

Welcome to COMP 6370

Computer and Network Security

Today's Lesson:

1. Course Introduction
2. Administrative Comments
3. Internet Standards, RFCs and Conventional Encryption

“All Warfare is Based on Deception”

Sun-Tzu



Course Objectives

- 1). Recognize potential risks and threats to computer operations and communications.
- 2). Understand Federal rules and regulations affecting computer security, including legal ramifications, FOIA, and policies.
- 3). Understand security issues unique to wireless communications.
- 4). Have a working knowledge of relevant cryptographic techniques.
- 5). Have a critical understanding of computer security with an emphasis on “end-to-end” vulnerabilities.



Background

- **Students should always gather intelligence about who they are dealing with.**
 - Intelligence gathering is not always malevolent, but does need to be monitored.
- **ENS policies and procedures.**
- **NSA Center of Academic Excellence**
- **Information Assurance Laboratory**
- **U.S. versus international perspectives.**

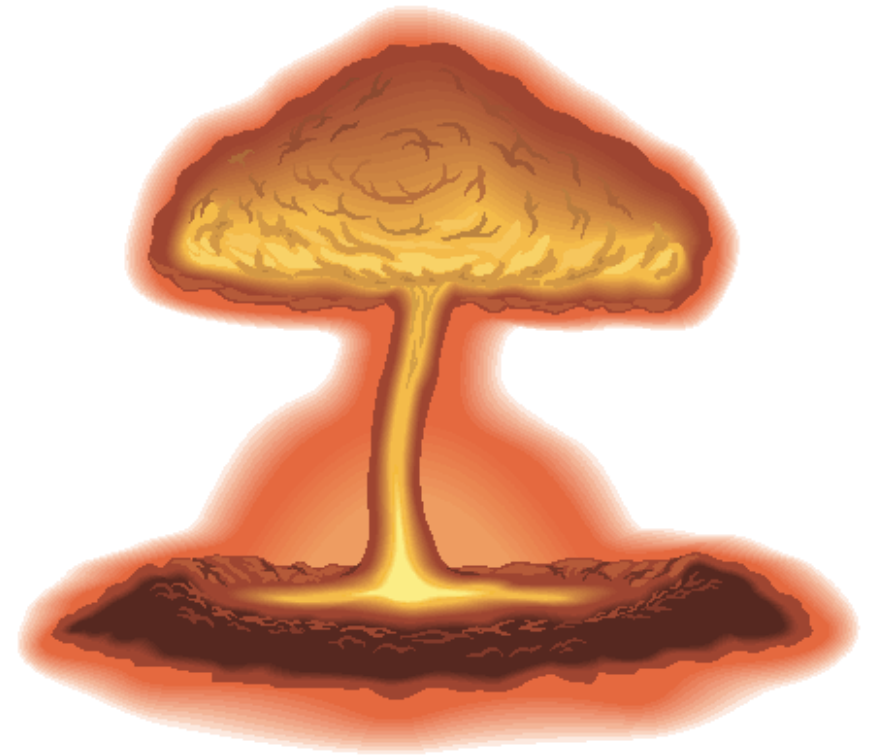


Information Assurance Minor (INAS), MSwE & Ph.D.

- **A student must take the following courses:**
 - COMP 6370 Computer and Network Security
 - ADMH 6180 Cryptography
- **A student must also take one course from the following:**
 - COMP 6320 Design and Analysis of Computer Network
 - COMP 6350 Digital Forensics
 - COMP 6500 Advanced Operating Systems
 - COMP 6520 Network and Operating System Administration
 - COMP 7360 Wireless and Mobile Networks
 - COMP 7370 Advanced Computer and Network Security
- **Annotation on transcript:**
INFORMATION ASSURANCE OPTION



