

What Could Go Wrong?

Threat Modeling Considerations in Medical and IoT Devices

2025/01/11 Trevor Slattery Blue Goat Cyber



Blue Goat Cyber

We Provide Full-Service Medical Device
Submissions & Postmarket Management





Introduction

Trevor Slattery joined Blue Goat Cyber in 2022 and serves as the Director of Medical Device Cybersecurity. A former penetration tester and security researcher, Trevor specializes in medical device security and has identified dozens of 0-day vulnerabilities in critical healthcare technologies.

He holds a background in application security and regulatory affairs, bringing a unique blend of technical expertise and strategic insight to safeguard patient safety and ensure regulatory compliance.

Medical Device Expertise

- Infusion Pumps
- Blood Glucose Monitors & Insulin Pumps
- Wearable ECGs & Remote Patient Monitors
- Pacemakers and Defibrillators
- Ventilators & Critical Care Machines
- Networked Surgical Robots & Deep Brain Stimulators



Why is Threat Modeling Important for Medical Devices?



- Major Impact: 53% of medical devices in 2022 had a known critical vulnerability
- Constant Attacks: 89% of facilities dedicated to healthcare experience around one cybersecurity attack per week



Examples of Medical Device Vulnerabilities

- Medtronic Insulin Pump Recall – Vulnerabilities allowed attackers to alter insulin delivery remotely, posing life-threatening risks
- St. Jode Pacemakers – Flaws allowed hackers to interfere with functionality such as battery depletion or pacing modification
- WannaCry Ransomware – Attack affected MRI machines and other medical equipment, demonstrating the severe impact of ransomware on connected devices



Why is Threat Modeling Important?

Threat modeling explores hypotheticals for devices and helps build out plans for building security into a device



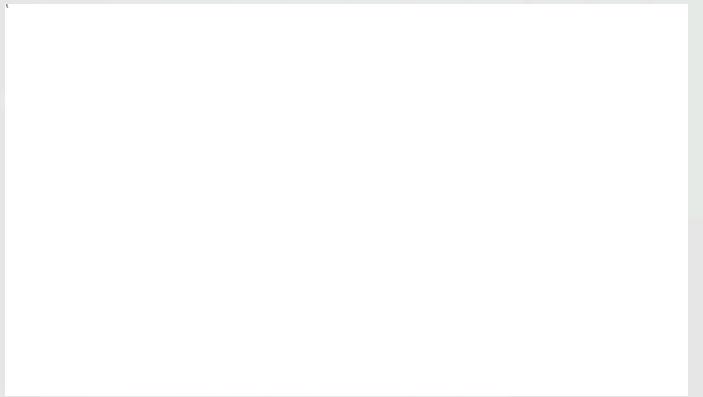
Threat modeling early and often contribute to security by design and reduces the chance of costly oversights



The 4 Questions:

Main Considerations

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?



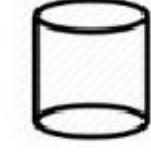
What are we working

Exploring the device itself on?

