DATA SECURITY

Mrs. S. Priyanka
Lecturer (Prob.) in Computer Science
Department of Computer Science
FAS/EUSL

Chapter - 1

1. Introduction To Computer Security

Outline Syllabus

- **Basic concepts in computer security**
- **Cryptography**
- **Program security** – Flaws and Defenses
- **Security** in conventional **operating systems**
- **Database management systems security**
- **Network security**

The term **security** is used in a variety of contexts.

- Personal security
- Corporate security
- Personnel security
- Energy security
- Homeland security
- Operational security
- Communications security
- Network security
- System security

Security

In the most general terms, security seems to mean something like "**protection of assets against threats**."

Computer Security

- Computer security is the protection of the items you value, called the **assets of a computer** or computer system.
- The goal of computer security is **protecting valuable assets**.

Why Information/Computer Security is Important?

- **You encounter computers daily in countless situations**,
- move money, control airplanes, monitor health, lock doors, play music, heat buildings, regulate hearts, tally votes, direct communications, regulate traffic, and do hundreds of other things that affect lives, health, finances, and well-being.
- Most of the time these computers work just as they should.
- But occasionally they do something horribly wrong, because of either a **benign failure or a malicious attack**.

On 11 February 2013, residents of Great Falls, Montana received the following warning on their televisions.

FIGURE 1-1 Emergency Broadcast Warning

[Beep Beep Beep: *the sound pattern of the U.S. government Emergency Alert System. The following text then scrolled across the screen:*]

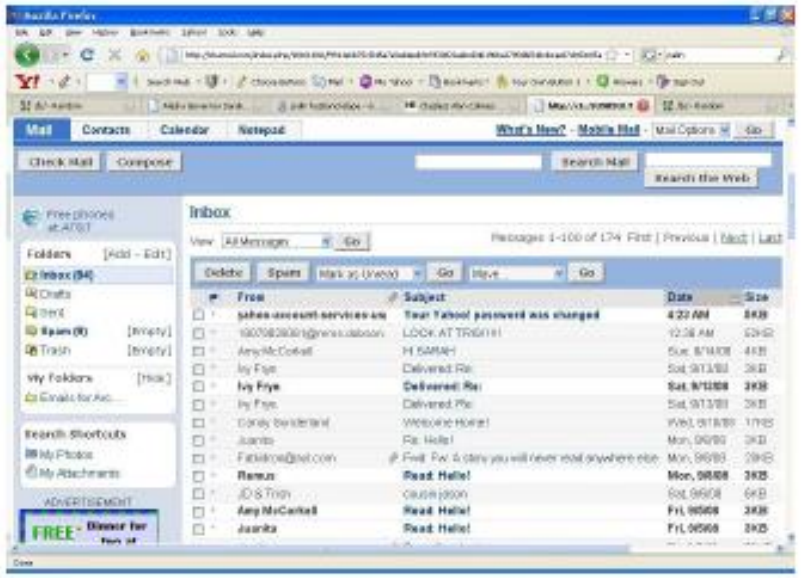
Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living. Follow the messages on screen that will be updated as information becomes available.

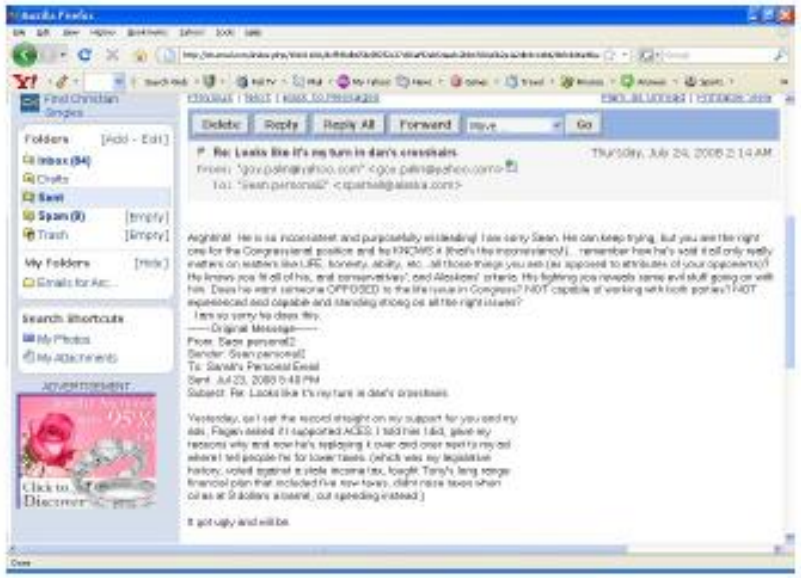
Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous. This warning applies to all areas receiving this broadcast.

[Beep Beep Beep]

The perpetrator of this hoax was never caught, nor has it become clear exactly how it was done.

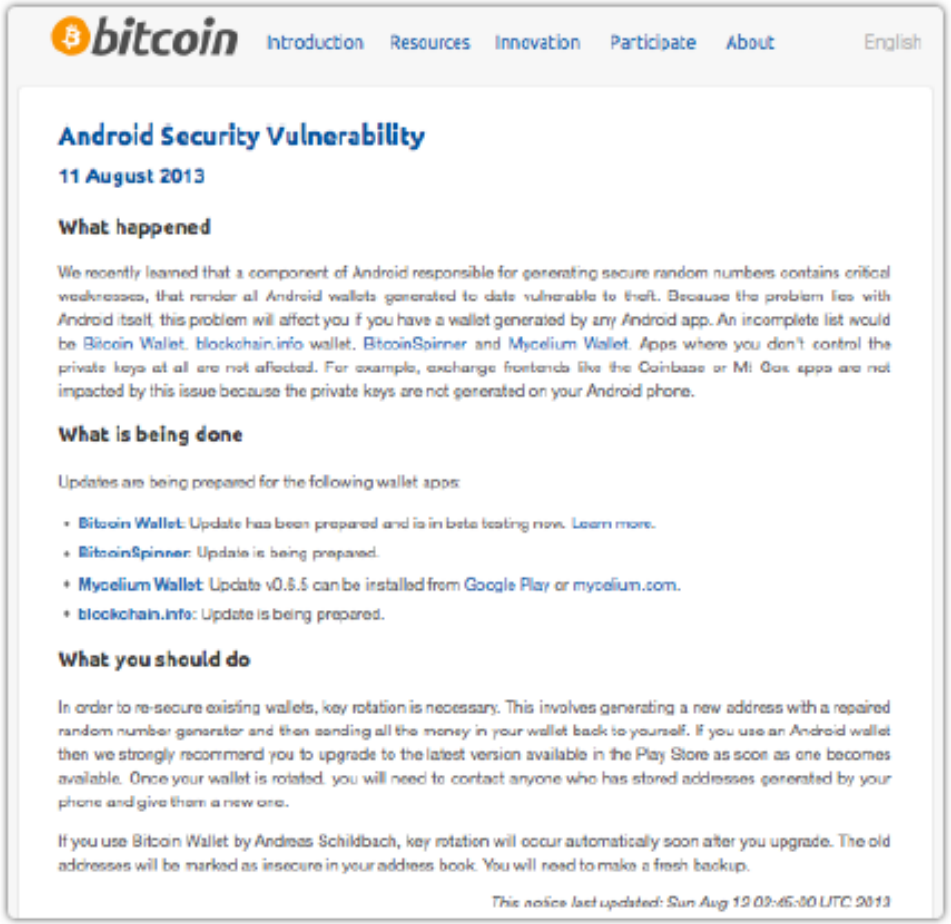
Sarah Palin email hack





https://www.wired.com/2008/09/palin-e-mail-ha/

Android random number flaw results in Bitcoin thefts



bitcoin Introduction Resources Innovation Participate About English

Android Security Vulnerability

11 August 2013

What happened

We recently learned that a component of Android responsible for generating secure random numbers contains critical weaknesses, that render all Android wallets generated to date vulnerable to theft. Because the problem lies with Android itself, this problem will affect you if you have a wallet generated by any Android app. An incomplete list would be Bitcoin Wallet, blockchain.info wallet, BitcoinSpinner and Mycelium Wallet. Apps where you don't control the private keys at all are not affected. For example, exchange frontends like the Coinbase or MtGox apps are not impacted by this issue because the private keys are not generated on your Android phone.

What is being done

Updates are being prepared for the following wallet apps:

- **Bitcoin Wallet**: Update has been prepared and is in beta testing now. Learn more.
- **BitcoinSpinner**: Update is being prepared.
- **Mycelium Wallet**: Update v0.6.5 can be installed from Google Play or mycelium.com.
- **blockchain.info**: Update is being prepared.

