Information Security

CS3002

Lecture 2

21st August 2024

Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

Risk Estimation

- Assets: Objects, data, people
- Vulnerability: Weakness of an asset
- Threat: loss of security due to vulnerability
- Attack: threat occurrence

- Risk estimation is the process of identifying vulnerabilities and threats and their impact and probability of occurring an attack.

Data Protection

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers

- An effective information security program is essential to the protection of the integrity and value of the organization's data

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided

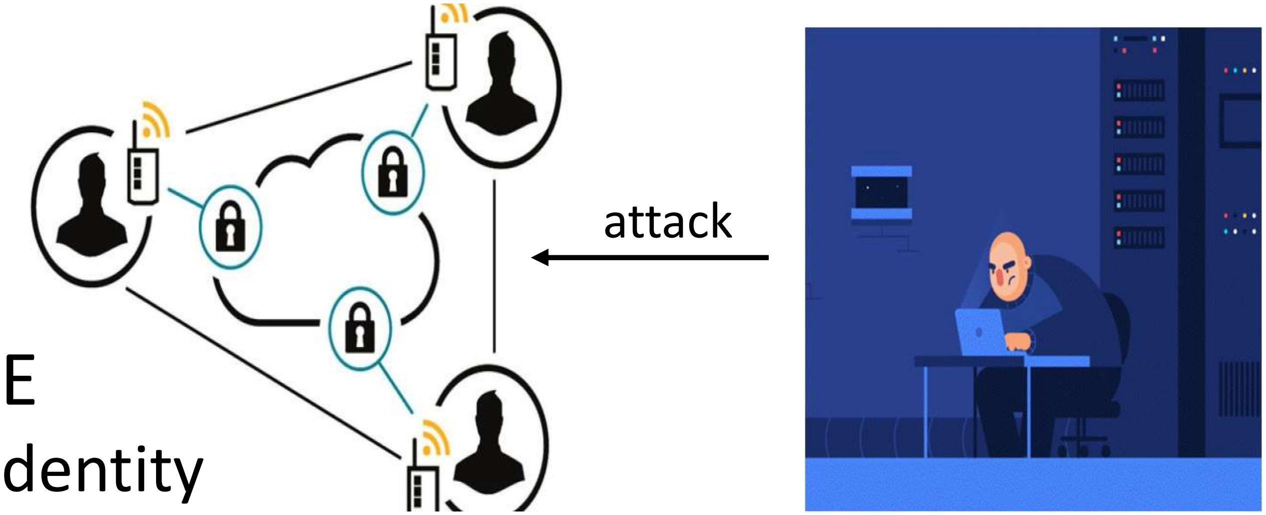
Threats

- A threat is an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the various kinds of threats facing the organization
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Threat Modeling

Threat Modeling

- Theoretical use cases considered to identify potential threats.


attack

- Microsoft STRIDE
  - S: Spoofing of identity
  - T: Tampering with data
  - R: Repudiation
  - I: Information disclosure
  - D: Denial of service
  - E: Elevation of privilege
- Requires realization of Assets and Vulnerabilities

Attacks

- An attack is the deliberate act that exploits vulnerability

- It is accomplished by a threat-agent to damage or steal an organization’s information or physical asset
  - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective

  - An exploit is a technique to compromise a system

  - An attack is then the use of an exploit to achieve the compromise of a controlled system

Some Classes of Attacks

- Phishing (~ fishing):
- "dear Internet banking user, please fill in the attached module and return it to us ASAP according to the privacy law 675 …"

- psychological pressure:
- "help me, otherwise I'll be in troubles …"
- "do it, or I'll report it to your boss …"
- showing acquaintance with the company's procedures, habits and personnel helps in gaining trust and make the target lower his defenses

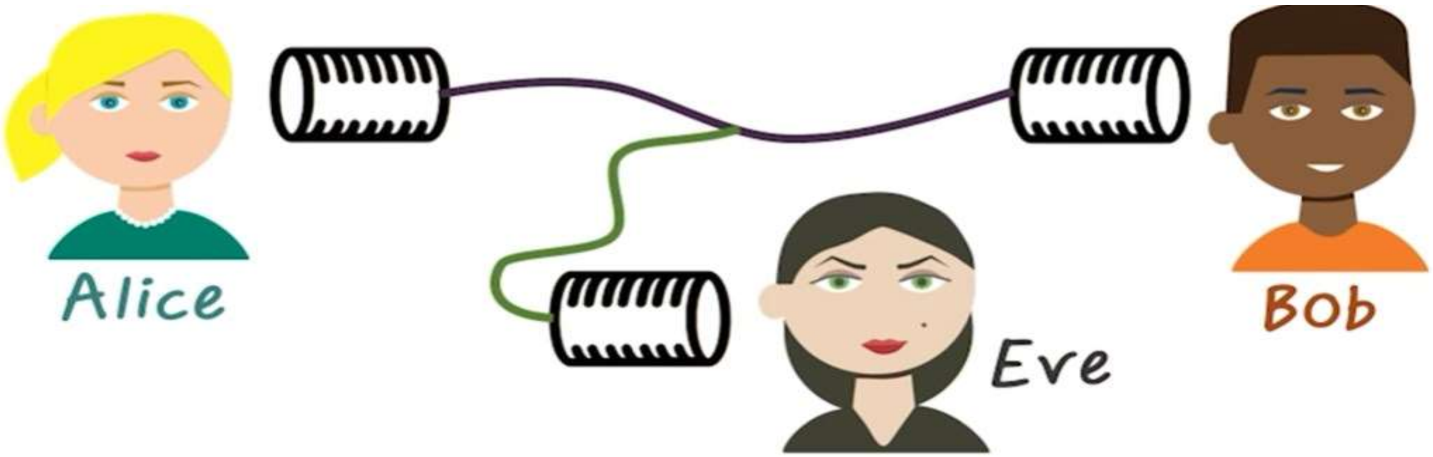
Phishing

Some Classes of Attacks

- Back Doors
  - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- Password Crack
  - Attempting to reverse calculate a password
  - Brute Force
    - The application of computing and network resources to try every possible combination of options of a password
  - Dictionary
    - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

