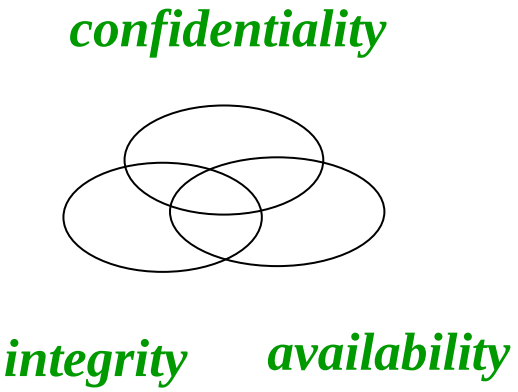
Introduction to Cryptography and Review of Computer Security

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

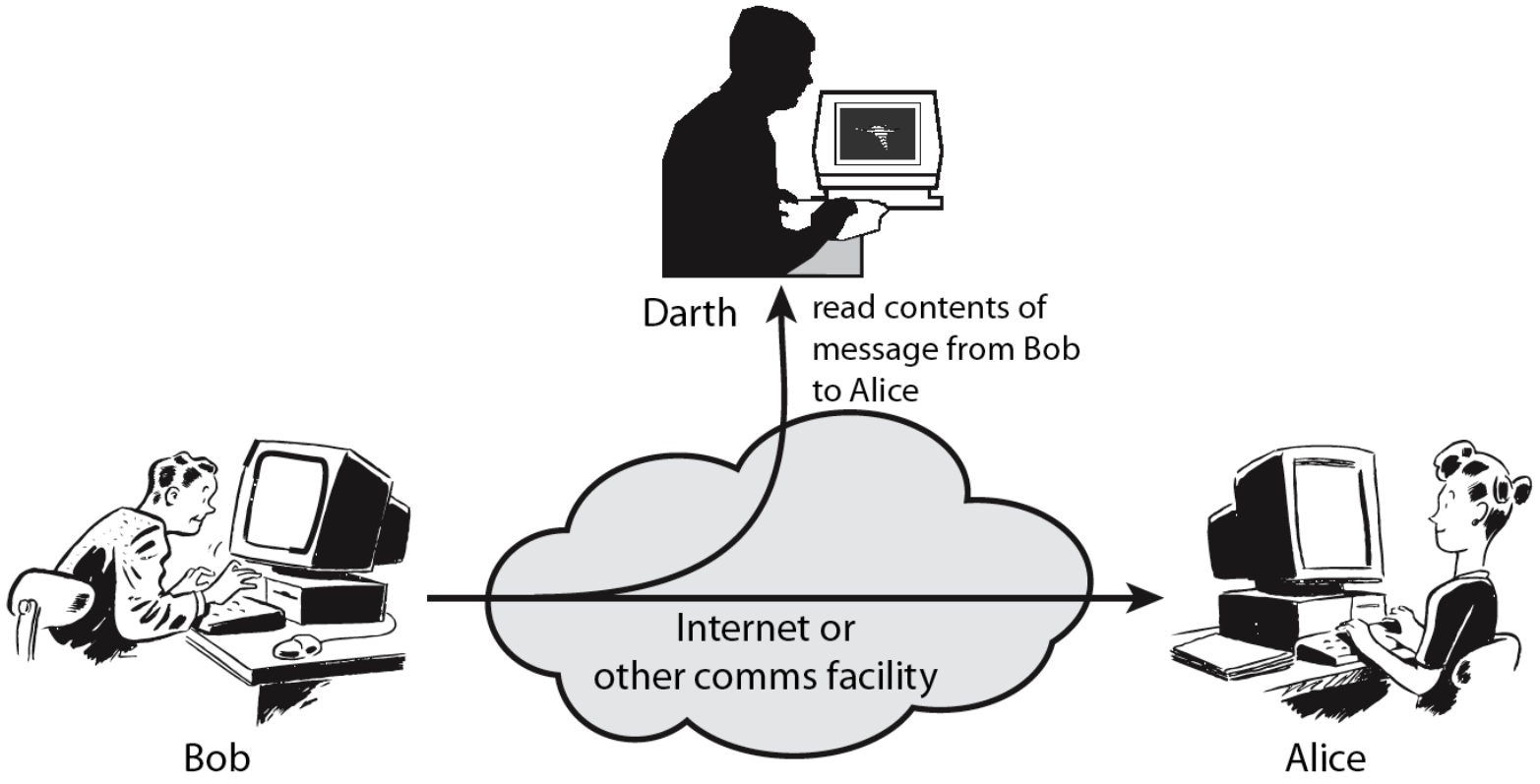
- ITU-T X.800: Security Architecture for OSI
  - ITU-T: International Telecommunication Union, Telecommunication standardization sector.
  - OSI: Open Systems Interconnection - an effort to standardize networking.
    - Started in 1982 by the International Organization for Standardization (ISO), along 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

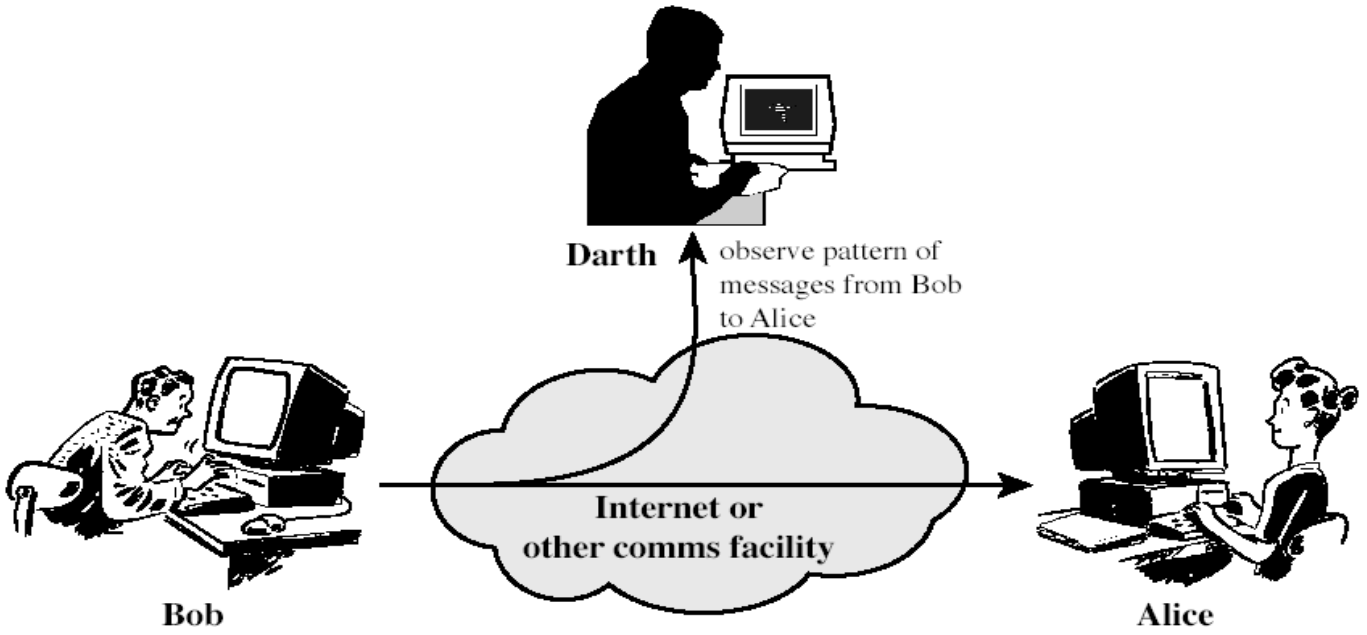
Passive Attacks

- 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 massages
  - 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

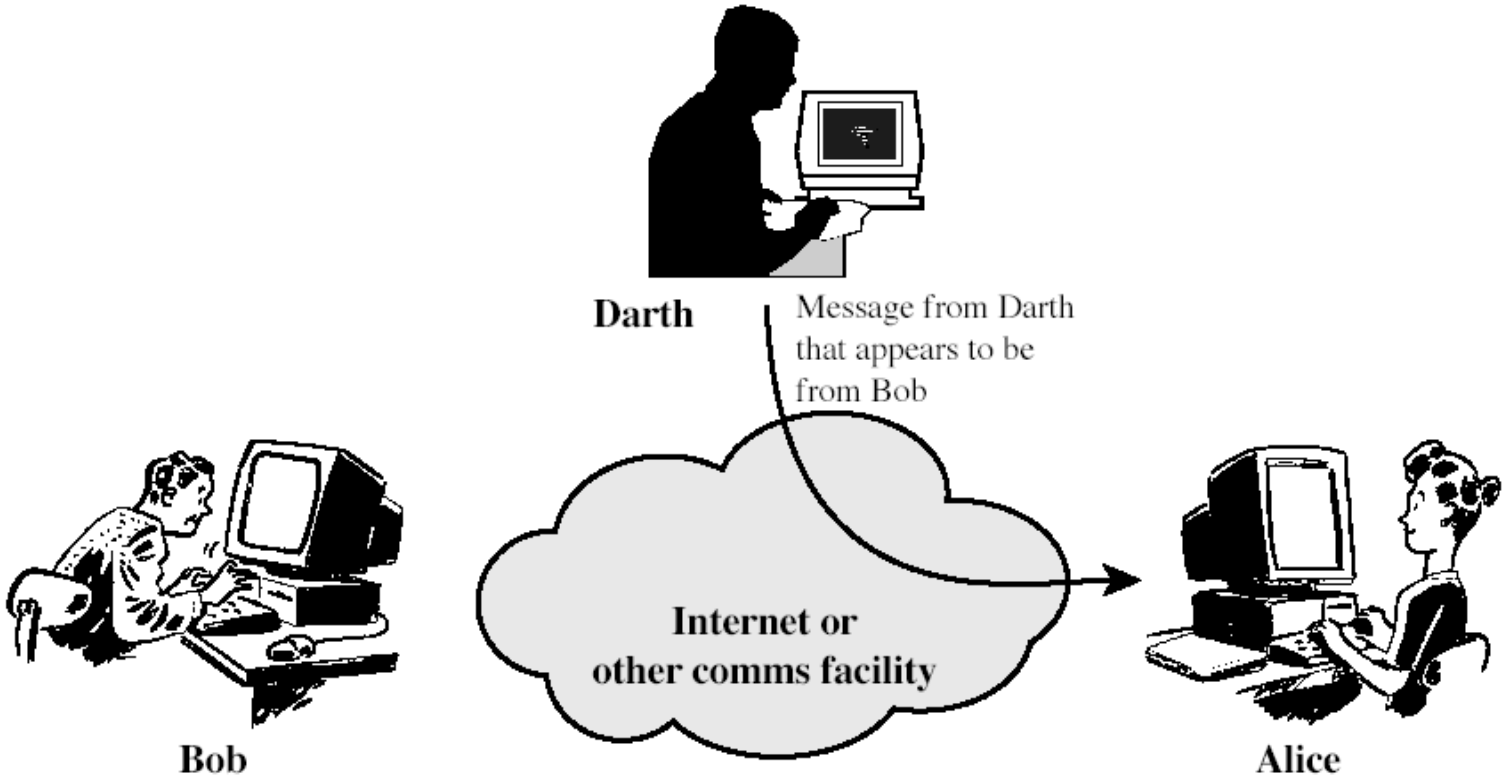
- How to cope with passive attacks?

