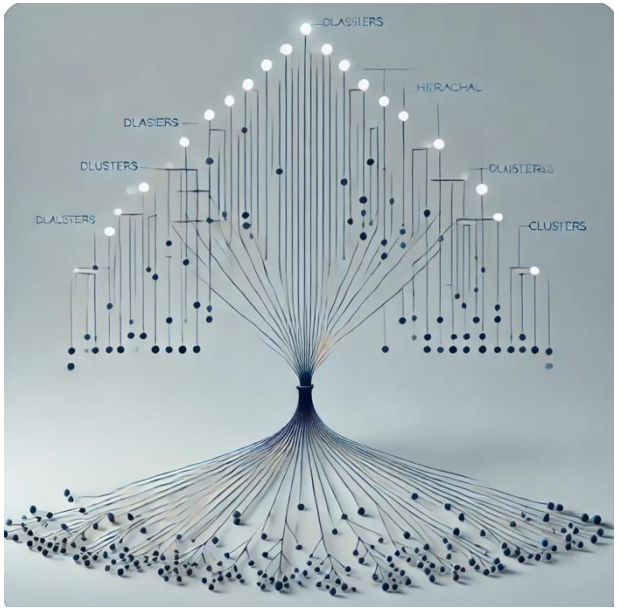
Examples: **Classifier** (returns discrete values – True /False – 0/1 – 1st/2nd/3rd)

- Logistic Regression
- Random Forest
- Neural Networks
- KNN
- XGBoost

MDEXPO
New England • October 8-10, 2024

Machine Learning/Data Mining: Machine learning is the use of algorithms that can train themselves using data.

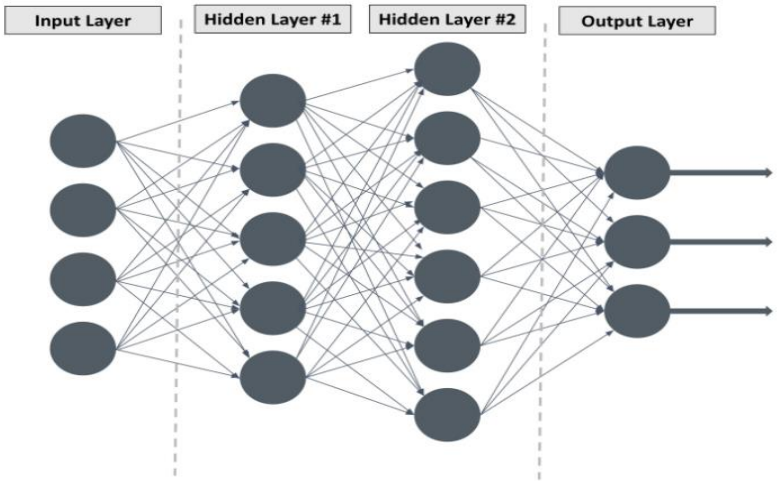
Unsupervised Machine Learning: Uses unlabeled datasets to find patterns in data related to grouping Or hierarchies



- K-means Clustering
- Hierarchical Clustering
- Association
- Dimensionality Reduction
- PCA

Data mining is often used in conjunction with **ML**, however they are completely different things. Whereas ML is designed to be automated, with a computer teaching itself. Data Mining is the interactive man-in-the-middle approach of data analysis

Deep Learning



A simple artificial neural network

Focused on the use of Neural Networks to try to teach a computer to think like a human.

It attempts to view the world in layered hierarchies

The hidden layers in a NN first loosely classify data into low level categories and develop higher level categories with each iterative run in the model

Narrow AI vs AGI

Narrow AI is focus on single task or group of tasks

- Chatbot
- Self-Driving Vehicles
- Language Translators
- Fraud Detection Systems

AGI – **Artificial General Intelligence** is the goal of AI development. It is the idea of an AI that Can think and act within the limits of human cognitive capabilities. (Doesn't EXIST YET)

Generative AI

AI designed to generate written, spoken, visual, and musical media through user prompts

- Built on massive data sets
- Completely self unaware – basically a matrix multiplication problem
- Can mimic human created writing/visual arts/speech
- ChatGPT – Gemini

Computer Vision: branch of computer science dedicated to teaching computers to interpret visual information like the human brain does.

Deepfakes: realistic video, image, or audio that have been manipulated using AI to create fake events such as creating a video of a person give a speech they did not give.

AI Cyber risks ?

Optimized Attacks using GenAI
Malware Development
Automation/ Scale Up attacks
Data Summation

Optimized Attacks using Gen AI

Generative AI (such as LLMs) adds a new level of threat. Phishing/Smishing/ Vishing attacks can not only be scaled out to unseen levels, but can be used to personalize email and SMS attacks, making their detection that much more difficult. (Guembe et al., 2022)

Gen AI's ability to quickly read through large corpuses of information/ finding patterns in data that might help an attacker find flaws in cloud architecture.

