

Cryptography (CS-452)

Week 1

Course Information

● Course: **CS-452** (3 credits)

◆ Time:

■ Monday 7:00 pm - 9:45 pm

◆ Place: CS-104 Teaching Lab

◆ Course Website: Titanium

● Instructor: **Mikhail I. Gofman, Ph.D., CISSP**

◆ Email: mgofman@fullerton.edu

◆ Phone: (657) 278-7304 (office)

◆ Office: CS-429

◆ Office Hours: Office Hours:

■ Monday, Tuesday, Wednesday: 2:30 pm -- 6:00 pm

■ Thursday: 4:00 pm - 5:00 pm

■ By Appointment

Prerequisites

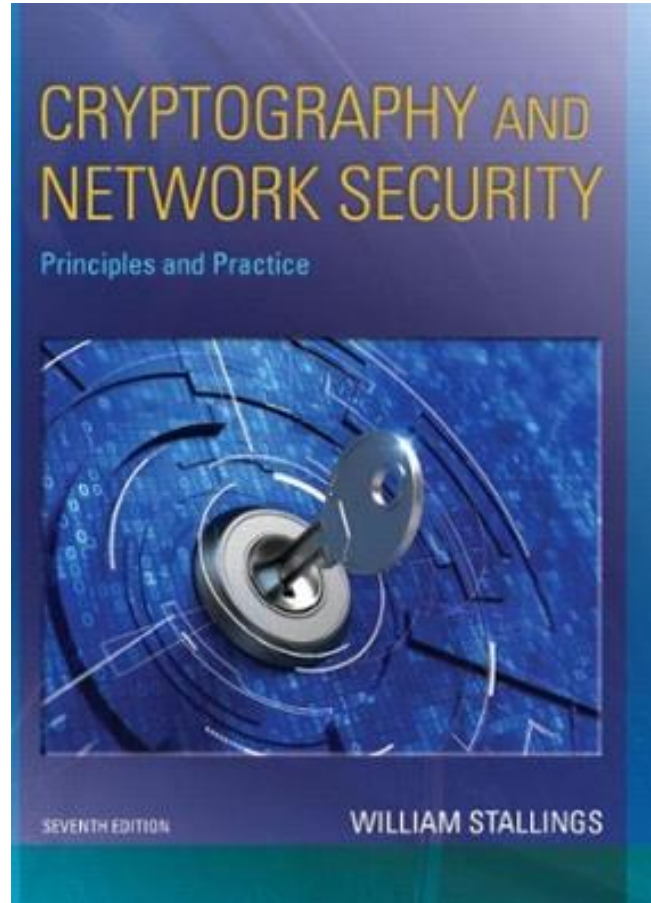
- Prior to taking this course, you must have taken (strictly enforced):
 - ◆ CPSC 311: Technical Writing for Computer Science
 - ◆ MATH 270B: Mathematical Structures II
 - ◆ Or, have the permission of the CS department.
- Failure to meet the prerequisites may result in you being dropped administratively.

Course Objectives

- To journey through principals and practices of cryptography, network security:
 - ◆ Fundamentals of network and network security.
 - ◆ Cryptography:
 - Encryption and decryption techniques
 - Cryptanalytic Techniques
 - Classical Ciphers
 - Symmetric Encryption
 - Public Key Cryptography
 - Key management
 - Digital signatures
 - Authentication protocols

Texts

- William Stallings Cryptography and *Network Security Principles and Practice, Sixth/Seventh Edition*. ISBN-13: 9780134444284 ISBN: 0134444280



- All additional materials shall be posted on [Titanium](#).

Evaluation (1)

● Course grade breakdown:

- ◆ Assignments: 25% (around 4 Assignments)
- ◆ Quizzes/Lab Exercises: 15% (may drop 1 lowest)
- ◆ Attendance and participation: 3% (may miss 1 class)
- ◆ Midterm: 20%
- ◆ Final Exam: 22%
- ◆ Final Project: 15%

- The course grade shall be **curved** over the entire class, and (**strictly**) assigned according to the following range:

A+: $\geq 95\%$	A: $\geq 92\%$	A-: $\geq 90\%$
B+: $\geq 88\%$	B: $\geq 82\%$	B-: $\geq 80\%$
C+: $\geq 78\%$	C: $\geq 72\%$	C-: $\geq 70\%$
D+: $\geq 68\%$	D: $\geq 62\%$	D-: $\geq 60\%$

Evaluation (2)

- All assignments shall be averaged together.
- All Quizzes/Labs shall be averaged together.
- The raw score is a weighted mean of:
 - ◆ Assignment average
 - ◆ Quizzes/Lab averages
 - ◆ Midterm exam
 - ◆ Final Exam
 - ◆ Final Project
 - ◆ Attendance and participation
- **Curve:**
 - ◆ The raw score shall be curved over an entire class.
 - ◆ The amount of curving depends on how everyone scores.
 - ◆ Curving shall not cause your grade to decrease.

Evaluation (3)

- Computing your raw score.
- Suppose John Doe receives the following scores:

- ◆ Assignments:

- Assignment 1: 100/100
- Assignment 2: 80/100
- Assignment 3: 70/100

$$\begin{aligned}\text{Average} &= (100 + 80 + 70) / 3 \\ &= 83.33\end{aligned}$$

- ◆ Quizzes/Labs:

- 50/100
- 90/100
- 80/100
- 100/100

$$\begin{aligned}\text{Average} &= \\ &= (90 + 80 + 100) / 3 = 90 \text{ (the lowest grade is dropped).}\end{aligned}$$

- ◆ Midterm Exam: 70/100
- ◆ Final Exam: 50/100
- ◆ Attendance: 100/100
- ◆ Final Project: 100/100

Evaluation (4)

Item	Category Average	Category Weight	Result (avg * weight)
Assignments	83.33/100	25	$(83.33/100) * 25 = 20.83$
Quizzes/Labs	90/100	15	$(83.33/100) * 15 = 13.5$
Midterm	70/100	20	$(70/100) * 20 = 14$
Final Exam	50/100	20	$(50/100) * 20 = 10$
Attendance	100/100	5	$(100/100) * 5 = 5$
Final Project	100/100	15	$(100/100) * 15 = 15$

Sum: $(20.83 + 13.5 + 14 + 10 + 5 + 15) = 78.33$

Evaluation (5)

- All grades shall be posted on Titatium.
- A spreadsheet called [gradecalcCS452.xlsx](#) can be used to forecast your grades.
 - ◆ Available on Titanium.
 - ◆ Replace numbers in the blue cells with your own grades.

Evaluation (6)

https://moodle-2015-2016.fullerton.edu/course/view.php?id=84106

Titanium 2015-2016 Mikhail Gofman

Spring 2016 CPSC 452-01 20068

My home ▶ My courses ▶ Spring 2016 ▶ A-G ▶ Spring 2016 CPSC 452-01 20068 Turn editing on

ADMINISTRATION

- Course administration
 - Turn editing on
 - Edit settings
 - Users
 - Filters
 - Reports
 - Grades
 - Outcomes
 - Backup
 - Restore
 - Import
 - Reset
 - Question bank
- Switch role to...
- My profile settings



PEOPLE

- Participants

ACTIVITIES

- Assignments
- Forums
- Quizzes
- Resources

SEARCH FORUMS


[News forum](#)
[News forum](#)

CPSC 452: Cryptography


Section: SEC-01

Meeting Times: M 7:00PM - 9:45PM


Room: CS-408

[Syllabus](#)

Contains important course information that all students are ~~required to read.~~

[Grade Calculator Spreadsheet](#)


~~Know how to check and request your grades.~~

[Grade Calculator Spreadsheet](#)
[Anonymous Feedback](#)

Please feel free to submit any questions, comments, or suggestions via the link below.

All submissions are *strictly anonymous*.

<http://ecs.fullerton.edu/~mgofman/teaching.html> (will open in a new tab).

[Instructions for Connecting to Titan Server from Windows](#)

Instructions for Linux users: simply open the terminal and type `ssh yourusername@ecs.fullerton.edu`


You will receive account information in class.

LATEST NEWS

[Add a new topic...](#)

(No news has been posted yet)

UPCOMING EVENTS

 [Presidents' Day - Campus Closed](#)
Monday, February 15, 12:00 AM

[Go to calendar...](#)
[New event...](#)







RECENT ACTIVITY

Activity since Saturday, January 23, 2016, 12:13 AM

[Full report of recent activity...](#)

No recent activity

QUICKMAIL

-  [Compose New Email](#)
-  [Signatures](#)
-  [View Drafts](#)
-  [View History](#)
-  [Alternate Emails](#)
-  [Configuration](#)

Assignments

- **Programming assignments:** may contain both, theoretical and programming questions.
 - ◆ To be done individually unless stated otherwise.
 - ◆ Must be completed on Tuffix virtual machine, unless stated otherwise:
 - VM download link: <https://bit.ly/3ggtl1T>
 - ◆ Students may use C, C++, Java, Python or C# (unless specified otherwise).
 - ◆ Familiarity with basic C and Unix is assumed.
- All completed assignments must be **submitted** via **Titanium**.
- Late assignments shall be **penalized 10%**.
- No assignment shall be accepted after **24 hours** from the deadline.

Quizzes

● In-Class quizzes:

- ◆ Closed book.
- ◆ Test your understanding of the material presented in class.
- ◆ Missed quizzes shall earn a **grade of 0** (unless you can provide written evidence of a legitimate excuse e.g. doctor's note).

● Lab Exercises:

- ◆ Require **critical thinking** (and creativity!).
- ◆ Late submissions shall be **penalized 10%**.
- ◆ No quiz shall be accepted after **24 hours** from the deadline.

Exams

- All exams are **comprehensive** and **closed book**.
- **Midterm:** 3/15/2021 (Tentative)
- **Final Exam:** 5/17/2021 7:00 p.m. - 8:50 p.m. (Monday)
 - ◆ Check with the Final Exam Schedule posted online.
- Missed exams shall be dealt with according to University policies on incompletes and withdrawals.

Attendance and Participation

- The attendance is **mandatory** and shall be taken at beginning of every class.
- ***Please don't forget to sign the attendance sheet!***
- You may miss **1 class** without incurring attendance penalties.
- Participate in class discussions (don't be afraid!).
- Ask questions!

Handouts

- The handouts are provided for your benefit
- *Will not be collected or graded*
- Highly *encouraged to complete them*
- If you attempt a handout question and get stuck, *the instructor will be happy to help*

Final Project

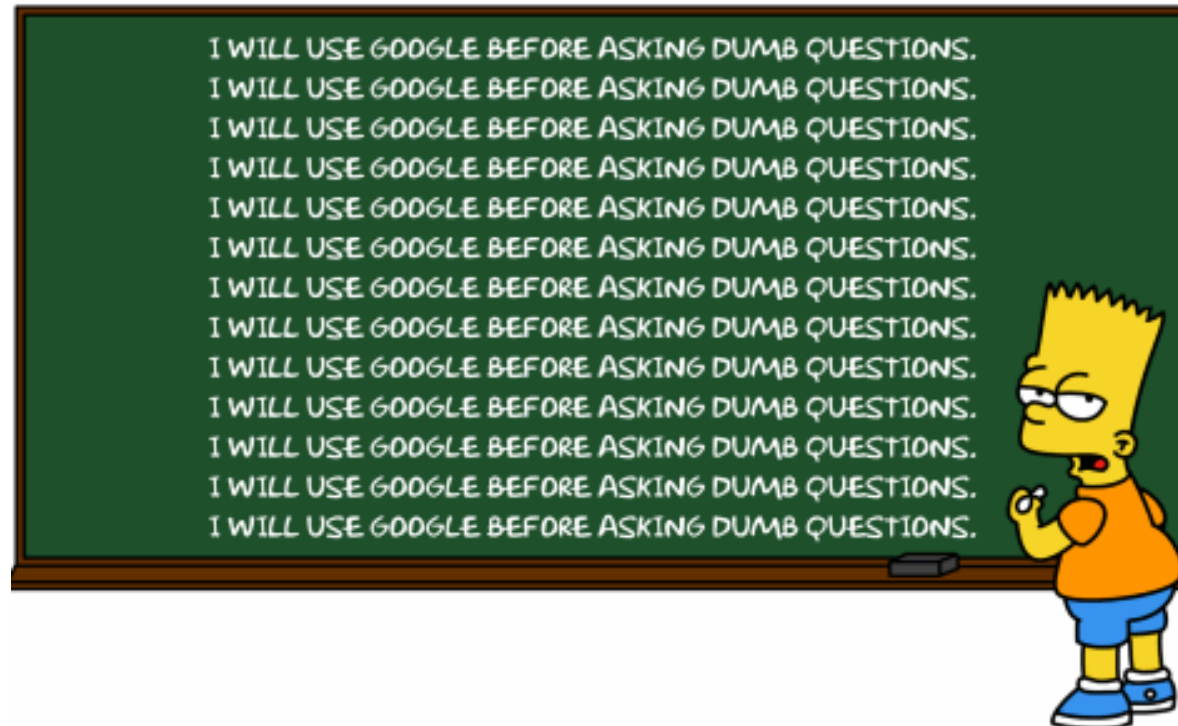
- Shall include a written component and a video or in-person presentation.
- May choose to do either a programming or a practical skills project.
- A list of choices shall be posted on Titanium during the semester.

Extra Credit

- Some assignments, exams, and quizzes may include **bonus sections**.
- **No** other forms of extra credit shall be granted.

