CSc 466/566

Computer Security

1 : Introduction — Terminology

Version: 2012/01/18 15:36:41

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

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 accesible to those with the proper authorization at appropriate times (availability).

Challenge to find a balance:

1. put the asset in a safe, throw a way the key (confidential but not available).

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.

Threats vs. Vulnerabilities — Examples

Threat: Adversaries might install keyloggers 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.

Vulnerability: Our locks are easy to pick.

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.

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

Threats vs. Vulnerabilities — Examples

Threat: Eco-terrorists want to discredit our organization.

Vulnerability: They can dump chemicals on our property and then report us to the New York Times as polluters.

Attacks

- 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

- We want to develop methods that will defend against attacks.
- Actions to be taken to defend against attack:
  - identify compromised machines,
  - removing malicious code,
  - patching systems to remove vulnerabilities, ...

Design, Implementation and Deployment

- The design of secure systems must take usability into account.
- Users will ignore inconvenient or hard-to-understand security measures.
- The implementation of a secure system needs to be tested.
- A deployed system must be continuously monitored:
  - detect security breaches
  - react to security breaches
- Security patches must be applied when they become available.

Outline

Models

- To build secure systems, we need sound models.
- Which security properties should be assured?
- What type of attacks can be launched?

Principle of Easiest Penetration

Definition (Principle of Easiest Penetration)
An adversary must be expected to use any available means of penetration — not the most obvious means, and not against the part of the system that has been best defended.

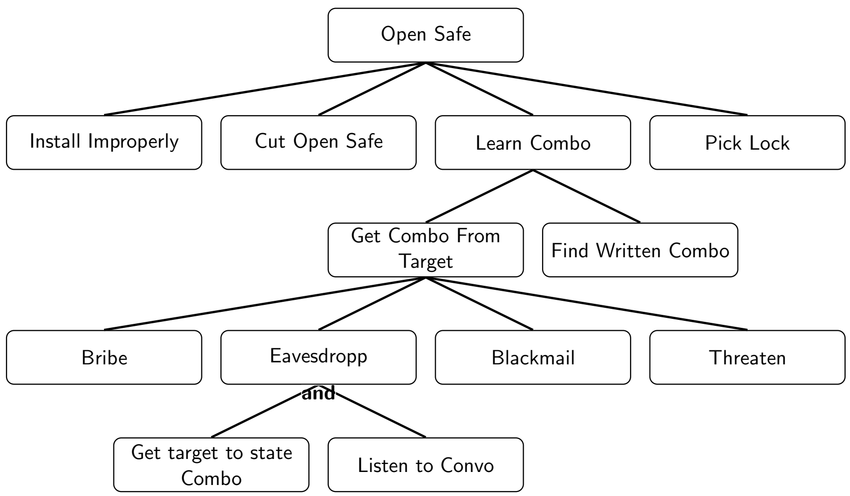
- The attacker will not behave the way we want him to behave.

Attack Trees

- We need to model threats against computer systems.
- What are the different ways in which a system can be attacked?
- If we can understand this, we can design proper countermeasures.
- Attack trees are a way to methodically describe the security of a system.
- Attack trees have both AND and OR nodes:
  - OR: Alternatives to achieving a goal.
  - AND: Different steps toward achieving a goal.

  Each node is a subgoal. Child nodes are ways to achieve that subgoal.

