CS458: Introduction to Information Security

Notes 1: Introduction

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

yelmehdwi@iit.edu

January 8th 2024

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, “Principles of Information Security”, 7th edition 2022, by Michael E. Whitman, Herbert J. Mattord, MIT Computer Systems Security, & Steven Gordon, CQUniversity

Welcome to CS458

Who we are. . .

- **Instructor**
  - Yousef Elmehdwi
    - 7th 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: `Mondays, 12:45 - 1:45 pm or by appointment`

Who we are. . .

- **TA**
  - Email: TBA
  - Office: TBA
  - Office Hours: TBA

What is our goal in this course?

- To provide a basic understanding of the problems of information assurance[1] 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

[1] *Information assurance is the practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves protecting the confidentiality, integrity, and availability of information.*

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 (Fall/Summer)
    - 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/`
- Other Security Courses
  - CS 527: Software Security
  - CS 528: Data Privacy and Security
  - CS 549: Cryptography
  - CS 558: Advance Computer Security
- New master of cyber-security degree
  - available for co-terminal students as well
  - `https://www.iit.edu/academics/programs/cybersecurity-mas`

Course Info

- Time: `M/W 11:25 am- 12:40 pm, WH-113`
- 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.

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
  - No electronic devices, no bathroom breaks
  - Midterm Exam: **04/03/2024**
  - Final: During finals week **April 29 - May 4th, 2024**
- **Assignments**:
  - 4 hands-on security exercises (at least)
    - Hands-on exercises: SEED Labs
  - Individual work

Workload and Grading

Assignments: Security exercises	30%
Midterm Exam	30%
Final Exam	40%

Letter Grade Distribution

Points	**Grade**
90 - 100	A
75 - 89	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

- 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 vs Information Security
- History of computer security and how it evolved into information security
- Introduce the CIA Triad
- What is privacy?
- Assets, vulnerabilities, threats, attacks, and defenses
- Architecture for Communication Security
- Computer Security Strategy

Why Security/Why we Worry about Security

- The word Security which can be inferred as the immunity from any risk or danger that may have undesired outcome.
- Before considering why we care about security, it's important to understand why we would care about security in general.
- We worry about security/Security concerns emerge when there's something valuable that could be (*at risk of being*) harmed.
  - *something valuable that could potentially be damaged, compromised, or lost due to various threats or risks*
- Example: individuals store a lot of sensitive data online, such as financial information and medical information. If criminals get their hands on this data, they can monetize it and profit from it.
- *Security measures are put in place to safeguard what is valuable from potential harm.*

  - *What is the value in security?*
  - *Where do such threats come from?*
  - *What kind of risk are we talking about?*
  - *Who is the source of the threat?*

Why Security is Important

- Confidentiality: In many cases, information and data need to be kept confidential in order to protect sensitive information, such as personal information, trade secrets, and financial data.
- Integrity: Security helps to ensure the integrity of data and systems by protecting against unauthorized modification or destruction. Important for maintaining the accuracy and reliability of information and systems.
- Availability: Ensuring that authorized users have access to information and systems when they need them is critical for many businesses and organizations.
- Legal and regulatory compliance: Security is often necessary to meet legal and regulatory requirements, such as data protection laws and industry-specific regulations.
- Reputation and trust: A breach of security can damage an organization's reputation and lead to a loss of trust from customers and clients.
- Financial impacts A security breach can result in financial losses, such as the cost of responding to the breach, lost business, and legal expenses.

Why Security is Important

- *Security is important because it helps to protect sensitive information, maintain the integrity of data and systems, and ensure the availability of resources for authorized users. It is also essential for meeting legal and regulatory requirements and maintaining trust and reputation*

Why study information security?

