Διάλεξη #1 - Security Fundamentals

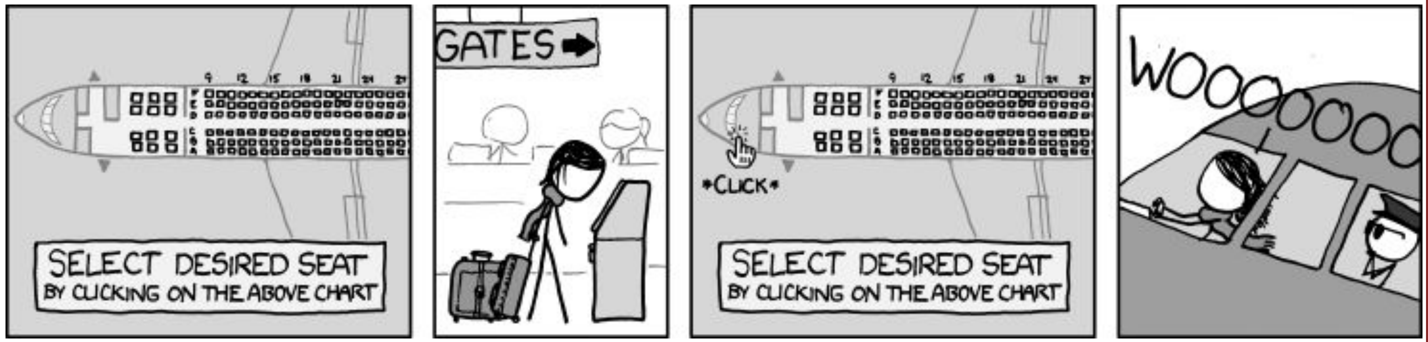
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

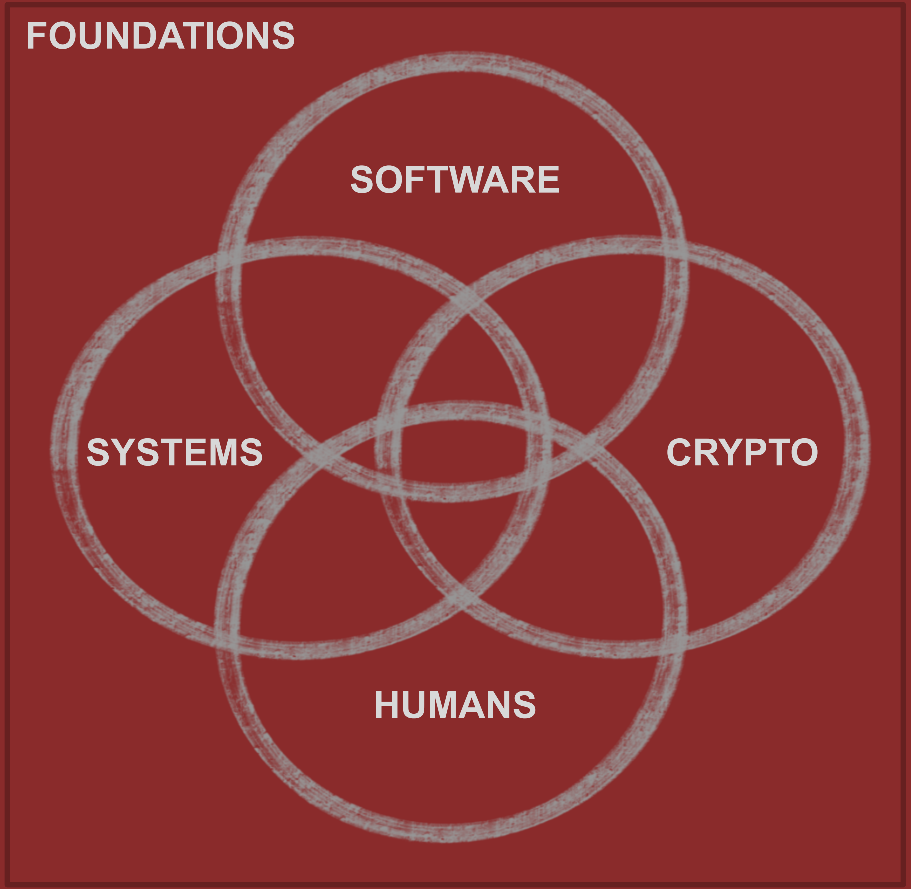
Εισαγωγή στην Ασφάλεια

Θανάσης Αυγερινός

(Security Mindset)

https://xkcd.com/726/


SELECT DESIRED SEAT
BY CLICKING ON THE ABOVE CHART
GATES
CLICK
SELECT DESIRED SEAT
BY CLICKING ON THE ABOVE CHART
WOOOOOOOO



Huge thank you to David Brumley from Carnegie Mellon University for the guidance and content input while developing this class

Ανακοινώσεις / Διευκρινίσεις

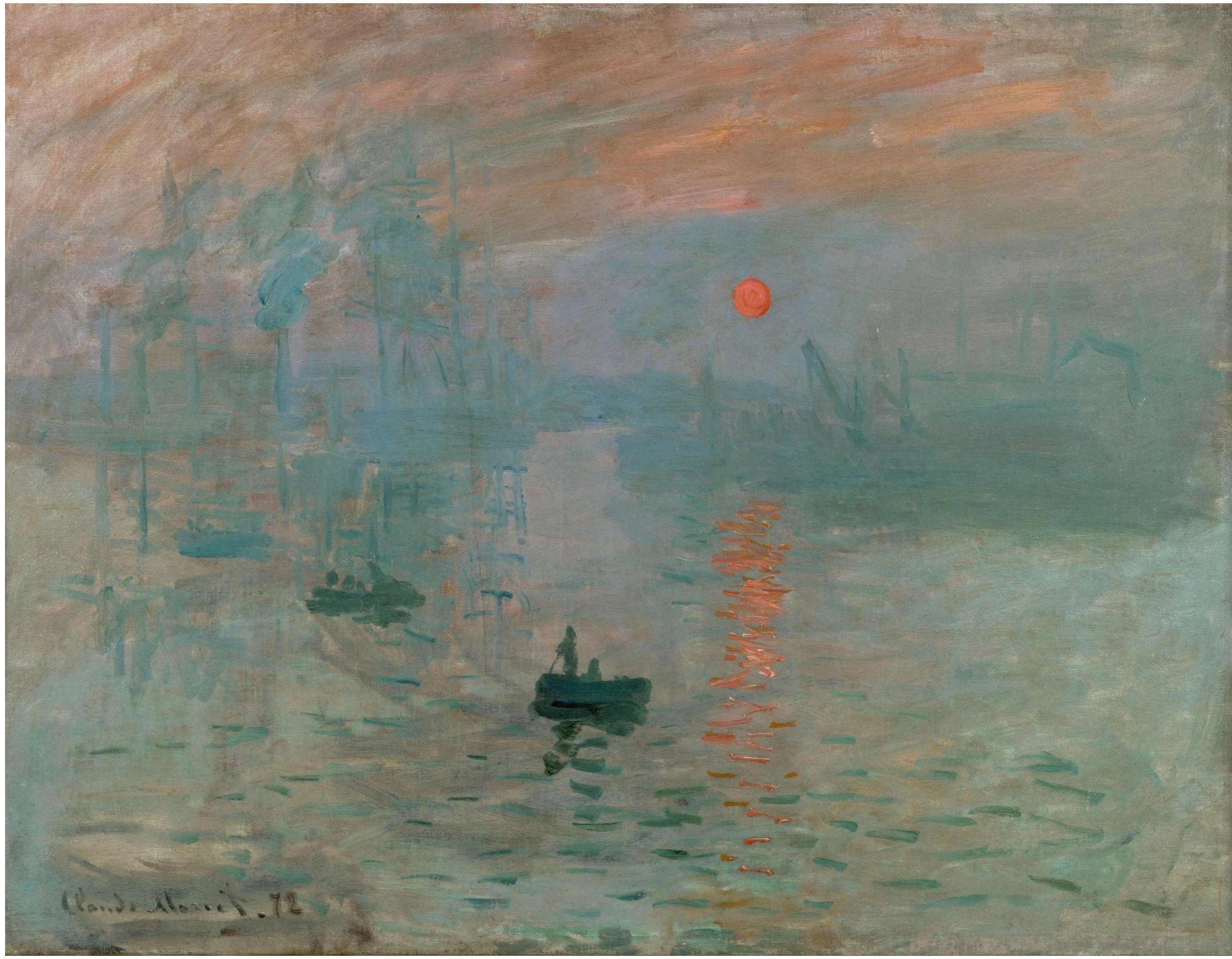
- Άρα δεν επιτρέπεται να κάνουμε scanf("%s", buffer);

Την Προηγούμενη Φορά

1. Διαδικαστικά
2. Σκοπός του μαθήματος
3. Ασφάλεια και Συστήματα
4. Σχέδιο για το μάθημα φέτος
5. Το πρώτο μας exploit

Σήμερα

- Security Fundamentals
    - Adversaries
    - Threat Models
    - Security Properties
    - Trusted Computing Base (TCB)
    - Security Principles



Two Concepts (Only a few I need you to memorize)

Defining The Adversary (1/2)

- Adversary = < Goals, Capabilities >
- Goal: What constitutes success?
  - May involve subgoals
  - Example goal: Gain control of X's data
    - Sub-goal: Reconnaissance: search online for info about X
      - Sub-goal: Access: Guess X's ssh password on Linux lab
        - » Sub-goal: Lateral movement: Use ssh account to move to other services / linked accounts
- Capabilities: What resources can the adversary use?
  - 1 computer or millions?
  - Physical or remote access?
  - Access to source code?

Why don't we include adversary's strategy?

