软件安全—恶意代码机理与防护
C1 软件安全概论

彭国军
武汉大学国家网络安全学院
guojpeng@whu.edu.cn

提纲

1.1 信息与信息安全

1.2 软件安全威胁与来源

1.3 软件安全威胁的典型防护措施

1.1 信息与信息安全

- 以下哪些属于信息？
  - “我是武汉大学的一名教师”
  - 手机收到的天气预报短信：“今天晚上有雨”
  - 网易云平台数据库中存储的用户登录口令
  - 云课堂上的一段MOOC教学视频
  - 课程管理系统中的学生选修名单及成绩
  - 结业证书上的个人与课程信息
  - 期末考试试卷
  - …

1.1.1 什么是信息

- 香农（C.E. shannon）：信息是用来消除随机不确定性的东西
- 其他相关观点：
  - 信息是客体相对于主体的变化。
  - 信息是有价值的消息。
  - 信息是确定性的增加。
  - 信息是反应客观世界中各种事物特征和变化的知识，是数据加工的结果，信息是有用的数据。

信息的表现形式

- 信息可以以多种形式表现：
  - 打印或书写在纸上，
  - 以电子数据的方式存储，
  - 或以胶片形式显示或者通过交谈表达出来等。

信息系统

- 狭义的信息系统：
  - 信息系统(Information System)是以提供信息服务为主要目的的数据密集型、人机交互的计算机应用系统。
- 广义的信息系统≠计算机应用系统

1.1.2什么是安全？

- 安全是指不受威胁，没有危险、不受危害、不受损失的一种可接受状态。
  - 例如：人类与生存环境的和谐相处，互相不伤害，不存在危险的隐患，是免除了不可接受的损害风险的一种状态。
  - 例如：人类生产过程中，将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类可接受标准以下的一种状态。

安全（Safety vs Security）

- Safety
  - 自然的，物理的，相对具体的
  - 如房屋、桥梁、大坝...
- Security
  - 社会的，人为的，相对抽象的
  - 如食品、软件...

1.1.3 什么是信息安全？

信息为什么存在安全问题？

信息的主要特点

- 信息是有价值的
  - 信息的价值是相对的
- 信息是流动的
  - 信源 ---信道-→ 信宿

信息安全的定义

- 对信息的保密性、完整性和可用性的保持。
  - 不可否认性+可控性

C onfidentiality
I ntegrity
A vailability

信息的安全属性

- **保密性**：信息仅被合法用户所知悉。
- **完整性**：数据的一致性，数据未被非法用户篡改。
- **可用性**：合法用户对信息和资源进行使用时，不会被不正当地拒绝。
- **真实性**：信息来源及其内容未被伪造。
- **不可抵赖性**：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。
- **可审查性**：对出现的信息安全问题提供调查的依据和手段。

信息的价值通过什么来体现？

- 保密性
- 可用性
- 完整性
- 真实性
- 不可否认性
- …

- 网易云平台数据库中存储的用户登录口令
- 期末考试试卷
- 云课堂上的一段MOOC教学视频
- 课程管理系统中的学生选修名单及成绩等

信息的价值在哪些情况下会丧失？

- 泄密（保密性）
- 被盗、损坏（可用性）
- 被篡改（完整性）
- 赖账（不可否认性）
- …

信息安全的实质

- 保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，以维护信息的价值，促进业务的连续性。
- 目前，信息安全已经被提升到了信息保障的地位。

信息保障（Information Assurance）

- 美国国防部对信息保障的定义：
  - “通过确保信息的可用性、完整性、可识别性、保密性和抗抵赖性来保护信息和信息系统，同时引入保护、检测及响应能力，为信息系统提供恢复功能。”

PDRR

=Protection+Detection+Reaction+Restoration

PDR;PPDR;PPDRR

P^2DR^2

- 信息安全是研究在特定的应用环境下，依据特定的安全策略(Policy)，对信息及其系统实施保护(Protection)、检测(Detection)、响应(Reaction)和恢复(Restoration)的科学。

网络空间安全已经上升为国家安全战略

没有网络安全，就没有国家安全

没有信息化，就没有现代化

- 信息安全事关国家安全、事关社会稳定，信息安全成为国家安全的重要组成部分，必须采取措施确保我国的信息安全。
- 确保我国信息安全，关键是人才。
- 信息安全专业承担着信息安全专业人才培养的重任。

