CS458: Introduction to Information Security

Notes 1: Introduction

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

yelmehdwi@iit.edu

August 23rd, 2021

Slides: Modified from: "Computer Security: Principles and Practice", 4th Edition. By: William Stallings and Lawrie Brown, "Cryptography and Network Security", 6/e, by William Stallings & Steven Gordon, CQUniversity

Welcome to CS458

Who we are. . .

- **Course Info**
  - Blackboard: Assignments, reading materials, lecture notes
  - Piazza: Class Discussions/Announcements
- **Instructor**
  - Yousef Elmehdwi
    - Fifth year at IIT, not first time teaching `CS458`☺
    - Email: `yelmehdwi at iit dot edu`
    - Research: data privacy and security
    - Office: Stuart Building, room `237D`
    - Office Hours: `Wednesdays, 6:00-7:00pm or by appointment`

What is our goal in this course?

- To provide a basic understanding of the problems of information assurance and the solutions that exist to secure information on computers and networks
- To be able to use this ability to design systems that are more protective of security

Things to cover in CS458

- Introduction to the major topics in computer security
  - human factors in security policy
  - basic applied cryptography, public key cryptography
  - key and identity management, authentication, access control
  - network security, database security, operating system security
  - denial-of-service attacks, malware ...
  - more ...
- Lots of security problems to consider
- But not nearly enough time available?

What this course is (and is not)

- This is a combination of lecture, discussion and hands-on security exercises class
- For those are interested in more hands-on experience
  - CS 495: Ethical Hacking and Penetration Testing (Spring 2022)
    - Provide a wide range of topics related to ethical hacking and penetration testing.
  - CSP 544: System and Network Security
    - Present an in-depth examination of topics in data and network security
    - http://cs.iit.edu/~khale/class/security/s20/
  - CS 558: Advance Computer Security
    - https://sites.google.com/site/cs558spring2019/home
  - CS 549 Cryptography
  - CS 595: Topics in Software Security, Fall 2020
  - New master of cyber-security degree
    - available for co-terminal students as well
    - https://www.iit.edu/academics/programs/cybersecurity-mas

Lectures

- Lecture slides in PDF format will be posted before the lectures (Blackboard)
- Lecture slides cover essential material
- Lectures will be recorded and uploaded to course Blackboard right after each class.
- Students can access the recorded lectures whenever they need them.
- Piazza
  - Announcements/Participating in discussions

Course syllabus

- You are expected to be familiar with the contents of the course syllabus
- Available on the course Blackboard
- If you haven't read it, read it after this lecture

Workload and Grading

- **Exams**
  - One midterm exam and one final
  - Closed book, closed notes exams
    - Only **ONE** sheet of paper printed on front and back is allowed
  - Midterm Exam: **10/18/2021**
  - Final: TBA **12/??/2021**
- **Assignments**:
  - 4 hands-on security exercises (at least)
    - Hands-on exercises: SEED Labs
  - Individual work

Workload and Grading

Assignments: Security exercises	40%
Midterm Exam	25%
Final Exam	35%

Letter Grade Distribution

Points	**Grade**
85 - 100	A
75 - 84	B
65 - 74	C
60 - 64	D
0 - 59	E

Hands-on Exercises

- **Lab 1**: `Lab Environment Setup`
- **Lab 2**: `Secret Key Encryption Lab`
- **Lab 3**: `MD5 Collision Attack Lab`
- **Lab 4**: `SQL Injection Attack`

Fraud and Late Assignments

- All work has to be original!
  - Cheating = 0 points for assignment/exam
  - Possibly **E** in course and further administrative sanctions
  - Every dishonesty will be reported to office of academic honesty

Recommended textbooks/ other readings

- **Textbooks:**
  - `Computer Security: Principles and Practice` by William Stallings and Lawrie Brown, any edition (4^{th})
    - Resource for students from the official textbook website
    - http://williamstallings.com/ComputerSecurity/CompSec4e-Student/
  - `Security in Computing`, 5^{th} Edition, by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies
  - Computer Security: A Hands-on Approach, Wenliang Du, 2017
- Additional Readings
  - Additional readings will be assigned throughout the semester, ranging from current news stories to technical articles to research papers.
  - All of the additional readings will either be freely available or copies will be provided for students.

What is expected from you

- Attend in-person lectures, if you can
- Be active and think critically
- Do hands-on Assignments
  - Start early and be honest
- Study for exams

A note on security

- In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks
- To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner
- In particular, you will comply with all applicable laws

Outline

- Computer Security Concepts
- Introduce the CIA Triad
- What is privacy?
- Assets, vulnerabilities, threats, attacks, and defenses
- Architecture for Communication Security
- Computer Security Strategy

Why study information security?

- To protect computers, networks, and the information they store, organizations are increasingly turning to information security specialists
- We begin by trying to answer the first question most students starting out in the field ask: *Why study information security?*

The Growing Importance of IT Security and New Career Opportunities

- Increased services to both vendors and employees create worlds of possibilities in satisfying customer needs, but ...
- They also create risks to the confidentiality, integrity, and availability of confidential or sensitive data

Increasing Demand by Government and Private Industry

- The number of information security specialist is expected to grow 36% from 2012 to 2022
- Higher demand for expertly trained individuals
  - U.S. Bureau of Labor Statistics
    - The security of computer networks will continue to increase in importance as more business is conducted over the Internet
    - There will be a high demand of managers proficient in computer security issues
    - Source: `www.collegegrad.com/careers/manage30.shtml`

- Read 10 Reasons Why a Cyber Security Degree is Worth It

Becoming an Information Security Specialist

- Getting a degree in information security will involve taking classes in security architecture, laws and ethics, access control, disaster recovery and planning
- Get the right certification
  - Certified Information Systems Security Professional (CISSP)
  - System Security Certified Practitioner (SSCP)
  - Global Information Assurance Certification (GIAC)
- Increase your disaster recovery and risk management skills
- Build a home laboratory
- Consider an internship in IS
- Take a second look at government jobs

Schools Are Responding to Demands

- Homeland security is a hot topic not only in corporate America.
- Higher education is also responding to the need with new and robust certificate programs, degrees, and special-interest courses.
- Hundreds of community colleges, 4-year universities, and post-graduate programs are offering degrees and certificates in emergency preparedness, counterterrorism, and security
  - Department of Homeland Security supports the Naval Postgraduate School for Homeland Defense and Security https://www.chds.us.[1]
  - The school educates high-ranking emergency management and public safety officials about policy analysis, advanced strategy, and information technology.