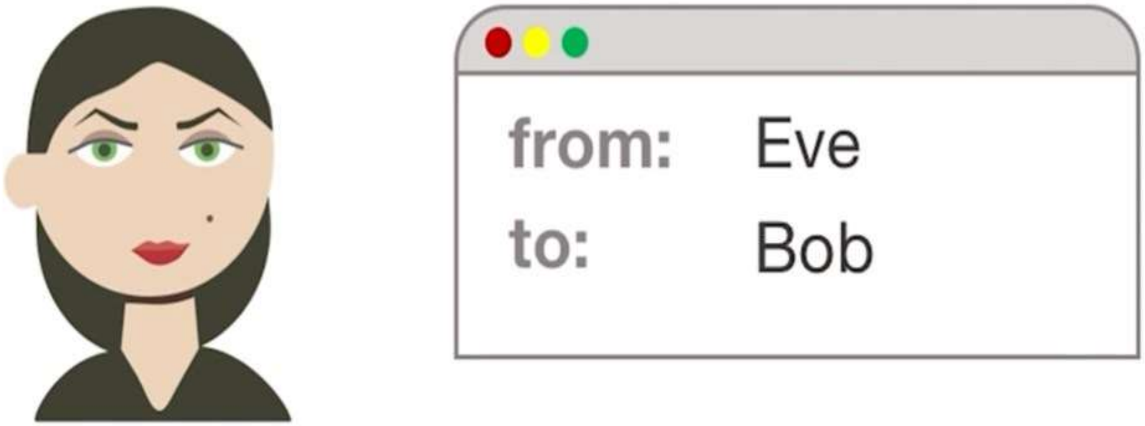
Some Classes of attacks

- Packet Sniffing / Eavesdropping
  - passwords and/or sensitive data are read by (unauthorized) third parties