Defining The Adversary (1/2)

- Adversary = < Goals, Capabilities >

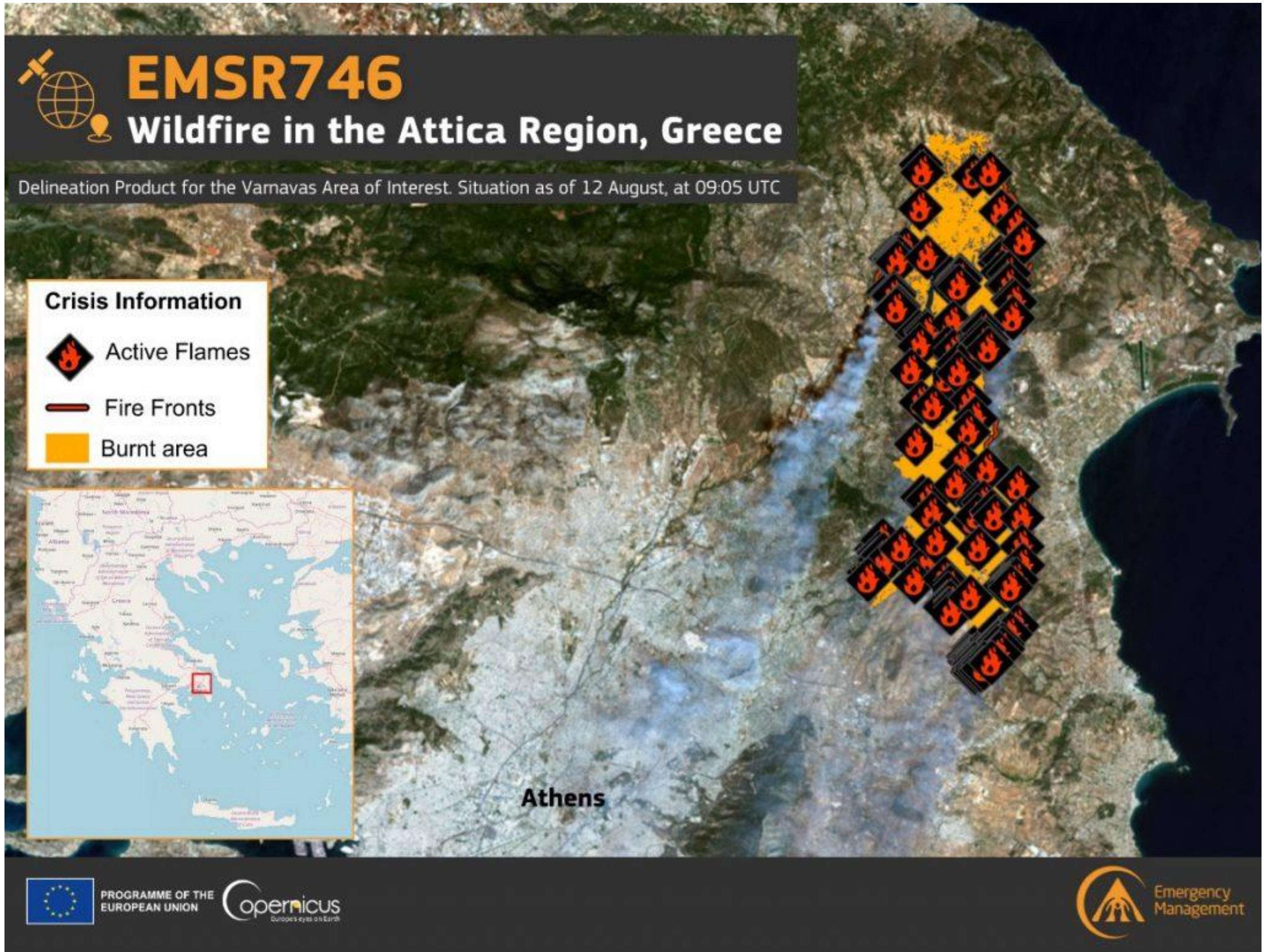
Belgium
Bonn
Luxembourg
GERMANY
Heidelberg
Nancy
Troyes
Epinal
FRANCE
Freiburg
Dijon
Switzerland

Why don't we include adversary's strategy?

Security Mechanism Classification for a property (2/2)

1. **Prevention**. Prevent issues from happening. Any precautionary measures.
2. **Detection**. Assuming an incident took place, detect them as early and as accurately as possible.
3. **Resilience**. Assuming one or multiple incidents took place, ensure the overall system security degrades gracefully and does not collapse.
4. **Deterrence**. Measures to ensure penalties for actors responsible for security incidents. Policy-based.

Fire Drill: How to Defend?


EMSR746
Wildfire in the Attica Region, Greece
Delineation Product for the Varnavas Area of Interest. Situation as of 12 August, at 09:05 UTC
Crisis Information
Active Flames
Fire Fronts
Burnt area
Athens
PROGRAMME OF THE EUROPEAN UNION
Copernicus
Emergency Management

Adversaries

Basic Adversary Metrics

Partial Orders

Adv_0 $\langle \text{Goals}_0, \text{Capabilities}_0 \rangle$

$>$

$<$

$\leftrightarrow$

$\#$

Adv_1 $\langle \text{Goals}_1, \text{Capabilities1} \rangle$

<u>Implication (A0 $\rightarrow$ A1)</u>:
A0's goals and capabilities are a superset of A1's

<u>Separation (A1 $\nrightarrow$ A0)</u>:
A1's goals and/or capabilities are not a superset of A0's

Strict Dominance A0 $>$ A1 $=$ A0 $\rightarrow$ A1 $\wedge$ A1 $\nrightarrow$ A0
Equivalence: A0 $\leftrightarrow$ A1 $=$ A0 $\rightarrow$ A1 $\wedge$ A1 $\rightarrow$ A0
Incomparable: A0 $\#$ A1 $=$ A0 $\nrightarrow$ A1 $\wedge$ A1 $\nrightarrow$ A0

Example Adversary Comparison

Adversary A0

- Goal: Modify the my-uni website
- Capabilities
  - View the website
  - Send data to the website
  - Modify local browser state
  - Access a normal user account on my-uni
  - Invoke system calls on `my-uni.uoa.gr`

Adversary A1

- Goal: Modify the my-uni website
- Capabilities
  - View the website
  - Send data to the website
  - Modify local browser state
  - ~~Access a normal user account on my-studies~~
  - ~~Invoke system calls on my-uni.uoa.gr~~

$A0 \rightarrow A1 \wedge A1 \nrightarrow A0$ hence A0 > A1, i.e., A0 strictly dominates A1

Threat Models

Threat Modeling

Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated, and countermeasures prioritized.

https://en.wikipedia.org/wiki/Threat_model

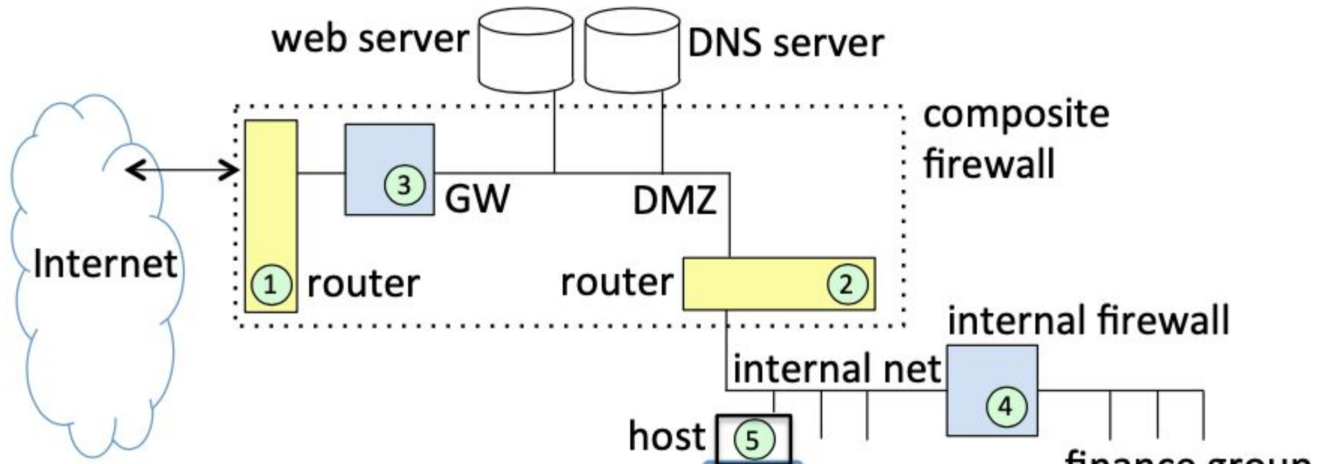
https://www.threatmodelingmanifesto.org/

Threat Model Includes

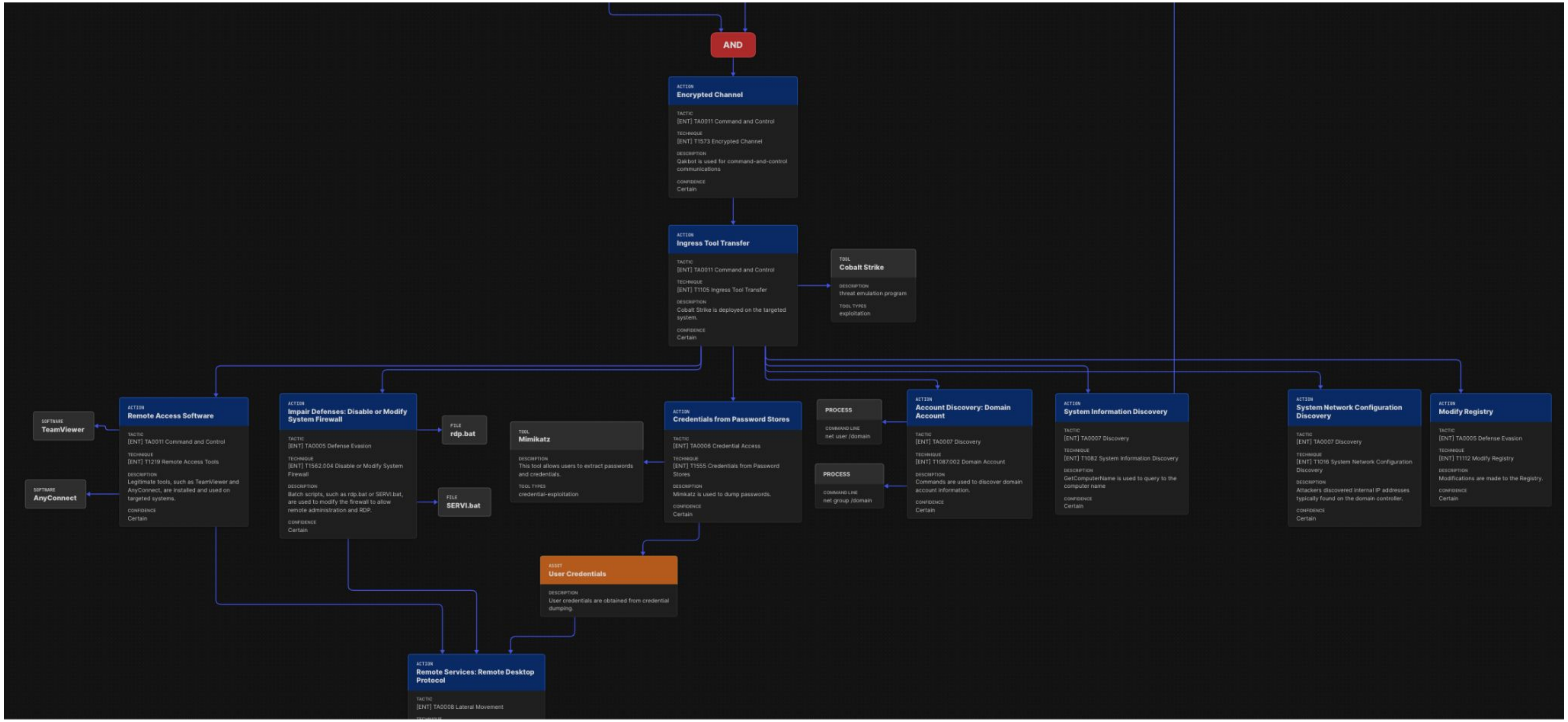
- Assets
  - What are you protecting?
  - Which matter most?
- System goals (functionality, security)
- Adversary definition – key characteristic
  - Risk assessment – we are in the insurance business!
    - Risk justifies the cost