What you should do

In order to re-secure existing wallets, key rotation is necessary. This involves generating a new address with a repaired random number generator and then sending all the money in your wallet back to yourself. If you use an Android wallet then we strongly recommend you to upgrade to the latest version available in the Play Store as soon as one becomes available. Once your wallet is rotated, you will need to contact anyone who has stored addresses generated by your phone and give them a new one.

If you use Bitcoin Wallet by Andreas Schildbach, key rotation will occur automatically soon after you upgrade. The old addresses will be marked as insecure in your address book. You will need to make a fresh backup.

This notice last updated: Sun Aug 11 03:45:00 UTC 2013

https://nakedsecurity.sophos.com/2013/08/12/android-random-number-flaw-implicated-in-bitcoin-thefts

The TLS heartbleed bug

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

What leaks in practice?

We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials we were able steal from ourselves the secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication.

http://xkcd.com/1354

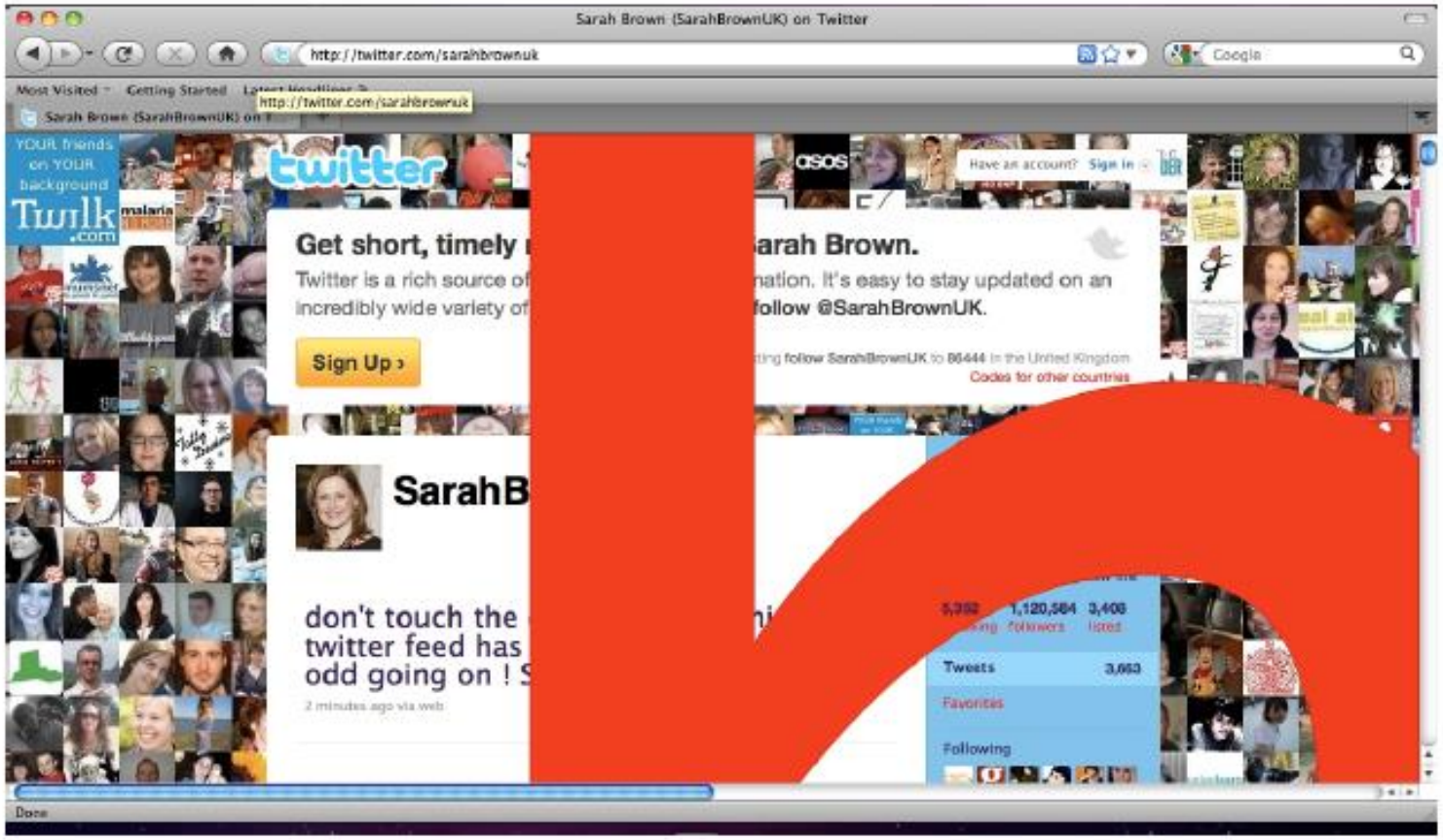
http://xkcd.com/1354heartbleed.com

LinkedIn password leak

http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm

http://techcrunch.com/2016/05/18/117-million-linkedin-emails-and-passwords-from-a-2012-hack-just-got-posted-online/

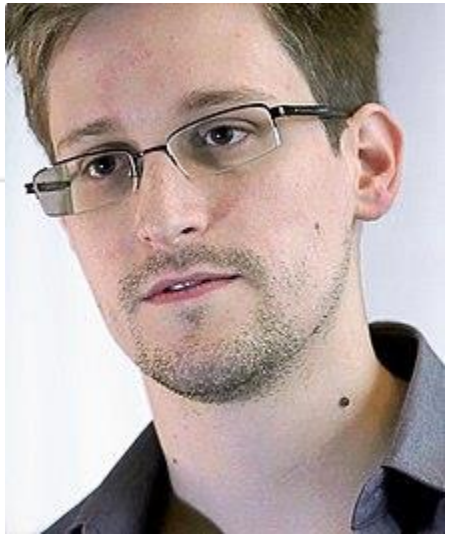
Twitter worm



http://www.pandasecurity.com/mediacenter/social-media/onmouseover-xss-vulnerability-on-twitter/

Edward Snowden: Leaks that exposed US spy programme

17 January 2014 | US & Canada



Edward Snowden, a former contractor for the CIA, left the US in late May after leaking to the media details of extensive internet and phone surveillance by American intelligence. Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges over his actions.

As the scandal widens, BBC News looks at the leaks that brought US spying activities to light.

US spy agency 'collects phone records'

The scandal broke in early June 2013 when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans.

Question: Why would security be any more difficult than most technological problems?

- Most technology-related efforts are concerned with ensuring that something good happens. Security is all about ensuring that **bad things never happen**.
- If security is all about ensuring that bad things never happen, that means **we have to know what those bad things are.**
- Unlike most technology problems, you have to defeat **one or more** actively malicious adversaries.
- Information management **systems are a complex**, "target-rich" environment comprising: hardware, software, storage media, peripheral devices, data, people.
- **Security is often an afterthought**. No-one builds a digital system for the purpose of being secure. They build digital systems to do something useful.
- The defender has to find and eliminate all exploitable vulnerabilities; the **attacker only needs to find one**!

Today: asset protection is easier

- Computer security is concerned with protecting computer system's information assets, as well as computer systems themselves.

- Assets = items of value

- Today: asset protection is easier; Very sophisticated alarm and camera systems silently protect secure places, genetic material (DNA), fingerprints, retinal patterns, voice, etc.

Assets

- A resource with **economic value** that an individual, corporation or country owns.
- Anything (Property, people, information) has value to the person/organization/country

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets

- To determine what to protect, we must first identify what has value and to whom.

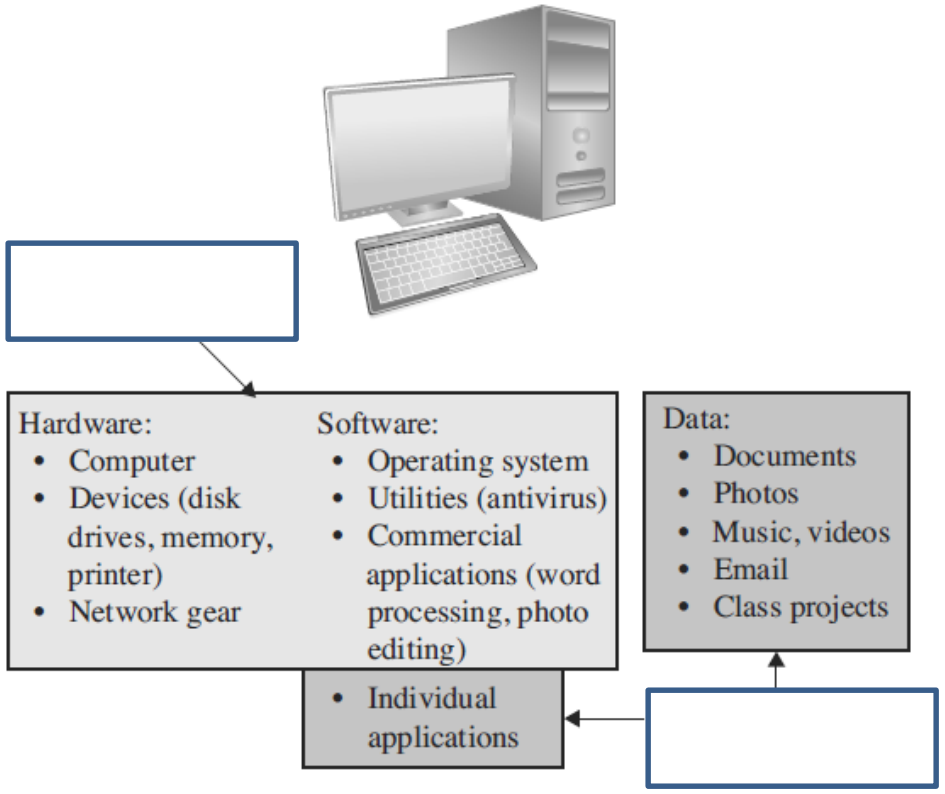


FIGURE 1-3 Values of Assets

The perceived value of an asset depends upon the ease with which the asset can be replaced.

