

# 2 网络与信息安全整体架构介绍

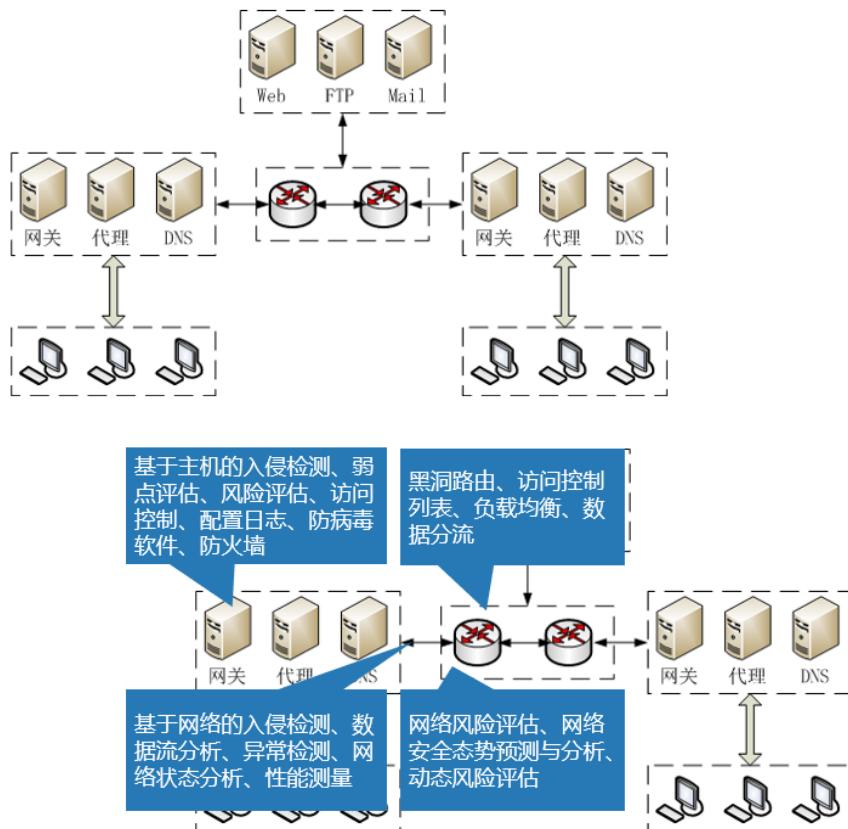
2019年4月21日 14:52

## 1 网络与信息安全整体架构

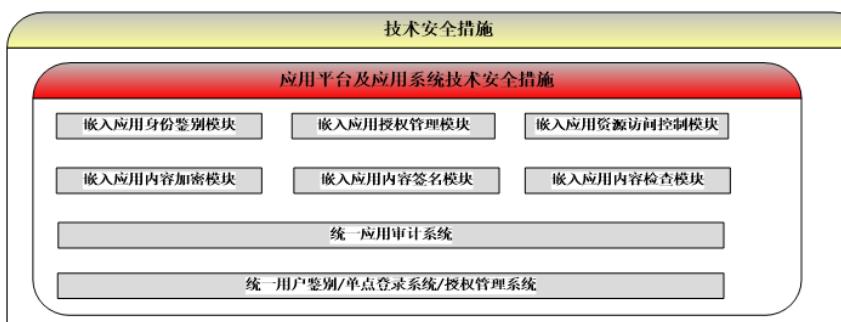
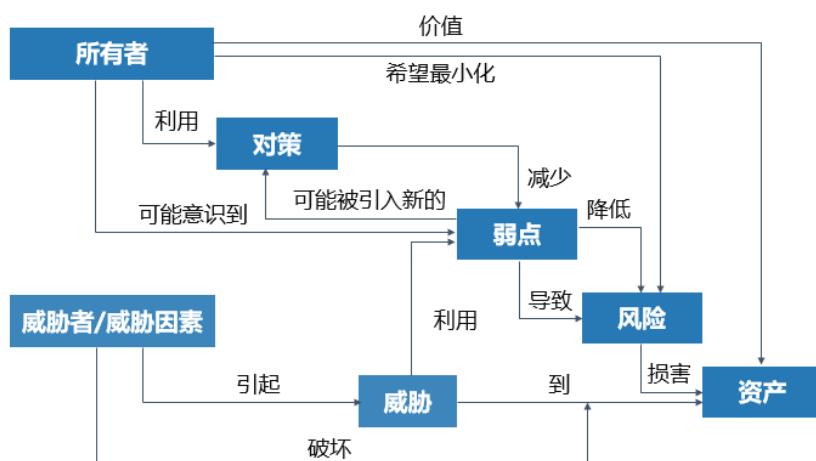
### 2 信息安全

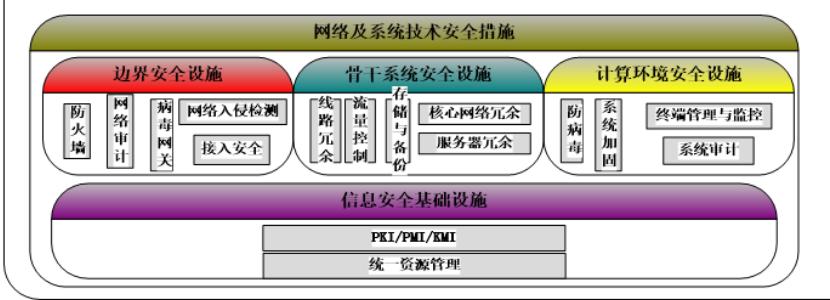
### 3 网络安全

## 1 网络与信息安全整体架构



数据流捕获、分析、还原，模式匹配，数据挖掘，神经网络，人工智能，数据库，关联分析，容灾，容侵，电子取证，授权管理，信任机制，网络性能评测，DNS安全，监控技术，密码技术。





## 2 信息安全

什么是信息安全—国内的回答

- 可以把信息安全保密内容分为：实体安全、运行安全、数据安全和管理安全四个方面。（沈昌祥）
- 计算机安全包括：实体安全、软件安全、运行安全、数据安全。（教科书）
- 计算机信息人机系统安全的目标是着力于实体安全、运行安全、信息安全和人员安全维护。安全保护的直接对象是计算机信息系统，实现安全保护的关键因素是人。（等级保护条例）

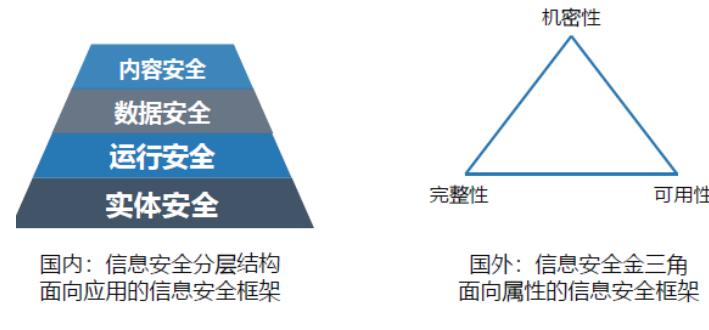
什么是信息安全—国外的回答

- 信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。（BS7799）
- 信息安全就是对信息的机密性、完整性、可用性的保护。（教科书）
- 信息安全涉及到信息的保密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。（信息安全重点实验室）

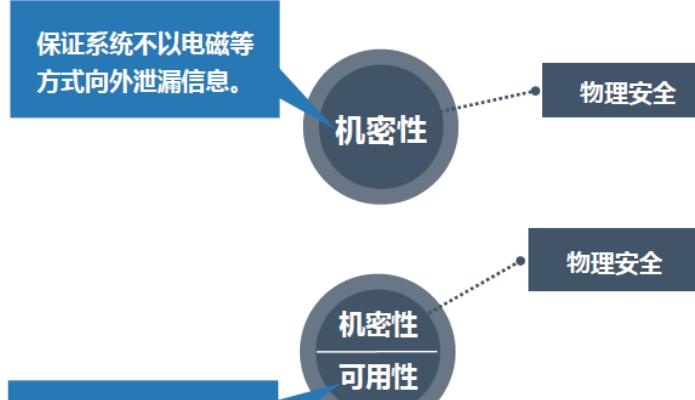
从信息安全的发展渊源来看

- 通信保密阶段 (40–70's, COMSEC)：
  - 以密码学研究为主
  - 重在数据安全层面
- 计算机系统安全阶段 (70–80's, INFOSEC)：
  - 开始针对信息系统的安全进行研究
  - 重在物理安全层与运行安全层，兼顾数据安全层
- 网络信息系统安全阶段 (>90's, NETSEC)：
  - 开始针对信息安全体系进行研究
  - 重在运行安全与数据安全层，兼顾内容安全层。

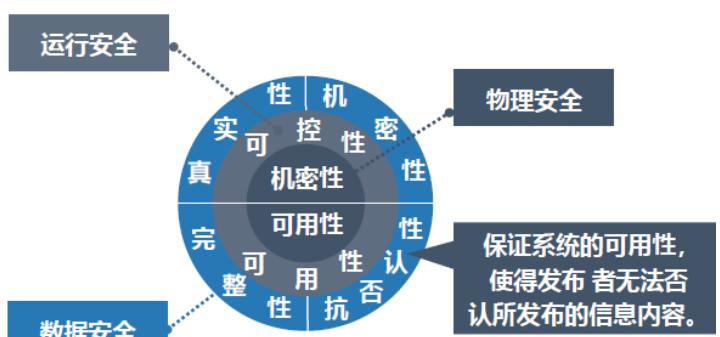
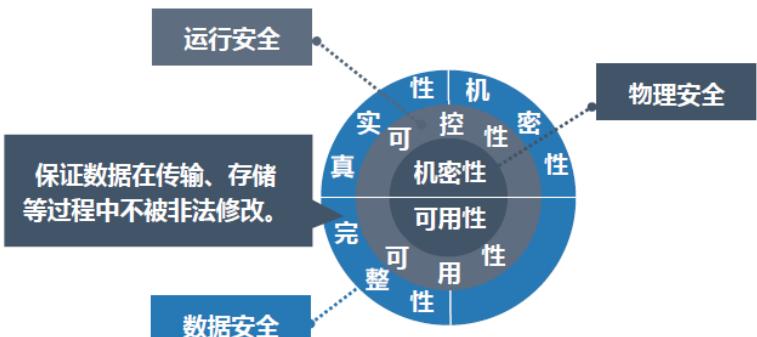
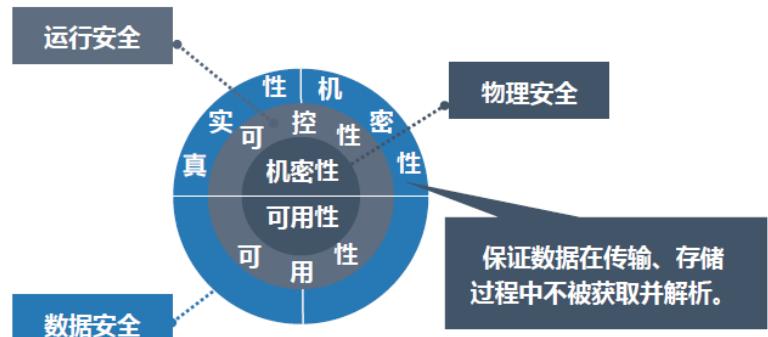
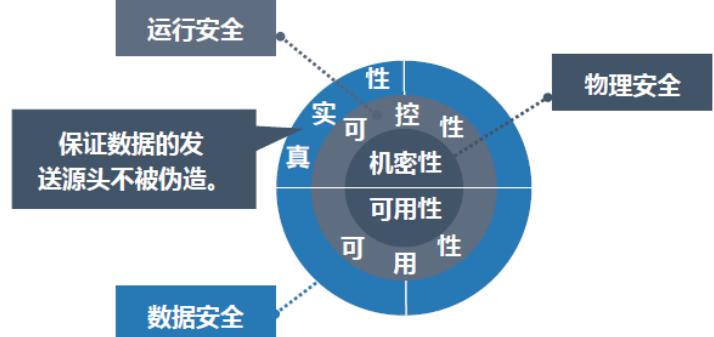
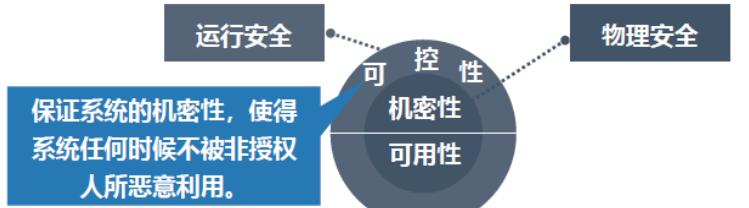
关于信息安全的两种主要论点

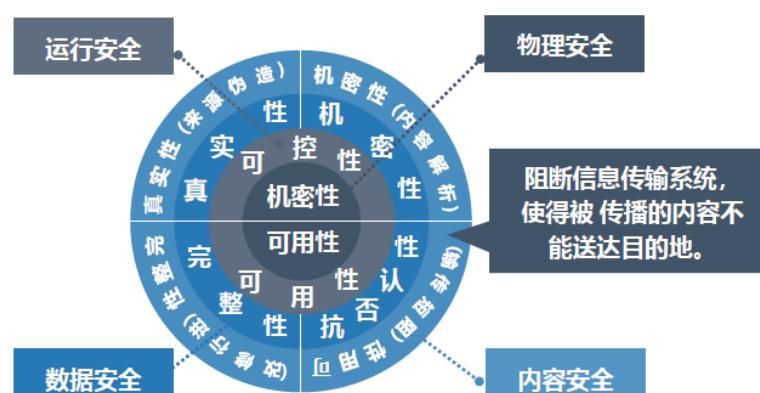
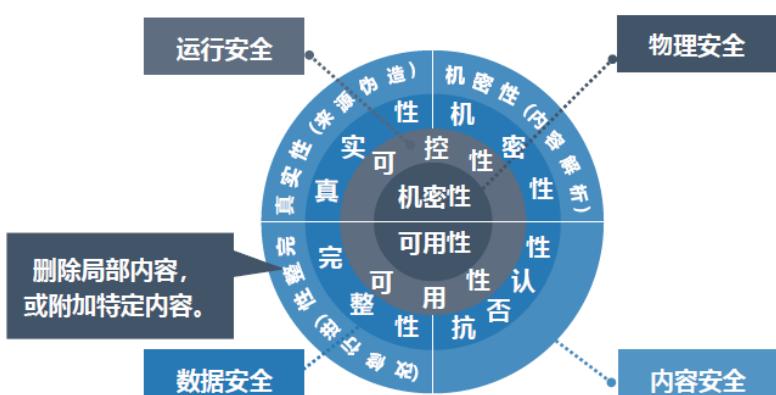
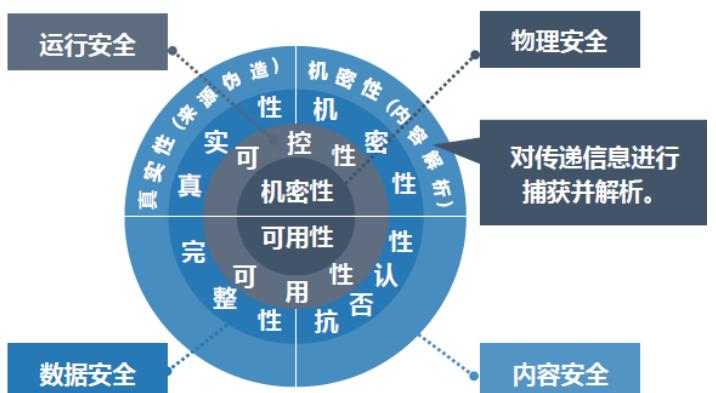


网络与信息安全涵盖范围



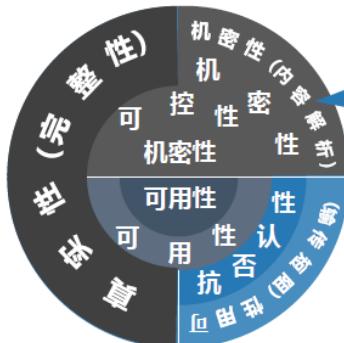
保证系统至少能够提供基本的服务。



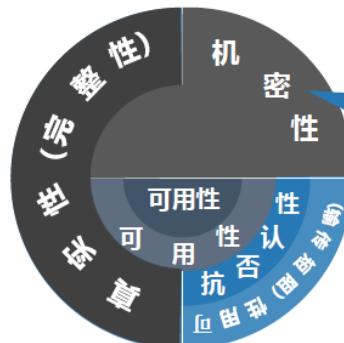


这些层面具有相同的性质，都可以归并为真实性。其中，完整性是真实性的子集，是表示内容因未被修改而是真实的。

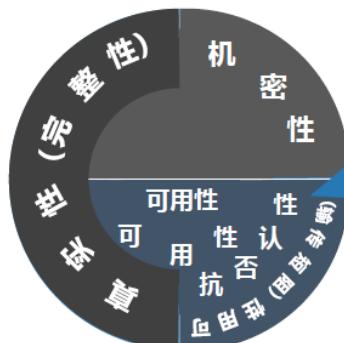




这些层面都反映出机密性特性，其中可控性是机密性的子集，是表示为保护机密性而进行访问控制。



保证信息与信息系统不被非授权者所获取与使用。主要防范技术是密码技术。



这些层面都反映出可用性的属性。其中抗否认性可以看作是可用性的子集，是为了保证系统确实能够遵守游戏规则，不被恶意使用所反映的可用性的属性。



保证信息与信息系统可被授权人员正常使用。主要防护措施是确保信息与信息系统处于一个可信的环境之下。

## 网络与信息安全框架

属性层次	机密性	真实性	可用性
物理安全	防泄漏		抗恶劣环境
运行安全	抗非授权访问		正常提供服务
数据安全	防解析	发布/路由/内容真实	抗否认
内容安全	信息解析	路由/内容欺骗	信息阻断

## 结论：什么是信息安全技术

- 信息安全技术是指在信息系统的物理层、运行层，以及对信息自身的保护（数据层）及攻击（内容层）的层面上，所反映出的对信息自身与信息系统在可用性、机密性与真实性方面的保护与攻击的技术。

### 3 网络安全

务虚：未来网络演变的假定

- 从总体角度来看，安全技术不会有大变化：
  - TCP/IP协议不会发生根本变化
  - 遍布世界的巨型资产不会轻易退出历史舞台
  - 带宽的提高仅是量的变化，并不会带来技术上面的质的变化
  - 无线网的出现只表明接入方式的变化，等效于以太网时期的广播效应，并不带来安全方面的本质问题
  - 防范对象仍为资源的恶意消耗与业务的盗用

务虚：新技术带来的困惑

- 在新技术出现后，期待着新的安全技术的突破
  - IPv6为网络安全的保护带来了灾难性的影响
    - IPv6的倡导者将着重点放在了保护数据安全之上，将网络安全问题交给终端用户。
  - IPv6无法解决一些目前存在的网络安全问题
    - 无法完全解决目前广泛存在的DoS攻击，更无法有效的防止DDoS攻击。
    - 无法有效防止针对协议本身的攻击，如SYNflood攻击。
    - 无法解决口令攻击，也无法防止利用缓冲区溢出进行的攻击。
  - PeerPeer网络将成为主流，与Grid共存。
    - Scalefree型结构带来危险，分散均衡将是潮流。
  - 三网融合（NGN）势在必行，属于分组网络
    - 能够建立不同于IP网的新的体系(信令与数据独立)吗？
  - 网络呼唤着保障体系，需要综合集成处理体系，从整体角度来相互印证是未来的主流
    - 全球化是当今世界主题，互联网的自主接入，构成一个复杂巨系统，孤立的技术发挥的作用有限。

计算机攻击技术对互联网安全的挑战

- 黑客工具的自动化程度及速度在不断提高
- 攻击工具的攻击能力与复杂程度在不断提高
- 安全漏洞的暴露速度在不断加快
- 防火墙被渗透的机会不断增加
- 不对称的威胁程度在不断增加
- 针对基础设施的攻击带来的威胁不断增加
  - 拒绝服务攻击
  - 蠕虫
  - 域名攻击
  - 路由攻击

未来互联网所面临的威胁

- 超级蠕虫病毒的大规模扩散
  - 理论上在数分钟之内可感染近千万台机器。
  - 多态性、混合型、独立性、学习能力、针对P2P
- 应用系统面临威胁
  - 电力、工厂、交通、医院……
- 利用程序自动更新存在的缺陷
  - 网络程序（如杀毒软件）的共性，带来极度危险
- 针对路由或DNS的攻击
- 同时发生计算机网络攻击和恐怖袭击

成熟的网络安全防护模型PPDRR





## 安全策略 (Policy) 的前沿技术

- 风险分析、安全评估
  - 如何评估系统处于用户自主、系统审计、安全标记、结构化、访问验证等五个保护级的哪一级?
- 漏洞扫描技术
  - 基于关联的弱点分析技术
  - 基于用户权限提升的风险等级量化技术
- 网络拓扑结构的发现，尤其是Peer-to-Peer网络拓扑结构的发现
  - 拓扑结构综合探测技术（发现黑洞的存在）
  - 基于P2P的拓扑结构发现技术（解决局域性问题）
- 态势预测与分析
  - 如何评估当前系统或网络环境所处的安全状态、未来的发展趋势
    - 热点舆论事件论坛、博客日本地震、海啸、核辐射中国抢盐
    - 热点网络事件蠕虫、僵尸网络、DDoS、LDDoS、数字大炮等

## 系统防护 (Protection) 的前沿技术

- 病毒防护，侧重于网络制导、移动终端防护。
  - 病毒将始终伴随着信息系统而存在。随着移动终端的能力增强，病毒必将伴随而生
- 隔离技术
  - 基于协议的安全岛技术：协议的变换与解析
  - 单向路径技术：确保没有直通路径
- 拒绝服务攻击的防护
  - DoS是个致命的问题，需要有解决办法
- 访问控制技术
  - 家庭网络终端(电器)、移动终端的绝对安全
  - 多态访问控制技术

## 入侵检测 (Detection) 的前沿技术

- 基于IPv6的入侵检测系统
  - 侧重于行为检测
- 向操作系统、应用系统中进行封装
- 分布式入侵检测
  - 入侵检测信息交换协议
  - IDS的自适应信息交换与防攻击技术
- 特洛伊木马检测技术
  - 守护进程存在状态的审计
  - 守护进程激活条件的审计
- 预警技术
  - 基于数据流的大规模异常入侵检测

## 应急响应 (Response) 的前沿技术

- 快速判定、事件隔离、证据保全
  - 紧急传感器的布放，传感器高存活，网络定位
- 企业网内部的应急处理
  - 企业网比外部网更脆弱，强化内部审计
- 蜜罐技术
  - 漏洞再现及状态模拟应答技术
  - 沙盒技术，诱捕攻击行为
- 僚机技术
  - 动态身份替换，攻击的截击技术
  - 被攻系统躲避技术，异常负载的转配

## 灾难恢复 (Restore) 的前沿技术

- 基于structure-free的备份技术

- 构建综合备份中心IBC (Internet Backup Center)
- 远程存储技术
- 数据库体外循环备份技术
- 容侵 (intrusion-tolerant) 技术
  - 受到入侵时甩掉被攻击部分
  - 防故障污染
- 生存 (容忍) 技术
  - 可降级运行, 可维持最小运行体系

## 数据价值发挥的解决方案

