Tufts Security & Privacy Lab

Tufts UNIVERSITY

Usable Security Research for Hospitals

April 10, 2025

Ronald E. Thompson III
Tufts University

MassCyberCenter
at the MassTech Collaborative

Quick introduction

Interested in why people make the decisions they do and building software to augment this with data

- Started career in behavioral modeling for elections
- Worked on Wall Street and with US Army Special Operations

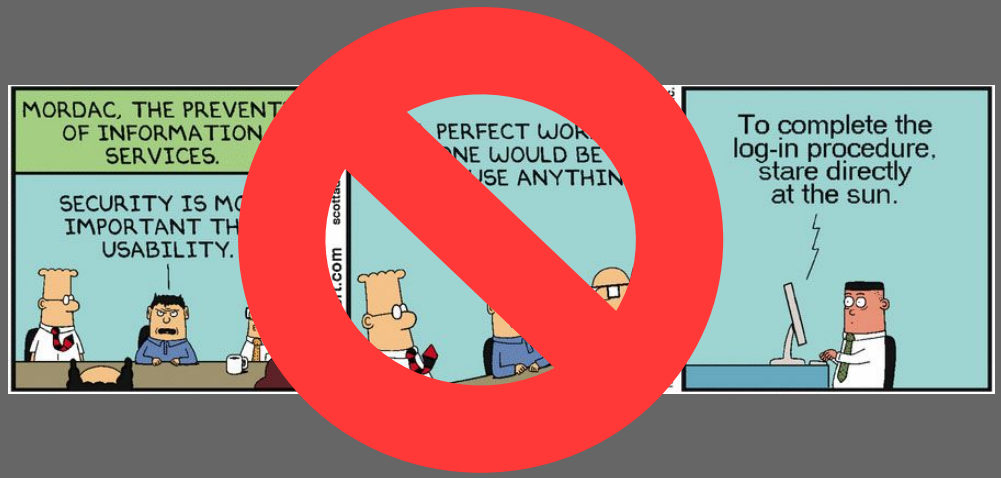
Came across issues with security in healthcare in pre-PhD career

- As the “biggest nerd,” was tasked with cybersecurity audits & training while working on a presidential campaign
- While on Wall Street invested in healthcare companies when they started disclosing vulnerabilities more

PhD research focuses on security in healthcare settings, including medical device security and hospital network security

What is usable security and what does our lab do?

- We look at how security professionals build, operate, use, and defend systems
- Goal is to develop tools and processes to make security easier to adopt and lower barriers to entry
- We combine knowledge of
  - Computer and Network Security
  - Human-Computer Interaction
- Previous work has included working with New York City Cyber Command
  - Conducted threat modeling training and on-site observations with security operations personnel
  - Highlighted specific benefits of threat modeling deployment in practice



NYC Cyber Command

Our lab has conducted work within healthcare specifically

- How medical device manufacturers threat model
  - Outcomes:
    - Created a generic process model for how MDMs can approach threat modeling
    - Provided guidance on how threat modeling fits in with Pre-Market Guidance
    - Conducted several trainings for MDMs in threat modeling

- What are the ways that care can be disrupted by potential cybersecurity incidents [IN PROGRESS]
  - Outcomes:
    - Publishing generic threat models based on the scenarios developed in the study that focuses on clinical impacts
    - Recommendations for hospitals on how to improve communications to clinical staff

Our lab has conducted work within healthcare specifically

- How medical device manufacturers threat model
  - Outcomes:
    - Created a generic process model for how MDMs can approach threat modeling
    - Provided guidance on how threat modeling fits in with Pre-Market Guidance
    - Conducted several trainings for MDMs in threat modeling

- What are the ways that care can be disrupted by potential cybersecurity incidents [IN PROGRESS]
  - Outcomes:
    - Publishing generic threat models based on the scenarios developed in the study that focuses on clinical impacts
    - Recommendations for hospitals on how to improve communications to clinical staff

