

Systems and Usable Security

Introduction to Computer Security

DR. NEMINATH HUBBALLI

NPTTEL

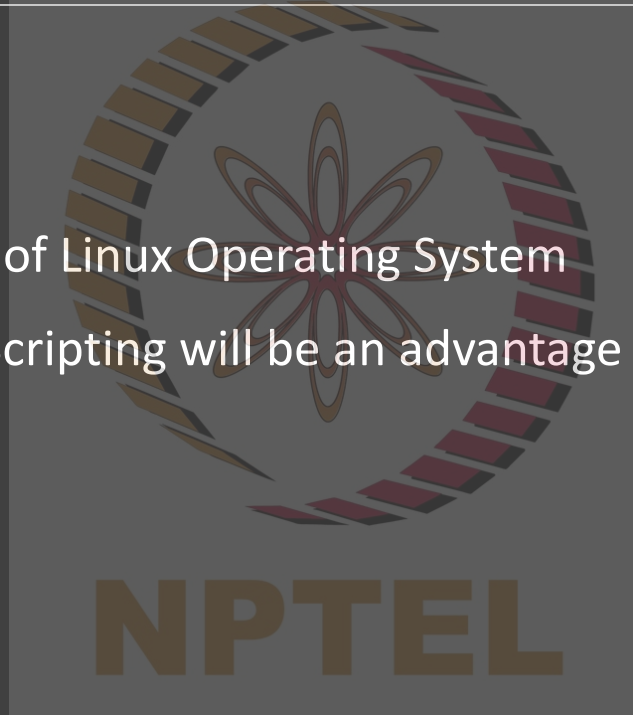
Prerequisites

Computer Networks

Operating Systems

Working Knowledge of Linux Operating System

Knowing Perl/Shell Scripting will be an advantage



