THREAT MODCON 2024 San Francisco

Making Threat Modeling More Natural

Recommendations for Practitioners and Tool Developers

Ronald E. Thompson, III
Tufts University

Tufts Security & Privacy Lab

THREAT MODCON 2024 SAN FRANCISCO

Agenda

Our Research Study

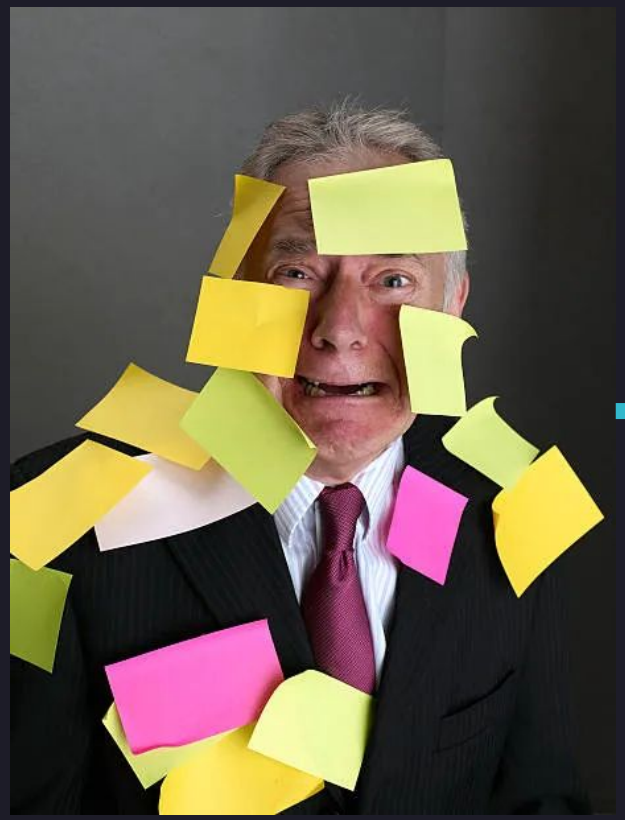
Our Threat Modeling Process Model

Applying Our Process Model to Tooling

Prototype Example

Tufts Security & Privacy Lab

What is usable security?



What is usable security?

Humans do security

Humans use tools & processes to do security

Those tools and processes can be hard or get in the way

We want to make these things fit into your current process, and not give you a migraine

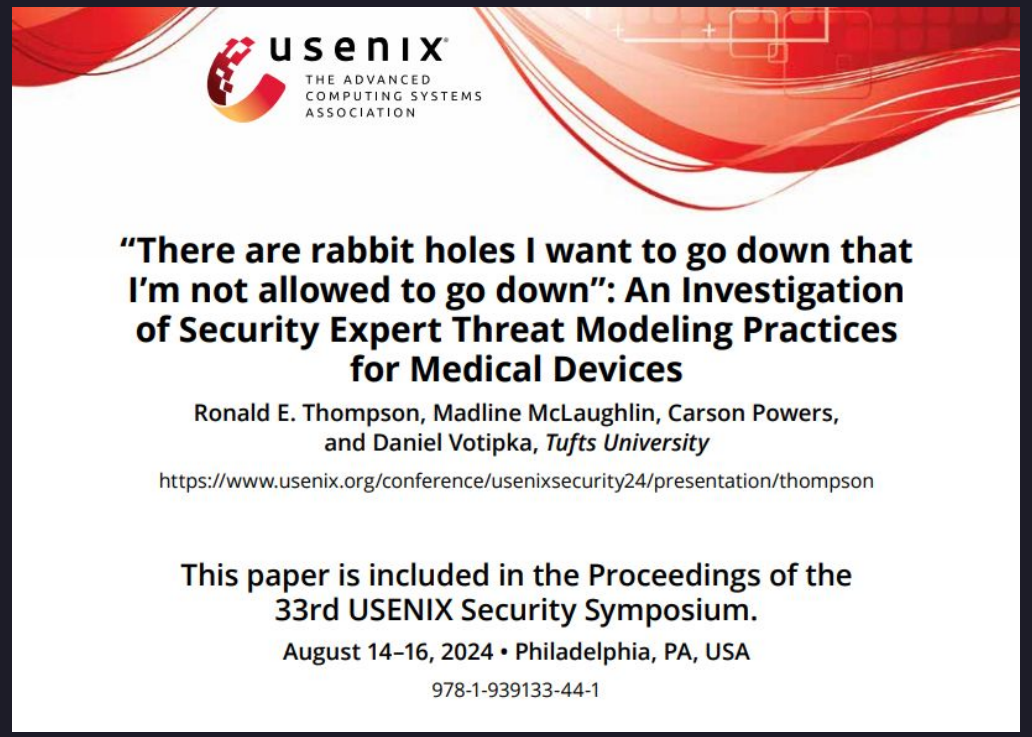
THREAT MODCON 2024 SAN FRANCISCO

Our Research

The Threat Modeling Naturally Tool: An Interactive Tool Supporting More Natural Flexible and Ad-Hoc Threat Modeling

Ronald E. Thompson*, Madison Red*, Richard Zhang*, Yaejie Kwon†, Lisa Dang*, Christopher Pellegrini∓, Esam Nesru‡, Mira Jain*, Caroline Chin* and Daniel Votipka*
*Tufts University; †Swarthmore College; ∓ Northeastern University;
‡ University of Maryland, Baltimore County

WS IW



usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

"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, Madline McLaughlin, Carson Powers, and Daniel Votipka, *Tufts University*

https://www.usenix.org/conference/usenixsecurity24/presentation/thompson

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Tufts Security & Privacy Lab

Vulnerabilities in medical devices are a continued issue

THREAT MODCON 2024 San Francisco

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

IEEE S&P

May. 2008

Insulin pumps are vulnerable to hacking, FDA warns amid recall

The Washington Post

Jun. 2019

Nine Vulnerabilities in Critical Infrastructure Used by 80% of Major Hospitals

ARMIS

Aug. 2021

Tufts Security & Privacy Lab

Medical Device Regulators are pushing secure-by-design

THREAT MODCON 2024 SAN FRANCISCO

Threat modeling includes a **PROCESS FOR IDENTIFYING SECURITY OBJECTIVES, RISKS, AND VULNERABILITIES** across the system, and then **DEFINING COUNTERMEASURES TO PREVENT, OR MITIGATE THE EFFECTS OF, THREATS** to the system throughout its lifecycle.

