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

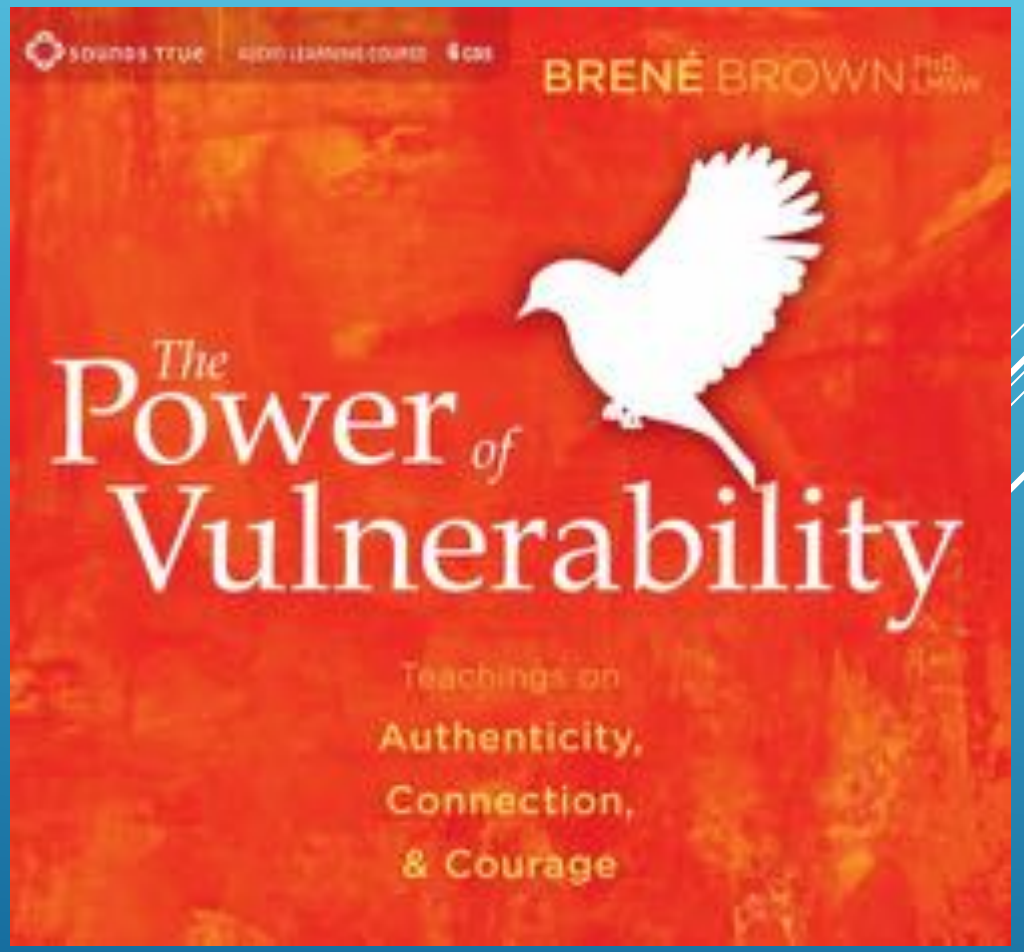
- Hacked together from Microsoft's STRIDE threat modelling approach
- Three questions:
  - What are you building?
  - What can go wrong? STRIDE
    - Spoofing of user identity
    - Tampering
    - Repudiation
    - Information disclosure
    - Denial of Service
    - Elevation of privileges
  - What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

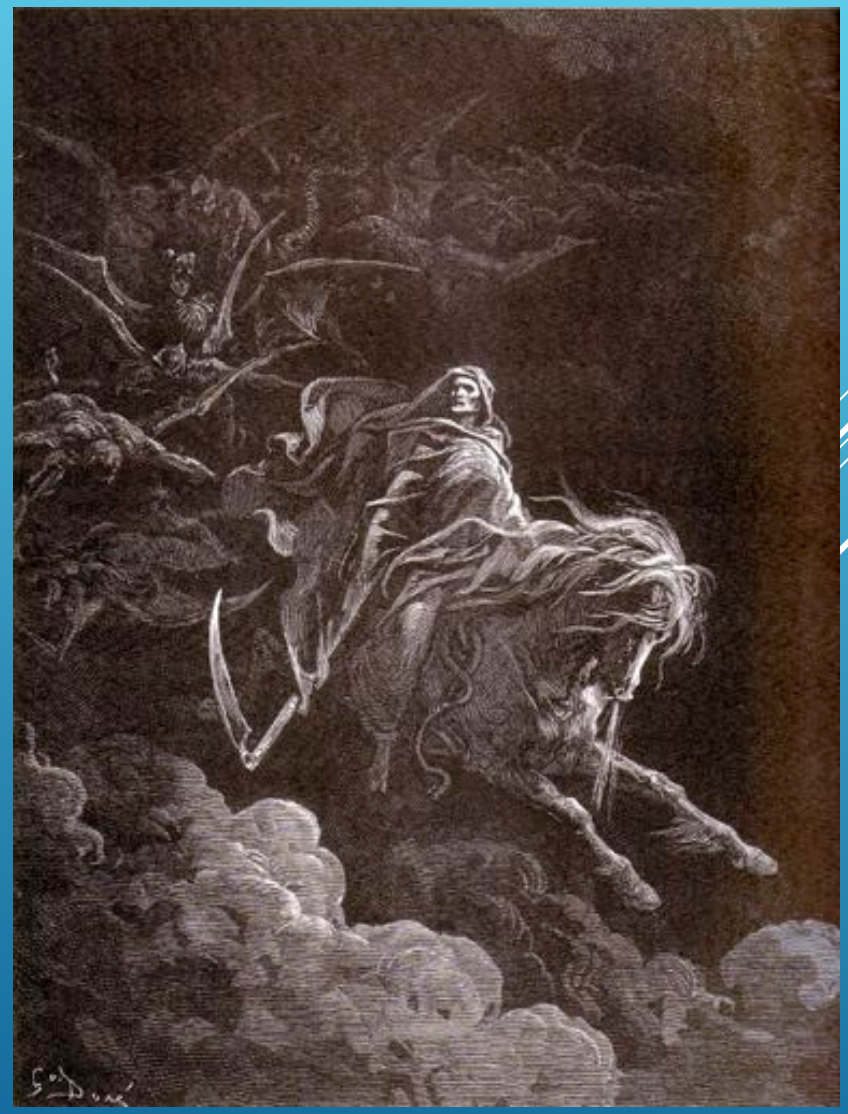


WHAT IS A THREAT?

- 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?

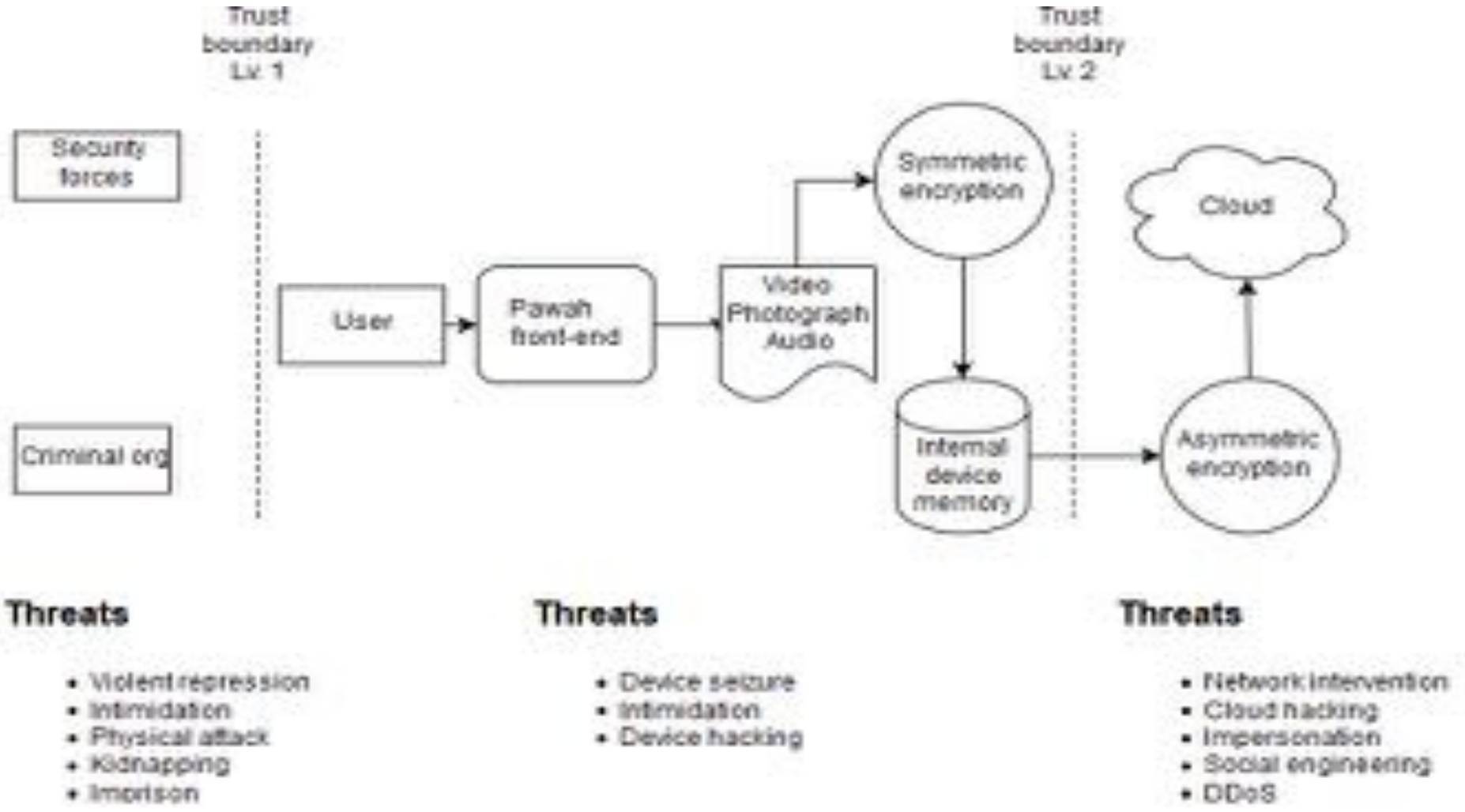
- Threat modelling: identifying the ways that something/someone can inflict loss or injury to us
- They will leverage vulnerabilities
- The event of loss and injury is the risk
- Why threat model? To put things in place to minimise the loss or injury

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



Trust boundaries – data shifts environment

Boundary around the app on the phone and cloud storage

THIS IS ALL VERY HIGH LEVEL

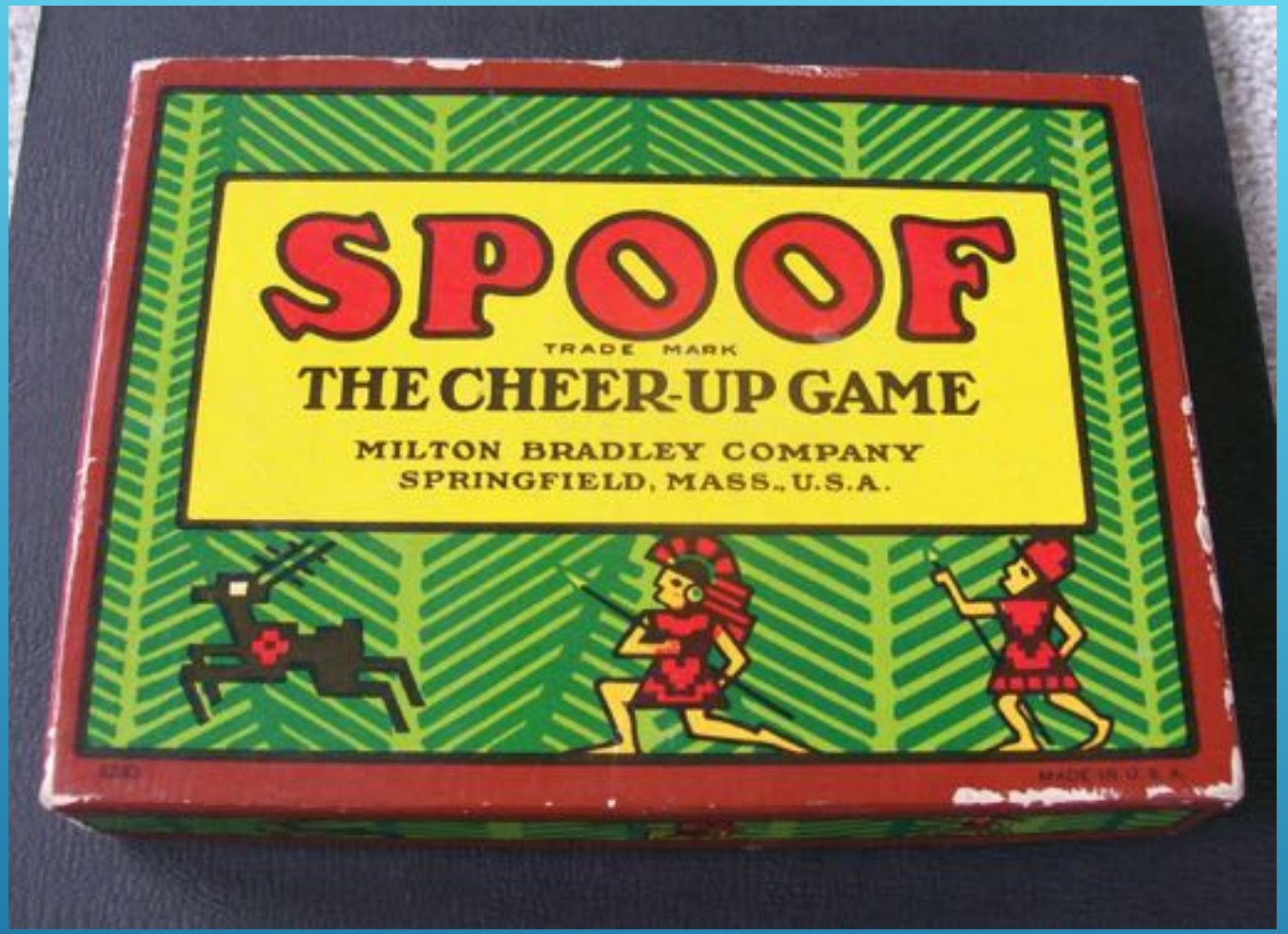
- Need to go lower
  - Enumerate
    - Technology
    - Protocols
    - Functionality that can be abused (PIN reset)
  - Flesh out connected systems
    - Cloud storage
    - Spoiler alert: Code repository
    - Spoiler alert: Log server