我们是否愿意采取措施来保护我们的信息安全？

- 作为大学生，我们拥有哪些信息？
  - 身份信息
  - 联系方式
  - 社会关系
  - 其他信息：
    - 数码相片/私人信件/口令/电子邮件/聊天记录/好友名单/上网记录/视频聊天/电话清单/协议/保密文件/课程作业/…

我们愿意保护我们的信息吗？

- 该信息的价值有多大？
- 可能面临哪些风险？
- 为保护该信息需要付出多少成本？

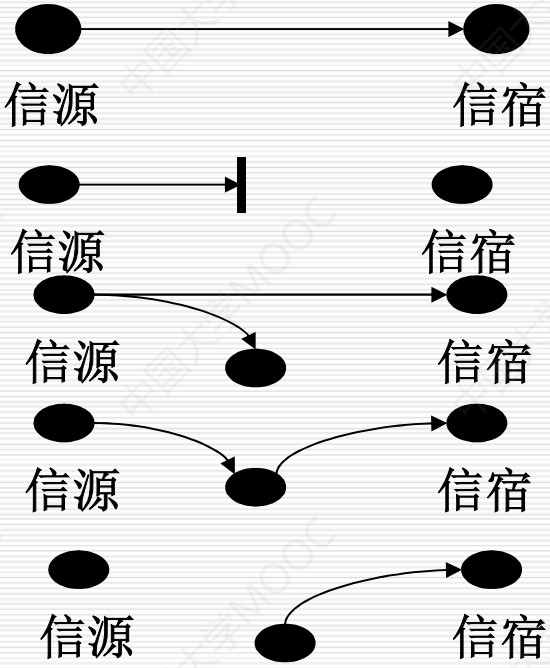
  - 在什么情况下愿意采取安全措施？
    - 认识到的价值*认识到的风险>认识到的成本？
  - 是否应该采取安全措施？
    - 真实价值*真实风险>真实成本？

