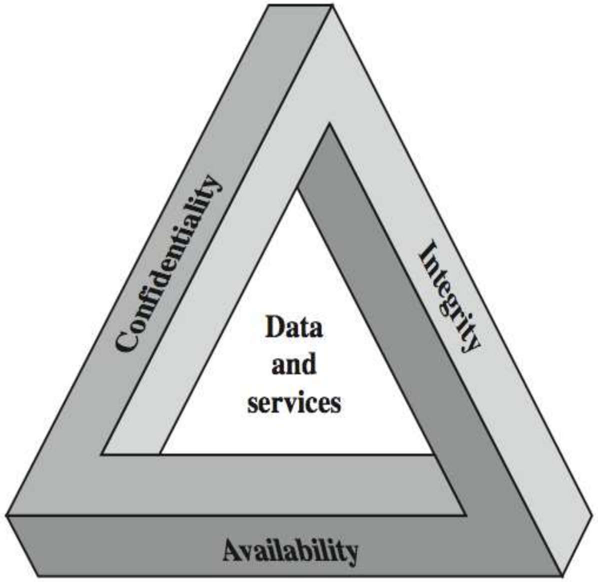
Computer Security

Computer Security Definition

- **Computer security**, also known as cyber **security** or IT **security**, is the protection of **computer** systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.
- It can also be defined as the preservation of information Confidentiality, Integrity and availability.

The Security Requirements Triad



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Computer Security
The protection afforded to an automated information system in order to attain the applicable objectives of preserving the ***integrity***, ***availability*** and ***confidentiality*** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

CIA Triad

- **Confidentiality, integrity and availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.
- In this context, **confidentiality** is a set of rules that limits access to information, **integrity** is the assurance that the information is trustworthy and accurate, and **availability** is a guarantee of reliable access to the information by authorized people.

Security Requirements

- **Confidentiality**
  - Preserving authorized restrictions on information ***access*** and ***disclosure***, including means for protecting personal privacy and proprietary information.
- **Integrity**
  - Guarding against information ***modifications*** or ***destruction***, including ensuring information non-repudiation and authenticity.
- **Availability**
  - Ensuring timely and reliable access to and ***use*** of information

