CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

- Why we need Computer Security?
- What is the Computer Security (Cybersecurity)? Its definitions, scope, and objectives
- Security Attacks
- Classification of hackers
  - The color of their Hats
  - What color of the hat you like to put on?
- Data privacy, protections in mobile platforms
  - Social Engineering
- System Security / Network Security
- Security in cloud computing environments
- Cryptography and Blockchains

Why we need Computer Security?

- My “horrible” experience
  - I chose an independent study instead of a capstone as a requirement of college graduation, about 20 years ago. (An IS/MIS related study)
  - My major --- Business
  - I want to see if tele-conferencing systems can help the people to make a decision quickly and efficiently
    - It proves to be effective and that is why we have “Zoom”
  - So, I designed a series of experiments and try to collect user’s data during their interactions
  - System:
    - PHP, Apache, MySQL and some Javascripts for UI.
    - Red Hat Linux v7.0

Why we need Computer Security?

- Our server is 7x24.
- One day, when I used to perform a reboot, something very horrible happens!
- You know the traditional booting style of Linux will produce lots of textual message. They are printed out onto the screen during the boot process.
- I saw lots of error messages!
  - I was thinking my hard drive was dying? Hardware errors?
  - Backdoors!
- The most horrible thing!
  - The data where I collected from users are stored in MySQL
  - Now, it totally looks like this! (see the next page)
  - SQL injection!

Why we need Computer Security?

User	IP Address	Talks in the meeting	For or against the proposal
John	!@##$#@%$T#RFsdfdfR$#	t5yk5rf34@#R$WEFDSA	87U^JYHTDRYGredvfdvf
Mary	Fsdfgeorf#@#!$Sdsdfrr4	Csdw#%RFD	%^&U^TYh4f43
Lisa	scewwe#@$@WEF43	Ytju7ujry5$^&%YRTGR	#!!@R$T#%TE$5654R
…	$#RferFferGERg	ERT%$GRTRFER54t44	&*O(*KJ5r6tG%R%

Why we need Computer Security?

  - There is no surprise for the earlier version of Linux, PHP and MySQL
  - My classmates are gone after May but I kept working on the coding and deploying the system, and re-doing the experiments.
  - I finally can graduate in July!
- The 1st time I realized the hackers, they are existing everywhere in the internet
- We need to understand the computer security, at least, to protect your works from being sabotaged or the system in your daily uses.

What is the Computer Security (Cybersecurity)? Its definitions, scope, and objectives

- According to the definition of the book (the only book I referenced in the syllabus)
  - Computer Security (or Cybersecurity) --- is the protection of information that is stored, transmitted, and processed in a networked system of computers.
  - All the devices with internet connection capability are included.
- Security Objectives (3 concepts)
  - The three concepts form what is often referred to as the **CIA triad.**
  - NIST is a governmental agency, they used to mention the 3 concepts as follows:

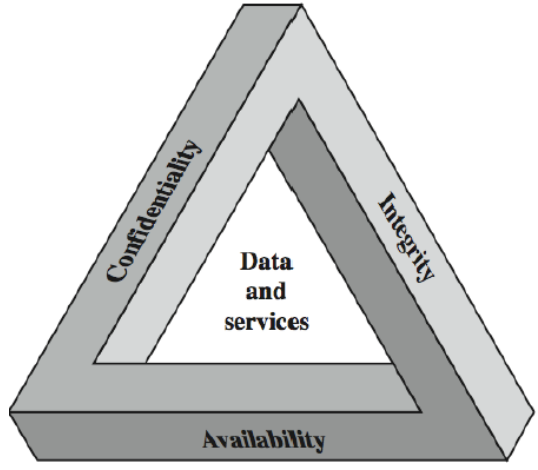
National Institute of Standards and Technology

Government agency

NIST
National Institute of Standards and Technology

What is the Computer Security (Cybersecurity)? Its definitions, scope, and objectives

- **Confidentiality:**
  - **Data confidentiality and Privacy**
    - Confidential information is not made available or disclosed to unauthorized individuals
- **Integrity:** (Guarding against unauthorized information modifications or destruction)
  - **Data Integrity**
    - Assures that data and the related programs are changed only in a specified and authorized manner
  - **System Integrity**
    - Assures that a system performs its function without deliberate or inadvertent unauthorized manipulation of the system.
- **Availability:**
  - Ensuring timely and reliable access to and use of information
    - The service is working properly and is not denied to authorized users.