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

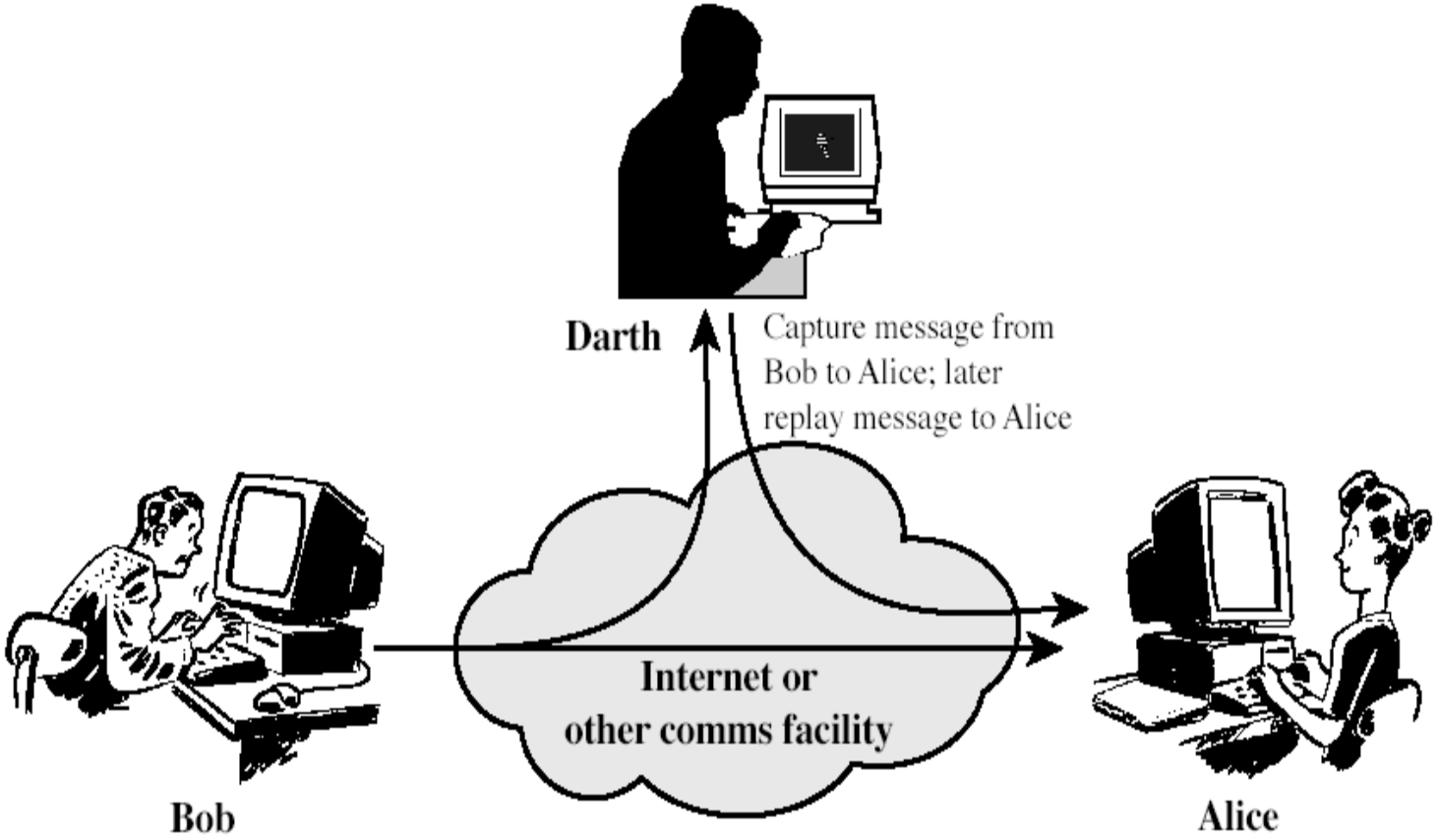
Active Attacks: Masquerade

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



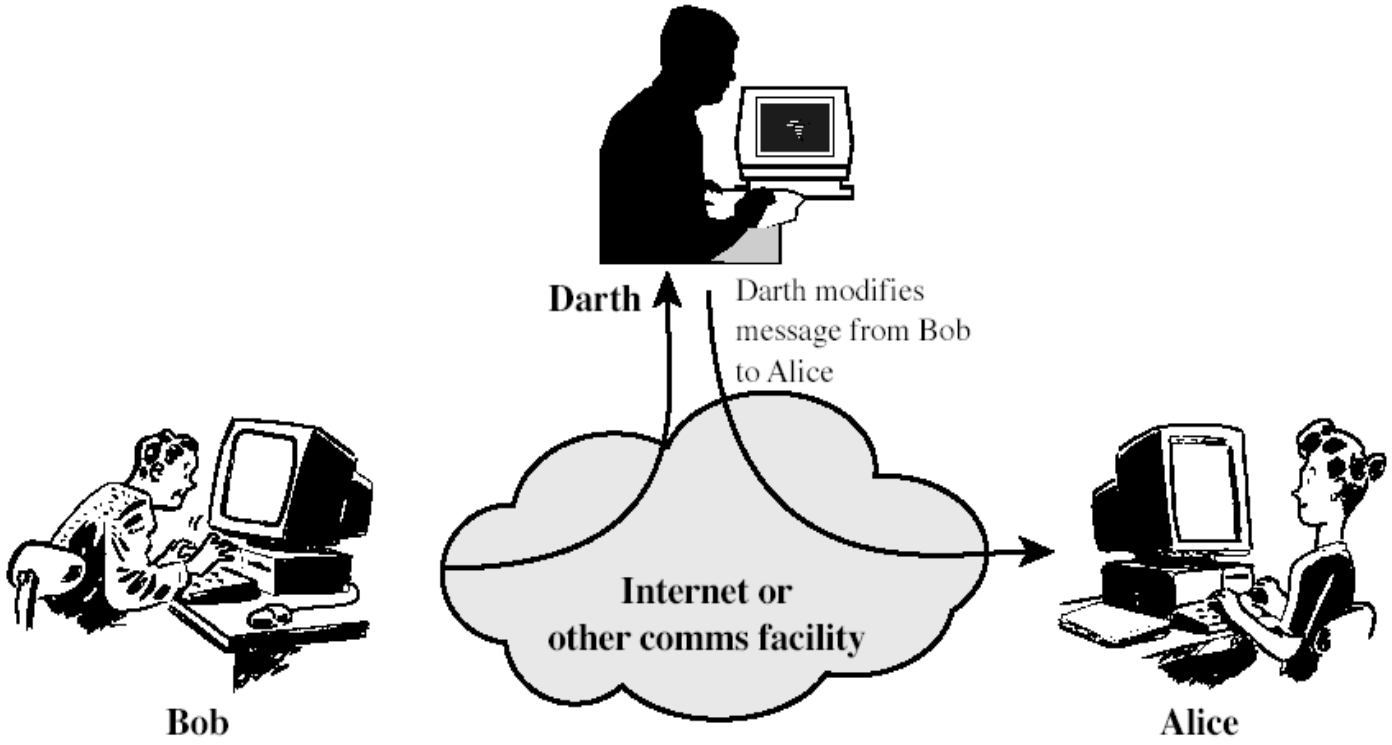
Active Attacks: Replay

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



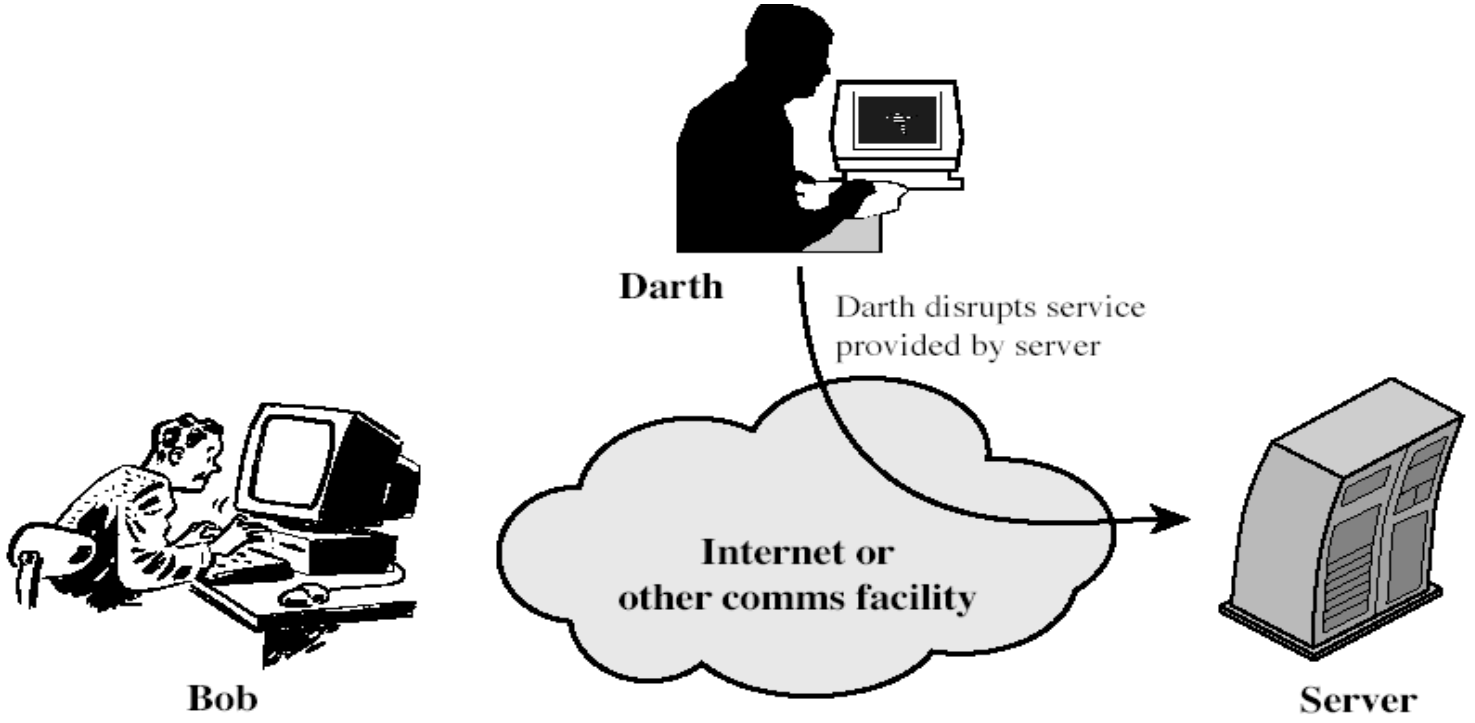
Active Attacks: Modification of Msg.

- 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

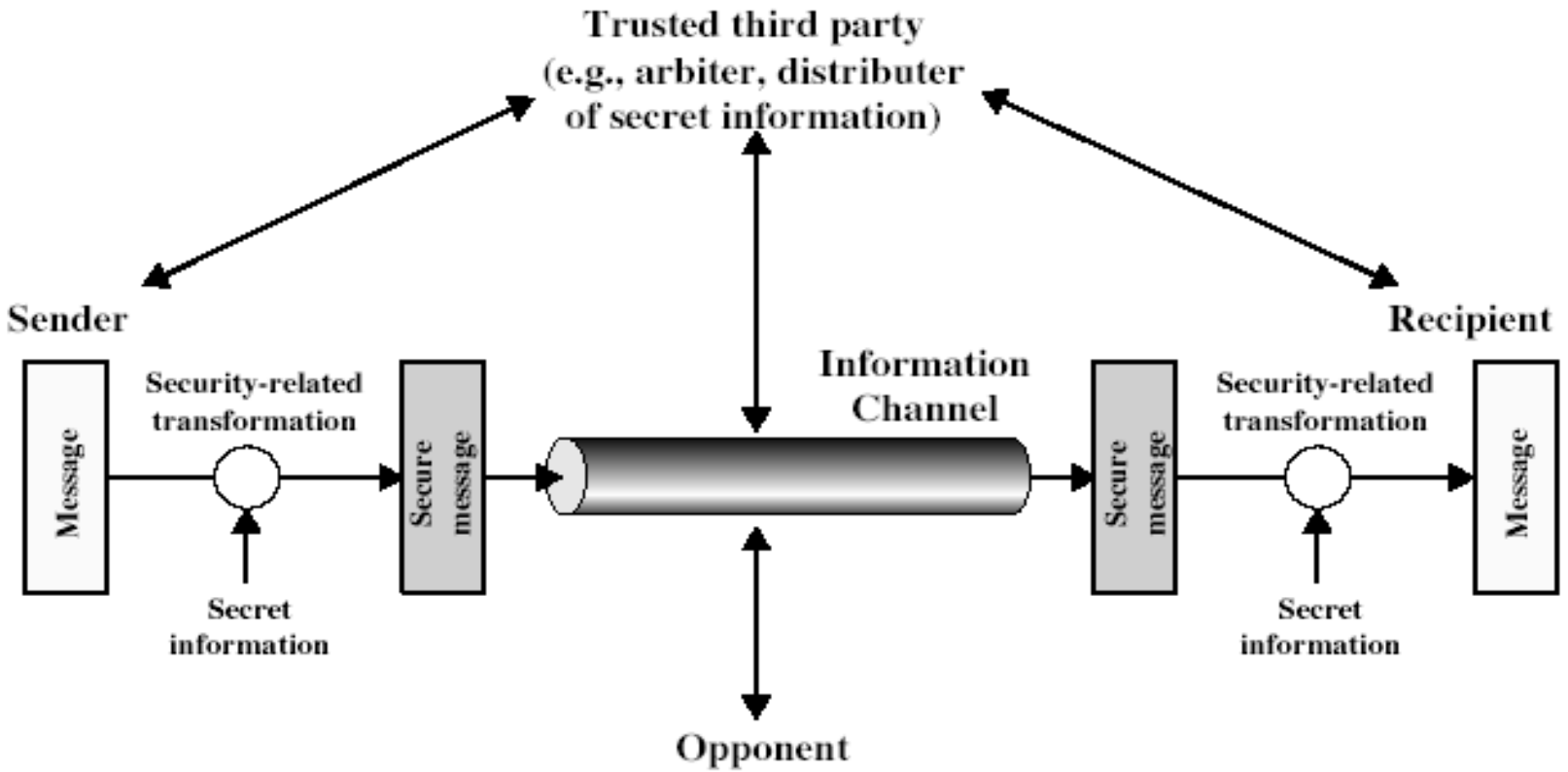
	Mechanism							
Service	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality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