Systematic Threat Modeling

- Diagram-based
- Attack trees
- Checklists
- STRIDE
- [MITRE ATT&CK]()
- [Tactics, Techniques and Procedures (TTP)]()



Attack Formalizations & Visualizations



ACTION
Encrypted Channel
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1573 Encrypted Channel
DESCRIPTION
Qakbot is used for command-and-control communications
CONFIDENCE
Certain

ACTION
Ingress Tool Transfer
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1105 Ingress Tool Transfer
DESCRIPTION
Cobalt Strike is deployed on the targeted system.
CONFIDENCE
Certain

TOOL
Cobalt Strike
DESCRIPTION
threat emulation program
TOOL TYPES
exploitation

SOFTWARE
TeamViewer

SOFTWARE
AnyConnect

ACTION
Remote Access Software
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1219 Remote Access Tools
DESCRIPTION
Legitimate tools, such as TeamViewer and AnyConnect, are installed and used on targeted systems.
CONFIDENCE
Certain

ACTION
Impair Defenses: Disable or Modify System Firewall
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1562.004 Disable or Modify System Firewall
DESCRIPTION
Batch scripts, such as rdp.bat or SERVI.bat, are used to modify the firewall to allow remote administration and RDP.
CONFIDENCE
Certain

FILE
rdp.bat

FILE
SERVI.bat

TOOL
Mimikatz
DESCRIPTION
This tool allows users to extract passwords and credentials.
TOOL TYPES
credential-exploitation

ACTION
Credentials from Password Stores
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1555 Credentials from Password Stores
DESCRIPTION
Mimkatz is used to dump passwords.
CONFIDENCE
Certain

PROCESS
COMMAND LINE
net user /domain

PROCESS
COMMAND LINE
net group /domain

ACTION
Account Discovery: Domain Account
TACTIC
[ENT] TA0007 Discovery
TECHNIQUE
[ENT] T1087.002 Domain Account
DESCRIPTION
Commands are used to discover domain account information.
CONFIDENCE
Certain

ACTION
System Information Discovery
TACTIC
[ENT] TA0007 Discovery
TECHNIQUE
[ENT] T1082 System Information Discovery
DESCRIPTION
GetComputerName is used to query to the computer name
CONFIDENCE
Certain

ACTION
System Network Configuration Discovery
TACTIC
[ENT] TA0007 Discovery
TECHNIQUE
[ENT] T1016 System Network Configuration Discovery
DESCRIPTION
Attackers discovered internal IP addresses typically found on the domain controller.
CONFIDENCE
Certain

ACTION
Modify Registry
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1112 Modify Registry
DESCRIPTION
Modifications are made to the Registry.
CONFIDENCE
Certain

ASSET
User Credentials
DESCRIPTION
User credentials are obtained from credential dumping.

ACTION
Remote Services: Remote Desktop Protocol
TACTIC
[ENT] TA0008 Lateral Movement

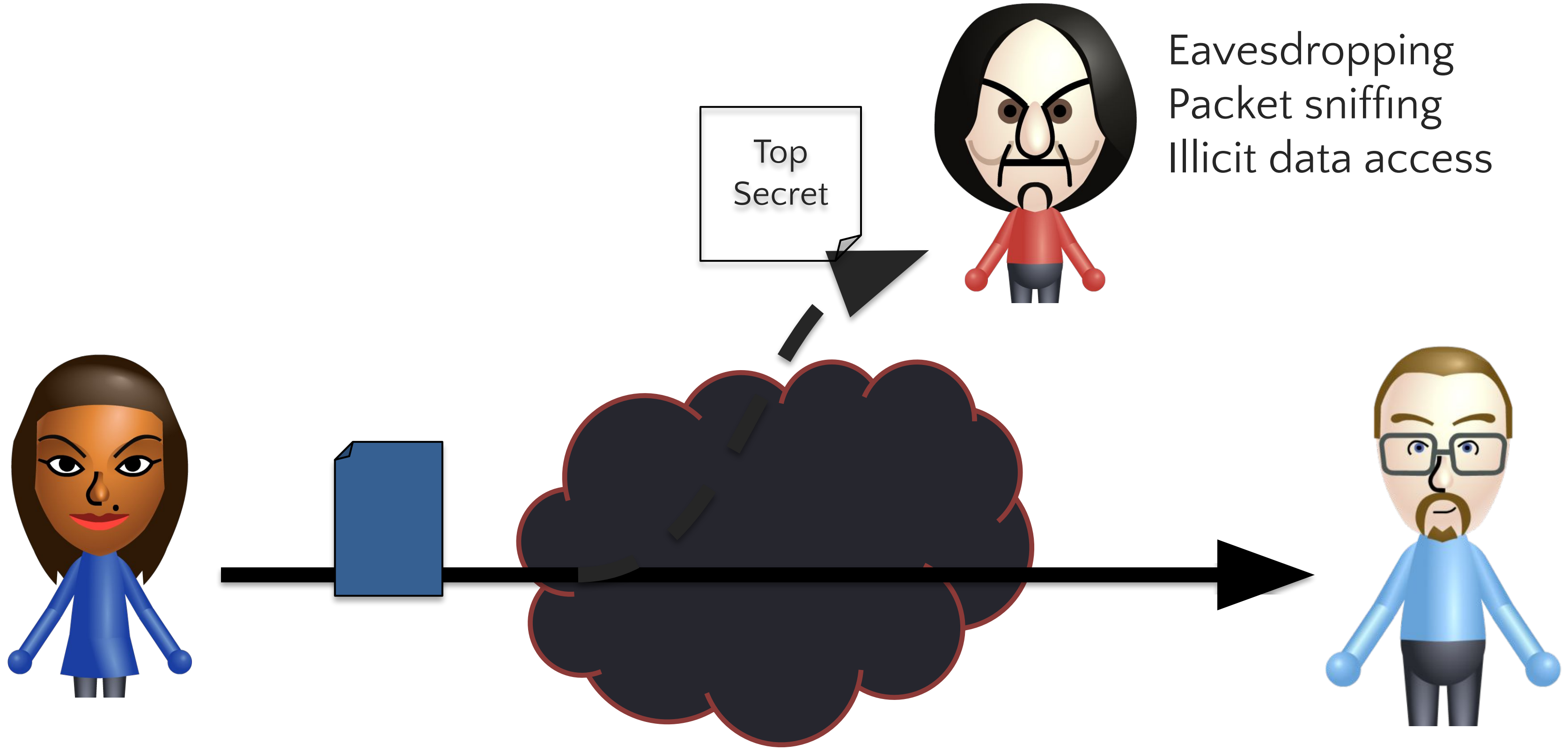
https://center-for-threat-informed-defense.github.io/attack-flow/example_flows/

https://oasis-open.github.io/cti-documentation/stix/intro.html

4 Key Security Properties

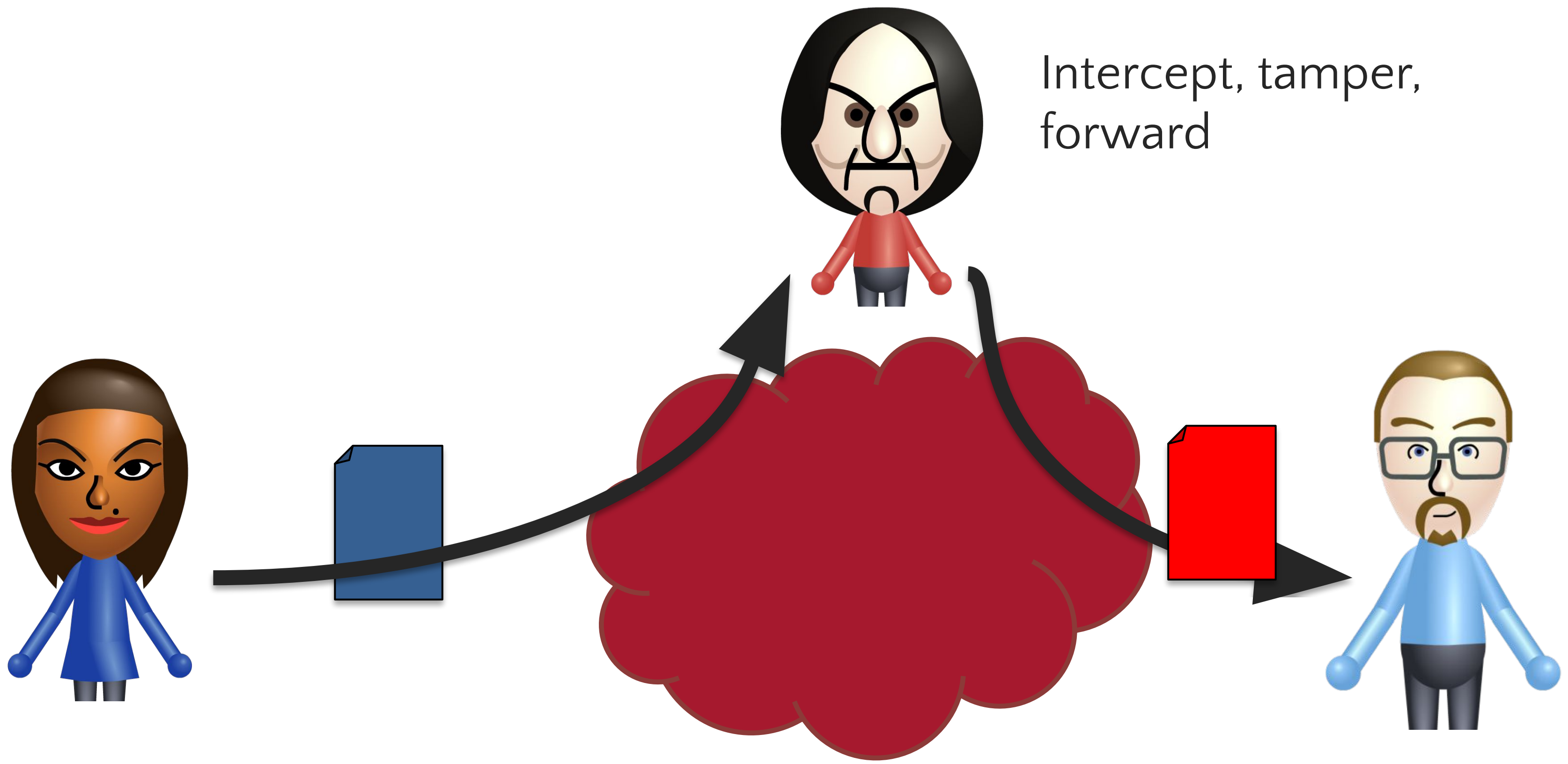
What Properties Do You Care About?