[1] The Center for Homeland Defense and Security (CHDS)

Achieving Security

- In the ideal world, we would like to achieve perfect security of information.
- It is impossible to protect everything against every attacker under all circumstances while maintaining usability (utility of the system).
- Given enough time, tools, skills, and inclination, a hacker can break through any security measure

What does “security” mean to you?

Security Mindset

- You see an advertisement for a new product. What is your reaction?
- Is your first reaction:
  - *"Wow! This is such a cool product. I can't wait to use it!'*

- Or is your reaction:
  - *"Wow! This is a neat product but I wonder what are the potential consequences of using it? Does it work as advertised? Is it safe? Can something go wrong while using it? Can someone else exploit it?"*

- Read: How to think like a security professional

Example: Nest Learning Thermostat

YouTube: How Nest Learning Thermostat Learns

- Read: Smart Nest Thermostat: A Smart Spy in Your Home

Security Mindset

- Security is not a product, it is a process [2]
- We need to learn to think with a "security mindset"
  - How could this system be attacked?
  - Who could attack this system?
  - Are they likely to attack the system?
  - What is the weakest point of attack?
  - How could this system be defended?
  - How effective will a given countermeasure be?
  - What is the trade-off between security, cost, and usability?

- Watch: Bruce Schneier: The Security Mindset

[2] https://www.schneier.com/crypto-gram/archives/2000/0515.html

Computer Security

- What is computer security?
  - Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated[3]
- Computer Security is about understanding and improving the behavior of computing technologies in the presence of adversaries
- Deals with various measures to protect computer related assets against a variety of threats
- Computer security is the protection of computing systems and the data that they store or access

[3]The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms , May 2013)

Key Security Objectives: Three Security Goals

- In the context of computers, security generally means three things:
  - Confidentiality: Access to systems or data is limited to authorized parties
    - **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: Refer to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.
    - **Data integrity** (the content of the information): Assure information and programs are changed only in a specified and authorized manner.
    - **System integrity**: Assure 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.
    - Keep data and resources available for authorized use especially during emergency or disasters
    - The system or data is there when you want it

CIA Triad

- `CIA == Confidentiality, Integrity, and Availability`
- Definition of a loss of security in each CIA triad:
- Confidentiality:
  - Prevent unauthorized reading of information
  - A loss of confidentiality is the unauthorized disclosure of information.
- Integrity:
  - Prevent unauthorized writing of information
  - A loss of integrity is the unauthorized modification or destruction of information

  Availability:
  - Ensures data is available in a timely manner when needed
    - Due to denial of service (DoS) threats
  - A loss of availability is the disruption of access to or use of information or an information system.

Security and reliability

- Security has a lot to do with “reliability”
- A secure system is one you can rely on to (for example):
  1. Keep your personal data confidential
  2. Allow only authorized access or modifications to resources
  3. Ensure that any produced results are correct
  4. Give you correct and meaningful results whenever you want them

What is privacy?

- There are many definitions of privacy
- A useful one: informational self-determination
  - This means that you get to control information about you
  - Control means many things:
    - Who gets to see it
    - Who gets to use it
    - What they can use it for
    - Who they can give it to
    - etc.

Security of an Information System

- Information security, sometimes shortened to *infosec*, is the practice of protecting information by mitigating information risks.

- We cannot protect information on its own.
- You need to look at the entire system within which the information exists.
- A system is only as strong as its weakest component.

Security of an Information System

- Understand the system and its components.
- Identify assets.
- Identify vulnerabilities.
- Identify attacks.
- Identify adversaries.

Computer Security Concepts

- Asset
- Vulnerability
- Threat
- Attack
- Countermeasure or control

Assets (System resource)

- Need to know what you are protecting!
- Asset: Things we might want to protect (Anything of value)
  - Physical Assets: Buildings, computers
  - Logical Assets: Intellectual property, reputation
- You need to know what there is to protect.
- You need to know what is worth protecting

Assets of Computer Systems to Protect

The assets of a computer system can be categorized as follows:

- Hardware
  - Including computer systems and other data processing, data storage, and data communications devices
- Software
  - Including the operating system, system utilities, and applications.
- Data
  - Including files and databases, as well as security-related data, such as password files.
- Communication facilities and networks
  - local and wide area network communication links, bridges, routers, and so on.

Vulnerabilities

- Vulnerabilities: Weaknesses in the security system that could be exploited to cause loss or harm
  - Its weakness or gabs in your security efforts. In other words, it is a known issue that allows an attack to succeed
- Examples:
  - A file server that doesn't authenticate its users
  - Bad passwords
  - Buggy software
  - Untrained employees
  - Lack of encryption
  - ...
- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)

Vulnerabilities

- General types of vulnerability correspond to the concepts of integrity, confidentiality, and availability:
  - The system can be corrupted, so it does the wrong thing or gives wrong answers (loss of integrity)
    - For example, stored data values may differ from what they should be because they have been improperly modified.
  - The system can become leaky (loss of confidentiality)
    - For example, someone who should not have access to some or all of the information available through the network obtains such access.
  - The system can become Unavailable or very slow (loss of availability)
    - That is, using the system or network becomes impossible or impractical.

Security Policy

- Set of the rules and practices that specifies how a system provides security services to protect assets.
- Refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it.