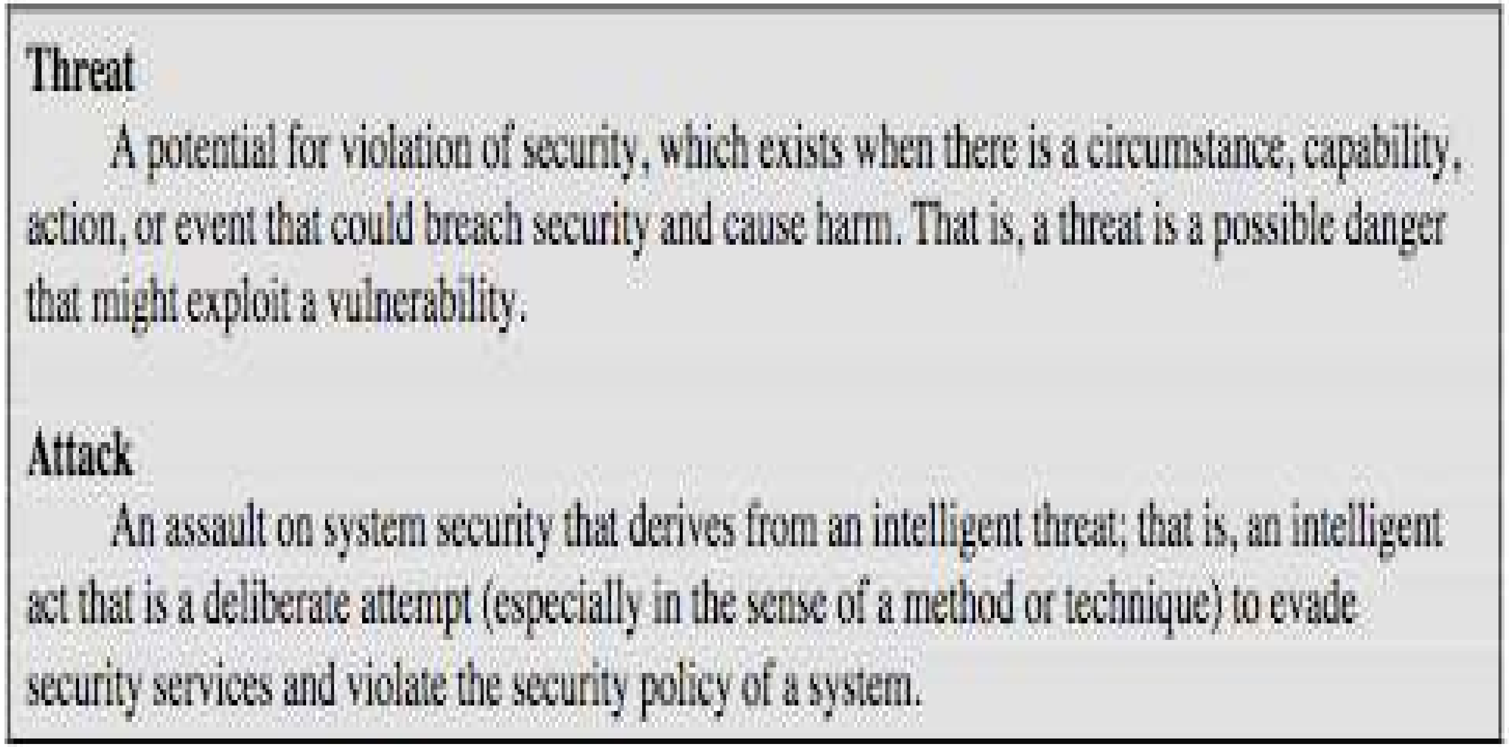
Goals of Computer Security

- Integrity:
  - Guarantee that the data is what we expect
- Confidentiality
  - The information must just be accessible to the authorized people
- Reliability
  - Computers should work without having unexpected problems
- Authentication
  - Guarantee that only authorized persons can access to the resources

Security Attacks, Mechanisms & Services

- **Security *Attack***
  - Any action that compromises the security of information
- **Security *Mechanism***
  - A process / device that is designed to detect, prevent or recover from a security attack.
- **Security *Service***
  - A service intended to counter security attacks, typically by implementing one or more mechanisms.

Threats & Attacks



Threat

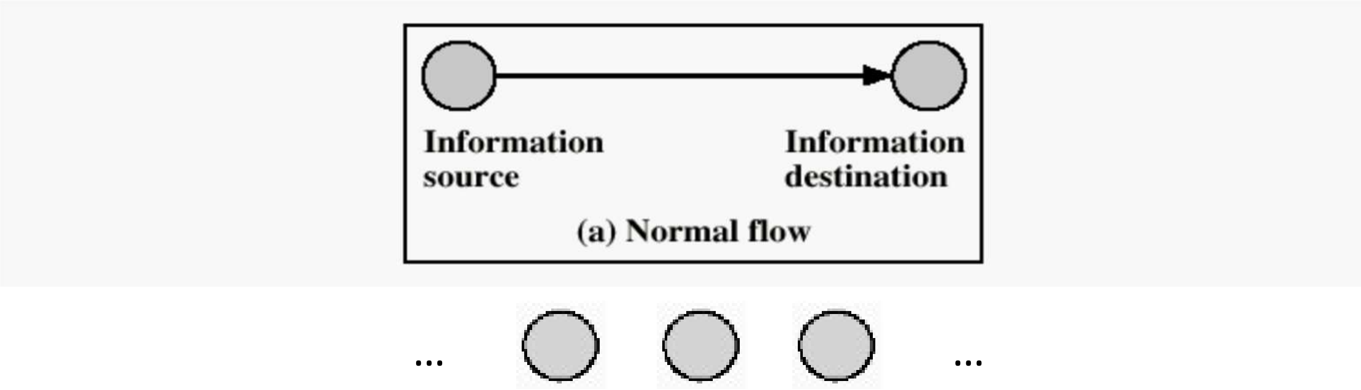
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

