INFO 6001: Information Security

Week 1: Introduction

FANSHAWE

Steve Spencer

- Professor, Curriculum Developer - School of IT. My bio is posted On FOL in Getting Started along with Course info and **Communications Expectations** **<< Read this!**

I'm available via:

- Discussion forum, posts to subscribed Topics generate a notice to my email with details.
- Student Support Session: Virtual Classroom every Friday 10 AM to Noon.
- e-mail - **sspencer@fanshaweonline.ca** **as per the Communication Expectations…**

An example – FOL email subject line must be edited:
A student in Section 2 for 23 Winter with a double cipher transposition question
= Subject: "**INFO-6001-02-23W**: double transposition cannot decrypt"

Only ***your*** course and section information should remain in the subject – this is easy! I have 150+ students and get a *lot* of e-mails, an **accurate subject line** makes triaging and not losing important e-mails simpler. I have to do this for my sanity and your service.

Mystery email will get viewed last (if at all).

What is Fanshawe Online?

- Fanshawe Online INFO-6001 is the course website.
  - Home Page: https://www.fanshaweonline.ca/d2l/home/1425466

- Everything related to your course will be posted there

- Sections in the course FOL page include:
  - Announcements (on main page – click the course title)
  - Course Plan
  - Content (lesson slides, recordings, and resources),
  - Discussion Forum (DF)
  - Evaluations (incl. grades, labs),
  - Submissions – “drop-boxes” do not close
  - FOL email

Agenda
What will we Discuss in this Lesson?

- The Routine

- Course Plan
- Course Outline
- General Course Overview

- Lesson / Discussion: Week 1: Chapter 1

The Routine – Lesson Sessions

- Recorded **Lessons** (aka lectures) will begin with "Housekeeping".
  - Usually administrative items and need-to-know notices
  - There will be a Status Page to review where we are in the Course
    - What Week & Chapter we are at, assessments completed, assessments due, etc
- I will discuss any questions stemming from the previous week, and highlight and particularly helpful Discussion Forum posts.
- The lesson **includes activities** for your to complete as part of the lesson.
- **Come prepared for class**
  - **Do the readings, write down your questions, read the slides completely when I do not – pause the recording and view the posted Lesson .pdf**
- **Be prepared to participate!**
  - **Even though we are working online, we can still work in groups, engage in class discussions, take up scenarios, do some online collaboration activities, and more**
- Will conclude each lesson with an invitation for **questions** and reminders for the next steps

The Routine – Lab Sessions

- **Lab Sessions** are *mandatory synchrono*us classes for all Full Time (FT) students.
  - Attendance and time is automatically taken by Bongo.
- W will discuss any questions stemming from the week's Lesson, and highlight any particularly helpful Discussion Forum posts.
- We will review the **Lab Assignment** for the week and **get it done**.
- The Lab Sessions will be recorded so that Online (OL) and Part-time (PT) students can use them as their asynchronous Lab time.
- For FT students, Labs are due by 1 hour after the scheduled session.
- If you have submitted the Lab early, you may ask to leave the session.
- For OL and/or PT students, the Lab is due by 11:30 PM the next day.

The Routine – Lab Sessions, *continued*

- For OL and/or PT students, the Lab is due by 11:30 PM the next day (Friday night)
- All Late submissions will be deducted at *20% of marked value per day* or portion thereof.
- The session will be informal and consist of back & forth clarifying and working out the problems. There will be quiet stretch's and a white board for tracking will be visible as we work.
- Lab Sessions with no Assignment for the Week will be covering *additional Lesson content and Textbook work.* This content will also be on the tests.
- The weekly Student Support Session for INFO6001 will be 10 AM to 12 PM Fridays.

The Routine – Lesson & Lab Sessions

- **Come prepared for class**
  - **Completely review the recorded Lesson, write down your questions and have them ready to ask.**
- **Be prepared to participate!**
  - **Remember that both Class and Discussion Forum participation is 10% of the Course Marks**

Recorded Sessions

- Virtual Classroom Session Listing is under FOL **Media Tools.**
- After a session, the VC meeting link will move from Active Meetings to the Recorded Meetings. After a short wait, you can Preview the session.
- Lesson links and pdf Slide decks will usually be available under the appropriate week in FOL **Content** section. If not, remind me.

- If the **recordings are not playing** correctly, what do you do?
  - Make sure you have the correct Browser / Java combo
  - Close down any background tasks
  - Check the audio settings
  - Call the Fanshawe IT Service Desk (519-452-4430 x4357) or you can email.
  - If all else fails, please notify me by email (correct subject line!)

Course Plan and Course Outline

FANSHAWE

Course Design: INFO 6001

- 4 hours/week
  - 2 hrs Lesson time and 2hrs Lab time

- Class time will consist of:
  - 50% - Discussions, Lectures and Exercises
  - 50% - Lab time
    - This will be the time you spend working on the labs, taking screenshots of your work, and creating your submission file (usually a .ppt file)

- Lab Sessions with no Assignment for the Week will be covering *additional Lesson content and Textbook work.* This content will also be on the tests.

Course Plan

- The approved week-by-week Course Topic and Evaluation Schedule. Hopefully this will be approved & posted by next week.

- Available exclusively in the Course Outline Section at the top of the FOL Content List

- This should be the top page in your course folder or binder.
  - Please do not ask any **topic, scheduling or eval questions** until you check.

- It is SUBJECT TO CHANGE as the Course Progresses
  - You will be notified by email when this occurs.
  - The Course Plan is the latest source of information.

FANSHAWE

Engage, Empower, Excite, Educate

COURSE PLAN

COURSE TITLE: Information Security	
COURSE CODE: INFO 6001	***SCHOOL: ITY***
Course Section(s): All	
Program: Information Security Management	
Duration: 14 weeks	
Term: 2022 ☐ Fall ☒ Winter ☐Summer	
Prepared by: Steve Spencer	

COURSE PLAN

The Course Plan provides an outline of topics that support the course learning outcomes and essential employability skills. It also provides an overview with respect to the scheduling of topics, required preparation for each topic and corresponding learning resources and evaluation items. Using the course plan will help you manage your time to get the most from the course and complete the evaluation items on time.

Lesson	*Topic*	*Delivery Details*	
		Preparation and/or Learning Resource(s)	*Evaluation*
1	Introduction to Network Security.	*Network Security Essentials by W Stallings. 6ed, Pub: Pearson.*	*Lab Assignment #1*
2	Symmetric Encryption & Message Confidentiality		*Lab Assignment #2*
3	User Authentication (Public Key cryptography & message authentication).		*Lab Assignment #3*
4	Key Distribution & User Authentication		

