BASIC CONCEPTS IN COMPUTER SECURITY

T. Mathanarupan

WHAT IS COMPUTER SECURITY?

- Computer security is refers to techniques for ensuring that **data stored** in a computer cannot be read or compromised by any individuals without authorization.
- Most computer security measures involve data **encryption** and **passwords**.
- The purpose of computer security is to device ways to prevent the weaknesses from being exploited.

WHAT IS COMPUTER SECURITY?

- We are addressing three important aspects of any computer-related system such as
- **confidentiality,**
- **integrity,**
- **availability**.

Computer security: Protection of the items you value- assets of a computer or computer system.

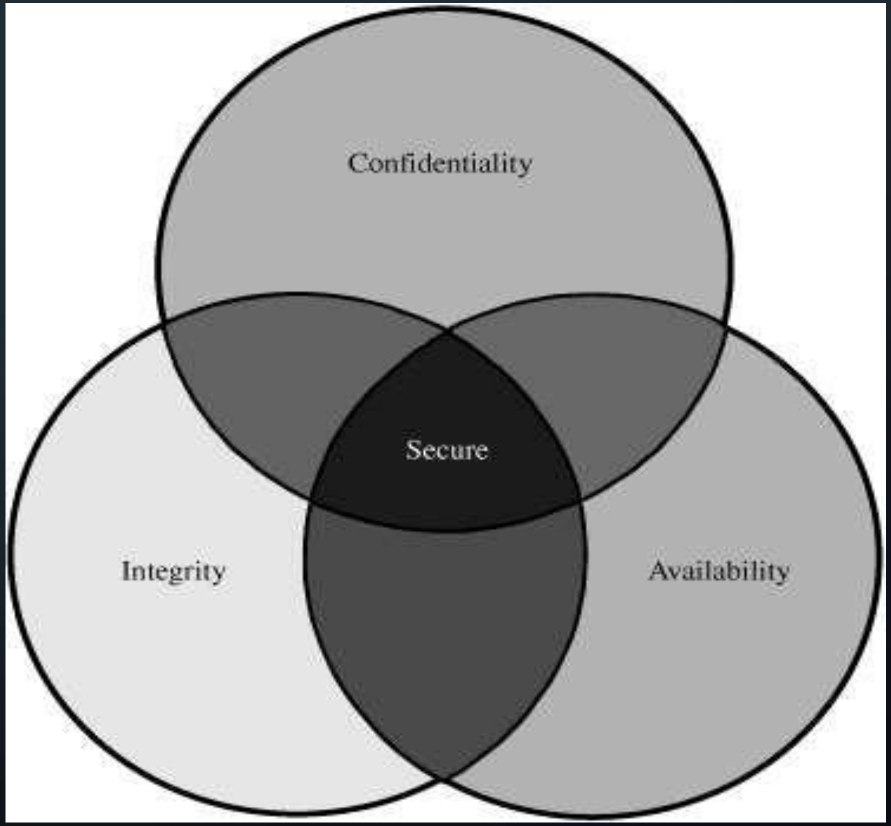
There are many types of assets, hardware, software, data, people, processes, or combinations of these.

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

WHAT IS COMPUTER SECURITY?

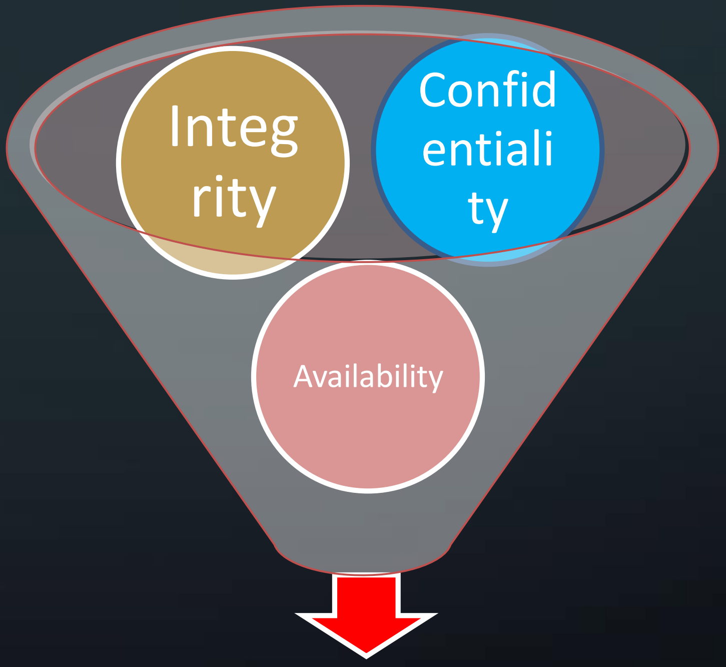
- These are the three goals in computing Security.

1. **Confidentiality**
2. **Integrity**
3. **Availability**



The Security Triad

Availability, **integrity, confidentiality** together (and rearranged), the properties are called the **C-I-A triad** or the **security triad**.



Information Security

THREE GOALS IN COMPUTING SECURITY

- **Confidentiality:** ensures that computer-related assets are **accessed** only by authorized parties. Confidentiality is sometimes called **secrecy** or **privacy**.
- **Integrity:** it means that assets can be **modified** only by authorized parties or only in authorized ways.
- **Availability**: it means that assets are **accessible** to authorized parties at appropriate times.

THREE GOALS IN COMPUTING SECURITY

- One of the challenges in building a secure system is finding the **right balance** among the goals, which often conflict.