FDA Pre-Market Cybersecurity Guidance [2023]

Tufts Security & Privacy Lab

Larger trend by governments to use threat modeling

THREAT MODCON 2024 SAN FRANCISCO

Use a tailored threat model during development to **PRIORITIZE THE MOST CRITICAL AND HIGH-IMPACT** products. Threat models consider a product's specific use-case and enables development teams to fortify products.

Principles and Approaches for Secure by Design Software

Signed by 19 Different National Agencies

Conducted a research study to understand…

THREAT MODCON 2024 San Francisco

How do MDM Security Experts identify specific threats and mitigations?

What processes do MDM Security Experts follow when navigating a system's design to identify threats?

Tufts Security & Privacy Lab

With experts, we developed three realistic mock device scenarios

THREAT MODCON 24 SAN FRANCISCO

Robotic Surgical System

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

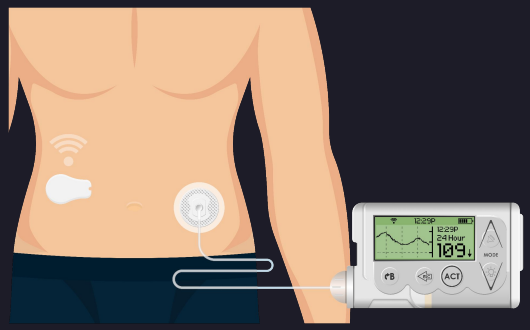
Next-Gen Sequencer

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



Tufts Security & Privacy Lab

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

Scenarios included requirements, a context diagram, and a DFD

THREAT MODCON 2024 San Francisco

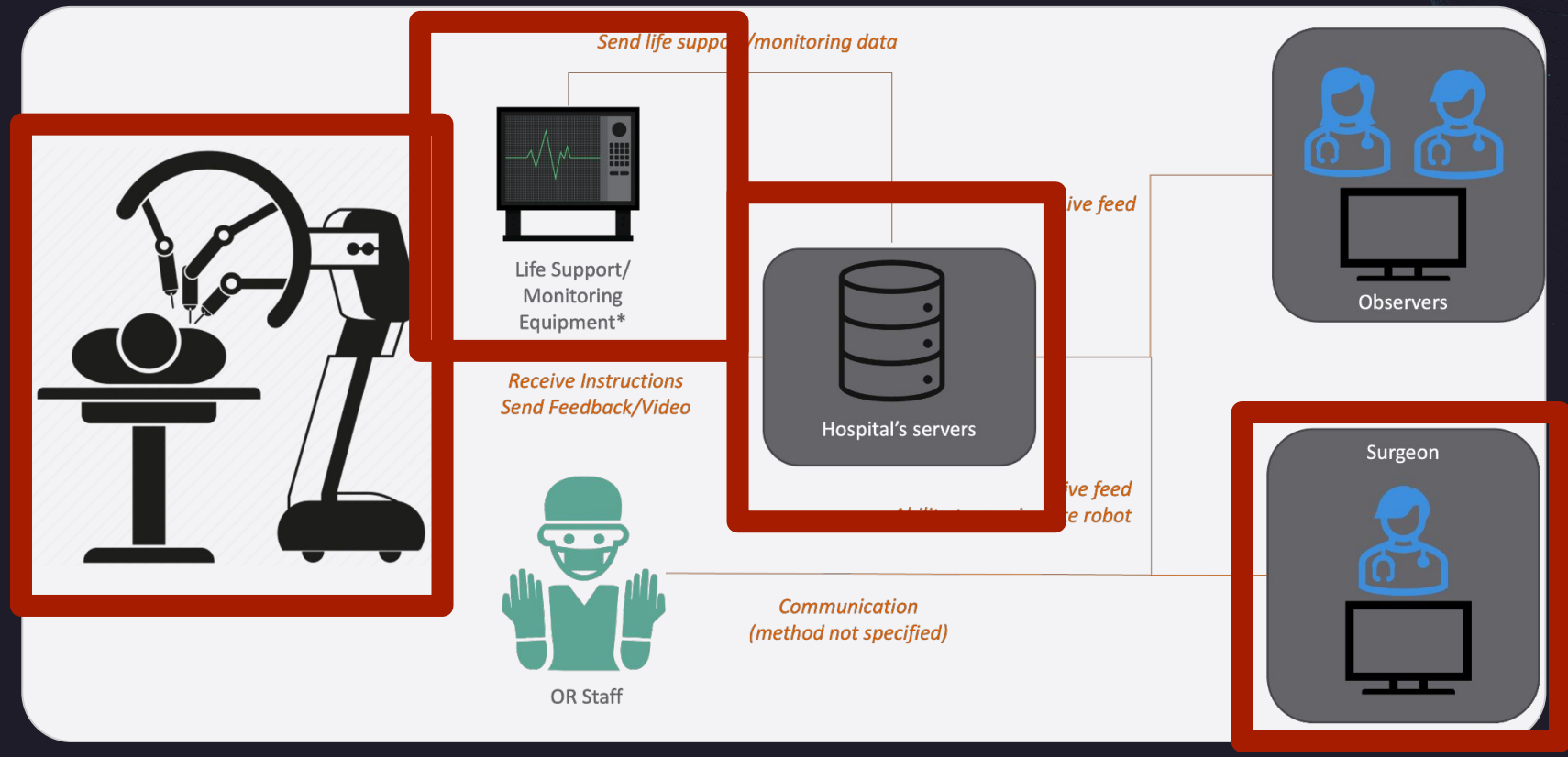
Robotic Surgical System

Allow for remote surgery

Store surgical reports on hospital server

Observers are able to watch the surgery (including the surgeon's viewpoint) from their computers

