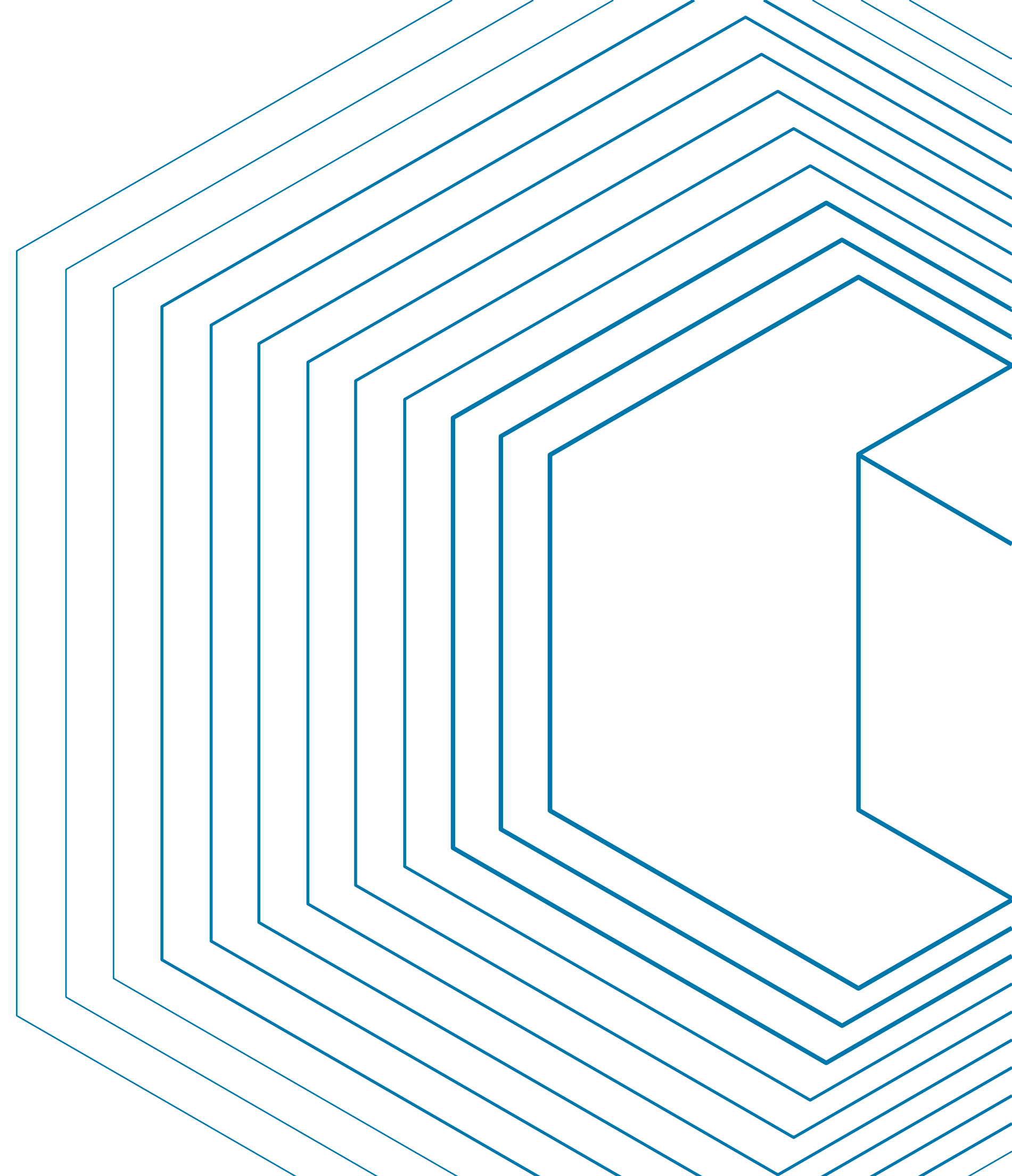


Security - Threat Model

Debbie Furman

Christopher DeRobertis (Dero)





Threat Model - what is it?

- Modeling the solution under test by looking at potential threats to that solution that can cause damage.
- There are various sections to a threat model
 - **Scope** - Need to clearly articulate the scope of the model
 - **Assets and Actors** - identify the Actors who can access the solution being modeled and the Assets that they may be trying to access
 - **Diagrams** - pictures of Architecture, touch points, data flows, etc.
 - **Problems** - Identify the problems that can occur if there is a breach and the severity of the problem, how to identify the problem and how to mitigate the problem
- The goal of doing this activity is to identify possible threats and sufficiently mitigate those threats.

Threat Modeling a House

Who can cause damage to a house?



Threat Modeling a House

Who can cause damage to a house?

People
Nature
Animals



Threat Modeling a House

What are the basic structure and features of a house?



Threat Modeling a House

What are the basic structure and features of a house?

Doors
Windows
Root cellars
Chimneys
Walkways
Driveway
Steps



Threat Modeling a House

Actor: Burglar

What are the different locations that a burglar might break into a house?



Threat Modeling a House

Actor: Burglar

What are the different locations that a burglar might break into a house?

- Back doors and windows, instead of the front ones
- Lower-level windows, like basement windows, instead of the second level ones
- Open windows, instead of closed ones
- Unlocked doors/windows, instead of locked ones



Threat Modeling a House

Actor: Burglar

What are the reasons a burglar might want to break into a house?



Threat Modeling a House

Actor: Burglar

What are the reasons a burglar might want to break into a house?

- Jewelry
- Electronics
- Cash
- Other valuables



Threat Modeling a House

Actor: Burglar

How is the house protected or ways that additional protections can be added to prevent a burglar?



Threat Modeling a House

Actor: Burglar

How is the house protected or ways that additional protections can be added to prevent a burglar?

- **Windows:** Shades, blinds, alarms
- **Doors:** Shades, blinds, locks, alarms
- **Walkways:** Video surveillance camera
- **Driveways:** Video surveillance camera



Threat Modeling a House

Actor: Burglar

If burglar gains access to inside house, how are the assets protected after infiltration?

- Jewelry
- Electronics
- Cash



Threat Modeling a House

Actor: Burglar

If burglar gains access to inside house, how are the assets protected after infiltration?

- **Jewelry:** safe, locked drawer, hidden
- **Electronics:** locks, passwords
- **Cash:** safe, locked drawer, hidden



Threat Modeling a House

More Questions

Actor: wild animals, bugs

How do you keep these things out of the house?

If they get in, how do you get rid of them -and- how do you prevent them from getting back in?



Threat Modeling a House

More Questions

Actor: Nature

How do you protect from floods, fires, etc?

Actor: Children

How do you protect your house from potential damage caused by children?



Threat Modeling a House

More Questions

Actor: IoT devices

Can these be jammed?

Can these be hacked?

Are they spying on you?



Threat Modeling a House

- **Scope** - Need to clearly articulate the scope of the model
- **Assets and Actors** - identify the Actors who can access the solution being modeled and the Assets that they may be trying to access
- **Diagrams** - pictures of Architecture, touch points, data flows, etc.
- **Problems** - Identify the problems that can occur if there is a breach and the severity of the problem, how to identify the problem and how to mitigate the problem
- **After threat model is created and reviewed**
 - Create variations to test the threats and verify mitigation
 - Standards testing (ISO, NIST, ...)
 - Threats by unauthorized users
 - API attack techniques
 - ...



Questions?

