

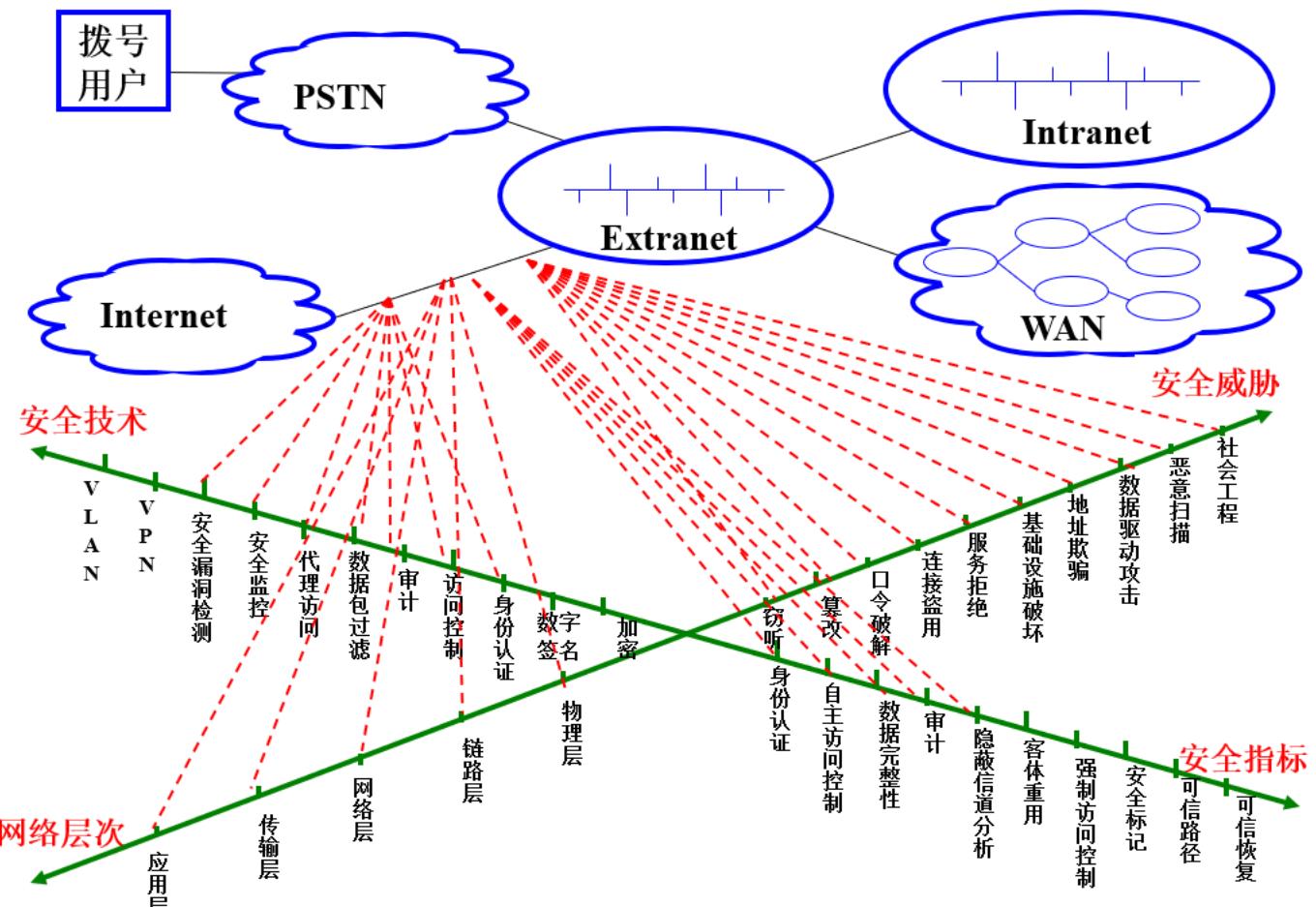
2 导论与基础

2019年4月21日 14:52

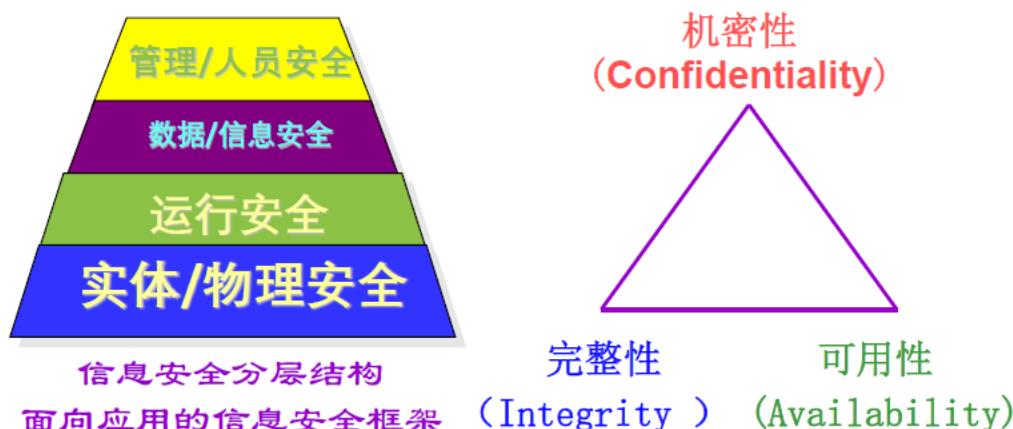
- [1 信息安全技术概论](#)
- [2 信息安全的层次划分](#)
- [3 信息安全的基本要素](#)
- [4 信息安全的诱因与威胁](#)
- [5 网络信息内容分类](#)
- [6 信息内容安全技术概述](#)
- [7 信息内容安全技术产品](#)

1 信息安全技术概论

信息安全技术架构



关于信息安全的两个主要视点



内容安全:

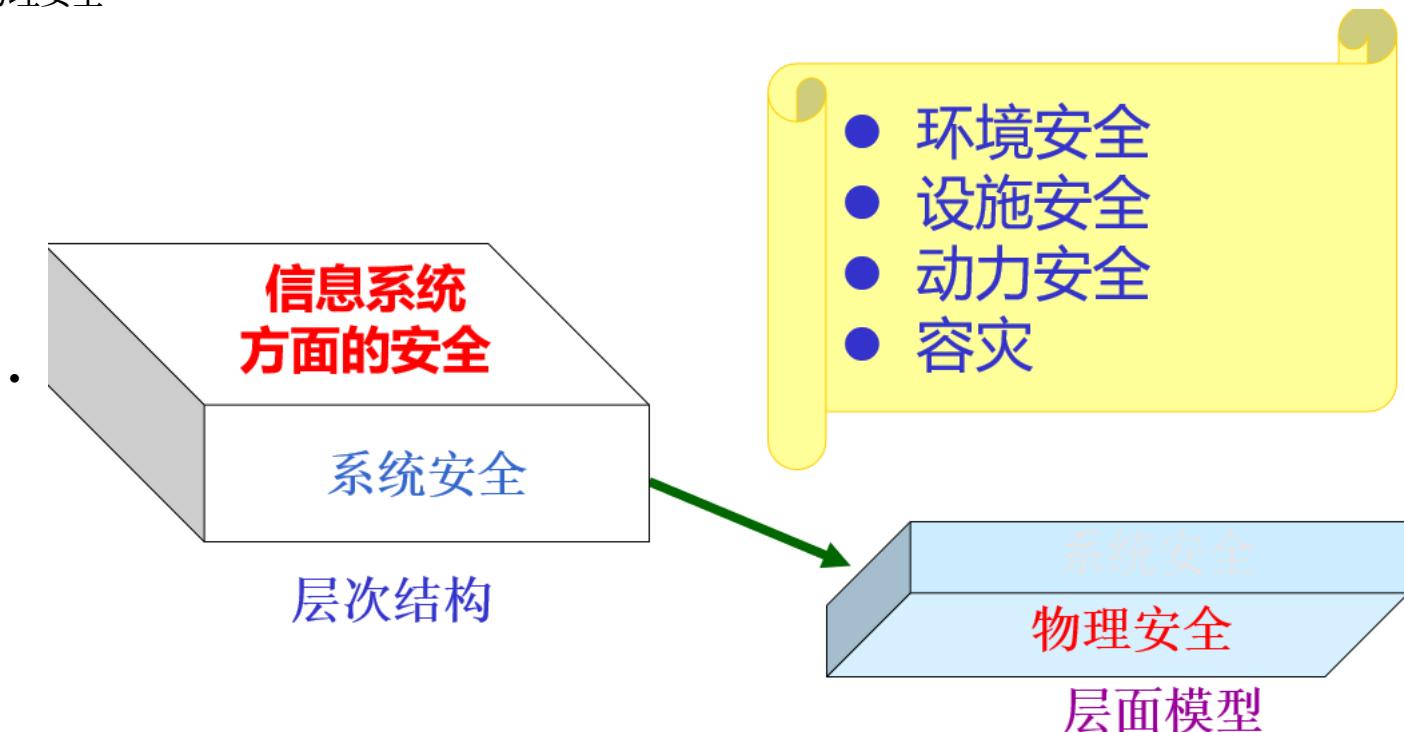
- 谁在关心文化安全? 内容安全的本质是什么?
 - 文化安全不是技术问题, 是哲学问题。
 - 内容安全着眼点是依据内容来对安全问题进行判断, 但需要通过技术方式来解决
 - 内容安全技术的本质是对数据的攻击技术
 - 国际社会经常将反网络病毒 (AntiVandalism) 、反垃圾邮件问题列入内容安全的范畴

信息对抗:

- 信息安全研究的是信息对抗的问题, 所引发的问题是:
 - 信息对抗与信息安全的关系是什么?
 - 信息对抗自身也存在体系问题, 包括不同层次的对抗问题
 - 信息隐藏是典型的信息内容对抗
- 在信息安全的角度考虑这个问题, 给出的命题是:
 - 一个客观存在的信息, 如何发现?
 - 信息获取、数据挖掘、情报分析
 - 如果我们不能掩盖一个信息, 那就淹没这个信息
 - 围绕信息利用的对抗行为(所谓虚虚实实真真假假)