We will cover some of the results we have found in this work

Some topline results from our most recent study that is relevant

Variance in potential harm, but integrity had highest likelihood of catastrophic harm

Availability attacks are associated with delay in care, which leads to harm

Communication between technologists and clinical staff needs improvement

Some login methods are perceived to impede care

Integrity attacks were seen to be more potentially harmful

Confidentiality attacks were seen to cause less harm than Integrity and Availability

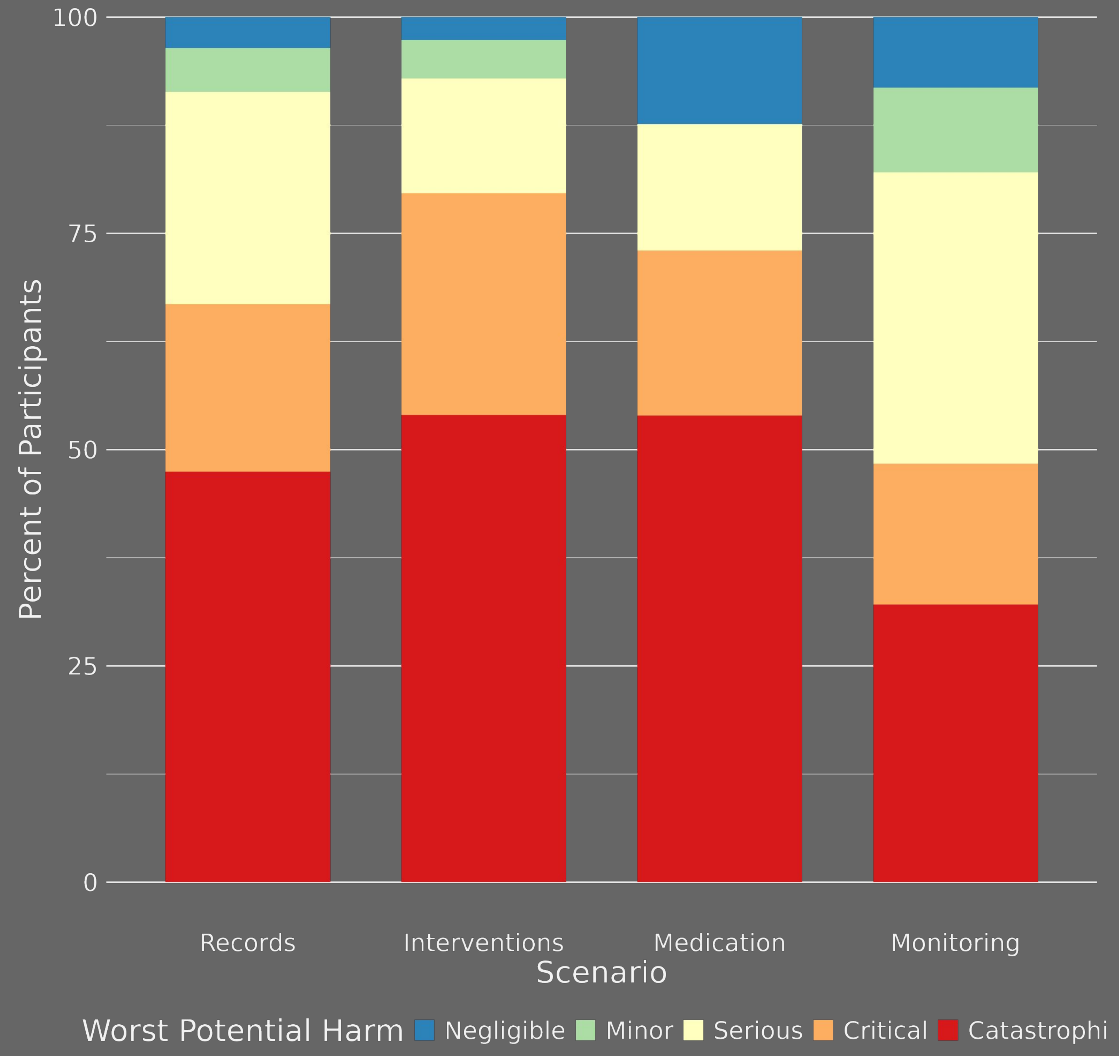
Integrity (OR: 48.62, p: <0.001)

