Data Transmission on the Internet

- Data travels in clear text
- Personal or confidential information is not secure
- Example: Credit card details

Transmission of Credit Card Details

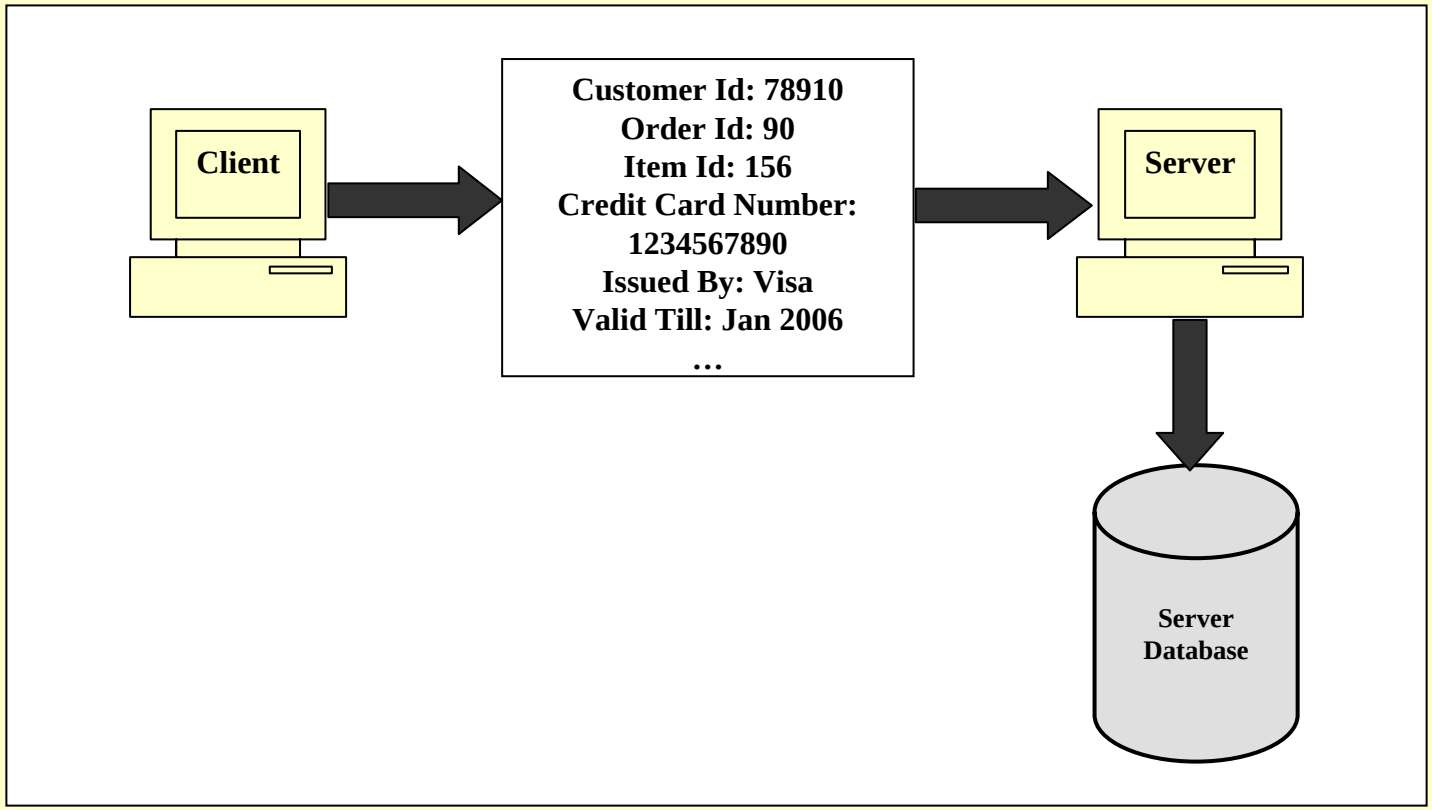


Fig 1.1

Confidentiality

- Also called as *privacy*
- Refers to the secrecy of information
- Only the sender and the receiver should have an access to the information

Loss of Confidentiality

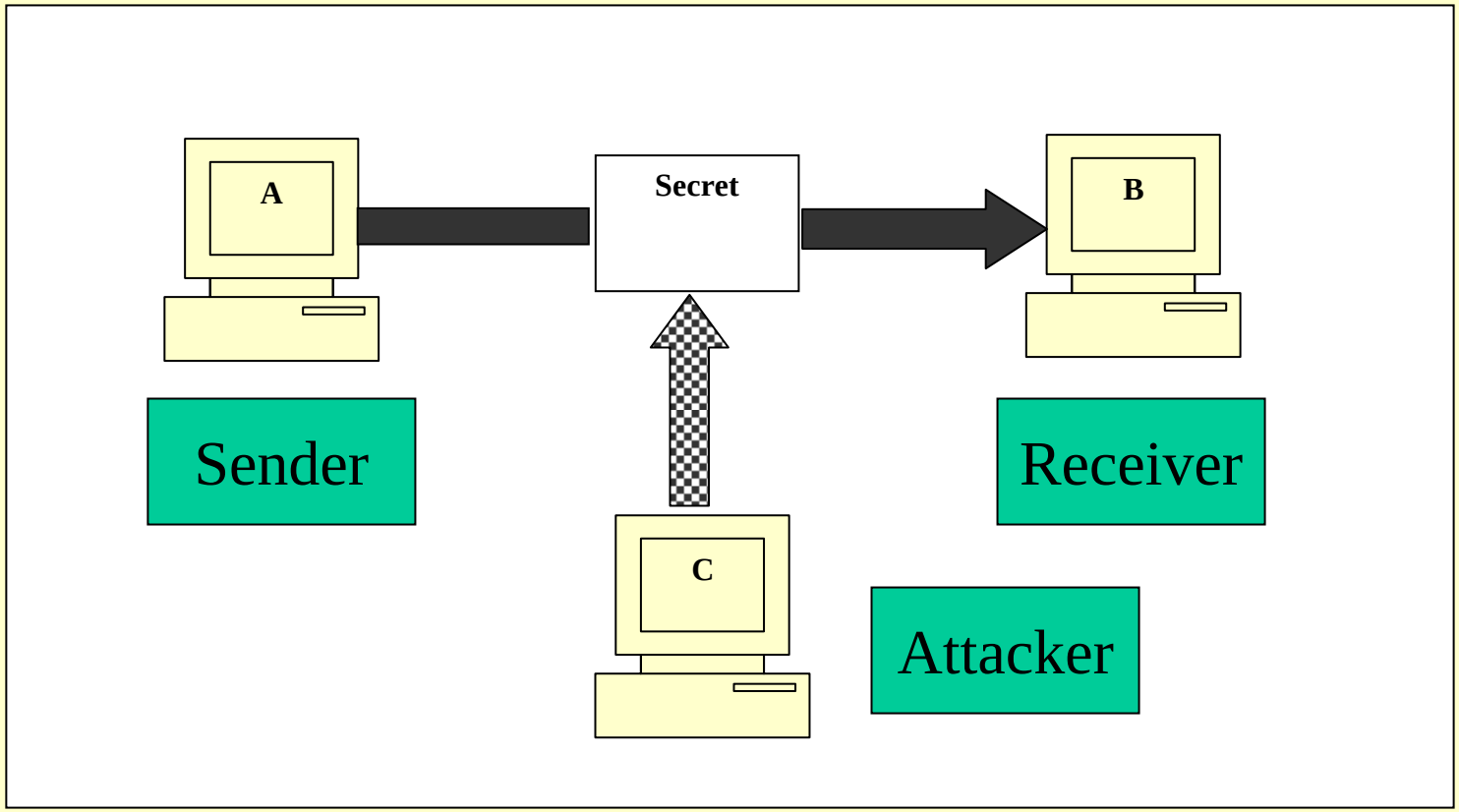


Fig 1.2

Authentication

- Identifies the sender/receiver of a message
- Required so that the communicating parties trust each other
- Answers *who is who*

