THREAT MODELING IN 600 SECONDS
(OK, I LIED, MORE LIKE 2,400)

Kat Fitzgerald
@rnbwkat evilkat@rnbwmail.com

1

WHOAMI

- *Kat Fitzgerald*

CEO @BSidesChicago, CFP Chair @BSidesPGH, DefCon 3!

Many years in Security, with an emphasis on Blue Teams, (former Purple), DevSecOps, IR.

Based in Kirkland, WA and a natural creature of winter, you can typically find me sipping Grand Mayan Extra 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!

2

WHY WE AREN'T HERE

- I won't solve all your security problems
- Neither will the person sitting(?) next to you
- 2016 - Université du Luxembourg
  - 43.5%

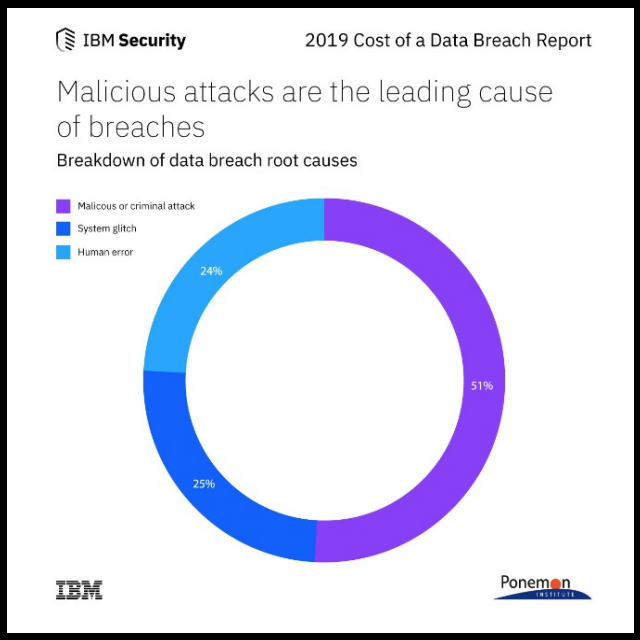
3

DON'T BELIEVE ME?

4

WHY WE ARE HERE

- 3 rules of SDLC
  - Security is not an Afterthought!
  - Vulns (and breaches) are real
  - Not if..
- And..
  - Companies spent $150B on Security "stuff" in 2021
    - Breaches and Incidents continue to rise



5

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*

6

TRADITION

- How it has been

Security Review & Pen Test
79 vulns

Development + QA

Oops!

Production Deadline

7

A BETTER WAY

- How it should be

Threat Modeling & Security Review
9 vulns

Development / Security

Remediation, Dev & Q&A

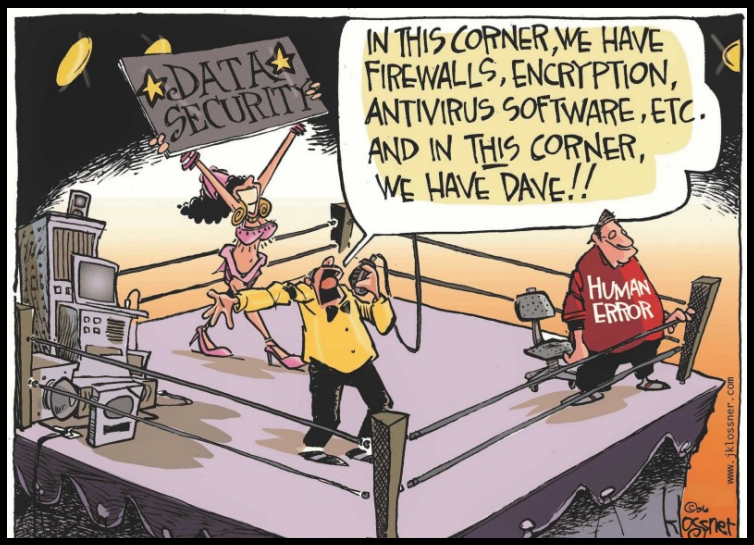
Production Deadline

Teamwork!

YAY!!