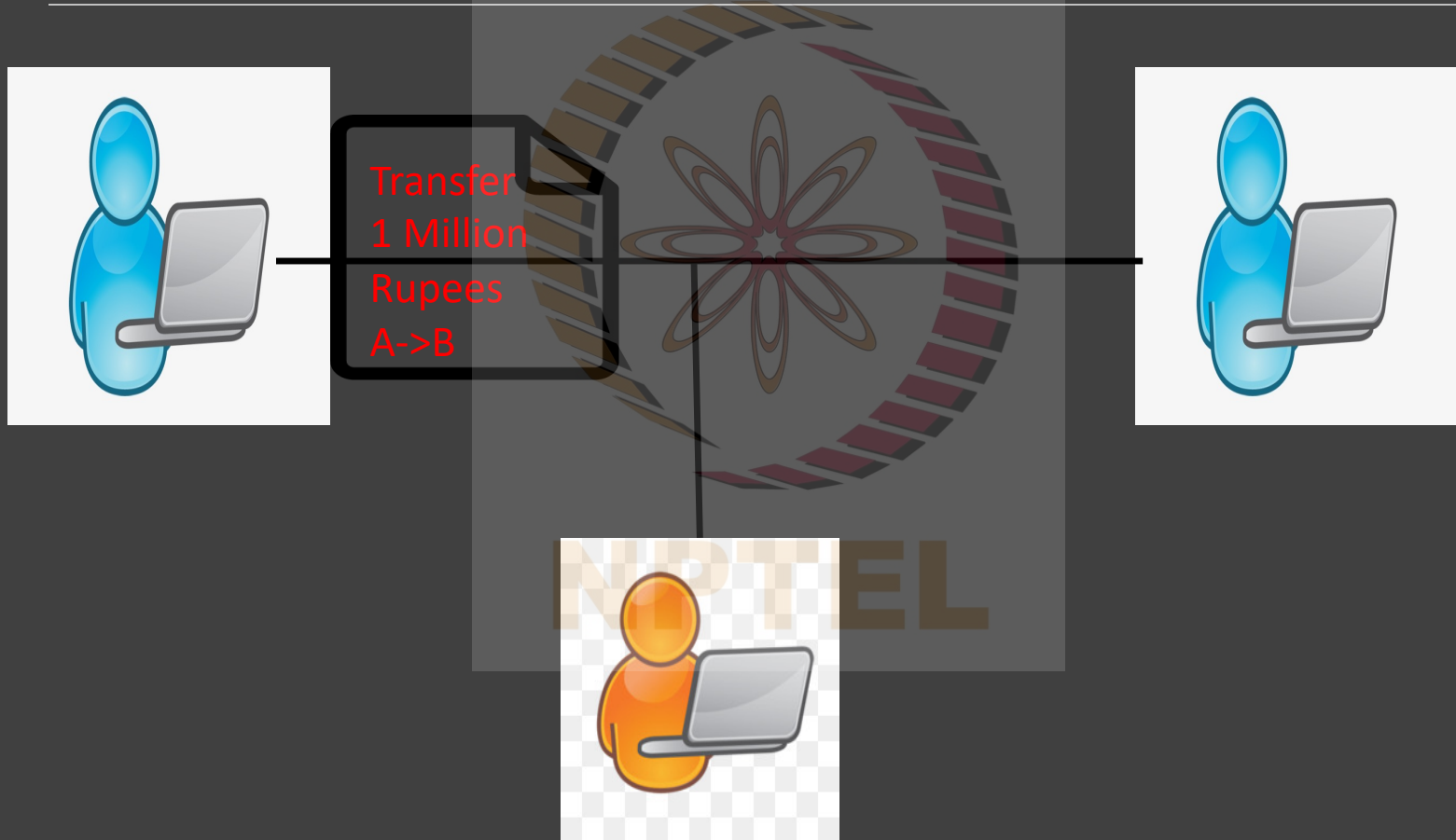
Course Content

We shall discuss

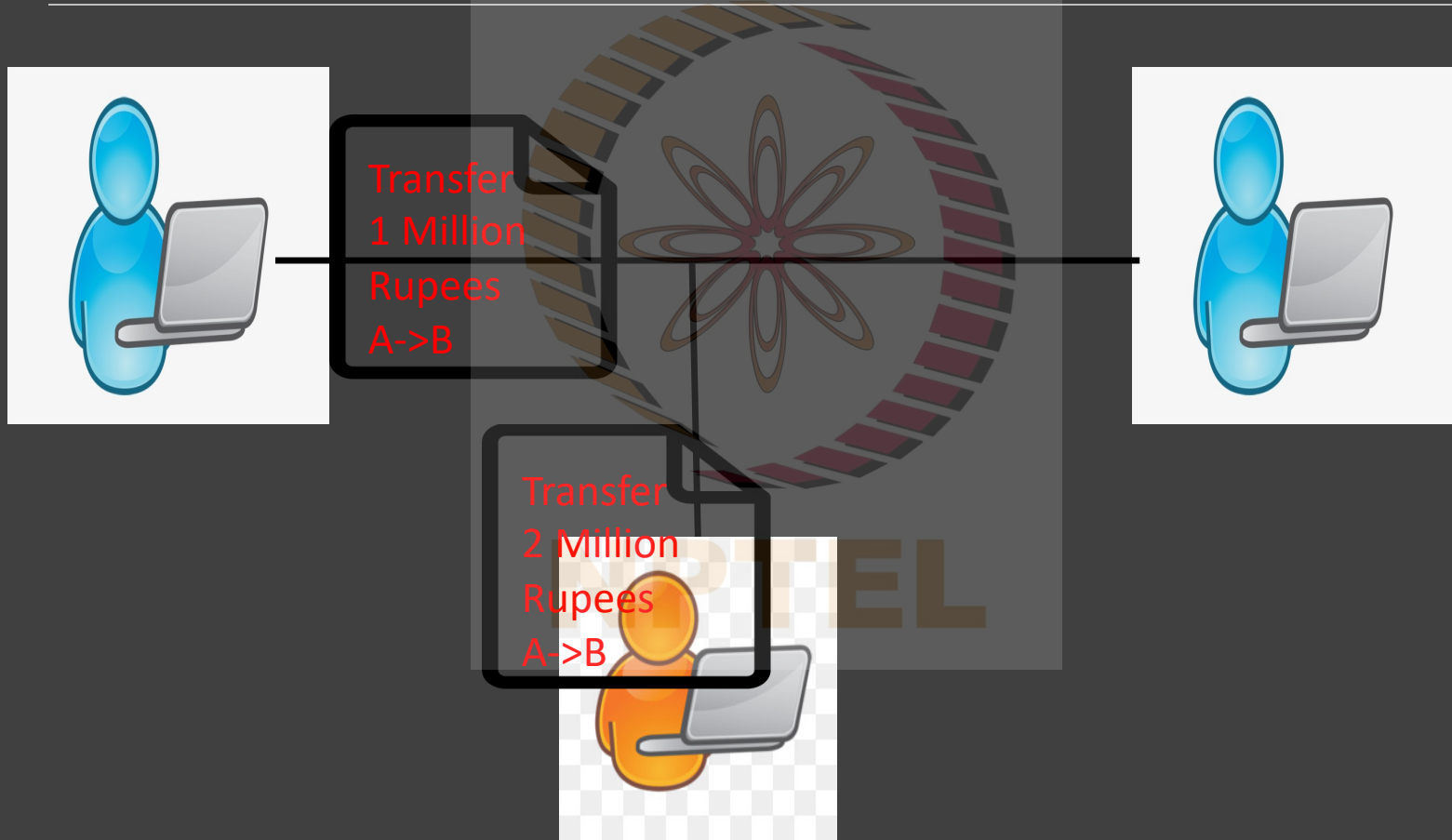
- ❑ Security issues, vulnerabilities, Exploits and attacks
- ❑ Operating System Security
- ❑ Web Security
- ❑ Usable Security



