BEHAVIORAL EMANIPULATION: ATTACKING VIA CARE DELIVERY WORKFLOWS

Ted Harrington
Executive Partner
Independent Security Evaluators (ISE)
@SecurityTed

Kostas Triantafillou, MD
Orthopaedic Traumatology and Geriatric Orthopedics
University Orthopaedic Surgeons
University of Tennessee Medical Center
Behavioral eManipulation

Technical Exploit + Human Behavior = Harm
Who Am I?
Agenda

- Context
- Attack Anatomies
- Remedies
Agenda

- Context
- Attack Anatomies
- Remedies
A Surgeon’s Perspective
Attacking Active Devices

- Insulin Pump
- Medication Infuser
- Defibrillator
Attacking Active, Passive, & Workflow

- Insulin Pump
- Medication Infuser
- Defibrillator
- Imaging
- Patient Monitors
- Medication Monitors
- Communication
- EMR
- Live Data Analysis
- Courier
- Pharmacy
- Transition of Care
- Nursing
- Physician
- Ancillary
Air France Flight 447
Rio Di Janeiro to Paris
2009
Agenda

1. Context
2. Attack Anatomies
3. Remedies
Hacking Hospitals

24 months, 12 healthcare facilities, 2 healthcare data facilities, 2 healthcare technology platforms, and 2 active medical devices

Digital attacks = patient harm?

securityevaluators.com/hospitalhack
Behavioral eManipulation: Attack Flow
Behavioral eManipulation: Methodology

1. Understand the care **workflow**
2. Manipulate **data**
3. Rely on **humans** to unwittingly deliver harm
Diagnostic Attack Scenarios

System of Safety Checks

Data Interpretation
Examples: Attacking System of Safety Checks

Blood

Allergies
Attacking System of Safety Checks
Diagnostic Attack Scenarios

System of Safety Checks

Data Interpretation
Examples: Attacking Data Interpretation

Monitoring

Labs
Attacking Data Interpretation
Fearmongering?

1) Who would even want to do this?
2) Why?
Patient Health v. Patient Data

HARM
FEAR
DISRUPTION/WARFARE

PROFIT
Agenda

- Context
- Attack Anatomies
- Remedies
Areas For Improvement

Secure Devices

Train Medical Professionals
Think Like An Attacker Thinks
Threat Model

ASSETS

$  

ADVERSARIES

ARCHITECTURE
Recognize Role of Compliance

HIPAA
The Health Insurance Portability and Accountability Act of 1996

FDA
Solution lies primarily with Device Manufacturers

- Design & Implement Threat Model
- Design & Implement Trust Model
- Partner with security experts
  - Perform Security Assessments
  - Think like Attacker
  - Build security into Design