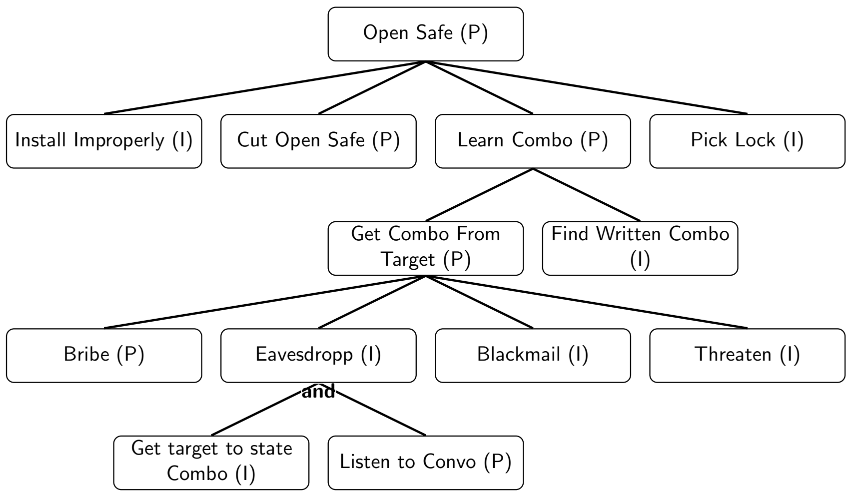
Attack Trees — Example I — Open a Safe



Attack Trees — Example I — Open a Safe

- Examine the safe/safe owner/attacker's abilities/etc. and assign values to the nodes:
  - P = Possible
  - I = Impossible
- The value of an OR node is possible if any of its children are possible.
- The value of an AND node is possible if all children are possible.
- A path of P:s from a leaf to the root is a possible attack!
- Once you know the possible attacks, you can think of ways to defend against them!

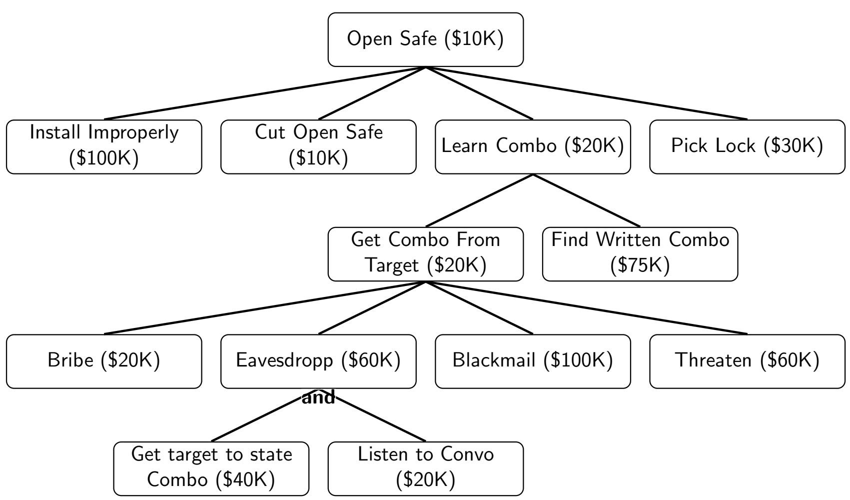
Attack Trees — Example I — Open a Safe



Attack Trees — Example I — Open a Safe

- We can be more specfic and model the cost of an attack.
- Costs propagate up the tree:
  - OR nodes: take the min of the children.
  - AND nodes: take the sum the children.

Attack Trees — Example I — Open a Safe



Attack Trees — Example II — Read a Message I

Goal: Read a message sent from computer A to B.

1. Convince sender to reveal message
   1. Bribe user, OR
   2. Blackmail user, OR
   3. Threaten user, OR
   4. Fool user.
2. Read message while it is being entered
   1. Monitor electromagnetic radiation, OR
   2. Visually monitor computer screen.
3. Read message while stored on A's disk.
   1. Get access to hard drive, AND
   2. Read encrypted file.
4. Read message while being sent from A to B.
   1. Intercept message in transit, AND
   2. Read encrypted message.

Attack Trees — Example II — Read a Message II

5. Convince recipient to reveal message
   1. Bribe user, OR
   2. Blackmail user, OR
   3. Threaten user, OR
   4. Fool user.
6. Read message while it is being read
   1. Monitor electromagnetic radiation, OR
   2. Visually monitor computer screen.
7. Read message when being stored on B's disk.
   1. Get stored message from B's disk after decryption
      1. Get access to disk, AND
      2. Read encrypted file.

      OR
   2. Get stored message from backup tapes after decryption.
8. Get paper printout of message
   1. Get physical access to safe, AND
   2. Open the safe.

