CSc 466/566

Computer Security

1 : Terminology I

Version: 2019/08/25 14:40:13

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

Definition (Computer Security)

Cybersecurity, computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Source: https://en.wikipedia.org/wiki/Computer_security

Security Mindset

- Bruce Schneier - The Security Mindset:

  https://www.youtube.com/watch?v=eZNzMKS7zjo&t=4s

Attack Scenarios

- In the next couple of slides, look up what each kind of security scenario is, and define it in your own terms.

What is a Phishing Attack?

Definition (Phishing)

What is a Phishing Attack?

Definition (Phishing)

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users

- Have you ever been phished?

Source: https://en.wikipedia.org/wiki/Computer_security

What is a Clickjacking Attack?

Definition (Clickjacking)

What is a Clickjacking Attack?

Definition (Clickjacking)

Clickjacking is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page.

- Why would someone want to do this?

Source: https://en.wikipedia.org/wiki/Computer_security

What is a Social engineering Attack?

Definition (Social engineering)

What is a Social engineering Attack?

Definition (Social engineering)

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.

Source: https://en.wikipedia.org/wiki/Computer_security

What is an Eavesdropping Attack?

Definition (Eavesdropping)

What is an Eavesdropping Attack?

Definition (Eavesdropping)

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network.

Source: https://en.wikipedia.org/wiki/Computer_security

What is a Denial-of-service Attack?

Definition (Denial-of-service attacks)

What is a Denial-of-service Attack?

Definition (Denial-of-service attacks)

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victims account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

Source: https://en.wikipedia.org/wiki/Computer_security

What is Malware?

Definition (Malware)

What is Malware?

Definition (Malware)

Malware is any software intentionally designed to cause damage to a computer, server or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer.

- What examples of types of malware have you heard of?

Source: https://en.wikipedia.org/wiki/Computer_security

Alice & Bob & Eve & Mallory & . . .

- Bruce Schneier - Who are Alice & Bob?:

  http://www.youtube.com/watch?v=BuUSi_QvFLY&feature=related
- A History of The World's Most Famous Cryptographic Couple: ttp://cryptocouple.com
- In *Alice and Bob can go on a holiday!*, S. Parthasarathy proposed to replace Alice and Bob by Sita and Rama, characters from Hindu mythology.

Alice & Bob & Eve & Mallory & . . .

- In the next couple of slides, try to draw a figure for each of the scenarios above. Include Alice and Bob (and whoever else is involved), the assets they have (Alice) or desire (Bob), such as credit card numbers, computers, etc.

Draw a Figure: Phishing Attack!

Draw a Figure: Clickjacking Attack!

Draw a Figure: Eavesdropping Attack!

Draw a Figure: Malware Attack!

Draw a Figure: Denial-of-service Attack!

Mechanisms

- Throughout the class we are going to discuss various mechanisms to build secure systems.
- As before, define these, and draw a figure!

What is a Firewall?

Definition (Firewall)

What is a Firewall?

Definition (Firewall)

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Source: https://en.wikipedia.org/wiki/Firewall_(computing)

What is a Anti-Virus Software?

Definition (Anti-Virus)

What is a Anti-Virus Software?

Definition (Anti-Virus)

Antivirus software (or anti-malware) is a computer program used to prevent, detect, and remove malware.

- Also known as AV software.

Source: https://en.wikipedia.org/wiki/Antivirus_software

Draw a System That Uses a Firewall!

Draw a System That Uses AV Software!

Outline

What is Computer Security?

Ensure that an asset (controlled-by, contained-in) a computer system

1. is accessed only by those with the proper authorization (confidentiality);
2. can only be modified by those with the proper authorization (integrity);
3. is accessible to those with the proper authorization at appropriate times (availability).

Risks

To mitigate the risks to computing systems we need to

1. learn what the threats are to the security;
2. learn how vulnerabilities arise when we develop the system;
3. know what mechanisms are available to reduce or block these threats.

Vulnerabilities

Definition (Vulnerability)

A vulnerability is a weakness in the security of a computer system that allows a malicious user to "do something bad."