8

THREAT MODELING IN 30 SECONDS



9

THE THREE STAGES

- Threat Modeling - 3 high level stages
  - Decompose application
  - Determine and rank threats
  - Determine mitigations

10

IDENTIFY, ENUMERATE, PRIORITIZE

Diagram
- What are we building?
- What/where are high-value targets?

Identify Threats
- What can go wrong?
- Where are attack vectors?

Mitigate
- What/How do we fix all the things?

Validate!

Attacks keep getting better, so should your TM!

11

IDENTIFY ASSETS

- What are you protecting
  - High level ← *Always*
  - Break it down as you go
- Other "assets"
  - CIA
    - Confidentiality
    - Integrity
    - Availability

12

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)*

13

DECOMPOSE

- Refine the Architecture
  - Show AAA
    - Don't forget the third "A"?
  - Trust Boundaries
  - Show Technologies
  - Ingress/Egress points

14

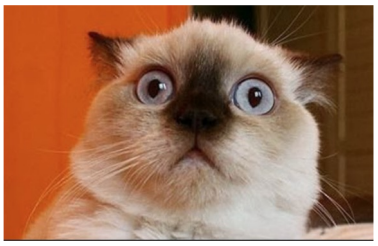
WHY?

- Most Vulnerabilities are introduced during *design phase*
- Architecture Flaws are hard to change
- Secure By Design!
- Attackers Think Differently

15

Identify Threats

- STRIDE
  - Spoofing
    Access using false identity
  - Tampering
    Modify data
  - Repudiation
    Prove who did it
  - Information Disclosure
    Access the data
  - Denial of Service
    Still counts!
  - Elevation of Privilege
    Assume priv user



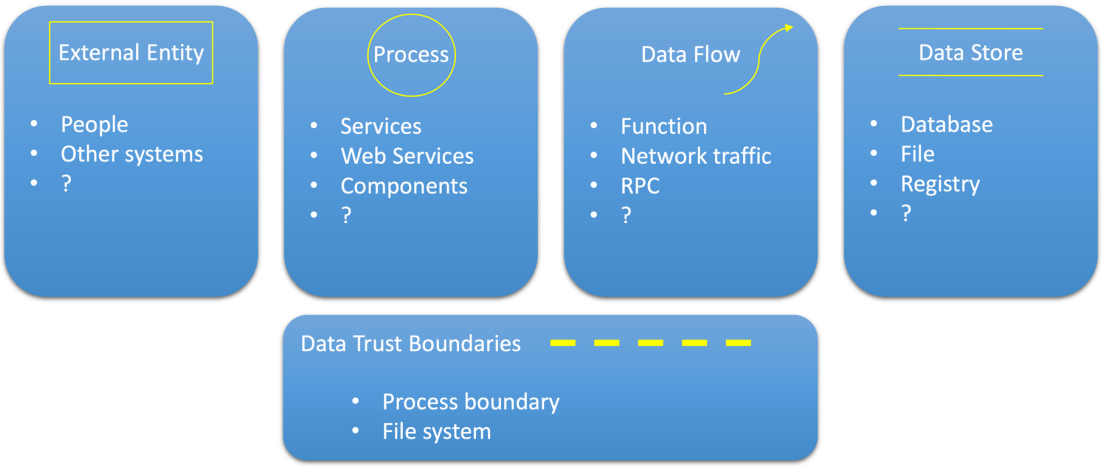
16

DFD – DATA FLOW DIAGRAM

- DFD = A graphical representation of the "flow" of data
  - Not the flow of control - that's a flow chart
- Processes can run in parallel
- Simple Steps
  - Start at High level (see, I told you)
  - This is the "Context Level" - entities & processes
  - Level 0 - Subprocesses
  - Level 1-n - Data flows, data stores and boundaries

17

DFD SYMBOLS



18

LET'S DO THIS!