Availability (OR: 23.53, p: <0.001)

Interventional devices were also seen to have more potential harm compared to Records

(OR: 1.91, p: 0.001)

Participants mentioned concern with patients receiving unnecessary care that could lead to harm



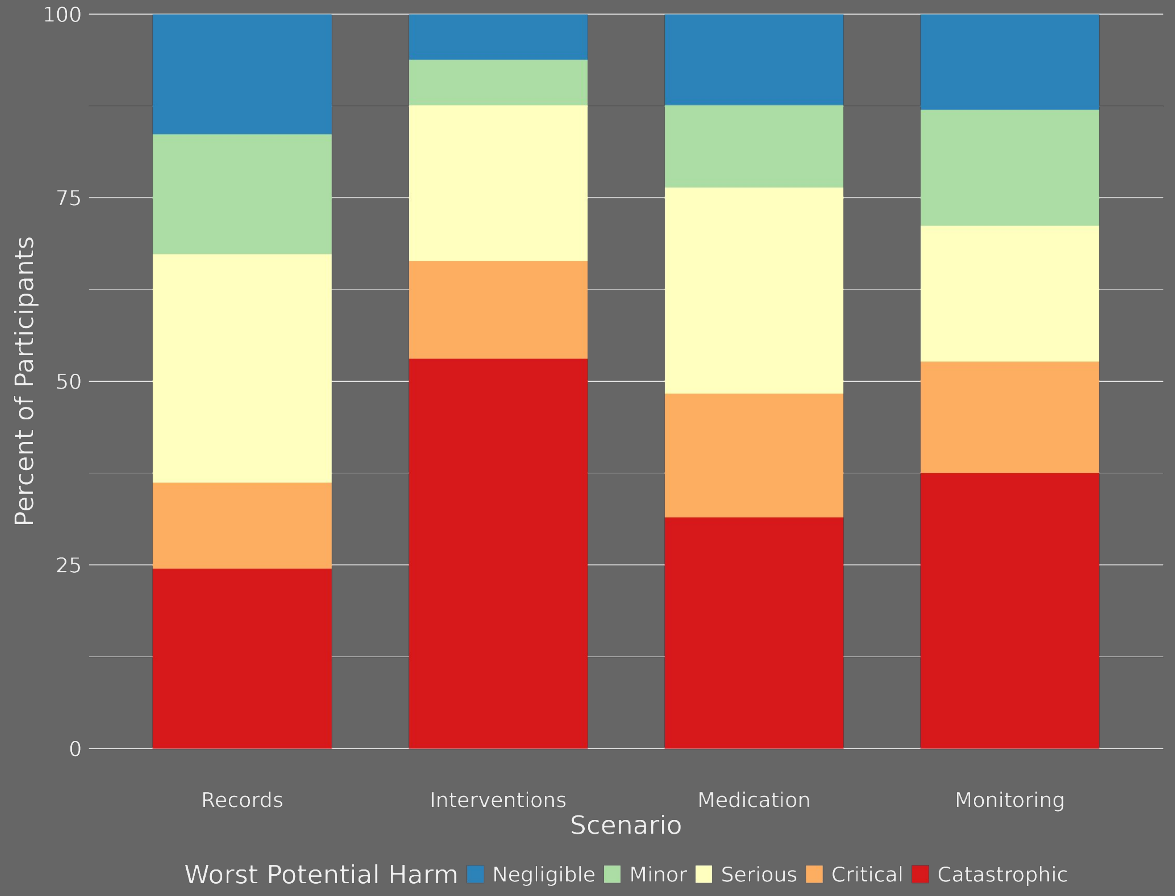
Variance in potential harm, but integrity had highest likelihood of catastrophic harm