(1) **Confidentiality** == **Secrecy** == Concealing information



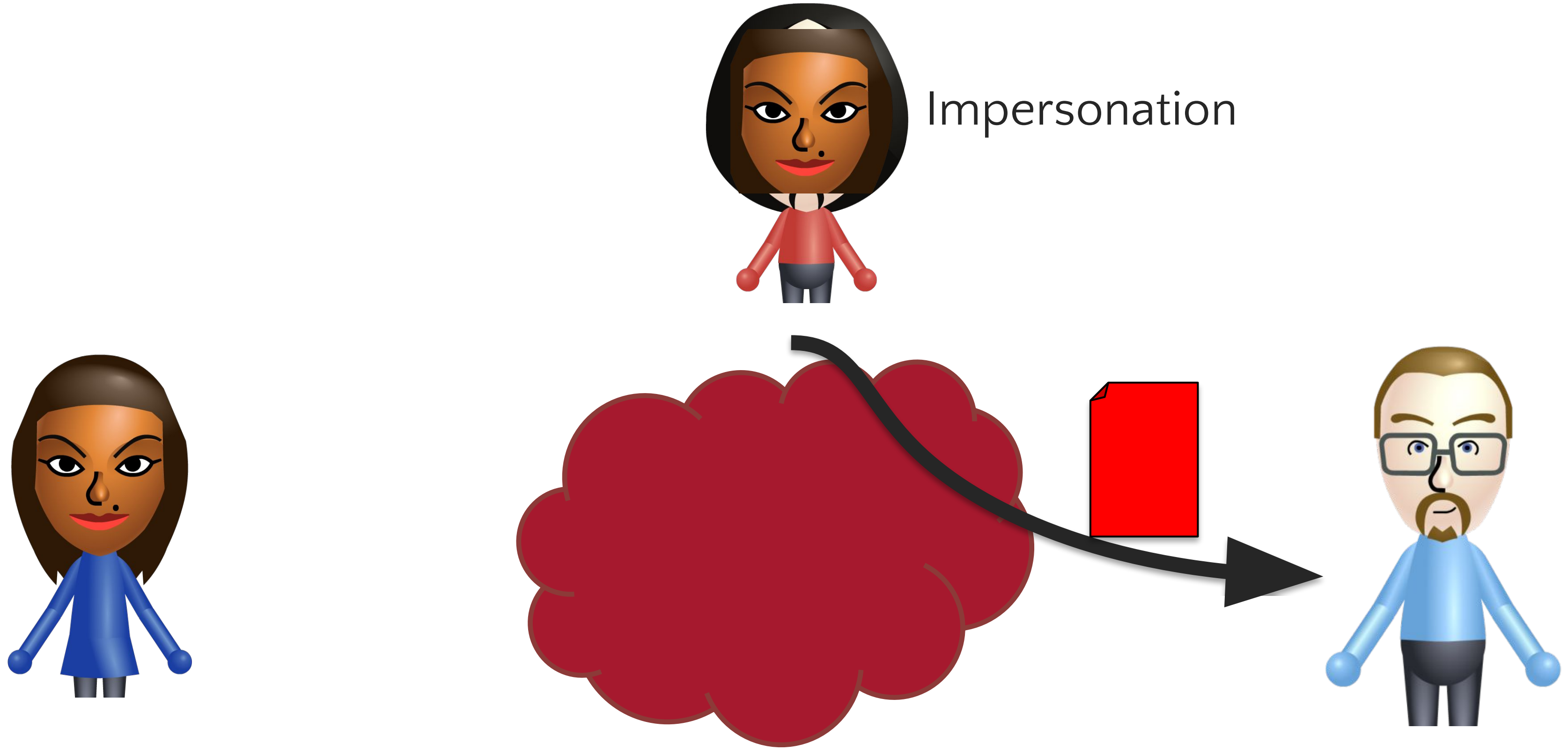
What Properties Do You Care About?

(2) **Integrity** == Prevention of unauthorized changes



What Properties Do You Care About?

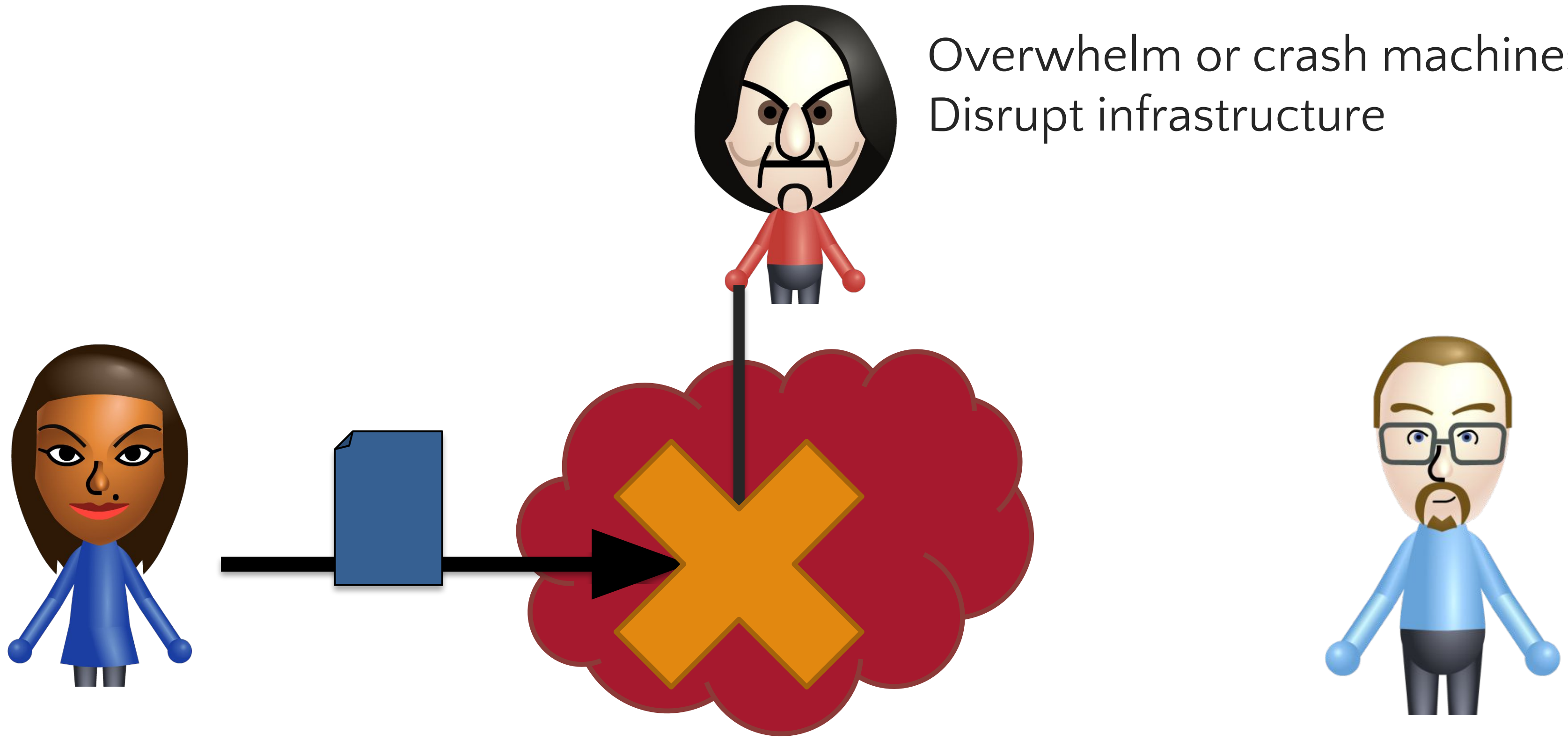
(3) **Authenticity** == Data and actions attributed to correct person



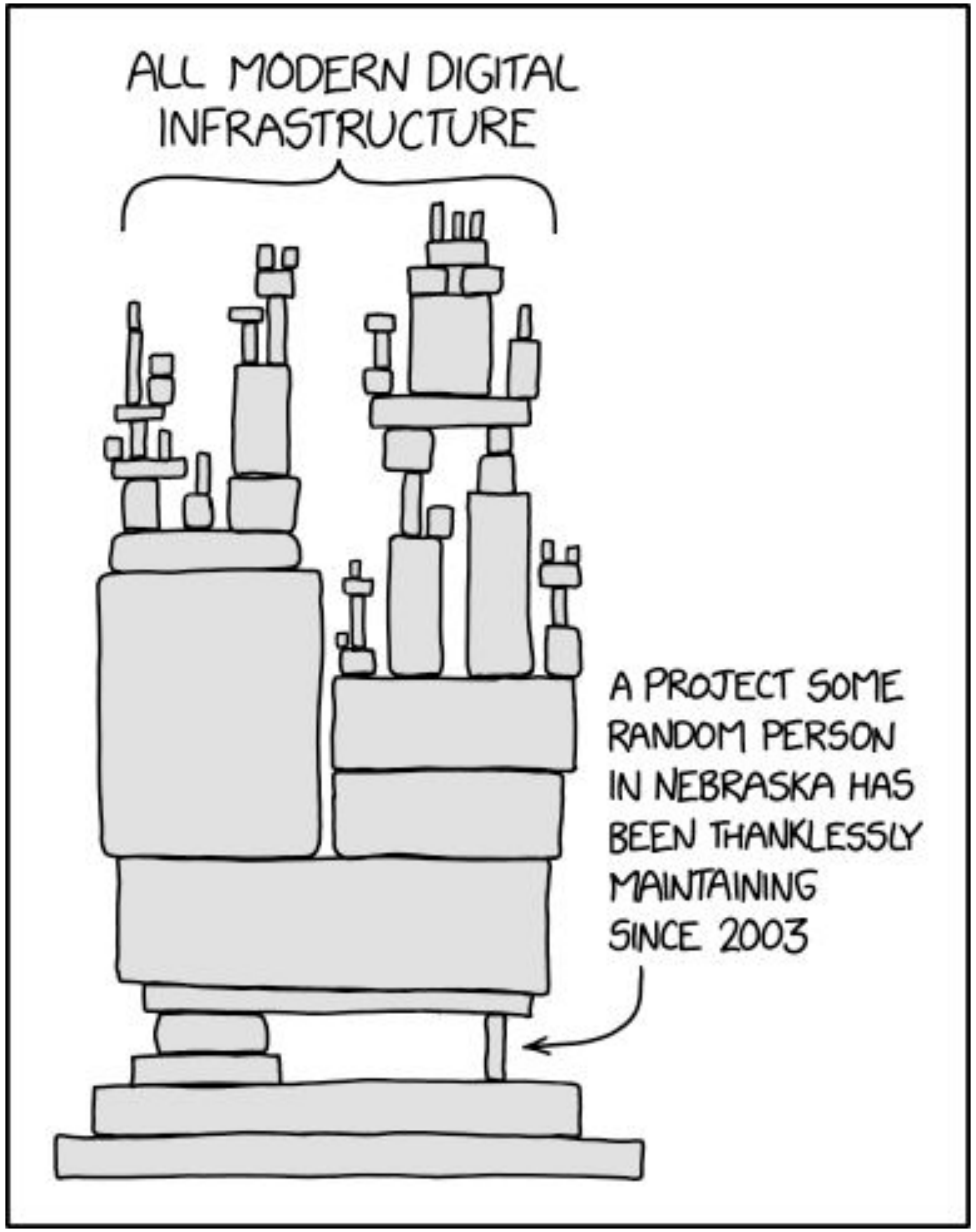
What Properties Do You Care About?