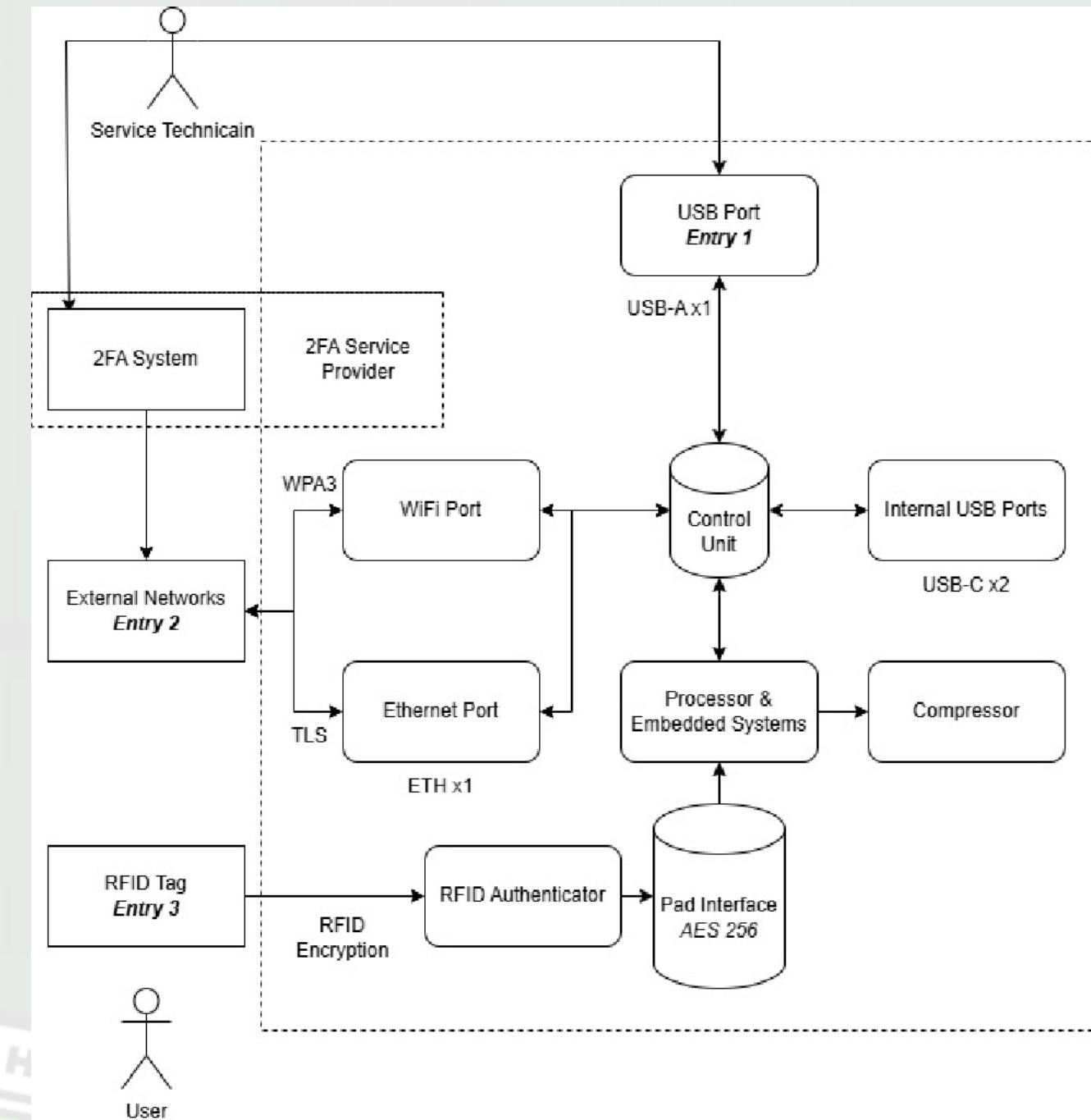
- What does the device do?
- What physical components are there?
- What logical components are there?
- What should the device not do?
- What environment should the device be in?



DFD3 Specification

Element	Symbol	Discussion
External entity		A sharp-cornered rectangle. Anything outside your control. Examples include people and systems run by other organizations or even divisions. For example, Joe's mobile phone, the Mint data aggregators (assuming you're modeling from a bank's perspective.). If you're modeling Mint, then the bank's systems would be external entities.
Process		A rounded rectangle. Any running code, including compiled, scripts, shell commands, SQL stored procedures, et cetera.
Data store		A drum. Anywhere data is stored, including files, databases, shared memory, S3, cookies, et cetera.
Data flows		An arrow. All the ways that processes can talk to data stores or each other.
Trust boundary	...	A closed shape drawn with a dashed or dotted line. Usually a box.

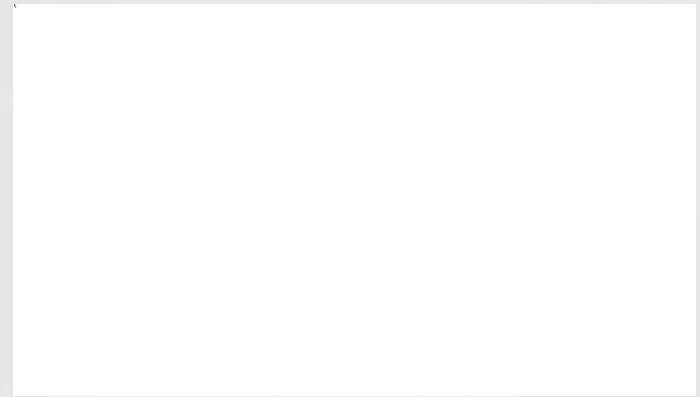
Threat Modeling Diagram Example



What can go wrong?