REMEMBER! BASIC THREAT MODELLING

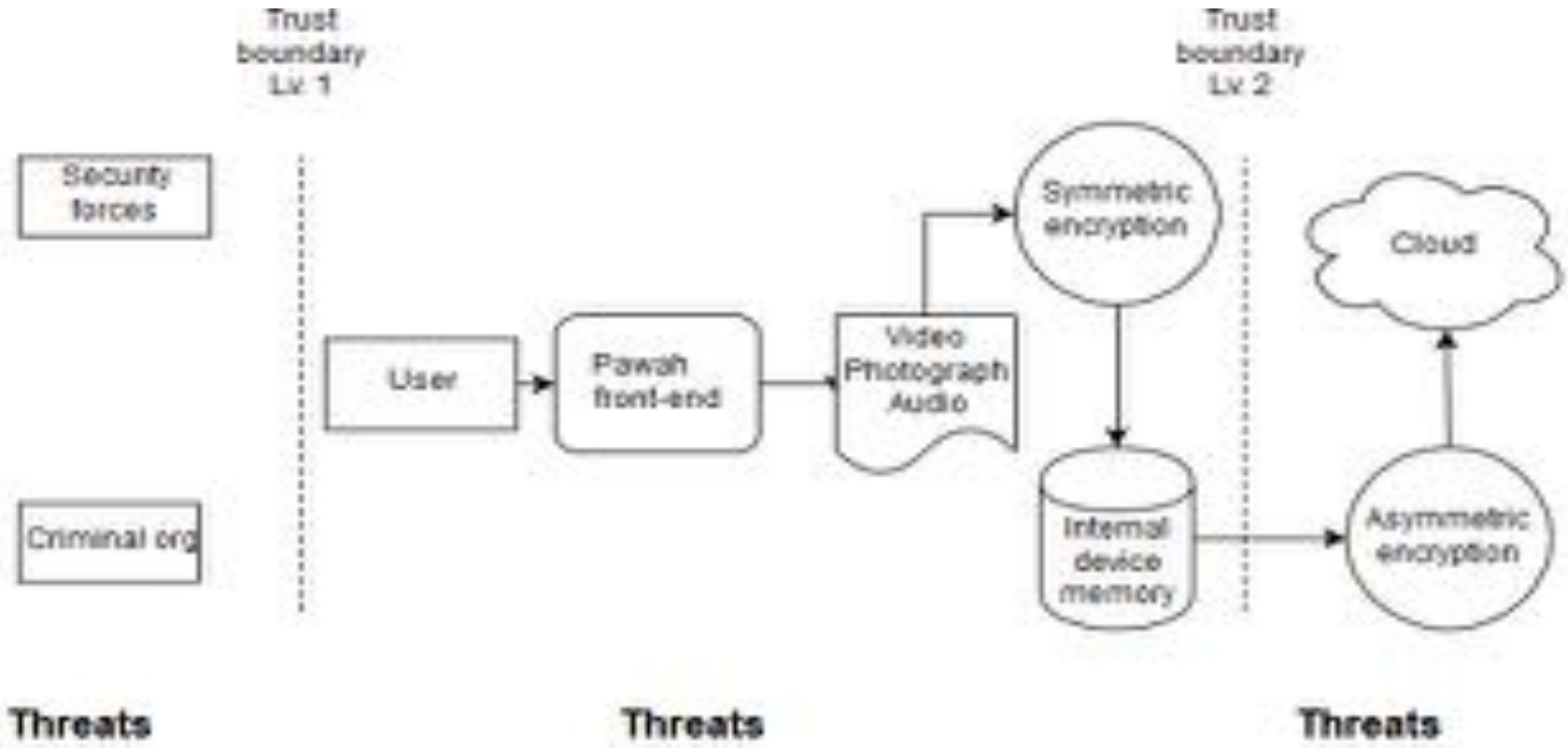
- Hacked together from Microsoft's STRIDE threat modelling approach
- Three questions:
  - What are you building?
  - **What can go wrong?**
  - What are you going to do about it?

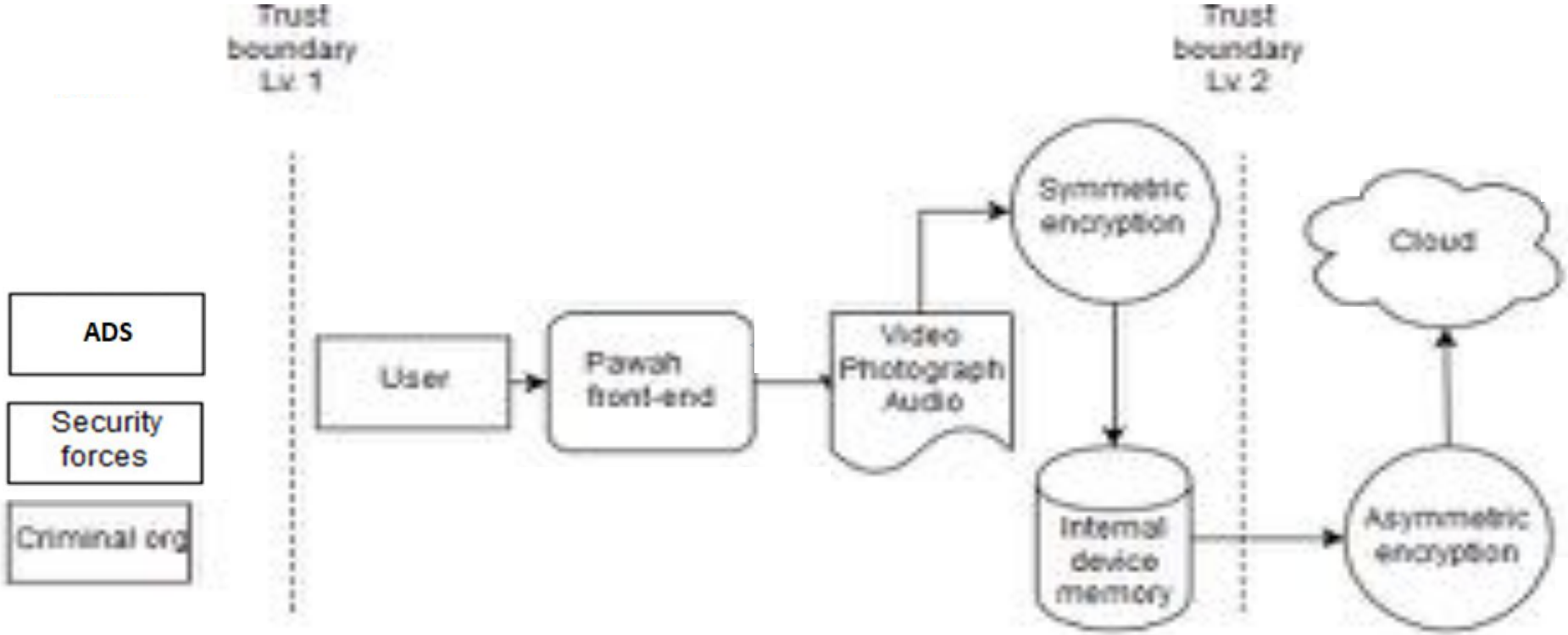
STRIDE

- 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
Cloud
Asymmetric encryption
Threats
Threats
Threats

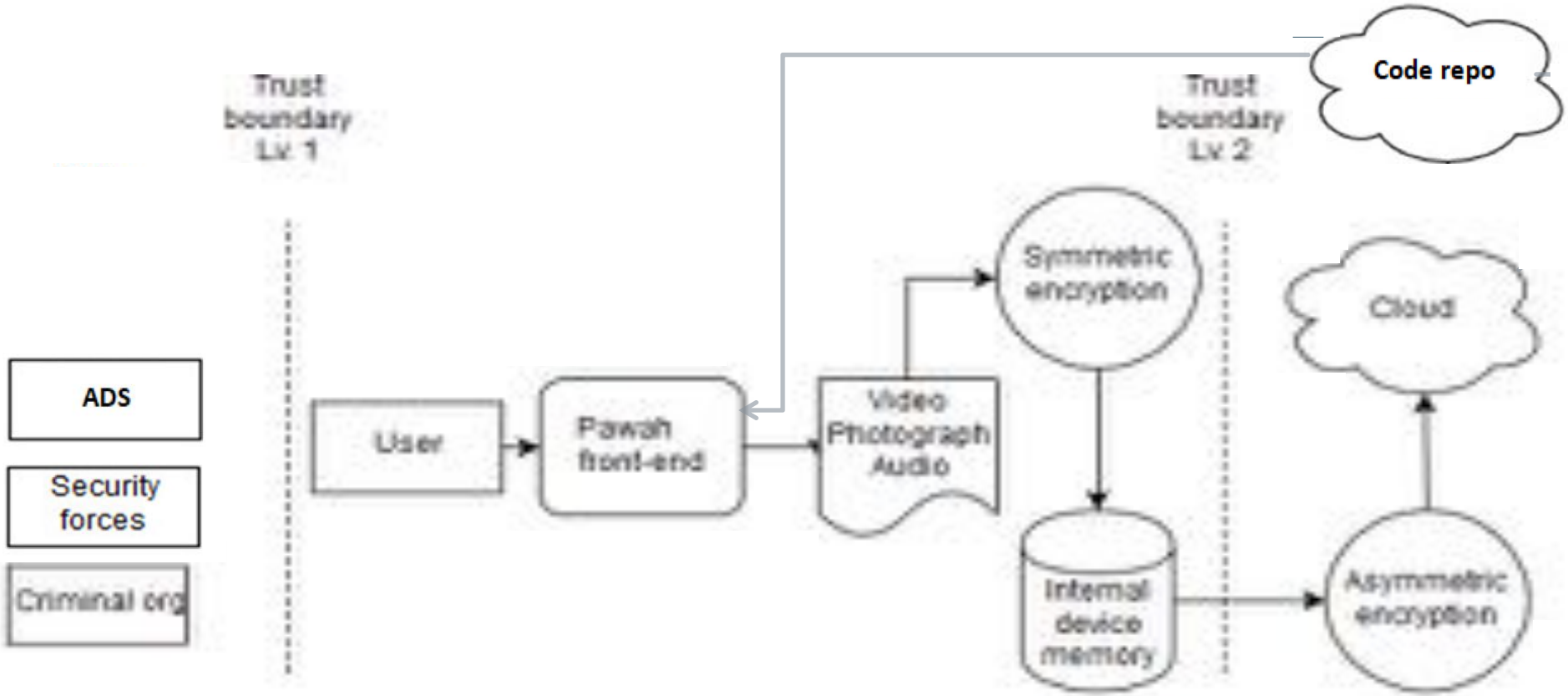


Threats

- External attacker impersonating user to access app

Threats

Threats



Threats

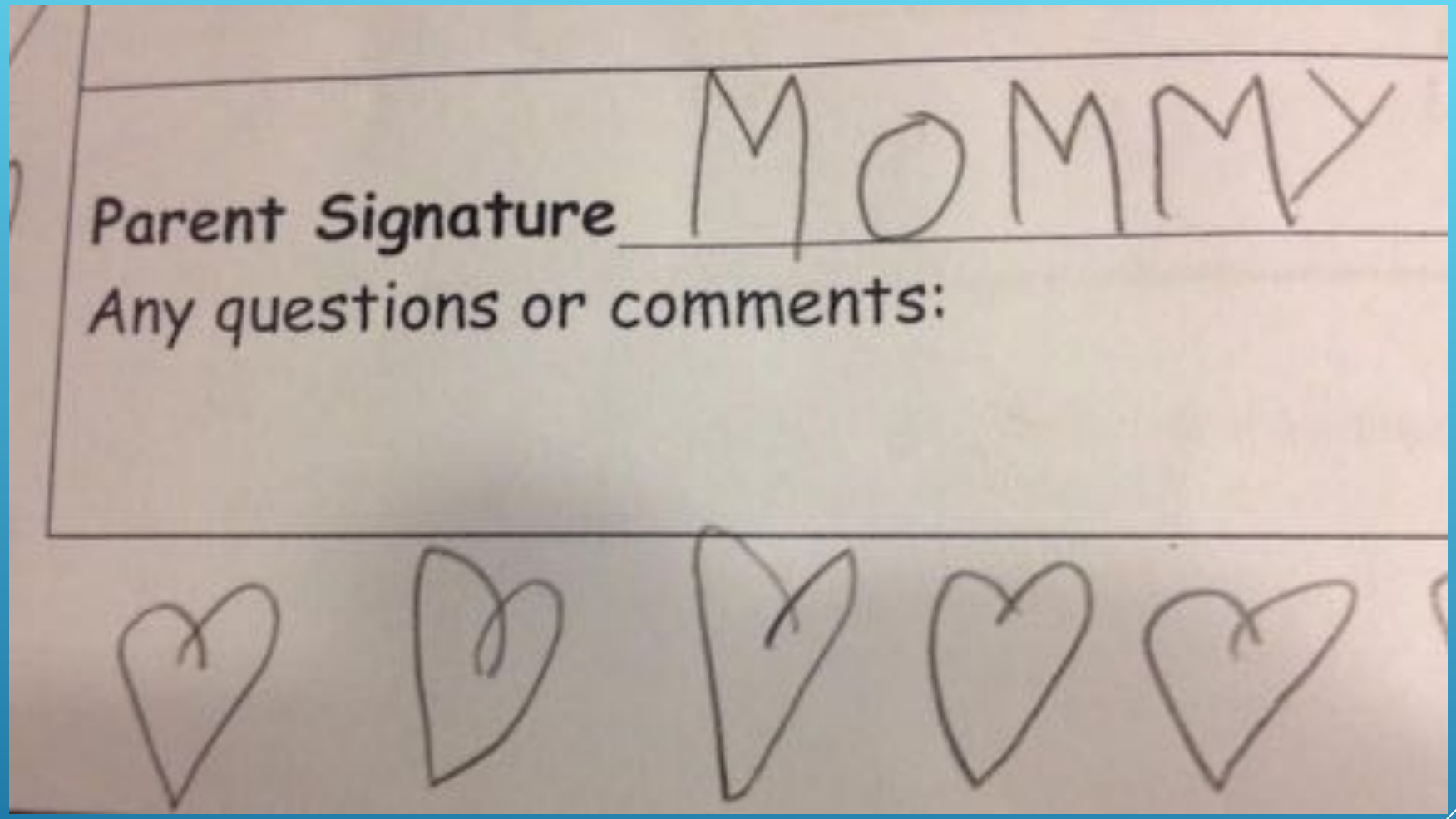
- External attacker impersonating user to access app
-
-
-