- To protect computers, networks, and the information they store, organizations are increasingly turning to information security specialists

- *Studying information security empowers individuals to contribute to organizational protection, pursue various career opportunities, and maintain the integrity of systems and data in an increasingly digital and interconnected world.*

Becoming an Information Security Specialist

- Obtain a degree: Most information security jobs require at least a bachelor's (or master) degree in a field such as computer science, information technology, or cybersecurity.
- Gain experience: Many information security jobs require some level of experience. You can gain experience through internships, part-time jobs, or by volunteering your skills to organizations in need.
- Get certified: Many information security jobs require or prefer candidates who are certified. There are several different certifications available, such as the Certified Information Systems Security Professional (CISSP) and the Certified Ethical Hacker (CEH).
- Stay up-to-date: The field of information security is constantly evolving, and it is important to stay up-to-date on the latest technologies and best practices.
- Build a home laboratory
- Network: Building relationships with other professionals in the field can be helpful in finding job opportunities and advancing your career.

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*

Security Mindset

- *What do we mean by the security mindset?*
  - Security mindset is the ability to be able to look for and identify potential or actual compromise.
    - This could be compromise or potential compromise of a process, system, application, operating system, platform, infrastructure and even a person
  - The security mindset involves thinking critically about potential security risks and vulnerabilities.
  - It involves being aware of the potential consequences of using new products or technologies
  - It involves considering the potential risks and vulnerabilities that may be present, and taking a proactive approach to identifying and addressing potential security issues.
  - *A security mindset is important for individuals and organizations to protect against cyber threats and maintain the confidentiality, integrity, and availability of information and systems.*

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

- We need to learn to think with a security mindset
- Security mindset
  - It requires you to think like an adversary - to be constantly thinking about how a malicious party might circumvent the goals of a system or product
    - *who is the bad actors, what possibly can exploit, what vulnerability do we have, and if they successful exploiting vulnerability, what the attack going to be.*
  - 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

Security Mindset

"Security requires a particular mindset. Security professionals - at least the good ones - see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it".
Bruce Schneier

Computer security and Information Security

- *Computer security and information security are related, often used interchangeably, but they are not the same thing*.
- Computer security
  - Refer specifically to the protection of computer systems and devices from threats such as unauthorized access, use, modification, or destruction.
  - It involves protecting the hardware, software, and data that make up a computer system.
- Information security
  - A broader term that encompasses the protection of information and information systems from a variety of threats.
  - This includes protecting against cyber threats such as hacking and malware, as well as physical threats such as theft or damage to hardware.
  - Also involves protecting the confidentiality, integrity, and availability of information, and ensuring that information is secure throughout its lifecycle, from creation to disposal.

Computer security and Information Security

- *So, while computer security is a subset of information security, the two terms are not interchangeable.*
- *Information security includes the protection of all types of information and information systems, not just computers.*
- Both computer security and information security are important for protecting sensitive and confidential information, and for ensuring the integrity and availability of information and information systems.

History of Information Security

- The history of computer security dates back to the 1950s, when the first computers were being developed.
- At the time, computers were large and expensive, and were only used by a small number of people, so security was not a major concern.
- As computers became more widely used, however, the need for security increased.
- In the 1960s and 1970s, computer security focused mainly on protecting against physical threats, such as unauthorized access to computer facilities or the theft of computer hardware.
- In the 1980s, the focus shifted to protecting against software-based threats, such as viruses and malware.
- The rise of the internet in the 1990s led to an increase in cyber threats, such as hacking and network attacks, and the field of computer security evolved into the broader field of information security.

History of Information Security

- Today, information security encompasses a wide range of technologies and practices that are used to protect information and information systems from a variety of threats.
- This includes protecting against cyber threats such as hacking and malware, as well as physical threats such as theft or damage to hardware.
- Information security also involves protecting the confidentiality, integrity, and availability of information, and ensuring that information is secure throughout its lifecycle, from creation to disposal.

The Evolution of Computer and Information Security: From Early Computers to the Cloud

- Early computers
  - In the early days of computing, security was not a major concern.
  - Computers were used primarily by governments and large corporations, and access was limited to a small number of trusted individuals.
- Rise of the internet
  - With the advent of the internet and the proliferation of personal computers, the need for security increased.
  - Hackers began targeting computers and networks, and viruses and other malware became a significant threat.
- Development of antivirus software
  - In response to the increasing threat of malware, companies began developing antivirus software to protect against viruses and other malicious software.
- Emergence of cybersecurity
  - As the internet continued to grow and become more central to daily life, cybersecurity emerged as a distinct field of study. Governments, businesses, and individuals all began taking steps to protect themselves against cyber threats.