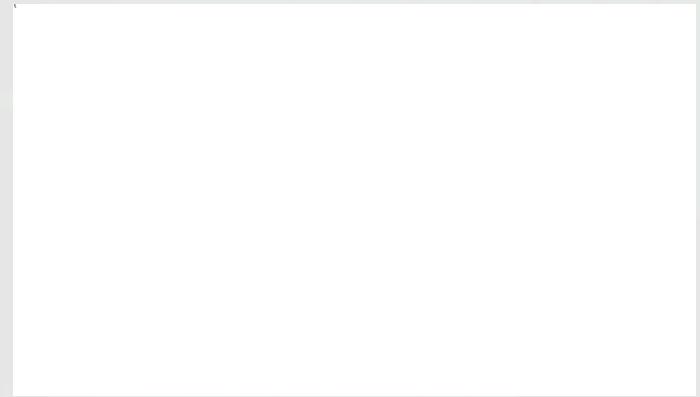
Developing Threats

- What is the intended use?
- What is the unintended use?
- What are the environmental concerns?



Threat Modeling Frameworks

- STRIDE
- PASTA
- DREAD
- ATT&CK
- OWASP Top 10



Using STRIDE for Physical Devices

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Mapping Threats to Categories

Threat	Category
The database contains sensitive information	Information Disclosure
Users can change other users' passwords	Tampering, Repudiation
Alternative OSes can be sideloaded from USB	Information Disclosure
Update notifications are sent from a phishing email	Spoofing

Mapping Categories to Threats

S	T	R	I	D	E
Update notifications are sent from a phishing email	Users can change other users' passwords	Users can change other users' passwords	The database contains sensitive information		
			Alternative OSes can be sideloaded from USB		

What are we going to do about it?

Creating Solutions



- How can threats in the system be mitigated?
- How can we reduce likelihood?
- How can we reduce impact?



Mapping Threats to Solutions

Threat	Solution
The database contains sensitive information	Databases are encrypted and access is controlled
Users can change other users' passwords	Proper access control is implemented and verified
Alternative OSes can be sideloaded from USB	BIOS settings are protected and USB devices whitelisted
Update notifications are sent from a phishing email	Device labeling has anti-phishing information

Did we do a good job?

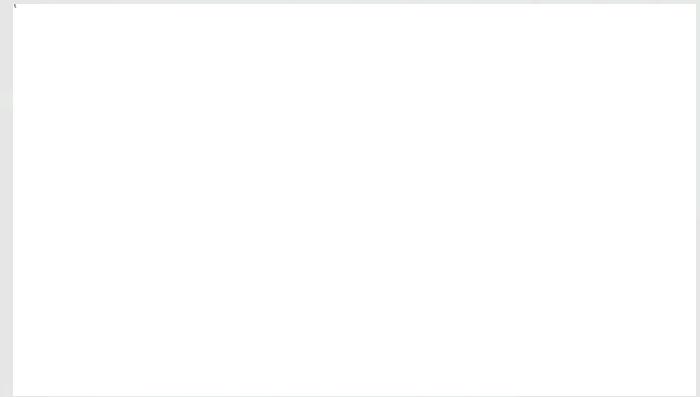
Process Review

- Did we miss any threats?
- Was our threat modeling framework appropriate?
- Are our mitigations sufficient?



Validation of Completion

- Penetration Testing
- Risk Assessments
- Overall Risk Management



Key Takeaways

- Threat modeling should be done early and often
- Review all modeling activities
- Diagrams should cover relevant details
- Methodologies should be carefully chosen
- Threat modeling should be validated with testing and risk assessments



Questions?

www.bluegoatcyber.com



trevor.slattery@bluegoatcyber.com

linkedin.com/in/trevor-slattery-34852b1a9



THANKS