哪些属于软件类威胁？

1.1.4 信息面临哪些安全威胁？

目前的几种攻击模式

正常的信息流动：



1）中断：

2）截取：

3）修改：

4）捏造：

思考

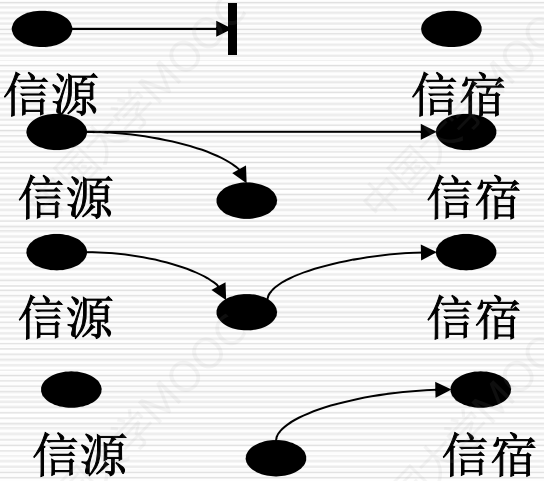
- 以上攻击模式分别破坏了信息的安全属性？

1）中断：

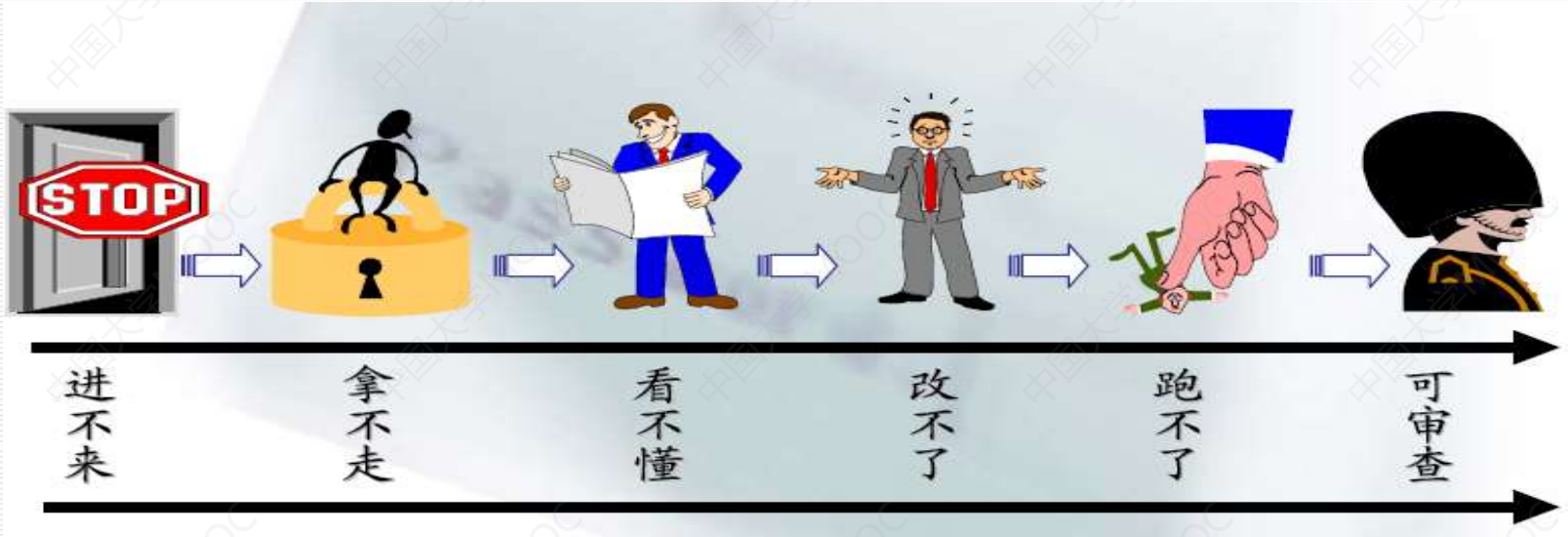
2）截取：

3）修改：

4）捏造：



1.1.5 信息安全防护



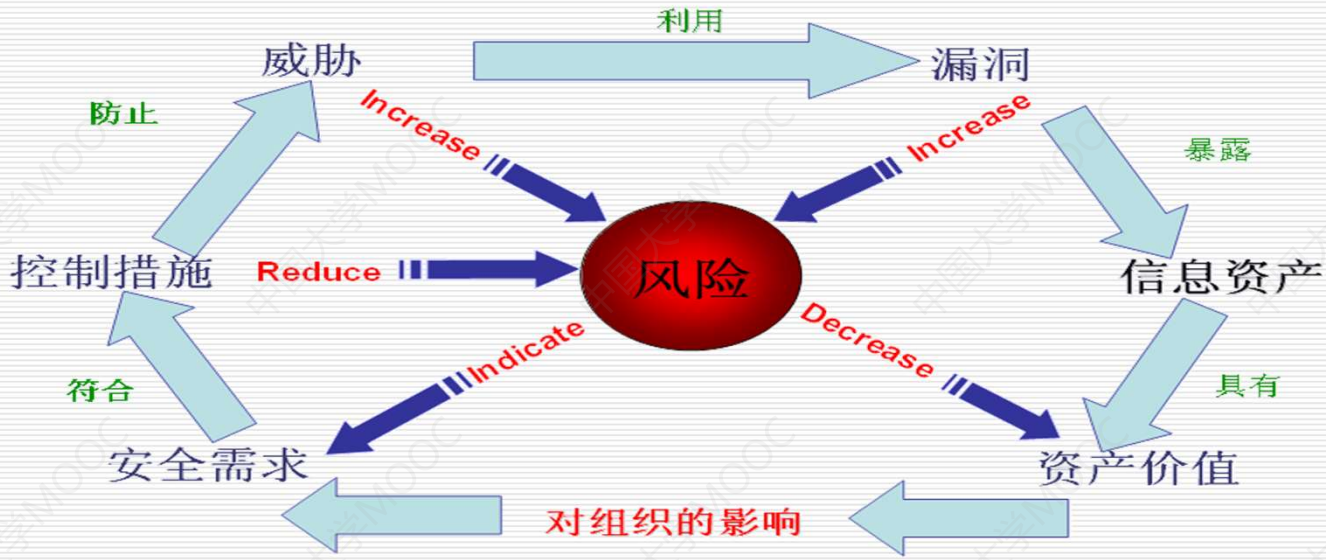
通过什么手段来保障信息安全？

- 安全管理手段
