CSC290A – Network Security

FAQs

- ***How Do Corporations Prevent Intrusions Into There Networks?***
- ***What Does SHA1 And MD5 Mean When You Download?***
- ***What Is A Certificate And How Does It Secure Your Internet Transaction?***
- ***Do You Really Have Privacy On The Internet?***

These are just a few of the many questions related to **Network Security**, one of the most active and rewarding areas in Information Technology. These and many other questions will be examined in this topical graduate seminar. This class uses slides, the Web, and hands-on demonstrations to explore a range of topics from the foundations of cryptography to the latest research concerning security on the Internet, while maintaining a healthy balance between theory and practice.

Course Description

- Survey of current issues, techniques, software, hardware and architectures related to network security. Examination of the protocols used for Internet services, their vulnerabilities and how they can be secured. Analysis of firewall design, cryptographic techniques, intrusion detection, port scanning, viruses, trojan horses and denial of services attacks. Basic principles of secure networking and application design will be studied and discussed.

- *Prerequisites:* None

Text

- **Required Text**
  William Stallings, *Network Security Essentials: Applications and Standards – 2/e*, Prentice-Hall, 2003, 432 pp., ISBN 0-13-035128-8

- **Reference**
  William Stallings, *Business Data Communications, 5*/e, Prentice-Hall, 2005, 608 pp., ISBN 0-13-144257-0

  Cheswick, W. and Bellovin, S., *Firewalls and Network Security: Repelling the Wiley Hacker*, Addison Wesley, 2003, 464 pp., ISBN 0-201-63466-X

  William Stallings, *Cryptography and Network Security: Principles and Practice*, 4/e, Prentice Hall, 2006, 569 pp., ISBN 0-13-187316-4

  Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2/e, Wiley, 1996, 784 pp., ISBN 047-111709-9

Grading

- Several **assignments**, three count
- **mid-term** and **end-term**
- Class **participation**
- Final **project** or **paper**
- **No make-up** test or **extended deadlines**

Point Allocation

Assignments 1-3:	5% each
Final Project:	30%
Mid-Term:	25%
End-Term:	25%
Participation:	5%

Attendance

- **Not Mandatory**, but…
- …you’ll probably **fail!**
- **Participation** is very important
- **Let me know** if you can’t make it

Course Schedule

1	1/30	Introduction
2	2/06	Cryptography
3	2/13	Cryptography
4	2/27	Authentication Applications
5	3/6	E-Mail Security
6	3/13	IP Security, Networking, Tools
7	3/20	IP Security, Networking, Tools - **Mid-Term Exam Due**
8	3/27	Firewalls
9	4/3	Web Security
10	4/19	Electronic Commerce
11	4/24	Intruder, Viruses and Denial of Service
12	5/1	Network Management Security - **Final Project/Paper Due**
13	5/8	Intrusion Detection / Special Topics/Review
14	5/15	**End-Term Exam Due**

Slides, Links & News

- www.cs.hofstra.edu/~cscvjc/Spring06

Class Rules

- Assignments are to be completed individually
- Academic **honesty** taken very seriously
- *Any attempt* to gain *unauthorized access* to any system will be dealt with **harshly**

Introduction

Network Security

Information Security

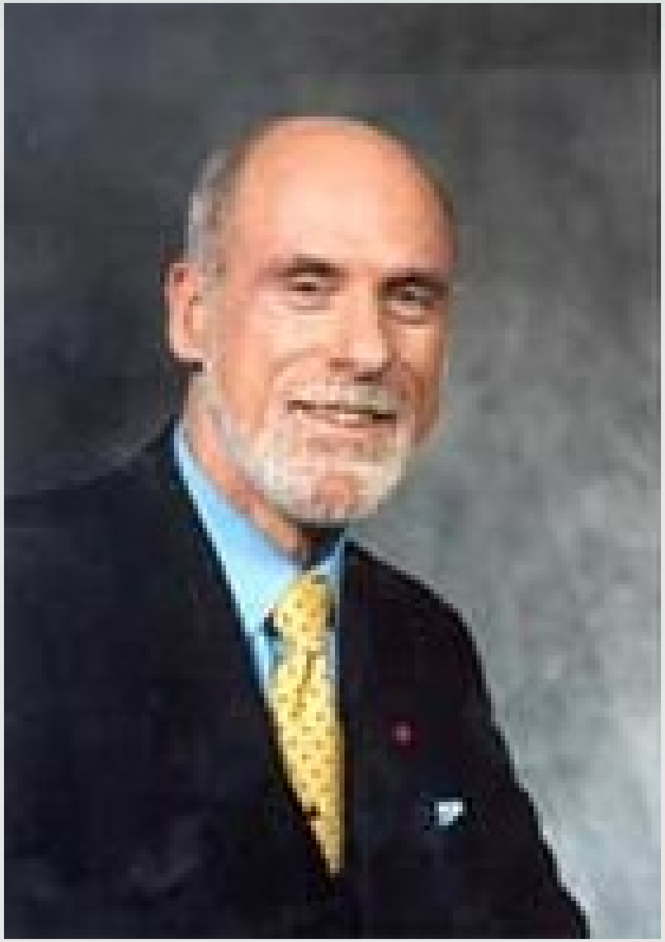
- Physical
- Administrative
- “Lockup the file cabinet”

Private Networks

- Isolated to individual organizations
- Emergence of **computer security**
- Sharing a system
- Protecting data

Networking

- Networks start talking to each other
- Gateways
- Arpanet
- TCP/IP Everywhere
- Vinton Cerf,
  “IP On Everything!”

