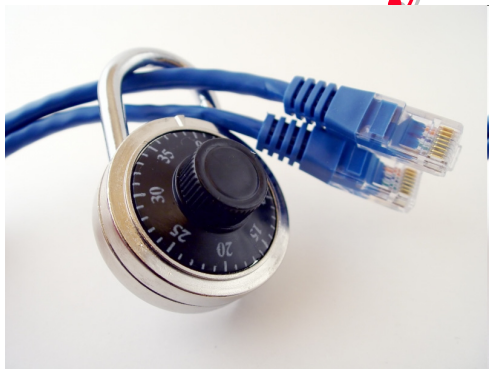
Cryptography and Network Security: Overview



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-11/

Overview

1. Computer Security Concepts
2. OSI Security Architecture
3. Security Attacks
4. Security Services
5. Security Mechanisms

These slides are based on Lawrie Brown's slides supplied with William Stalling's book "Cryptography and Network Security: Principles and Practice," 5th Ed, 2011.

Standards Organizations

- National Institute of Standards & Technology (NIST)
  http://csrc.nist.gov/
- Internet Society (ISOC):
  Internet Engineering Task Force (IETF), ietf.org
  Internet Architecture Board (IAB)
- International Telecommunication Union
  Telecommunication Standardization Sector (ITU-T)
  http://www.itu.int
- International Organization for Standardization (ISO)
  http://www.iso.org

Security Components

- **Confidentiality**: Need access control, Cryptography, Existence of data
- **Integrity**: No change, content, source, prevention mechanisms, detection mechanisms
- **Availability**: Denial of service attacks,
- Confidentiality, Integrity and Availability (**CIA**)