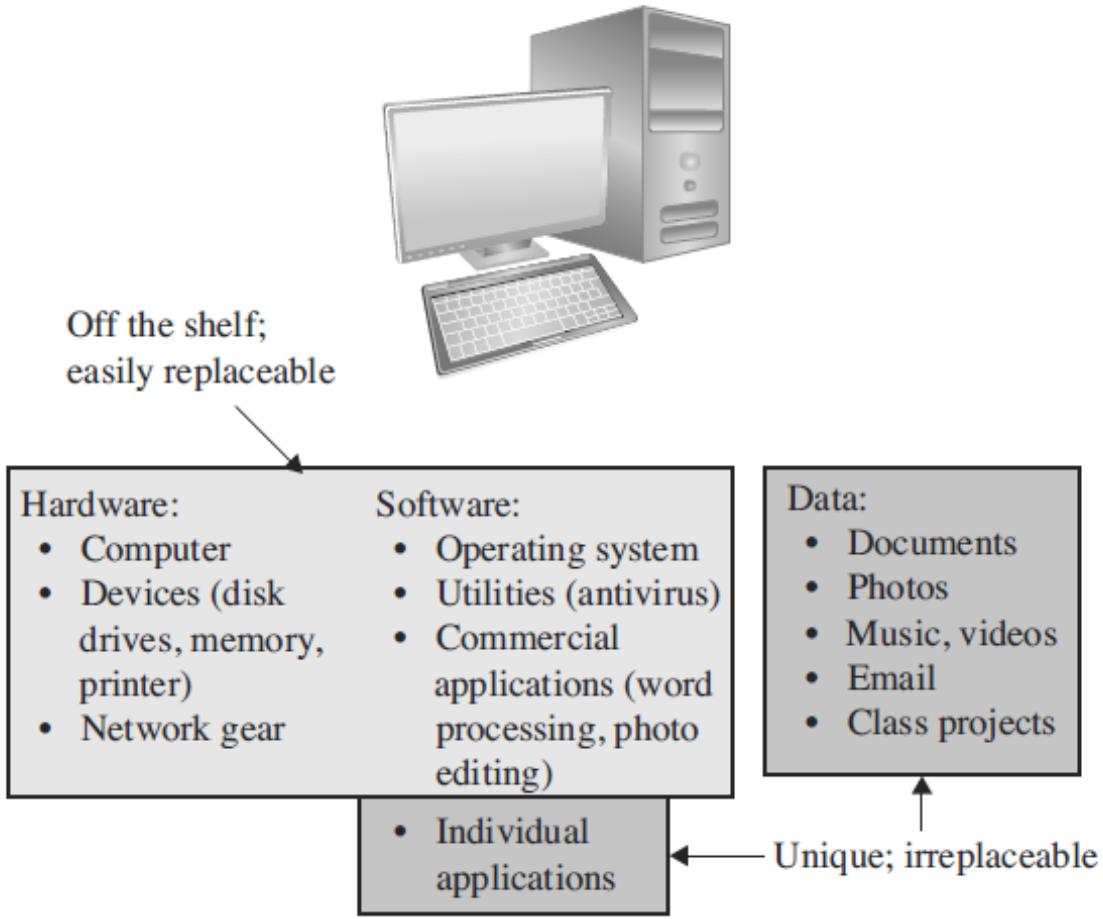


FIGURE 1-3 Values of Assets

Vulnerability

A vulnerability is a weakness of an asset that could be exploited to cause harm.

For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

Threat

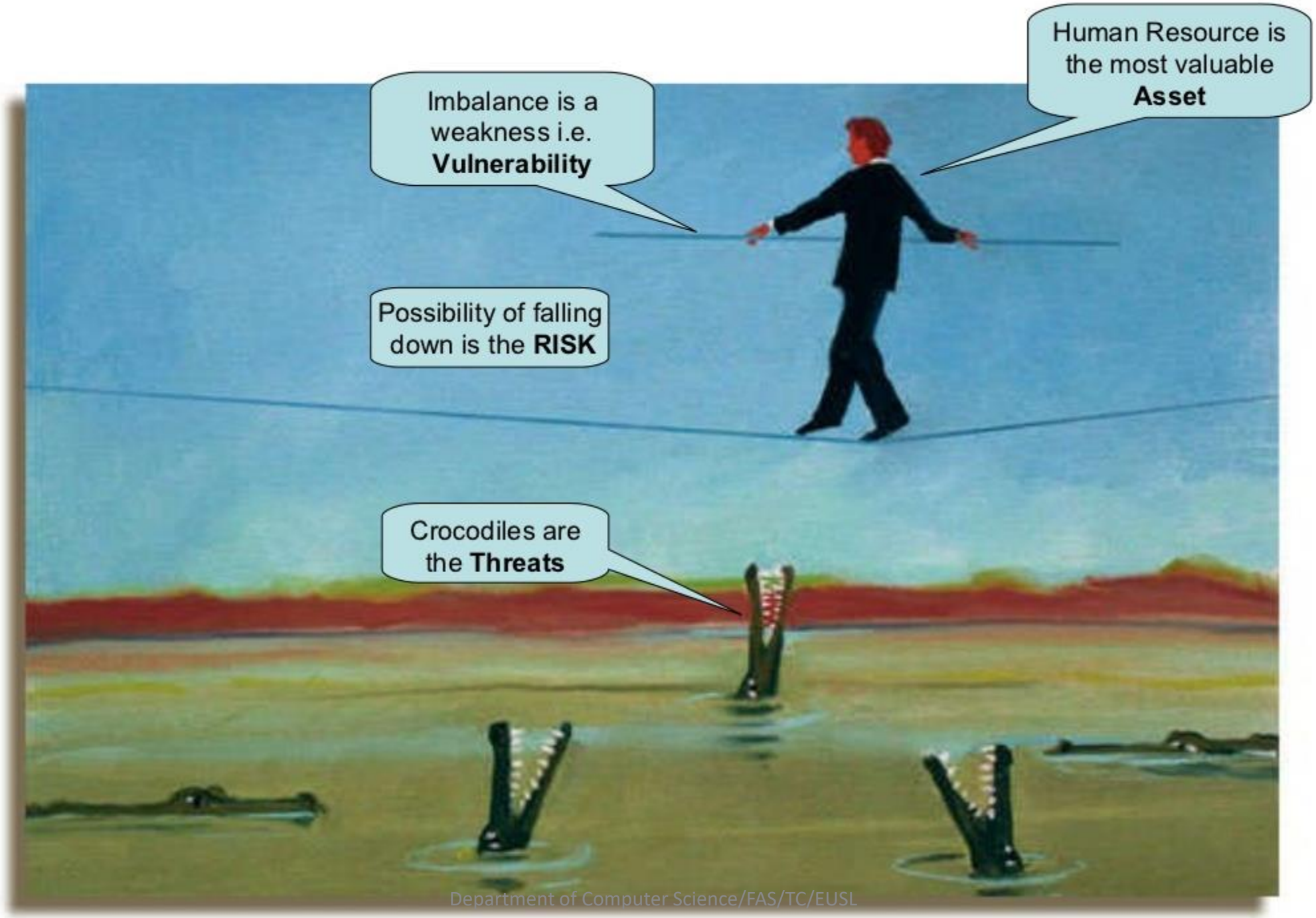
- A threat to a system is a set of circumstances that has potential to cause loss or harm.
- Any possible danger

Risk

- The probability of a threat being materialized by exploiting a vulnerability.
- The likelihood that the event (exploitation of vulnerability) will occur.