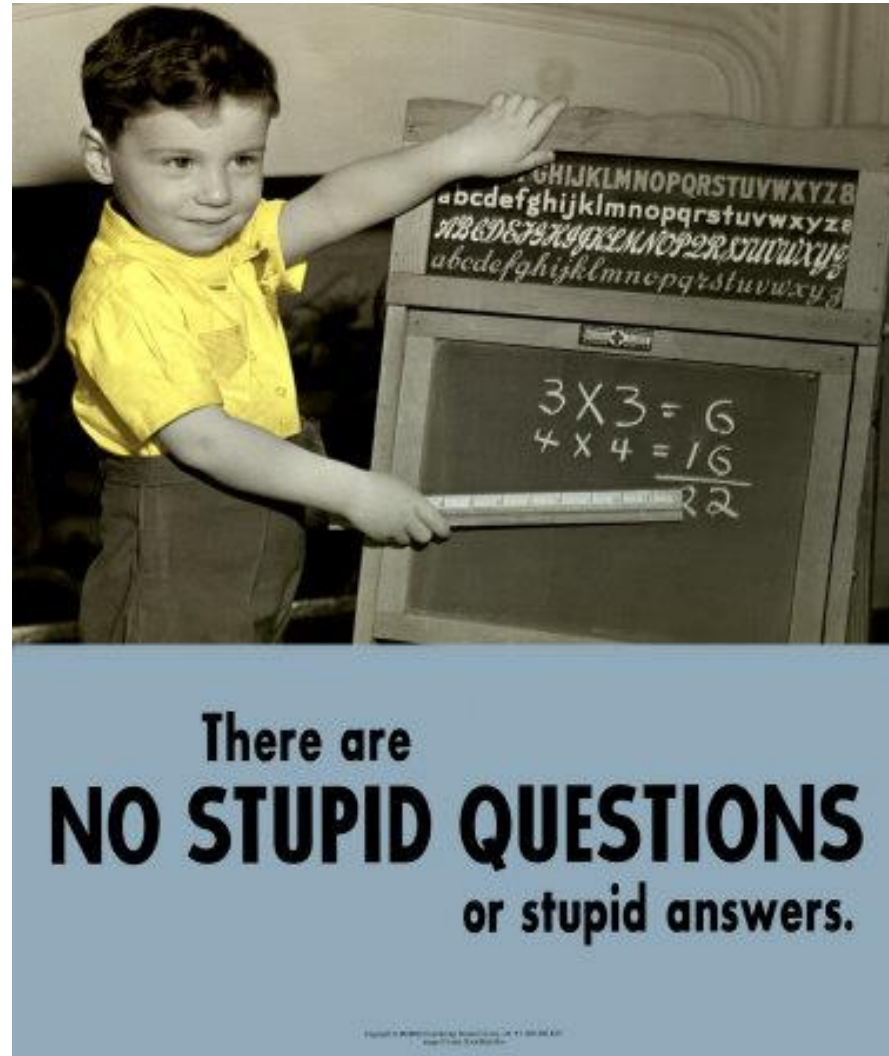
Asking Questions

- **Never** be afraid to ask:
 - ◆ In class or after class.
 - ◆ During office hours.
 - ◆ Make **Google** your friend (can't beat the availability and response time!...and avoid awkward moments...)



Asking Questions


- Remember, there is no such thing as a stupid question!



Anonymous Feedback

- Please feel free to anonymously submit your comments and suggestions about the course through:

◆ <https://bit.ly/2uyM2Oz>



Anonymous Question/Feedback Form

Anonymous Question/Feedback Form

* Required

Please Specify the Course *

☐ CPSC-452

☐ CPSC-455

Feedback/Question: *

Your answer

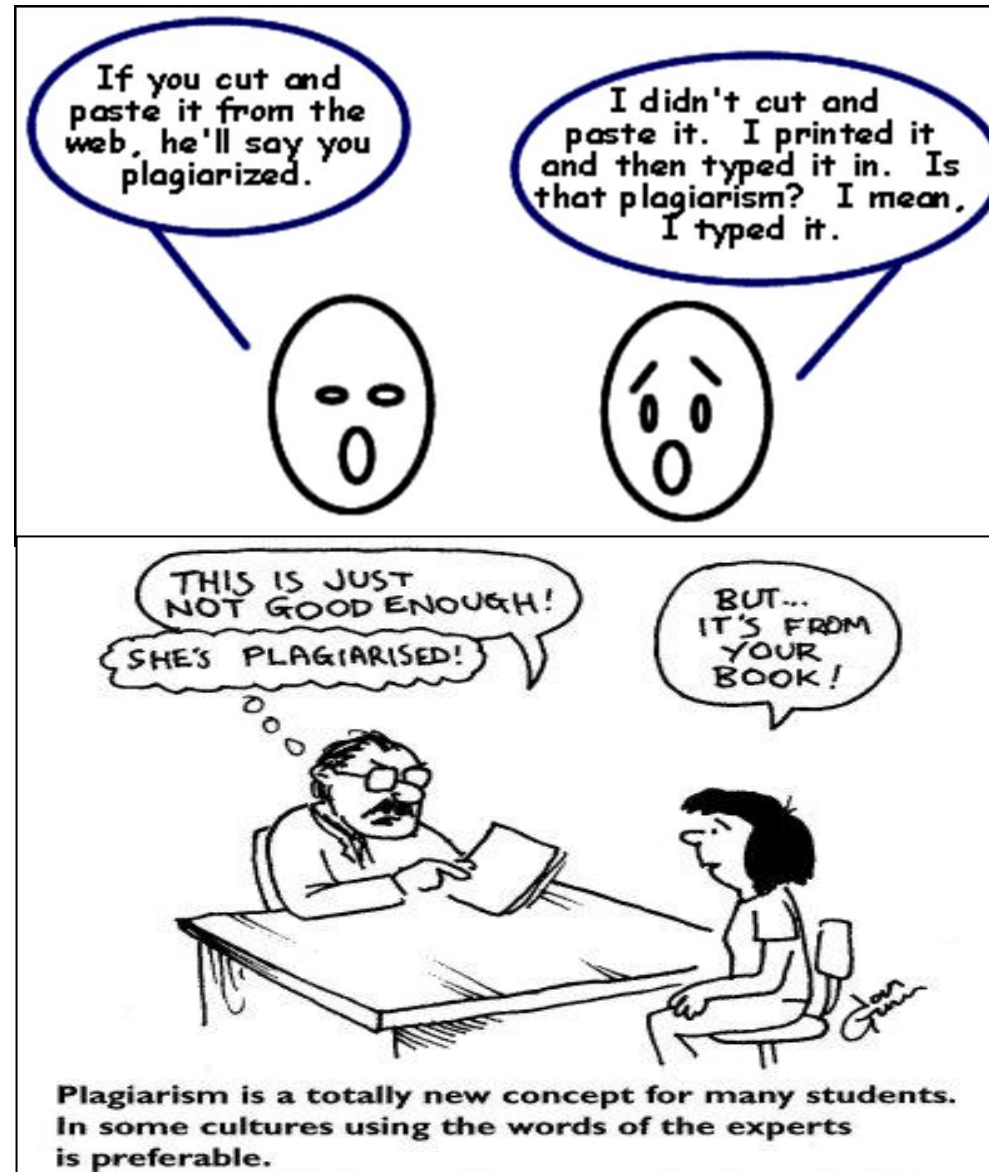
Submit

Class Cancellation Policy

- All class cancellations shall be announced by **email**.
- Instructor does not arrive within the first **15 minutes** of class = class is canceled.



Academic Honesty



Academic Honesty



- Incidents of cheating shall be treated with **utmost seriousness**.
- You may **discuss** the problems with other students, however, you must write **your own solutions**.
- Discussing solutions to the problem is **NOT acceptable**.
- Copying an assignment from another student or allowing another student to copy your work may lead to an automatic **F for this course**.
- If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please **consult the instructor before you collaborate**.
- **Moss** shall be used to detect plagiarism in programming assignments.

Emergency Policy

- Please familiarize yourself with the actions to take in case of an emergency.
- The information can be found at <http://prepare.fullerton.edu/>

Disabled Student Services

- Information for students with disabilities can be found at:
<http://www.fullerton.edu/DSS/>

Course Syllabus

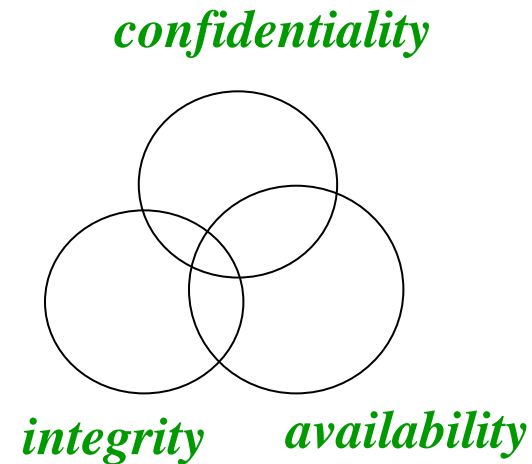
- You are **required** to read the syllabus!
- A copy of the syllabus is available on Titanium.
- If something is not clear, **ask** the instructor.

Introduction to Computer Security

Stallings Chapter 1

What is Security

- Computer security rests on three basic components: **confidentiality**, **integrity**, and **availability**.



Confidentiality, Integrity and Availability

- **Confidentiality**: only authorized people or systems can access the data or resource
- **Integrity**: assurance that the information is authentic and complete
 - ◆ **Data integrity**: the assurance that data received is exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay)
 - ◆ **Origin integrity**: the source of data is trustworthy
 - ◆ **System Integrity**: the assurance that the system performs intended function without inadvertent or deliberate unauthorized manipulation of the system
- **Availability**: people have the ability to use the information or resource desired

The AIC Triad?

- Sometimes the CIA triad is referred to as the **AIC triad** to avoid confusion with the Central Intelligence Agency (which is also CIA)
- Each letter still has the **same meaning**

DAD: The opposite of CIA

• DAD triad is the opposite of CIA:

- ◆ Disclosure
- ◆ Alteration
- ◆ Destruction

Background

- Information Security requirements have changed in recent times.
- Traditionally provided by physical and administrative mechanisms.
 - ◆ **Physical**: e.g., the use of rugged filing cabinets with a combination lock for storing sensitive documents.
 - ◆ **Administrative**: e.g. personnel screening procedures used during the hiring process.
- The use of **computer**: requires automated tools to protect files and other stored information.
- The use of **networks**: requires measures to protect data during transmission.

Examples: Security Violation

- User **A** transmits a file, which contains sensitive information to user **B**. User **C**, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission
- A message is sent from a **customer** to a **stockbroker** with instructions for various transactions. Subsequently, the investments lose value and the customer **denies** sending the message

Aim of Course

- Consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information



OSI Security Architecture

OSI Security Architecture

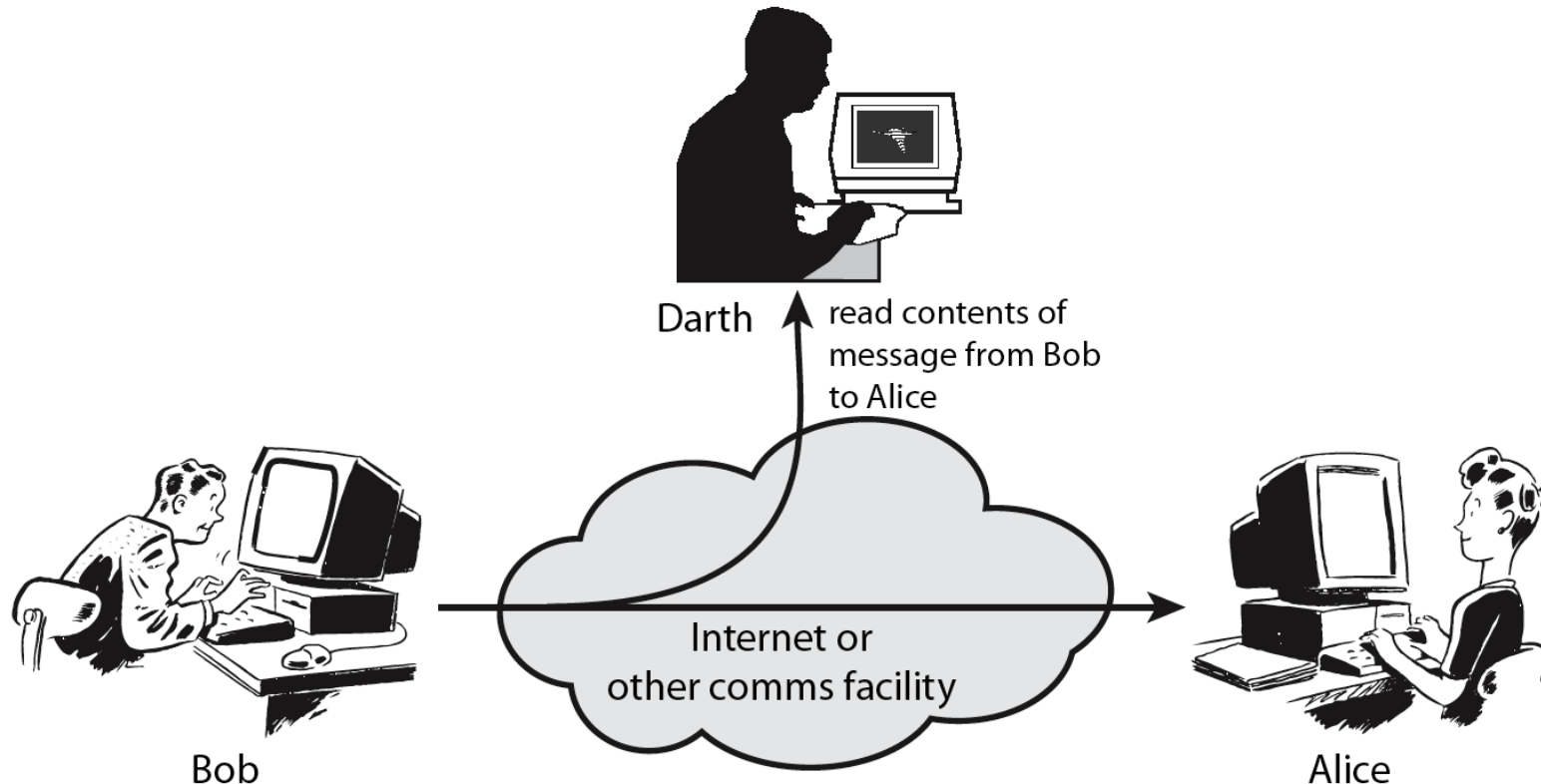
- **ITU-T X.800:** Security Architecture for OSI
 - ◆ **ITU-T:** International Telecommunication Union, Telecommunication standardization sector.
 - ◆ **OSI:** Open Systems Interconnection - an effort to standardize networking.
 - Started in 1982 by the International Organization for Standardization (**ISO**), along with the ITU-T
 - ◆ **Systematic way** of defining the requirements for security
- Considers 3 aspects of information security:
 - ◆ Security attacks
 - ◆ Security mechanisms
 - ◆ Security services