Threats

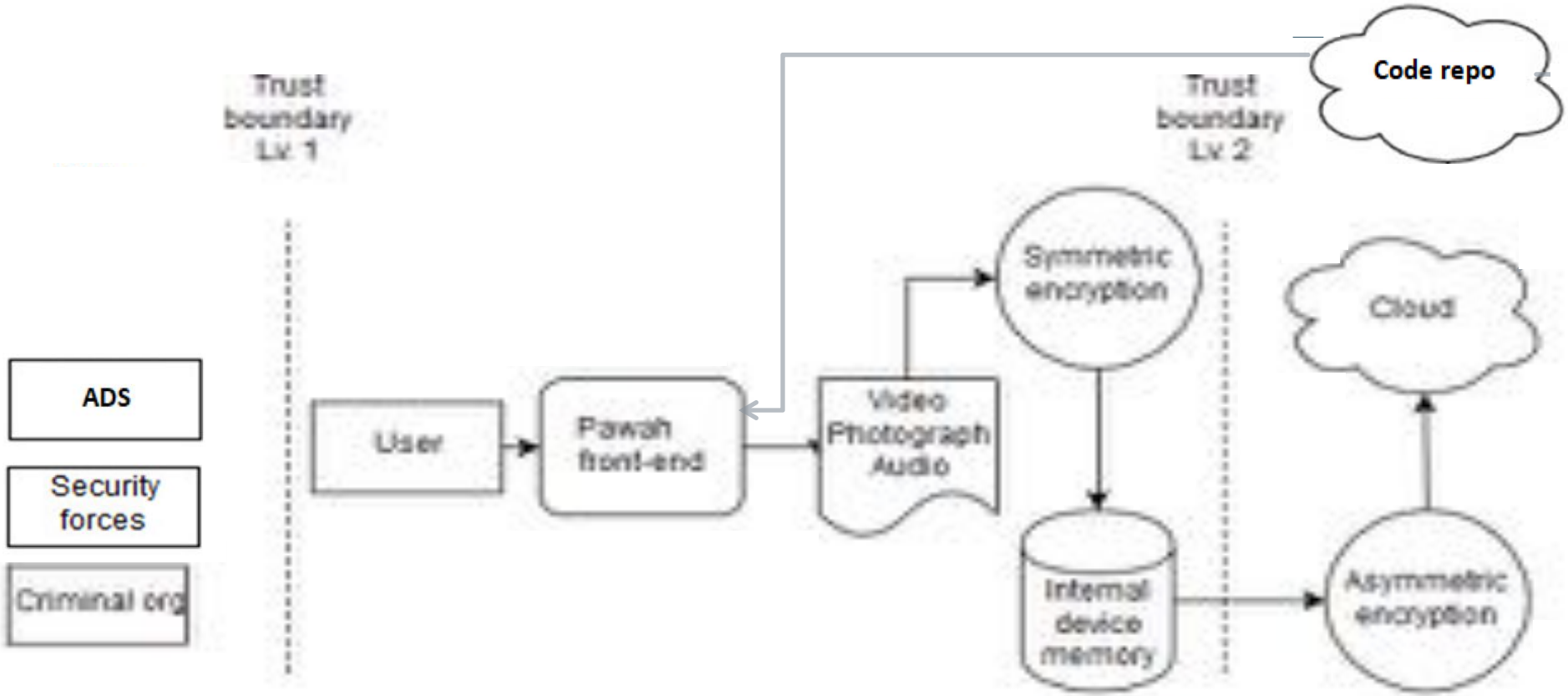
-
-
-
-

Threats

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



STRIDE - TAMPERING



Threats

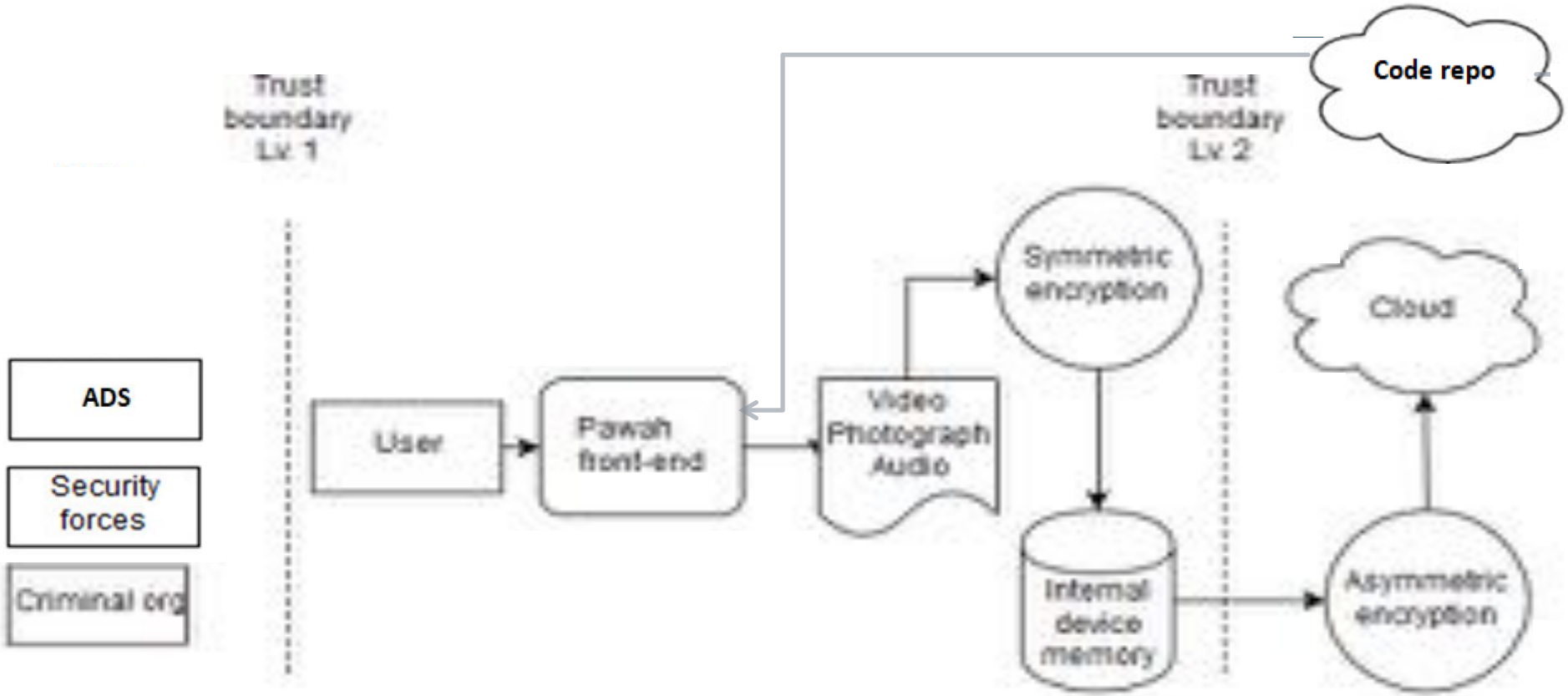
- External attacker impersonating user to access app
-
-
-

Threats

-
-
-
-

Threats

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



Threats

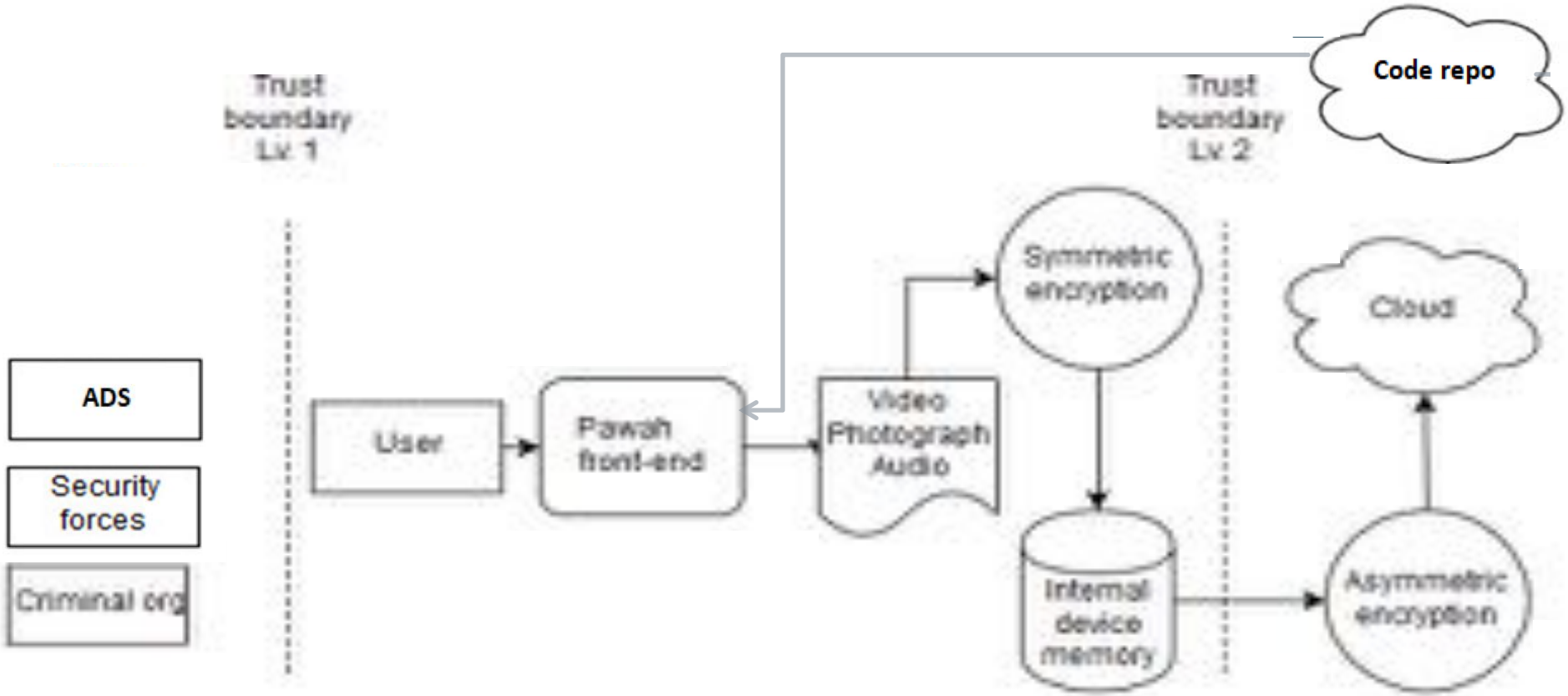
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

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



Threats

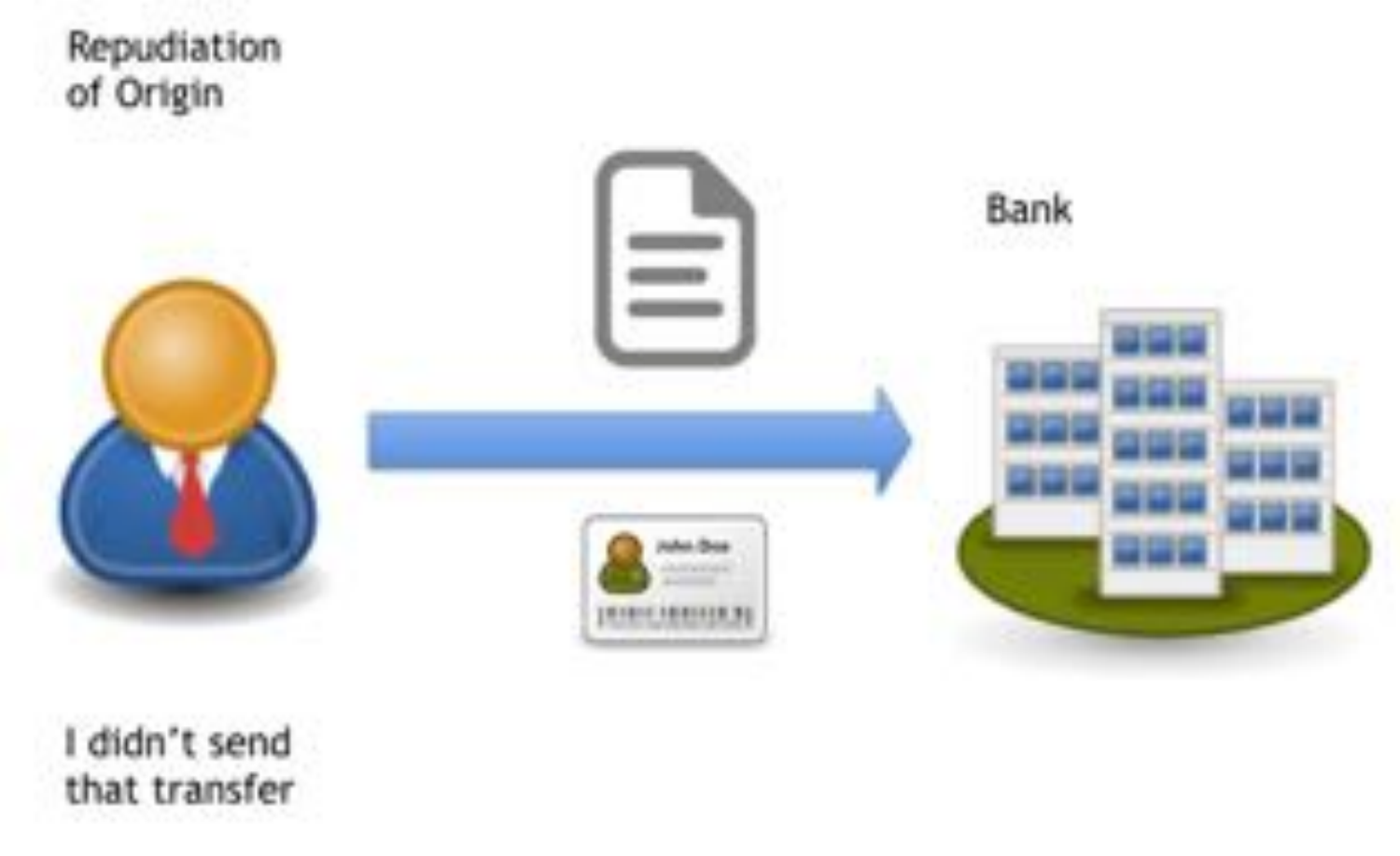
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-