Some Classes of Attacks

- IP Spoofing / Masquerading
  - someone takes the place of a (legitimate) host

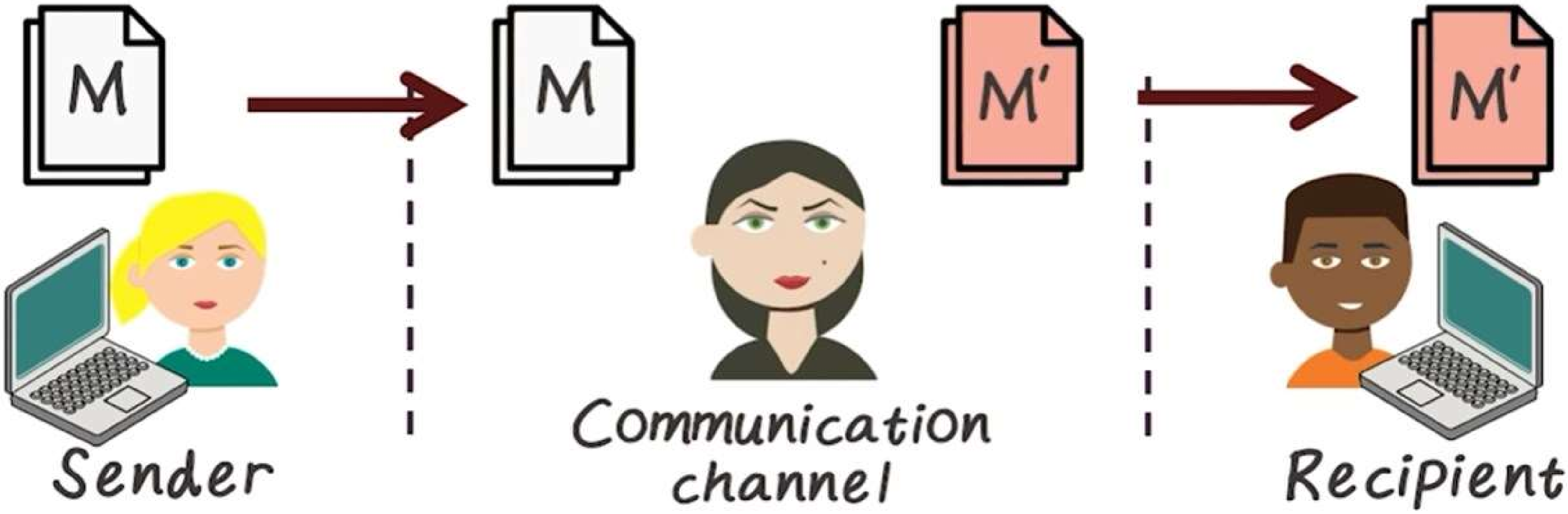


from: Eve

to: Bob

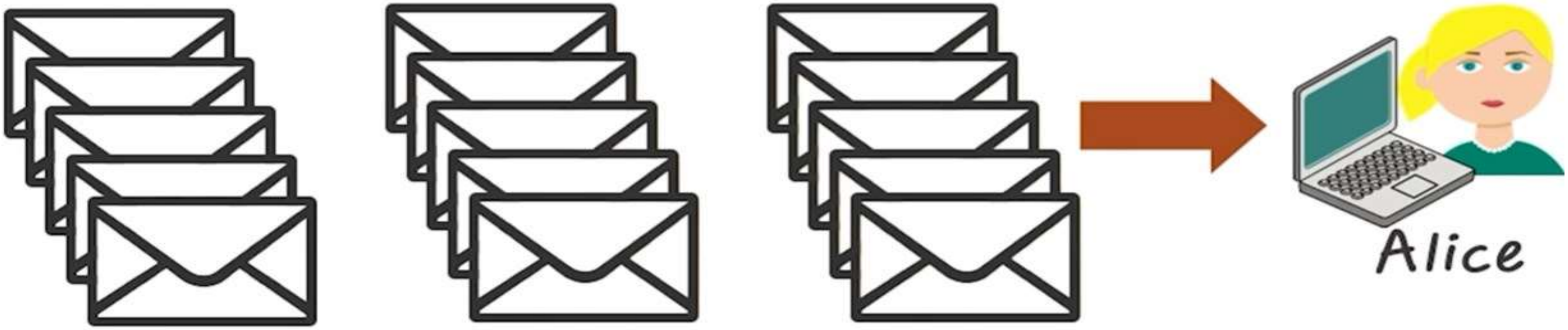
Some Classes of Attacks

- Connection Hijacking /Data Spoofing /Alteration
  - data inserted / modified during their transmission



Some Classes of Attacks

- Denial-of-service (DoS)
  - the functionality of a service is limited or disrupted (e.g. ping bombing)



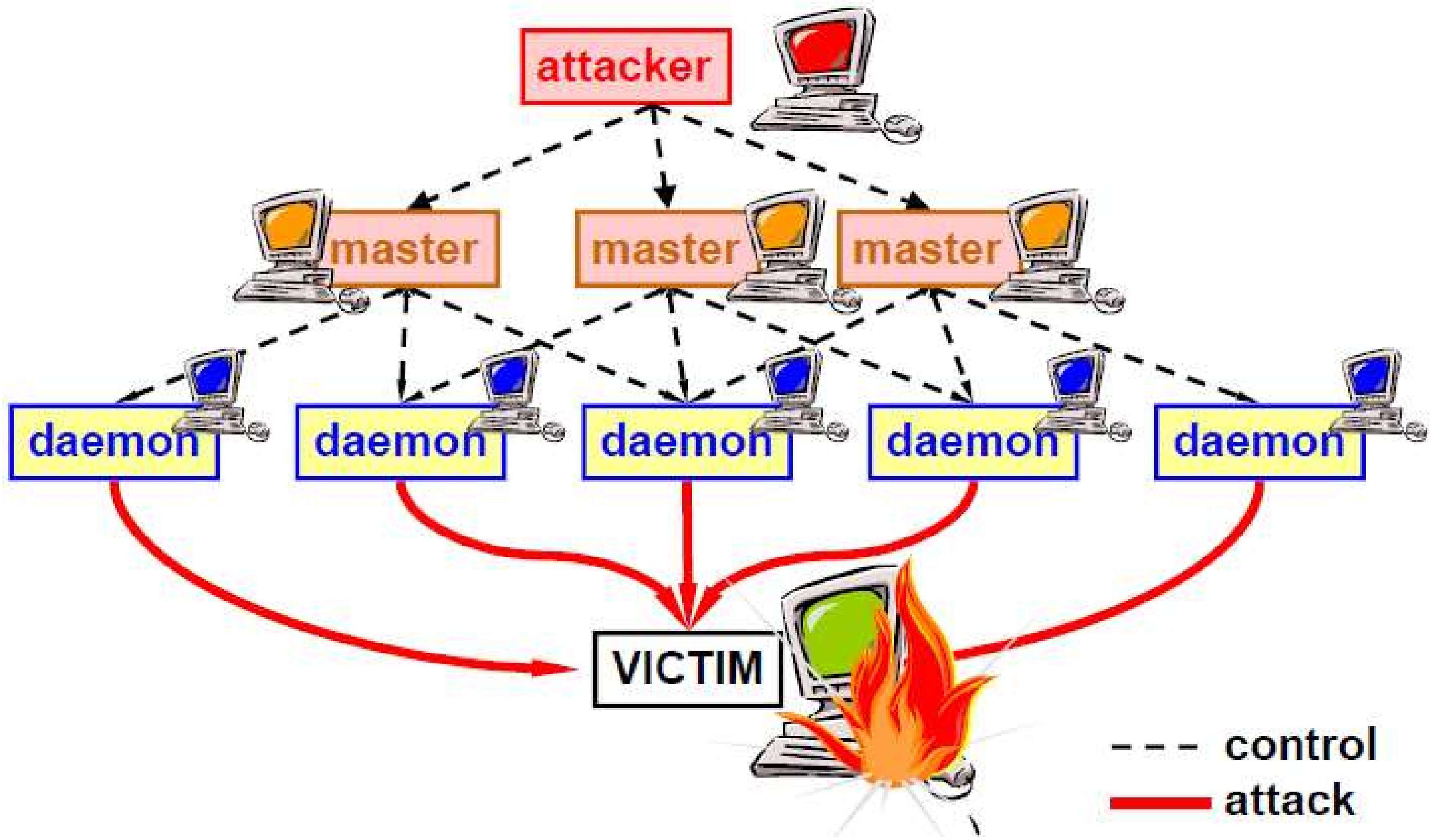
Distributed Denial of Service (DDoS)

- Software for DoS installed on many nodes (named daemon, zombie or malbot) to create a Botnet

- Daemons remotely controlled by a master (often via encrypted channels) and have auto-updating feature