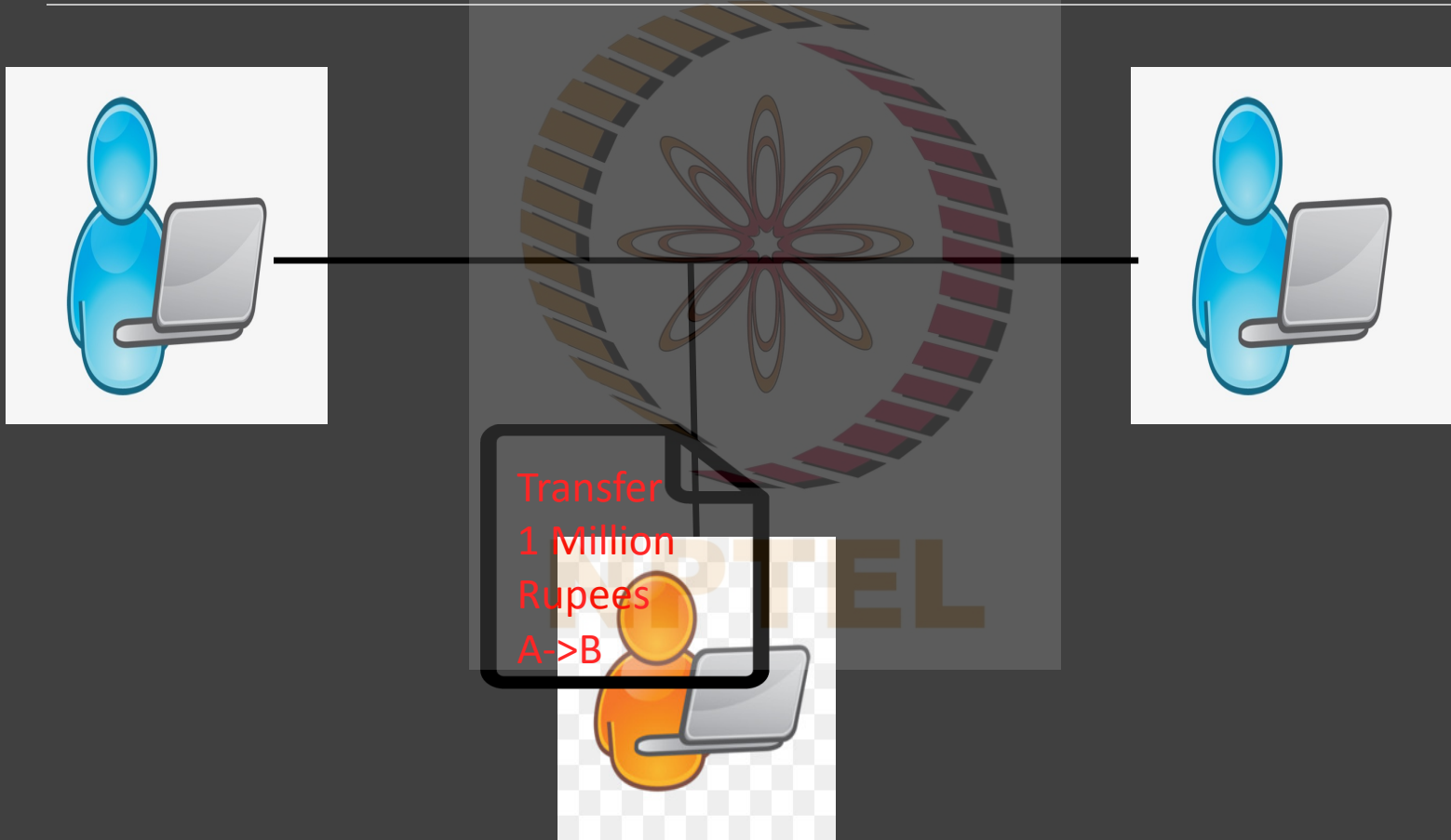
Why Computer Security



Why Computer Security



Why Computer Security



What is Computer Security ?