Security Attacks

- Any action that **compromises** the security of information owned by an organization
- **Information security**: how to prevent attacks and to detect attacks on information-based systems
- Can focus on generic types of attacks
 - ◆ Passive
 - ◆ Active

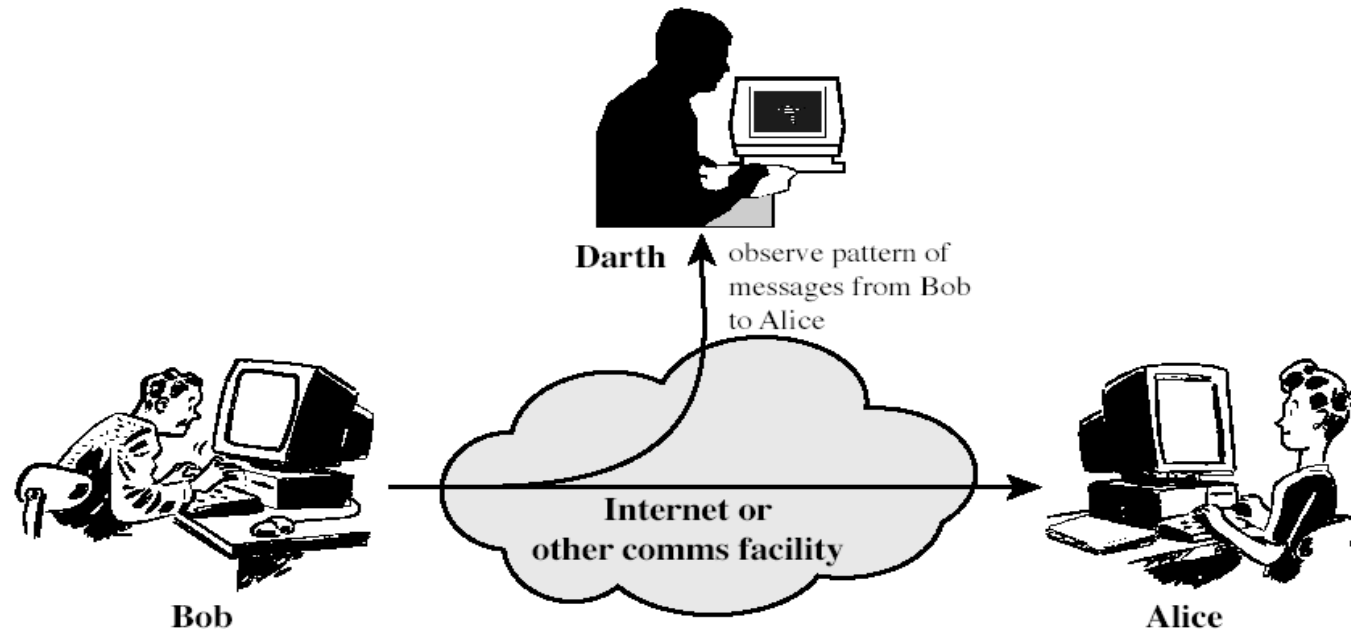
Passive Attacks

- Attempts to learn or make use of the information from the system but does not affect system resources
 - ◆ 1) **The release of mesg. contents:** eavesdropping on or monitoring of transmissions.



Passive Attacks

- 2) **Traffic analysis**: may not be able to extract the information (e.g., because it's encrypted), but might still be able to observe the pattern of these messages
 - ◆ Observe the **frequency** and **length** of messages being exchanged.
 - ◆ **Example**: timing attack on the SSH protocol used timing information to deduce information about passwords



Passive Attacks

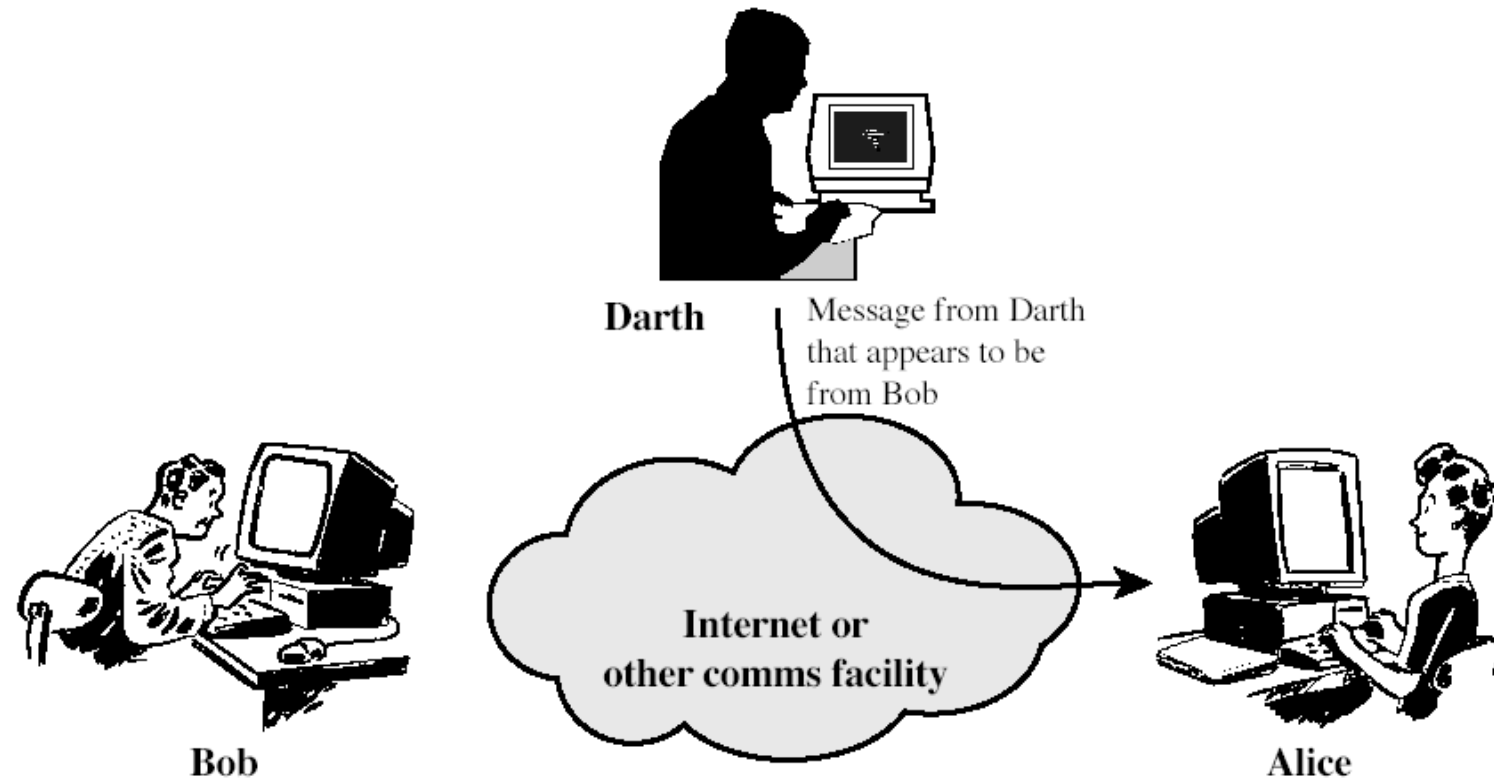
- How to cope with passive attacks?

Passive Attacks

- Very difficult to **detect** because they do not involve any alteration of the data
- It is feasible to **prevent** the success of these attacks
- The emphasis in dealing with passive attacks is on **prevention** rather than **detection**

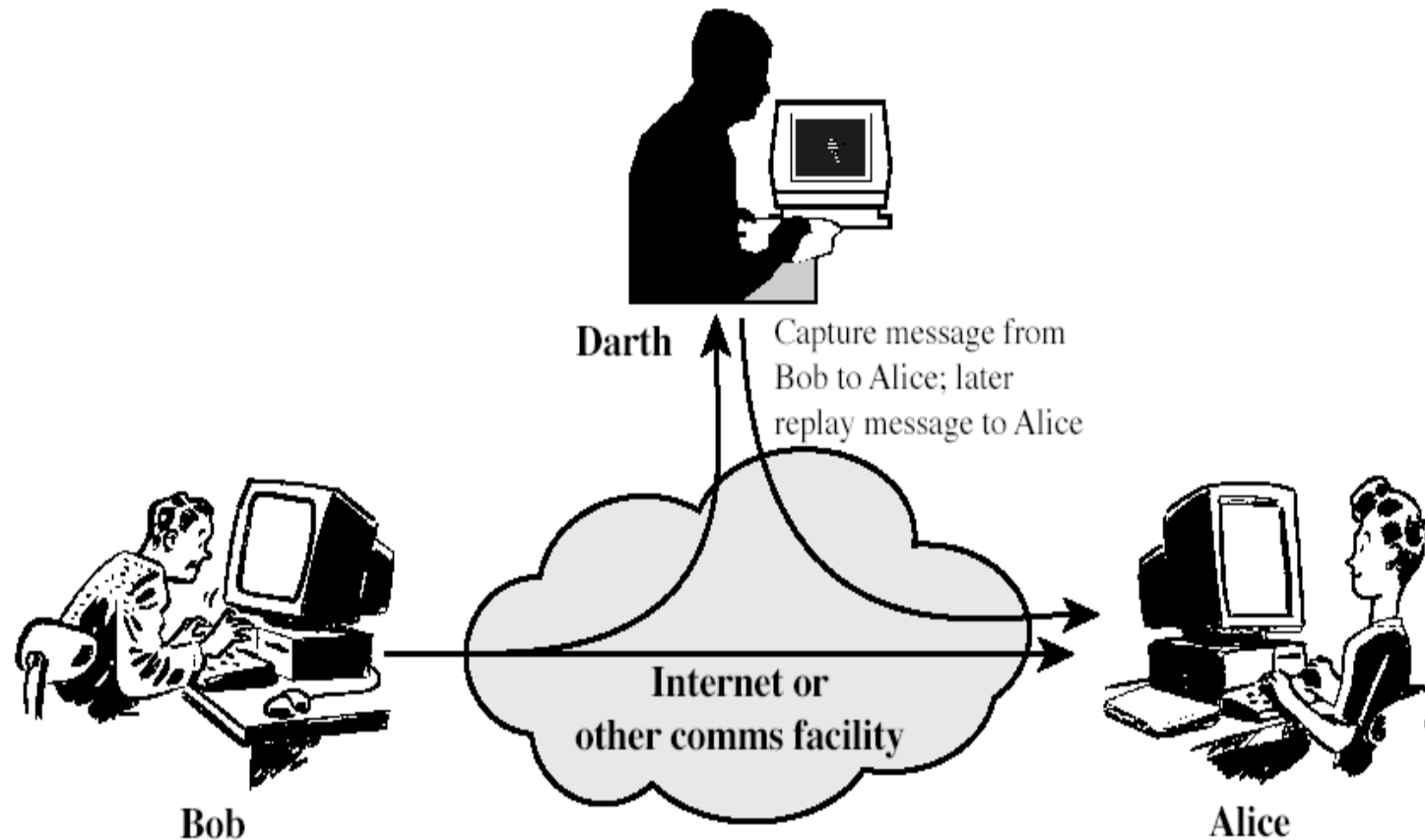
Active Attacks: Masquerade

- Attempts to alter system resources or affect their operation
 - ◆ **Masquerade:** one entity pretends to be a different entity



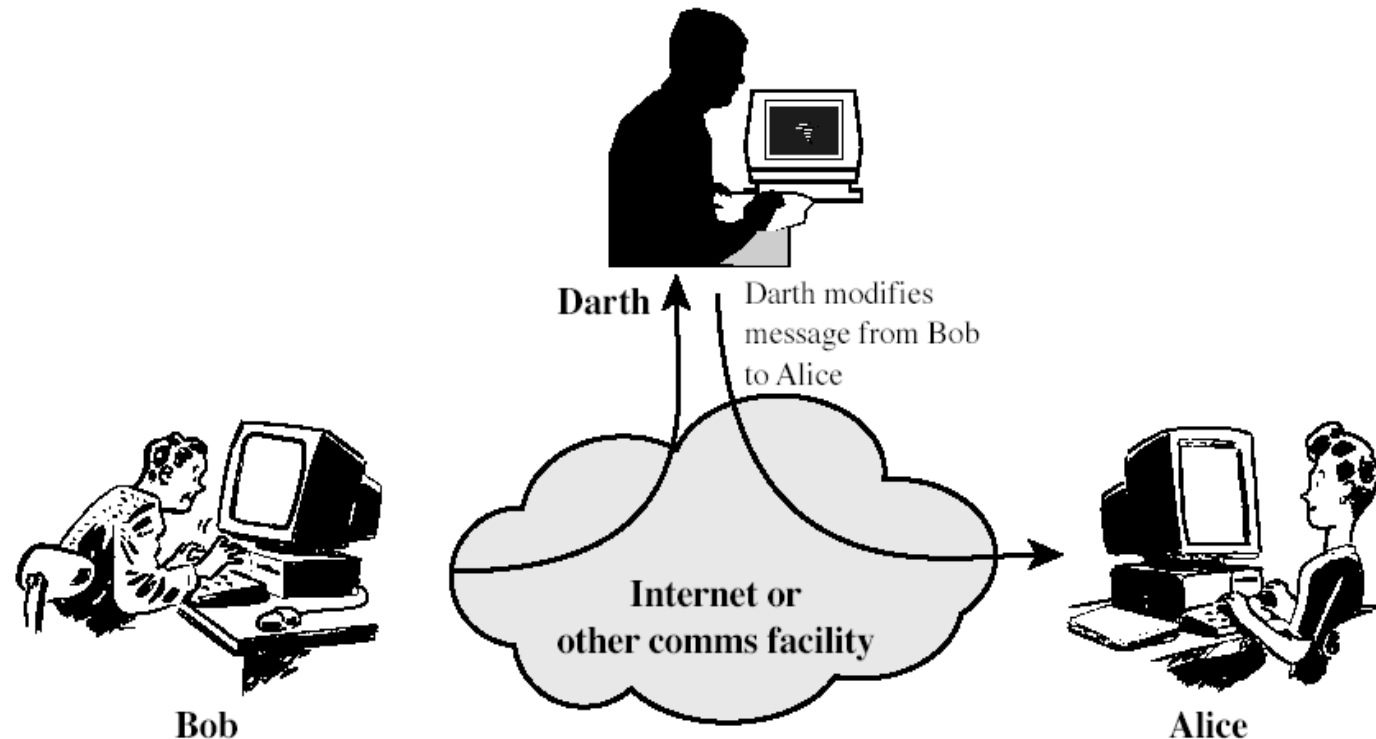
Active Attacks: Replay

- **Replay:** capture the data unit and transmit to the receiver later to produce an unauthorized effect.