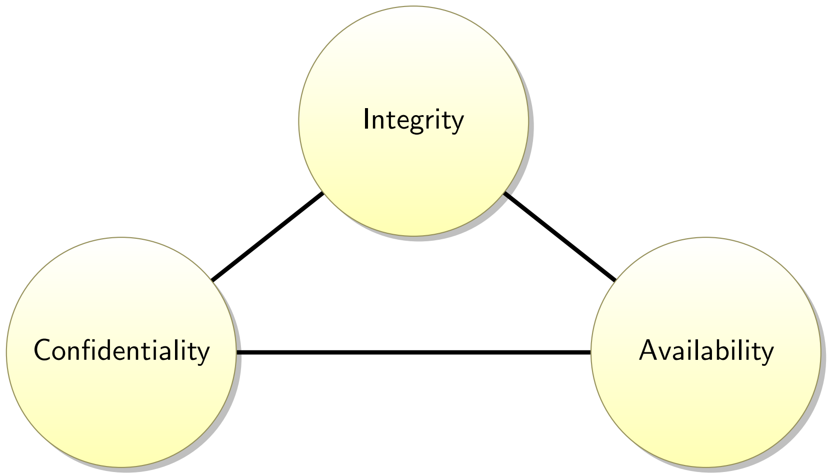
In-class Exercise: Attack Trees

- Alice wants to make sure that Bob cannot log into any account on the Unix machine she is administering.
- Alice draws an attack tree to see what Bob's attack options are.
- Show the tree!
- Source: Michael S. Pallos, http://www.bizforum.org/whitepapers/candle-4.htm.

Outline

Confidentiality, Integrity, Availability

- The C.I.A. Triad.
- These are the primary 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.

Confidentiality: What do we need to hide?

- We may want to conceal the data itself:
  - Social security number in a personell record
  - Plan of attack against Bagdad
  - Number of CPU cores on the iPhone5
  - The government used waterboarding against our enemies
- Or, we may want to conceal the existence of data:
  - There exists a plan to attack Bagdad
  - There exists plans for an iPhone5.
  - The government tortured our enemies

Confidentiality: Simple Ciphers

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

Confidentiality: Mechanisms

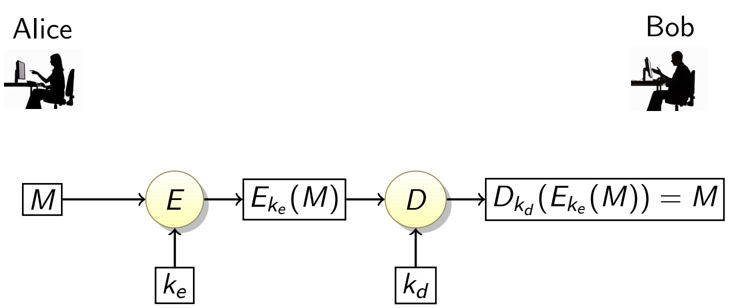
- Encryption — scramble a message so that the content can only be read by those who know a secret
- Access control — rules and policies to limit access to confidential information.
- Authentication — Determine the identity/role someone has.
- Authorization — Based on access control policies, can a person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

Confidentiality: 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.

Confidentiality: Mechanisms — Encryption



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

Confidentiality: 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.

Confidentiality: 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, . . .



Confidentiality: Mechanisms — Authorization

Definition (Authentication)

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.

Confidentiality: Mechanisms — Physical Security

Definition (Physical Security)

Physical barriers to limit access to protected resources.

- Locks, windowless rooms, . . .
- Sound dampening material, Faraday cages, . . . — to shield against eavesdropping
- Protected processors


Example: A web site asks for our credit card number

What happens?

1. Browser authenticates the website — is `chase.com` really who they say they are?
2. Web site checks that our browser is authentic.
3. Web site checks its access control policy — are we allowed to access the site?
4. Our browser asks the web site for a key to encrypt our credit card.
5. The browser sends the encrypted credit card to the web site.
6. The data center is protected by physical security.

Integrity — Concepts

Definition (Integrity)

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

- Example: whispering game (pass a message from child-to-child, sitting in a circle). Whispering doesn't preserve integrity!
- Benign compromise: a bit gets flipped on disk, the disk crashes, ...
- Malicious compromise: virus infects our system and destroys files, ...
- Writing, changing, deleting, creating, ...