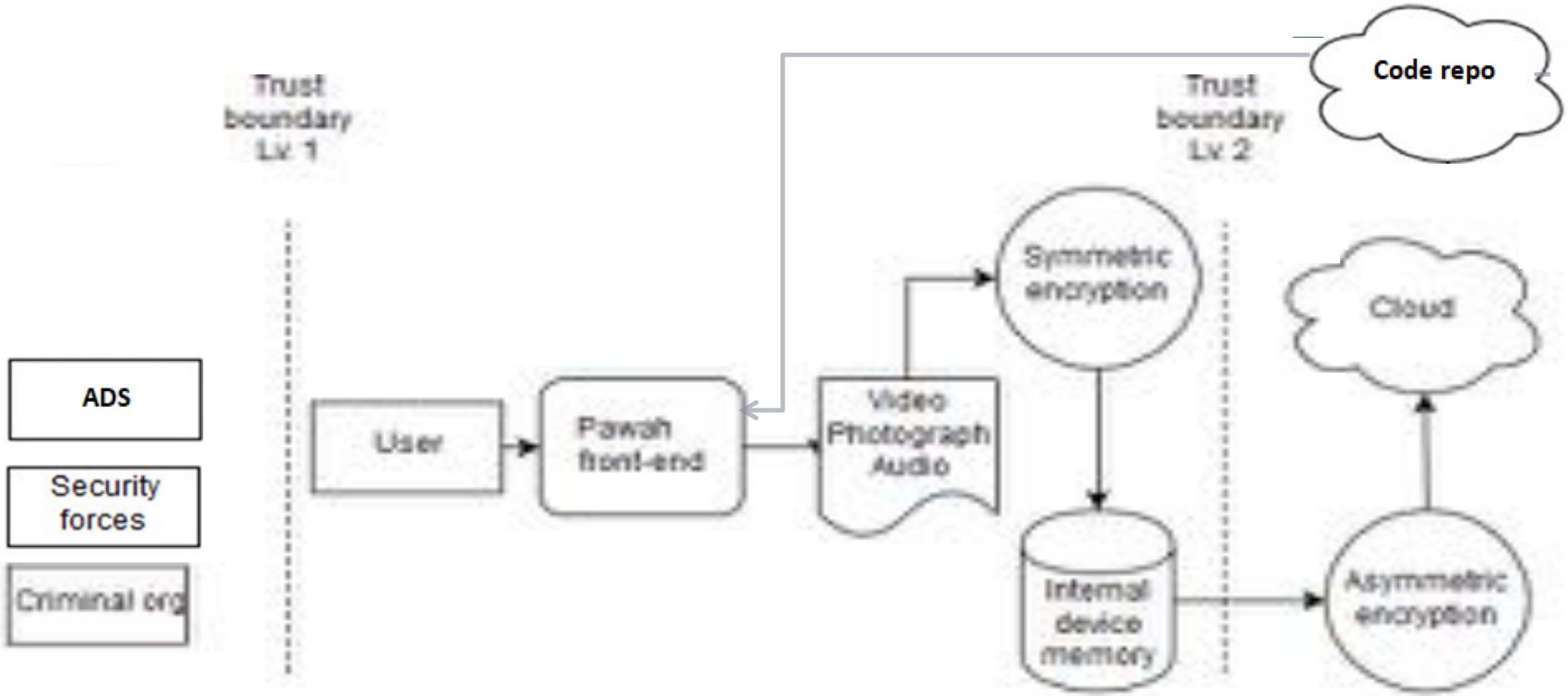


STRIDE - REPUDIATION

THIS IS A HARD ONE

- Someone claims the footage is false or of someone else
  - Other than a forensic chain of custody we can't do much about that
- For your app could someone perform an action and claim it wasn't them?

STRIDE - INFORMATION DISCLOSURE



Threats

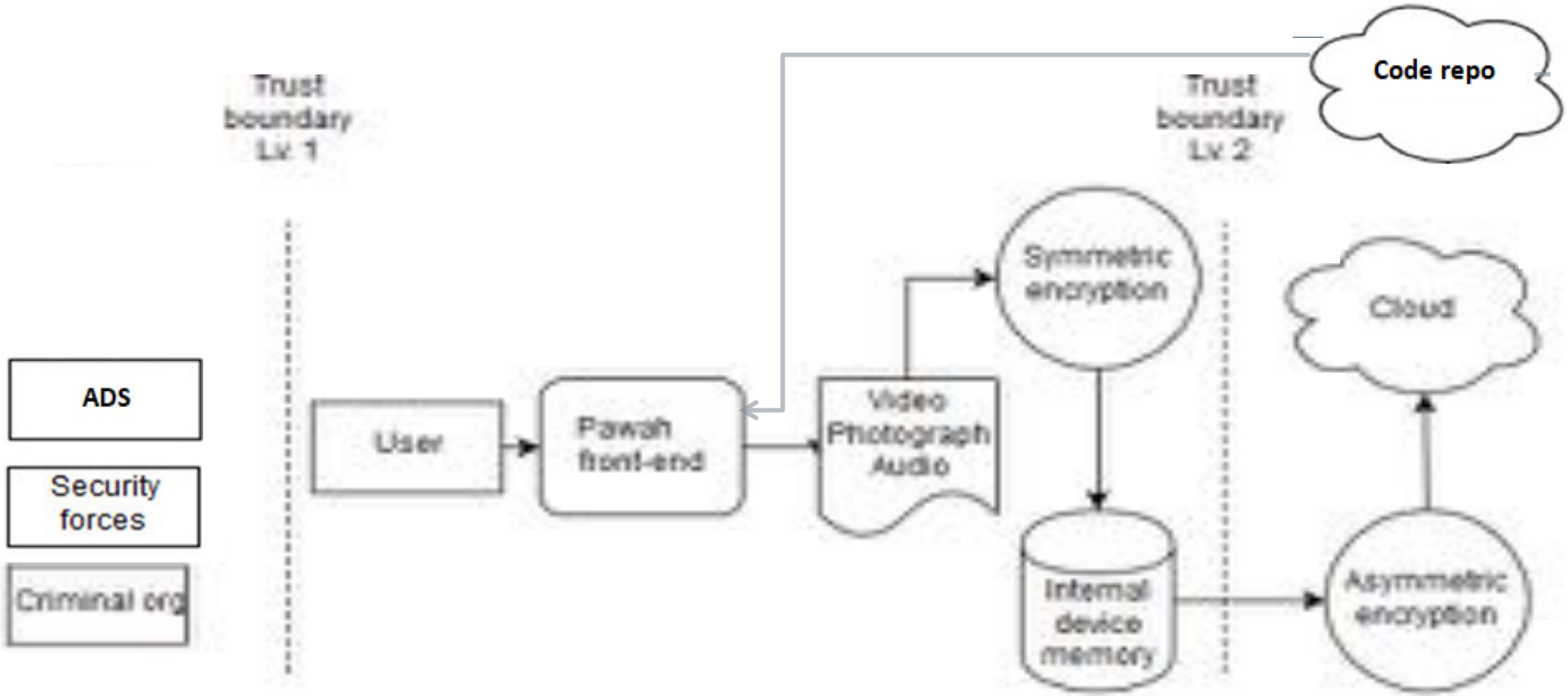
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

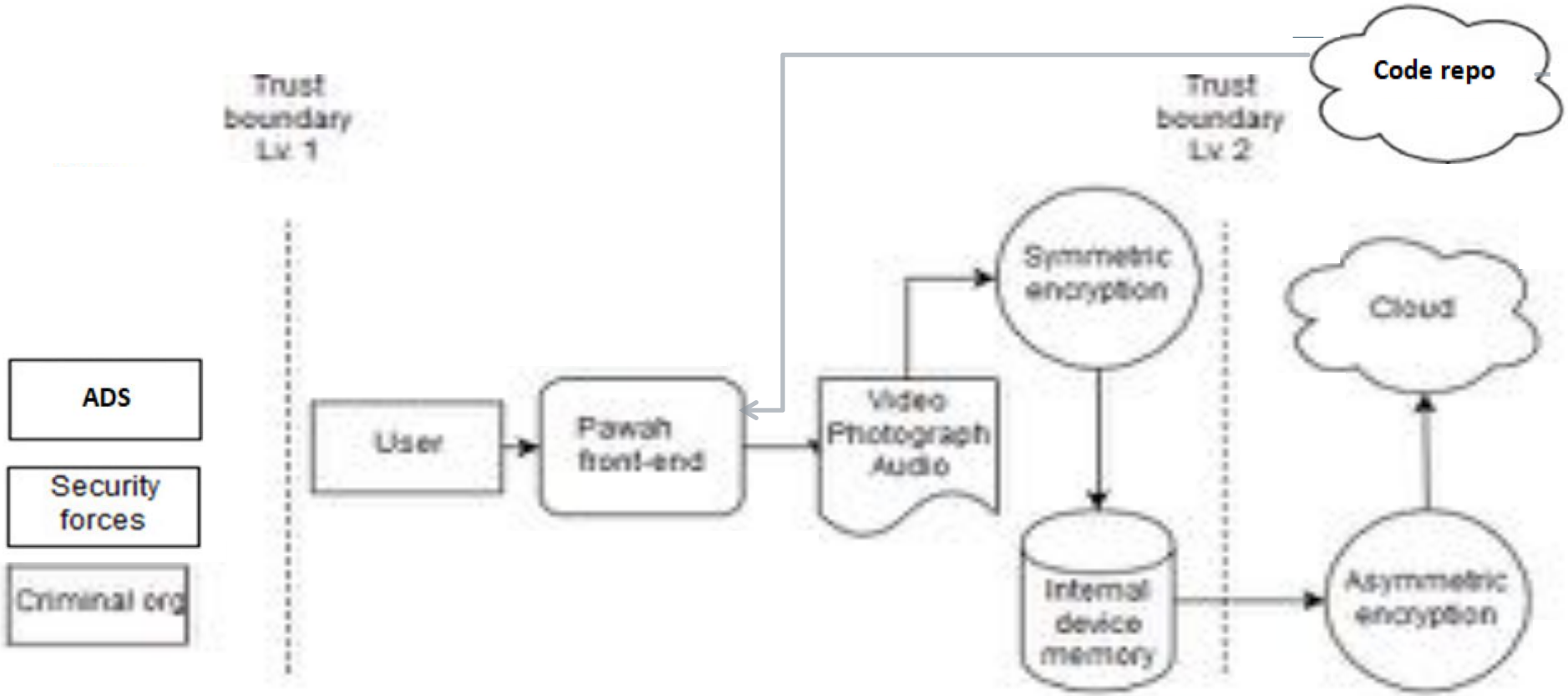
Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information

WE NEED TO GO DEEPER

- Enumerate
  - Technology
  - Protocols
  - Functionality that can be abused (PIN reset)
- Flesh out connected systems
  - Code repository
  - Cloud storage
  - Log server

STRIDE - DENIAL OF SERVICE



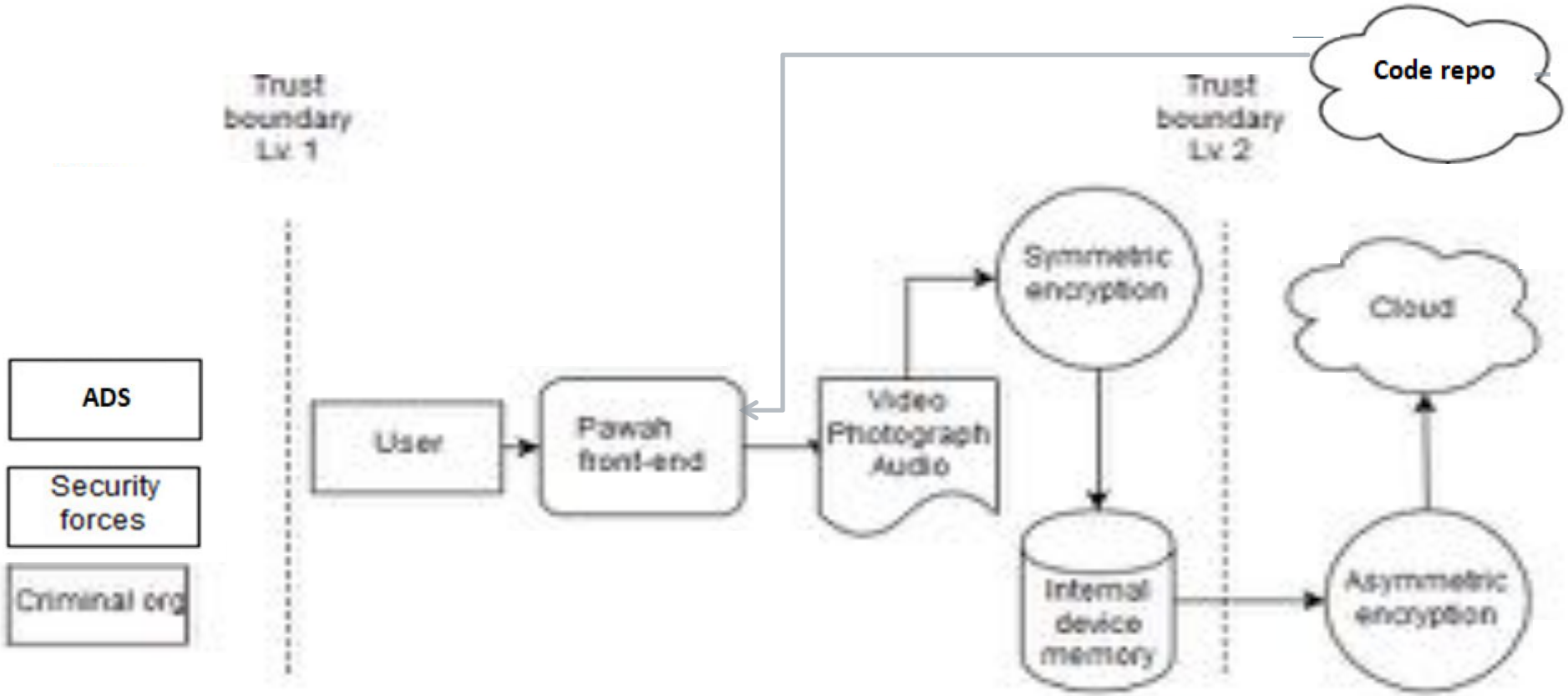
Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

