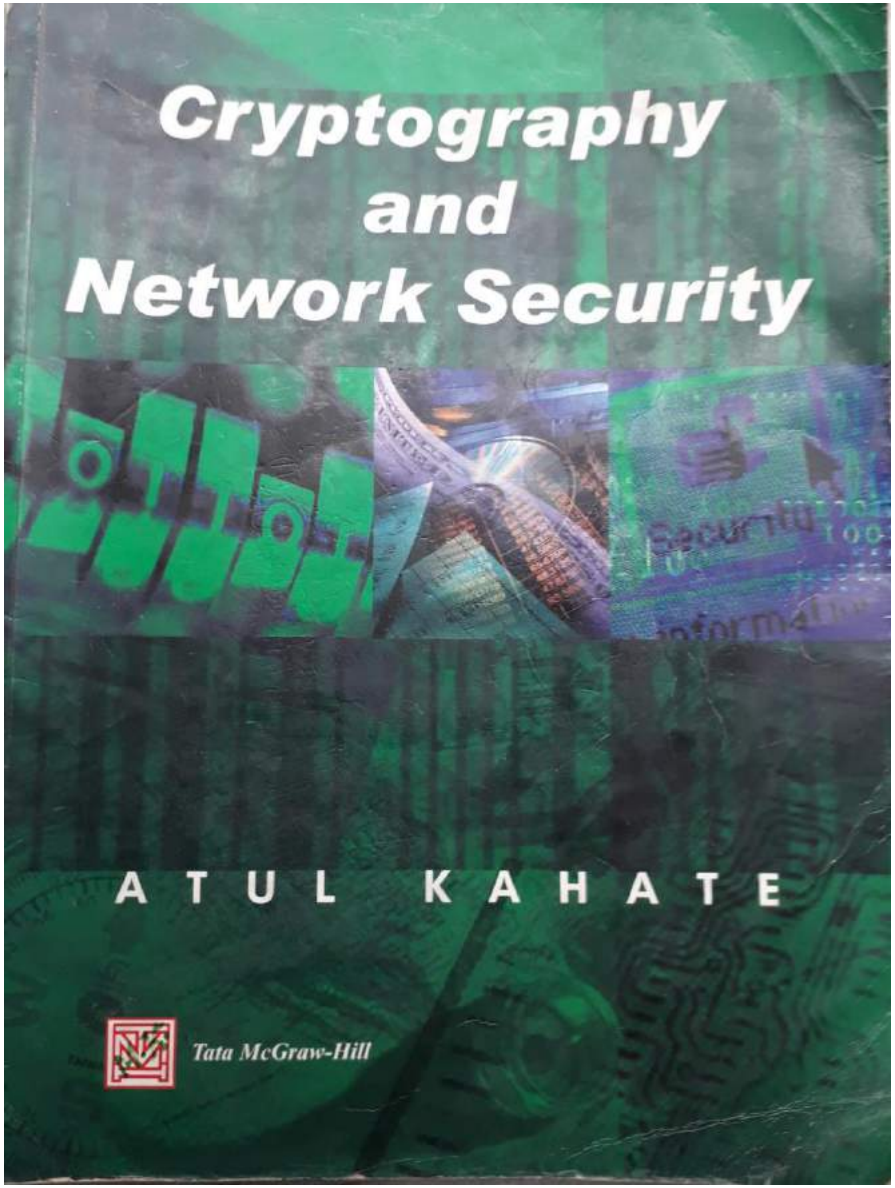
Books (1/2)