Definitions

Computer Security - generic name for the collection of tools designed to protect data and to prevent hackers

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Threat – a potential damage that can be materialized through some flaw in the system

Vulnerability – a weak point in a system where a threat can sneak in

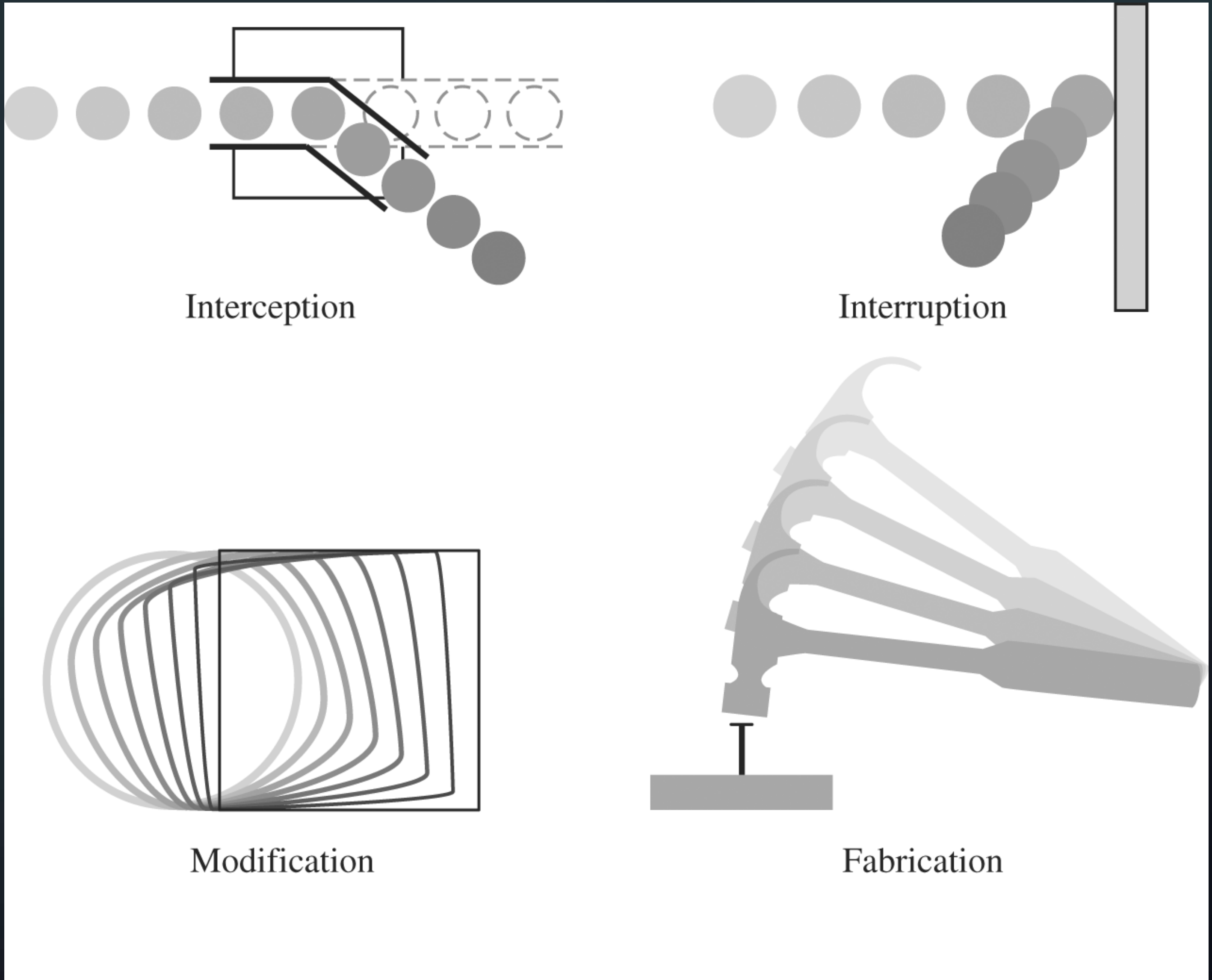
Risk – the probability of a threat being materialized by exploiting a vulnerability

Control – any procedure that is in place to assure security of a system

THREATS

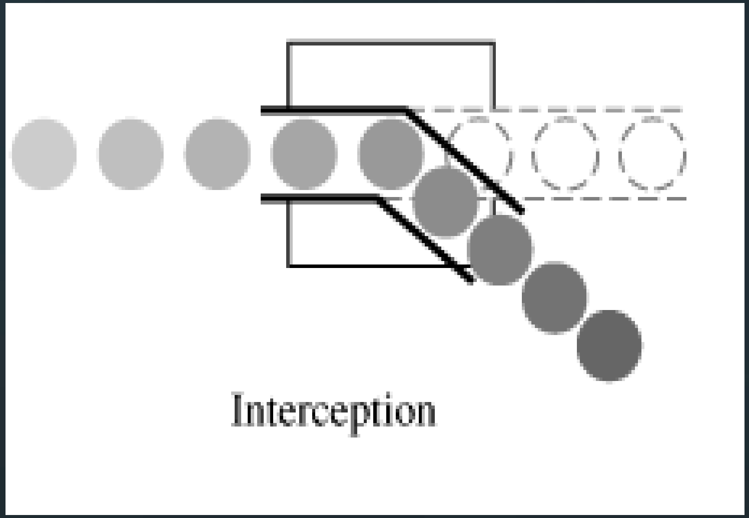
- A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.
- There are many threats to a computer system, including **human-initiated** and **computer-initiated** ones.
- A threat is blocked by control of a vulnerability.
- We can view any threat as being one of four

Threats



Pfleeger/Pfleeger Fig. 01-02

interception



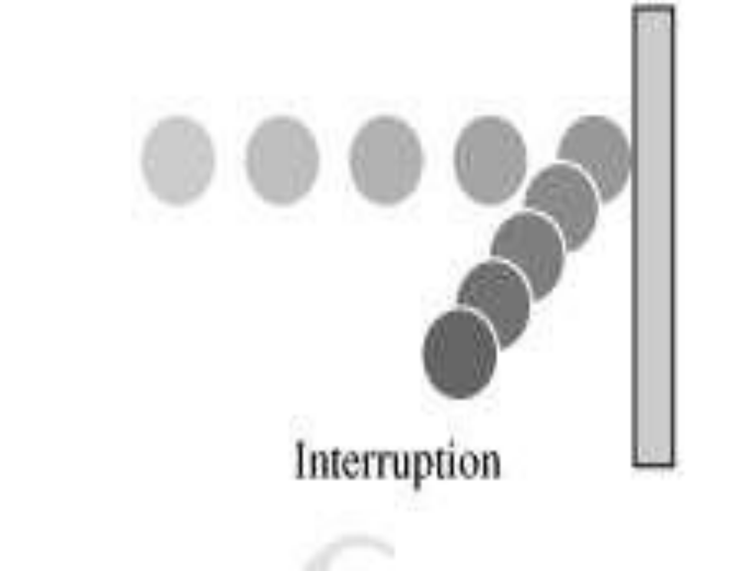
- An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system.

