§1.1 信息安全的目标

一、信息安全问题

信息：数据、消息和资讯等。

信息安全：信息在产生、传输、处理和存储过程中不被泄露或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。

信息安全本质上体现为网络信息安全。

网络与信息安全的主要任务：

1、网络安全任务：保障网络资源稳定可靠运行，受控合法使用

2、信息安全任务：机密性，完整性，不可否认性，可用性

3、其他：病毒防治，预防内部犯罪

§1.1 信息安全的目标

常见的攻击：

- 口令破解：攻击者可通过获取口令文件，然后运用口令破解工具获得口令，也可通过猜测或窃听等方式获取口令
- 连接盗用：在合法的通信连接建立后，攻击者可通过阻塞或摧毁通信的一方来接管已经过认证建立起来的连接，从而假冒被接管方与对方通信
- 服务拒绝：攻击者可直接发动攻击，也可通过控制其它主机发起攻击，使目标瘫痪，如发送大量的数据洪流阻塞目标
- 网络窃听：网络的开放性使攻击者可通过直接或间接窃听获取所需信息

§1.1 信息安全的目标

- 数据篡改：攻击者可通过截获并修改数据或重放数据等方式破坏数据的完整性
- 地址欺骗：攻击者可通过伪装成被信任的IP地址等方式来骗取目标的信任
- 社会工程：攻击者可通过各种社交渠道获得有关目标的结构、使用情况、安全防范措施等有用信息从而提高攻击成功率
- 恶意扫描：攻击者可编制或使用现有扫描工具发现目标的漏洞进而发起攻击
- 基础设施破坏：攻击者可通过破坏路由信息等基础设施，使目标陷于孤立
- 数据驱动攻击：攻击者可通过施放病毒、特洛伊木马、数据炸弹等方式破坏或遥控目标

§1.1 信息安全的目标

二、信息安全的主要威胁

1、通信过程中的威胁：信息在计算机网络系统的通信过程中面临的一种外部威胁。

攻击手法：截获、中断、伪造、篡改

2、存储过程中的威胁：存储在计算机系统或服务器、数据库中数据信息面临的一种严重攻击威胁。

攻击手法：数据窃取、变更、重放、抵赖攻击

3、加工处理中的威胁：信息在加工过程中，通常以源码出现，加密保护对处理中的信息不起作用。因此这期间有意攻击和意外操作都极易使系统遭受破坏，造成损失。

§1.1 信息安全的目标

瑞星公司发布《2025年中国网络安全报告》，网络安全威胁正呈现智能化、隐蔽化与全局化新特征。网络攻击手段持续升级，人工智能技术与供应链渗透成为最突出的安全挑战。

看点一：木马主导、勒索转向精准化

2025年，瑞星“星核”平台共截获病毒样本总量4972万个，恶意网址总量突破1.69亿个，较往年呈现持续增长态势。从恶意软件类型分布看，木马病毒以73.35%的占比成为第一大威胁，后门病毒、蠕虫等类型分别占据12.13%和7.86%。勒索软件呈现明显的“靶向化”趋势，攻击手法从单纯的数据加密升级为“双重勒索+”模式，结合数据窃取、敏感信息拍卖等复合手段，对勒索目标形成全方位胁迫。

§1.1 信息安全的目标

看点二：AI呈现“双刃剑”特性

一方面，攻击者开始利用AI自动生成恶意代码、构造高仿真钓鱼邮件，大幅降低攻击门槛。另一方面，AI系统自身暴露出一定的脆弱性，成为新型攻击入口。AI安全已从技术防护问题，演变为覆盖模型全生命体系的治理挑战。

§1.1 信息安全的目标

看点三：银狐木马仿冒策略与隐蔽加载技术升级

近年来，持续活跃的远控木马家族“银狐”，在2025年展现出强烈的对抗意图和快速迭代能力，实现了隐蔽植入与信息窃取。

攻击者高度集中仿冒高频刚需软件，WPS办公软件、搜狗输入法等成为被仿冒最多的前几类软件。在技术层面，银狐木马通过商用打包工具构造多层恶意载荷，利用多种技术增强隐蔽性。

§1.1 信息安全的目标

看点四：AI将深度融入攻防两端

报告预测，2026年AI技术将进一步融入攻防两端，含漏洞正常驱动的滥用将更为普遍。基于AI的自动化漏洞挖掘可能缩短零日漏洞的响应时间，加剧防御压力。“银狐”木马等成熟威胁仍将保持高活跃度，企业需建立覆盖大模型全生命周期的安全治理体系，以AI技术对抗AI攻击，在动态博弈中寻求新的安全平衡。

§1.1 信息安全的目标

2026网络安全新趋势：AI重构攻防，信任成为新防线

一、AI流量飙升令智能体攻防成为新战场，AI Agent身份认证将“被动防护”转向“主动建立信任”

二、AI加速API攻击规模化，API攻击面极具扩大，成为主要威胁载体

三、AI重构攻防态势，前置式主动网络安全主动出击，破解潜在攻击路径

四、AI浏览器、AI手机诱发智能体基础设施全新威胁

五、AI驱动的新型多重勒索更趋于自动化，攻击面持续扩大

六、合规与AI可信双驱动，数据质量与治理成为Agentic AI时代的新挑战

§1.1 信息安全的目标

三、网络信息安全特征与保护技术

1、信息安全特征

- 完整性：信息在传输、交换、存储和处理过程保持非修改，非破坏和非丢失的特性。
- 保密性：杜绝信息泄漏给非授权的个人或实体，强调有用信息只为授权对象使用。
- 可用性：网络信息被授权实体正确访问。
- 不可否认性：通信双方在信息交互过程中，确信参与者身份，以及参与者所提供的信息的真实同一性。
- 可控性：对流通在网络系统中的信息传播及具体内容能够实现有效控制。

§1.1 信息安全的目标

2、信息安全保护技术

- 主动防御保护技术

  数据加密、身份鉴别、存取控制、权限设置、虚拟专用网技术。

- 被动防御保护技术

  防火墙、入侵检测系统、安全扫描器、口令验证、审计跟踪、物理保护与安全管理

§1.1 信息安全的目标

3、信息安全服务

对信息的保密性、完整性和真实性进行保护和鉴别，以便防御各种安全威胁和攻击。

- 鉴别服务
- 访问控制服务
- 数据保密性
- 数据完整性
- 防止否定服务（抗抵赖）

§1.1 信息安全的目标

4、信息安全机制

- 加密机制
- 数字签名机制
- 访问控制机制
- 数据完整性机制
- 鉴别交换机制
- 通信业务填充机制
- 路由控制机制
- 公证机制