Crossing the street is risky

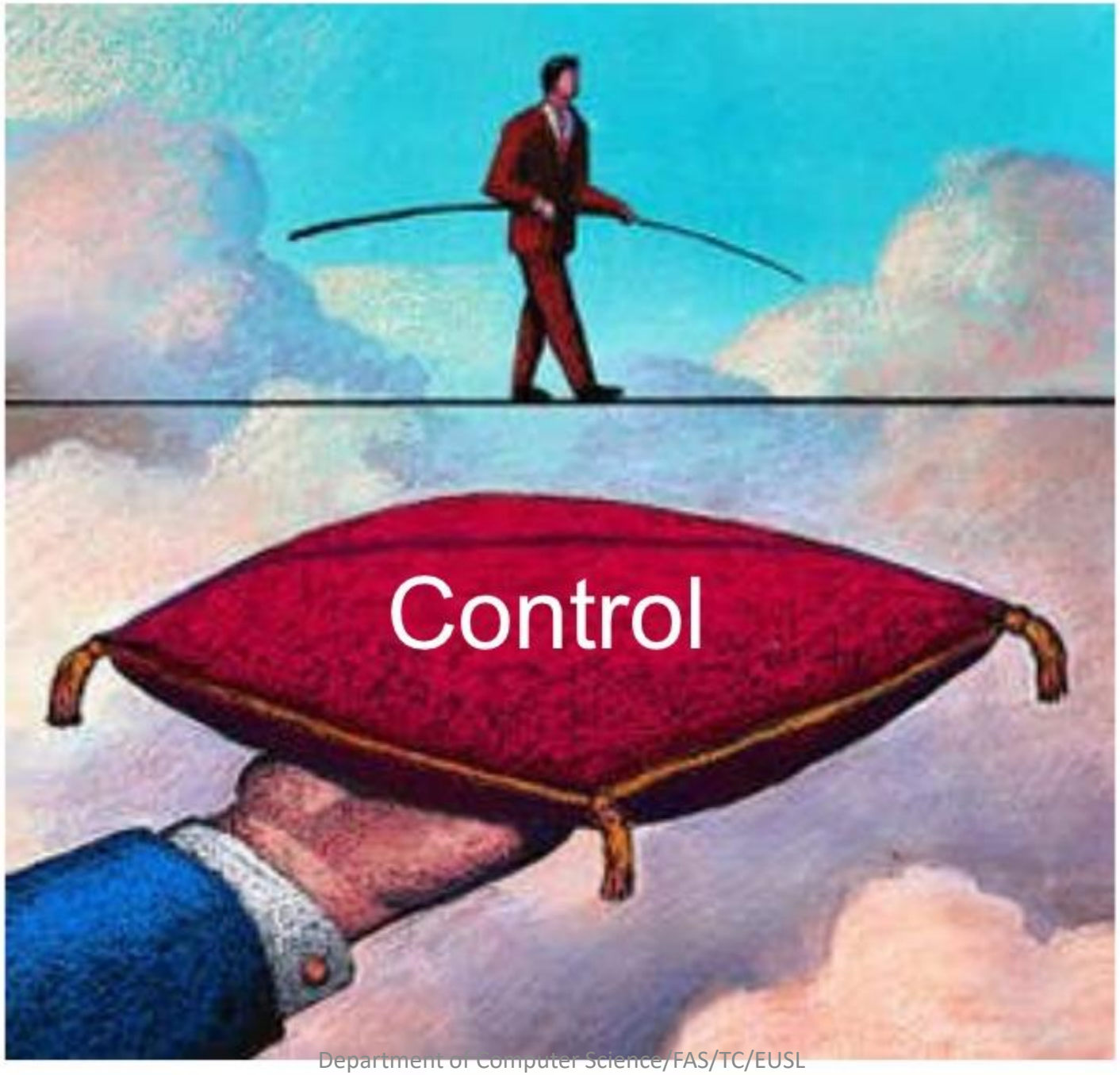
But, you still cross the street!

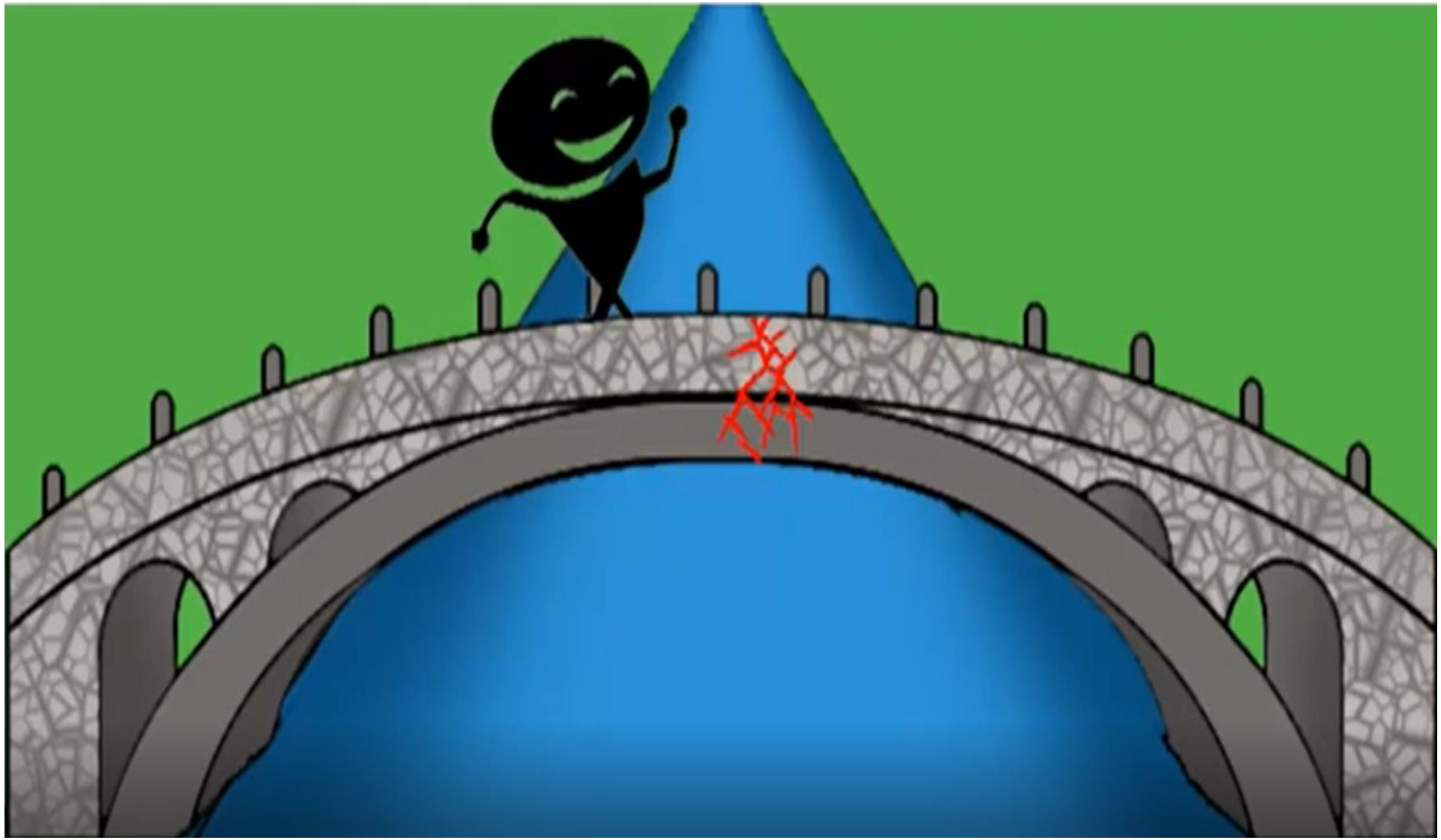

Human Resource is the most valuable **Asset**
Imbalance is a weakness i.e. **Vulnerability**
Possibility of falling down is the **RISK**
Crocodiles are the **Threats**