Some integrity attacks are hard to independently verify

> “If you could show me that the potassium was low every day, every day the potassium is low, I give them extra potassium chloride. That's what we used to kill people in executions in this country, it's one of the agents. More immediately to this example, you could totally... I have **NO WAY OF INDEPENDENTLY VERIFYING THE POTASSIUM** concentration in someone's blood, which is **DIFFERENT THAN IMAGING TO SOME EXTENT**. If you try to convince me someone's arm is broken, I still see the patient.
>
> - Surgical Resident (R1)

Variance in potential harm, but integrity had highest likelihood of catastrophic harm

When participants talked about the potential harm that could occur from a loss of Availability, many mentioned Delay in Care



Interventions and Patient Monitoring were seen to most likely cause the most harm to the patient if they were not available

While it is frustrating, not having EHR access was not seen as harmful

Participants did not mention Delay of Care for Confidentiality or Integrity attacks

Availability attacks are associated with delay in care, which leads to harm

Clinical staff are often kept in the dark about what is going on

> “I actually **FOUND OUT** about [the security incident] **THROUGH A PATIENT** who had worked for the IT department of the hospital.
>
> - Critical Care APP (AP8CC)

> “I feel like I've gotten emails about them saying possibly there was a breach in security in the hospital, but **I DON’T KNOW ANYTHING ABOUT IT**.
>
> - MedSurg RN (RN9)

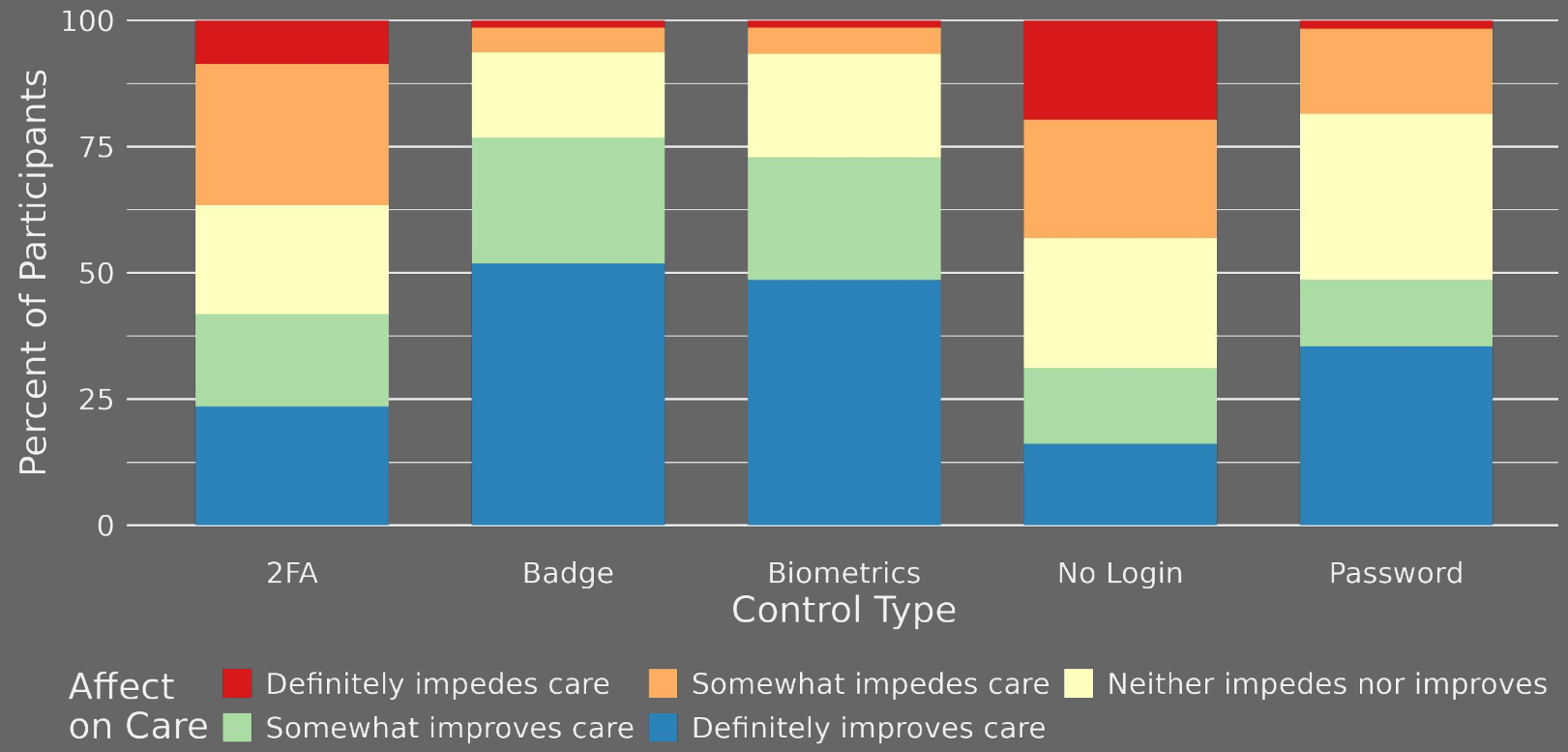
Communication between technologists and clinical staff needs improvement