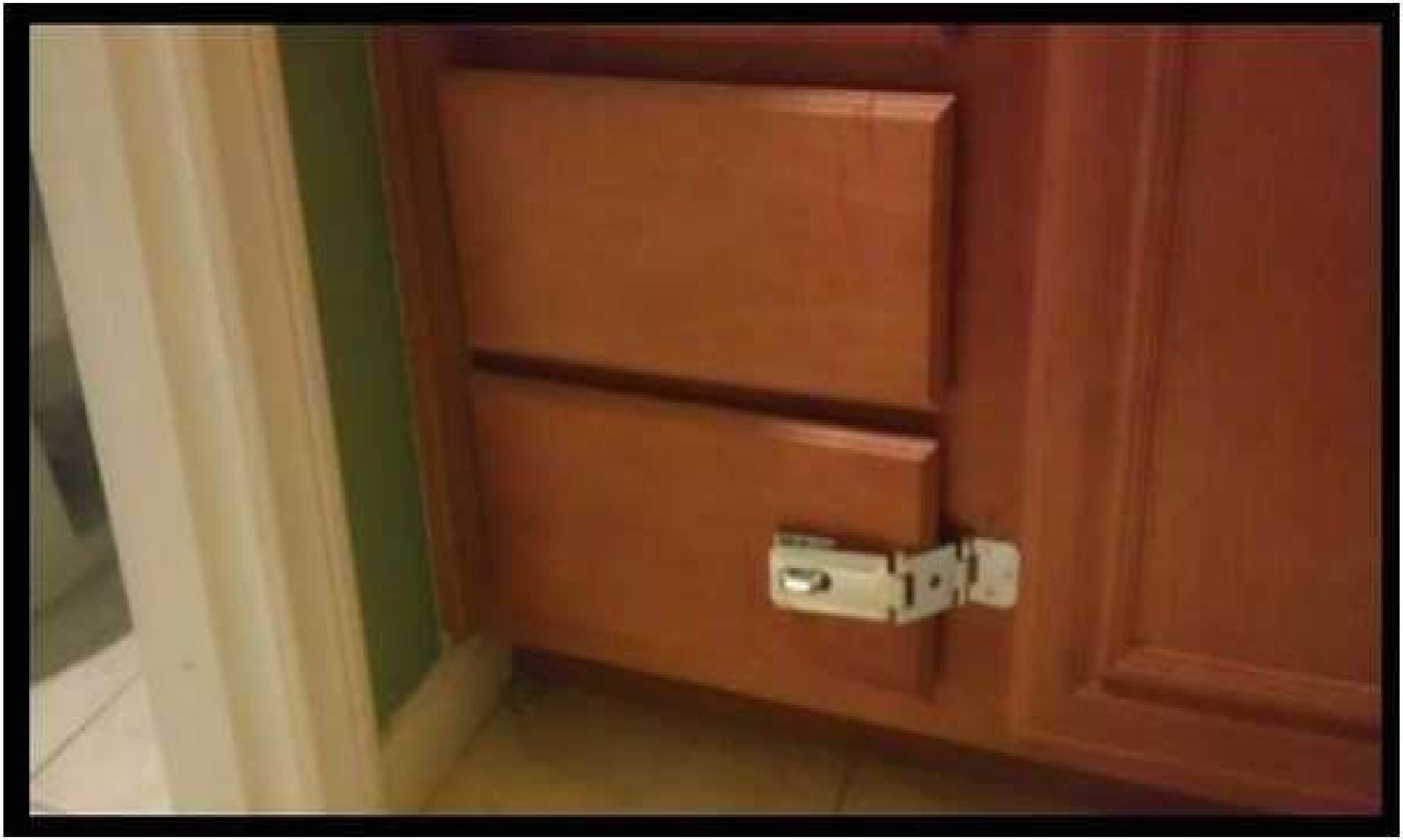
- Effect of the base DoS attack multiplied by the number of daemons

Distributed Denial of Service (DDoS)