Deals with art of protecting computer resources

What are the resources

- Memory
- Computing power
- Data

Protection against

- Human errors
- Bad guys outside
- Dishonest people inside



When to Say System is Secure

The goal of computing is to do something useful

We write computer programs to do useful computation

All programs take some input and usually generate some output

A system/program is said to be secure if

- For an expected input supplied with good intent it generates a desired output
- For an unexpected input supplied with malicious intent it does not fail

Why We Should Care about Security?

We use internet for many things

- Online banking
- Online shopping
- Booking tickets ...

We store many things in computers

- Photos
- Files

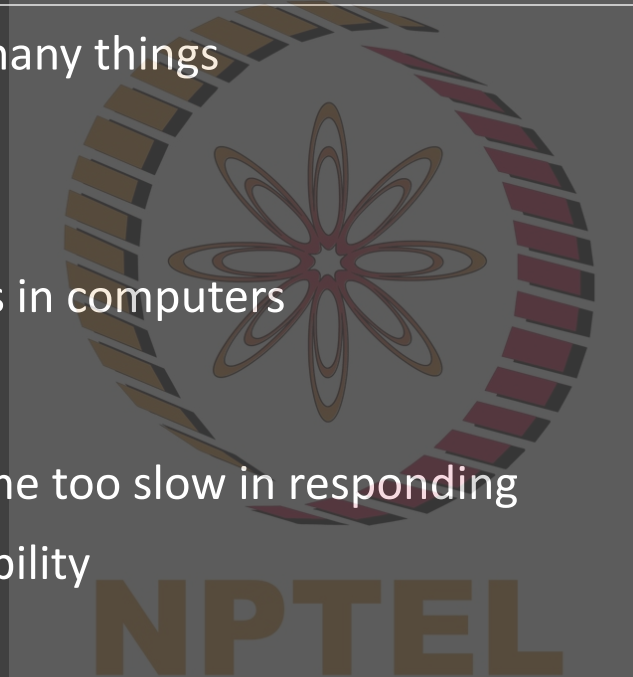
Computer may become too slow in responding

Reputation and credibility

- Media glare

You may be contributing to computer crime without your knowledge

- Ex. Open wireless networks
- Legal aspects



Who Are Vulnerable to Attacks ?

Financial institutions

Defense organizations

Government agencies

Pharmaceutical companies

IT companies

Intellectual property management companies

Academic institutions

Everyone connected to internet !



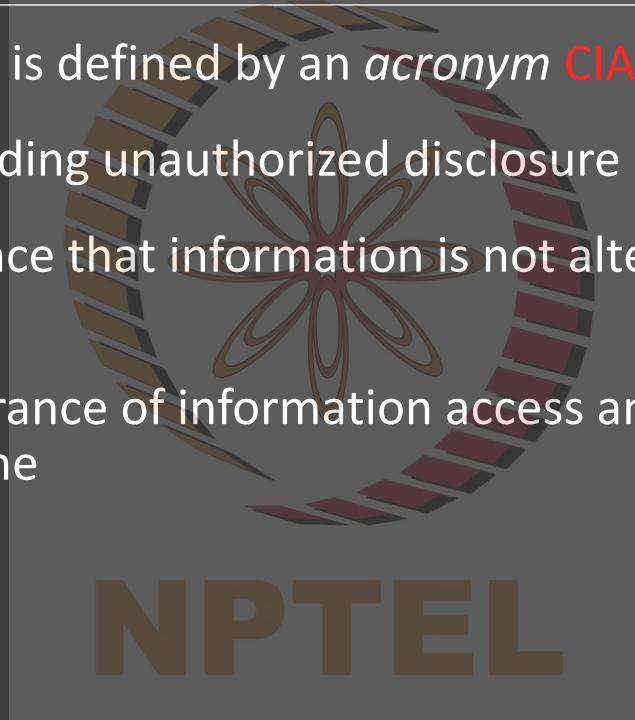
CIA Principles of Security

Information security is defined by an *acronym* **CIA**

Confidentiality: Avoiding unauthorized disclosure of information

Integrity: An assurance that information is not altered midway of transmission

Availability: An assurance of information access and modification in a reasonable timeframe