EXAMPLE TIME

- Identify Assets
- Identify External Entities
- Trust Boundaries
  - Systems, privileges, integrity, networks – all examples

19

THREAT MODEL THIS

Women's Leather RFID Blocking Small Wallet

20

THREAT MODEL THIS

21

DFD CHECKLIST

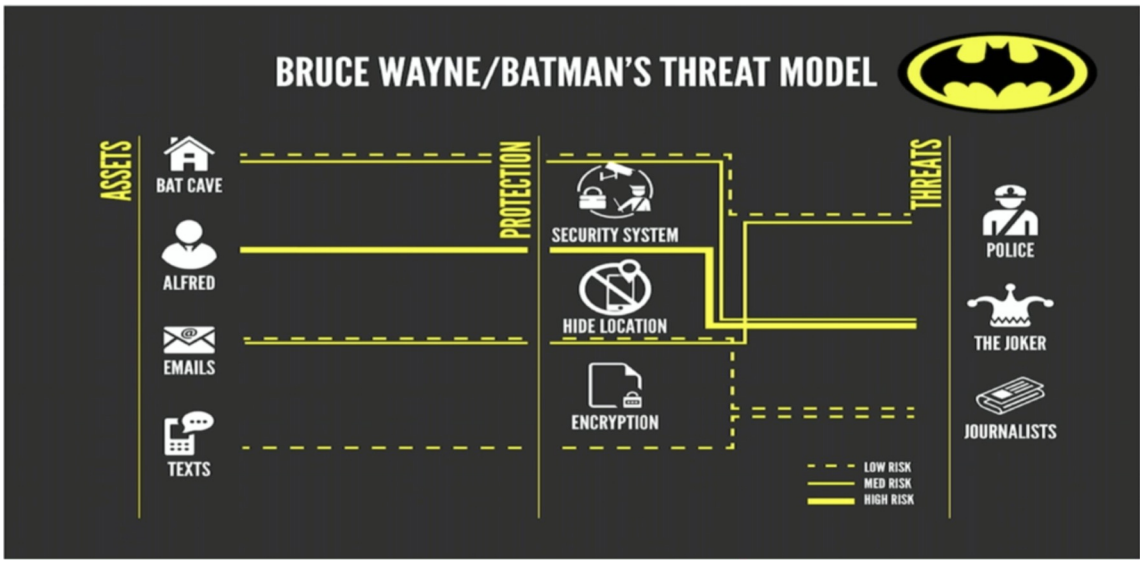
- Define Scope
- Break down, identify all the assets
- Start your diagram
  - Context (L0)
  - Just keep ~~swimming~~ layering
  - Add dataflows (not a flowchart)
- Add where important data:
  - lives
  - transits
  - transforms

22

DFD CHECKLIST (2)

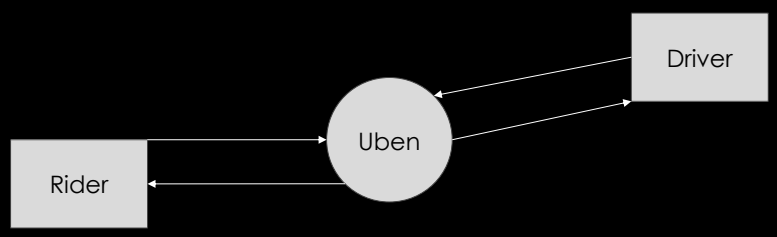
- Start with DFD 0 – Context
  - Label all assets
- Add "flows" including directions
  - Label main action on each flow
  - Don't forget protocols
- Add Trust Boundaries (and networks)
- Label "types" of data and flow
- Add ppl and types
- Label each Authentication process
- Label each Authorization process
- Add order of all the actions
- Identify "Crown Jewels"
  - Data Classification
  - Transit/Rest

23



24

"RIDE-SHARING APP"

