Security Basics

Introduction to Computer and Network Security

What we will learn

- What computer security means
- The 3 main goals: confidentiality, integrity, availability
- Assets, threats, vulnerabilities, and impact
- Authentication and access control
- Security systems like passwords, backups, firewalls, encryption, IDS
- Basic cryptography
- Basic security classifications

Section 1: What is computer security?

In this section we will see:

- what computer security means
- computer security vs network security
- why security matters

What is computer security?

Computer security means protecting:

- information
- computer systems
- computer services

So that they remain:

- confidential
- correct
- available

Real-life analogy

Think of a house.

- **Confidentiality** = strangers should not enter
- **Integrity** = nobody should secretly change your things
- **Availability** = you should still be able to use your house

Computer security vs network security

Computer security

- protects one computer

Network security

- protects many connected computers and their communication

Pause and question

Where do you see security in daily life, and what are they protecting?

Examples:

- phone lock
- ATM PIN
- classroom key
- WhatsApp lock
- bank OTP

Section 1 summary

We learned:

- security means protection
- it applies to computers and networks
- security is about privacy, correctness, and access

Section 2

The three goals of security

In this section we will see:

- confidentiality
- integrity
- availability

why all three matter together

The 3 goals

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

These are the core goals of computer security.

Confidentiality

Confidentiality means:

only authorised people should access data

Examples:

- medical records
- exam marks
- salary details
- passwords

Integrity

Integrity means:

data should not be changed in an unauthorised way

Examples:

- marks should not be altered
- attendance should not be edited secretly
- bank balance should stay correct

Availability

Availability means:

authorised users should get data or service when needed

Examples:

- college website should open during admission
- ATM should work when people need money
- hospital systems should be reachable

Simple analogy: library

Imagine a library.

- **Confidentiality** = only allowed people can see some records
- **Integrity** = nobody changes book records secretly
- **Availability** = library should be open and usable

Important idea

A system is not useful if it is so locked down that nobody can use it.

Security should protect, but it should also let real users do real work.

Think about this

Which is worse?

- A student can see another student’s marks
- A student’s marks are changed
- The marks portal is down on result day

Why?

Section 2 summary

We learned:

- confidentiality = prevent unauthorised access
- integrity = prevent unauthorised change
- availability = keep systems usable

Section 3

Security problems and risk thinking

In this section we will see:

- what we protect
- what we protect it from
- what happens if protection fails

Risk analysis in simple words

Ask 3 questions:

1. What do we need to protect?
2. What do we need to protect it from?
3. How do we protect it?

Step 1: Identify assets

Assets are things that matter and need protection.

Examples:

- hardware
- software
- data
- people
- documents
- supplies

Asset examples

Hardware

- computers, routers, printers, disks

Software

- operating system, apps, utilities

Data

- files, databases, backups, logs

People

- users, admins, operators

Step 2: Identify threats

Threats are things that can cause harm.

Examples:

- unauthorised access
- disclosure of information
- denial of service
- accidental mistakes
- intentional attacks

Step 3: Identify impact

Impact means: what damage happens if the attack succeeds?

Examples:

- privacy loss
- money loss
- work disruption

Real-life analogy: school bag

Asset:

- your school bag

Threat:

- theft, rain, damage, wrong handling

Impact:

- books lost, homework gone, money gone

Protection:

- zip, label, careful storage

Reflect

Pick one thing from your daily life:

- phone
- email
- notebook

Now say:

- what is the asset?
- what is the threat?
- what is the impact?

Section 3 summary

We learned:

- security starts with assets
- then we identify threats
- then we estimate impact
- then we choose protection

Section 4

Threats and vulnerabilities

In this section we will see:

- what a threat is
- what a vulnerability is
- four common attack types

Threat vs vulnerability

Threat

- something that can cause harm

Vulnerability

- a weakness that can be exploited

A weakness causes harm only when someone or something uses it.

Easy analogy

A thief is a **threat**.

An unlocked door is a **vulnerability**.

If the door is locked well, the thief has less chance.

Four attack types

1. **Interruption**
2. **Interception**
3. **Modification**
4. **Fabrication**

Interruption

An asset becomes unavailable or unusable.

Examples:

- disk failure
- deleted file
- crashed operating system

This mainly hurts **availability**.

Interception

An unauthorised person or system gains access.

Examples:

- copying files secretly
- reading messages
- wiretapping

This mainly hurts **confidentiality**.

Modification

An unauthorised party changes something.

Examples:

- changing database values
- editing a file secretly
- altering transmitted data

This mainly hurts **integrity**.

Fabrication

A fake object, message, or transaction is created.

Examples:

- fake transaction
- fake account
- fake email pretending to be real

This can hurt trust, integrity, and security.

Common vulnerabilities

Examples from the unit:

- poor password management
- lack of training
- no security policy
- weak authentication
- clear-text passwords
- wrong permissions
- poor system management

Attackers often need 3 things

- **Method** = tools or skills
- **Opportunity** = chance or access
- **Motive** = reason

Think deeper

A weak password is not an attack.

So what is it?

- a threat?
- a vulnerability?
- a control?

Explain why.

Exercise

Classify each item:

1. Forgotten logout on lab computer
2. Student copies another student’s file
3. Fake payment screenshot sent to shop
4. Server power cable removed

For each, say:

- attack type
- security goal affected

Section 4 summary

We learned:

- threats cause harm
- vulnerabilities are weaknesses
- attacks may interrupt, intercept, modify, or fabricate

Section 5

User authentication and access control

In this section we will see:

- how a system checks who you are
- types of authentication
- access control basics

What is authentication?