Confidentiality

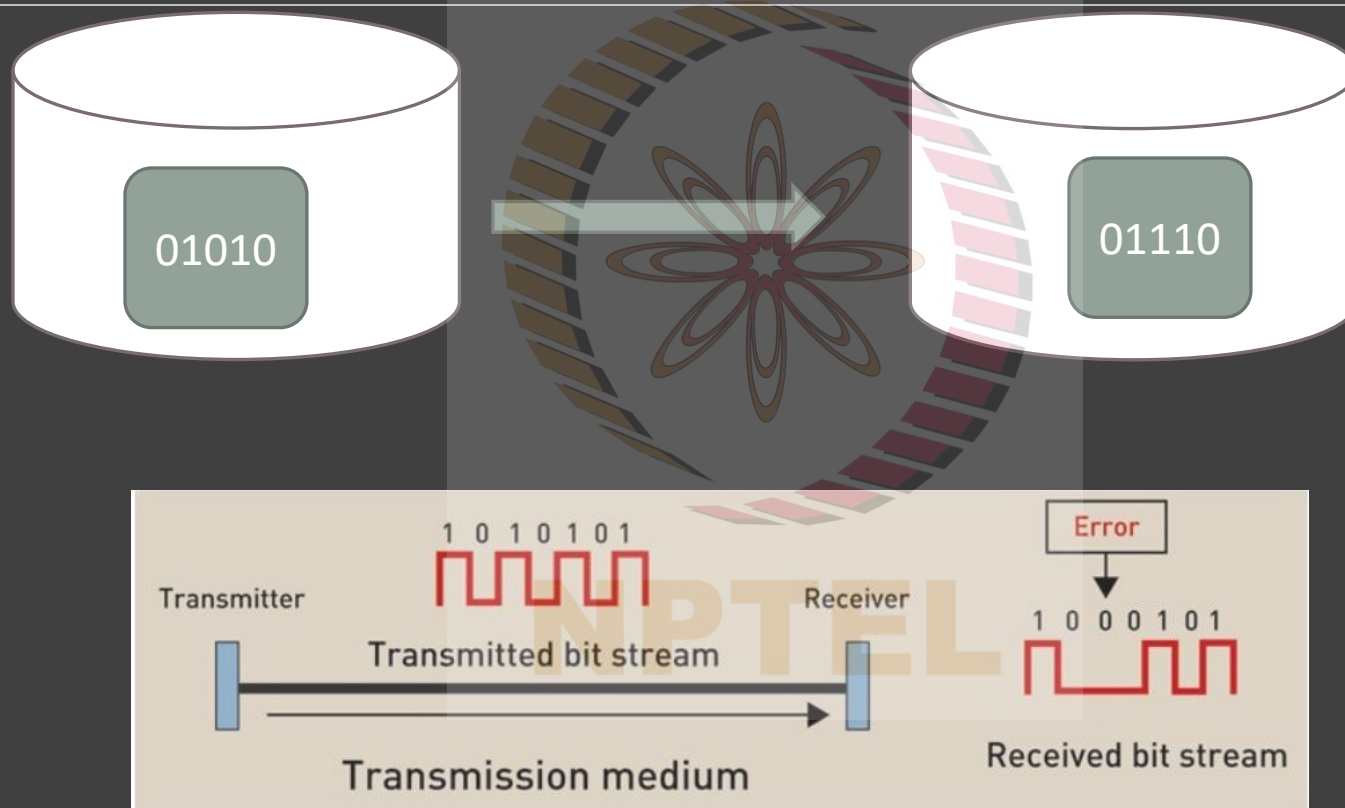
Provide access to legitimate users

Block access to illegitimate users

Confidentiality can be achieved through

- Encryption: Transform data to a meaningless unit for transmission and storage. Show it correctly to intended users
- Access control: Control who can claim access to
- Authentication: Determining identity of person claiming access
 - Something person has
 - Something person knows
 - Something he/she is
- Authorization: Determining whether the person is allowed to access something
- Physical security: Establishing physical barriers

Integrity Compromise



Integrity

Integrity compromise

- System induced: hardware flips a bit
- Malicious: someone rewrites the data

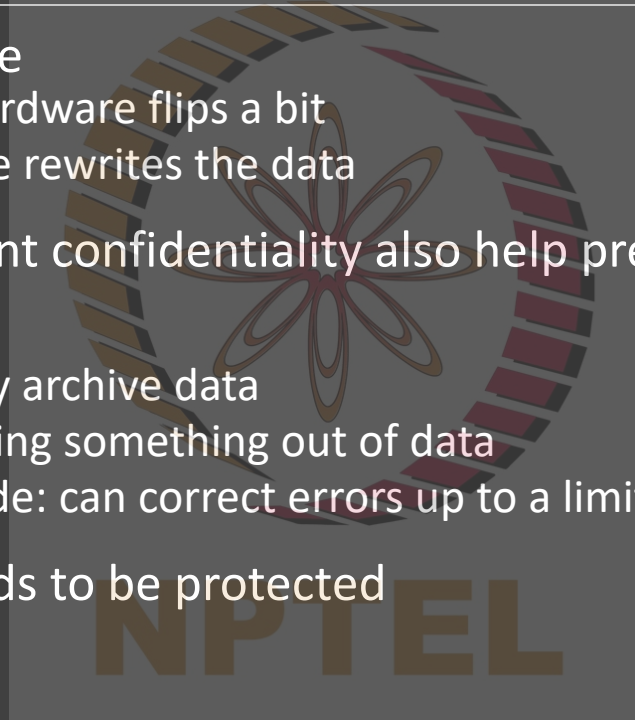
Techniques to prevent confidentiality also help prevent integrity