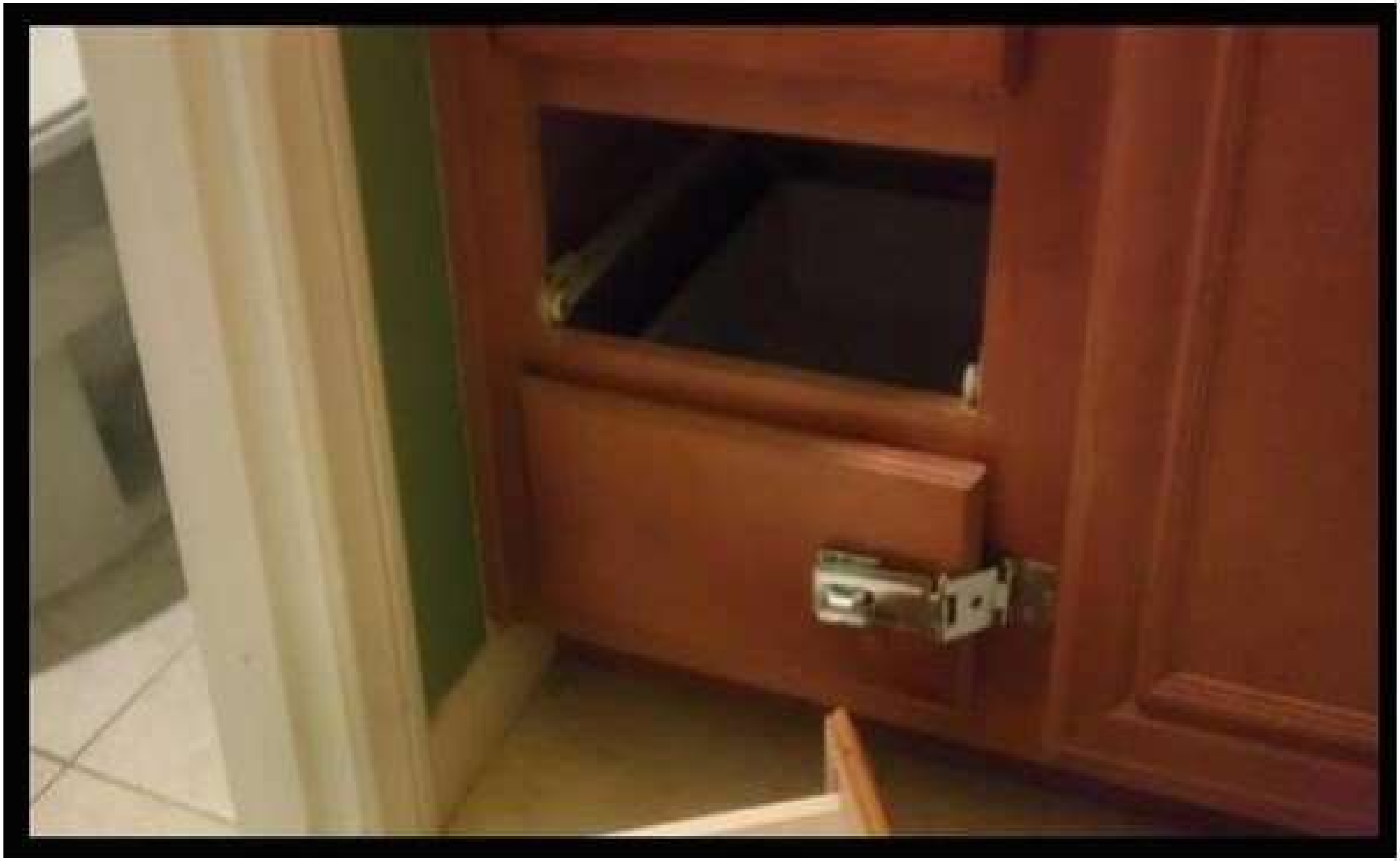


Security Design Principles

What’s wrong with this picture?



What’s wrong with this picture?



Security Design Principles

Principal of ….

- Least Privilege
- Separation of Privilege
- Fail-safe Defaults
- Complete Mediation
- Economy of Mechanism
- Least Common Mechanism
- Psychological Acceptability
- Open Design

1. Least Privilege

- Provide bare minimum privileges to a program or user to function properly
- Temporary elevation should be relinquished immediately
- Granularity of privileges

Advantage

- Abuse of privileges is restricted
- Damage caused by the compromised user or application is reduced

Least Privilege

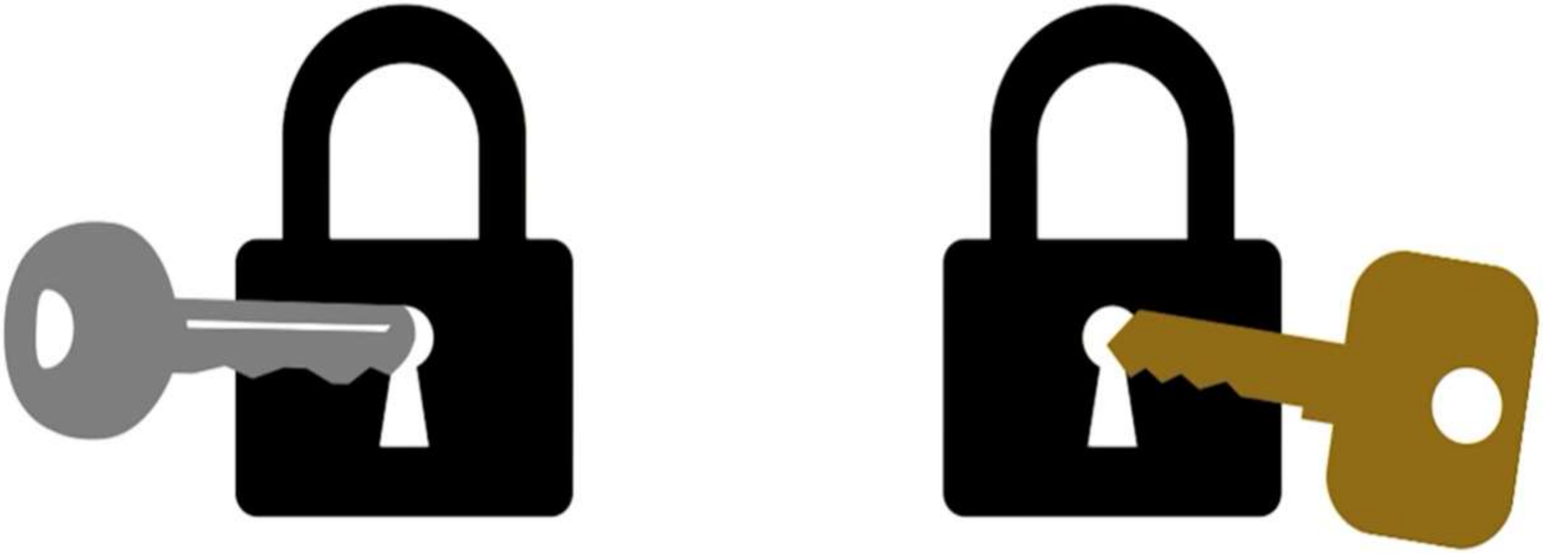
2. Separation of Privilege

- Access should not be granted based on single condition
- Multiple conditions should be required to achieve access to restricted resources

Examples:

- Two persons to sign checks
- Password login + OTC to perform financial transactions