(4) **Availability** == Ability to use resources when needed

Overwhelm or crash machines,
Disrupt infrastructure



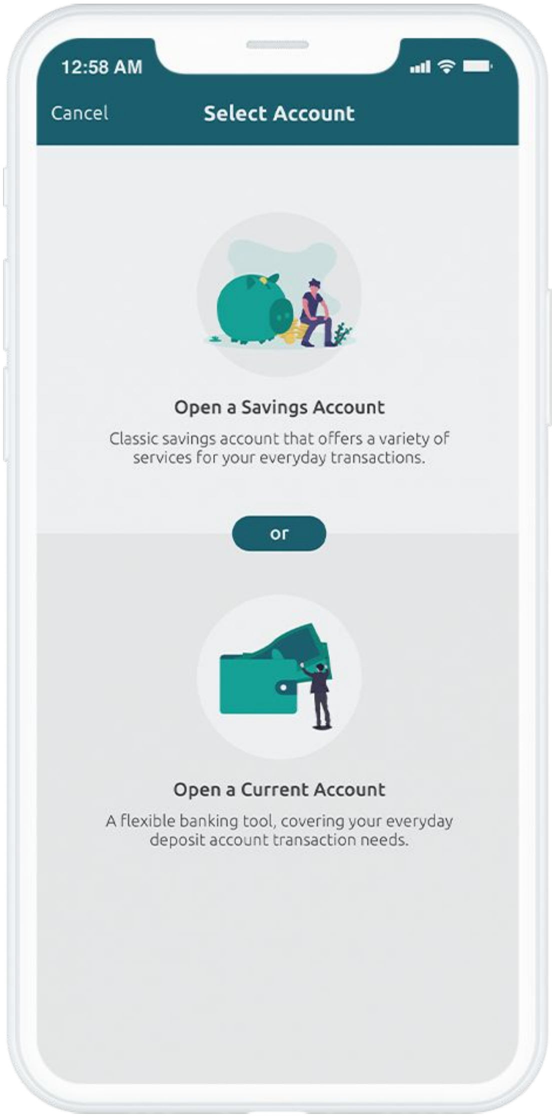
Trusted
Computing Base
(TCB)


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

https://xkcd.com/2347/

Why Should I Trust This?

What does this application rely on for its security?



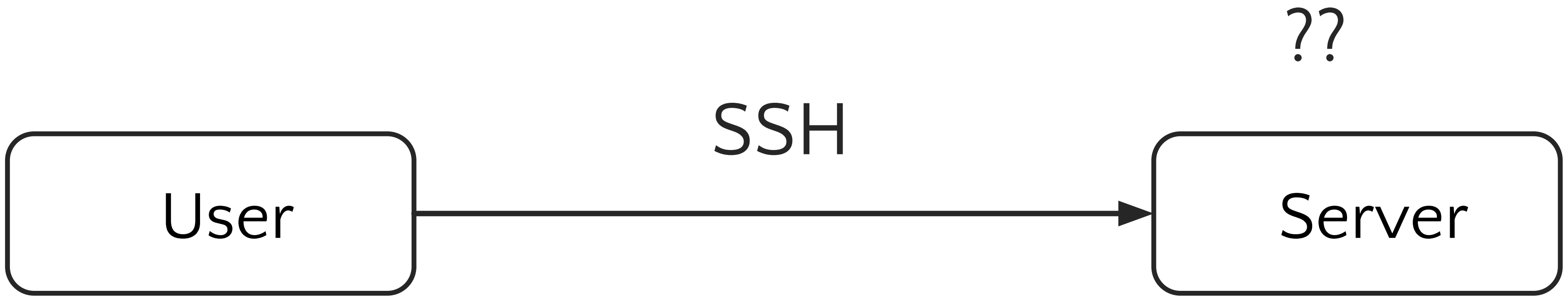
Classic savings account that offers a variety of services for your everyday transactions.

A flexible banking tool, covering your everyday deposit account transaction needs.

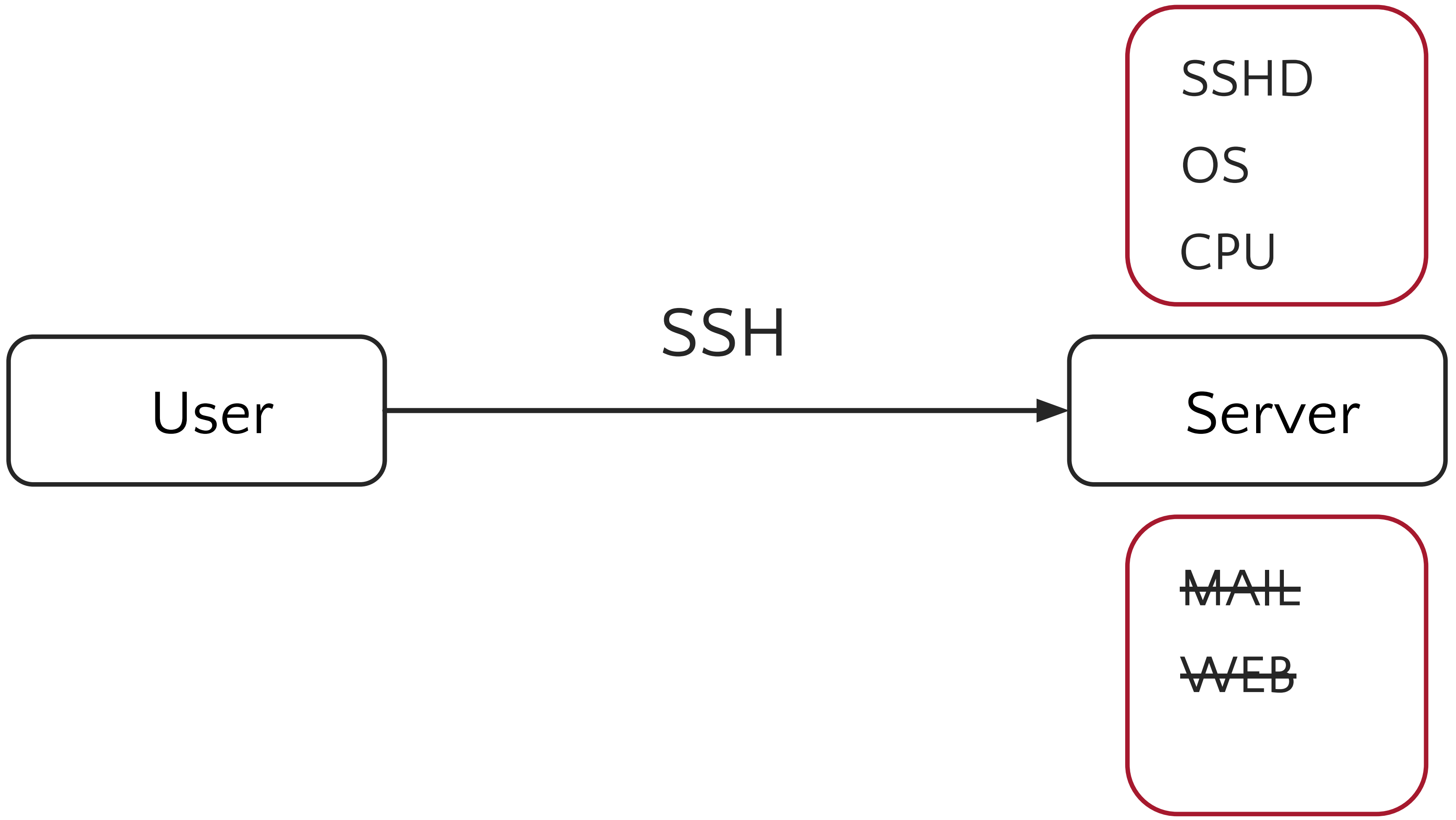
Trusted Computing Base (TCB)

- Component X’s TCB is all other components that must operate securely for X to be secure
- Corollary 1: If TCB is secure, X has a chance of being secure
- Corollary 2: If TCB misbehaves, no guarantees about X’s security!
- Trusted != Trustworthy

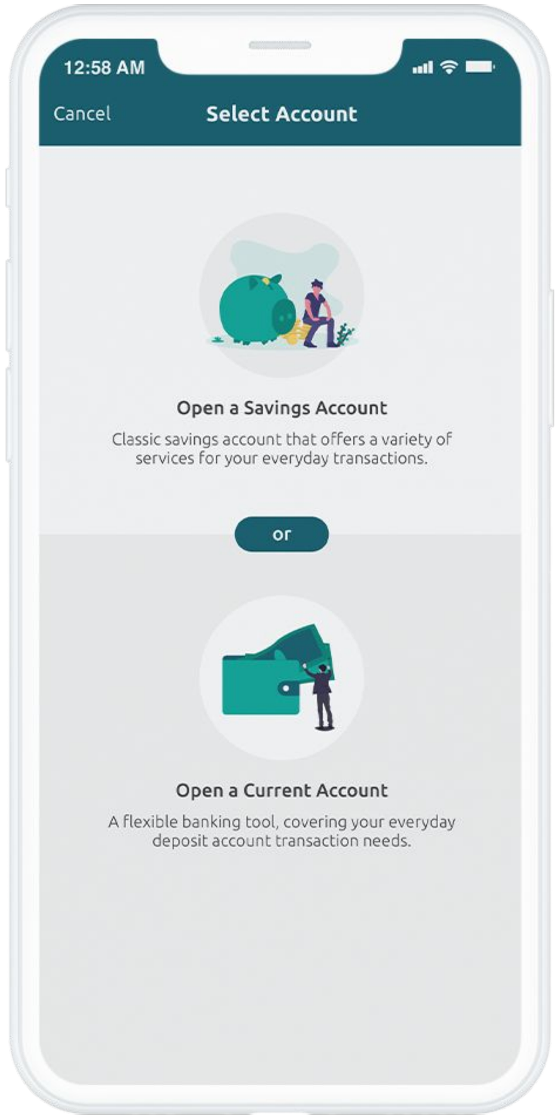
Example of TCB



Example of TCB



What is the TCB here?