Absence of Authentication

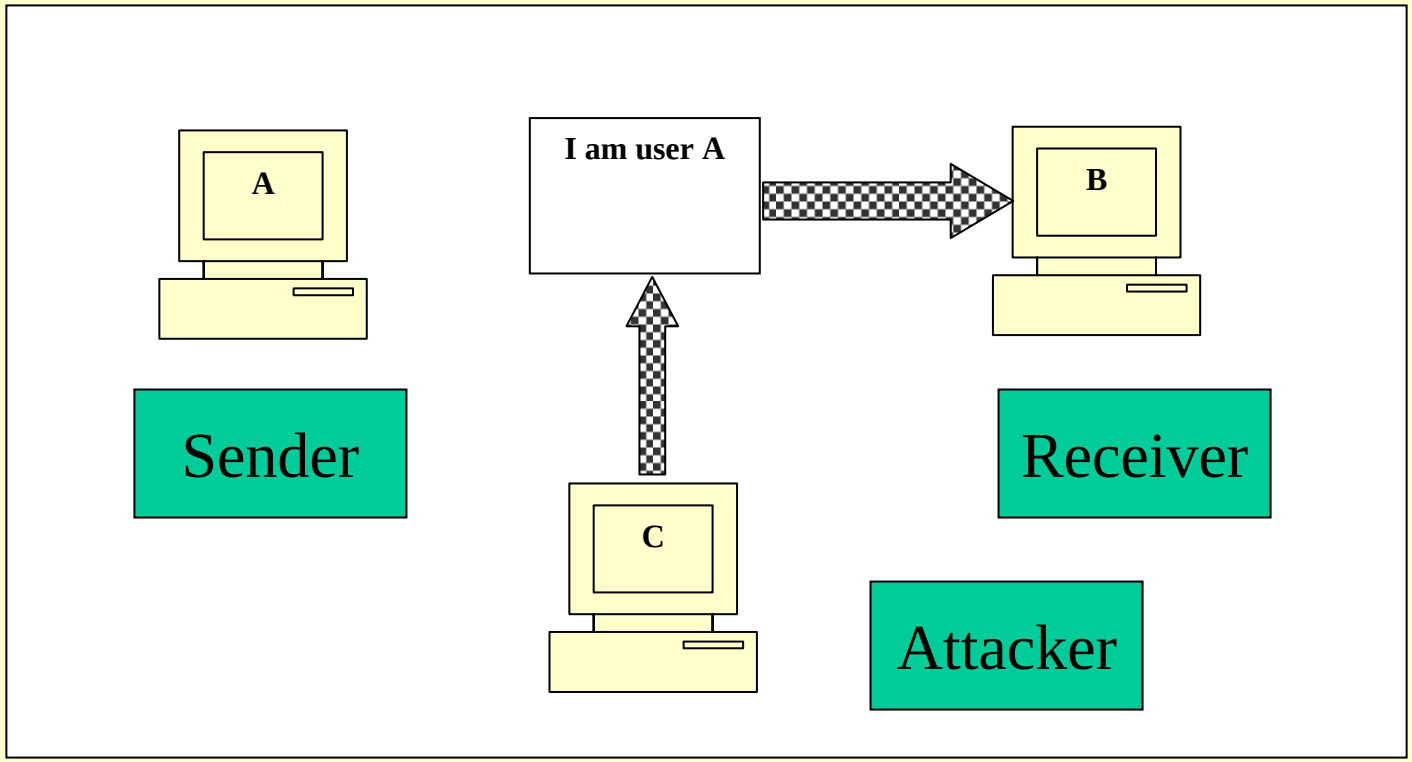


Fig 1.3

Integrity

- Ensures that any changes to a message are detected
- The message from the sender to the receiver must travel without any alterations
- Changes need to be prevented, or at least, detected

Loss of Message Integrity

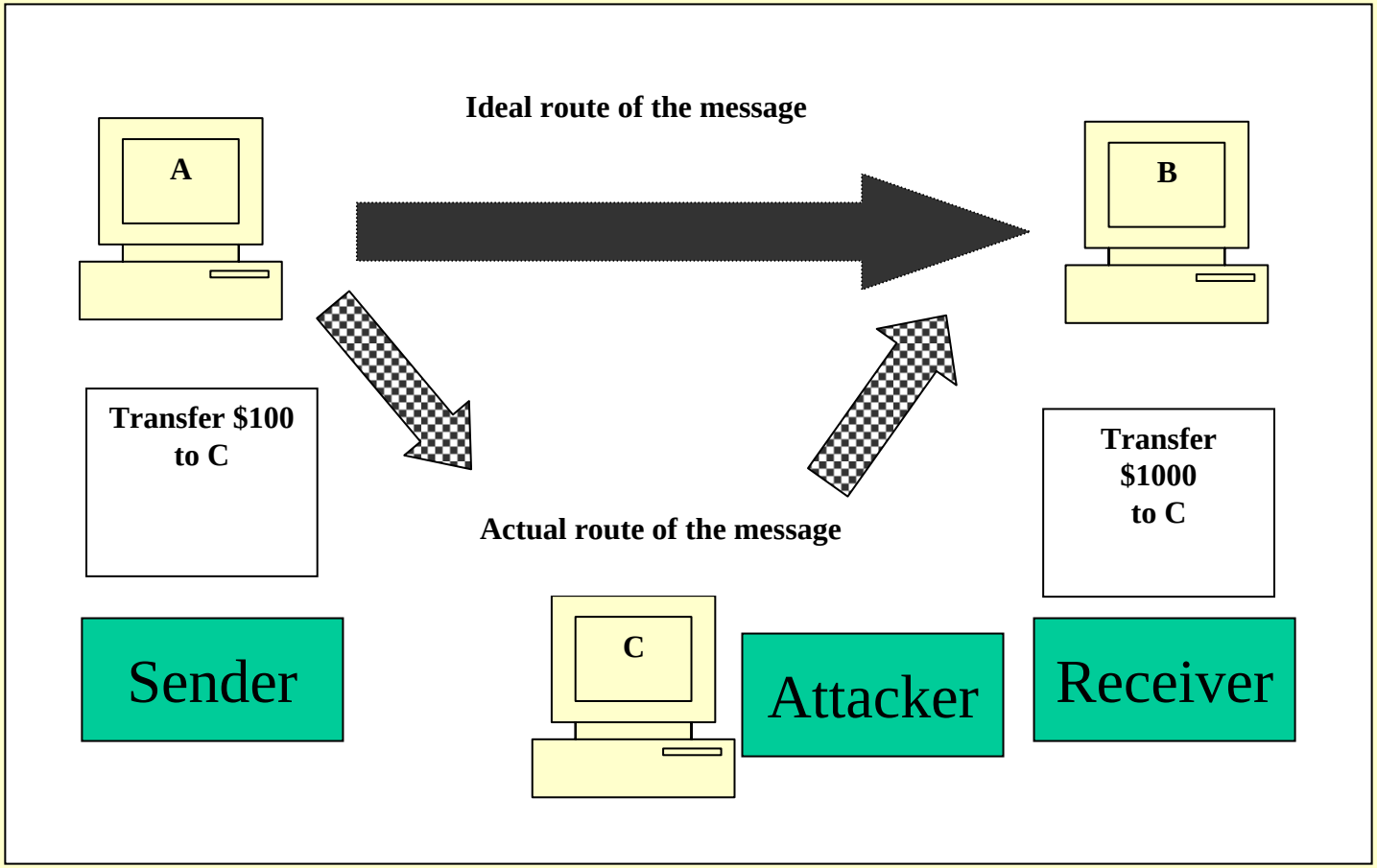


Fig 1.4

Availability

- Resources/applications must be available to authentic users all the time
- Attackers can deny the availability
- *Denial Of Service (DOS)* is an example of an attack on availability