- A vulnerability could be exploited for different reasons to affect many different assets.
- Something bad:
  - take control of the system,
  - slow down the system so that it's unusable,
  - access private data,
  - ...

Threats

Definition (Threat)

A threat is a set of circumstances that could possibly cause harm, a potential violation of security.

- Threats include
  - who might attack against what assets,
  - what resources they might use,
  - what goal they have in mind,
  - when/where/why they might attack,
  - with what probability they might attack.
- A threat is blocked by a control of vulnerabilities.

What's a KeyLogger?

- USB-to-USB connector, installed between keyboard and computer.
- Logs passwords to flash memory.
- Attacker can retrieve the logger or data can be transmitted wirelessly.

Threats vs. Vulnerabilities — Examples

Threat: Adversaries might install key-loggers in the computers in our Personnel Department so they can steal social security numbers.

Threats vs. Vulnerabilities — Examples

Threat: Adversaries might install key-loggers in the computers in our Personnel Department so they can steal social security numbers.

Vulnerability: The computers in the Personnel Department do not have up to date anti-malware software

Threats vs. Vulnerabilities — Examples

Threat: Thieves could break into our facility and steal our equipment.

Threats vs. Vulnerabilities — Examples

Threat: Thieves could break into our facility and steal our equipment.

Vulnerability: Our locks are easy to pick.

Threats vs. Vulnerabilities — Examples

Threat: Employees (insiders) might release confidential information to our competitors.

Threats vs. Vulnerabilities — Examples

Threat: Employees (insiders) might release confidential information to our competitors.

Vulnerability: Our employees don't understand what information is sensitive so they don't know how to protect it.

Threats vs. Vulnerabilities — Examples

Threat: A disgruntled employee could sabotage our factory.

Threats vs. Vulnerabilities — Examples

Threat: A disgruntled employee could sabotage our factory.

Vulnerability: We don't do background checks on our employees.

Threats vs. Vulnerabilities — Examples

Threat: Eco-terrorists want to discredit our organization.

Threats vs. Vulnerabilities — Examples

Threat: Eco-terrorists want to discredit our organization.

Vulnerability: Our perimeter fences are weak, so they can dump chemicals on our property and then report us to the NYT as polluters.

Attacks

Definition (Attack)

An attack is an attempt by an adversary to cause damage to valuable assets, by exploiting vulnerabilities.

- We analyze potential attacks to determine what kind of damage they could cause:
  - theft, sabotage, destruction, espionage, tampering, or adulteration.

Defenses

Definition (Defense)

A defense is a mechanism that prevents or reports on or repairs after an attack.

- Actions to be taken to defend against attack:
  - identify compromised machines,
  - remove malicious code,
  - patch systems to remove vulnerabilities, ...

Summary of Concepts

- Asset:

Summary of Concepts

- Asset: Something of value we need to protect
- Vulnerability:

Summary of Concepts

- Asset: Something of value we need to protect
- Vulnerability: A weakness in the security of a computer system
- Threat:

Summary of Concepts

- Asset: Something of value we need to protect
- Vulnerability: A weakness in the security of a computer system
- Threat: Circumstances that could violate security
- Attack:

Summary of Concepts

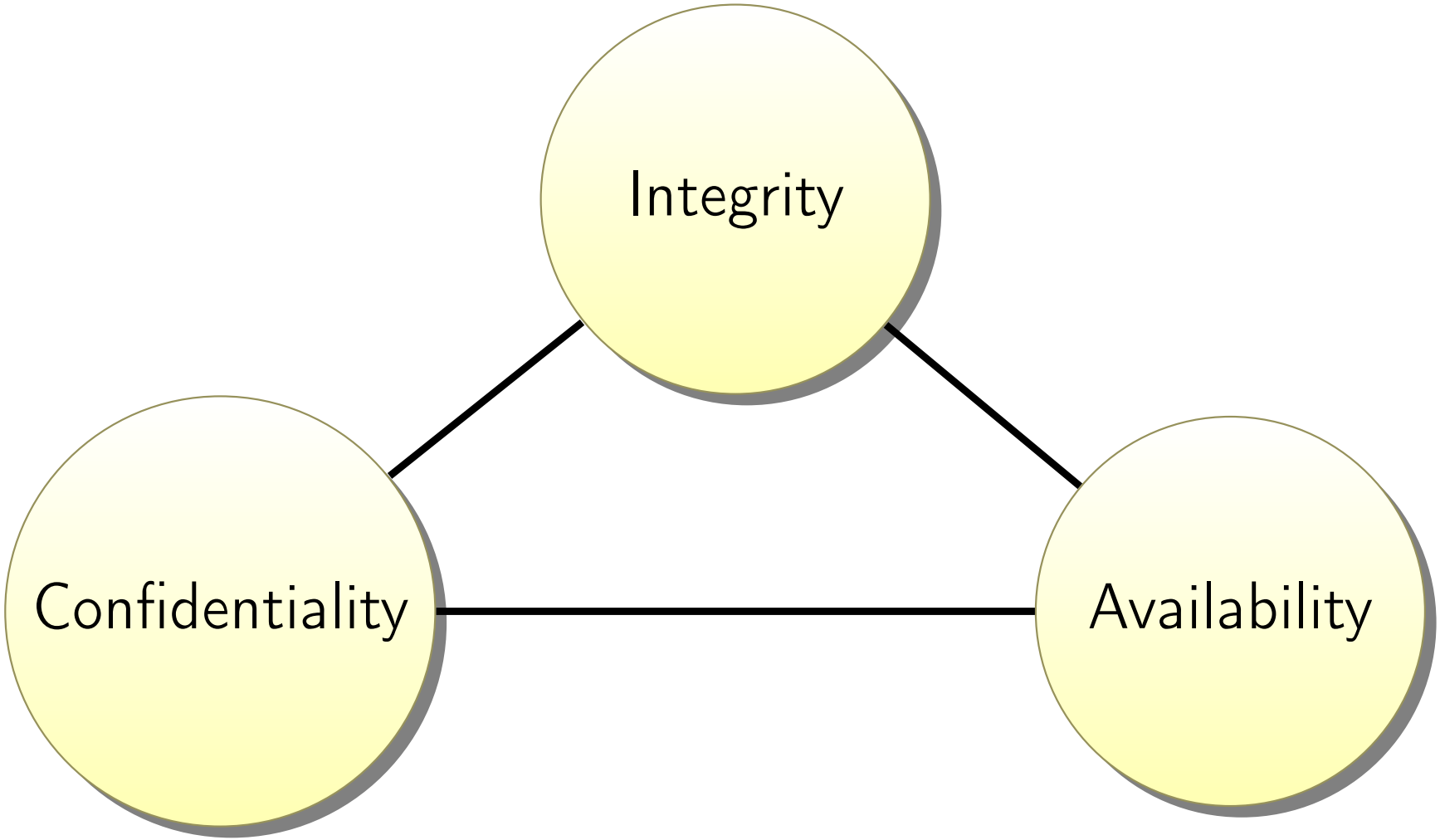
- Asset: Something of value we need to protect
- Vulnerability: A weakness in the security of a computer system
- Threat: Circumstances that could violate security
- Attack: Exploiting vulnerability to cause damage to an asset
- Defense:

Summary of Concepts

- Asset: Something of value we need to protect
- Vulnerability: A weakness in the security of a computer system
- Threat: Circumstances that could violate security
- Attack: Exploiting vulnerability to cause damage to an asset
- Defense: Mechanism that prevents/reports/repairs an attack

Outline

Goals of information security



Confidentiality

Definition (Confidentiality)

Avoidance of unauthorized disclosure of information or resources.

- You're authorized to read the data $\Rightarrow$ you get to read it.
- You're unauthorized $\Rightarrow$ you get to know nothing about the data.
- Reading, viewing, printing, knowing existance of, ...

Confidentiality: Who needs it?

