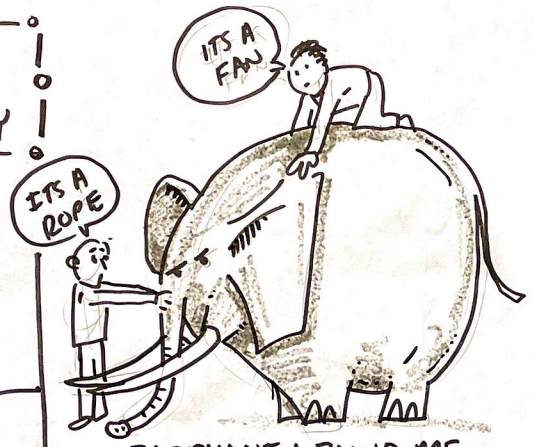
RAHUL RAGHAVAN

We45

THREAT MODELING WINS FOR AGILE APPLICATION SECURITY



ELEPHANT + BLIND ME

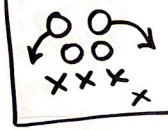
WHAT THREAT IS MODELING DEPENDS ON WHERE YOU STAND

WHY THREAT MODELS FAIL

APP SEC TODAY

- TOOLING
- TEST ITERATIONS
- * "X" AS CODE

→ THREAT MODELING AS CODE



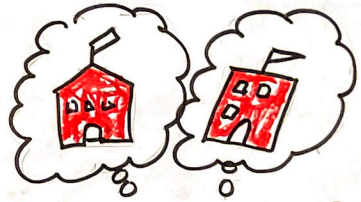
THREAT PLAYBOOK
- STORY-BASED
- AVAILABLE PUBLICALLY

3 FLAVORS OF TEST CASE
- TOOL
- SCRIPT
- HYBRID

MOTIVATION FOR THREAT MODEL DIFFERS BASED ON YOUR ROLE

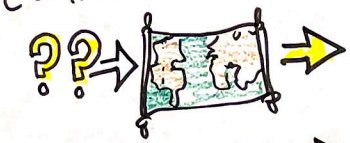
- BUT HAS SOMETHING FOR EVERY PERSON
- BUT NO "ONE SIZE" FITS ALL

FAILURE MODES
- NOT UNDERSTAND "WHY" WE ARE THREAT MODELING
- OVER-EMPHASIZE ON HOW?



THREAT MODEL SCHOOLS OF THOUGHT
- STORY-DRIVEN
  - WHAT IF?
  - ABUSE CASES
  - FOCUS ON DEPTH
- COMPONENT DRIVEN
  - SYSTEM FOCUS
  - KNOWN ISSUES
  - FOCUS ON SCALE

COMPONENT THREAT MODELING



THREATS →

COUNTER MEASURES →

STORY-DRIVEN THREAT MODELING

USE CASE — WHAT DOES IT DO?

WHAT COULD POSSIBLY GO WRONG?

ABUSE CASE