… but *threat* and *attack* used nearly interchangeably

Security Threats / Attacks



(a) Normal flow

Security Threats / Attacks

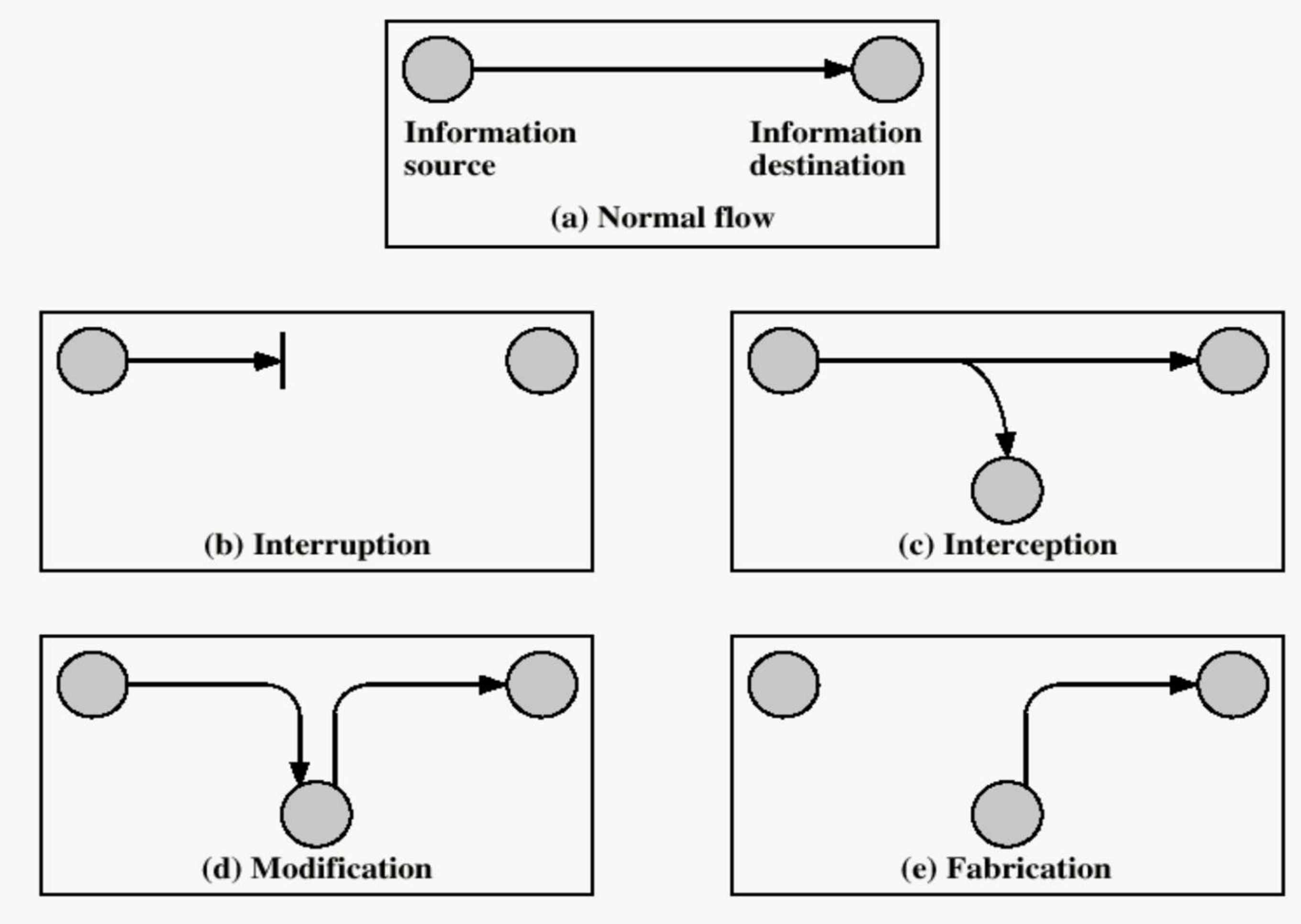
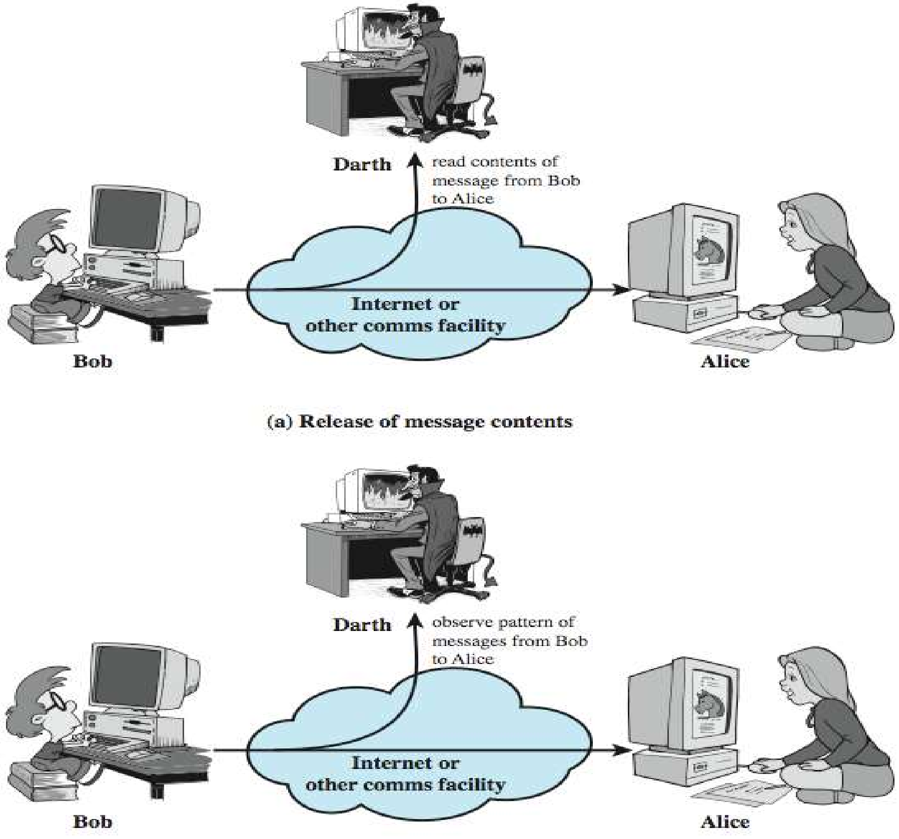


