MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

FIT3031: INFORMATION & NETWORK SECURITY

– Lecture 1:
– Introduction to Information and Network Security

Unit Structure: Lecture Topics

- ✓ OSI security architecture
  - **common security standards and protocols for network security applications**
  - **common information risks and requirements**
- operation of private key encryption techniques
- operation of public encryption techniques
- concepts and techniques for digital signatures, authentication and non-repudiation
- security threats of web servers, and their possible countermeasures
- Wireless Security Issues
- security threats of email systems and their possible countermeasures
- IP security
- intrusion detection techniques for security purpose
- risk of malicious software, virus and worm threats, and countermeasures
- firewall deployment and configuration to enhance protection of information assets
- network management protocol for security purpose

LN1: Outline

- **Security Concept**
- **OSI Security Architecture**
  - Security Attacks
  - Security Mechanisms
  - Security Services
- **Methods of Defense**
- **A model for Internetwork Security**
- **Internet standards and RFCs**

Background

- **Traditionally, before the widespread use of computers, security was provided by**
  - physical means – locked filing cabinets
  - administrative mechanisms – rigid hiring process
- **In recent times, especially in global networking environment, the security requirements have changed**
- **Ensuring security is a far more complicated issue today**
- **computer use requires automated tools to protect files and other stored information**
- **use of networks and communications links requires measures to protect data during transmission**

Importance of Security

- **The Australian Institute of Criminology survey in 2016 revealed**
  (http://aic.gov.au/media_library/publications/tandi_pdf/tandi526.pdf)
  - The rapid growth of the internet is transforming how we engage and communicate. It also creates new opportunities for fraud and data theft.
  - In a sample of more than 13 million emails identified as spam, more than 100,000 contained malicious attachments; nearly 1.4 million contained malicious web links that allows cybercriminals to remotely access them.
  - The Australian economy relies on networked computer systems across all business sectors to facilitate service delivery and communication between government, the private sector and the general public
  - About 91,927 small businesses reported a response to security breach in 2013
  - these organizations suffered financial loss
    - $890m
    - loss of productivity, customer confidence
  - number of breaches rising

Importance of Security

- **The US Defense Department revealed that Pentagon recently suffered a massive cyber-attack** (http://www.mobiledia.com/news/98487.html)
  - In March 2011, hackers possibly working for a foreign government broke into a Pentagon contractor's computer system and stole 24,000 files.
- **Pentagon admitted similar attack in June 2007**
- **Massive hacking to Sony PlayStation Network in April, 2011**
- **Massive hacking to Sony Pictures Network in December, 2014**
  - It took forensic analyst few days to understand the complete extent of intrusion
- **There are serious concern about security and privacy of Facebook, Twitter, etc.**
- **Many more examples … (http://www.cnet.com/topics/security/)**

Definitions

- **Computer Security or Information Security**
  - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security**
  - measures to protect data during their transmission
    - > crucial in distributed system, networks and communication facilities
- **Internet Security**
  - measures to protect data during their transmission over a collection of interconnected networks
    - > Internetwork security

Definitions ….

- **Data Security**
- **Cyber Security**
- **No clear boundaries between these forms of security today**
- **For example, a virus introduced physically into a system may spread quickly over the Internet**

Security Focus

- **Consists of measures to deter, prevent, detect, and correct security violations that involve the storage and transmission of information**
- **Few Examples:**
  - **A** transmits a sensitive file to **B** that must be protected from disclosure. **C**, not authorized to read the file, monitors the transmission and captures the file during transmission
  - **D** intercepts a message during transmission, changes the content and transmits to **F** as if it originated from **E**.
  - A message is sent from a customer to a stockbroker with instructions of transactions. Subsequently, the investments lose value and the customer denies sending the message

Levels of Impact

- **can define 3 levels of impact from a security breach**
  - Low
  - Moderate
  - High

OSI Security Architecture

OSI Model			
Layer		Protocol data unit (PDU)	Function[3]
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
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

OSI Security Architecture

- **ITU-T X.800 “Security Architecture for OSI”**
- **defines a systematic way of defining and providing security requirements**
- **provides a useful, if abstract, overview of concepts we will study**
- **A systematic approach is necessary to address the task(s)**
- **OSI security architecture provides a useful framework that defines such a systematic way**
  - To define the security requirements and
  - Adopt approaches to satisfy those requirements

OSI Security Architecture

- **OSI Security Architecture focuses on three aspects of information security :**
  - **security attacks**
  - **security mechanisms**
  - **security services**

Security Attacks

- **Any action that compromises the security of information owned by an organization**
  - **Vulnerability**: a weakness in a computer system that might be exploited to cause loss or harm
  - **Threat**: circumstances that have the potential to cause loss or harm
  - **Control**: a protective measure
- **Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems**
- **often *threat* & *attack* are used to mean the same thing**
- **Have a wide range of attacks**
- **Can focus on generic types of attacks**

Security Attacks - Taxonomy

- **A security attack may attempt to do one or more of the following:**
  - **Interruption:** an attack on availability
  - **Interception:** an attack on confidentiality
  - **Modification:** an attack on integrity
  - **Fabrication:** an attack on authenticity
- **Two types of security attacks:**
  - **Passive** Attacks
  - **Active** Attacks

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 a communication line, disabling a file management system, etc.

Interception

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

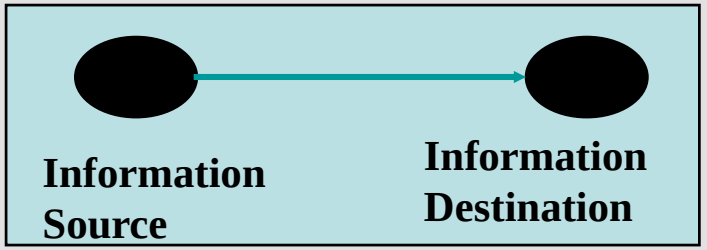
Modification

- **Also known as *tampering a resource*.**
- **Resources can be data, programs, hardware devices, etc.**

Fabrication

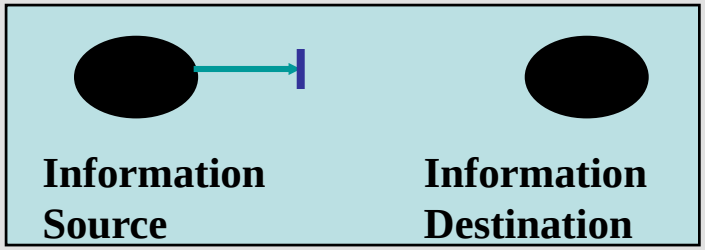
- **Also known as *counterfeiting* (of objects such as data, programs, devices, etc).**
- **Allows to by-pass the authenticity checks.**
- **e.g.: insertion of spurious messages in a network, adding a record to a file, counterfeit bank notes, fake cheques,…**
- ***impersonation/masquerading***
  - to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

Security Attacks - Taxonomy

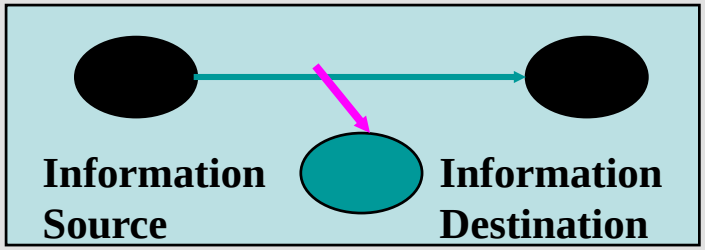


Source and Destination - can be what is supposed to be and what you get

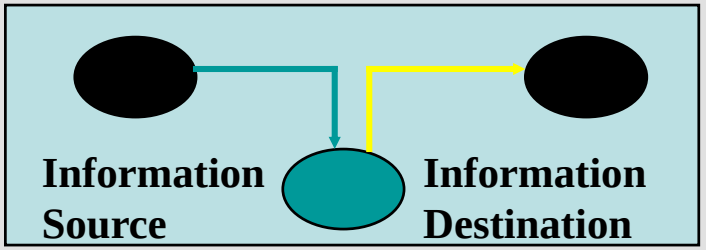
Normal



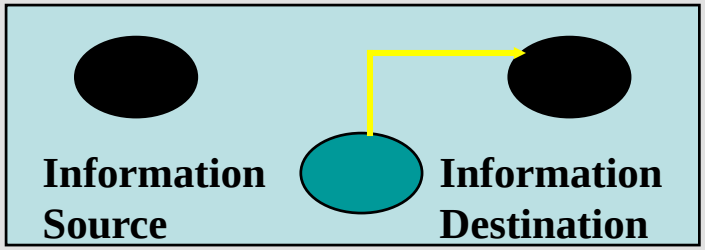
Interruption



Interception



Modification



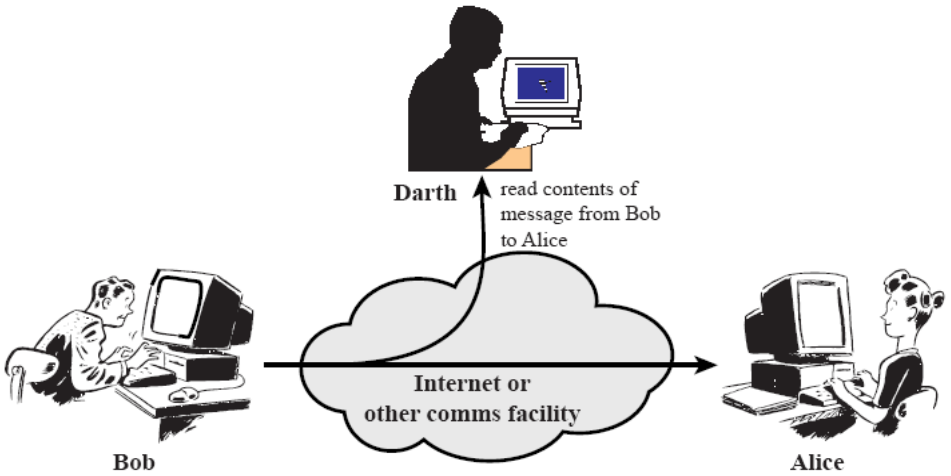
Fabrication

Passive Attacks

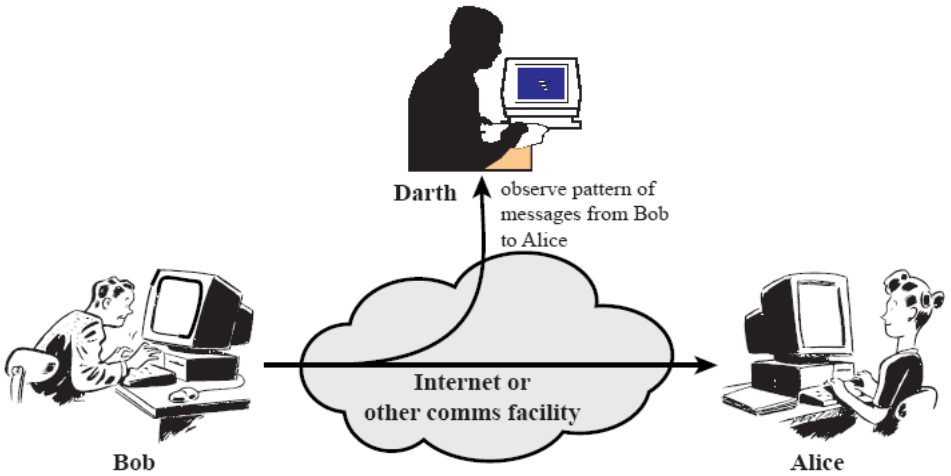
- Nature: **eavesdropping on, or monitoring of, transmission of information between the communicating parties**
- Goal: **to capture information during transmission**

- **Two types of Passive attack:**
  - **Release of message content**
    - capture and read the content
  - **Traffic analysis:**
    - can't read the information, but observe the pattern
    - determine the location and identity of communicating parties
    - observe frequency and length of communication

Passive Attacks…



(a) Release of message contents

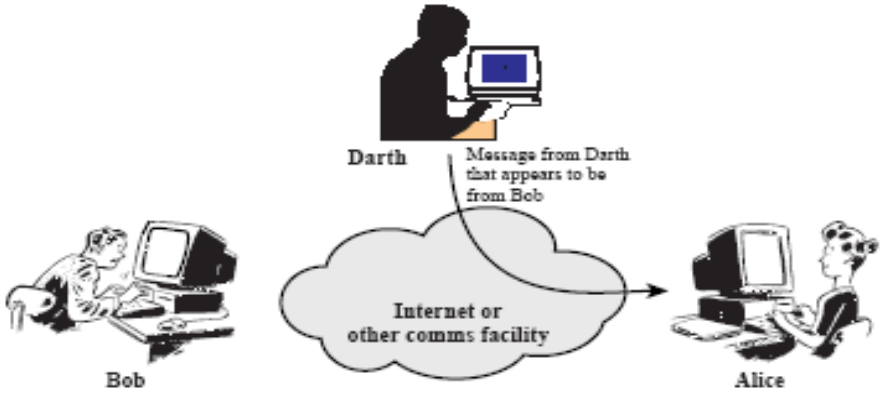


(b) Traffic analysis

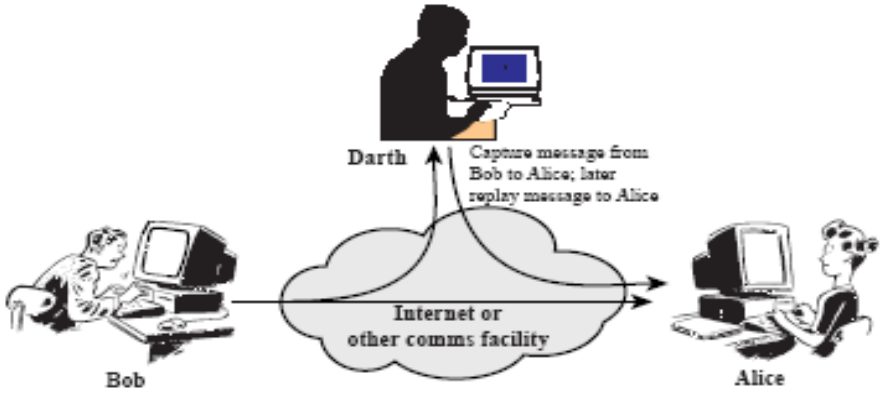
Active Attacks

- **Modifies a data stream or creates a false data streams**
- **Four types of active attacks:**
  - **Masquerade:** one entity pretends to be a different entity
    - > authentication sequences are captured and replayed
    - > an entity can gain extra privileges
  - **Replay:** passive capture of data and subsequent retransmission
  - **Modification of Message:** messages can be altered, delayed or reordered to produce unauthorized effect
  - **Denial of Service:** prevents normal use or management of communication facilities
    - > usually have a specific target
    - > disruption of services of an entire network or suppression of all messages directed to a particular destination

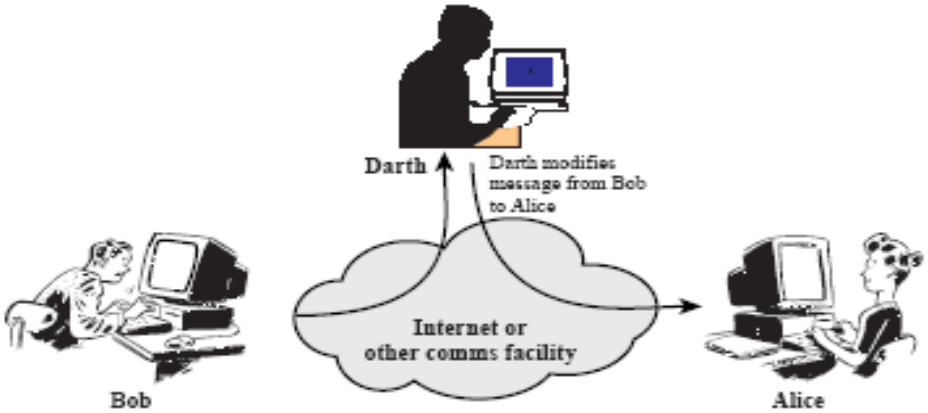
Active Attacks



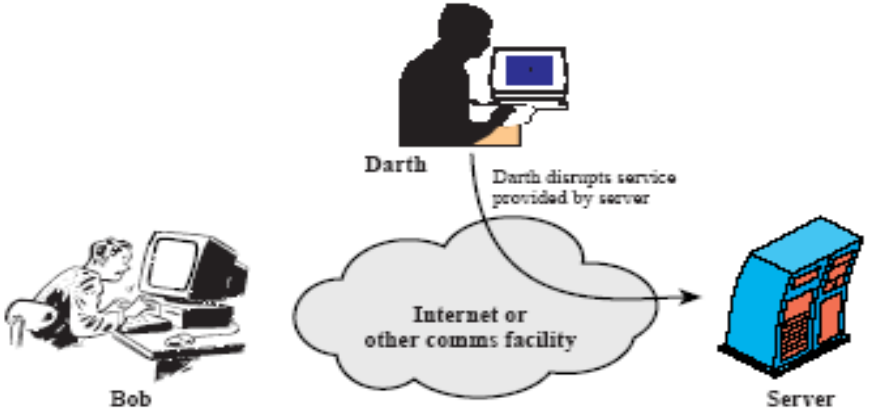
(a) Masquerade



(b) Replay

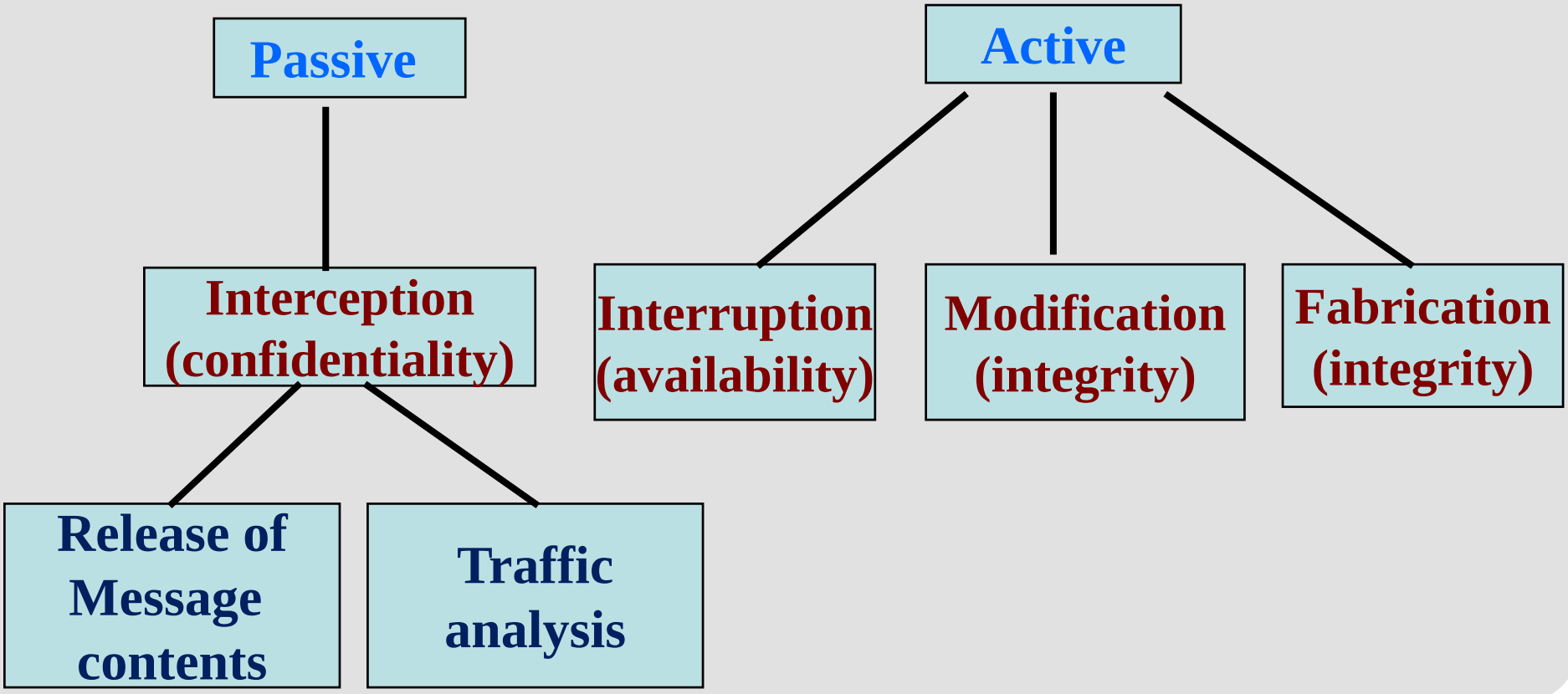


(c) Modification of messages



(d) Denial of service

Attacks


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

Security Services

- **Enhance the security of the data processing systems and the information transfers of an organization**
- **Intended to counter security attacks**
- **Make use of one or more security mechanisms to provide the service**
- **Replicate functions normally associated with physical documents**
  - e.g have signatures, dates;
  - need protection from disclosure, tampering, or destruction;
  - be notarized or witnessed;
  - be recorded or licensed

Security Services (X.800)

- **X.800 (OSI Security Architecture) definition:**
  - *a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers*
  - *Security services are implemented by security mechanism*
- **X.800 defines security services into 6 major categories:**
  - **Confidentiality**
  - **Integrity**
  - **Authentication**
  - Non-repudiation
  - Access control
  - Availability

Security Services (X.800) …

- **Data Confidentiality – protection of data from unauthorized disclosure**
- **Data Integrity - assurance that data received is as sent by an authorized entity**
- **Authentication: assures that the communication is authentic**
  - communicating entities are who they claim to be
  - have both peer-entity & data origin authentication
- **Access Control - prevention of the unauthorized use of a resource**
- **Non-Repudiation - protection against denial by one of the parties in a communication**
  - Receiver can prove that sender has sent the message
  - Sender can proof the receiver has received the message
- **Availability – resource accessible/usable**
  - May be subject to Denial of Service or virus attack

Security Mechanism

- **feature designed to detect, prevent, or recover from a security attack**
- **no single mechanism that will support all services required**
- **however one particular element underlies many of the security mechanisms in use:**
  - cryptographic techniques
- **hence our focus is on this topic**

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**

Security Mechanism (X.800)…

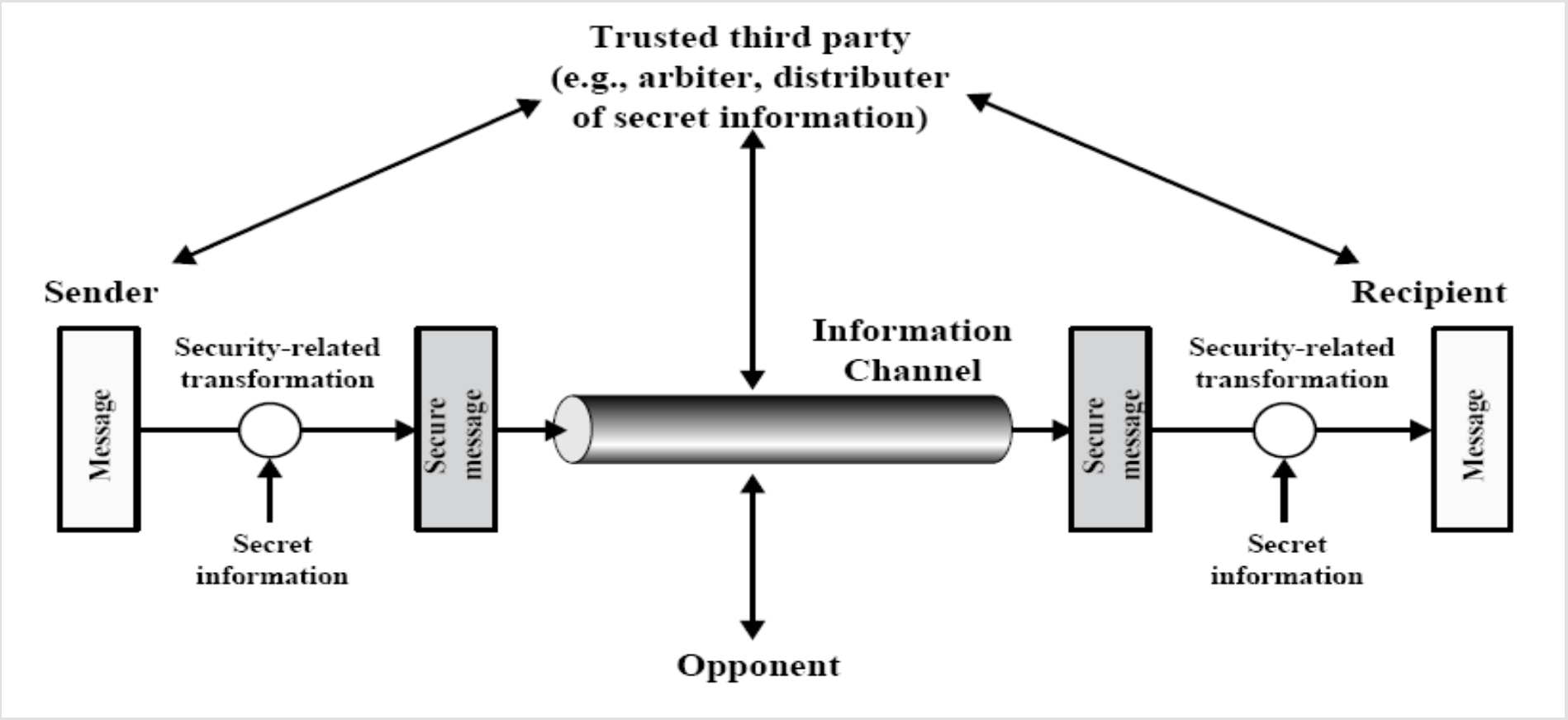
- **Security services are implemented by one or more security mechanism**
- **security mechanisms are invoked at appropriate layers and in appropriate combinations**
- **See the Table 1.4 for relationship between different security service and mechanism**

Relationship between Security Services & Mechanisms

Table 1.4 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

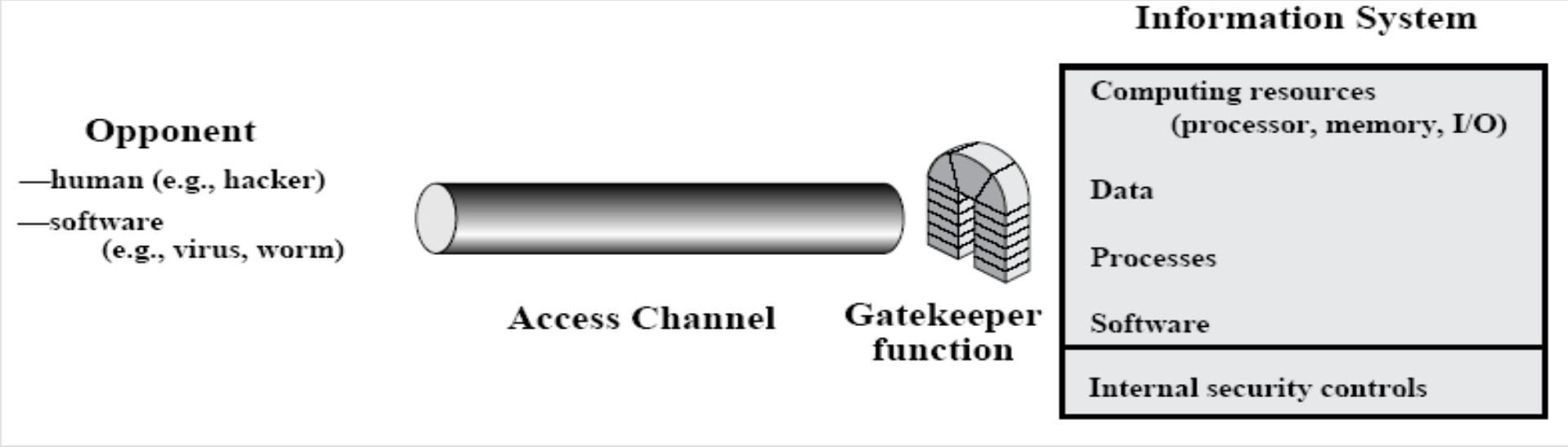
Model for Network Security



Model for Network Security…

- **This model requires us to :**
  - **design** a suitable algorithm for the security-related transformation
  - **generate** the secret information (keys) used by the algorithm
  - **develop** methods to **distribute** and share the secret information
  - specify a **protocol enabling** the principals to use the **transformation** and secret information for a security service

Model for Network **Access** Security



Model for Network **Access** Security…

- **This model requires us to:**
  - select appropriate **gatekeeper** functions to identify users
  - implement security **controls** to ensure only authorised users access designated information or resources
- **Trusted computer systems can be used to implement this model**

Security Management

- **OSI Security Architecture defines three areas of security management**
  - **System security management:** concerned with the management of security aspects of the overall distributed computing environment
  - **Security service management:** concerned with the management of particular security services
  - **Security mechanism management:** concerned with the management of particular security mechanisms

Internet Standards & RFCs

- **The Internet society**
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)
- **Standards development and publications of the internet society is done by these 3 organizations of the internet society.**

Internet RFC Publication Process

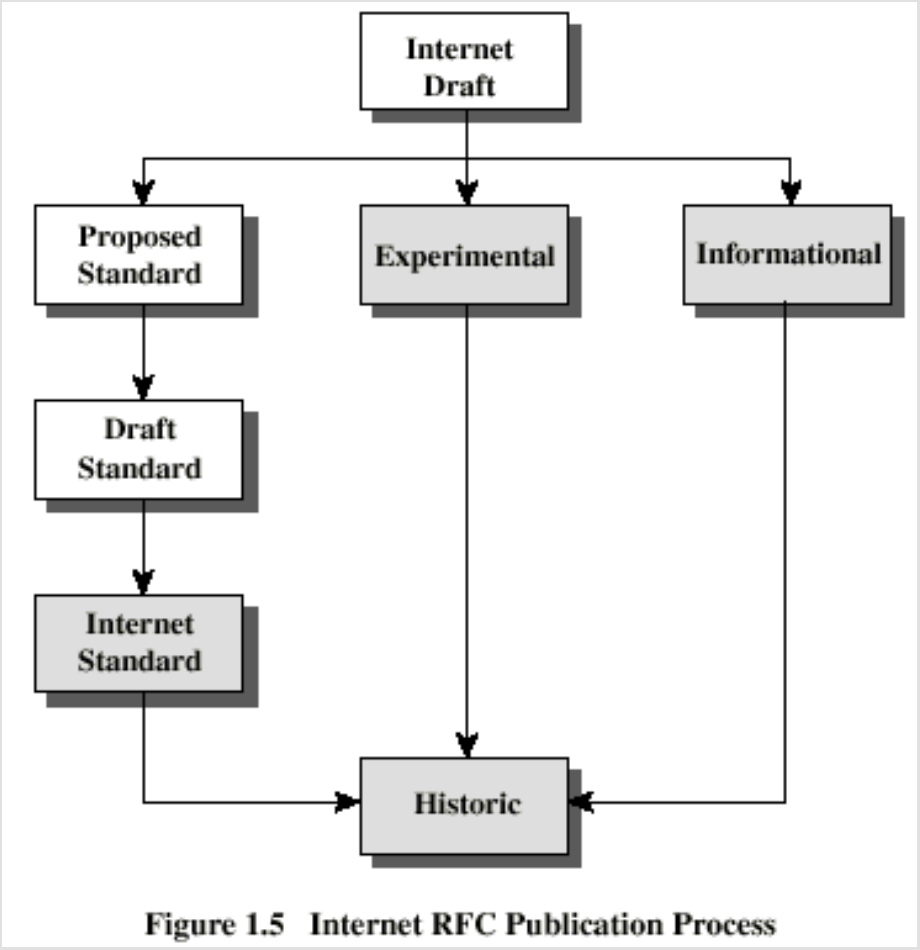


Figure 1.5 Internet RFC Publication Process

- The **Internet Engineering Steering Group** (**IESG**) is a body composed of the **Internet Engineering Task Force (IETF)** chair and area directors.
- The **IESG** is responsible for the technical management of IETF activities and the Internet standards process.

ISO Standard

- **ISO/IEC JTC 1 is a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)**
- **ISO/IEC JTC 1/SC 27 IT Security techniques**

ISO Standard

ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies

Print | Split | Merge

FIT3031_CL_SSB-01_ON-CAMPUS

Download XLSX

Displaying Dates: 1/1/18 to 29/3/19

	Monday	Tuesday	Wednesday	Thursday	Friday
8 AM					
9 AM					
10 AM		FIT3031_CL_SSB-01_ON-CAMPUS/Lecture_1/01 CL_14AII/E7 Lec HT [121] 2/1/18 to 30/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/Lecture_2/01 CL_14AII/E7 Lec HT [121] 3/1/18 to 31/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/Lecture_3/01 CL_14AII/E7 Lec HT [121] 4/1/18 to 1/2/18	
11 AM					
12 PM					
1 PM		FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/01-P1 CL_14Rnf/G11A Digital Lab [24] 9/1/18 to 30/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/02-P1 CL_14Rnf/143 Digital Lab [20] 9/1/18 to 30/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/05-P1 CL_14Rnf/G12B Digital Lab [16] 9/1/18 to 30/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/01-P2 CL_14Rnf/G11A Digital Lab [24] 3/1/18 to 31/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/02-P2 CL_14Rnf/143 Digital Lab [20] 3/1/18 to 31/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/05-P2 CL_14Rnf/G12B Digital Lab [16] 3/1/18 to 31/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/01-P3 CL_14Rnf/G11A Digital Lab [24] 4/1/18 to 1/2/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/02-P3 CL_14Rnf/143 Digital Lab [20] 4/1/18 to 1/2/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/05-P3 CL_14Rnf/G12B Digital Lab [16] 4/1/18 to 1/2/18	
2 PM					
3 PM		FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/06-P1 CL_14Rnf/143 Digital Lab [20] 9/1/18 to 30/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/03-P1 CL_14Rnf/G11A Digital Lab [24] 9/1/18 to 30/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/04-P1 CL_14Rnf/G12B Digital Lab [16] 9/1/18 to 30/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/06-P2 CL_14Rnf/143 Digital Lab [20] 3/1/18 to 31/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/03-P2 CL_14Rnf/G11A Digital Lab [24] 3/1/18 to 31/1/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/04-P2 CL_14Rnf/G12B Digital Lab [16] 3/1/18 to 31/1/18	FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/06-P3 CL_14Rnf/143 Digital Lab [20] 4/1/18 to 1/2/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/03-P3 CL_14Rnf/G11A Digital Lab [24] 4/1/18 to 1/2/18 FIT3031_CL_SSB-01_ON-CAMPUS/L-aboratory/04-P3 CL_14Rnf/G12B Digital Lab [16] 4/1/18 to 1/2/18	
4 PM					
5 PM					

Further Reading

- **Study Guide 1**
- **Chapter 1 of the textbook: *Network Security Essentials-Application & Standards" by William Stallings* 5th Edition, Prentice Hall, 2013**

- **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.**