Ex:

- Illegal copying of program or data
- Network wiretapping

interruption

- In an **interruption** is an asset of the system becomes lost, unavailable, or unusable.

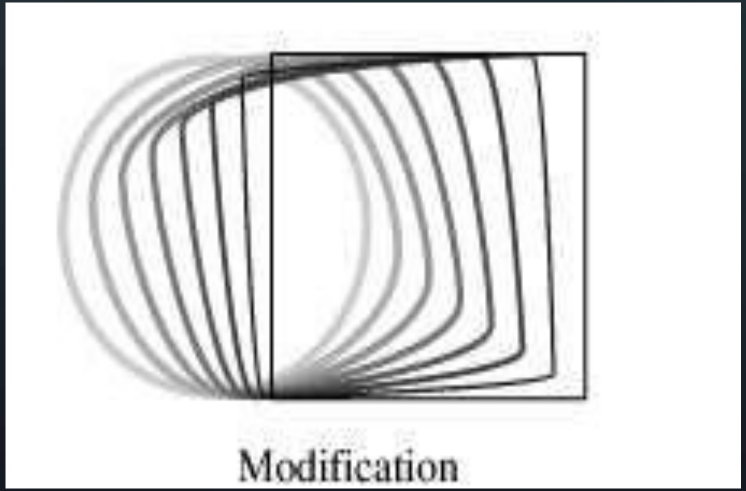


Ex:

- ➢ Erasure of a program or data file
- ➢ malfunction of an operating system (can’t find a disk file.)

modification

- If an unauthorized party not only accesses but tampers with an asset, is called as a **modification**.

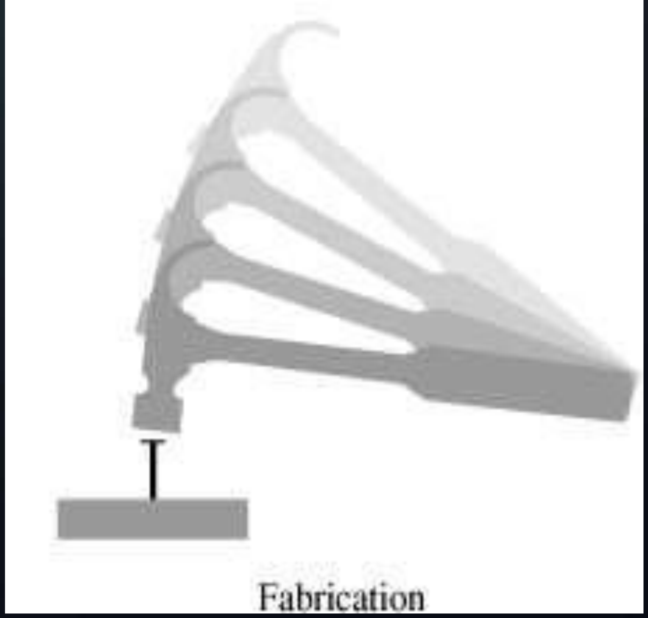


Ex:

- ➢ Change the values in a database
- ➢ Alter a program to performs deferent computation
- ➢ modify data being transmitted

fabrication

- An unauthorized party might create a **fabrication** of counterfeit objects on a computing system.
- The uninvited may insert spurious transactions to a network communication system or add records to an existing data



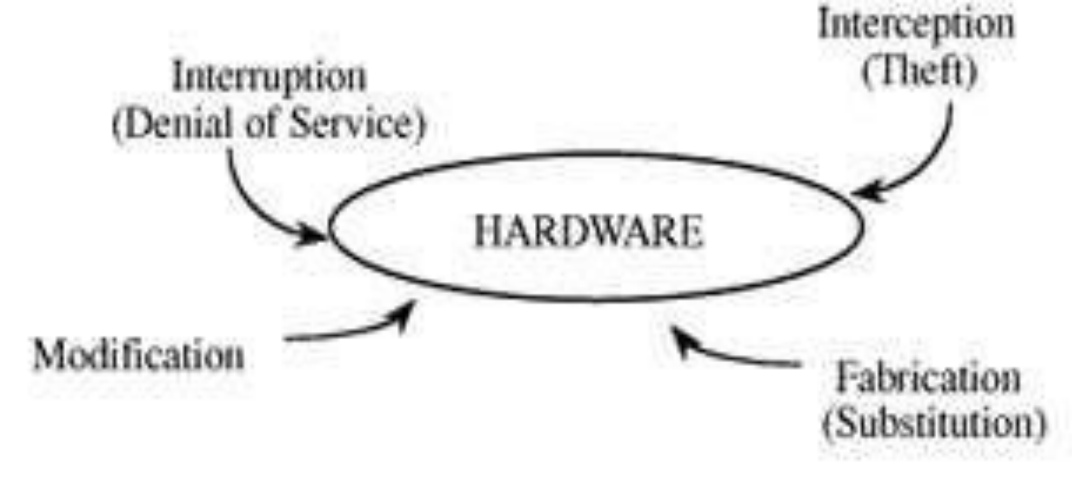
VULNERABILITY

- Vulnerability is a **weakness** in the security system.
- Weaknesses can appear in any element of a computer, both in the **hardware, operating system,** and **the software**.