Attack on Availability

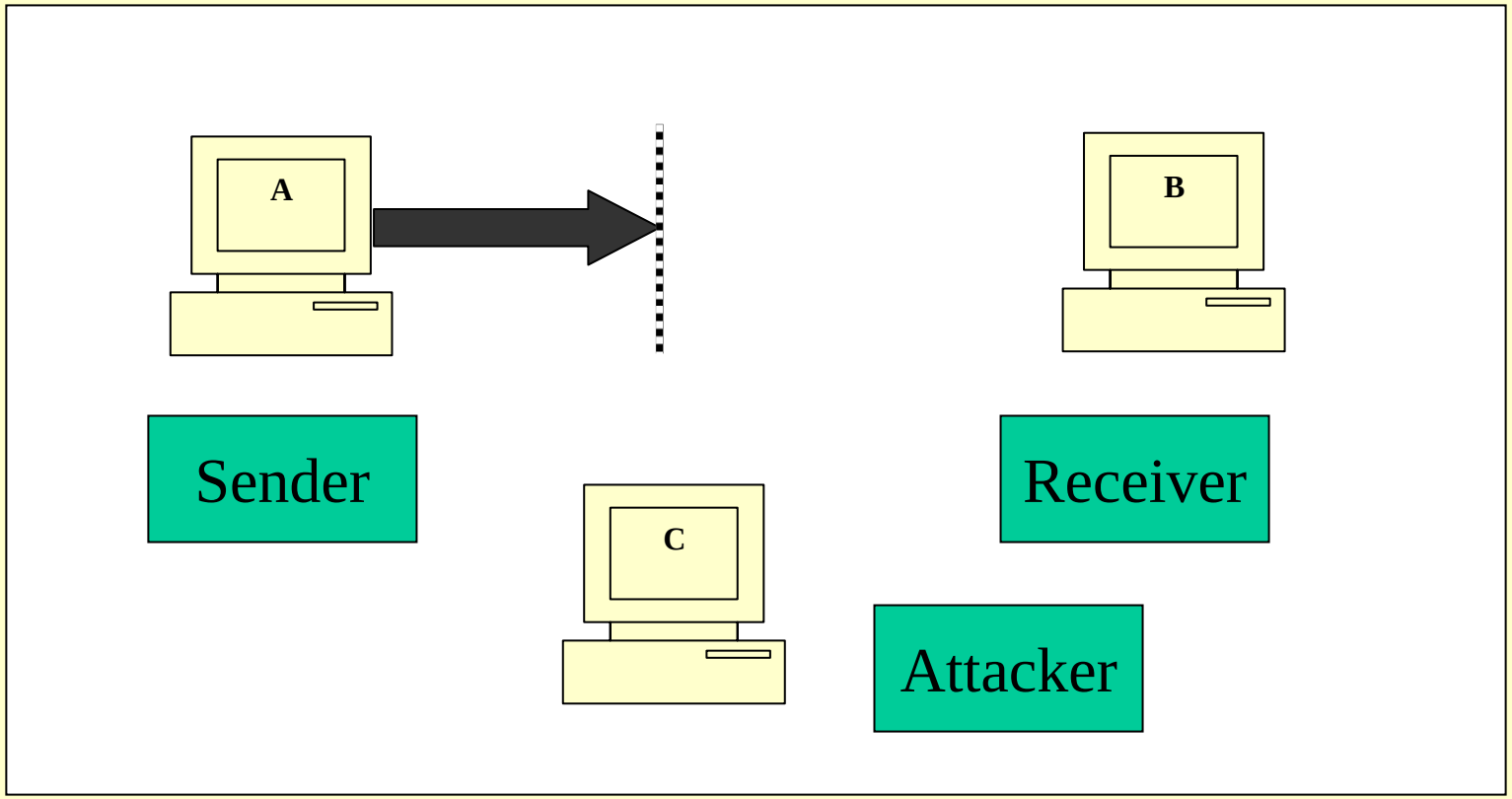


Fig 1.5

Types of Attacks

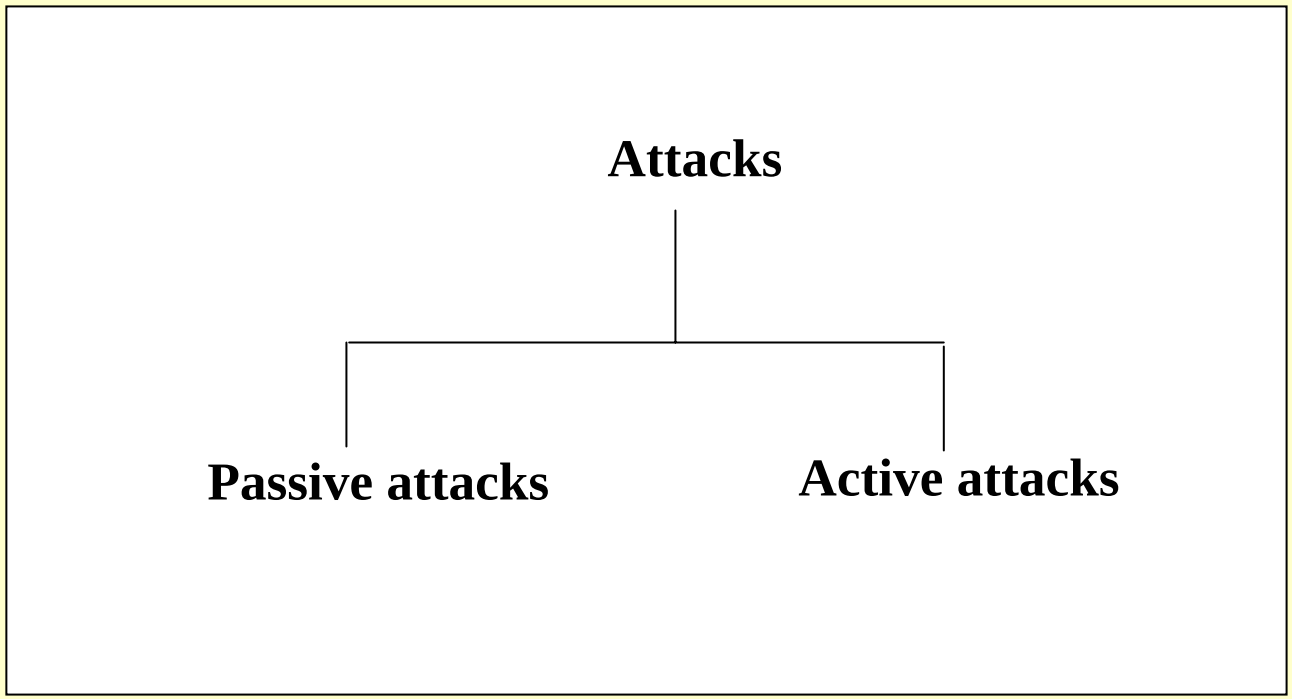


Fig 1.6

Classification of Passive Attacks

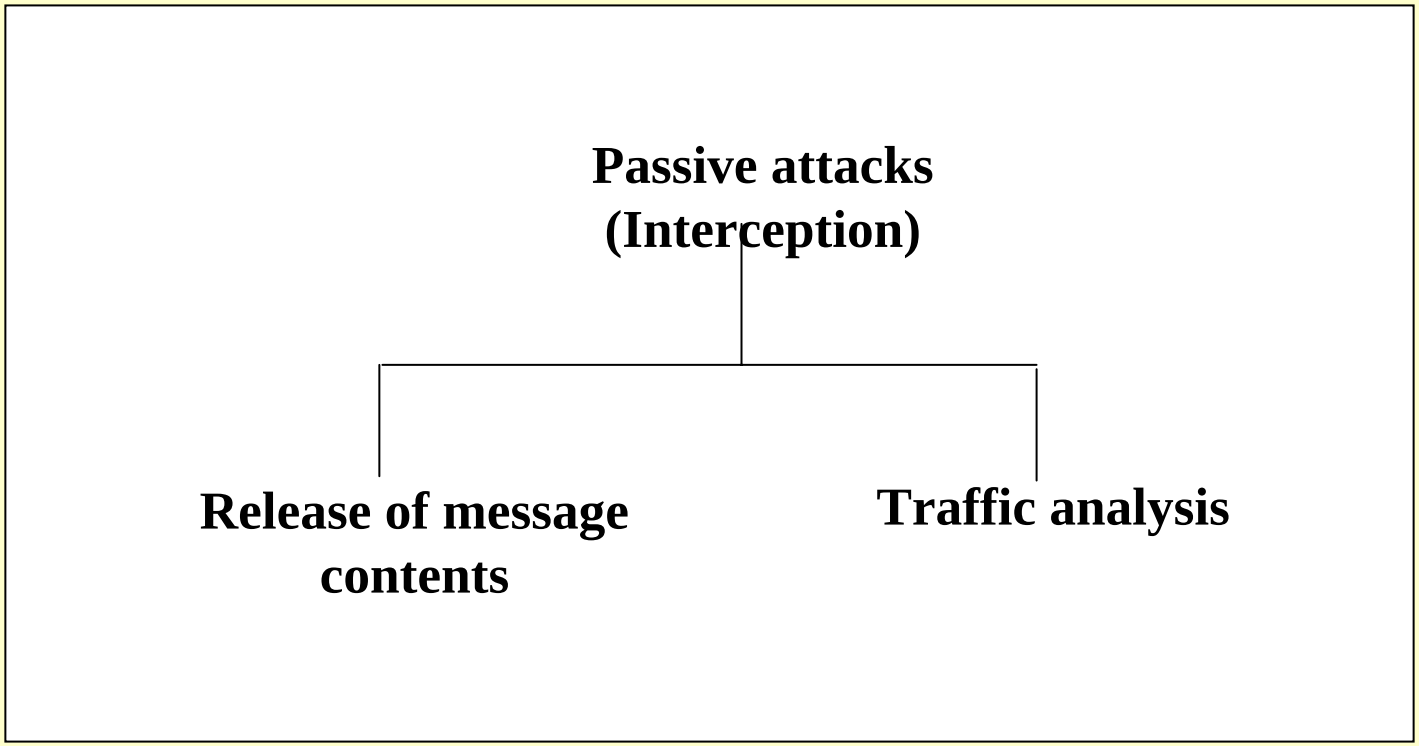


Fig 1.7

Classification of Active Attacks