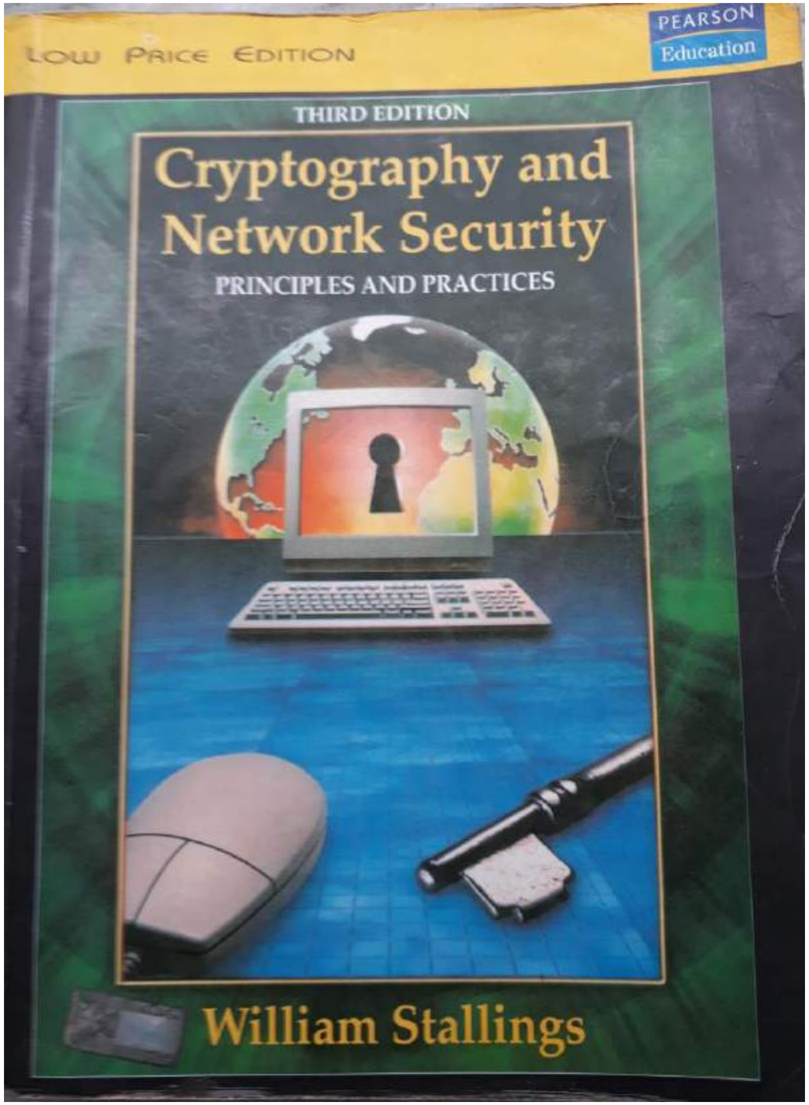


Cryptography and Network Security

ATUL KAHATE

Tata McGraw-Hill

Books (2/2)



LOW PRICE EDITION

PEARSON Education

THIRD EDITION

Cryptography and Network Security

PRINCIPLES AND PRACTICES

William Stallings

Information Security

“Three people can keep a secret only if two of them are dead”

----- Benjamin Franklin

Security Models

1) No security
2) Security through obscurity
3) Host security
4) Network security

Principles of Security

1) Confidentiality
2) Authentication
3) Integrity
4) Non-repudiation
5) Access control
6) Availability