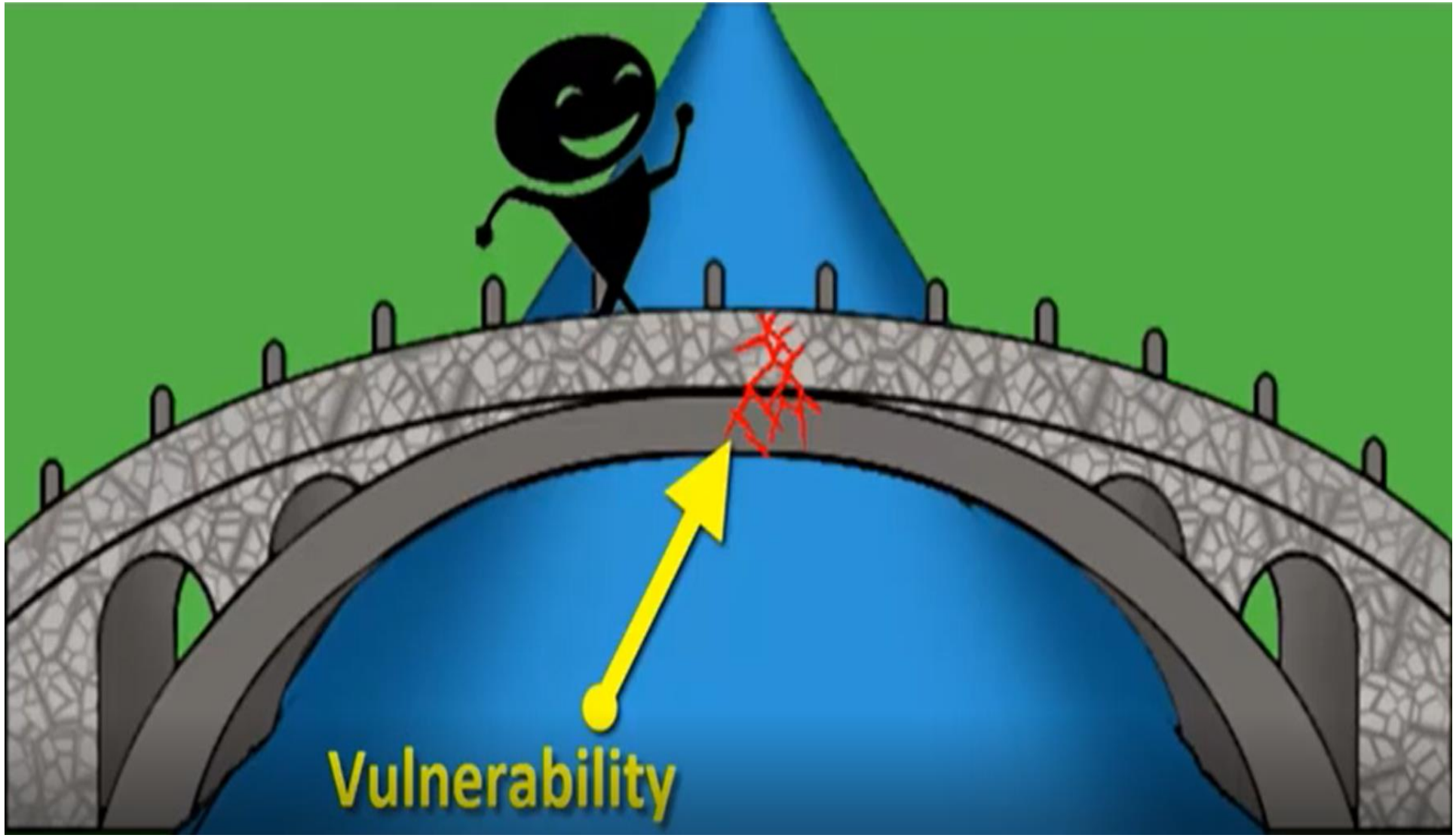
Control

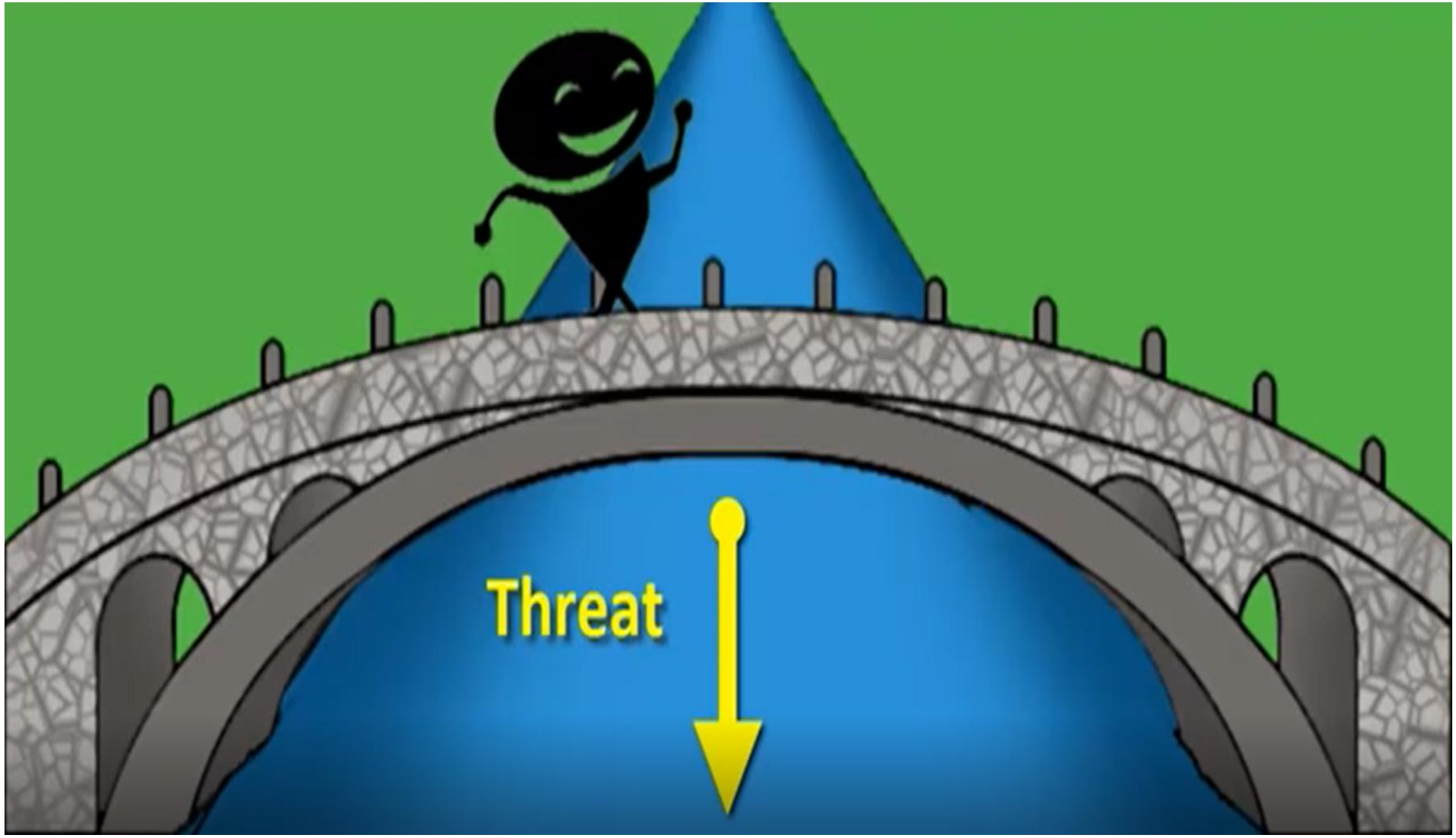
- How do we address these problems? We use a **control or countermeasure as protection.**
- **Controls prevent threats from exercising vulnerabilities.**
- Any procedure/device that is in place to assure security of a system.
- A **control is an action, device, procedure, or technique that removes or reduces a vulnerability.**