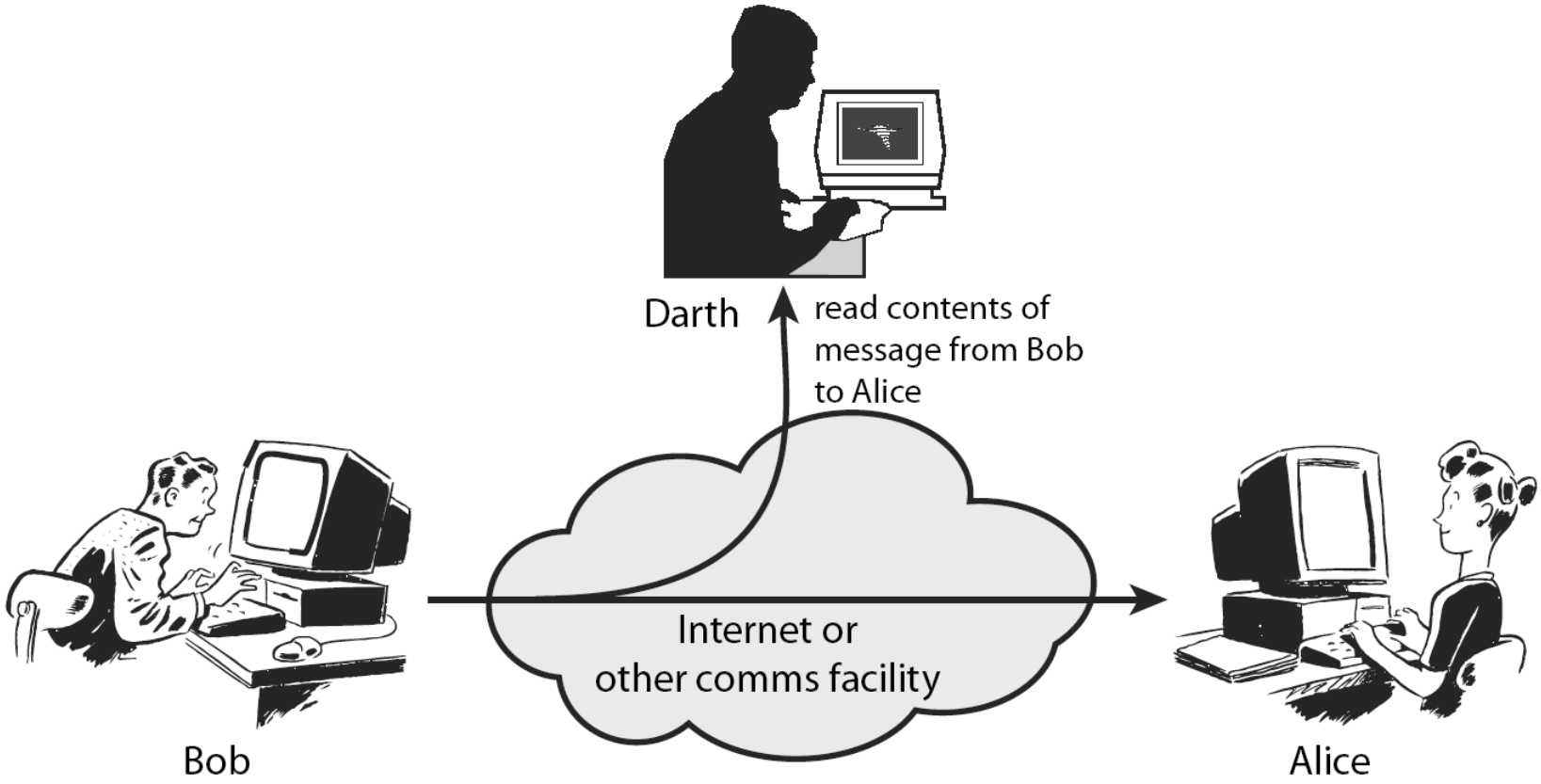
OSI Security Architecture

- ITU-T X.800 "Security Architecture for OSI"
- Defines a systematic way of defining and providing security requirements
- Provides a useful, if abstract, overview of concepts