Third-party monitoring equipment should send vitals to surgeon's console



Tufts Security & Privacy Lab

Our results fall into three major findings

THREAT MODCON 2024 San Francisco

Flexible process for brainstorming threats and controls

Safety considerations are critical, unclear how to integrate

} RQ1

Ad-hoc Navigation & Reliance on Use Cases for prioritization — RQ2

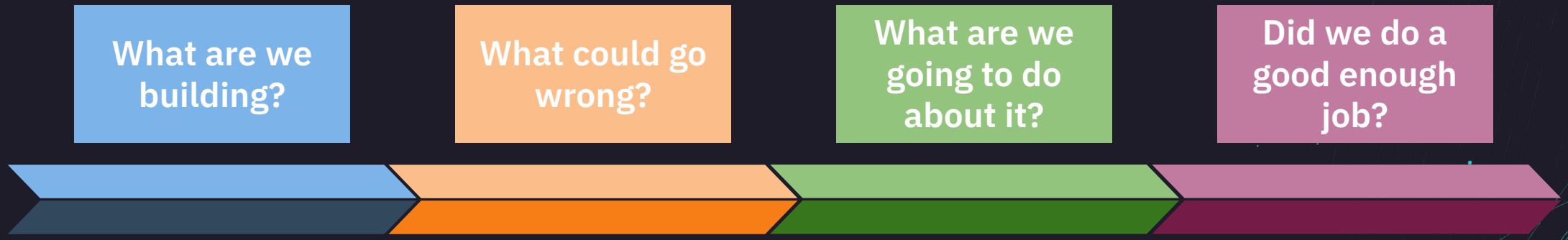
Our results fall into three major findings

THREAT MODCON 2024 San Francisco

Flexible process for brainstorming threats and controls

Participants relied explicitly & implicitly on the Four Questions

THREAT MODCON 2024 San Francisco



Diagramming

Data Flow Diagram, UML, State Diagram, Swim Lanes

Threat Brainstorming

STRIDE, LINDDUN, Attack Trees, OWASP Top 10

Mitigation Assignment

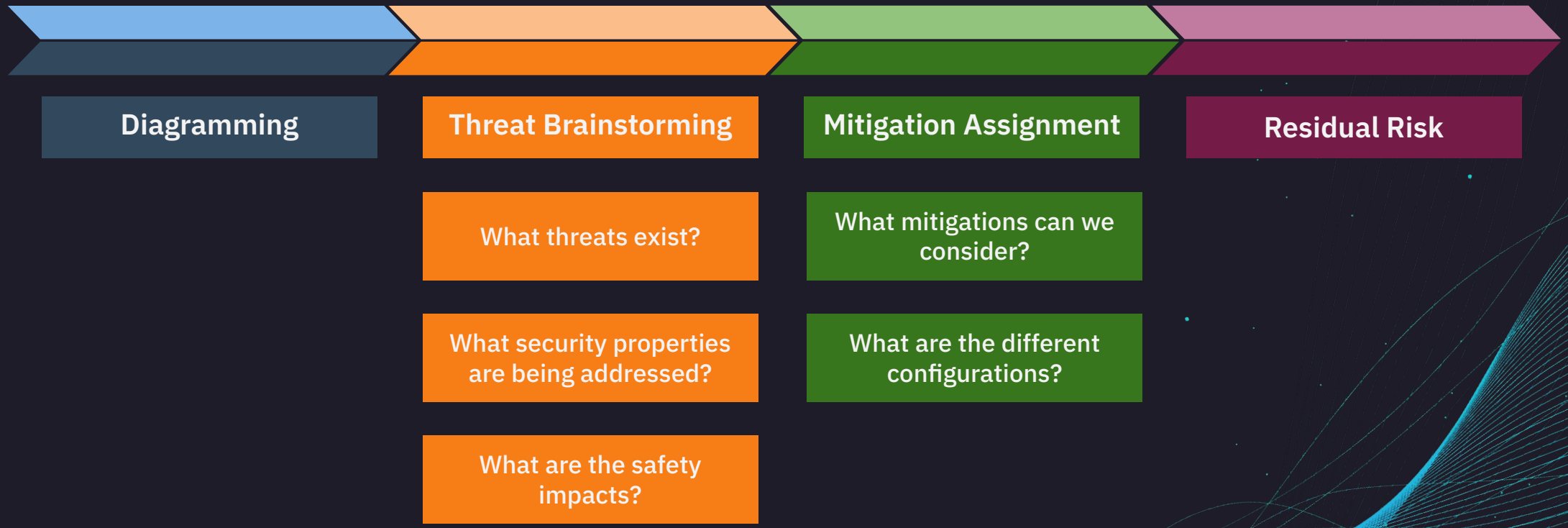
NIST 800-53, CIS Critical Security Controls

Residual Risk

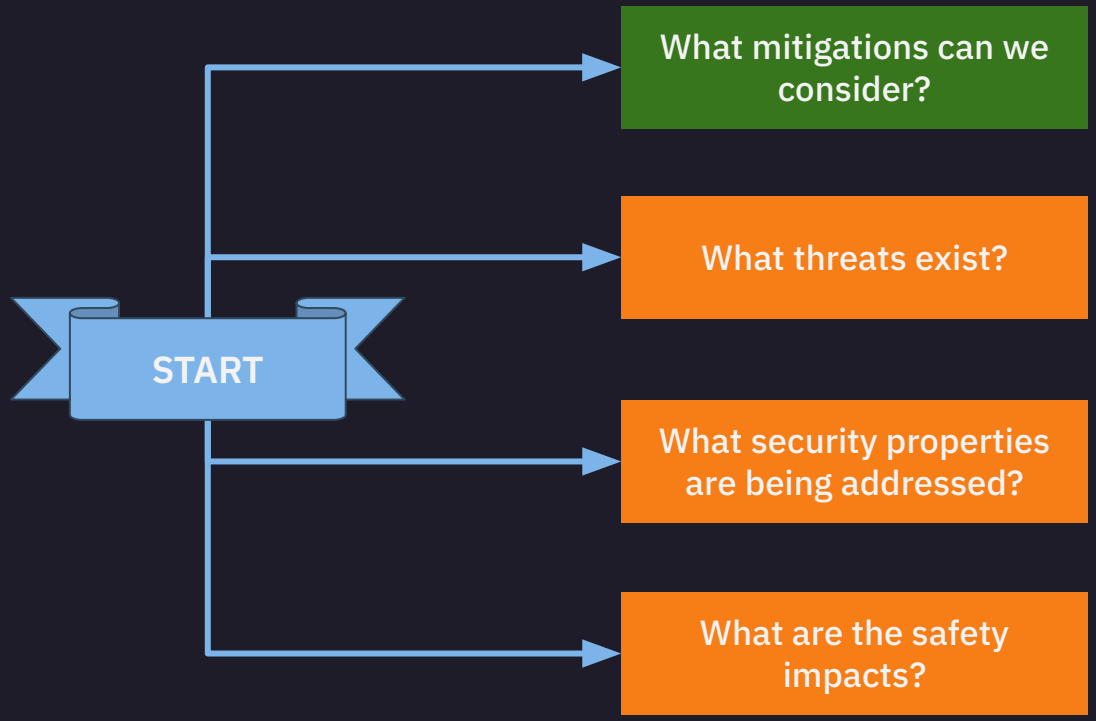
Sufficiently decreased risk to an acceptable level