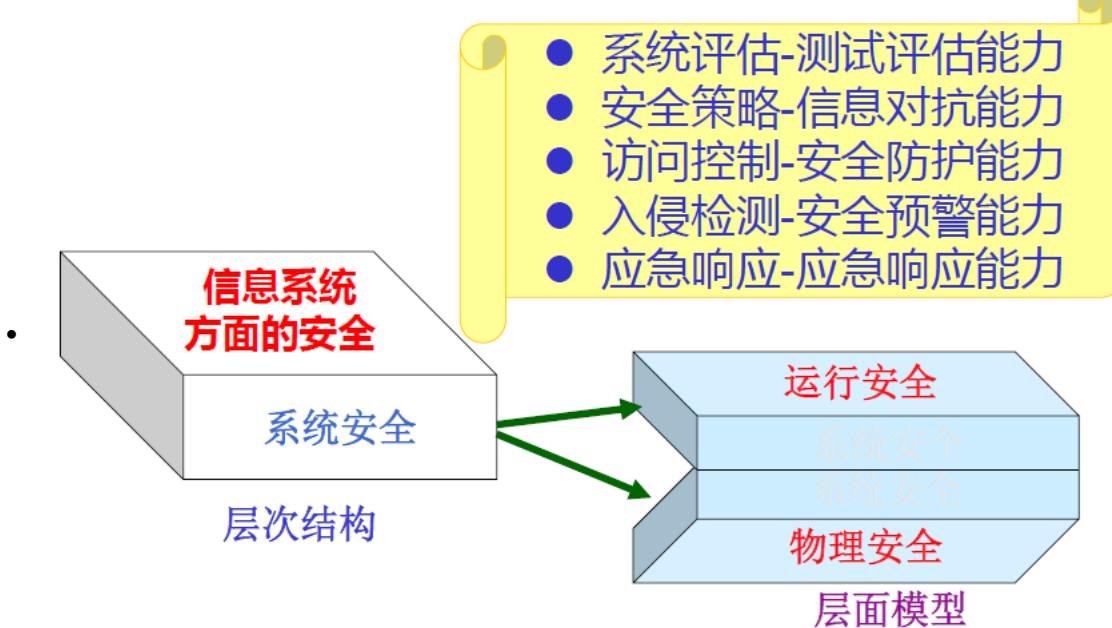
2 信息安全的层次划分

物理安全



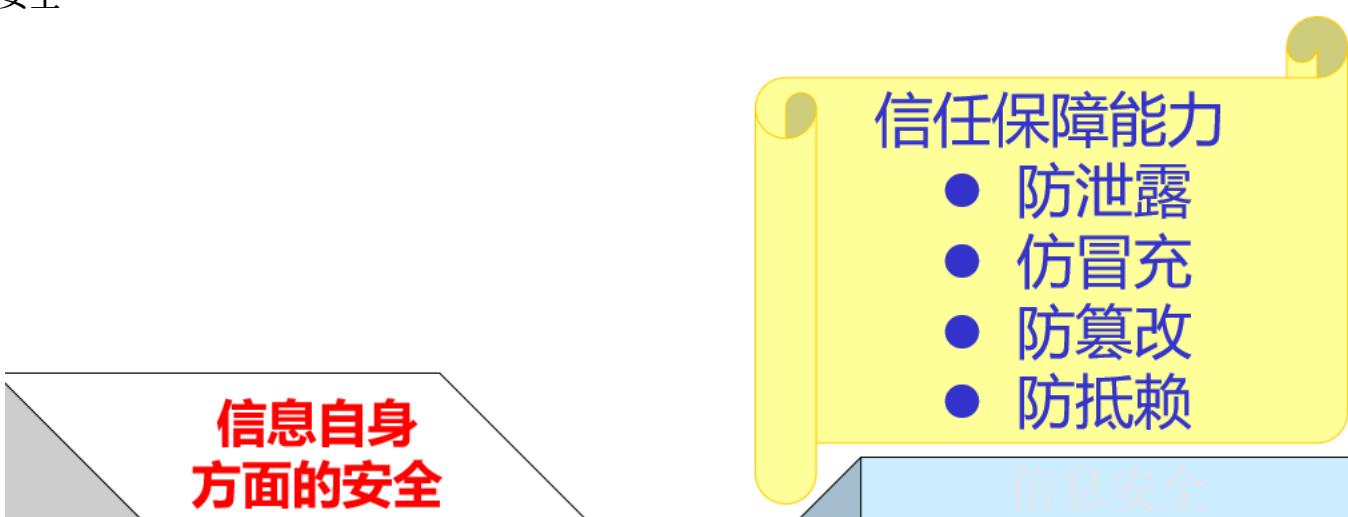
- 指对网络与信息系统物理装备的保护。主要涉及网络与信息系统的机密性、可用性、完整性等属性
- 所涉及的主要技术:
 - 加扰处理、电磁屏蔽: 防范电磁泄露
 - 容错、容灾、冗余备份、生存性技术: 防范随机性故障
 - 信息验证: 防范信号插入
- 863计划关注的重要技术
 - 灾难恢复与故障容错技术
 - 网络可生存性技术
 - 空间信息系统安全技术
- 242计划关注的重要技术
 - 系统数据、网络和服务的可生存性技术
 - 系统容灾技术

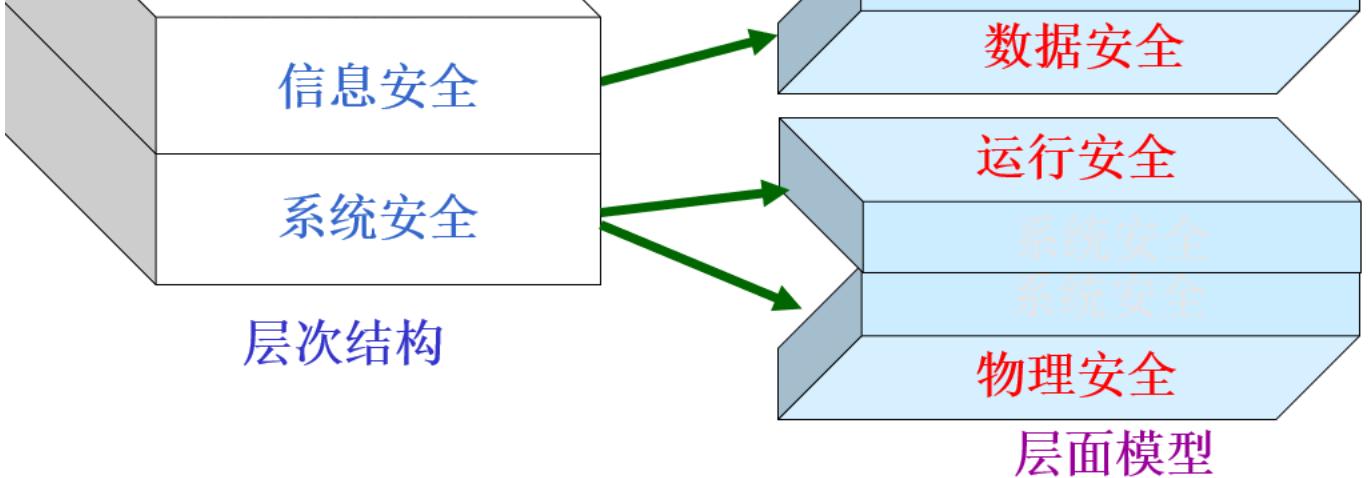
运行安全



- 指对网络与信息系统的运行过程和运行状态的保护。主要涉及网络与信息系统的真实性、可控性、可用性等
- 主要涉及的技术
 - 风险评估体系、安全测评体系：支持系统评估
 - 漏洞扫描、安全协议：支持对安全策略的评估与保障
 - 防火墙、物理隔离系统、访问控制技术、防恶意代码技术：支持访问控制
 - 入侵检测及预警系统、安全审计技术：支持入侵检测
 - 反制系统、容侵技术、审计与追踪技术、取证技术、动态隔离技术：支持应急响应
 - 网络攻击技术，Phishing、Botnet、DDoS、木马等技术
- 863计划关注的重要技术
 - 可信安全计算、网络环境技术
 - 生物识别技术
 - 病毒与垃圾邮件防范技术
 - 测试评估技术
 - 高性能安全芯片技术
- 242计划关注的重要技术
 - 大流量网络数据获取与实时处理技术
 - 专用采集及负载分流技术
 - 宏观网络安全监测技术
 - 异常行为的发现、网络态势挖掘与综合分析技术
 - 大规模网络建模、测量与模拟技术
 - 宏观网络应急响应技术
 - 大规模网络安全事件预警与联动响应技术
 - 异常行为的重定向、隔离等控管技术
 - 网络安全威胁及应对技术
 - 僵尸网络等网络攻击的发现与反制技术
 - 漏洞挖掘技术

