CYBER SECURITY

CHAPTER 1&2

DR. ALA BERZINJI

COMPUTER SECURITY

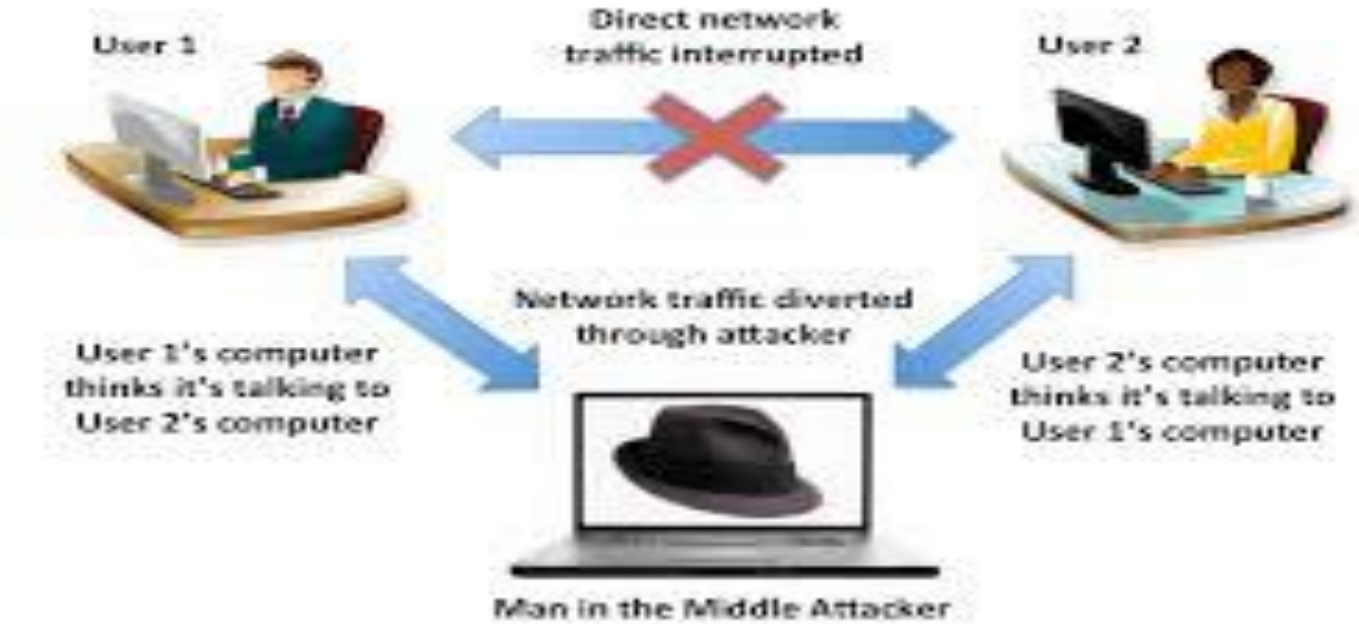
The original focus of computer security was on multiuser systems.