  - 安全管理制度
  - 安全组织建设
  - 人员安全管理
  - 系统建设管理
  - 系统运维管理等

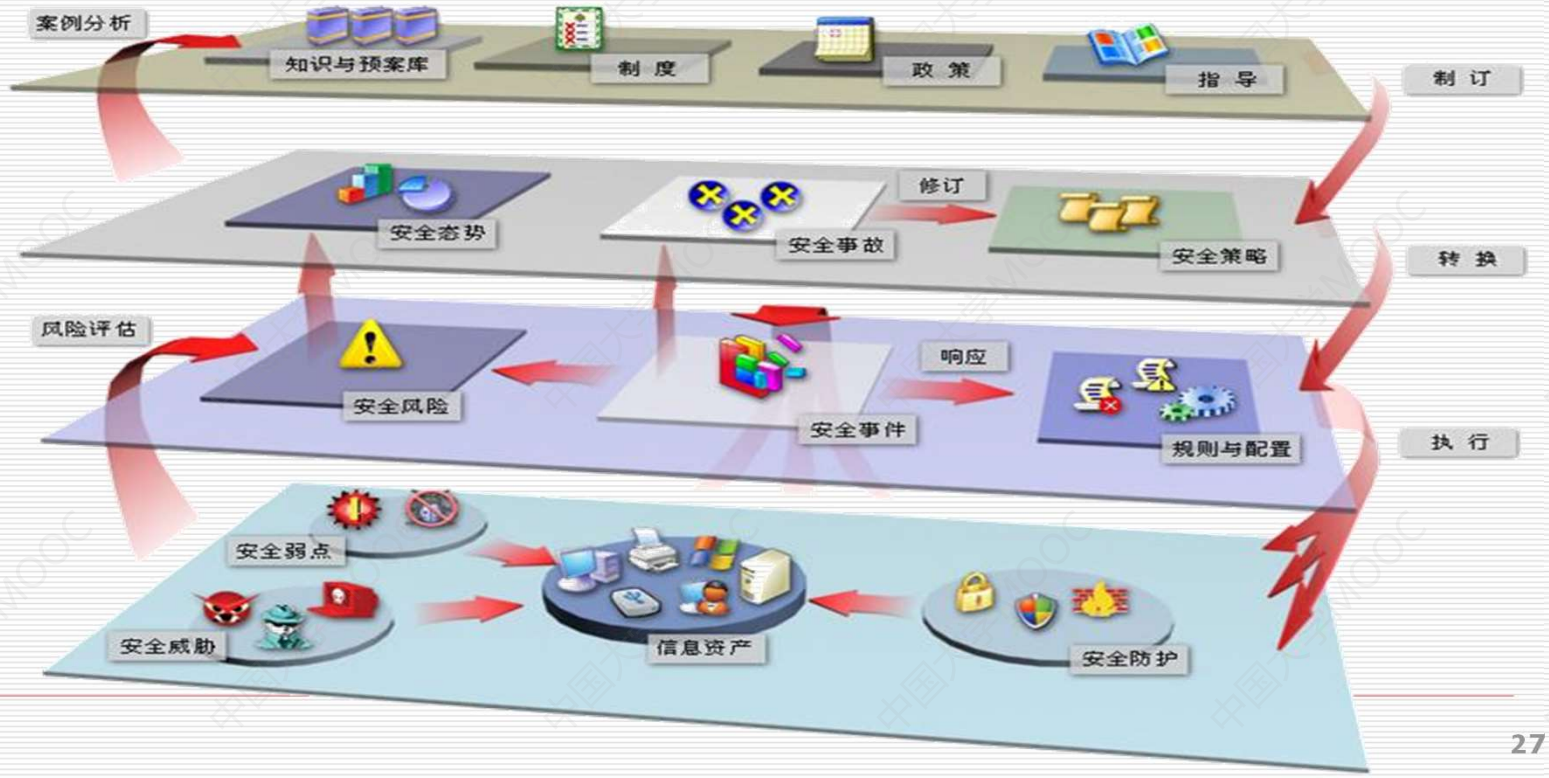
- 安全技术手段
  - 物理安全、主机安全、网络安全、应用安全、数据安全与备份恢复等
  - 身份认证，访问控制，数据加密，数字签名…
  - 防火墙，杀毒软件…

安全贵在未雨绸缪

因果关系



因果关系（立体）


案例分析
知识与预案库
制 度
政 策
指 导
制 订
安全态势
安全事故
修订
安全策略
转 换
风险评估
安全风险
响应
安全事件
规则与配置
执 行
安全弱点
安全威胁
信息资产
安全防护