They can also be used to take advantage of sudden events worldwide to push geopolitical destabilizing messages via email, SMS, or social media.

Malware development

Gen AI is very helpful when it comes to rudimentary programming, and it will continue to get better. While LLM companies do have some guardrails up, researchers have been able to by pass safety features allowing them to use ChatGPT to create advanced Malware.

This lowers the bar to entry, allowing people with limited coding experience to potentially create advanced malware/ransomware. (Kaloudi, Li 2020)

Automate / Scale Up

AI is already being used to scale up and automate more personalized social engineering attacks. From Phishing and Smishing attacks that not only look legitimate, but are personalized to the receiver, to the use of deepfake technology to mimic voices familiar to the potential victim.

AI will also allow for automated/scaled up vulnerability exploits. ML will make the automated attack smarter and more focused on the victim network as it learns. (Guembe et al., 2022)

Data Summation/ Data Theft/Poisoning

AI's ability to summarize data make it a great tool for analyzing vast stores of data on a network and quickly determining high value targets (NCSC)

Once the AI intruder can identify the data sources, it can be guided to steal / encrypt / or poison the data (where data used to train AI systems is intentional corrupted to make the ML models either fail or return intentional false information)

AI will also allow for automated/scaled up vulnerability exploits. ML will make the automated attack smarter and more focused on the victim network as it learns. (Guembe et al., 2022)

Clinical Engineering Concerns

HTM Departments are limited by a few constraints:

- IT department limits what you can do
- Vendors limit access to certain configuration
- FDA Regulations limit what can be done to software/hardware

HIPPA violations can be costly (both in penalties and brand reputation)

Small devices like IV pumps can connect to networks via WIFI and Bluetooth

Clinical Engineering Concerns

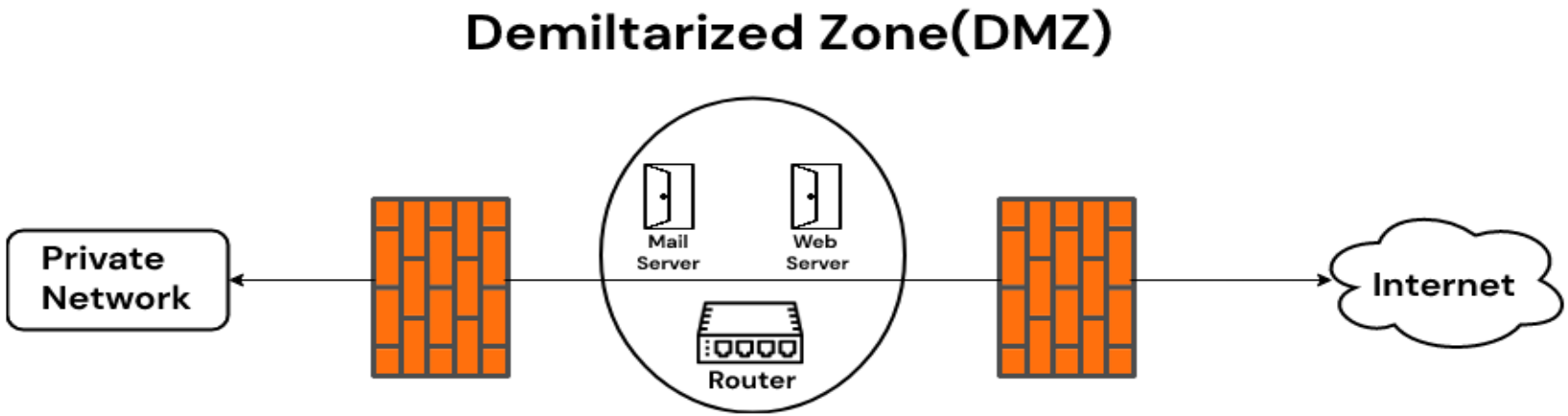
MDEXPO
New England • October 8-10, 2024

IT department limits what you can do:

IT usually owns the network, leaving CE departments at their mercy

- Try to segment your networks utilizing Firewalls
- Segment WIFI
- Ask about network/event logging

*Clinical Engineers need to be the advocate for placing patient safety first



Clinical Engineering Concerns

Vendors limit access to certain configuration:

- Some vendors still use universally known Admin passwords:
  - Search of Reddit forums show people requesting and sharing passwords
  - LLMs will make finding these passwords even easier
- Vendors may not let you turn off certain features (ex Bluetooth or WIFI)
- USB protections may not be activated
- Unused ports are often still “On”

Clinical Engineering Concerns

FDA Regulations limit what can be done to software/hardware:

Software is part of the FDA approval process, meaning there are limits what can be done to harden software.

Can default passwords be changed?

Can antivirus software be installed?

Can unused ports be disabled?

Can remote access be disabled?

Clinical Engineering Concerns

HIPPA violations can be costly (both in penalties and brand reputation)

Beyond patient financial information, the threat of patient care data theft of great concern.

AI can help cyber criminals quickly summarize data on a network. This will make spotting celebrities or other VIPs that may have been patients.

