信息安全概论

罗文坚

2021年秋季

教学目的

- 课程定位：信息安全领域基础课程
  - 《密码学基础》与《网络安全》等课程的先修课程。

- 课程目的：
  1. 对信息安全领域知识有较全面的了解；
  2. 掌握信息安全领域的基本原理和工作机制；
  3. 具有解决一些信息安全问题的能力；
  4. 为学生进一步在信息安全领域进行深入学习打下基础。

教学目标

- 课程目标：
  1. 全面了解信息安全知识领域的体系结构，了解信息安全发展历史，了解信息安全技术产生与发展，了解信息安全问题对国家及社会的影响；

  2. 理解密码的基本理论及应用方法，掌握身份认证及访问控制的基本方法，具有设计信息安全方案的初步能力，了解网络威胁的产生机理与网络防御的基本技术，具有解决信息安全问题的初步能力；

  3. 了解信息安全系统、工程的技术标准及操作规范，明确有关信息安全的法律法规，建立初步的信息安全工程素质和全面的信息安全法律意识。

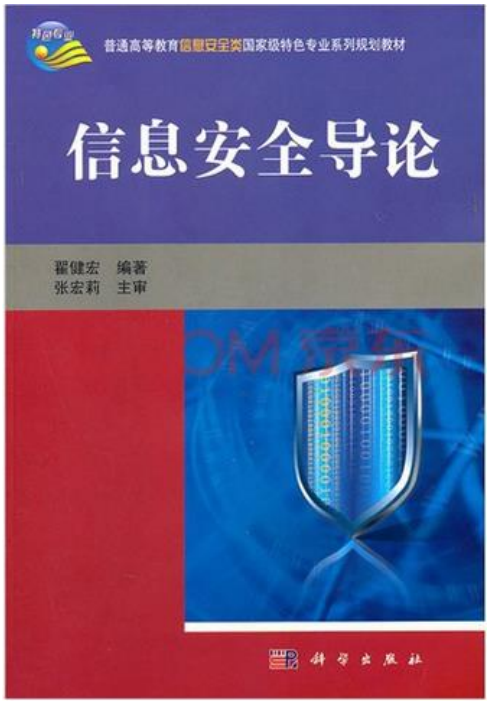
教学内容

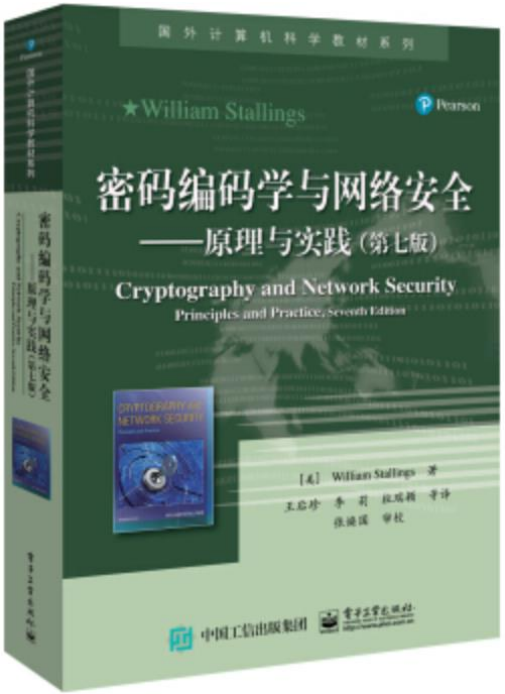
- 总学时：32；讲课学时：32
- 教学内容：
  1. 信息安全概述
  2. 密码学基础
  3. 物理安全
  4. 身份认证
  5. 访问控制
  6. 网络威胁
  7. 网络防御
  8. 网络安全协议
  9. 内容安全
  10. 信息安全管理

教材

- 教材：翟健宏. 信息安全导论. 北京: 科学出版社. 2019.

- 主要参考书：Stallings William著, 王后珍等译.《密码编码学与信息安全—原理与实践(第7版). 电子工业出版社. 2017.





成绩考核

- 期末考试（开卷）：60％
- 作业（+课堂练习）：40%

- 教师：
  - 罗文坚，luowenjian@hit.edu.cn，信息楼L1721

- 助教：4人
  - 常亚桐、宋振、罗永康、杨向凯。

- 课件发布：QQ群。

第1章 信息安全概述

本章内容

- 1.1 信息安全的理解
- 1.2 信息安全威胁
- 1.3 互联网的安全性
- 1.4 信息安全体系结构

信息与信息安全

- 信息：事物运动的状态与方式
  - ISO给出的解释：“信息是通过施加于数据上的某些约定而赋予这些数据的特定含义”。
  - 通常我们可以把消息、信号、数据、情报和知识等都看作信息。信息本身是无形的，借助信息介质以多种形式存在或传播。
- 信息安全
  - ISO给出的定义：“在技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”。
  - 信息安全的目的：“确保以电磁信号为主要形式的、在计算机网络化系统中进行获取、处理、存储、传输和应用的信息内容在各个物理及逻辑区域中的安全存在，并不发生任何侵害行为”。

