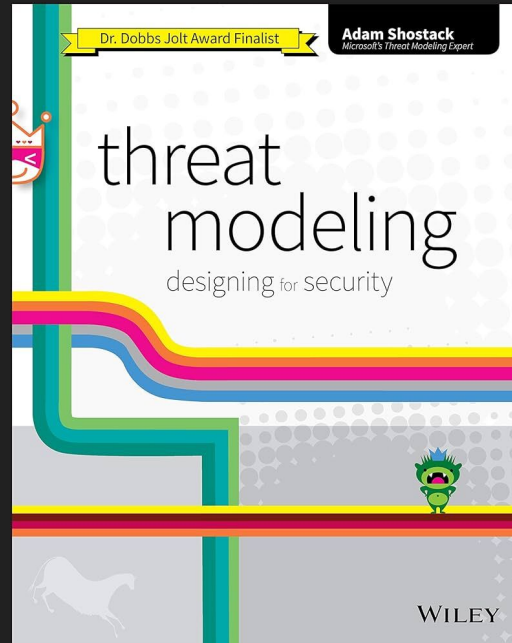


Whose Threat Model is it  
Anyway!?

# The Presentation where the Scenarios are Made Up And the Controls Don't Matter



# AKA Travis Read a Book on Threat Modeling and now he has Opinions



Starring: My Garage Door! (Later)



# About Me

- Travis Friesen, <letters go here>
- Senior Infrastructure Developer at Neo Financial
  - With a generous side helping of Cloud Security

# About Me

- I do computers

# About Me

- I do computers
  - Just like everyone else



I like to Cook!



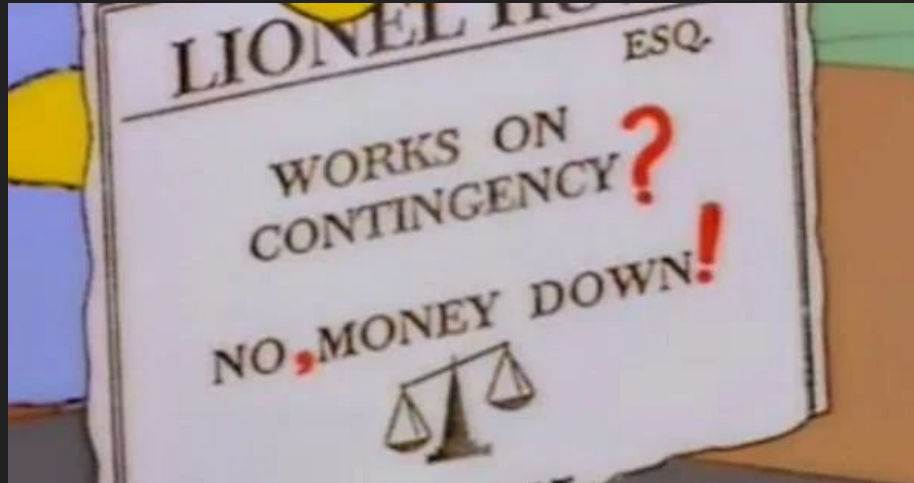


Just turned 40

(Probably) Have ADD

# What is Threat Modelling? A Threat Model?

- Threat Modelling -> creating a Threat Model ?
  - No!



# Threat Modelling vs A Threat Model

- Threat Model is what you use to do Threat Modelling
- Threat Model -> inputs, framework within which you do Threat Modelling
  - Threat Model is what informs the activity of Thread Modelling

# Threat Modelling vs A Threat Model

- Think of it like the initial parameters for a model of the solar system
  - Or other system



What. Is. Threat. MODELLING?