COMPUTER SECURITY

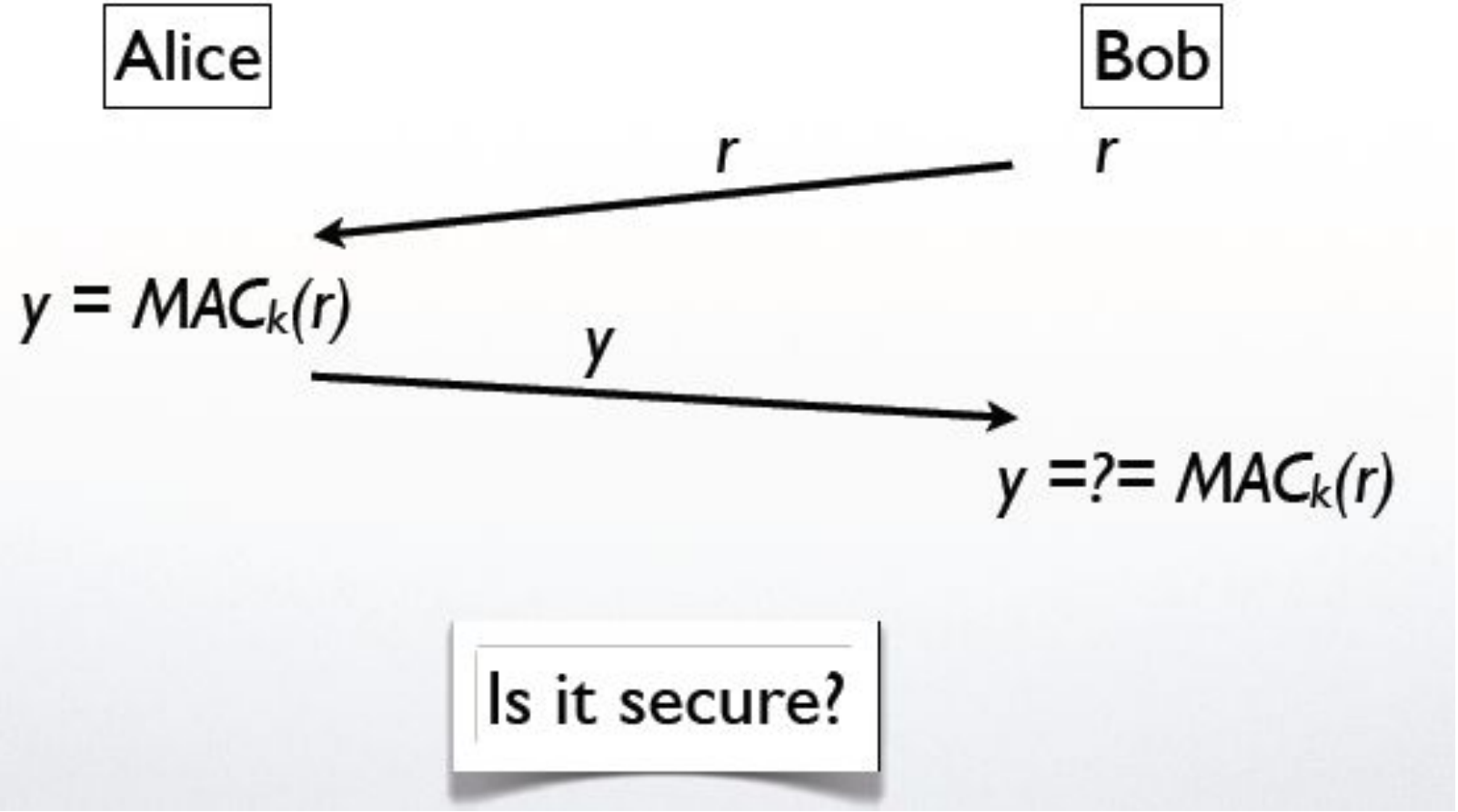
Today's focus is on computing devices that may figure as the end systems in a network.

COMPUTER SECURITY

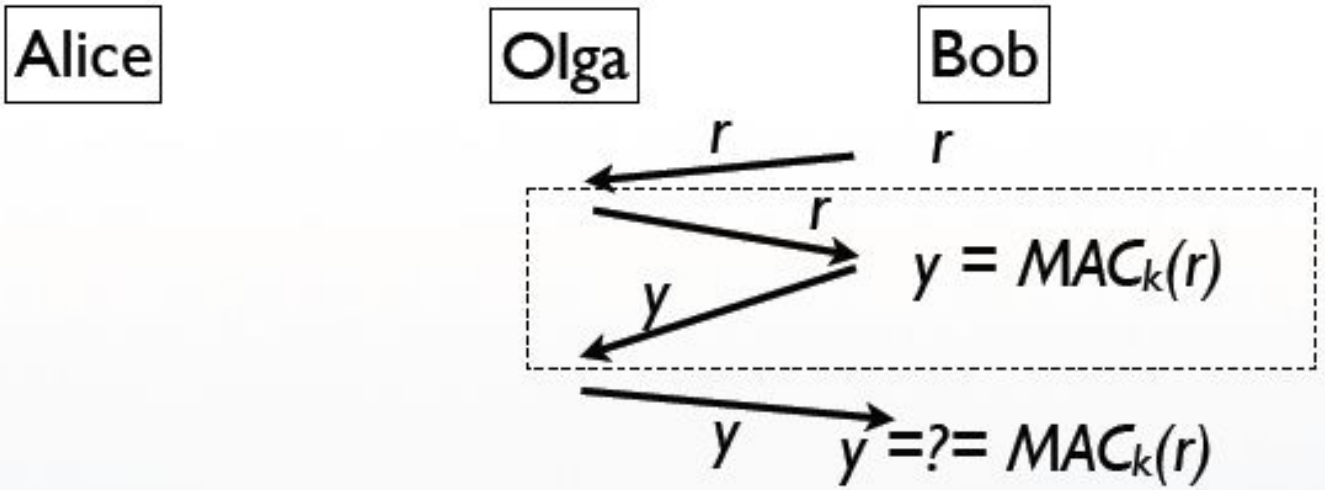
Traditional Network security services protect traffic between nodes.



