MEDICAL DEVICE THREAT MODELING WITH TEMPLATES

Valery Berestetsky
Principal Product Security Leader
GE Healthcare

Jonathan Schaaf
Staff Product Security Analyst
GE Healthcare
Murphy’s law is not a curse, it’s a design approach.
Threat Modeling: Life Cycle

- Vision
- Model
- Identify Threats
- Validate
- Mitigate
Vision:
Software Applications vs Medical Devices

How is your product different?
Model: What’s Different?

How is your product different?
Model: What’s Different?

Web Application

Medical Environment

How is your product different?
Identify Threats: Are We Covered with STRIDE?

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege
- Abuse
- Patient Safety
There are tools for this!
Demo Time – Our Template

MICROSOFT THREAT MODELING TOOL 2016

Threat Model:

Create A Model
Model your system by drawing diagrams. Make sure you capture important details.

Open A Model
Open an existing model and analyze threats against your system. Don't worry, the tool will help you identify them.

Getting Started Guide
A step-by-step guide to help you get up and running now.

Template For New Models

Template Workflow
1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template: 

Create New Template
Define threats, threat types and custom threat properties for your threat model from scratch.

Open Template
Open an existing Template and make modifications to better suit your specific threat analysis.

Template Workflow
Use templates to define threats that applications should look for. 
1. Define scenarios
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template

Generic Physical Medical Component

Pharmaceutical Pump
Remotely Controllable Patient Table
Ionizing Radiation Source
Moving Gantry or C Arm
Emergency stop
Safety Interlock
Image Detector
Sensor
Clinical Information Display
Imaging Device

RSA Conference 2018
Threat modeling answers “What can possibly go wrong?” question
If nothing else, threat model. Use STRIDE (or another framework)
Tooling isn’t essential, but can make life a lot easier
Anything can be threat modeled. Ask “What can possibly go wrong?”

Questions?

jonathan.p.schaaf@ge.com
valery.berestetsky@ge.com
Apply What You Have Learned Today

- 3 weeks: Familiarize yourself with threat modeling; consider reading a book, downloading a tool and make yourself familiar with it
- 6 weeks: get a customized template and build a threat model with it
- 3 months: create your own template and submit to the community!
“Whatever can go wrong, will go wrong,” by Nick T. Spark, ISBN 978-1411684690
Microsoft Threat Modeling Github: https://github.com/Microsoft/threat-modeling-templates
Existing NCC Group Automotive Threat Modeling Template
Image attributions:
  XKCD number 319, https://xkcd.com/319/ Creative Commons BY-NC version 2.5
Microsoft Threat Modeling Tool
  Preview Release https://aka.ms/tmtpreview, includes Microsoft Azure template