In addition

- Backup: periodically archive data
- Checksum: computing something out of data
- Error correction code: can correct errors up to a limit

Metadata : also needs to be protected

- Owner
- Size of file
- Last read and write timings
- Location of data



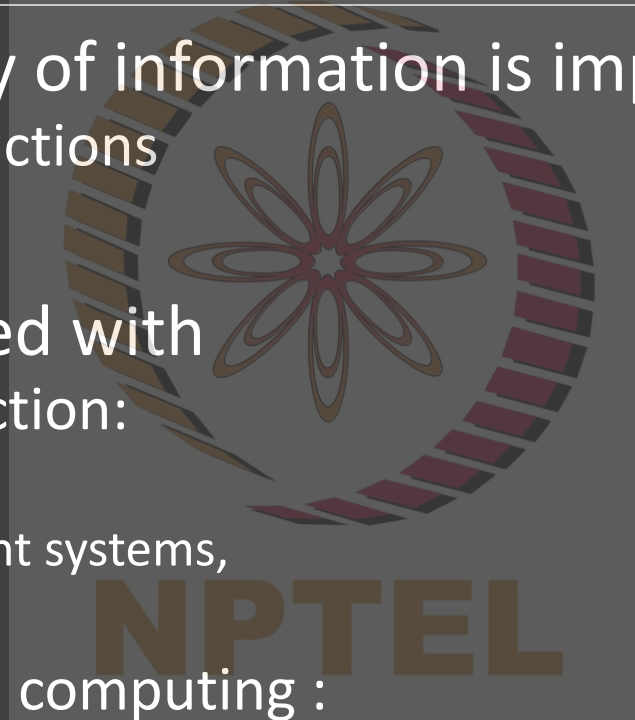
Availability

Timely delivery of information is important

- Banking transactions
- Stock quotes

Can be achieved with

- Physical protection:
 - guards,
 - fire management systems,
 - locks
- Redundancy in computing :
 - RAID
 - Fault tolerance systems



The Value of Your Data

Lost data

- Financial loss

Confidential data

- Danger of going into wrong hands

Downtime

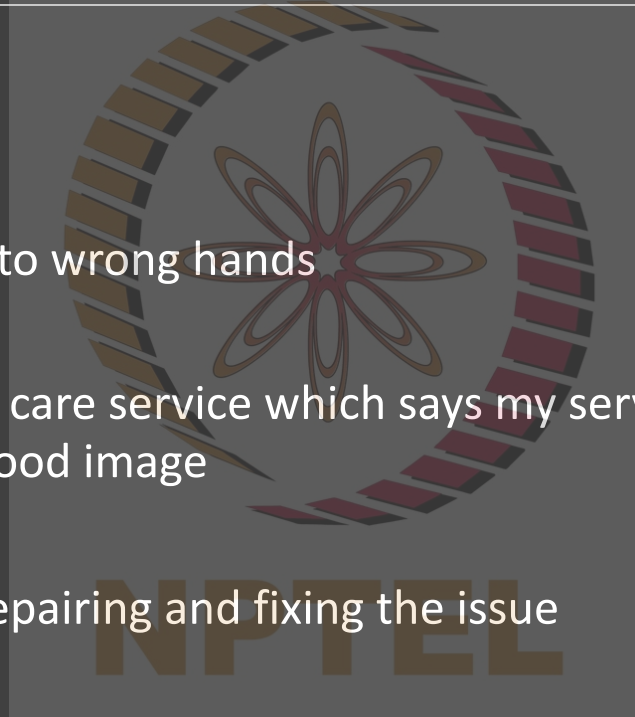
- Calling a customer care service which says my server is down
- It does not carry good image