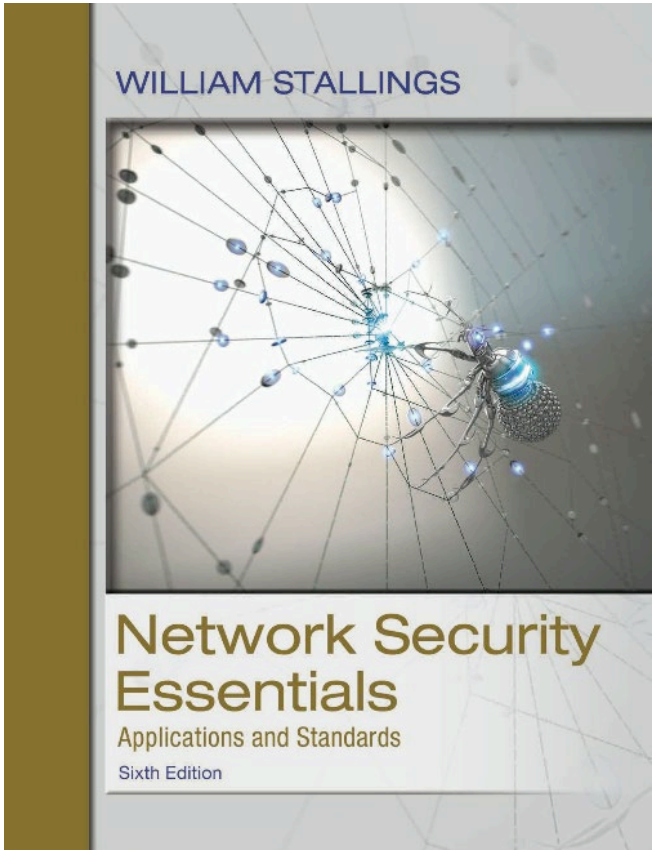
5	**Test #1**		***15%***
6	Network Access Control and Cloud Security.		*Lab Assignment #4*
7	Transport Level Security.		
8	Wireless Security.		*Lab Assignment #5*
9	Email Security.		
10	**Test #2**		***20%***
11	IP Security.		*Lab Assignment #6*
12	Malicious Software.		*Lab Assignment #7*
13	Malicious Software and Perimeter Protection.		*Lab Assignment#8*
14	Review & **Test #3**		***25%***
	Class and online discussions	Class and online discussions	***10%***
	Labs and Reflection		***30%***

The Course Plan may change according to students' learning needs and/or unanticipated disruptions. You will be notified of any significant change via FOL prior to changes being implemented as specified in Policy 2-B-10.

Course Outline

- This document is NOT Subject to Change
  - However, any deviations to topics, scheduling or evaluations as determined by the Professor will be in the Course Plan.
- Assessment / Evaluations values:
  - 8 Practical Labs: total of 30% (3.75% each)
  - Discussions and Participation: 10%
  - 3 unit tests: total of 60% (15%/20%/25%)
    - The Course itself is Cumulative, so the Tests are not Cumulative.
- Scheduling is in *the Course Plan*
- Course Textbook is "***Network Security Essentials***" **Sixth** Edition
  - by William Stallings. Resources available at http://williamstallings.com/NetworkSecurity/
- *You should also consider using*:
  - Other **online resources** (articles, news items, forums, vendor manuals, etc.)
  - Instructional **videos**
  - Find scenarios and case studies and **apply** what you are learning to those cases

Required Text



Network Security Essentials

(6th Edition)

Author: William Stallings

Publisher: Cengage Learning

- *This text is easy to find but previous editions are better than nothing!*
- *E-books are even easier to "find"… (ahem)*

Course Outline – Evaluating your work

- Missed Assignments and Tests
  - Tests are password protected
  - Tests will have a designated start time. You must start within 15 minutes of the assigned test opening – the Password will be changed at that point.
  - Students are **not entitled** to complete missed tests
  - In case of a significant event supported by documentation AND professor's approval AND prior notification, a missed test may be completed.
  - Proof of Alien Abduction is required for any post schedule notification!

- Re-writes & extra grade items
  - Students will **not be permitted** to rewrite tests
  - Students will **not be entitled** to extra work or assignments in order to raise a grade

- Assignments require screenshots to show your work. Your name in the screenshot is required. I prefer a screenshot of your whole screen – not just one window. (Please close any NSFW materials!)

Course Outline Document

Course Learning Outcomes

Upon successful completion of this course, you will be able to reliably demonstrate the following Course Learning Outcomes which will be taught and evaluated:

1.) Analyze the actions of social engineering tools and malware such as viruses, worms and Remote Access Trojan programs in terms of actions and ability to infect computer and network systems.
2.) Evaluate the different encryption algorithms and compare the methods used by symmetric and asymmetric encryption algorithms to protect and secure user data.

3.) Examine how encryption and hash algorithms are used with Digital Certificates and Digital Signatures.
4.) Create secure passwords and evaluate security policies that can resist password guessing attacks.
5.) Compare the difference between the SSL/TLS and SSH protocols for secure communications.
6.) Analyze the methods used by hackers to attack computer networks.
7.) Compare the actions taken by the different types of TCP/IP based network attacks.
8.) Evaluate the processes used in the RADIUS and Kerberos protocols to implement Authentication, Authorization and Accounting services to provide access control.
9.) Analyze the operation of wireless networks and how the IEEE802.11i protocol addresses security issues for authentication and data confidentiality.

Important Course Outline details..

- Missed Tests
  - Students are **not entitled** to complete missed tests
  - In case of a significant event supported by documentation AND professor's approval AND prior notification, a missed test *may* be completed
- Re-writes & extra grade items
  - Students will **not be permitted** to rewrite tests
  - Students will **not be entitled** to extra work or assignments in order to raise a grade

Course Overview

FANSHAWE

Information Security - Course Positioning Overview

- **This is the "macro" class in ISM**.

FIRST…

- We will cover most common InfoSec Methodologies from a *management perspective*
- A good structure for this wide coverage is BCM.
- **BCM** – Business Continuity Management consists of :
  - Definition, Need, Best Practices, Tools
  - Business Impact Analysis - InfoSec
  - Contingency Planning – Availability with InfoSec & maintenance of Plans
  - Implementing a Information Security Management System (**ISMS**)
  - Planning, Planning, & more planning for avoiding bad outcomes
  - Policy design, procedures, delivery, education, training,
  - Disaster Avoidance and Disaster Recovery

NOW…

- The ISM Program already has the complete occupational focus on InfoSec / NetSec by adopting the CISSP certification path and the CISSP course.
- SO our chosen text has a focus in the **security *implementation*** in each technology by examining the common solutions, protocols and the Cryptography behind each.

How will you be evaluated in this course?

Testing! There are THREE tests in this course (worth a total of 60%)

- For FT Students, ALL Tests are taken during the scheduled Lab period.
- For OL & PT students that cannot make the Lab Session, Tests are taken in the weekly Friday Student Support Session + An Alternate test time is made available.
- Written quizzes and exams use the **Respondus Lockdown Browser and Monitor.**
- ***NOT OPEN BOOK***, but you will have access to the course lecture slides
- *Any method* may be used to test the class
  - Short answer, long answer, M/C, T/F, FIB, Matching,
- Working AND tested PC or laptop. A sample "check" quiz with Monitor is posted.
- Recommend to use wired ethernet LAN connection (RJ45 patch cable) and a plugged-in power supply (*Respondus does not like blips or long latency!*)
- Expect an average time of 30-60 seconds per question
  - *(you won't have time to look everything up, so study as though you didn't have the slides)*
- Testable material includes anything discussed "in class" (both verbally and on the slides), in discussion forums, in the textbook, any articles or resources I share, and in the labs.