Confidentiality

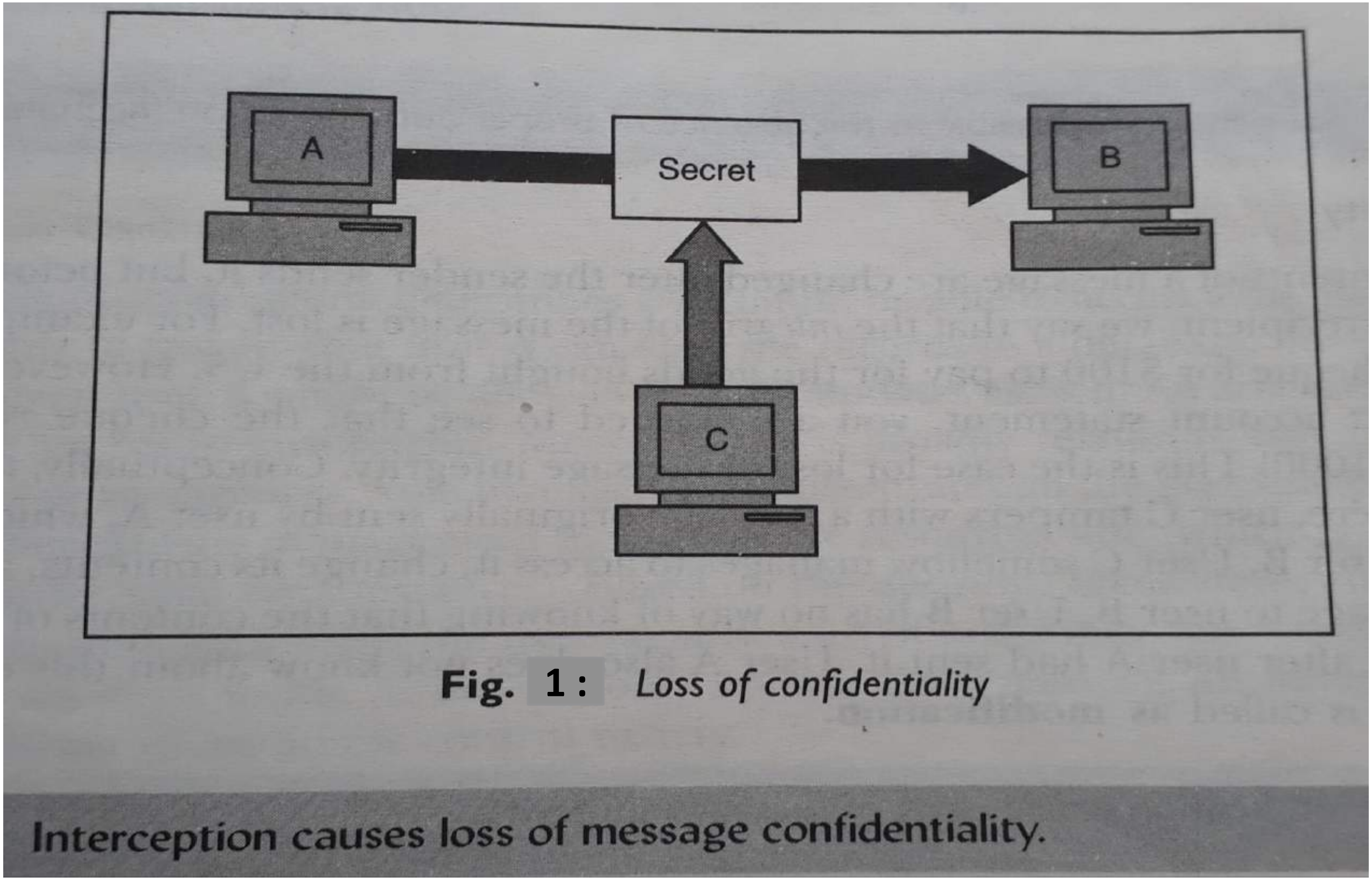


Fig. 1 : *Loss of confidentiality*

Interception causes loss of message confidentiality.

Authentication

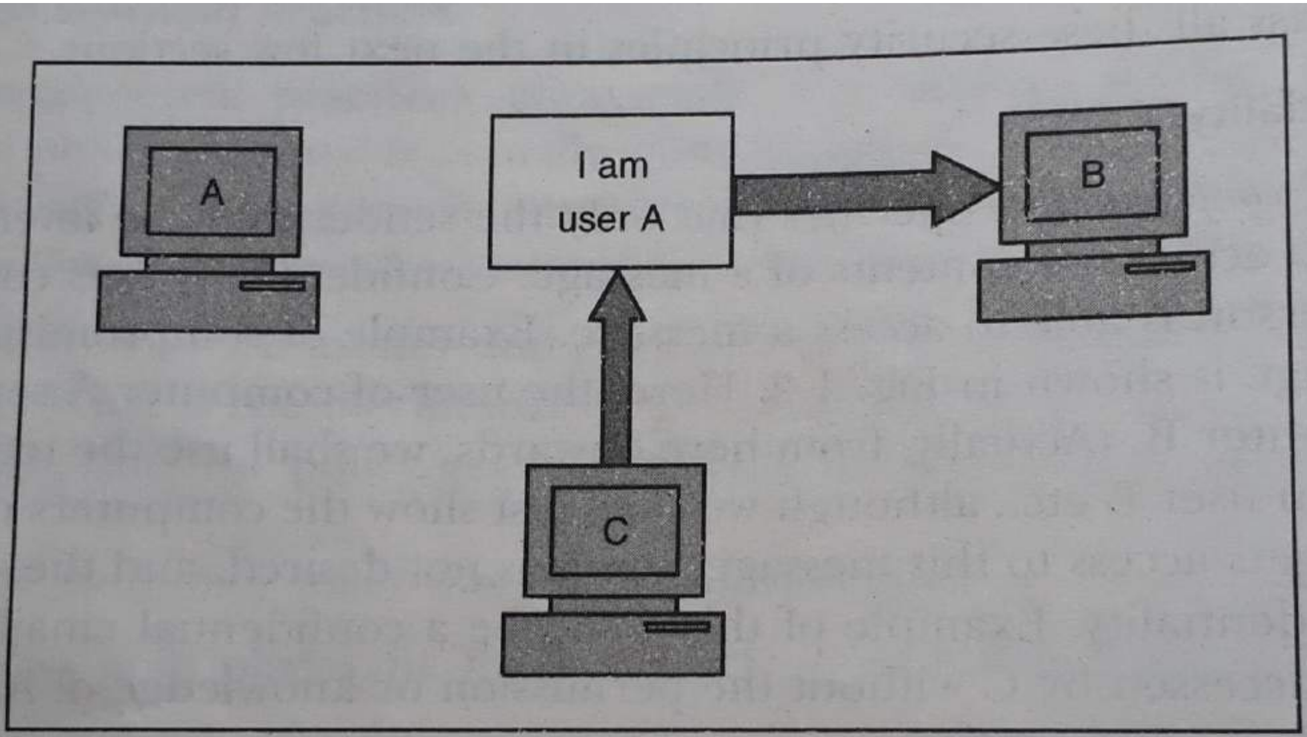


Fig. 2 : *Absence of authentication*

Fabrication is possible in the absence of proper authentication mechanisms.