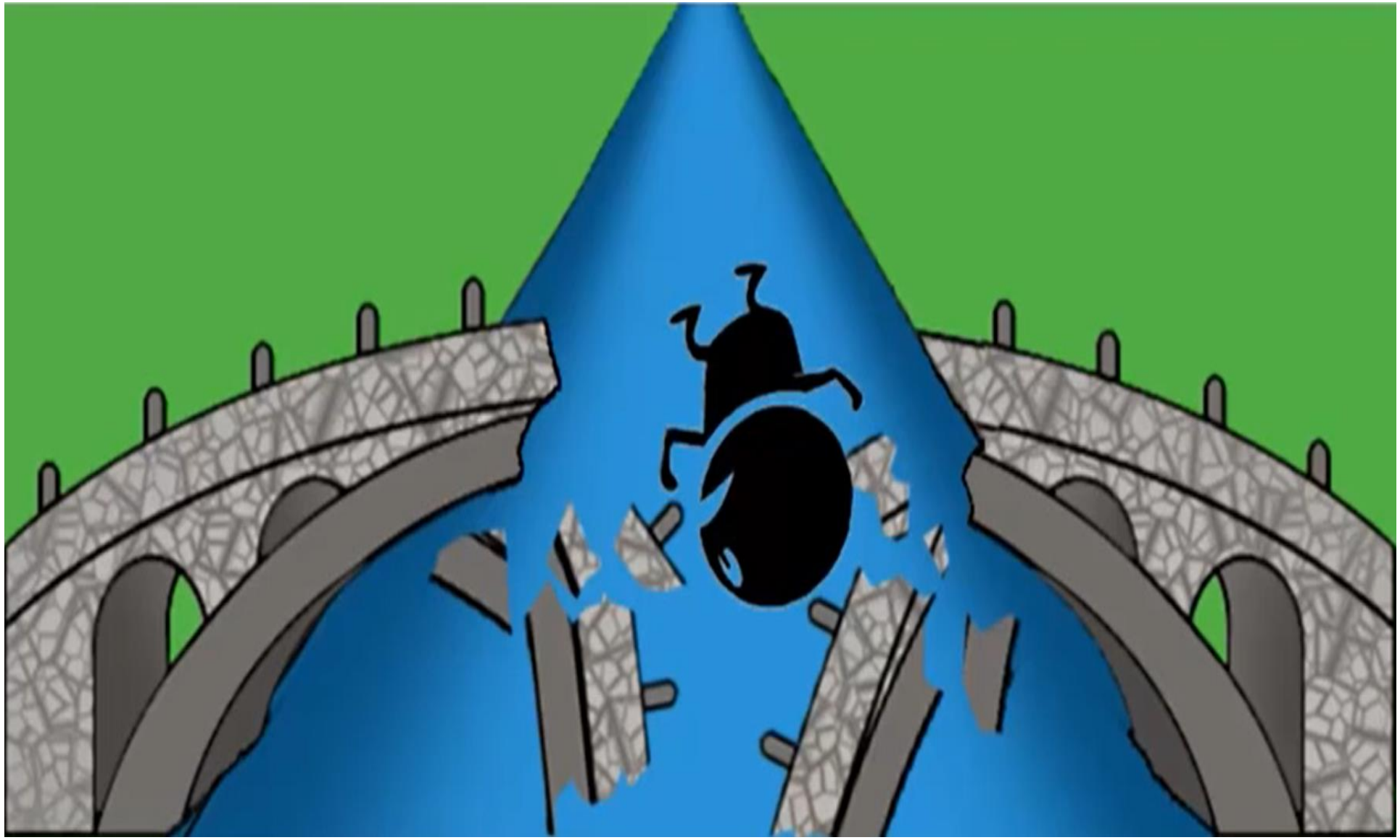
A threat is blocked by control of a vulnerability