信息安全的发展阶段

- 信息安全的发展阶段
  - 通信安全—→ 信息安全—→信息保障

- 通信安全（COMSEC）阶段
  - 20世纪90年代以前，这一阶段的信息安全可以简单称为通信安全，主要目的是保障传递的信息安全，防止信源、信宿以外的对象查看信息。

- 信息安全（INFOSEC）阶段
  - 20世纪90年代以后，主要保证信息的机密性、完整性、可用性、可控性、不可否认性。

信息安全的发展阶段

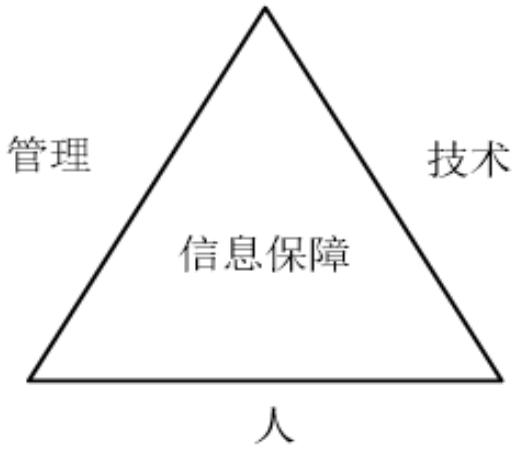
- 信息安全（INFOSEC）阶段
  - 要点：机密性、完整性、可用性、可控性、不可否认性。
  - ➢ 机密性（Confidentiality）指信息只能为授权者使用而不泄漏给未经授权者的特性。
  - ➢ 完整性（Integrity）指保证信息在存储和传输过程中未经授权不能被改变的特性。
  - ➢ 可用性（Availability）指保证信息和信息系统随时为授权者提供服务的有效特性。
  - ➢ 可控性（Controllability）指授权实体可以控制信息系统和信息使用的特性。
  - ➢ 不可否认性（Non–Repudiation）指任何实体均无法否认其实施过的信息行为的特性，也称为抗抵赖性。

信息安全的发展阶段

- 信息保障（IA，Information Assurance）阶段
  - 1996年，美国国防部提出了信息保障：
    - 保护（Protect）、检测（Detect）、反应（React）、恢复（Restore）四个方面。
  - 我国也对信息保障给出了相关解释：
    - 信息保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

信息安全的发展阶段

- 信息保障（IA，Information Assurance）阶段
  - 信息保障三大要素：
    - 人是信息保障的基础；
    - 技术是信息保障的核心；
    - 管理是信息保障的关键。



  - 信息安全不是一个孤立静止的概念，具有系统性、相对性和动态性。

本章内容

- 1.1 信息安全的理解
- 1.2 信息安全威胁
- 1.3 互联网的安全性
- 1.4 信息安全体系结构

信息安全威胁的基本类型

- 信息泄露：信息被有意或无意泄露给某个非授权的实体。
- 信息伪造：某个未授权的实体冒充其他实体发布信息，或者从事其他网络行为。
- 完整性破坏：非法手段窃取信息的控制权，未经授权对信息进行修改、插入、删除等操作，使信息内容发生不应有的变化。
- 业务否决或拒绝服务：攻击者通过对信息系统进行过量的、非法的访问操作使信息系统超载或崩溃，从而无法正常进行业务或提供服务。
- 未经授权访问：某个未经授权的实体非法访问信息资源，或者授权实体超越其权限访问信息资源。

信息安全威胁的主要表现形式

- 攻击原始资料
  - 人员泄露，废弃的介质，窃取
- 破坏基础设施
  - 破坏电力系统，破坏通讯网络，破坏信息系统场所
- 攻击信息系统
  - 物理侵入，特洛伊木马，恶意访问，服务干扰，旁路控制，计算机病毒
- 攻击信息传输
  - 窃听，业务流分析，重放。
- 恶意伪造
  - 业务欺骗，假冒，抵赖
- 自身失误
- 内部攻击

本章内容

- 1.1 信息安全的理解
- 1.2 信息安全威胁
- 1.3 互联网的安全性
- 1.4 信息安全体系结构

互联网的发展现状

- 1983年，ARPA和美国国防部通信局研制TCP/IP协议，该协议被做为其BSD UNIX的一部分。
- 1986年，NSF利用Internet Protocol，连接5个科研教育服务机构，建立了NSFnet广域网。
- 1987年开始，中国四大网络CSTnet、CERNET、Chinanet、GBnet与Internet直连。
- 2007年底，我国互联网用户1.62亿，其中宽带上网用户达到1.22亿，中文网站89.8万个，IPv4地址总数9800多万个，国际出口带宽总量为368927Mbps。