They discussed common implicit & explicit threat related questions

THREAT MODCON 2024 SAN FRANCISCO

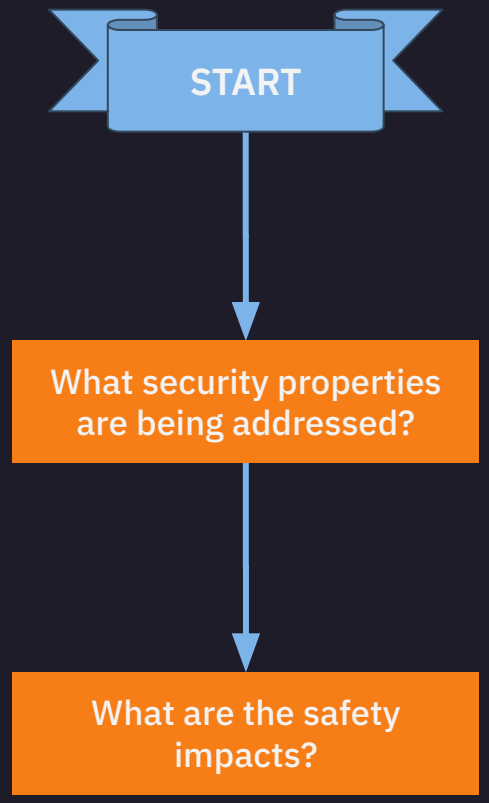


When looking at a specific part, they initially answered different questions



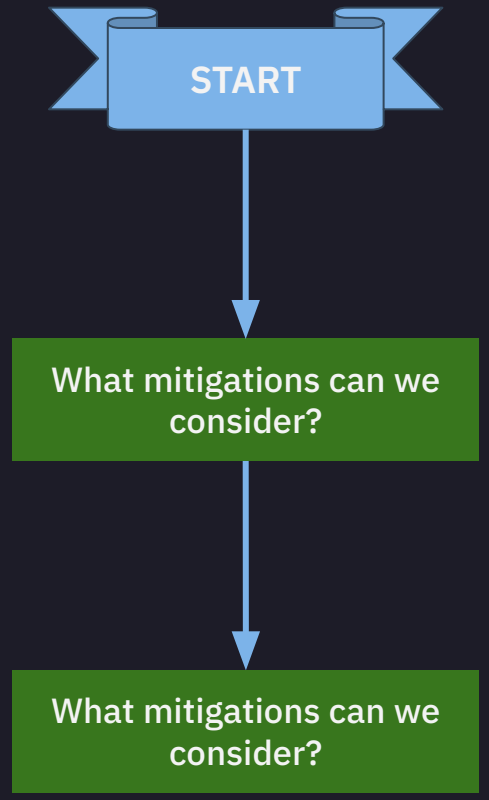
Similar to the findings of prior work we found that these questions can be implicit assumptions *[Van Landuyt & Joosen, Softw Syst Model 21]*

Evaluating the component would involve answering the initial question & linking it to another question



"**INTEGRITY** of the data that flows across the system as well as the **AVAILABILITY** of the data flow and both could result in **HARM TO THE PATIENT**."

It might also involve thinking about additional answers to the same question



“If the hospitals in charge of setting it up themselves, ideally I'd say put it on a **SEPARATE VLAN** and then have more **INDIVIDUAL ACCESS** for that. And then obviously the researchers and providers only a couple would've access to that for the people who would actually need it. So it'd be more **ROLE BASED ACCESS**.”

Our results fall into three major findings

THREAT MODCON 2024 San Francisco

Safety considerations are critical, unclear how to integrate

Despite suggestions from standards to separate them, security must consider the impact on safety & clinical efficacy

THREAT MODCON 2024 San Francisco

> “We can’t just look at where data resides, **WE CAN’T JUST SAY, ‘HEY, HARDEN YOUR SERVERS,’** and things of that general statements. We have to really look at the function and what the data that’s flowing between each component to understand and wrench its **IMPACT TO AFFECTING THAT CLINICAL WORKFLOW**.”

