网络空间安全及法律法规

第一章 网络空间安全概述

第一节 信息时代下网络空间安全学科浅谈

信息论的基本观点:

1. 信息是内涵，系统是载体。
2. 信息不能脱离它的载体商孤立存在。
3. 信息只有存储、处理、传输三种状态

信息的安全属性三要素（C、I、A）：

1. 机密性（Confidentiality）：保证信息与信息系统不被非授权者截获和未经授权使用。
2. 完整性（Integrity）：信息是完整的，真实的、未被篡改的、正确的。
3. 可用性（Avalaibility）：信息与信息系统服务可被授权人正常使用

信息系统安全层次结构：面向应用信息安全框架（自高向低）

1. 内容安全：信息安全在政治、法律、道德层次上的要求，是语义层次的安全
2. 数据安全：数据免受未授权的泄露、篡改和毁坏
    - 数据的秘密性（Secrecy)：数据不被未授权者知晓的属性
    - 数据的完整性(Integrity)：数据是正确的、真实的、未被篡改的、完整无缺的属性
    - 数据的可用性(Availabity)：数据可以随时正常使用的属性

3. 行为安全：主体行为的过程和结果来考察是否会危害信息安全
4. 设备安全：软硬件系统的安全（稳定、可靠、可用）
    a. 信息系统设备的安全是信息系统安全的首要问题
    b. 信息设备是信息系统安全的物质基础
    - 设备的稳定性（Stability)：设备在一定时间内不出故障的概率
    - 设备的可靠性(Reliability)：设备在一定时间内正常执行任务的概率
    - 设备的可用性(Availabity)：设备随时可以正常使用的概率

信息安全三大定律：

1. 普遍性定律：哪里有信息，哪里就有信息安全问题。
2. 中性定律：安全与方便是一对矛盾体
3. 就低性定律（木桶原理）：一个系统的安全性取决于它最薄弱部分的安全性

网络空间安全学科是研究**信息获取、信息存储、信息传输和信息处理领域中**信息安全保障问题的一门新兴学科。

研究方向：

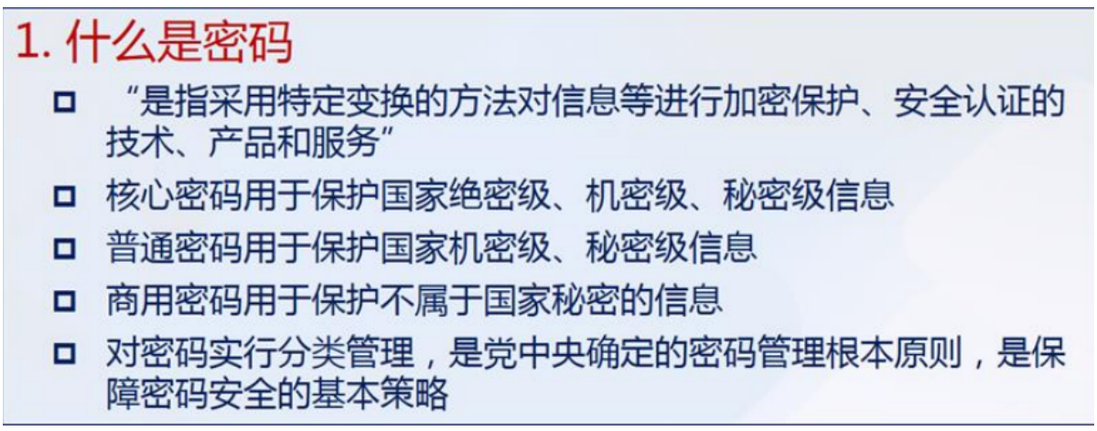
1. 密码学：由密码编码学和密码分析学组成
    a. 密码编码学：主要研究对信息进行编码以实现信息隐藏
    b. 密码分析学：主要研究通过密文获取对应的明文信息
2. 网络安全：在网络的各个层次和范围内采取防护措施，以便能对各种**网络安全威胁进行检测和发现**，并采取相应的**响应措施**，确保网络环境的信息安全
3. 系统安全：
    - 信息系统是信息的载体，一般是直接面对用户的服务系统
    - 信息系统安全的特点是从系统的整体上考虑安全威胁与防护
4. 信息内容安全：
    - 信息内容安全是信息安全在政治、法律、道德层次上的要求
    - 信息内容在政治上是健康的，是符合国家法律法规的，是符合中华民族优良的道德规范的
5. 信息对抗：
    - 信息对抗是为消弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施
    - 实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权

第二节 网络空间安全法律法规与标准

我国网络空间安全国家战略的五个具体要求：和平、安全、开放、合作、有序

网络空间的安全威胁根据主体不同，可分为黑客攻击、有组织网络犯罪、网络恐怖主义、国家支持的网络战四种类型

- 《中华人民共和国网络安全法》是我国**第一部全面规范网络空间安全管理**方面问题的基础性法律，是我国网络空间法治建设的重要里程碑
    - 等级保护：
        - 等级保护涉及的内容：信息系统、信息安全产品、信息安全事件
        - 分级依据：重要程度、危害程度、保护水平 (业务信息、系统服务）
        - 保护级别划分：自主保护级、指导保护级、监督保护级、强制保护级、专控保护级
        - 安全管理：自主定级-----审核批准----系统建设----安全测评
- 《中华人民共和国密码法》&《保密法》



