THREAT MODELLING

When you’ve never done it before

WHO AM I?

- Kade Morton
- Security Consultant with Quantum Security
- BA Criminology and Criminal Justice
- Mentor Mozilla Open Leaders

THIS IS THE STORY

- Of going from knowing nothing…
- To basic threat modelling
- This is the beginning but not the end

MOZILLA OPEN LEADERS

- https://foundation.mozilla.org/en/opportunity/mozilla-open-leaders/
- Mentees that have already been through OL are invited to be mentors
- You help mentees work through OL coursework
- Provide skills based assistance

WHO WAS I MENTORING?

- Asuntos del Sur
- ADS has the central objective of becoming a platform for deliberations and transformation actions to generate more democratic and inclusive societies in Latin America.

BASIC THREAT MODELLING

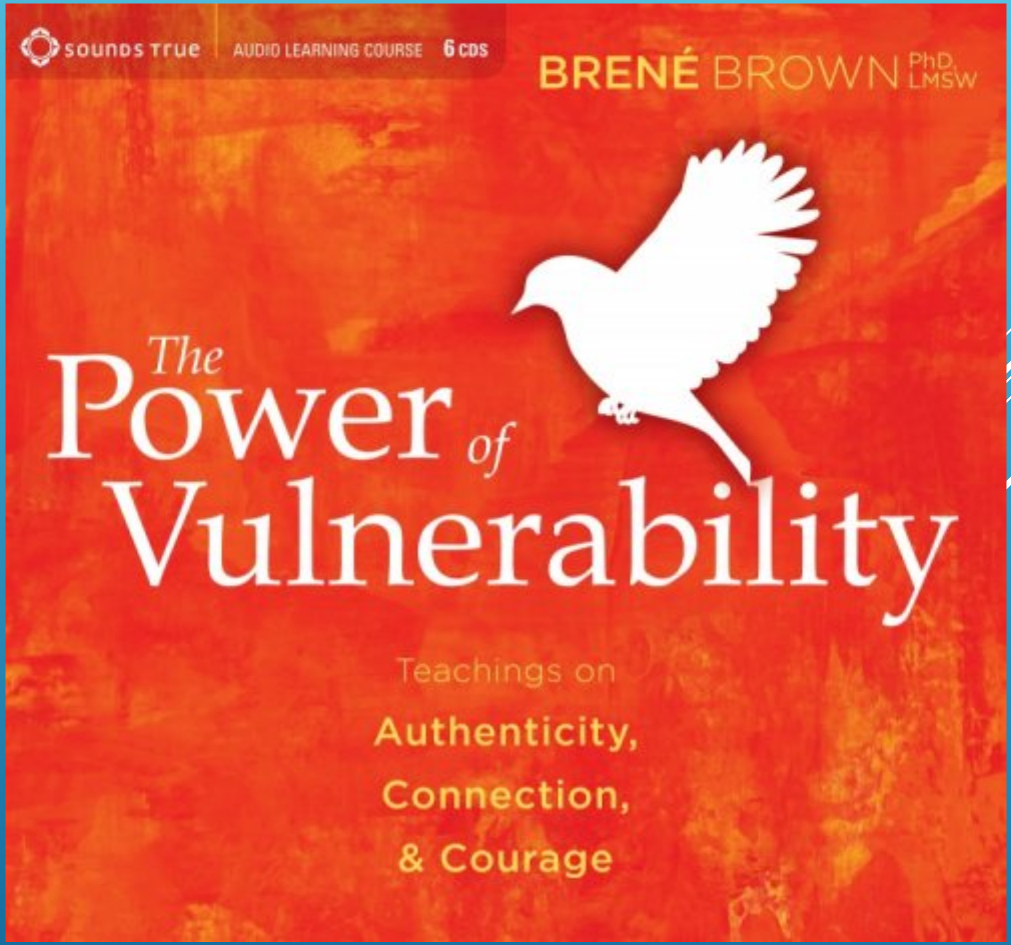
- Hacked together from Microsoft's STRIDE threat modelling approach
- Three questions:
  - What are you building?
  - What can go wrong? STRIDE
    - Spoofing of user identity
    - Tampering
    - Repudiation
    - Information disclosure
    - Denial of Service
    - Elevation of privileges
  - What are you going to do about it?