The types of vulnerabilities we might find as they apply to the assets of **hardware, software,** and **data.**

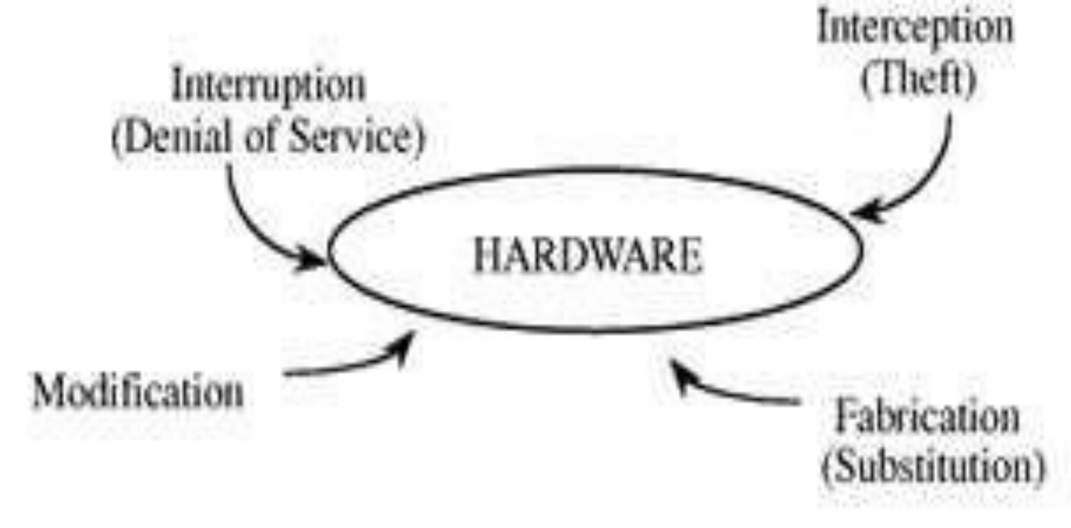
HARDWARE VULNERABILITY

- Hardware is more visible than software, largely because it is composed of **physical objects**.
- it is rather simple to attack by adding devices, changing them, removing them, intercepting the traffic to them, or flooding them with traffic until they can no longer function.



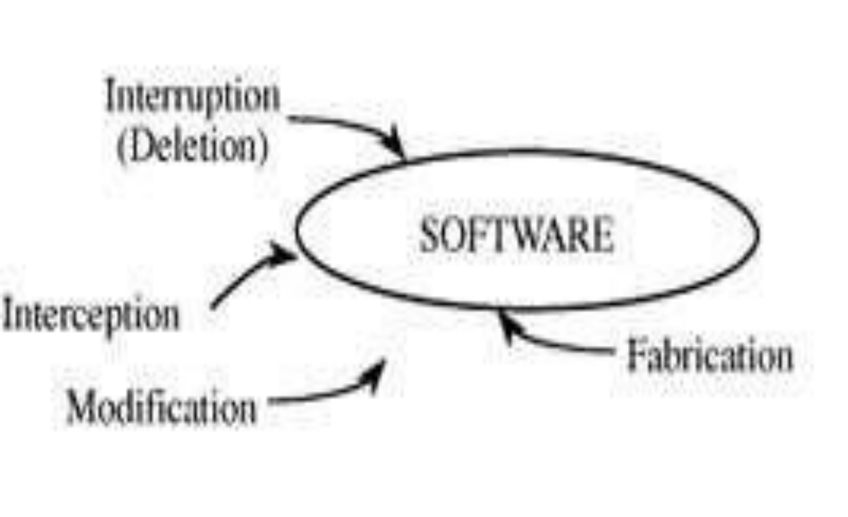
HARDWARE VULNERABILITY

- other ways that computer hardware can be attacked physically.
- Computers have been liquid with water, burned, frozen, gassed and electric shock with power.



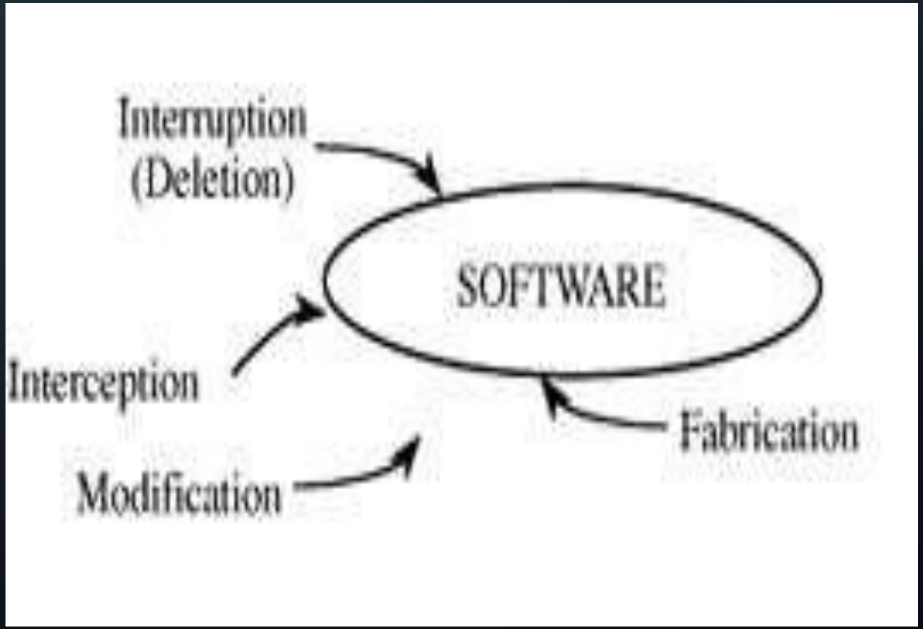
SOFTWARE VULNERABILITIES

- Software can be replaced, changed, or destroyed or it can be modified, deleted or misplaced accidentally. Whether intentional or not these attacks exploit the software's vulnerabilities.



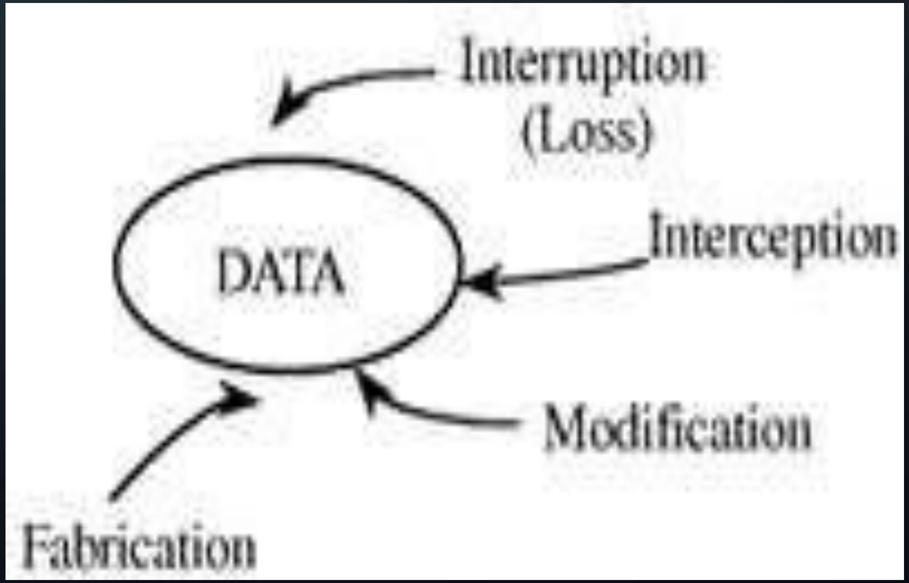
SOFTWARE VULNERABILITIES

- Sometimes, the attacks are obvious, as when the software no longer runs. More subtle are attacks in which the software has been altered but seems to run normally.