根据秘密的性质不同，秘密可分为：

- 国家秘密：所谓国家秘密是指关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项（《保密法》第二条）
    - 绝密级：最重要的国家机密，泄露会使国家安全和利益遭受特别严重的损害
    - 机密级：重要的国家秘密，泄露会使国家安全和利益遭受严重的损害
    - 秘密级：一般的国家秘密，泄露会使国家安全和利益遭受损害

  解密期：绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年（《保密法》第十五条）
- 工作秘密：是各级国家机关产生的事项。工作秘密的主体是各级国家机关。工作秘密是涉及机关单位的公务活动和内部管理的事项。工作秘密是不属于国家秘密，又不宜公开的事项。
- 商业秘密：是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。
- 个人秘密：个人隐私

- 《中华人民共和国数据安全法》重点确立了数据安全保护的各项基本制度，完善了多项重要管理制度，形成了我国数据安全的顶层设计
- 《中华人民共和国个人信息保护法》：确立个人信息保护原则、规范处理活动保障权益、禁止“大数据杀熟”、严格保护敏感个人信息

第二章 密码学基础

第一节 密码学概述

古典密码：

- 古典替换：将明文字母替换成其他的字母、数字和符号
  1. 单表替换：一个明文字母对应的密文字母是确定的

     凯撒密码：每个字母用其后的第三个字母替换
  2. 多表替换：一个明文字母可以表示为多个密文字母

     维吉尼亚密码：根据密钥来决定用哪一行的密表来进行代换。
  3. 多字母替换：用密钥字母和其它字母构造一个5X5的密钥表矩阵，加密时则采用代换规则

     普莱费尔密码：将明文中的双字母组合作为一个单元，并将这些单元转换为密文的双字母组合。其三个步骤为：编制密码表、整理明文、编写密文
     仿射密码--Hill密码：m个连续的明文字母用m个密文字母代替，该代替由m个线性方程决定
- 古典置换：又称换位密码，是通过重新排列明文中元素的位置而不改变元素本身来实现加密的体制

一次一密密码：

- 一次一密密码需要使用一个大的真随机字母集作为密钥，这个字母集被写在纸上，并粘成一个乱码本。加密时，需要将明文字符和乱码本的密钥字符进行模26加法运算
- 密钥本身随机，而且密钥只使用一次。即使获得了上次通信的密文和密钥，攻击者仍然无法确定下次通信的真正密钥。

现代密码：

- DES算法（一种分组密码，其输入的明文长度为64bit，密钥长度为56bit，输出的密文长度为64bit）
- 公钥密码体制，又称双钥密码体制或非对称密码体制（Two-key/AsymmetricCryptosystem），就是在加密和解密的过程中分别使用不同的密钥
  - 对于公钥密码体制，安全性主要取决于构造算法所依赖的数学难题。
  - 多项式求根、离散对数问题（ECC/EIGamal）、大整数因式分解（RSA）、背包问题（背包密码）、DiffieHellman问题（Diffie-Hellman算法）、二次剩余问题(Rabin)、模n的平方根问题等
- 量子密码：保密通信的双方使用量子态作为信息载体，并利用量子力学原理，建立共享密钥的方法，具有不可窃听性+一次一密的不可破译性

面临的挑战：

- 云计算/存储：用密码感知数据存在、用密码确保数据的安全性、用密码确保用户的隐私
- 大数据：大数据的数据量特别巨大，数据存在多样性，使密码算法需要处理的数据规模不断增大，使用密码技术的成本不断提高，这就要求密码算法具有高效性和很强的适应性（柔性性）
- 物联网：密码要适应数据多样性、适应网络多样性和多层次、适应各层次的资源差异较大

- 新型计算机：强大的计算能力
- 区块链技术：区块链由于需要在众多节点间通过共识机制达成一致，因此其性能目前还比较低下

第二节 密码学基本概念

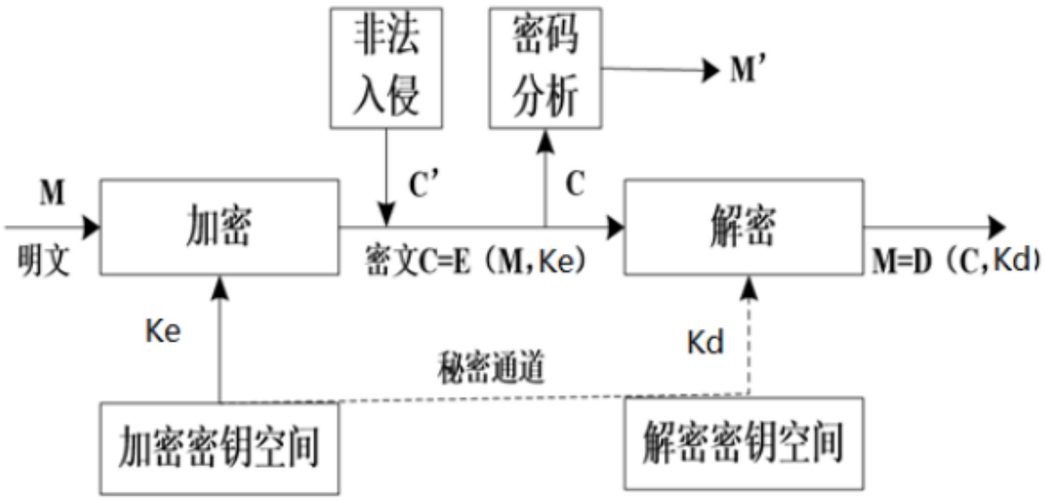
密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换

