Course Aims

- Course Spec:
- To provide an overview of Cyber Security, providing broad coverage.

解释网络安全的基本概念，包括道德黑客、数字取证和渗透测试。

- Explain cyber security fundamentals concepts including Ethical hacking, Digital Forensics and Penetration testing;
- Explain a number of different security protocols;
- Evaluate an existing or proposed system in terms of potential vulnerabilities and recommend the most appropriate security solution to apply in a number of different scenarios;
- Summarise the key vulnerabilities, threats, and attacks with regards to network security and explain approaches to mitigate these issues;
- Implement an aspect of cyber security;

INTRO TO CYBER SECURITY

Name some cyber attacks

Weak Passwords

网络钓鱼攻击

Phishing attacks

Trade secrets and insider data theft

勒索软件

Ransomware

Malware Attacks

内部威胁

Insider Threats

Sensitive data leaks and breaches

敏感数据的泄露和违规行为

High-level plan for secure system

Systematic thought is required for successful defense

成功的防御需要系统性的思考

- Goal: Protect assets
  - only legible entity/authorized users could receive a file or use the system
- Aspects of Cyber Security (asset protection)
  - ✓ Confidentiality, Integrity, Availability, Authenticity, Accountability, Non-repudiation
- Threat model: assumptions about what the attacker can do
  - ✓ e.g., can guess the password, cannot physically steal our server

High-level plan for secure system

Systematic thought is required for successful defense

- Policy: Some plan (rules) that will get your system to achieve the goal
  - ✓ e.g., set permissions on a file so it's only readable by Alice
  - ✓ Policy must include human components (e.g., do not share passwords)
- Mechanism: Software/hardware that your system uses to enforces policy
  - ✓ user accounts, passwords, encryption
- Often layered: mechanism of one layer is policy of next level down 一层的机制是下一层的政策

Why need Cyber Security?

- To protect
  - Assets
    - Assets are things that need protection and are usually digital, such as files.
  - Some assets, such as keys and passwords, are important for cyber security but are not stored as files.
- Aspects of Cyber Security (asset protection):
  - ✓ Confidentiality, Integrity, Availability, Authenticity, Accountability, Non-repudiation

Confidentiality

- The protection of information in the system so that an unauthorized person cannot access it

- This implies an access control mechanism.

  访问控制机制

  - Users must be identified. **被识别**
  - Users are then authenticated. **被授权**
  - Users are then authorised to access various assets. The access can be controlled, for example, with read, write and execute permissions.

Confidentiality

- **Privacy** is the confidentiality of personal information. 隐私是指个人信息的保密性。
- Examples
  - Using a password to control access.
  - Encrypting files

使用密码来控制访问。
加密文件

Integrity

- Ensure nothing is lost or deleted.
  - Either accidentally or deliberately. 无论是意外还是故意的。
- Make sure nothing is changed.

- Examples.
  - Use a message digest to detect if a file has been changed.
  - Use a public key certificate for network communications.

Availability

有能力满足需求。

- Have capacity to meet demands.
- Resources are allocated fairly.
- Fault tolerance and recovery from failure.

  容错和从故障中恢复。
- Examples
  - Protect against denial of service attacks.

防止拒绝服务攻击。

Authenticity

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- It **validates** the source or origin of data and other file transfers through proof of identity
  - This ensures that the message (email, payment transaction, digital file, etc.) was not corrupted or intercepted during transmission

Accountability

- Accountability **问责制**
  - a crucial element of Building Integrity (BI) initiatives and one of the key principles of Good Governance. A responsible, responsive, and democratic security sector cannot be conceived without accountable personnel, institutions, and procedures.
  - an essential part of an information security plan
  - Pointed towards who is responsible for each cyber role in an organization

Non- repudiation

- Non-repudiation 不可否认的
  - The author / owner of a document cannot say it was not them.
  - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
  - Non-repudiation **provides evidence of data's origin, authenticity, and integrity**
  - **Digital file is properly tracked and users' action are logged**

Case study

- What aspects of security does Gmail have?

Confidentiality

Availability

Integrity

Accountability

Non-repudiation

- Can you give other examples?

Threats

- What are we protecting assets from? Threats
- Different types of asset security are subjects to different threats. 是会受到不同的威胁
  - A threat against confidentiality will be different from a threat against availability.
- When protecting an asset, we need to consider all possible threats.
- There are many different techniques to make sure we have considered all threats.
  - Standard lists of threats.
  - Standard techniques for dealing with them.

Vulnerabilities

- Different ways of protecting assets lead to different vulnerabilities.
- We can check the security of a system in two different ways.
  - From the viewpoint of an attacker. What are the attackers goals? How can they achieve them?
  - From the viewpoint of the defender. What are the system's vulnerabilities?
- All the vulnerabilities collected together are called the **attack surface**.
  - As a defender, we want to reduce the attack surface.

Protection and Risk

- Protecting our assets from threats leads to a discussion of risks.
  - Protection has a costs.
  - The value of an asset might be less than the cost of protecting it.
  - Some forms of protection may be cheaper than others.
- Risks involve the probability of something happening, together with the effect of the attack succeeding. 风险包括某件事情发生的概率，以及攻击成功的影响。

Technical Solutions are Essential

- Unbreakable encryption to keep secrets and ensure data is not changed.
  - The algorithm can't be broken without the key.
  - Keys must be kept secret.
- Digital signatures to allow legally enforceable contracts.
  - So that signatures can't be forged.
- Secure message digests to provide document fingerprints without revealing the document content.
  - So that two different documents can't have the same message digest.
- Secure protocols to make sure the basic building blocks of encryption signatures and message digests are used correctly.
  - So that it is not possible to bypass the use of a key.

… but Not Enough

- People!

- Users may not comply with security policies.
- Organizations may develop policies that users find very difficult to use.
- Developers may not adhere to security guidelines when building systems.
- Regulatory bodies may not provide appropriate policies and rules and then may not enforce them.

- Need to consider socio-technical systems.
  - Consider people as well as the technical aspects of any system.

Questions

1. Explain, with examples, how a system that uses all the best encryption techniques can still be insecure.
2. Explain , with examples, the terms Confidentiality, Integrity and Availability (CIA).
3. Explain with examples how security problems can arise in hardware, software, networks, personnel, site and organization.
   - What CIA aspects are affected by each of your examples
4. What is Security Engineering and how is it similar to / different from Software Engineering?