Tufts Security & Privacy Lab

Safety and security teams operate independently and use different language

THREAT MODCON 2024 SAN FRANCISCO

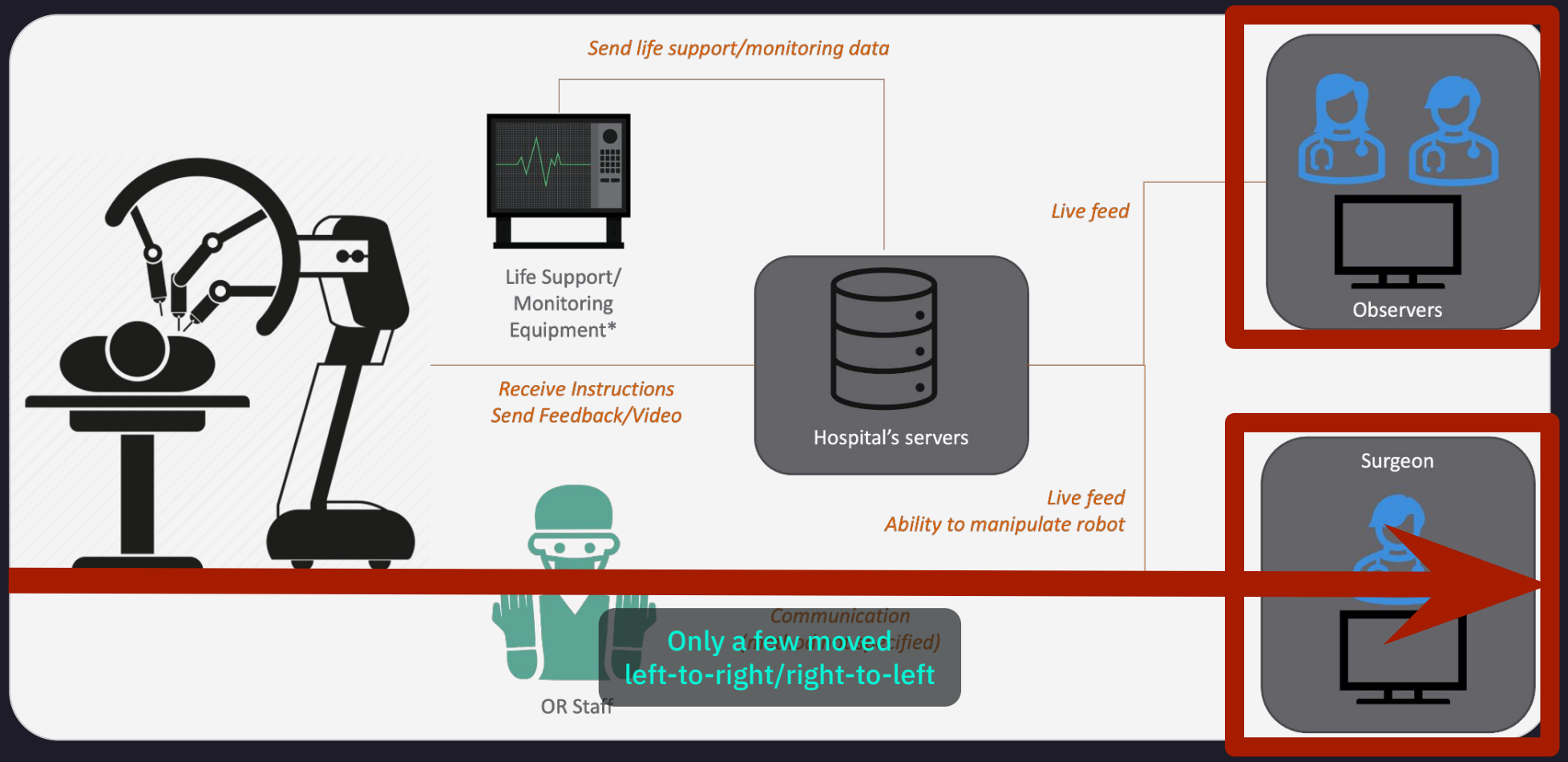
> “The integration of this is very important, and we have **SEPARATE PROCESSES THAT HAVE SYNCHRONIZATION POINTS**, but without necessarily the two groups understanding each other, it **[POTENTIAL MISCOMMUNICATION] IS PRETTY DANGEROUS**.”

Our results fall into three major findings

THREAT MODCON 2024 San Francisco

Ad-hoc Navigation & Reliance on Use Cases for prioritization

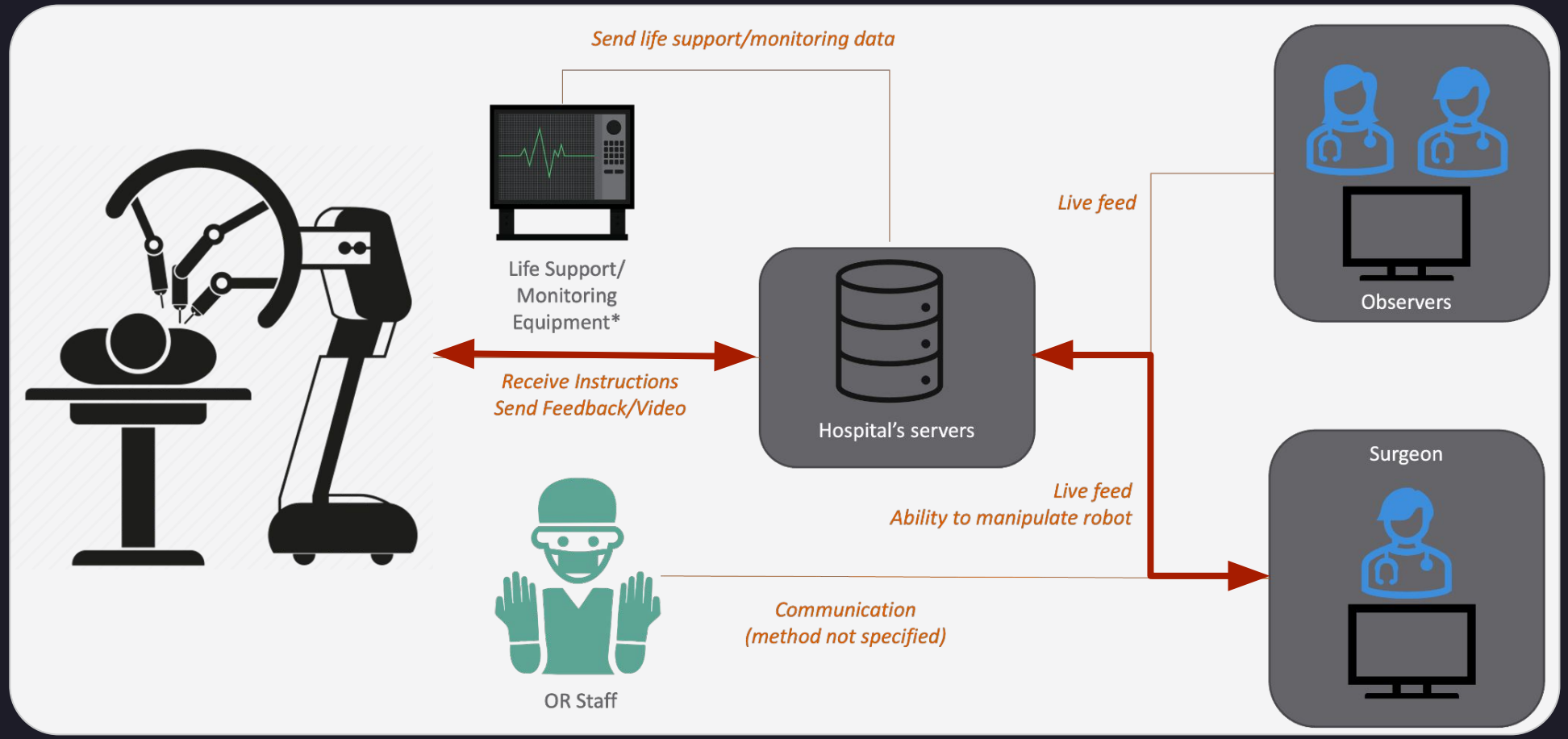
Participants would bounce between parts of the system based on what they previously thought about