Security Attacks

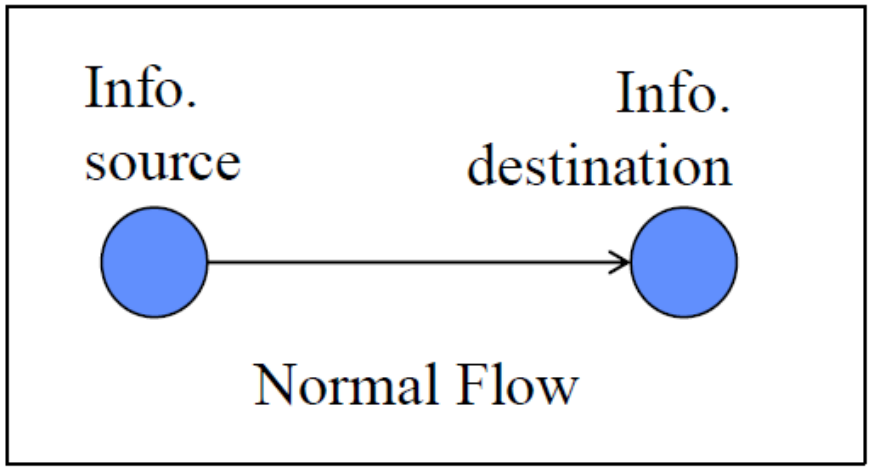
- A useful means of classifying security attacks, from the introduction of the book, are *passive attacks* and *active attacks*
- Passive attacks
  - A passive attack attempts to learn or make use of information from the system but **does not affect system resources**
  - For example, eavesdropping, sniffing sensitive data or monitoring of data transmissions
  - The goal of the attacker is to collect, analyze and release the content of the data
  - Passive attacks are very difficult to detect because they do not involve any alteration of the data

Security Attacks

- Active Attacks (This kind of attacks is very hostile)
    - The common attacks in this category are as follows:
        - **Masquerade**
            - One entity pretends to be a different entity
                - For example, if someone uses a normal account to login then quickly execute a backdoor program to get the access rights of the root.
                - Or, if one hacker captures root's password and use this password to login to the system (replay)
        - **Data Modification or Fabrication**
                - Here is a high level description: "Allow John Smith to read confidential file accounts"
                - What if I can modify that as "Allow Fred Brown to read confidential file accounts" ?
        - **Denial of Service**
                - The goal is the disruption of a specific service or an entire network.
                - A very common example: DDoS attack (Ping (ICMP) flood)
                - Sometimes, that means --- your security mechanism is really good. I had nothing to do but to paralyze your service

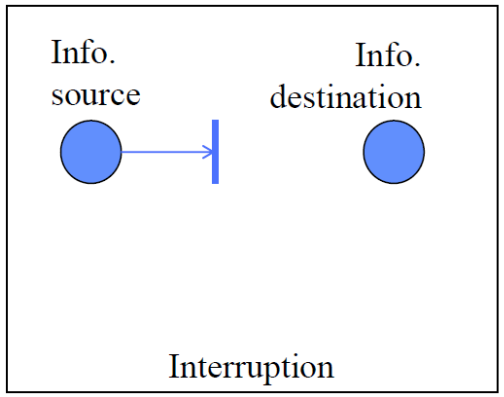
Security Attacks

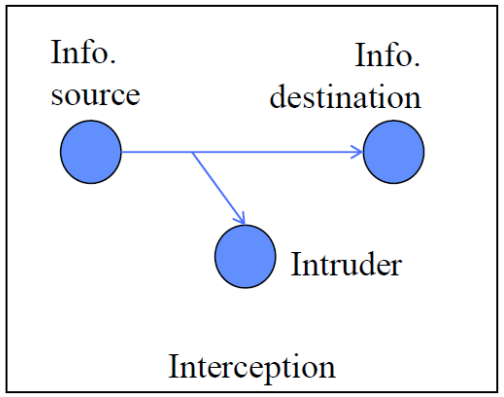
- From a service provider's perspective, the info. source provider has to be trusted and secure. It cannot get compromised.
- When the host is trusted and secure: (everything looks OK)