Figure 1.1 Security Threats

Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

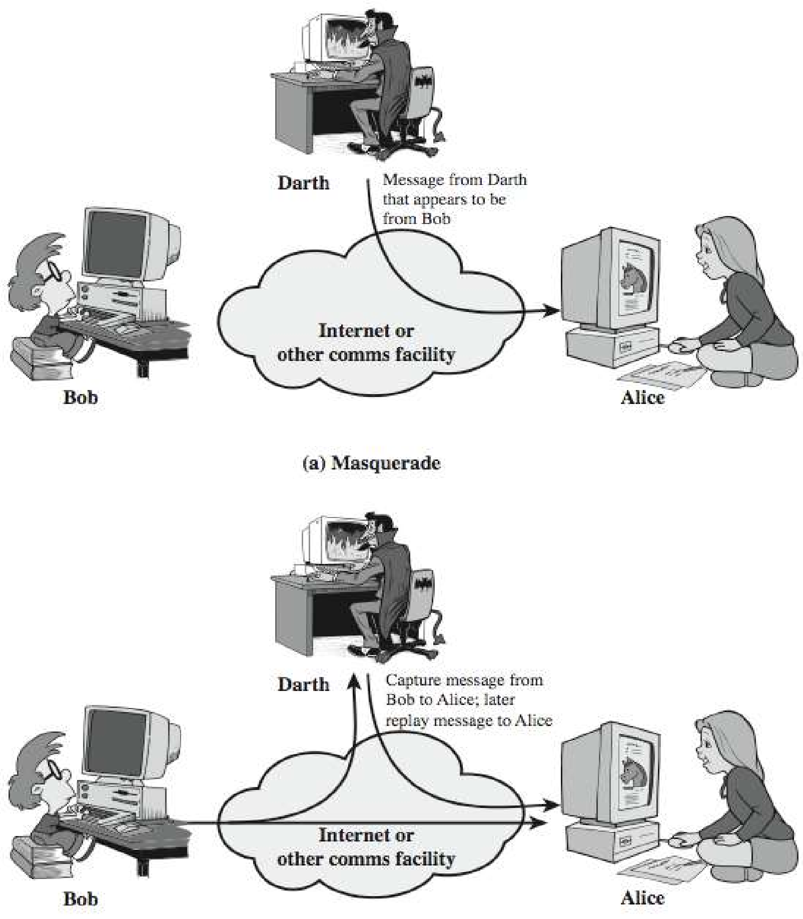
(a) Release of message contents

Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

A **passive attack** is a network **attack** in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

Active Attacks (1)