- Who needs confidentiality?
  - Government
  - Military
  - Industry
- Originated in the military — information needs to be restricted to those with a need to know.
- Industry — Personnel records, designs, ...
- Industrial espionage is a huge problem.

Goal 1: Concealing the data itself

- Social security number in a personnel record
- Plan of attack against Baghdad
- Number of CPU cores on the new iPhone
- The government used waterboarding against our enemies

Goal 2: Concealing the existence of data

- There exists a plan to attack Baghdad
- There exists plans for a new iPhone
- The government tortured our enemies

Mechanisms

- Encryption — scramble a message so that it can only be read if you know a secret

Mechanisms

- Encryption — scramble a message so that it can only be read if you know a secret
- Access control — rules and policies to limit access to confidential information.

Mechanisms

- Encryption — scramble a message so that it can only be read if you know a secret
- Access control — rules and policies to limit access to confidential information.
- Authentication — Determine the identity/role someone has.

Mechanisms

- Encryption — scramble a message so that it can only be read if you know a secret
- Access control — rules and policies to limit access to confidential information.
- Authentication — Determine the identity/role someone has.
- Authorization — Based on access control policies, can a person have access to a resource?

Mechanisms

- Encryption — scramble a message so that it can only be read if you know a secret
- Access control — rules and policies to limit access to confidential information.
- Authentication — Determine the identity/role someone has.
- Authorization — Based on access control policies, can a person have access to a resource?
- Physical security — Physical barriers (locks, doors, . . .) to limit access to computers and data.

Mechanisms — Encryption

Definition (Encryption)

Transform a message using a secret encryption key so that the content cannot be read unless you have access to the decryption key.

- Caesar used a simple form of cryptography.
- Cipher: Substitute $A \to D$, $B \to E$, $C \to F$, ...
- Easily broken today, but secure 2000 years ago, when few people were literate.

Mechanisms — Encryption

Alice

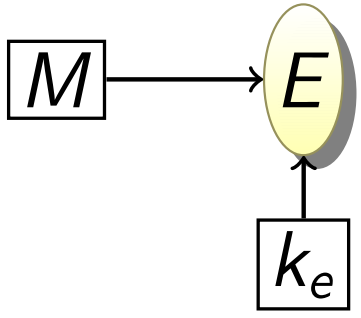
Bob

- M = Cleartext message; k_e = encryption key; k_d = decryption key; E = encryption function; D = decryption function

Mechanisms — Encryption

Alice

Bob

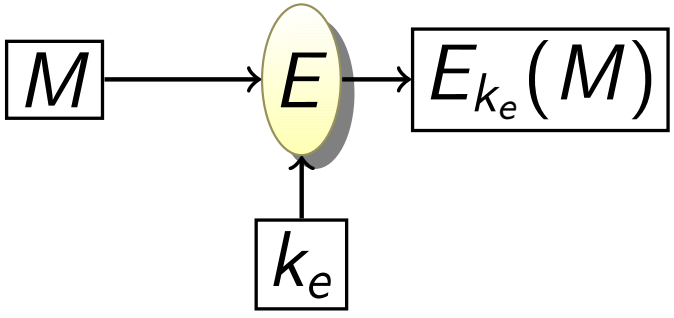


- M = Cleartext message; k_e = encryption key; k_d = decryption key; E = encryption function; D = decryption function

Mechanisms — Encryption

Alice

Bob

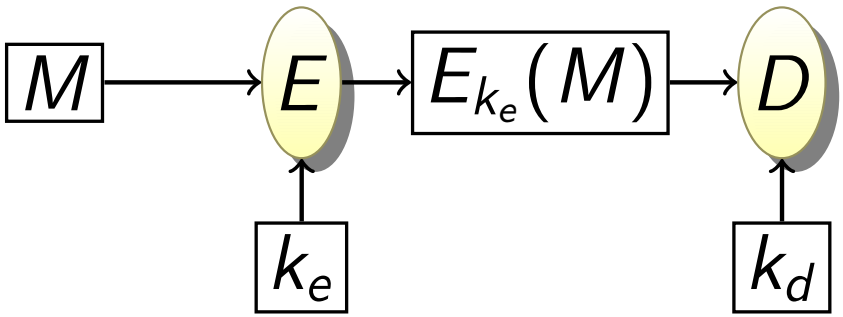


- M = Cleartext message; k_e = encryption key; k_d = decryption key; E = encryption function; D = decryption function