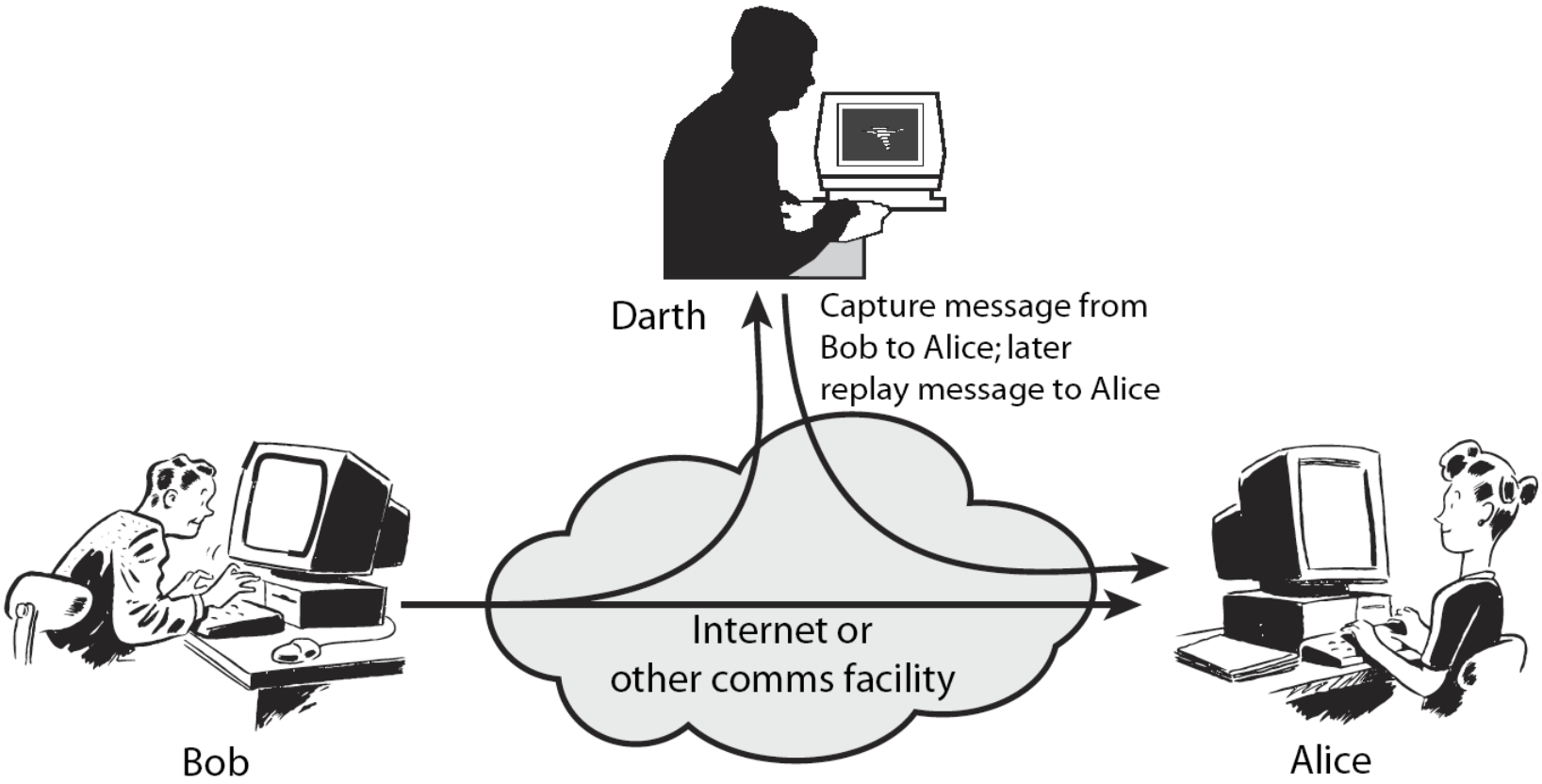
Aspects of Security

- Aspects of information security:
  - **Security attack**
  - **Security mechanism**
  - **Security service**
- Note:
  - *Threat* – a potential for violation of security
  - *Attack* – an assault on system security, a deliberate attempt to evade security services

Passive Attacks



Active Attacks



Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **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
- **Availability** – resource accessible/usable

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- However one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**

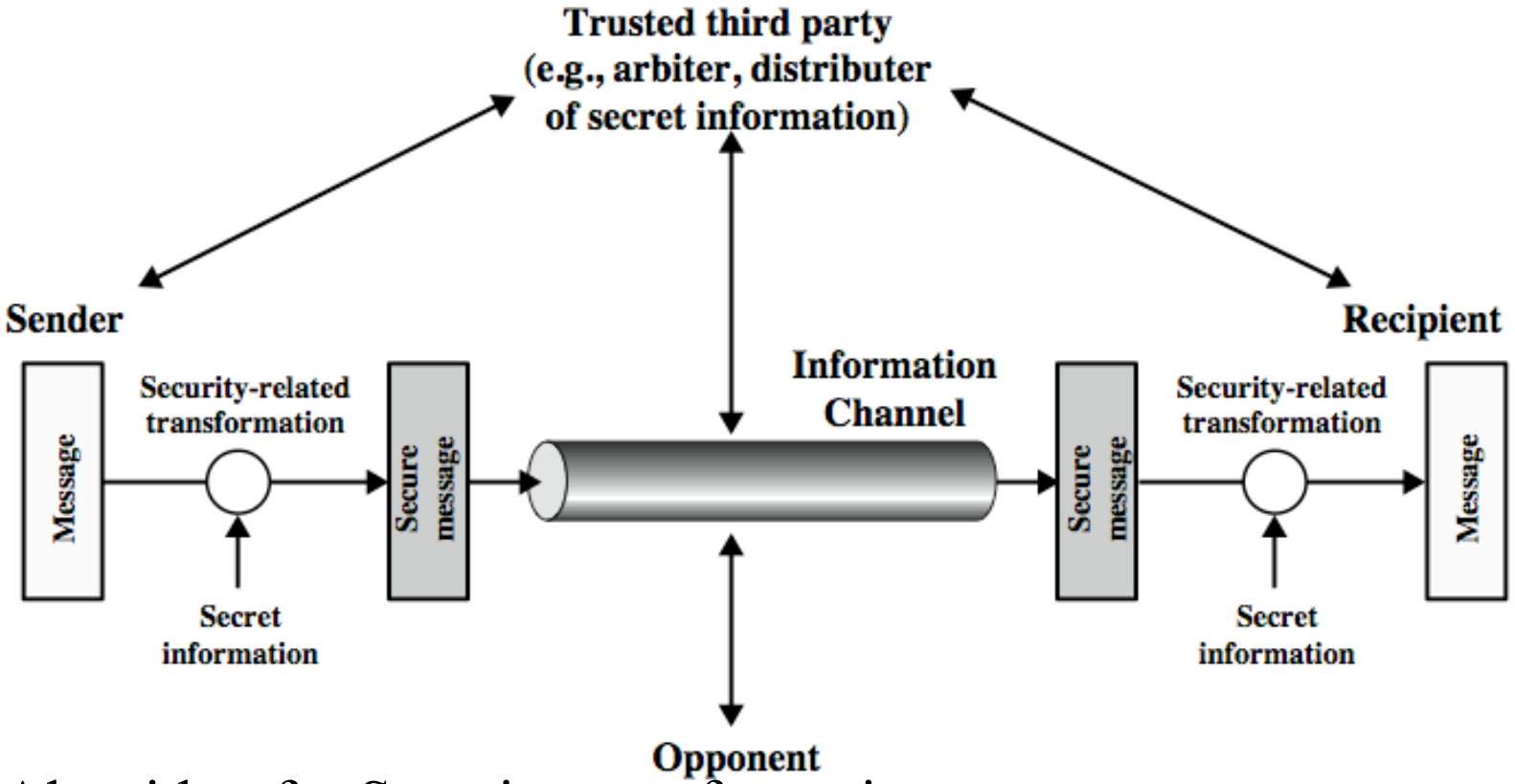
Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms:
  - Trusted functionality, security labels, event detection, security audit trails, security recovery