WHAT IS A RISK?

- A risk is the "possibility of loss or injury"
- An **event** that causes loss or injury

WHAT IS A VULNERABILITY?

- A vulnerability is "an opening to attack or damage"
- An **intrinsic aspect** about something that enables loss or injury


sounds true
AUDIO LEARNING COURSE 6 CDS
BRENÉ BROWN PhD, LMSW
The Power of Vulnerability
Teachings on Authenticity, Connection, & Courage

WHAT IS A THREAT?

- A threat is "an indication of something impending"
- **Something/someone** might inflict loss or injury

WHAT DO YOU GET WHEN YOU PUT ALL THAT TOGETHER?

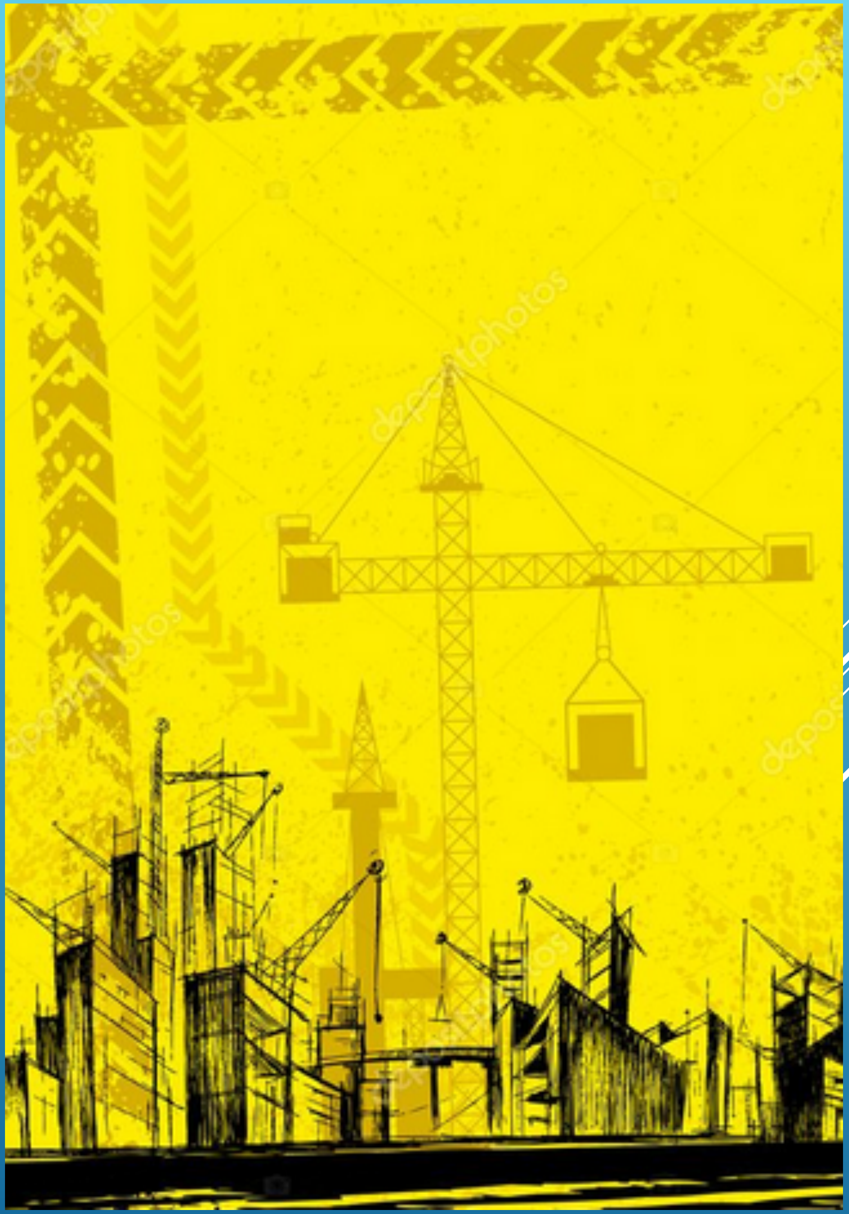
- We may all die (event, risk) because we are malnourished (intrinsic aspect, vulnerability) and can't fight off the plague (something, threat)
- Our web app may disclose information about users (event, risk) because hackers (someone, threat) exploit the lack of sanitisting entries to input fields (intrinsic aspect, vulnerability) in our web app

WHAT IS THREAT MODELLING AND WHY WOULD I WANT TO DO IT?