互联网的安全现状

- 2000年开始，病毒制造产业化操作，黑色产业链每年的整体利润预计高达数亿元。

- 黑客窃取的个人资料，包括QQ密码、网游密码、银行账号、信用卡帐号，等等。任何可以直接或间接转换成金钱的东西，都成为不法分子窃取的对象。

- CERT（Computer Emergency Response Team）统计：
  - 在1988年安全事件6件，2001年5万件，2003年为13万7千多件，在2003年以后发生呈线性增长。
- 据中国计算机网络应急技术处理协调中心统计：
  - 2006年26476件，是2005年9112件的三倍。

安全事件

- 1988年,著名的“Internet蠕虫事件”使得6000余台计算机的运行受到影响。
- 1998年2月份，黑客利用Solar Sunrise弱点入侵美国防部网络，攻击相关系统超过500台计算机，而攻击者只是采用了中等复杂工具。
- 2000年春季,黑客分布式拒绝服务攻击（DDOS）大型网站，导致大型ISP服务机构Yahoo网络服务瘫痪。
- 2001年5月,中美黑客大战。
- 2001年8月，“红色代码”蠕虫利用微软web服务器IIS 4.0或5.0中index服务的安全缺陷，攻破目的机器，并通过自动扫描感染方式传播蠕虫，已在互联网上大规模泛滥。
- 2003年，“冲击波”蠕虫的破坏力就更大；安全专家Bruce Schneier撰文分析认为，美国2003年8月份大停电与“冲击波蠕虫”相关。

国内信息安全事件（2010年1-2月）

- 公安部物证鉴定中心网站被黑客篡改：1月2日，公安部物证鉴定中心的中英文网站遭黑客入侵，网站页面不断被篡改。

- 商务中国网站DNS服务器遭受非法攻击：1月15日，商务中国网站DNS服务器遭受非法攻击，部分域名解析服务受到影响，网站无法访问。

- 入侵网站改成绩被诉，系首例：“黑客”，北京教育考试院原工作人员孟某，涉嫌利用木马病毒程序进入北京教育考试院网上证书查询系统，篡改全国计算机等级考试成绩，被检方提起公诉。

- 百度被黑11小时无法正常访问：1月12日上午8点左右，搜索引擎网站百度被发现无法打开，网站处于无法访问状态。当日中午11：10左右，百度首次公开证实由于域名在美国注册，被自称为“伊朗网军”的黑客非法篡改，导致不能正常访问。

- 央视官网被黑两小时，主页篡改：2月15日，中央电视台官方网站间断无法登录，www.cctv.com主页变成了一欧洲美女子照片。

- 女孩设山寨“彩票网”获有期徒刑：创办山寨“中国彩票官方网”，以提供中奖号码为诱饵骗取彩民入会费4万余元，25岁的女孩王某，因诈骗罪被北京宣武法院判处有期徒刑2年。

国内信息安全事件（2010年1-2月）

- 河南：大量遭拒绝服务攻击。2010年1月，有3353个IP地址所对应的主机被境外通过木马程序秘密控制，有3046个IP地址对应的主机被僵尸网络控制，被篡改网站数量70个，感染恶意代码的主机数量为3498个。

- 重庆：青年农民办钓鱼网站行骗，盗取网购者5.2万余元。重庆市潼南县农村青年张某在网上租来域名和空间，做山寨淘宝、山寨易趣、山寨腾讯拍拍。通过这些“钓鱼网站”，盗走网购消费者5.2万余元。1月10日，张某因构成盗窃罪和传授犯罪方法罪，一审被判刑6年。

- 上海：窃用他人账户套现，上海一网店店主被判7年。淘宝某店铺声称代人缴费后可打折收取账单金额，然而店铺卖家用来缴费的却是从不正当途径取得的他人银行账户内钱款。1月25日，上海一中院做出二审判决，认定网店店主犯信用卡诈骗罪。

- 广东：黑客受雇潜入人事网篡改数据被判刑。黑客受雇潜入广东人事网篡改查询数据，为假证“转正”，并添加10多个虚假职称人员的资料。2010年1月26日，24岁的朱某因两次非法侵入广东人事网上传并篡改数据，犯非法入侵计算机信息系统罪被越秀区法院判处有期徒刑1年零7个月。

国内信息安全事件（2010年1-2月）

- **湖北：**黑客培训网站。湖北警方成功摧毁国内规模最大的黑客培训网站“黑鹰安全网”，该网站招收会员逾18万人，向其提供木马程序，“传授”、“交流”非法控制他人计算机的“技巧”。