COMPUTER SECURITY



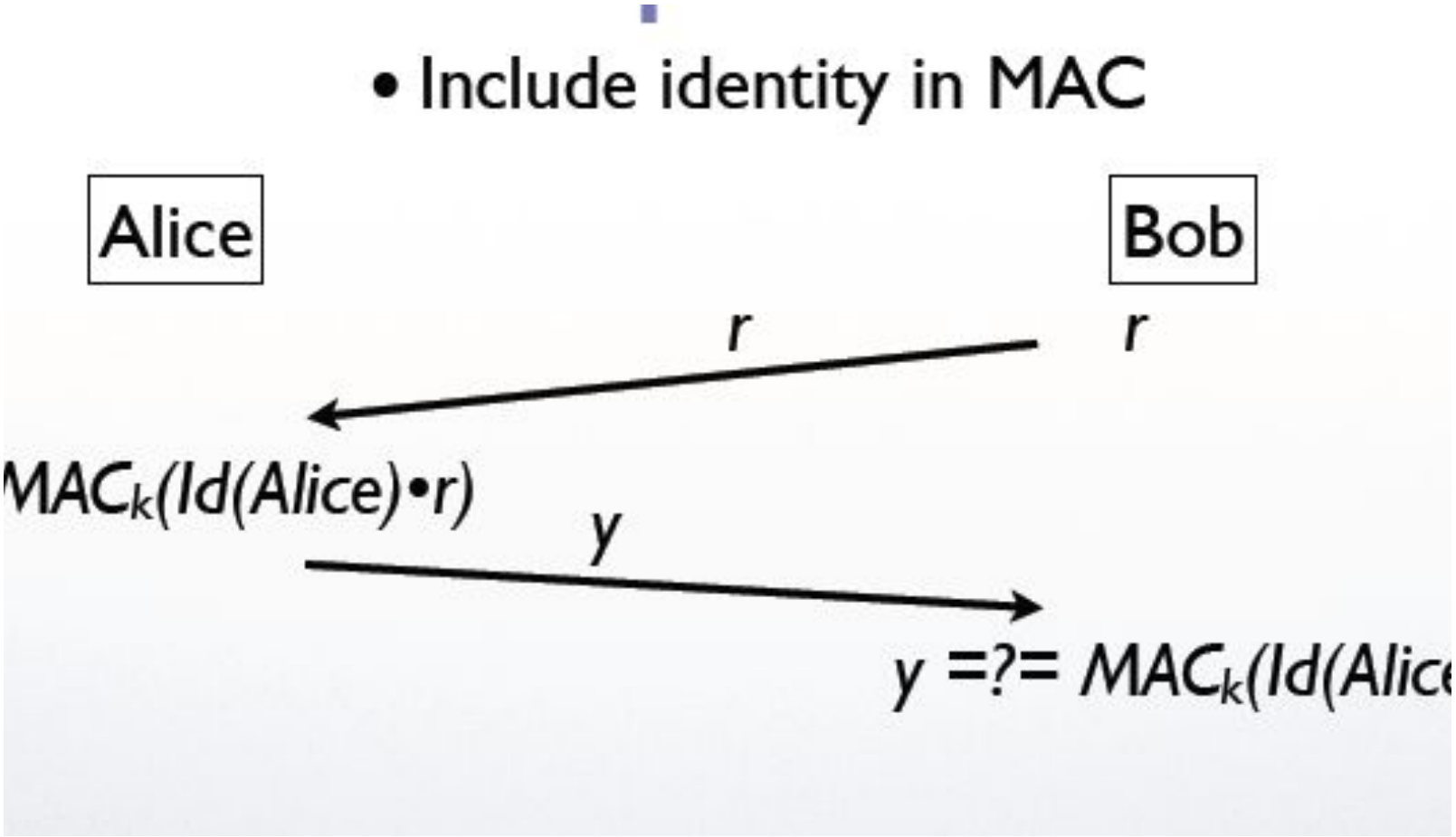
COMPUTER SECURITY