DATA VULNERABILITY

- a data attack is a more widespread and serious problem than either a hardware or software attack.
- data items have greater public value than hardware and software because more people know how to use or interpret data.



ATTACKS

- A human who exploits a vulnerability crime an attack on the system. An attack can also be launched by another system, as when one
- system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function.

ATTACKS

- Unfortunately, we have seen this type of attack frequently, as denial-of-service attacks flood

  servers with more messages than they can handle.

CONTROL

- The control is an action, device, procedure or technique that removes or reduces a vulnerability.
- We use a control as a protective measure.
- There are so many ways to control.

Services, Mechanisms, Attacks

- need systematic way to define requirements
- consider three feature of information security:

1. **security attack**
2. **security mechanism**
3. **security service**

Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents

Eg: have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**

Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

OSI Security Architecture

- Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

Security Services (X.800)

Authentication - assurance that the communicating entity is the one claimed

Access Control - prevention of the unauthorized use of a resource

Data Confidentiality –protection of data from unauthorized disclosure

Data Integrity - assurance that data received is as sent by an authorized entity

Non-Repudiation - protection against denial by one of the parties in a communication

Security Mechanisms (X.800)

specific security mechanisms:

digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

pervasive security mechanisms:

trusted functionality, security labels, event detection, security audit trails, security recovery

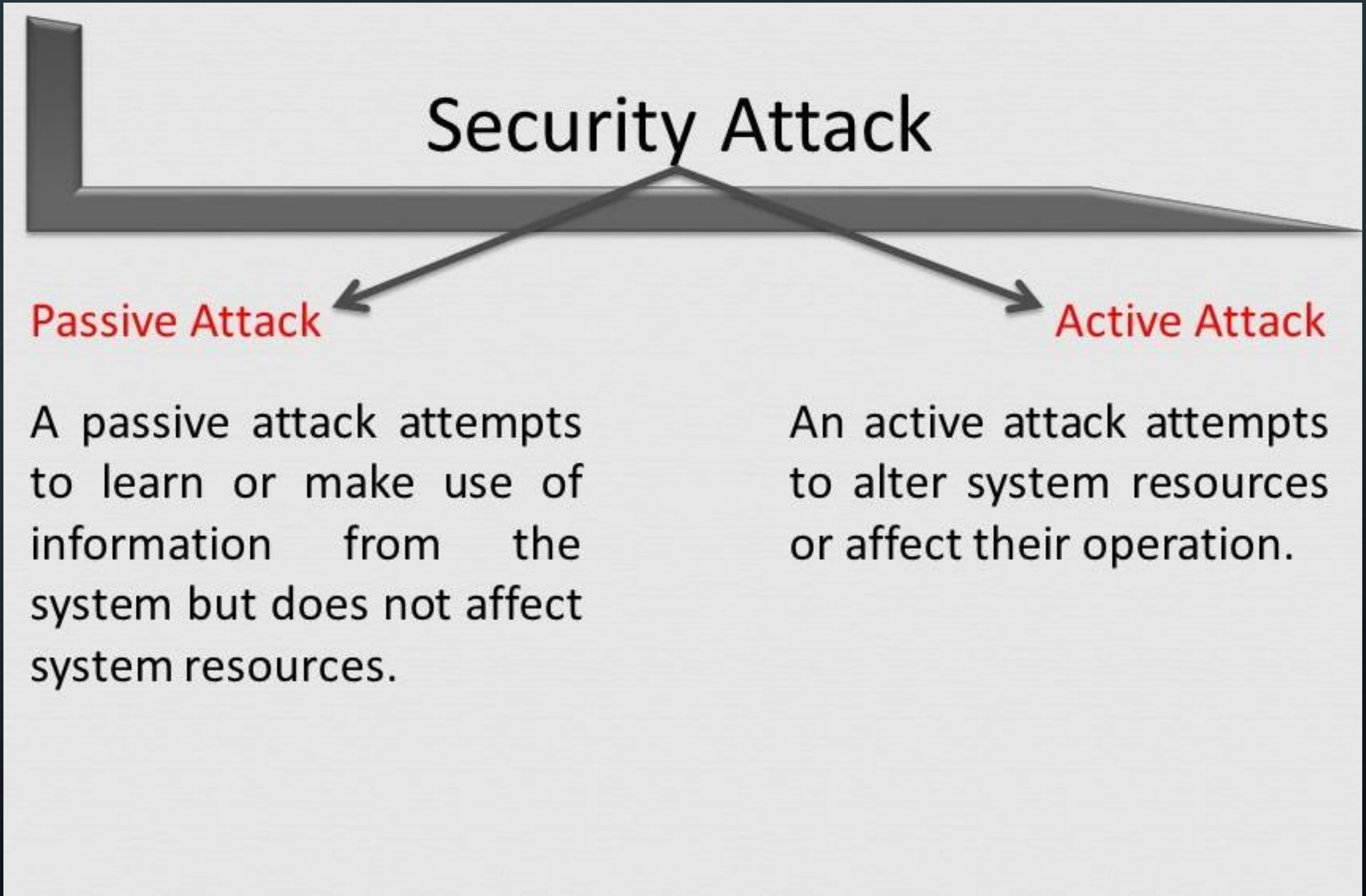
Classify Security Attacks as

passive attacks - monitoring of, transmissions to:

- obtain message contents,
- monitor traffic flows

active attacks – modification of data stream to:

- replay previous messages
- modify messages in transit
- denial of service



Security Attack

Passive Attack

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

Active Attack

An active attack attempts to alter system resources or affect their operation.