- Threat modelling: identifying the ways that something/someone can inflict loss or injury to us
- They will leverage vulnerabilities
- The event of loss and injury is the risk
- Why threat model? To put things in place to minimise the loss or injury

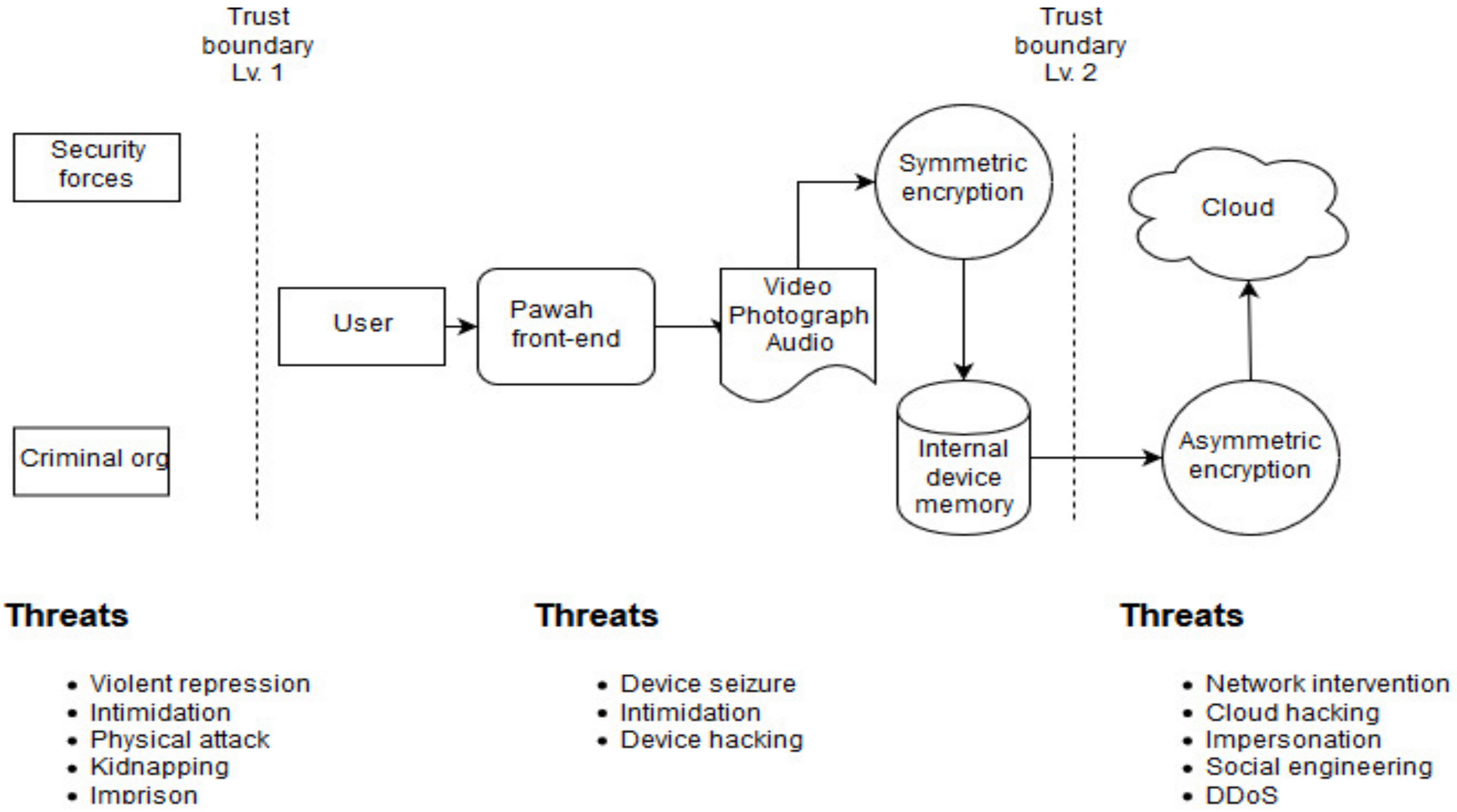
REMEMBER! BASIC THREAT MODELLING

- Three questions:
  - **What are you building?**
  - What can go wrong?
  - What are you going to do about it?