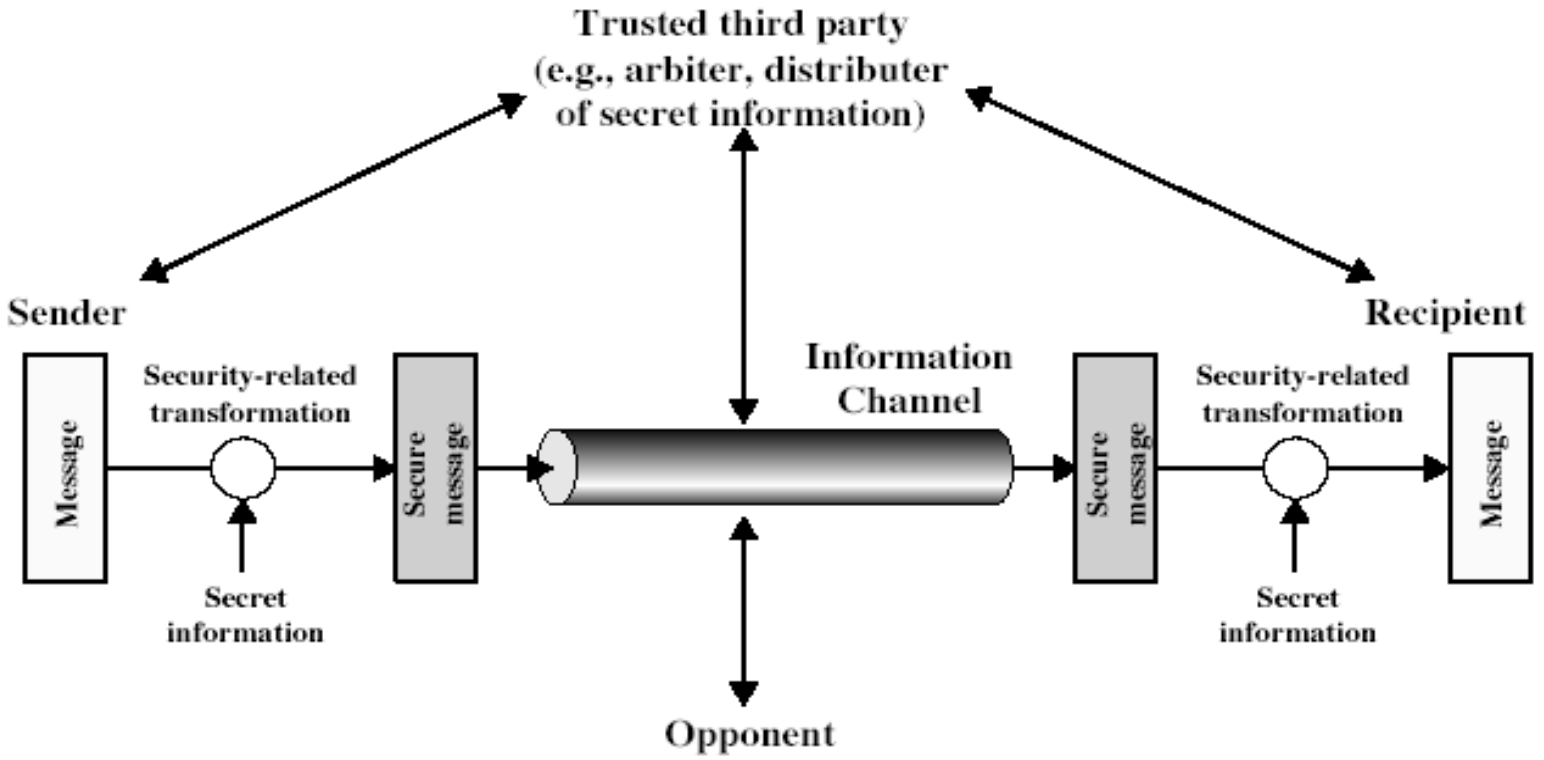
Model for Network Security

- 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

What's the Internet

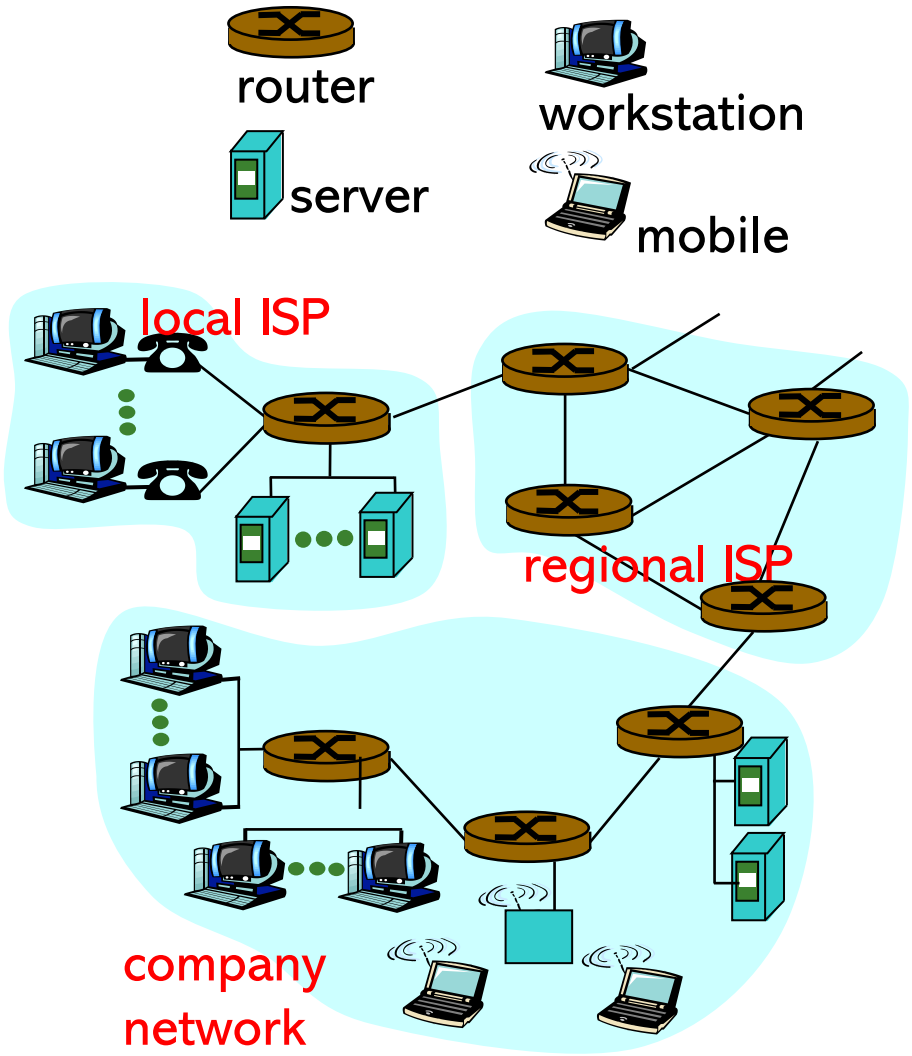
- We will be studying cryptographic security protocols for protecting the in-motion data on the internet.
- Therefore, we will review the basics of the internet's structure and function

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 modern, DSL, etc.



What's a protocol?...

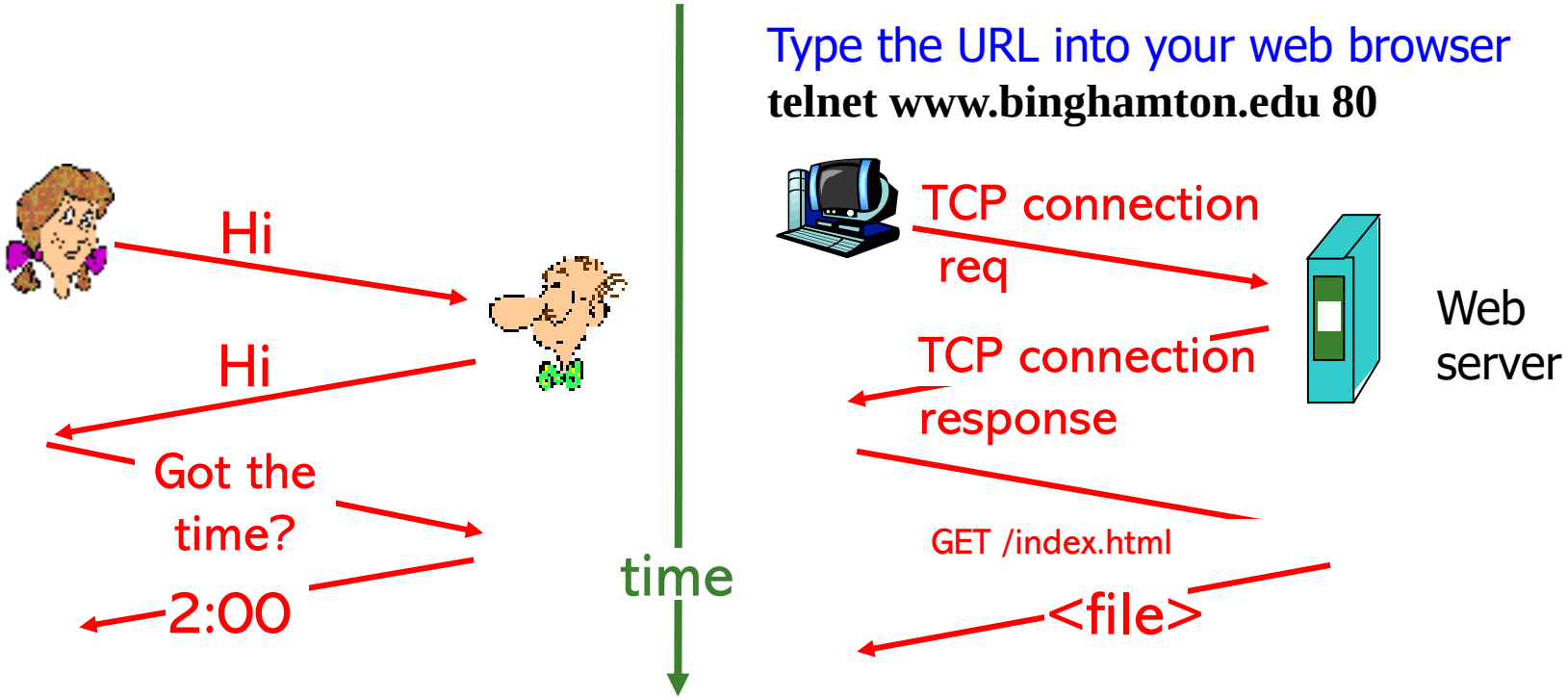
- All communication activity in Internet governed by protocols

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:



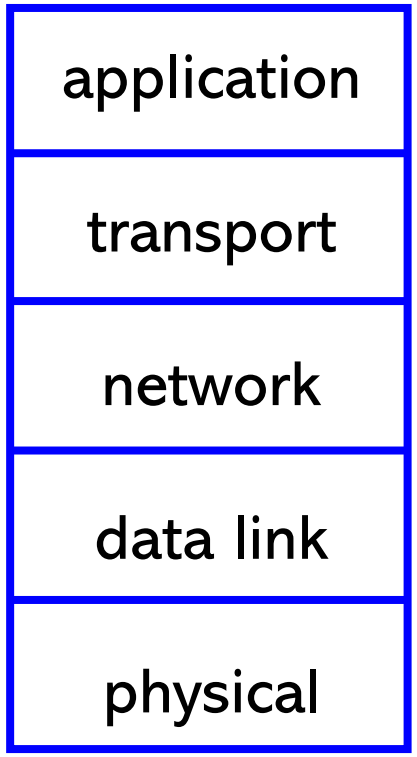
A network protocol is similar to a human protocol except that the entities sending and receiving msgs are hardware/software components of some device.

