CAN304 W1

Three key objectives of Computer Security

CIA: Confidentiality, Integrity, Availability.

Confidentiality: 保留对信息访问和披露的授权限制，包括保护个人隐私和专有信息的手段。

Integrity: 防止不当信息修改或破坏，包括确保信息不可否认性和真实性。

Availability: 确保及时可靠地获取和使用信息。

其他的 objectives：

Authenticity: 验证用户是否是他们所说的人 (users' authenticity)；messages' authenticity (integrity)。

Accountability: 确保一实体的操作可以以唯一方式跟踪到该实体；supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action。

Terminology

计算机安全 (computer security)，处理受各种威胁 (threats) 影响的计算机相关资产 (assets)，并采取各种措施 (measures) 来保护这些资产。

System Resource (Asset): Hardware，Software，Data，Communication facilities and networks。

Security Policy: 一组规则和做法，用于指定或规范系统或组织如何提供安全服务以保护敏感和关键的系统资源 (比如删文件要 root 权限)。

Vulnerability: 系统设计、实现或操作和管理中的缺陷或弱点，可能被利用来违反系统的安全策略。

- General categories of vulnerabilities of a computer system or network asset: be corrupted, leaky, unavailable.

Exploit: 利用漏洞 (vulnerability) 的实际事件，术语还指用于利用漏洞的代码或方法。

Threat: 违反安全性的可能性，当存在可能违反安全性并造成伤害的情况、能力、操作或事件时，存在这种可能性。也就是说，threat 是可能利用漏洞的可能危险。

Attack: 被执行的 threat，如果成功，则会导致安全破坏或威胁后果。

Attacker: 执行 attack 的代理。

Countermeasure: 一种操作、设备、过程或技术，它通过消除或阻止威胁、漏洞或攻击、通过最大限度地减少威胁、漏洞或攻击可能造成的危害，或者通过发现和报告威胁、漏洞或攻击以便采取纠正措施来减少威胁、漏洞或攻击。

Types of attack:

Active attack: 试图改变系统资源或影响其操作。

Passive attack: 尝试从系统中学习或利用不影响系统资源的信息。

Inside attack: 由安全边界内的实体（"内部人员"）发起。内部人员有权访问系统资源，但以未经授权者批准的方式使用它们。

Outside attack: 由未经授权或非法的系统用户（"外部人员"）从外围发起。

Threat consequences and attacks

Four kinds of threat consequences:

Unauthorized disclosure，Deception，Disruption，Usurpation.

Unauthorized disclosure: 实体获得对其未获授权的数据的访问权的情况或事件。

可能造成的后果：

- Exposure: 敏感数据将直接发布给未经授权的实体；
- Interception: 未经授权的实体直接访问在授权源和目标之间传输的敏感数据；
- Inference: 未经授权的实体通过从通信的特征或副产品进行推理来间接访问敏感数据；
- Intrusion: 未经授权的实体通过规避系统的安全保护来获得对敏感数据的访问权限。

Deception: 可能导致被授权的实体收到虚假数据并相信这是真实数据。

可能造成的后果：

- Masquerade: 未经授权的实体通过冒充授权实体来访问系统或执行恶意行为；
- Falsification: 虚假数据欺骗被授权实体；
- Repudiation: 一个实体通过错误地否认对某一行为的责任来欺骗另一个实体 (比如否认自己的攻击行为)。

Disruption: 中断或阻止系统服务和功能正确运行的情况或事件。

可能造成的后果：

- Incapacitation: 通过禁用 (disabling) 系统组件来阻止或中断系统操作；
- Corruption: 通过对系统功能或数据进行不利修改 (modifying)，改变系统操作；
- Obstruction: 通过阻碍 (hindering) 系统操作来中断系统服务传递的威胁操作。

Usurpation: 导致未经授权的实体控制系统服务或功能的情况或事件。

可能造成的后果：

- Misappropriation: 实体假定对系统资源进行未经授权的，逻辑上的或物理上的控制；
- Misuse: 使系统组件执行对系统安全有害的功能或服务。

Threats to assets

Hardware: Major threat is availability, 例如设备被盗或被禁用 (Confidentiality).

Software: Major threat is availability, 例如软件被删或被病毒改写其功能 (Confidentiality, integrity).

Data: A much more widespread problem is data security, 例如数据被删除/未经授权的读取/对统计数据的分析揭示了真实数据 (Availability, confidentiality, integrity).

Communication lines and networks: Major threat is network security.

