MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

MONASH University
Information Technology

FIT2093 INTRODUCTION TO SECURITY

Lecture 1:
Introduction to cyber security

Unit Structure

- Introduction to cyber security
- Authentication
- Access Control
- Fundamental concepts of cryptography
- Symmetric encryption techniques
- Introduction to number theory
- Public key cryptography
- Integrity management
- Practical aspects of cyber security
- Hacking and countermeasures
- Database security
- IT risk management & Ethics and privacy

LN1:Outline

- Define what we mean by cyber security
- Brief history of IT security
- Terminology
- Security concepts
- Functional requirements of security
- Security architecture
- Security strategy

What you mean by cyber security?

- **Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access**
- **In a computing context, security includes both cyber security and physical security**

Defining security

- **The security of a system, application, or protocol is always relative to**
  - –a set of desired properties
  - –an adversary with specific capabilities
- **For example, standard file access permissions in Linux and Windows are not effective against an adversary who can boot from a CD**

History of IT Security

IT Security History – 1930s to 1940s

- **Cipher machine called Enigma was invented in 1918 by German engineer, Arthur Scherbius.**
- **Used by the Germans in WWII**

1960s

- The term “hacker” was introduced by a group of MIT (Massachusetts Institute of Technology) students.
- US Department of Defense created ARPANet, which later was developed as Internet.
- UNIX operating system was developed by Ken Thompson.
- C programming language was introduced by Dennis Ritchie

Dennis Ritchie

Ken Thompson

PDP-1

1970s

- **Bolt, Beranek and Newman introduced TELNET protocol which allowed public access to ARPANet.**
- **Steve Jobs and Steve Wozniak introduced Apple personal computer.**
  - PC becomes a springboard for remote attack on large computer system.
- **Jim Ellis and Tom Trusscott created USENET, a bulletin-board style system.**
  - It is popular forums for hackers to share information

1980s

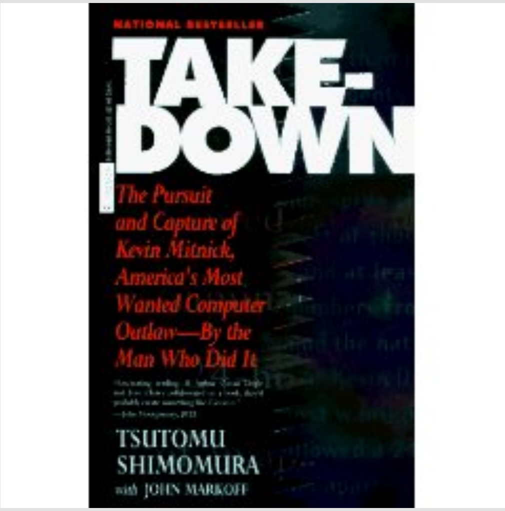
- **IBM introduced Intel 8086 PC. It is relatively inexpensive system which allowed the proliferation of PCs at homes and offices.**
- **TCP/IP.**
- **The Magazine 2600: The Hacker Quarterly is created.**
- **Hackers clubs**
  - 414 gangs, Legion of doom, Chaos Computer Club.
- **The Computer Fraud and Abuse Act was introduced in the US based on the case of Ian Murphy (Captain Zap).**
  - Morris “worm”
  - Herbert Zinn
- **Computer Emergency Response Team (CERT) was created by DARPA to alert computer users to the threats such as worms.**

1990s

- ARPANet was decommissioned → traffic was transferred to Internet.
- LINUX was introduced by Linus Torvalds.
- Web Browser was introduced which increased the public access to WWW.
- Prominent Hackers
  - Vladimir Levin
  - Kevin Mitnick.
  - Kevin Poulsen

adrian lamo, kevin mitnick, kevin poulsen

1990s


NATIONAL BESTSELLER
TAKE-DOWN
The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It
TSUTOMU SHIMOMURA
with JOHN MARKOFF