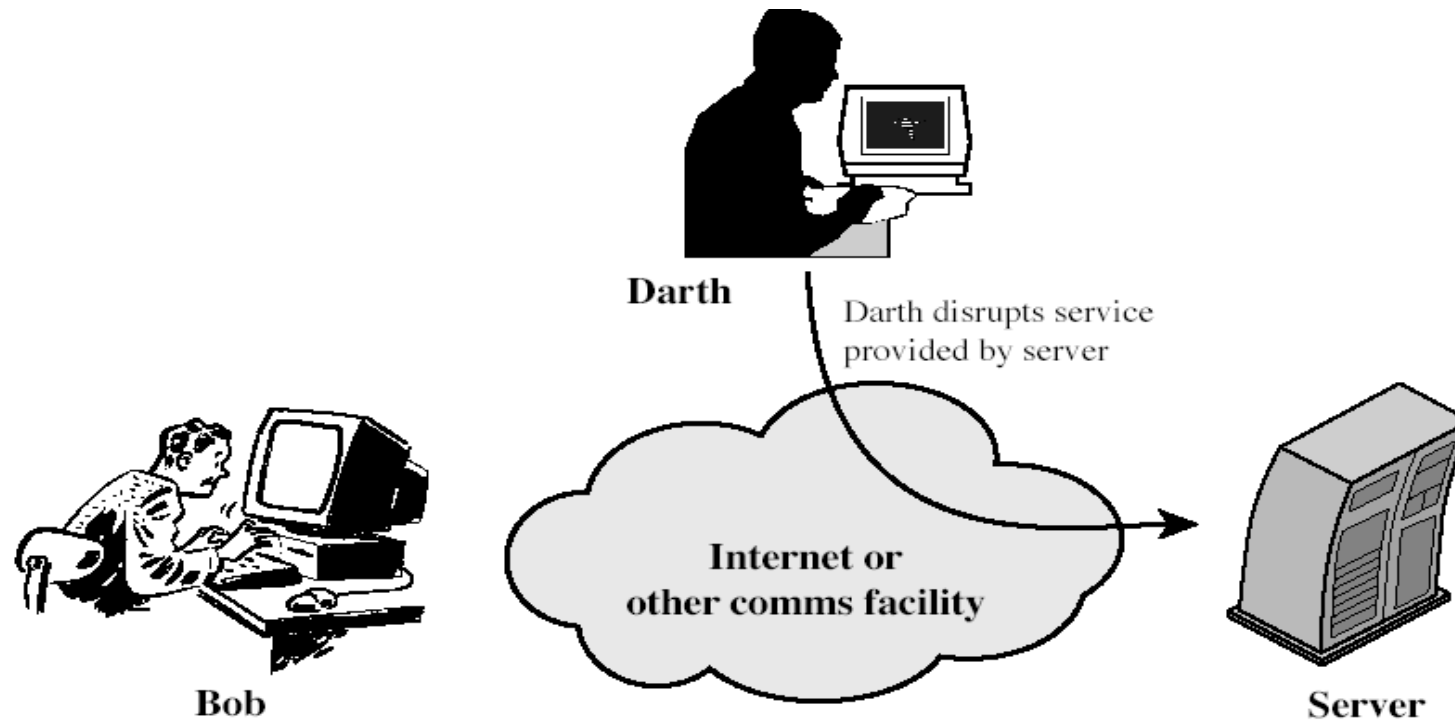
Active Attacks: Modification of Msg.

- **Modification of messages:** some portion of a legitimate message is altered, or messages are delayed or reordered
 - ♦ E.g. Allow a to read confidential file f1 → allow b to read confidential file f2



Active Attacks: DOS

- **Denial of service:** prevents or inhibits the normal use or management of communications facilities
 - ◆ E.g., An entity may suppress all messages directed to a particular destination
 - ◆ E.g., disruption of an entire network by overloading it with messages so as to degrade performance



Security Services

- Provided by a system to give a specific kind of protection to system resources
- Intended to counter security attacks
- Using one or more security mechanisms
- X.800 divides these services into 5 categories and 14 specific services.

Security Services (X.800)

- **Authentication**: assurance that the communicating entity is the one claimed
- **Access control**: prevention of the unauthorized use of a resource
 - ◆ Controls who can have access to a resource

Security Services (X.800)

- **Data Confidentiality:** protection of data from unauthorized disclosure
 - ◆ Protection of transmitted data from passive attacks
 - ◆ **Broader service:** protects all user data transmitted between two users over a period of time (e.g., TCP connection)
 - ◆ **Narrower service:** protection of a single message or specific fields within a message

Security Services (X.800)

- **Data Integrity:** assurance that data received is as sent by an authorized entity
 - ◆ Integrity can apply to a stream of messages, a single message, or selected fields within a message
 - ◆ Most useful: **total stream protection**
 - **Connection-oriented integrity service:** assures that messages are received as sent with no duplication, insertion, modification and denial of service

Security Services (X.800)

- **Nonrepudiation:** protection against denial by one of the parties in a communication
 - ◆ Proof that the message was sent by the specified party
 - ◆ Proof that the message was received by the specified party

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

Security Mechanisms (X.800)

● Specific security mechanisms:

- ◆ **Encipherment:** the use of mathematical algorithms to transform data into a form that is not readily intelligible
- ◆ **Digital signatures:** data appended to a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery
- ◆ **Access control:** a variety of mechanism that enforces access rights to resources
- ◆ **Data integrity:** a variety of mechanisms used to assure the integrity of a data unit or stream of data units

Security Mechanisms (X.800)

• Specific security mechanisms:

- ◆ **Authentication exchange:** a mechanism intended to ensure the identity of an entity by means of information exchange
- ◆ **Traffic padding:** the insertion of bits into gaps in a data stream to frustrate traffic analysis
 - Make it difficult for an attacker to distinguish between true data flow and noise
 - Make it difficult to deduce the amount of traffic

Relationship Between Security Services and Mechanisms

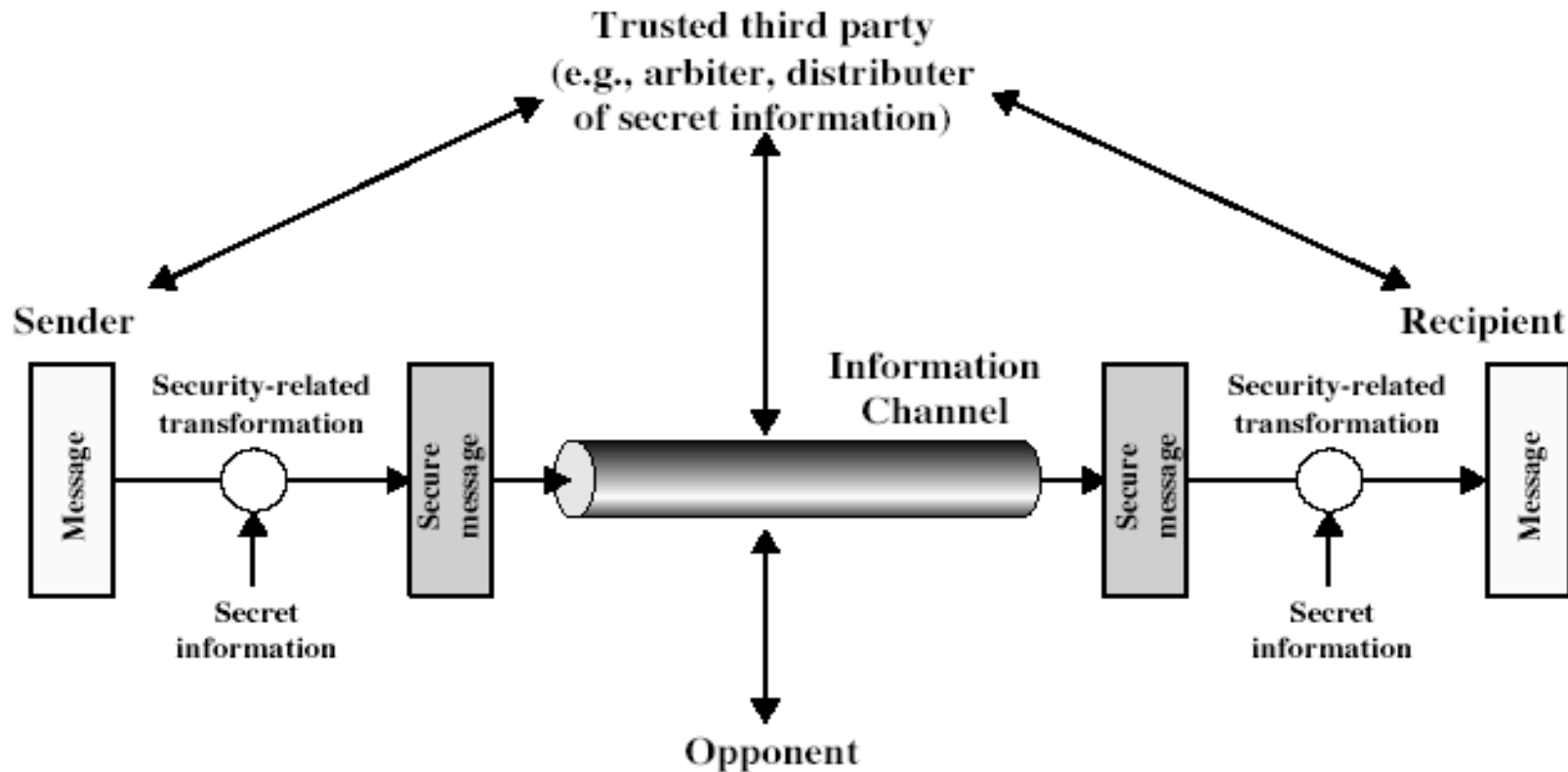
Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality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

How Cryptography Relates to Network Security

- Roadmap:
 - ◆ A model for network security
 - ◆ Introduction to Network

Model for Network Security

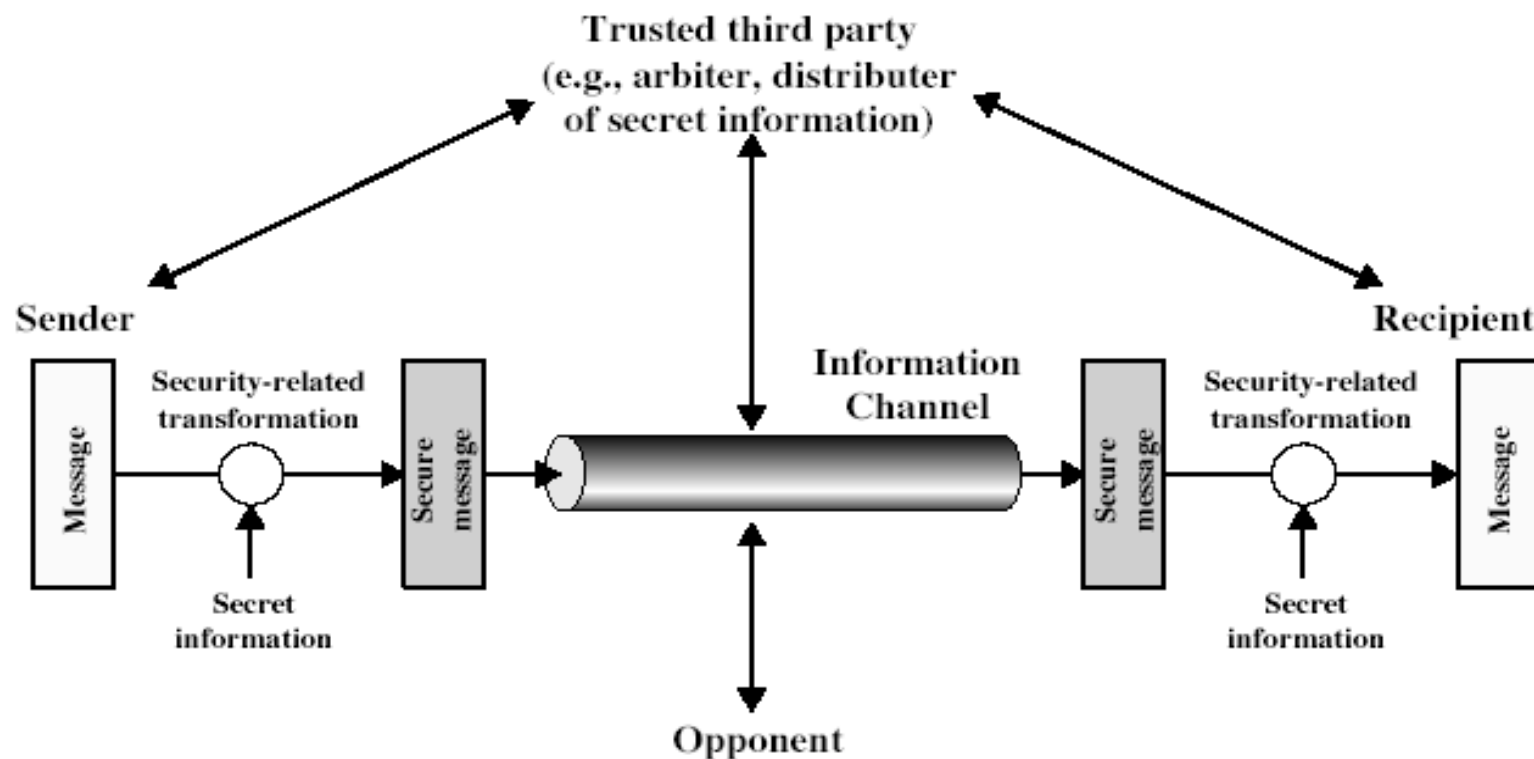
- A logical information channel is established by defining a route through the Internet from source to destination and by the use of communication protocols by the two principals