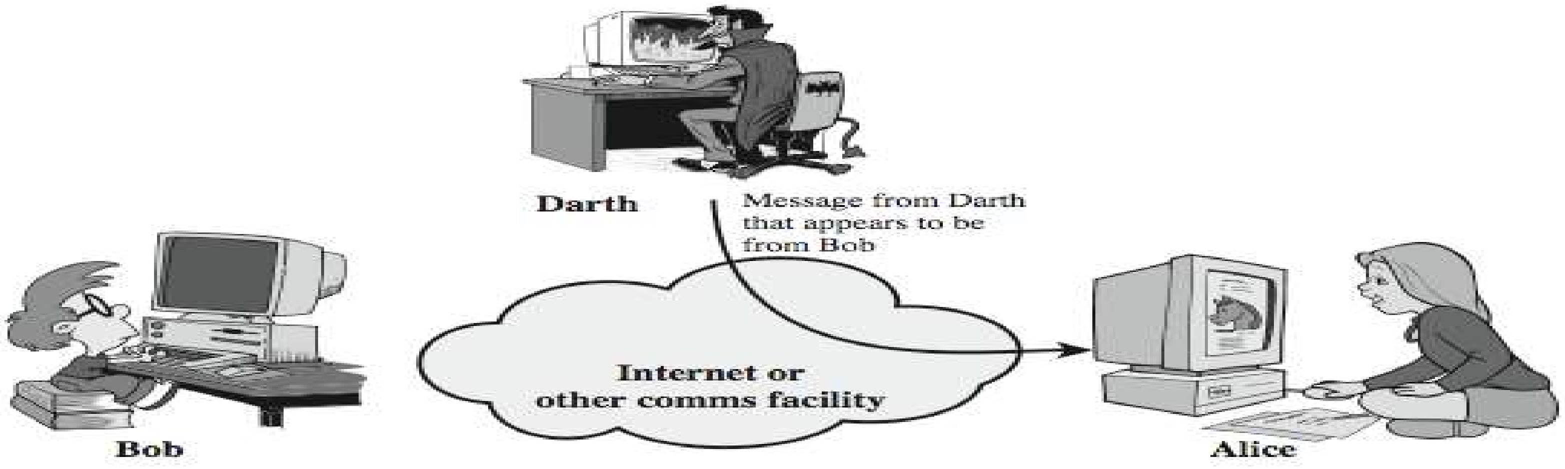

Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice

(a) Masquerade

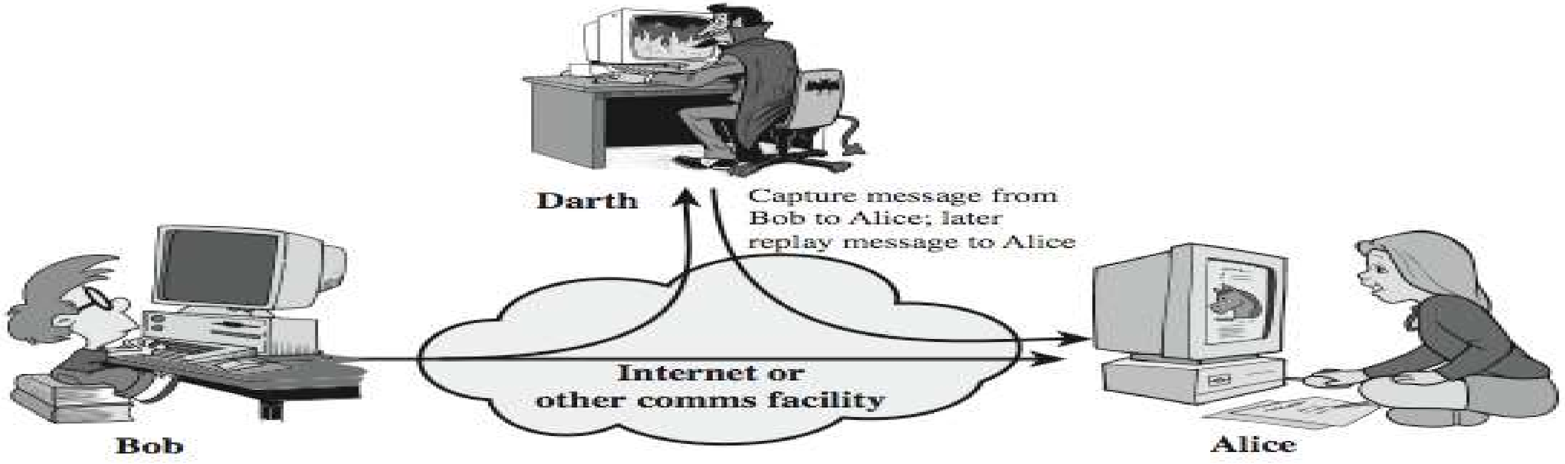
(b) Replay

An **active attack** is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. Types of **active attacks**: In a masquerade **attack**, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.

Active Attacks (1)

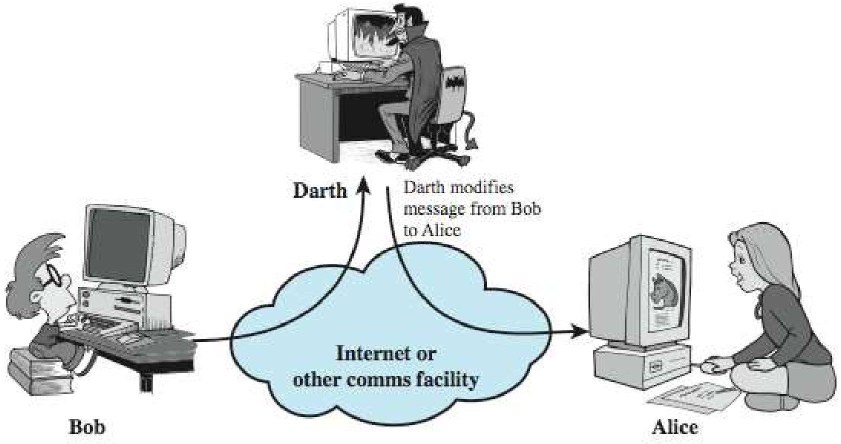

Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

(a) Masquerade


Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice

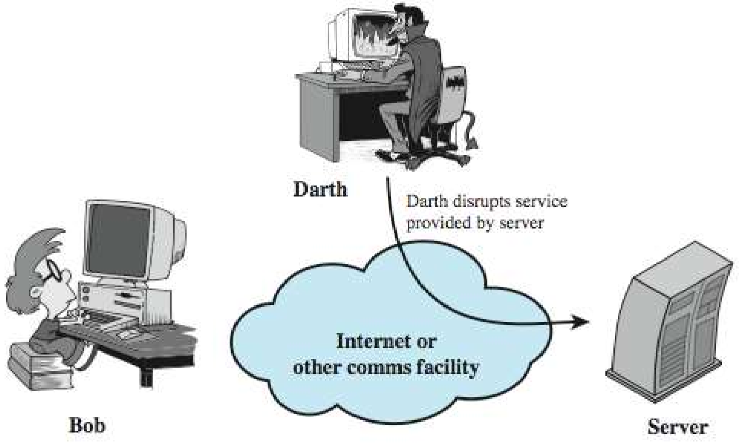
(b) Replay

Active Attacks (2)



Darth modifies message from Bob to Alice

(c) Modification of messages



Darth disrupts service provided by server

(d) Denial of service

Some Types of Computer Attacks

- What are some common attacks?
  - Network Attacks
    - Packet sniffing, man-in-the-middle, DNS hacking
  - Web attacks
    - Phishing, SQL Injection, Cross Site Scripting
  - OS, applications and software attacks
    - Virus, Trojan, Worms, Rootkits, Buffer Overflow
  - Social Engineering
    - (NOT social networking)
- Not all hackers are evil wrongdoers trying to steal your info
  - Ethical Hackers, Consultants, Penetration testers, Researchers

Network Attacks

- Packet Sniffing
  - A **packet** analyzer (also known as a **network** analyzer, protocol analyzer or **packet sniffer**—or, for particular types of **networks**, an Ethernet **sniffer** or wireless **sniffer**) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital **network** or part of a **network**.
  - Internet traffic consists of data “packets”, and these can be “sniffed”
  - Leads to other attacks such as password sniffing, cookie stealing session hijacking, information stealing

Network Attacks

- Man in the Middle
  - Insert a router in the path between client and server, and change the packets as they pass through
- DNS hijacking
  - Insert malicious routes into domain name system (DNS) tables to send traffic for genuine sites to malicious sites

Web Attacks

- Phishing
  - An evil website pretends to be a trusted website
  - Example:
    - You type, by mistake, “mibank.com” instead of “mybank.com”
    - mibank.com designs the site to look like mybank.com so the user types in their info as usual
    - BAD! Now an evil person has your info!