Tsutomu Shimomura

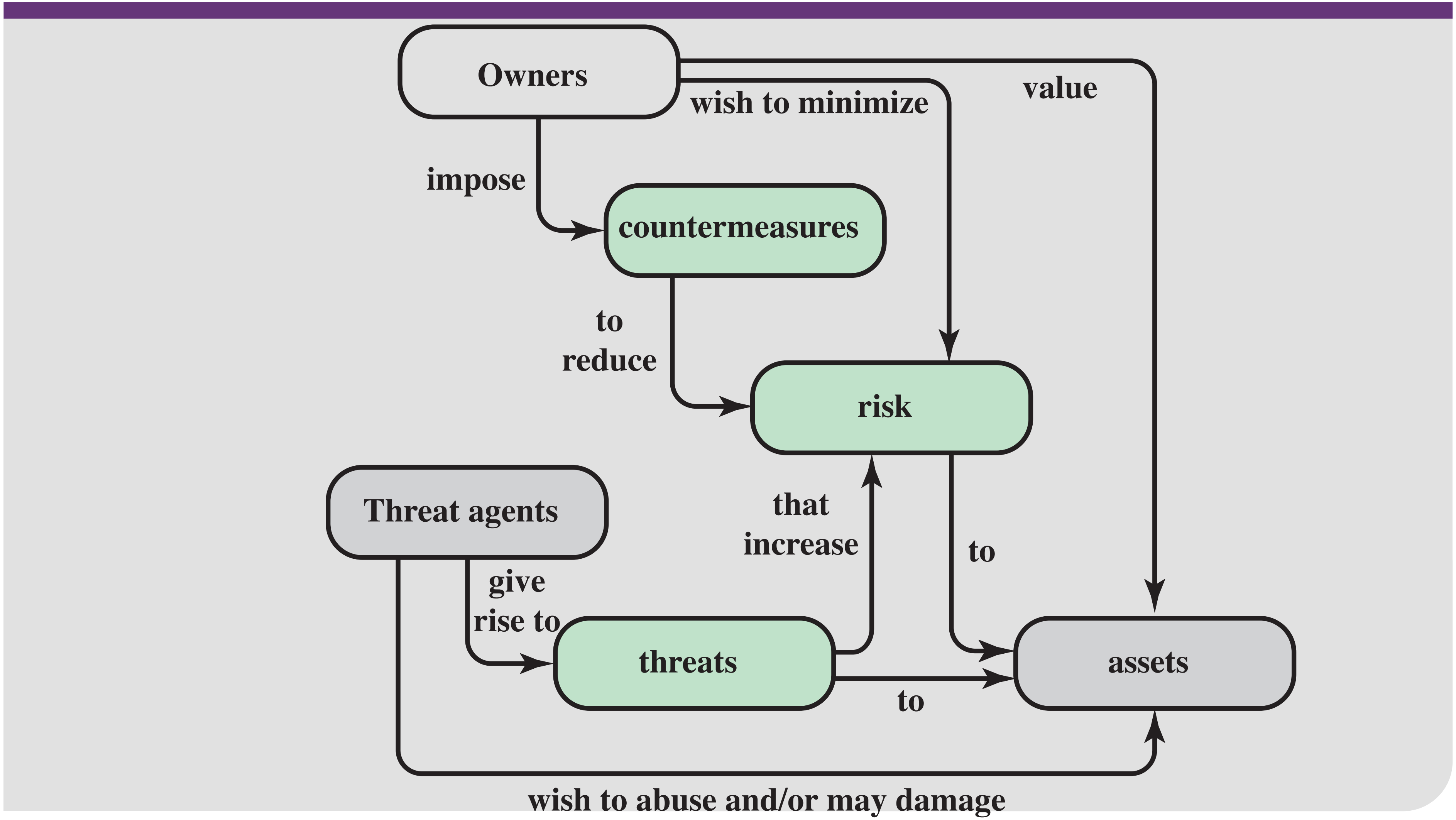
2000s….

- **Distributed Denial of Service attacked was unleashed in February 2000.**
- **Attacks by "common" people to gain monetary advantage.**
- **2010: Operation Aurora**
  - *targeted attack on Google's infrastructure originating from China*
- **2013: NY times, Adobe, Yahoo's email accounts hacked.**
- **Hacker Group in China linked to big cyber attacks: Symantec**
- **Cybercrime – major security threat today**

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. must decide where to deploy mechanisms
5. involve algorithms and secret info
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

Security Terminology



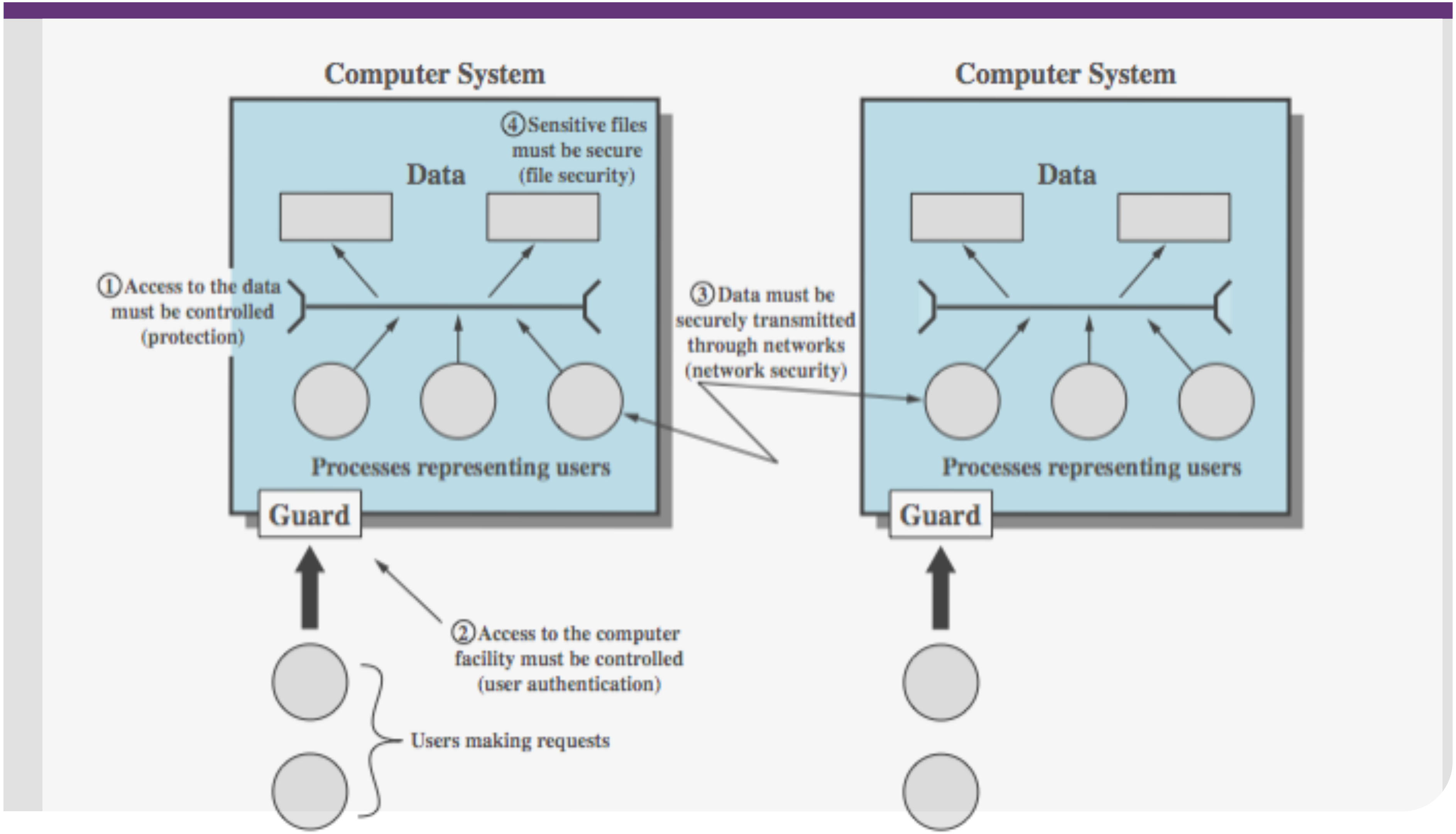
Other terms used are

- **Threat**
  - circumstances that have the potential to cause loss or harm
- **Vulnerability**
  - a weakness in a computer system that might be exploited to cause loss (of information) or harm (the contents)
- **Attack**
  - an action that exploits a vulnerability
  - any action that compromises the security of system and information owned by an organisation

Assets of a Computer System

- **What are we protecting?**
  - Hardware
    - Computer
    - Network
    - Infrastructure
  - Software
  - Data/Information
  - Communication facilities and networks

Scope of Computer Security


Computer System
Data
④Sensitive files must be secure (file security)
①Access to the data must be controlled (protection)
Processes representing users
Guard
③Data must be securely transmitted through networks (network security)
Computer System
Data
Processes representing users
Guard
②Access to the computer facility must be controlled (user authentication)
Users making requests

How the protection is achieved?

- **Prevention**
  - prevention – to avoid the breach of security (pre-emptive)
- **Detection**
  - Detection – investigate a security breach (post operation)
- **Recover**

Security Protection

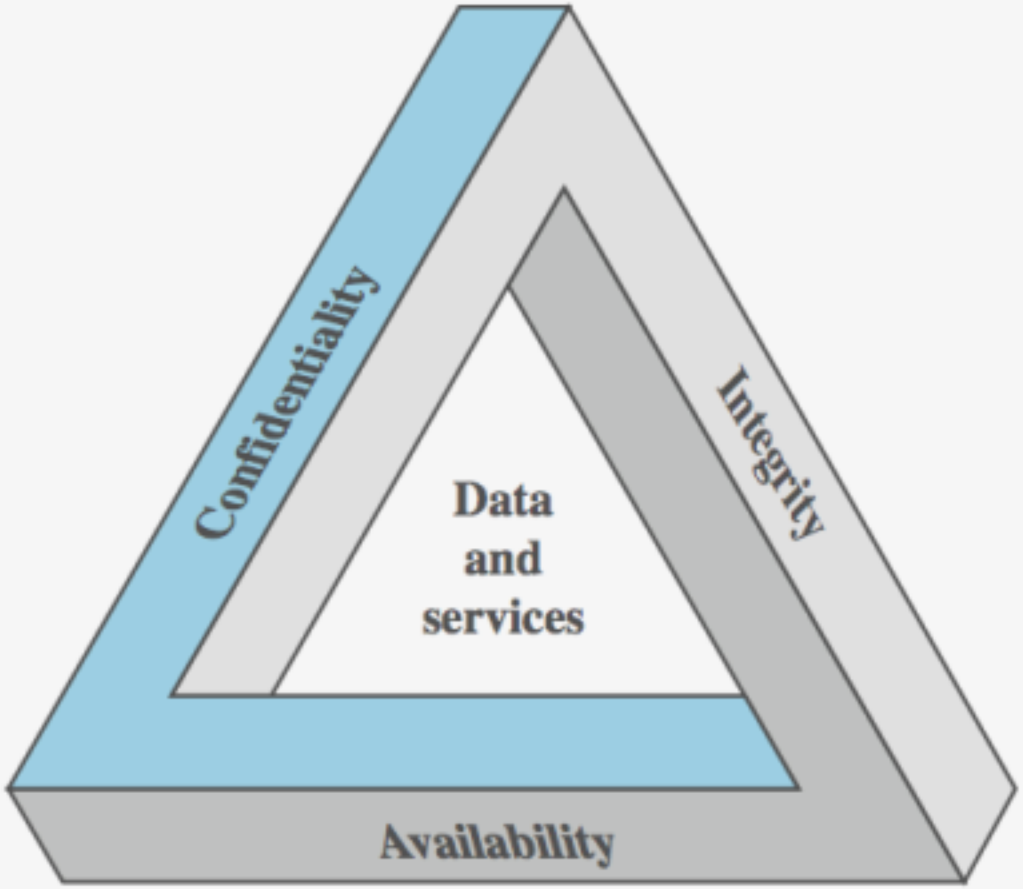
- **Physical Security Protection**
  - protecting IT infrastructure from physical damage from intentional destruction by individuals/natural disaster.
  - protecting IT infrastructure from physical access by unauthorised party.
- **Logical Security Protection (also known as information security)**
  - Protection of the information to preserve confidentiality, integrity and availability of information.

Properties that are being compromised

Security mechanism

- **designed to detect, prevent, or recover from a security attack.**
  - may need multiple mechanisms

Key Security Concepts



Levels of Impact

- **Low: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals**
- **Moderate: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals**
- **High: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals**

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Sensitive information can only be accessed by authorised parties
- Access can be in the form of:
  - reading, copying, distributing.
- A loss of confidentiality is the unauthorized disclosure of information.
- Tools for confidentiality: Encryption, Authentication, Access Control

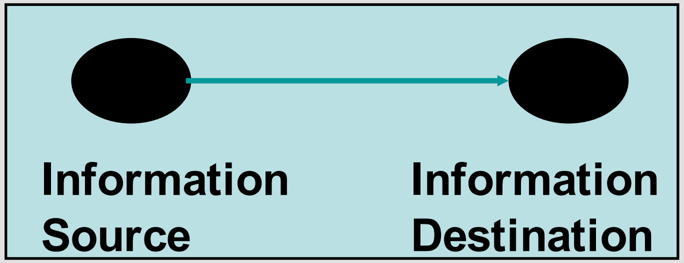
Integrity

- **Protecting information from unauthorised modification.**
- **To ensure the authenticity of the data.**
  - – data should be genuine, not merely “appear” to be genuine.
  - – Authenticity refers to the truthfulness of origins
- **Ensuring information non-repudiation**
  - – prevents either sender or receiver from denying a transmitted message
- **Tools for Integrity: Backups, checksums, digital signatures**

Availability

- **The information should be accessible and useable (without delay) upon demand by an authorised entity.**
- **Tools:**
  - Physical protections
  - Computational redundancies: computers and storage devices that serve as fallbacks in the case of failures.

Security

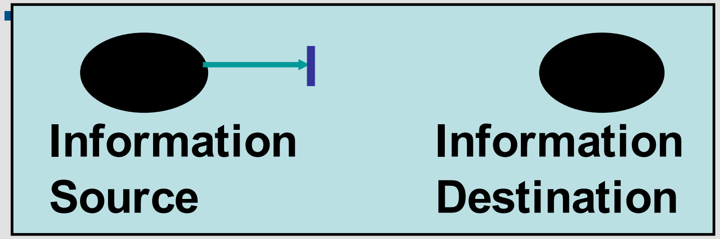


Normal

Source and Destination - can be what is supposed to be and what you get

Security Attack : Interruption

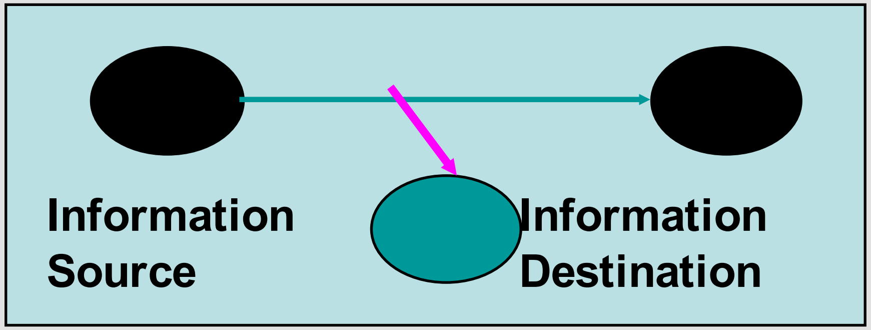
- Also known as ***denial of services***.
- Information resources (hardware, software and data) are deliberately made unavailable, lost or unusable, usually through malicious destruction.
- e.g: cutting your home phone/cable modem line, disabling a file management system, email spam to fill up the mail queue and slow down an email server, etc.



Interruption – Attack on Availability

Security Attack : Interception

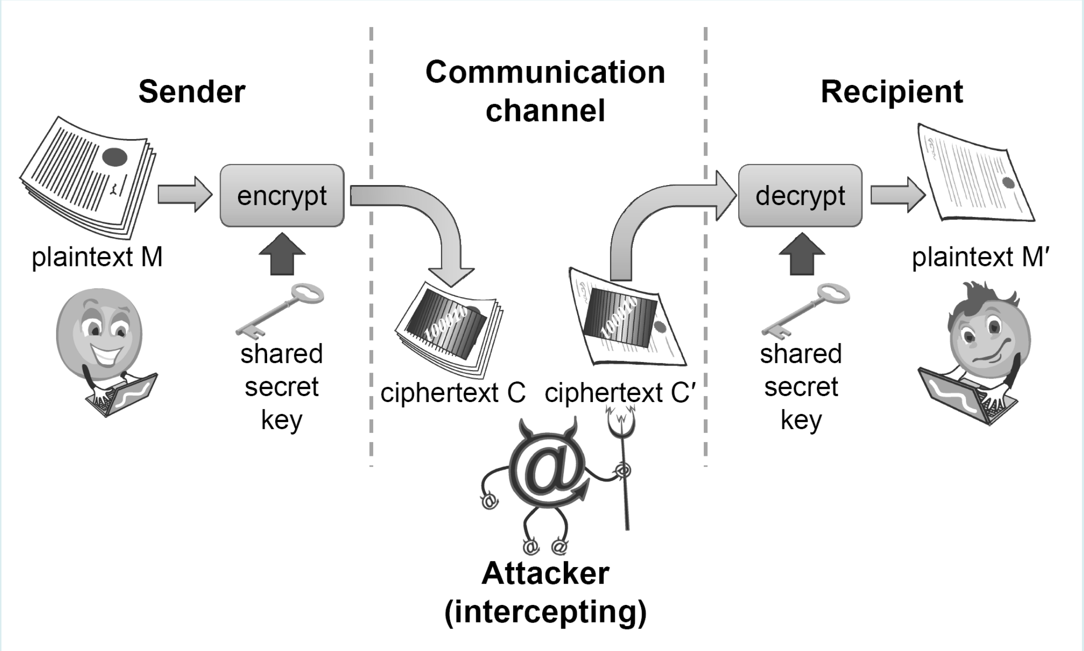
- **Also known as *un-authorised access*.**
- **Difficult to trace as no traces of intrusion might be left.**
- **e.g: illegal eavesdropping or wiretapping or sniffing, illegal copying.**



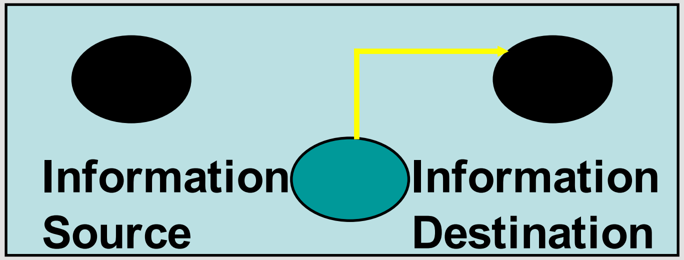
Interception – Attack on Confidentiality

Security Attack : Modification

- Also known as *tampering a resource*.
- Resources can be data, programs, hardware devices, etc.
- Example: man-in-the-middle attack where a network steam is intercepted, modified and retransmitted



Security Attack: Fabrication



Fabrication!
(Attack on Authenticity)

How to identify a fake cheque?

Fabrication

- Also known as ***counterfeiting*** (of objects such as data, programs, devices, etc).
- Allows to by pass the authenticity checks.
- e.g: insertion of spurious messages in a network, adding a record to a file, counterfeit bank notes, fake cheques,…
- ***impersonation/masquerading***
  - to gain access to data, services etc.
  - One entity pretends to be a different entity

Repudiation

- **The denial of a commitment or data receipt**
- **This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.**
- **Tools: digital signatures**

Network Security Attacks

- **classify as passive or active**
- **passive attacks → eavesdropping**
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent
- **active attacks → modify/fake data**
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

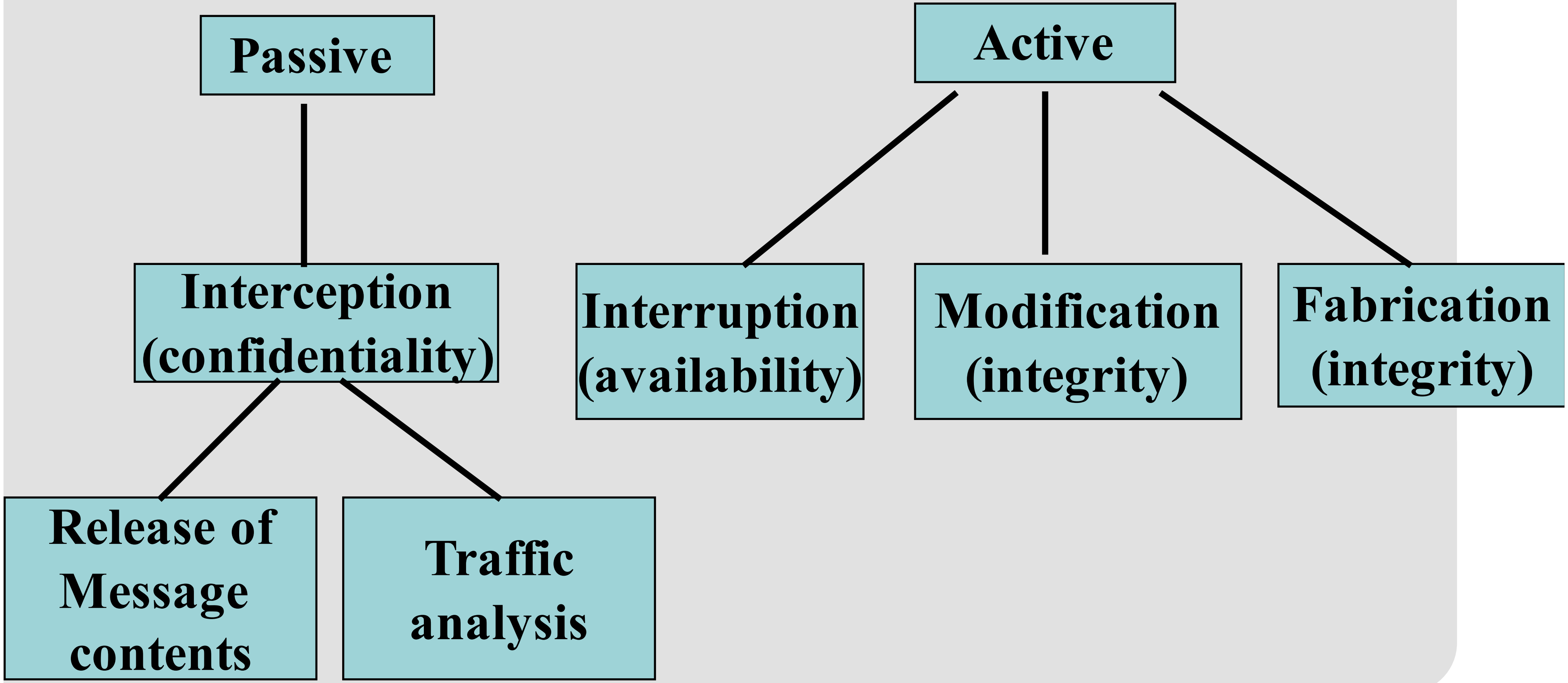
Passive Attacks

- **release of message contents - opponent learns contents of sensitive transmissions**
- **traffic analysis - can occur even when contents of messages are masked, (e.g encryption)**
  - an opponent can still observe the pattern of messages and determine location and identity of communicating hosts, frequency and length of messages being exchanged, and hence guess the nature of communications.
- **The goal is to obtain information to breach confidentiality property.**
  - e.g: getting your pin or password while typing

Active Attacks

- **Active attacks involve modification of data stream or creation of false data:**
- **masquerade - when one entity pretends to be another.**
- **replay - passive capture of data and subsequent retransmission.**
- **modification of messages -- a legitimate message is altered, delayed or reordered.**
- **denial of service prevents or inhibits the normal use or management of communications facilities, or the disruption of an entire network**
- **Violating integrity, availability properties**

Attacks


Passive
Active
Interception (confidentiality)
Interruption (availability)
Modification (integrity)
Fabrication (integrity)
Release of Message contents
Traffic analysis

Managing IT Security in Organisation

- **Identity Management**
  - to authorize user access to system resources.
    - > Access Control, Authentication
- **Vulnerability Management**
  - to help uncover and remedy threats early.
    - > Firewalls
- **Threat Management**
  - to respond to intrusions and attacks on the network.
    - > Intrusion Detections
- **Trust Management**
  - to protect the confidentiality and secure informati

Gate Keeper to verify only authorised users

Preventive measure by identifying and fixing security holes

Minimising the damage due to security breach – post operation

Internal organisation policies and methods

Principles of Security

- **Principle of *easiest penetration***
  - an intruder will use any means of penetration
- **Principles of *timeliness***
  - items only need to be protected until they lose their value
- **Principles of *effectiveness***
  - controls must work, and they should be efficient, easy to use, and appropriate.

Strategic Planning and Risk Management

- **Cost of securing information is expensive.**
- **Cost of not securing information is even more expensive.**
- **How can we plan an IT Security strategy within financial constraints and not posing any inconvenience to users? - Security dilemma**

RISK MANAGEMENT and STRATEGIC PLANNING

Security Functional Requirements

- **technical measures:**
  - access control; identification & authentication; system & communication protection; system & information integrity
- **management controls and procedures**
  - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- **overlapping technical and management:**
  - configuration management; incident response; media protection

X.800 Security Architecture

- **X.800, *Security Architecture for OSI***
- **systematic way of defining requirements for security and characterizing approaches to satisfying them**
- **defines:**
  - security attacks - compromise security
  - security mechanism - act to detect, prevent, recover from attack
  - security service - counter security attacks and enhances the security of the system

Security Services (X.800)

- **Authentication - assurance that communicating entity is the one claimed**
  - – have both peer-entity & data origin authentication
- **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**
- **Availability – resource accessible/usable**

Security Mechanism (X.800)

- **Specific security mechanisms:**
  - encipherment
  - 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
- ***specific security mechanisms* are protocol layer specific, whilst the *pervasive security mechanisms* are not**

Computer Security Strategy

- **specification/policy**
  - what is the security scheme supposed to do?
  - codify in policy and procedures
- **implementation/mechanisms**
  - how does it do it?
  - prevention, detection, response, recovery
- **correctness/assurance**
  - does it really work?
  - assurance, evaluation

Summary

- History of security
- Terminology
- Security concepts
- Security functional requirements
- Security architecture
- Security strategy

Further Reading

- **Chapter 1 of the textbook: *Computer Security: Principles and Practice" by William Stallings & Lawrie Brown,* Prentice Hall, 2015**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor's Manual and other resources made available by the author of the textbook.**