AI can also help attackers focus on specific treatments. Knowing who is receiving treatment for STDs, mental health, or addiction services, provides threat actors with a list of potential blackmail targets.

Clinical Engineering Concerns

Small devices like IV pumps can connect to networks via WIFI and Bluetooth

IoT (Internet of Things) is focused on these small, generally unsophisticated devices.

IoT devices often lack much in the way of security. Many have default Root passwords that can easily be found.

The lack of security means these devices are more susceptible to brute force attacks

They can be turned into zombie or bots and used in DDoS attacks

Since they ride on the network, a single compromised IoT device can compromise an entire network.

Protect Yourself:
Step 1: Conduct a Risk Assessment

- Identify vulnerable devices and systems
- Evaluation the potential import of a cyberattack on patient safety
- Prioritize devices based on risk level
- Regularly update the risk assessment to account for new threats
- Improve Knowledge Management (Morse, 2024)

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 2: Implement Access Controls

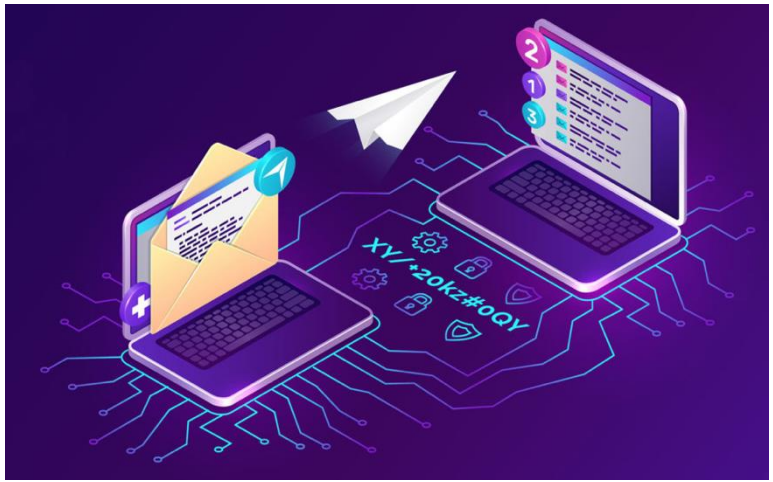
- User Authentication: Require strong passwords and MFA if possible
- Role-Based Access: Limit device access to authorized personnel
- Logging: Monitor access logs to detect suspicious activity

Tips: Don’t use single admin accounts, each admin should have a unique login
Change default passwords where possible (a quick look at Reddit and Facebook showed me plenty of instances of someone asking for an admin password for a device and people sending it)
Even admins should have a non-admin account that is used for most day to day work

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 3: Secure Communications

- Encryption: Use encryption for data in transit and at rest
- Network Segmentation: Separate medical devices from other networks (don’t put on guest WiFi)
- Firewall Protection: Use firewalls. Create DMZs to protect your equipment (Kaloudi & Li, 2020)



MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 4: Regular Software Updates

- Apply security patches and software updates when available
- Ensure vendors supply timely security updates
- Automate updates where possible.

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 5: Implement Intrusion Detection Systems (most likely IT job)

- Deploy intrusion detection systems (IDS) to monitor for unusual activity
- Implement real-time monitoring for signs of attacks
- Set up alerts for suspicious behaviors, such as unauthorized access attempts

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 6: Incident Management Plan

- Develop a clear incident response plan
- Define roles and responsibilities during a cyber incident
- Regularly conduct drills to prepare for cyberattacks on medical devices

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 7: Vendor Management & Collaboration

- Ensure vendors adhere to cybersecurity best practices
- Request cybersecurity certifications from device manufactures
- Engage in open communication with vendors to address vulnerabilities

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Step 8: Employee Training & Awareness

- Train healthcare staff on cybersecurity best practices
- Create awareness around phishing/smishing and other social engineering attacks
- Encourage employees to report suspicious behavior or potential threats.

MDEXPO
New England • October 8-10, 2024

Protect Yourself:
Conclusion

- A multi-layered approach is key to protecting medical devices and patient safety
- Regularly assess and update security measures
- Collaborate across departments and with vendors to stay resilient

MDEXPO
New England • October 8-10, 2024

Questions?

My Contact Info:

Benjamin Larson Ph.D
bjlarson@captechu.edu

https://www.linkedin.com/in/benjamin-larson-phd-8903a647

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, *36*(1), 1–34. https://doi.org/10.1080/08839514.2022.2037254

Kaloudi, N., and J. Li. 2020. The AI-based cyber threat landscape. *ACM Computing Surveys* 53 (1):1–34. doi:10.1145/3372823.

Morse, R. (2024). A Qualitative Study of Cybersecurity Risk Management Framwork: Lack of Knowledge Management and Systemic Risk: Preprint

The near-term impact of AI on the cyber threat. NCSC. (n.d.). https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

MDEXPO
New England • October 8-10, 2024