Mechanisms — Encryption

Alice

Bob

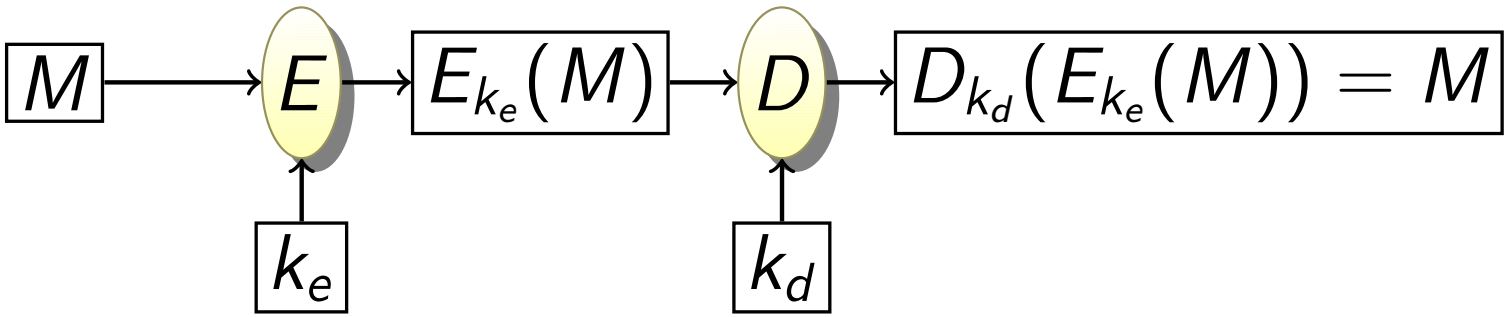


- M = Cleartext message; k_e = encryption key; k_d = decryption key; E = encryption function; D = decryption function

Mechanisms — Encryption

Alice

Bob



- M = Cleartext message; k_e = encryption key; k_d = decryption key; E = encryption function; D = decryption function

Mechanisms — Access Control

Definition (Access Control)

Rules and policies that restrict access to confidential information.

- Information can be accessed by those with a need to know.
- Can be
  - identity based — person's name or computer's serial number.
  - role based — what position (manager, security expert) the user has in the organization.

Mechanisms — Authentication

Definition (Authentication)

Ways to determine the identity or role someone has.

- We identify someone by a combination of
  1. something they have — smart card, radio key fob
  2. something they know — password, mother's maiden name, first pet's name
  3. something they are — fingerprint, retina scan

Mechanisms — Authorization

Definition (Authorization)

Determine if a person/system is allowed to access a resource.

- Authorization is based on an access control policy.
- Authorization prevents an attacker from tricking the system to let him access a protected resource.

Mechanisms — Physical Security

Definition (Physical Security)

Physical barriers to limit access to protected resources.

- Locks, windowless rooms, ...
- Sound dampening material, Faraday cages
- Protected processors

Example: chase.com

- What happens when we surf to `chase.com` and it asks for our credit card number?

1. Browser checks that the web site is really who they say they are — authentication.

Example: chase.com

- What happens when we surf to `chase.com` and it asks for our credit card number?

1. Browser checks that the web site is really who they say they are — authentication.
2. Web site checks that our browser is authentic — authentication.

Example: chase.com

- What happens when we surf to `chase.com` and it asks for our credit card number?

1. Browser checks that the web site is really who they say they are — authentication.
2. Web site checks that our browser is authentic — authentication.
3. Web site checks if we are allowed to access the site — access control.

Example: chase.com. . .

4. Our browser asks the web site for key to encrypt our credit card — encryption.

Example: chase.com. . .