HOW TO SECURE THE COMPUTER

There are two ways

1. **Physical secure**
2. **Other secure methods**

PHYSICALLY SECURE COMPUTERS

- Obtain physical computer locks for all your computers

PHYSICALLY SECURE COMPUTERS

- Attach mobile proximity alarms to your computers.

PHYSICALLY SECURE COMPUTERS

- **Store computers in an area with secure access.**
- Or place the computers in a locked room

PHYSICALLY SECURE COMPUTERS IN YOUR COLLEGE

- Station security guards at entry points to the college building.

PHYSICALLY SECURE COMPUTERS IN YOUR COLLEGE

- **Verify windows and doors are properly locked after office hours.**

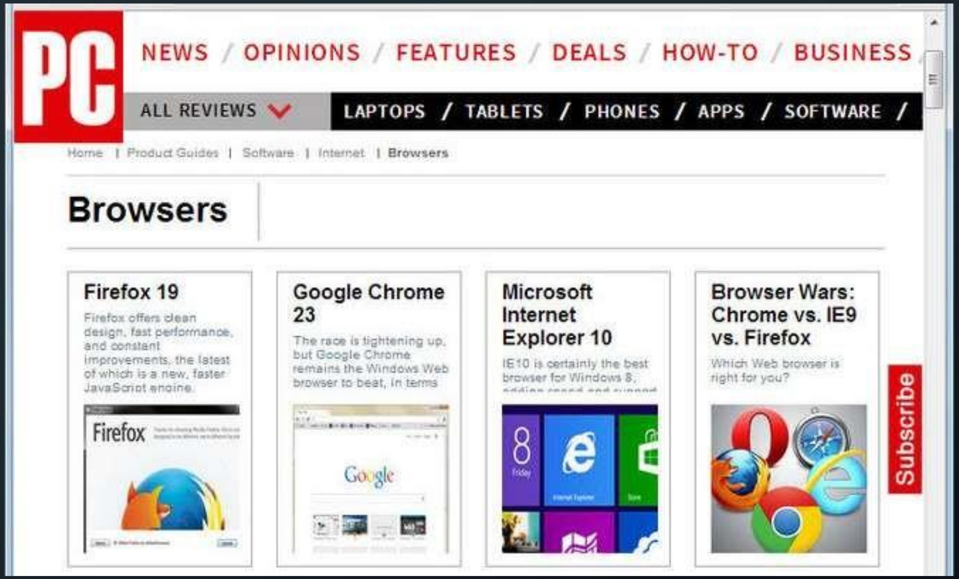
SECURE THE COMPUTER

- Choose a good secur ed operating system

Mac vs. Windows: Your Best Arguments

SECURE THE COMPUTER

- **Choose a web browser** based on its security and vulnerabilities because most malware will come through via your web browser


PC
NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS
ALL REVIEWS
LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE /
Home | Product Guides | Software | Internet | Browsers
Subscribe

Browsers

Firefox 19

Firefox offers clean design, fast performance, and constant improvements, the latest of which is a new, faster JavaScript engine.

Google Chrome 23

The race is tightening up, but Google Chrome remains the Windows Web browser to beat, in terms

Microsoft Internet Explorer 10

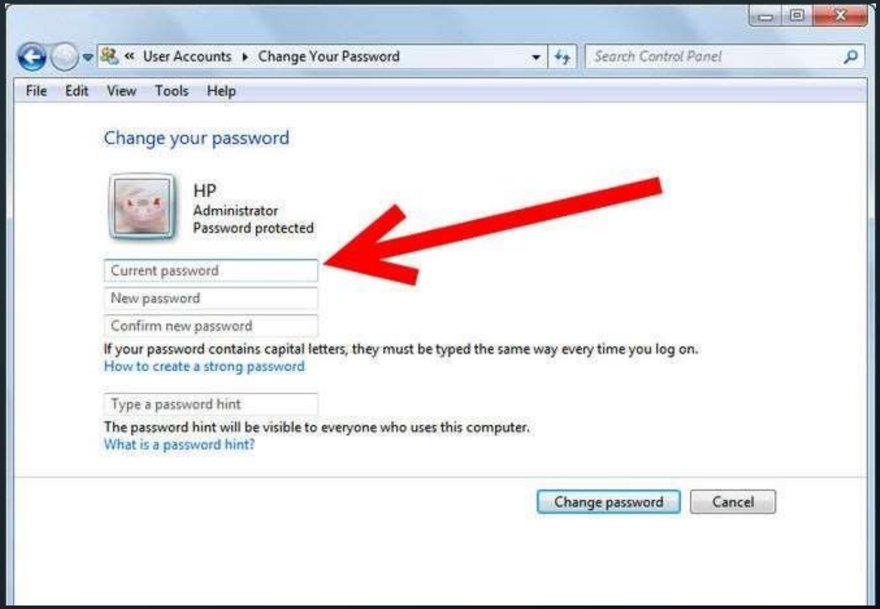
IE10 is certainly the best browser for Windows 8,

Browser Wars: Chrome vs. IE9 vs. Firefox

Which Web browser is right for you?

SECURE THE COMPUTER

- **When setting up**, use strong passwords in your user account, router account etc. Hackers may use dictionary attacks and brute force attacks.



Change your password

If your password contains capital letters, they must be typed the same way every time you log on.