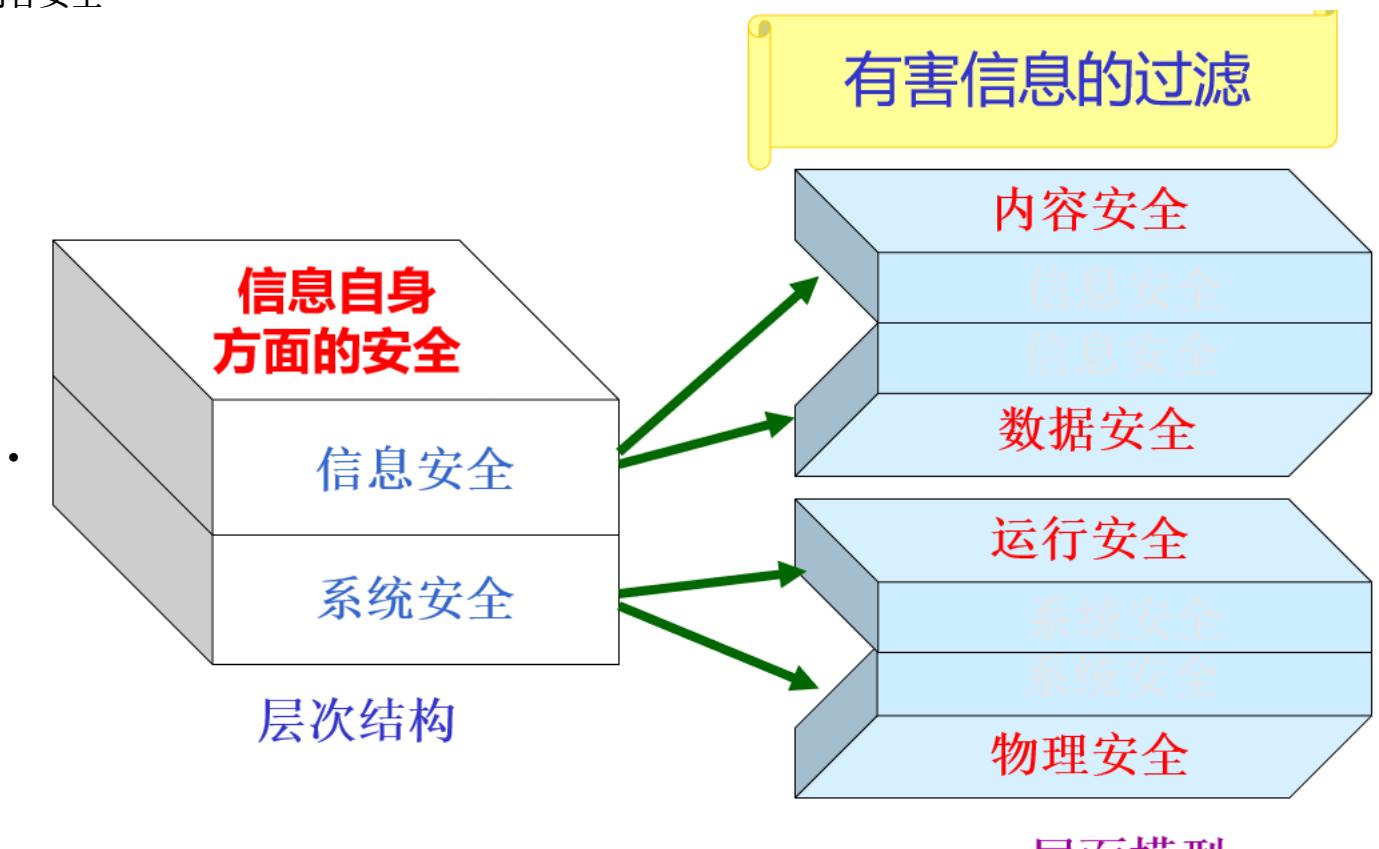
数据安全





- 指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，使得在数据处理层面保障信息依据授权使用，不被非法冒充、窃取、篡改、抵赖。主要涉及信息的机密性、真实性、完整性、不可否认性等
- 主要涉及的技术
 - 对称与非对称密码技术及其硬化技术、VPN等技术：防范信息泄密
 - 认证、鉴别、PKI等技术：防范信息伪造
 - 完整性验证技术：防范信息篡改
 - 数字签名技术：防范信息抵赖
 - 密钥共享技术：防范信息破坏
- 863计划关注的重要技术
 - 密码技术
 - 应用密码技术
 - 网络信任体系技术