Open a Savings Account

Classic savings account that offers a variety of services for your everyday transactions.

Open a Current Account

A flexible banking tool, covering your everyday deposit account transaction needs.

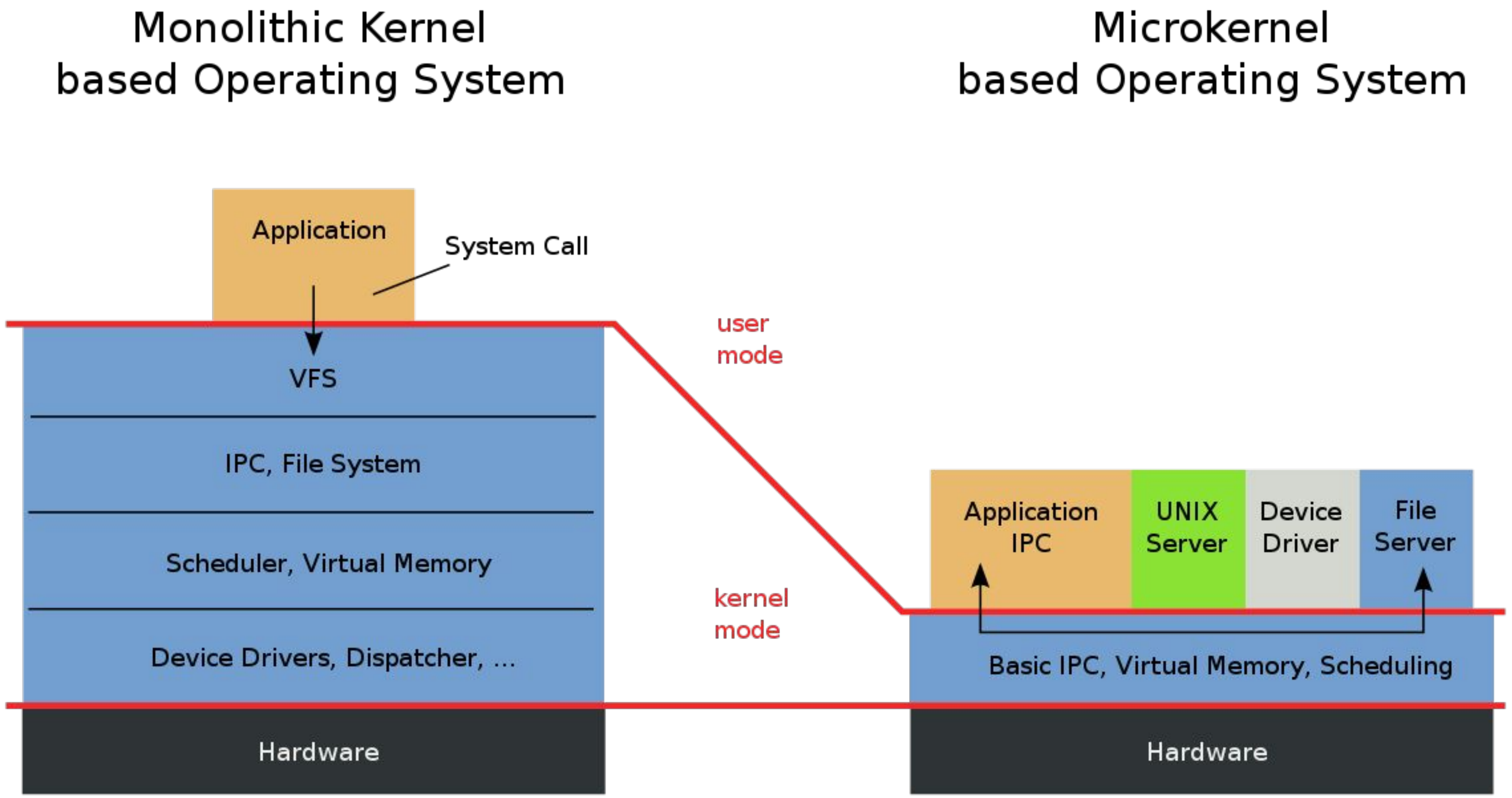
Ideal TCB Design

- Verifiable
  - Implies you want TCB to be as small as possible
    - (even when not verifiable, smaller = less buggy)
- Tamper proof
  - E.g., must prevent messing with the SSHD or OS executables

Why Do We Care About a TCB?

- Securing every piece of a system is hard!
- Identifying the TCB allows us to separate a system into a part that **must** be trusted and a part that **doesn't have to** be
- Can focus security efforts on the trusted piece
  - Reason about security more rigorously
- Caveat: Determining TCB is easier said than done

Example: Operating system kernel



Participation Question

Which of the following is ***NOT*** in the TCB of a *web browser* on your laptop?

A. The laptop’s OS
B. JavaScript the browser downloads when you visit a website
C. The laptop’s hardware
D. The browser’s cryptographic library

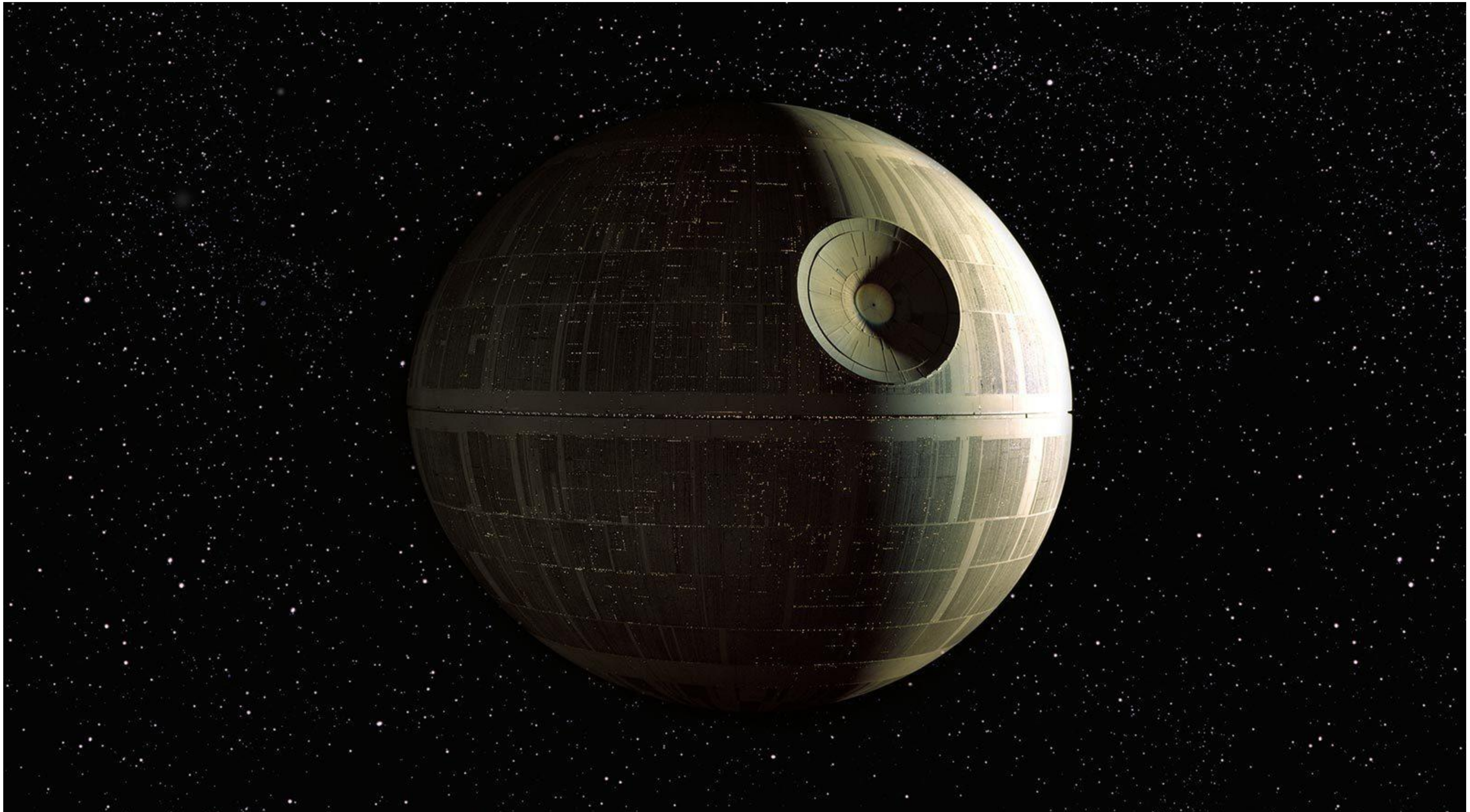
Designing Secure Systems

The Key Principles

- **Economy of mechanism a.k.a. KISS**
- Fail-safe defaults
- Don’t rely on security by obscurity
- Complete mediation
- Least privilege
- Separation of duty
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

$\left.\begin{matrix} \\ \\ \end{matrix}\right\}$ Later

See the reading for more useful principles



Keep It Simple, Stupid (KISS)