Also add authentication for the observers

Add authentication for the surgeon

Participants rely on Use Cases to help them focus, but this is not accounted for in formalized threat modeling processes



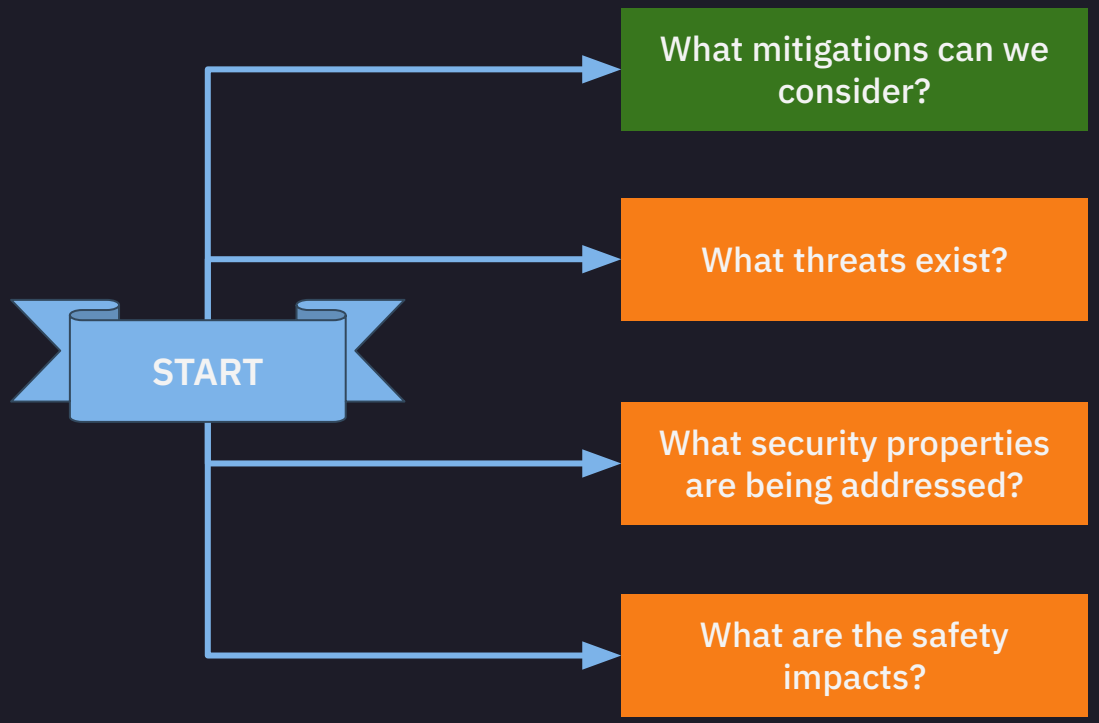
Adding more color to prior work that has found Data Flow Diagrams are not sufficient for threat modeling *[Sion et al, ICSEW 20]*