The Evolution of Computer and Information Security: From Early Computers to the Cloud

- Growth of information security
  - With the increasing reliance on computers and the internet to store, process, and transmit sensitive information, the field of information security emerged. Information security focuses on protecting the confidentiality, integrity, and availability of information and data.
- Rise of the cloud
  - The growing use of cloud computing has led to the need for additional security measures to protect data stored in the cloud.
- Current state of security
  - Today, computer and information security are major concerns for individuals, businesses, and governments around the world.
  - With the increasing use of the internet and connected devices, the need for effective security measures continues to grow.

What is Security

- A state of being secure - refers to a condition of being protected from danger or harm; also, it can refer to the actions taken to make someone or something secure.
- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- The Confidentiality, Integrity, and Availability Triad (CIA) is the information security model of most organizations when managing data.
- To achieve a state of security, organizations often use a combination of policy, awareness, training, education, and technology.
    - These tools can help to prevent security breaches and protect against cyber threats.

Key Security Objectives: Three Security Goals

- In the context of computers, security generally means three things:
  - Confidentiality
    - Restricting access to systems and data to only authorized parties, protecting sensitive information from unauthorized disclosure.
  - Integrity
    - Protecting data from unauthorized or improper modification, maintaining the trustworthiness and accuracy of the information.
  - Availability
    - Ensuring that systems and resources are accessible to authorized users when needed, and that services are not denied to them, particularly during emergencies or disasters.

CIA Triad

- The CIA Triad is a fundamental concept/security model in information security and stands for three core principles: confidentiality, integrity, and availability.
- *It helps to ensure that sensitive data and resources are protected from unauthorized access, alteration, or disruption, and that they remain available to authorized users when needed.*
- These principles are used as a guide to design and evaluate security policies, systems, and practices in order to protect information and data.
- Expanded into list of critical characteristics of information, including authenticity, accountability, non-repudiation, and reliability.

CIA Triad: loss of security

- A loss of security refers to a situation where one or more elements of the CIA Triad -Confidentiality, Integrity, or Availability- is compromised, leading to potential risks, vulnerabilities, or breaches in information security.
- Let's examine how a loss of security can impact each element of the CIA Triad

CIA Triad: loss of security

- Confidentiality:
  - Prevent unauthorized reading of information
  - A loss of confidentiality is the unauthorized disclosure of information.
    - *If confidentiality is lost, sensitive information may be accessed or disclosed to unauthorized individuals or entities. This can lead to financial loss, reputational damage, legal liabilities, and other negative consequences.*
- Integrity:
  - Prevent unauthorized writing of information
  - A loss of integrity is the unauthorized modification or destruction of information
    - *If integrity is lost, data or systems may be modified or destroyed in an unauthorized manner. This can lead to incorrect or unreliable information, business continuity issues, and other negative consequences.*

Availability:

  - Ensures data is available in a timely manner when needed
  - A loss of availability is the disruption of access to or use of information or an information system
    - *If availability is lost, authorized users may be unable to access data or systems when needed. This can lead to lost productivity, financial losses, and other negative consequences.*

Prevention and Mitigation

- Addressing and preventing a loss of security requires a comprehensive approach to information security management.
    - Implement strong access controls, authentication, and encryption.
    - Monitor and audit for unauthorized access or alterations.
    - Employ redundancy, disaster recovery plans, and robust infrastructure.
    - Proactive security measures, continuous monitoring, and risk assessment.
    - Timely incident response to minimize potential security losses.

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 System (IS) is the entire set of hardware, software data, people, procedures, and networks that enable a business to use information.
    - set of components necessary to use information as a resource in the organization
- 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.

We worry about security when we have something of value and there is a threat source that poses some kind of risk could be harmed

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.
- 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 or gaps in the security system that could be exploited[1] 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)

[1] *Exploits are the means through which a vulnerability can be leveraged for malicious activity by hackers; these include pieces of software, sequences of commands, or even open-source exploit kits.*

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.