Integrity

- Confidentiality originated in the military arena.
- Integrity originated with corporations (banks) that needed to ensure records (accounts) to be unmodified.

Integrity — data vs. origin

- data integrity — ensure that the contents of data is maintained
- origin integrity — ensure that the source of the data is maintained.
- Example:
  - NYT writes: "Our source Bob at Apple tells us that the iPhone5 will have 64 cores!"
  - Story is correct (data integrity maintained).
  - Alice leaked, not Bob (origin integrity violated).

Integrity: Mechanisms

- Backups — periodically archive data.
- Checksums — Check if a file has been altered by periodically computing a function

  $$f(\textit{data file}) \rightarrow \textit{128-bit number}$$

  over its contents.
- Data correcting codes: store data in such a way that small defects can be automatically corrected.

Integrity: Principles of Mechanisms

- Mechanisms typically make use of redundancy — we store data in multiple ways/locations.
- Mechanisms can
  - prevent integrity violations
  - detect integrity violations
  - correct (recover from) integrity violations
- Metadata (data about the data) also needs to be protected:
  - file owner
  - file creation/modification date
  - file protection bits (RWX)

Integrity: Evaluating

- How do we evaluate the integrity of data?
- We trust in the data if we trust
  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 relies on our trust in the source of the data.

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: Mechanisms

- Physical protection:
  - power generators (to withstand power outages)
  - blast walls (to withstand bombs)
  - thick walls (to withstand storms/earthquakes/...)
- Computational redundancy:
  - RAID (redundant array of inexpensive disks) (to withstand disk crash)
  - server farms (to withstand hardware failures)

Availability: Example

- Bob steals lots of credit cards
- `blacklist.visa.com` broadcasts invalid credit card numbers
- Bob attacks `blacklist.visa.com` so that merchants cannot receive blacklisted numbers.

In-Class Exercise I — Classify!

1. Alice and Bob are students. Alice copies Bob's homework.
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.
3. Alice sends Bob a check for $10. He changes it to $100.
4. Bob registers `cocacola.com` before the CocaCola Company has a chance to.

In-Class Exercise II

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

Source: Bishop, *Introduction to Computer Security*.

In-Class Exercise III

Give examples of situations when each of these is true:

1. Prevention is more important than detection and recovery.
2. Detection is more important than prevention and recovery.
3. Recovery is more important than prevention and detection.

Source: Bishop, *Introduction to Computer Security*.

In-Class Exercise IV

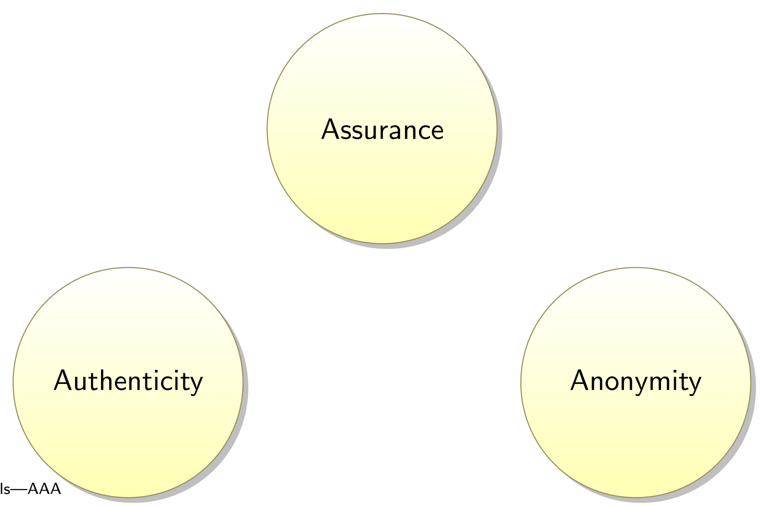
1. Give an example of a site for which it is beneficial to allow users to download arbitrary programs from the Internet.
2. Give an example of a site for which it is *not* beneficial.