Threats

- Threats are potentials for vulnerabilities to turn into attacks on systems
- Represent potential cause of security harm to an asset
- i.e., a loss or harm that might befall a system
  - e.g., users' personal files may be revealed to the public

Attacks

- Attacks (threats carried out) an action which exploits a vulnerability to execute a threat
- Examples:
  - Telling the file server you are a different user in an attempt to read or modify their files are ways of exploiting a vulnerability to damage assets
  - Bad passwords: using password crackers.
  - Buggy software: launching an SQL injection attack.
  - Untrained employees: tricking them to share their credentials.
  - Lack of encryption: eavesdropping on communications.
- Threat Action: An attack
- Attacker/Threat Agent Entity that attacks/carrying out the attack, or is threat to system (adversary, attacker, malicious user)

Attacks

- Attacks can be classified as:
  - Passive: attempt to learn or make use of information from the system that does not affect system resources
  - Active: attempt to alter system resources or affect their operation
- Attacks can also be classified based on the source/origin of the attacks:
  - Inside Attack
    - initiated by entity with authorized access to system.
  - Outside Attack
    - initiated by unauthorized user of system

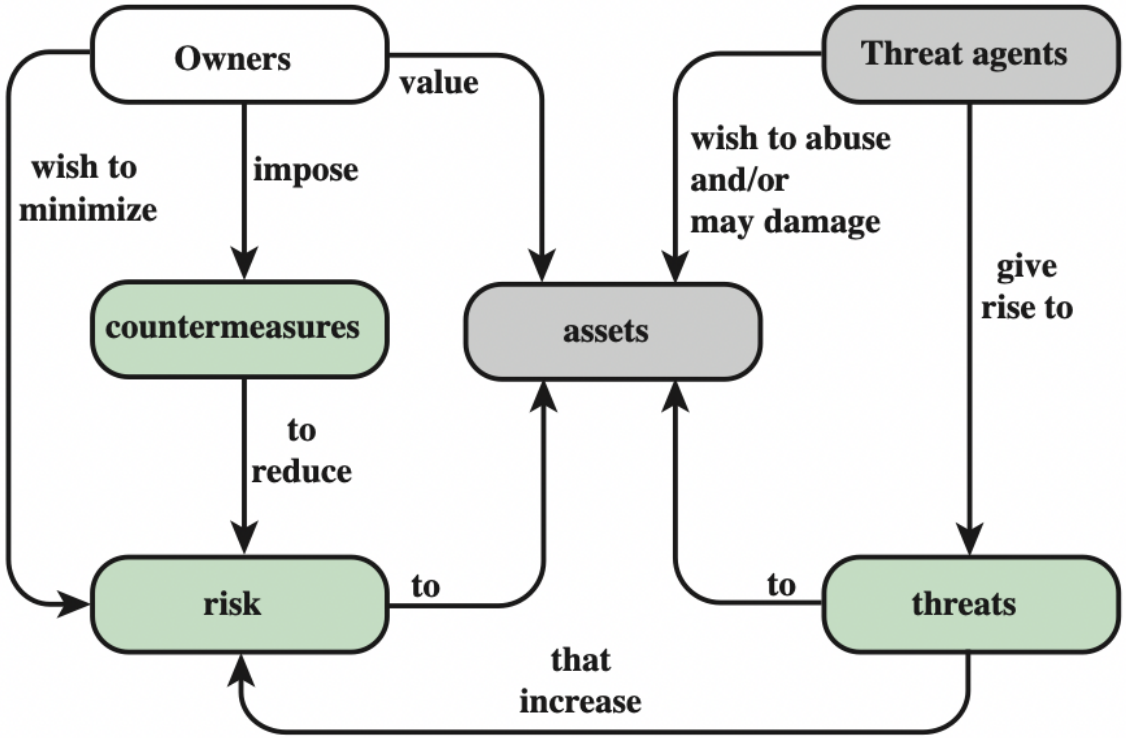
Risk

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability
- Examples of risk include:
  - Financial losses
  - Loss of privacy
  - Damage to your reputation
  - Legal implications
  - Even loss of life

Control/Countermeasures

- Q: How can we defend against a threat?
  - A threat is blocked by control of vulnerability
- Means used to deal with security attacks
  - i.e., a mechanism that is designed to detect, prevent, or recover from a security attack.
  - Prevent, detect, respond, recover
- Even with countermeasures, vulnerabilities may exist, leading to risk to the assets
- Aim to minimize the risks

Computer Security Concepts and relationships



Example of defense

- Threat: your car may get stolen
- How to defend?
  - Prevent: Immobilizer? Is it possible to absolutely prevent?
  - Deter: Store your car in a secure parking facility
  - Deflect: Have sticker mentioning car alarm, keep valuables out of sight
  - Detect: Car alarms, OnStar
  - Recover: Insurance

How secure should we make it?

- Principle of Easiest Penetration
  - "A system is only as strong as its weakest link"
  - The attacker will go after whatever part of the system is easiest for him, not most convenient for you.
  - In order to build secure systems, we need to learn how to think like an attacker!
  - How would you get private information from the US Social Security Administration database?
- Principle of Adequate Protection
  - "Security is economic"
  - Don't spend $100,000 to protect a system that can only cause $1,000 in damage

Weakest link

Defense of computer systems

- Remember we may want to protect any of our assets
  - Hardware, software, data
- Many ways to do this
  - Cryptography
  - Software Controls
  - Hardware Controls
  - Physical Controls
  - Policies and Procedures

Cryptography

- Protecting data by making it unreadable to an attacker
- Authenticating users with digital signatures
- Authenticating transactions with cryptographic protocols
- Ensuring the integrity of stored data
- Aid customers' privacy by having their personal information automatically become unreadable after a certain length of time

Hardware controls

- Not usually protection of the hardware itself, but rather using separate hardware to protect the system as a whole
- Fingerprint readers
- Smart tokens
- Firewalls
- Intrusion detection systems

Physical controls

- Protection of the hardware itself, as well as physical access to the console, storage media, etc.
- Locks
- Guards
- Off-site backups
- Don't put your data center on a fault line in California
- Don't put your nuclear power plant in a tsunami zone

Policies and procedures

- Non-technical means can be used to protect against some classes of attack
- If an employee connects his own Wi-Fi access point to the internal company network, that can accidentally open the network to outside attack
  - So don't allow the employee to do that!
- Rules about choosing passwords
- Training in best security practices

High-level plan for thinking about security

- What is Security: Achieving some goal in the presence of an adversary.
  - Many systems are connected to the Internet, which has adversaries. Thus, design of many systems might need to address security, i.e. will the system work when there's an adversary?
- High-level plan for thinking about security
  - Policy: The goal you want to achieve. e.g., only Alice should read file F
    - Common goals: confidentiality, integrity, availability.
  - Threat model: assumptions about what the attacker could do. e.g. can guess passwords, cannot physically grab file server. Better to err on the side of assuming attacker can do something.
  - Mechanism: knobs that your system provides to help uphold policy. e.g. user accounts, passwords, file permissions, encryption.
  - Resulting goal: no way for adversary within threat model to violate policy.

What is Security?

- Network and Internet Security
  - Measure to deter, prevent, detect, and correct security violations that involve transmission of Information.

Architecture for Communications Security

- In order to let different devices (computers, routers, cellular phones) to communicate data in a standardized way, communication protocols had been defined.
- Systematic approach to define requirements for security and approaches to satisfying those requirements.
- ITU-T [4]Recommendation X.800, Security Architecture for OSI
  - OSI Security Architecture
  - Provides abstract view of main issues of security
  - Security aspects: Attacks, mechanisms and services
  - Focuses on security of networks and communications systems
  - Concepts also apply to computer security

[4] The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations sponsored agency that develops standards, called Recommendations, relating to telecommunications and to open systems interconnection (OSI). The ITU-T organization published a large set of protocols

Aspects of Security

- Security Attack
  - Any action that attempts to compromise the security of information or facilities
- Security Mechanism
  - A method for preventing, detecting or recovering from an attack
  - i.e., Techniques designed to prevent, detect or recover from attacks
  - No single mechanism can provide all services
  - Common in most mechanisms: cryptographic techniques
- 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
    - Uses security mechanisms to enhance the security of information or facilities in order to stop attacks
    - i.e., Security services implement security policies and are implemented by security mechanisms.

Security Services

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non-repudiation
- Availability

Security Services: Authentication

- Who created or sent the data
- 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
  - Peer entity authentication
  - Data origin authentication

Security Services: Access Control

- Prevent misuse of resources
- 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 identified, or authenticated, so that access rights can be tailored to the individual

Security Services: 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 includes 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

Security Services: Data Integrity

- Can apply to a stream of messages, a single message, or selected fields within a message
- Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays
- A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

Security Services: 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

Security Services

- Authentication
  - Assure that the communicating entity is the one that it claims to be. (Peer entity and data origin authentication)
- Access Control
  - Prevent unauthorized use of a resource
- Data Confidentiality
  - Protect data from unauthorized disclosure
- Data Integrity
  - Assure data received are exactly as sent by authorized entity (has not been altered)
- Non-repudiation
  - Protect against denial of one entity involved in communications of having participated in communications
- Availability
  - System is accessible and usable on demand by authorized users according to intended goal

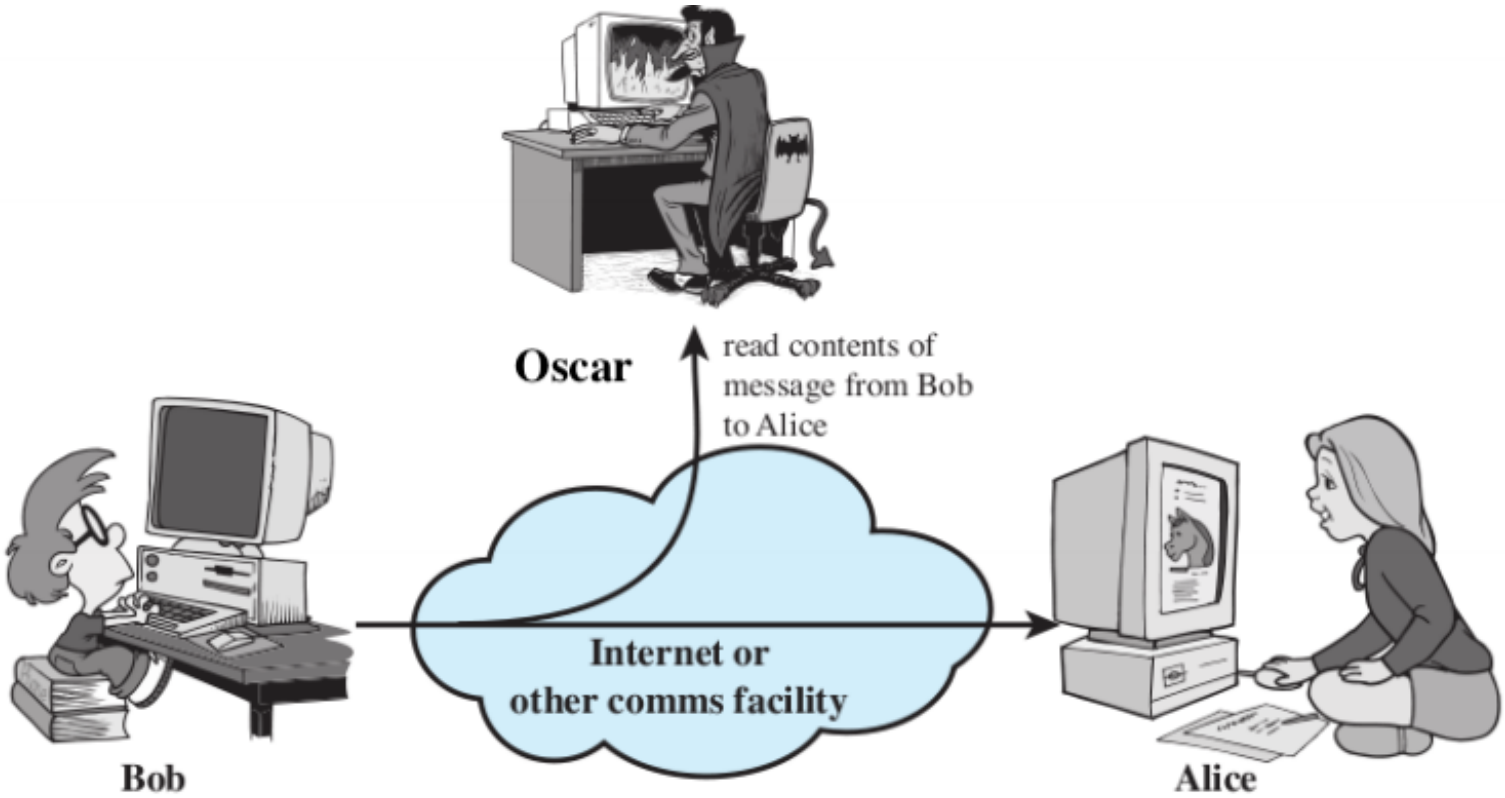
Security Services and Mechanisms

	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				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