Authentication means:

proving who you are to the system

Common example:

- username + password

Three ways to authenticate

1. **Something you know**
    - password, PIN
2. **Something you have**
    - ID card, token, key
3. **Something you are**
    - fingerprint, face, voice

Stronger authentication

- Using two or more methods together is stronger.
- 2FA - Two factor Authentication

Example:

- ATM card + PIN
- phone + OTP
- laptop password + fingerprint
- password + token

Authentication vs authorisation

Authentication

- Are you really who you say you are?

Authorisation

- What are you allowed to do?

Example:

- login to email = authentication
- read-only vs edit rights = authorisation

Discuss

Which do you use most often?

- password
- PIN
- OTP
- fingerprint
- face unlock

Which feels safest? Which feels easiest?

Exercise

For each system, suggest good authentication:

1. College library login
2. Bank app
3. Social media account
4. Exam result portal
5. Lab administrator login

Section 5 summary

We learned:

- authentication proves identity
- authorisation controls actions
- systems may use passwords, tokens, or biometrics

Section 6: Security systems and facilities

In this section we will see:

- access control practices
- password rules
- user account management
- backups
- firewalls
- antivirus
- physical controls
- auditing

Good system access control

What to look for:

- unique user ID for each user
- need-to-use access
- encrypted stored passwords
- inactivity timeout
- audit logs
- protection of sensitive OS files

Password management basics

Good passwords should:

- be reasonably long
- include mixed-case letters, numbers and symbols
- not be easy to guess like names, birthdays
- don't use dictionary words
- not be shared
- be stored safely
- unique on every system

Beginner password advice

Bad:

- 12345678
- password
- admin
- your name

Better:

- mix of words and symbols
- hard to guess
- not reused everywhere

Privileged users

Privileged users are users with extra power.

Examples:

- administrator
- root user
- system operator

Their access should be:

- limited
- logged
- carefully managed

User account management

Good practice includes:

- only authorised users get accounts
- keep records of users
- remove access when someone leaves
- review old or unused accounts

Data and resource protection

Every important data set should have an owner responsible for it.

That helps with:

- accountability
- integrity
- proper care
- clear responsibility

Backups

Backups mean keeping extra copies of important data.

Why?

- recovery after mistakes
- recovery after attacks
- recovery after hardware failure

Keep backups:

- updated
- checked
- documented

Firewall

- A firewall is like a gatekeeper between networks.
- It checks traffic entering or leaving a network.

Firewall analogy

Think of a security guard at a building gate.

- checks who comes in
- checks basic rules
- blocks some entries
- allows some entries

A badly configured guard can also block the wrong people.

Encryption

Encryption changes readable data into unreadable form.

- readable data = plaintext
- unreadable data = ciphertext

Only someone with the right key should read it again.

IDS: Intrusion Detection System

An IDS watches systems or network activity
and looks for suspicious behaviour.

Examples:

- many failed logins
- unusual traffic
- strange patterns

It can:

- detect
- alert

Security is not only software.

- antivirus software
- clear policies and procedures
- locks and guards
- fire/water precautions
- air conditioning
- site planning

Security is not only software.

People matter too

Many breaches are caused by people.

So organisations must think about:

- hiring
- training
- monitoring
- handling employee departure

Auditing

Auditing means checking logs and records carefully.

Why it matters:

- detect suspicious actions
- track access
- support investigation

Red flags:

- many failed logins
- same account from many places
- attempts to shut down critical servers

Think deeper

Which is the weakest part of security?

- software
- hardware
- passwords
- people
- process

Defend your answer.

Exercise

Group task: Secure a small college lab.

Your lab has:

- 20 computers
- one Wi-Fi router
- projector
- student logins
- shared printer

Suggest controls for:

- passwords

Section 6 summary

We learned:

- access must be controlled
- passwords must be managed well
- backups, firewall, IDS, antivirus, policies, and auditing all help
- security includes people and physical space too

Section 7

Cryptography basics

In this section we will see:

- what cryptography does
- encryption and decryption
- symmetric and asymmetric keys

What is cryptography?

Cryptography is the use of mathematical methods to protect information.

Main idea:

- convert readable data into unreadable data
- convert it back when needed

Two key actions

Encryption

- plaintext → ciphertext

Decryption

- ciphertext → plaintext

Symmetric cryptography

Same key is used for:

- encryption
- decryption

Simple idea:

- both sides share one secret key

Asymmetric cryptography

Different keys are used:

- one key for encryption
- another key for decryption

This is also called:

- public key cryptography

Simple analogy

Symmetric:

- one shared room key

Asymmetric:

- one key locks, another key unlocks
- A number lock where anyone can lock but only you can open

Why encryption helps

Encryption helps protect:

- confidentiality
- sometimes integrity
- communication safety

But it may also add:

- processing load
- overhead
- delay

Exercise

What's the term for?

1. Readable message
2. Scrambled unreadable message
3. Turning readable into scrambled
4. Turning scrambled back to readable

Section 7 summary

We learned:

- cryptography protects data
- encryption scrambles data
- decryption restores data
- symmetric uses same key
- asymmetric uses different keys

Final summary

Today we learned:

- security protects information and systems
- the 3 goals are confidentiality, integrity, availability
- we identify assets, threats, vulnerabilities, and impact
- attacks may interrupt, intercept, modify, or fabricate
- authentication and access control matter
- passwords, backups, firewalls, IDS, antivirus, policies, and auditing help
- cryptography protects data
- intrusion detection looks for suspicious activity

Thank you!

Any questions?

Thejesh GN