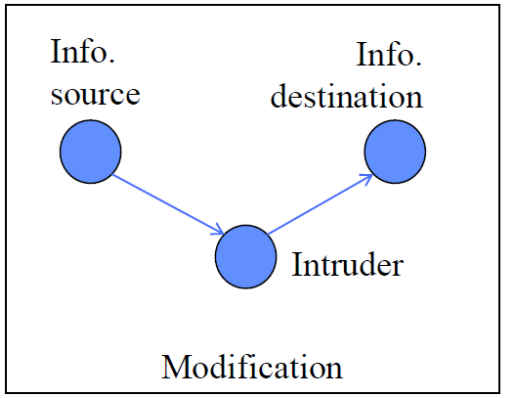


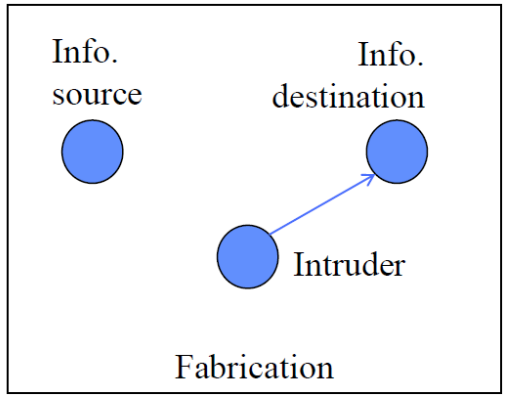
Security Attacks

- When the server is not secure or a presentation of hackers, it can be like this:









The upper 2 figures represents passive attacks and the lower 2 are active attacks

Classification of hackers

- The term *hacker* will be used to refer to any individual, or groups, authorized or otherwise, who is attempting to surreptitiously access a computer system or network, without regard to their ethical intentions.
- The term ***cracker*** is also commonly used in place of hacker – specifically in reference to those who are attempting to break passwords, bypass software restrictions, or otherwise circumvent computer security.
- Cracker is a kind of hacking activity and it is a subset of hacking activity.

The Color of their Hats

- “Good guys” and “bad buys” can be easily distinguished by the “color” of their cowboy hats, especially in the classic Hollywood scenes of the old American west movies.
- In this class, you might have the chance to approach to some hacking skills, but don’t do the hacking activities!
  - I don’t to bail you out of the detention
  - I don’t like to get into trouble, please. ^_^

The Color of their Hats

- *BLACK HAT*
  - A ***black hat*** hacker (or cracker) is one who is unambiguously attempting to subvert the security of a computer system (or closed-source software code) or networking against the will of its owner.
  - The goal of the black hat hacker is to gain unauthorized access to the system, either to obtain or destroy information, cause a disruption in operation, deny access to legitimate users, or to seize control of the system for their own purposes.
    - Mostly, but is not 100% correct. They are hacking for the money.
  - No matter what kind of “noble intentions” they claimed. For example, entities from adversarial nations that are hacking for the purposes of warfare. They are still black hat hackers regardless of their justifications

The Color of their Hats

- *WHITE HAT*
  - A ***white hat*** hacker has been specifically authorized by the owner or custodian of a target system to discover and test its vulnerabilities.
  - This is known as ***penetration testing***.
  - You guys will definitely learn that in the later of the class
  - The white hat hacker uses the “same tools” and procedures as a black hat hacker, and often has equal knowledge and skills.
  - In fact, it is common for a former black hat to find legitimate employment as a white hat because black hats typically have a great deal of practical experience with system penetration.
  - Government agencies and corporations like to hire them because they have experiences

The Color of their Hats

- *GRAY HAT*
  - As you can make a quick guess from the keyword --- “gray”. A gray hat hacker does not necessarily have the permission of a system owner or custodian, and therefore could be considered to act unethically when attempting to detect security vulnerabilities
  - However, a gray hat is not intended to performing bad activities. Rather, they are essentially conducting unauthorized penetration testing with the goal of alerting the owner to any potential flaws.
  - Sometimes, they not only want to warn the system owner but also like to show off

What color of the hat you like to put on?