WHAT WAS ASUNTOS DEL SUR BUILDING?

- an app designed to defend the right to social protest
- …an application that allows the confidential and comprehensive recording of evidence of acts of human rights violations so that they can be subsequently reported



Threats

- Violent repression
- Intimidation
- Physical attack
- Kidnapping
- Imprison

Threats

- Device seizure
- Intimidation
- Device hacking

Threats

- Network intervention
- Cloud hacking
- Impersonation
- Social engineering
- DDoS

Trust boundaries – data shifts environment

Boundary around the app on the phone and cloud storage

THIS IS ALL VERY HIGH LEVEL

- Need to go lower
  - Enumerate
    - Technology
    - Protocols
    - Functionality that can be abused (PIN reset)
  - Flesh out connected systems
    - Cloud storage
    - Spoiler alert: Code repository
    - Spoiler alert: Log server

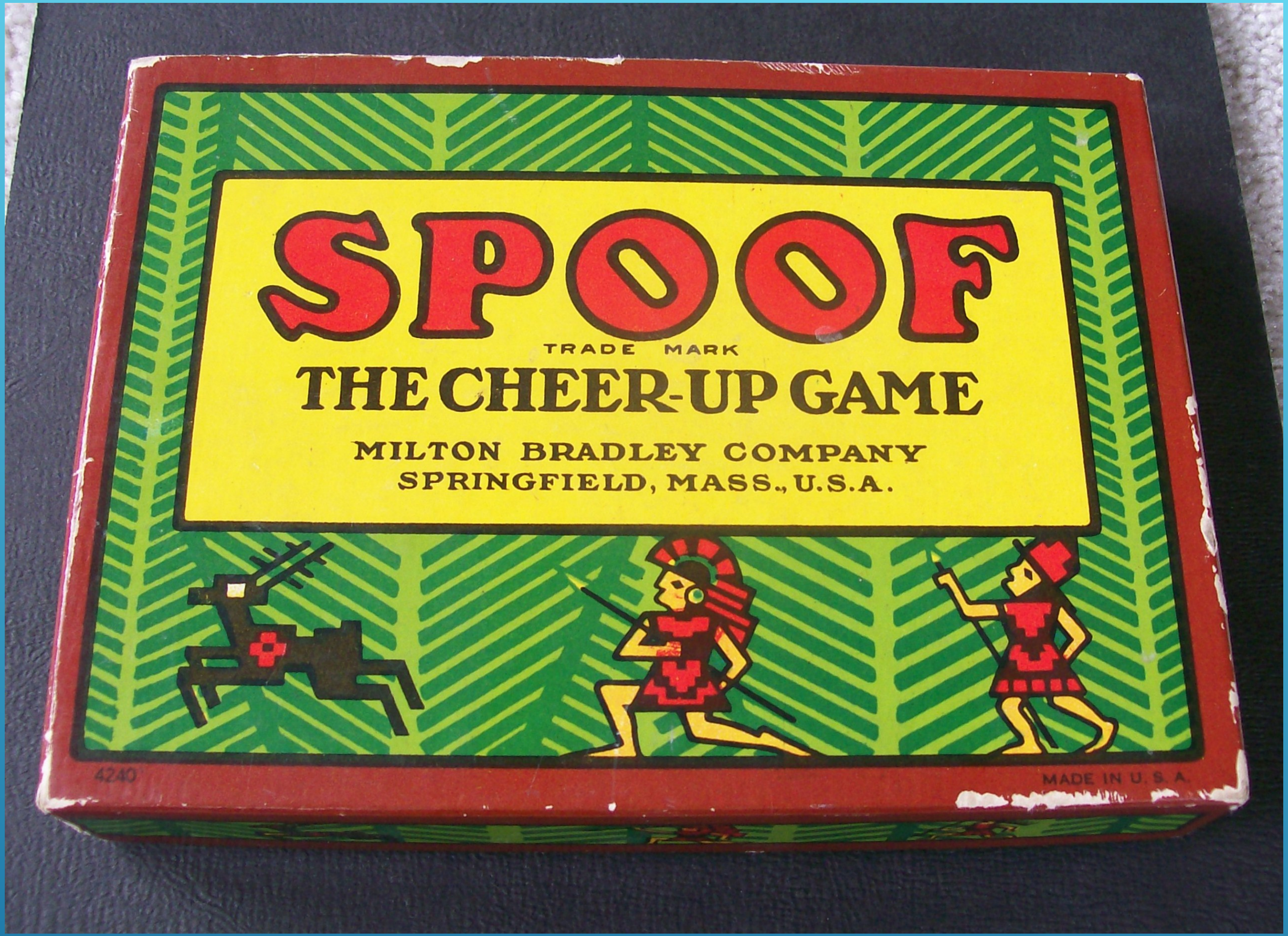
"You can't just copy-pase pseudocode into a program and expect it to work"
that's where you're wrong kiddo
python