Web Attacks - Injection Flaws (SQL Injection)

– What is SQL Injection

- SQL injection is the actual injection of SQL commands into web applications through user input fields.
- When an application uses internal SQL commands and you also have user input capabilities (like a login screen), SQL commands can be injected that can create, read, update, or delete any data available to the application.

– Prevention

- You can put tight constraints on user inputs. But the best method of preventing SQL injection is to avoid the use of dynamically generated SQL in your code. Instead use stored or canned procedures.
- And then again, run a scan to make sure your application is not vulnerable to SQL injections.

Web Attacks - Cross Site Scripting

- What is Cross Site Scripting? Cross Site Scripting
  - Writing a complex Javascript program that steals data left by other sites that you have visited in same browsing session.
    - In it's simplest form, it's a process that can occur anywhere a web application uses input from a malicious user to generate output without validating or encoding the input.
    - During a Cross Site Scripting attack, a malicious source sends a script that is executed by the end user's browser. It allows attackers to embed code from one webpage into another webpage by changing its HTML code.
    - It's been used to deface web sites, conduct phishing attacks, or it can take over a user's browser and force them to execute commands they're unaware of.
    - Cross Site Scripting attacks usually come in the form of JavaScript however, any active content poses a potential danger.
  - Prevention
    - Validate the users input against what is expected
    - Encode user supplied output
    - After you believe you've done the right things during code development, inspect your code with a scan.

Malicious File Execution

– What is Malicious File Execution

- When Developers program applications to use input files provided by the user and the bad guy is the one entering the file, a malicious file is executed unknowingly, thus we have malicious file execution.
- Malicious file execution attacks can occur anytime the application accepts filenames or files from a users.
- When these files are executed, they can be used to do just about anything from stealing data to taking over the entire system.

– Prevention

- Strongly validate user input using "accept known good" as a strategy, or isolate incoming files and check them legitimacy before executing them.
- Disable certain PHP commands.

Virus

- Definition
  - Piece of code that automatically reproduces itself. It’s attached to other programs or files, but requires user intervention to propagate.
- Infection (targets/carriers)
  - Executable files
  - Boot sectors
  - Documents (macros), scripts (web pages), etc.
- Propagation

  is made by the user. The mechanisms are storage elements, mails, downloaded files or shared folders

Worm

- Definition
  - Piece of code that automatically reproduces itself over the network. It doesn’t need the user intervention to propagate (autonomous).
- Infection
  - Via buffer overflow, file sharing, configuration errors and other vulnerabilities.

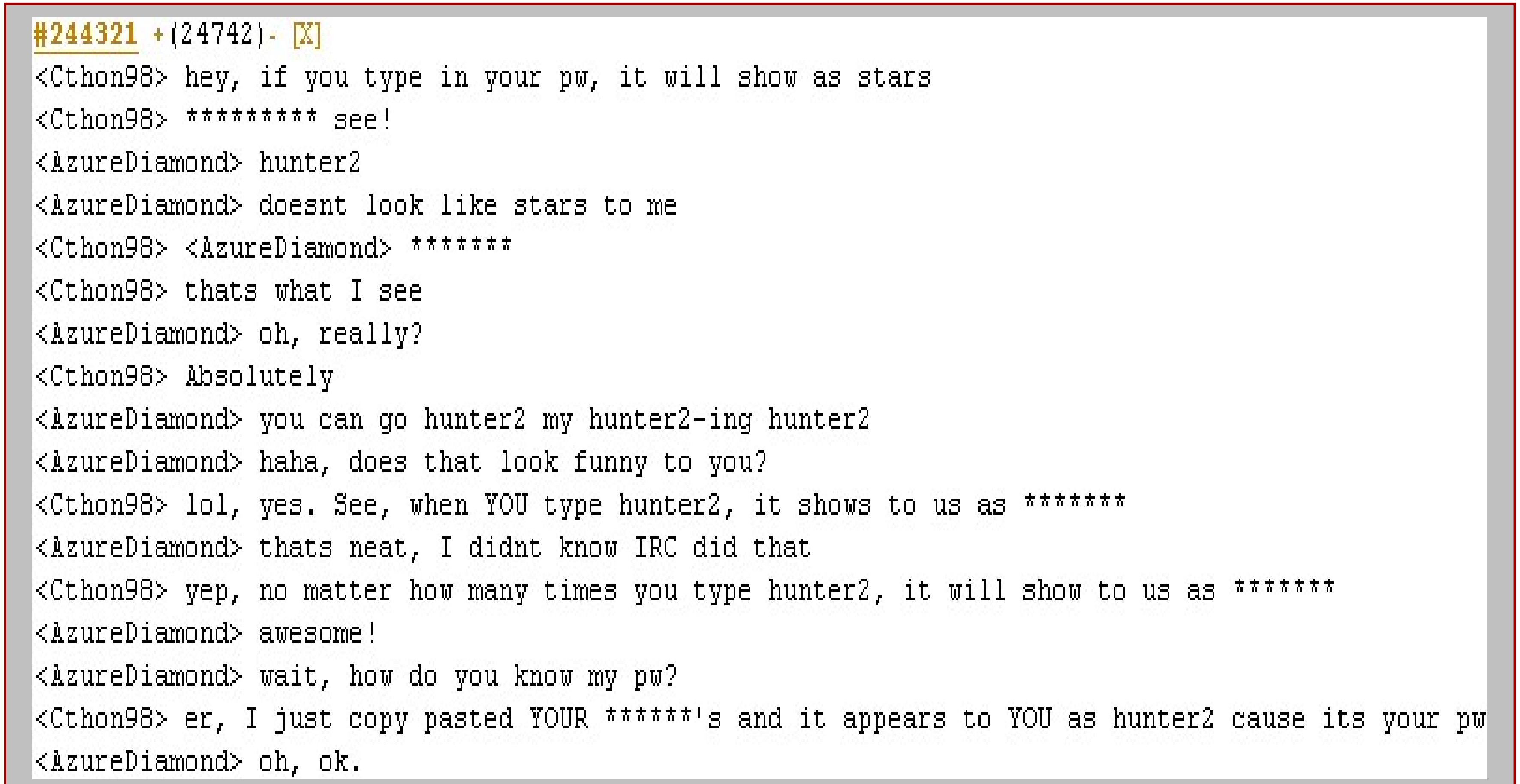
A **buffer overflow**, or **buffer** overrun, is an anomaly where a program, while writing data to a **buffer**, overruns the **buffer's** boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