- What color of the hat you want to put on? ^_^
  - I would like the one I can get paid. You know what I mean.

Data privacy, protections in mobile platforms

- Lots of people, they don’t even need to have a laptop (because they already have a desktop), but cannot live without smart phones.
- Many of us are getting used to pay the bills or manage our accounts registered in the commercial websites, for example, banks, Amazon or Walmart.
- Mobile platforms, are becoming more and more vulnerable, not really for the hacking activities but for a more realistic thing --- the cyber warfare of the social engineering.

Social Engineering

- You know what? If I would like to conduct the social engineering, I don’t even need to know complicated programming / coding skills. All I need to do is:
  - Use the related tools / software if it is needed.
  - Target the victims with specific backgrounds
  - Try to make up a story to build up a pipeline
  - Role playing: hire the related guys to do the role plays.
- Everything starts with your, the most sensitive data --- phone numbers!
- I will tell you my friend’s use case in the later class!

Social Engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Mostly, it is presented as scams to lure the users to expose their data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via interactions. (So it is step by step. You can stop the whole process if you are aware it is a social engineering)
- Social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.
- In addition, hackers try to exploit a user's lack of knowledge.
  - An use case – It was related with Netflix scams. It almost got me ☺

Data privacy, protections in mobile platforms

- I remember to setup my phone number, registered in the social media or Apps as private, for example, Facebook.
  - But how did you know your account registered in Walmart didn’t get hacked, for example?
  - Because, you have a phone number registered in that website.
  - Not just the Walmart, it could be MANY.
    - i.e. Pizza Hut or Domino’s
  - If ANY ONE of the website get hacked, your phone number, the most sensitive data is spreading in the internet
- It seems that it is very hard to do protect such kind of data, there is still something we can do to protect ourselves.
- You will learn the skills and details in the later of the classes

System Security / Network Security

- You will lean the related tools being a “white hat” hacker
  - Penetration testing
- You might learn the steps of the most commonly seen steps for hacking activities
  - For example, if I’m a hacker the first step is to know is there any services open in the targeting system and their ports.
- You might learn the commonly seen system in the older version of Linux distributions
- You will learn how to use the tools to analyze the packets sending in the networks.

Security in cloud computing environments

- You might have the chances to learn the security mechanism in the AWS. For example,
  - AWS Identity Services can help you manage identities, resources, and permissions.
  - AWS Detection and Response Services can help you identify potential security misconfigurations, threats, or unexpected behaviors.
- They offer tons of services (security related) but we cannot go through all of them for the very limited amount of time. I will pick up a bunch of useful ones.

Cryptography and Blockchains

- Traditionally, cryptography referred almost exclusively to "encryption", which is the process of converting plaintext into an unintelligible form of ciphertext.
- Decryption is operated in the reverse way. It is moving from the unintelligible ciphertext back to plaintext.
- A cipher refers a pair of algorithms that carry out the “encryption” and the “reversing” decryption.
- The detailed operation of a cipher is controlled both by the algorithm and the “key”.
- The key distribution algorithm is traditionally a challenging part in the related research area.

Cryptography and Blockchains

- An overly simplified model

- Since Cryptography is a way of securing data against unauthorized access, in the blockchain, cryptography is used to secure transactions between two nodes in the blockchain network.
- There are two main concepts in blockchain: cryptography and hashing

Cryptography and Blockchains

- Cryptography encrypts messages in the P2P network, and hashing is used to secure the block information and helps the linkage of the blocks in the blockchain.
- You will learn this and its applications in this class.