Integrity

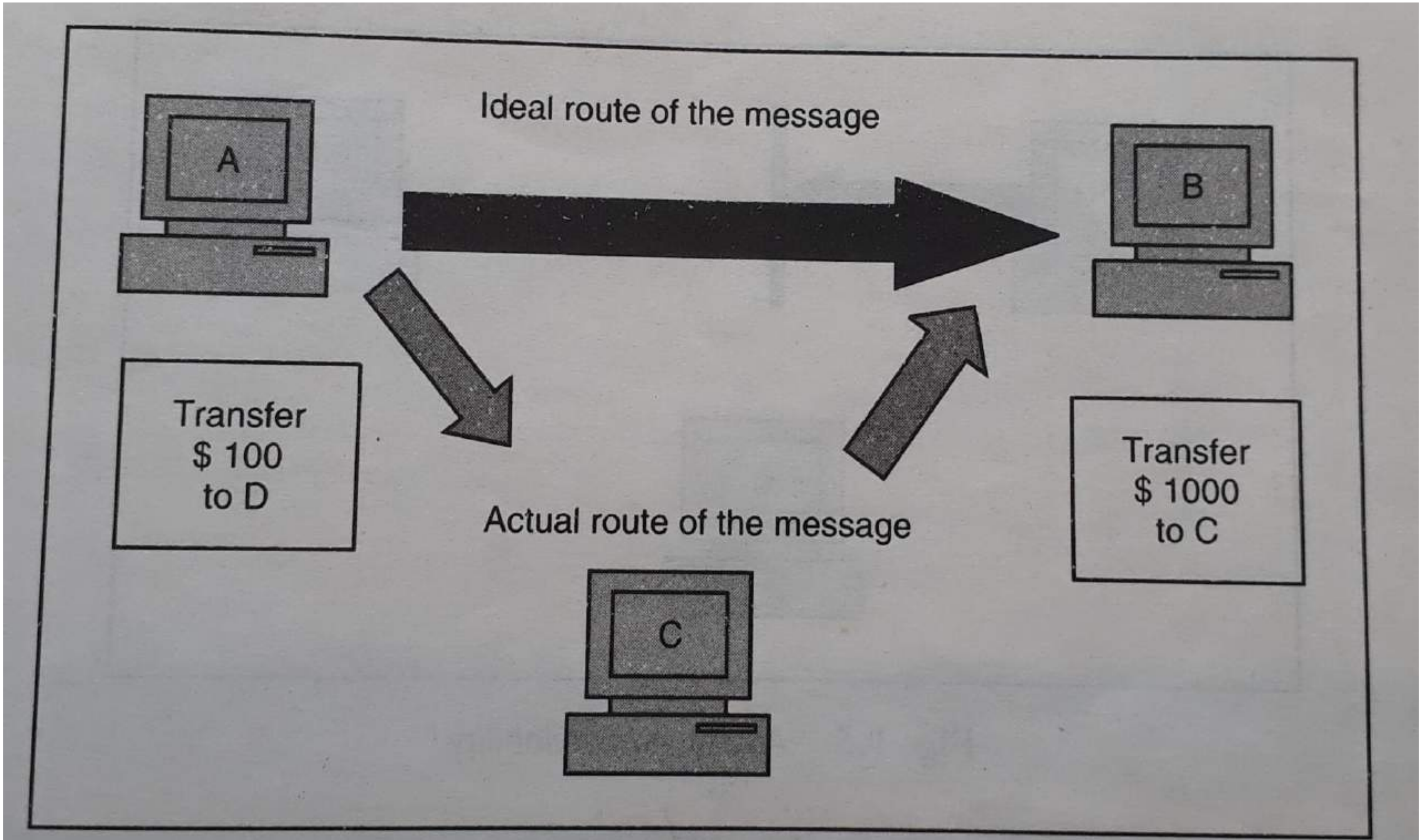


Fig. 3 : *Loss of integrity*

Non-repudiation

- Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.
- Digital Signature can be used to maintain this principle of security.

Access Control

- Access control specifies and controls who can access what.
- Access control is broadly related to two areas:

  a) Role Management – which user can do what.

  b) Rule Management – which resource is accessible and under what circumstances.