# Brainstorming

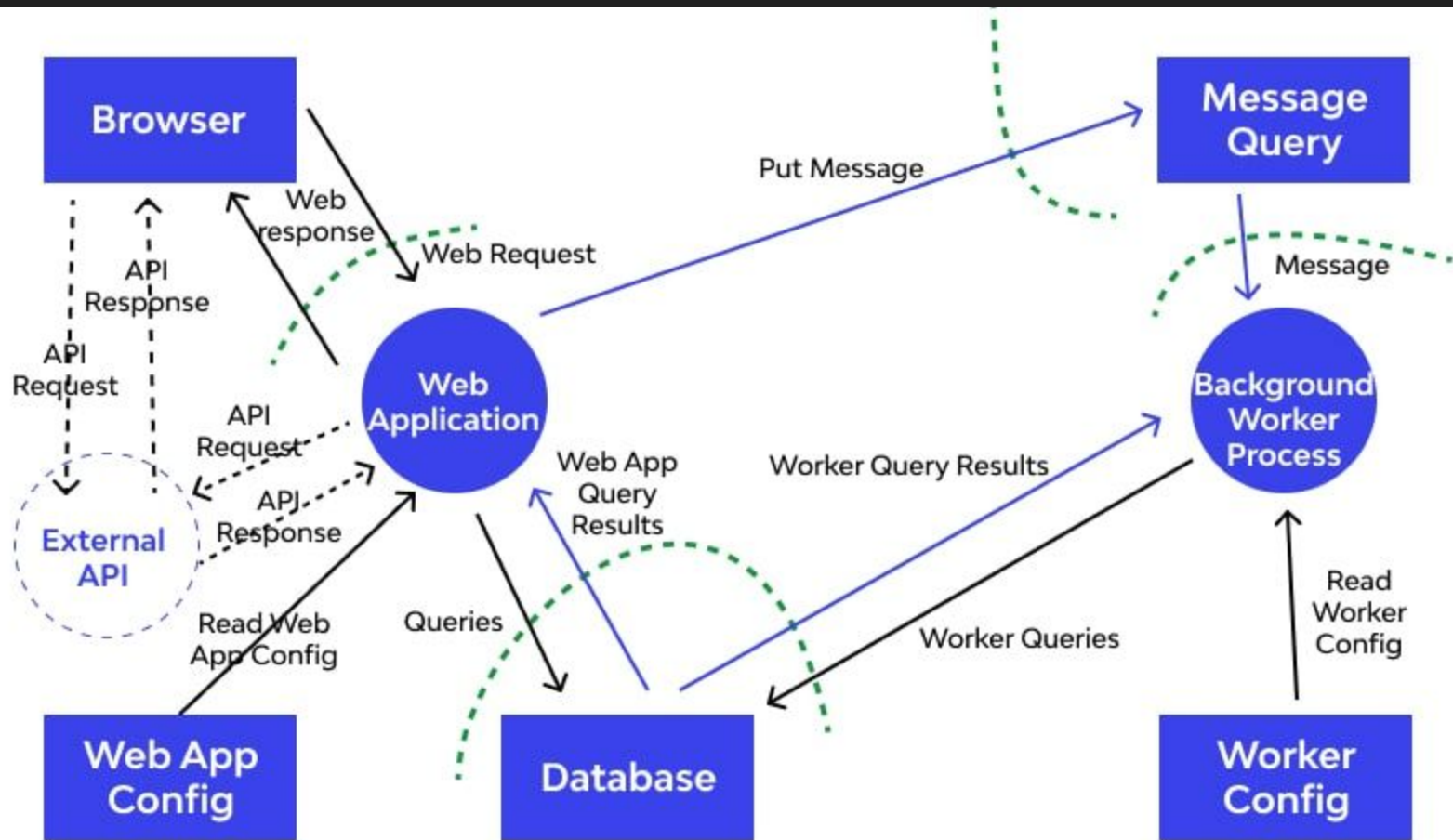
- Fancy Brainstorming
  - Ideally focussed and structured
- Finding ways to improve the security of a system by ‘modelling potential threats’

# Why do Threat Modelling?

- Ultimately: make your system(s) moar secure.
- Find vulnerabilities and bugs
  - Ideally, earlier in the development process
- *Focused* approach to security

# What is a Threat Model?

- High level description or diagram (model) of the system we're trying to secure
- Threat Actors and their motivations
- Potential goals, resources, 'crown jewel' that a threat actor might be interested in
  - Money, data, CPU time



# Importance of a good Threat Model

- Allows you to focus on *relevant* threats
- Sometimes less important about what's *in* your Threat Model than what *isn't*
- All controls have a cost

# Threat Actors: Example Categories

- Government Agencies (CIAs, NSAs, KGB, etc)
- Big-time criminals
- Hacktivists, competitors
- Small-time criminals, insiders
- Script kiddies



# What's not in my Threat Model?

- (Probably) The NSA
  - You're just not that interesting
- (Probably) Your cloud provider
  - The path of madness
  - Have to take it fully seriously, or not at all

# Threat Models: A Case Study: My Garage Door

“After learning to pick locks for the first time, I immediately went home and purchased new locks for my front door.”