Grades



Lecture 1

Internet Standards, RFCs and Conventional Encryption

Slides modified from Henric Johnson
Blekinge Institute of Technology, Sweden



Outline

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

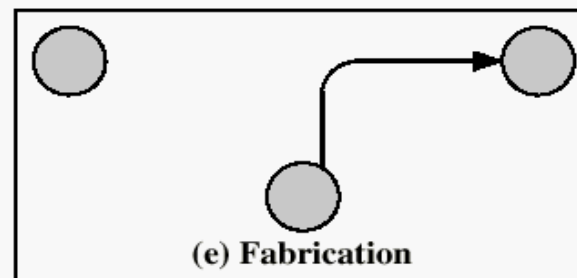
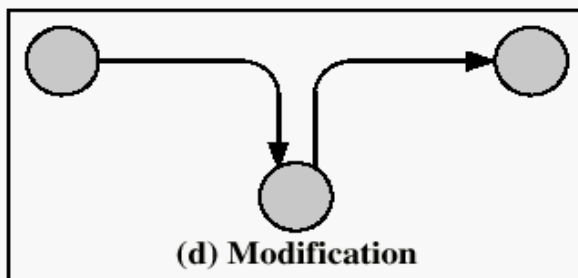
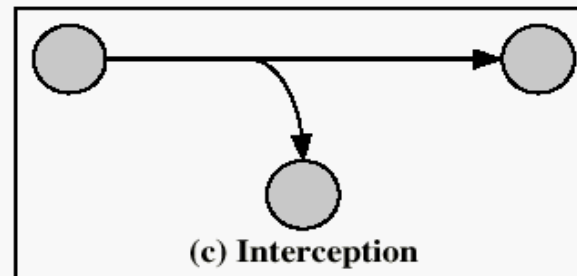
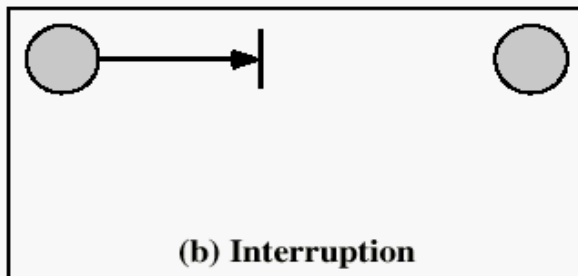
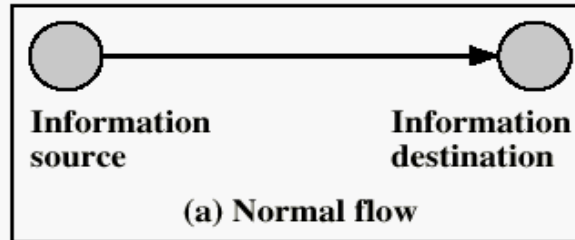