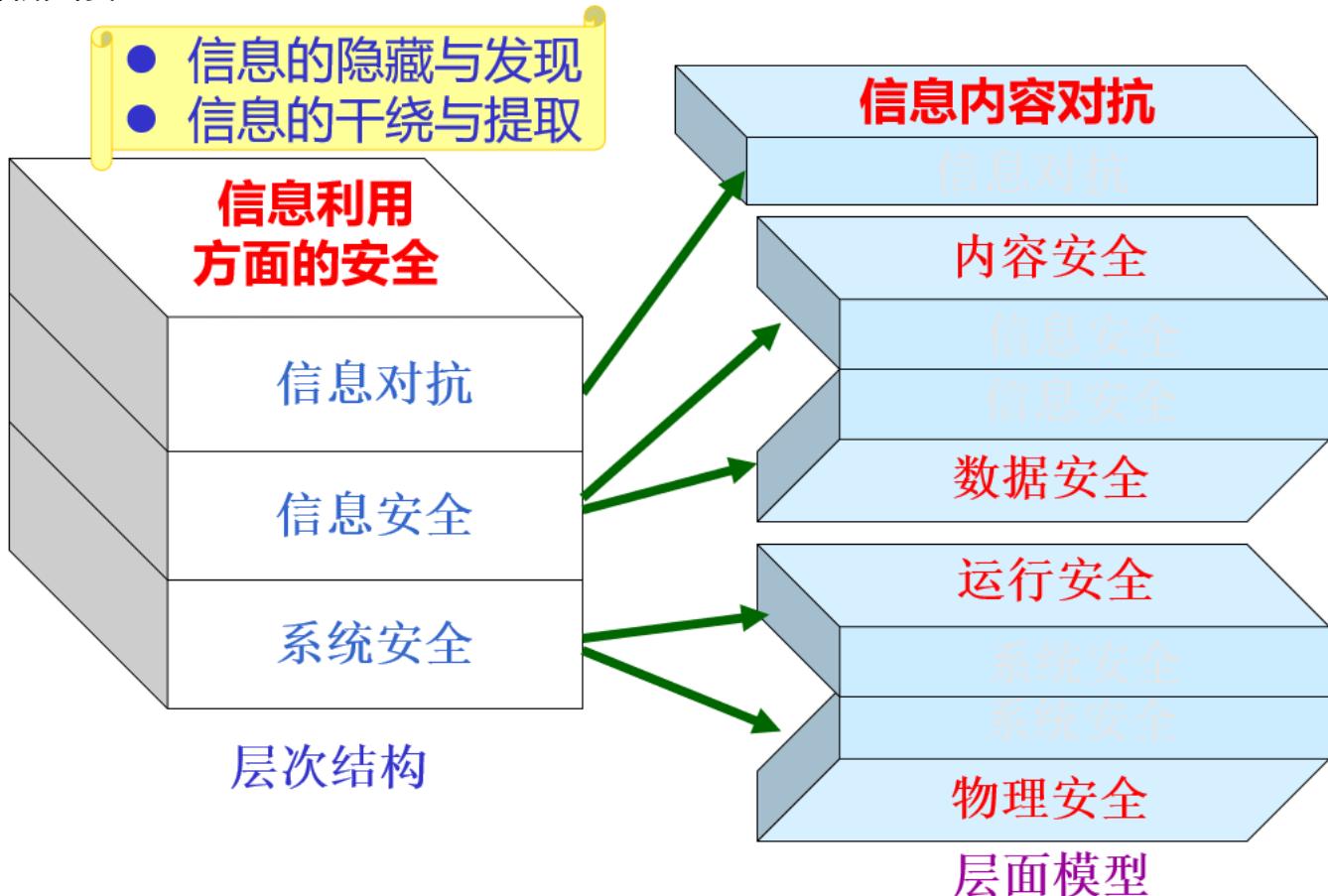
内容安全



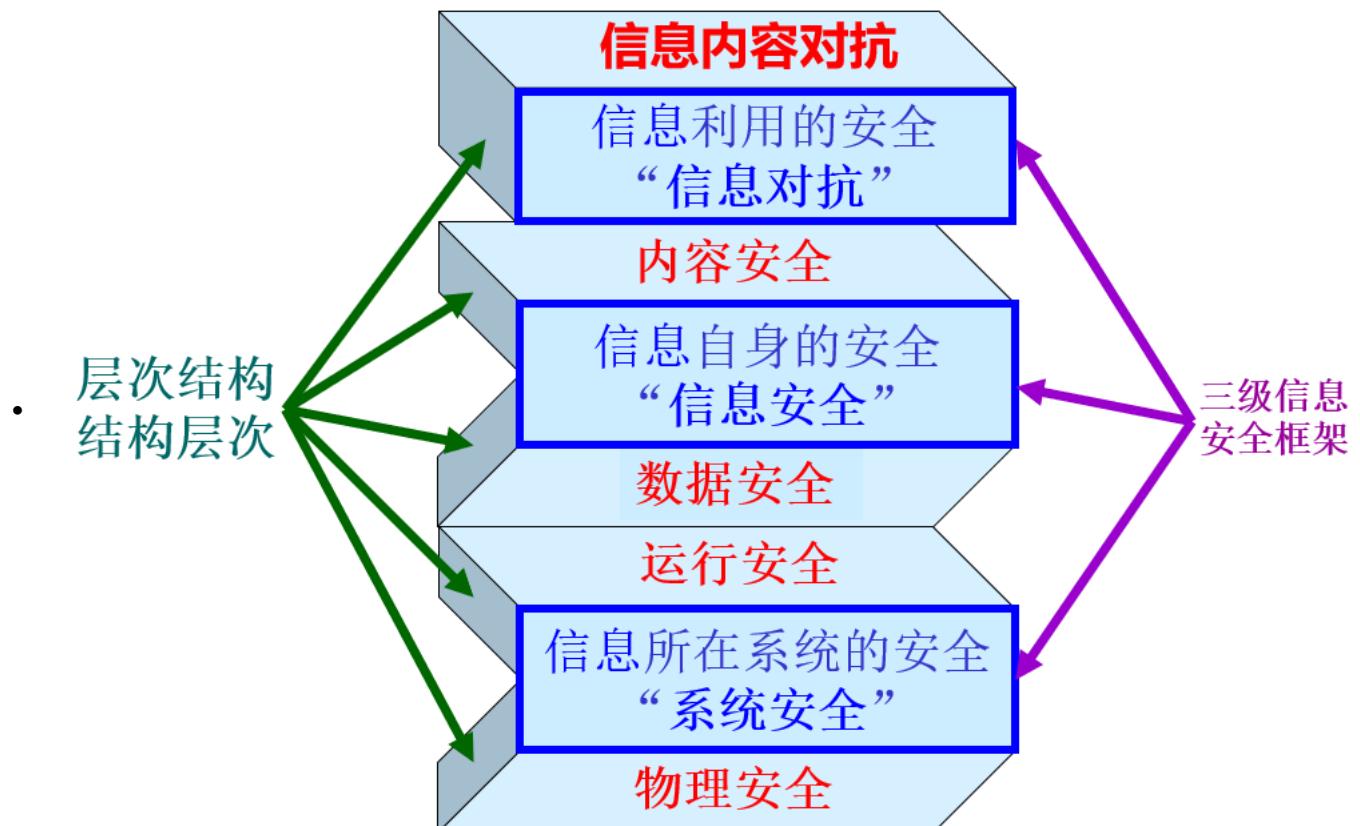
- 指对信息在网络内流动中的选择性阻断，以保证信息流动的可控能力。主要涉及信息的机密性、真实性、可控性、可用性等
- 主要涉及的技术：
 - 文本识别、图像识别、流媒体识别、群发邮件识别等：用于对信息的理解与分析；
 - 面向内容的过滤技术（CVP）、面向URL的过滤技术（UFP）、面向DNS的过滤技术等：用于对信息的过滤。
- 863计划关注的重要技术
 - 网络监控技术

- 面向互联网
- 面向广播电视台
- 面向VoIP
- 面向短信息
- 242计划关注的重要技术
 - 基于互联网的监控技术
 - P2P网络行为的发现与监控技术
 - 大规模特征串匹配算法与数据流查询技术
 - 垃圾信息检测与过滤技术
 - 垃圾信息自动识别技术
 - 垃圾信息综合举报、分类与处理技术
 - 反色情绿色上网软件技术
 - 网站服务性质识别与色情网站自动发现技术
 - 图像与网络流媒体识别技术

信息利用的安全

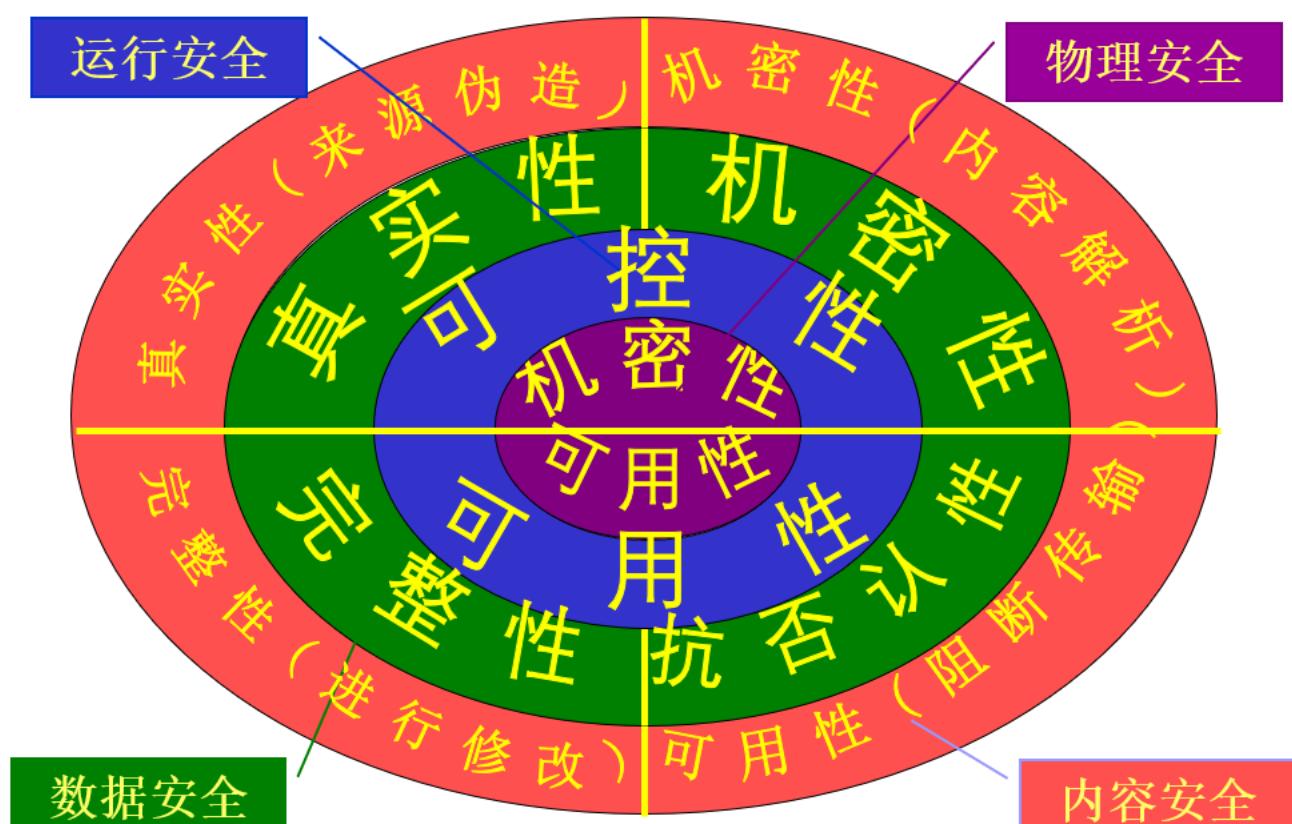


- 指对信息有效内容真实性的隐藏、保护与分析。主要涉及信息有效内容的机密性、完整性等
- 所涉及的主要技术:
 - 数据挖掘技术: 发现信息
 - 隐写技术、水印技术: 保护信息
 - 即时通、MSN等协议的分析技术: 对特定协议的理解,
 - VoIP识别技术: 对数字化语音信息的理解
 - 音频识别与按内容匹配: 锁定音频目标进行
- 863计划关注的重要技术
 - 灾难恢复与故障容错技术
 - 网络可生存性技术
 - 空间信息系统安全技术
- 242计划关注的重要技术
 - 舆情挖掘与预警技术
 - 特定主题信息的识别、特征发现技术
 - 敏感/热点事件发现及趋势预测技术
 - 信息隐藏技术
 - 基于图像或音频的隐写、检测及还原工具库
 - 非拼装隐藏信息的快速检测



3 信息安全的基本要素

信息安全分层结构：面向应用的信息安全框架



- 物理安全:对传递信息进行捕获并解析
- 运行安全:路由欺骗,域名欺骗
- 数据安全:删除局部内容, 或附加特定内容
- 内容安全:阻断信息传输系统, 使得被传播的内容不能送达目的地

信息安全的基本属性视点

- 机密性 (Cf)
- 真实性 (Au)
- 可控性 (Ct)

- 可用性 (Av)
- 信息安全四要素: CACA

信息安全经纬线——层次模型与要素模型的结合

	机密性	真实性	可控性	可用性
物理安全	✓	✓		✓
运行安全		✓	✓	✓
数据安全	✓	✓		✓
内容安全	✓	✓	✓	✓
信息内容对抗	✓	✓		

4 信息安全的诱因与威胁

网络不安全的原因

- 根本原因--冯诺依曼结构
 - 数字计算机的数制采用二进制
 - 计算机应该按照程序顺序执行
 - 软件=数据+程序
- 直接原因
 - 自身缺陷+开放性+黑客攻击