Separation of Privilege



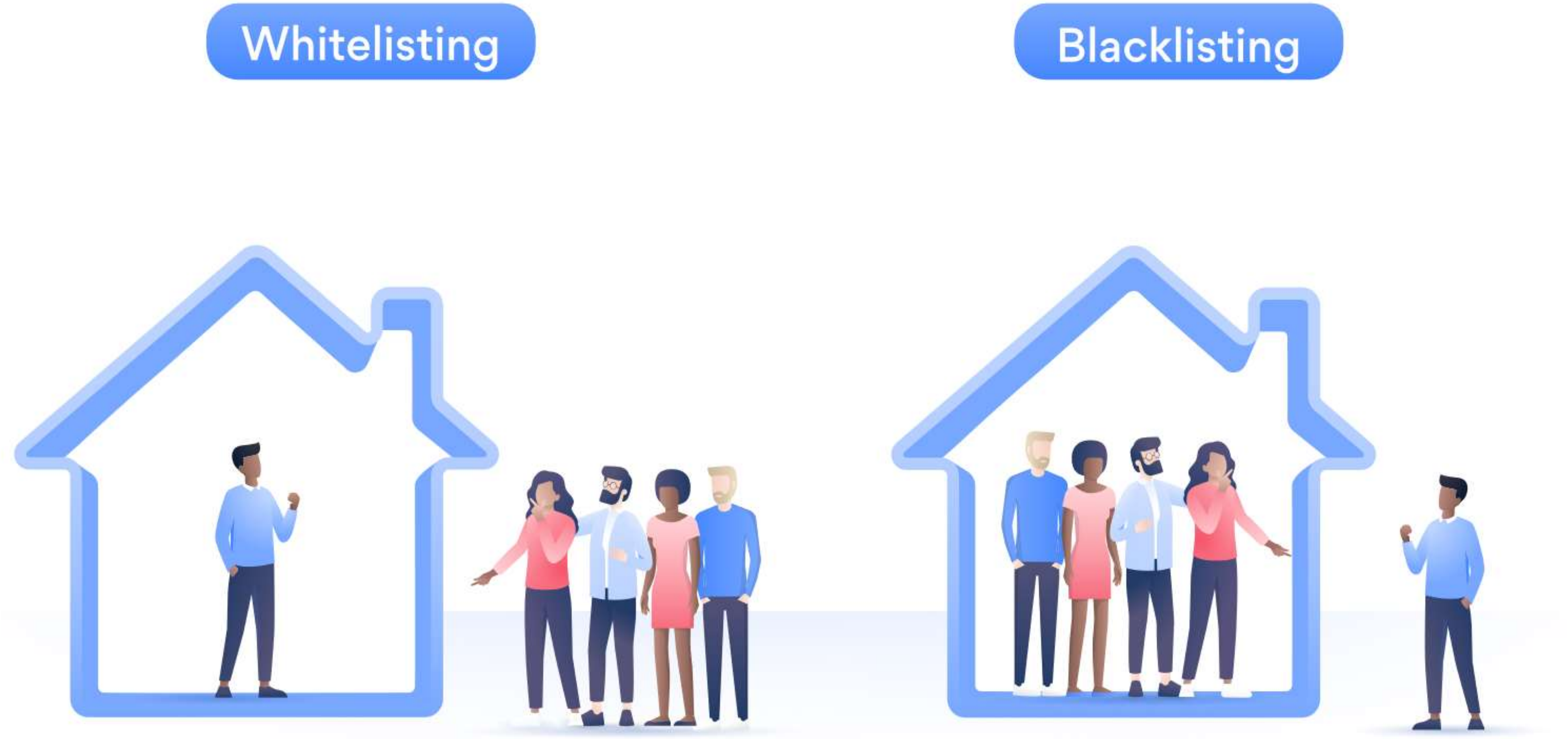
3. Fail-safe Defaults

- The default configuration of a system should have a conservative approach…
  - Default access to an object is none
  - Explicit access to an object should be given

Examples

- Access Control Lists
- Firewall rules

Fail-safe Defaults



4. Complete Mediation

- Instead of one time check, every access to a resource must be checked for compliance with a protection scheme
- restricts the caching of information
- Security vs performance issue

- Whenever a subject attempts to read an object, the operating system should mediate the action. First, it determines if the subject can read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should again check that the subject can still read the object. Most systems would not make the second check. They would cache the results of the first check, and base the second access upon the cached results.
  - DNS cache poisoning