- 古典密码学包含两个互相对立的分支，即密码编码学（Cryptography）和密码分析学（Cryptanalytics）。前者编制密码以保护秘密信息，而后者则研究加密消息的破译以获取信息。二者相反相成，共处于密码学的统一体中。
- 现代密码学除了包括密码编码学和密码分析学外，还包括安全管理、安全协议设计、散列函数
  等内容。

密码学的目的：使不知道如何解密的攻击者不可能由其截获的密文中得到任何有意义的明文信息

保密通信：

- 链路加密：在数据传输的每一节点上，对数据全部加密
- 端到端加密：加密过程在两个端系统上完成，源主机或终端对数据进行加密，加密形式的数据原封不动传过网络到达目的主机或终端
- 加密功能的逻辑位置越高层，得到加密的信息就越少，但是被加密的信息越安全



- 若ke = kd，则加密算法称为单钥加密体制（One-key Cryptosystem ）（对称加密体制（ Symmetric Cryptosystem ）或秘密密钥加密体制（Scret-key Cryptosystem)
- 若ke ≠ kd，则加密算法称为双钥加密体制(Two-key Cryptosystem ）（非对称加密体制(Asymmetric Cryptosystem)或公钥加密体制（Public -key Cryptosystem）

密码的安全性：

- 无条件安全（Unconditionally secure）：无论破译者有多少密文,他也无法解出对应的明文,即使他解出了,他也无法验证结果的正确性.

- 计算上安全（Computationally secure）：只要给攻击者足够的时间和存储资源， 都是可以破译的
- 不可攻破的密码系统：理论上虽然可以攻破，但是真正要攻破的话，所需要的计算资源如计算机时间和容量超出了实际上的可能性

密钥分析的实质就是在攻击者不知道密钥的情况下，对所截获的密文或明-密文对采用各种不同的密码分析方法试图恢复出明文或密钥，常见类型有：

- 唯密文攻击：破译者具有密文串和加密算法
- 已知明文攻击：破译者具有明文串和相应的密文串和加密算法，推算出密钥
- 自适应选择明文攻击：破译者具备选择明文串并构造出相应的密文串，比“已知明文攻击”更有
  效的推算出密钥和算法
- 选择密文攻击：破译者密文串、加密算法、可选择密文串，并构造出相应的明文

常见方法有：

- 穷举攻击法：穷尽密钥搜索攻击
- 数学攻击方法：
  - 差分密码分析：通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特.（针对分组密码）
  - 确定性分析法--线性密码分析：本质上是一种已知明文攻击方法,通过寻找一个给定密码算法的有效的线性近似表达式来破译密码系统
  - 确定性分析法--插值攻击方法：使用一个代数函数来代表一个S-Box，此函数可以用已知明文攻击法取得样本点，再用拉格朗日插值法产生。这个代数函数可能是在有限体上的二次函数、多项式函数或有理函数
  - 统计分析法：利用明文的已知统计规律进行破译的方法。
- 物理攻击方法：
  - 侧信道攻击（能够直接获取密码算法运算过程中的中间值信息；能够分段恢复较长的密钥）
    侧信道攻击主要面向密码实现的物理安全性，采用能量分析攻击、电磁分析攻击、计时攻击、缓存攻击、故障攻击等一系列方法对其实现安全性进行分析

密码学基本数学知识：

- 整数分解：整数分解又称为素因数分解，即任意一个大于1的自然数都可以写成素数乘积的形式
- 模运算：给定一个正整数n，任意一个整数a,一定存在等式： $a = qn + r$, $0 \le r < n, q = [a/n]$
- 有限域：元素个数有限的域，又被称为Galois域
  - 定义了加法和乘法
  - 集合内的元素经过加法和乘法计算，结果仍然在集合内
  - 计算符合交换率、结合率、分配率

    - 加法和乘法有单位元素（所有的集合内的值都有对应的负数，所有集合内非零值都有倒数）
    - 有限域的元素个数一定是某个素数的幂
- 欧几里得算法：求两个整数最大公因子的快速算法gcd(a, b)= gcd(b, a mod b)
- 中国剩余定理：求解一次同余式组
- 实数域上椭圆曲线：满足方程：$y^2 = x^3 + ax + b$的所有点(x, y)的集合。

国内外密码算法概览：

- 序列密码原理：由种子密钥通过密钥流发生器得到的密钥流为：K=k1k2.....kn,则加密变换为：C=c1c2.....cn，其中 ci=mi⊕ki，(i=1,2,.....,n),其中m,k,c是0，1 序列，⊕表示模2加法（异或）
- 流密码：也称为序列密码，它是对称密码算法的一种。
    - 流密码具有实现简单、便于硬件实施、加解密处理速度快、没有或只有有限的错误传播等特点。
    - 流密码强度依赖于密钥流产生器所生成序列的随机性和不可预测性。
- 分组密码：将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为n的组
  （可看成长度为n的矢量）x = (x0, x1,…, xn-1),分别在密钥 k = (k0, k1,… , kt-1) 的控制下变换成等长的输出数字序列y = (y0, y1,…, yn-1)
    - 典型的分组密码：DES（三重DES）、IDEA、RC4、RC5、CAST-128 等
    - 设计要求：分组长度足够大（≥128~256比特）、密钥量要足够大（≥128~192~256比特）、算法足够复杂（包括子密钥产生算法）、加密、解密算法简单，易软、硬件实现等等
- DES算法：
    - DES是一种分组密码,假设明文m是有0和1组成的长度为64比特的符号串,密钥k也是64比特的0,1符号串
    - 64比特密钥k只有56比特有效，其他8倍数的8位是奇偶校验位，在算法中不起作用
- Feistel密码结构：将不够安全的单个循环扩展到多个循环
- 高级加密标准 AES：Rijndael算法、最终标准FIPS PUB197
- 公钥加密体制： 基于单向陷门函数的概念。单向函数是一些易于计算但难于求逆的函数，而单向陷门函数就是在已知一些额外信息的情况下易于求逆的单向函数，这些额外信息就是所谓的陷门。
    - 典型公钥算法：RSA算法三种方式都适合，Diffe-Hellman算法只适合于密钥交换，DSS（数字签名标准）适合于数字签名，EIGamal适合于前两种，椭圆曲线算法（ECC）三种都适合。