Services and Mechanisms Relationship

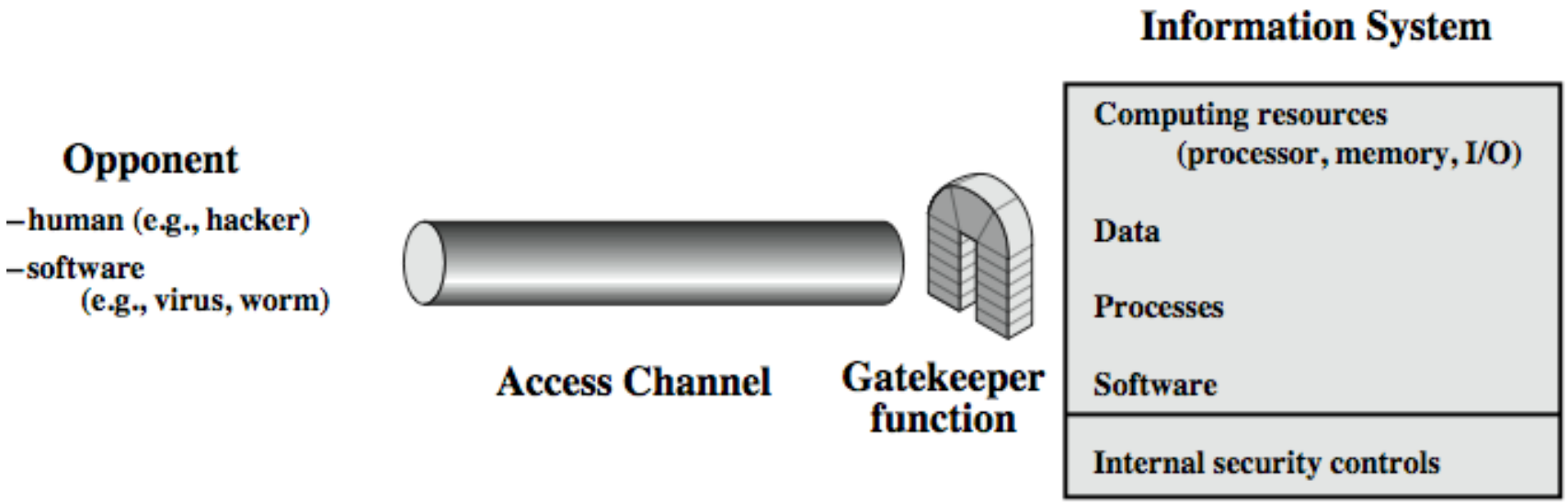
Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality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