Attacks, Services and Mechanisms

- **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



Stallings' Taxonomy

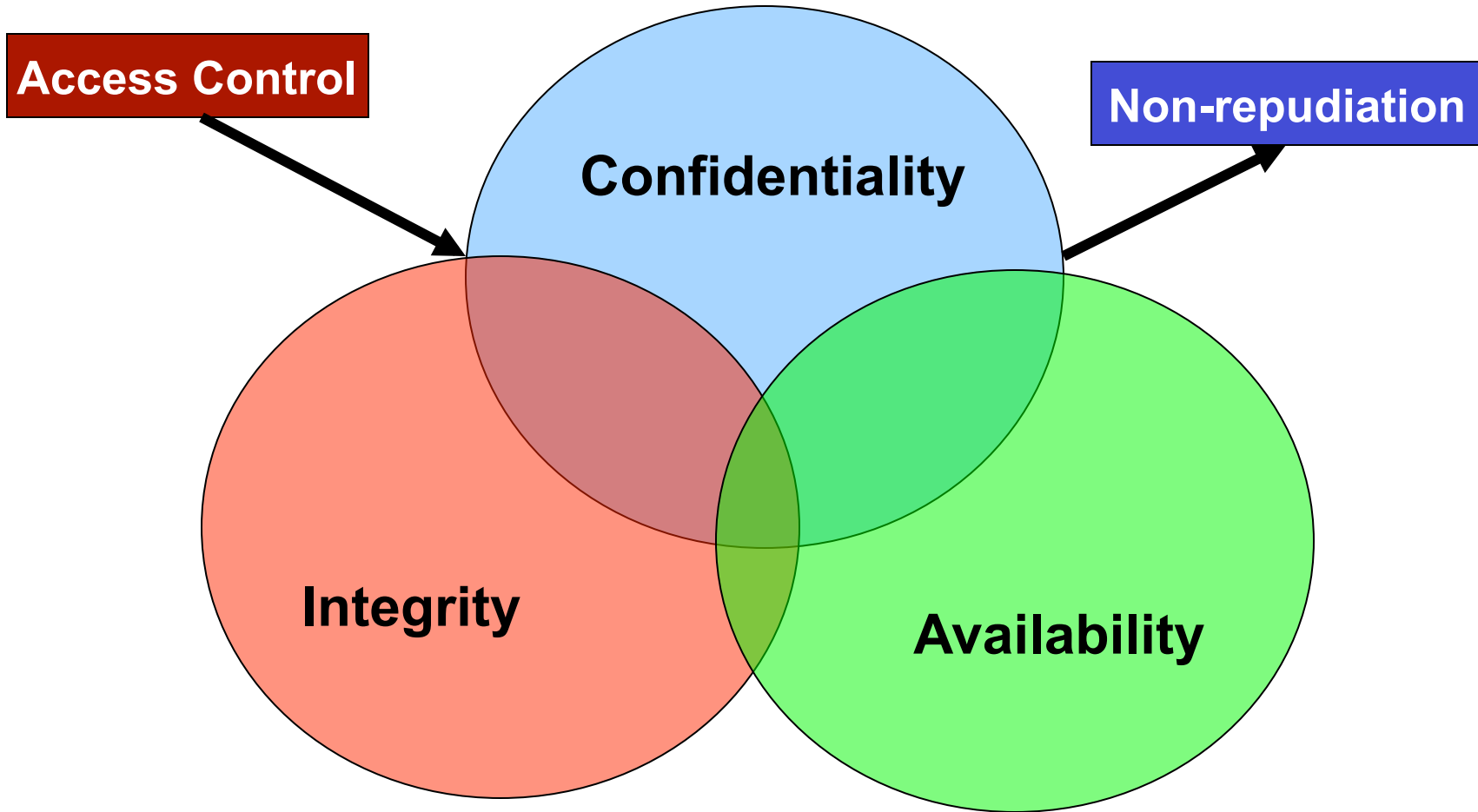


Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

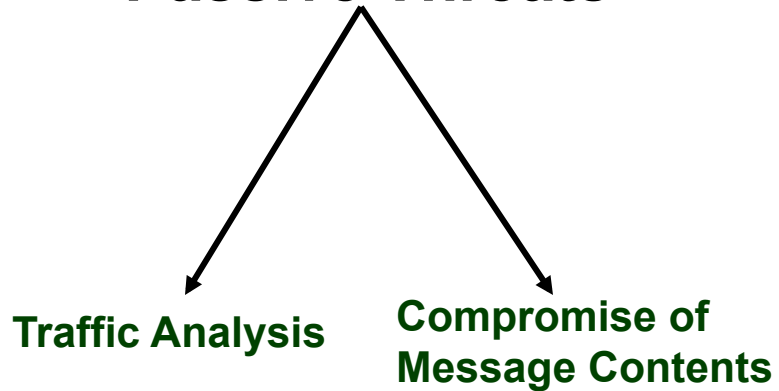


Security Goals

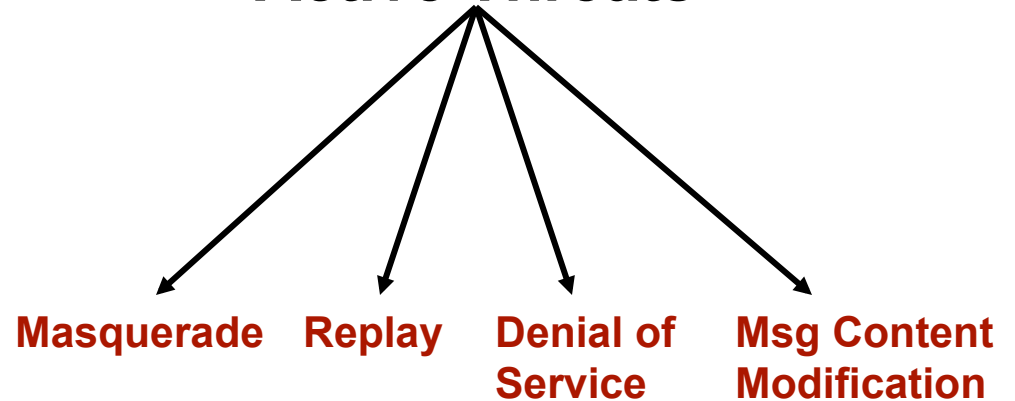


Active and Passive Security Threats

Passive Threats



Active Threats



Sensitive Data (U.S. Government)