第三节 密码学新进展及研究方向

公钥基础设施（Public Key Infrastructure， PKI）是一个用公钥概念与技术来实施和提供安全服务的具有普适性的安全基础设施。

- 数字证书库：是CA颁发证书和撤销证书的存放地
- 认证机构（CA Certificate Authority)
- 注册机构（RA Registration Authority），RA可单独实现，也可合并在CA中实现
- 公钥证书由证书管理机构CA (Certificate Authority)为用户建立，其中的数据项包括与该用户的秘密钥相匹配的公开钥及用户的身份和时间戳等，所有的数据项经CA用自己的秘密钥签字后就形成证书

身份基公钥密码(IdentityBasedCryptograph，IBC)，使用能唯一标识用户身份的信息作为公钥，例如电话号码或Email地址等，简化了传统公钥密码体系中的用户证书管理。

身份基加密：

1. 系统建立算法：PKG生成系统公开参数和主密钥；
2. 密钥提取算法：用户将ID提交给PKG，PKG生成ID对应的私钥；
3. 加密算法：利用用户身份ID加密消息，生成加密密文；
4. 解密算法：利用身份ID对应的私钥解密密文，得到明文消息。

身份基签名：

1. 系统建立算法：PKG生成系统公开参数和主密钥；
2. 密钥提取算法：用户将ID提交给PKG，PKG生成ID对应的私钥；
3. 签名算法：给定用户身份ID的私钥和消息，生成消息的签名；
4. 验证算法：给定用户身份ID、签名和消息，验证签名是否正确

属性基公钥密码：密钥和密文都与一组属性相关联,加密者根据将要加密的消息和接收者的属性构造一个加密策略，当属性满足加密策略时，解密者才能够解密。

> 在属性基加密中，系统的每个权限都可以用一个属性来表示。系统中存在一个属性权威(Attribute Authority，AA)，属性权威对每个用户的属性进行认证，并颁发相应密钥。

属性基签名（Attribute-Based Signature，ABS）是由模糊身份签名发展而来的：

- 根据签名的生成过程分为：密钥策略属性基签名（KP-ABS）、签名策略属性基签名（SP-ABS）
- 当且仅当属性集合满足访问结构时，签名者可以对消息生成合法签名
- 属性基签名特点是匿名性

同态密码可以在不泄露敏感信息的前提下完成对密文的处理

- 安全云计算与委托计算
- 远程文件存储

抗量子密码

- 基于量子物理学的量子密码
- 基于生物学的DNA密码
- 基于数学的抗量子计算密

轻量级密码：为资源受限的设备定制专属的密码解决方案；对吞吐率的要求比普通密码算法低；

第三章 网络安全基础

第一节 网络安全概述

计算机网络是指将地理位置不同，具有独立功能(或自治能力)的多个计算机系统用通信设备和线路连接起来，并以功能完善的网络软件（网络协议、网络操作系统等）进行信息交换,实现资源共享和协同工作的系统。

安全威胁： 指某个人、物、事件或概念对某一资源的保密性、完整性、可用性或合法使用所造成的危险

1. 窃听
2. 信息泄露（密码破解、数据破译等）
3. 病毒感染、木马、蠕虫等恶意代码的攻击
4. 非法使用（如缓冲区溢出攻击）
5. 完整性侵犯(通过篡改、删除和插入等破坏信息）
6. 拒绝服务（DDOS攻击）
7. 假冒 (攻击者利用冒充手段窃取信息、入侵系统、 破坏网络正常通讯或欺骗合法主机和合法用户。)
8. 流量分析 (通过对网上的信息流的观察和分析推断出网上传输的有用信息，例如有无传输、传输的数量、方向和频率等。)
9. 其他威胁(人员疏忽/误操作、电磁泄漏、消息重发、业务否认、截获/修改等。。。。。。。)

安全攻击：一种故意逃避安全服务（特别是从方法和技术上）并且破坏系统安全策略的智能行为；任何可能危及机构信息安全，破坏系统安全属性的行为；攻击就是某个安全威胁的具体实施。