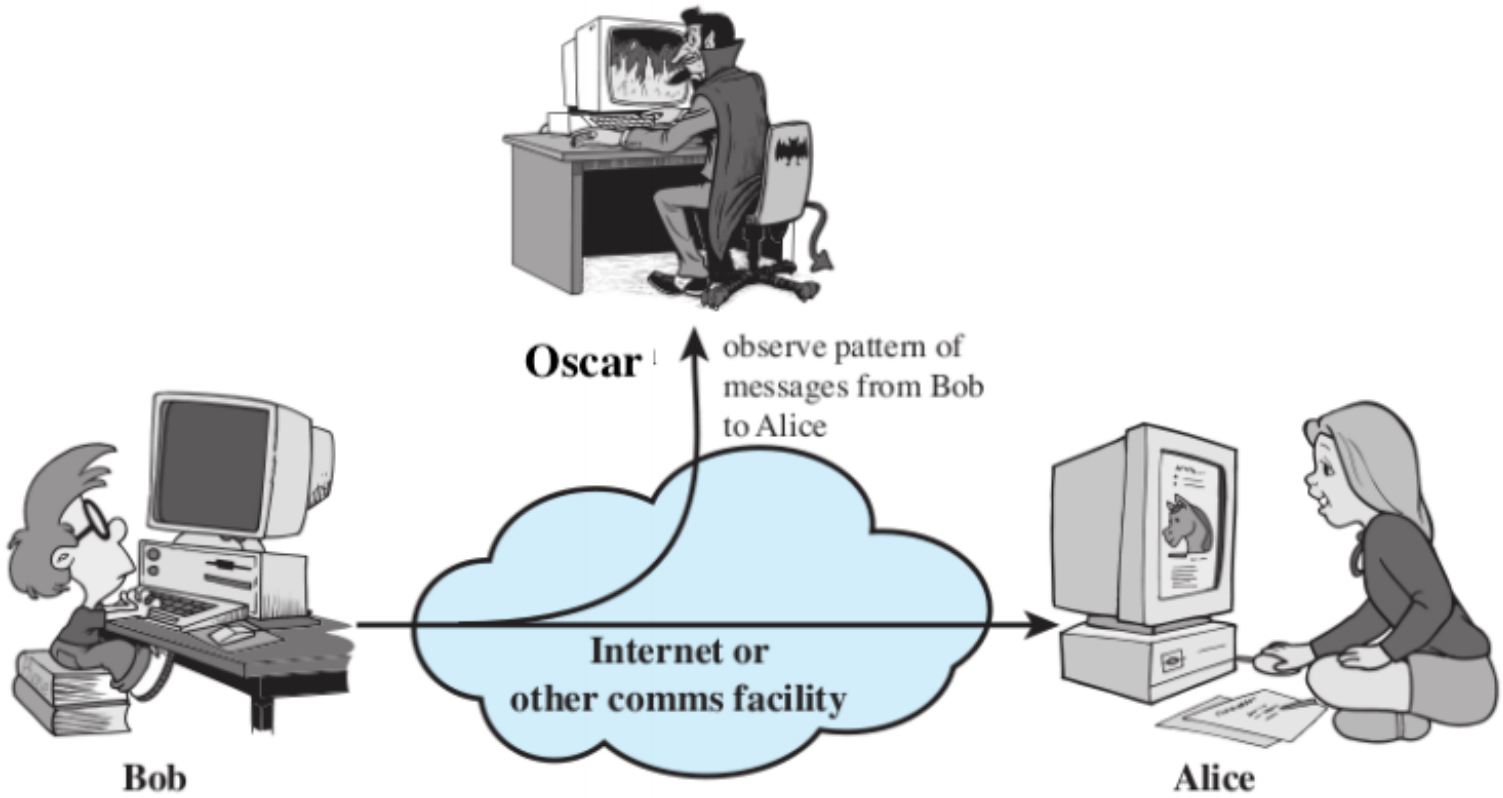
Attacks on Communication Lines

- Passive Attack
  - Attempt to learn or make use of information, but not affect system resources, e.g.,
    1. Release message contents
    2. Traffic analysis
  - Relatively hard to detect, but easier to prevent (usually by encryption)
- Active Attack
  - Attempt to alter system resources or affect their operation.
  - i.e., involve some modification of the data stream or the creation of a false stream,
  - Can be subdivided into four categories:
    1. Masquerade
    2. Replay
    3. Modification of messages
    4. Denial of service
  - Relatively hard to prevent (because it would require physical protection of all communications facilities and paths at all times), but easier to detect