Staff time

- Time invested in repairing and fixing the issue

Reputation

- Damage
- Financial loss



Security Mechanism

Economy of mechanism

- The easier and simple a security mechanism the better it is to understand

Fail-safe defaults

- Default configuration should be conservative

Complete mediation

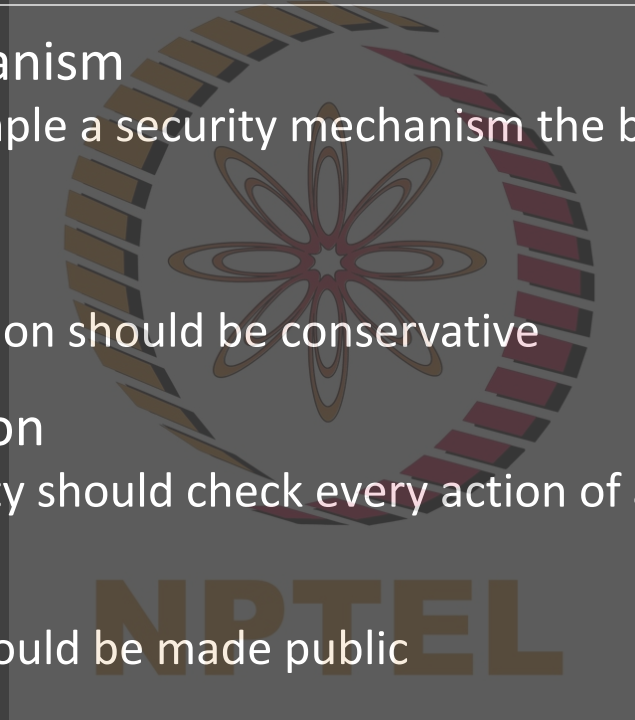
- A security authority should check every action of a user