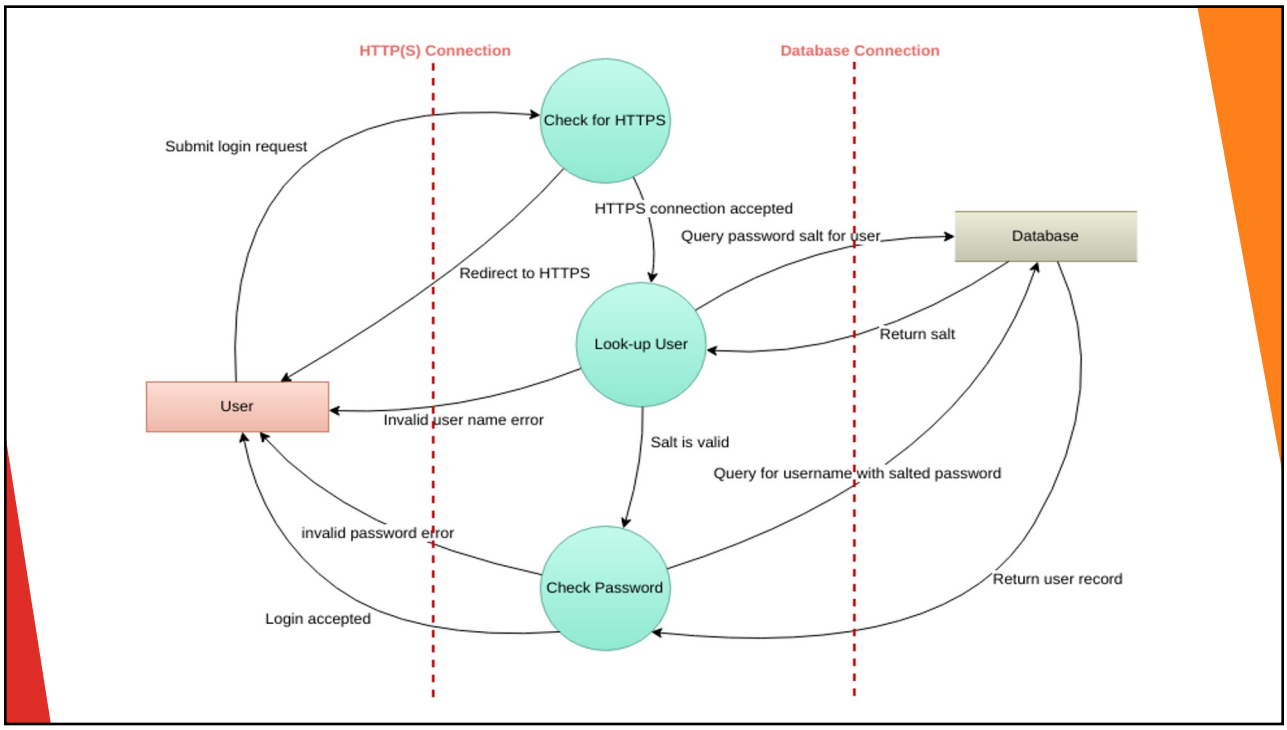


25

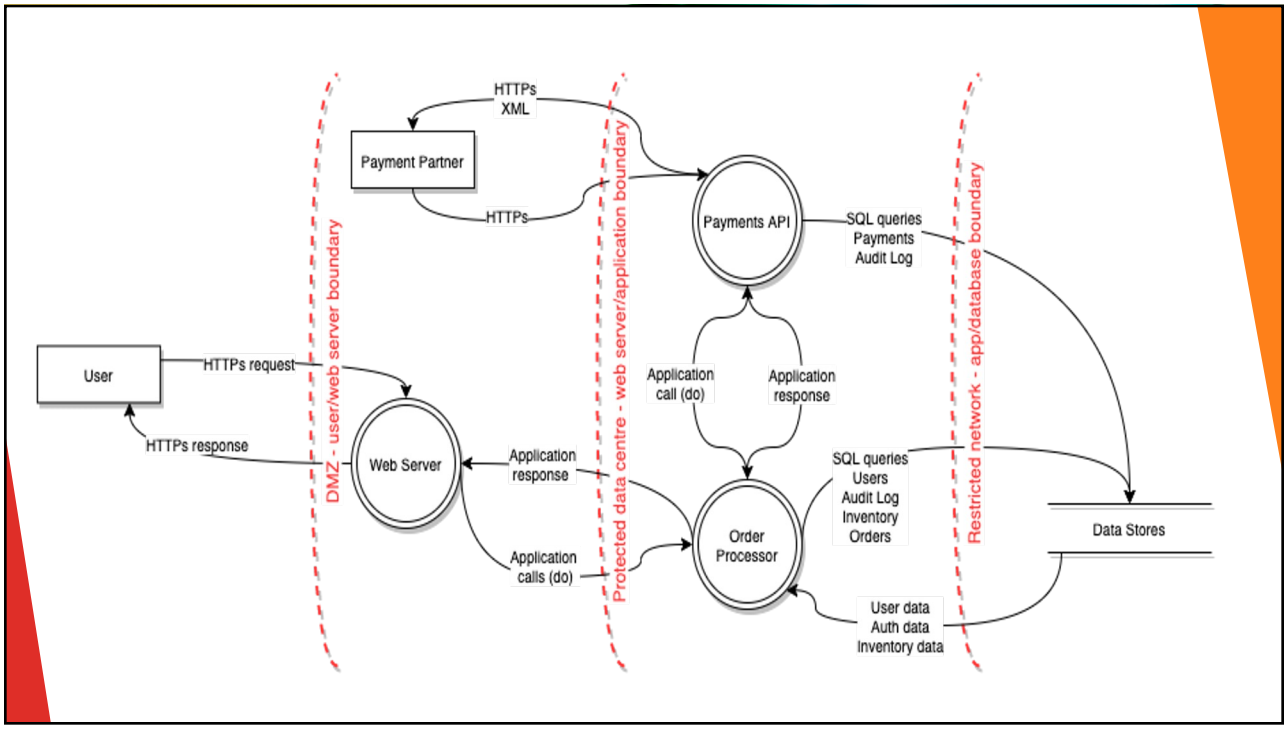
DFD 1

- And remember ..
- Defining Threats
  - Describe the Attack
  - Describe the Context
  - Describe the Impact