Availability

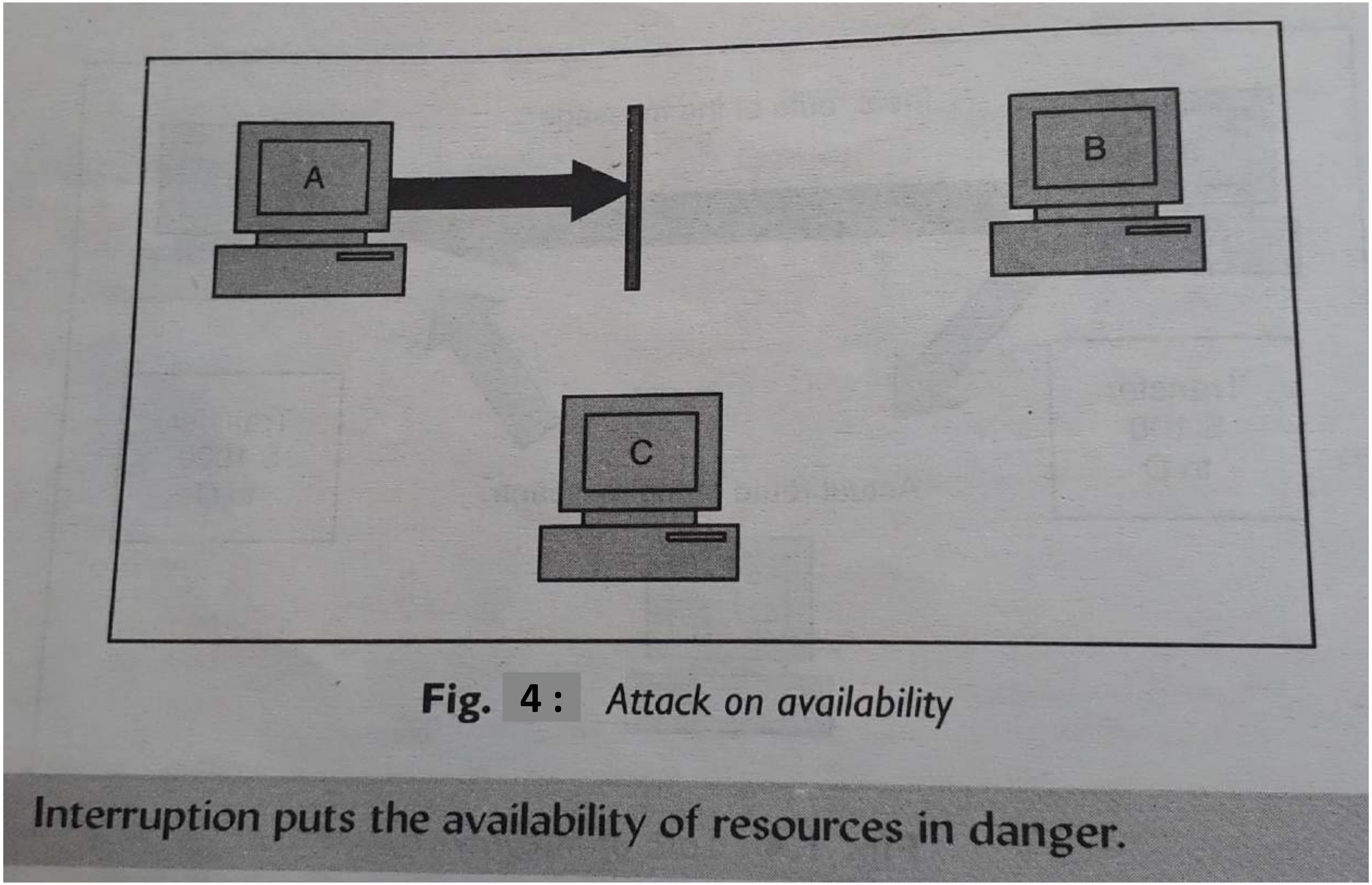


Fig. 4 : *Attack on availability*

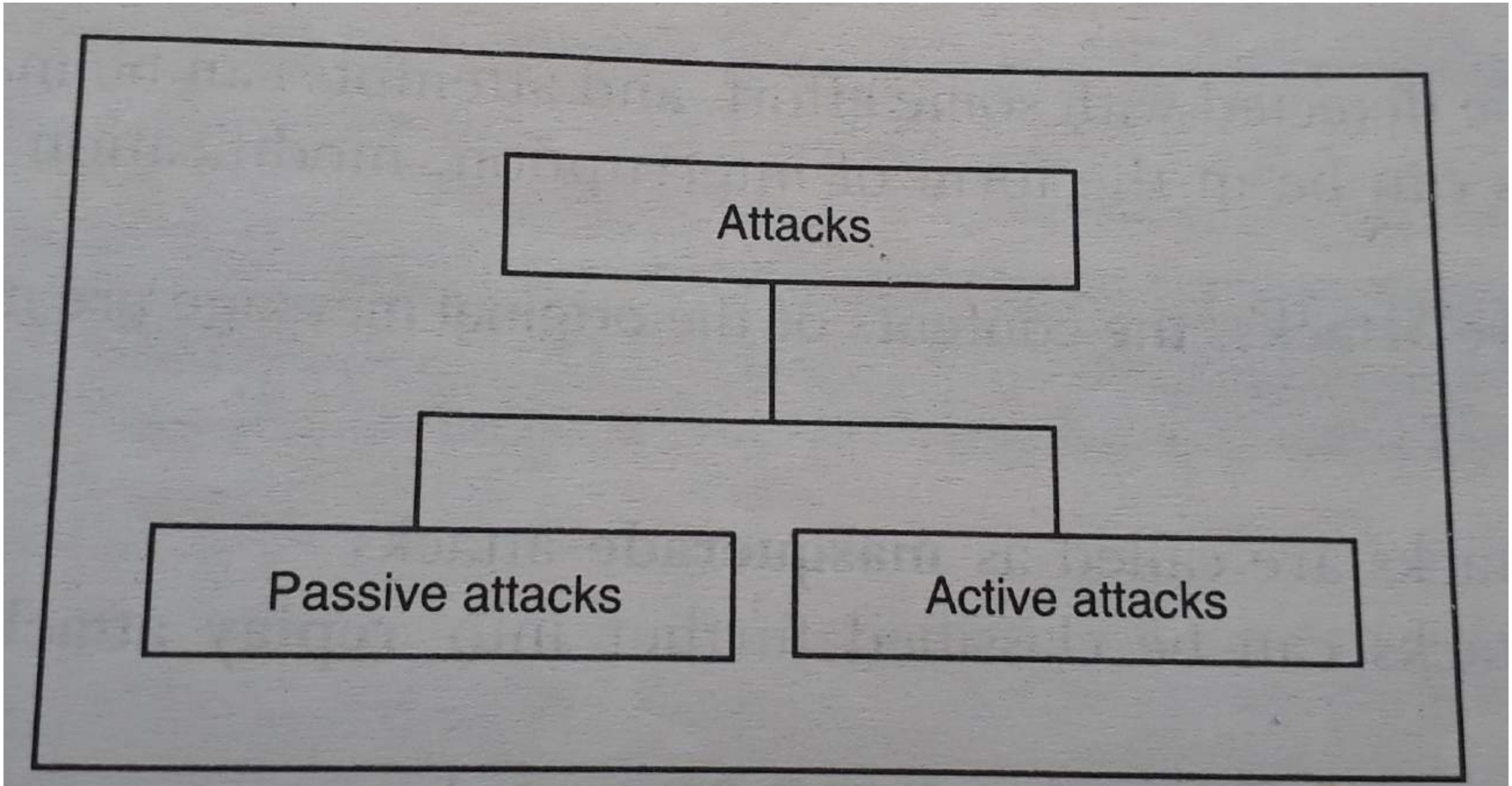
Interruption puts the availability of resources in danger.

Types of Attack

Broad Categories

1) Theoretical concepts behind the attacks
2) Practical approaches used by the attackers