- **Unclassified**
- **Sensitive but Unclassified (SBU)**
- **FOUO**
- **Confidential**
- **Secret**
- **Top Secret**
- **Top Secret SCI (Compartmented)**
- **So secret that the classification itself is classified**
 - **Other countries have other designations**
 - **secret discreet**
 - **NOFORN**



Security Services

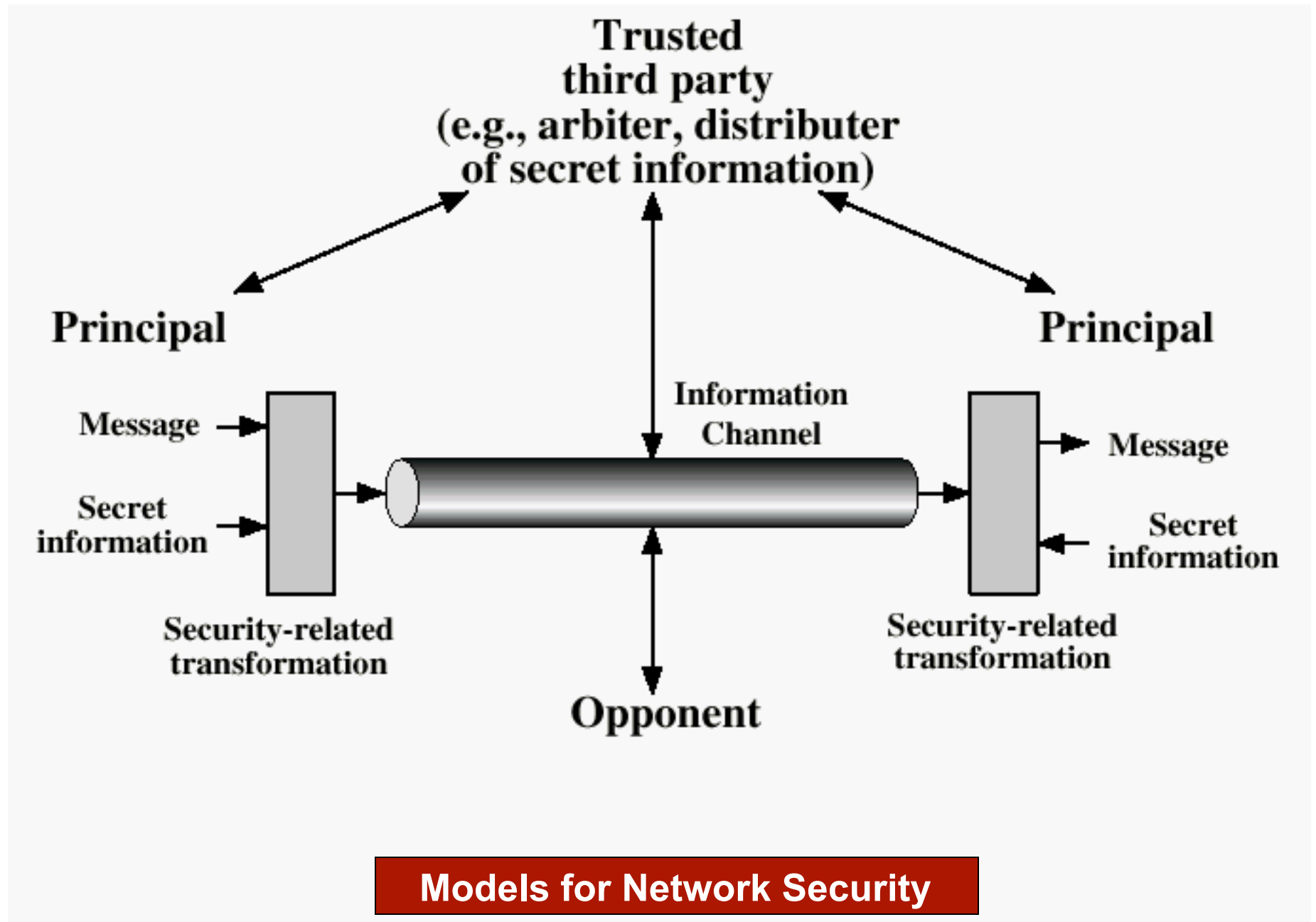
- **Confidentiality (privacy)**
- **Authentication (who created or sent the data)**
- **Integrity (has not been altered)**
- **Non-repudiation (the order is final)**
- **Access control (prevent misuse of resources)**
- **Availability (permanence, non-erasure)**
 - **Denial of Service Attacks**
 - **Virus that deletes files**