Note: Test time lost due to PC problems is not recoverable – use the check Quiz

Assignments (Labs)

- Hand in ALL assignments/Labs on time. ***Late penalties apply***.
- Put the assignment name and your FOL-ID in the file name
  - (ex. LRobertson12345_Lab1.pptx) Do not use your student number.
- Assignments need a title page/slide that includes 5 things:
  - your name, student number, course code, assignment number, and date
- All assignments submitted via FOL in the correct submission box
  - **Assignments submitted in any other method (including email) will not be accepted**
  - Assignments submitted using the wrong submission box will not get graded.
  - Submission drop-box is open at the beginning of the Lab session and does not close. The due date for you is the noted time, e.g. 5:00 PM or 11:30 pm. You must submit before this time or your submission is marked late.
- Assignments must be submitted uncompressed (no archive files), and using PowerPoint or Word files (not .pdf).
- Use this command in *every* screenshot: `whoami & date /t & time /t`
- **Ensure that your VM and/or host name has a personal identifier.**

How to be successful in this course…

- This is a "**Lecture and Lab style" class**, so I suggest you take notes during the recorded lecture
- *Do not underestimate* the work required for this course
  - Online ≠ easy!
- Slides are a HANDOUT that highlights key points, but they do not cover all you need to know.
- Not all concepts are fully explained on the slides
- Everything in the lessons / resources / exercises is fair game for the tests.
- **Ask questions** if you don't understand something – **you likely won't be the only person.**
- Memory alone will not suffice. Understanding and application are key!!

Student Success

- Show respect for your professor and your peers
  - **Be active and participate** in online class discussions
  - **HELP EACH OTHER**. Create your own study groups (or use the discussion forum). Some of you may solve problems faster than your peers – share your success by showing them how!
- **Prepare properly** for lectures and tests
- Do all the required **and recommended** work
- Do not miss tests
- Read and understand the assignment **rubrics**!

Chapter 1

Introduction

This week's learning outcomes

1. Describe the key security requirements of confidentiality, integrity, and availability
2. Describe the security architecture for OSI
3. Discuss the types of security threats and attacks
4. Explain fundamental security design principles
5. Discuss the use of attack surfaces and attack trees
6. List and describe some key organizations involved in cryptography standards

Computer Security Concepts

- Before the widespread use of data processing equipment, the security of information valuable to an organization was provided **primarily by physical and administrative means**
- With the introduction of the computer, the need for **automated tools for protecting files** and other information stored on the computer became evident
- Another major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer
- **Computer security**: The generic name **for the collection of tools designed to protect data and to thwart hackers**
- **internet security** (lower case “i” refers to any interconnected collection of networks) aka “NetSec”
  - Consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Computer Security

- The NIST *Computer Security Handbook* defines the term computer security as:

> "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes **hardware**, software, firmware, information/data, and telecommunications)"

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad

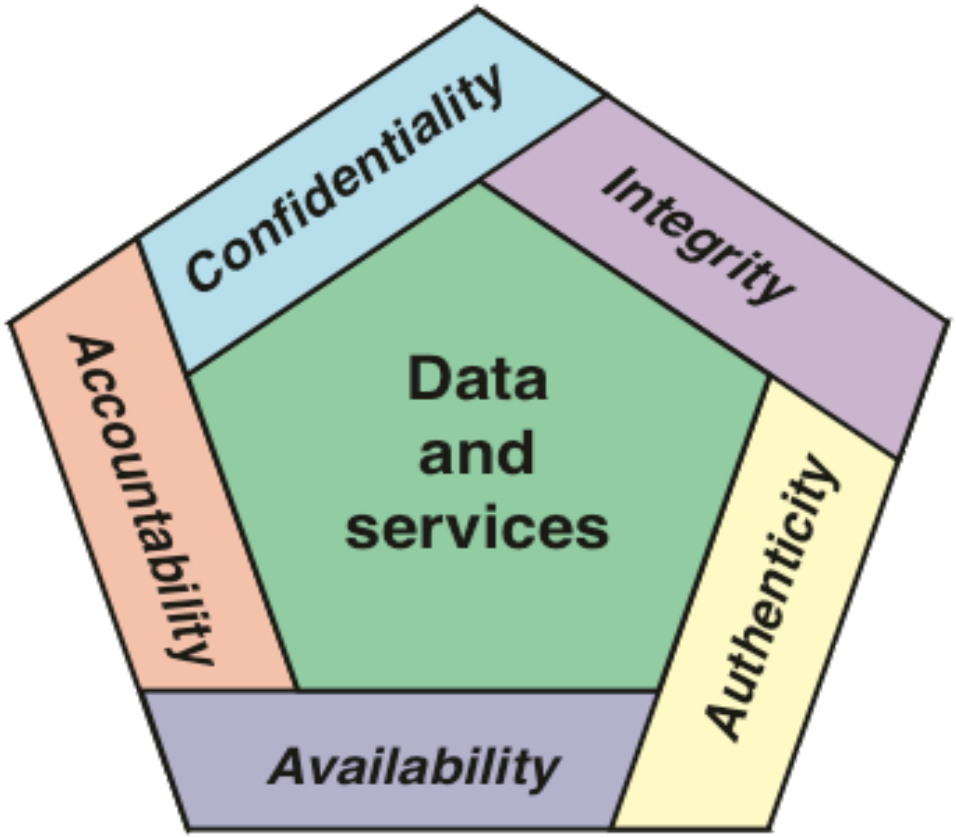


Figure 1.1 Essential Network and Computer Security Requirements

Possible additional concepts:

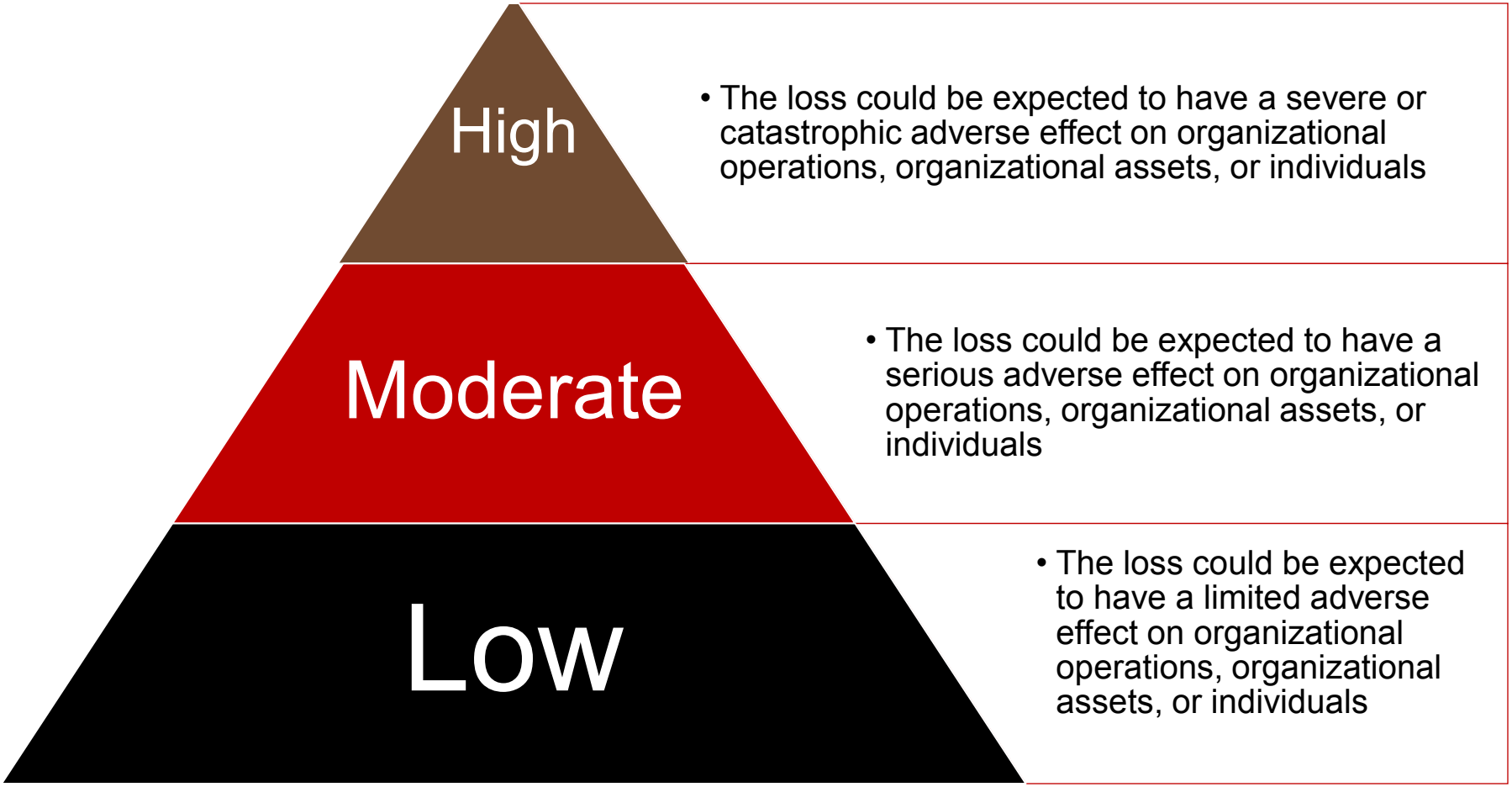
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security Levels of Impact