Protocol Layers

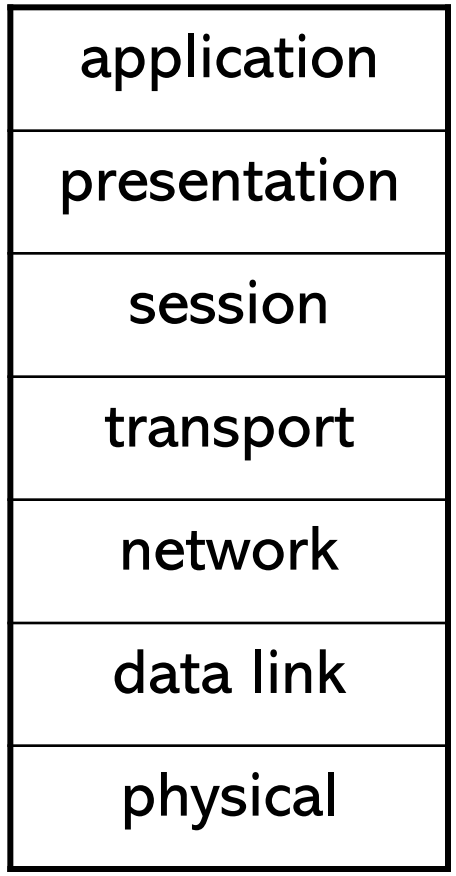
- Dealing with complex systems:
  - Provide a structural way to discuss system components.
  - Modularization eases maintenance, updating of system
    - Change of implementation of layer's service transparent to rest of system

Protocol Layers (Cont.)

- TCP/IP model: 5 layers

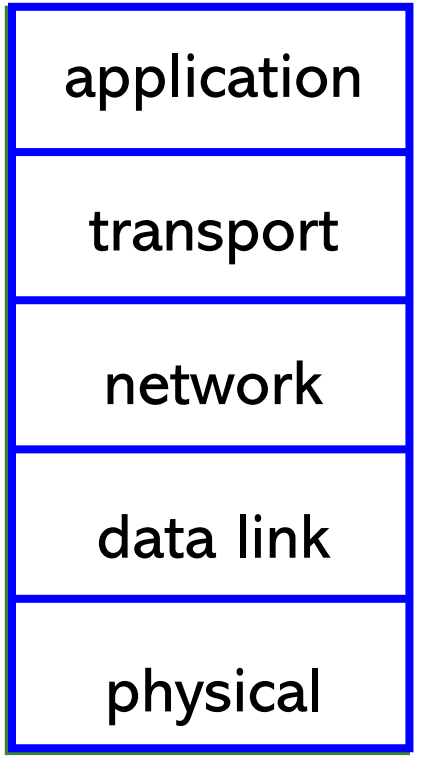


- OSI reference model: 7 layers



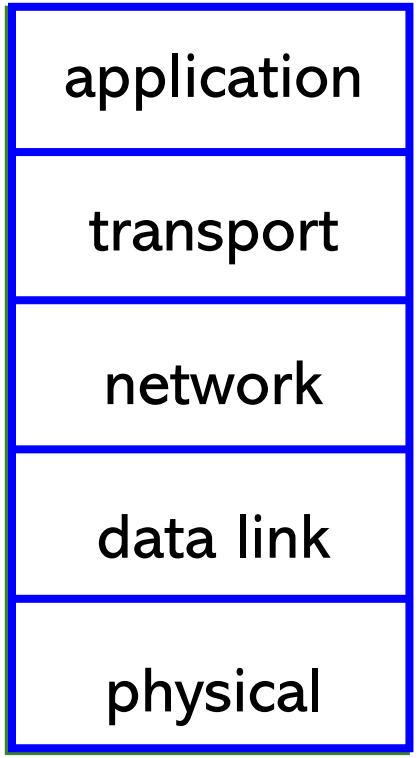
Internet protocol stack (TCP/IP Model)

- 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.



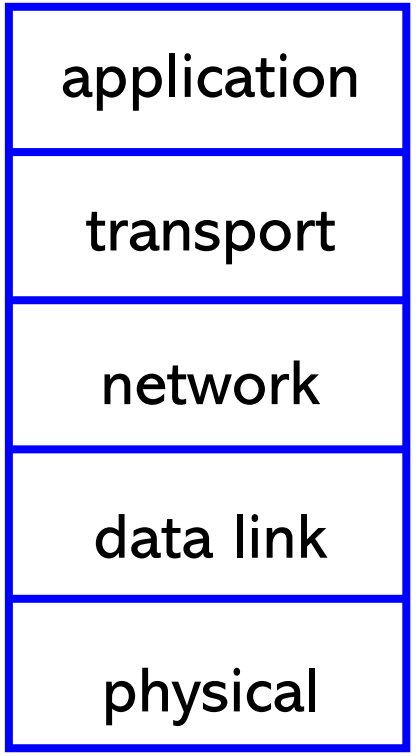
Internet protocol stack (TCP/IP Model)

- 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).



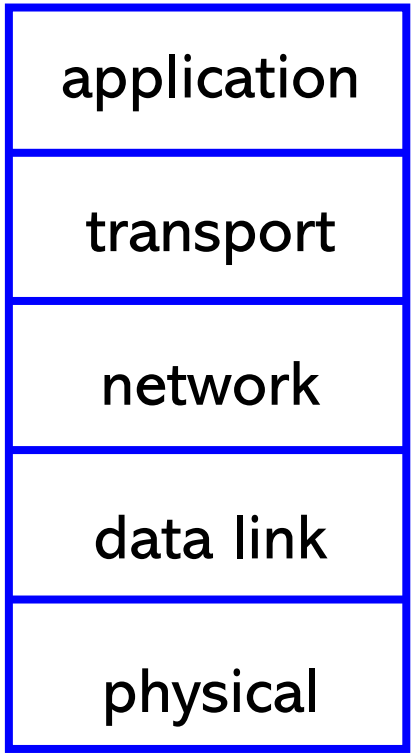
Internet protocol stack (TCP/IP Model)

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

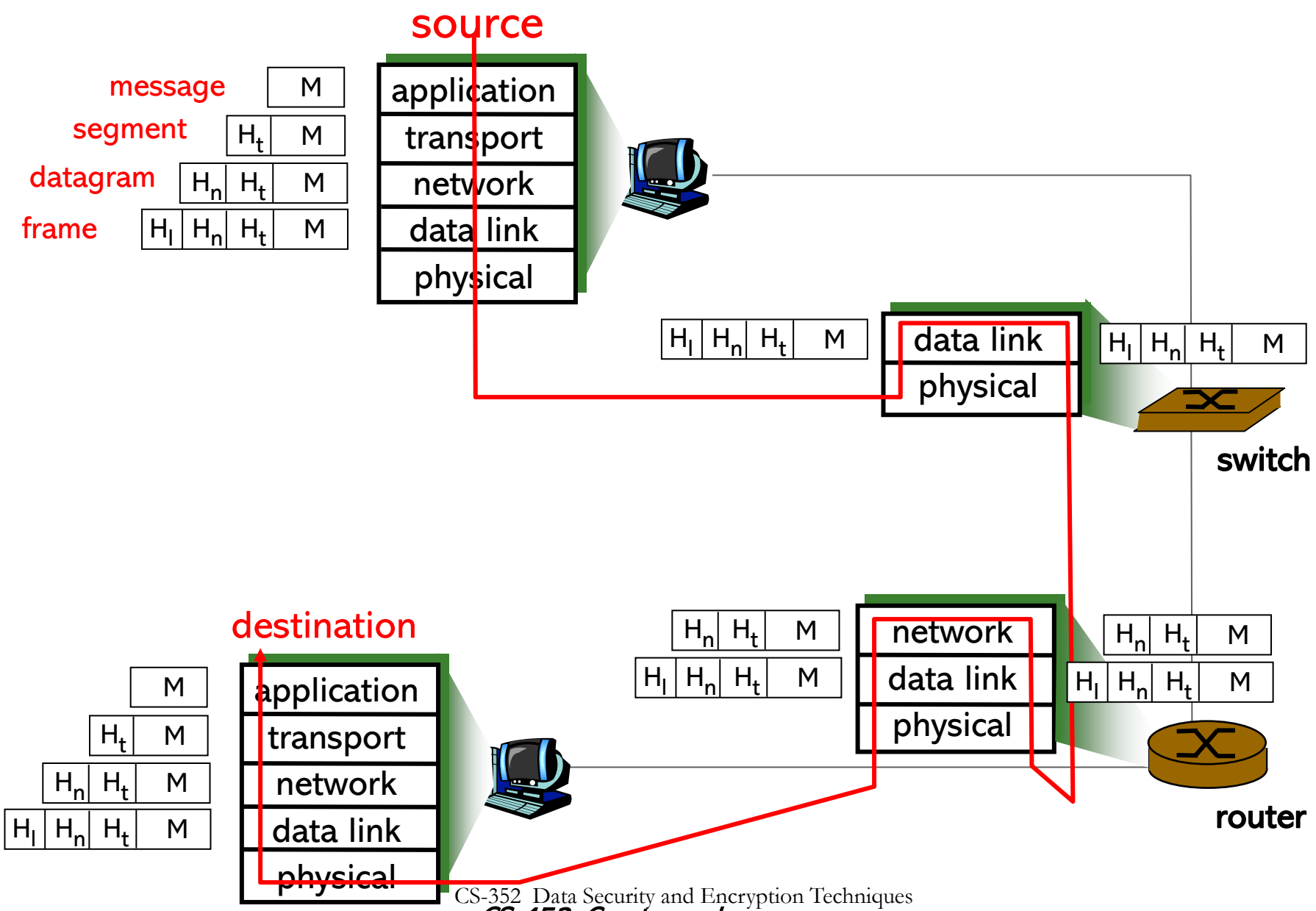


Internet protocol stack (TCP/IP Model)

- 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.

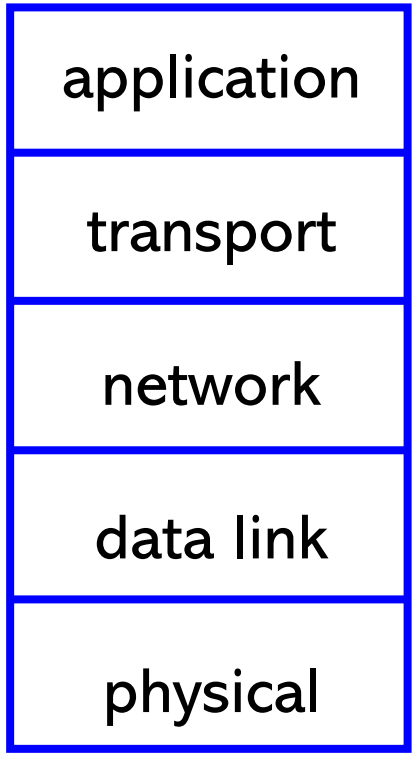


TCP/IP Model in Action Example

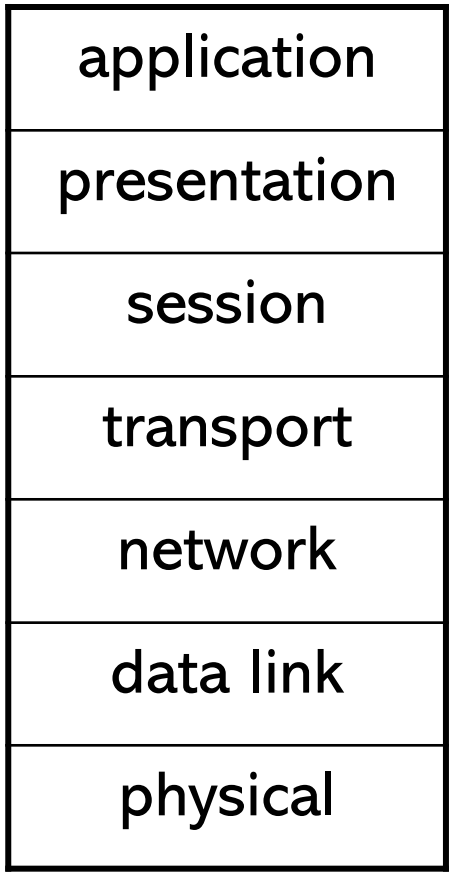


TCP/IP vs OSI Model

- TCP/IP model: 5 layers



- OSI reference model: 7 layers



- OSI has two extra layers:
  - Presentation: handles data compression, ***encryption***, and other data processing tasks before data is sent across the internet
  - Session: manages sessions between applications
  - In the TCP/IP model, the functions of the presentation/session layer are often implemented in the application layer

Network Programming

- Please check out the "Simple Python Socket Codes" posted on CANVAS underneath this presentation:
  - Illustrates a basic TCP server and client written in Python
  - Illustrates the basics of sending and receiving data over the internet – this is how it is generally done in the real-world

