UNIK4250 Security in Distributed Systems
University of Oslo
Spring 2012

Meeting 1

Course Information

Background and Basic Concepts

How to survive UNIK4250

- Mix of lectures and guided study
  - Because of low number of students
- Basic requirements
  - Read text book
  - Come to meetings
  - Work on the workshop questions
    - Will be discussed during the meetings
  - Work on the obligatory assignment
    - To be defined.

Course Resources

- Learning material will be made available on Fronter:
  - https://blyant.uio.no/
    - lecture notes, workshop questions, assigment description etc.
- Various additional resources
  - To be specified during the semester

Course Assessment

- Course weight: 10 study points
- Final exam: 100%
  - Normally oral examination
  - Written examination in case of many students
- Academic dishonesty (including plagiarism and cheating) is actively discouraged, see
  - http://www.uio.no/english/studies/admin/examinations/cheating/

Course Staff

- Coordinator:
  - Prof Audun Jøsang
  - josang@mn.uio.no
  - Tel +98431433
- Guest lecturers
  - Tor Hjalmar Johansen, Telenor
  - Leif Nilsen, Thales
  - Josef Noll, UNIK
- UNIK administration
  - http://www.unik.no
  - Email: postmottak@unik.no
  - Tel: +64 84 47 00

Who do I contact?

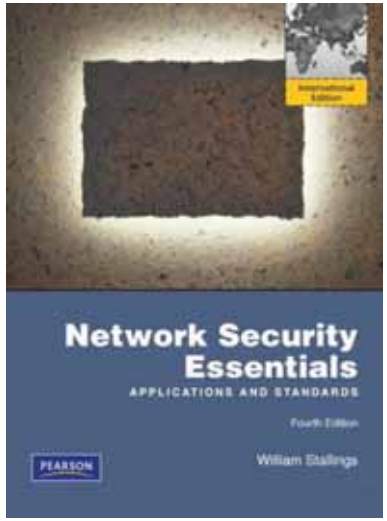
- Coordinator
  - for help with course material,
  - attendance problems, exam marking
  - for general course related matters

- Administration
  - For any matters external to this course,
    e.g. enrolment problems, IT access problems

Syllabus and text book

- The syllabus for this course consists of the text book and additional material which will be clearly specified.
- Adequate comprehension of the material requires that you also
  - read the text book and additional material
  - attend workshops
  - work out answers to the workshop questions
- Text book:

  Network Security Essentials, 4th Ed, 2010
  William Stallings



- The book is relatively dry (no humour).
  - Contains some crypto necessary for understanding network security

Chapters of textbook Network Security Essentials

1. Introduction
2. Symmetric Encryption and Message Confidentiality
3. Public-Key Cryptography and Message Authentication
4. Key Distribution and User Authentication
5. Transport-Level Security
6. Wireless Network Security
7. Electronic Mail Security
8. IP Security
9. Intruders
10. Malicious Software
11. Firewalls
12. Network Management Security
13. Legal and Ethical Issues

Additional lectures

- Mobile network security
- DNSSEC
- Security of semantic mobile networks.

Learning language

- All syllabus material and workshop questions to be provided in English.
- Specific Norwegian documents as background material
- List of Norwegian translations of English security related terms to be developed during the semester.

Workshops

- Workshops will be organised in connection with the meetings.
- Workshop questions relate to the topic presented the previous week.
- Written answers to workshop questions will be provided
- The purpose of the workshops is to facilitate better learning of the lecture material

Other security courses at UiO

- UNIK4220 – Introduction to Cryptography (autumn)
  - Leif Nilsen (Thales)
- INF3510 – Information Security (spring)
  - Audun Jøsang (IfI)
- UNIK4270 – Security in Operating Systems and Software (autumn)
  - Audun Jøsang (IfI)
- UNIK4720 Trust and Reputation Systems
  - Audun Jøsang (IfI),
  - (not yet scheduled)
- ITLED4230 Information Security Governance
  - Audun Jøsang (IfI)
  - Part of IT Management Master's

Security in Distributed Systems Background and Basic Concepts

Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

Norwegian terms

English		Norwegian
• Security	→	• Sikkerhet
• Safety	→	• Trygghet
• Certainty	→	• Visshet

- Security
- Safety
- Certainty

→ • Sikkerhet

Definitions

- **Computer Security** - generic name for the protection of data and to thwart hackers on computer systems
- **Network Security**: two main areas
  - **Communication Security:** measures to protect data during their transmission
  - **Perimeter Security:** measures to protect networks from unauthorized access
- **Internet Security** - measures to protect information stored and transmitted across a collection of interconnected networks