- **湖南：**黑客篡改湖南通管局主页。1月29日，湖南省通信管理局网站被黑。黑客篡改主页，留言声称，因为几个月网站备案都未审批通过，所以不满而攻击。

- **珠海：**首例侵犯公民信息安全案宣判。1月3日，被告人周某因非法出售公民个人信息资料被珠海市香洲人民法院以非法获取公民个人信息罪判处有期徒刑1年6个月，并处罚金。

近期代表性安全事件

- 30人贩卖6亿条个人信息
  - 2020年1月，镇江丹阳警方侦破一起公安部督办的侵犯公民个人信息案，涉及10多个省市，抓获犯罪嫌疑人30名。该团伙采用境外聊天工具和区块链虚拟货币收付款，共贩卖个人信息6亿余条。
- 台积电生产工厂和营运总部中勒索病毒
  - 2020年8月3日晚间，台积电生产工厂和营运总部，突然传出电脑遭病毒入侵且生产线全数停摆的消息。
- 某黑客组织对我国关键领域发动钓鱼邮件攻击
  - 钓鱼邮件攻击，邮件以“海事政策分析和对南亚的港口安全影响”、“2020年自主研发项目立项论证报告”等主题，主要针对我国政府部门、科研机构相关人员发起定向邮件攻击。

近期代表性安全事件

- 委内瑞拉国家电网干线遭攻击，全国大面积停电
  - 2020年5月，委内瑞拉副总统罗德里格斯宣布消息，委内瑞拉国家电网干线遭到攻击，造成全国大面积停电。
- 新西兰证交所连续一周遭受DDoS攻击导致交易中断（2020年8月25-31日）
- 黑客入侵500多组商店和家庭摄像头！已被广州警方刑拘（2021年8月）
  - 该案是广东省首例打击非法入侵“常规摄像头”的黑客案件，具有典型意义。
- App侵害用户权益专项整治行动
  - 针对App侵害用户隐私安全的问题，工信部已建立全国App技术检测平台，对国内上架的热门App进行技术检测。

安全趋势

- 集团化、产业化的趋势
  - 产业链：病毒木马编写者→专业盗号人员→销售渠道→专业玩家
  - 病毒不再安于破坏系统，销毁数据，而是更关注财产和隐私。
  - 电子商务成为热点，针对网络银行的攻击也更加明显。
- “黑客”逐渐变成犯罪职业
  - 财富的诱惑，使得黑客袭击不再是一种个人兴趣，而是越来越多的变成一种有组织的、利益驱使的职业犯罪。
  - 事例：拒绝服务相关的敲诈勒索和“网络钓鱼”。

安全趋势

- 恶意软件的转型
  - 恶意软件在行为上将有所改观，病毒化特征削弱，但手段更“高明”，包含更多的钓鱼欺骗元素。
  - 我国是恶意软件最多的国家。

- 网页挂马危害继续延续
  - 服务器端系统资源和流量带宽资源大量损失。
  - 成为网络木马传播的“帮凶”。
  - 客户端的用户个人隐私受到威胁。

安全趋势

- 利用应用软件漏洞的攻击将更为迅猛
  - 新的漏洞出现要比设备制造商修补的速度更快。
  - 一些嵌入式系统中的漏洞难以修补。
  - 零日攻击现象日趋普遍。

- Web2.0的产品受到挑战
  - 以博客、论坛为首的web2.0产品成为病毒和网络钓鱼的攻击目标。
  - 社区网站上带有社会工程学性质的欺骗往往超过安全软件所保护的范畴。
  - 自动邮件发送工具日趋成熟，垃圾邮件制造者正在将目标转向音频和视频垃圾邮件。

安全趋势

- 无线网络、移动手机成为安全重灾区，消费者电子设备遭到攻击的可能性增大
  - 在无线网络中被传输的信息没有加密或者加密很弱，很容易被窃取、修改和插入，存在较严重的安全漏洞。
  - 手机病毒利用普通短信、彩信、上网浏览、下载软件与铃声等方式传播，还将攻击范围扩大到移动网关、WAP服务器或其他的网络设备。
  - 越来越多采用USB标准进行连接，并使用了更多存储设备和电脑外围产品。