Examples of Security Requirements

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

Regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous online poll

Availability

The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

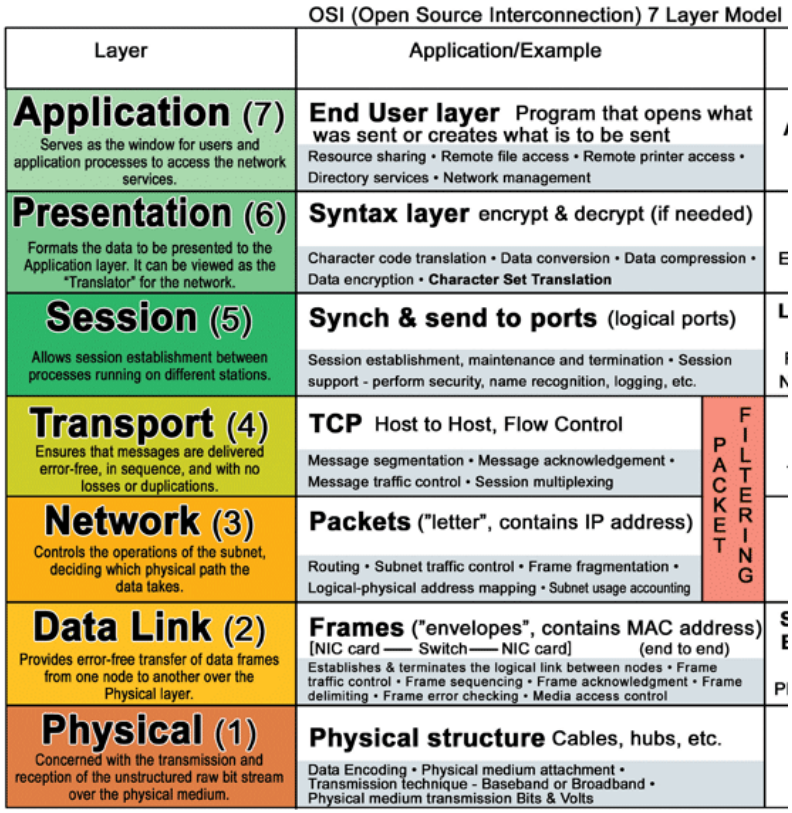
An online telephone directory lookup application would be classified as a low-availability requirement

Computer Security **Challenges**

- **Security is not simple or easy**
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought

- Security mechanisms typically involve more than a particular **algorithm** or protocol
- Security is essentially a **battle of wit$** between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

OSI Network Model



OSI Security Architecture

- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Table 1.1
Threats and Attacks (IETC RFC 4949)
Internet Security Glossary, V2

Threat

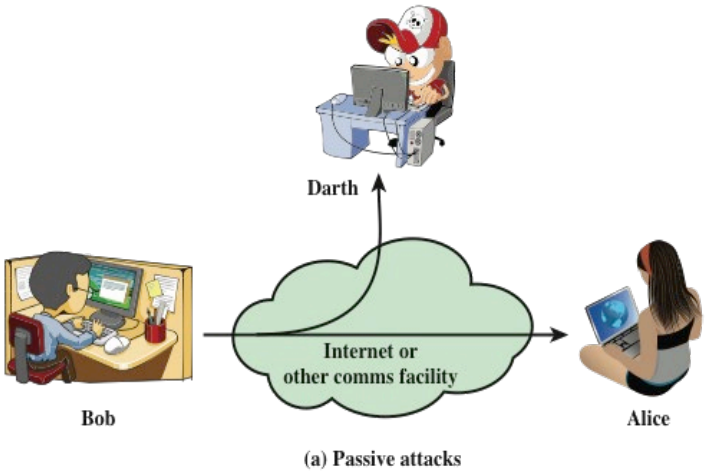
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

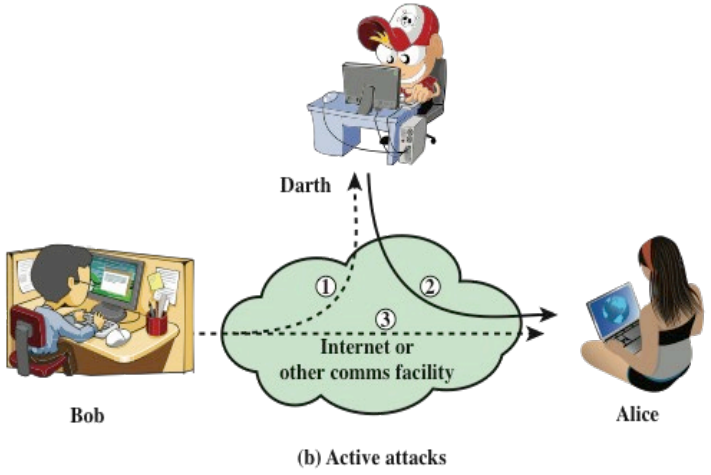
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A ***passive attack*** attempts to learn or make use of information from the system but does not affect system resources
- An ***active attack*** attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Figure 1.2 Security Attacks

Passive Attacks

- Two types of passive attacks are:
  - Reading content: The release of message contents
  - Monitoring traffic: Traffic analysis