REMEMBER! BASIC THREAT MODELLING

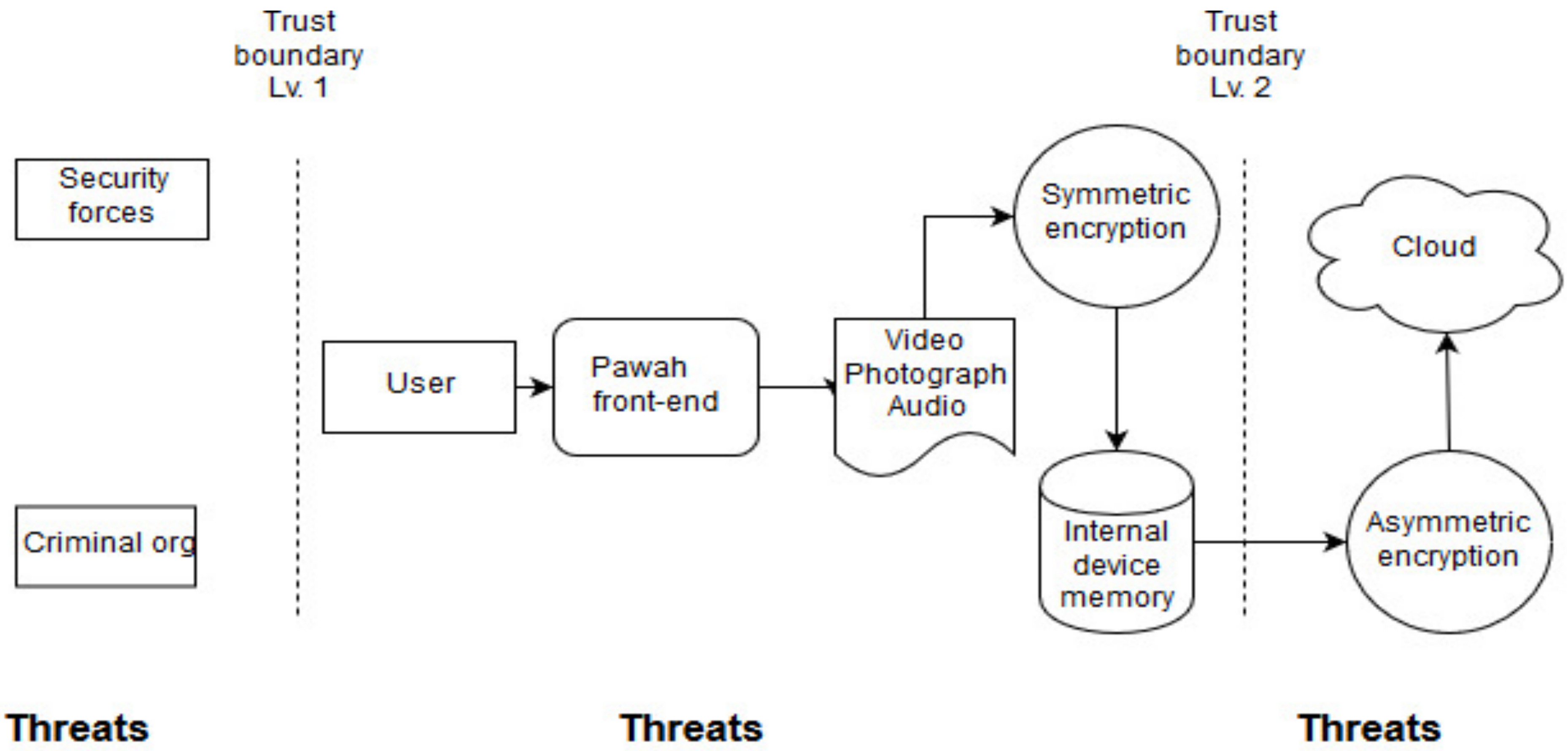
- Hacked together from Microsoft's STRIDE threat modelling approach
- Three questions:
  - What are you building?
  - **What can go wrong?**
  - What are you going to do about it?

