“There are rabbit holes I want to go down that I’m not allowed to go down”: An Investigation of Security Expert Threat Modeling Practices for Medical Devices

Ronald E. Thompson III, Madeline McLaughlin, Carson Powers, and Daniel Votipka

Tufts UNIVERSITY

Motivation

A need to understand the actual ways security experts threat model in practice

Threat modeling is critical part of ensuring safe and secure medical devices

Developing better tools and methods requires understanding how experts navigate threat models

Research Questions

How do medical device manufacturers security experts identify specific threats & mitigations?

What processes do MDM security experts follow when navigating a system’s design to identify threats?

Participants

We interviewed 12 experts involved in securing medical devices

Participants started their careers in...
...medical devices (6)
...security (6)

Participants hold roles in/as...
...large manufacturers (4)
...specialized manufacturers (4)
...consultants for manufacturers (4)

Participants had worked for...
...<5 years (2)
...5-10 years (1)
75% >10 years {
...10-20 years (2)
...20-30 years (4)
...30+ years (3)

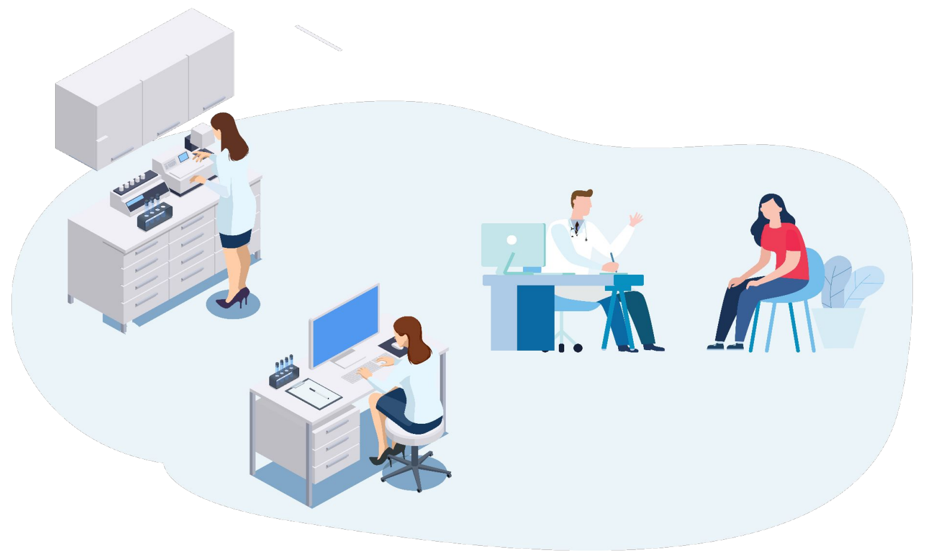
Medical Device Scenarios - Participants were shown two scenarios

Robotic Surgical System

Type: Surgical System
Setting: Hospital
Potential Harm: Patient Death
Classification: Class II

Next-Gen Sequencer

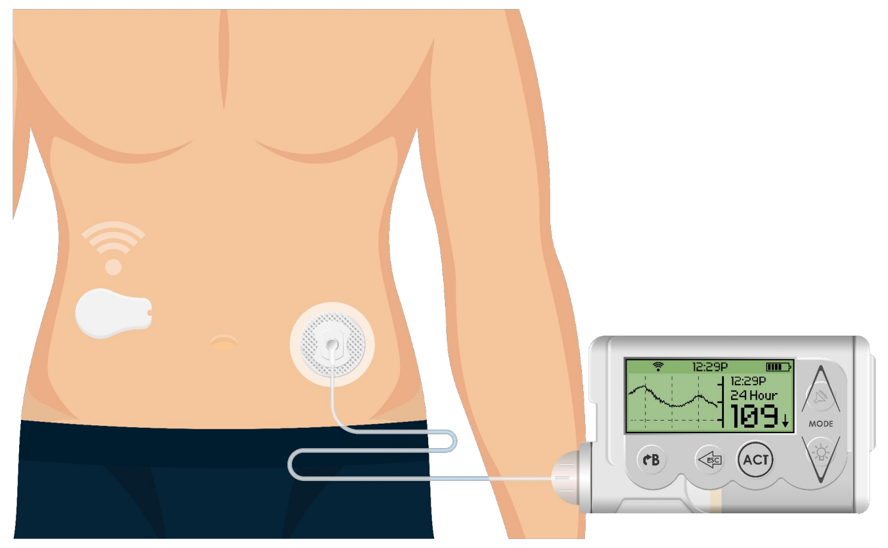
Type: Diagnostic Equipment
Setting: Laboratory
Potential Harm: Diagnostic Error
Classification: Class II/IIa