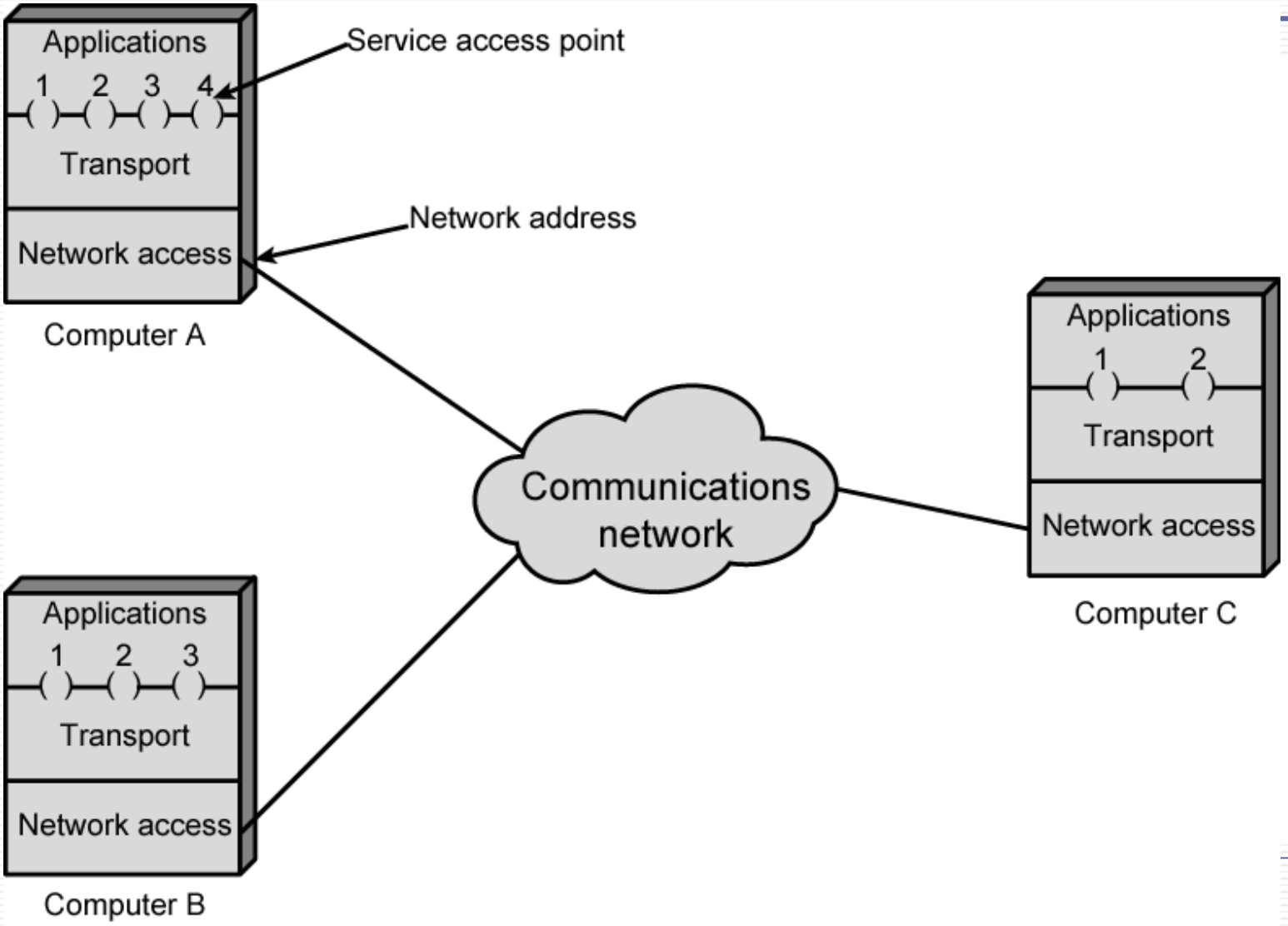
Aim of Course

- our focus is on **Internet Security**
- which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information

Communication Protocol Architecture

- Layered structure of hardware and software that supports the exchange of data between systems as well as a distributed application (e.g. email or web access)
- Each protocol consists of a set of rules for exchanging messages, i.e. “the protocol”.
- A protocol session is an actual instance of communication according to the rules of a protocol.

Protocol Architectures and Networks



Addressing Requirements

- Two levels of addressing required
  - Each computer needs unique network address
  - Each application on a (multi-tasking) computer needs a unique address within the computer (enables transport layer to service multiple applications
    - Application addresses called service access points (SAPs) or ports (SAP is OSI name for port)

Protocol Data Units (PDU)

- protocols are used to communicate at each layer
- Control information is added to user data at each layer
- Transport layer may fragment user data
- Each fragment has a transport header added
  - Destination SAP (port)
  - Sequence number
  - Error detection code
- This gives a transport protocol data unit

Standardized Protocol Architectures

- Required for devices to communicate
- Vendors have more marketable products
- Customers can insist on standards based equipment
- Two standards:
  - OSI Reference model
    - Never lived up to early promises
  - TCP/IP protocol suite
    - Most widely used
- Also: IBM Systems Network Architecture (SNA)