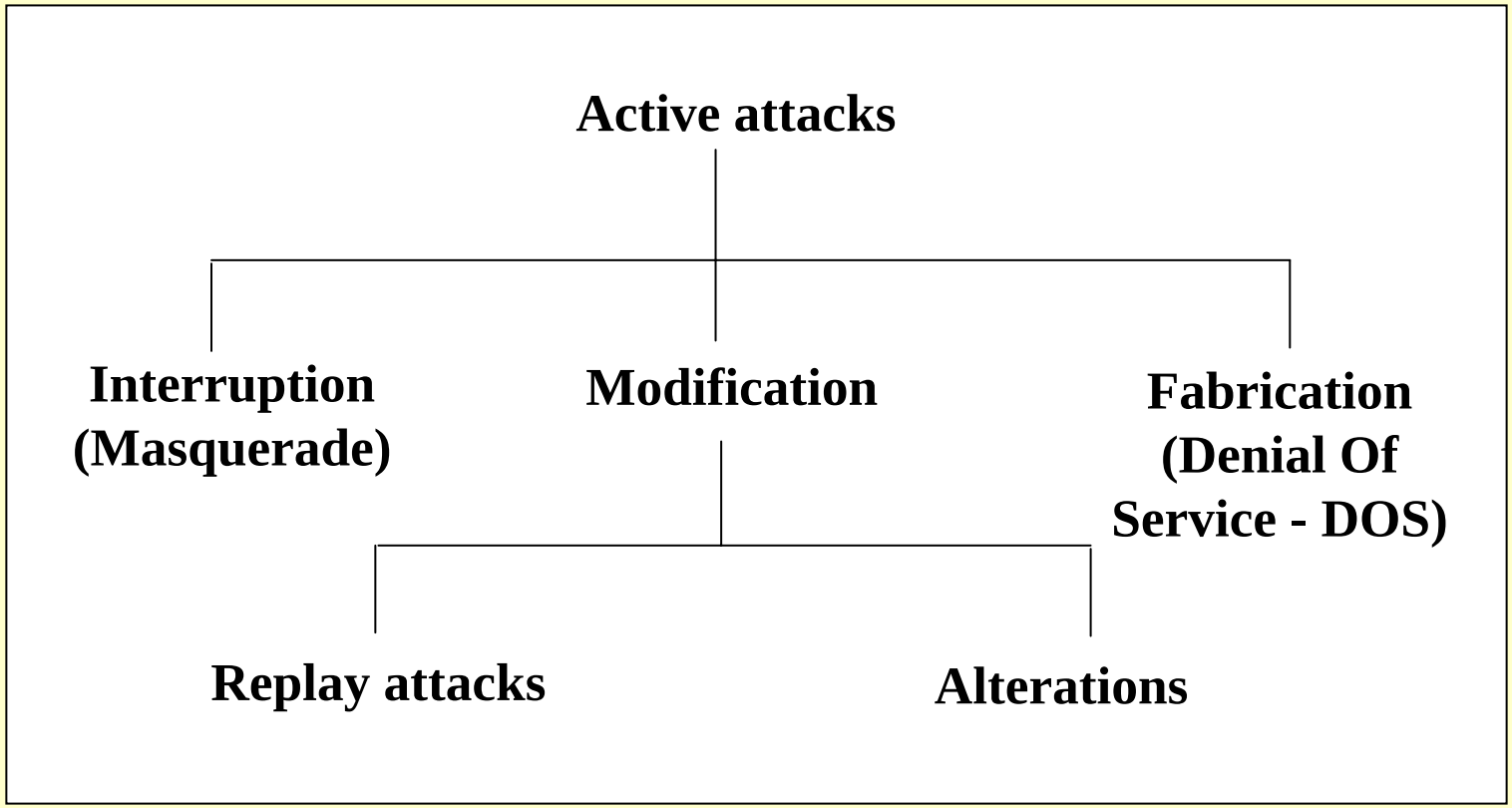


Fig 1.8

Practical Side of Attacks

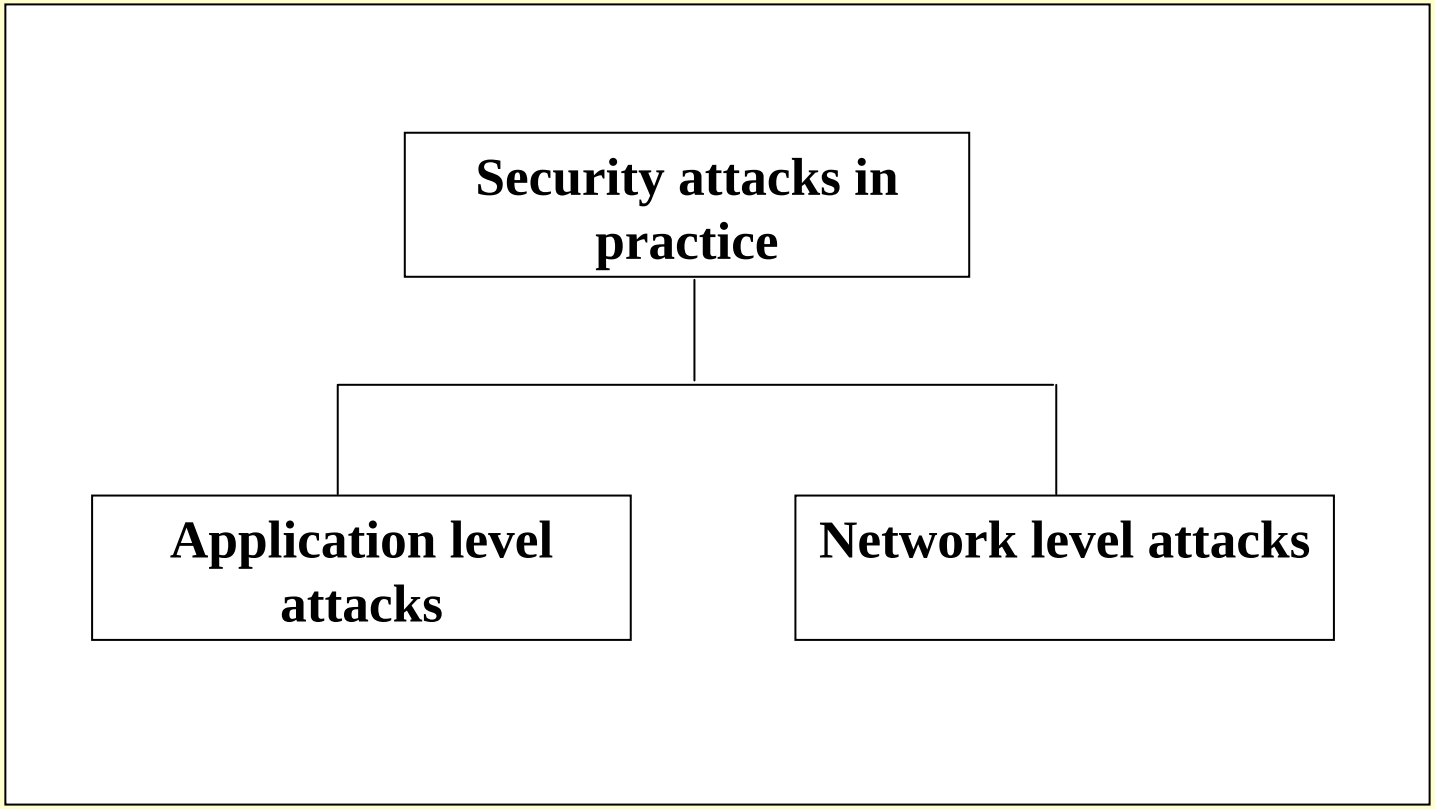


Fig 1.9

Virus

- Program that causes damage to other programs/applications/data
- Contains malicious code
- Propagates as it damages