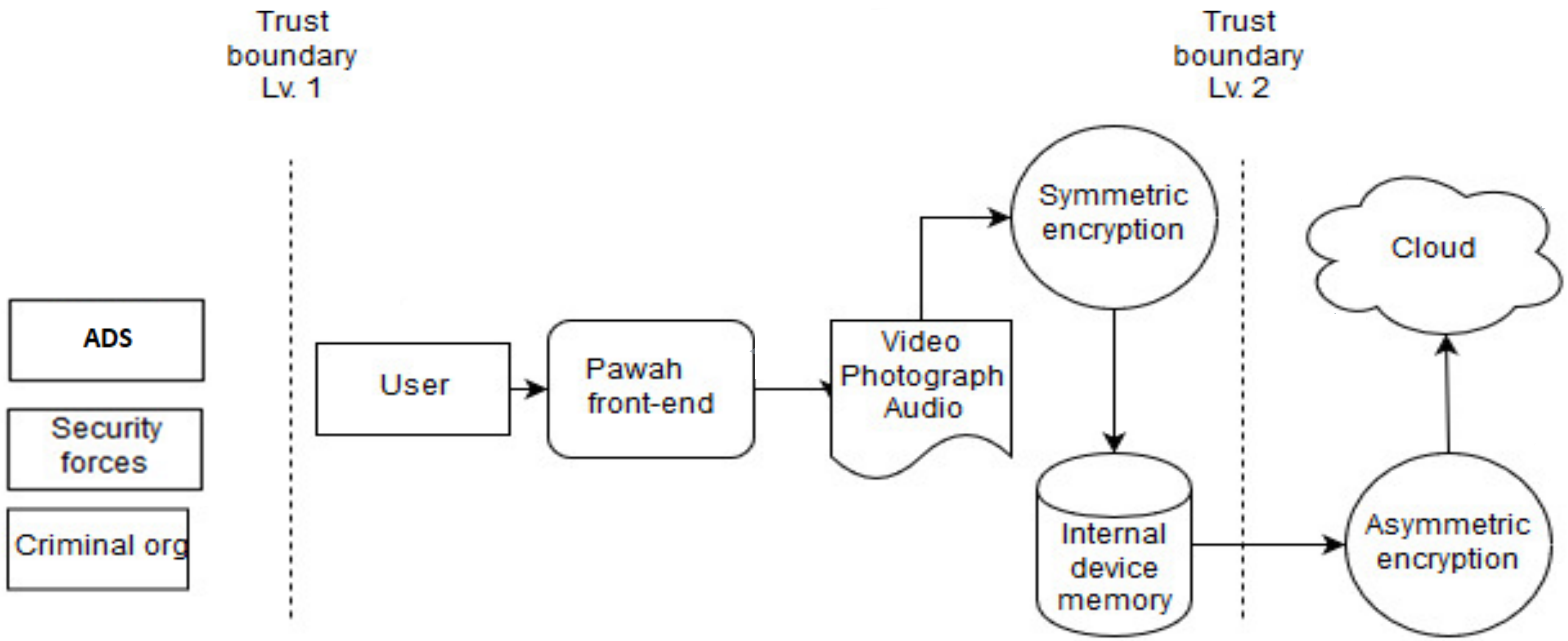
STRIDE

- Spoofing of User Identity
- Tampering
- Repudiation
- Information disclosure
- Denial of Service
- Elevation of privileges
  - Created by Microsoft
  - https://web.archive.org/web/20070303103639/http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx



STRIDE - SPOOFING OF USER IDENTITY


Trust boundary Lv. 1
Trust boundary Lv. 2
Security forces
Criminal org
User
Pawah front-end
Video Photograph Audio
Symmetric encryption
Internal device memory
Asymmetric encryption
Cloud
Threats
Threats
Threats



Threats

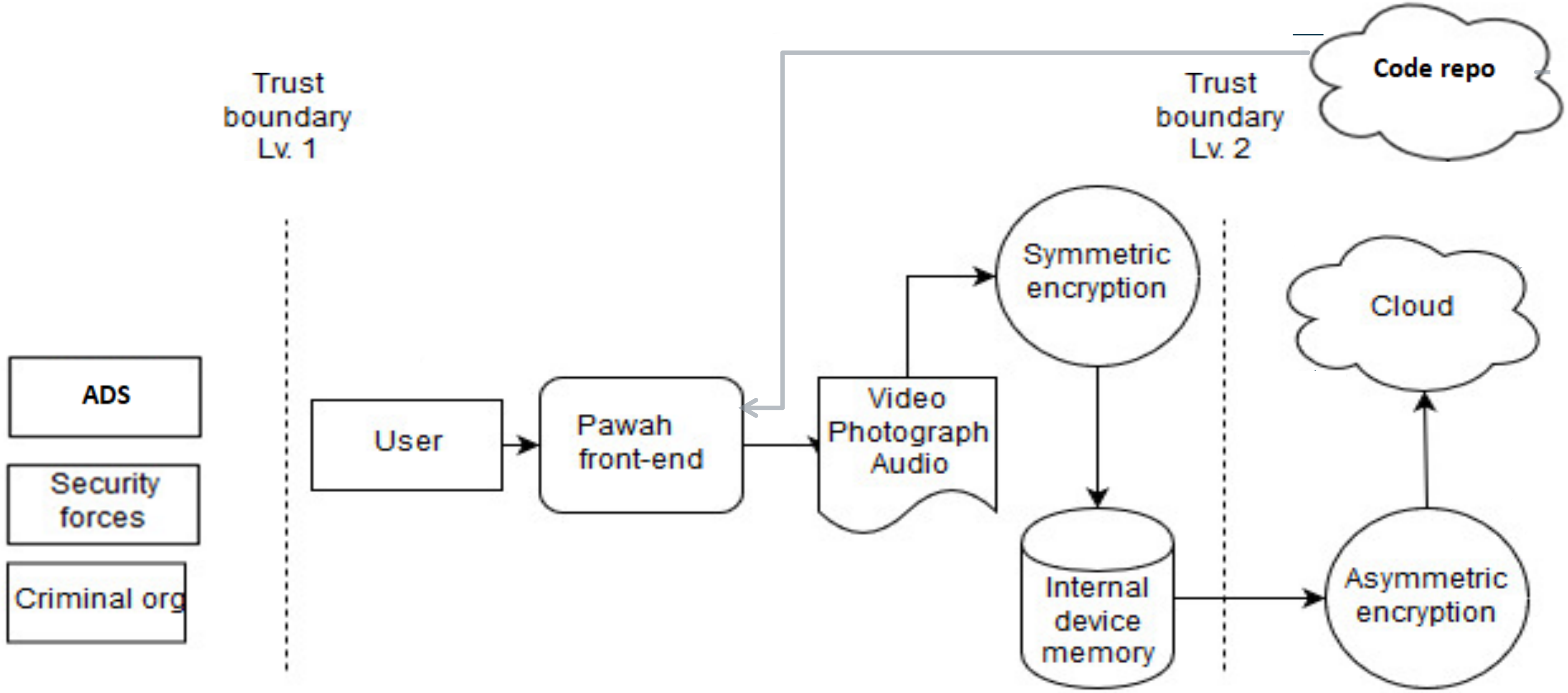
- External attacker impersonating user to access app
-
-
-