Model for Network Security



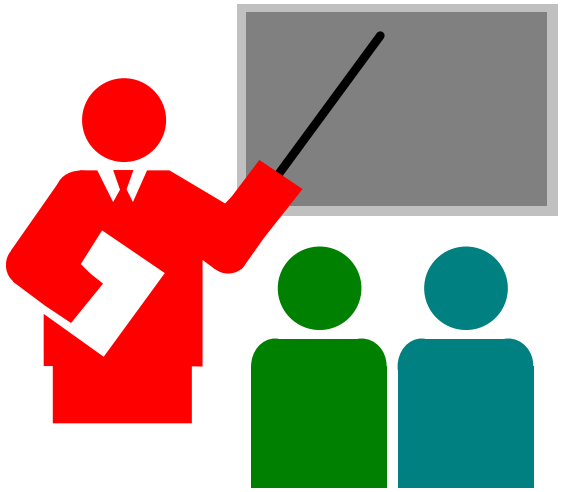
1. Algorithm for Security transformation
2. Secret key generation
3. Distributed and share secret information
4. Protocol for sharing secret information

Model for Network Access Security



1. Select appropriate gatekeeper functions to identify users
2. Implement security controls to ensure only authorised users access designated information or resources

Summary



- NIST, IETF, ITU-T, ISO develop standards for network security
- CIA represents the 3 key components of security
- ISO X.800 security architecture specifies security attacks, services, mechanisms
- Active attacks may modify the transmitted information.
- Security services include authentication, access control, …

Lab Homework 2

1. Read about the following tools
   a. **Wireshark**, network protocol analyzer, http://www.wireshark.org/download.html
      Use ftp client to download in binary mode (do not use browser)
   b. **Advanced Port Scanner**, network port scanner, http://www.scanwith.com/Advanced_Port_Scanner_download.htm
   c. **LAN Surveyor**, network mapping shareware with 30 day trial, http://www.solarwinds.com/products/lansurveyor/
2. Use advanced port scanner to scan one to three hosts on your local net (e.g., CSE571XPS and CSE571XPC2 in the security lab) to find their open ports.
3. Use network surveyor to show the map of all hosts on your local net
4. Ping www.google.com to find its address. Start Wireshark. Set capture filter option "IP Address" to capture all traffic to/from this address. Open a browser window and Open www.google.com . Stop Wireshark. Submit a screen capture showing the packets seen.

Security URLs

- Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu/about/history/coast/archive/
- IETF Security area, sec.ietf.org
- Computer and Network Security Reference Index, http://www.vtcif.telstra.com.au/info/security.html
- The Cryptography FAQ, http://www.faqs.org/faqs/cryptography-faq/
- Tom Dunigan's Security page, http://www.csm.ornl.gov/%7edunigan/security.html
- IEEE Technical Committee on Security and Privacy, http://www.ieee-security.org/index.html
- Computer Security Resource Center, http://csrc.nist.gov/

Security URLs (Cont)

- Security Focus, http://www.securityfocus.com/
- SANS Institute, http://sans.org/
- Data Protection resource Directory, http://www.dataprotectionhq.com/cryptographyanddatasecurity/
- Helger Lipmaa's Cryptology Pointers, http://www.adastral.ucl.ac.uk/%7ehelger/crypto/

Newsgroups and Forums

- sci.crypt.research, sci.crypt, sci.crypt.random-numbers
- alt.security
- comp.security.misc, comp.security.firewalls, comp.security.announce
- comp.risks
- comp.virus
- Security and Cryptography Forum, http://forums.devshed.com/security-and-cryptography-17/
- Cryptography Forum, http://www.topix.com/forum/science/cryptography
- Security Forum, http://www.windowsecurity.com/
- Google groups, http://groups.google.com
- LinkedIn Groups, http://www.linkedin.com