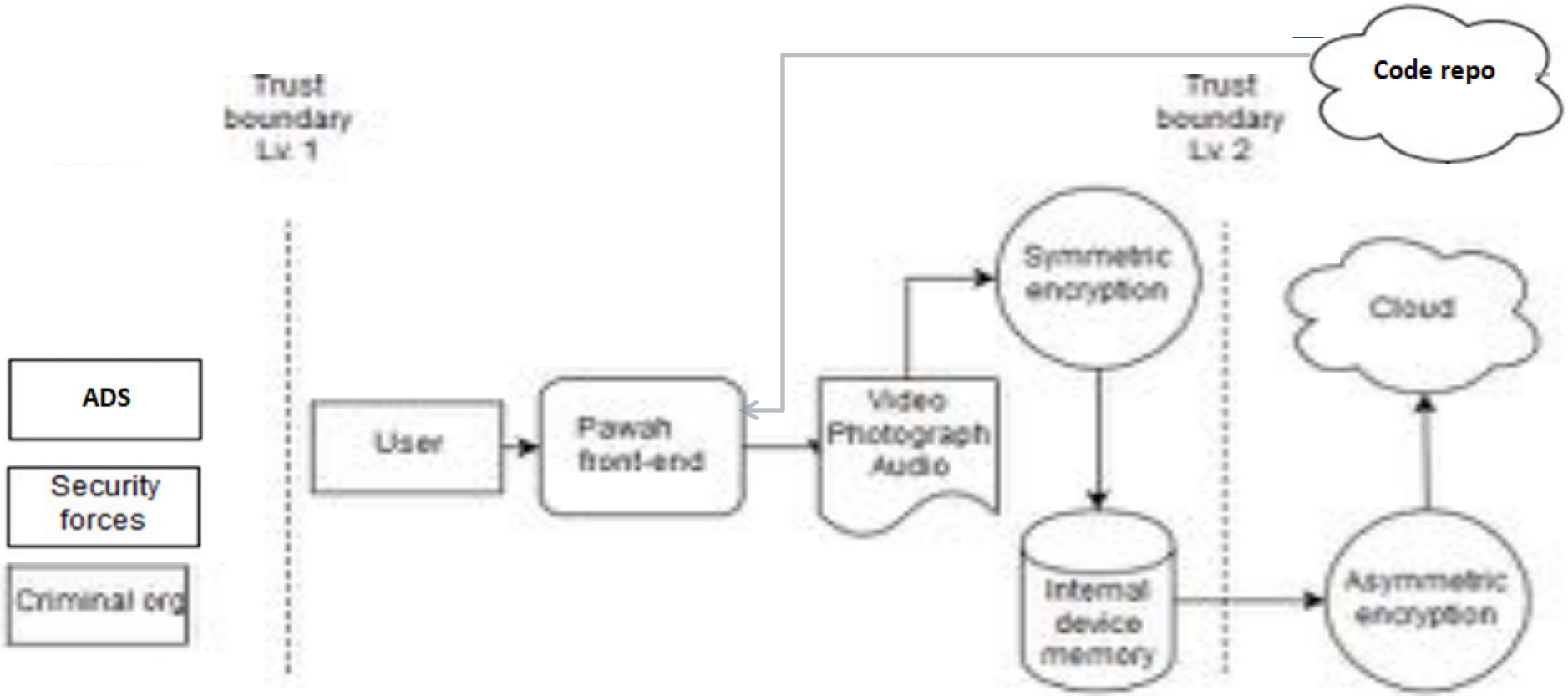
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

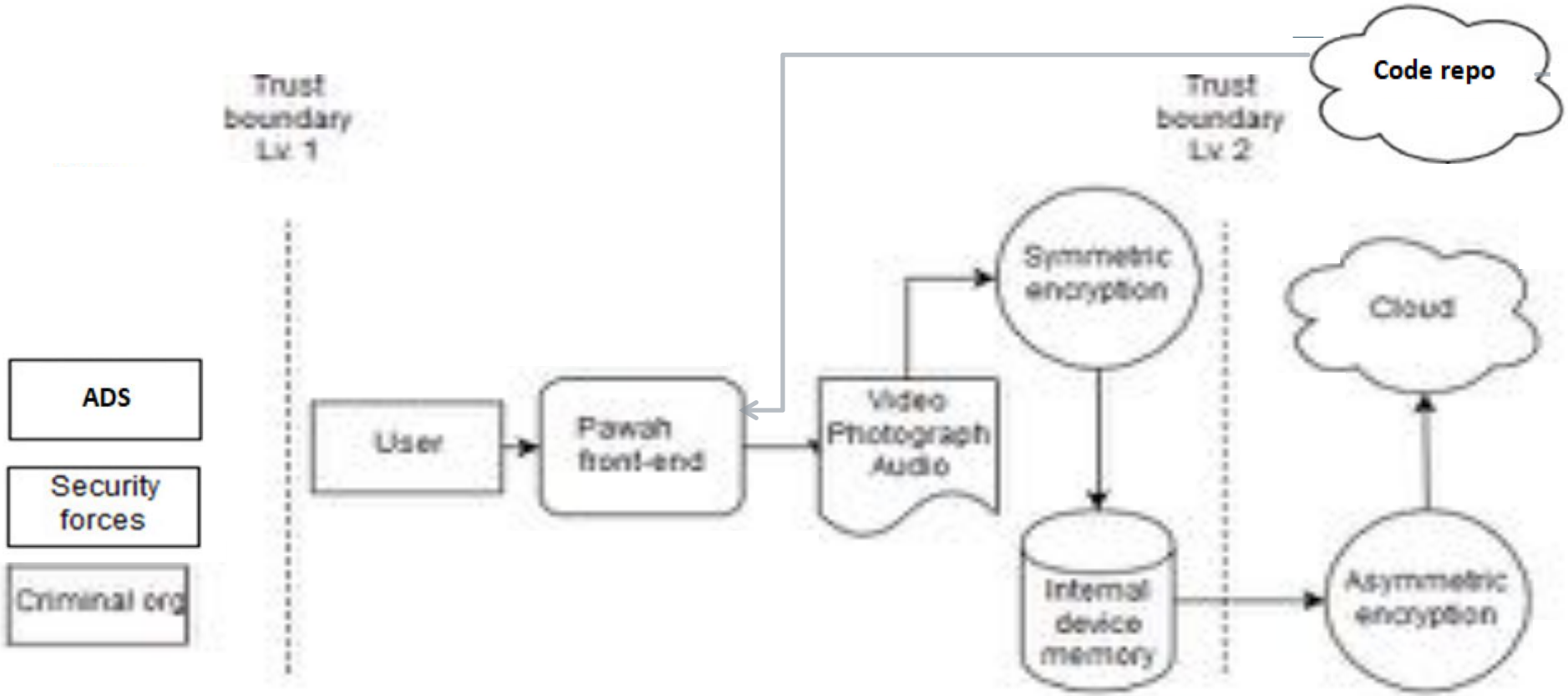
Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information

STRIDE – ELEVATION OF PRIVILEGES



Threats

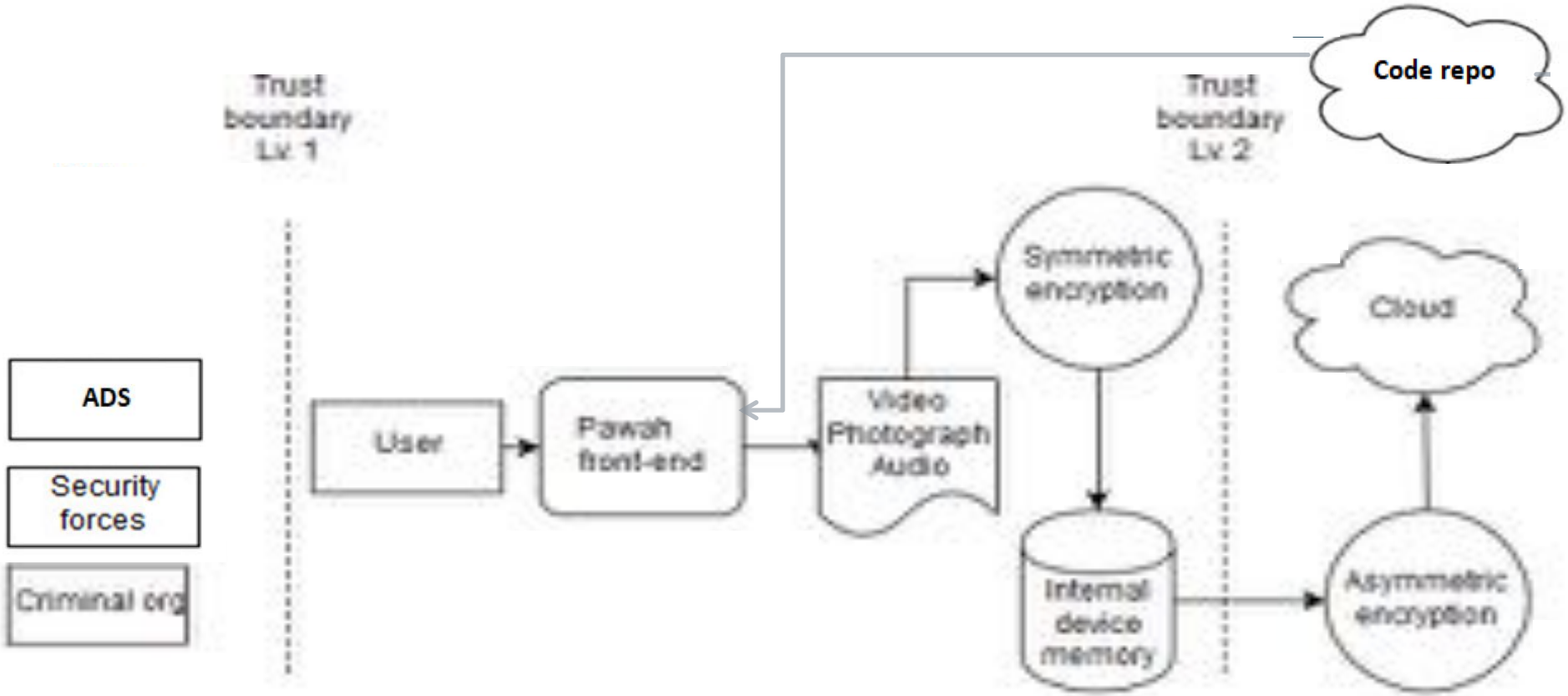
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

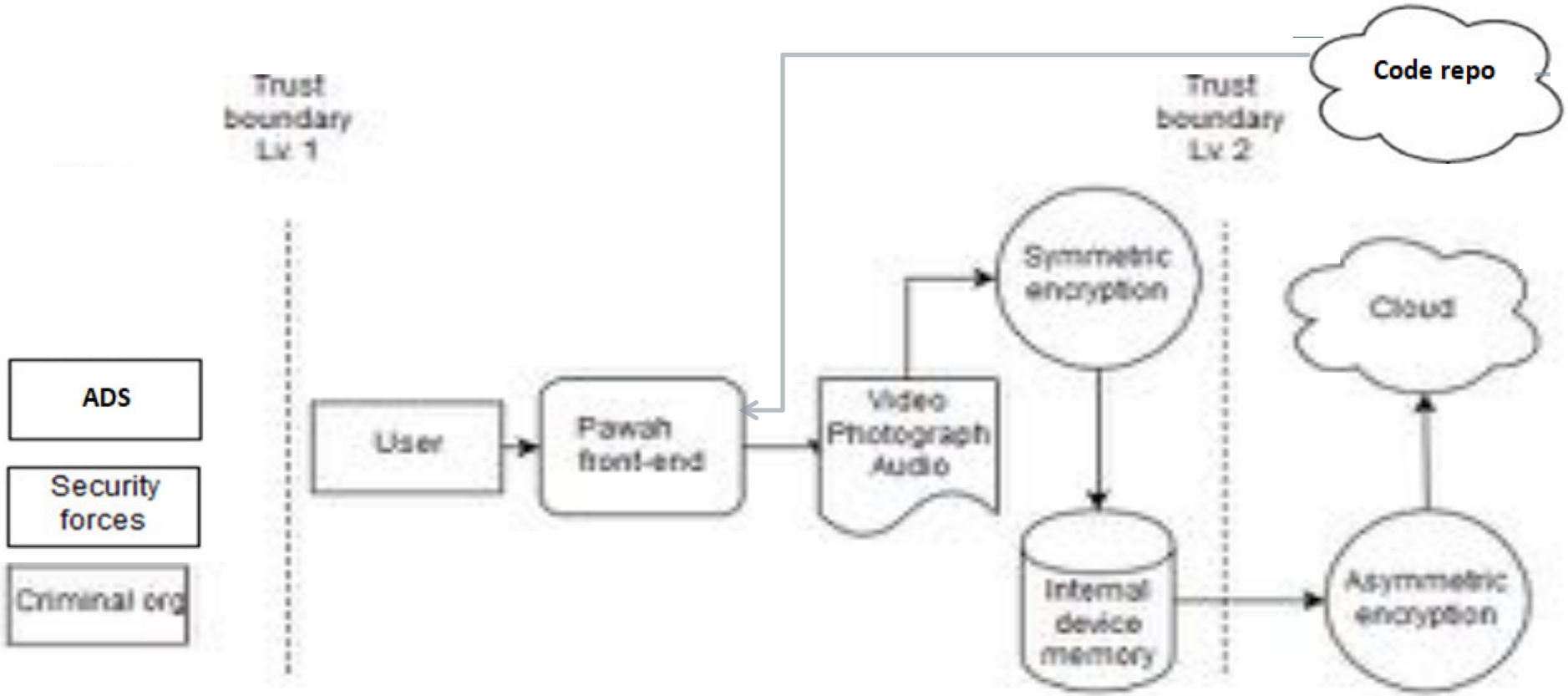
Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-

BUT WAIT, THERE'S MORE!