Threats

- Threats are potentials for vulnerabilities to turn into attacks on systems
- Threats are potential dangers or harmful events that could exploit vulnerabilities in a system or organization, leading to negative impacts.
- 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
- Attacks lead to compromises or security breaches.
- 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/Threat Source

- Entity that attacks/carrying out the attack, or is threat to system (adversary, attacker, malicious user)
  - Cybercriminals: want to profit from your sensitive data for financial gain
  - Nation-states: countries do it for political advantage or for espionage.
  - Hacktivists: Activists who want others to notice their work to inspire action or change.

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

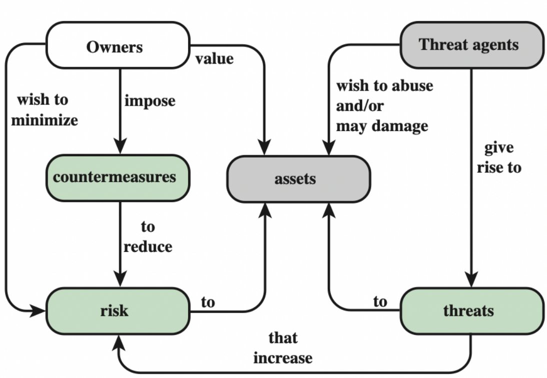
Risk

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability
- Risk is the likelihood that a threat will exploit a vulnerability to cause damage to an asset.
- It's a combination of the potential impact and the probability of a threat occurring.
- 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.
    - *Ideally, a countermeasure can be devised to prevent a particular type of attack from succeeding. When prevention is not possible, or fails in some instance, the goal is to detect the attack and then recover from the effects of the 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



How secure should we make it?

- Principle of Easiest Penetration
- Principle of Adequate Protection

Principle of Easiest Penetration

- A security principle that states:
  - a system is only as secure as its weakest link, and
  - an attacker will often target the easiest point of entry in a system rather than the most obvious one.
- This principle emphasizes the importance of identifying and addressing potential vulnerabilities in a system, as well as testing and regularly reviewing the security controls that are in place.
- To secure a system, it is essential to think like an attacker, and understand how they may attempt to exploit vulnerabilities.

Principle of Adequate Protection

- Highlights the need for balancing the cost of security measures with the potential impact of security incidents
- It advises organizations not to overspend on security measures to protect a system that would only cause limited damage if compromised.
- It is crucial to have a proper security risk assessment, to weigh the costs and the risks, and make sure that the right protection measures are in place, not too much or too little.
- This principle considers both technical and economic factors in implementing the most effective security measures to protect the assets.

- Security is economic *Don't spend $100,000 to protect a system that can only cause $1,000 in damage*

Weakest link

Balancing Information Security and Access

- Balancing information security and access requires a balance between protection and availability.
- This is known as the security vs. accessibility trade-off.
- Organizations must determine the appropriate level of security measures to implement based on the potential risks and consequences of a security breach.
- This includes balancing the need to protect sensitive information with the need to allow employees, customers, and other stakeholders access to that information.
- *The goal is to find a balance that ensures the confidentiality, integrity, and availability of information while also enabling the organization to function effectively.*
- Must allow reasonable access, yet protect against threats

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

- Cryptography is the practice of protecting data by converting it into an unreadable format (encryption) that can only be accessed by someone who has the proper decryption key.
- Some of the common uses of cryptography include:
  - Protecting data by making it unreadable to an attacker through the use of encryption algorithms.
  - Authenticating users with digital signatures that use a combination of encryption and hashing to prove the identity of the sender.
  - Authenticating transactions with cryptographic protocols such as `SSL/TLS`, which provide secure communication between web browsers and servers.
  - Ensuring the integrity of stored data by using cryptographic techniques such as message authentication codes (MAC) to detect unauthorized changes to data.
  - Aid customers' privacy by having their personal information automatically become unreadable after a certain length of time[1]

[1] *many organizations have implemented a time limit to have the personal information of their customer automatically become unreadable after a certain length of time for protecting their customer's privacy.*