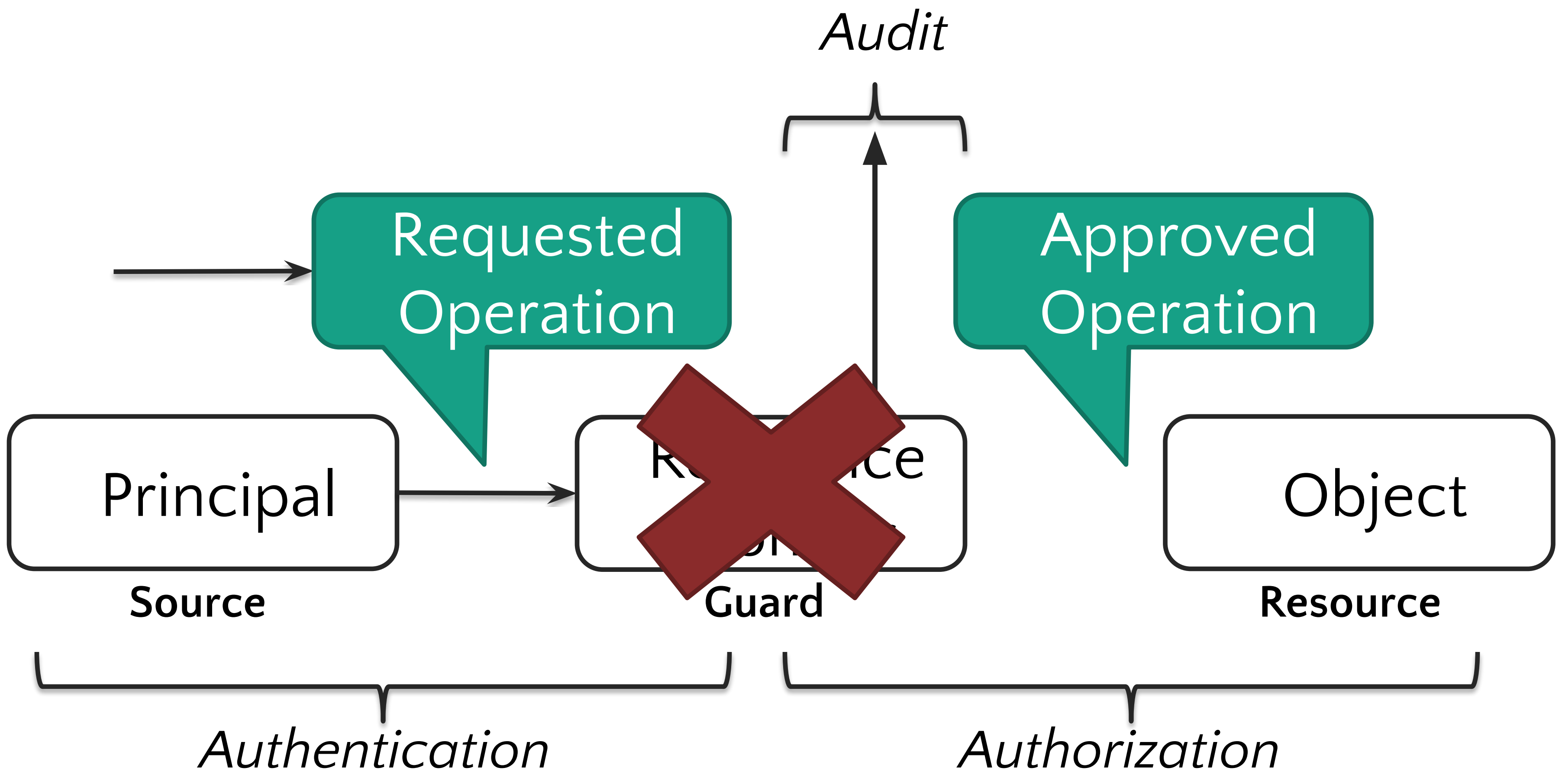
- Rule of thumb:
  1–5 defects per 1K lines of code
- Windows 10 = 50M LOC; Linux 6.7 = 27M LOC
  - In both cases, essentially all in the TCB
- Smaller, simpler TCB is easier to reason about
  - e.g.: seL4 (a formally verified microkernel) = 89k LOC

The Key Principles

- Economy of mechanism a.k.a. KISS
- **Fail-safe defaults**
- Don't rely on security by obscurity
- Complete mediation
- Least privilege
- Separation of duty
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

} Later

Fail-safe Defaults (Fail Closed)



The Key Principles

- Economy of mechanism a.k.a. KISS
- Fail-safe defaults
- **Don't rely on security by obscurity**
- Complete mediation
- Least privilege
- Separation of duty
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

} Later

No Security by Obscurity

- Common fallacy: System is more secure if the design remains secret
- Keeping designs secret is hard!
  - Someone has to build/implement it
  - Users interact with it
  - The design may be sold to lots of people
- Finding flaws in your own design is hard!

A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LAIH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, ...
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

https://xkcd.com/257/

The Key Principles

- Economy of mechanism a.k.a. KISS
- Fail-safe defaults
- Don’t rely on security by obscurity
- **Complete mediation**
- Least privilege
- Separation of duty
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

} Later

Complete Mediation

- Every access to every object is checked by the reference monitor
- Easier said than done!
- TOCTTOU problems

Mediation: TOCTTOU Vulnerabilities

Time-Of-Check-To-Time-Of-Use

```
int openfile(char *path){
   struct stat s;
   if (stat(path,&s) < 0))
      return -1;

   if (!S_ISREG(s.st_mode)){
      error("only regular files allowed");
      return -1;
   }
   return open(path,O_RDONLY)
}
```

Change path

Mediation: TOCTTOU Vulnerabilities

Time-Of-Check-To-Time-Of-Use

```
void withdraw(int w){
   b = getbalance();
   if (b<w)
      error(“not enough $$”);

   b = b-w;
   send(w)
}
```

Buy

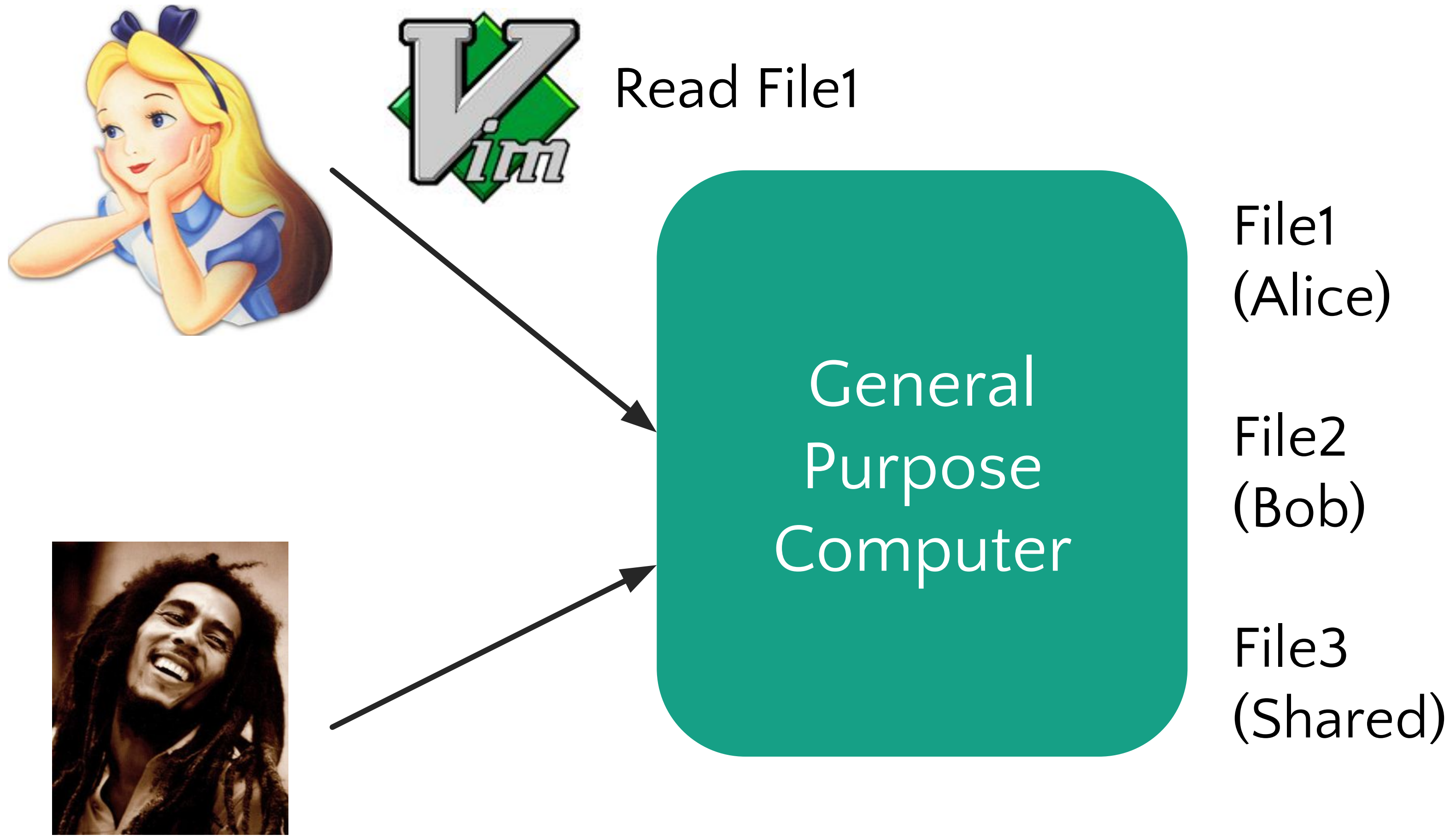
The Key Principles

- Economy of mechanism a.k.a. KISS
- Fail-safe defaults
- Don’t rely on security by obscurity
- Complete mediation
- **Least privilege**
- Separation of duty
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

} Later

Least Privilege

A user or entity should only have access to the specific data, resources and applications needed to complete a required task and nothing more.