网络自身的安全缺陷

- 协议本身会泄漏口令
- 连接可成为被盗用的目标
- 服务器本身需要读写特权
- 基于地址
- 密码保密措施不强
- 某些协议经常运行一些无关的程序
- 业务内部可能隐藏着一些错误的信息
- 有些业务本身尚未完善,难于区分出错原因
- 有些业务设置复杂,很难完善地设立
- 使用CGI的业务

网络开放性

- 业务基于公开的协议
- 远程访问使得各种攻击无需到现场就能得手
- 连接是基于主机上的社团彼此信任的原则

常见攻击分类

- 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;

- 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DNS或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。

网络安全的任务

- 保障各种网络资源稳定、可靠地运行、受控、合法地使用

信息安全的任务

- 机密性 (confidentiality) 完整性(integrity) 抗否认性(nonrepudiation) 可用性(availability)

内容安全的任务

- 依据内容对文化安全问题进行判断
- 通过技术问题解决文化安全问题

内容安全的技术本质：对数据的攻击技术

信息对抗的任务

- 内容隐藏<->内容挖掘

5 网络信息内容分类

网络信息存在形式

- 从服务特性角度分类
 - 一阶网络资源管理
 - 文件形式
 - 超文本/超媒体形式
 - 网站网页形式
 - 半结构化/非结构化数据库组织形式
 - 二阶网络资源管理
 - 主题目录形式
 - 搜索引擎形式
 - 虚拟图书馆形式
 - 三阶网络资源管理
 - 元搜索引擎形式
- 从传输特性角度分类
 - 有线网络传输
 - 光信号传输
 - 电信号传输
 - 无线网络传输

波段名称	频段(f) 范围	波长(λ) 范围
长波	15~100KHz	20000~3000m
中长波	100~150KHz	3000~2000m
中短波	150~1500KHz	2000~200m
短波	1.5~30MHz	200~10m
超短波	30~300MHz	10~1m
微波(分米波)	300~3000MHz	1m~10cm
微波(厘米波)	3~30GHz	10~1cm
微波(毫米波)	30~300GHz	1cm~1mm
微波(超毫米波)	大于 300GHz	小于 1mm

网络信息文化标准分类

- 网络违法犯罪案件
 - 利用互联网进行违法案件

(1) 利用互联网煽动危害国家安全的；
 (2) 利用互联网进行邪教组织活动的；
 (3) 利用互联网捏造或者歪曲事实、散布谣言，扰乱社会秩序的；
 (4) 在互联网上建立淫秽色情网站、网页，提供淫秽站点链接，传播淫秽色情信

- 息，组织网上淫秽色情表演的；

(5) 利用互联网进行赌博的；

(6) 利用互联网进行盗窃、诈骗和敲诈勒索的；

(7) 利用互联网侮辱诽谤他人或捏造事实诽谤他人的；

(8) 利用互联网窃取、篡改、删除他人电子邮件或其他数据资料，侵犯公民通讯自由和通信秘密的；

(9) 利用互联网进行其他违法犯罪活动。

○ 危害互联网运行安全的违法案件

- (1) 进行网络入侵和攻击破坏活动的;
 - (2) 故意制作、传播计算机病毒等破坏程序的;
 - (3) 违反国家规定, 擅自中断网络运行或互联网服务的;
 - (4) 违反国家规定, 对信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作, 造成严重后果的;
 - (5) 其他危害网络安全的。

○ 重大的互联网运行安全突发事件

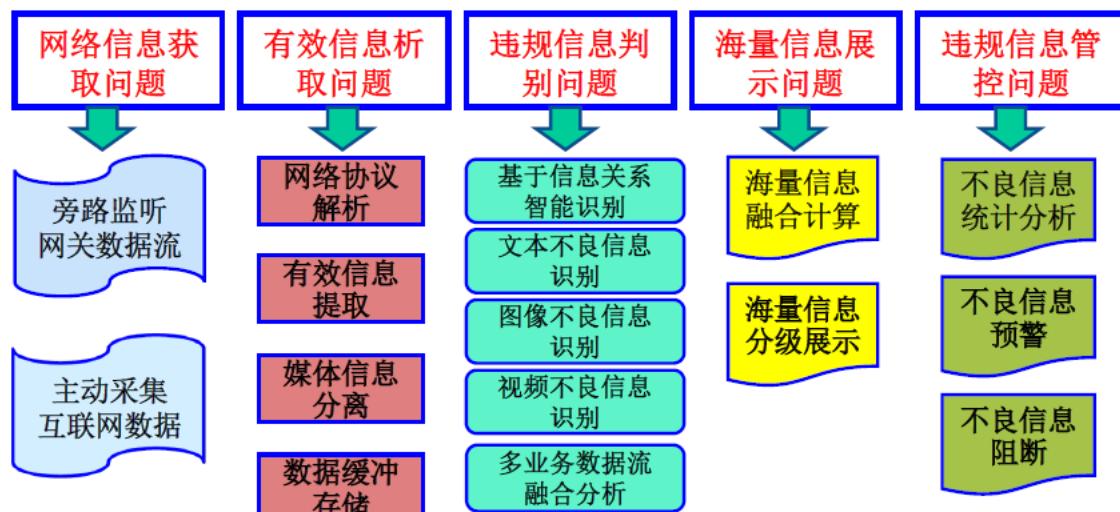
• 网络违法信息

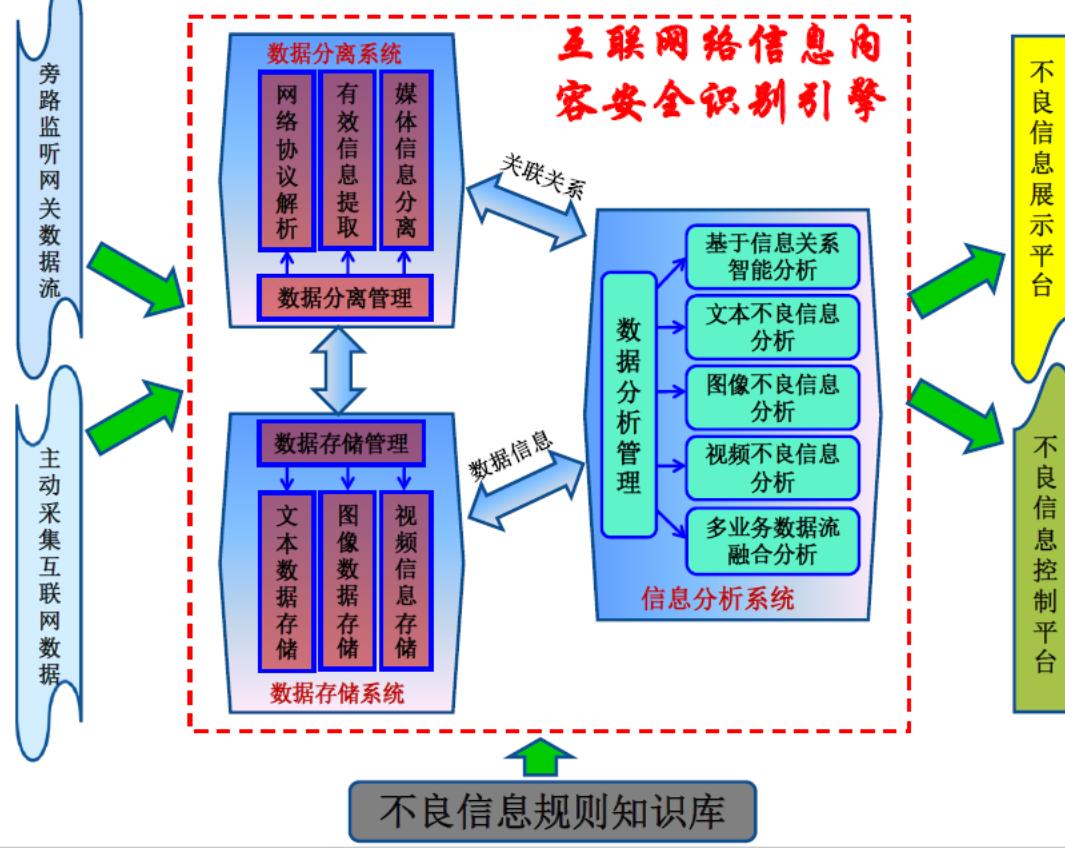
- (1) 反对宪法所确定的基本原则的；
 - (2) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
 - (3) 损害国家荣誉和利益的；
 - (4) 煽动民族仇恨、民族歧视，破坏民族团结的；
 - (5) 破坏国家宗教政策，宣扬邪教和封建迷信的；
 - (6) 散布谣言，扰乱社会秩序，破坏社会稳定；
 - (7) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
 - (8) 侮辱或者诽谤他人，侵害他人合法权益的；
 - (9) 含有法律、行政法规禁止的其它内容的。

• 网络不良信息

- - (1) 违背社会主义精神文明建设要求
 - (2) 违背中华民族优良文化传统与习惯
 - (3) 违背社会公德的各类信息
 - (4) 包括文字、图片、音视频等等

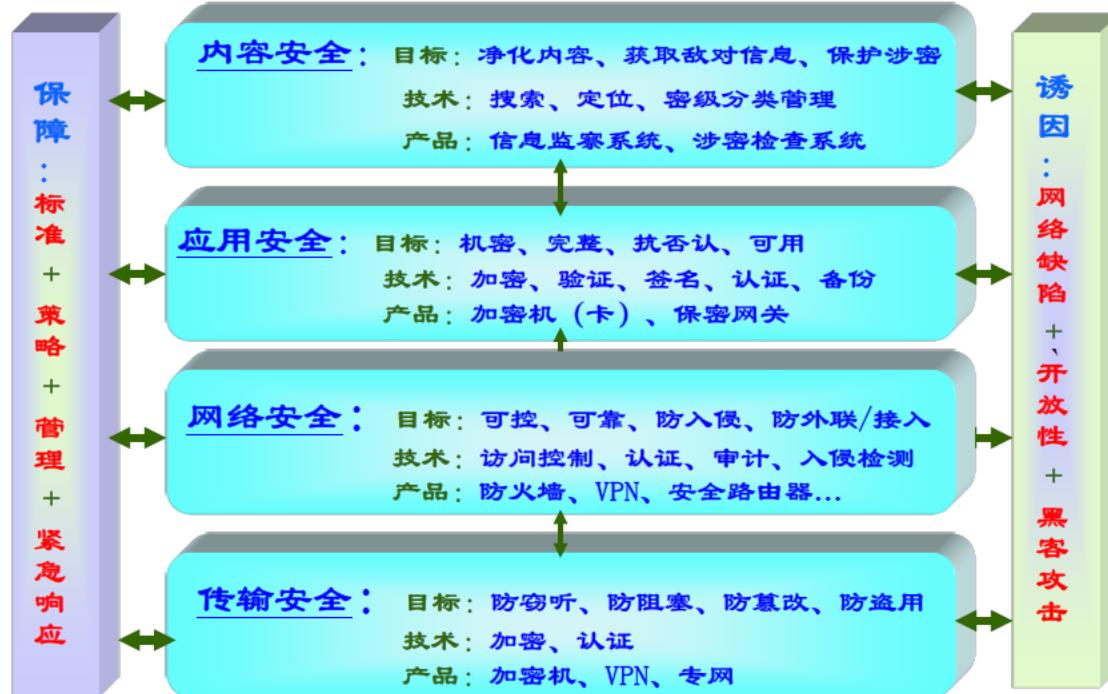
6 信息内容安全技术概述





7 信息内容安全技术产品

- 信息安全技术及产品



- 信息内容安全产品

- 当前，内容过滤正在成为越来越热门的话题。据IDC的分析统计预测，作为安全领域的一个重要分支，2007年，内容安全市场的市值将达到65亿美元。内容安全通常指称可提供反垃圾邮件、防毒、内容过滤/网页过滤、信息隐私等防护功能。
- 美国内容过滤软件整个市场每年的营业额达数十亿美元，而我国目前的市场规模只是美国的一个零头，很多网络安全企业对这个领域都非常看好。
- 网络安全在2002年得到了惊人发展，作为其中一部分的内容过滤技术也越来越受重视。
- 我国的过滤软件市场与发达国家相比，还处于发展的初级阶段。在美国，从事内容过滤软件研制的几大专业公司都是上市公司。
- 内容过滤产品要做好，技术难度和市场难度都很大。