Model for Network Security

• Trusted third party

- ❖ Responsible for distributing the secret information to the two principals
- ❖ Arbitrate disputes between the two principals concerning the authenticity of a message transmission

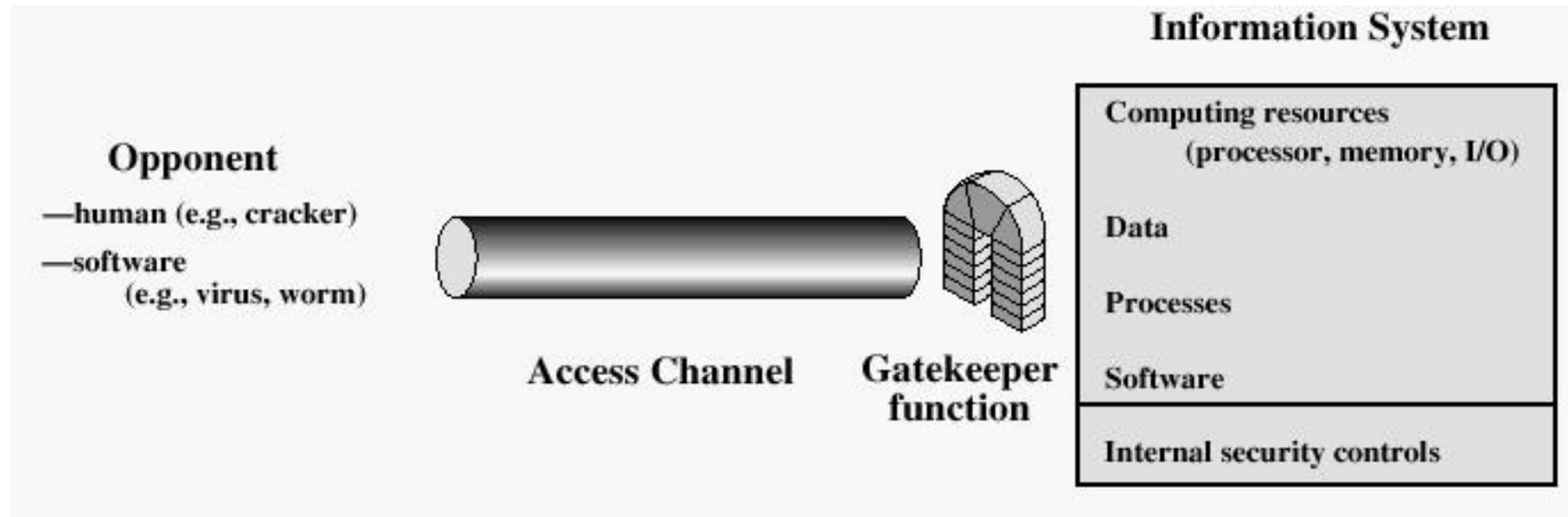


Model for Network Security

- 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

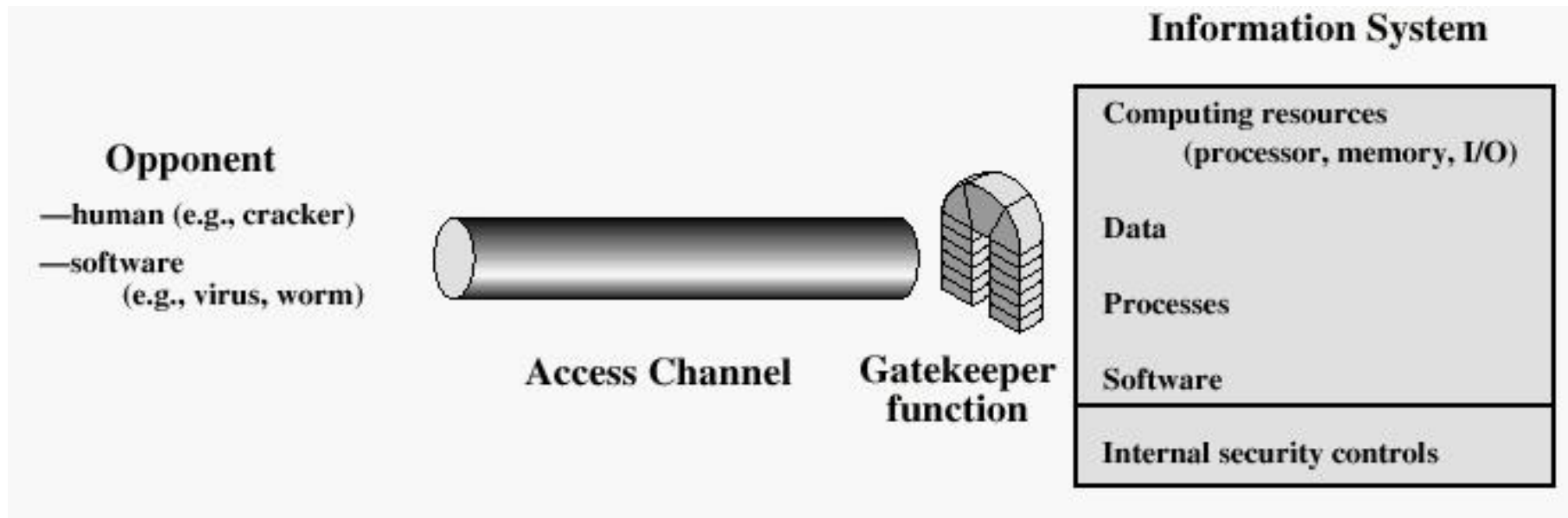
Model for Network Access Security

- Concerned with controlled access to information or resources on a computer system, in the presence of possible opponents
- **Hackers:** attempt to penetrate systems that can be accessed over a network



Model for Network Access Security

- **Virus and worms:** software attacks. Such attacks can be introduced into a system by means of a disk or be inserted into a system across a network



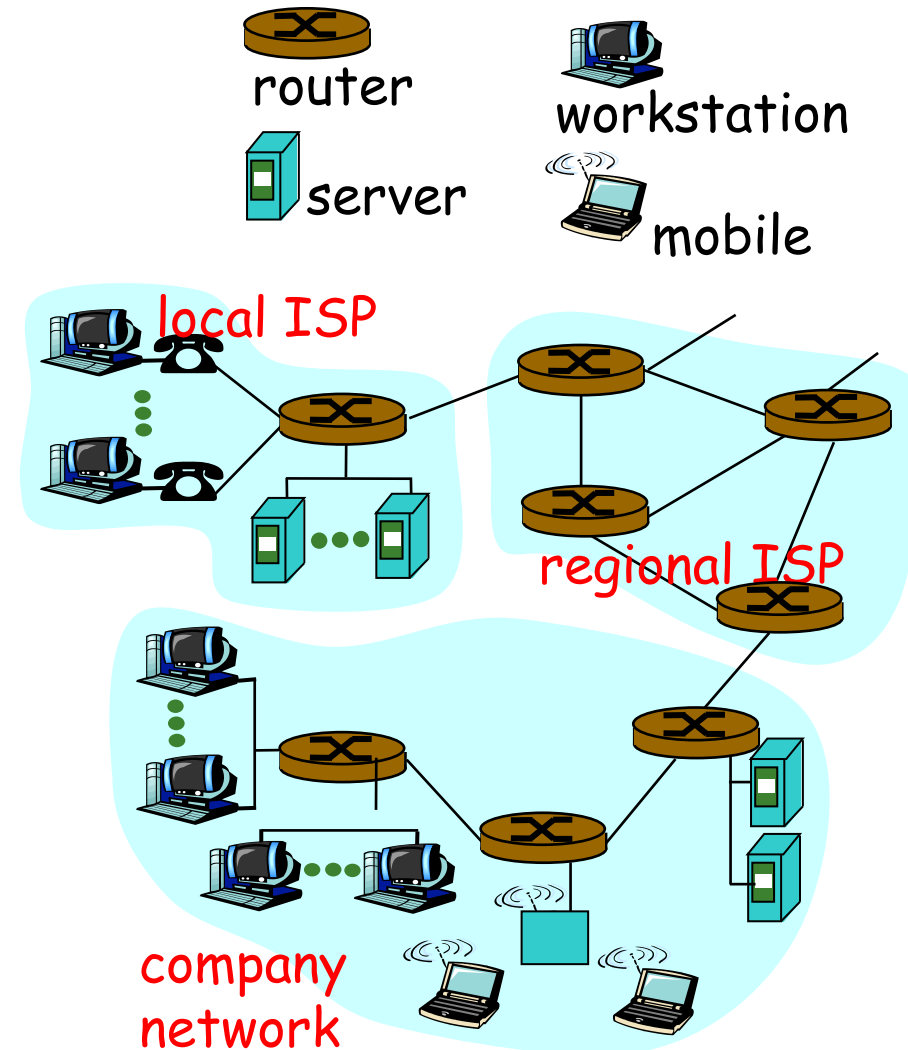
Model for Network Access Security

- Security mechanisms needed to cope with unwanted access.
 - ❖ Gatekeeper function:
 - Password-based login procedures designed to deny access to all but authorized users
 - Screening logic designed to detect and reject worms, viruses, and other similar attacks.
 - ❖ Internal controls
 - Monitor activity and analyse stored information in an attempt to detect intruders.

What's the Internet

What's the Internet

- A network that interconnects millions of computing devices (end systems) throughout the world
- End systems access internet through **Internet Service Providers (ISPs)**, companies that provide access to the Internet
 - ◆ AT&T, Sprint, 56kbps dial-up modern access, cable modem, DSL, etc.



What's a protocol?...

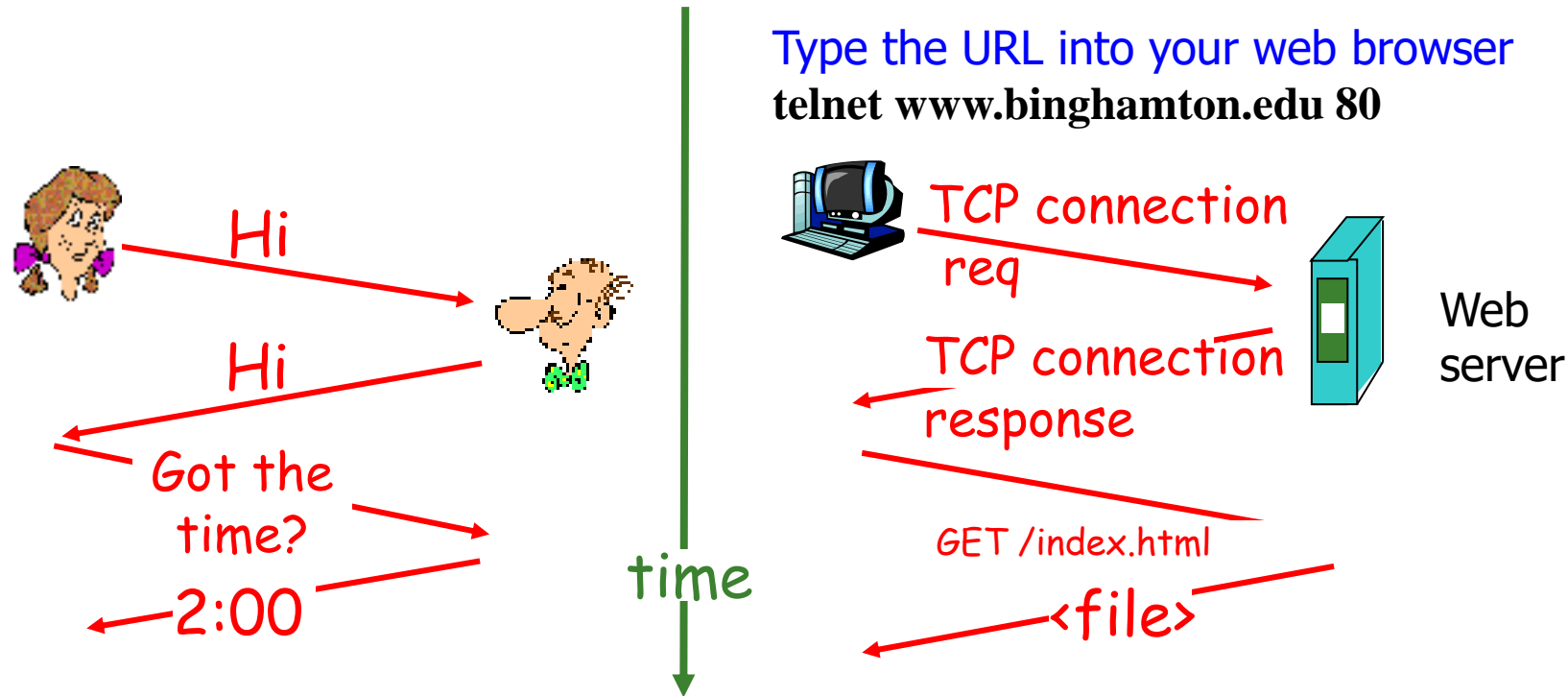
- All communication activity in Internet governed by protocols

What's a protocol?...

- All communication activity on the Internet governed by protocols
 - ◆ E.g. Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP)
- A network protocol defines a **language** of rules and conventions for communication between network devices.
- Protocols define **format**, **order of messages sent and received** among network entities, and **actions taken** on message transmission

What's a protocol?

A human protocol and a computer network protocol:



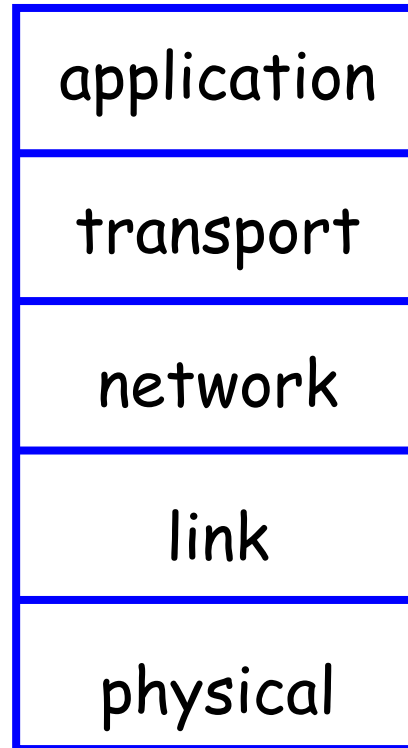
A network protocol is similar to a human protocol except that the entities sending and receiving msgs are hardware/software components of some device.