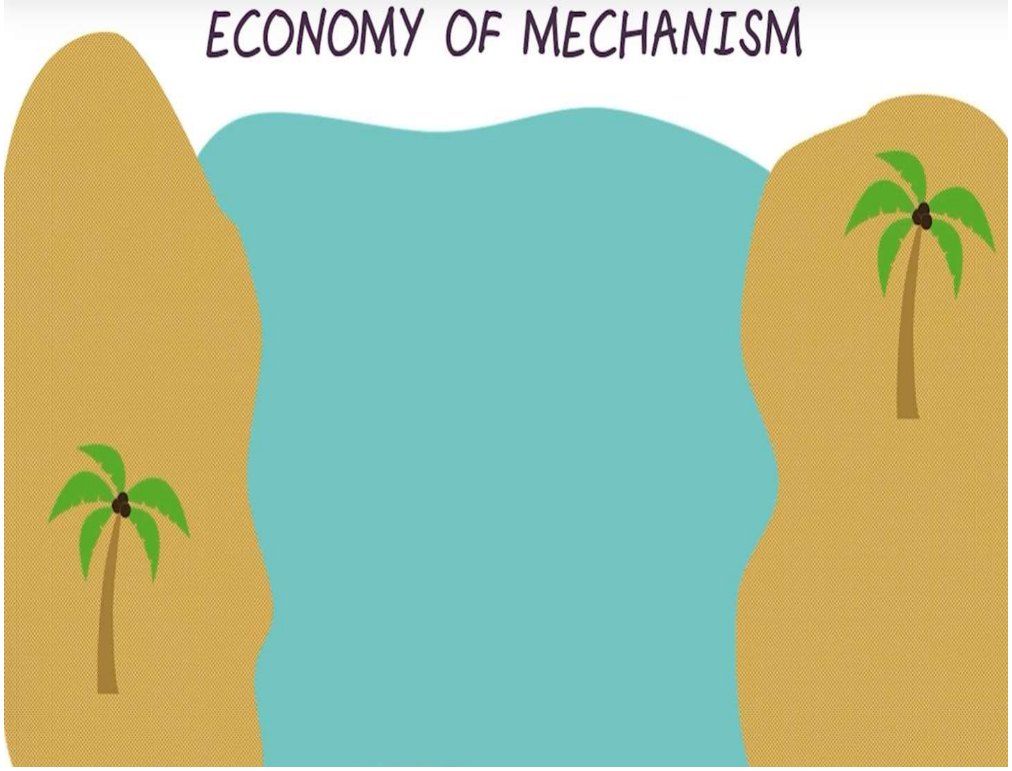
Complete Mediation

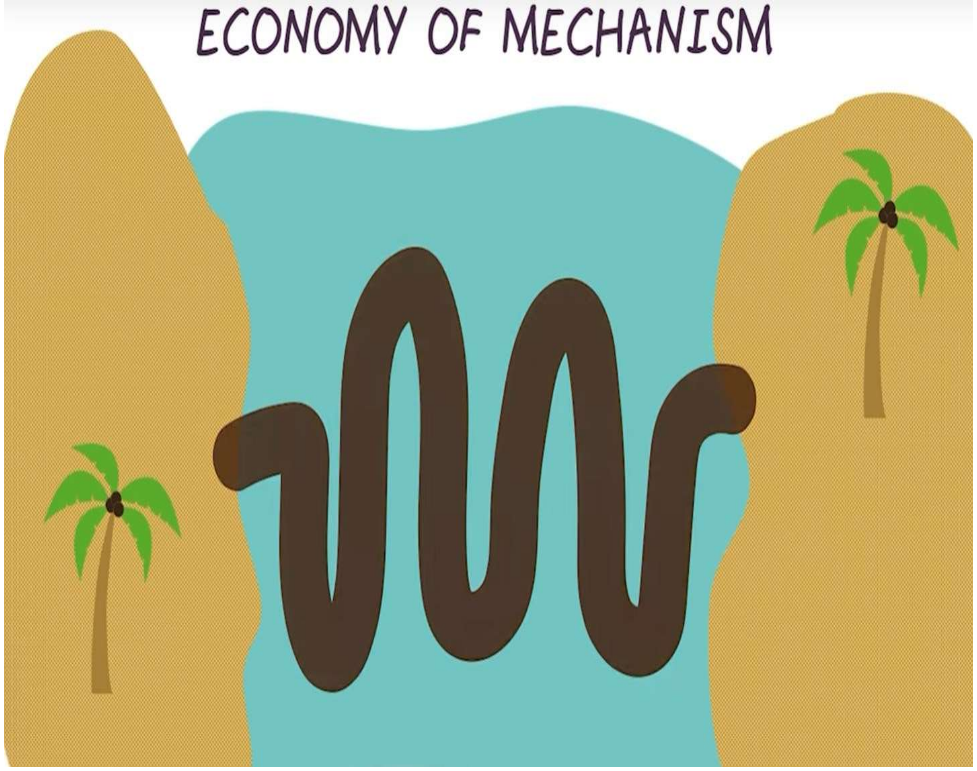
5. Economy of Mechanism

- Simplicity in design and implementation of security measures
  - Complex design provides more opportunities for adversary

- A simple secure framework provides…
  - Fewer errors
  - Development, testing and verification of security measures is easy
  - Less assumptions