Designing a Security Service (Secure Data Transfer – see next)

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

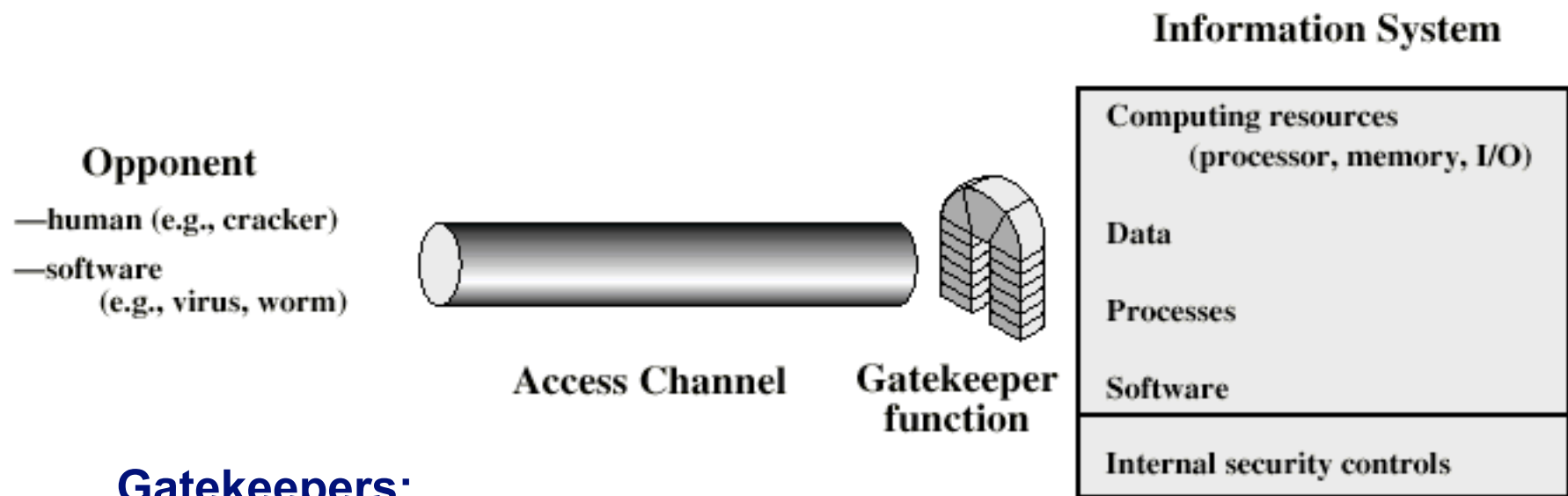




Models for Network Security



Networks Access Security Model



Gatekeepers:

Passwords/Logins
Screening Logic
ex. malware

After gatekeepers come various forms of internal controls as the last line of defense

Preventing unwanted access



Methods of Defense

- **Encryption**
- **Software Controls (access limitations in a data base, in operating system protect each user from other users)**
- **Hardware Controls (smartcard)**
- **Policies (frequent changes of passwords)**
- **Physical Controls**



Security Standards

Internet - Internet Engineering Task Force (IETF)

De Facto (PGP email security system, Kerberos-MIT)

ITU (X.509 Certificates)

**National Institute of Standards and Technology
(SHA –1 secure hash function)**

IEEE

DOD, Nat. Computer Security Center

- Tempest (radiation limits)
- Orange Book: Class A1, B3, C1, C2, ...