- Target selection algorithm
  - Email addresses, DNS, IP, network neighborhood
- Payload
  - Malicious programs
  - Backdoor, DDoS agent, etc.

Backdoor, trojan, rootkits

- Goal
  - The goal of *backdoor*, *Trojan* and *rootkits* is to take possession of a machine subsequently through an infection made via a backdoor.
- Backdoor
  - A *backdoor* is a program placed by a black-hacker that allows him to access a system. A *backdoor* have many functionalities such as keyboard-sniffer, display spying, etc.
- Trojan
  - A *Trojan* is a software that seems useful or benign, but is actually hiding a malicious functionality.
- Rootkits (the ultimate virus)
  - *Rootkits* operate like *backdoor* and *Trojan*, but also modify existing programs in the operating system. That allows a black-hacker to control the system without being detected. A *rootkit* can be in user-mode or in kernel-mode.

Social Engineering



```
#244321 +(24742)- [X]
<Cthon98> hey, if you type in your pw, it will show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
<AzureDiamond> you can go hunter2 my hunter2-ing hunter2
<AzureDiamond> haha, does that look funny to you?
<Cthon98> lol, yes. See, when YOU type hunter2, it shows to us as *******
<AzureDiamond> thats neat, I didnt know IRC did that
<Cthon98> yep, no matter how many times you type hunter2, it will show to us as *******
<AzureDiamond> awesome!
<AzureDiamond> wait, how do you know my pw?
<Cthon98> er, I just copy pasted YOUR ******'s and it appears to YOU as hunter2 cause its your pw
<AzureDiamond> oh, ok.
```

*http://bash.org/?244321

Social Engineering

- Why is this social engineering?
  - Manipulating a person or persons into divulging confidential information
- I am not dumb, so does this really apply to me?
  - YES! Attackers are ALSO not dumb.
  - Social Engineers are coming up with much better and much more elaborate schemes to attack users.
  - Even corporate executives can be tricked into revealing VERY secret info
- What can I do to protect myself?
  - NEVER give out your password to ANYBODY.
  - Any system administrator should have the ability to change your password without having to know an old password

Password Attacks

- Password Guessing
  - Ineffective except in targeted cases
- Dictionary Attacks
  - Password are stored in computers as hashes, and these hashes can sometimes get exposed
  - Check all known words with the stored hashes
- Rainbow Tables
  - Trade off storage and computation – uses a large number of pre-computed hashes without having a dictionary
  - Innovative algorithm, that can find passwords fast!
    - e.g. 14 character alphanumeric passwords are found in about 4-10 minutes of computing using a 1GB rainbow table

Computer Security Issues

- **Vulnerability** is a point where a system is susceptible to attack.
- A **threat** is a possible danger to the system. The danger might be a person (a system cracker or a spy), a thing (a faulty piece of equipment), or an event (a fire or a flood) that might exploit a vulnerability of the system.
- **Countermeasures** are techniques for protecting your system

Vulnerabilities in Systems

- How do viruses, rootkits enter a system?
  - Even without the user doing something “stupid”
- There are vulnerabilities in most software systems.
  - Buffer Overflow is the most dangerous and common one. A **buffer overflow**, or **buffer** overrun, is an anomaly where a program, while writing data to a **buffer**, overruns the **buffer's** boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.
- How does it work?
  - All programs run from memory.
  - Some programs allow access to reserved memory locations when given incorrect input.
  - Hackers find out where to place incorrect input and take control.
  - Easy to abuse by hackers, allows a hacker complete access to all resources