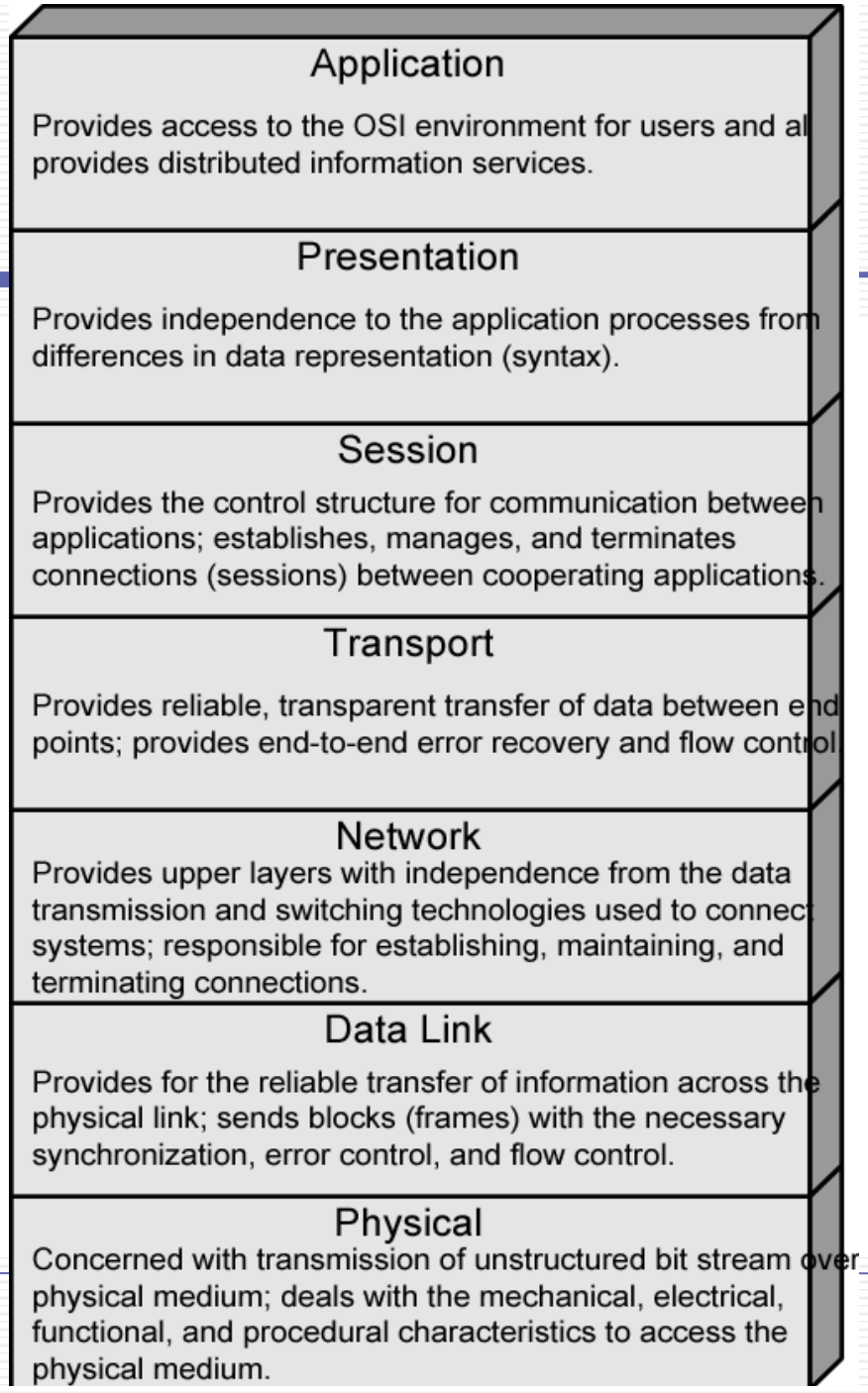
OSI

- Open Systems Interconnection
- Developed by the International Organization for Standardization (ISO)
- Seven layers
- A theoretical system delivered too late!
- TCP/IP is the de facto standard

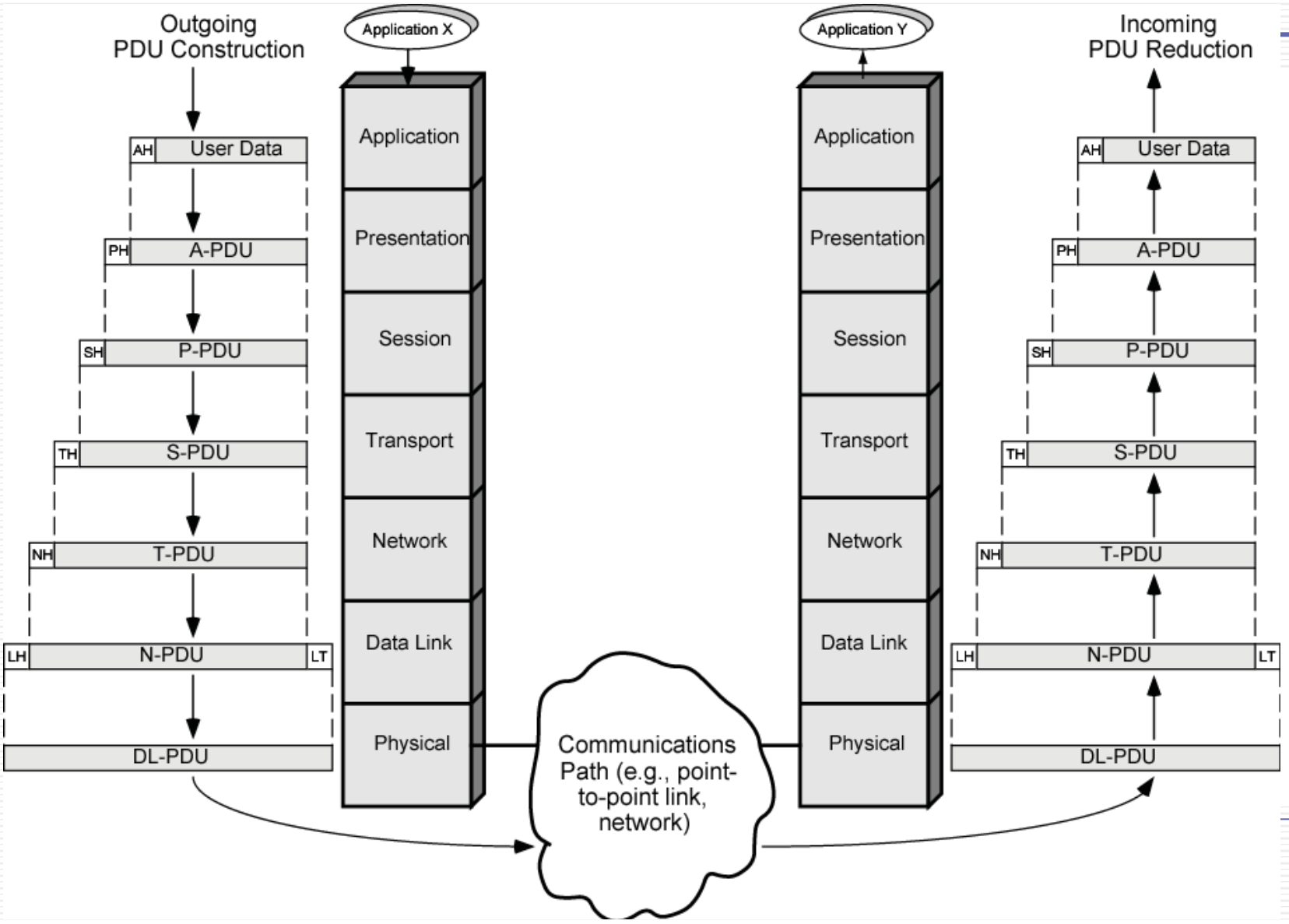
OSI - The Model

- A layer model
- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers

OSI Layers


Application
Provides access to the OSI environment for users and al
provides distributed information services.
Presentation
Provides independence to the application processes from
differences in data representation (syntax).
Session
Provides the control structure for communication between
applications; establishes, manages, and terminates
connections (sessions) between cooperating applications.
Transport
Provides reliable, transparent transfer of data between end
points; provides end-to-end error recovery and flow control
Network
Provides upper layers with independence from the data
transmission and switching technologies used to connect
systems; responsible for establishing, maintaining, and
terminating connections.
Data Link
Provides for the reliable transfer of information across the
physical link; sends blocks (frames) with the necessary
synchronization, error control, and flow control.
Physical
Concerned with transmission of unstructured bit stream over
physical medium; deals with the mechanical, electrical,
functional, and procedural characteristics to access the
physical medium.