THREAT MODCON 2024 SAN FRANCISCO

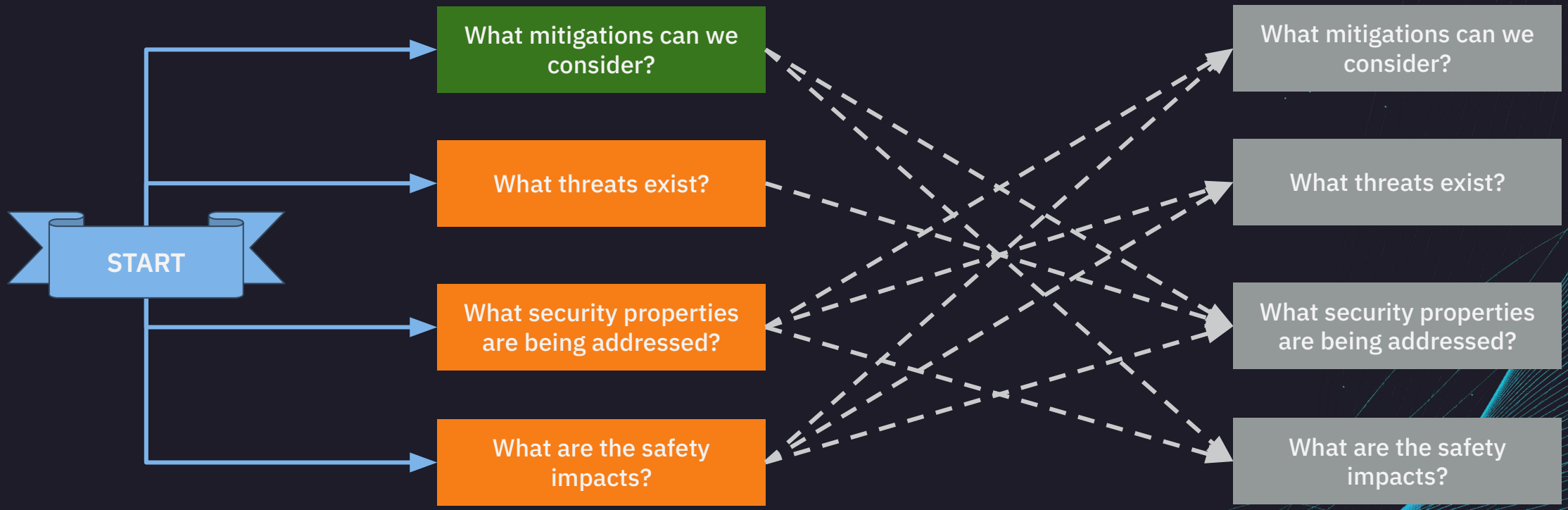
Our Process Model

Tufts Security & Privacy Lab

When evaluating a component, users can start at any of the following points



This can mean they are making implicit assumptions that are not always recorded during threat modeling



THREAT MODCON 2024 san francisco

Applying Our Process Model to Tooling

Tufts Security & Privacy Lab

Design goals that focus on usability & flexibility

THREAT MODCON 2024 San Francisco

- Support varied approaches
- Uninterrupted brainstorming
- Incomplete information and alternative configurations
- Evolving Interface

Tufts Security & Privacy Lab

Support varied approaches

Users have varied approaches to threat modeling, often adjusting their process while looking at the same system. Automation should fade into the background, suggesting threats and mitigations related to the current focus, only broadening focus when it appears the user is stuck.

Thompson et al. There are rabbit holes I want to go down that I'm not allowed to go down. USENIX Security 24

Not forcing user into a prescribed method by the tool designers, but instead allow it to be defined by the user.

Includes both high level threat modeling methods (such as PASTA) and more specific brainstorming (STRIDE, LINDDUN).

Uninterrupted brainstorming

THREAT MODCON 24 San Francisco

Various configurations may exist for a single system. Threat modeling tools should support this annotation and recommend common configurations the user may not have considered.

Thompson et al. There are rabbit holes I want to go down that I'm not allowed to go down. USENIX Security 24

Provide recommendations for the part of the system that is currently being investigated and anticipate what the user might look at next

As architects are looking at their system, they may need to accommodate different configurations based on customer needs.

Instead of having to create a whole new threat model, the tool should allow them to specify this different logic.

Incomplete information and alternative configurations

Because there are a variety of approaches when navigating the system, tooling should allow users to cycle through alternative visualizations. This includes allowing them to isolate specific use cases, as this was common among participants.

Thompson et al. There are rabbit holes I want to go down that I'm not allowed to go down. USENIX Security 24

Allow users to create focused views of a use case or dive more deeply into a specific part of the system

Most tools just provide a single view as a Data Flow Diagram - which has found to not be sufficient

Sion et al. Security Threat Modeling: Are Data Flow Diagrams Enough? ICSEW 20

Evolving Interface

Interfaces with drag-and-drop, common among threat modeling interfaces are easier for experts to navigate

Schniederman and Plaisant. Designing the user interface: strategies for effective human-computer interaction. 2010.

Novices should be presented with specific instructions and views should be refined as they continue to learn and improve

Lim, Benbasat, and Todd. An experimental investigation of the interactive effects of interface style, instructions, and task familiarity on user performance. TOCHI 96