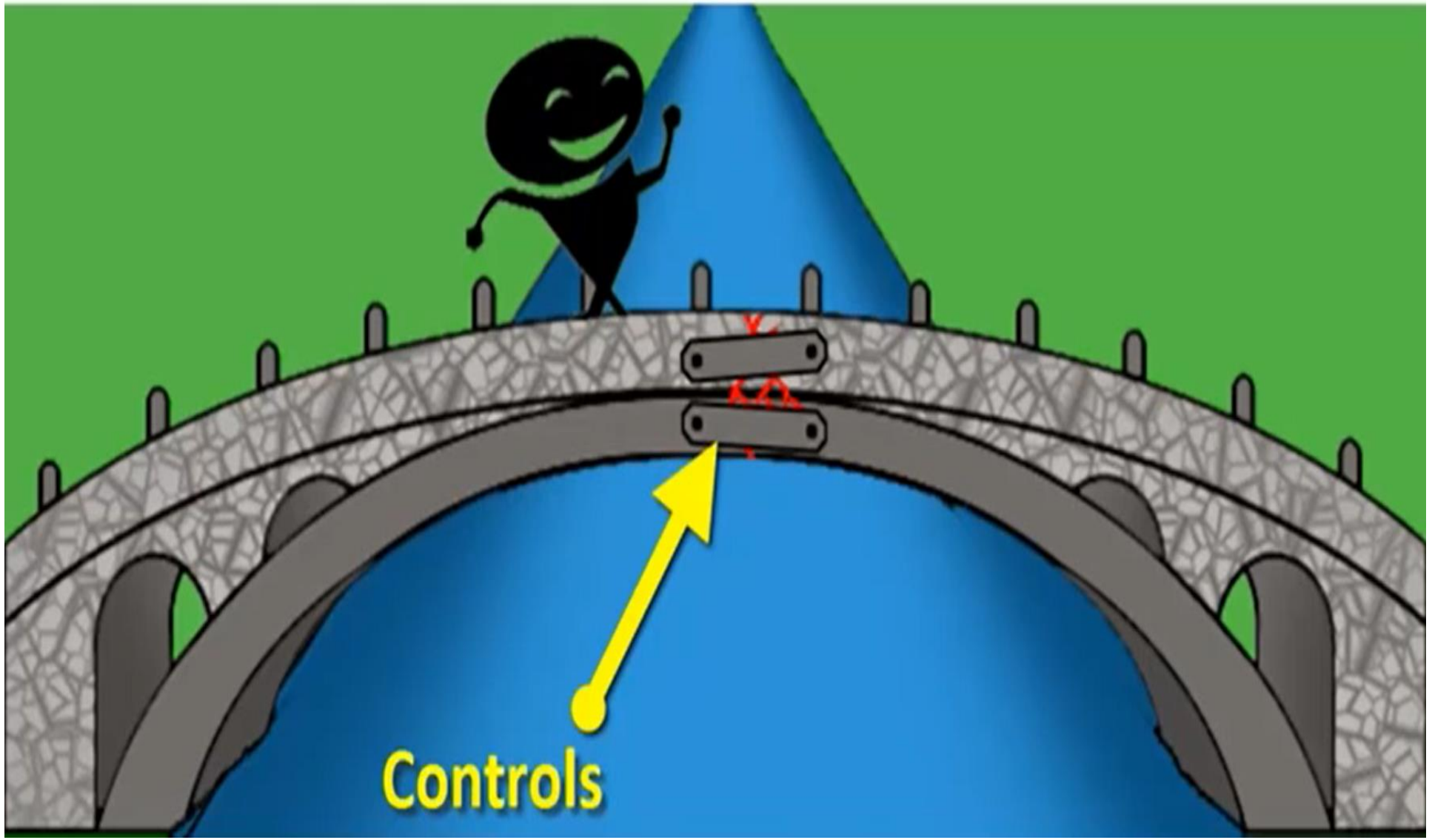

Control

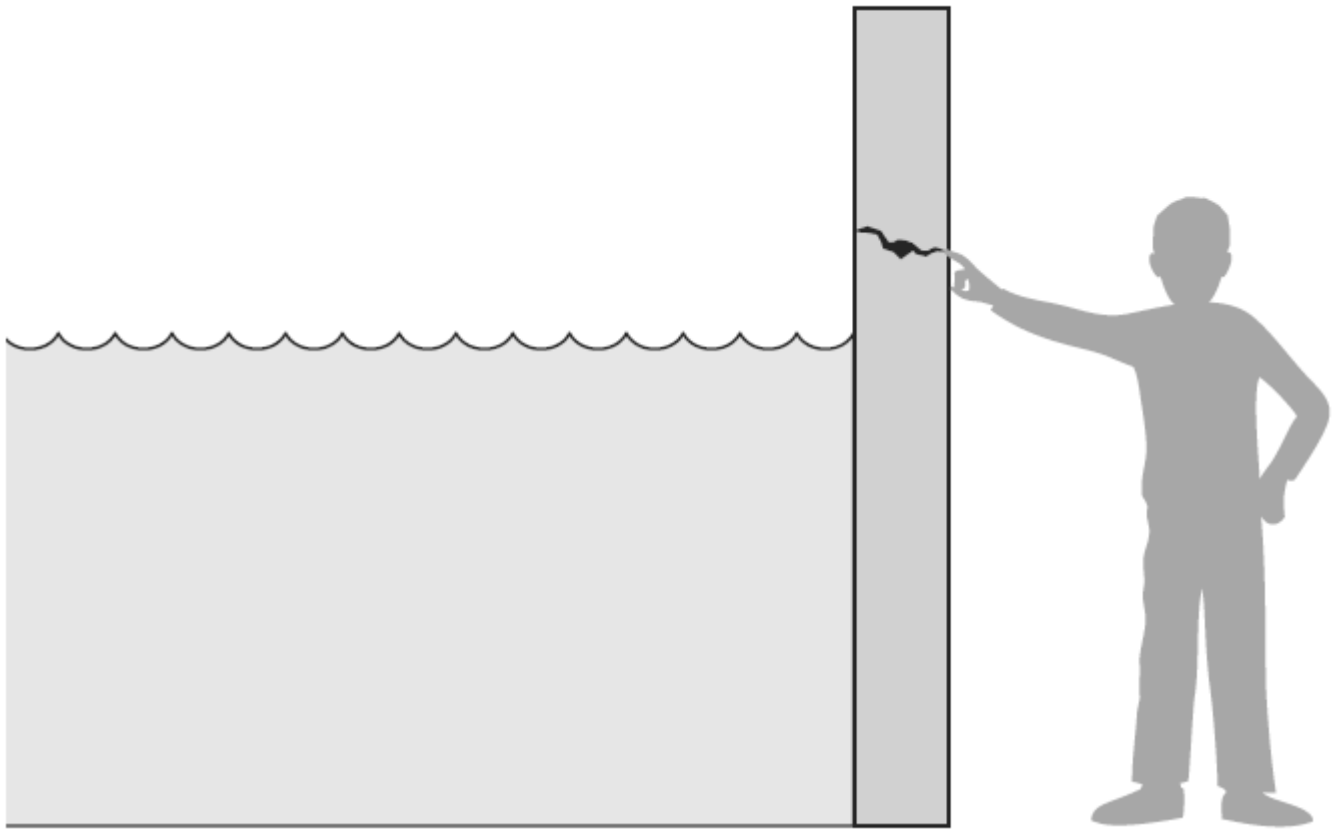



Vulnerability


Threat




Controls



- Here, a wall is holding water back. The **water** to the left of the wall is a **threat** to the man on the right of the wall: The water could rise, overflowing onto the man, or it could stay beneath the height of the wall, causing the wall to collapse.
- So the threat of harm is the potential for the man to get wet, get hurt, or be drowned. For now, the wall is intact, so the threat to the man is unrealized.
- However, we can see a **small crack in the wal**l - a **vulnerability** that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.
- he man is placing his **finger in the hole**, **controlling** the threat of water leaks until he finds a more permanent solution to the problem.

Examples in a Computer-based System

- **Assets-**
- **Vulnerability-**
- **Threats-**
- **Risk-**
- **Control-**

Examples in a Computer-based System

- **Assets-** Hardware, software and data
- **Vulnerability-** the system does not verify user's identity before allowing data access.
- **Threats-** human initiated (criminals), computer initiated, natural disasters
- **Risk-** Possibility of unauthorized access and unauthorized data manipulation.
- **Control-** A software, which checks the user identity before allowing data access. Antivirus Program.

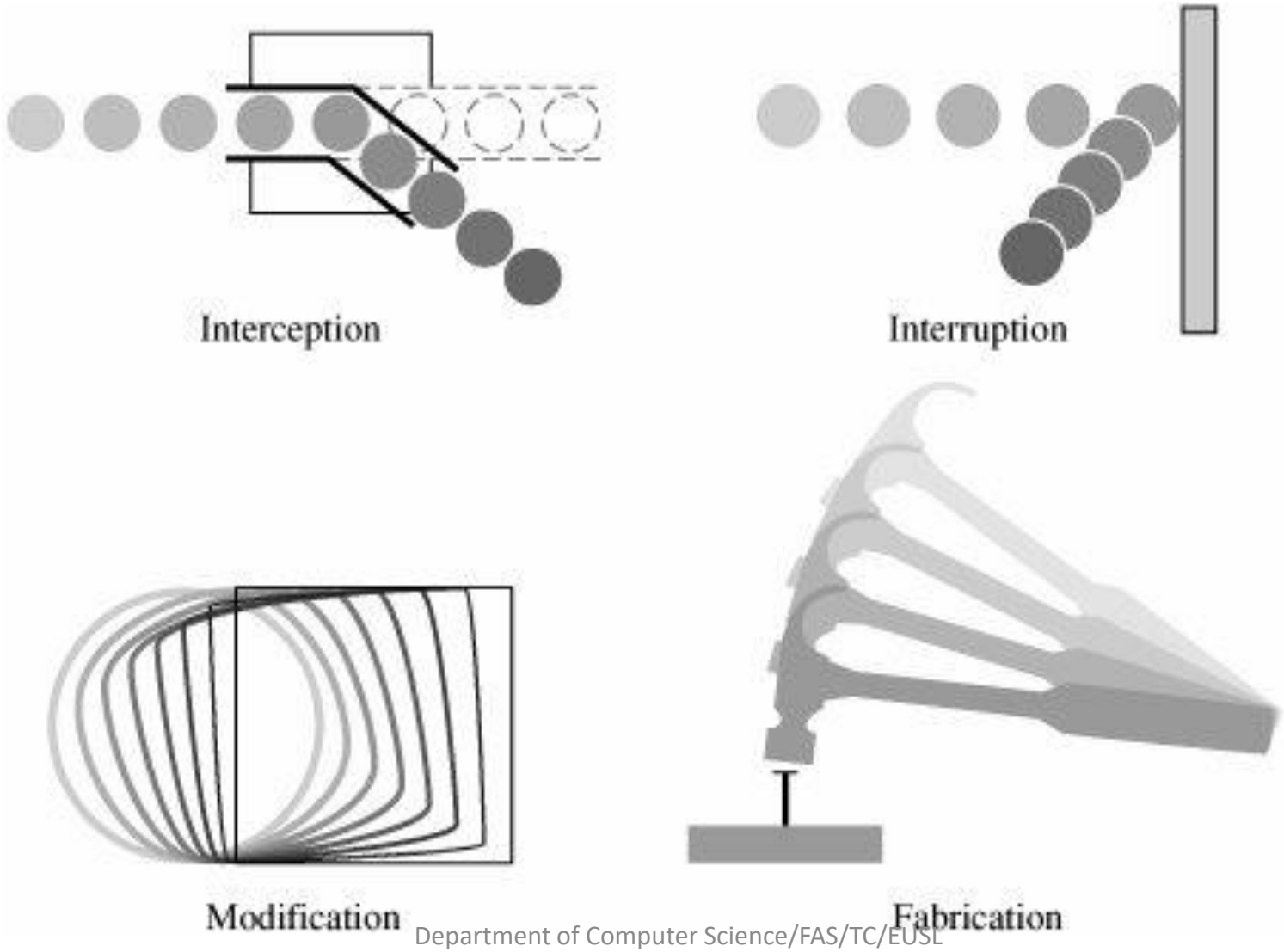
Attack

- Attack ? It is a realization of a threat.
- In *computer* and *computer networks* an **attack is any attempt** to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Threats

- What bad things can happen to assets?
- Who or What can cause or allow those bad things happen?
- Sending email, searching the web – expect it to be available for use when you want.
- When you write a document and save it, you trust that the document will reload exactly as you saved.
- Send a confidential message, you don’t want them broadcast to other people.