Economy of Mechanism

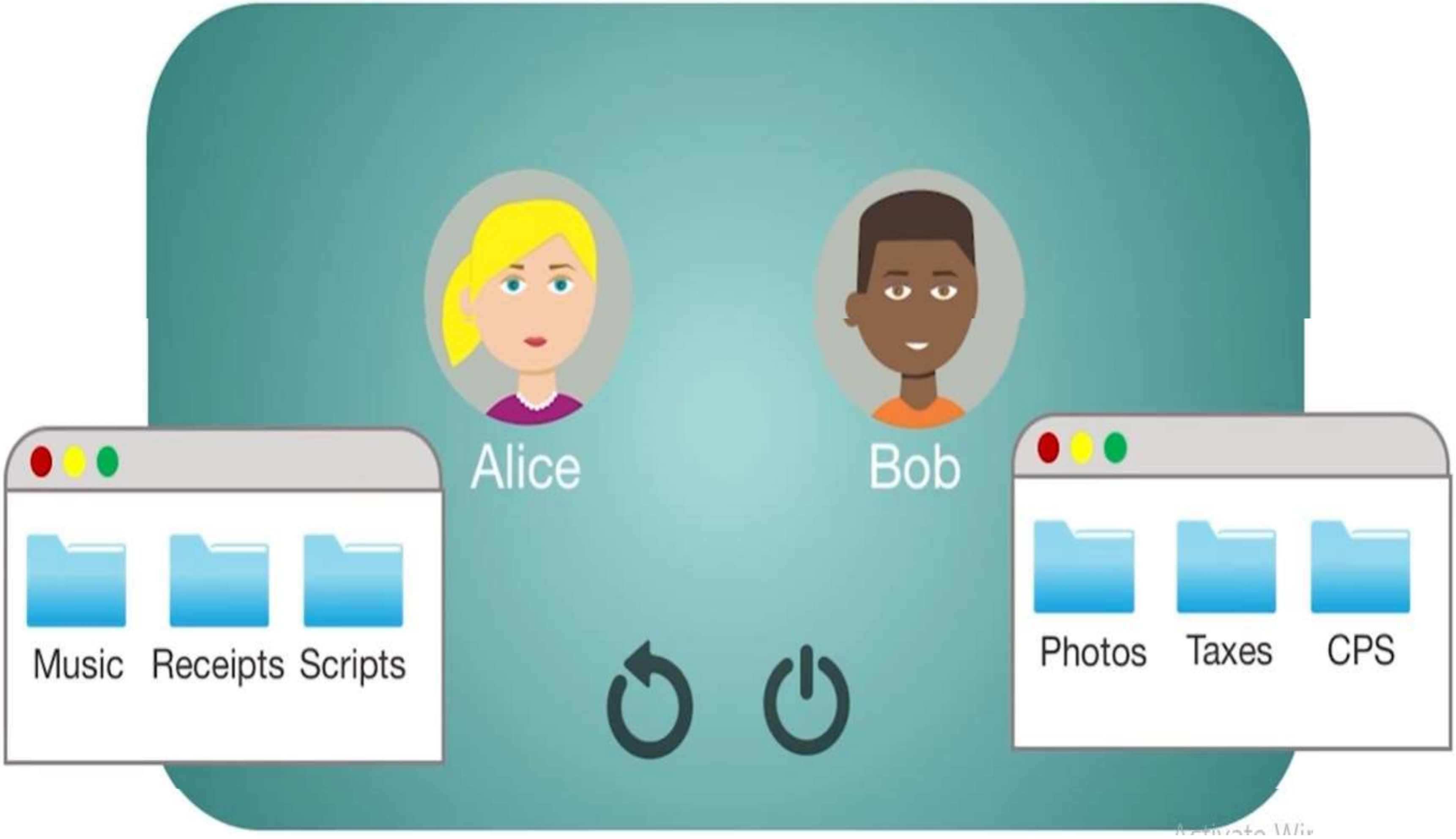




6. Least Common Mechanism

- In shared systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized
- Separate channel for users
- Separation of network resources

Least Common Mechanism



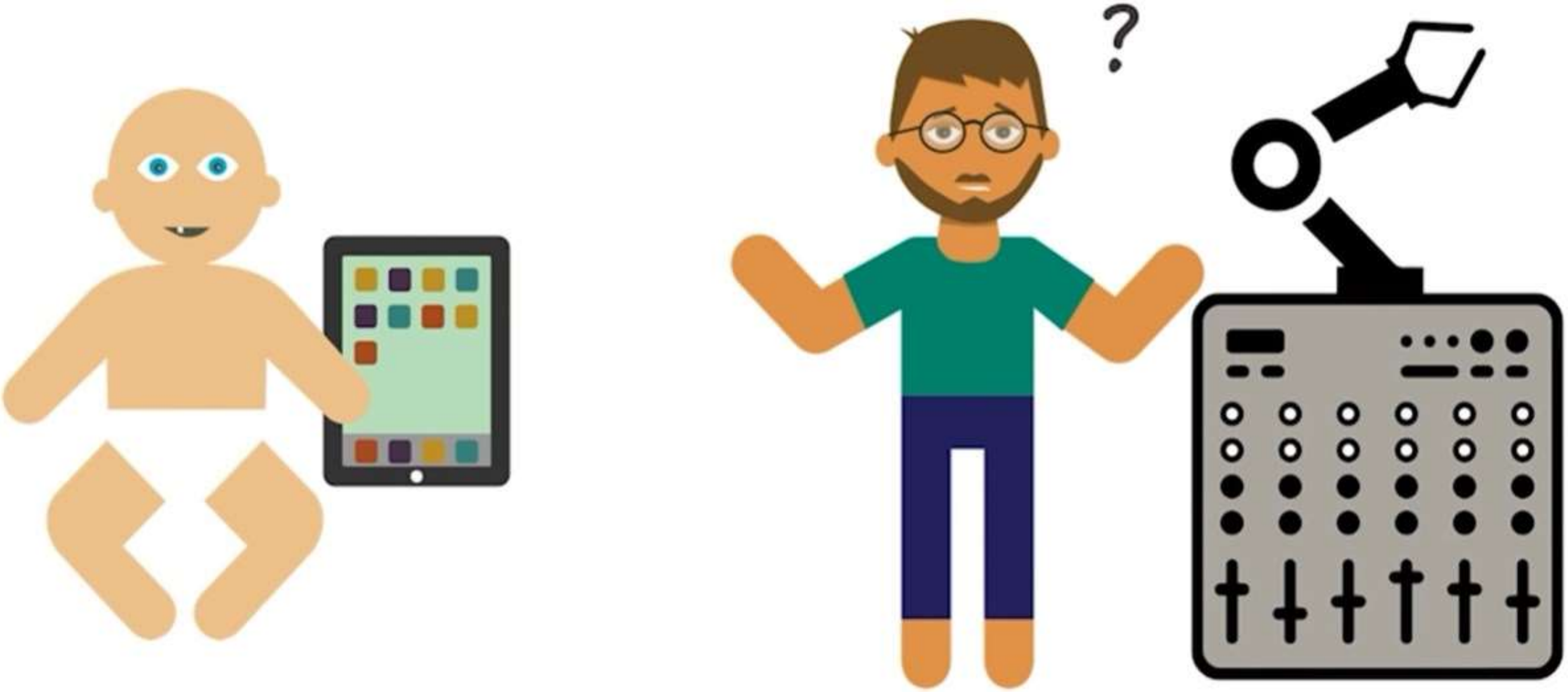
7. Psychological Acceptability

- Security mechanism should not make the resources difficult to access

- User interface should be well designed and intuitive

- Security related setting should consider the expectation of ordinary users

Psychological Acceptability



8. Open Design