The Key Principles

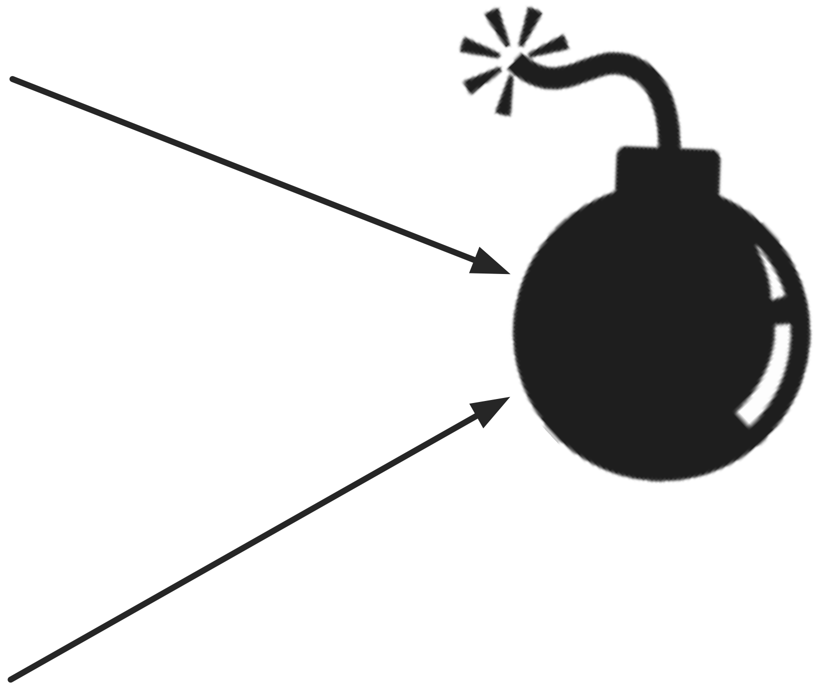
- Economy of mechanism a.k.a. KISS
- Fail-safe defaults
- Don't rely on security by obscurity
- Complete mediation
- Least privilege
- **Separation of duty**
- Defense in depth
- Factor in users/acceptance/psychology
- Work factor/economics

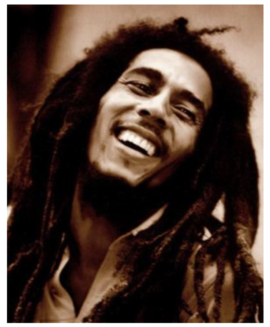
} Later

Separation of Duty (SoD)

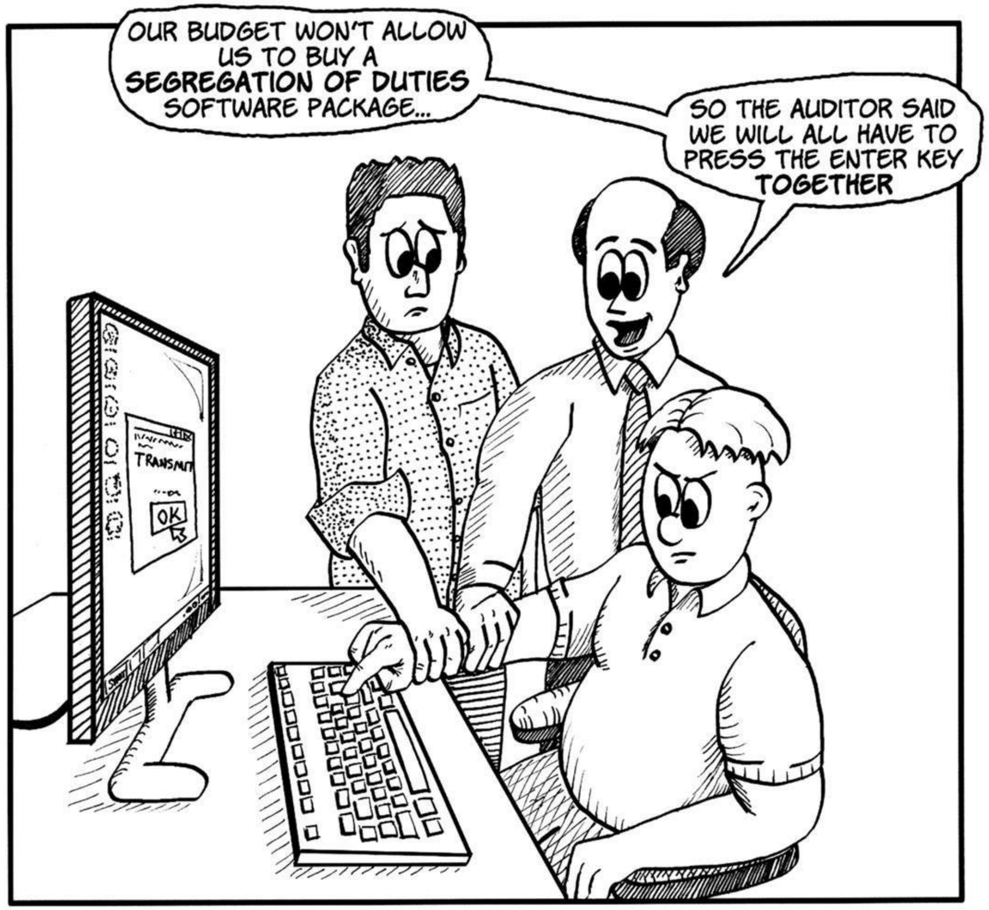
Having more than one person required to complete a task!

Push Pull Request
Launch Missile





Approve Pull Request
Launch Missile


OUR BUDGET WON'T ALLOW US TO BUY A SEGREGATION OF DUTIES SOFTWARE PACKAGE...
SO THE AUDITOR SAID WE WILL ALL HAVE TO PRESS THE ENTER KEY TOGETHER
TRANSMIT
OK

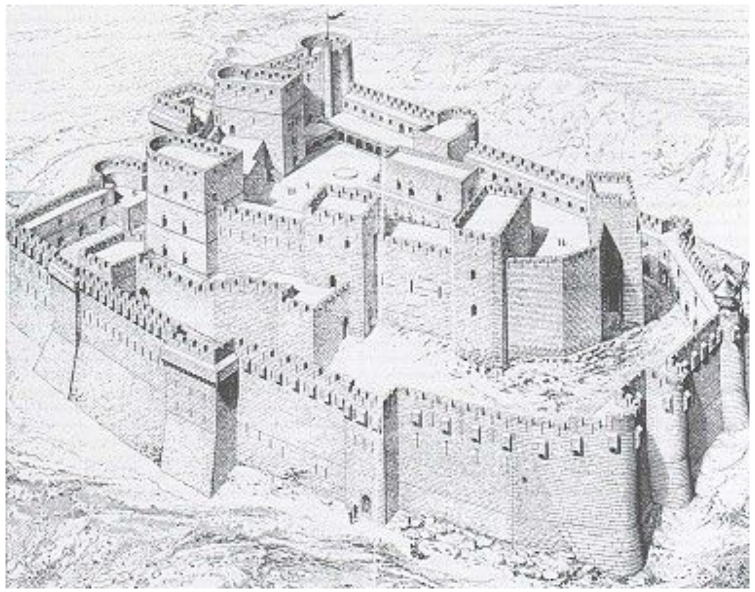
The Key Principles

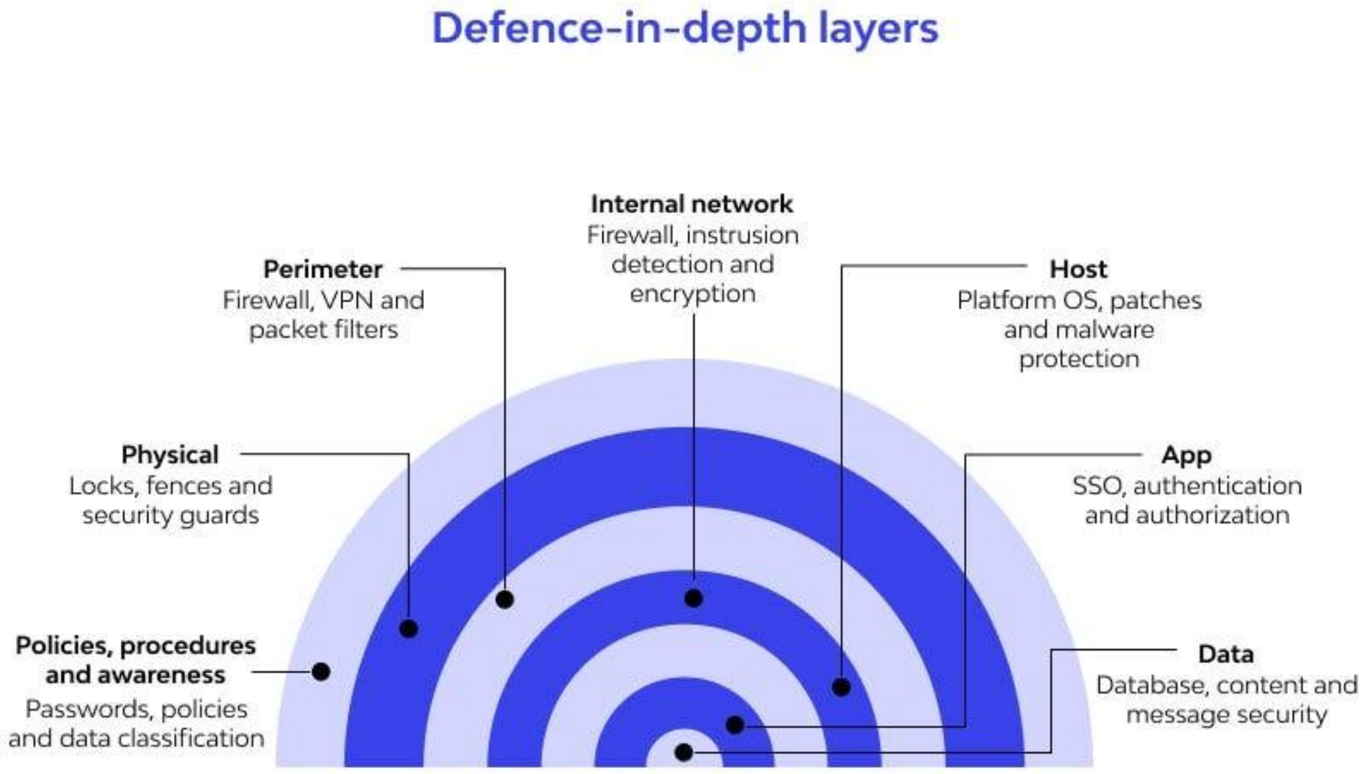
- Economy of mechanism a.k.a. KISS
- Fail-safe defaults
- Don't rely on security by obscurity
- Complete mediation
- Least privilege
- Separation of duty
- **Defense in depth**
- Factor in users/acceptance/psychology
- Work factor/economics

} Later

Defense in Depth

- Few defensive measures are perfect
- Plan for failures
- Beware risk compensation!




Defence-in-depth layers
Internal network
Firewall, instrusion detection and encryption
Perimeter
Firewall, VPN and packet filters
Host
Platform OS, patches and malware protection
Physical
Locks, fences and security guards
App
SSO, authentication and authorization
Policies, procedures and awareness
Passwords, policies and data classification
Data
Database, content and message security

Participation Question

Systems based on ACLs (like UNIX) typically deny access entirely if a subject is not listed on the relevant ACL. This is an example of which principle?

A. Fail-safe defaults

B. Complete mediation

C. Separation of duty

D. Defense in depth

I Followed All Security Principles - Am I Secure?

- Defense in Depth
- Patched systems
- 24/7 monitoring/ alerting
- Annual compliance auditing
- Experienced IT/ Security team
User clicks on an email

Ευχαριστώ και καλή μέρα εύχομαι!

Keep hacking!