信息安全意义

- 互联网安全不仅影响普通网民的信息和数据的安全性，而且严重的影响国家的健康发展。

- 网络安全与政治
- 网络安全与经济
- 网络安全与军事
- 网络安全与社会稳定

互联网的安全性分析

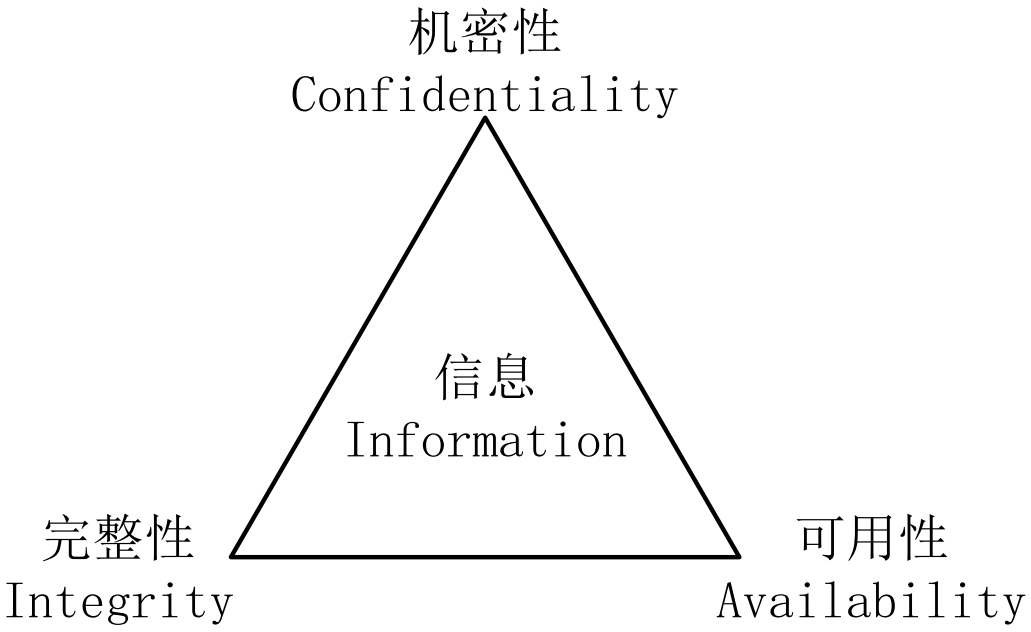
- 互联网的设计原始背景
- 网络传输的安全性
- 信息系统的安全性
  - 基础网络应用成为黑客及病毒的攻击重点。
  - 系统漏洞带来的安全问题异常突出。
  - Web程序安全漏洞愈演愈烈。
- 社会工程学攻击越来越多