The OSI Environment



Elements of Standardization

- Protocol specification
  - Operates between the same layer on two systems
  - May involve different operating system
  - Protocol specification must be precise
    - Format of data units
    - Semantics of all fields
    - allowable sequence of PCUs
- Service definition
  - Functional description of what is provided
- Addressing
  - Referenced by SAPs

OSI Layers (1)

- Physical
  - Physical interface between devices
    - Mechanical
    - Electrical
    - Functional
    - Procedural
- Data Link
  - Means of activating, maintaining and deactivating a reliable link
  - Error detection and control
  - Higher layers may assume error free transmission

OSI Layers (2)

- Network
  - Transport of information
  - Higher layers do not need to know about underlying technology
  - Not needed on direct links
- Transport
  - Exchange of data between end systems
  - Error free
  - In sequence
  - No losses
  - No duplicates
  - Quality of service

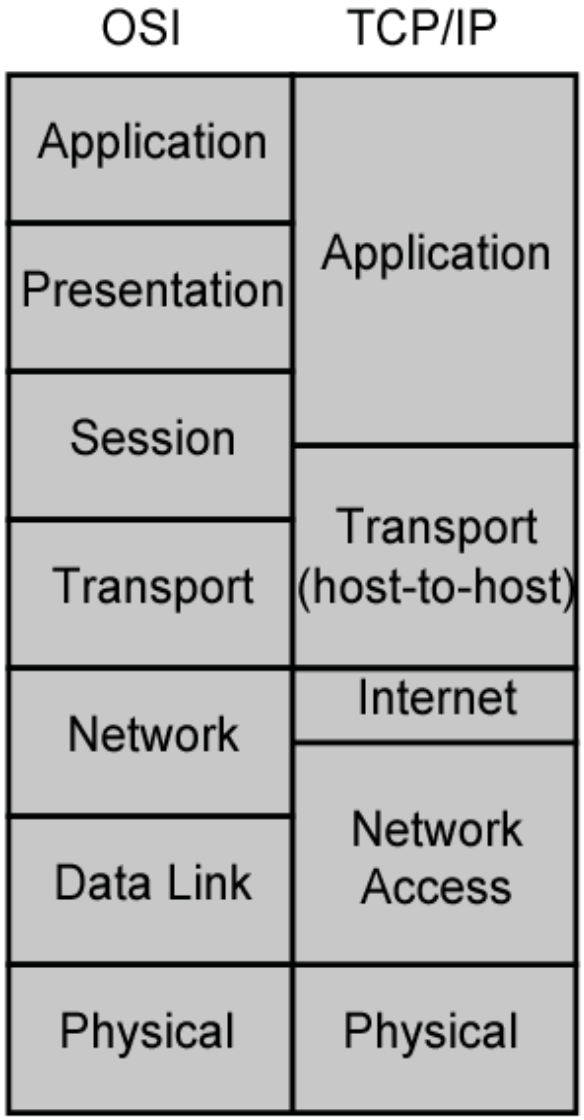
OSI Layers (3)

- Session
  - Control of dialogues between applications
  - Dialogue discipline
  - Grouping
  - Recovery
- Presentation
  - Data formats and coding
  - Data compression
  - Encryption
- Application
  - Means for applications to access OSI environment

TCP/IP Protocol Architecture

- Developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET)
- Used by the global Internet
- No official model but a working one.
  - Application layer
  - Host to host or transport layer
  - Internet layer
  - Network access layer
  - Physical layer

OSI v TCP/IP


OSI
TCP/IP
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport (host-to-host)
Internet
Network Access
Physical

TCP

- Usual transport layer is Transmission Control Protocol
  - Reliable connection
- Connection-Oriented
  - Temporary logical association between entities in different systems
- TCP PDU
  - Called TCP segment
  - Includes source and destination port (c.f. SAP)
    - Identify respective users (applications)
    - Connection refers to pair of ports
- TCP tracks segments between entities on each connection
- Example: FTP

UDP

- Alternative to TCP is User Datagram Protocol
- Not guaranteed delivery
- Connectionless
- No preservation of sequence
- No protection against duplication
- Minimum overhead
- Adds port addressing to IP
- Example: SNMP