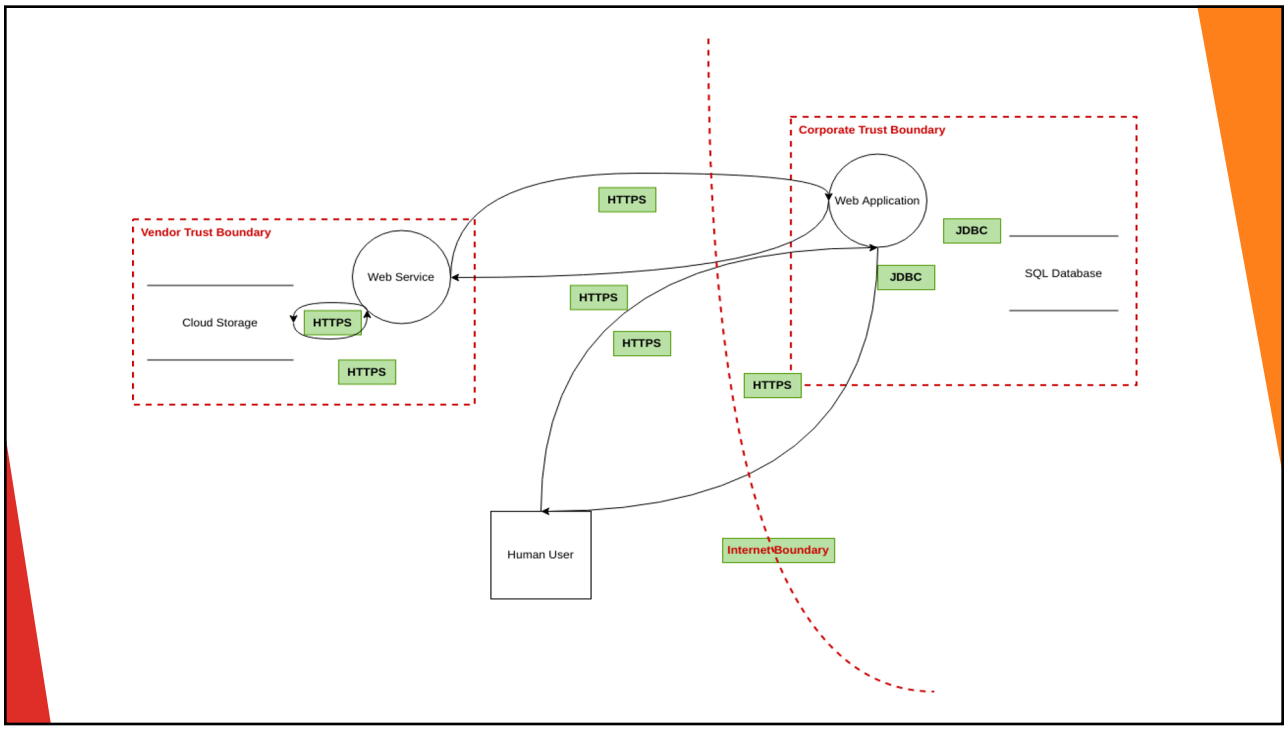
26


HTTP(S) Connection
Database Connection
Check for HTTPS
Submit login request
HTTPS connection accepted
Query password salt for user
Database
Redirect to HTTPS
Look-up User
Return salt
User
Invalid user name error
Salt is valid
Query for username with salted password
invalid password error
Check Password
Return user record
Login accepted