Software controls

- Security measure that are used to protect computer systems and networks from unauthorized access and other types of threats.
- Some common examples of software controls include:
    - Passwords and other forms of access control, such as biometric authentication, which are used to restrict access to systems and data to authorized users.
    - Operating systems that include built-in security features, such as user accounts and permissions, which can be used to separate users' actions from each other on a system and prevent one user from accessing or modifying another user's data.
    - Virus scanners watch for some kinds of malware
    - Development controls[1] enforce quality measures on the original source code
    - Personal firewalls that run on your desktop and monitor incoming and outgoing network traffic in order to block unauthorized access or suspicious activity.

[1] *Development controls, which are practices and tools that are used to enforce quality measures on the original source code, such as code review and testing, to help identify and fix any potential vulnerabilities or bugs that could be exploited by an attacker.*

Hardware controls

- Security measure that use separate hardware devices to protect computer systems and networks
- Some common examples of hardware controls include:
  - Biometric readers, such as fingerprint readers, which are used to authenticate users based on their unique physical characteristics, providing an additional layer of security beyond traditional username and password authentication.
  - Smart tokens, which are small, portable devices that generate one-time passcodes, which are required in addition to a user's regular credentials to gain access to a system.
  - Firewalls, which are specialized hardware devices that monitor and control incoming and outgoing network traffic, blocking unauthorized access and other suspicious activity.
  - Intrusion detection systems, which are used to detect and alert on suspicious activity on a network, such as unauthorized access attempts, traffic that appears to be coming from a compromised device, and other types of malicious activity.

Physical controls

- Security measure that are designed to protect the hardware itself and prevent physical access to the console, storage media, and other critical components of a computer system or network.
- Some common examples of physical controls include
    - Locks, such as keyed locks, combination locks, and smart card locks, which are used to restrict access to computer rooms, data centers, and other sensitive areas.
    - Security guards, who can monitor access to sensitive areas and prevent unauthorized personnel from entering.
    - Off-site backups, which can include storing copies of critical data at remote locations to protect against the possibility of fire, flood, or other types of natural disasters.
    - Location-based controls, such as placing data center or power plant in area with less risk of natural disaster like earthquakes, tsunamis, etc.
        - *Don't put your data center on a fault line in California*
        - *Don't put your nuclear power plant in a tsunami zone*

Security Policy

- A set of rules and practices that specify how a system or organization provides security services to protect its assets.
- It defines the measures that are in place to ensure the confidentiality, integrity, and availability of data, networks, and systems.
  - *i.e., a set of rules and guidelines that an organization creates to keep its information, technology, and resources safe.*
- Security policies are like a set of instructions that everyone in the organization follows to make sure everything stays secure.

Security Policy

- Security policies cover things like:
  - Who can access what
    - *explain who is allowed to use certain computers, programs, and information.*
  - How to keep data safe
    - *provide steps for keeping data (like customer information or trade secrets) safe from being stolen or lost.*
  - What to do if something goes wrong
    - *give instructions on how to handle problems like computer hacks, data breaches, or other security issues.*
  - Using the internet and emails safely
    - *provide guidelines for using the internet and emails in a way that doesn't put the organization at risk.*
  - Making sure software is up to date
    - *explain why it's important to regularly update software and how to do it.*
  - Training employees
    - *include instructions for teaching employees about security risks and how to protect the organization.*
  - Physical security
    - *might cover things like locking doors, keeping servers in safe places, and making sure only authorized people can enter certain areas.*

Aspects of Security

- The (Open Systems Interconnection) security architecture provides a systematic approach to address the dynamic and evolving nature of security challenges in information systems.
- By focusing on attacks, mechanisms, and services, it offers a framework for organizations to build and maintain a secure environment for their data, systems, and networks.
  - Designed to provide a comprehensive framework for addressing and enhancing the security of information systems.