Source: Bishop, *Introduction to Computer Security*.

Outline

Assurance, Authenticity, Anonymity

- In addition to the C.I.A. triad we also have the A.A.A. triad of secondary security goals.



Assurance, Authenticity, Anonymity

- Assurance — can we trust systems/people to behave as expected?
- Authenticity — is an issued statement/permission/policy/... genuine?
- Anonymity — can records/transactions not be tied to a particular individual?

Assurance

Definition (Assurance)

The way in which trust is provided and managed in a computer system.

- Trust — the degree to which we expect people and systems to behave as expected. (Many other definitions of trust!)

Assurance: Concepts

- To ensure trust, we first specify
  1. policies — Specifications of how people/systems are expected to behave;
  2. permissions — Descriptions of actions that people/systems are allowed to perform.
- Then we put in place
  1. Protections — Mechanisms that enforce policies and permissions.

Assurance: Example I — Apple iTunes

- Apple defines policies for buying/downloading/playing/copying songs.
- Apple grants permission to access a song Bob has paid for.
- Apple uses DRM (Digital Rights Management) technologies to protect against illegal copying.
- Bob expects Apple to abide by its policy for handling credit cards.
- Bob grants Apple permission to charge $.99 to her credit card when he buys a song.
- Bob has a protection agreement with Visa so that he's not charged if his card is stolen.

Assurance: Example II — University Computer Usage

- Bob is enrolled in 466/566.
- The department has a policy in place saying students can use department computers for homework assignments only.
- Bob is granted permission by the department to use `lectura.cs.arizona.edu` according to the policy.
- The department uses passwords/groups/file modes/monitoring/... to protect against unauthorized use of CPU/memory/storage resources.

Authenticity

Definition (Authenticity)

The ability to determine that statements, policies, permissions issued by persons or systems are genuine.

- We need to be able to enforce contracts.
- We cannot enfore the contract unless we know it's genuine.

Authenticity: Nonrepudiation

Definition (Nonrepudiation)

The property that authentic statements issued by a person or system cannot be denied.

- A person could claim they didn't sign a contract, or say it was signed by someone else.

Authenticity: Mechanisms

- Blue-ink signatures — achieves nonrepudiation by allowing a person to commit to the authenticity of a document, by signing their name on it.
- Digital signatures — achieves nonrepudiation for digital documents, using cryptography.

Anonymity

Definition (Anonymity)

Records or transactions cannot be attributed to any individual.

- Our identity is tied to the online transactions we perform:
  - medical records
  - purchases
  - legal records
  - email
  - browsing history

Anonymity: Mechanisms

- Aggregation — merging data from many people, but only when sums/averages can't be mined for an individual's information.
- Mixing — randomly merging different streams of transactions, information, communications so that they can be queried/searched/... but no information about an individual can be extracted.
- Proxies — trusted agents performing actions on behalf of a person, such that it can't be traced back to that individual.
- Pseudonyms — fake identities used in online communication, such that only a trusted party knows the connection to the real identity.

Anonymity: Examples — U.S. Census

- The Census publishes data (race, ethnicity, gender, age, salary) by zip-code.
- They won't publish the information if it would expose details about an individual.

Anonymity: Examples — https://www.torproject.org

- Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.
- Individuals use Tor to keep web sites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers.
- Journalists use Tor to communicate more safely with whistleblowers and dissidents.
- Law enforcement uses Tor for visiting or web sites without leaving government IP addresses in their web logs, and for security during sting operations.

Anonymity: Examples — Pseduo-Anonymous Remailers

- `http://anon.penet.fi` — no longer active.
- Alice wants to send an anonymous love letter M to Bob:
  1. Alice sends M to `anon.penet.fi`.
  2. `anon.penet.fi` strips off headers.
  3. `anon.penet.fi` assigns an ID `anon42` to M.
  4. `anon.penet.fi` stores `anon42` $\rightarrow$ Alice.
  5. `anon.penet.fi` sends M to Bob with `anon42@anon.penet.fi` as the return address.
  6. Bob can respond, through `anon.penet.fi`.
- In 1995 The Church of Scientology made a legal attack on `anon.penet.fi` to reveal the identity behind `an144108@anon.penet.fi`.