Network security attacks:

- Passive attacks
    - Release of message contents, 例如重要信息被泄露
    - Traffic analysis, 信息是加密的，但信息的 pattern 会被发现
    - Passive attacks 很难检测，因为它们不涉及对数据的任何更改。
- Active attacks
    - Replay, 例如对数据单元进行被动捕获，随后重新传输以产生未经授权的效果
    - Masquerade, 一个实体假装是另一个实体
    - Modification of messages, 例如合法邮件的某些部分被更改，或消息被延迟或重新排序
    - Denial of service, 试图占用网站资源，使需要访问该网站的用户无法正常使用

Countermeasures

Security design principles

Fundamental security design principles:

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privileges
- Least privilege
- Least common mechanism
- Psychological acceptability

Economy of mechanism:

安全措施的设计应经济性的开发、使用和验证。

应增加很少或没有开销；只应做需要做的事；尽量保持简单和小。

Fail-safe designs:

访问决策 (Access decisions) 应基于权限 (permission) 而不是排除，并默认为缺乏访问权限。

因此，如果出现问题或被遗忘或未完成，则不会丢失安全性。

Complete mediation:

对受保护对象的每次访问都应用安全性，必须根据访问控制机制 (access control mechanism) 检查每次访问。

通常，用户打开文件后，不会检查权限是否发生更改。但为了完全实现complete mediation，每次用户读取文件中的字段或记录，或数据库中的数据项时，系统都必须执行访问控制。

Open design:

安全机制的设计应当是公开的，而不是秘密的。假设所有潜在的攻击者都知道有关设计的一切，并完全理解它。不过这并不一定意味着发布有关安全系统的所有重要信息。

Kerckhoffs principle：加密系统应该是安全的，即使系统的所有内容（除了密钥）都是公开的。

Separation of privileges：

提供将用于一种目的的特权与用于另一种目的的特权分开的机制（例如访问麦克风/摄像头，和获得位置信息需要分别授权）。使安全系统具有灵活性，以减轻计算机安全攻击的潜在损害。

Least privilege：

系统的每个进程和每个用户都应使用执行任务所需的最少权限集进行操作（比如只需要读文件，就不给修改文件的权限）。需要另一个请求才能执行其他类型的访问。

Least common mechanism:

该设计应最大限度地减少不同用户共享的功能，从而提供相互的安全性。

耦合（coupling, 模块及模块之间信息或参数依赖的程度）可能会导致安全漏洞。

Psychological acceptability:

机制必须易于使用，足够简单，人们会不假思索地使用它。必须很少或从不阻止允许的访问。

Computer security strategy

A comprehensive security strategy involves three aspects:

- Specification/policy:
    - What is the security scheme supposed to do?
- Implementation/mechanisms:
    - How does it do it?
- Correctness/assurance:
    - Does it really work?

Security policies:

安全策略描述安全系统的行为方式。策略说应该发生什么，而不是如何实现它。

在制定安全策略时，安全经理需要考虑以下因素：1, 被保护资产的价值；2，系统的漏洞；3，潜在威胁和攻击的可能性。

权衡：易用性与安全性；安全成本与故障/恢复成本。

Security implementation：

Security implementation involves four complementary courses of action:

- Prevention
  - encrypting the data, authenticate via password, etc.
- Detection
  - intrusion detection, detection of DoS attack
- Response
  - halt the attack and prevent further damage
- Recovery
  - backup system

Assurance and evaluation：

Assurance 处理以下问题：安全系统设计是否符合其要求？安全系统实施是否符合其规范？

Assurance 表示为一定程度的置信度，而不是正式证明设计或实现是正确的。

Evaluation 是根据一定的标准检查计算机产品或系统的过程。评估包括测试，也可能包括形式分析或数学技术。

Tools for security

- Cryptographic tools
  - Encryption, message authentication code, digital signature, etc.
- Access control (仅允许授权方访问系统)
- User authentication (例如通过密码确认)
- Intrusion detection/prevention, firewall
  - Intrusion detection：一种安全服务，用于监视和分析系统事件，以便查找以未经授权的方式访问系统资源的尝试，并提供实时或近乎实时的警告。IDS: Intrusion detection system.
  - firewall: 保护网络免受恶意外部攻击的机器，通常位于局域网/广域网和互联网之间。运行特殊软件来调节网络流量。
  - Intrusion prevention system (IPS): Also known as intrusion detection and prevention system (IDPS)。IDS 的扩展，包括尝试阻止或阻止检测到的恶意活动的功能。