Lack communication extends to when devices need updates

> “We want to have at least one [infusion pump] in every patient room, but often we don't even have that. We'll have to be looking around the unit for one, which is ridiculous, but **SOMEONE COMES AROUND THE HOSPITAL AND TAKES THEM IF THEY’RE NOT BEING USED**. I think it's for maintenance reasons to check, but then it's like we find ourselves hiding pumps in cabinets because we know these people come around... You see this person come around the unit and you're like, "**OH, NO, TAKE ALL YOUR PUMPS, HIDE YOUR PUMPS**."
>
> - MedSurg RN (RN9)

Communication between technologists and clinical staff needs improvement

Badge access is seen to improve care while 2FA is mixed



When comparing different logins to traditional username & password:

2FA impeded care
(OR: 0.49, p: <0.001)

Badge access improved care
(OR: 2.77, p: <0.001)

Biometrics improved care
(OR: 2.28, p: <0.001)

Some login methods are perceived to impede care

Badge access is common, while 2FA is polarizing especially when employed across multiple hospitals

> “We badge into all the computers. So the first time I badge for the day, it makes me put my password in and then it's like 12 hours from that mark.
>
> - MedSurg RN (RN9)

> “I'm in a patient room, and we're trying to review a hospitalization. And I have to go through 2 factor authentication to get into the [EHR]. And then I forget which of these 3 apps to open so it can take a while.
>
> - Attending Physician (A11)

Some login methods are perceived to impede care

It is imperative that clinicians are more incorporated into developing threat models and understanding cyber risk

CONTEXT FOR DEVICES

01

Ensuring the context of what unit the device is being used in determines the balance of integrity and availability as well as a tolerance for a potential delay in care

ENGAGEMENT

02

Hospitals need to provide proactive communications on cyber incidents and security measures. Provide clinical debriefs for providers similar to other types of events

SECURITY TO BACKGROUND

03

Security should blend into the background and have minimal impediment on care. Finding a way to still allow badge access while still maintaining security controls

It is imperative that clinicians are more incorporated into developing threat models and understanding cyber risk

CONTEXT FOR DE… …GROUND

01

Ensuring the c… …nto the
the device is b… …minimal
determines th… …nding a
integrity and a… …e access
a tolerance fo… …security
care

What we are not suggesting

We are not suggesting clinicians become security experts & understand every aspect of the technologies they rely on

Conversely, InfoSec should not be expected to understand every aspect of care

We are building on this research and looking to partner with hospitals so that we can develop recommendations for network architecture, incident response, and certificates management.