Theoretical Concepts



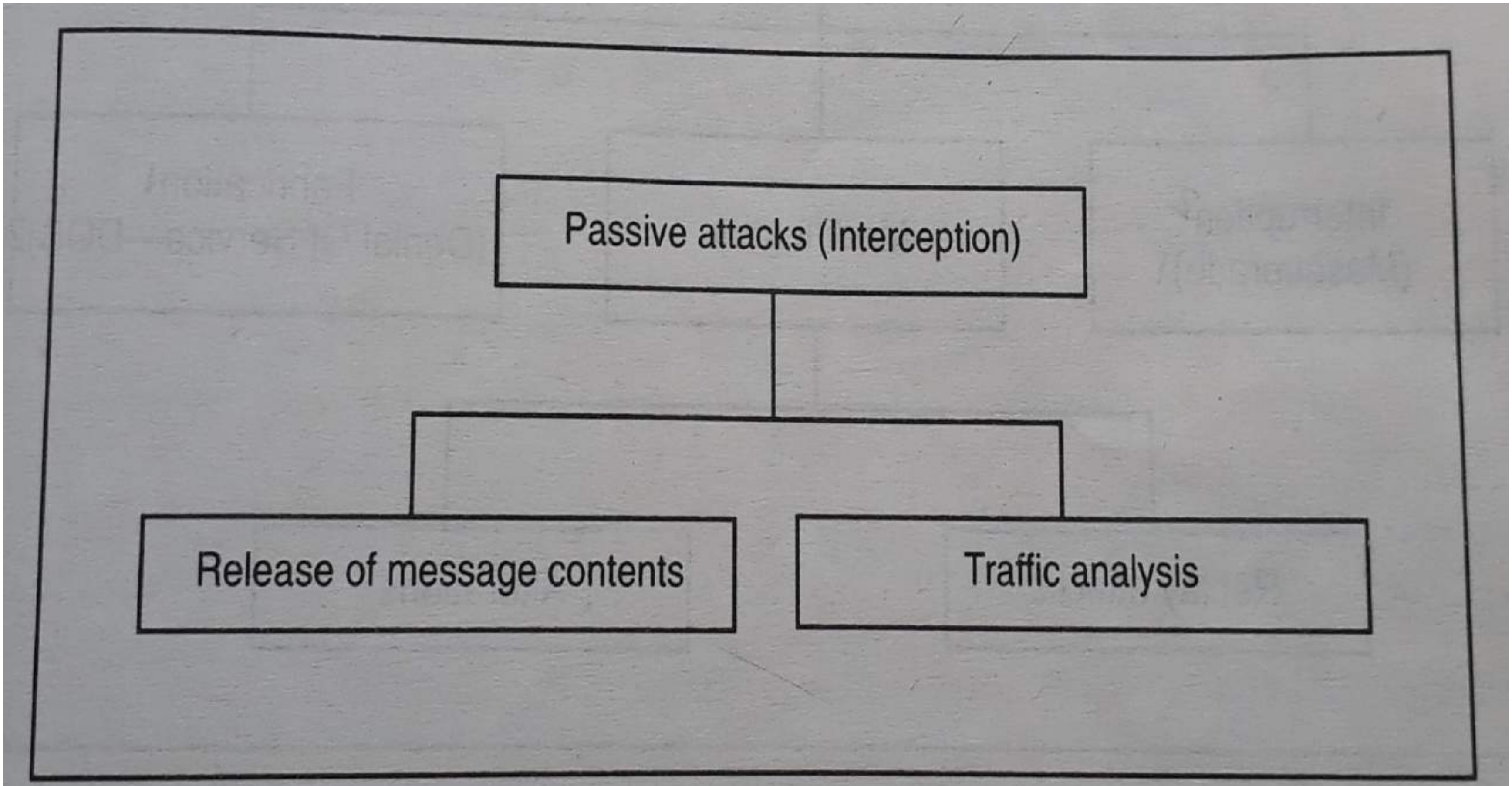
Attacks

Passive attacks

Active attacks

Fig. 5 : *Types of attacks*

Passive Attacks



Passive attacks (Interception)