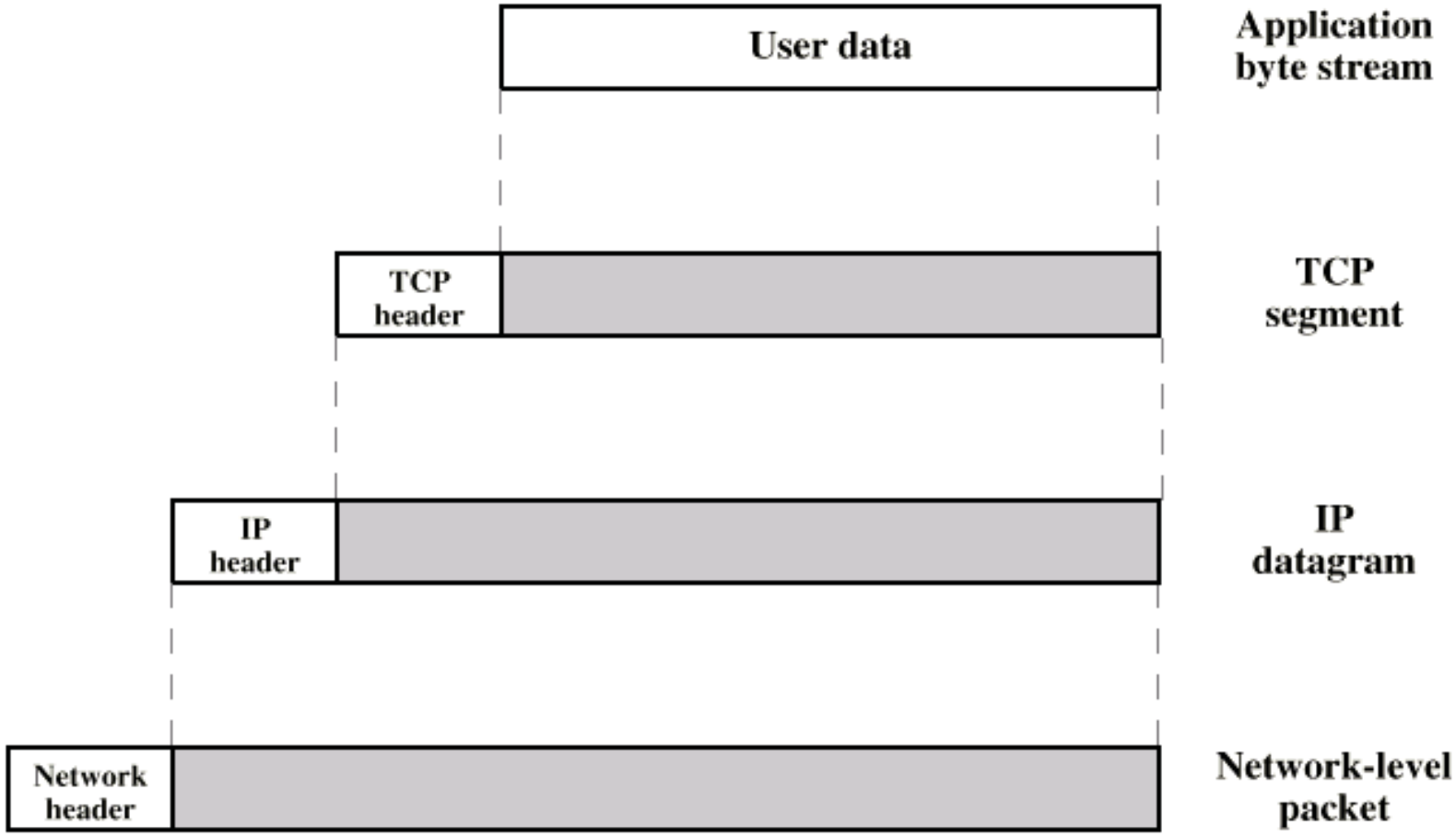
Addressing level

- Level in architecture at which entity is named
- Unique address for each end system (computer) and router
- Network level address
  - IP or internet address (TCP/IP)
- Process within the system
  - Port number (TCP/IP)

Trace of Simple Operation

1. Process associated with port 1 in host A sends message to port 2 in host B
2. Process at A hands down message to TCP to send to port 2
3. TCP hands down to IP to send to host B
4. IP hands down to network layer (e.g. Ethernet) to send to router J
5. Generates a set of encapsulated PDUs

PDUs in TCP/IP



OSI Security Architecture

- Originally specified as ISO 7498-2
- Republished as ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Aspects of Security

- Consider 3 abstract aspects of information security:
  - **security goal**
  - ↑
  - **security service**
  - ↑
  - **security control/mechanism**
- The purpose of security mechanism and services is to mitigate against and prevent attacks

High Level Security Services

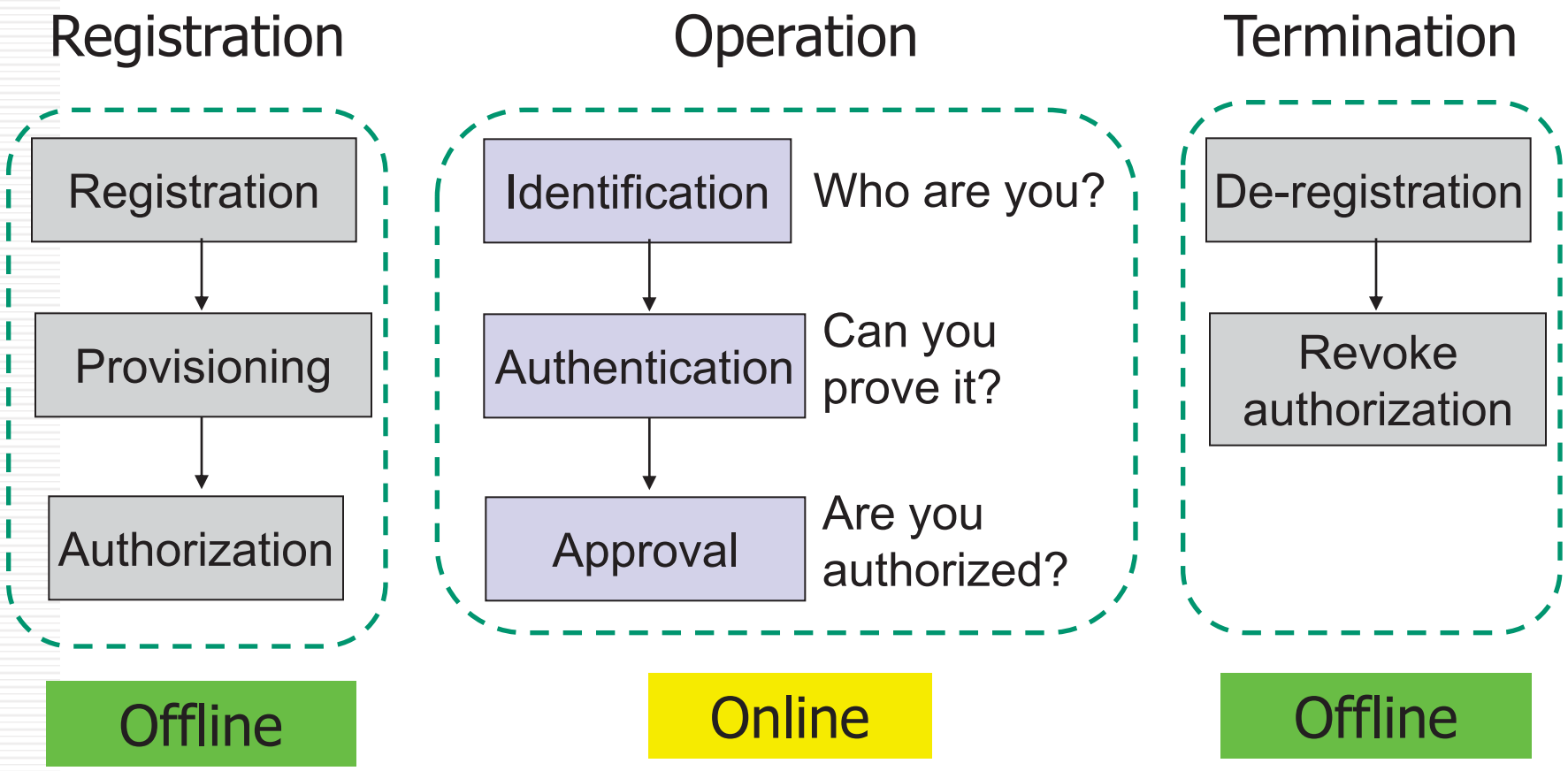
- The traditional definition of information security is to have preservation of the three CIA properties:
  - **Confidentiality**: preventing unauthorised disclosure of information
  - **Integrity**: preventing unauthorised (accidental or deliberate) modification or destruction of information
  - **Availability**: ensuring resources are accessible when required by an authorised user

Additional Services and mechanisms

The CIA properties apply to information, but are often inappropriate. e.g. for controlling usage of resources, for which additional security services are needed.