- 被动攻击：对所传输的信息进行窃听和监测
- 主动攻击：恶意篡改数据流或伪造数据流等攻击行为

攻击树：一种以分支模型直观地表示计算机安全威胁的方法（或威胁建模）

> 攻击的目标，如访问机密文件，是攻击树的根。每个分支代表实现该目标的不同方法，这些分支机构可能会从多个方向跳出，有各种不同的选择来实施这些方法

攻击过程：预攻击（踩点和扫描）→ 攻击（入侵、获取权限、提升权限）→ 后攻击（清除日志、安插后门）

安全攻击常见的八种形式：

1. 口令窃取：利用已知或假定的口令尝试登录（口令字典、 暴力破解）/根据窃取的口令文件进行猜测/窃听某次合法终端之间的会话，并记录所使用的口令

   可使用OTP或基于令牌的机制，例如一次性口令方案改进

2. 欺骗攻击：采用欺骗的方式（假冒、伪装等）获取合法信息并加以利用，获得权限
3. 缺陷和后门攻击：缓冲器溢出（堆栈粉碎）攻击或网络蠕虫攻击

   缺陷：指程序中某些代码不能满足特定需求。

   后门：指能绕开正常的安全访问机制而直接访问程序的程序代码。

4. 认证失效攻击：使系统对访问者所采取的身份认证措施无效，易导致服务器被攻击者欺骗
5. 协议缺陷攻击：利用协议本身的缺陷进行攻击，如TCP/IP协议、WEP协议等
6. 信息泄露攻击：利用协议、软硬件等获取信息，进而攻破系统
7. 指数攻击：能够使用程序快速复制并传播攻击
8. 拒绝服务攻击（DOS攻击）：使合法的系统用户不能及时地得到应得的服务或系统资源，即让目标机器停止提供服务或资源访问，如泛洪攻击和Smurf攻击

高隐蔽未知攻击：为了获取某个组织甚至是国家的重要信息有针对性的进行的一系列攻击行为的整个过程。具有极强的隐蔽能力和很强的针对性

软件漏洞：信息安全风险的主要根源之一，是网络攻防对抗中的重要目标

高级长期威胁（APT攻击）：定向信息收集→外网攻击突破→构建控制通道→内部横向渗透→数据收集上传→攻击痕迹清理

社会工程学（Social Engineering）：通过受害者心里弱点、本能反应、好奇心、信任、贪婪等心里陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法

OSI安全体系结构：主要包括三部分内容，即安全服务、安全机制和安全攻击。

- ISO 7498-2对 OSI规定了五个方面的安全服务：认证、数据保密性、数据完整性、访问控制和非否认服务。
    1. 认证服务：提供关于某个实体(人或事物)身份的保证,这意味着当某个实体具有一个特定的身份时,认证服务将提供某种方法来证实这一声明是正确的
    2. 访问控制服务：实施授权的一种方法，防止对资源的未授权使用，包括防止以未授权方式使用某一资源。
    3. 机密性服务：保护信息不泄露或不暴露给那些未授权掌握这一信息的实体。包括数据的机密性服务和业务流机密性服务

       保密粒度：流（stream）、消息（message）、选择字段（field）
    4. 完整性服务：确保数据的价值和存在性没有改变，针对对数据进行修改、增加、删除或重新排序等攻击行为所采用的安全服务。完整性服务能对抗篡改攻击。
    5. 非否认服务：是指用以阻止参与某次通信交换的一方在事后否认曾经发生过本次交换这一事实
- 安全机制：加密、数字签名、访问控制、数据完整性、认证交换、路由控制、公证、流量填充

安全服务与安全机制的关系

服务形式 / 安全服务	加密	数字签名	访问控制	数据完整性	认证交换	防业务流分析	路由控制	公证
认证	是	是			是			
访问控制		是	是					
机密性	是					是	是	
完整性	是	是		是				
非否认		是		是				是

网络安全模型：

- 网络通信：在开放网络环境中保护信息的传输
    1. 对发送的信息进行与安全相关的转换
    2. 由两个主体共享的秘密信息，而对开放网络是保密的
- 访问安全：考虑了黑客攻击、病毒与蠕虫等的非授权访问。
    1. 网闸或看门人功能：组织非授权用户访问
    2. 内部安全控制（监控）：监测有害入侵者的存在
- P2DR-时间模型：可量化的、可由数学证明的、基于时间的的安全模型, 包含安全策略(Policy)、防护(Protection)、检测(Detection)和响应(Response);

第二节 网络安全防护技术

防火墙：由软件和硬件组成的系统，它处于安全的网络和不安全的网络之间，属于边界防护设备，由系统管理员设置访问控制规则，对进出网络边界的数据流进行过滤

- 非军事化区（DMZ）：为了配置管理方便，内网中需要向外提供服务的服务器往往放在一个单独的网段，这个网段便是非军事化区。
- 三种要求：
    1. 所有进出网络数据流都必须经过防火墙
    2. 只允许经授权的数据流通过防火墙
    3. 防火墙自身对入侵免疫，即确保自身安全
- 四种控制机制：
    1. 服务控制:确定了可访问的Internet服务类型,这种控制是双向的
    2. 方向控制:确定特定的服务请求可以发起和通过的方向,即允许通过防火墙进入或离开
    3. 用户控制:控制特定用户对某些服务的访问权限
    4. 行为控制:控制特定服务的应用方式,如控制外部用户只能访问只能访问本地web服务器的部分信息
- 防火墙工作于OSI模型的层次越高，能提供的安全保护等级就越高
- 防火墙分类：
    - 应用级网关防火墙（应用层）：代理对整个数据包进行检查。
    - 电路级网关防火墙（会话层）：不允许端到端TCP直接连接，相反电路级网关充当中介，接收外来请求，转发请求。

      通常作为应用代理服务器的一部分。一旦会话连接有效后网关仅复制、传递数据，而不进行过滤，只在客户和服务器间中转数据。
    - 包过滤防火墙（网络层）：对数据包施加过滤规则，对数据包IP头和传输字段内容进行检查。
- 如何用好防火墙
    - 制定完整的安全策略
    - 考虑防火墙的可扩充性

    - 考虑与其他安全产品的配合使用
    - 经常维护升级防火墙

入侵检测系统：通过可搜索的数据库的方式，发现网络或系统中存在的潜在安全问题和被攻击的迹象。不具有访问控制的能力，也不能独立地防止任何一种攻击。

- 事件提取→入侵分析→入侵响应→远程管理
- 异常检测技术：又称为基于行为的入侵检测技术，用来识别主机和网络中的异常行为。
    - 阈值检测：异常检测技术先定义一组系统正常活动的阈值
    - 用户轮廓(Profile): 通常定义为各种行为参数及其阀值的集合，用于描述正常行为范围。
    - 异常检测系统的效率取决于用户轮廓的完备性和监控的频率。
- 误用检测技术：又称为基于知识（或规则）的检测技术或者模式匹配检测技术，收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵

虚拟专网（VPN）：将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网。通过加密和验证等安全机制建立虚拟的数据传输通道，以保障私有数据信息。

- 分类：
    - 远程访问（Access VPN）,也称为VPDN
    - 网关-网关VPN
- 互联网安全协议（IPSEC）体系
    - 传输模式（主机与主机的直接通信）：保护IP载荷。应用于主机之间端对端通信，该模式要求主机支持IPSec。
    - 隧道模式（关联到多台主机的网络访问连入设备）：保护整个IP包。把一个包封装在另一个新包里面，整个源数据包作为新包的载荷部分。应用于网关模式中，即在主机的网关（防火墙、路由器）上加载IPSec。

功能/模式	认证首部（AH）	封装安全负荷（ESP）	ESP+AH
访问控制	Yes	Yes	Yes
认证	Yes	—	Yes
消息完整性	Yes	—	Yes
重放保护	Yes	Yes	Yes
机密性	—	Yes	Yes

AH、ESP或AH+ESP既可以在隧道模式中使用，又可以在传输模式中使用

- TLS：基于会话的加密和认证的Internet协议，为通信的两个实体提供了一个安全的通道。

计算机病毒防护技术：

- 广义上讲，能够引起计算机故障、破坏计算机数据、影响计算机正常运行的指令或代码，均统称计算机病毒
- 规定：计算机病毒，是指编制或者在计算机程序中插入 的破坏计算机功能或者毁坏数据，影响计算机使用， 并能自我复制的一组计算机指令或者程序代码
- 反病毒技术的三个发展阶段：
    1. 基于简单特征码查杀的单一专杀工具阶段
    2. 基于光谱特征码查杀、主动防御拦截的综合杀毒软件阶段
    3. 基于云、人工智能和大数据技术的互联网查杀阶段

安全漏洞扫描技术：

- 漏洞扫描即针对通用漏洞的检测，需要依据通用漏洞的形成原理和其造成的外部表现来判断。由系统维护人员识别安全风险，依据结果对漏洞实施有针对性的防护或修补
- 漏洞按照被公布时间的不同阶段，可分为
    - 1 Day 漏洞：发现并公布的最新漏洞
    - N Day 漏洞：被公布的历史漏洞
    - 0 Day 漏洞：未被公开的漏洞
- 扫描过程：
    1. 存活判断：为保证扫描效率，启动扫描任务前会首先探测目标系统是否存活
    2. 端口扫描：对已经存活的主机，需要探测主机上开启了哪些端口
    3. 系统和服务识别：采用黑盒测试方法，通过研究其对各种探测的响应形成识别指纹，进而识别目标主机运行的操作系统
    4. 漏洞检测：扫描器根据识别的系统与服务信息调用内置或用户外挂的口令字典进行口令猜测，并同时启动远程非登陆漏洞扫描
- 安全漏洞类别：
    - 配置漏洞：由于软件的默认配置或者不恰当的配置导致的安全漏洞
    - 设计漏洞：指软件、硬件和固件设计方面的安全漏洞
    - 实现漏洞：由于软件、硬件和固件的实现错误导致
- 漏洞扫描的种类：
    - 系统漏洞扫描
    - 特定服务的漏洞扫描：WEB服务/数据库服务/FTP服务/Mail服务
    - 信息泄漏漏洞扫描：用户信息/共享信息
    - 人为管理漏洞扫描：弱口令/错误配置
    - 网络及管理设备漏洞扫描：路由器、交换机/SNMP设备

第三节 网络安全与工程管理及新兴网络安全技术

安全等级划分：

1. 用户自主保护级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络
2. 系统审计保护级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络
3. 安全标记保护级：一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络
4. 结构化保护级：一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络
5. 访问验证保护级：一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络

网络安全管理内容：

- 访问控制：出入控制/存取控制
- 安全检测：安全扫描/入侵检测
- 用户鉴权：主体特征/口令机制/智能卡/数字证书
- 传输安全：传输数据加密/数据完整性鉴别/防抵赖

网络安全事件分为7个基本分类，网络安全事件分为4个级别。

网络安全应急处理过程：准备阶段→检测阶段→抑制阶段→根除阶段→恢复阶段→总结阶段

网络安全挑战

- 工业互联网：含有大量CPS设备，安全防护措施相对滞后
- 移动互联网
- 物联网安全：架构僵化，控制系统中心化单一化；通信兼容性差；多主体协同成本高

第四章 系统安全基础

第一节 系统安全概述及原理

系统安全：系统安全是指在系统生命周期内应用系统安全工程和系统安全管理方法，辨识系统中的隐患，并采取有效的控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。

在网络空间中观察系统的环境：系统在风险的包围之中，必须具有一定的安全性，才能正常运转，系统的安全性需要以系统化的视野去观察

威胁建模：

- 威胁：给某物造成伤害或损失的意图
- 风险：某物遭受伤害或损失的可能性
- 安全：某物能避免或抵御他物带来的潜在伤害或损失
- 基本类型：以风险/资产/攻击者/软件为中心

访问控制分类:

- 基于身份/角色/标签的访问控制
- 自主/强制访问控制

入侵监测分类：

- 基于监测的对象：主机/网络入侵检测
- 基于监测方法：基于特征/异常的入侵检测

第二节 系统安全结构

硬件系统安全：

- 处理器硬件从可用指令集和可用内存区域两个方面出发，定义了处理器工作的两种状态：内核态和用户态，用户态程序不能干扰内核态的程序
    - 内核态：操作系统用，看到所有的指令和地址空间
    - 用户态：其他程序用，看到其中部分的指令和地址空间
- 硬件防篡改方法：
    - 提供密码计算功能
    - 提供数字指纹
- 硬件系统面临的威胁：硬件木马

操作系统安全：

- 安全功能：
    - 用户管理与身份认证：注册用户档案；用户登录过程
    - 自主访问控制：文件的拥有者可以自主确定任何用户对该文件的访问权限；访问权限既可以授给用户，也可以授给用户组
    - 强制访问控制：信息按照保密程度划分了多个级别，用户按照职务层次划分了多个等级。访问许可的判断依据是信息的级别和用户的等级，不是用户的意愿
    - 日志功能：记录系统中发生的重要活动的详细信息

数据库系统安全：

- 主要威胁：
    - 非法访问数据库信息
    - 恶意破坏数据库或未经授非法修改数据库
    - 用户网络访问数据库时受到各种攻击，如搭线窃听等
- 攻击手段：
    - 数据推理（Inference）：根据合法的非敏感数据推导出非法的敏感数据
    - SQL注入攻击：SQL命令插入到Web表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的SQL命令

应用系统安全：

- 跨站脚本（XSS）攻击：在网站上注入恶意的客户端代码。若受害者运行这些恶意代码，攻击者就可以突破网站的访问限制并冒充受害者。

- Cookie：浏览网站时由网络服务器创建并由网页浏览器存放在用户计算机或其他设备的小文本文件，包括用户的IP地址、用户密码个人资料等重要信息。

第五章 内容安全基础

第一节 内容安全概述

信息内容安全(Content-basedInformation Security)是研究利用计算机从包含海量信息并且迅速变化的网络中对特定安全主题相关信息进行自动获取、识别和分析的技术。

安全威胁：

- 泄露（指对信息的非授权访问）、欺骗、破坏和篡夺
- 恶意用户产生并传播的恶意内容

以内容为中心的未来互联网：旨在将内容名称而不是IP地址作为传输内容的标识符，从而实现信息的路由。

网络信息内容获取：

- 网络爬虫
  - 服务于搜索引擎等搜索类应用的网络爬虫
  - 针对性进行信息收集的网络爬虫
- 信息内容的特征抽取与选择：
  - 文本信息：采用向量空间模型来描述文本向量。通过特征选择来降维，找到代表性特征
  - 音频信息：基于帧或片段进行特征分类
  - 图像信息：颜色特征；纹理特征；边缘特征；轮廓特征

信息过滤：对陆续到达的信息进行过滤，是满足用户信息需求的信息选择过程。

第二节 网络舆情内容监测

网络舆情内容监测功能分解：

- 高仿真网络信息深度提取
- 基于语义的海量文本特征快速提取与分类
- 非结构信息自组织聚合表达

内容中心网络：

- 信息流：具备快速高效的数据传输能力和增强的可靠性
- 架构：摒弃以IP地址为中心的传输架构，采用以内容名称为中心的传输架构
  - 内容信息对象：存储在计算机中并通过计算机访问的所有类型的对象
  - 命名：信息对象的标识，具有全局性和唯一性。其地位与TCP/IP架构的IP地址类似
  - 路由

    - 缓存：每个CCN节点维护缓存表，用于缓存CCN路由器接收的内容消息对象，以便响应后继接收到的相同请求。
    - 应用程序编程接口：根据请求和交付内容信息对象定义，用于内容信息对象的发布和获取操作。
- 攻击分类：
    - 命名相关攻击：监视列表攻击、嗅探攻击
    - 缓存相关攻击：驱逐流行内容攻击
    - 路由相关攻击：DDOS攻击、欺骗攻击
    - 其他攻击：假冒攻击、重放攻击

第六章 应用安全基础

第一节 应用安全概述及身份认证与信任管理

应用安全是指为保障各种应用系统在信息的获取，存储，传输和处理各个环节的安全所涉及的相关技术的总称

- 云计算：数据所有权和管理权的分离
- 工业互联网：数据汇集到云端，要保证系统的可靠运行，需要保证数据的机密性、完整性、访问和流转的可控性以及系统软硬件的安全性
- 大数据：大数据是一种规模大到在获取、存储、管理、分析方面大大超出了传统数据库软件工具能力范围的数据集合
- 人工智能：网络安全防护、密码设计与分析领域
- 区块链：信息共享、版权保护、物流、供应链金融、跨境支付、数字资产、数字货币。本身安全问题、隐私保护问题亟待解决

身份认证：证实客户的真实身份与其所声称的身份是否相符的过程：

- 用户名/口令认证（所知）
- 动态口令/一次性口令OTP（所有）
- 挑战 — 答应认证（所有）
- 基于生物特征的认证（个人特征）
- 图灵测试
- 多因子认证