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

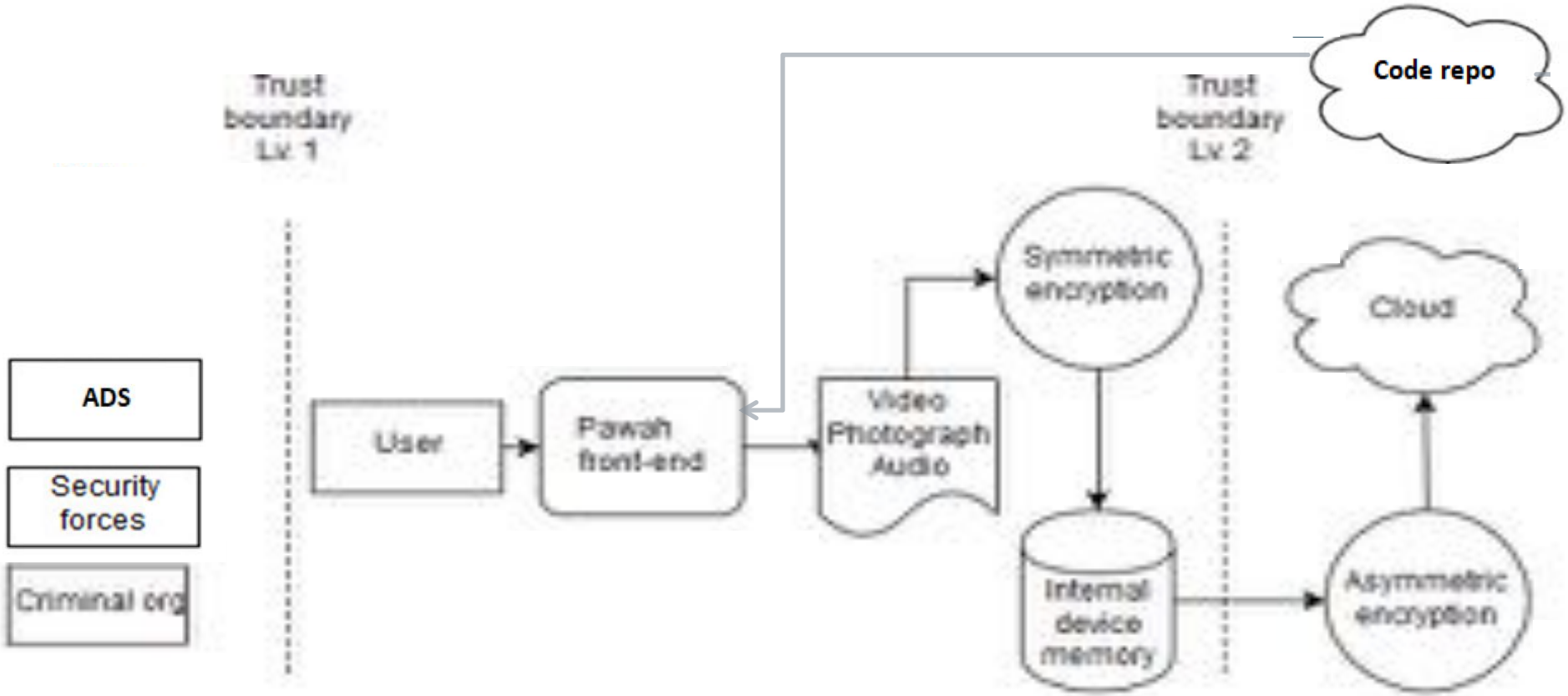
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

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?**



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

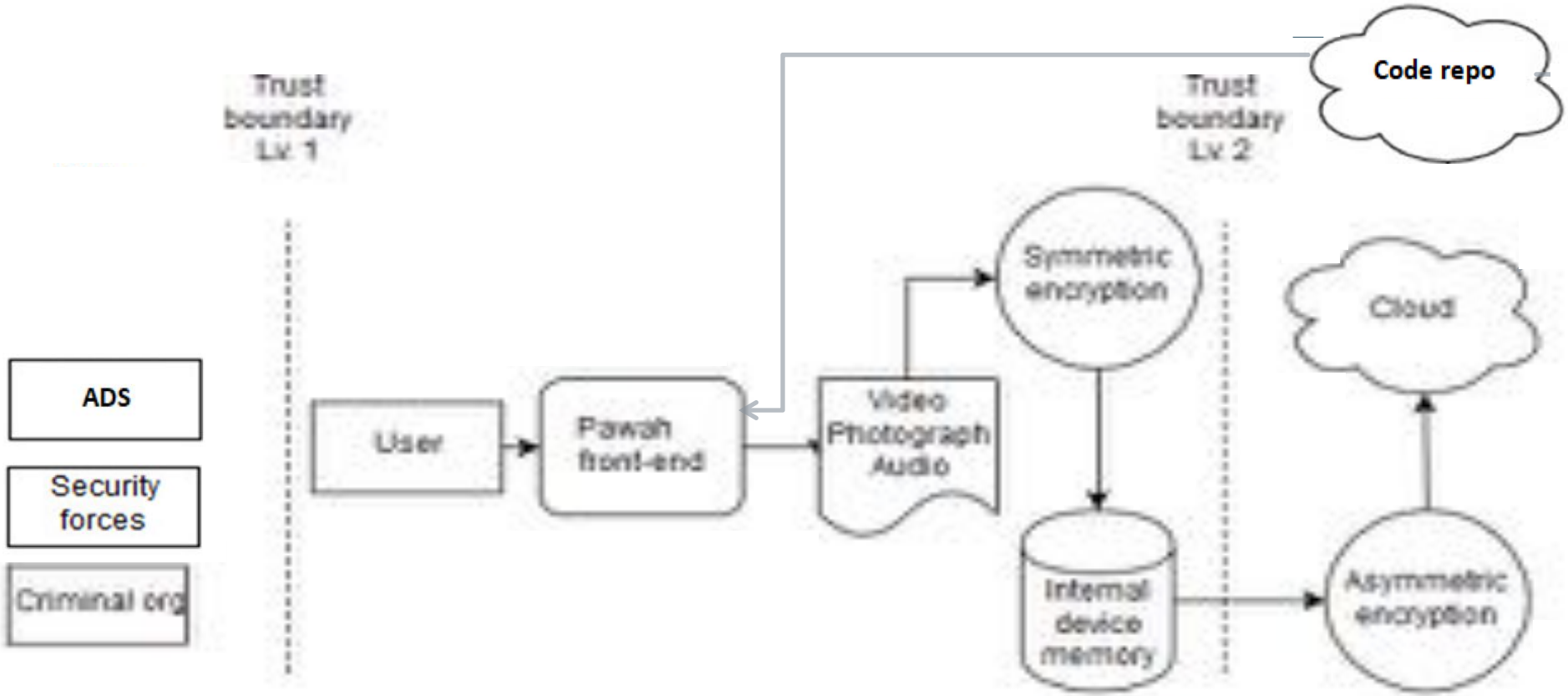
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – SPOOFING

- Someone impersonating a user to access data on phone, code repository, cloud storage
  - Credentials hashed with secure algorithm
  - Two factor authentication on code repository and cloud storage
  - IP whitelisting to access code repository and cloud storage if possible
  - Access Control Policy
    - Accounts are tied to identity
    - Permission only given if the user needs it
    - Accounts are revoked when user leaves
    - Accounts regularly audited
    - Someone is responsible for all this



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

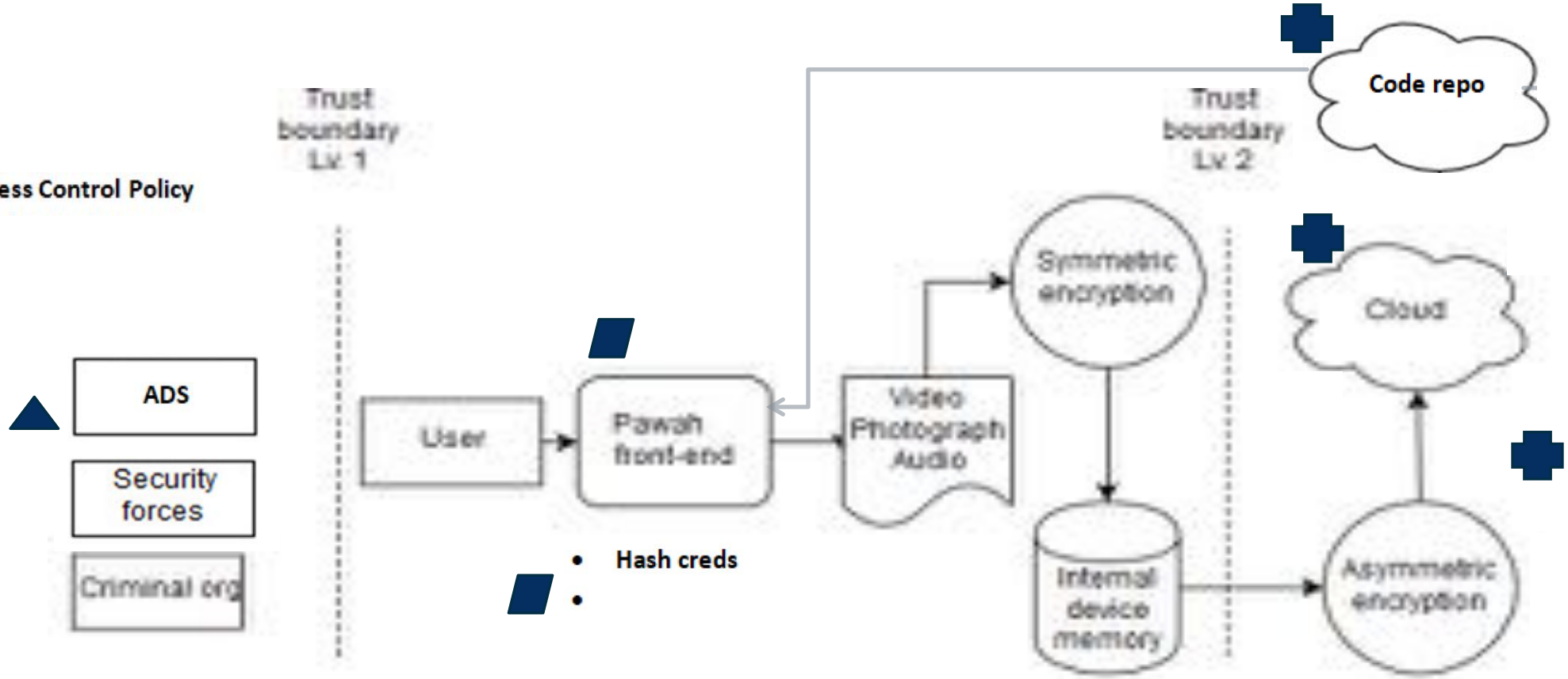
Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

- Access Control Policy
-
-
-



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

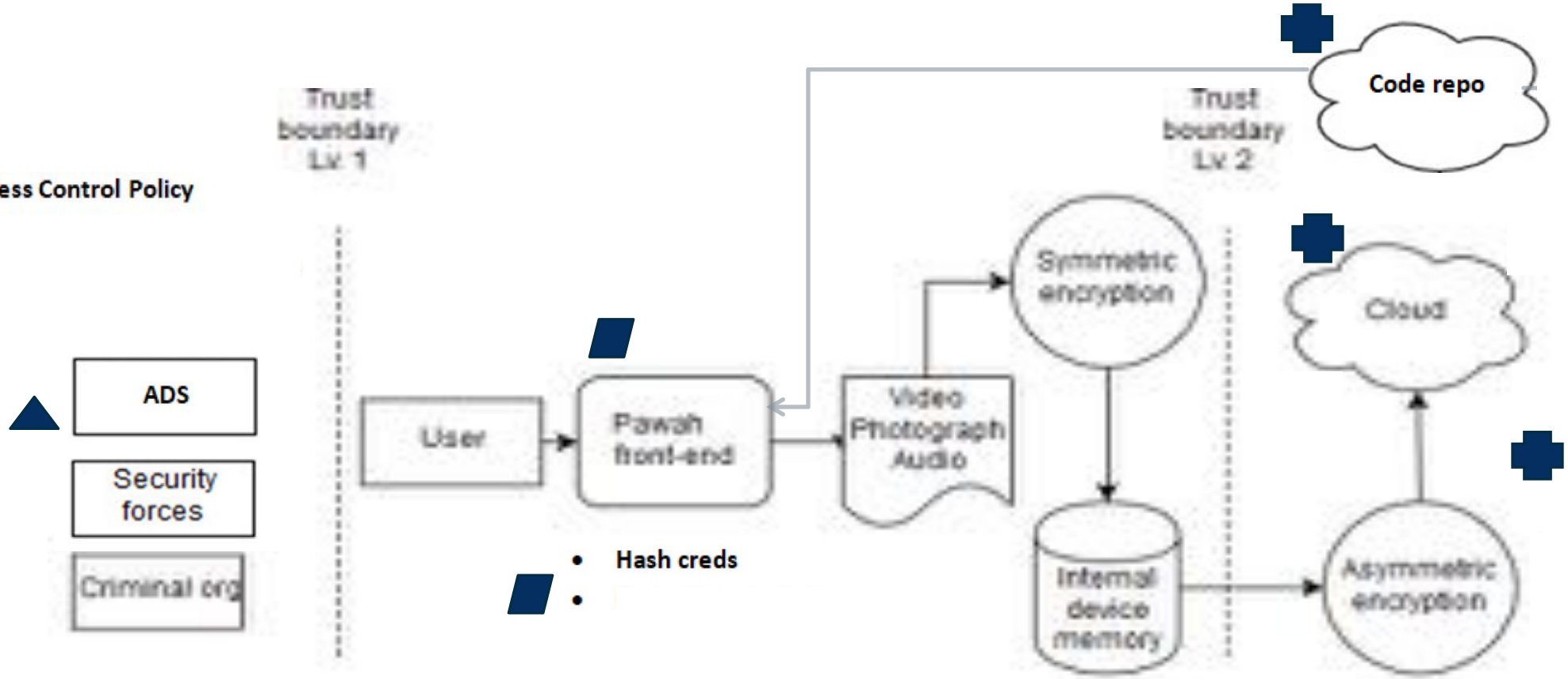
Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – TAMPERING

- Data being modified on the phone, cloud storage, anywhere in between
  - File integrity by matching hashes of files at different stages
- Tampering with source code or logs
  - Log all actions of users
  - State in employee contracts what is unacceptable so they have no recourse
  - Forward logs to centralised, hardened log server with strong access control

- Access Control Policy
-
-
-



- Hash creds
- 2FA
- IP whitelisting
-
-
-

- Hash creds
-

Threats

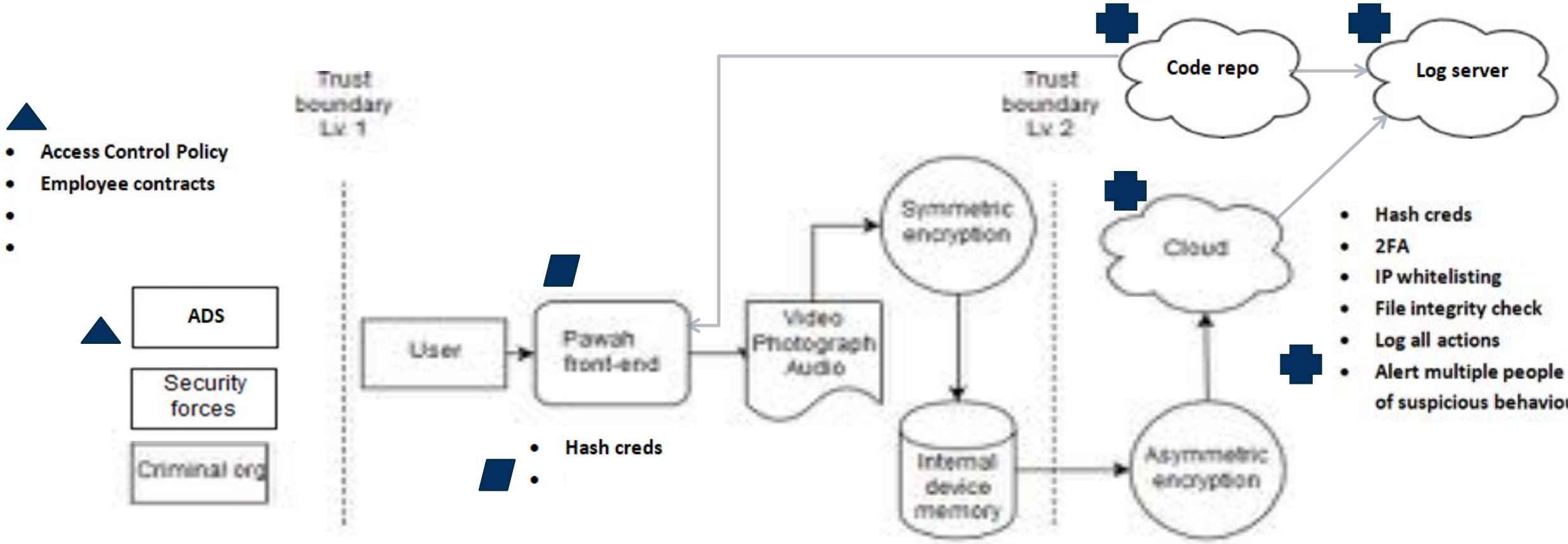
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