- Authentication:
  - **Entity authentication (user authentication):** the process of verifying a claimed identity
  - **Data Origin Authentication (message authentication):** the process of verifying the source (and integrity) of a message
- Non-repudiation:
  - create evidence that an action has occurred, so that the user cannot falsely deny the action later
- Access Control:
  - enforce that all access and usage happen according to policy

Access Control Phases



Confusion about Authorization

- The term “authorization” is often wrongly used in the sense of “access control”
  - e.g. *“to get authorized the user must type the right password”*
  - Common in text books literature
  - Specifications (RFC2904)
  - Cisco AAA Server (Authentication, Authorization and Accounting)
- Wrong usage of “authorization” leads to absurd situations:
  1. You steal somebody’s password, and access his account
  2. Login screen gives warning: *“Only authorized users may access this system”*
  3. You get caught for illegal access and prosecuted in court
  4. You say: *“The text book at university said I was authorized if I typed the right password, which I did, so I was authorized”*

Information States

- Information is considered to exist in one of three possible states:
  - Storage
    - Information storage containers – electronic, physical, human
  - Transmission
    - Physical or electronic
  - Processing (use)
    - Physical or electronic
- Security controls for all information states are needed

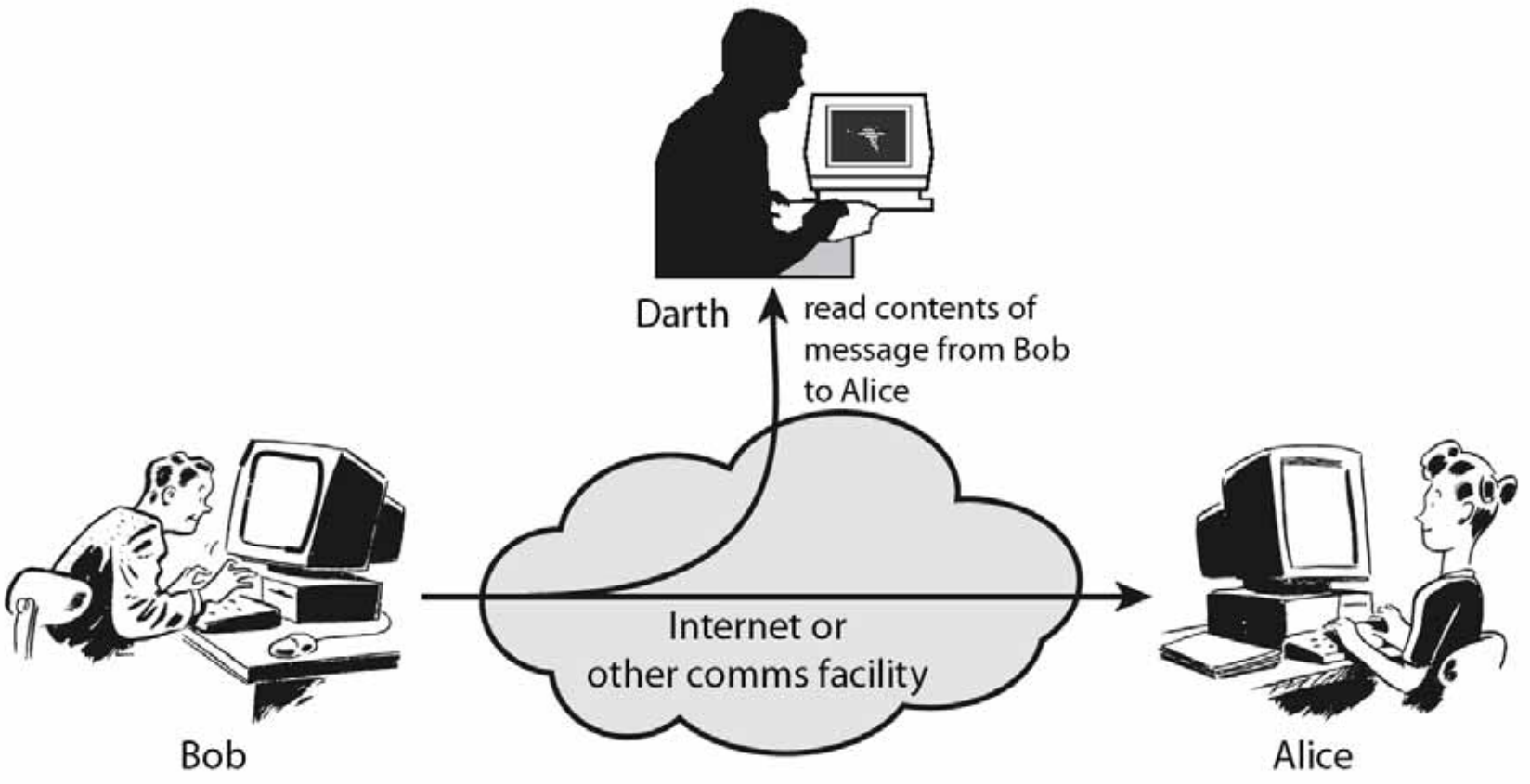
Threats, Vulnerabilities and Attacks

- Threat: Type of incident that can cause harm
  - e.g. virus infection
  - made possible through the presence of vulnerabilities
- Vulnerability: Weakness in a system that could allow a threat to cause harm
  - e.g. anti-malware filter outdated or not present
  - allows threats to succeed
- Attack: Deliberate attempt to realise threats by exploiting vulnerabilities
  - e.g. sending email infected with malware