本章内容

- 1.1 信息安全的理解
- 1.2 信息安全威胁
- 1.3 互联网的安全性
- 1.4 信息安全体系结构

面向目标的知识体系结构

- 信息安全的三个基本目标



信息安全的三个基本目标（金三角）

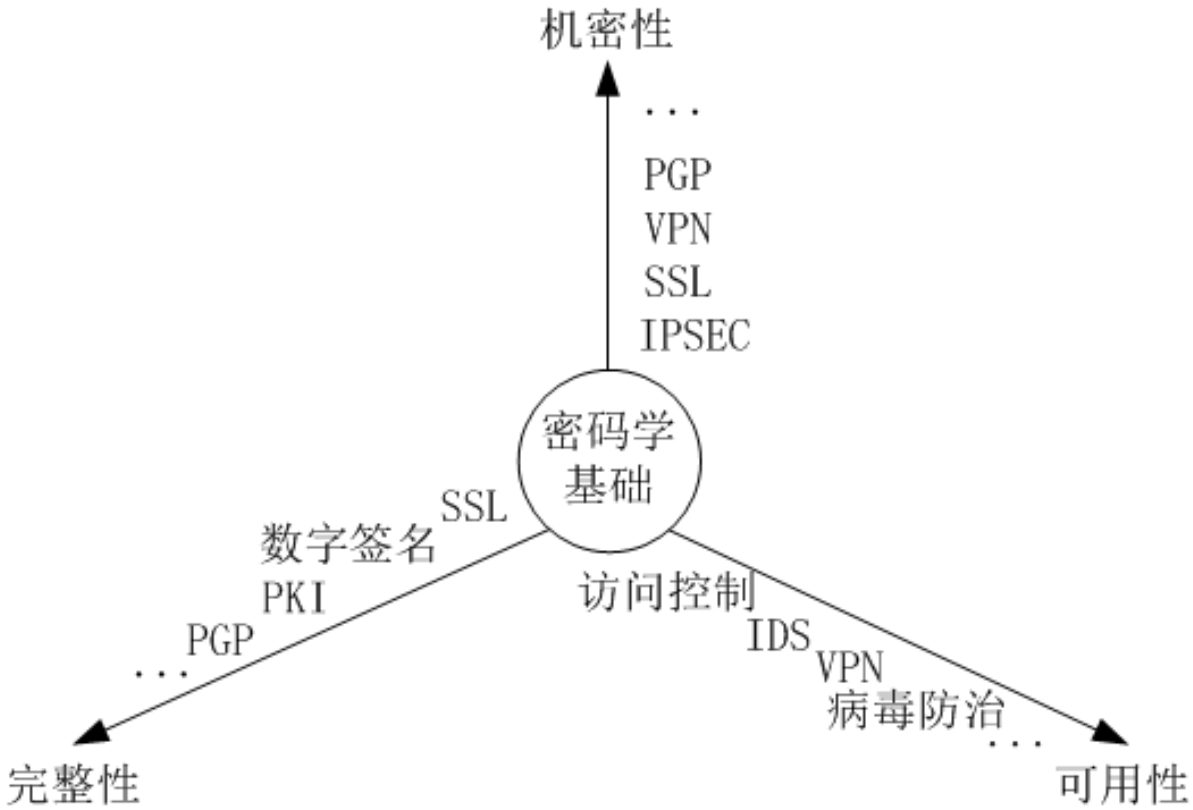
CIA三元组

- CIA三元组是信息安全的三个最基本的目标：
  - 机密性Confidentiality：指信息在存储、传输、使用过程中，不会泄漏给非授权用户或实体；
  - 完整性Integrity：指信息在存储、使用、传输过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；
  - 可用性Availability：指确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源。

- DAD（Disclosure、Alteration、Destruction）是最普遍的三类风险。
  - 泄露、篡改、破坏。

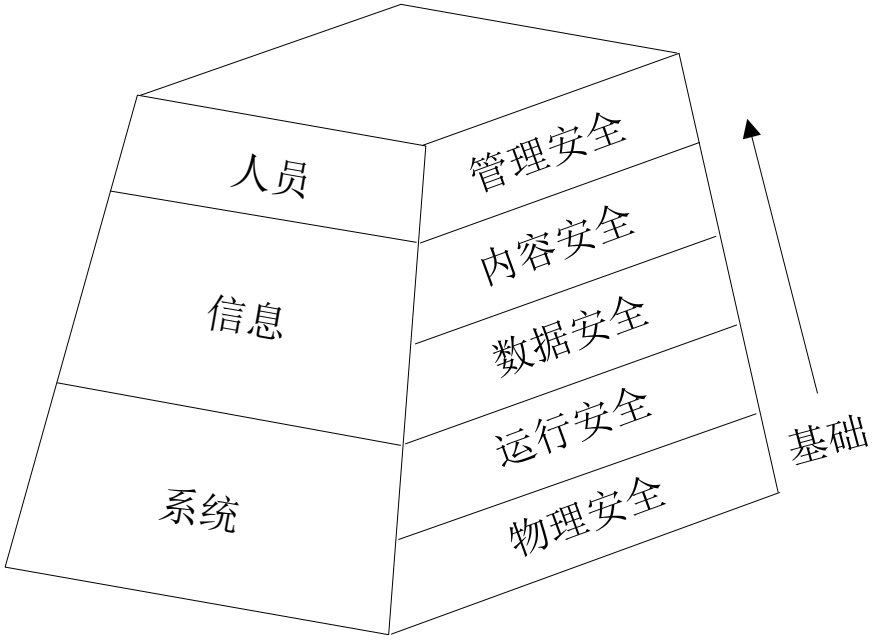
围绕CIA三元组展开的知识体系

- 密码学是三个信息安全目标的技术基础。
- CIA技术存在着一定程度上的内容交叉。



面向应用的层次型技术体系架构

- 信息系统基本要素
  - 人员、信息、系统
- 安全层次
  - 三个不同部分存在五个安全层次与之对应
  - 每个层次均为其上层提供基础安全保证



面向应用的层次型信息安全技术体系结构

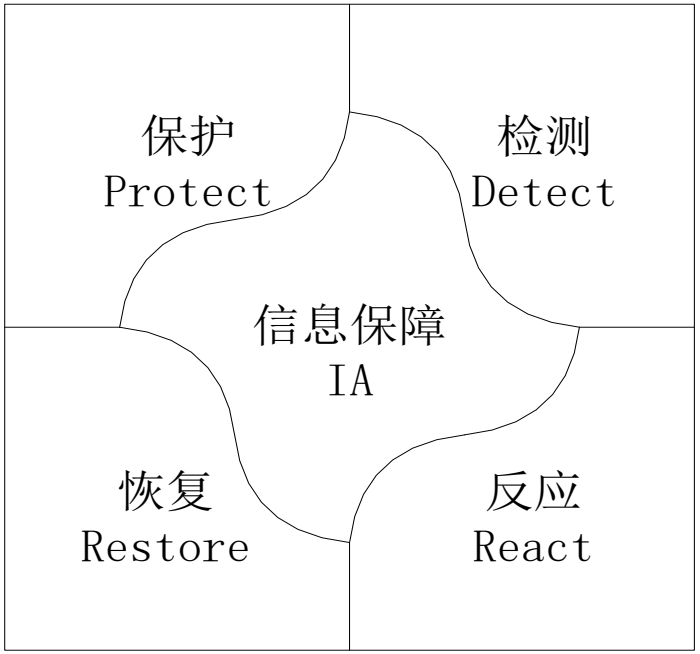
安全层次

- 物理安全
  - 指对网络及信息系统物理装备的保护。
- 运行安全
  - 指对网络及信息系统的运行过程和运行状态的保护。
- 数据安全
  - 指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。
- 内容安全
  - 指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。
- 管理安全
  - 指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护。