Example of Virus

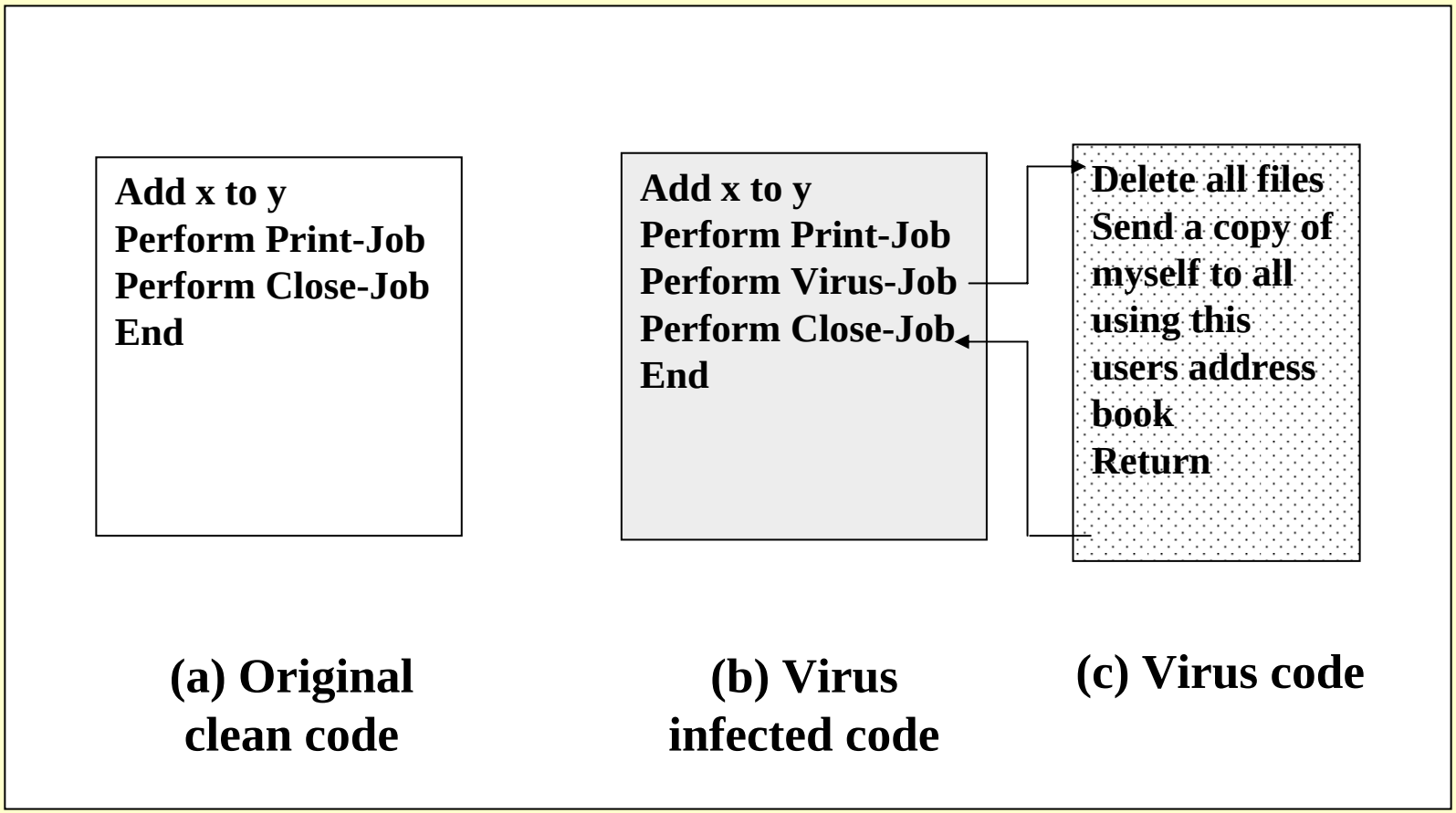


Fig 1.10

Worm

- Propagates as it damages
- Does not damage a program/data
- Consumes resources, and brings system to a halt

Example of Worm

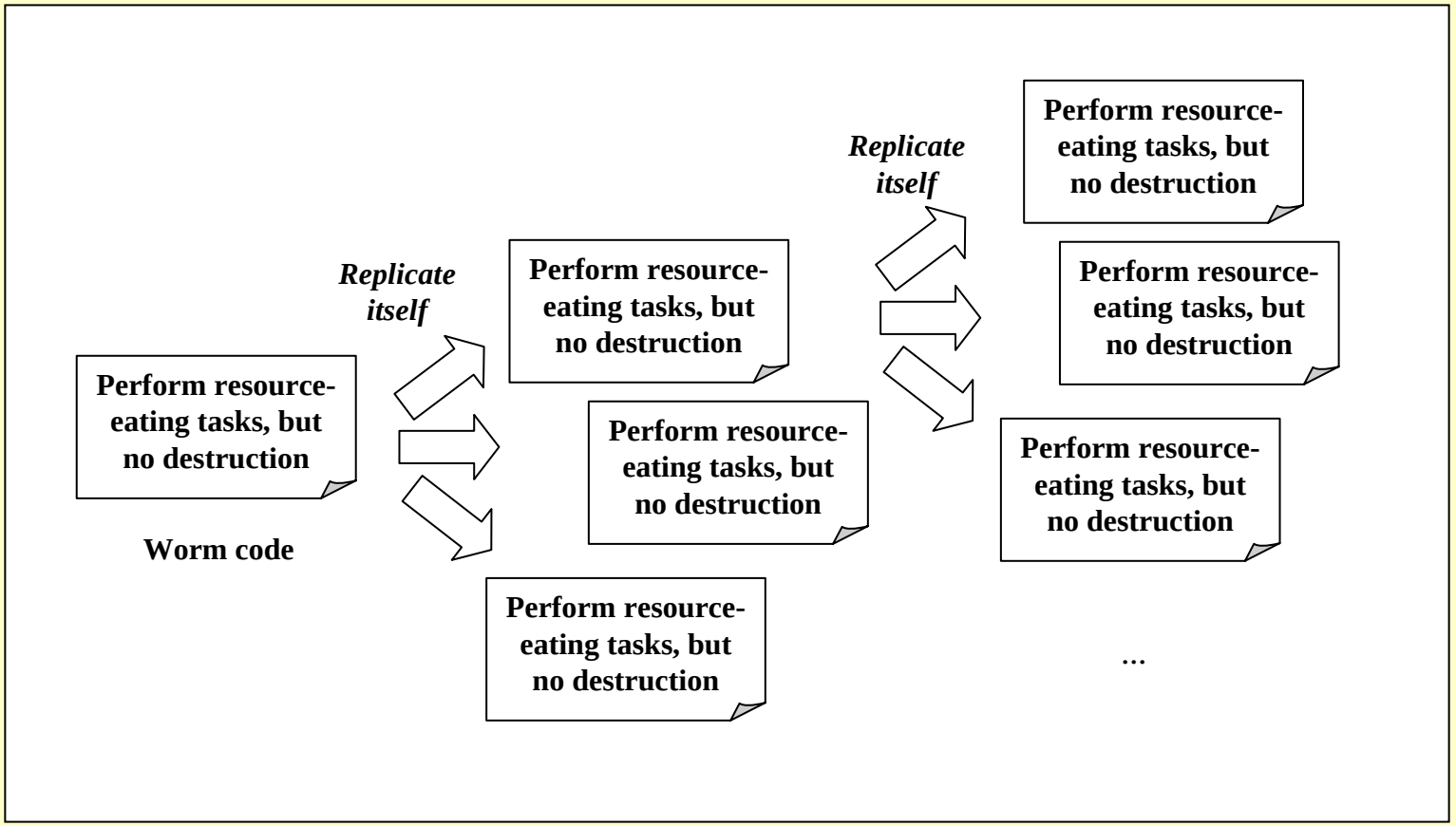


Fig 1.11

Trojan Horse

- Silently observes user actions and captures confidential information
- Uses captured information for its use
- Example: Capturing user id and password