Open design

- Security design should be made public

Separation of privilege

- Multiple conditions should be required to get access



Security Mechanism

Least privileges

- Every program must have bare minimum privileges to run

Least common mechanism

- Sharing among users should be minimum

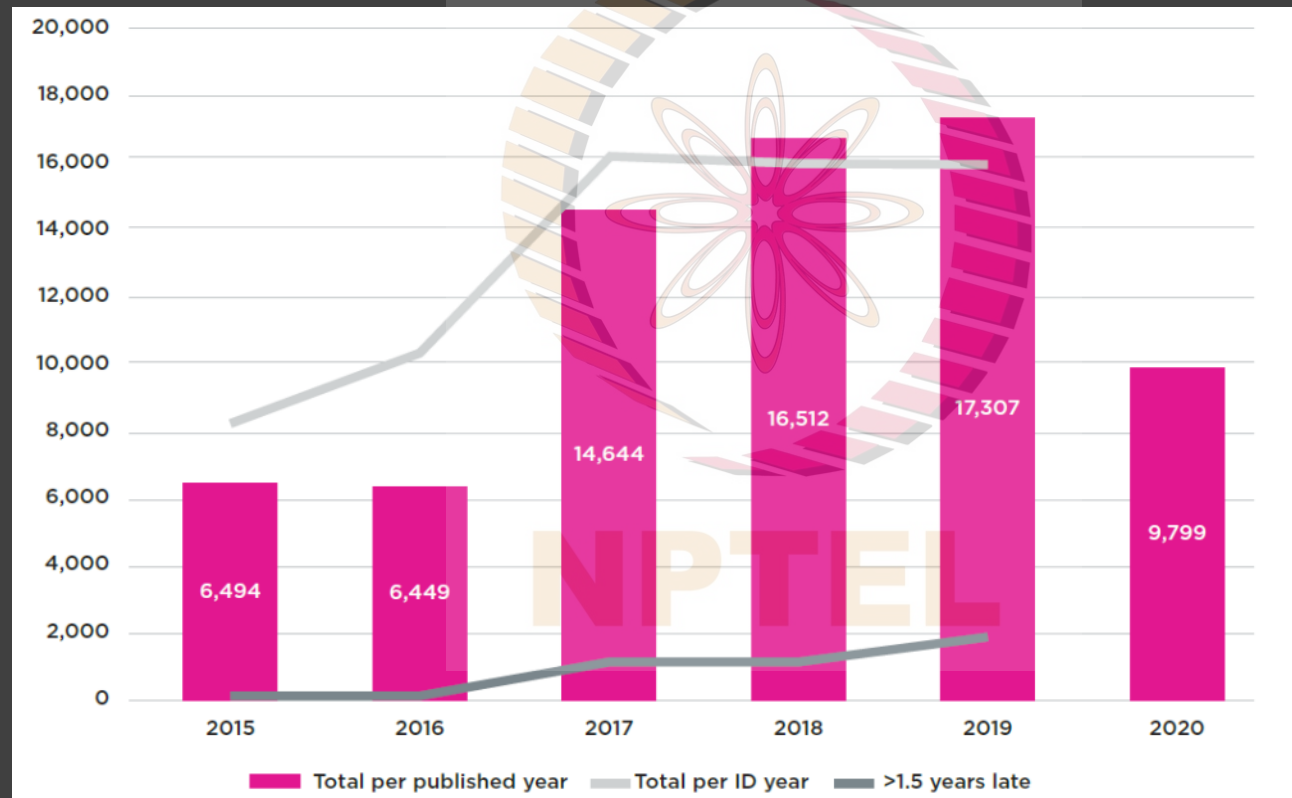
Psychological acceptability

- User interfaces should be intuitive

Compromise recording

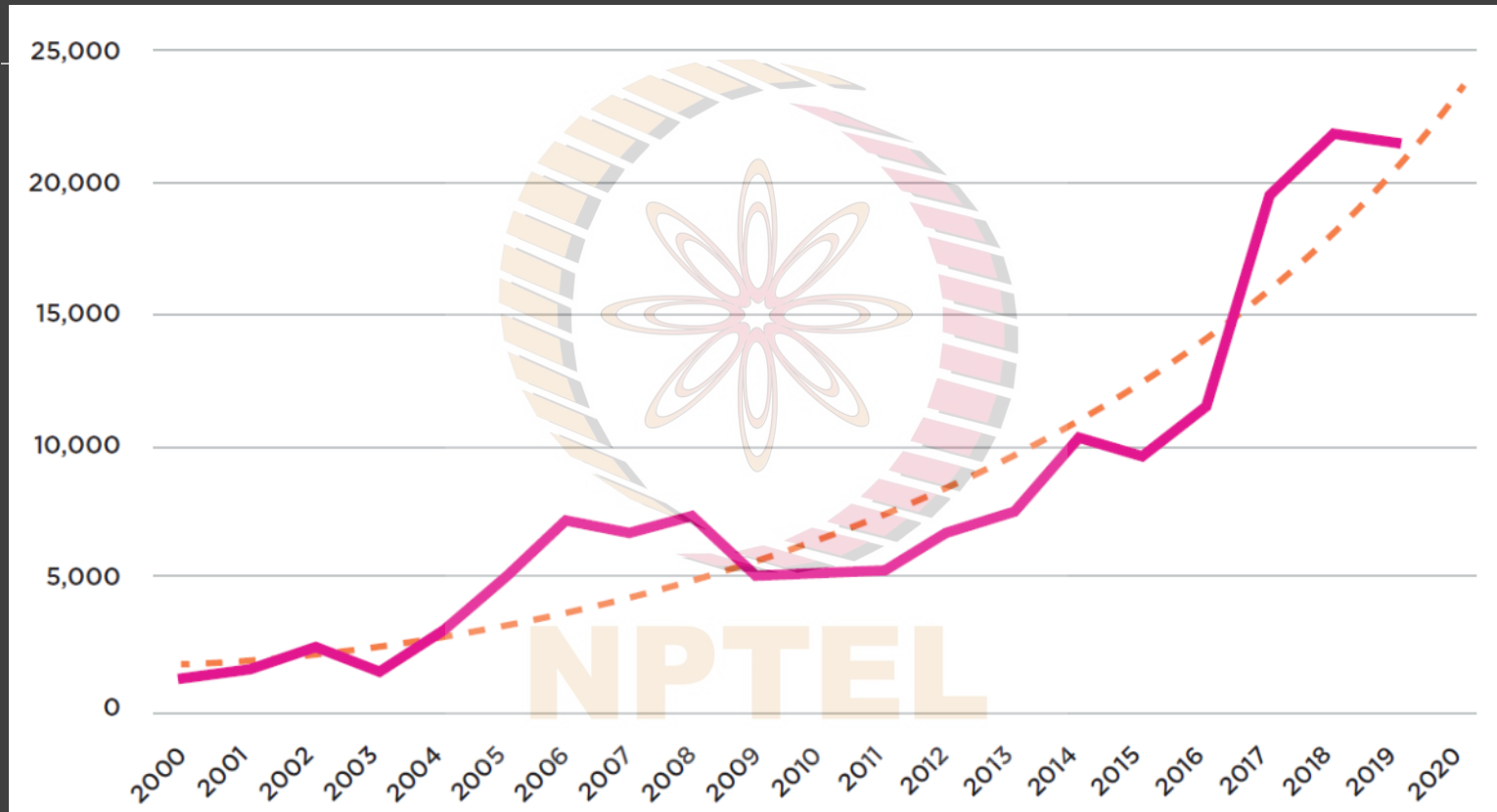
- Sometimes it is more desirable to record details of an attack rather than designing a comprehensive security mechanism

Vulnerability Trend



Source: Skybox Security Report

Vulnerability Trend



Source: Skybox Security Report