面向过程的信息安全保障体系

- 美国国防部提出的“信息安全保障体系”诠释了安全保障的内涵。

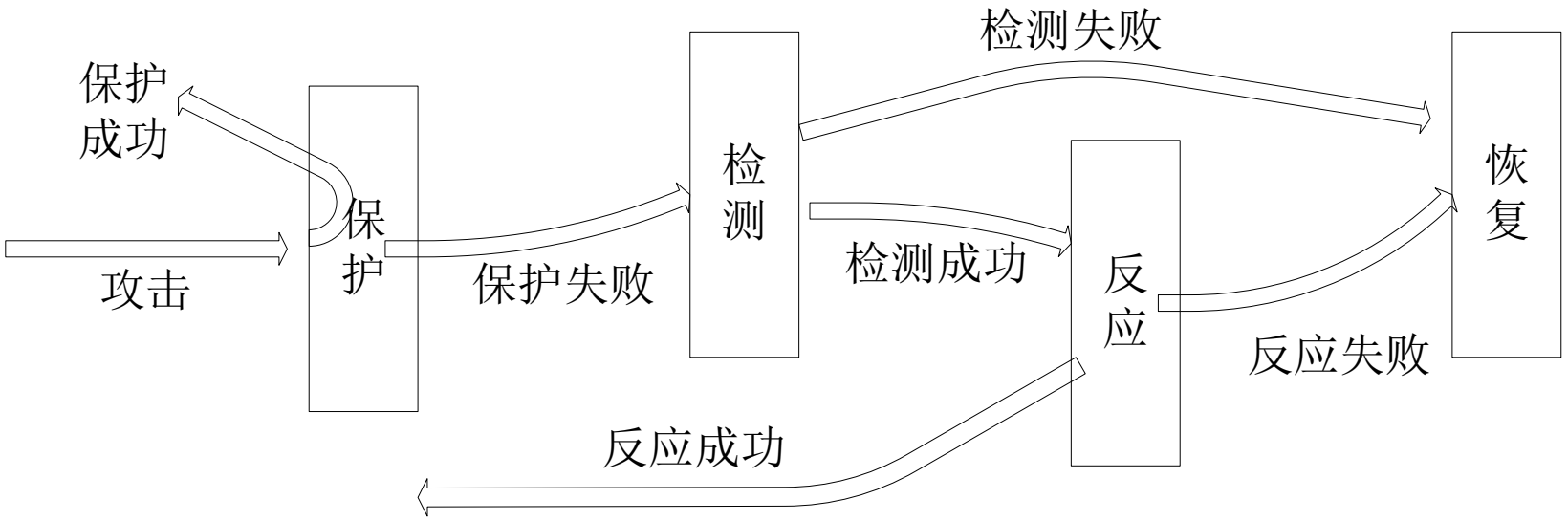
- 信息安全保障体系包括四个部分内容，即PDRR。
  - 保护（Protect）
  - 检测（Detect）
  - 反应（React）
  - 恢复（Restore）