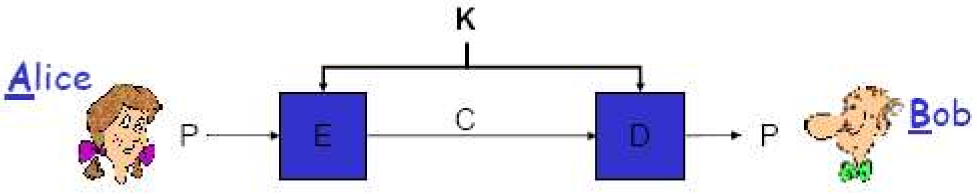
How can you achieve security?

- Many techniques exist for ensuring computer and network security
  - Cryptography
  - Secure networks
  - Antivirus software
  - Firewalls
- In addition, users have to practice “safe computing”
  - Not downloading from unsafe websites
  - Not opening attachments
  - Not trusting what you see on websites
  - Avoiding Scams - **spam** is unsolicited junk email sent indiscriminately in bulk, often for commercial purposes.

Cryptography

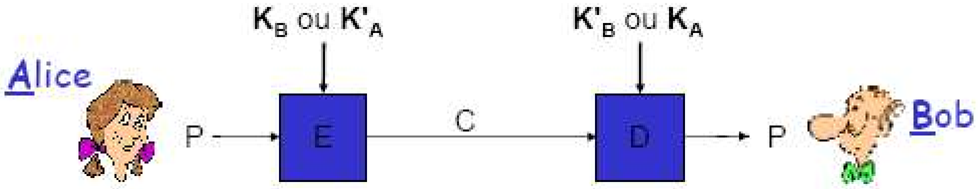
- Simply – secret codes
- Encryption
  - Converting data to unreadable codes to prevent anyone form accessing this information
  - Need a “key” to find the original data – keys take a few million-trillion years to guess
- Public keys
  - An ingenious system of proving you know your password without disclosing your password. Also used for digital signatures
  - Used heavily in SSL connections
- Hashing
  - Creating fingerprints of documents

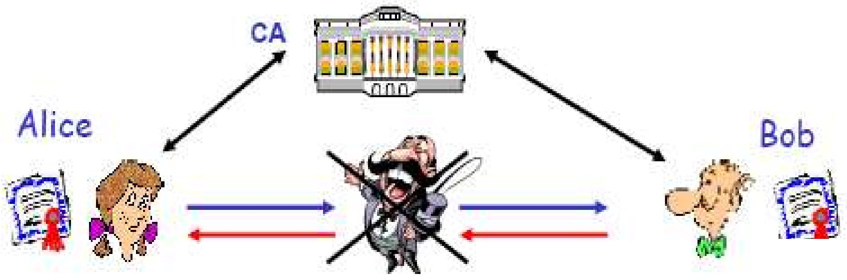
Cryptographic Protocols



Symmetric encryption

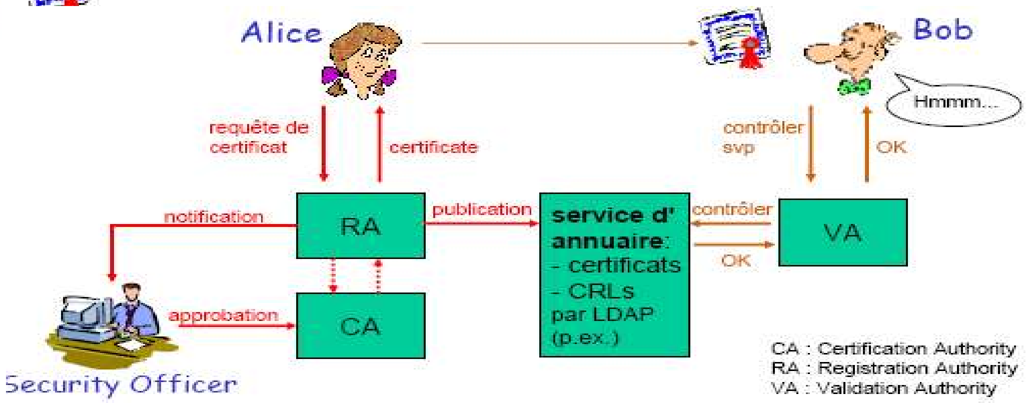
Asymmetric encryption





Authentication

Public Key Infrastructure


Alice
Bob
Hmmm...
requête de certificat
certificate
contrôler svp
OK
notification
RA
publication
service d' annuaire: - certificats - CRLs par LDAP (p.ex.)
contrôler
OK
VA
approbation
CA
Security Officer
CA : Certification Authority
RA : Registration Authority
VA : Validation Authority

Cryptography

- **Symmetric encryption** is the oldest and best-known technique. A **secret key**, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet.
- **Asymmetric cryptography**, also known as public key **cryptography**, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (**asymmetric**). One key in the pair can be shared with everyone; it is called the **public key**.

Firewall

- Firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication