1 信息安全概论

信息安全 涉及到信息的保密性 (confidentiality)、完整性 (integrity)、可用性 (availability)、可控性 (controllability)。

广义的信息安全，除了上述技术因素，还包括法律、管理等其他内容。

安全性 (security) 是一种抵御可能的风险和威胁的能力，而我们只关心由于人为因素所产生的风险和威胁。

威胁 (threats) 是对安全的潜在破坏。这种破坏不一定要实际发生才成为威胁。

攻击 (attack) 是可能导致破坏的行为，行为人被称为攻击者。

- 截获（被动攻击）：仅窃听，不更改信息流；
- 中断（主动攻击）：中断信息流；
- 篡改（主动攻击）：修改信息流；
- 伪造（主动攻击）：伪造信息流。

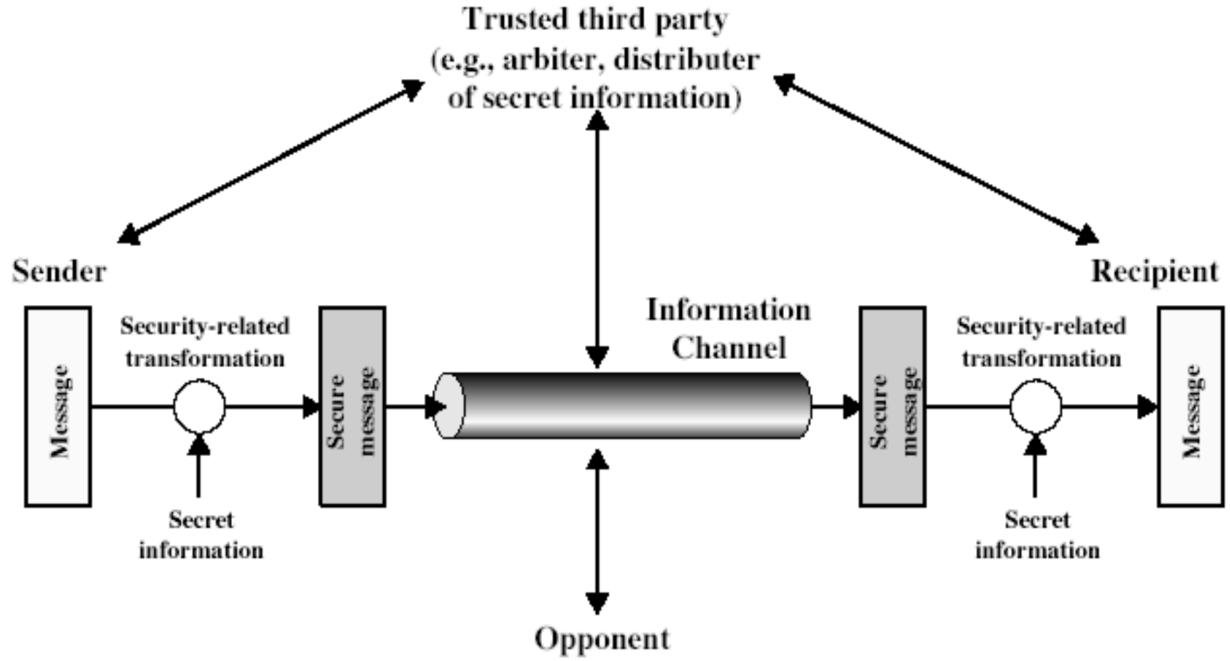
主要的安全需求

- **保密性** (confidentiality)：防止非授权用户读取一些机密信息；
- **数据完整性** (data integrity)：防止非授权用户篡改信息；
- **认证性 (数据来源的可靠性)** (authenticity)：防止非授权用户伪造信息、假冒合法用户发送信息；
- **不可否认性** (non-repudiation)：防止信息发送者事后否认自己的行为；
- **访问控制** (access control)：数据库存放信息的安全。

如何达到安全

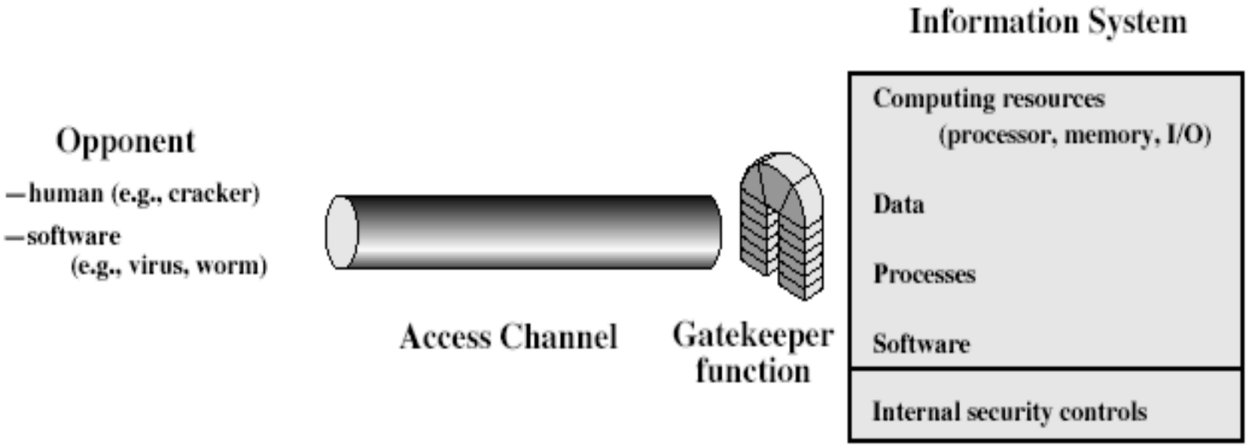
- 提供安全服务；
- 制定安全策略；
- 完善安全机制。

网络安全模型



- 设计安全变换算法；
- 生成变换算法的秘密信息；
- 设计分配秘密信息的方案；
- 指定一个协议，使得通信主体可以使用变换；
- 提供安全服务。

网络访问控制安全模型



- 需要合适的网关识别用户；
- 实施安全控制，保证只有授权用户才能访问指定的信息或资源；
- 可信的计算机系统可以实施这种系统。