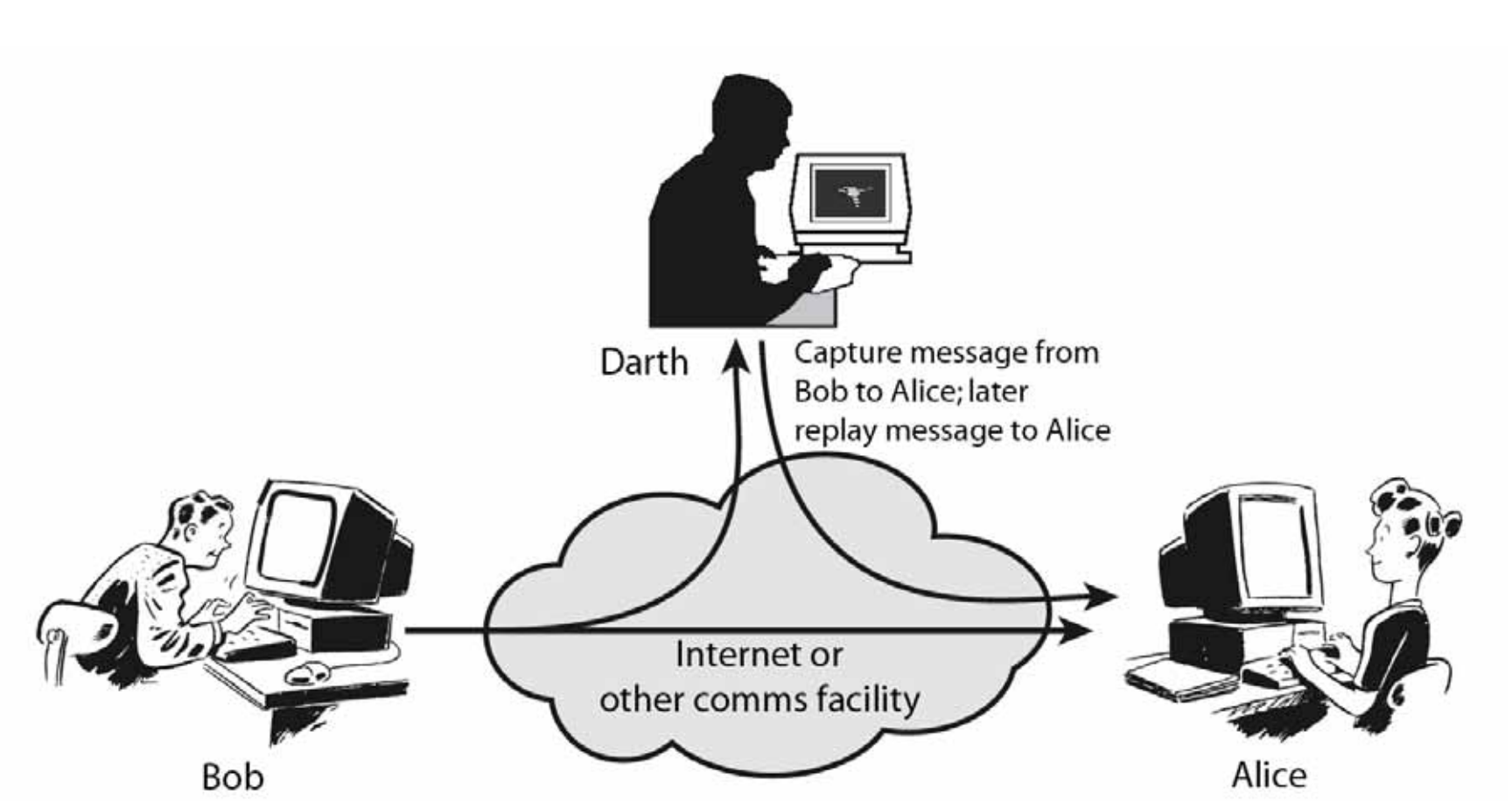
Threat/Attack Categories

- Four high level classes of threats:
  - Interception:
    - an unauthorised party gains access to information assets
  - Interruption:
    - information assets are lost, unavailable, or unusable
  - Modification:
    - unauthorised alteration of information assets
  - Fabrication:
    - creation of counterfeit information assets

Passive Attacks



Active Attacks



Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Metaphors

- Security professionals like metaphors
  - Digital signature
  - Electronic signature
  - Blind signature
  - Firewall
  - Certificate
  - Trust anchor
  - Key, Secret Key, Public Key, Private Key
  - Key ring
- Usability studies show that bad metaphors make people misunderstand
- Better to coin new term than to use a bad metaphor

Security Services

- X.800:
  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828:
  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Services (X.800)

TABLE 2/X.800

Illustration of the relationship of security services and layers

Service	Layer						
	1	2	3	4	5	6	7*
Peer entity authentication	·	·	Y	Y	·	·	Y
Data origen authentication	·	·	Y	Y	·	·	Y
Access control service	·	·	Y	Y	·	·	Y
Connection confidentiality	Y	Y	Y	Y	·	Y	Y
Connectionless confidentiality	·	Y	Y	Y	·	Y	Y
Selective field confidentiality	·	·	·	·	·	Y	Y
Traffic flow confidentiality	Y	·	Y	·	·	·	Y
Connection Integrity with recovery	·	·	·	Y	·	·	Y
Connection integrity without recovery	·	·	Y	Y	·	·	Y
Selective field connection integrity	·	·	·	·	·	·	Y
Connectionless integrity	·	·	Y	Y	·	·	Y
Selective field connectionless integrity	·	·	·	·	·	·	Y
Non-repudiation Origin	·	·	·	·	·	·	Y
Non-repudiation. Delivery	·	·	·	·	·	·	Y

Y Yes, service should be incorporated in the standards for the layer as a provider option.

· Not provided.

* It should be noted, with respect to layer 7, that the application process may, itself, provide security services.

Note 1 – Table 2/X.800 makes no attempt to indicte that entries are of equal weight or importance; on the contrary there is a considerable gradation of scale within the table entries.

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**
- hence our focus on this topic