We want to address difficulties with incident response & planning as well as encrypted network protocols

Proposed Studies

- What are the challenges of implementing encrypted network healthcare protocols (DICOM, HL7)?

- How can we develop augmented network maps for hospitals focusing on the clinical impact and communicating this information?

Given the HIPAA changes, there is a need to address challenges with encrypted channels

We are hoping to speak with the Risk and Device Management teams to understand how medical devices are onboarded and certificates are managed by the hospital

- Anecdotally, we have heard that hospitals are not using Secure DICOM
  - We want to understand why and to see how we can improve these TLS-enabled protocols

- As part of this, we could help the hospital start to transition devices to using encrypted channels in compliance with HIPAA rule changes

- We want to establish guidance and best practices for how to roll out TLS-enabled versions of these protocols for both current and legacy devices that allows the hospital to maintain control without increasing the burden on InfoSec teams

Given the HIPAA changes, there is a need to address challenges with encrypted channels

We are hoping to speak with the Risk and Device Management teams to understand how medical devices are onboarded and certificates

- Anecdotally, we have hea
  - We want to understa LS-enabled protocols
- As part of this, we could h ing encrypted channels in compliance with HIPAA ru
- We want to establish guid enabled versions of these protocols for both current maintain control without increasing the burden on

Benefits for You

1. We are able to provide guidance on strategies to implement certificate management
2. We can help with the initial rollout working with InfoSec

Building and communicating network maps focused on clinical impacts

We are looking to work with a hospital to build network maps and incident response plans for the different clinical technologies deployed

- We want to follow patients' journeys both in the physical hospital space as well as on the network
  - Hoping to focus on all patients in the ED that require imaging and follow their care until being admitted
  - Example: Stroke patient walks in to ED, goes to Triage, sent to Radiology for Head CT, back to ED where ischemic stroke is diagnosed, then to Interventional Radiology for treatment
- Would involve shadowing clinical staff and then looking at any related network resources, such as passive monitoring (such as network tap) and network architecture to trace the patient journey
- Rely on this information to build a clear understanding of how clinical workflows map to the network and then get feedback from clinical staff on how different threats would impact care
- Build a template incident response plan based on this as well as communication recommendations

Building and communicating network maps focused on clinical impacts

We are looking to work with a hospital to build network maps and incident response plans for the different clinical technologies deployed

- We want to follow patients' journeys both in the physical hospital space as well as on the network
  - Hoping to focus on all patients i… ED that require imaging and follow their care until being admitted
  - Example: Stroke patient wa… adiology for Head CT, back to ED where ischemic stroke is d… ology for treatment

- Would involve shadowing clin… …ted network resources, such as passive monitoring (such as n… …ucture to trace the patient journey

- Rely on this information to build a clear understanding of how clinical workflows map to the network and then get feedback from clinical staff on how different threats would impact care

- Build a template incident response plan based on this as well as communication recommendations

We are open to changes and having a discussion with partners

Building and communicating threat models focused on clinical impacts

We are looking to work with a hospital to build threat models for the different clinical technologies deployed

- Our initial thought is focus … ely on imaging to make the problem more manageabl…
  - For example, what sy… s in (initial charting, CT diagnosis, and Interv…
- Would involve either pass… ady developed by the hospital
- Rely on this information t… om clinical staff on how different threats would im…
- Build a template incident … nication recommendations

Benefits for You

1	We will conduct threat modeling training with InfoSec, Clinical Engineering and others
2	We will build and provide you with network maps highlighting clinical impact
3	We will help you develop incident response plan and communication strategies

Contact us

Email : rthomp06@cs.tufts.edu

Interest Form
http://go.tufts.edu/tsp_hospital_interest

Funding

Medcrypt

NSF

ARPA H