Anonymity: Examples — OKCupid.com

- OKCupid.com is a free dating site.
- Users are identified by pseudonyms so as not to reveal their real identity.

Outline

Threats and Attacks

- We've seen some goals of computer security.
- What are the attacks that can compromise security?
  1. Eavesdropping
  2. Alteration
  3. Denial-of-service
  4. Masquerading
  5. Repudiation
  6. Correlation

Threats and Attacks: Eavesdropping

Definition (Eavesdropping)

Interception of information intended for someone else while transmitted over a communication channel.

- An attack on confidentiality.
- Examples:
  1. Packet sniffers (monitor nearby Internet traffic).
  2. `tcpdump`, `wireshark`, etc.
  3. Sniff on wireless web traffic:

```
> sudo tcpdump -A -i en1 port 80
```

Threats and Attacks: Alteration

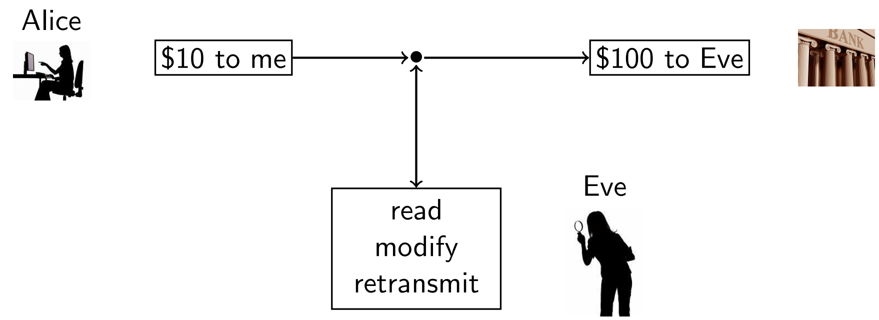
Definition (Alteration)

Unauthorized modification of information.

- An attack on data integrity.
- Examples:
  1. Cracking: tamper with an application to remove a license check.
  2. Computer virus: modify an application to insert and replicate themselves.

Threats and Attacks: Alteration. . .

- Examples:
  3. Man-In-The-Middle (MITM) attack: intercept, alter, and retransmit network packets.



Threats and Attacks: Denial-of-Service

Definition (Denial-of-Service (DOS))

Interrupt or degrade access to a service or a piece of data.

- An attack on data availability.
- Examples:
  1. Spam: Fills up your email inbox.
  2. Distributed DOS (DDOS): A Botnet floods `amazon.com` with packets to prevent you from buying books.
  3. Alice floods Bob's machine with requests in order to slow it down, as her orc slays his troll in World of Warcraft.

Threats and Attacks: Masquerading

Definition (Masquerading)

Create information that appears to be from someone who isn't the author.

- An attack on authenticity.
- Examples:
  1. Phishing: `BankOfAmerica.com` looks like `BankOfAmerica.com`, but isn't, and is used to gather username/passwords.
  2. Spoofing: Send a network packet with the wrong return IP address.

Threats and Attacks: Repudiation

Definition (Repudiation)

Denial of commitment or receipt of data.

- An attack on assurance.
- Examples:
  1. Blue-Ink Signatures: "That's not my handwriting!"
  2. "I never ordered this book from `amazon.com`!"

Threats and Attacks: Correlation/Traceback

Definition (Correlation/Traceback)

Merging several sources of information to determine a a particular piece of information, or the source of the information.

- An attack on anonymity.

Outline

Readings

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

Acknowledgments

Material and exercises have also been collected from these sources:

1. Roger G. Johnston, *Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities*, jps.anl.gov/Volume4_iss2/Paper3-RGJohnston.pdf.
2. Bruce Schneier, *Attack Trees*, Dr. Dobb's Journal December 1999, http://www.schneier.com/paper-attacktrees-ddj-ft.html.
3. Bishop, *Introduction to Computer Security*.
4. Michael S. Pallos, http://www.bizforum.org/whitepapers/candle-4.htm.