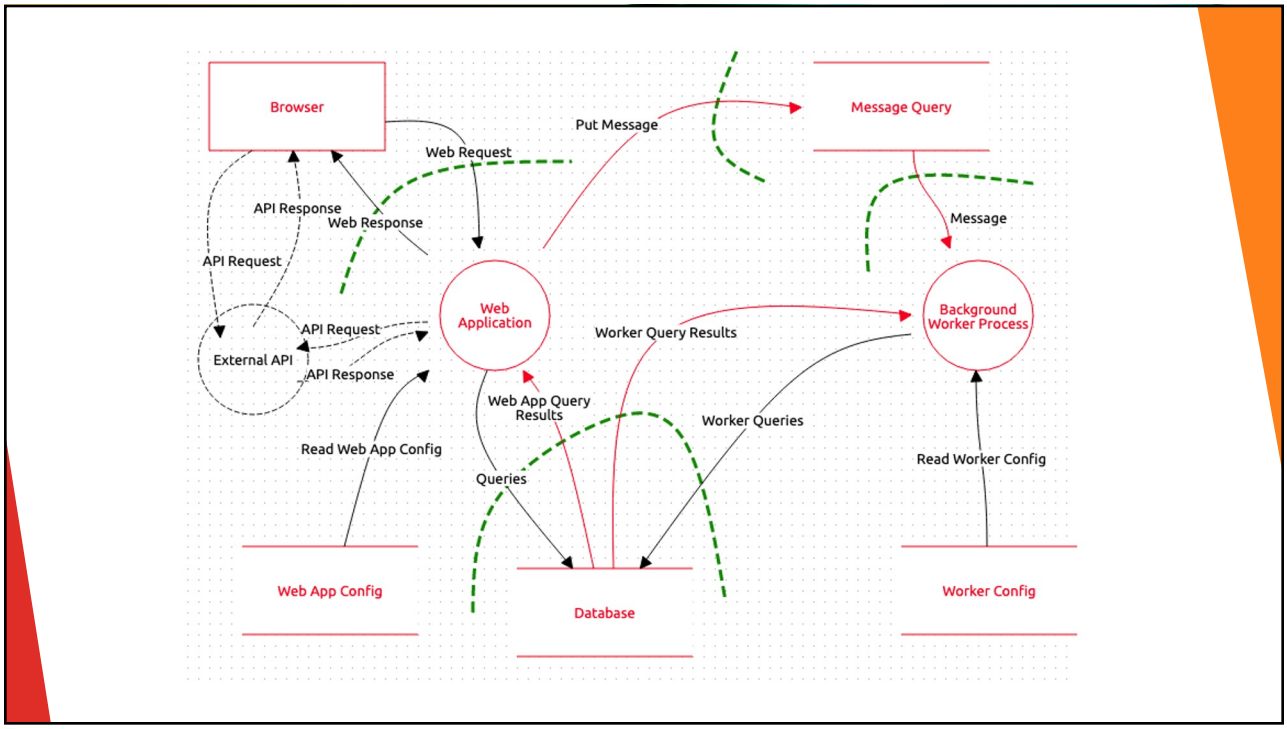
27


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

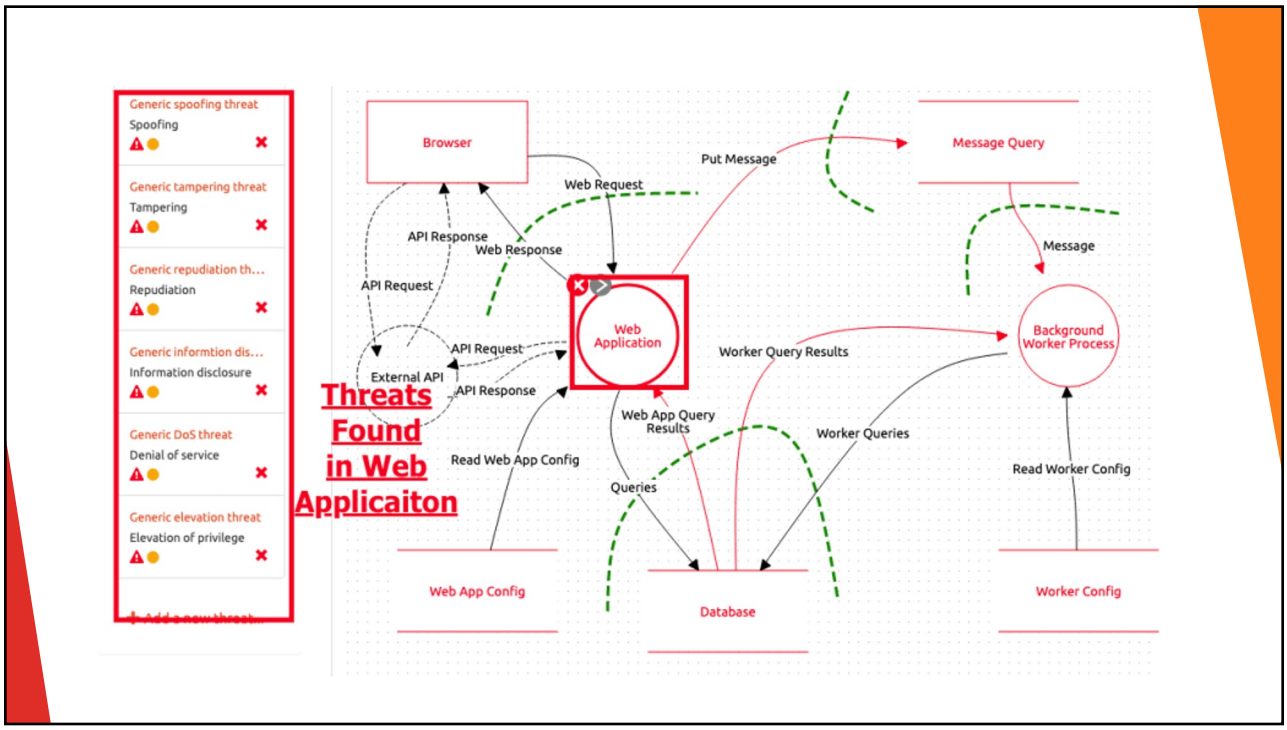
28


Corporate Trust Boundary
Web Application
JDBC
SQL Database
JDBC
HTTPS
Vendor Trust Boundary
Web Service
Cloud Storage
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
Human User
Internet Boundary