Example of Trojan Horse

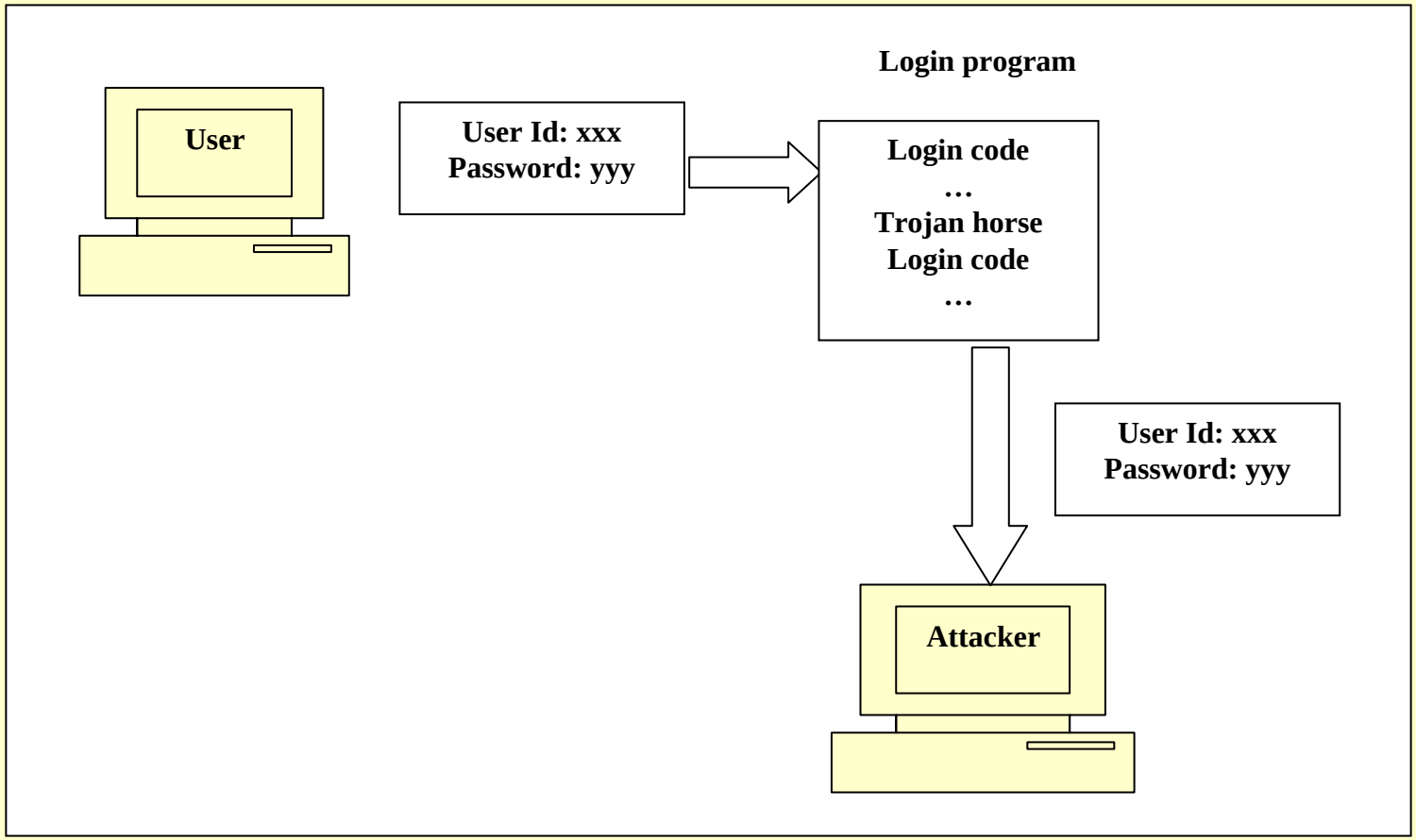


Fig 1.12

HTTP Protocol

- Hyper Text Transfer Protocol
- Used for communication between a browser and server on the Internet
- Based on a Request-Response model

HTTP Protocol

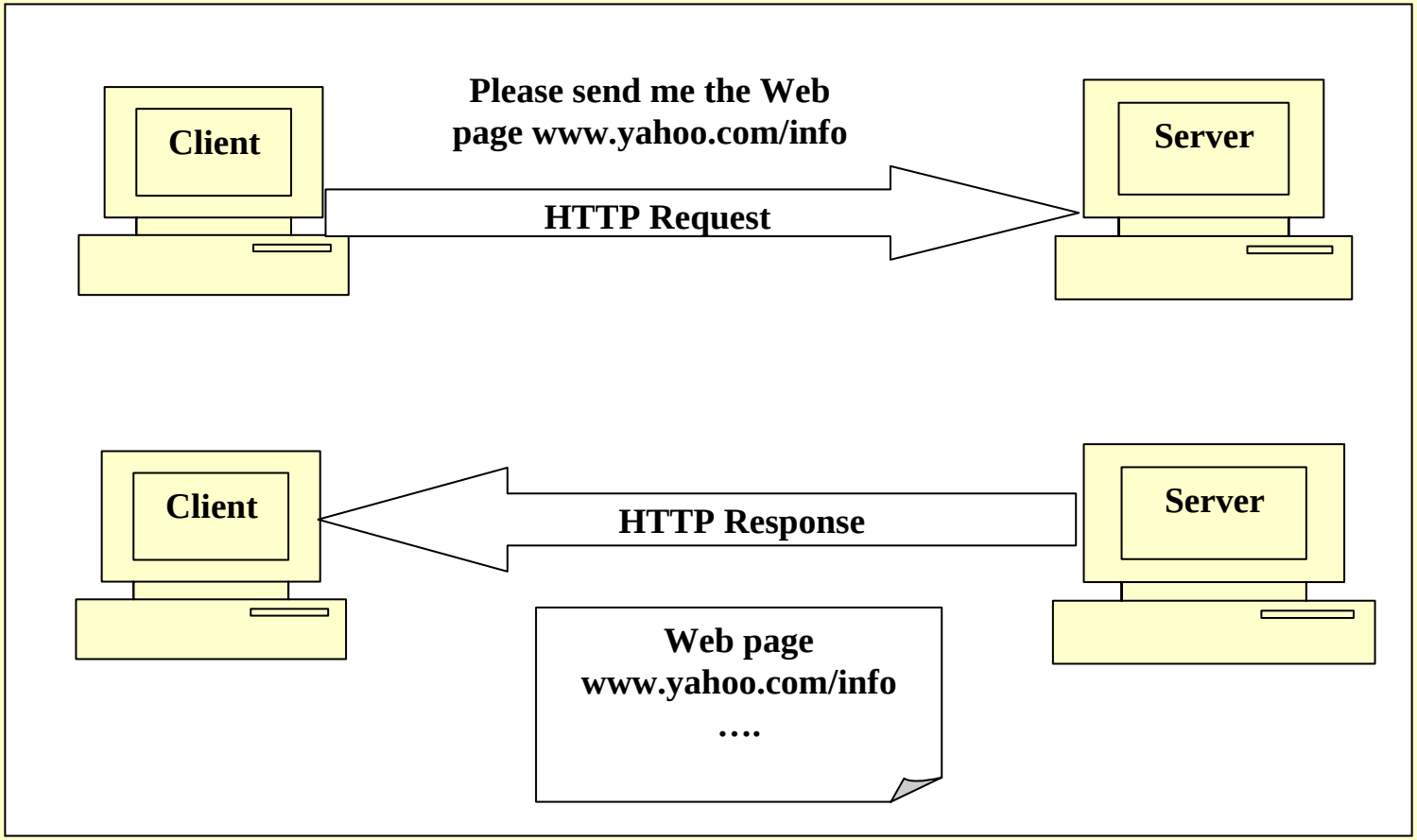


Fig 1.13

Java Applet/ActiveX Control

- Small programs that get downloaded along with an HTML page to the client
- Executes on the client browser
- Makes Web pages *active*