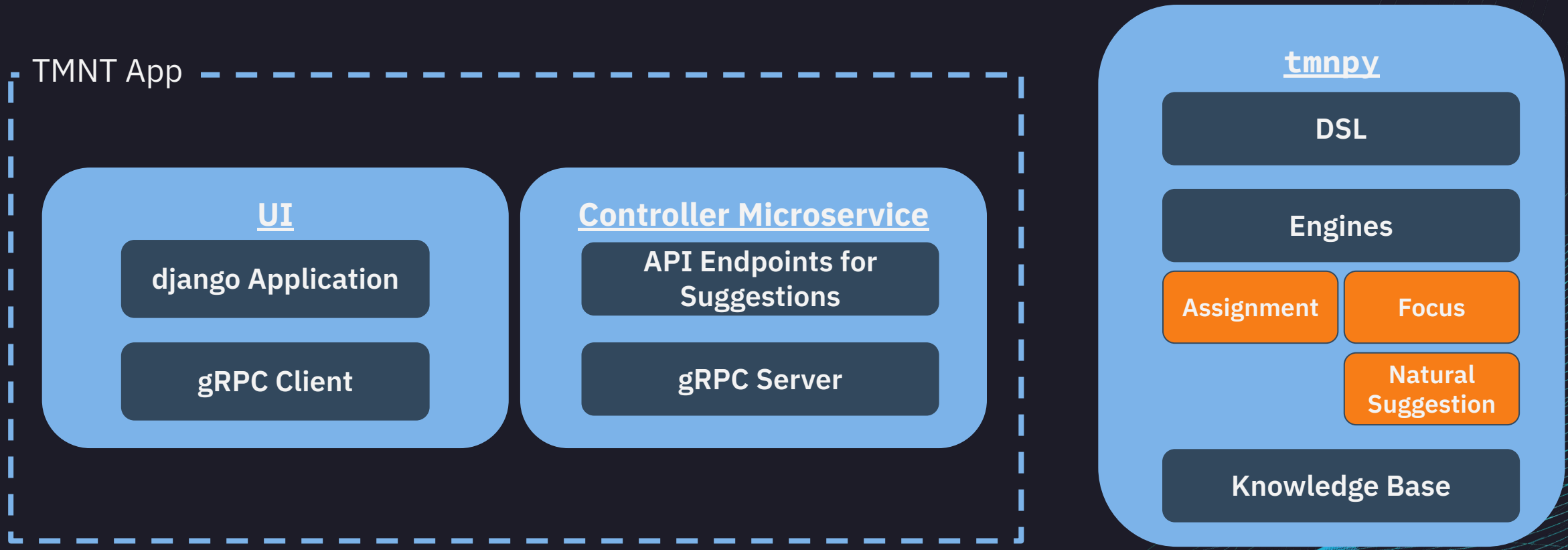
THREAT MODCON 2024
SAN FRANCISCO

Prototype Example

Tufts Security & Privacy Lab

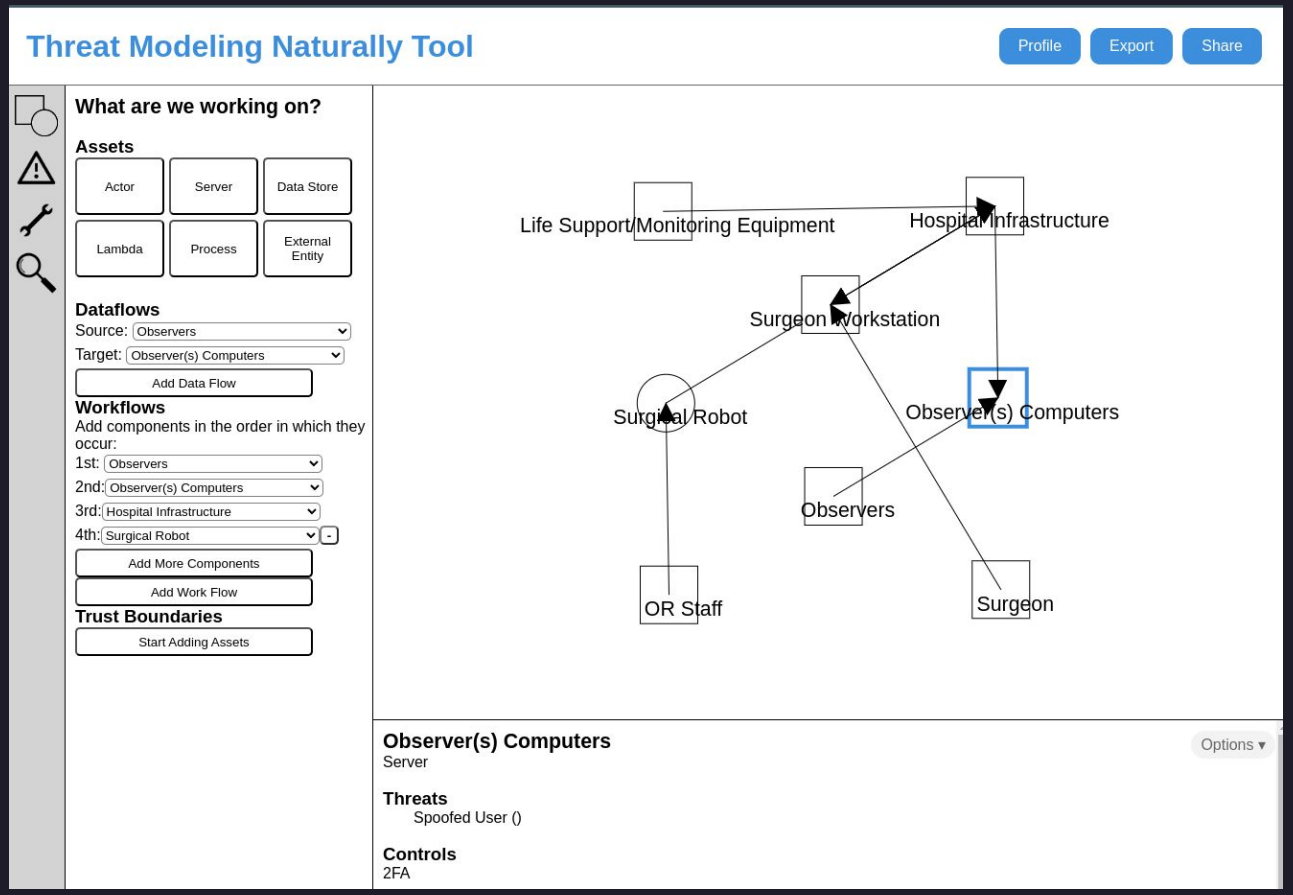
We developed a prototype application that can be leveraged for future threat modeling research

THREAT MODCON 2024 SAN FRANCISCO



Tufts Security & Privacy Lab

Leveraging familiar design - Visual Studio Code - that will allow WoZ experiments and collect data

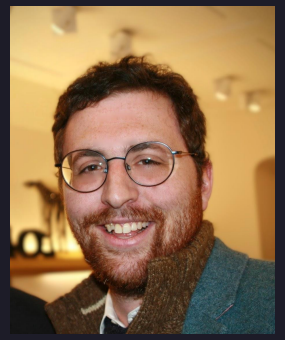


Looking to collaborate with tool developers to implement “natural” functionality

Develop a common threat modeling data standard that allows for interoperability and flexibility for users

Tufts Security & Privacy Lab

Research Team



Ronald Thompson
Tufts University

Madeline McLaughlin
Tufts University

Carson Powers
Tufts University

Dan Votipka, PhD
Tufts University

Prototype Team

Christopher Pellegrini - Northeastern
Madison Red - Tufts (*graduated*)
Richard Zhang - Tufts (*graduated*)
Yaejie Kwon - Swarthmore
Esam Nesru - UMBC
Lisa Dang - Tufts
Mira Jain - Tufts (*graduated*)
Carolin Chin - Tufts (*graduated*)

THREAT MODCON 2024 SAN FRANCISCO

Funding

Medcrypt

CISCO

Questions?

rthomp06@cs.tufts.edu

tsp.cs.tufts.edu

Tufts Security & Privacy Lab

Want to read our work?

go.tufts.edu/sec24

go.tufts.edu/wsiw24

go.tufts.edu/tmnt

THREAT MODCON 2024 SAN FRANCISCO

Funding

Medcrypt

CISCO

Questions?

rthomp06@cs.tufts.edu

tsp.cs.tufts.edu

Tufts Security & Privacy Lab


THREAT MODELING
CONNECT
POWERED BY
IRIUSRISK
THREAT
MODCON
2024
SAN FRANCISCO
ADVANCING THREAT MODELING CAPABILITIES TOGETHER