Data Classification in Government and Commercial Sectors

Data Classification (1)

- Data classification, or categorization: protection of data based on its need for secrecy, sensitivity, or confidentiality:
  - Data classification category is often used to select the cryptographic mechanisms for protecting the data
  - Data classification categories are referenced to in cryptographic standards (e.g., FIPS-140 series).
  - Understanding data classification is therefore also important in cryptography

- Primary objective: formalize and stratify the process of securing data based on assigned labels of importance and sensitivity

Data Classification (2)

- Why classify data?
  - Demonstrate organization's commitment to protecting valuable assets
  - Helps identify most critical assets
  - Justifies the use of a particular mechanism for protecting the data
  - Required by many security compliance measures
  - Helps establish the guidelines for who may access the data, authorized use, and parameters for declassification or destruction
- Data is classified based on its usefulness, lifetime, maturity, national security implications etc

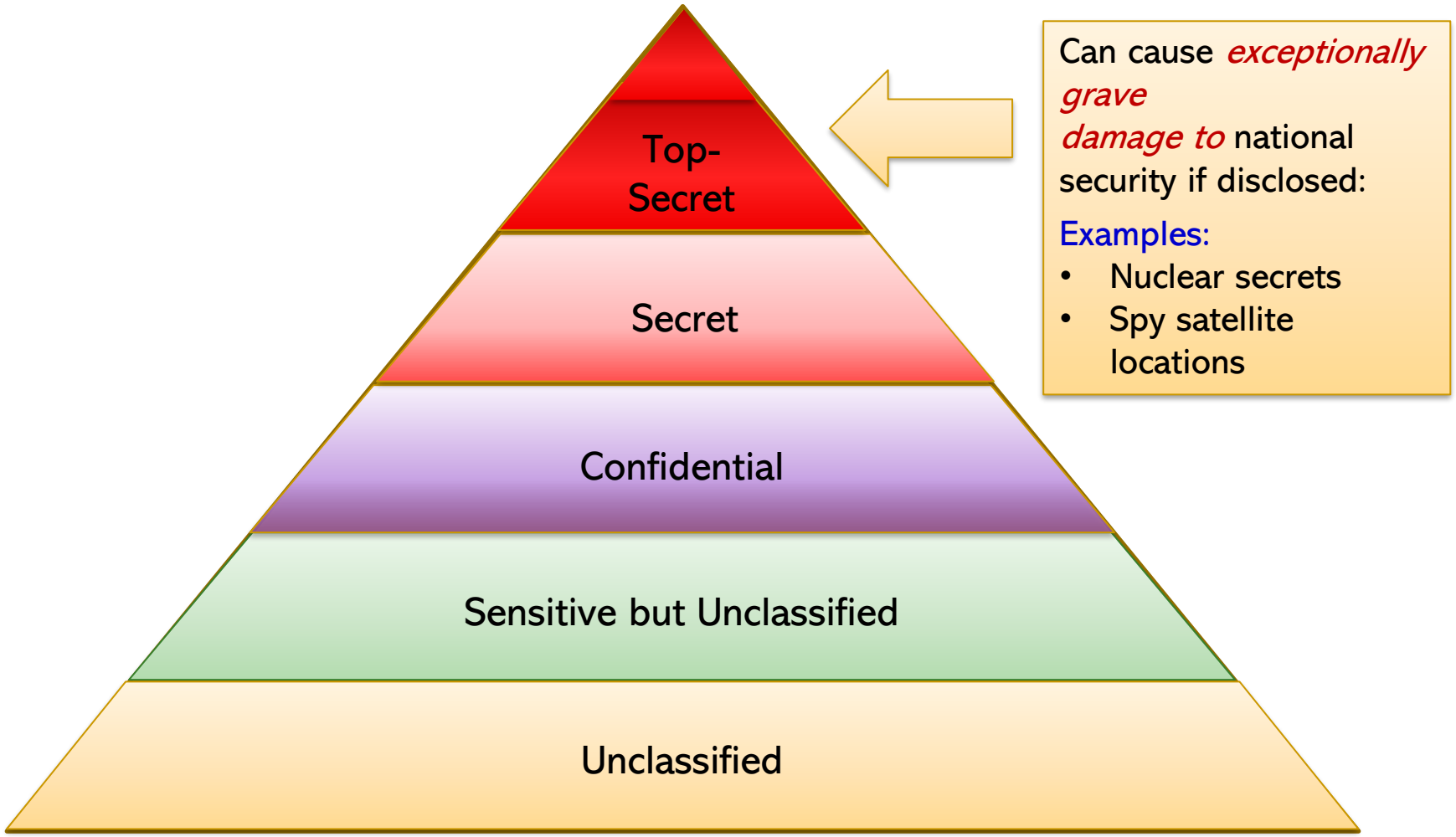
Data Classification (3)

- ISC^2 7-step guide to classifying data:
  - 1. Identify the custodian of the data, and define their responsibilities
  - 2. Define criteria for classifying and labeling the data
  - 3. Classify the resource
  - 4. Document any exceptions to the classification policy that were discovered, and integrate them into evaluation criteria
  - 5. Select the security controls that will be applied to each classification level to provide the necessary level of protection
  - 6. Specify the procedures for declassifying resources and the procedures for transferring custody of a resource to an external entity
  - 7. Create an enterprise-wide awareness program to instruct all personnel about the classification system.

Data Classification (4)

- Government/military and commercial/private sectors use different hierarchical schemes for classifying data.
- We will study these next

Government/Military Classification Scheme (1)

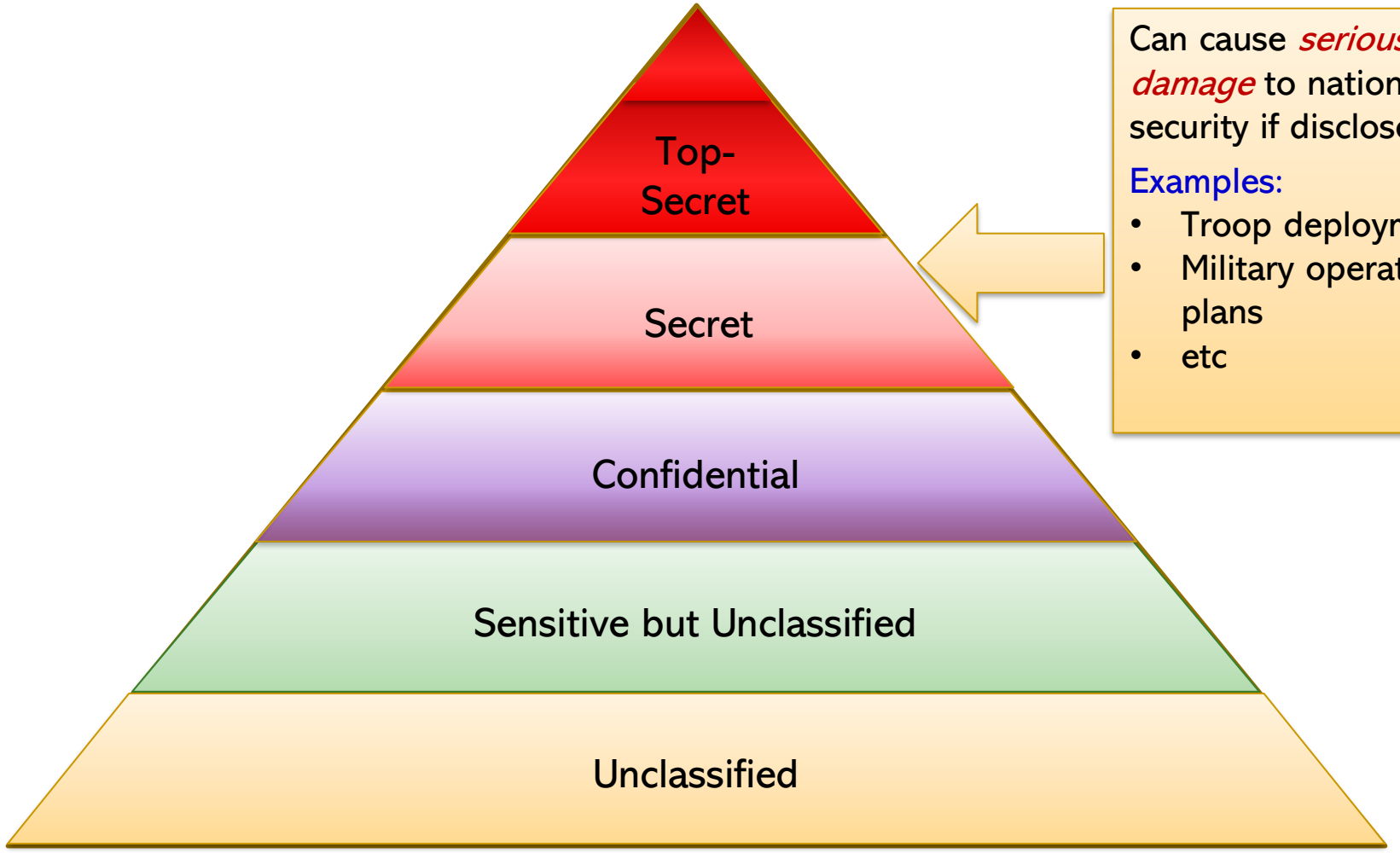


Can cause *exceptionally grave damage to* national security if disclosed:

Examples:

- Nuclear secrets
- Spy satellite locations

Government/Military Classification Scheme (2)

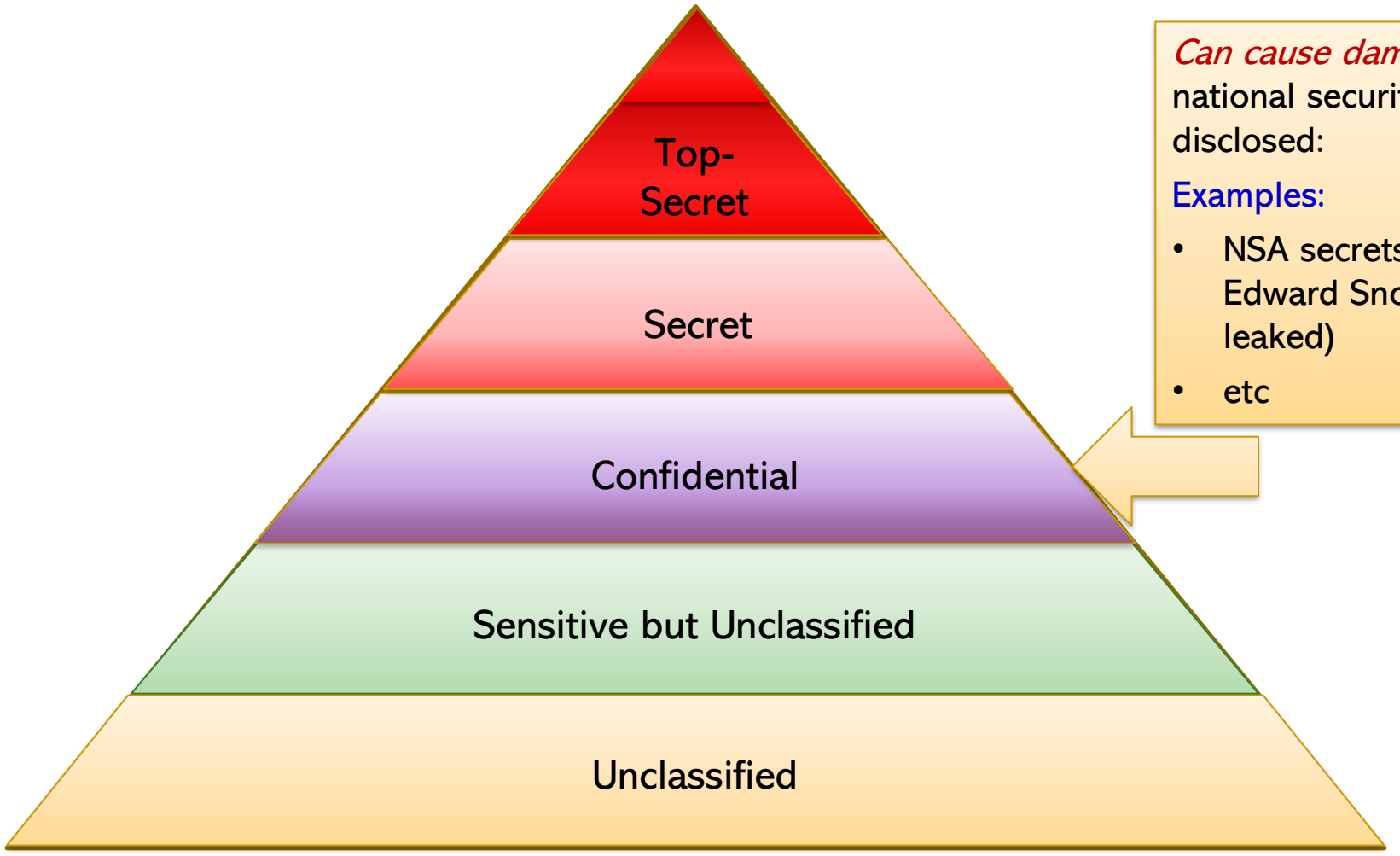


Can cause *serious damage* to national security if disclosed:

Examples:

- Troop deployments
- Military operation plans
- etc

Government/Military Classification Scheme (3)

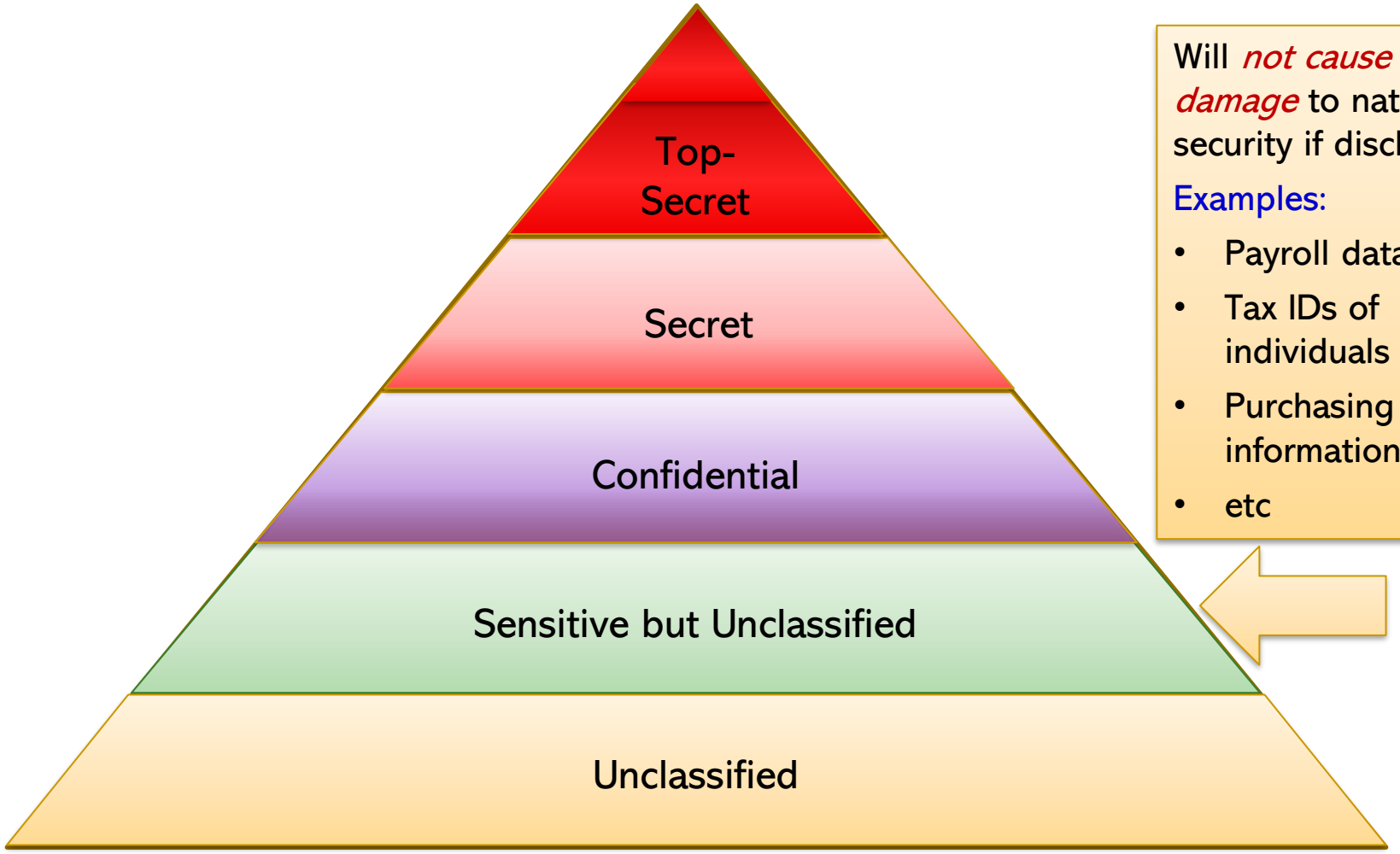


Can cause damage to national security if disclosed:

Examples:

- NSA secrets (what Edward Snowden leaked)
- etc

Government/Military Classification Scheme (4)

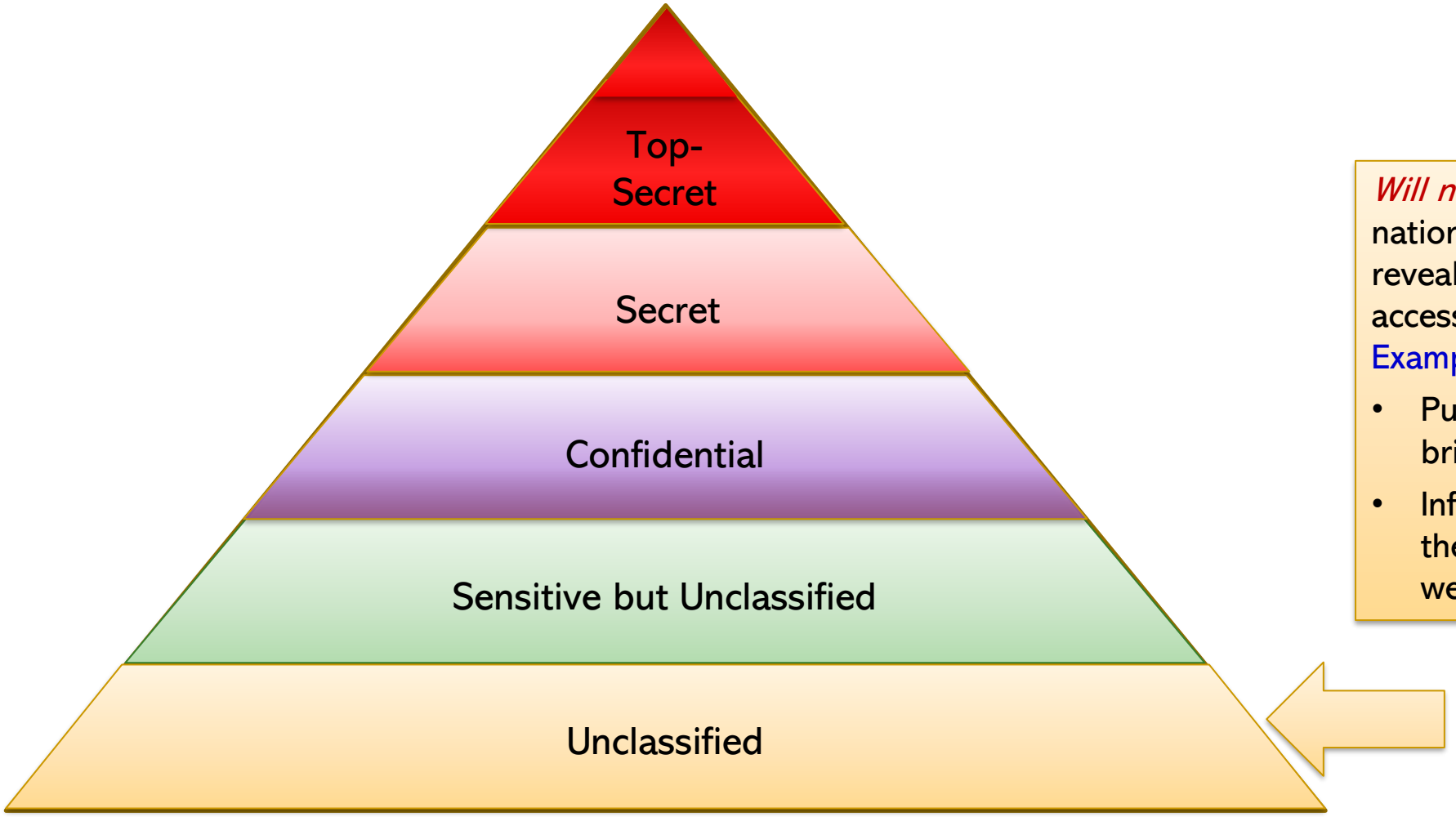


Will *not cause serious damage* to national security if disclosed:

Examples:

- Payroll data
- Tax IDs of individuals
- Purchasing information
- etc

Government/Military Classification Scheme (5)

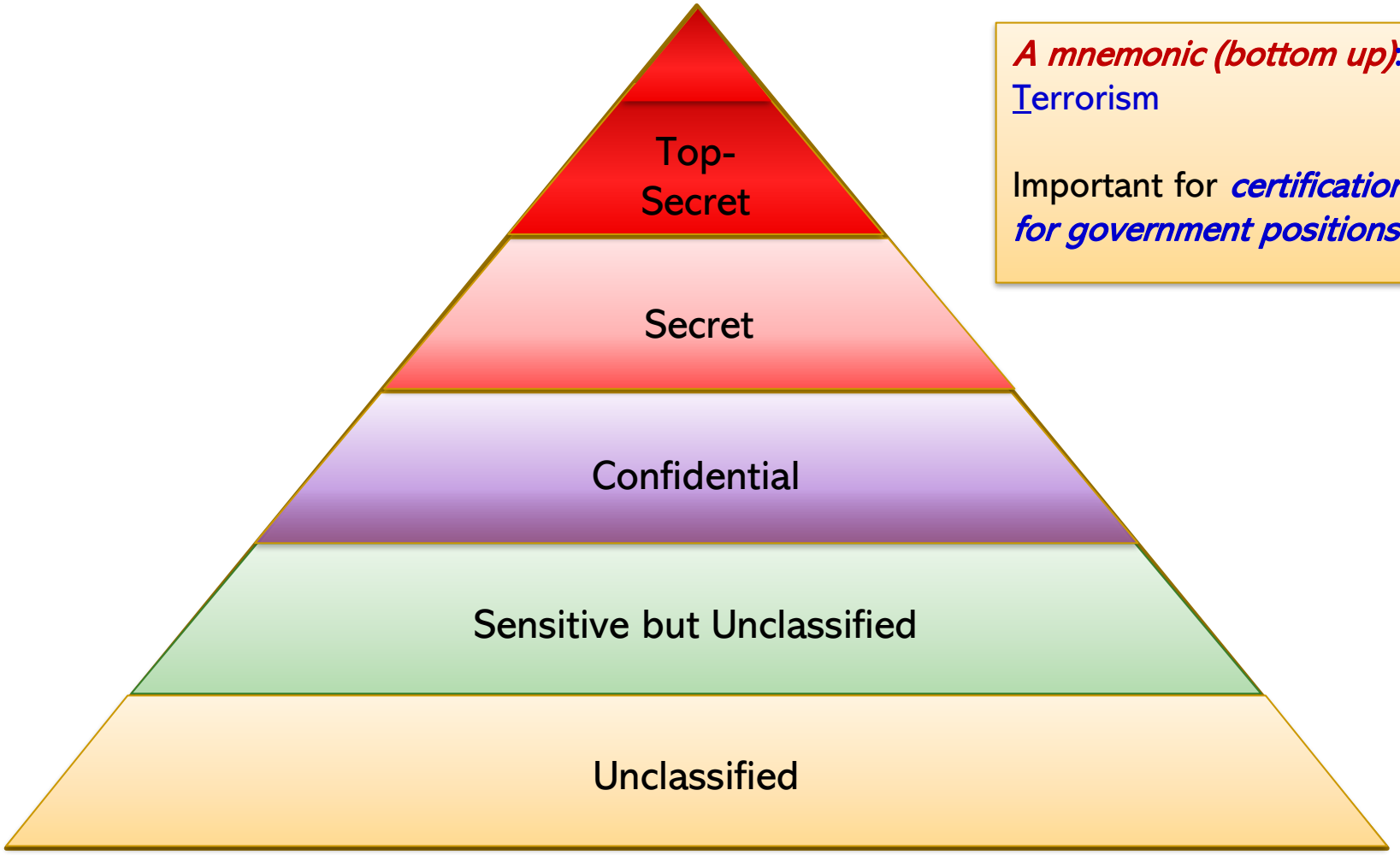


Will not impact national security if revealed; accessible to all

Examples:

- Public news briefings
- Information on the DoD public website

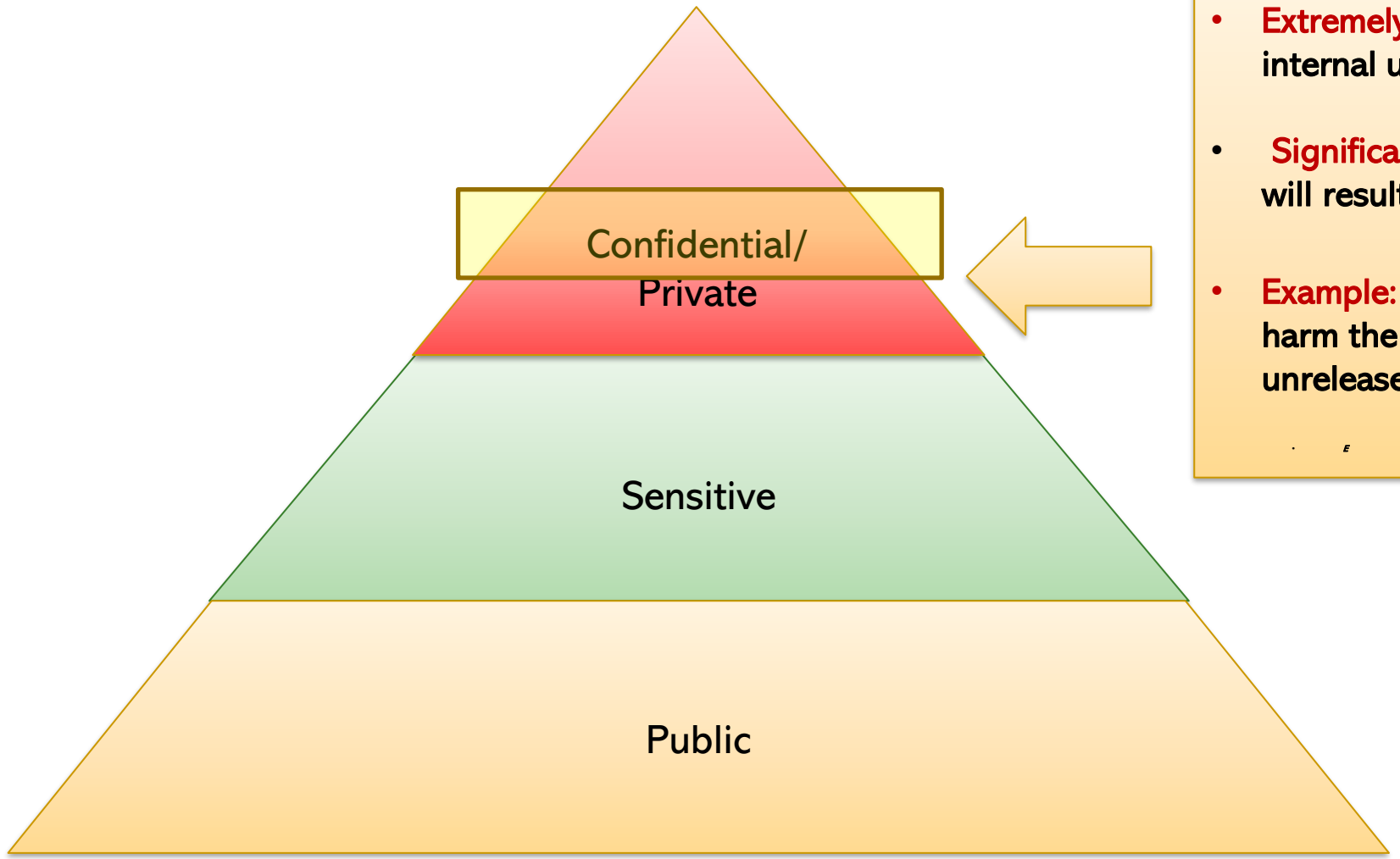
Government/Military Classification Scheme (6)



A mnemonic (bottom up): US Can Stop Terrorism

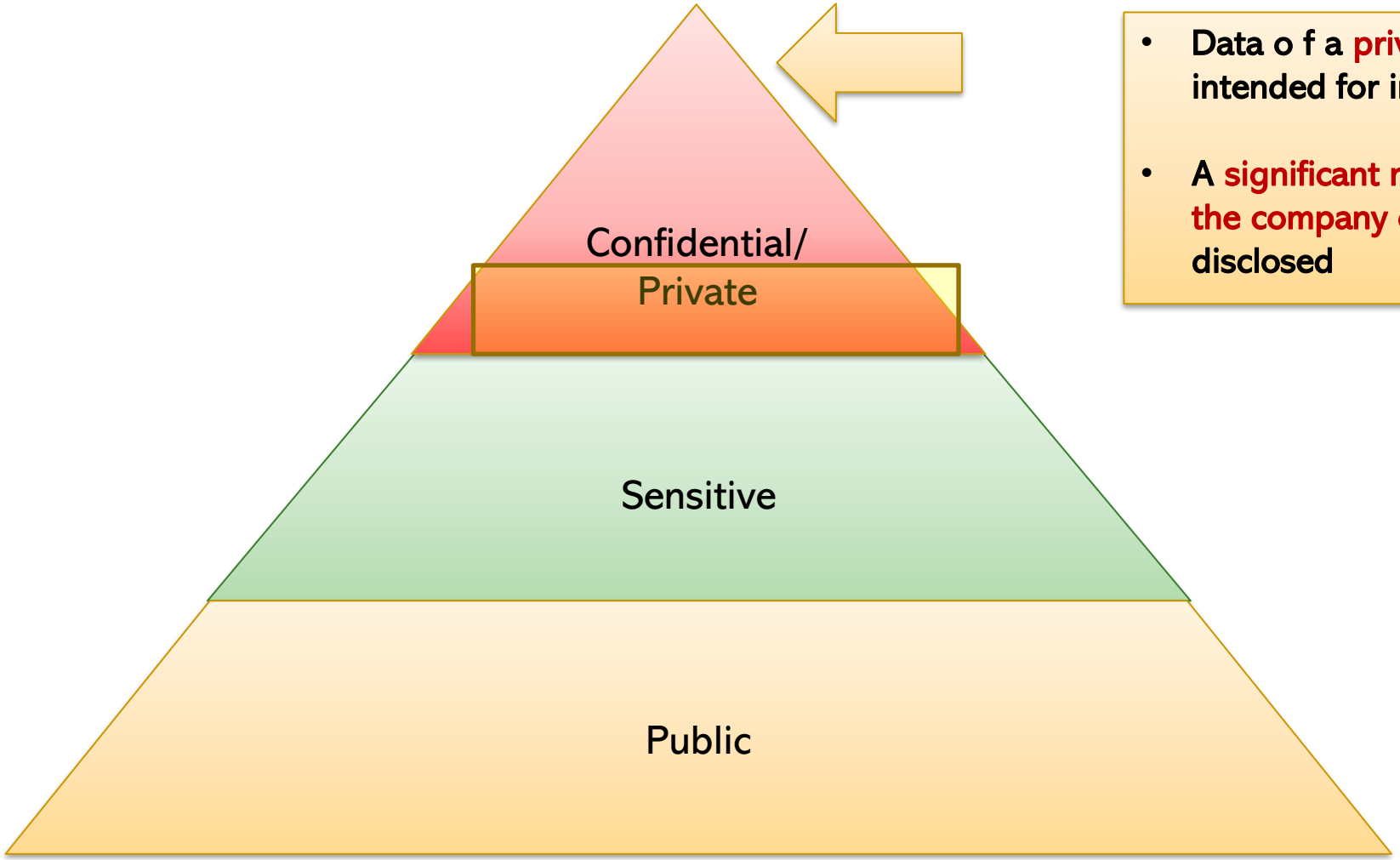
Important for ***certification exams*** and ***interviews for government positions***

Commercial business/private sector classification (1)



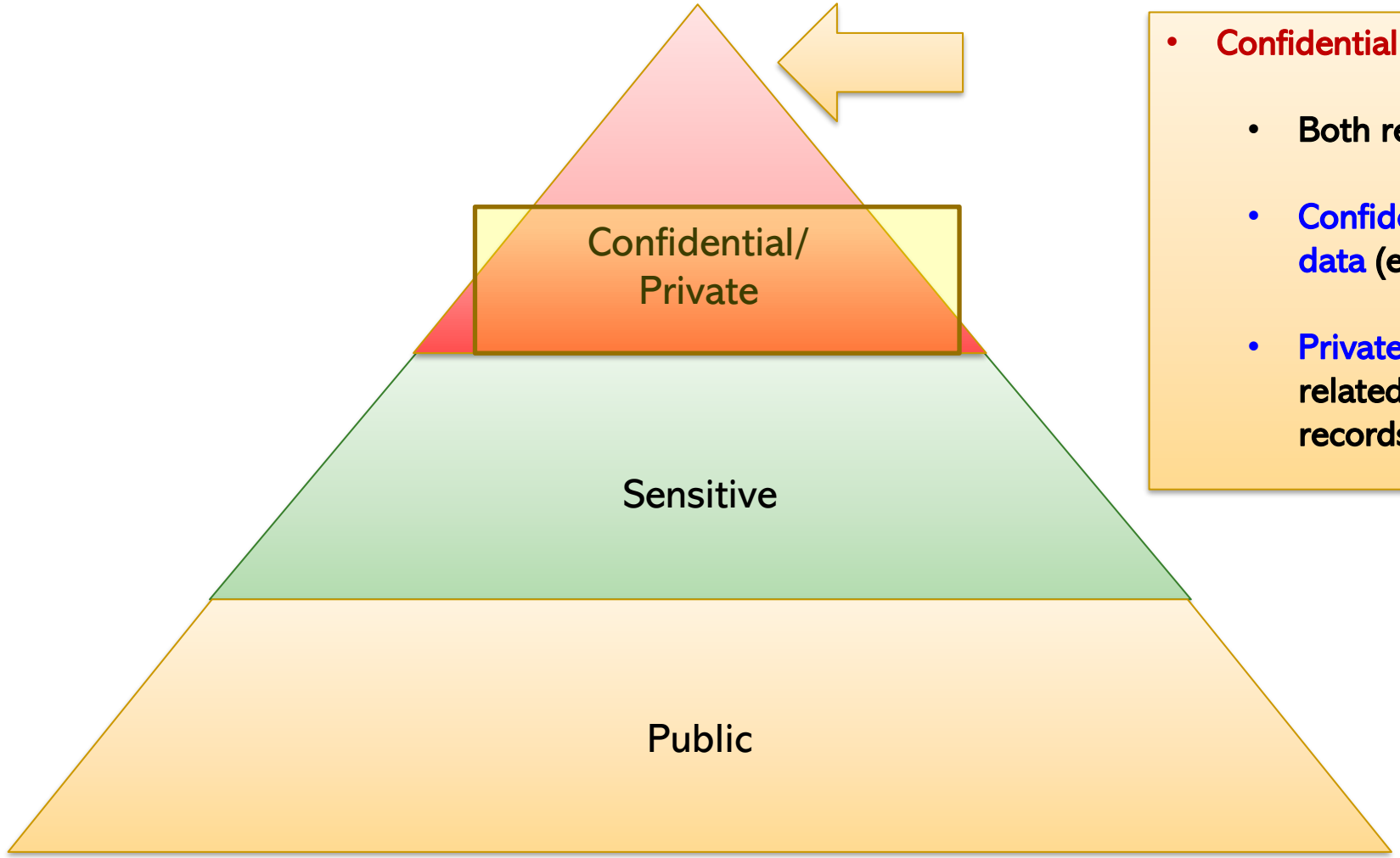
- **Extremely sensitive** and for company's internal use only
- **Significant negative impact** to the company will result if the data is disclosed:
- **Example:** data that if disclosed can seriously harm the company's competitive edge: e.g., unreleased product designs

Commercial business/private sector classification (1)