4. Our browser asks the web site for key to encrypt our credit card — encryption.
5. The browser sends the encrypted credit card to the web site.

Example: chase.com. . .

4. Our browser asks the web site for key to encrypt our credit card — encryption.
5. The browser sends the encrypted credit card to the web site.
6. The data center is protected by physical security.

Draw the Chase Scenario Above!

Integrity — Concepts

Definition (Integrity)

Ensure that information hasn't been modified in an unauthorized way.

- Benign compromise: a bit gets flipped on disk, the disk crashes, ...
- Malicious compromise: virus infects our system and destroys files, ...
- Writing, changing, deleting, creating, ...

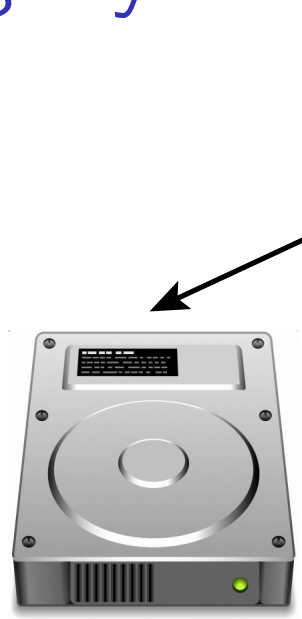
We trust the data if we trust. . .

Alice

Bob

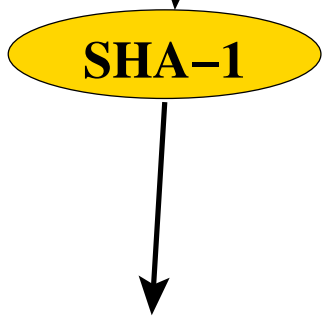
1. its origin (how/from whom was it obtained?);
2. how it was protected before it arrived at our machine;
3. how it was protected in transit to our machine;
4. how it is protected on our machine

Integrity: Mechanisms



Backup

Prevent integrity violation



0x0A76F7D10...

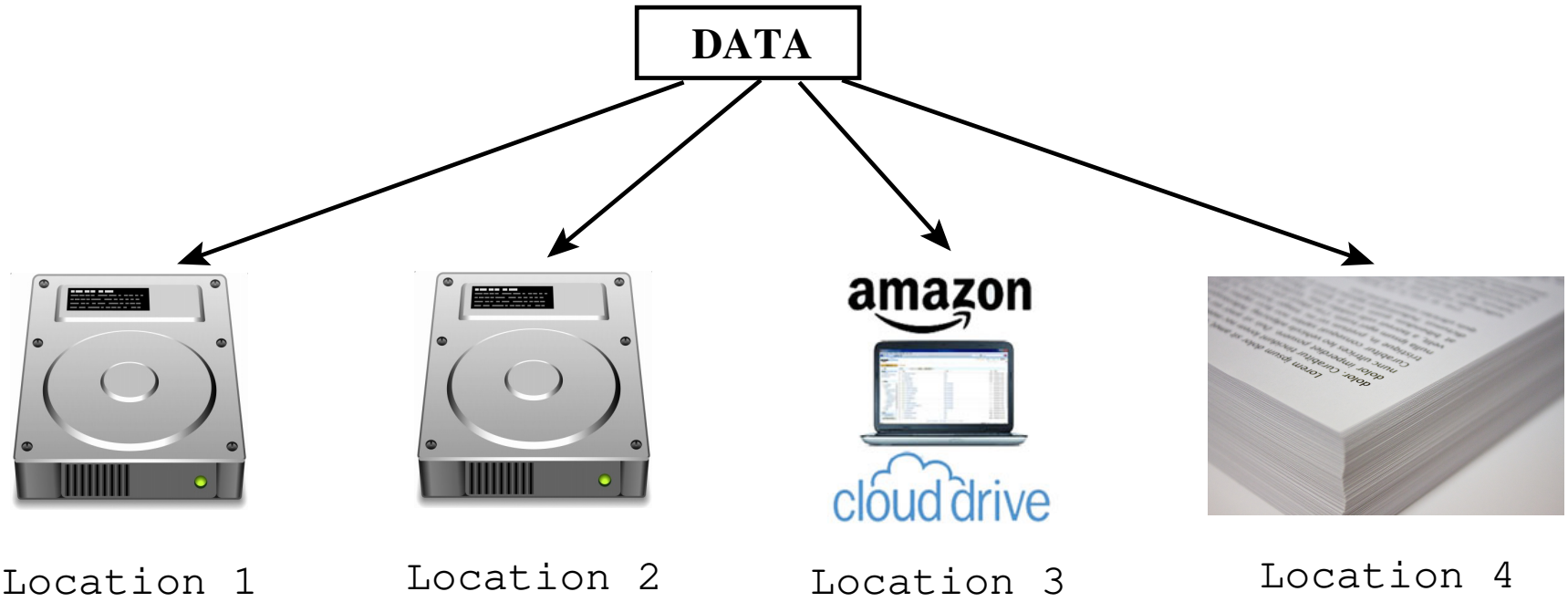
Has checksum changed since last time?