Release of message contents

Traffic analysis

Fig. 6 : *Passive attacks*

Active Attacks

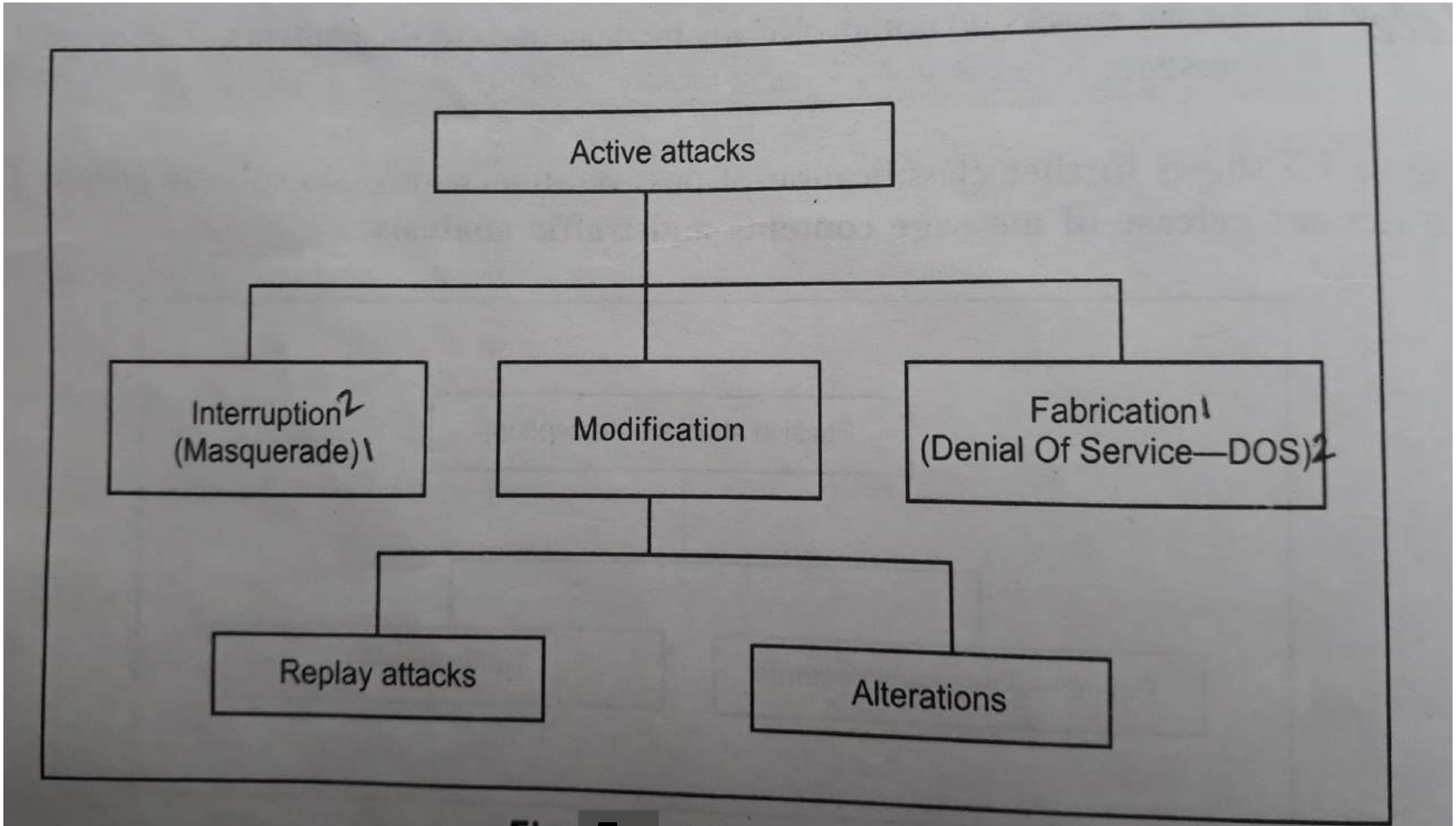


Fig. 7 : *Active attacks*

The Practical Side of Attacks

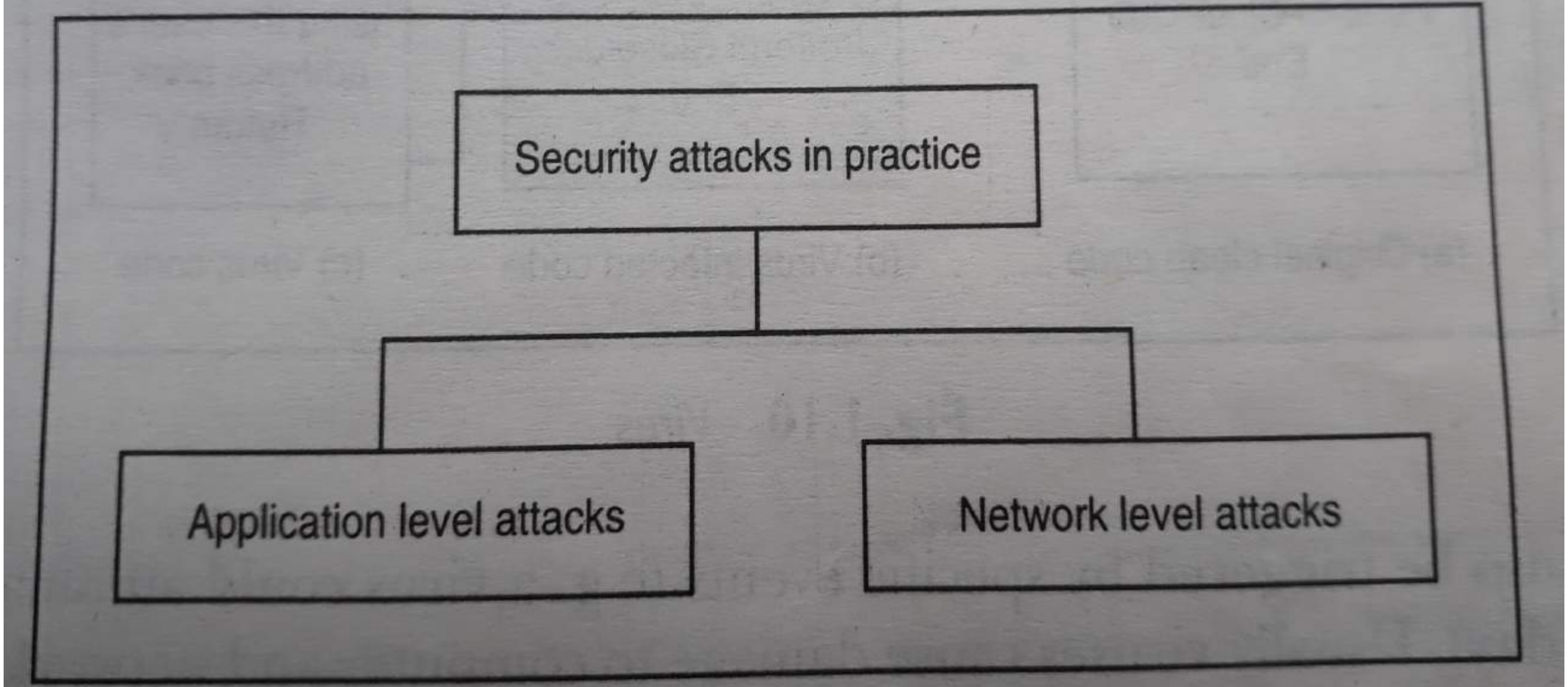


Fig. 8 : *Practical side of attacks*

Specific Attacks

1) Packet Sniffing (Snooping) / IP Sniffing
2) Packet Spoofing / IP Spoofing

Next Topic

Basic Cryptographic Techniques

a) Substitution Techniques

b) Transposition techniques

Thank You

QUESTIONS?