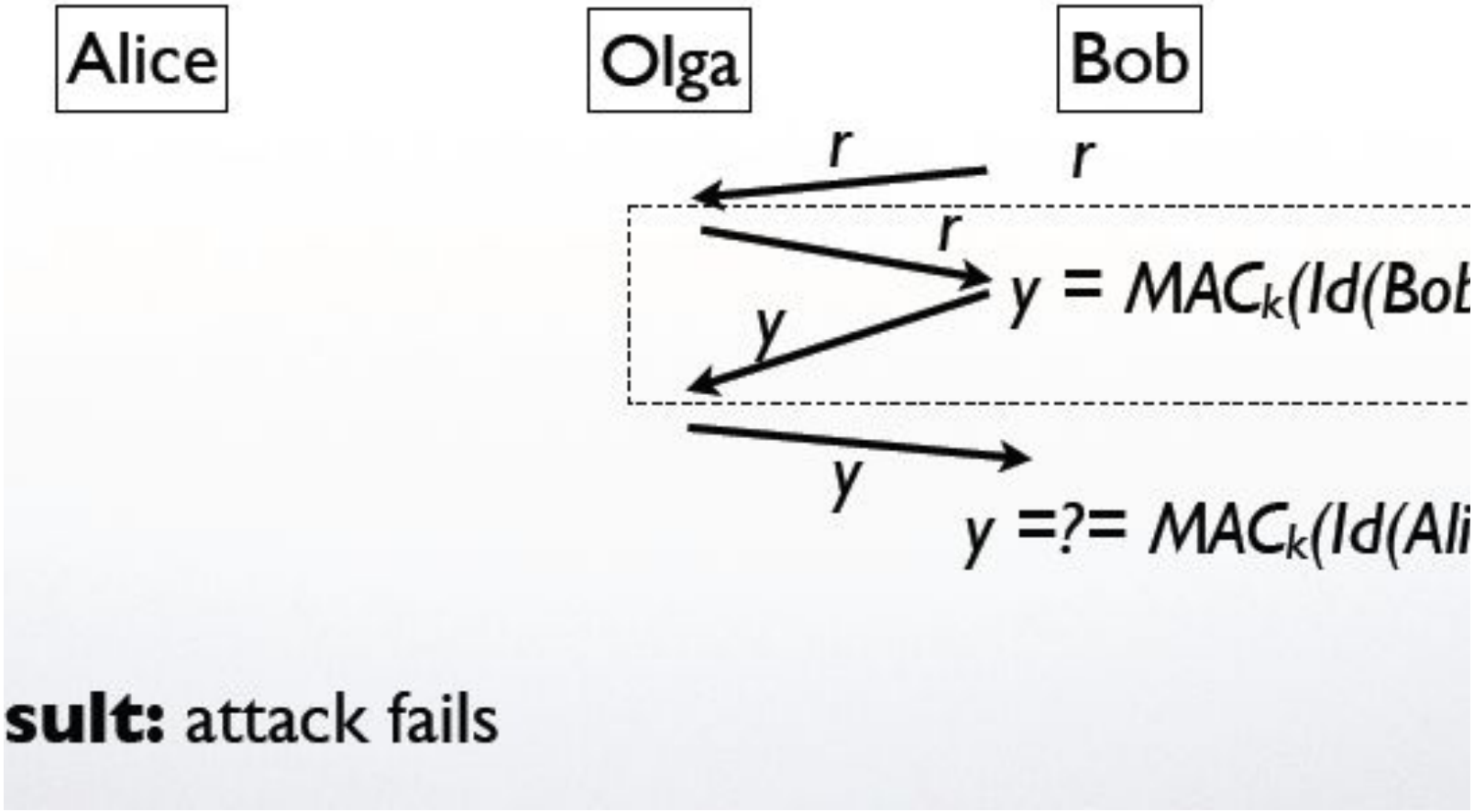
- Bob thinks Olga is Alice, although Olga doesn't know *k*.