Threats

-
-
-
-

Threats

-
-
-
-
-



Threats

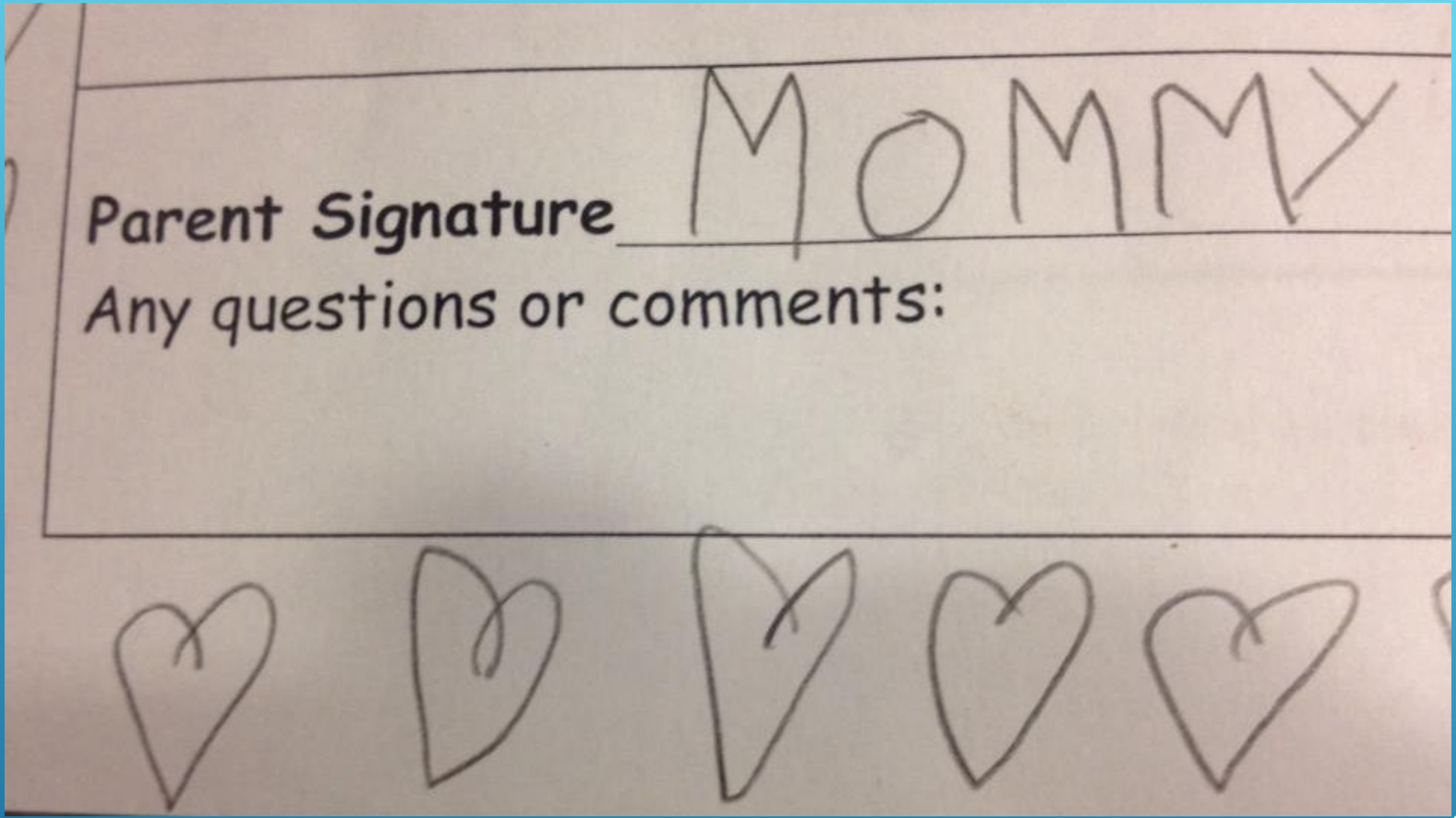
- External attacker impersonating user to access app
-
-
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
-
-
-



Parent Signature MOMMY

Any questions or comments:

STRIDE - TAMPERING