Detect integrity violation

Error correcting bits

Correct integrity violation

Integrity: Principles of Mechanisms



Redundancy!

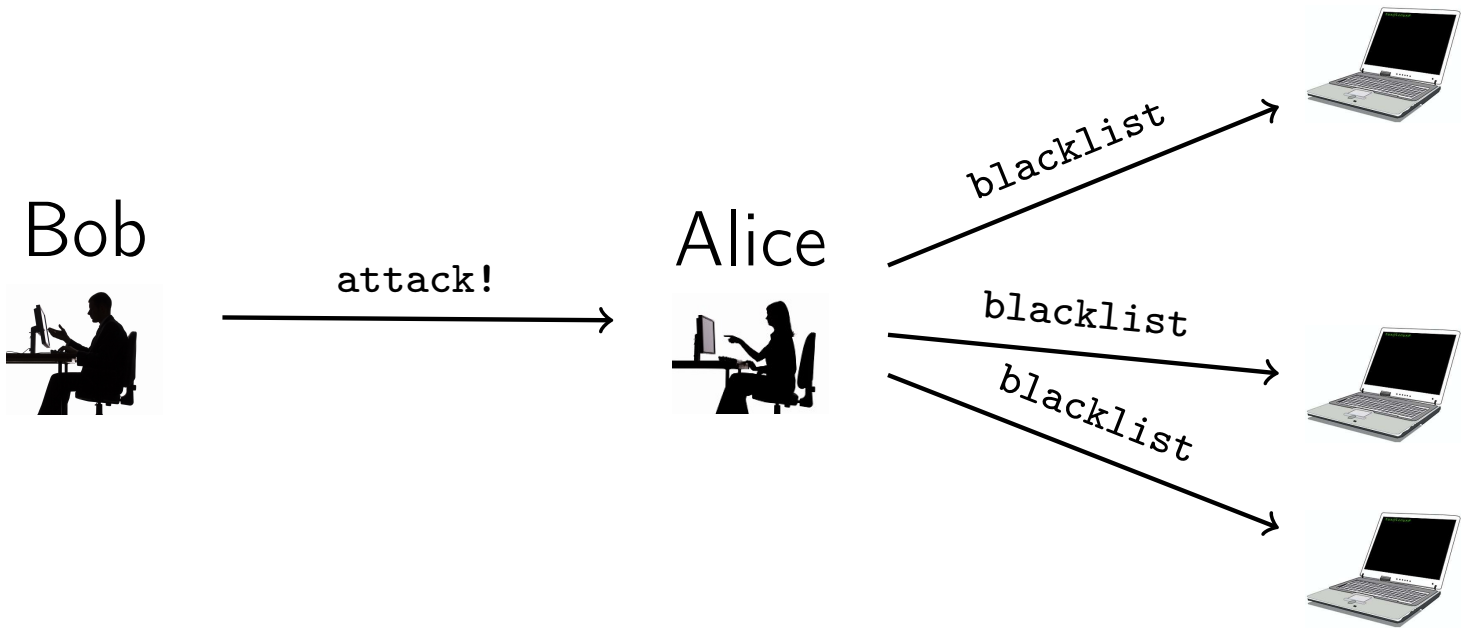
Availability

Definition (Availability)

Ensure that information/systems/... are accessible by those who are authorized in a timely manner.