Kind of Attacks

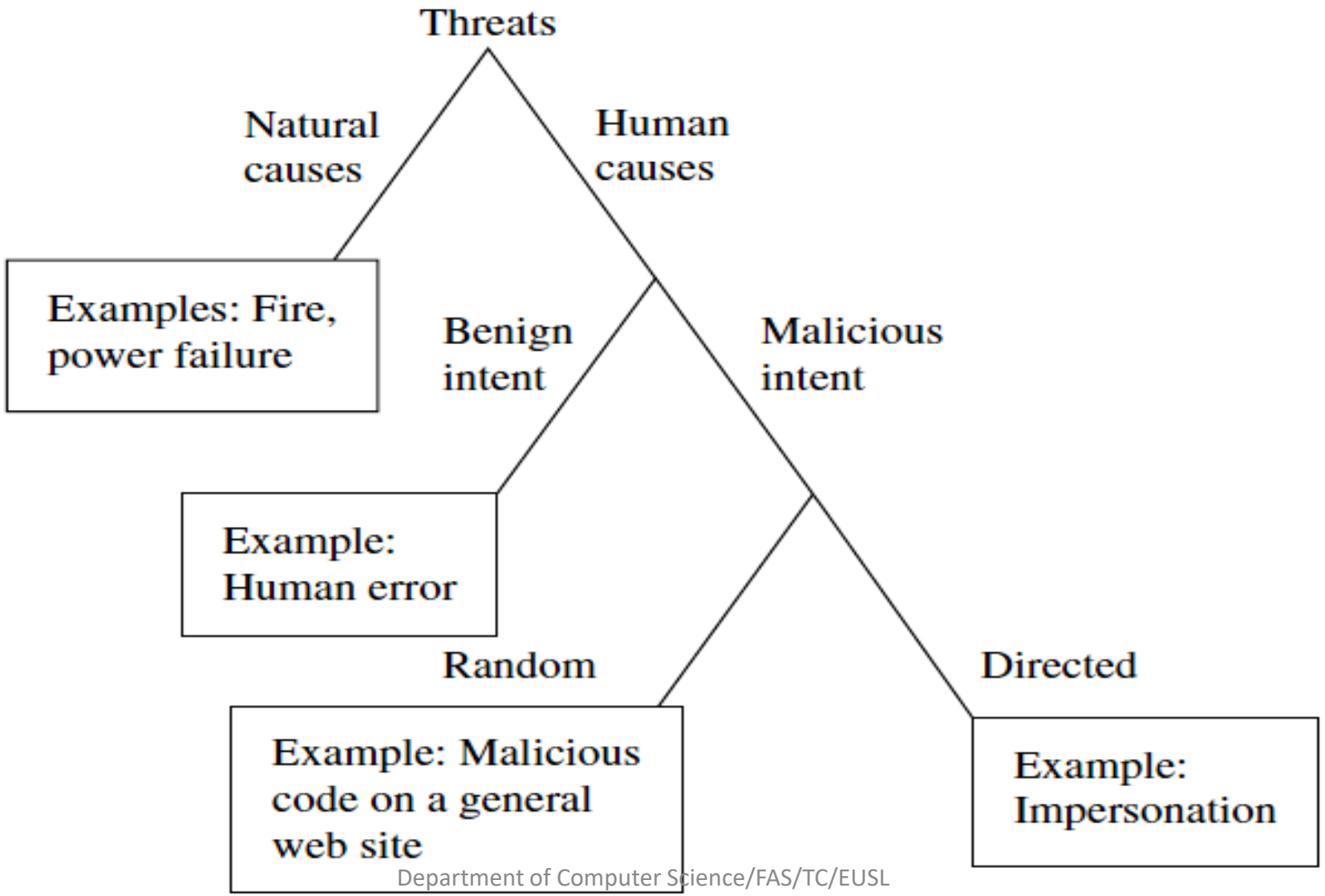


Kind of Acts

- An **interception** means that some unauthorized party has gained access to an asset.
- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable.
- **modification**. Modifying the assets.
- An unauthorized party might create a **fabrication** of counterfeit objects on a computing system.

Explain the four kind of attacks in communication with the help of diagram.

Types of Threats



The Meaning of Computer Security

Computer Security Goals/CIA Triad

- Confidentiality (secrecy or privacy) ensures that computer-related assets are accessed only by authorized parties.
- *An employee should not come to know the salary of his manager*
- Integrity means that assets can be modified only by authorized parties or only in authorized ways.
- *An employee should not be able to modify his/her own salary*
- Availability means that assets are accessible to authorized parties at appropriate times.
- *Pay-checks should be printed on time as stipulated by law*

Two more properties communication network

- **Authentication:** the ability of a system to confirm the identity of a sender.
- **Non-repudiation:** the ability of a system to confirm that a sender cannot convincingly deny having sent (do) something.

Confidentiality

- Some things obviously need confidentiality protection. Examples: Student grade, financial transaction, medical records.
- Ensuring confidentiality can be difficult.
- For example, who determines which people or systems are authorized to access the current system?
- By “accessing” data, do we mean that an authorized party can access a single bit? the whole collection? Can someone who is authorized disclose those data to other parties?

Integrity

- if we say that we have preserved the integrity of an item, we may mean that the item is
  - precise
  - accurate
  - unmodified
  - modified only in acceptable ways
  - modified only by authorized people
  - consistent

Availability

- an object or service is thought to be available if
  - It is present in a usable form.
  - It has capacity enough to meet the service's needs.
  - It is making clear progress, and, if in wait mode, it has a bounded waiting time.
  - The service is completed in an acceptable period of time..

1. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a). John peeks at kamal's password when he is logging in.

b). There is a process running in Kamal's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases.

c). John copies a file from Kamal's account and then deletes the file .

1. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a). John peeks at kamal's password when he is logging in. [CONFIDENTIALITY]

b). There is a process running in Kamal's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases. [INTEGRITY]

c). John copies a file from Kamal's account and then deletes the file . [CONFIDENTIALITY] [AVAILABILITY]

a. John copies Mary's homework.

b. Paul crashes Linda's system.

c. Carol changes the amount of Angelo's cheque from $100 to $1,000.

d. Gina forges Roger's signature on a deed.

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

a. John copies Mary's homework. [CONFIDENTIALITY]

b. Paul crashes Linda's system. [INTEGRITY] [AVAILABILITY]

c. Carol changes the amount of Angelo's cheque from $100 to $1,000. [INTEGRITY]

d. Gina forges Roger's signature on a deed. [INTEGRITY]

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name. [AVAILABILITY]

The meaning of Computer Security

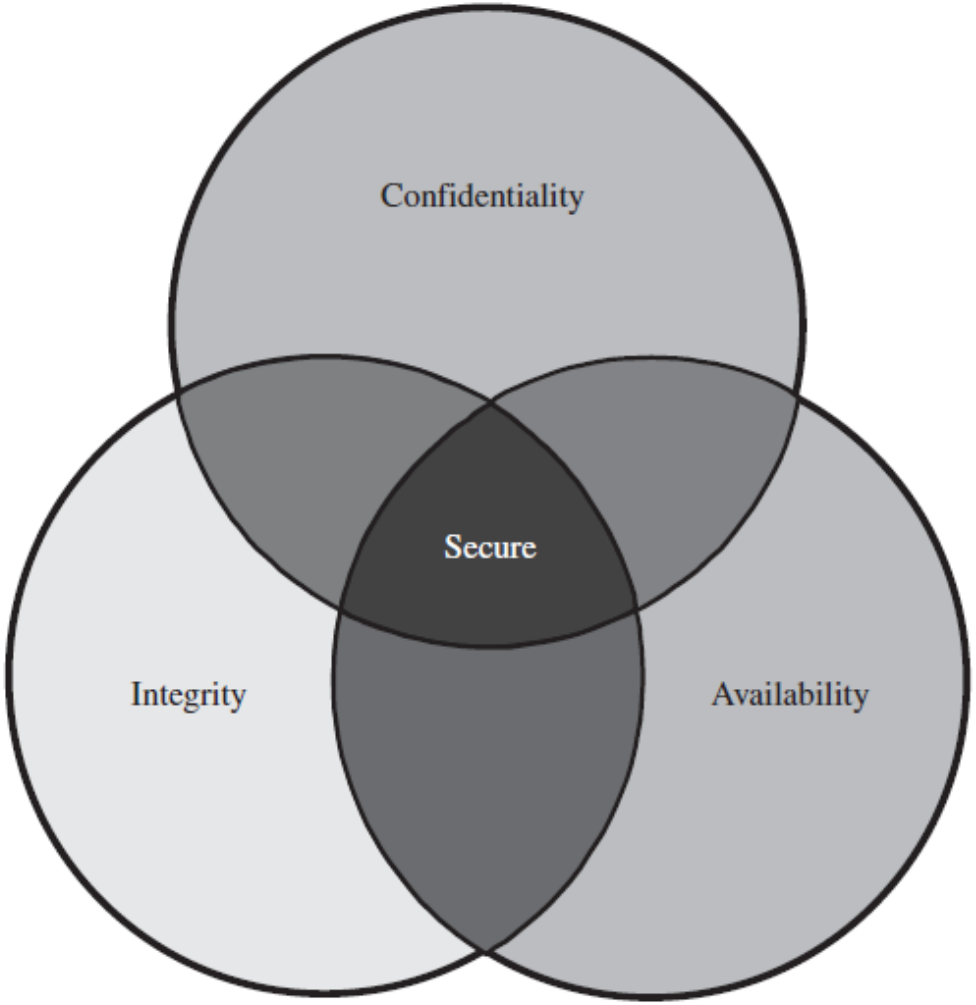


FIGURE 1-3 Relationship Between Confidentiality, Integrity, and Availability.

One of the challenges in building a secure system is finding the **right balance among the goals**.

Methods of Defense/Controls

- **Prevention: Blocking the attack or closing the vulnerability,** Physical barriers, access controls, encryption, firewalls, human awareness, etc.
- **Deter/Deflect it:** By making the attack harder, by making another target more attractive.
- **Detection:** Audits, checks and balances.
- **Recover: from its effects,** backup

Common Control Mechanisms

- **Physical Controls:** locks and keys, human guards.
- **Procedural or Administrative Controls:**
  - Laws and regulations, policies and procedures, copyrights, patents, contracts, agreements
- **Technical Controls:**
  - Encryption (Next Chapter!)
  - Access Control/Authentication systems
  - Backups
  - Firewall
  - Intrusion detection system.
- **Special Controls** for Software, Hardware, Data, Network, OS, Database.

Access Control

- **Access control** (AC) is the selective restriction of **access** to a place or other resource. The act of accessing may mean consuming, entering, or using.
- includes **identification, authorization, authentication**, access approval, and audit.
- Its function is to control which principals (persons, processes, machines, . . .) have access to which resources in the system—which files they can read, which programs they can execute, how they share data with other principals, and so on.

Identification/Authentication/Authorization

- **Identification** occurs when a subject claims an **identity** (such as with a username) and **authentication** occurs when a subject proves their **identity** (such as with a password).
- Once the subject has a proven **identity**, **authorization techniques can grant or block access to objects based on their proven identities.**
- Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices.