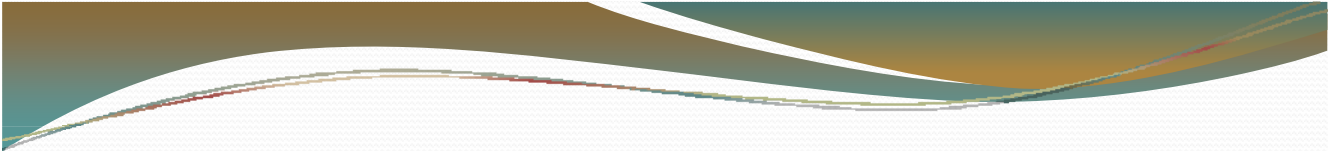


Network Security Essentials Chapter 1

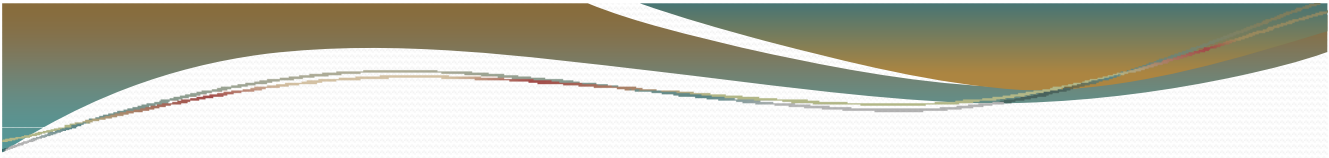
Fourth Edition
by William Stallings

Lecture slides by Lawrie Brown



The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

- 
- *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure..*

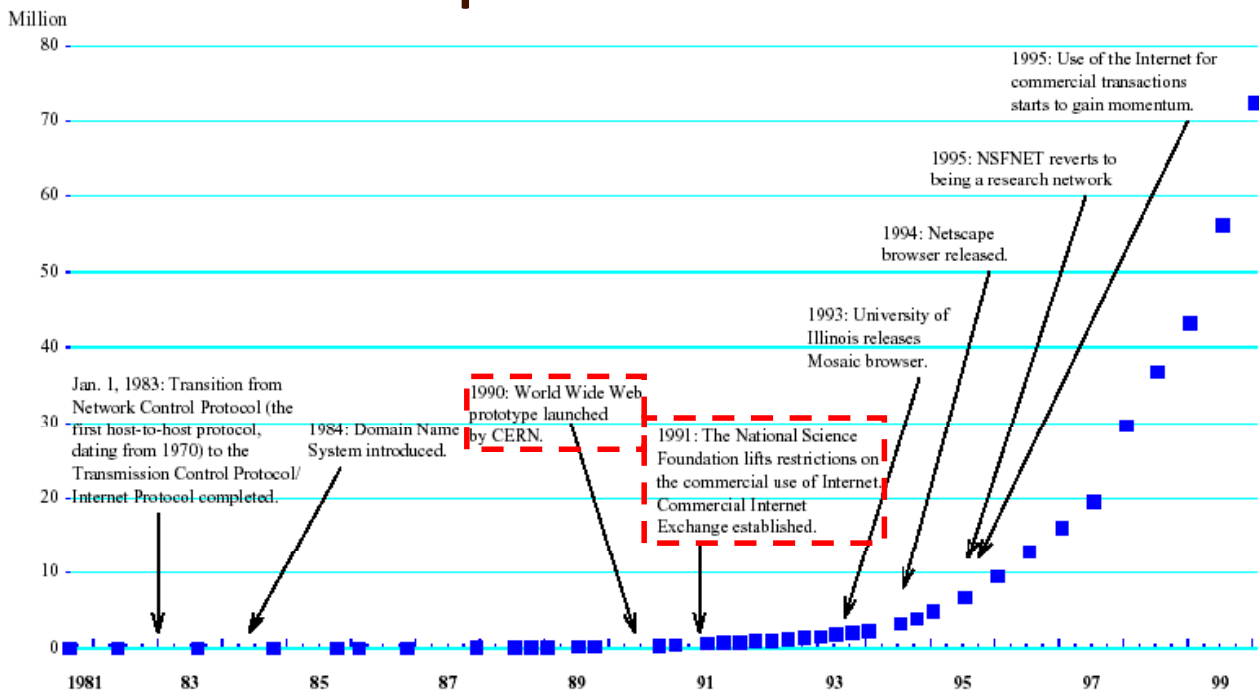
— On War, Carl Von Clausewitz



Introduction

- Notion of Security
 - Information security
 - The introduction of the computer
 - Computer security
 - The introduction of distributed systems and the use of networks and communication facilities
 - Network security / internet security

The Development of Internet

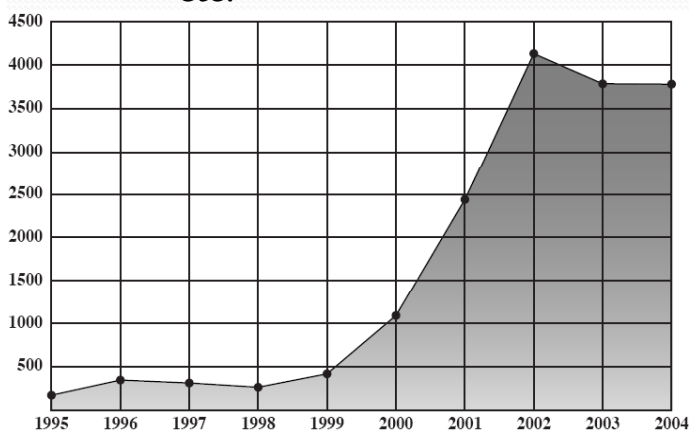


Source: OECD (www.oecd.org/dsti/sti/it/index.htm); Internet Software Consortium (www.isc.org); CERN (public.web.cern.ch/public/); NSF (www.nsf.gov); Hobbes' Internet TimeLine v.5.0 (www.isoc.org/zakon/internet/history/hit.html).

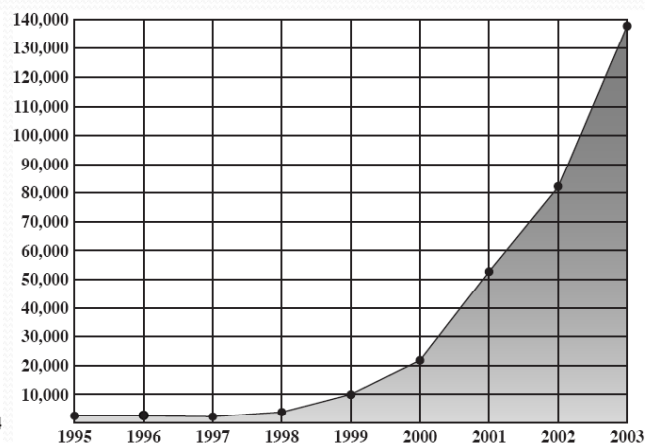
Security trends

• CERT Statistics

- Vulnerabilities: Operating systems, Internet routers and network devices.
- Incidents: DOS, IP spoofing, eavesdropping, packet sniffing, etc.



(a) Vulnerabilities reported



(b) Incidents reported

網路監視器 - [擷取: 2 (Summary)]

檔案(F) 編輯(E) 顯示(D) 工具(T) 選項(O) 視窗(W) 說明(H)

Internet Domain Name System Packet F#: 1/28 關閉: 42 (x2A) L: 38 (x26)

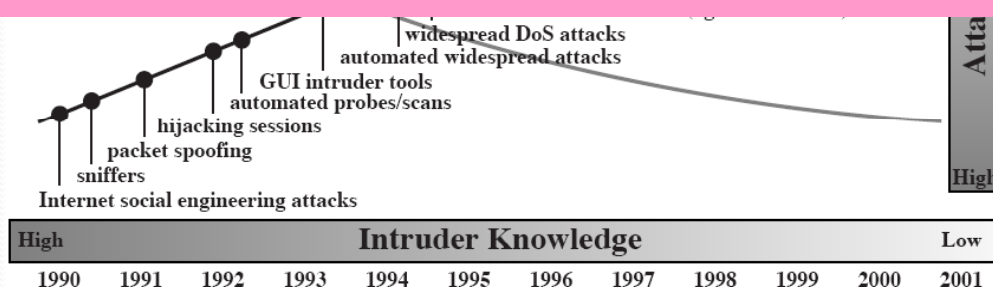
框架	時間	來源 MAC 位址	目的 MAC 位址	通訊協定	說明
1	1.393	0080C85235FF	KIKUKO	DNS	Ox1:Std Qry for kikuko.eagles.net.tw.
2	1.426	KIKUKO	0080C85235FF	DNS	Ox1:Std Qry Resp. for kikuko.eagles.net.tw.
3	4.461	0080C85235FF	KIKUKO	DNS	Ox1:Std Qry for kikuko.eagles.net.tw.
4	4.478	KIKUKO	0080C85235FF	DNS	Ox1:Std Qry Resp. for kikuko.eagles.net.tw.
5	4.481	0080C85235FF	KIKUKO	TCPS., len: 4, seq: 12030348-1203
6	4.482	KIKUKO	0080C85235FF	TCP	.A...S, len: 4, seq: 17023648-1702
7	4.482	0080C85235FF	KIKUKO	TCP	.A...S, len: 4, seq: 12030349-1203
8	4.531	KIKUKO	0080C85235FF	FTP	Resp. to Port 1060, '220 kikuko Micros
9	4.645	0080C85235FF	KIKUKO	TCP	.A...., len: 0, seq: 12030349-1203
10	5.995	0080C85235FF	KIKUKO	FTP	Req. from Port 1060, 'USER wjsheen'
11	5.998	KIKUKO	0080C85235FF	FTP	Resp. to Port 1060, '331 Password requ
12	6.147	0080C85235FF	KIKUKO	TCP	.A...., len: 0, seq: 12030363-1203
13	8.429	KIKUKO	0080C85235FF	SMB	C ech
14	8.430	0080C85235FF	KIKUKO	SMB	R echo, len: 1
15	8.723	KIKUKO	0080C85235FF	NBIPX	Session Data, Ack, Recv Seq Ox2D1, Ox2
16	9.480	0080C85235FF	KIKUKO	FTP	Req. from Port 1060, 'PASS wjshpwd'
17	9.482	KIKUKO	0080C85235FF	FTP	Resp. to Port 1060, '530 User wjsheen
18	9.651	0080C85235FF	KIKUKO	TCP	.A...., len: 0, seq: 12030377-1203
19	10.652	0080C85235FF	KIKUKO	FTP	Req. from Port 1060, 'QUIT'
20	10.664	KIKUKO	0080C85235FF	FTP	Resp. to Port 1060, '221 '
21	10.666	KIKUKO	0080C85235FF	TCP	.A...F, len: 0, seq: 17023773-1702
22	10.666	0080C85235FF	KIKUKO	TCP	.A...., len: 0, seq: 12030383-1203
23	10.666	0080C85235FF	KIKUKO	TCP	.A...F, len: 0, seq: 12030383-1203
24	10.667	KIKUKO	0080C85235FF	TCP	.A...., len: 0, seq: 17023774-1702

Trends in Attack Sophistication and Intruder Knowledge

sophisticated command and control
increase in worms
anti-forensic techniques
home users targeted
DDoS attacks
distributed attack tools

Intruder Knowledge

Cryptography algorithms for confidentiality and authentication assume greater importance.

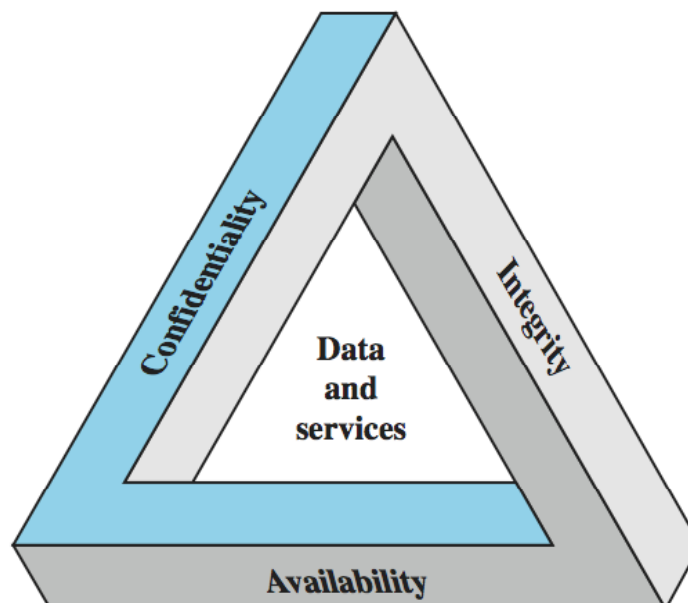


Source: CERT

Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts





Levels of Impact

- Define 3 levels of impact from a security breach
 - Low
 - Moderate
 - High



Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service



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
- for us it provides a useful, if abstract, overview of concepts we will study

Aspects of Security

- consider 3 aspects of information security:
 - **security attack**
 - **security mechanism**
 - **security service**
- note terms
 - *threat* – a potential for violation of security
 - *attack* – an assault on system security, a deliberate attempt to evade security services

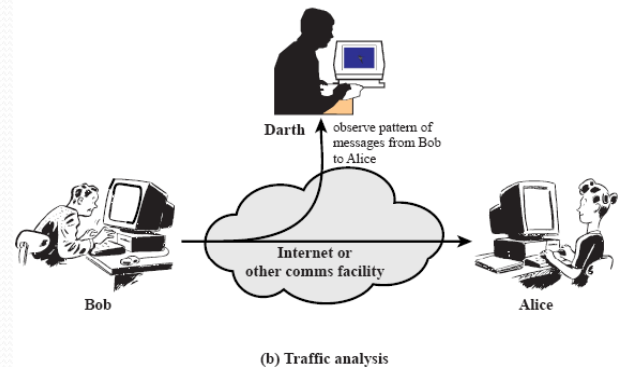
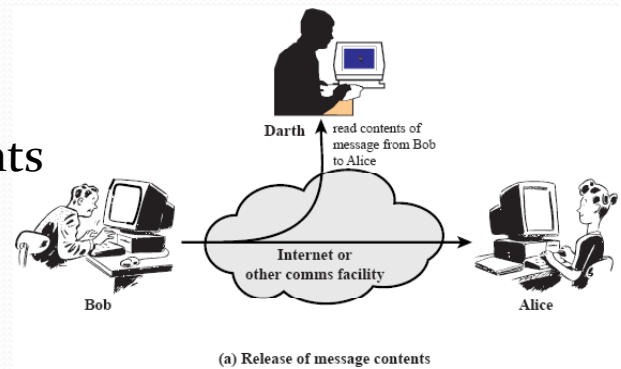
Security Attacks

- Security attacks
 - Passive attacks · Active attacks
- **Passive attacks**
 - They attempt to learn or make use of information from the system but does not affect system resources.
 - The nature of eavesdropping on, or monitoring of, transmissions.

Security Attacks

Passive Attacks

- Two types of passive attacks:
 - Release of message contents
 - Traffic analysis



Security Attacks

Passive Attacks

- The example of the MIME Internet e-mail format.

```
邮件原始稿
From: "Vanessa Shaw" <vanessa@iim.nctu.edu.tw>
To: "M.H.Shaw" <n8734805@cc.nctu.edu.tw>
Subject: Test Secure E-Mail
Date: Wed, 10 May 2000 13:21:42 +0800
Content-Type: multipart/alternative;
  boundary="-----_NextPart_000_0022_01BFBA82.AE5516B0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2014.211

This is a multi-part message in MIME format.

-----_NextPart_000_0022_01BFBA82.AE5516B0
Content-Type: text/plain;
  charset="big5"
Content-Transfer-Encoding: quoted-printable

Please verify vanessa's digital signature,
and then decrypt the mail using M.H.Shaw's private key.
sincerely yours, vanessa shao.

-----_NextPart_000_0022_01BFBA82.AE5516B0
Content-Type: text/html;
  charset="big5"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content=3D"text/html; charset=3Dbig5" http-equiv=3DContent-Type>
<META content=3D"MSHTML 5.00.2014.210" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgcolor=3D#ffffff>
<DIV>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</DIV>
<DIV><FONT size=3D2>Please verify vanessa's digital =
signature.</FONT></DIV>
<DIV><FONT size=3D2>and then decrypt the mail using M.H.Shaw's private=20
key.</FONT></DIV>
<DIV>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</DIV>
<DIV><FONT size=3D2>sincerely yours, vanessa =
shao.</FONT></DIV></BODY></HTML>

-----_NextPart_000_0022_01BFBA82.AE5516B0--
```

Passive Attacks

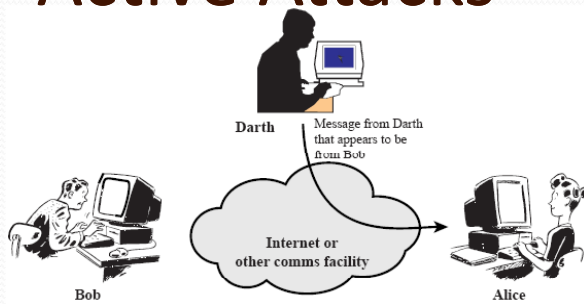
- It's feasible to prevent the success of these attacks, usually by means of **encryption**.
 - **Attention:** page 25(2)
- Prevention rather than detection

Active Attacks

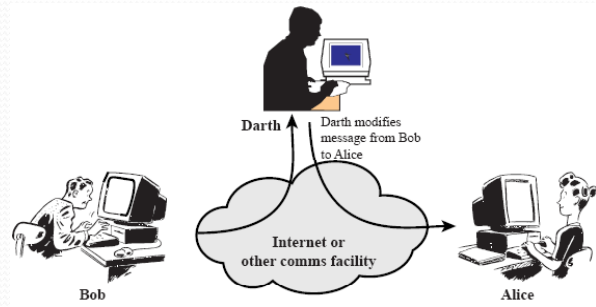
- **Active attacks**
 - They attempt to alter system resources or affect their operation.
 - They modification of data stream to:
 - **masquerade** of one entity as some other
 - **replay** previous messages
 - **modification** of messages
 - **denial of service**
 - **Attention:** page 25(L1)~26(1)

Security Attacks

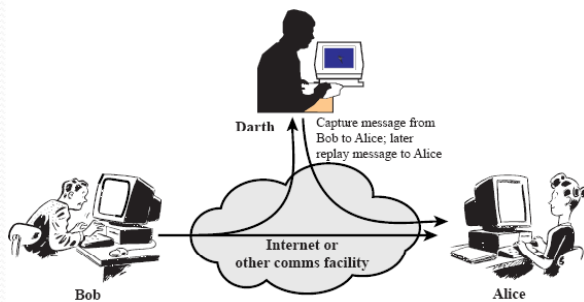
Active Attacks



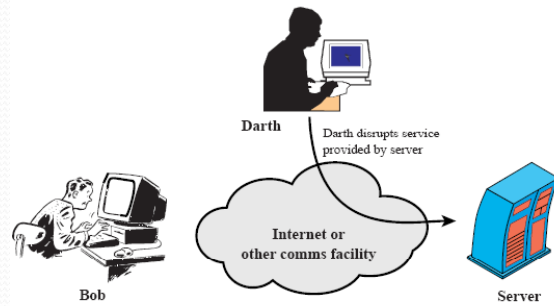
(a) Masquerade



(c) Modification of messages



(b) Replay



(d) Denial of service

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- **using one or more security mechanisms**
- often replicates functions normally associated with physical documents
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:
“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
- RFC 2828:
“a processing or communication service provided by a system to give a specific kind of protection to system resources”

Security Services (X.800) *Table 1.2*

- **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 Services (X.800) *Table1.2*

- **Authentication** (who created or sent the data)
 - Peer entity authentication
 - Corroboration of the identity of a peer entity connected.
 - Data origin authentication
 - Corroboration of the source of a data unit.
- **Access control** (prevent misuse of resources)
- **Data Confidentiality** (privacy)
 - Connection confidentiality
 - Connectionless confidentiality
 - Selective-field confidentiality
 - Traffic-flow confidentiality

25

Security Services (X.800) *Table1.2*

- **Data Integrity** (has not been altered)
 - Connection-oriented integrity service
 - Connectionless integrity service
- **Nonrepudiation** (the order is final)
 - Nonrepudiation, Origin
 - Nonrepudiation, Destination
- **Availability** (permanence, non-erasure)
 - Denial of Service Attacks
 - Virus that deletes files

26



Security Mechanism

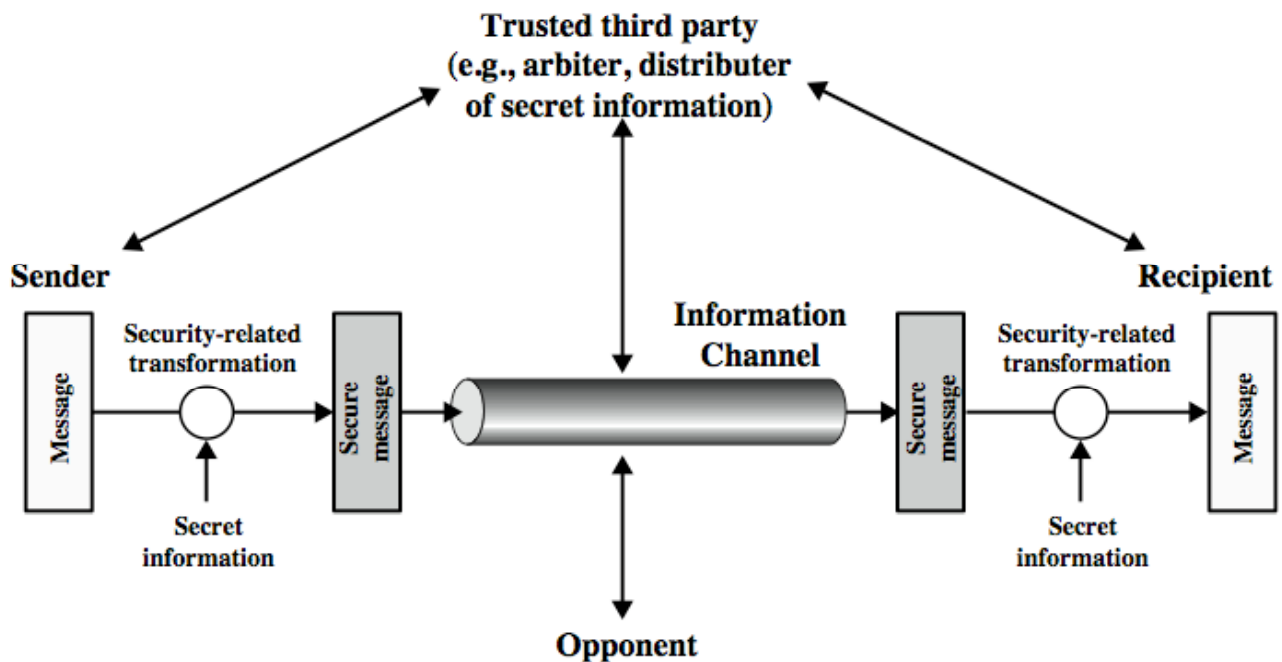
- feature designed to detect, prevent, or recover from a security attack
- **no single mechanism that will support all services required**
- however one particular element underlies many of the security mechanisms in use:
 - **cryptographic techniques**
- hence our focus on this topic



Security Mechanisms (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

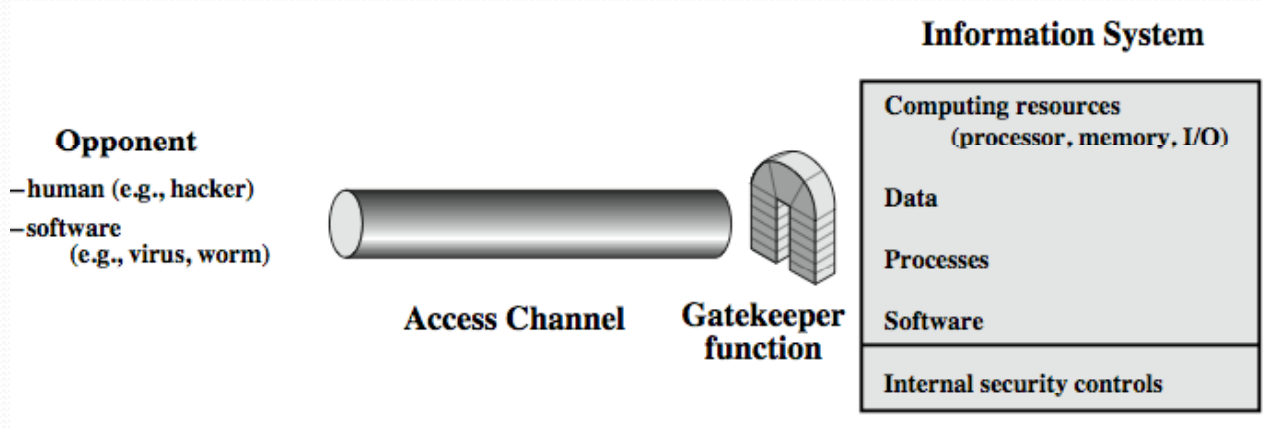
Model for Network Security



Model for Network Security

- using this model requires us to:
 1. design a suitable algorithm for the security transformation
 2. generate the secret information (keys) used by the algorithm
 3. develop methods to distribute and share the secret information
 4. 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

- using this model requires us to:
 1. select appropriate gatekeeper functions to identify users
 2. implement security controls to ensure only authorised users access designated information or resources



Summary

- topic roadmap & standards organizations
- security concepts:
 - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security