Protocol Layers

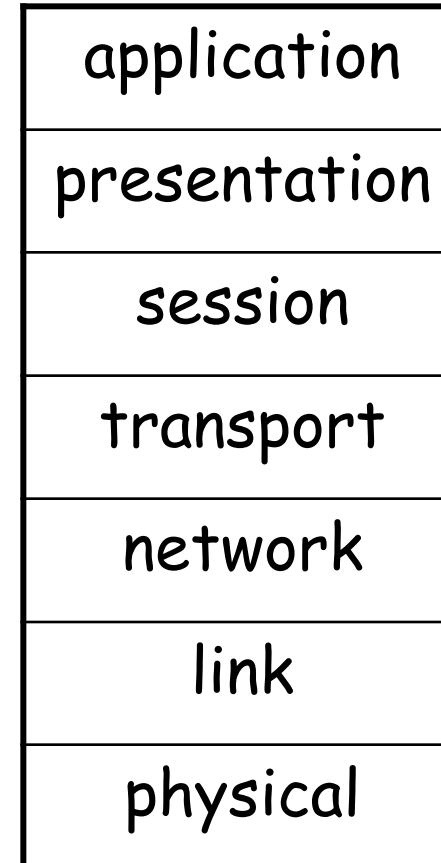
- Dealing with complex systems:
 - ◆ Provide a structural way to discuss system components.
 - ◆ Modularization eases maintenance, updating of system
 - Change of implementation of layer's service transparent to rest of system

Protocol Layers (Cont.)

- TCP/IP model:
5 layers



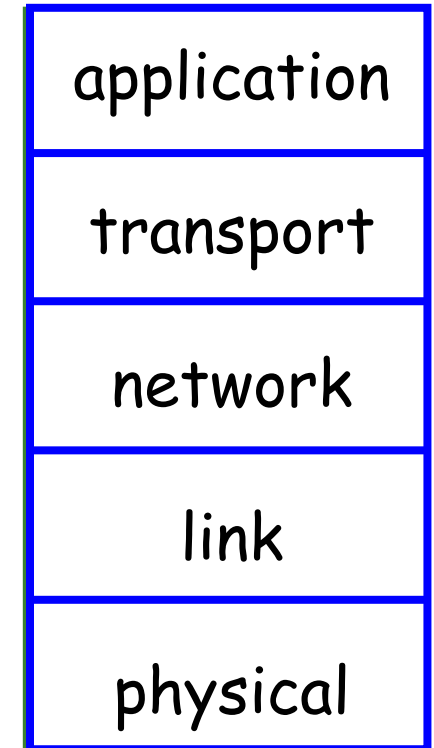
- OSI reference
model: 7 layers



Internet protocol stack (TCP/IP Model)

● Application

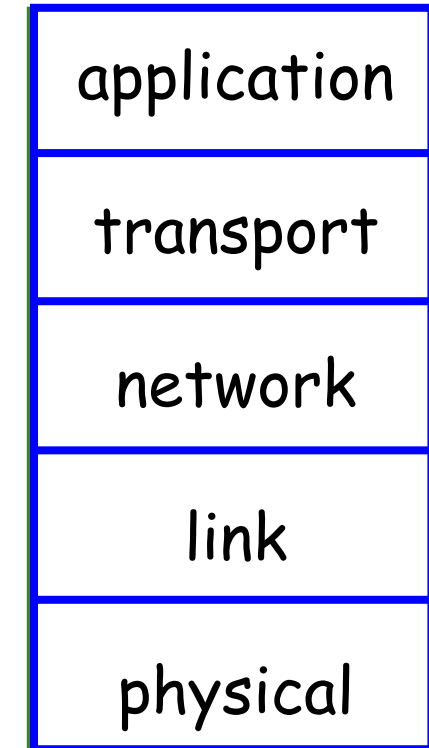
- ◆ Provides a means for the user to access information on the network through an application
- ◆ Supports network applications and application-layer protocols such as **FTP**, **HTTP**, **SMTP**
- ◆ Data sent over the network is passed into the application layer where it is encapsulated into the application layer protocol. The data is passed down into the transport layer.



Internet protocol stack (TCP/IP Model)

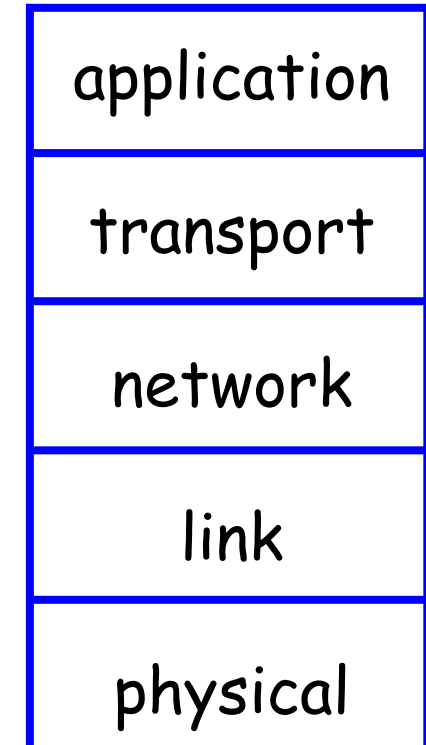
● Transport

- ◆ Provides transparent transfer of data between end users
- ◆ Controls the reliability of a given link through flow control, segmentation/ desegmentation, and error control
- ◆ Converts messages into **TCP** segments or User Datagram Protocol (**UDP**), etc.
 - TCP: a reliable connection-oriented protocol.
 - UDP: an unreliable, connectionless protocol, application: e.g., streaming media (audio, video, voice over IP etc).



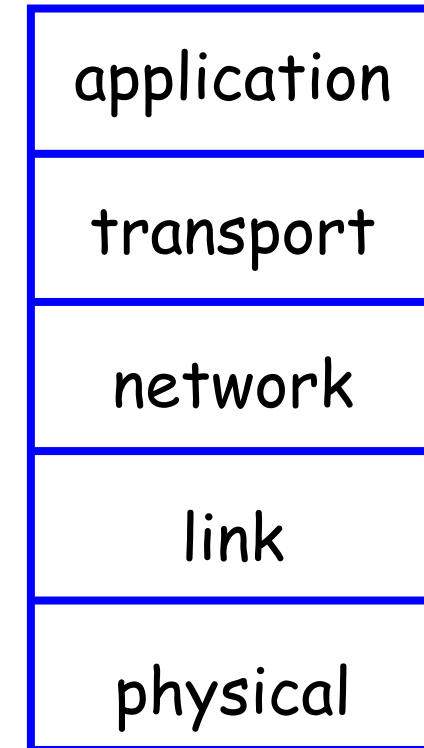
Internet protocol stack (TCP/IP Model)

- **Network:** routes datagrams from source to destination
 - ◆ Routers operate at this layer
 - ◆ IP, routing protocols
- **Link:** provides the functional and procedural means to transfer data between network entities
 - ◆ Bridges and link-layer switches operate.

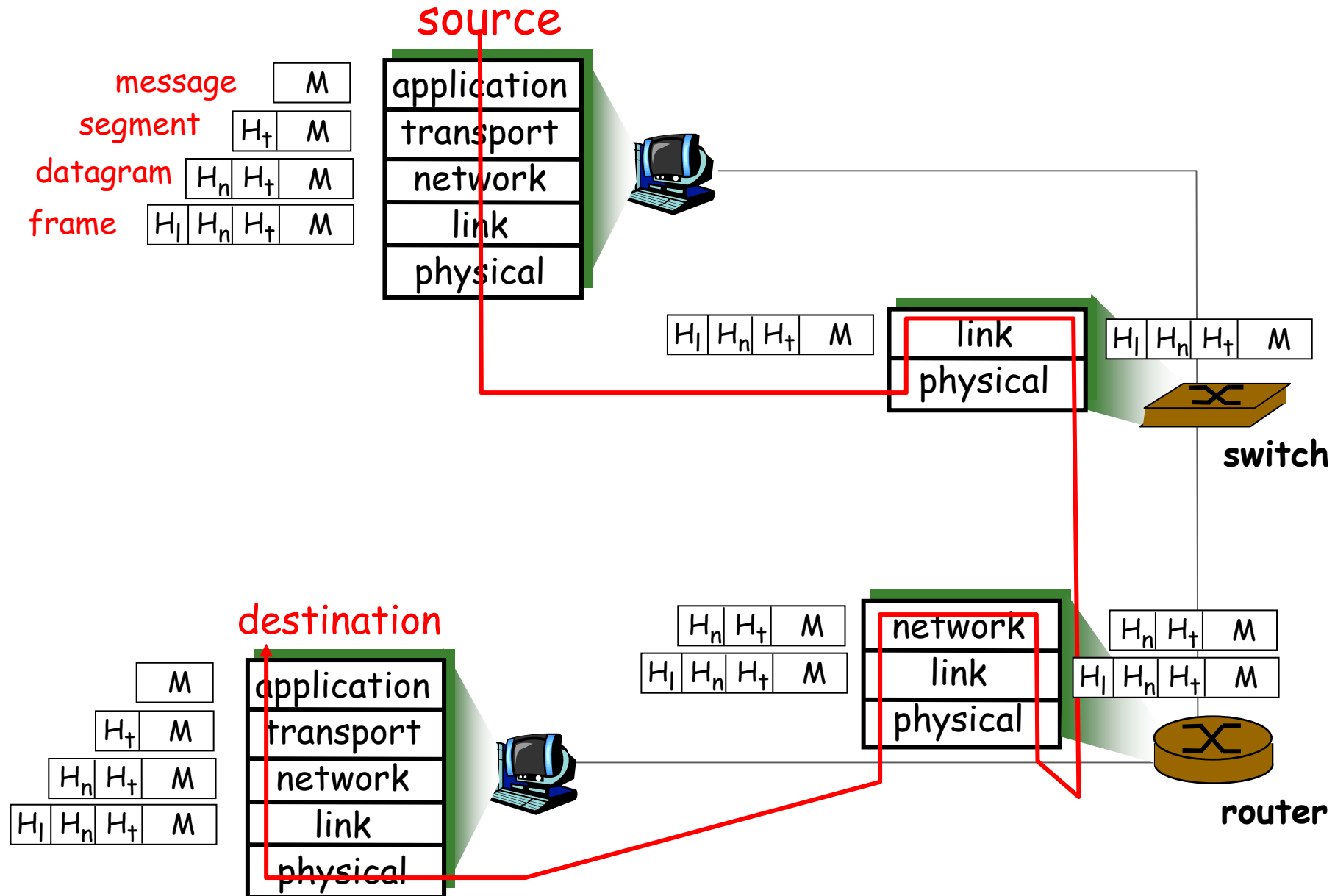


Internet protocol stack (TCP/IP Model)

- **Physical:** encodes and transmits raw data over network communications media (e.g., optical fiber)
 - ◆ Make sure that when one side sends a 1 bit, it is received by the other side as 1 bit.



Example



The Federal Information Processing Standard (FIPS) Publication 140-2

Government standards for cryptographic modules

FIPS 140 Series (1)

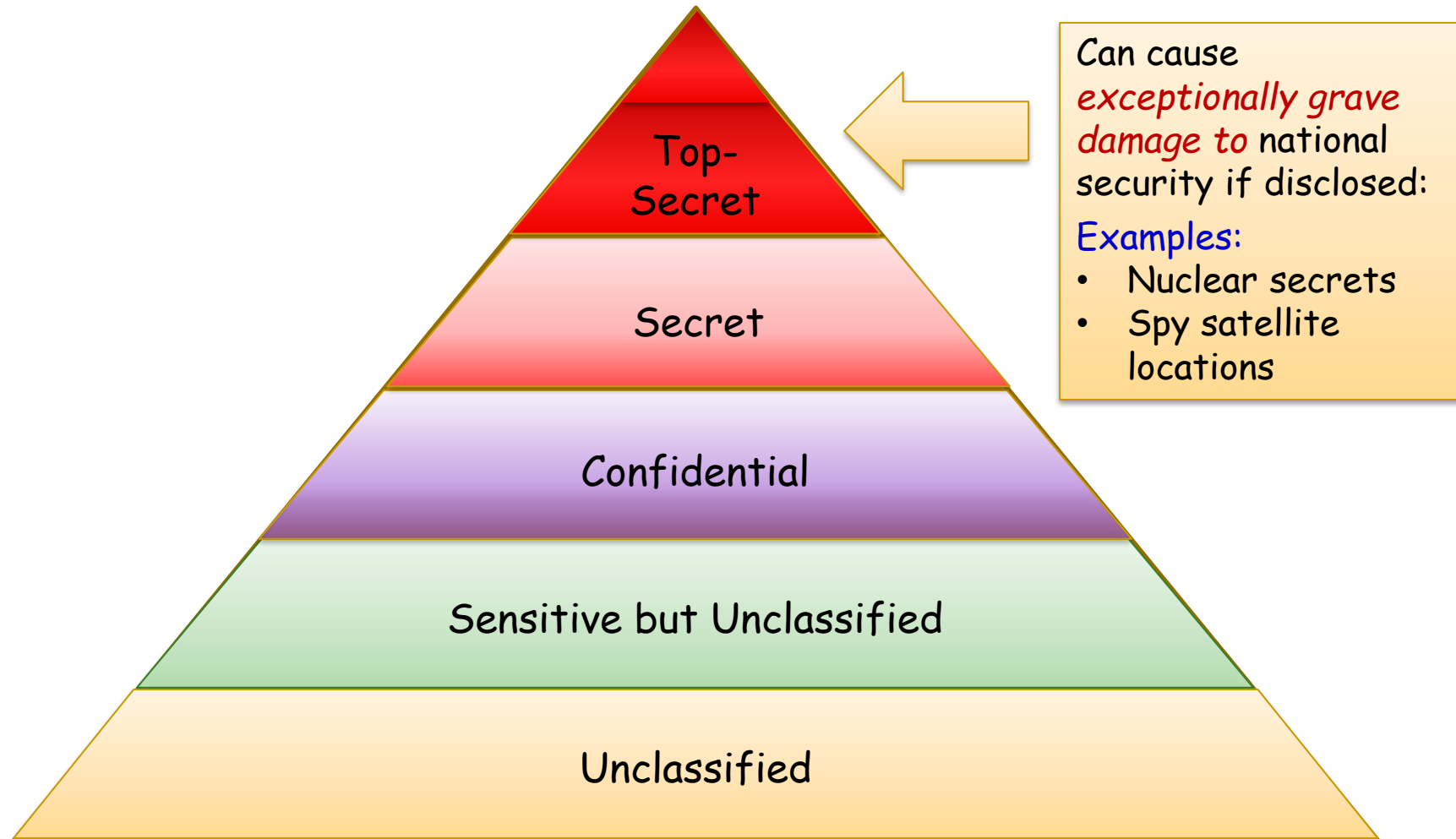
- **FIPS-140 Official title:** Security Requirements for Cryptographic Modules
- **U.S. Government standard** for securing cryptographic modules used in systems that process *sensitive but unclassified data*
 - ◆ *Maintained by the National Institute of Standards (NIST)*
- **Commercial vendors, government contractors, and in-house developers** designing cryptographic software and hardware for the government agencies can be required to comply with FIPS 140

FIPS 140 Series (3)

- What exactly is "sensitive but unclassified data"?