How can the protocol be fixed?

COMPUTER SECURITY



COMPUTER SECURITY



sult: attack fails

ATTACKS AND ATTACKERS

These systems transmitted the traffic between a mobile device and a base station, anyone with write equipment could listen in on telephone calls.

Solution:

GSM

ATTACKS AND ATTACKERS

Customer and merchant

Solution:

Secure Socket Layer(SSL) was developed by NetScape to deal with this very problem

ATTACKS AND ATTACKERS

Scanning Internet traffic for packets containing credit card numbers is an attack with a low yield.

ATTACKS AND ATTACKERS

Identity theft, using somebody else's "identity' (name, social security number, bank account number) to gain access to a resource.

ATTACKS AND ATTACKERS

The goal of security engineering is to raise the effort involved in an attack to a level where the coast exceed the attacker's gains.

But

Not every attackers is motivated by wish for money.

SECURITY

Software may crash communication networks may go down, hardware components may fail, human operators may make mistakes.

- As long as these failures cannot be directly attributed to some deliberate human action they would not be classified as security issues.

SECURITY

Accidental failures would count as **reliability issues**.

Operating mistakes would be attributed to **usability issues**.

Security is concerned with **intentional failures**.

SECURITY

The root cause of security problems is human nature.

SECURITY MANAGEMENT

Protecting the assets of an organization is the responsibility of management.

Assets Include

- Sensitive information Like product plans, customer records or financial data, and the IT infrastructure of the organization.

SECURITY MANAGEMENT

Not every member has to become a security expert, but all members should know:

- Why security is important for them self and for them organization;
- What is expect of each member;
- Which good practice should they follow.

SECURITY POLICIES

Security policies state what should be protected but may also indicate how this should be done.

MEASURING SECURITY

We can try to measure security by measuring the coast of mounting attacks. We can consider

- The time an attacker has to invest in the attack,
- The expenses the attacker has to incur, and
- The knowledge necessary to conduct the attack.

RISK AND THREAT ANALYSIS

In the Process of risk analysis, values are assigned to assets, Vulnerabilities and threats.

- Risk= Assets * Threats * Vulnerabilities

ASSETS

Assets have to be identified and valued. In an IT system, assets include:

- Hardware: Laptops, Servers, routers, PDA's, mobile phones, smart cards etc. ;
- Software: applications, operating systems, database management systems, source code, object code etc.;
- Data and information: essential data for running and planning your business, design documents, digital content, data about your customers etc.;
- Reputation:

ASSETS

It is important to

- Identify assets
- Valuation of assets

VULNERABILITIES

Vulnerabilities are weaknesses of a system that could be accidentally or intentionally exploited to damage assets. In an IT system, typical vulnerabilities are:

- Accounts with system privileges where the default password, such as ‘MANAGER” has not been changed;
- Program with unnecessary privileges;
- Program with known flaws;
- Weak access control setting on resources, e.g. having kernel memory world writeable;
- Weak firewall configurations that allow access to vulnerable services.

VULNERABILITIES

اكتب في الامتحان

Vulnerabilities scanner provide a systematic and automated way of identifying vulnerabilities.

A vulnerability that allows an attacker to take over a systems account is more critical than a vulnerability that gives access to an unprivileged user account.

THREATS

Threats are actions by adversaries who try to exploit vulnerabilities to damage assets.

استغلال الثغرات الأمنية

There are various ways to identify threats. We can categorize threats by the damage done to assets.

THREATS

for example Microsoft threat model for software security lists the following categories:

1. Spoofing identities
2. Tampering with data
3. Repudiation
4. Information disclosure
5. Denial of services(DoS)
6. Elevation of privilege

THREATS

Then we can identify the source of attacks.

Would the adversary be a member of your organization or an outsider, a contractor or a former member?