信息保障体系

面向过程的信息安全保障体系

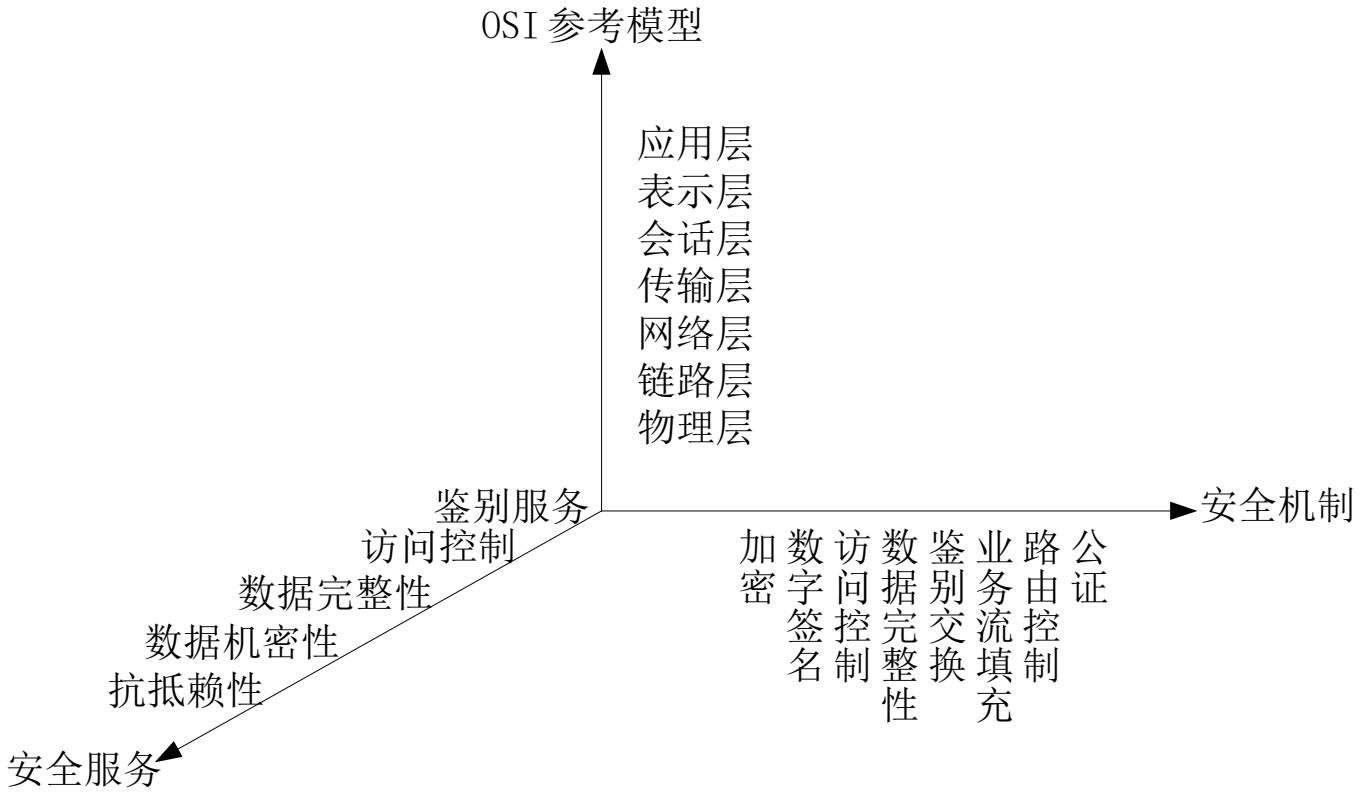
- 信息安全保障是一个完整的动态过程，而保护、检测、反应和恢复可以看作信息安全保障四个子过程。



PDRR 模型安全保障动态过程示意图

OSI开放系统互连安全体系结构

- **ISO7498-2（1989）：《信息处理系统、开放系统互连、基本参考模型—第2部分：安全体系结构》。描述的开放系统互联安全体系结构是一个普遍适用的安全体系结构。**



ISO7498-2 安全体系结构三维图

安全服务（Security Service）

1. 鉴别服务：确保某个实体身份的可靠性。
2. 访问控制：确保只有经过授权的实体才能访问受保护的资源。
3. 数据机密性：确保只有经过授权的实体才能理解受保护的信息。
4. 数据完整性：防止对数据的未授权修改和破坏。
5. 抗抵赖性：用于防止对数据源以及数据提交的否认。

安全机制（Security Mechanism）

1. 加密：用于保护数据的机密性。
2. 数字签名：保证数据完整性及不可否认性的一种重要手段。
3. 访问控制：访问实体成功通过认证，访问控制对访问请求进行处理，查看是否具有访问所请求资源的权限，并做出相应的处理。
4. 数据完整性：用于保护数据免受未经授权的修改。
5. 鉴别交换：用于实现通信双方实体的身份鉴别。
6. 业务流填充：针对的是对网络流量进行分析攻击。
7. 路由控制：可以指定数据报文通过网络的路径。路径上的节点都是可信任的。
8. 公证机制：由第三方来确保数据完整性、数据源、时间及目的地的正确。

安全服务与OSI各协议层之间的关系

ITU-T X.800

安全服务	OSI协议层						
	物理	链路	网络	传输	会话	表示	应用
对等实体鉴别			Y	Y			Y
数据源鉴别			Y	Y			Y
访问控制服务			Y	Y			Y
连接机密性	Y	Y	Y	Y		Y	Y
无连接机密性		Y	Y	Y		Y	Y
选择字段机密性						Y	Y
流量机密性	Y		Y				Y
有恢复功能的连接完整性				Y			Y
无恢复功能的连接完整性			Y	Y			Y
选择字段连接完整性							Y
无连接完整性			Y	Y			Y
选择字段非连接完整性							Y
源发方抗抵赖							Y
接收方抗抵赖							Y

思考题

① 怎么理解信息安全、机密性、完整性、可用性，试举例说明；

② “信息安全是当今社会的亟待解决的重大问题”，你认为如何？

③ 你了解的网络安全是什么样的？你了解的密码学是什么样的？

④ 为什么会话层不提供安全服务？为什么最适合配置安全服务的是物理层、网络层、传输层及应用层，而其他各层不太适宜配置安全服务？

休息是为了走更远的路！