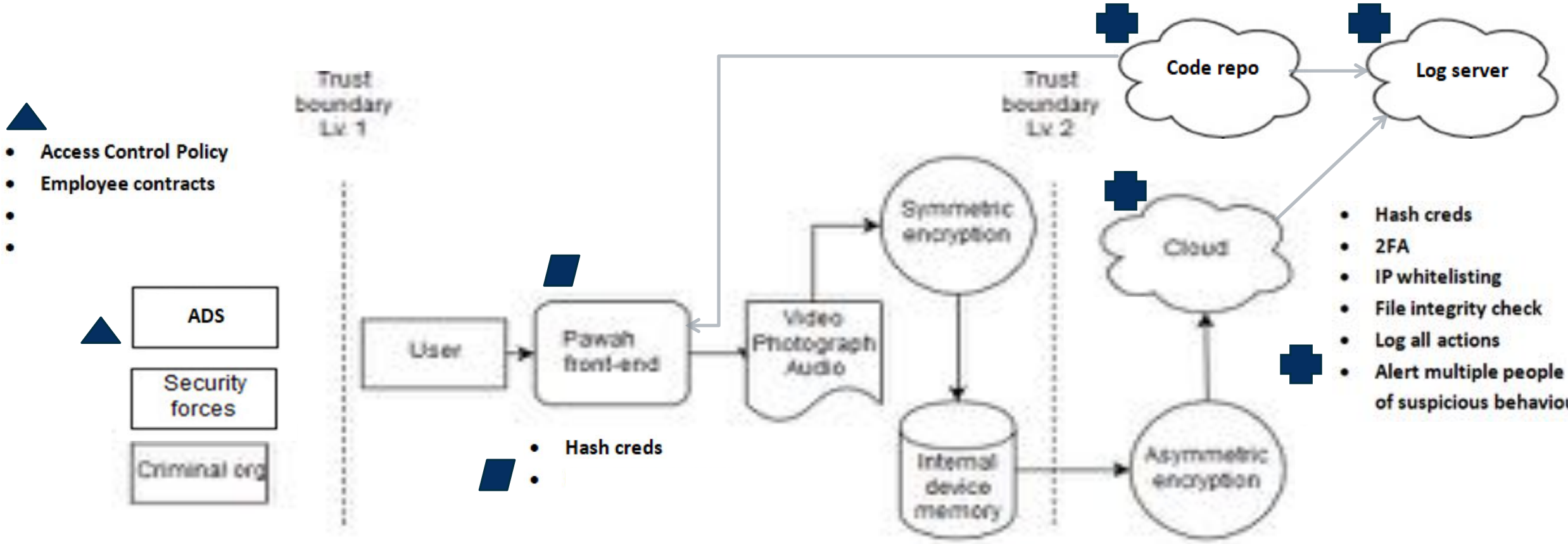
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE - REPUDIATION

- Someone claims the footage is false or of someone else
  - Other than a forensic chain of custody we can't do much about that
- For your app could someone perform an action and claim it wasn't them?

STRIDE –INFORMATION DISCLOSURE

- Footage is tied to particular users
  - Policy to review footage with lawyers before being submitted as evidence
  - Remove metadata so footage can be posted online anonymously
  - Need further controls once done a deep dive



Threats

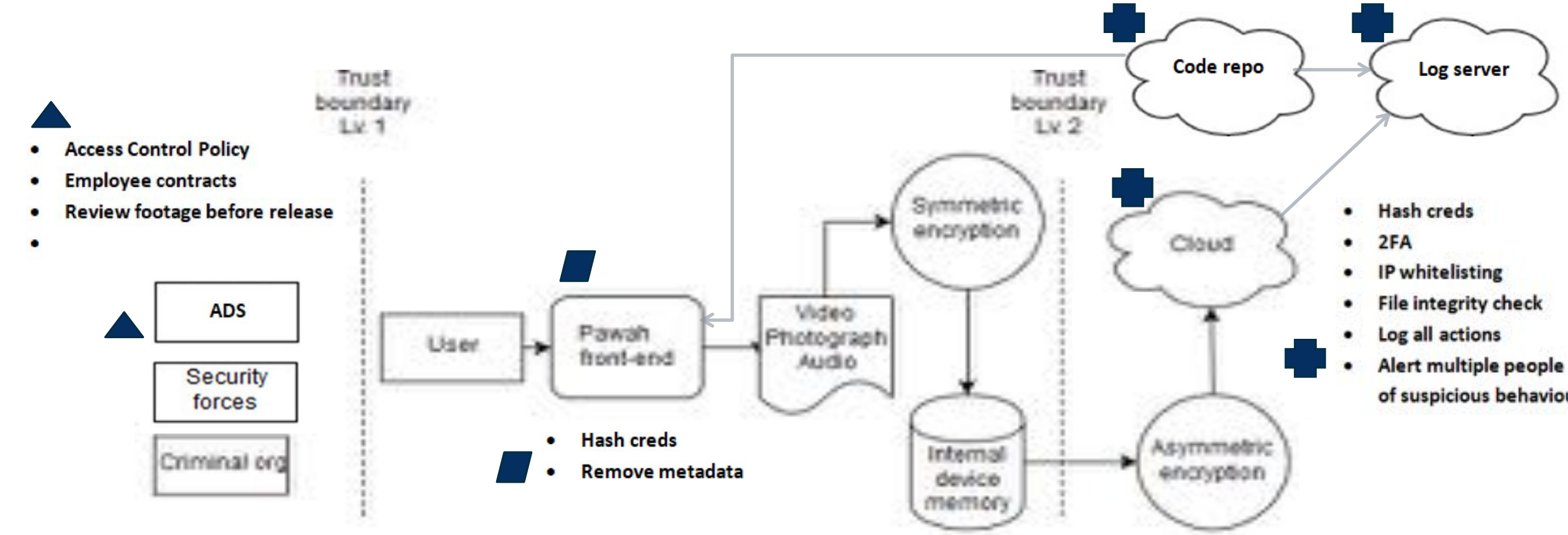
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

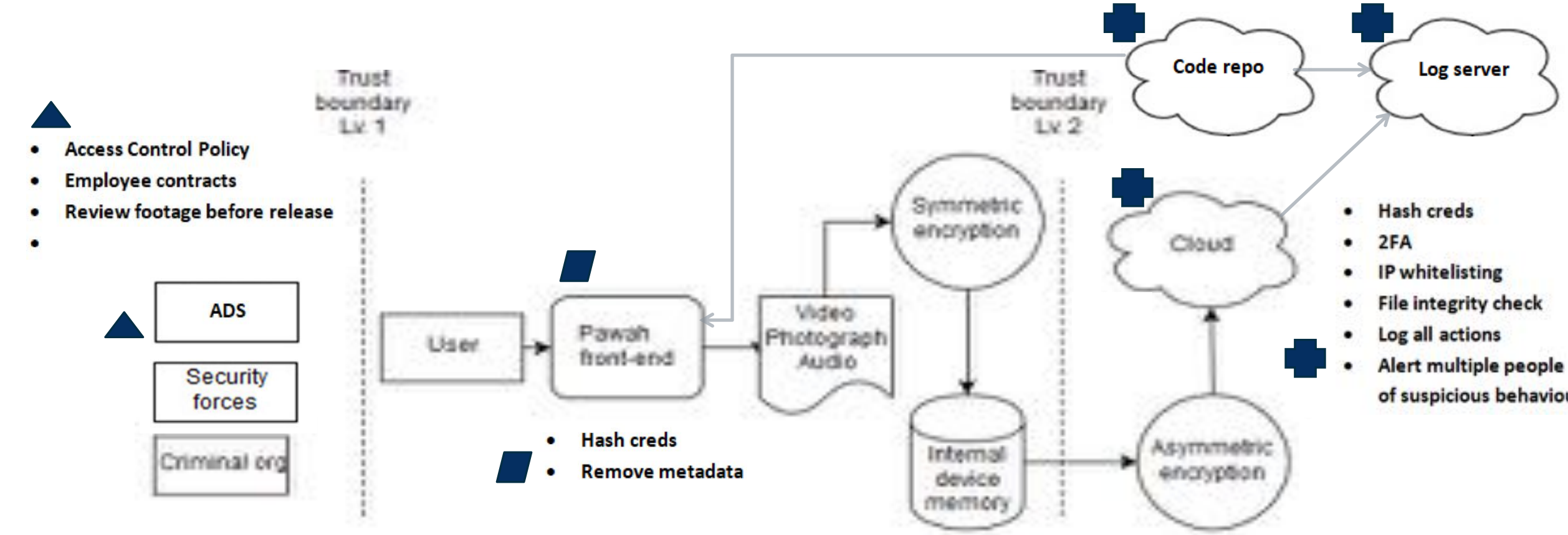
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – DENIAL OF SERVICE

- DDoS attack against the cloud storage (however that may be)
  - Employ DDoS mitigation services like Cloudflare
  - Cap how much footage a user can upload



Threats

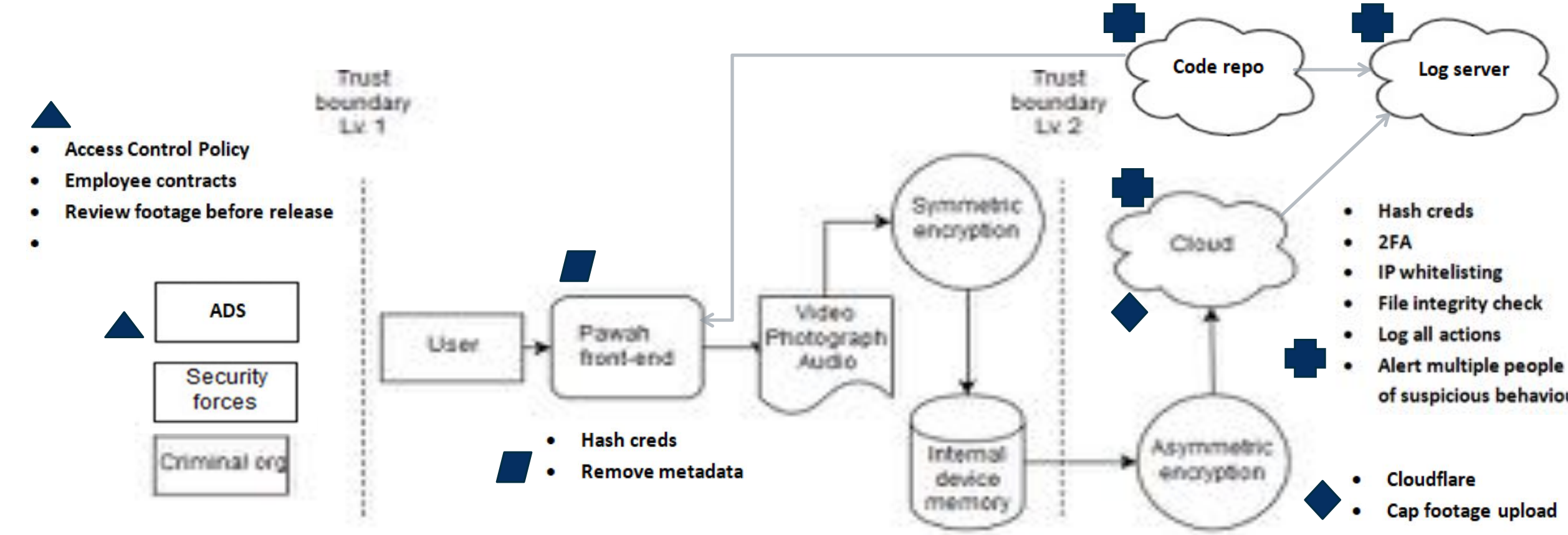
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

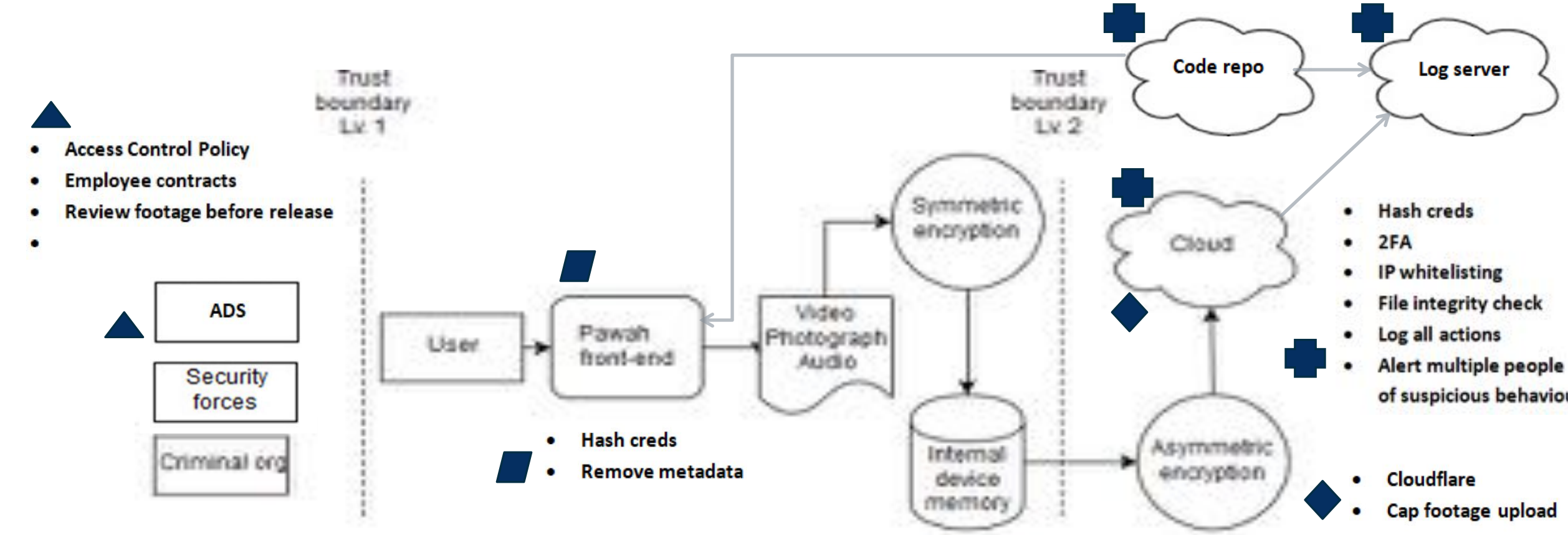
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

STRIDE – ELEVATION OF PRIVILEGES

- Someone gaining administrator rights to the code repository or cloud storage
  - Log all actions by users
  - Flag multiple people of new admins being created
  - Flag multiple people of admins performing anomalous behaviour like logging in outside of work hours.



Threats

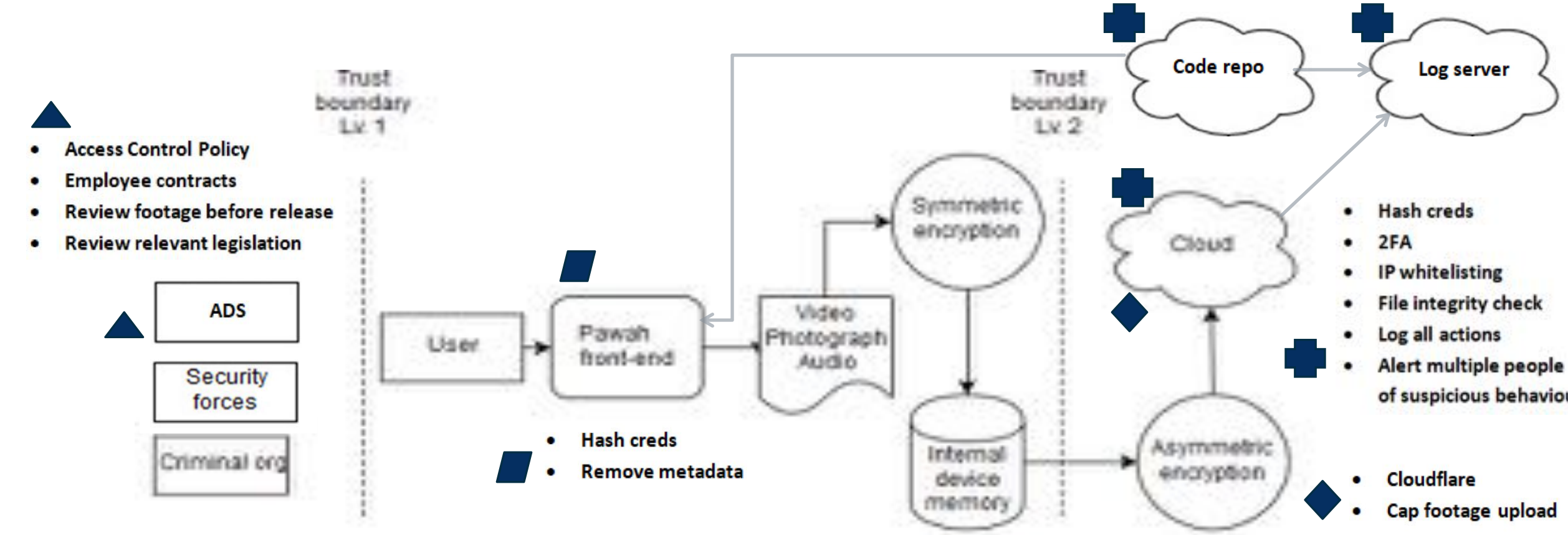
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

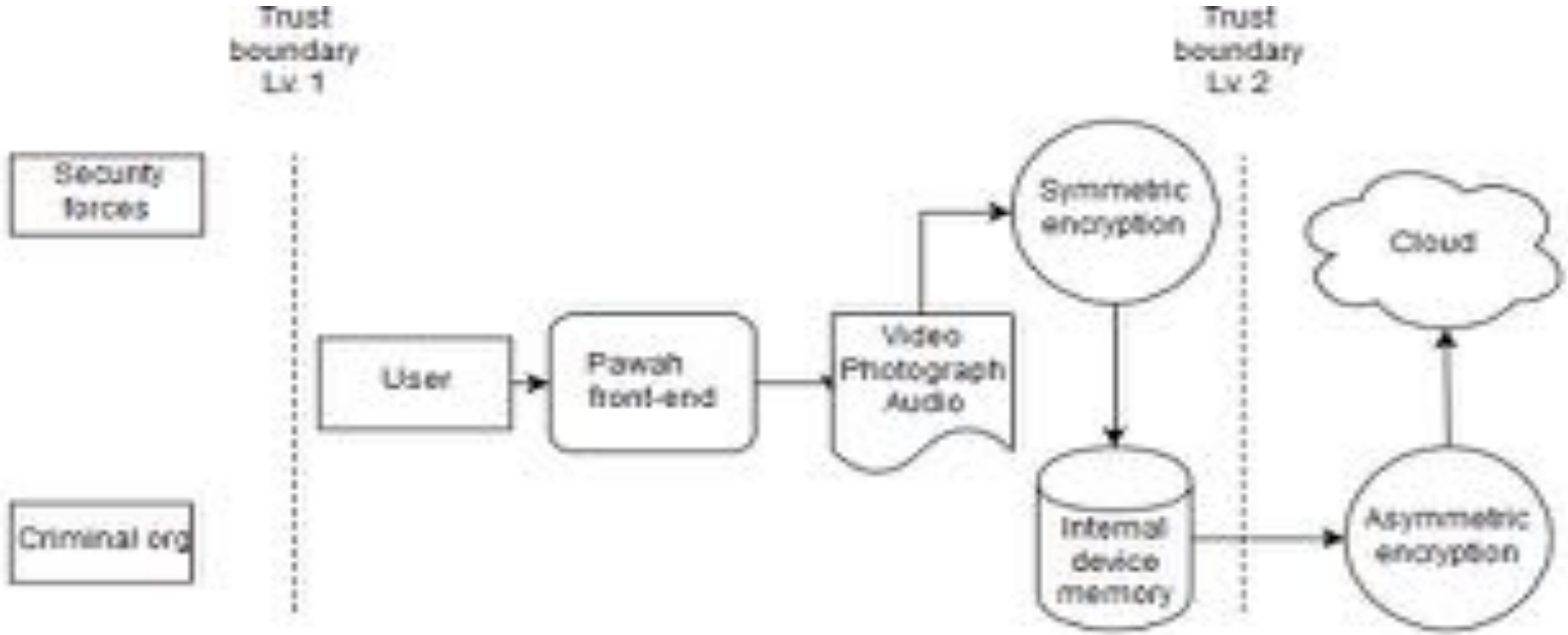
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

TAKING THIS FURTHER

- These are basics
- Need to go lower
  - Technology
  - Protocols
  - How can each functionality be abused?
- How can attackers bypass the controls we already have?
- Make threat modelling iterative
- Assign responsibility



Threats

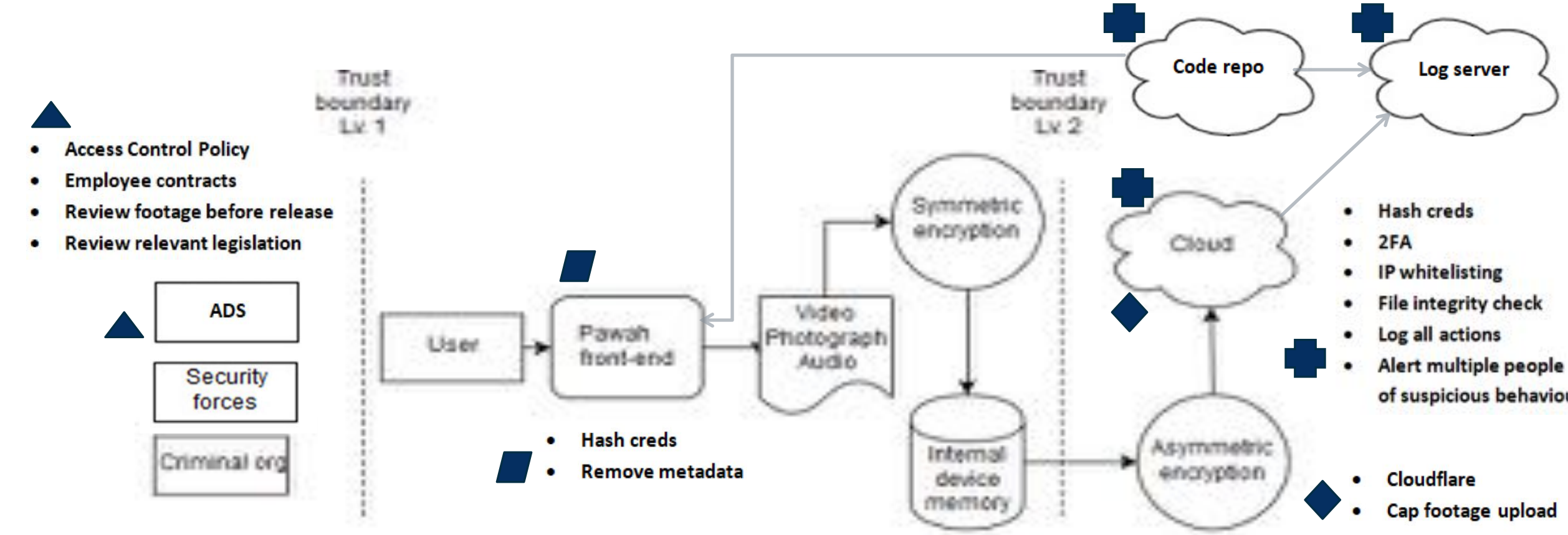
- Violent repression
- Intimidation
- Physical attack
- Kidnapping
- Imprison

Threats

- Device seizure
- Intimidation
- Device hacking

Threats

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



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

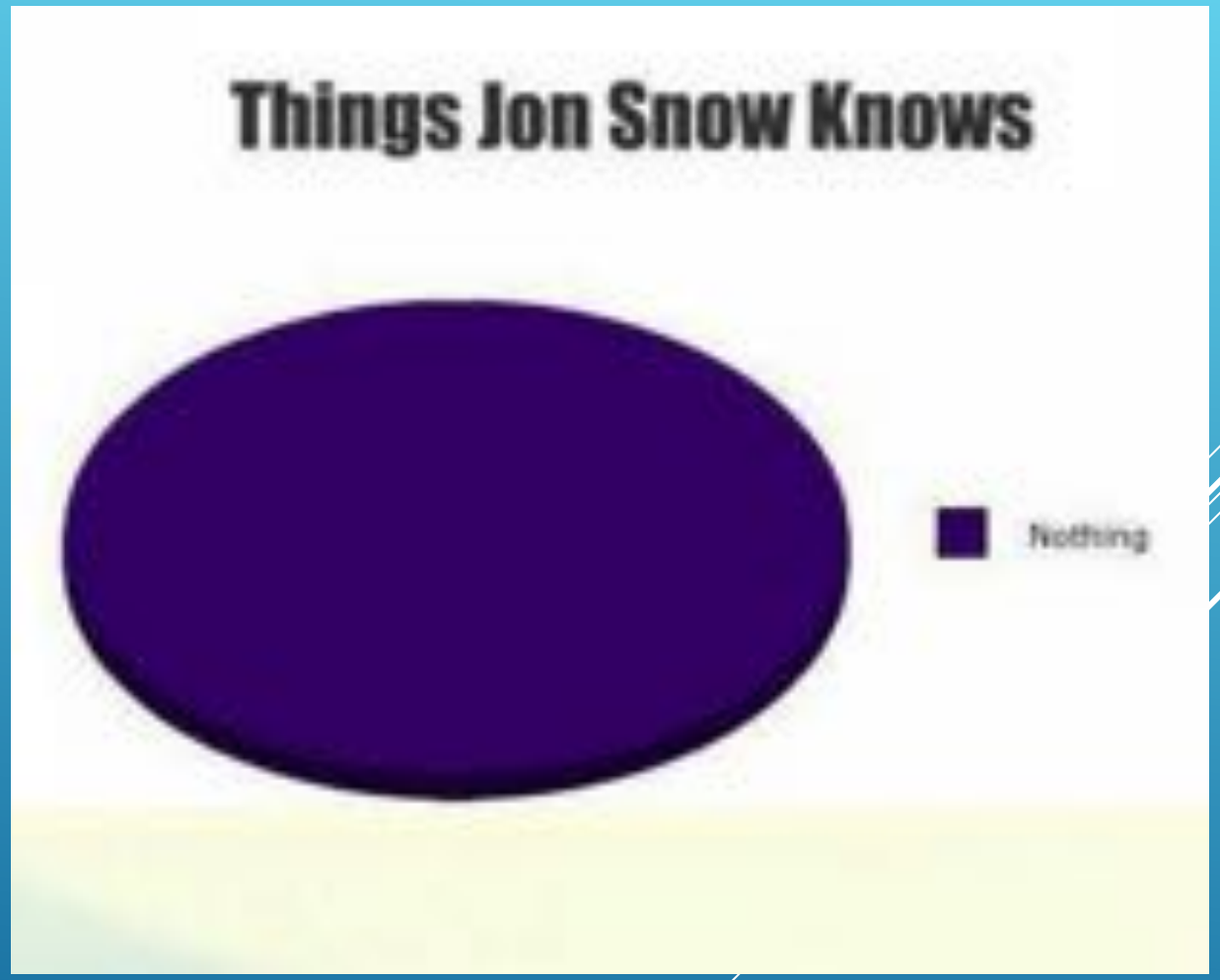
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation

IF YOU KNOW NOTHING…

- What are we building?
- What can go wrong? STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Denial of Service
  - Elevation of Privileges
- What are you going to do about it?
- This is the beginning but not the end



RESOURCES USED

- https://users.encs.concordia.ca/~clark/courses/1601-6150/scribe/L04c.pdf
- Threat Modelling with STRIDE adapted from Threat Modelling: Designing for Security (Wiley, 2014) by Adam Shostack
- https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649749(v=pandp.10)
- Walkthrough: Creating a Threat Model for a Web Application