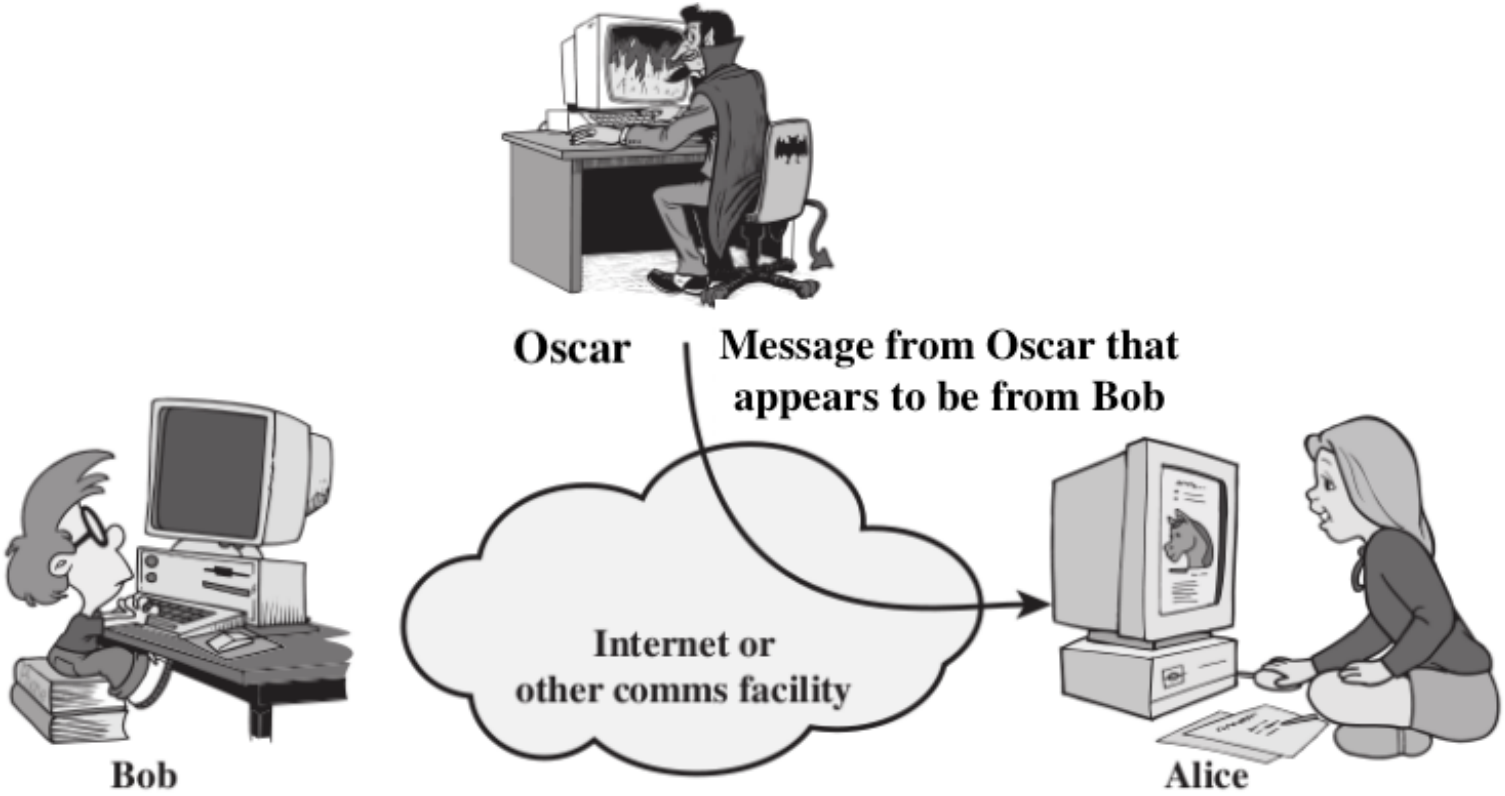
Release Message Contents



Traffic Analysis



Masquerade Attack

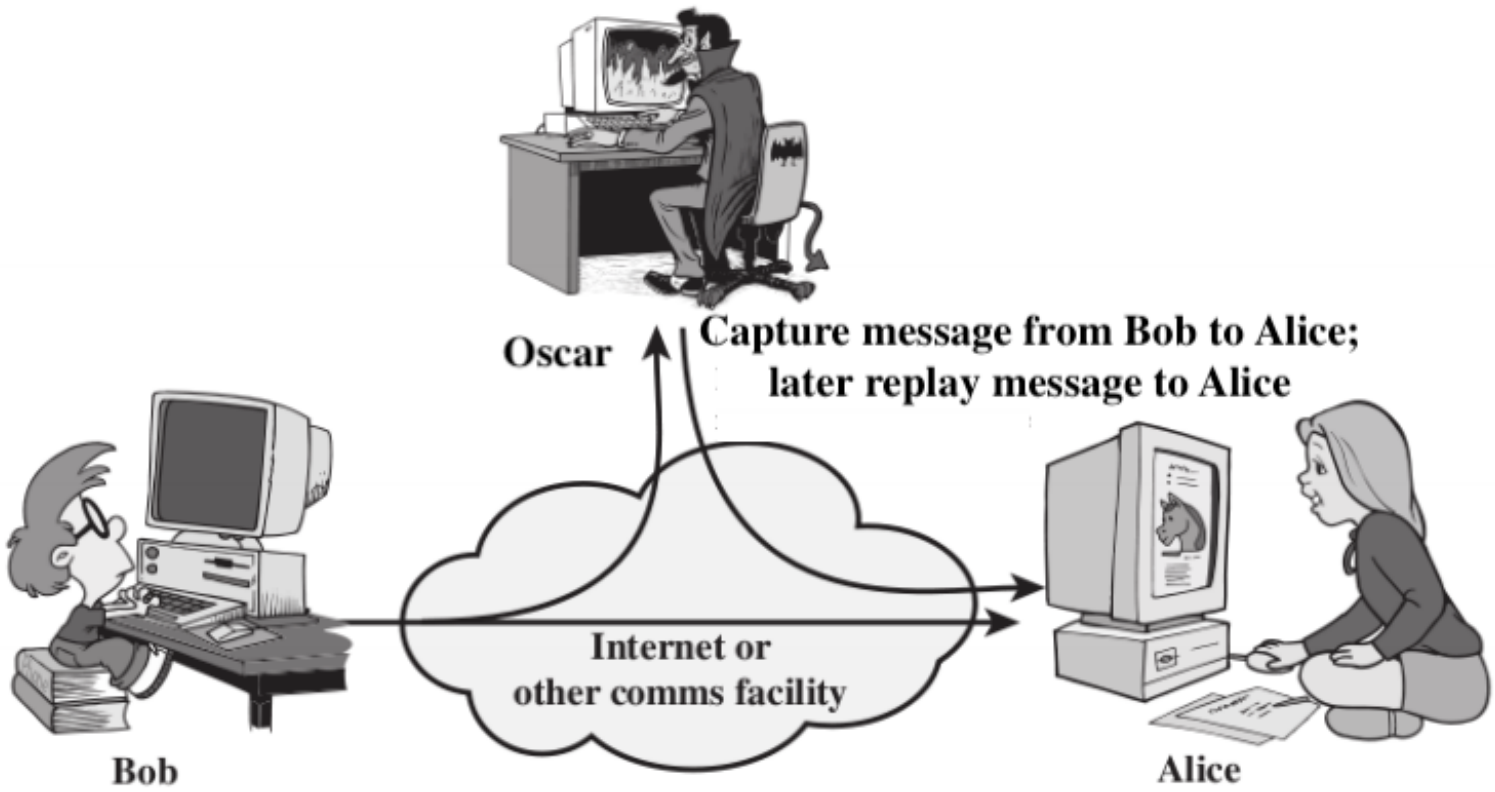


- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

“On the Internet, nobody knows you’re a dog”[5]

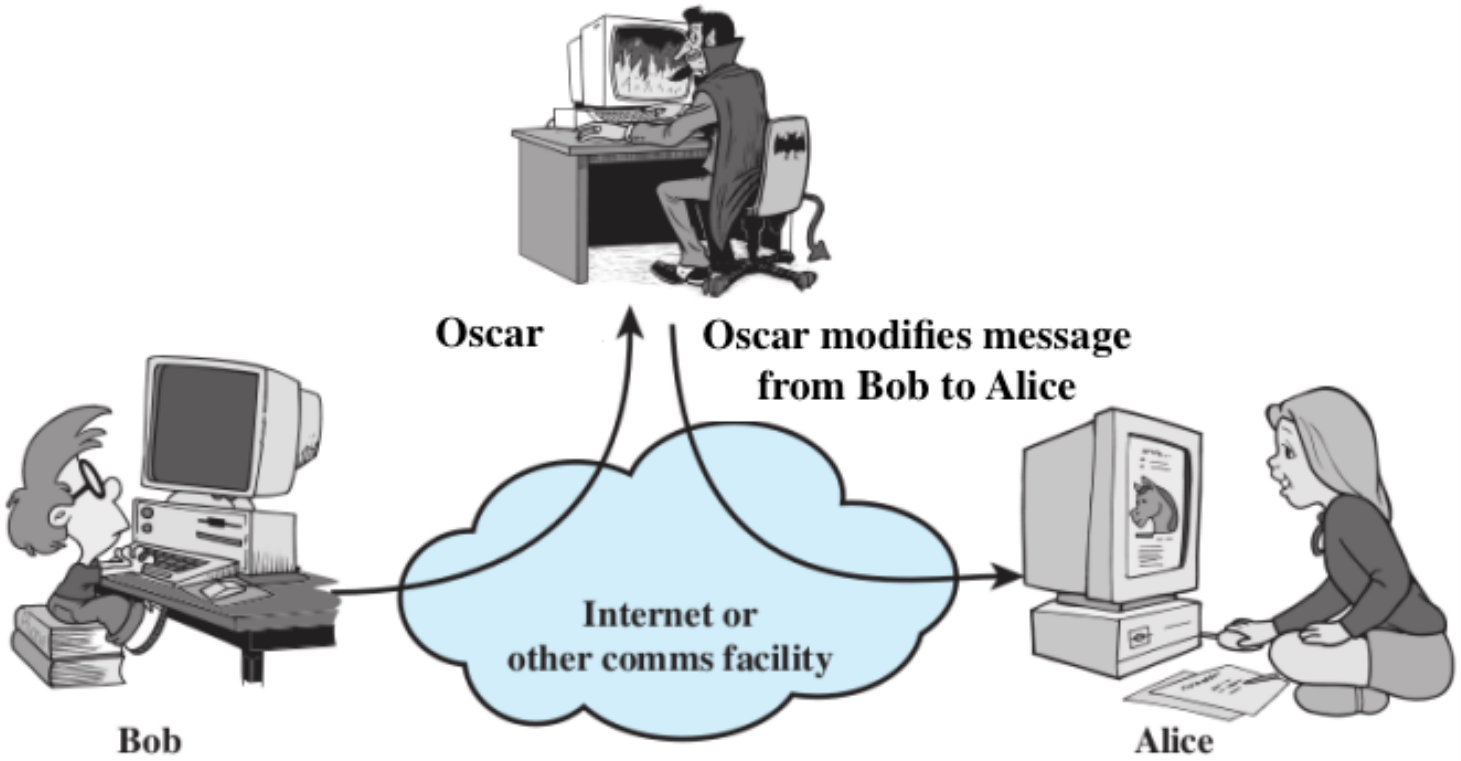
[5] Credit: Peter Steiner, The New Yorker magazine