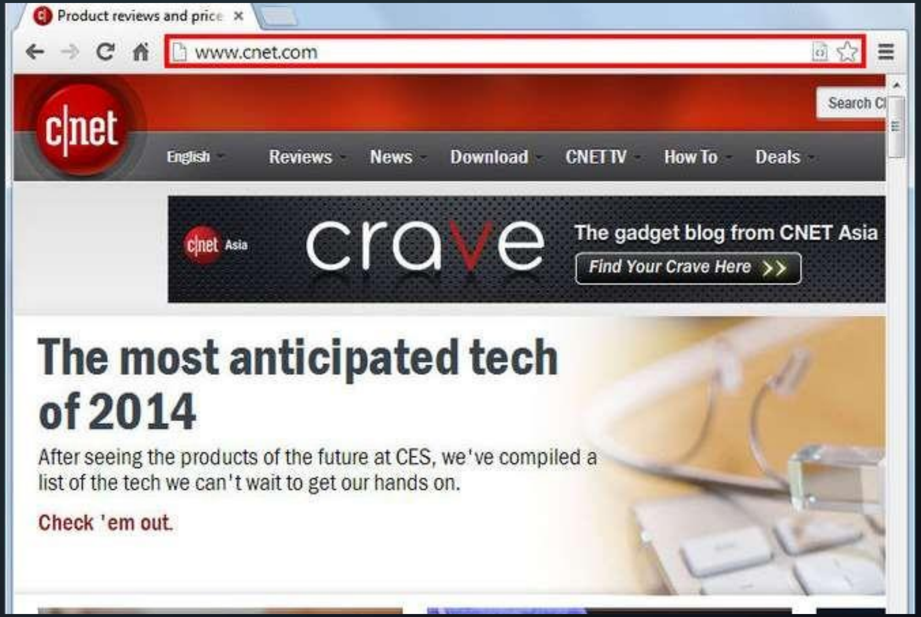
How to create a strong password

The password hint will be visible to everyone who uses this computer.

What is a password hint?

SECURE THE COMPUTER

- When downloading software (including antivirus software), get it from a **trusted source**



The gadget blog from CNET Asia

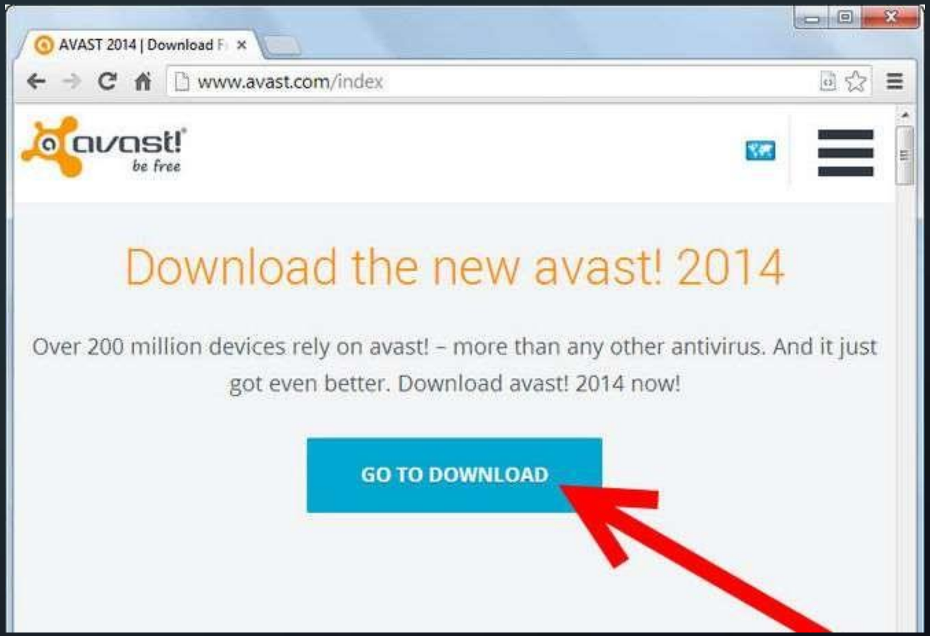
The most anticipated tech of 2014

After seeing the products of the future at CES, we've compiled a list of the tech we can't wait to get our hands on.

Check 'em out.

SECURE THE COMPUTER

- **Install good antivirus software** because Antivirus software is designed to deal with modern malware including viruses, Trojans, key loggers, rootkits, and worms.

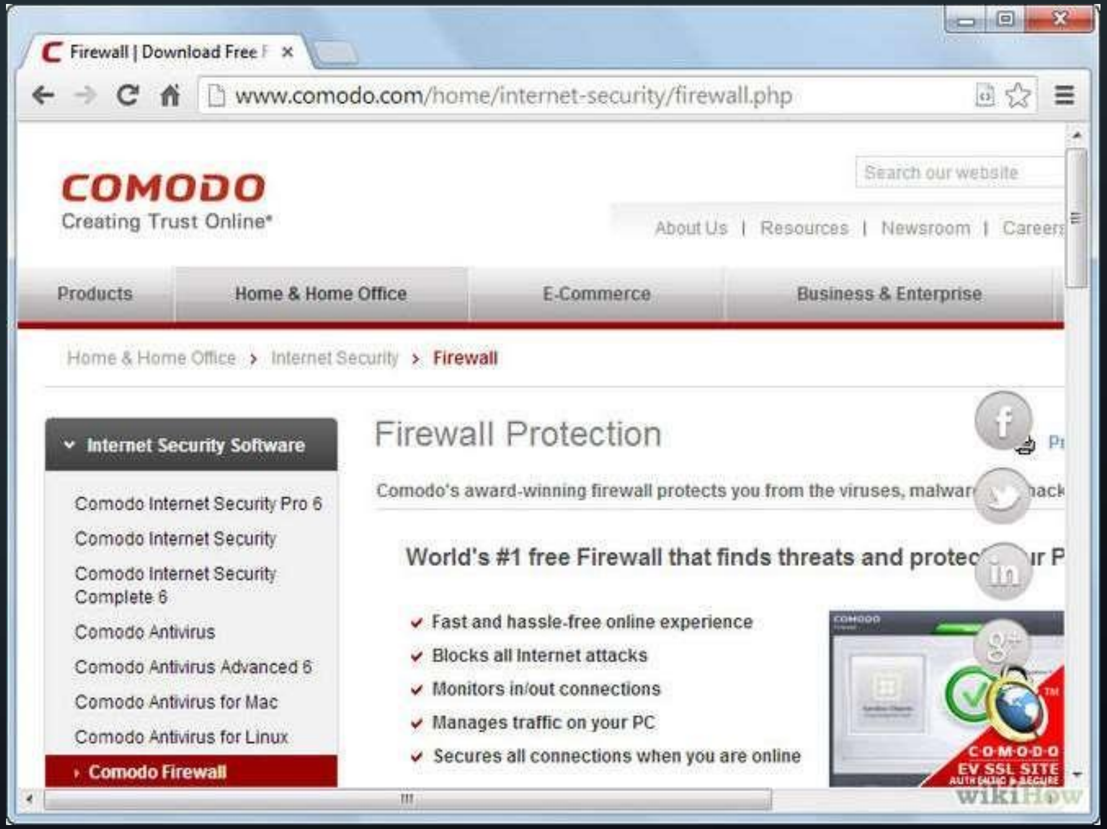


Download the new avast! 2014

Over 200 million devices rely on avast! – more than any other antivirus. And it just got even better. Download avast! 2014 now!

