Threat Modeling(in 600 seconds)

w/Architecture Diagrams

Kat Fitzgerald
@rnbwkat
evilkat@rnbwmail.com

1

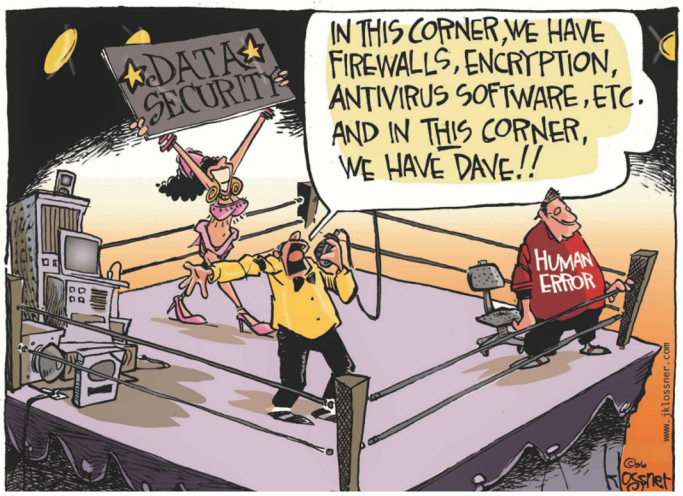
$whoami

$ whoami

- CEO @BSidesChicago,
  2019 COO @dianainitiative,
  CFP Chair @BSidesPGH, DefCon 3!
- Based in Kirkland, WA and a natural creature of winter, you can typically find me sipping Casa Noblé Añejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos
- Honeypots, Refrigerators and IoT (Internet of Threats) are a few of my favorite things
- Handouts will be on github.com/rnbwkat

2

Threat Modeling in 30 seconds or less



3

Threats

- In Simplest Terms
  - Network
  - Host
  - Application
- But what is Threat Modeling?
  - *.. is the practice of identifying and prioritizing potential threats and security mitigations to protect something of value*

4

The Process

Identify	Identify Assets
Document	Document Architecture
Decompose	Decompose the Application
Identify	Identify Threats
Document	Document Threats
Rate	Rate Threats

5

Document the Architecture

Define WHAT it does and HOW

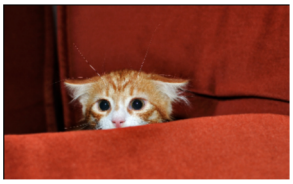
Who does it?

Diagram the Application <- FTW!!

- List Assets
- Show Data Flow
- Show Encryption
  - *(include protocols/ciphers where possible)*

6

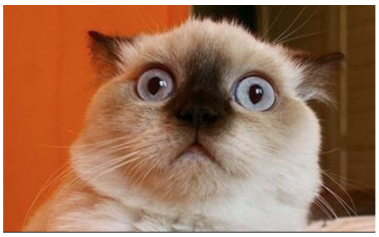
Decompose



- Refine the Architecture
  - Show AAA
    - What happened to the third "A"?
  - Trust Boundaries
  - Show Technologies
  - Ingress/Egress points
- Put on your "Anonymous" mask
  - Vulnerabilities?

7

Identify Threats - STRIDE



- ***S*poofing** - Can attacker gain access using false identity?
- ***T*ampering** - Can attacker modify data as it flows through app?
- ***R*epudiation** - Can we prove who did it?
- ***I*nformation Disclosure** - Can attacker gain access to data?
- ***D*enial of Service** - Can attacker reduce availability?
- ***E*levation of Privilege** - Can attacker assume priv user?

8

Diagraming 101

External Things

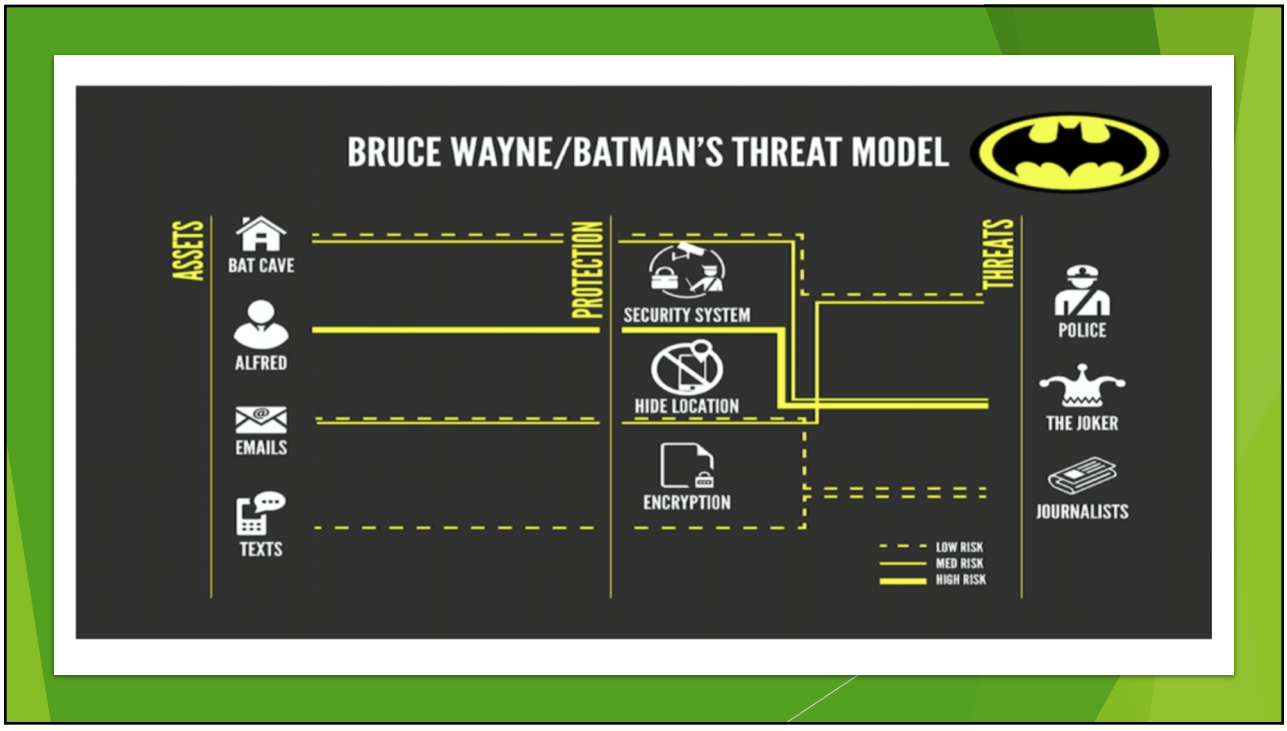
Services/ Components

Data Flow
- Traffic
- Encryption
- Direction
- RPC,etc

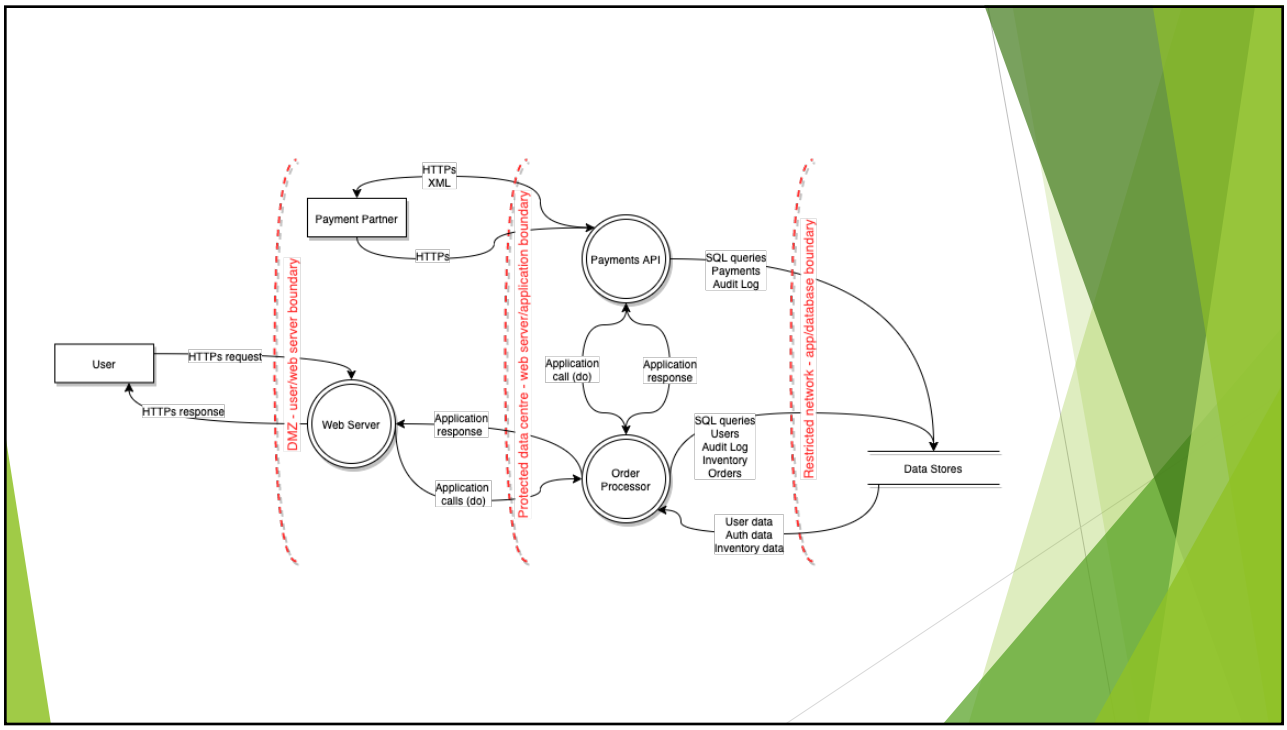
Data Store
- DB
- Cloud
- Keys

Trust Boundaries!

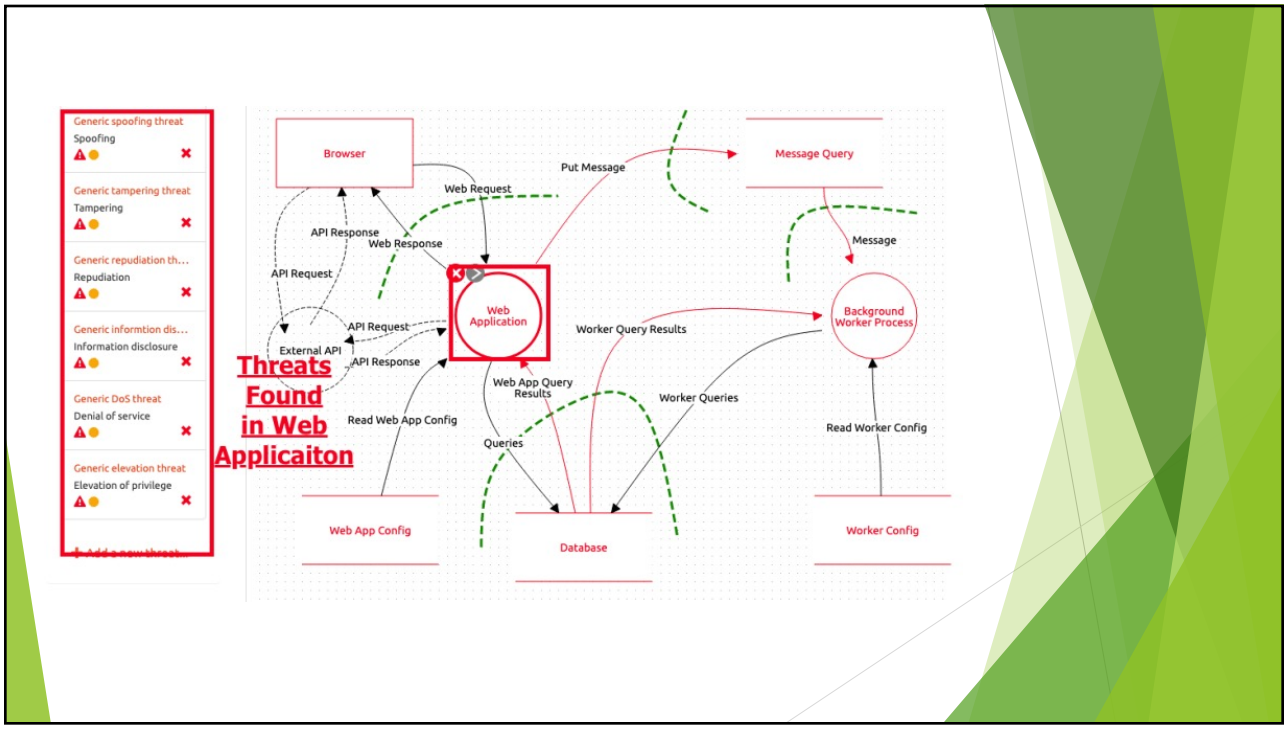
9



10


HTTPs
XML
Payment Partner
HTTPs
Payments API
SQL queries
Payments
Audit Log
User
HTTPs request
HTTPs response
Web Server
Application
response
Application
calls (do)
Application
call (do)
Application
response
Order
Processor
SQL queries
Users
Audit Log
Inventory
Orders
User data
Auth data
Inventory data
Data Stores
DMZ - user/web server boundary
Protected data centre - web server/application boundary
Restricted network - app/database boundary

11


Generic spoofing threat
Spoofing
Generic tampering threat
Tampering
Generic repudiation th…
Repudiation
Generic informtion dis…
Information disclosure
Generic DoS threat
Denial of service
Generic elevation threat
Elevation of privilege
Threats Found in Web Applicaiton
Browser
Web Request
API Response
Web Response
API Request
Web Application
API Request
External API
API Response
Read Web App Config
Web App Config
Queries
Web App Query Results
Database
Put Message
Message Query
Message
Background Worker Process
Worker Query Results
Worker Queries
Read Worker Config
Worker Config

12

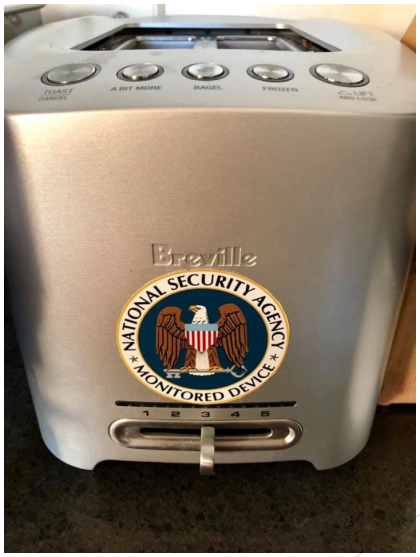
Takeaways

- Validate the Threat Model
  - Is there a design diagram?
  - Does diagram match code?
  - Are threats enumerated?
  - STRIDE

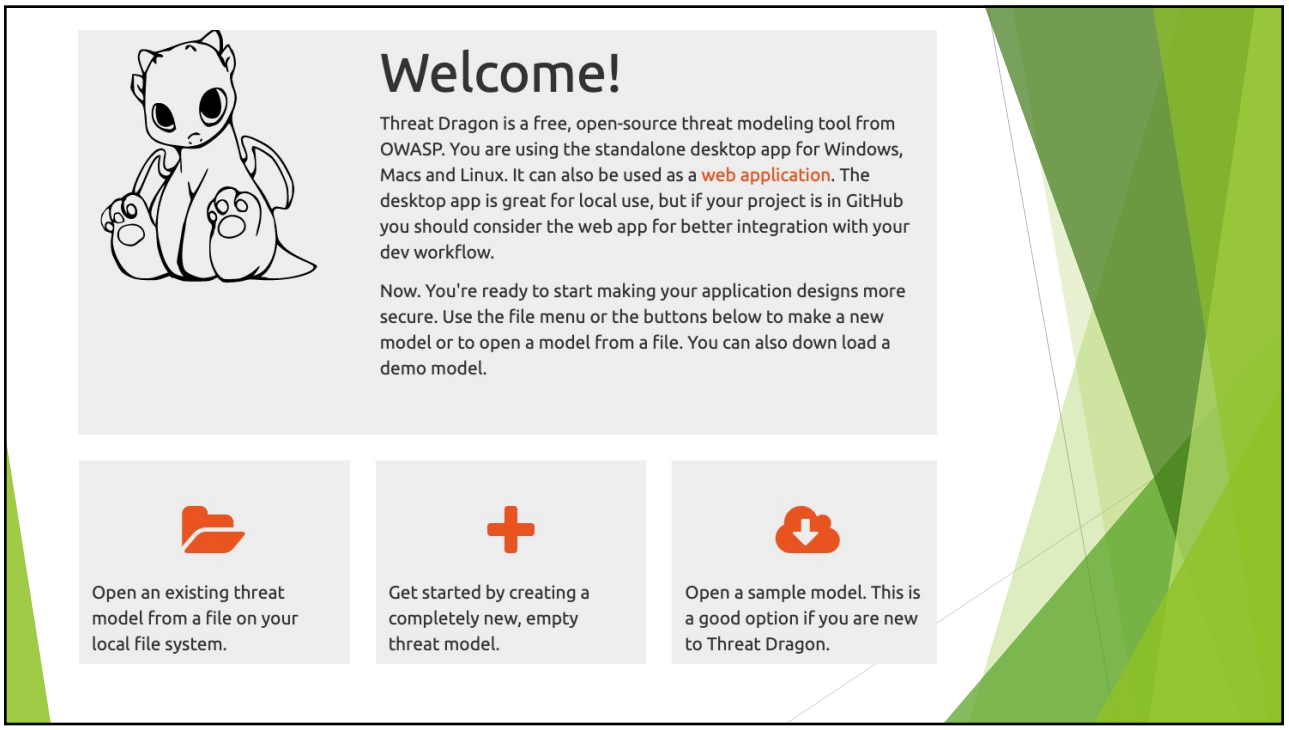
13

Some References

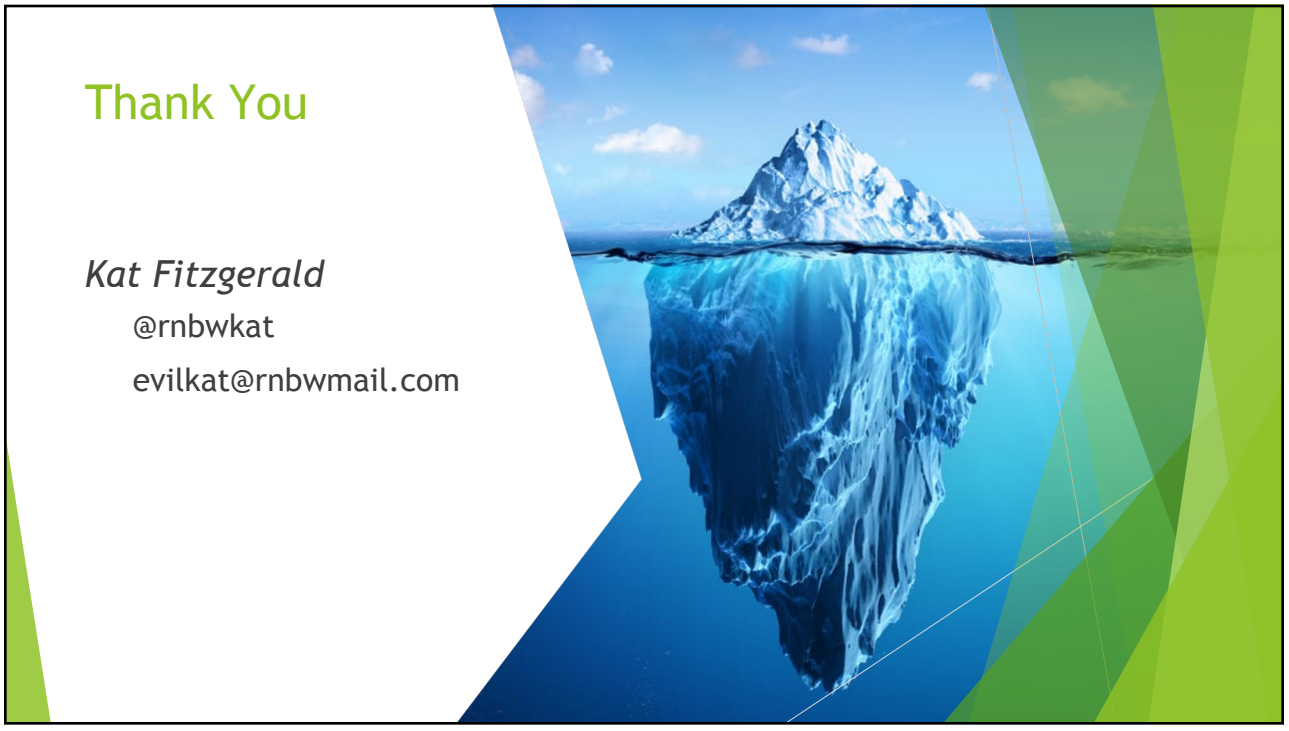
- Threat modeling by DDSec
- STRIDE
- Threat Modeling Manifesto
- OWASP Threat Dragon
- OWASP Threat Model Project



14


Welcome!
Threat Dragon is a free, open-source threat modeling tool from OWASP. You are using the standalone desktop app for Windows, Macs and Linux. It can also be used as a web application. The desktop app is great for local use, but if your project is in GitHub you should consider the web app for better integration with your dev workflow.
Now. You're ready to start making your application designs more secure. Use the file menu or the buttons below to make a new model or to open a model from a file. You can also down load a demo model.
Open an existing threat model from a file on your local file system.
Get started by creating a completely new, empty threat model.
Open a sample model. This is a good option if you are new to Threat Dragon.

15


Thank You
Kat Fitzgerald
@rnbwkat
evilkat@rnbwmail.com

16