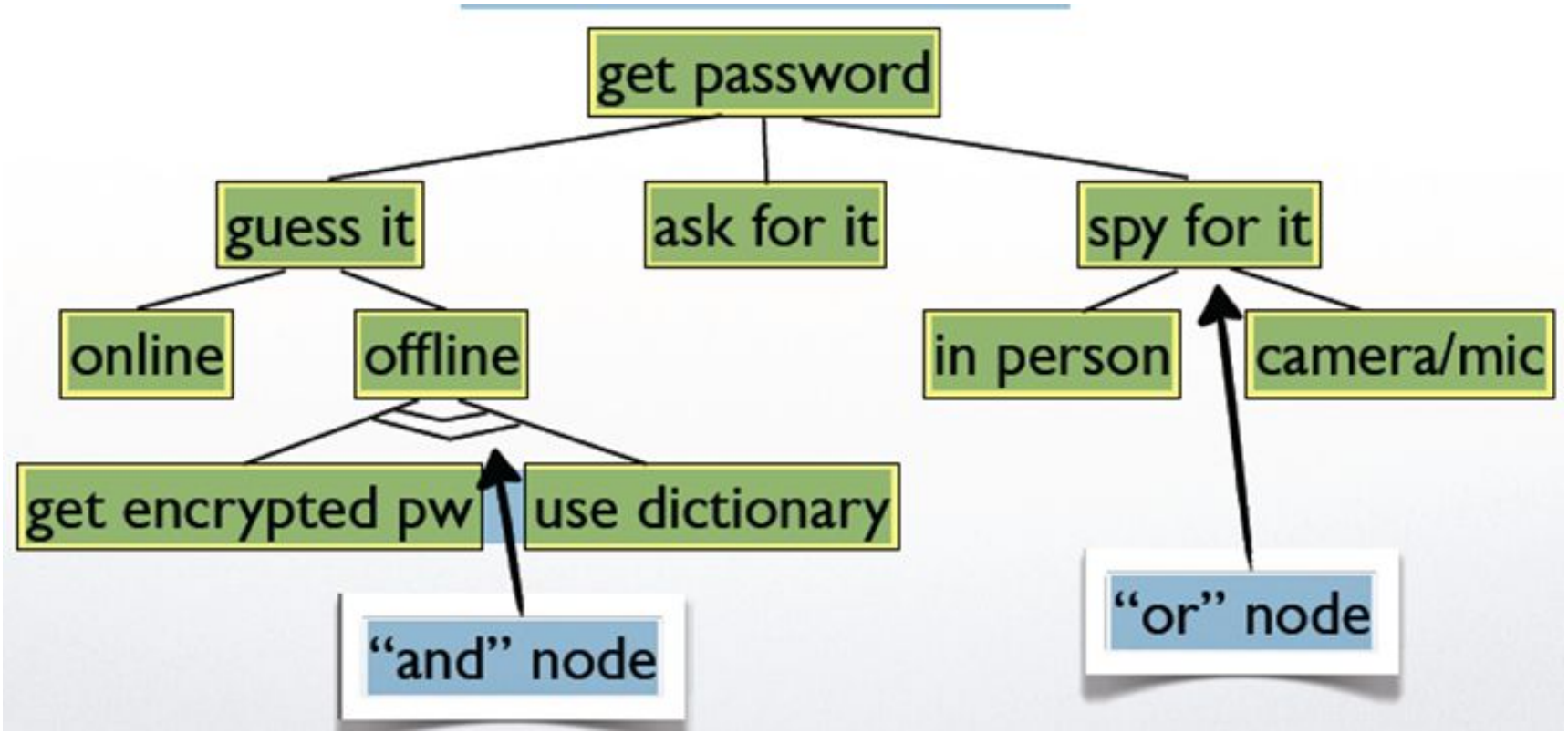
Has the adversary direct access to your systems or is the attack launched remotely?

THREATS

We can also analyze how an attack is executed in detail. An attack may start with innocuous steps, gathering information needed to move on to gain privileges on one machine, from there jump to another machine, until the final target is reached.