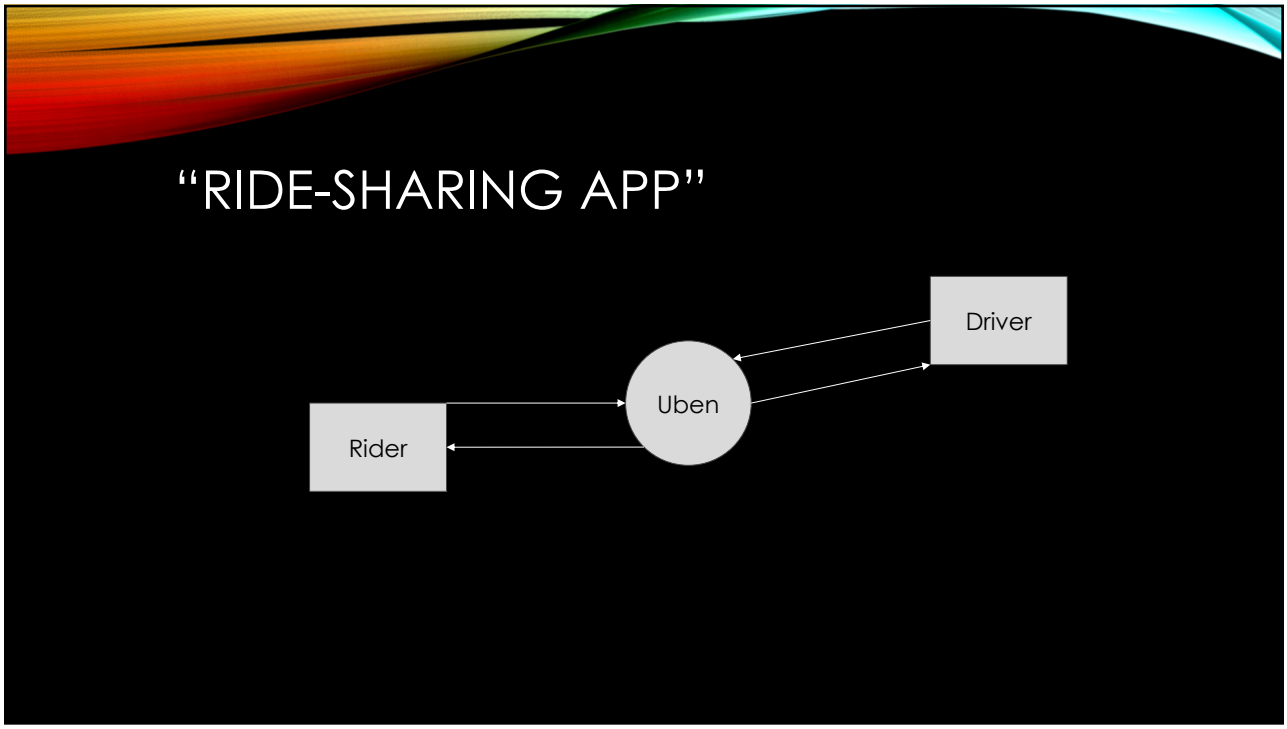
29


Browser
Put Message
Message Query
Web Request
API Response
Web Response
Message
API Request
Web Application
Background Worker Process
API Request
External API
API Response
Worker Query Results
Web App Query Results
Worker Queries
Read Web App Config
Queries
Read Worker Config
Web App Config
Database
Worker Config

30


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
Put Message
Message Query
API Response
Web Response
Message
API Request
Web Application
Background Worker Process
API Request
Worker Query Results
External API
API Response
Web App Query Results
Worker Queries
Read Web App Config
Queries
Read Worker Config
Web App Config
Database
Worker Config

31


"RIDE-SHARING APP"
Driver
Uben
Rider

32

TAKEAWAYS

- Validate the Threat Model
- Detailed DFD
- Trust Boundaries are Critical
- Are threats enumerated?
  - STRIDE
- Define Done(?)
  - CTM – Continuous Threat Modeling

33

TAKEAWAYS (PT 2)

- Secure by Design
  - Not by Incident!
- Threat Actors have all the time in the world
  - You don't
- Diagraming!
  - Trust Boundaries are Critical!
- Iterate - CTM

And finally - Threat Modeling can model ANYTHING, not just programs. Next time you fly..

34

TOOLS / RESOURCES

- Threat Modeling w/Terraform
- IriusRisk Community & Commercial
- Cairis
- SecuriCAD (Foreseeti)

35

AND SOME MORE

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

36

Thank You!!

@rnbwkat
evilkat@rnbwmail.com

37