Aspects of Security

- Security Attack
  - Any action that aims to compromise the security of information owned by an organization.
  - These attacks can take various forms, including unauthorized access, disclosure, modification, or destruction of data, systems, or networks.
  - The goal is to protect against such actions and maintain the confidentiality, integrity, and availability of information.
- Security Mechanism
  - Methods designed to detect, prevent, or recover from security attacks.
  - They act as security barriers to safeguard an organization's assets.
  - These mechanisms may operate independently or in conjunction with others to provide specific security services.
  - Some common security mechanisms include
  - Common security mechanisms are as follows:
    - Cryptography
    - Message digests and digital signatures
    - Digital certificates
    - Public Key Infrastructure (PKI): A framework that manages digital keys and certificates, facilitating secure communication.

Aspects of Security

- Security Service
  - Security services are functionalities offered by security mechanisms to enhance the security of a system.
    - Security services represent the specific functionalities offered by security mechanisms.
  - These services can include authentication, access control, data confidentiality, data integrity, and non-repudiation.
  - By employing security mechanisms and services, organizations can establish a robust defense against potential security threats.
    - *e.g., authentication ensures that only authorized individuals or systems access resources, access control regulates permissions, data confidentiality protects sensitive information from unauthorized disclosure, and non-repudiation prevents denial of actions taken.*
  - By providing these services, the OSI security architecture helps organizations establish a robust and multi-faceted defense against security threats.

Security Services

- There are several core security services that organizations often utilize:
  - Authentication
  - Access Control
  - Data Confidentiality
  - Data Integrity
  - Non-repudiation
  - Availability

Security Services: Authentication

- Used to assure the identity of the sender or creator of the data.
- It is a process of verifying the identity of a user, device, or system, to ensure that it is not an imposter or malicious actor.
- Two specific authentication services
  - Peer Entity Authentication: This service is used to authenticate the identity of other entities with which the system is communicating.
  - Data Origin Authentication: This service is used to authenticate the origin of a message or data, to ensure that it was sent by the entity that it claims to be from.

- *Both of these services are important for ensuring the authenticity and integrity of communication, in order to prevent unauthorized access, tampering, or impersonation. It ensures that the data or communication is from the intended source and not an imposter or an attacker.*

Security Services: Access Control

- Used to prevent misuse of resources and ensure that only authorized users have access to the available resources.
- Access control can take many forms, such as:
  - Discretionary Access Control (DAC) which allows the owner or administrator of a resource to decide who is allowed to access it.
  - Role-based Access Control (RBAC) which allows access based on the role of the user within the organization.
  - Mandatory Access Control (MAC) where the access is granted based on a set of predefined rules.
  - Attribute-based access control (ABAC) where the access is granted based on the attributes of the requestor, the resource, and the context in which the access request is made.

Security Services: Data Confidentiality

- Responsible for ensuring that the data is kept extremely safe from third-party intruders.
- Types of data confidentiality services:
    - Protecting data in transit: used to protect data that is being transmitted between two parties, such as over a network or through the internet. This can include both passive and active protection measures, such as encryption, to prevent unauthorized access or eavesdropping.
    - Protecting data at rest: used to protect data that is stored on a device or system, such as on a HD or in a DB. This can include access controls, encryption, and backups to prevent unauthorized access or data loss.
    - Protecting traffic flow from analysis: used to protect the characteristics of the traffic flow, such as the source and destination, frequency, length and other characteristics of the traffic on a communication facility. This can include measures such as traffic padding and traffic encryption, to prevent an attacker from observing the traffic flow.
- *Data Confidentiality services are important for maintaining the privacy and security of sensitive information, and they can take many forms to protect data in transit, at rest and traffic flow from analysis.*

Security Services: Data Integrity

- Ensure that the transmitted information received by the receiver is well-authenticated and there is no tampering with the information received.
- It helps to ensure that the data received is the same as the data that was sent, and that it has not been modified, deleted, or tampered with in any way.
  - Message integrity: used to ensure that the data integrity of a specific message, it uses a digital signature, or message authentication code (MAC) which provides a hash of the data and a secret key, and appending that to the message.
- *Data Integrity services are important for maintaining the authenticity and accuracy of transmitted information, and they can take many forms to protect a stream of messages, individual messages, or selected fields within a message.*