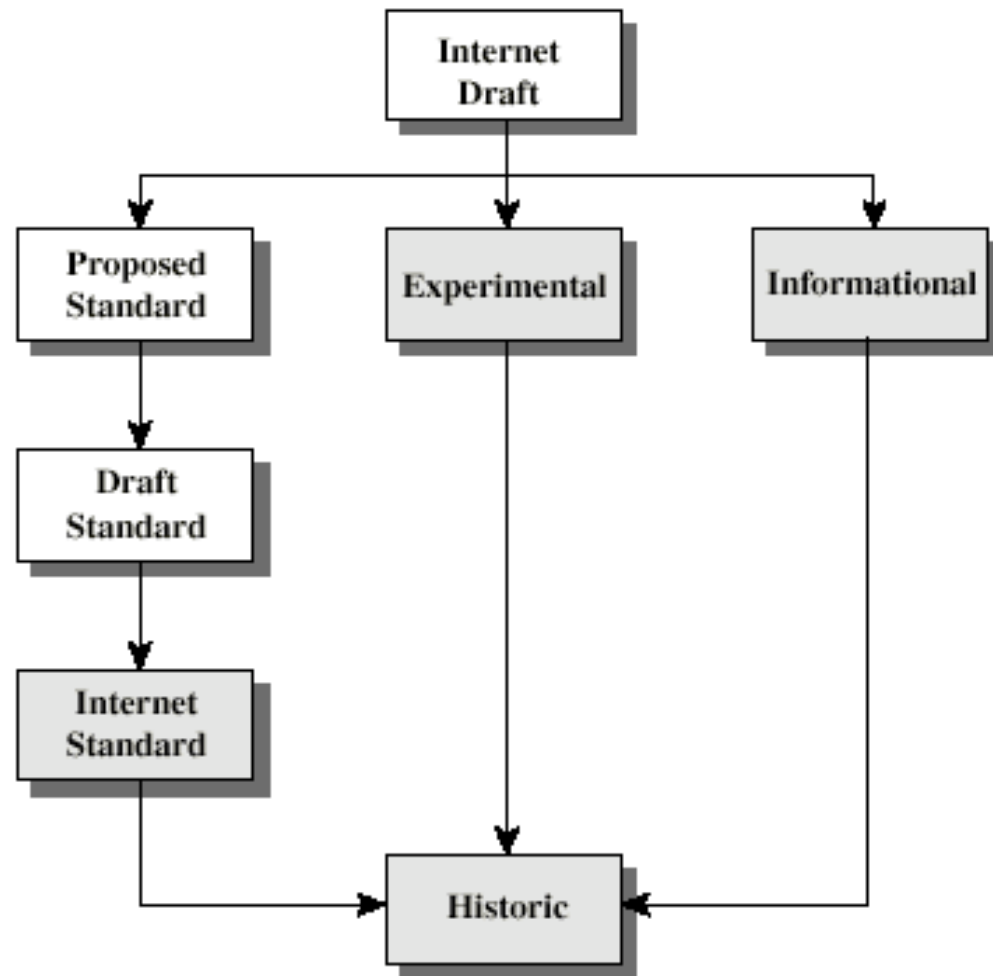
Export Controls

- High Performance Computers
- Systems with “Hard” Encryption



Internet RFC Publication Process

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



Note: there exists an internet security group



Viruses, Worms, and Trojan Horses

Virus - code that copies itself into other programs

Payload - harmful things it does, after it has had time to spread.

Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses)).

Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).

Logic Bomb - malicious code that activates on an event (e.g., date).

Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.



Virus Protection

1. **Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.**
2. **Do not execute programs (or "macro's") from unknown sources (e.g., PS files, HyperCard files, MS Office documents, Java, ...), if you can help it.**
3. **Avoid the most common operating systems and email programs, if possible.**



Recommended Reading

- **Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001.**
- **Internet Request for Comments**
<http://www.rfc-editor.org/>
- **Security RFCs**
<http://www.cert.dfn.de/eng/resource/rfc/>



This course is important

- **Computer and Network Security is the antithesis of information warfare.**

“War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied.”

Sun-Tzu