To get a fuller picture of potential threats, a forest of attack trees can be constructed:

ASSETS


get password
guess it
ask for it
spy for it
online
offline
in person
camera/mic
get encrypted pw
use dictionary
"and" node
"or" node

SECURITY

- Prevention
- Detection
- Reaction

COMPUTER SECURITY

In a first attempt to capture the notation of computer security, the definition most frequently proposed covers three aspects:

- Confidentiality
- Integrity
- Availability

CONFIDENTIALITY

- **Unauthorized users should not learn sensitive information.**
- **Confidentiality (privacy, secrecy) captures this aspect of computer security.**

INTEGRITY

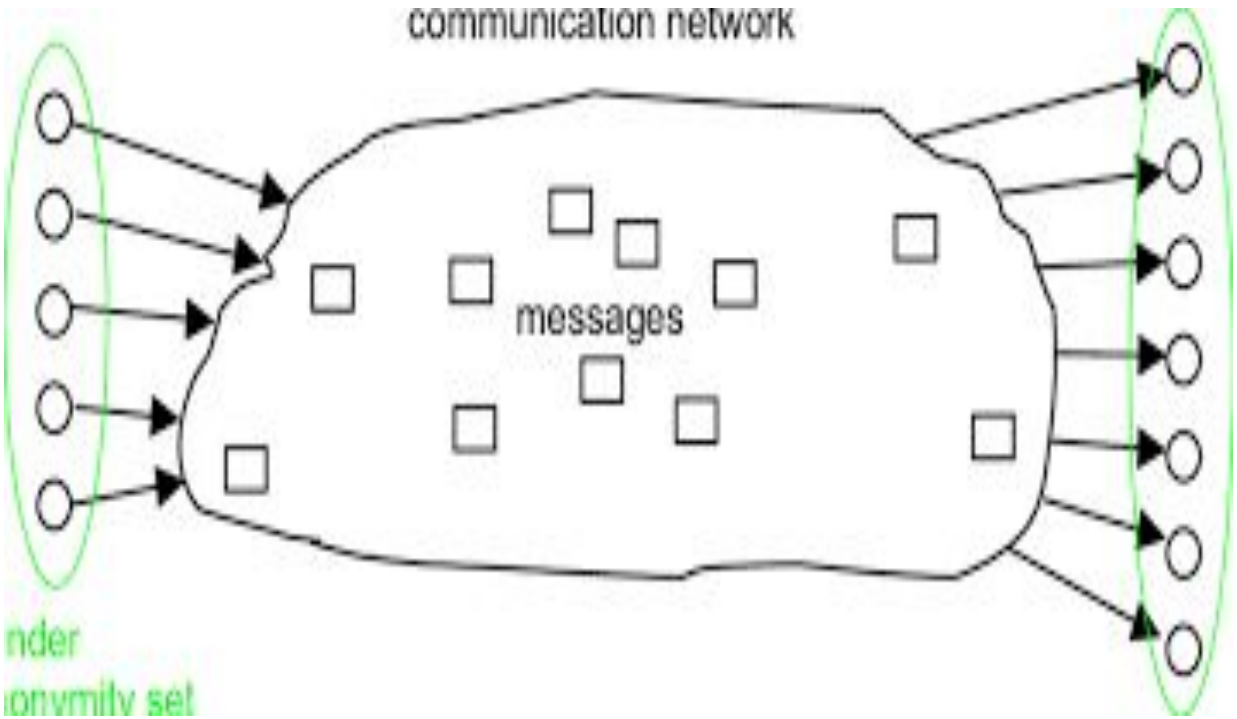
- **Integrity is about making sure that everything is as it is supposed to be.**
- **No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.**

AVAILABILITY

- **The property of being accessible and useable upon demand by authorized entity.**

UNLINKABILITY

- **Two or more items of interest (messages, actions, events, users) are unlikable if an attacker cannot sufficiently distinguish whether they are related or not.**



ANONYMITY

- **A subject (user) is anonymous if it cannot be identified within a given anonymity set of subject.**

ACCOUNTABILITY

- **Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsibility party.**

NON-REPUDIATION

- non-repudiation is related to accountability.
- services provide evidence that a specific action occurred.
- Provide unforgeable evidence that a specific action occurred
- Digital signatures provide non-repudiation.

RELIABILITY

- **Is relating to accidental failures, and safety, relating to the impact of system failures on their environment.**

DEPENDABILITY

- **The property of a computer system such that reliance can justifiably be placed on the service it delivers.**

COMPUTER SECURITY

In computer Security the term

CIA = Confidentiality, Integrity and Availability.