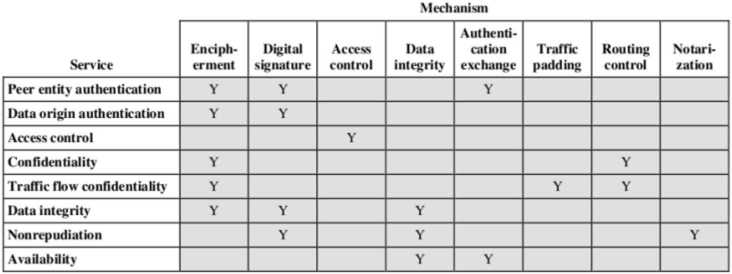
Security Services: Nonrepudiation

- Used to Prevent either sender or receiver of a transmitted message from denying that the message was sent or received.
- 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

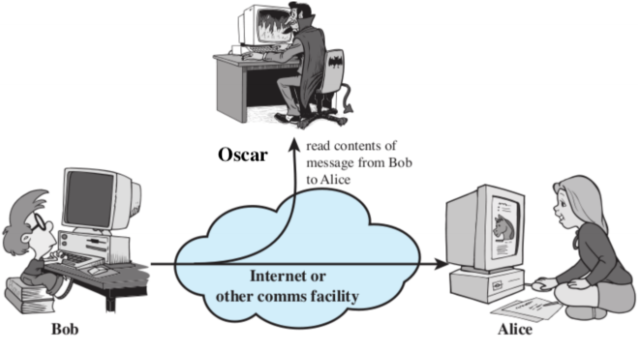


	Mechanism							
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Attacks on Communication Lines

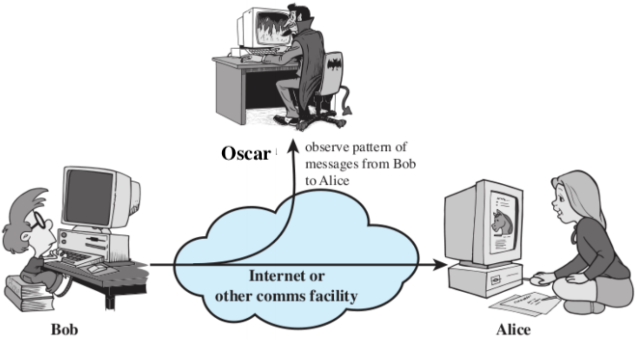
- Passive Attack
  - Attempt to learn or make use of information, but not affect system resources, e.g.,
    1. Release message contents
    2. Traffic analysis
  - Relatively hard to detect, but easier to prevent (usually by encryption)
- Active Attack
  - Attempt to alter system resources or affect 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


Oscar
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

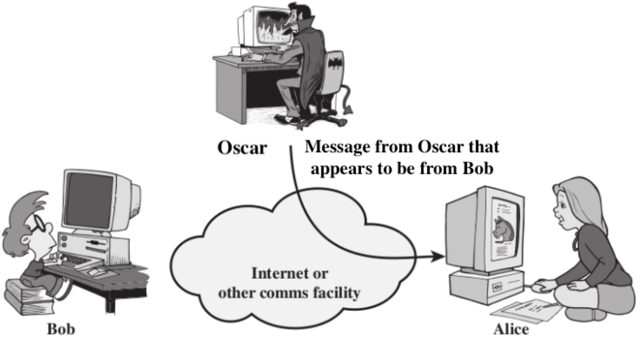
Message Content is the type of passive Attack that involves the intruder stealing all the message/data transmitted. Here, the information gathered by the intruder is stolen unethically.

Traffic Analysis


Oscar
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

Masked Traffic Analysis: This type of passive Attack involves messages/data being encrypted before transmission. Here, the message being masked/encrypted the intruder can't read the message but only understand the pattern and length of encryption.

Masquerade Attack


Oscar
Message from Oscar that appears to be from Bob
Internet or other comms facility
Bob
Alice

Masquerade is a type of active attack, the attacker tampers the information received by the receiver by claiming itself as the sender.