Locks are for keeping honest people out









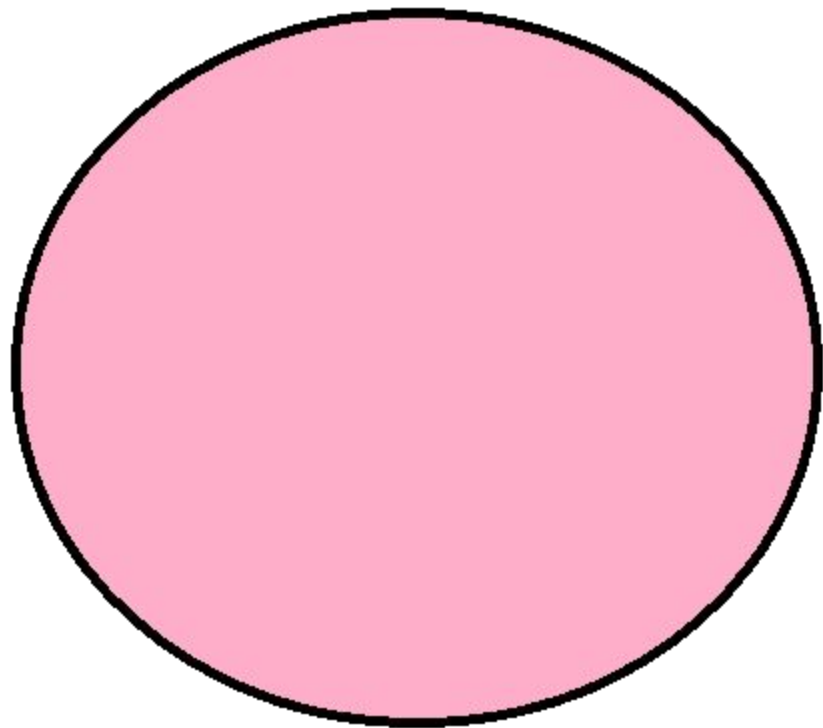




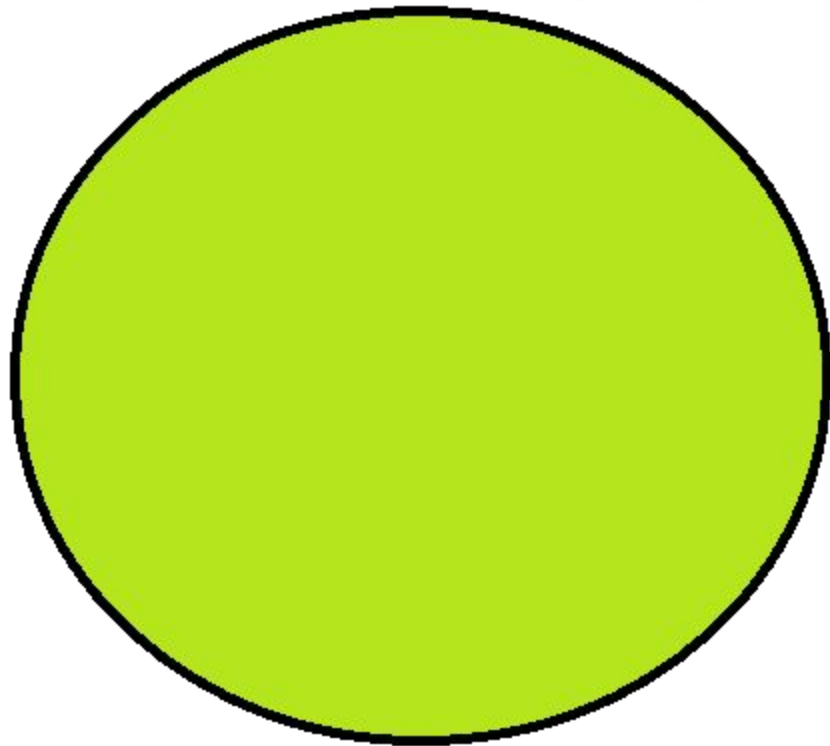
# LOCK PICKING



**People willing to learn  
to pick locks**



**People interested in the  
contents of my garage**



In my threat model:

- People with bolt-cutters

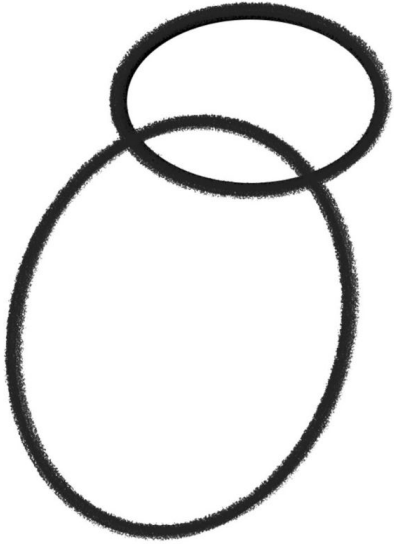
Not in my threat model:

- People who know how to pick locks

# How to do Threat Modelling

- Step 1: Build your Threat Model
  - Describe system and components at a high level
  - Determine threat actors and motivations
    - Coming for you money or your data? What is valuable to them?

## Step 2: Do the threat modelling



Step 1: Draw some circles



Step 2: Draw the rest of the owl!

## Tip? Think like an attacker!

- How could an attacker abuse this system?
- Great idea, Easier said than done
  - Most people don't know how to think like an attacker
  - Requires special skills



# S.T.R.I.D.E.

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

# STRIDE Examples

- Spoofing
  - What if an attacker sends data from a fake IP? An account?
- Tampering
  - Replay messages
  - Modifying cookies or request URLs
- Information Disclosure
  - Revealing error messages, introspection

# Similarly

(But more concretely)

- OWASP Top 10
- MITRE ATT&CK

# Attack Trees



## Step 3

- Actually fix the bugs and vulnerabilities you find