SECURE THE COMPUTER

- Download and install a firewall


Firewall | Download Free F
www.comodo.com/home/internet-security/firewall.php
COMODO
Creating Trust Online*
Search our website
About Us | Resources | Newsroom | Careers
Products
Home & Home Office
E-Commerce
Business & Enterprise
Home & Home Office › Internet Security › Firewall
Internet Security Software
Comodo Internet Security Pro 6
Comodo Internet Security
Comodo Internet Security Complete 6
Comodo Antivirus
Comodo Antivirus Advanced 6
Comodo Antivirus for Mac
Comodo Antivirus for Linux
Comodo Firewall
COMODO EV SSL SITE
wikiHow

Firewall Protection

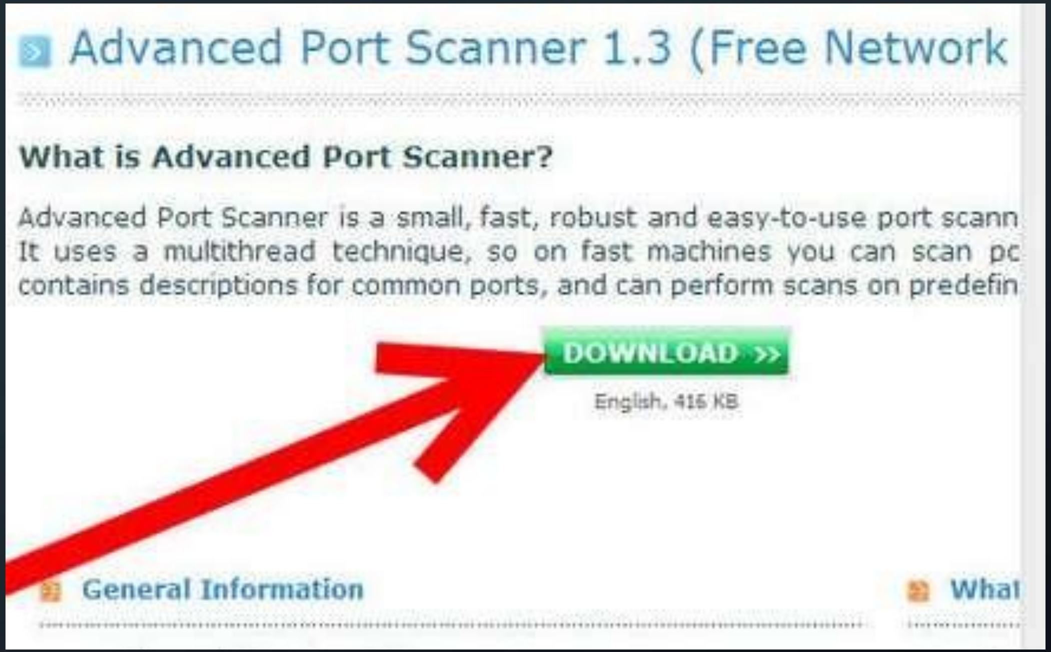
Comodo's award-winning firewall protects you from the viruses, malwar hack

World's #1 free Firewall that finds threats and protec ur P

- ✓ Fast and hassle-free online experience
- ✓ Blocks all Internet attacks
- ✓ Monitors in/out connections
- ✓ Manages traffic on your PC
- ✓ Secures all connections when you are online

SECURE THE COMPUTER

- **Close all ports.** Hackers use port scanning (Ubuntu Linux has all ports closed by default)



Advanced Port Scanner 1.3 (Free Network

What is Advanced Port Scanner?

Advanced Port Scanner is a small, fast, robust and easy-to-use port scann
It uses a multithread technique, so on fast machines you can scan pc
contains descriptions for common ports, and can perform scans on predefin

Software Security

What is a Software?

- Software, in simple words, is a collection of instructions that enable the user to interact with a computer, its hardware, or perform tasks.
  Without software, computers would be useless.
- Examples are AVG, Windows 7, Outlook, Computer drivers etc.

Types of Software

- There are two main types of software:-

  1)Application software:

Application software are often called productivity programs or end-user programs because they enable the user to complete tasks such as creating documents, spreadsheets, databases, and publications, doing online research, sending email, designing graphics etc.

Examples are Microsoft Excel, Outlook, Skype etc.

2) System Software:

Systems software includes the programs that are dedicated to managing the computer itself, such as the operating system, file management utilities, and disk operating system (or DOS).

Without systems software installed in our computers we would have to type the instructions for everything we wanted the computer to do!

Examples are Microsoft Windows, Mac OS X, LINUX etc.

Software Security

- Software security:-

Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability.

Why do we need software security?

Any compromise to integrity, authentication and availability makes a software unsecure. Software systems can be attacked to steal information, monitor content, introduce vulnerabilities and damage the behavior of software. Malware can cause DoS (denial of service) or crash the system itself. Buffer overflow, stack overflow, command injection and SQL injections are the most common attacks on the software

- Command injection can be achieved on the software code when system commands are used predominantly. New system commands are appended to existing commands by the malicious attack.
- The only way to avoid such attacks is to practice good programming techniques. System-level security can be provided using better firewalls. Using intrusion detection and prevention can also aid in stopping attackers from easy access to the system.

- Advantages:

The advantages of software security are as follows:-

1)Protects system against viruses, worms, spyware and other unwanted programs.

2)Protection against data from theft

3)Protects the computer from being hacked.

4)Minimizes computer freezing and crashes.

5) Gives privacy to users.

- Disadvantages:

Following are the disadvantages of software security:-

1)Firewalls can be difficult to configure correctly.
2)Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
3) Makes the system slower than before.
4)Need to keep updating the new software in order to keep security up to date.
5) Could be costly for average user.

THANK YOU