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack.
    - For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place

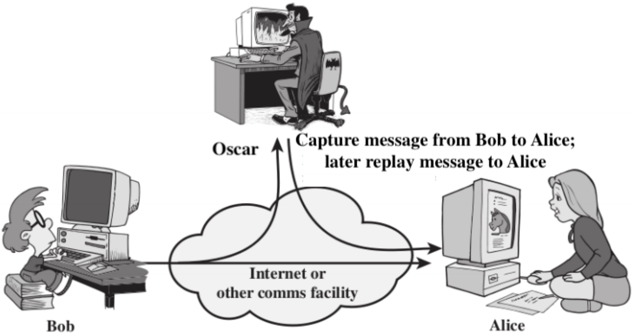
“On the Internet, nobody knows you’re a dog”[2]

61
P. Steiner

“On the Internet, nobody knows you’re a dog.”

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

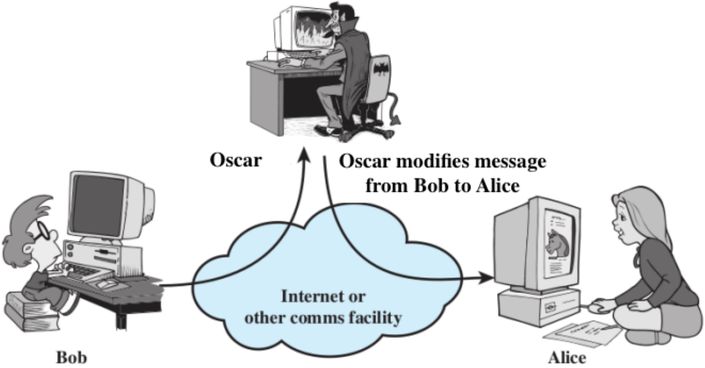
Replay Attack


Oscar
Capture message from Bob to Alice;
later replay message to Alice
Internet or
other comms facility
Bob
Alice

Replay is a type of active attack, the attacker attacks the transmitted message through a passive channel and make the final message received by the receiver may appear to be authorized and safe

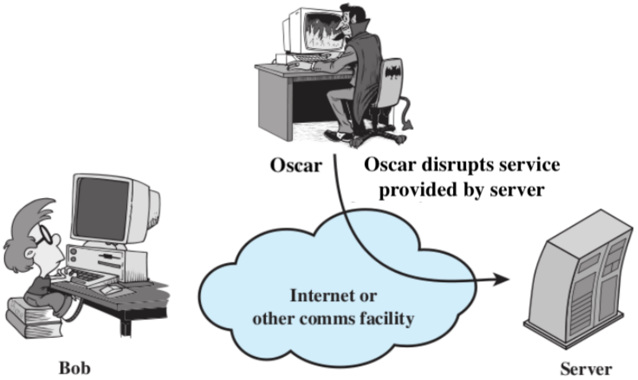
- Involves the passive capture of a previously transmitted message and replaying it to produce an unauthorized effect

Modification Attack


Oscar
Oscar modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

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

Denial of Service Attack


Oscar
Oscar disrupts service provided by server
Internet or other comms facility
Bob
Server

Denial of Services is a type of active attack, the receiver is prevented from receiving the transmitted message as there is an overflow of requests to the receiver, which makes the services hampered from their usual behavior.

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

Computer Security Strategy and Principles

The first step in devising security services and mechanisms is to develop a security policy.

- 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

Organizations Involved in Security Standards Development

- Notable organizations involved in security standards include:
  - The International Association of IT Security Professionals (ISC): This organization is focused on the development of security professionals and the certification of IT security professionals worldwide.
  - The Center for Internet Security (CIS): This organization is focused on the development of best practice guidelines and standards for IT security.
  - The Payment Card Industry Security Standards Council (PCI SSC): This organization is focused on the development of standards for protecting cardholder data for the payment card industry.
  - The Open Web Application Security Project (OWASP): This organization is focused on the development of best practice guidelines and standards for web application security.
  - The Internet Engineering Task Force (IETF): This organization is focused on the development of standards for the Internet's infrastructure and protocols.
- *All these organizations work together to develop and maintain security standards that are essential for the safety and security of individuals and organizations worldwide.*

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