Introduction: Network Security

Book: William Stallings, Network Security Essentials:
Applications and Standards, 3rd.
Slides reference: Henric Johnson
Blekinge Institute of Technology, Sweden

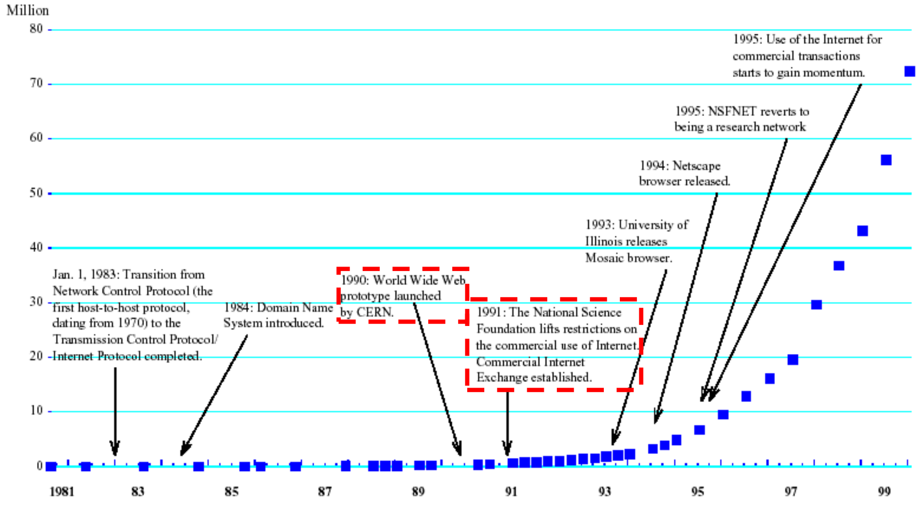
Outline

- Introduction
- Security trends
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security
- Internet standards and RFCs

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



Jan. 1, 1983: Transition from Network Control Protocol (the first host-to-host protocol, dating from 1970) to the Transmission Control Protocol/ Internet Protocol completed.

1984: Domain Name System introduced.

1990: World Wide Web prototype launched by CERN.

1991: The National Science Foundation lifts restrictions on the commercial use of Internet. Commercial Internet Exchange established.

1993: University of Illinois releases Mosaic browser.

1994: Netscape browser released.

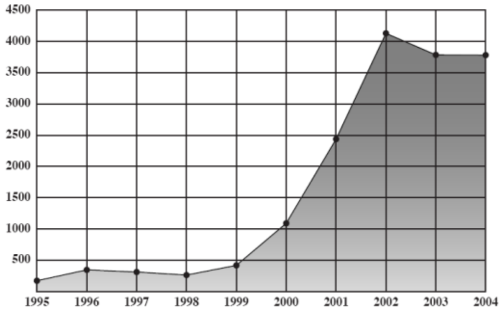
1995: NSFNET reverts to being a research network

1995: Use of the Internet for commercial transactions starts to gain momentum.

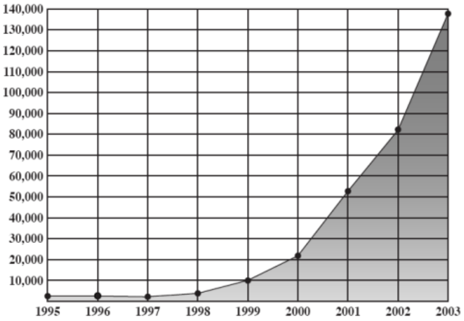
Source: OECD (www.oecd.org/dsti/sti/it/index.htm); Intenet Software Consortium (www.isc.org); CERN (public.web.cern.ch/public/); NSF (www.nsf.gov); Hobbes' Internet TimeLine v.5.0 (www.isoc.org/zakon/internet/history/hit.html).

Security trends

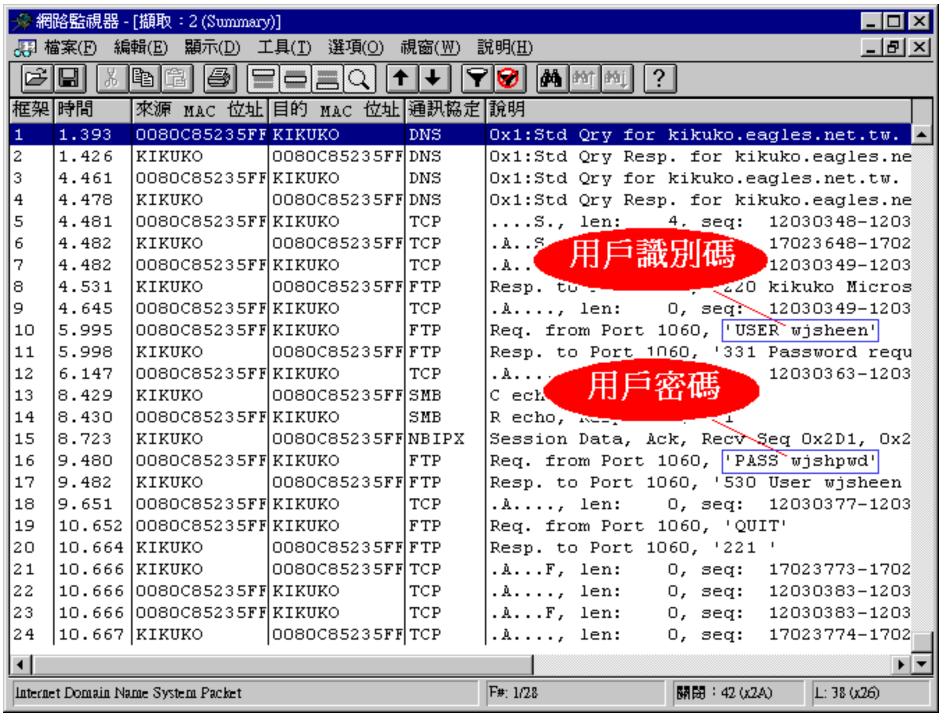
- CERT Statistics
  - Vulnerabilities: Operating systems, Internet routers and network devices.
  - Incidents: DOS, IP spoofing, eavesdropping, packet sniffing, etc.



(a) Vulnerabilities reported



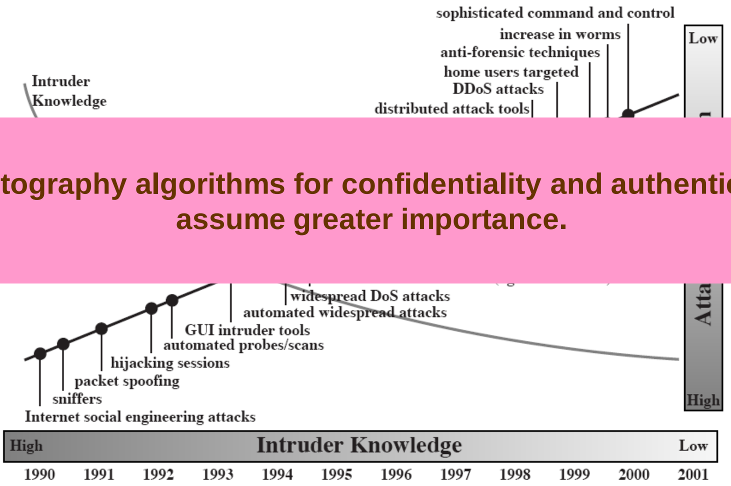
(b) Incidents reported



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	0x1:Std Qry for kikuko.eagles.net.tw.
2	1.426	KIKUKO	0080C85235FF	DNS	0x1:Std Qry Resp. for kikuko.eagles.ne
3	4.461	0080C85235FF	KIKUKO	DNS	0x1:Std Qry for kikuko.eagles.net.tw.
4	4.478	KIKUKO	0080C85235FF	DNS	0x1:Std Qry Resp. for kikuko.eagles.ne
5	4.481	0080C85235FF	KIKUKO	TCP	....S., len: 4, seq: 12030348-1203
6	4.482	KIKUKO	0080C85235FF	TCP	.A..S 17023648-1702
7	4.482	0080C85235FF	KIKUKO	TCP	.A.. 12030349-1203
8	4.531	KIKUKO	0080C85235FF	FTP	Resp. to 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.... 12030363-1203
13	8.429	KIKUKO	0080C85235FF	SMB	C ech
14	8.430	0080C85235FF	KIKUKO	SMB	R echo,
15	8.723	KIKUKO	0080C85235FF	NBIPX	Session Data, Ack, Recv Seq 0x2D1, 0x2
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

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

Trends in Attack Sophistication and Intruder Knowledge



Cryptography algorithms for confidentiality and authentication assume greater importance.

Source: CERT

Security Architecture for OSI (X.800)

- Security Attack
  - Any action that compromises the security of information.
- Security Mechanism
  - A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security Service
  - A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

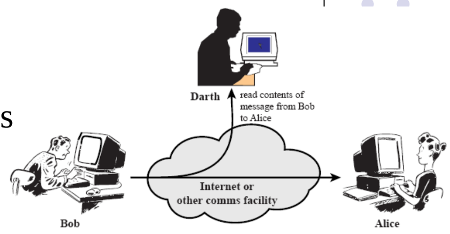
Security Attacks

- Security attacks
  - Passive attacks、Active attacks

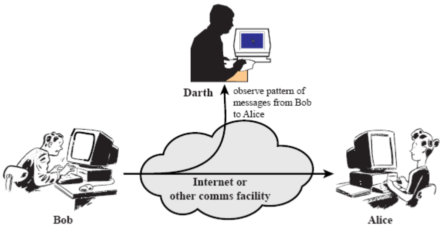
- **Passive attacks**
  - They attempt to learn or make use of information from the system but does not affect system resources.
  - The nature of eavesdropping on, or monitoring of, transmissions.

Security Attacks
Passive Attacks

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


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

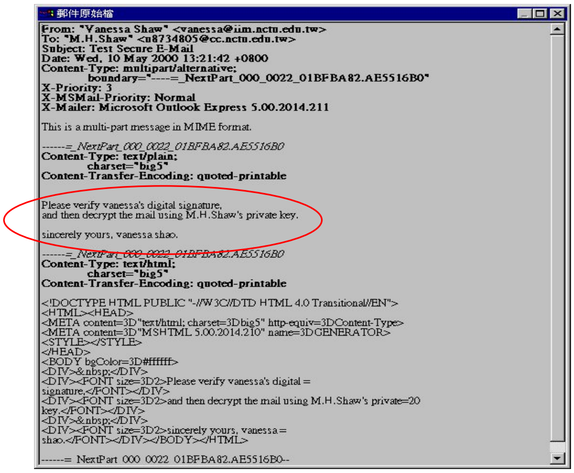

Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

Security Attacks

Passive Attacks

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



```
From: "Vanessa Shaw" <vanessa@iim.nctu.edu.tw>
To: "M.H.Shaw" <u8734805@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;</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;</DIV>
<DIV><FONT size=3D2>sincerely yours, vanessa =
shao.</FONT></DIV></BODY></HTML>

------= NextPart 000 0022 01BFBA82.AE5516B0--
```

Security Attacks

Passive Attacks

- It’s feasible to prevent the success of these attacks, usually by means of **encryption**.
  - Attention: page 8

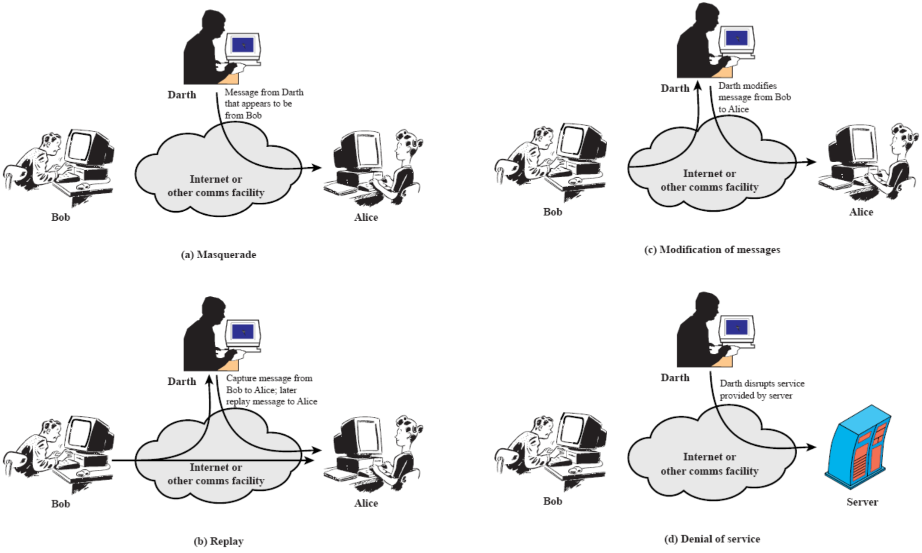
- Prevention rather than detection

Security Attacks
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 11

13

Security Attacks
Active Attacks


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice
Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice
Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(a) Masquerade

(c) Modification of messages

(b) Replay

(d) Denial of service

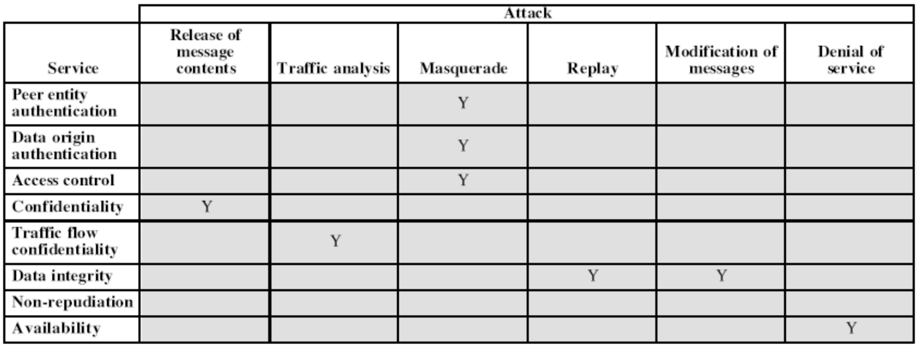
Security Services

- **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

Security Services

- **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

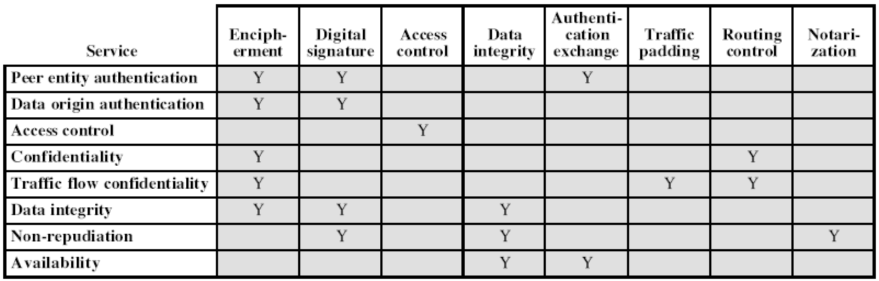
Relationship between Security Services and Attacks



	Attack					
Service	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation						
Availability						Y

Security Mechanisms

- Relationship between security services and mechanisms (See Table 1.4)



Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
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			

- Encipherment
  - Reversible encipherment mechanisms
  - Irreversible encipherment mechanisms

Model for Network Security

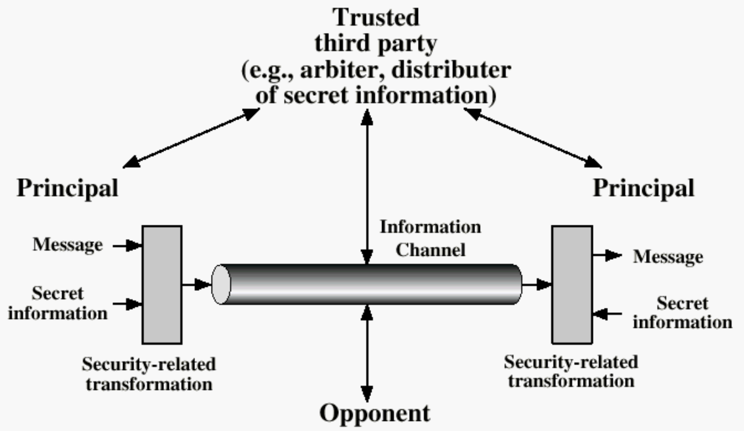


Figure 1.3 Model for Network Security

Model for Network Security

- Using this model requires us to:
  - design a suitable algorithm for the security 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

Network Access Security Model

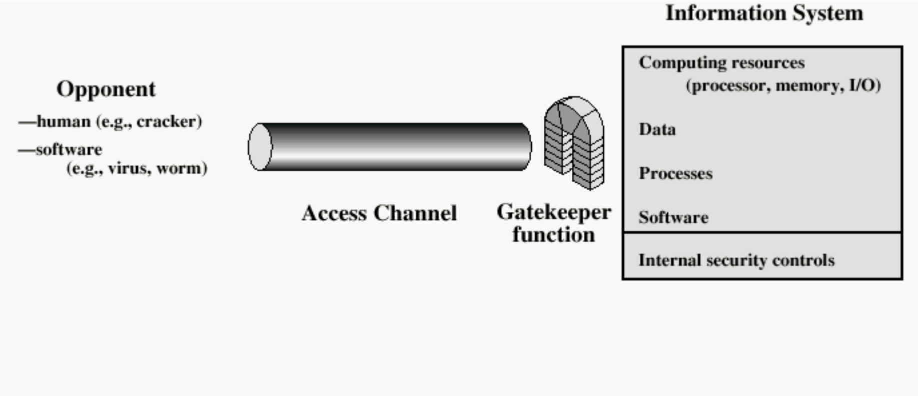


Figure 1.4 Network Access Security Model

Network Access Security Model

- Using 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

Internet standards and RFCs

- The Internet society
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)

Internet RFC Publication Process

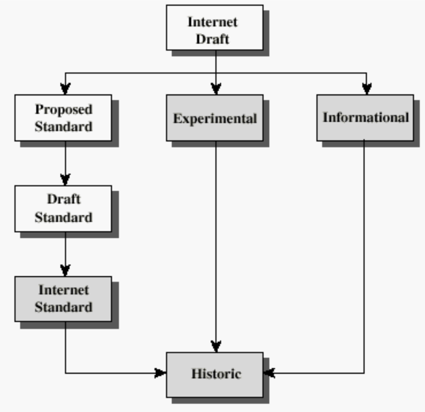
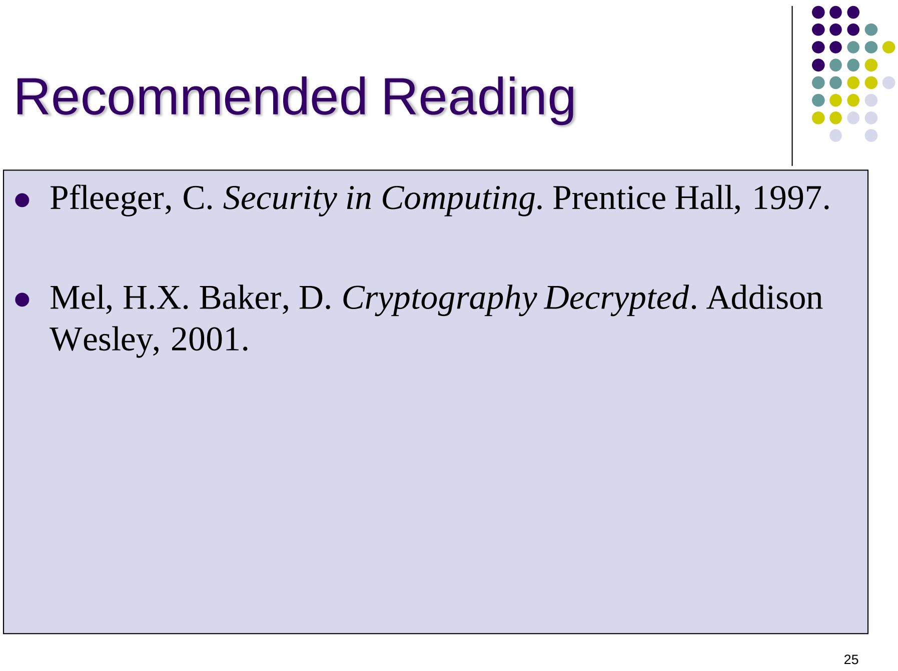


Figure 1.5 Internet RFC Publication Process



Recommended Reading

- Pfleeger, C. *Security in Computing*. Prentice Hall, 1997.
- Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001.