Artificial Pancreas

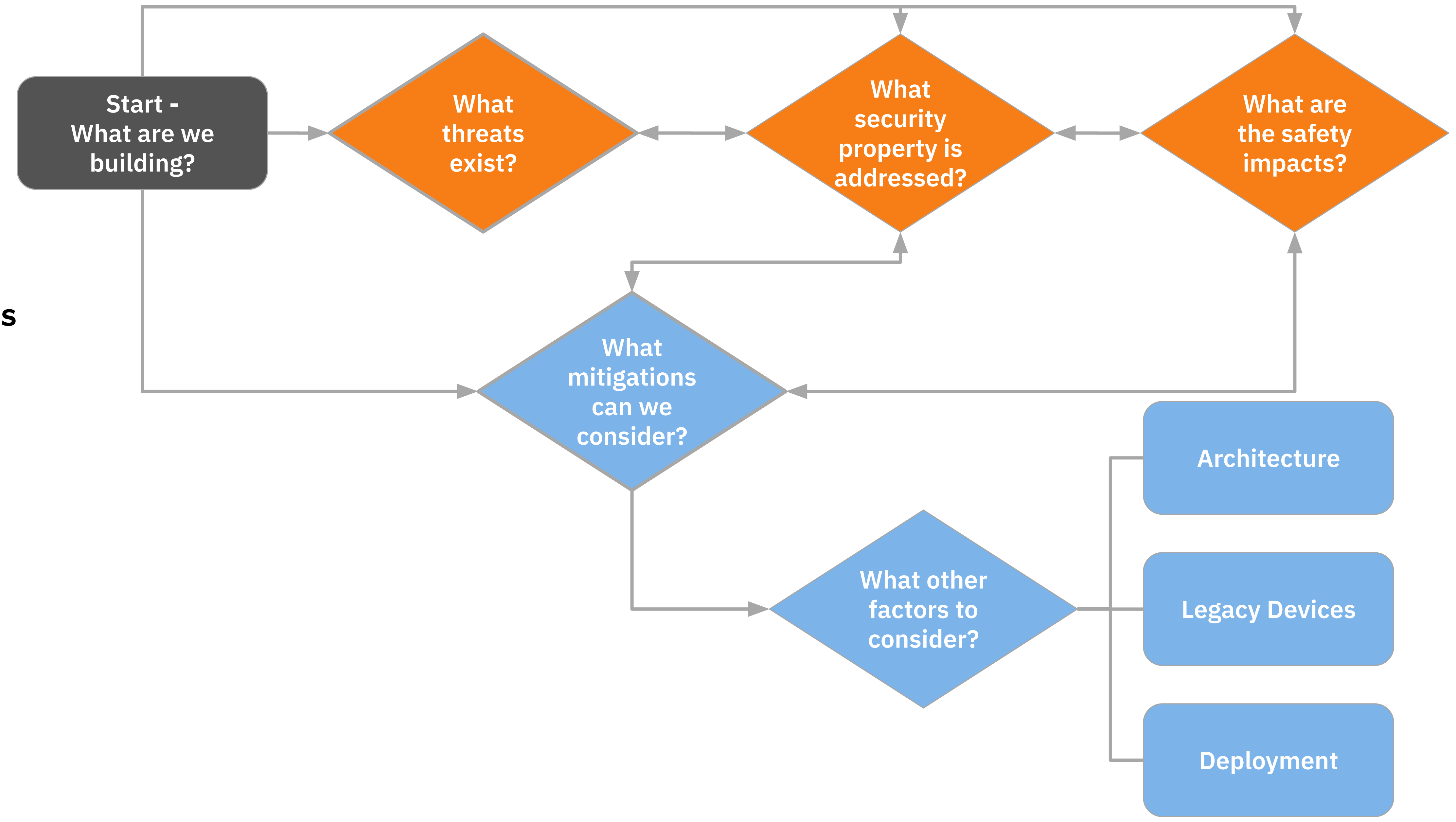
(Insulin Pump & Continuous Glucose Monitor)

Type: Implantable Medical Device
Setting: Implant
Potential Harm: Patient Death
Classification: Class III



All three scenarios are based on devices that are currently being used on the market today. Classifications are using FDA Guidance, EU MDR/IVDR, and Health Canada

Process Model Observed from Participants


Start - What are we building?
What threats exist?
What security property is addressed?
What are the safety impacts?
What mitigations can we consider?
What other factors to consider?
Architecture
Legacy Devices
Deployment

Results & Recommendations

1. **Flexible process for brainstorming threats and controls**

   Recommendations:
   Free-flowing process through interaction
   Allow for multiple configurations

2. **Safety considerations are critical, unclear how to integrate**

   Recommendations:
   Integrate with safety risk processes
   Prompt for multi-patient harm

3. **Use Cases/Workflows are useful tools for prioritization**

   Recommendations:
   Use-case views

Medcrypt CISCO

Tufts Security & Privacy Lab tsp.cs.tufts.edu

Read our Full Paper from USENIX Security 2024