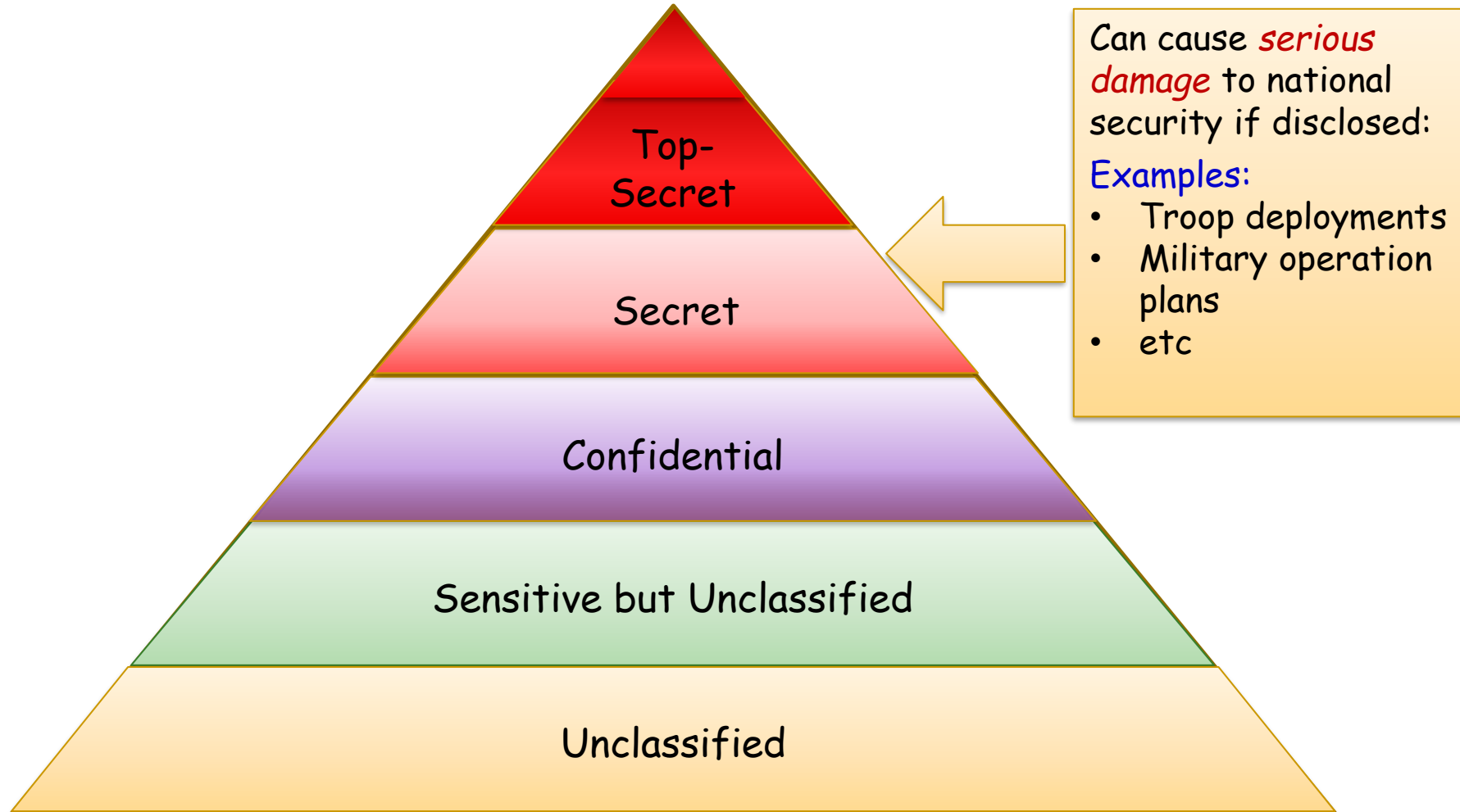
FIPS 140 Series (4)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



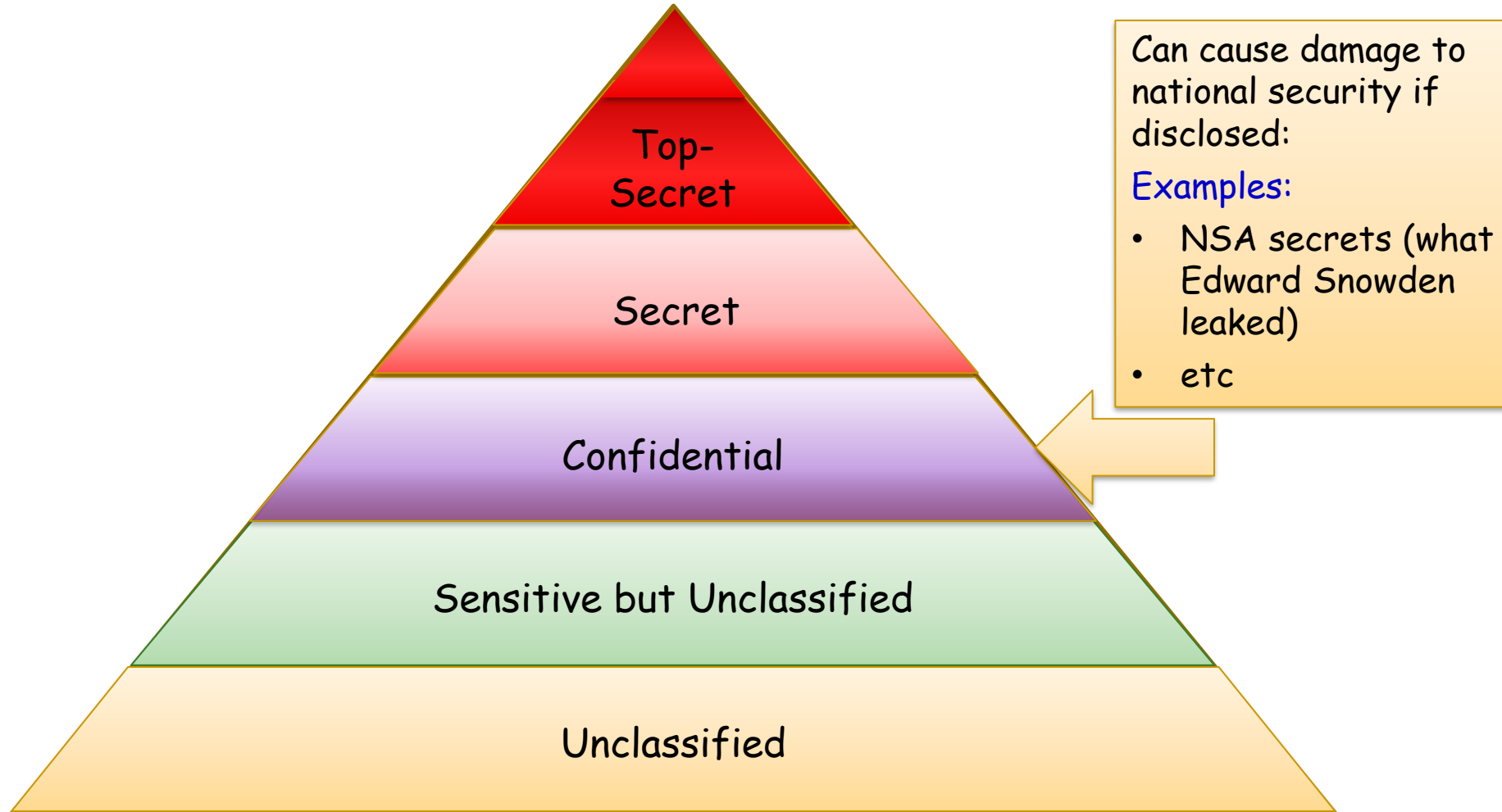
FIPS 140 Series (4)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



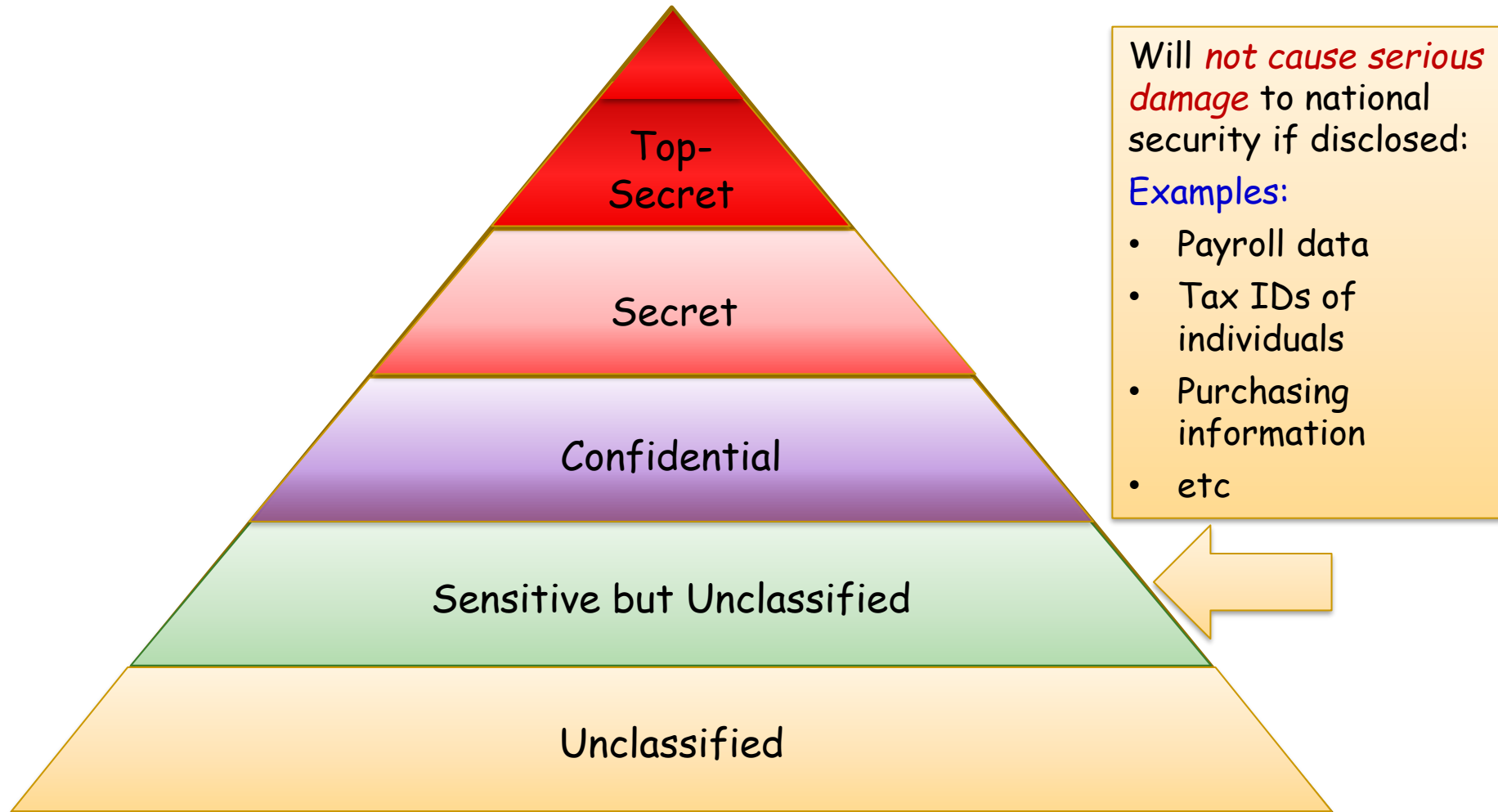
FIPS 140 Series (5)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



