

# Part III-B: Computer Science Technology and Society

Lecture by 尹云飞

Note by THF

2024 年 9 月 26 日

## 目录

1 信息安全与社会	2
1.1 信息安全与社会的关系 . . . . .	3

## 课程要求

教师邮箱: yinyunfei@cqu.edu.cn

课程: 信息技术与社会 (信社)

课程目标: 32 学时, 课上考核

课程内容: 信息安全、网络技术、信息处理、电子商务、网络游戏与人类社会的关系, 大数据、云计算、深度学习

成绩组成: 平时表现 (50%) + 课程报告 (50%, 带 PPT 讲解, 心得报告, 技术调研, 小论文)

平时成绩: 出勤 (10%) + 课堂分享 (20%) + 回答问题、讨论、作业 (20%)

采用翻转课堂: 教师 40%, 主体转换分享 10%, 主体转换报告 50%, 期末考核 (与主体转换报告结合)

# 1 信息安全与社会

**Question.** 何为信息安全?

**Notation.** 网络攻击: 利用漏洞进行对硬件、软件和系统数据的攻击

攻击可分为主动式攻击(篡改、伪造、拒绝服务)和被动攻击(流量分析、窃听)

攻击层次: 简单拒绝服务, 非读写权限, 管理员权限

攻击方法: 特洛伊木马, www 欺骗, 口令入侵, 电子邮件, 端口扫描等

攻击位置: 本地, 远程, 伪远程

**Question.** 如何防范网络攻击?

1. 谨慎不明邮件、链接、软件、游戏
2. 复杂的密码设置
3. 系统补丁和防火墙
4. 代理服务器

**Notation.** 信息安全常用技术:

1. 密码学(编码学和解码学)
2. 认证技术(Authentication)
3. PKI(公钥基础设施, Public Key Infrastructure): 通过核对证书确认公钥所属
4. 信息隐藏: 对不需要隐秘信息的人来说该信息的载体正常且无法访问
5. 访问控制
6. 防火墙: 位于内网和外网之间的网安系统
7. 入侵检测: 主动(特征) + 被动(异常)

**Notation.** 非对称加密(SHA, RSA 等)中: 公钥用于加密信息, 私钥用于解密信息

**Notation.** 信息安全的两大方面: 攻击和防守

**Notation.** 主动入侵检测: 检测主体活动是否符合入侵活动的特征, 效率较高

被动入侵检测: 假设入侵者活动异常于正常主体的活动, 效率较低

**Definition.** 计算机病毒：编写者在程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用、自我复制的一段计算机指令或程序代码

计算机病毒具有传播性，隐蔽性，感染性，潜伏性，可激发性，表现性/破坏性

生命周期：

开发 → 传播 → 潜伏 → 发作 → 发现 → 消化 → 消亡

其他常用技术：

安全扫描

系统安全

安全风险评估

信息安全管理

## 1.1 信息安全与社会的关系

**Definition.** 社会即“关系”：在特定环境下形成的个体间的存在关系的总和

使用信息技术属于社会，部分使用行为导致了安全问题

**Example.** 云计算、云存储：非个人控制信息安全

人肉搜索：威胁日常生活安全

数据集中：风险集中

系统复杂：难以解决系统安全

**Notation.** In lecture 3 I didn't mark anything.