Web Page containing Applet

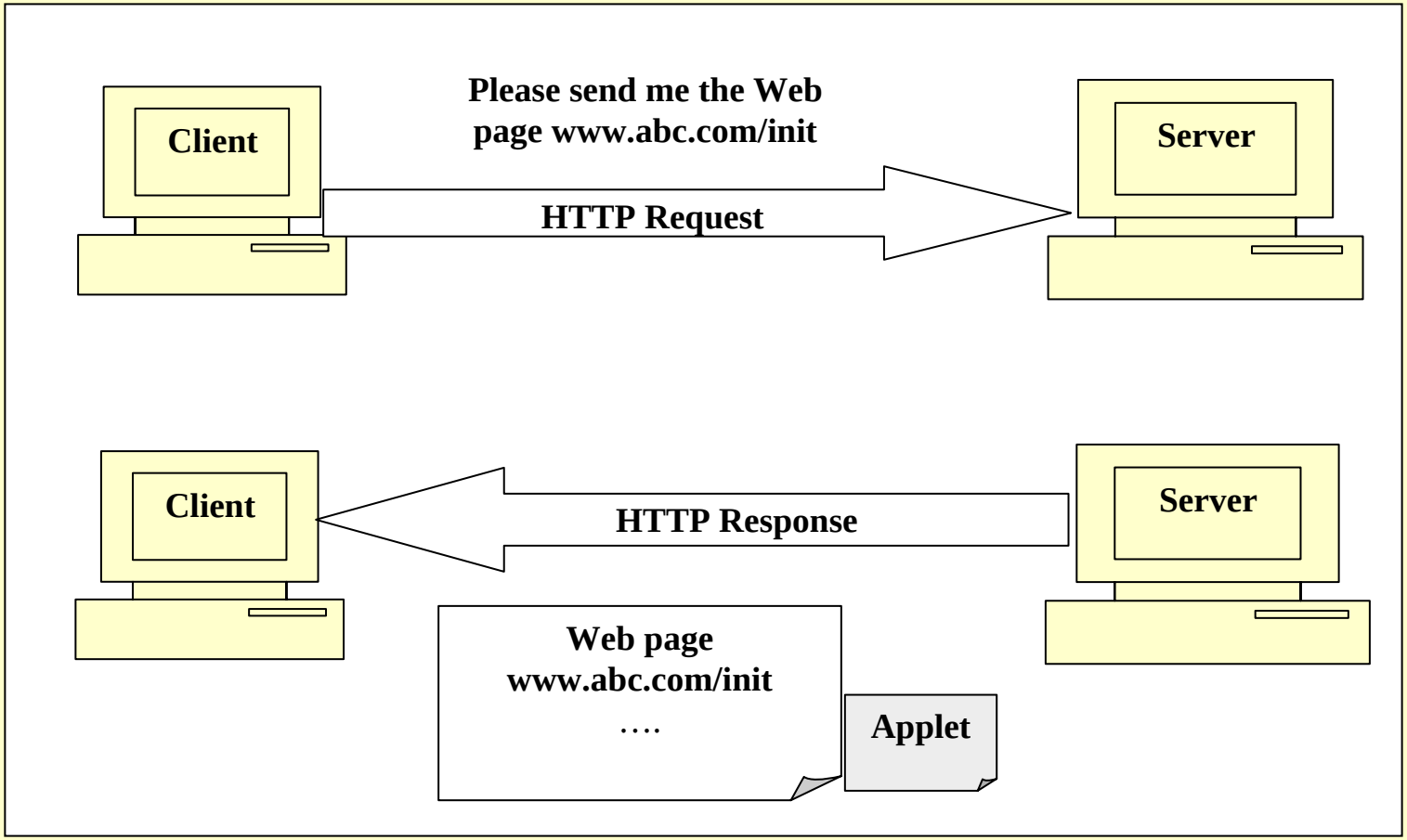


Fig 1.14

Cookie

- HTTP protocol is stateless
- For client to remember its *state*, some mechanism is needed
- Cookie allows client to remember its state

Cookie Creation

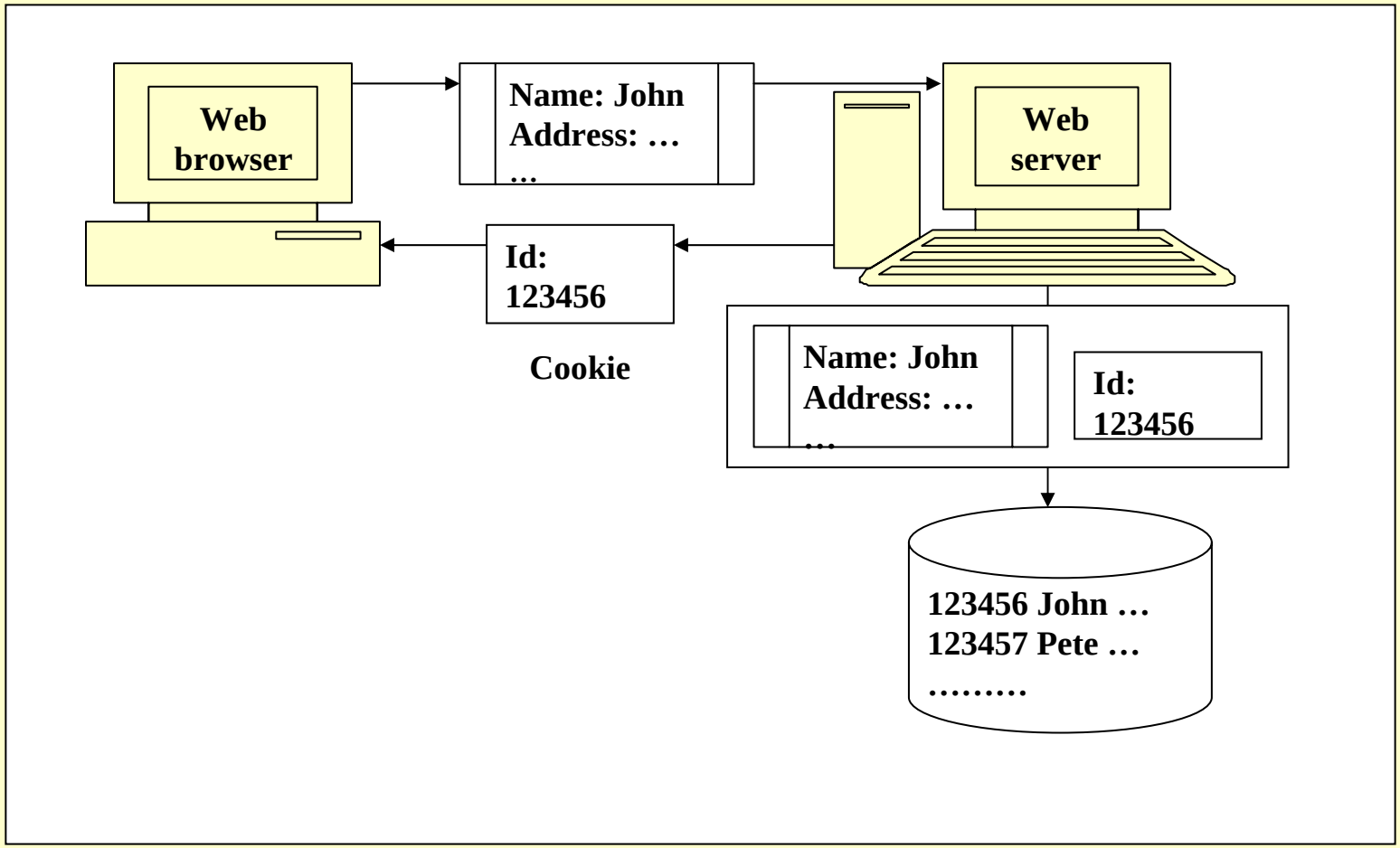


Fig 1.15 (a)

Cookie Usage

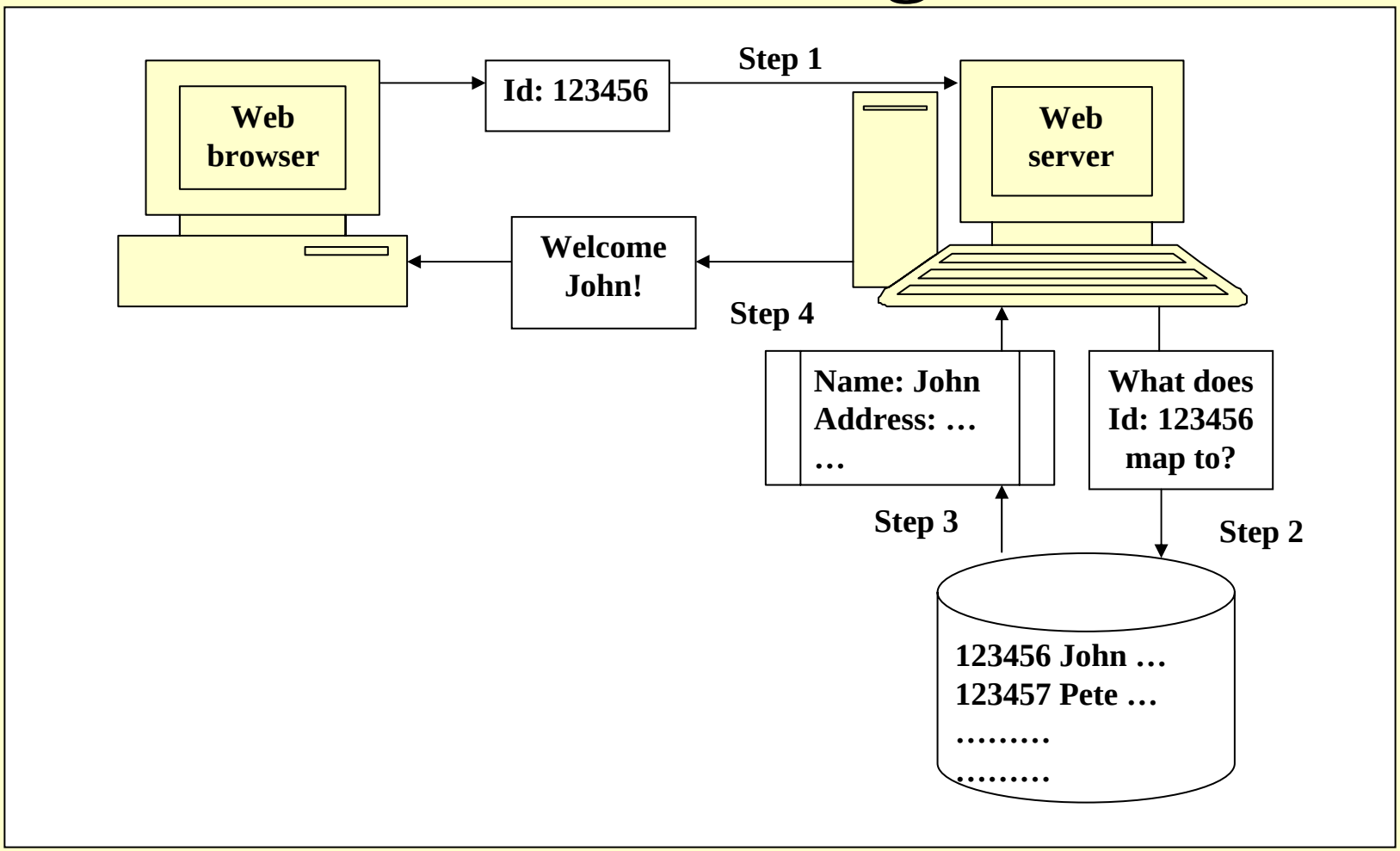
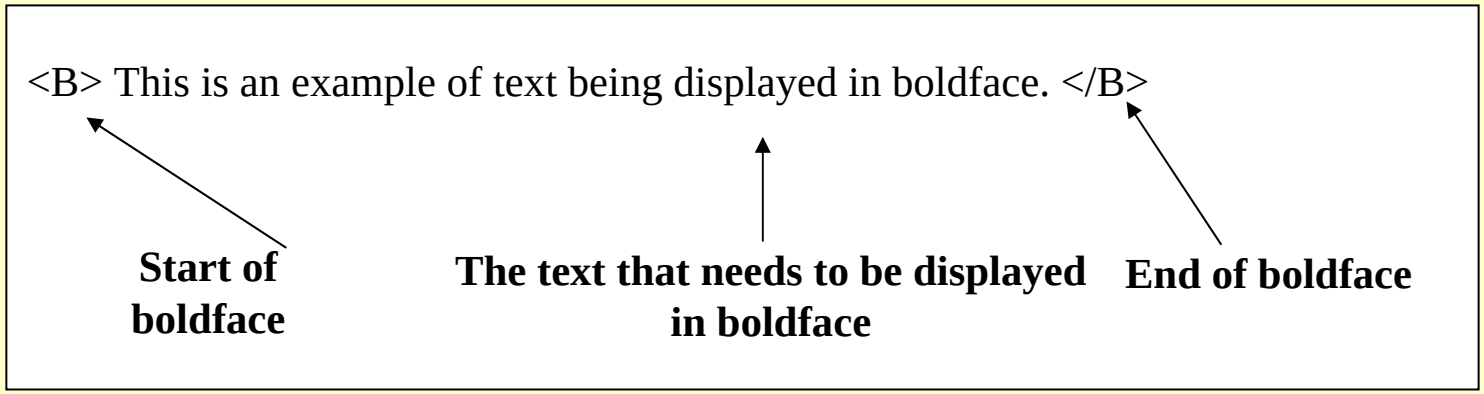