TABLE 1/X.800

Illustration of relationship of security services and mechanisms

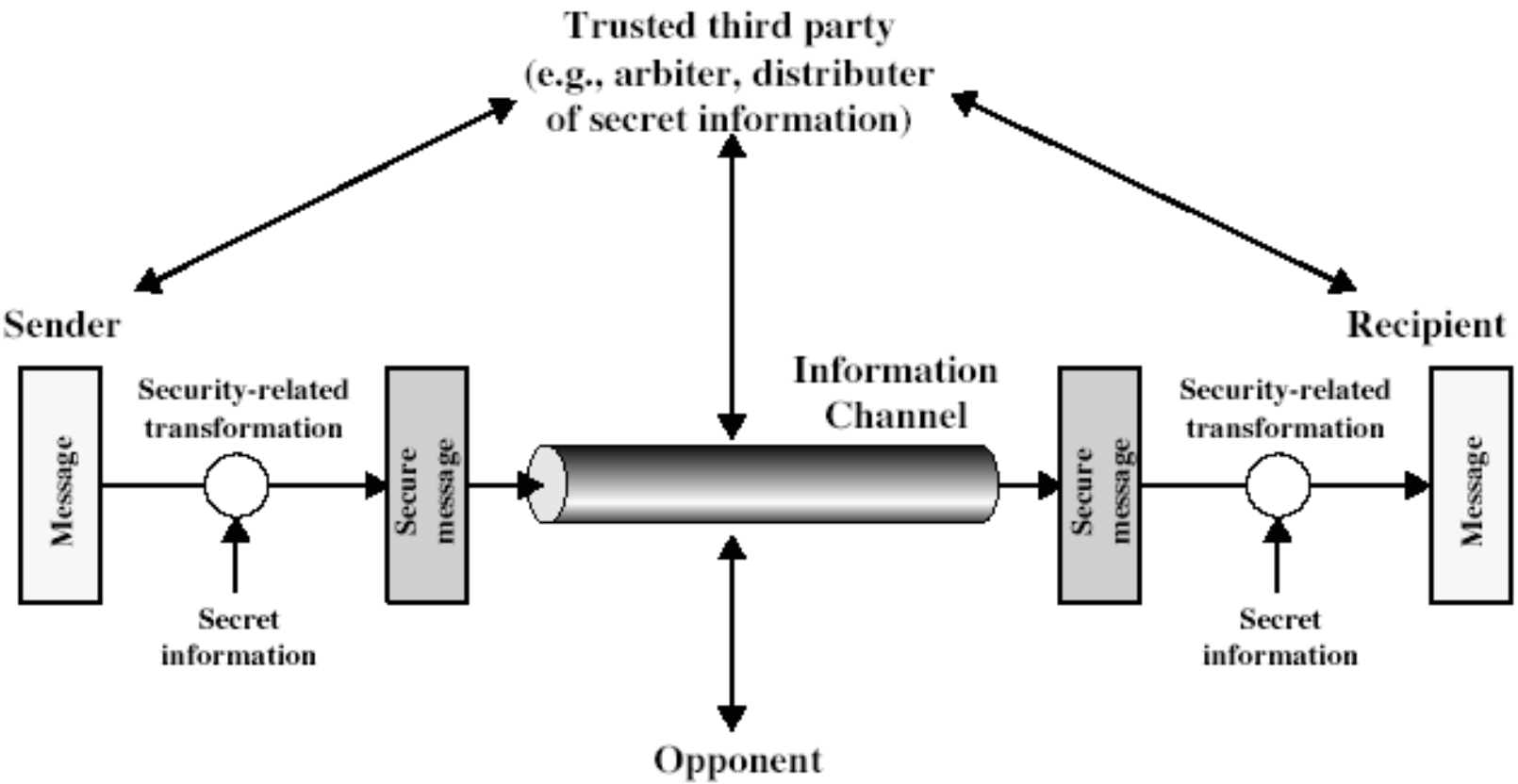
Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	.	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

· The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropiate, either on its own or in combination with other mechanisms.

Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

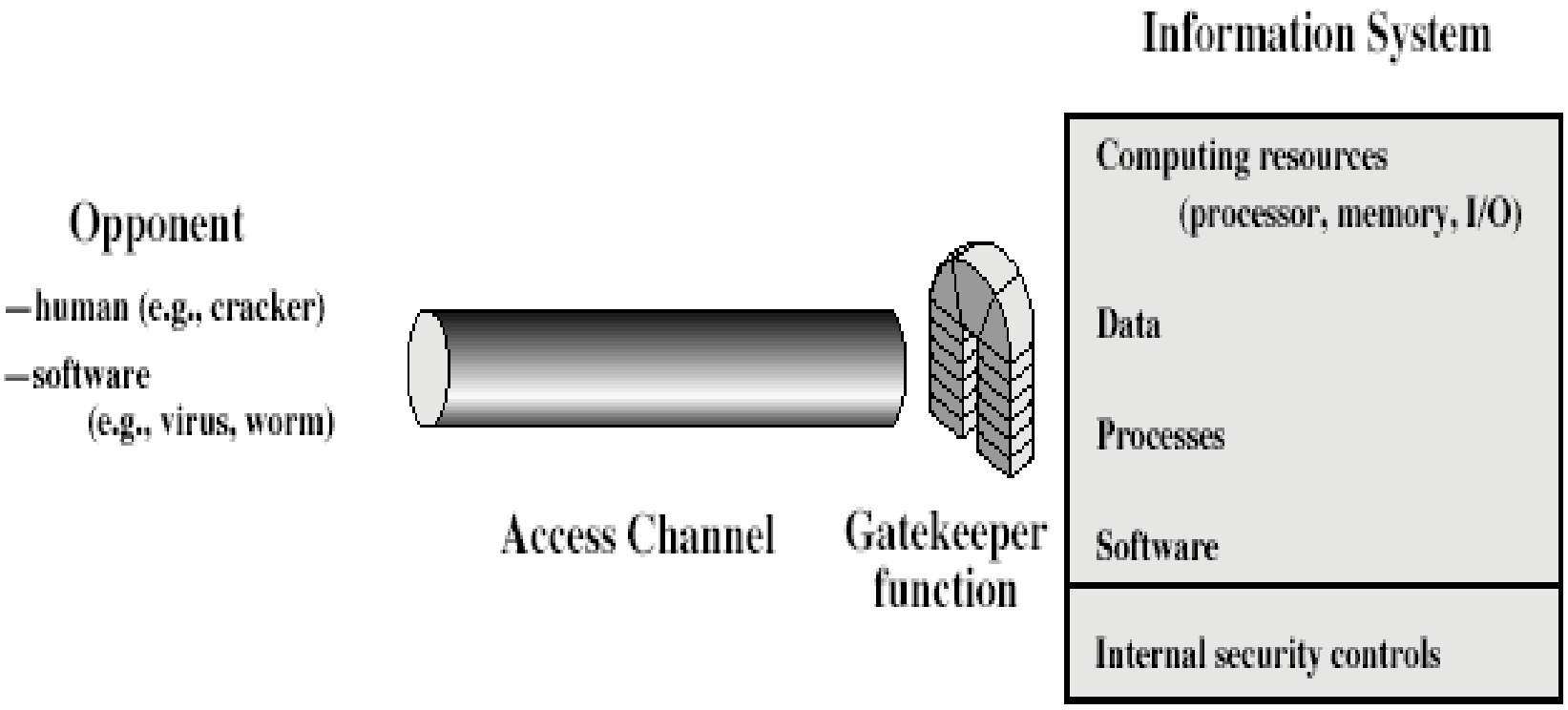
Model for Network Security



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
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- Using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- Trusted computer systems may be useful to help implement this model

Looking into the crystal ball for 2012

http://www.websense.com/content/webcast-what-security-threats-can-we-expect-in-2012-december-2011.aspx

End of Lecture