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

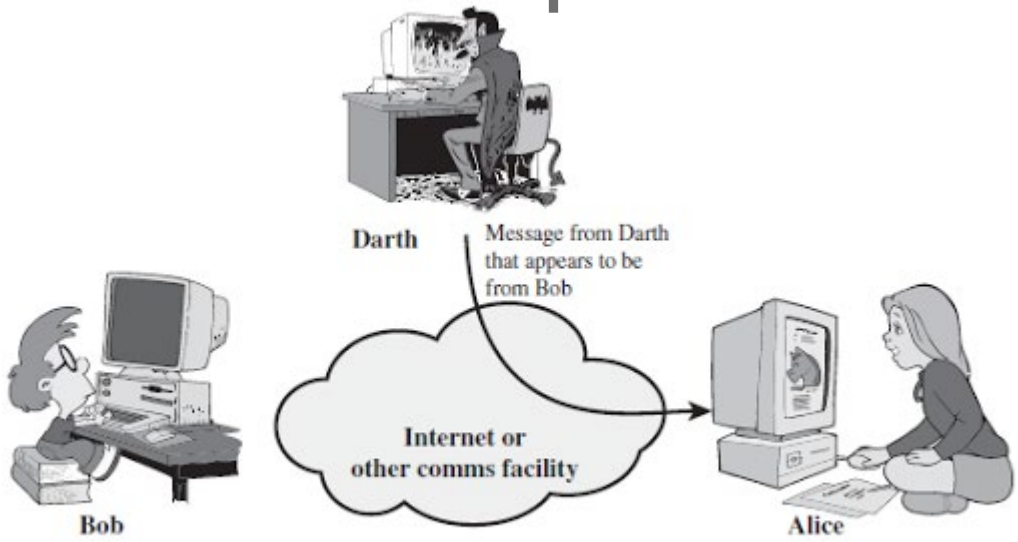
Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Active Attack: Masquerade



(a) Masquerade

Takes place when one entity pretends to be a different entity

Active Attack: Replay

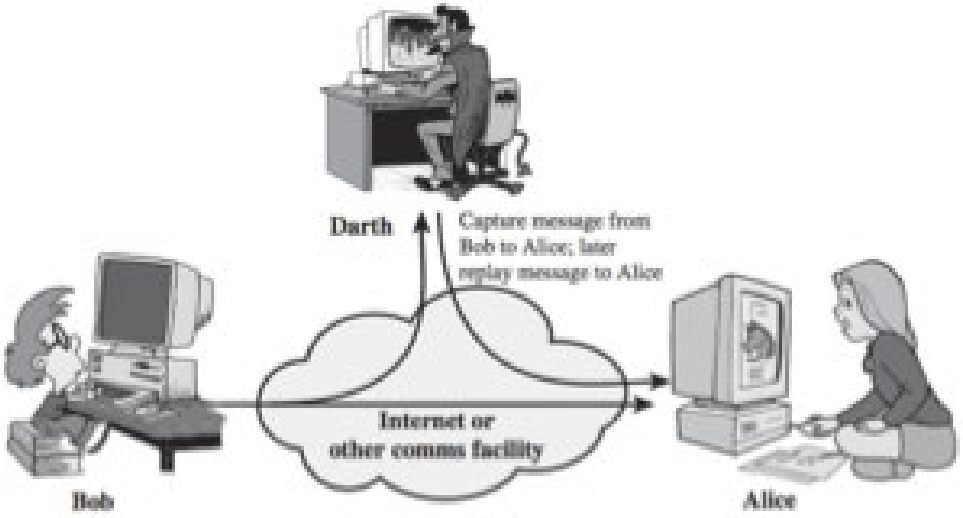
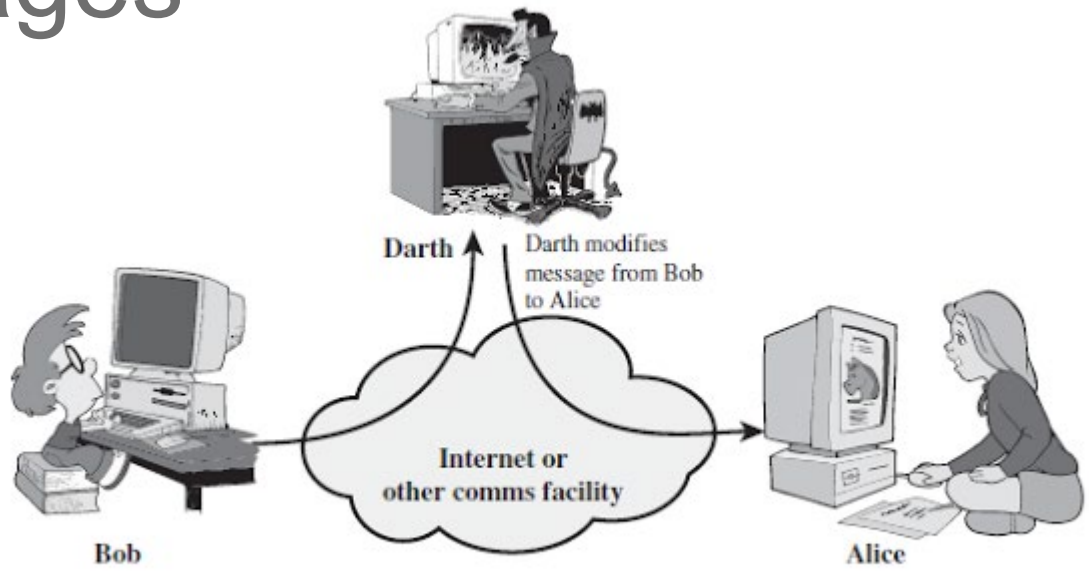


Figure 1.7 Replay

Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

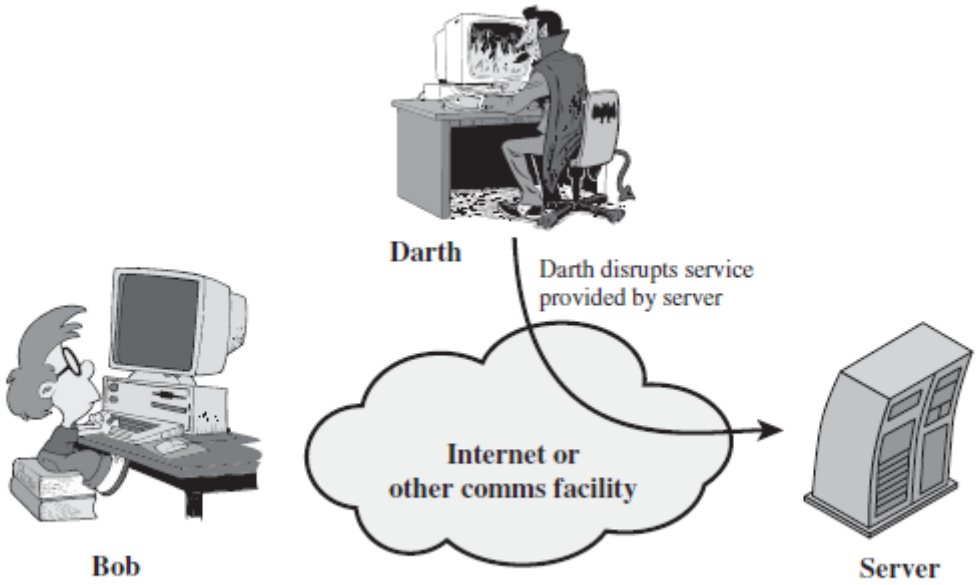
Active Attack: Modification of Messages



(c) Modification of messages

Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Active Attack: Denial of Service



(d) Denial of service

Prevents or inhibits the normal use or management of communications facilities

Security Services

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

AUTHENTICATION	DATA INTEGRITY
The assurance that the communicating entity is the one that it claims to be.	The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.	**Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.	**Connection Integrity without Recovery** As above, but provides only detection without recovery.
ACCESS CONTROL	**Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).	**Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
DATA CONFIDENTIALITY	**Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
The protection of data from unauthorized disclosure.	**NONREPUDIATION**
Connection Confidentiality The protection of all user data on a connection.	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Connectionless Confidentiality The protection of all user data in a single data block	**Nonrepudiation, Origin** Proof that the message was sent by the specified party.
Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.	**Nonrepudiation, Destination** Proof that the message was received by the specified party.
Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.	