Replay Attack



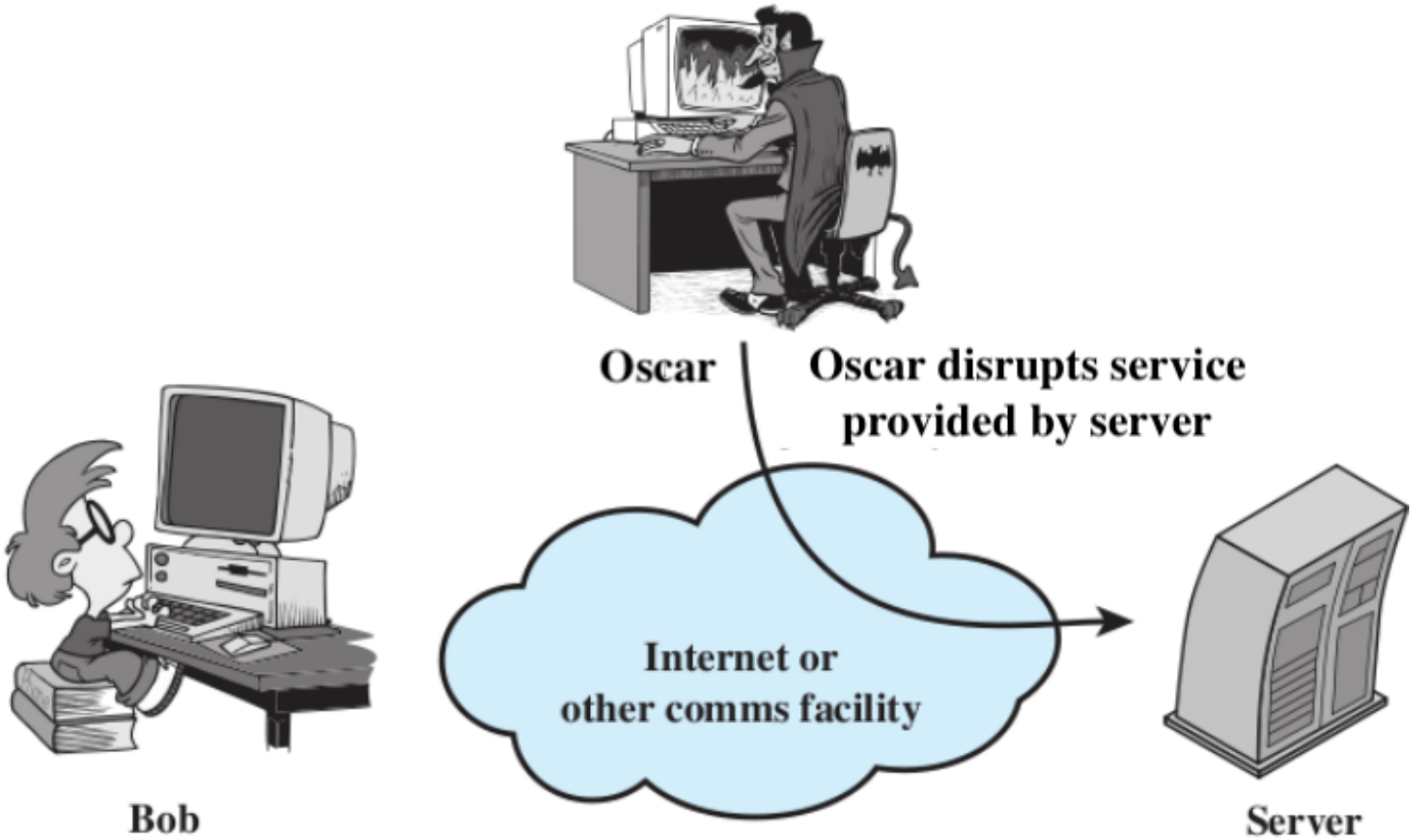
- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification Attack



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

Denial of Service Attack



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

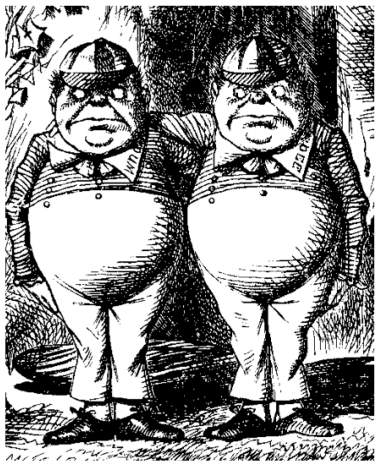
Computer Security Strategy and Principles

- Policy: What is the security scheme supposed to do?
  - Informal description or formal set of rules of desired system behavior
  - Consider: assets value; vulnerabilities; potential threats and probability of attacks
  - Trade-offs: Ease of use vs security; cost of security vs cost of failure and recovery
- Implementation: How does it do it?
  - Security implementation involves four complementary courses of action
    - Prevention, detection, response, recovery
- Assurance: Does it really work?
  - Security consumers want to feel that the security infrastructure of their systems meet security requirements and enforce security policies.
    - Assurance: degree of confidence that security measures work as intended
    - Evaluation: process of evaluating system with respect to certain criteria

The Cast of Characters

- Alice and Bob are the **good guys**

- Eve /Oscar are the **bad guys**



- Eve is our generic “intruder”

Think Like Eve/Oscar

- Good guys must think like bad guys!
- A police detective
  - Must study and understand criminals
- In information security
  - We want to understand Eve's/Oscar's methods
  - We might think about Eve's/Oscar's motives
  - We'll often pretend to be Eve/Oscar

Think Like Eve/Oscar

- Think like the bad guy
- Always look for weaknesses
- Find the weak link before Eve does
- It's OK to break the rules
- But don't do anything illegal!
- But, we cannot act like Eve/Oscar
  - Except in this class
  - and even then, there are limits

Standardizations

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important of these organizations are:
  - National Institute of Standards and Technology (NIST)
    - NIST is a 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
  - Internet Society (ISOC)
    - ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards
  - International Telecommunication Union (ITU-T)
    - ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
  - International Organization for Standardization (ISO)
    - ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards

Recap

- What is our goal in this course?
  - Identify security and privacy issues
  - Design systems that are more protective of security and privacy
- What is security?
  - Confidentiality, Integrity, Availability
- What is privacy?
  - Informational self-determination

Recap

- Assets, vulnerabilities, threats, attacks and controls
  - You control a vulnerability to prevent an attack and block a threat
- Methods of defense
  - Cryptography, software controls, hardware controls, physical controls, policies and procedures
- The OSI security architecture
  - Security attacks
  - Passive attacks
  - Active attacks
- Security services
- Authentication, Access control , Data confidentiality , Data integrity , Nonrepudiation , Availability service
- Security mechanisms

Reading

- Information Security: Principles and Practice, 2nd edition
  - Chapter 1 (Till 1.2.2)
- Computer Security: principles and practice
  - Chapter 1: 1.1, 1.2, 1.7
- Security in Computing
  - Chapter 1: 1.1, 1.2, 1.4