Fig 1.15 (b)

HTML

- Hyper Text Markup Language
- Tag-based language used to create Web pages
- Browser can interpret HTML

Example of HTML Tags



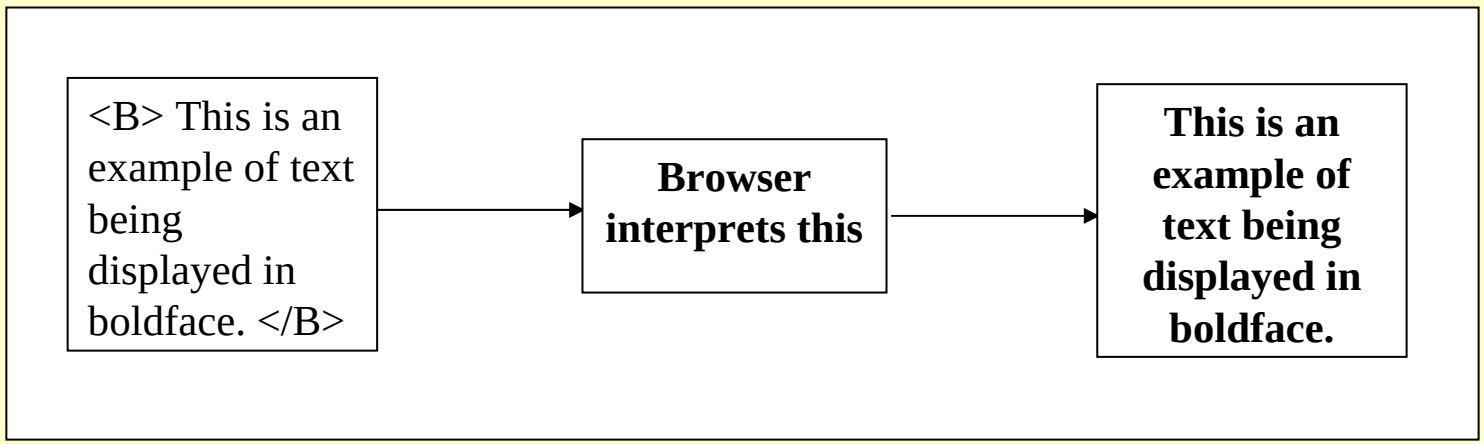


Fig 1.16, 1.17

Java Security

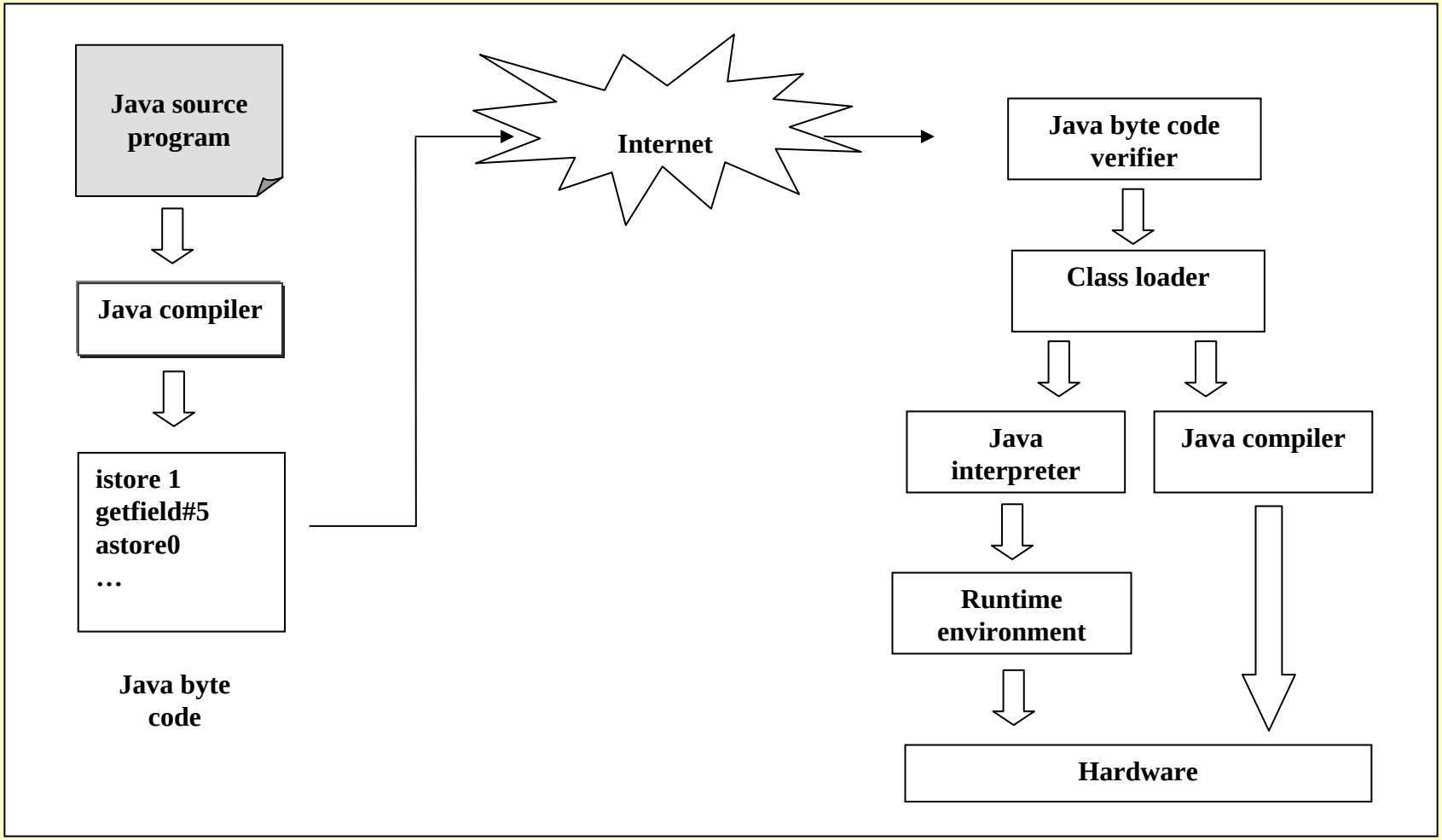


Fig 1.18