# Threat Modeling Workshop



## **Threat Modelling**

Security is goals vs adversaries

Policy: What do you want the system to do?

Threat Model: Assumptions about the bad guys

Mechanisms: HW, SW and systems to mitigate



# Lecture Recap...

STRIDE, PASTA and DREAD



STRIDE PASTA

**Identify** assets

Create an architecture overview

Decompose the application

**Identify threats** 

**Document threats** 

Rate threats

Define business and security objectives

Define the technical scope

Decompose the application

Perform a threat analysis

Identify weaknesses and vulnerabilities

Attack and exploit enumeration

Risk impact analysis

## Damage Reproducibility Exploitability Affected Users Discoverability

**DREAD** 

None = 0 Low = 1 Medium = 2 High = 3

(D+R+E+A+D)/5 = RISK

Is RISK > 1:

Fix NAO

Is RISK <1:

**FIX TOMORROW** 

(DreaD-D)



# "All models are wrong, but some are useful"

George Box, 1976



## Netflix is offering user contributions!

Today's challenge

#### Netflix

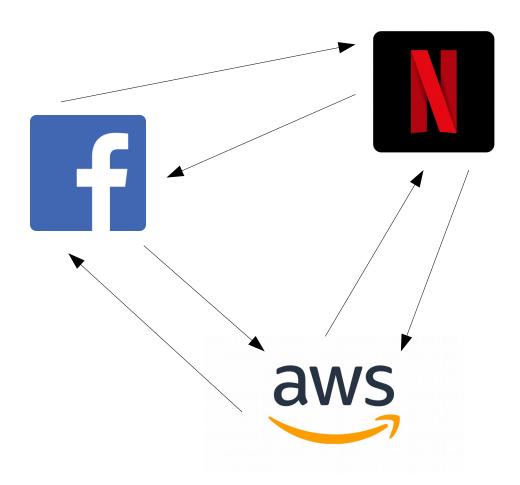
- User submissions
- Video Streaming

## Facebook API

- OAuth
- User Identification

#### Amazon Web Services

- Cloud storage
- Microservices



#### Systems Thinking/ Trust Boundaries

Mat Honan, wired.com, 2012 - https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

- Gmail
  - Reset Password, sends to secondary email address
- me.com (Apple)
  - Reset Password, requires address and last four digits of credit card
- Amazon
  - Can add credit cards without being logged in, requires account name, email address and billing address (via phone)
  - Reset Password, requires credit card