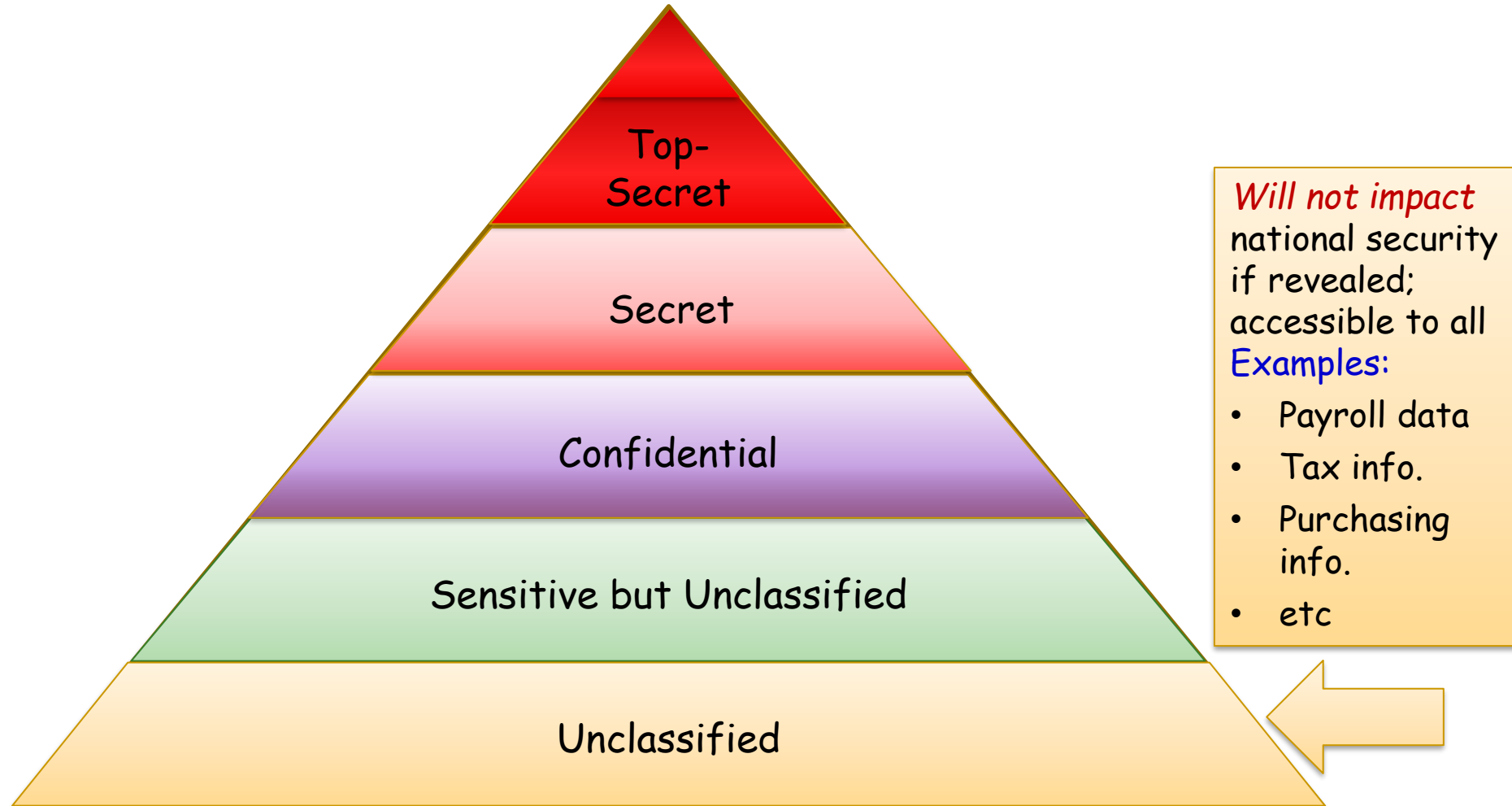
FIPS 140 Series (6)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



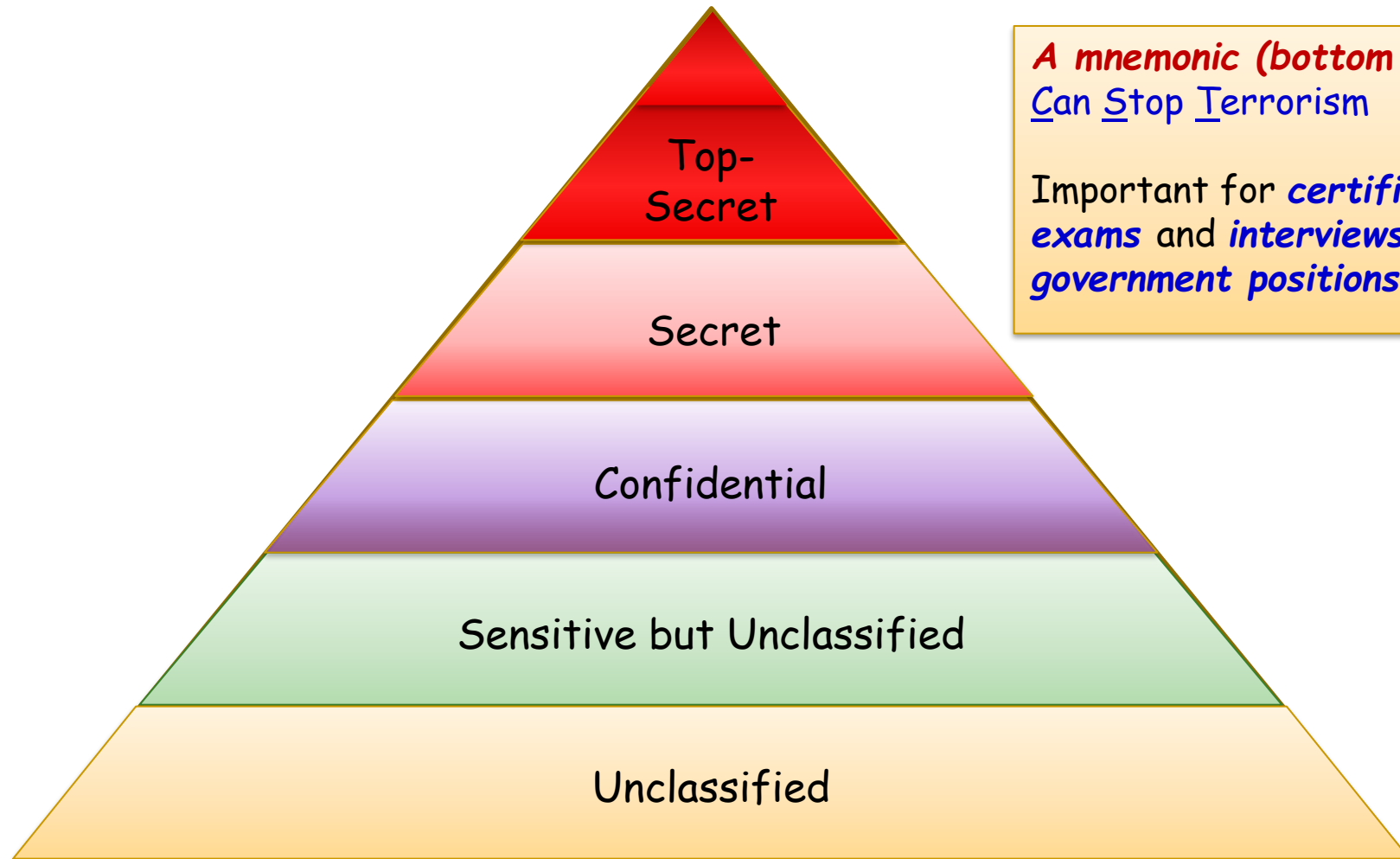
FIPS 140 Series (7)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



FIPS 140 Series (7)

- What exactly is "sensitive but unclassified data"?
- A U.S. Government for classifying data:



*A mnemonic (bottom up): US
Can Stop Terrorism*

Important for *certification exams* and *interviews for government positions*

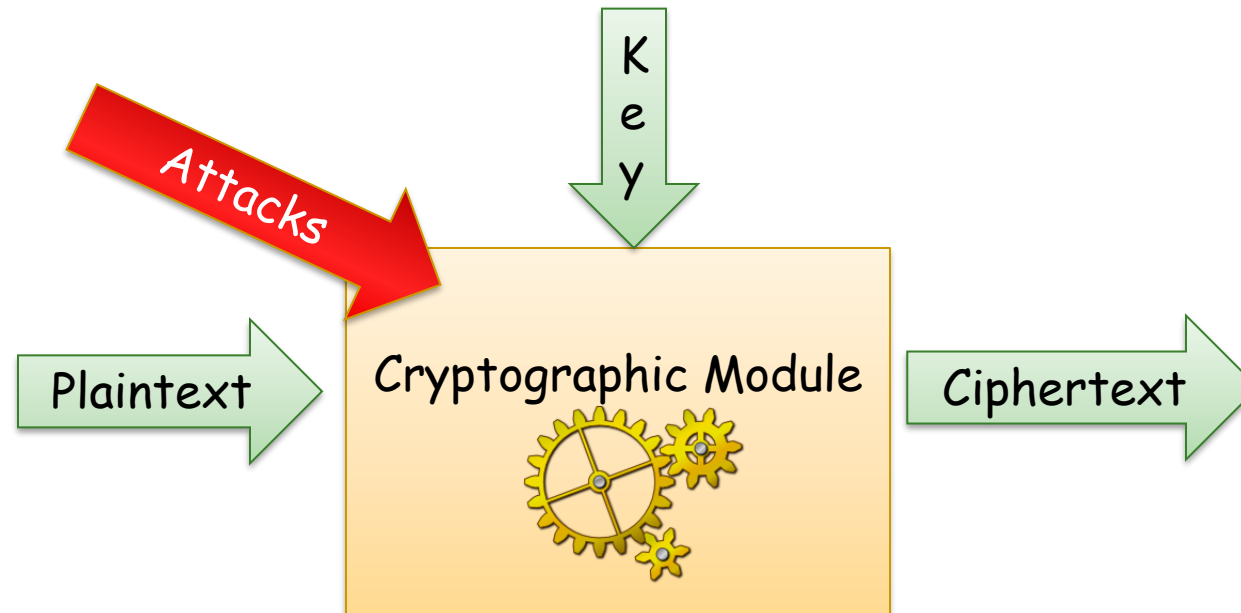
FIPS 140 Series (8)

● Versions of the standard

- ◆ 140-1: **previous** version (issued in 1994)
- ◆ 140-2: **current** version (issued 2001; will no longer be accepted after September 2026)
- ◆ 140-3: **current** version

FIPS 140 Series (9)

- **Basic idea:** cryptographic software and hardware components of a system (i.e., cryptographic modules) must be **secured against attacks**
 - ◆ Critical for protecting confidentiality and integrity of information processed by the module
 - ◆ Compliance with 140 series **does not guarantee that the module is secure**



FIPS 140 Series (10)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
 - ◆ 1. *Cryptographic module specification*: what must be documented
 - ◆ 2. *Cryptographic module ports and interfaces*: what information enters and exits the module and how it should be separated
 - ◆ 3. *Roles, services and authentication*: what users are allowed to perform what actions with the module and how these users are authenticated
 - ◆ 4. *Finite state model*: documentation describing what states of the module and how transitions between the states happen

FIPS 140 Series (11)

- Scope of 140 series: specifies module security requirements in the following 11 areas:

- ◆ 5. *Physical Security*:

- Whether module should be resistant to physical tampering; and
- Whether if physically tempered with, tempering should be easily detectable; and
- Whether the module should be robust to extreme environmental conditions

- ◆ 6. *Operational Environment*: the type of operating system utilized by the module and what operating systems can use the module

FIPS 140 Series (12)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
 - ◆ 7. *Cryptographic key management:*
 - *Cryptographic keys:* pieces of secret information necessary to encrypt/decrypt data
 - Specifies how the keys are *generated, stored, and destroyed*
 - ◆ 8. *Electromagnetic Interference (EMI)/Electromagnetic Compatibility (EMC):*
 - All electronics generate *electromagnetic fields* that can expose sensitive data and interfere with other electronics;
 - This area outlines *concerns and security requirements regarding module's EMI/EMC.*

FIPS 140 Series (13)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
 - ◆ 9. *Self-tests*: specifies how the module should test itself and when and how to act if a particular test fails (e.g., power-up tests, conditional tests, etc)
 - ◆ 10. *Design assurance*: documentation requirements showing that the module was well designed and implemented
 - ◆ 11. *Mitigation of attacks*: if the module is designed to mitigate a specific attack, then it must included in the documentation

FIPS 140 Series (14)

- FIPS 140-2 defines **four levels of security** for a module
- **Level 1 is least secure**
- **Level 4 is the most secure**

FIPS 140 Series (15)

• 140-2 Levels:

S
e
c
u
r
i
t
y

Level	Requirements
Level 1	<ul style="list-style-type: none">• All components must be <i>production grade</i>• Must not have <i>serious security issues</i>
Level 2	<ul style="list-style-type: none">• Adds a requirement that <i>tampering attempts must leave evidence</i>• Module <i>must implement authentication based on user roles</i>
Level 3	<ul style="list-style-type: none">• Adds a requirement that the module <i>must be tamper resistant</i>• Must be able to <i>authenticate users based on user identity</i>• Imposes additional requirements on <i>module interface security</i>
Level 4	<ul style="list-style-type: none">• Adds <i>stricter physical security</i> requirements• Requires resistance against attacks targeting the <i>device environment</i>

FIPS 140 Series (17)

- Example of FIPS 140-2 compliant device (Level 2):

audible LIMITED TIME ONLY SAVE \$50 ON YOUR 1ST YEAR OF MEMBERSHIP GET THE DEAL >

no results



CipherShield 256 bit AES USB-C
FIPS 140-2 Level 2 HIPAA USB 3.1
Gen 2 Hardware Encrypted Disk-
On-The-Go External Slim Portable
Hard Drive (2TB)
by BUSlink

List Price: \$209.99
Price: **\$169.99** & FREE Shipping. Details
& FREE Returns
You Save: \$40.00 (19%)

W. Best price **W.+**

Get \$50 off instantly: Pay \$119.99 upon approval for the Amazon Rewards Visa Card. No annual fee.
Free Amazon product support included

Source: www.amazon.com

FIPS 140 Series (18)

- Example of FIPS 140-2 compliant device (Level 3):



Click image to open expanded view

Source: www.amazon.com

SecureData 2TB SecureDrive KP
FIPS 140-2 Hard Drive with Pin
Authentication
by SECUREDATA

List Price: \$419.93

Price: **\$273.50** & FREE Shipping

You Save: **\$146.43 (35%)**

W. Get 1% back **W. +**

Get \$50 off instantly: Pay \$223.50 upon approval for the Amazon Rewards Visa Card. No annual fee.

Capacity: 2 TB

1 TB	2 TB	5 TB
\$229.00	\$273.50	\$499.00

- Fips 140-2 Level 3 validated: certificate #3297. Assembled in U. S. A.
- Unlock with a (7-15 digit pin) via on-board keypad. Usb 3. 0 (2. 0 compatible)/ bus powered.
- Admin/user, Read-Only, auto-lock modes. Bad USB protection. Brute force anti-hacking self Erase mechanism
- Preloaded with USB Antivirus (DriveSecurity by ClevX) with an ESET engine
- Plug-and-play software free operation, OS and platform independent - works w/Windows, Mac, Linux

References

- **TCP/IP model:** http://en.wikipedia.org/wiki/TCP/IP_model
- **ITU-T X.800:** <https://www.itu.int/rec/T-REC-X.800-199103-I>
- **FIPS-140:** <https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf>

Acknowledgement

- Some slides are borrowed from Dr. Ping Yang