## 概述

#### 本章主要关注问题：

**我们需要保护什么样的财产**

**这些财产是如何受到威胁的**

**我们可以做什么来应对这些威胁**

#### 计算机安全的概念

计算机安全的三个关键目标

机密性 ： 包括数据机密性和隐私性

完整性 ： 数据完整性和系统完整性

可用性 ： 确保系统能够及时响应

补充：真实性 可说明性

成功的攻击往往是通过一个完全不同的方式来观察问题，从而探测机制中不可预见的弱点

对于部分用户和系统管理者，在安全保障失效之前，很少看到安全投入带来的好处

计算机资产分类

* 硬件
* 软件
* 数据
* 通信设施和网络

攻击的分类

Active attack

Passive attack

Inside attack

Outside attack

威胁后果 ： 非授权泄露

Attack ：暴露 截获 推理 入侵

威胁后果 ： 欺骗

Attack ：冒充 伪造 抵赖

威胁后果 ： 破坏

Attack ： 失能 损坏 阻碍

威胁后果 ： 篡夺

Attack ：盗用 误用

|  |  |  |  |
| --- | --- | --- | --- |
|  | 可用性 | 机密性 | 完整性 |
| 硬件 | 设备拒绝提供服务 | 未加密的USB被盗 |  |
| 软件 | 程序被删除拒绝访问 | 非授权拷贝 | 对软件进行修改 |
| 数据 | 文件被删除拒绝访问 | 非授权读取数据 | 对数据文件的修改 |
| 通信线路和网络 | 消息删除通信不可用 | 消息或流量被观察 | 消息被修改伪造 |

安全要求：

Access control ：限制授权

Awareness and training

Audit and accountability

Certification，accreditation ，and security assessment

Configuration management

Contingency planning

Identification and authentication

Incident respond

Maintenance

Media protection

Planning

Physical and environment protection

Personal security

Risk assessment

System and service acquisition

System and communication protection

System and information integrity

如果你认为技术可以解决安全问题，那么你并不理解安全问题

安全设计原则

Economy of mechanism

Fail-safe default

Complete mediation

Open design

Separation of privilege

Least privilege

Least common mechanism

Psychology acceptability

Isolation

Encapsulation

Modularity

Layering

Least astonishment

攻击面

* 网络攻击面
* 软件攻击面
* 人为攻击面