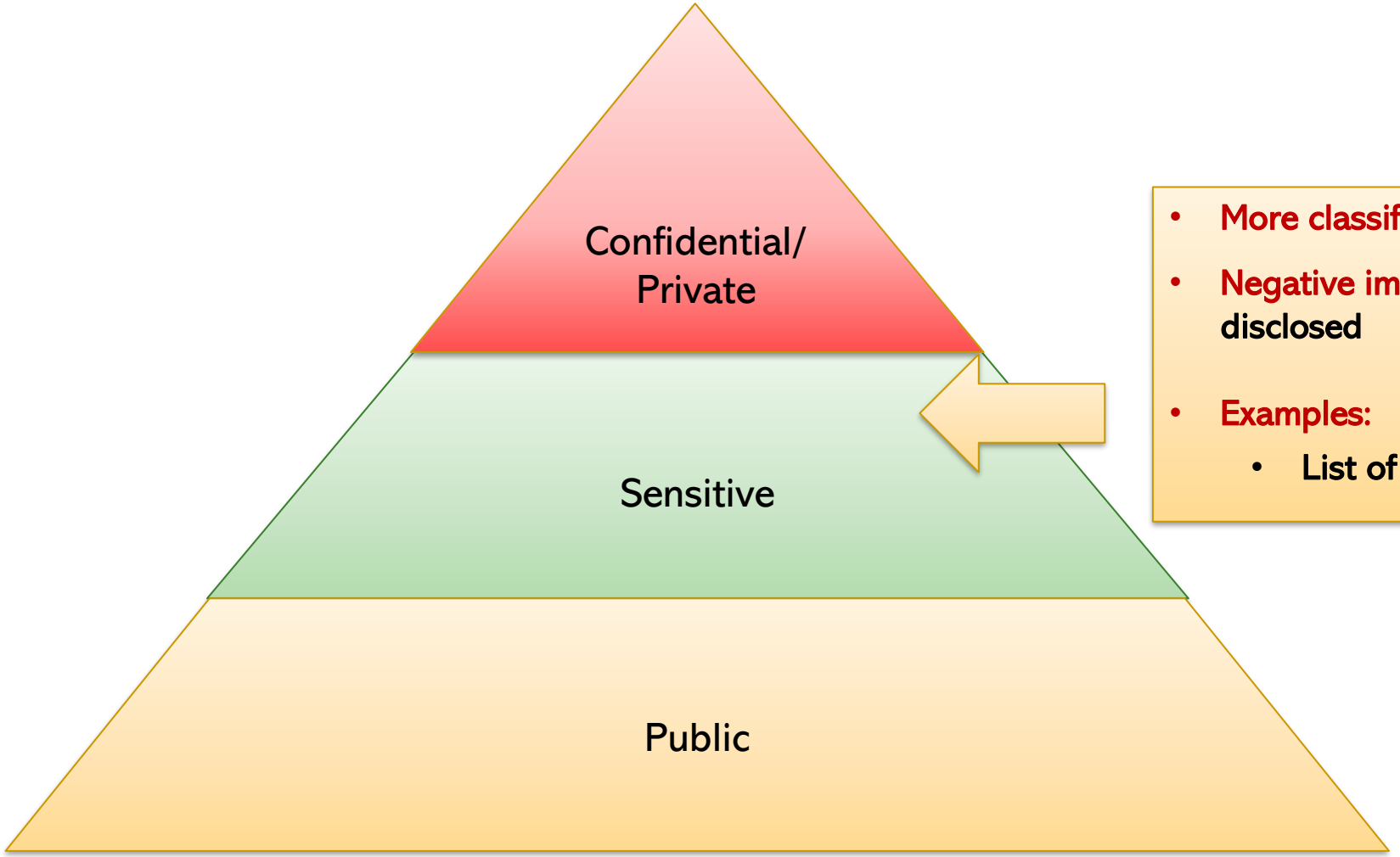
- Data o f a private or personal nature and intended for internal use only.
- A significant negative impact could occur for the company or individuals if private data is disclosed

Commercial business/private sector classification (1)



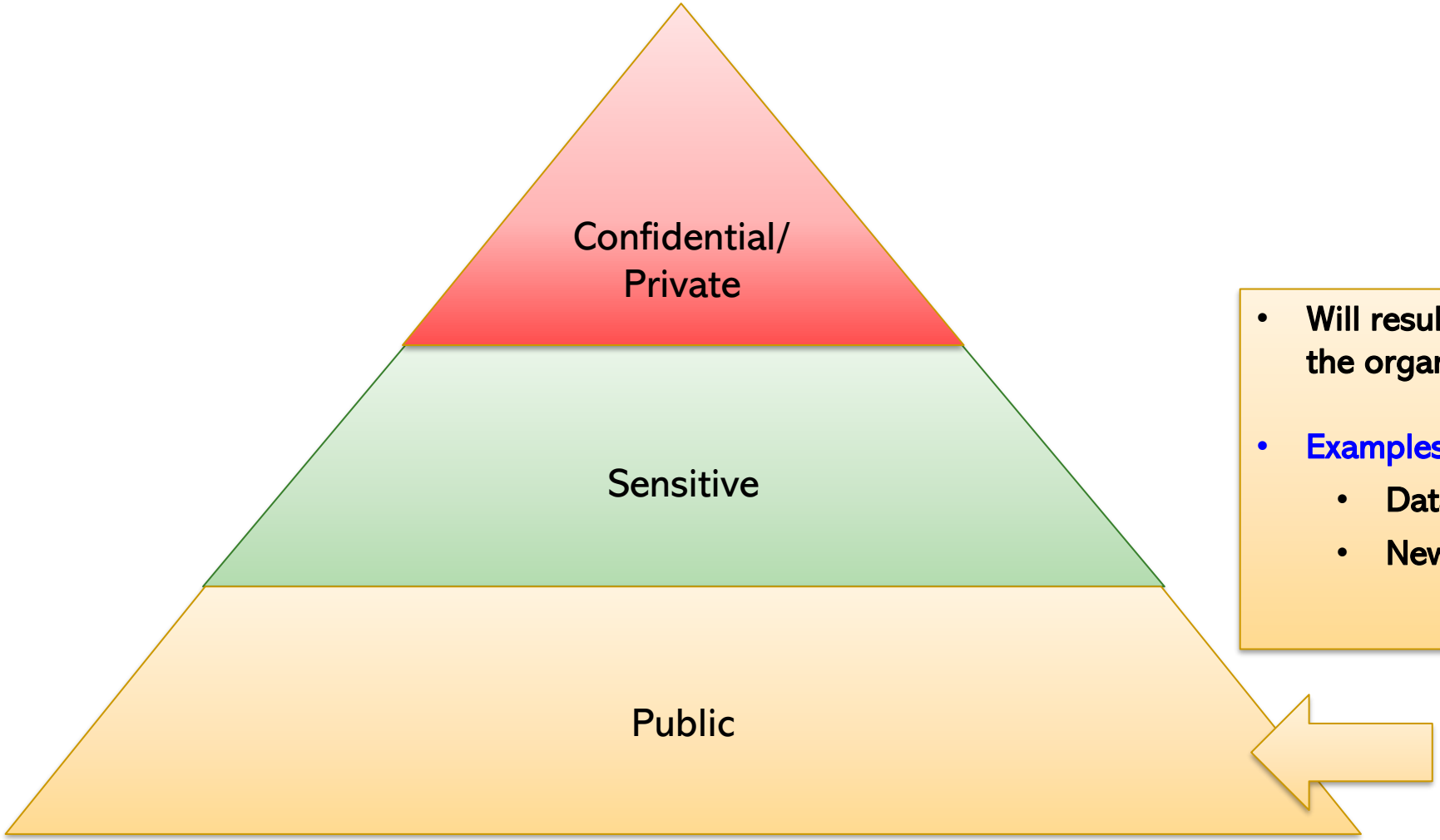
- **Confidential vs Private:**
  - Both require same level of security
  - Confidential generally refers to company data (e.g., product designs)
  - Private generally refers to the data related to individuals (e.g., medical records).

Commercial business/private sector classification (1)



- More classified than public data
- Negative impact will result to the company if disclosed
- Examples:
  - List of laid off employees

Commercial business/private sector classification (1)



- Will result in no negative impacts for the organization if disclosed
- Examples:
  - Data on the public website
  - News etc

Commercial business/private sector classification (1)

- Example: SONY 2014 Data Breach

Here is what the whole private sector classification looks like in the context of the Sony data breach in November 2014:

- "Confidential/Proprietary/" Level — unreleased movies
- "Private" Level — salary information on 30,000 employees
- "Sensitive" Level — lists of laid-off or dismissed employees; embarrassing emails
- "Public" Level — Sony managed to protect the integrity of such information provided by them (e.g., on their website)

Source: https://resources.infosecinstitute.com/certification/information-and-asset-classification/

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

Government standards for cryptographic modules

FIPS 140 Series (1)

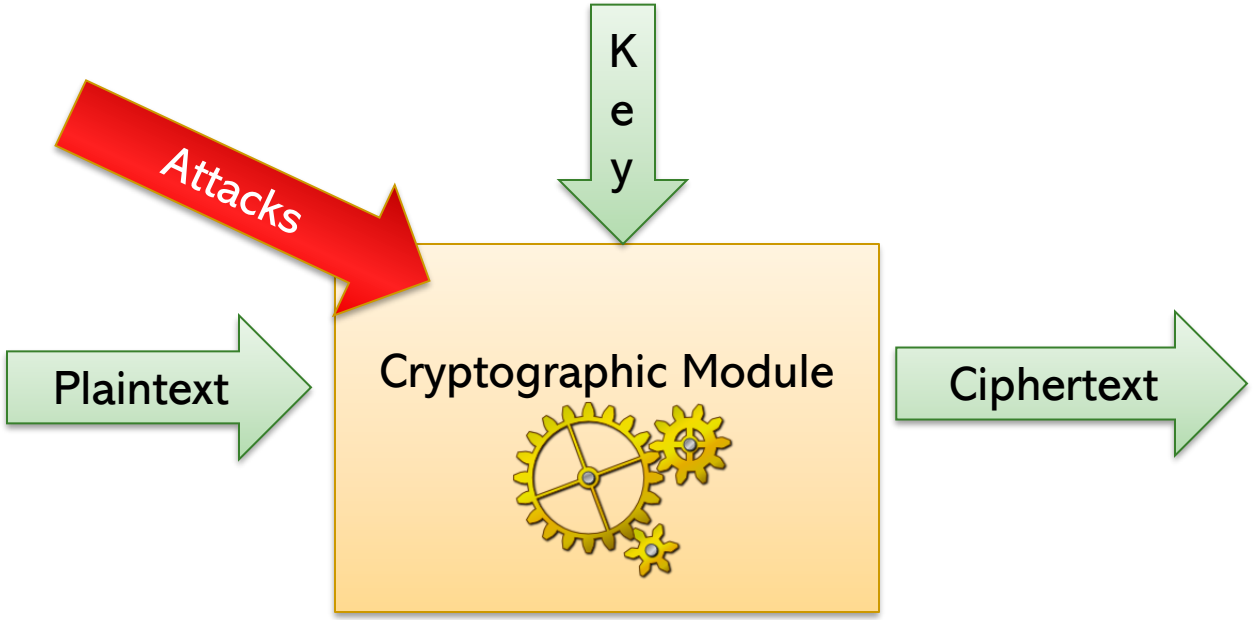
- FIPS-140 Official title: Security Requirements for Cryptographic Modules
- U.S. Government standard for securing cryptographic modules used in systems that process *sensitive but unclassified data*
  - *Maintained by the National Institute of Standards (NIST)*
- Commercial vendors, government contractors,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

FIPS 140 Series (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

FIPS 140 Series (10)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
  - *2. Cryptographic module ports and interfaces:* what information enters and exits the module and how it should be separated

FIPS 140 Series (10)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
  - *3. Roles, services and authentication:* what users are allowed to perform what actions with the module and how these users are authenticated

FIPS 140 Series (10)

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

FIPS 140 Series (11)

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

FIPS 140 Series (12)

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

FIPS 140 Series (13)

- Scope of 140 series: specifies module security requirements in the following 11 areas:
  - *10. Design assurance:* documentation requirements showing that the module was well designed and implemented

FIPS 140 Series (13)

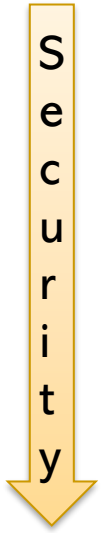
- Scope of 140 series: specifies module security requirements in the following 11 areas:
  - 11. *Mitigation of attacks:* if the module is designed to mitigate a specific attack, then it must included in the documentation

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:



Level	Requirements
Level 1	• All components must be *production grade* • Must not have *serious security issues*
Level 2	• Adds a requirement that *tampering attempts must leave evidence* • Module *must implement authentication based on user roles*
Level 3	• Adds a requirement that the module *must be tamper resistant* • Must be able to *authenticate users based on user identity* • Imposes additional requirements on *module interface security*
Level 4	• Adds *stricter physical security* requirements • Requires resistance against attacks targeting the *device environment*

FIPS 140 Series (17)

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

Source: www.amazon.com

FIPS 140 Series (18)

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

Click image to open expanded view

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

Source: www.amazon.com

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