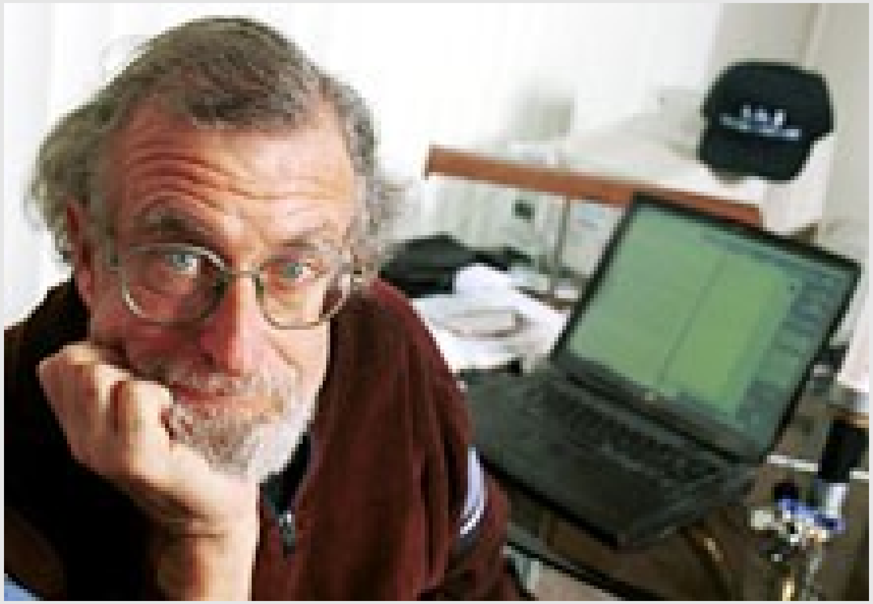


Maturing of the Internet

- Telephones used by 50% of worlds population
- Internet attains similar level of growth by 2010 – max growth
- Connecting computers and programmable devices
- More **devices** than people

Early Hacking

- Cap’n Crunch cereal prize
- Giveaway **whistle** produces 2600 MHz tone
- Blow into receiver – free phone calls
- “Phreaking” encouraged by Abbie Hoffman
- Doesn’t hurt anybody



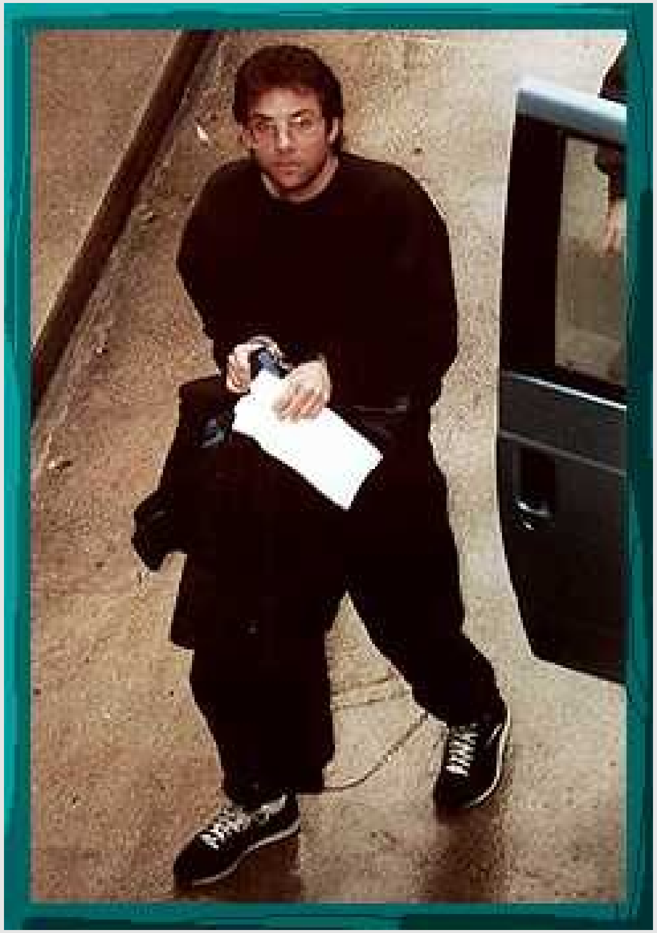
Captain Crunch

- **John Draper**
- `71: **Bluebox** built by many
- Jobs and Wozniak were early implementers
- Developed “EasyWriter” for first IBM PC
- High-tech hobo
- White-hat hacker

The Eighties

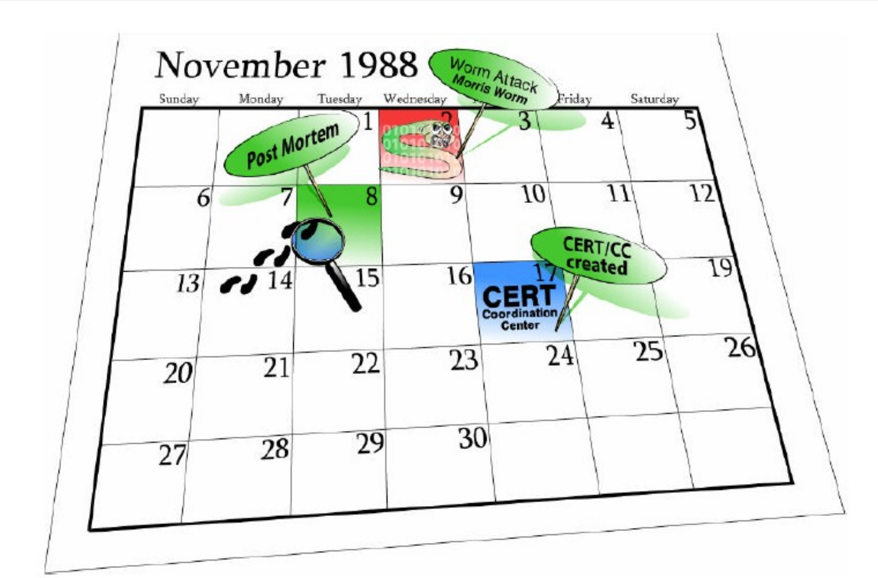
- 1983 – “War Games” movie
- Federal Computer Fraud and Abuse Act - 1986
- Robert Morris – Internet **worm** -1988
- Brings over 6000 computers to a halt
- $10,000 fine
- His Dad worked for the NSA!!!

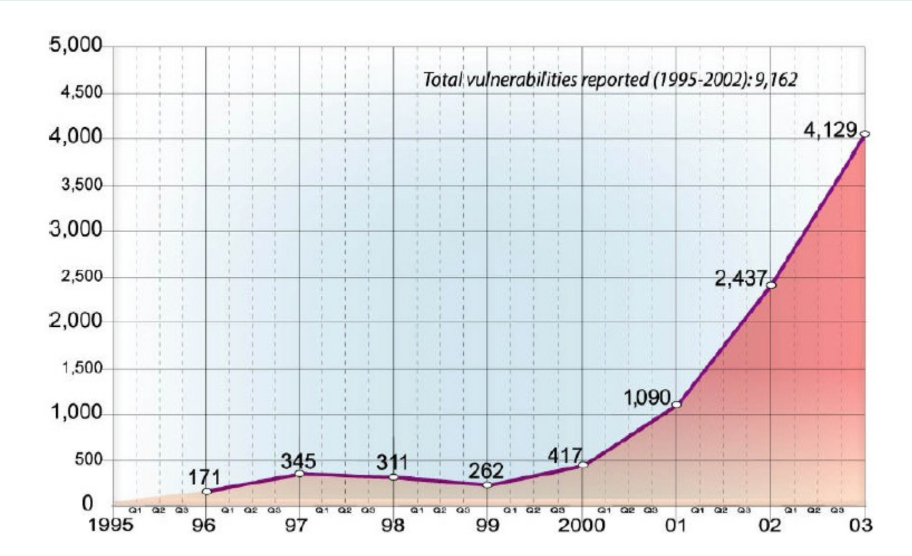
It Got Worse

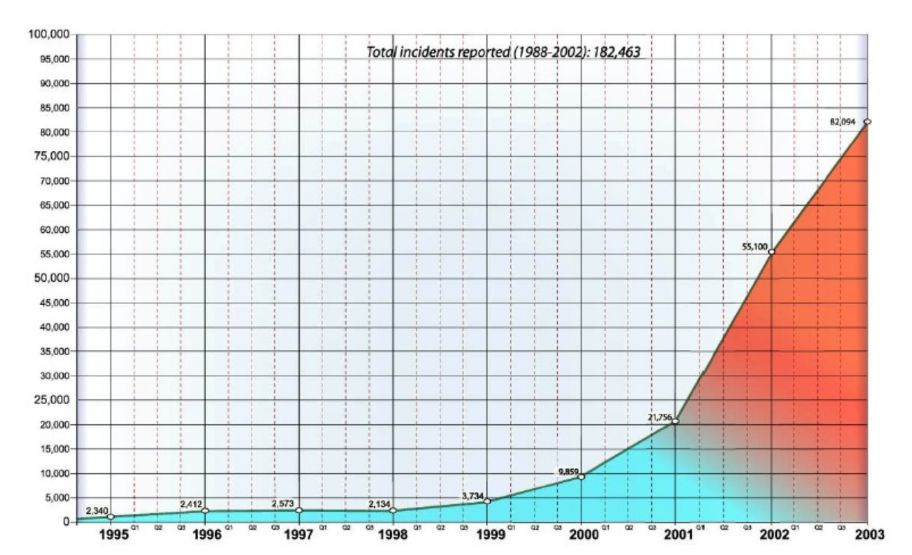


- 1995 – Kevin Mitnick arrested for the 2nd time
- Stole 20,000 credit card numbers
- First hacker on FBI’s *Most Wanted* poster
- Tools: password sniffers, spoofing
- http://www.2600.com

Tracking Attacks





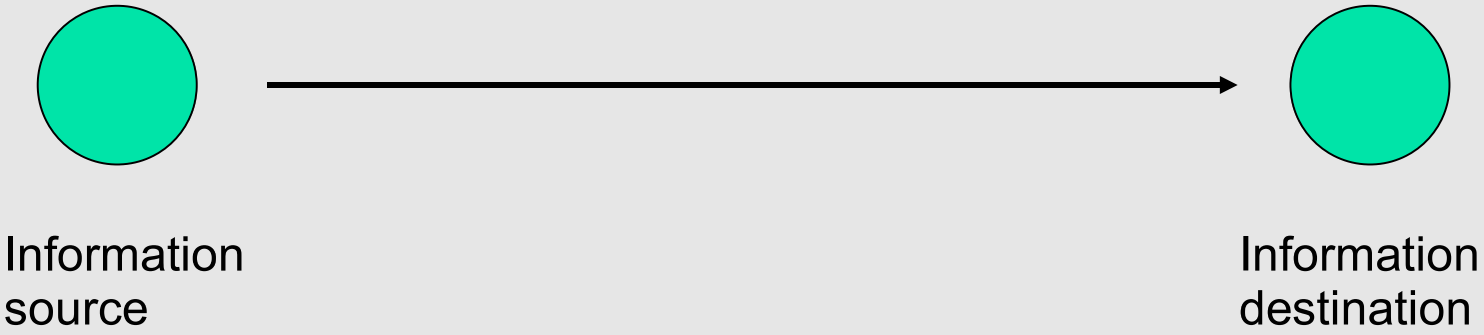


http://www.cert.org

Services, Mechanisms, Attacks (OSI Security Architecture)

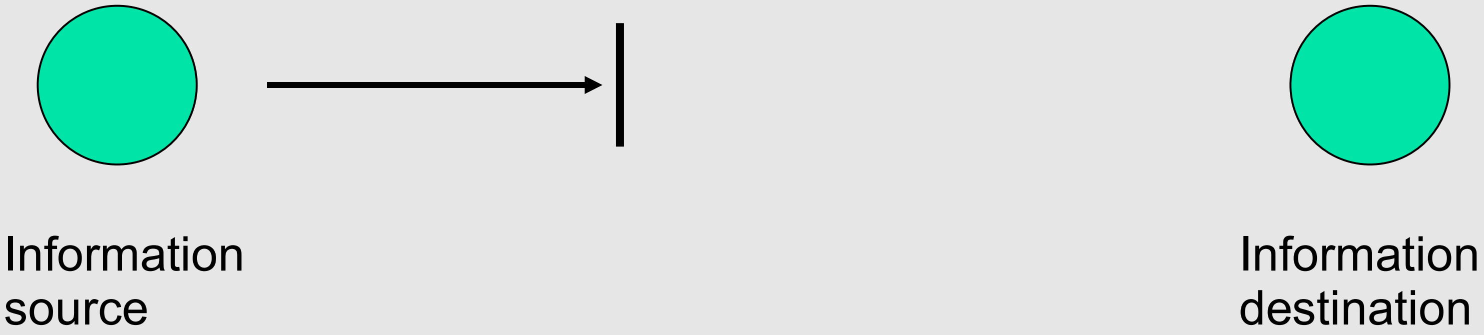
- Attack – action that compromises the security of information owned by an organization
- Mechanisms – detect, prevent or recover from a security attack
- Services – enhance the security of data processing systems and xfers – counter security attacks

Security Attacks



Normal Flow

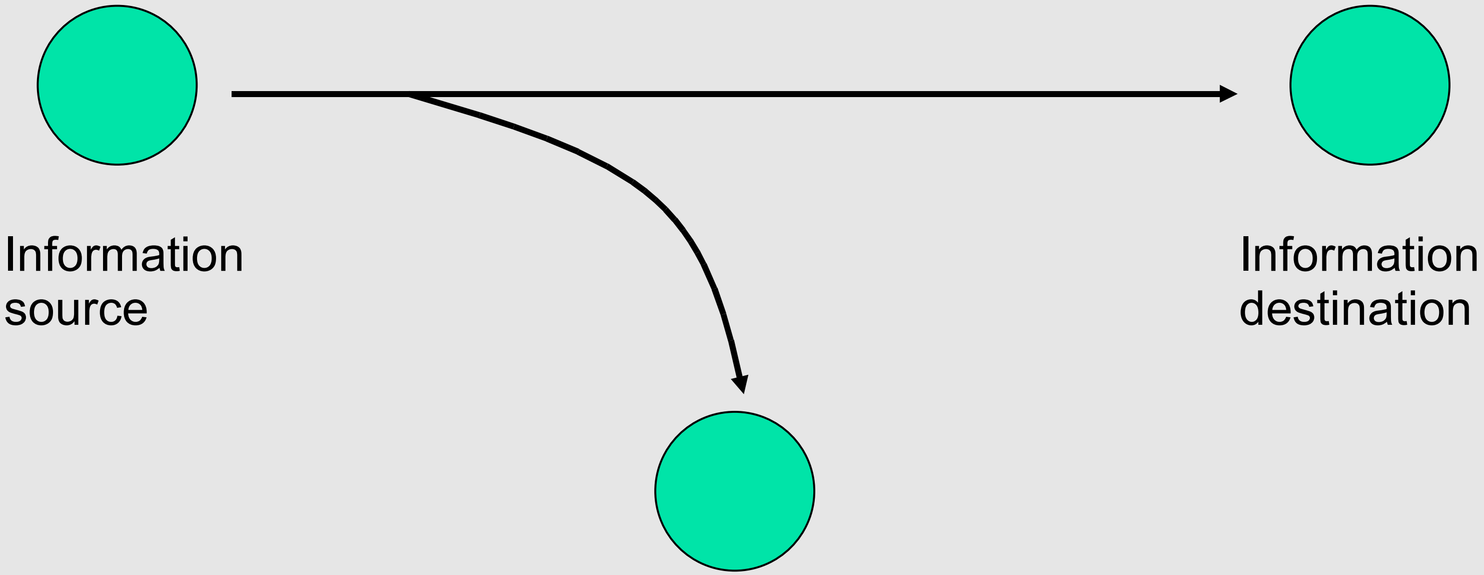
Security Attacks



Interruption

- Attack on **availability**

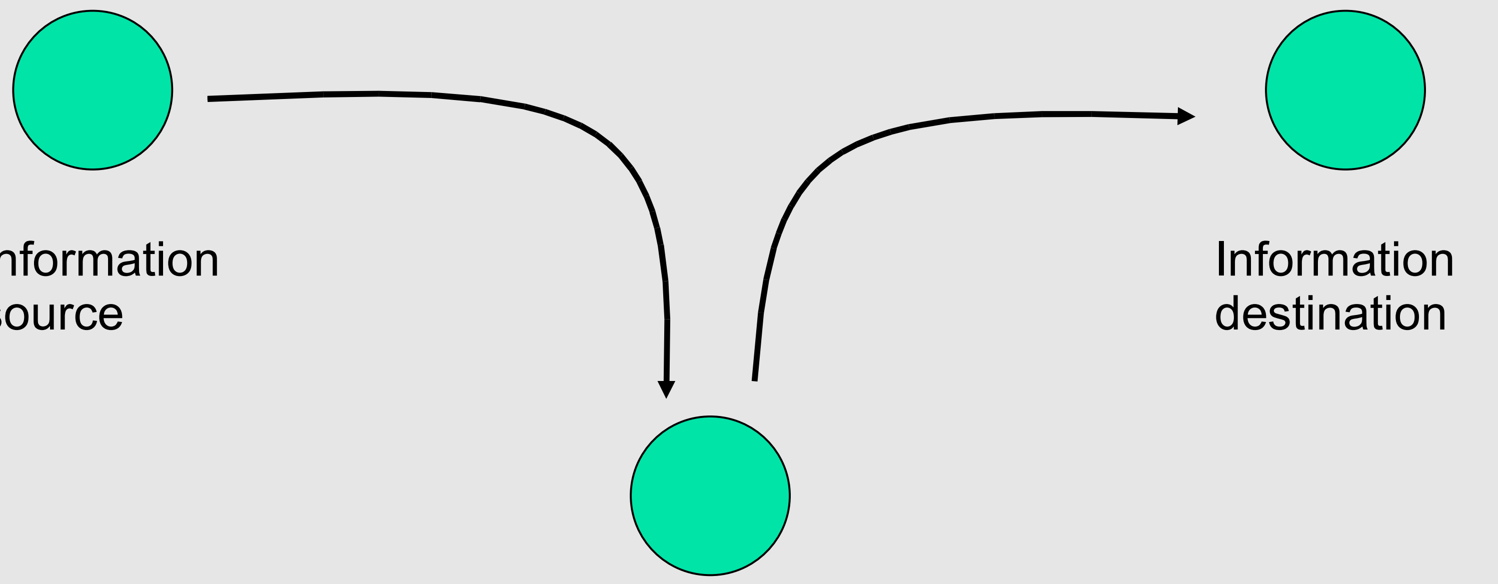
Security Attacks



Interception

- Attack on **confidentiality**

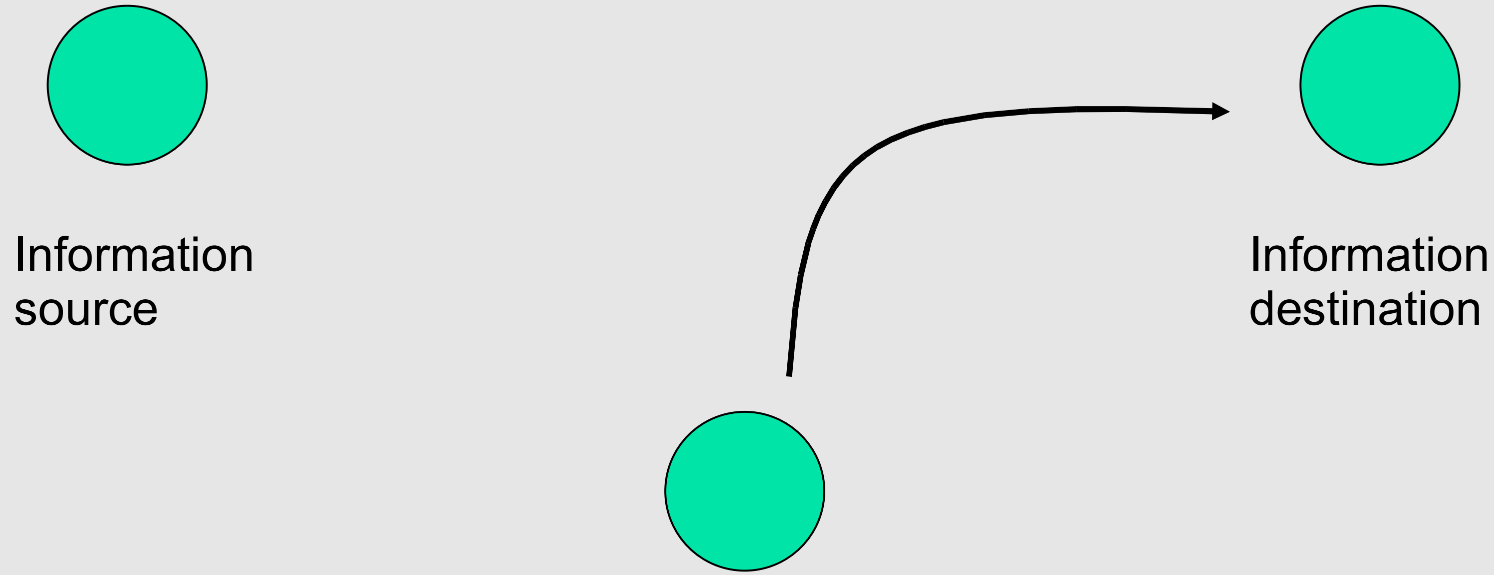
Security Attacks



Modification

- Attack on **integrity**

Security Attacks

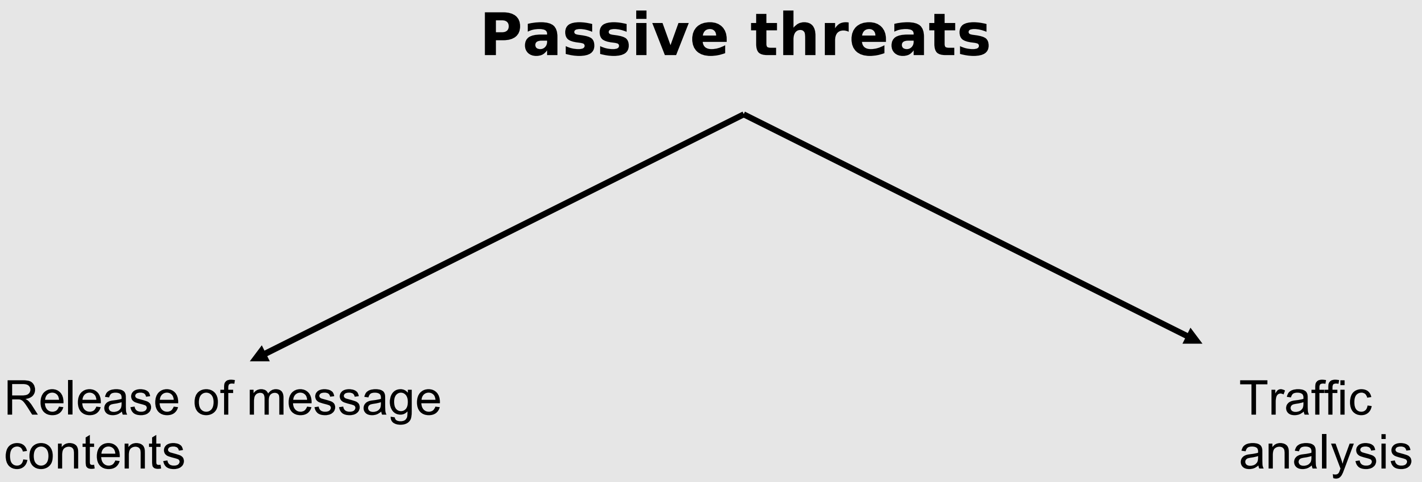

Information source

Information destination

Fabrication

- Attack on **authenticity**

Security Attacks



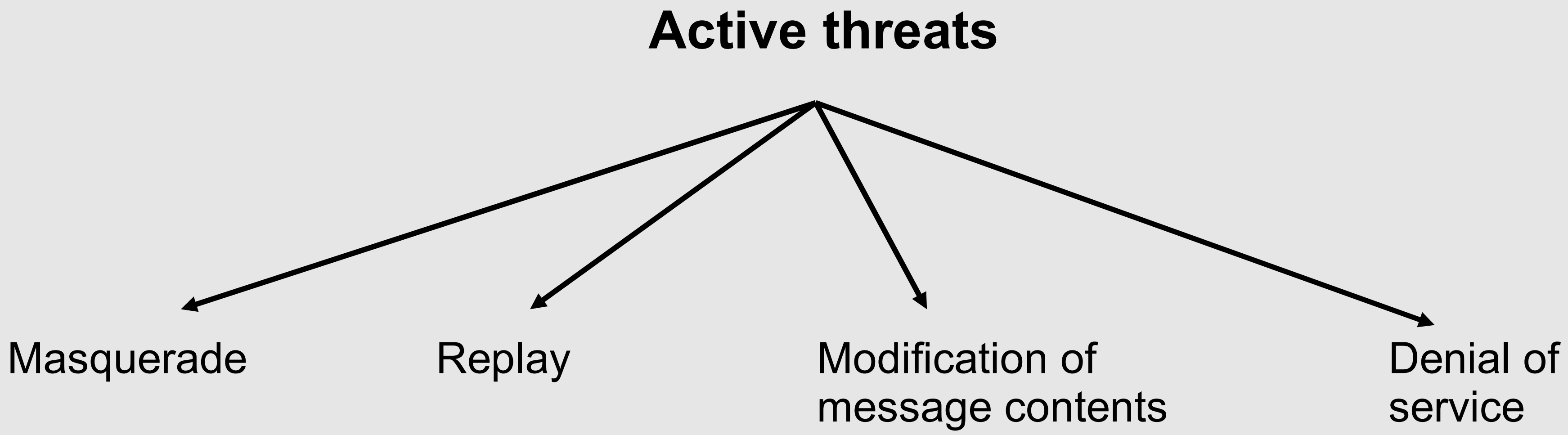
Passive threats

Release of message contents

Traffic analysis

- eavesdropping, monitoring transmissions

Security Attacks



- some modification of the data stream

Security Attacks

NEW YORKER

Steiner
"On the Internet, nobody knows you're a dog."

On the Internet, nobody knows you’re a dog

- by Peter Steiner, New York, July 5, 1993

Security Attacks

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

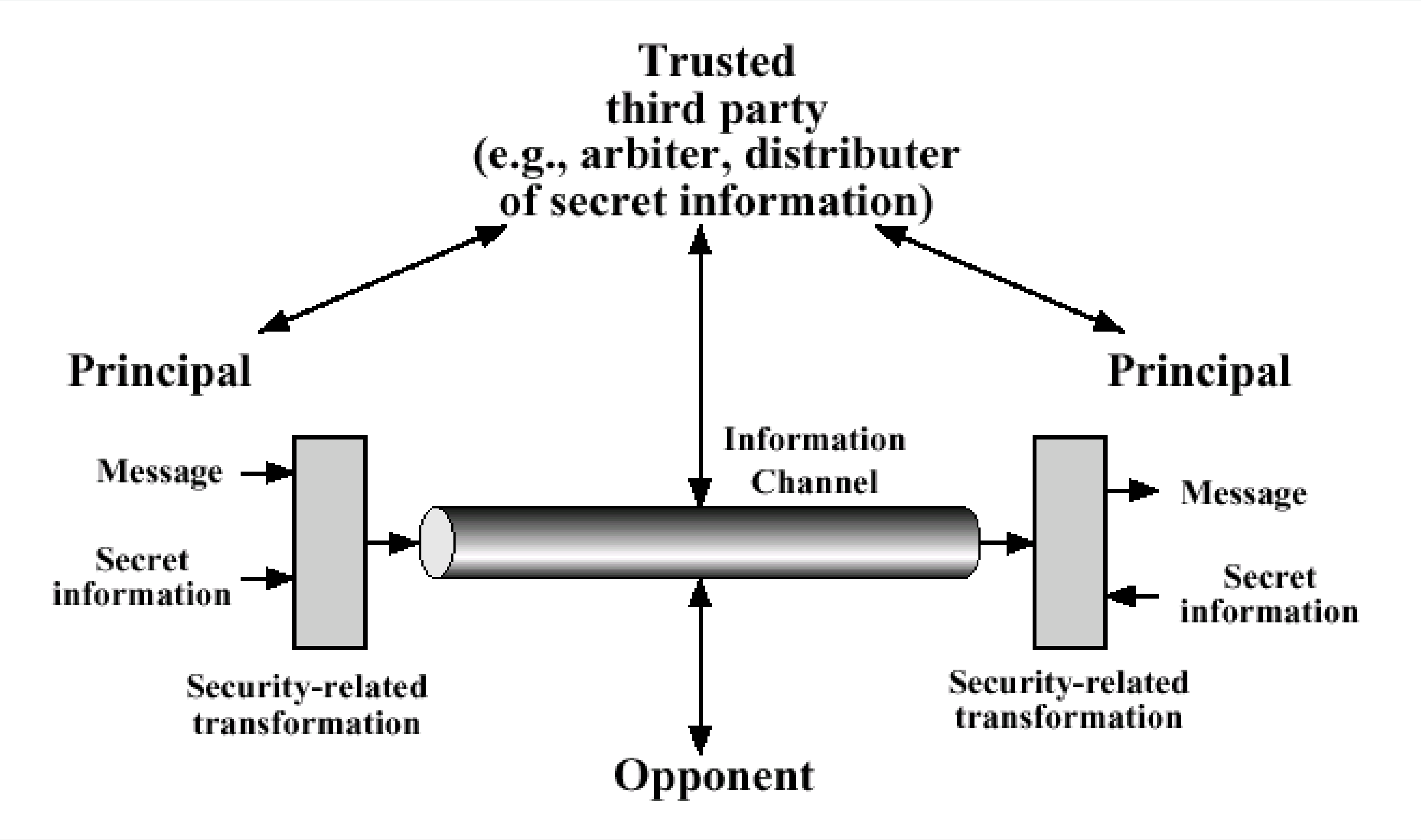
Security Services

- Confidentiality – protection from passive attacks
- Authentication – you are who you say you are
- Integrity – received as sent, no modifications, insertions, shuffling or replays

Security Services

- Nonrepudiation – can’t deny a message was sent or received
- Access Control – ability to limit and control access to host systems and apps
- Availability – attacks affecting loss or reduction on availability

Network Security Model


Trusted third party (e.g., arbiter, distributer of secret information)
Principal
Principal
Message
Secret information
Information Channel
Message
Secret information
Security-related transformation
Security-related transformation
Opponent

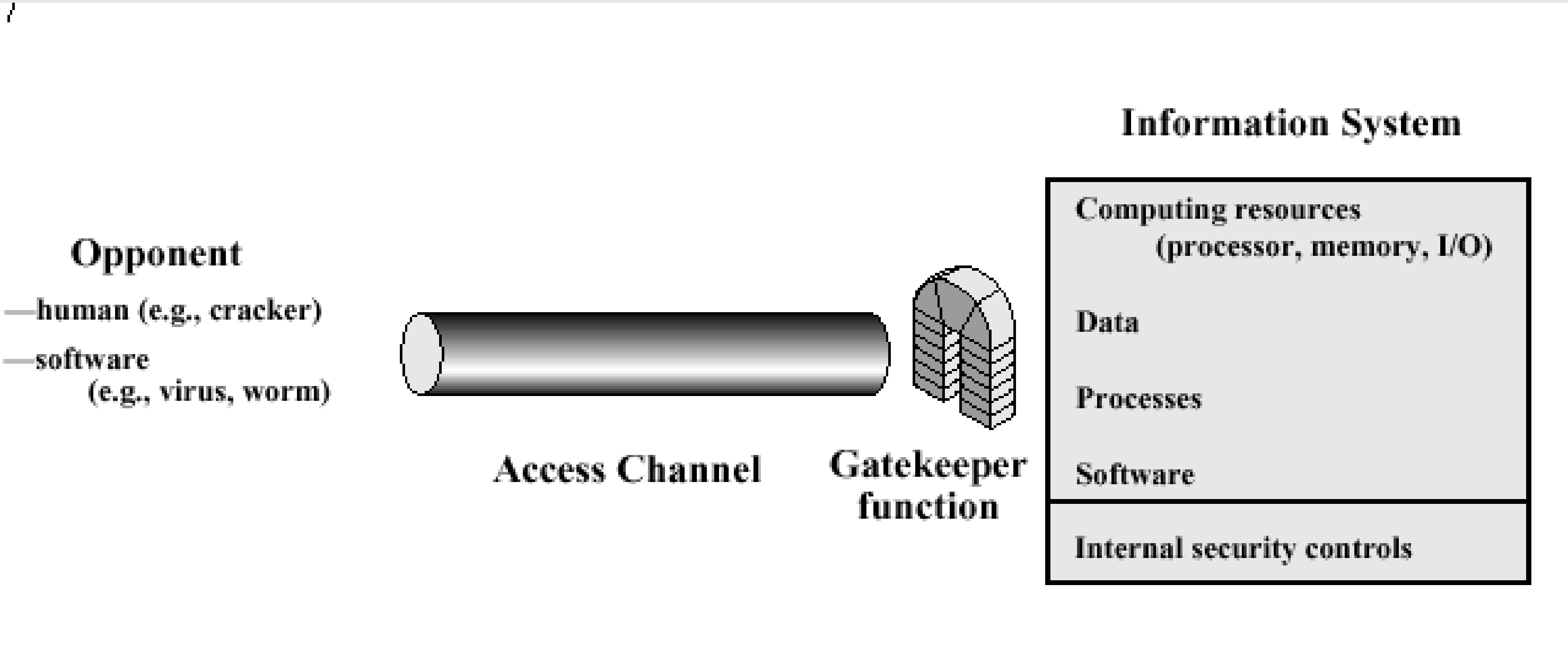
Network Security Model

Four basic tasks in designing a security service:

- Design algorithm
- Generate secret information to be used
- Develop methods to distribute and share info
- Specify a protocol to be used by the two principals

Protocols – Simple To Complex

Network Access Security Model



Internet Standards and RFCs

- **Internet Architecture Board** (IAB)
  - overall architecture

- **Internet Engineering Task Force** (IETF)
  - engineering and development

- **Internet Engineering Steering Group** (IESG)
  - manages the IETF and standards process

Request For Comments (RFC)

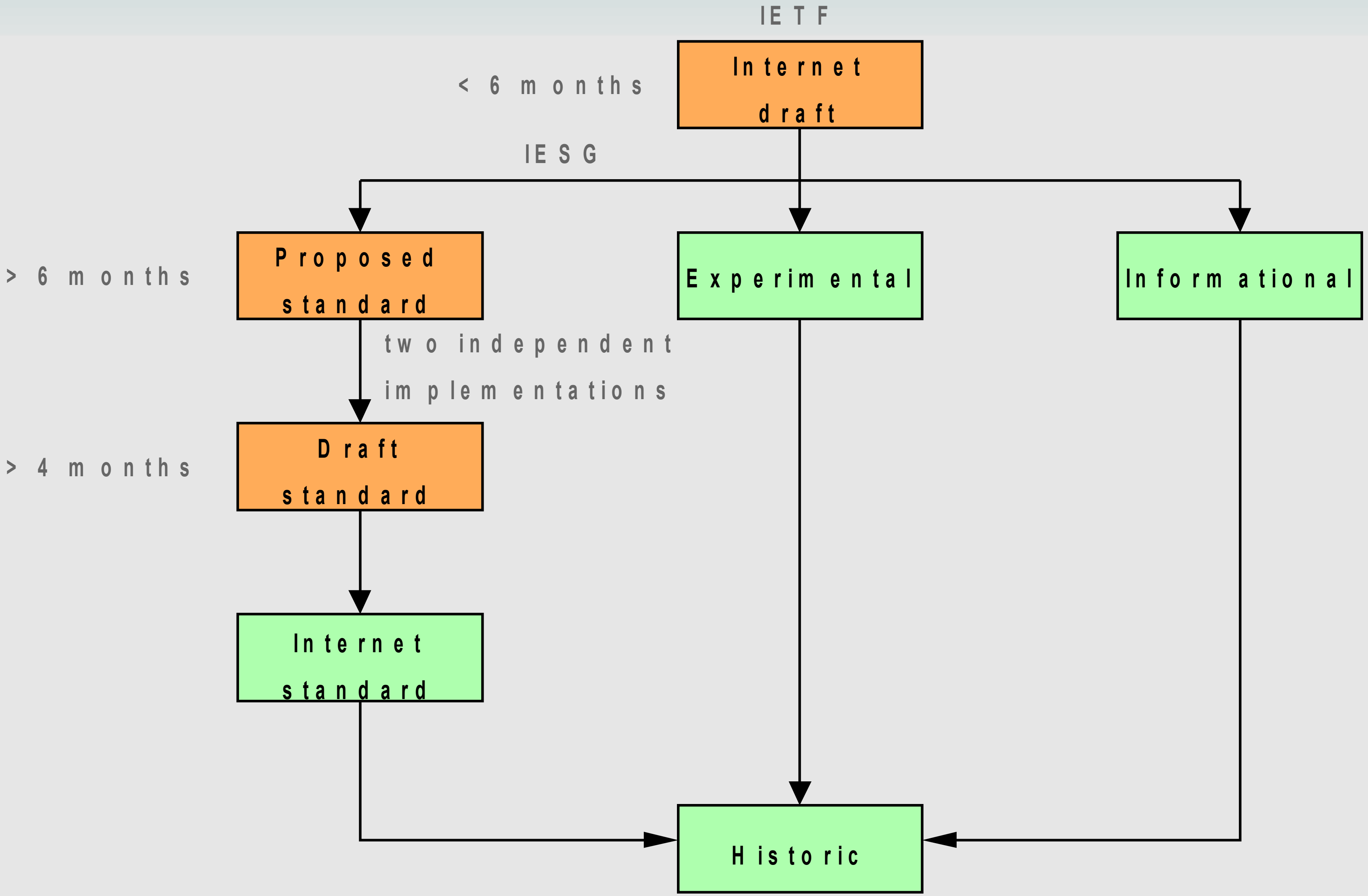
- RFCs are the working notes of the Internet research and development community

Standardization Process

- Stable and well understood
- Technically competent
- Substantial operational experience
- Significant public support
- Useful in some or all parts of Internet

Key difference from ISO: **operational experience**

RFC Publication Process



Some Current Topics

- http://www.aclu.org/pizza/images/screen.swf
- Eavesdropping Leaps Into 21st Century – *Matthew Fordahl*, NY Times, 1/22/2006
- Privacy for People Who Don't Show Their Navels – *Jonathan D. Glater*, NY Times, 1/25/2006
- Why We Listen – *Philip Bobbitt*, NY Times, 1/30/2006

Useful Websites

- http://www.williamstallings.com/NetSec2e.html
  Some recommended sites by the text author
- http://www.rfc-editor.org/rfcsearch.html
  Search RFCs
- http://www.cert.org
  Center for Internet security
- http://www.counterpane.com/alerts.html
  Some recent alerts

Homework

- Read Chapter One
- Read NYTimes Articles Under “Documents” http://www.cs.hofstra.edu/~cscvjc/Spring06
- Be Ready To Discuss

Have A Nice Week!!!