- Some information is time sensitive — it's only valuable if we can get to it when we need it:
  - Stock quotes
  - Credit card number black lists

Availability: Example



1. Bob steals credit cards numbers
2. Alice broadcasts invalid numbers
3. Bob attacks Alice
4. Merchants don't get blacklisted numbers

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable. Availability
3. Alice sends Bob a check for \$10. He changes it to \$100.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable. Availability
3. Alice sends Bob a check for \$10. He changes it to \$100.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable. Availability
3. Alice sends Bob a check for \$10. He changes it to \$100. Integrity
4. Bob registers `cocacola.com` before the CocaCola Company has a chance to.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable. Availability
3. Alice sends Bob a check for \$10. He changes it to \$100. Integrity
4. Bob registers `cocacola.com` before the CocaCola Company has a chance to.

Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework. Confidentiality
2. Alice and Bob play computer games over a LAN. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable. Availability
3. Alice sends Bob a check for \$10. He changes it to \$100. Integrity
4. Bob registers `cocacola.com` before the CocaCola Company has a chance to. Availability (unless he allows them to buy the domain)

Exercise II

- Give an example of a situation where a compromise of confidentiality leads to a compromise in integrity.

Exercise II

- Give an example of a situation where a compromise of confidentiality leads to a compromise in integrity.

(1)Bob steals a password (compromising its confidentiality); (2) Then Bob uses the password to impersonate Alice, who is a user authorized to change the data.

Integrity requires that only authorized users make only authorized changes to data.

Source: Bishop, *Introduction to Computer Security*.

Exercise III

Give examples of situations when each of these is true:

1. Prevention is more important than detection and recovery.

Exercise III

Give examples of situations when each of these is true:

1. Prevention is more important than detection and recovery. Nuclear command and control system. By the time an intrusion is detected and recovered from, an attacker could have launched nuclear weapons.
2. Recovery is more important than prevention and detection.

Exercise III

Give examples of situations when each of these is true:

1. Prevention is more important than detection and recovery. Nuclear command and control system. By the time an intrusion is detected and recovered from, an attacker could have launched nuclear weapons.
2. Recovery is more important than prevention and detection. Banking computer that maintains account balances. The bank must be able to recover the balance of all accounts to ensure it provides accurate service to its customers.

Source: Bishop, *Introduction to Computer Security*.

Exercise III. . .

Give examples of situations when each of these is true:

1. Detection is more important than prevention and recovery.

Exercise III. . .

Give examples of situations when each of these is true:

1. Detection is more important than prevention and recovery. Protection of medical records from unauthorized emergency room personnel. If someone is brought into an emergency room, there may not be time to secure the patient's permission to access his medical records. But if the records are accessed illicitly, the security personnel should detect it.

Source: Bishop, *Introduction to Computer Security*.

Exercise IV

1. Give an example of a site for which it is beneficial to allow users to download arbitrary programs from the Internet.

Exercise IV

1. Give an example of a site for which it is beneficial to allow users to download arbitrary programs from the Internet. University (emacs): students benefit from learning about variety of tools.
2. Give an example of a site for which it is *not* beneficial.

Exercise IV

1. Give an example of a site for which it is beneficial to allow users to download arbitrary programs from the Internet. University (emacs): students benefit from learning about variety of tools.
2. Give an example of a site for which it is *not* beneficial. Insurance company, military installation: downloaded applications could destroy or exfiltrate data.

Source: Bishop, *Introduction to Computer Security*.

Outline

Readings

- Chapter 1 in *Introduction to Computer Security*, by Goodrich and Tamassia.