公钥基础设施PKI：是一种遵循标准的利用公钥理论和技术建立的提供安全服务的基础设施。

身份认证的主流标准：

- 远程认证拨入业务协议RADIUS：用于接入认证和计费服务
- 在线快速身份认证FIDO（Fast Identity Online）：完全通过本地身份认证实现无口令的登录

- 联盟身份管理FIM（Federated Identity Management）：使用户使用同一个身份在组成联盟的所有企业中访问相应的资源，如Oauth认证服务

访问控制：限制访问主体（用户、进程、服务等）对访问客体（文件、系统等）的访问权限，从而使计算机系统在合法范围内使用。控制模型有

- 自主访问控制模型DAC：资源拥有者按照自己的意愿来决定是否将自己所拥有资源的访问权限授予其他用户，策略灵活但安全性较差
- 强制访问控制模型MAC：为用户和数据划分安全等级，实现了信息的单向流动，但权限管理效率偏低、缺少灵活性
- 基于角色的访问控制模型RBAC：通过角色对访问控制策略进行描述，系统中的用户和权限均对应于某些特定的角色。角色的引入实现了用户与权限之间的分离，简化了授权管理

零信任模型：网络边界内外的任何实体,在未验证之前都不予以信任。即“持续验证，永不信任”

第二节 隐私保护与新兴应用及其安全

隐私保护：在发布或者共享数据中不能识别出具体个人的数据

- K-匿名性：对同一个准标识符至少要有k条记录，使得一组公开的数据中，任何一个人的信息都不能和其他至少k-1人区分开

  无法防范同质化攻击和背景攻击

- L-多样性：在 K-匿名性的基础上对每个等价类都保证敏感属性至少有个L个取值，使得攻击者最多以$\frac{1}{L}$的概率确认某个体的敏感信息

  难以防范偏斜攻击和相似度攻击

- T-相近性：要求每个 K-匿名性中敏感属性值的统计分布与该属性在整个数据集中的总体分布 “接近”。
- 差分隐私：实现仅分享可以描述数据库的一些统计特征、而不公开具体到个人的信息。

移动应用安全风险

云计算及其安全：

- 虚拟化技术：裸金属架构/寄居架构/容器
- 攻击模式：
  - 虚拟机逃逸：利用虚拟机管理软件或者虚拟机中运行软件的漏洞，控制虚拟机管理系统或者在宿主机上运行恶意软件，进而获得其他虚拟机的完全控制权限
  - 边信道攻击：攻击者控制的虚拟机与目标虚拟机使用相同的物理层硬件，二者交替执行。

区块链及其安全：用哈希串联信息，实现完整性，防止篡改，公开验证。

- 比特币与区块链：
  - 比特币网络中，数据以文件的形式被永久记录，称这些记录为区块
  - 新区块一旦被记录在区块链上，就不能被改变或者删除
  - 时间戳记录特定的数据生成时间
  - 默克尔树用来存储当前区块的所有交易信息
  - 难度系数用于控制区块的生成速度，比特币每10分钟产生一个区块
- 共识机制：网络中各个参与节点需要确认交易的机制，使得在网络中存在故障或不可信节点的情况下，区块链网络中的交易能按照预期的正确方式执行，确保各个节点最终结果的一致性。
- 智能合约：运行在链上并可针对区块链数据库进行读写操作的代码，可以自动执行参与方指定的数字契约
- 区块链主要类型：
  - 公有链：自由加入和退出
  - 联盟链：通过授权加入和退出
  - 私有链：私有机构单中心网络
- 安全风险：
  - 51%算力攻击：当攻击者掌握了超过全网50%的算力，就很容易阻止其他节点确认交易，也可以逆转当前区块已经完成的交易，并在网络中双花电子货币。
  - 攻击交易所：加密货币交易所拥有大量的加密货币，对交易所的攻击可能导致数字货币被窃。
  - 软件漏洞：需要完备的代码审计、渗透测试和智能合约监控
  - 隐私泄露：公有链数据可以公开获取，通过大数据关联分析，可能对特定用户去标识化，从而泄露用户隐私信息

人工智能及其安全：

- 主要技术领域：
  - 自然语言处理：通过计算机对自然语言的分析，对词法、句法、语法和语义进行理解分析，实现人机信息交流
  - 计算机视觉：让计算机具备理解图像表示内容、图像中物体存在的关系等能力。如文字识别、图像处理、图像识别

    - 深度学习：通过建立模拟人脑分析学习的神经网络对数据进行解释。
    - 数据挖掘：从数据中提取出具有潜在价值的信息和知识。
- 安全问题：
    - 对抗样本：对待预测样本添加特定很小的扰动或者进行细微的修改，使模型对于该样本判断出错
    - 模型萃取：通过构造请求向目标服务发起查询，取得目标模型参数或者构造出与目标模型功能相似可替代的模型
    - 训练数据窃取：攻击模型训练集，获得训练数据集的具体样本及统计分布，或者判断某条数据是否在该训练数据集中
    - 投毒攻击：在模型训练过程中修改训练数据集或者投放精心构造的恶意样例，来使训练数据中毒或者被污染，从而干扰机器学习模型的训练过程，降低最终得到模型的判断准确性
- 人工智能与网络空间安全的影响：
    - 复杂性挑战：复杂的技术构成和应用场景势必会产生新的安全漏洞
    - 网络犯罪：伪造语音、图片、视频，生成虚假内容，识别验证码
    - 隐私保护侵犯：收集、识别个人隐私，精准画像
    - 不确定性风险：人工智能不可控，产生意外损害
    - 智能网络攻防：自动化的网络攻防
    - 人工智能伦理：人工智能与人类的关系，是否会取代人类