Table 1.2

Security Services X.800 – (1991)

(This table is found on page 12 in the textbook)

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Enchipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
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			

Authentication

- Concerned with **assuring** that a communication is **authentic**
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- **Peer entity authentication**
- **Data origin authentication**

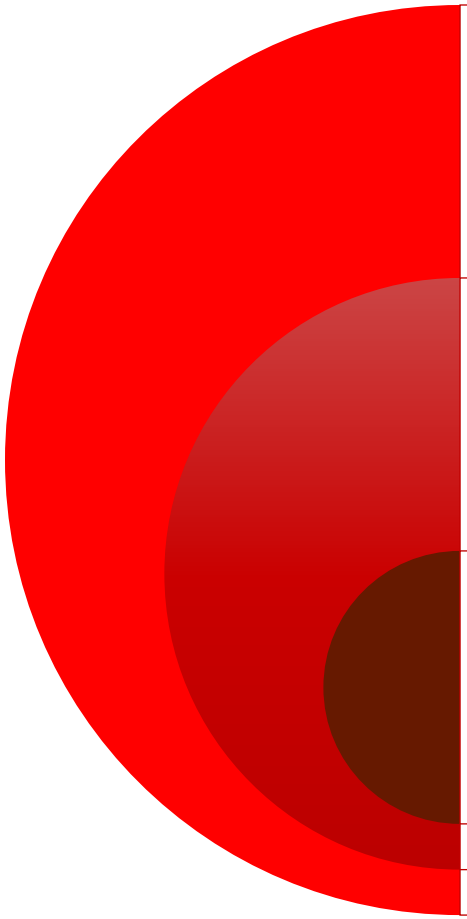
Access Control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual

Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service include the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity



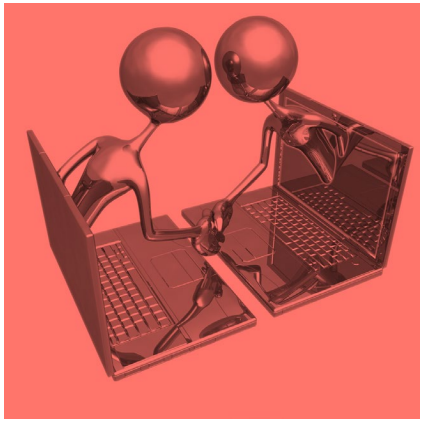
Can apply to a stream of messages, a single message, or selected fields within a message

Connection-oriented integrity service deals with a stream of messages and assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service deals with individual messages without regard to any larger context and generally provides protection against message modification only

Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message



Availability service

- Availability
  - The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system
- Availability service
  - One that protects a system to ensure its availability
  - Addresses the security concerns raised by denial-of-service attacks
  - Depends on proper management and control of system resources

Optional DF Topic for this week?

1. Read the next 3 slides on the various security design principles.
2. Choose 3 of these principles from the list
3. Develop a scenario (or describe an actual case) where *each* of these three design principles would have prevented an attack
4. Create a discussion forum post under “Weekly Discussions” > “Week 1” discussion forum and share your work.
5. Remember to cite your sources!

Fundamental **Security Design Principles**

- The National Centers of Academic Excellence in Information Assurance/Cyber Defense list the following as fundamental security design principles:
    1. Economy of mechanism
    2. Fail-safe defaults
    3. Complete mediation
    4. Open design
    5. Separation of privilege
    6. Least privilege
    7. Least common mechanism
    8. Psychological acceptability
    9. Isolation
    10. Encapsulation
    11. Modularity
    12. Layering
    13. Least astonishment

Security design principles

- Economy of mechanism
  - The design of security measures embodied in both hardware and software should be as simple and small as possible
- Fail-safe default
  - Access decisions should be based on permission rather than exclusion—the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted
- Complete mediation
  - Every access must be checked against the access control mechanism
- Open design
  - The design of a security mechanism should be open rather than secret
- Separation of privilege
  - A practice in which multiple privilege attributes are required to achieve access to a restricted resource
- Least privilege
  - Every process and every user of the system should operated using the least set of privileges necessary to perform the task
- Least common mechanism
  - The design should minimize the functions shared by different users, providing mutual security
- Psychological acceptability
  - Implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access

Security design principles

- Isolation
  - A principle that applies in three contexts: first, public access systems should be isolated from critical resources to prevent disclosure to tampering; second, the processes and files of individual users should be isolated from one another except where it is explicitly desired; third, security mechanisms should be isolated in the sense of preventing access to those mechanisms
- Modularity
  - Refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation
- Encapsulation
  - Viewed as a specific form of isolation based on object-oriented functionality
- Layering
  - Refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems
- Least astonishment
  - A program or user interface should always respond in the way that is least likely to surprise or astonish the user

Attack surface

- Consists of the reachable and exploitable vulnerabilities in a system
  - Examples:
    - Open ports on outward facing Web and other servers, and code listening on those ports
    - Services available on the inside of a firewall
    - Code that processes incoming data, e-mail, XLM, office documents, and industry-specific custom data exchange formats
    - Interfaces, SQL, and Web forms
    - An employee with access to sensitive information vulnerable to a social engineering attack
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code
  - Human attack surface
    - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

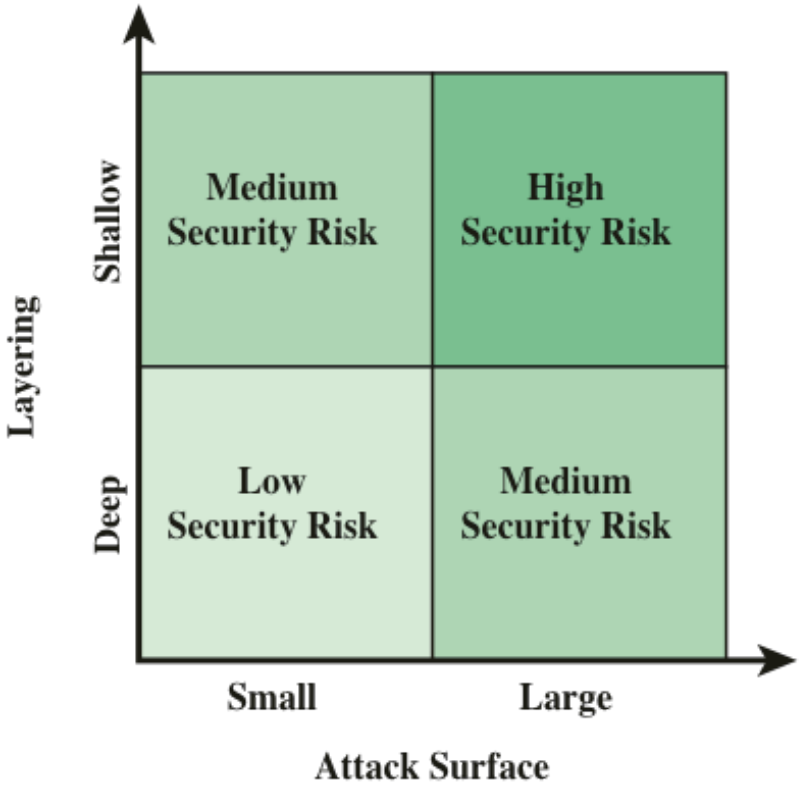


Figure 1.3 Defense in Depth and Attack Surface

Attack trees

A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

The security incident that is the goal of the attack is represented as the root node of the tree

The ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree

The final nodes on the paths outward from the root, the leaf nodes, represent different ways to initiate an attack

Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

Attack Controls

In general, the concept of risk reduction as relates to attacks are categorized as Controls.

Controls:

- Means, methods, actions, techniques, processes, procedures or devices that reduce the vulnerability of a system, or reduce the possibility of a Threat that exploits a vulnerability in a system (a Risk).

The two primary forms of implemented Controls:

Safeguards:

- **Proactive** measures implemented to deny access to, or attack on systems or information.
- Protection against known exploitation of systems or information that are vulnerable to attacks.

  e.g. a firewall protecting a private network

Countermeasures:

- **Reactive** measures to respond, reduce, redirect or resolve attacks against systems

  e.g. an intrusion detection and prevention system on a private network

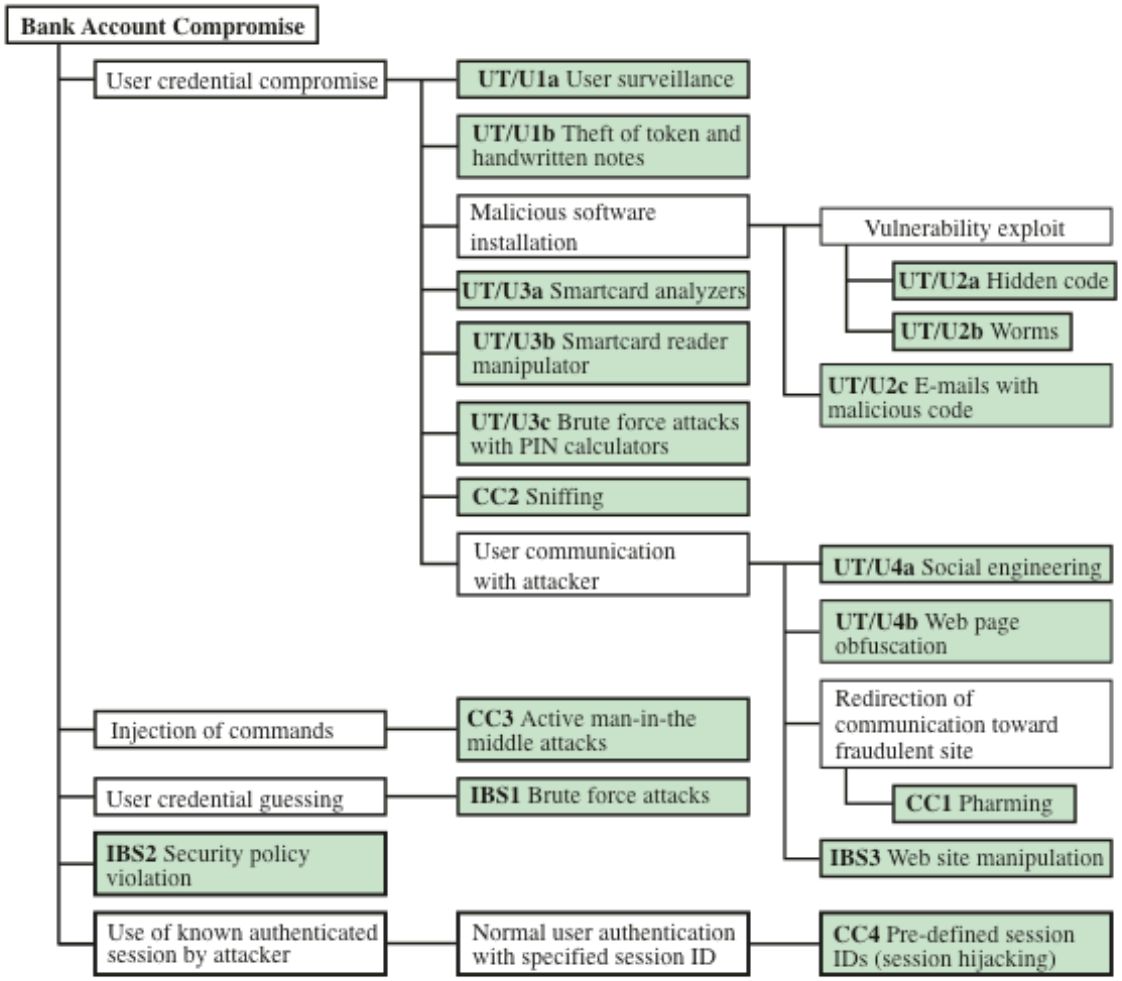


Figure 1.4 An Attack Tree for Internet Banking Authentication

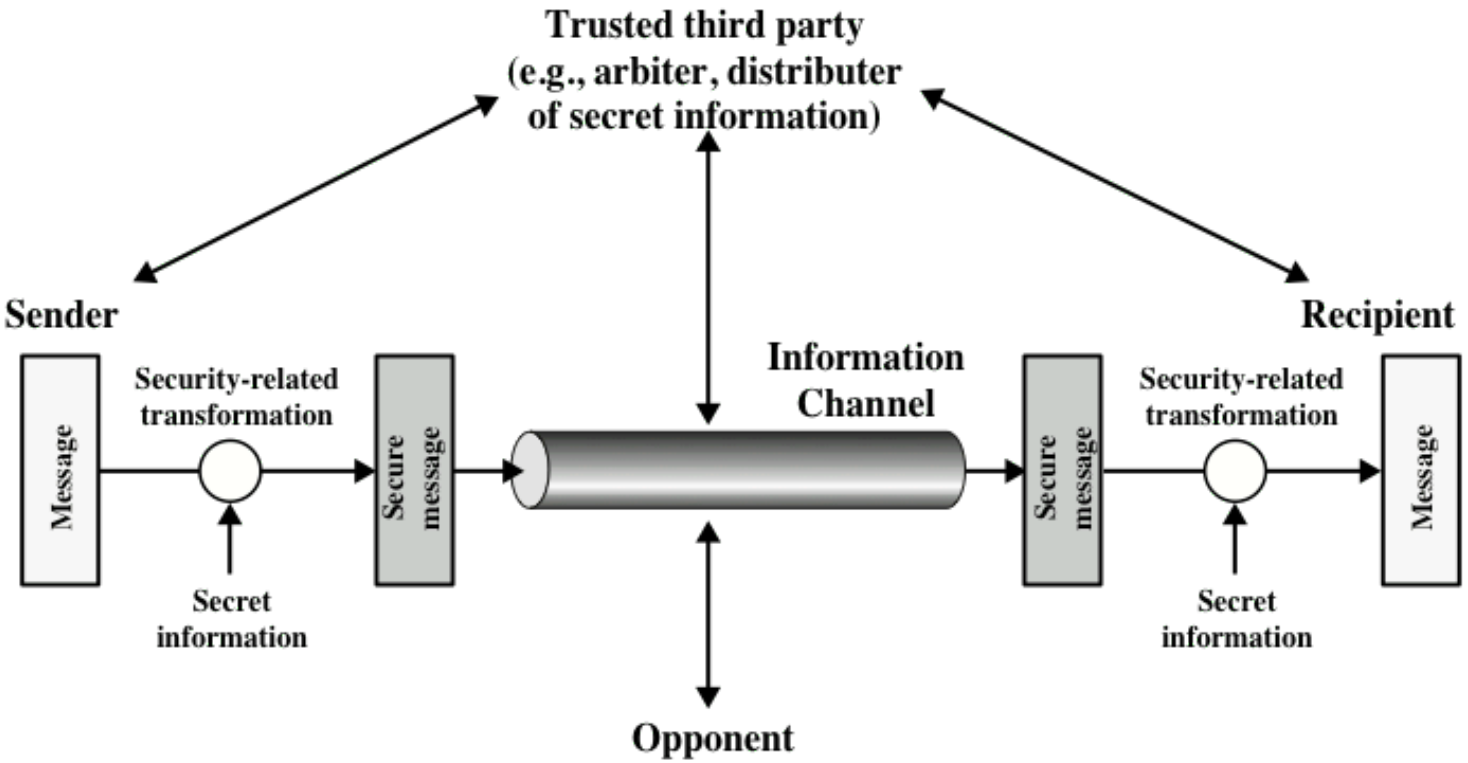


Figure 1.5 Model for Network Security

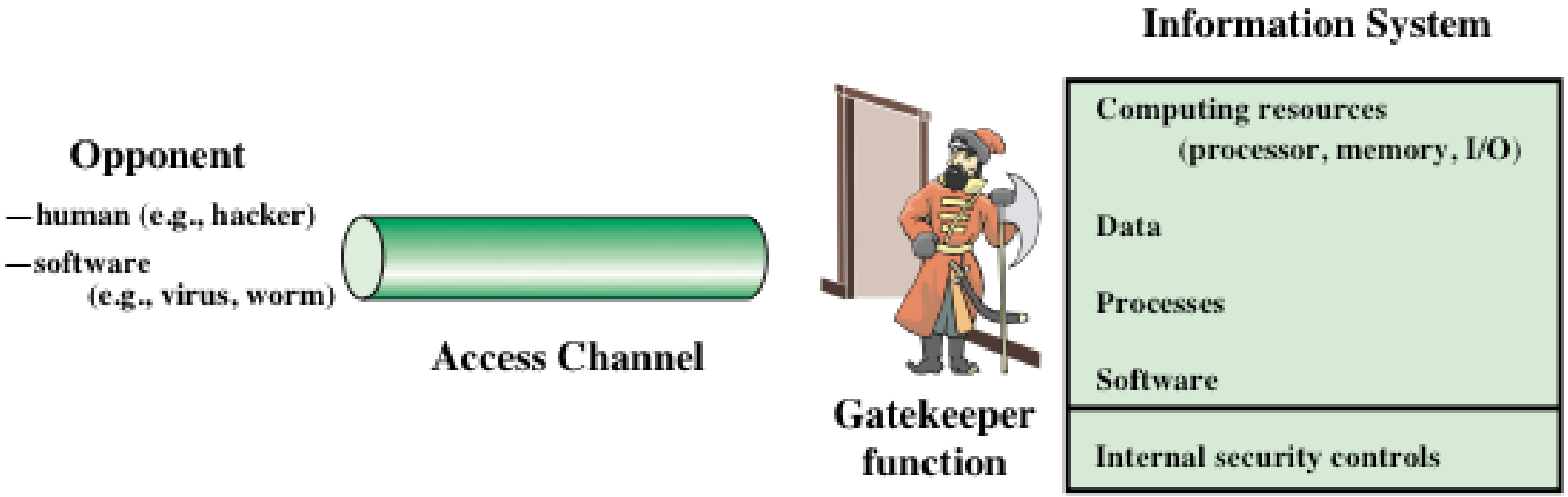
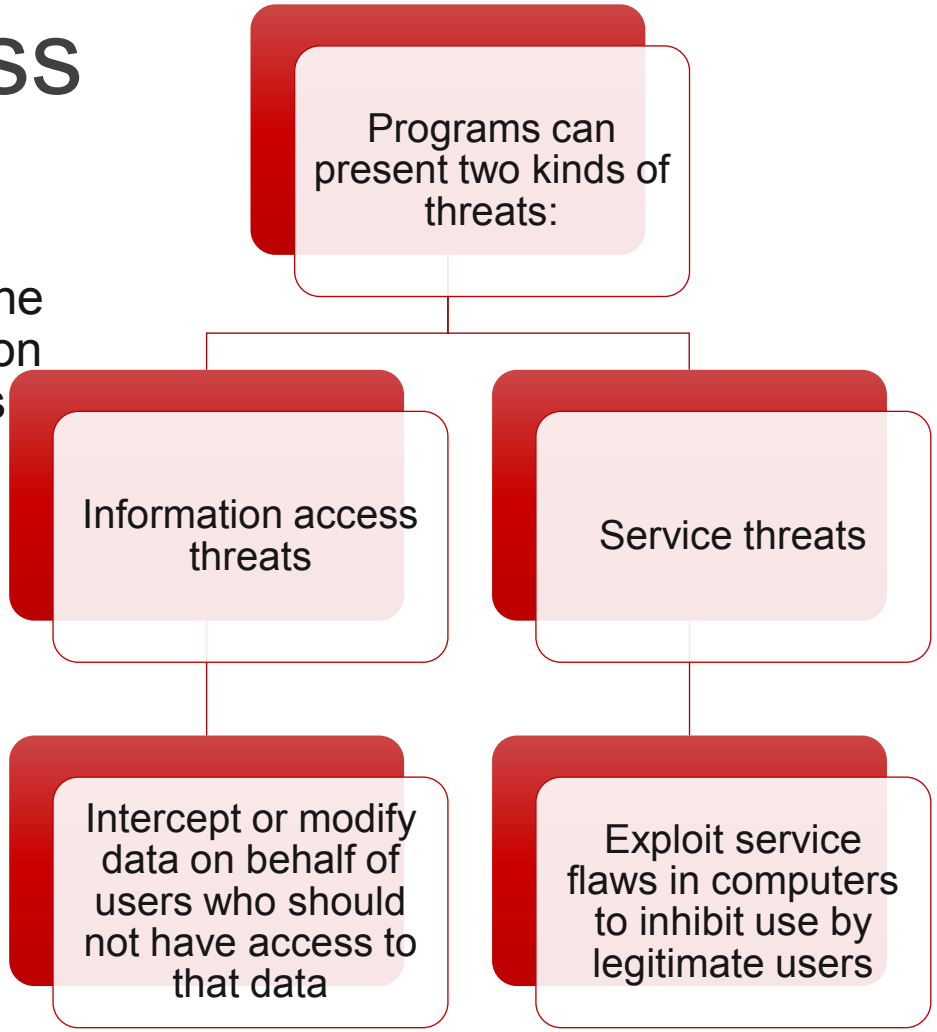


Figure 1.6 Network Access Security Model

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs



Standards

NIST

- National Institute of Standards and Technology
- U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation
- NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

ISOC

- Internet Society
- Professional membership society with worldwide organizational and individual membership
- Provides leadership in addressing issues that confront the future of the Internet
- Is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB)
- Internet standards and related specifications are published as Requests for Comments (RFCs)

Reminders

- Read the Chapter 1 of Textbook (focus on the summary and the SEVEN Review questions at the end of the chapter).
- Read the Key Terms (p.42) and identify 5 terms you didn't know before. Create a discussion forum post and share!
- Contribute to the Week 1 Discussion Forum on FOL
  - Share your bio and comment on the bios of others
- **Week 1 Lab Sessions:**
  - **Section 1: Thursday 10 AM – 11:50 AM**
  - **Assignment #1 is done in Lab**