第一次作业

1.请列举几个平时在使用计算机和网络访问时遇到的信息安全问题？以及当时的解决方案？

1.用户密码方面安全性较弱：采取定期更换强密码，不同用户间密码不重复等方式

2.恶意程序：安装部分程序时通过网络分享下载，程序安全性无法得到保证，采用下载到虚拟机或由杀毒软件查杀等方式

3.个人隐私泄露：采取网络上少使用个人信息，避免使用重复手机号和邮箱等问题，减少信息泄露风险。

2.当前我国面临的网络信息安全的现状是怎样的？

1.我国网络建设日益完备，但信息安全等方面的制度尚不完善，抵抗渗透和非法入侵的能力较差

2.存在敌对势力和黑客组织的蓄意攻击，对我国网络信息安全造成极大威胁

3.公民信息遭到严重泄露，个人对自我信息的保护能力严重不足。

第二次作业

1. 什么是网络空间？为什么网络空间存在严峻的信息安全问题？

答： 网络空间是是信息时代人类赖以生存的信息环境，是所有信息系统的集合。所以网络空间是一种复杂巨系统，因此网络空间存在严峻的信息安全问题。

2. 网络空间安全学科的主要研究方向及内容是什么？

答：

密码学研究领域涵盖密码编码学和密码分析学，关注点包括对称密码、公钥密码、Hash 函数、密码协议等，还包括新兴领域如生物密码、量子密码和混沌密码。此外，密码学也关注密码的管理与应用。

网络安全致力于在各网络层次和范围内采取保护措施，以便检测和应对各种网络安全威胁。主要研究领域包括网络安全威胁、通信安全、协议安全、网络防护、入侵检测、态势感知、紧急响应、灾难恢复、可信网络和网络安全管理。

系统安全包括系统安全威胁与等级保护、系统设备安全、硬件子系统安全、软件子系统安全、访问控制、可信计算、系统安全测评认证以及应用系统安全。

信息内容安全包括内容的安全威胁、内容获取、内容分析与识别、内容管理、信息隐藏、隐私保护，以及与内容安全相关的法律保障。

信息对抗领域主要研究通信对抗、雷达对抗、光电对抗以及计算机网络对抗等方面的问题。

3. 信息安全的三大定律是什么？

答：就低性定律：在信息安全中，个体或实体应该被授予最低限度的权限，以便执行其工作或任务。这有助于减少潜在的风险，因为不需要的权限可能被滥用或导致安全漏洞。

中性定律：在设计安全系统时应该尽量减少共享的机制或组件。

普遍性定律：安全系统的设计和实施应该是公开的，而安全性不应该依赖于系统的保密性。

4. 简述信息安全分级保护和信息安全等级保护

信息安全分级保护： 信息安全分级保护是一种将信息根据其重要性和敏感程度划分为不同等级，并为每个等级制定相应的安全保护措施和管理规定的方法。常见的等级划分包括机密、秘密、内部和公开等级。对于不同等级的信息，需要采取相应的安全措施，如访问控制、数据加密和安全审计，以确保信息的保密性、完整性和可用性。

信息安全等级保护： 信息安全等级保护是一种根据信息系统的重要性和安全风险水平将信息系统划分为不同等级，并为每个等级确定相应的安全控制措施和管理要求的方法。通常将信息系统分为一级、二级、三级等级，每个等级需要满足特定的安全标准和技术要求，包括系统访问控制、安全审计、漏洞管理和应急响应，以防止信息系统受到攻击、数据泄露和服务中断。

5. 我国商用密码标准体系如何来刻画？举例说明我国商用密码标准都有哪些？

我国的商用密码标准体系是由国家密码管理局负责制定和管理的，旨在确保商用信息系统和数据的安全。这一体系涵盖了商用密码产品和系统的技术规范、测试评估方式以及安全保护措施等方面

2011 年，我国自主研制的 ZUC（祖冲之）密码算法被 3GPP 组织采纳为新一代宽带无线移动通信系统（LTE）国际标准
2012 年 3 月成为国家密码行业标准（GM/T 0001-2012)
2016 年成为国家标准（GB/T 33133--2016)
2017 年，SM2、SM9 数字签名算法正式成为 ISO 国际标准

6. **网络空间安全学科的方法论是什么？在运用这一方法论分析和解决问题时，应当注意什么？**

答：以解决网络空间安全问题为目标、以适应网络空间安全需求为特征的具体科学方法论。运用时强调底层性和系统性、实行综合治理，追求整体效能、坚持”以人为核心“的原则，人是最积极的因素也是一个薄弱环节、定性分析与定量分析相结合

第三次作业

1. 《中华人民共和国网络安全法》哪一年开始实施？它的实施具有什么意义？

《中华人民共和国网络安全法》于 2017 年 6 月 1 日开始实施，
《中华人民共和国网络安全法》的实施标志着我国在网络空间安全管理方面迈出了重要的法治步伐。是我国首部全面规范网络空间安全管理的法律，为网络空间法治建设奠定了基础，使互联网在法治轨道上运行，强调了依法治网的原则，为网络空间的健康运行提供了法律保障，确保了网络环境的稳定和有序。系统化了网络安全管理的做法，将一些已经成熟的制度化，为未来可能的制度创新提供了原则性指导，以不断适应快速发展的网络领域的需求。这部法律是我国网络安全领域的法律支柱，有助于规范互联网行为，维护国家网络安全，促进网络空间的持续健康发展。

2. 根据《中华人民共和国保守国家秘密法》，国家秘密具有哪些特征？
国家事务重大决策中的秘密事项、国家建设和武装力量活动中的秘密事项、外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项、国民经济和社会发展中的秘密事项、科学技术中的秘密事项、维护国家安全活动和追查刑事犯罪中的秘密事项、经国家保密行政管理部门确定的其他秘密事项。

3. 根据《中华人民共和国保守国家秘密法》，请简述有哪些违反规定的行为？
泄露国家秘密：未经授权，擅自泄露国家秘密给未经授权的人员或组织，或者向外国、境外机构或个人泄露国家秘密。
窃取、刺探、收买、非法获取国家秘密：通过非法手段获取、窃取、刺探或收买国家秘密。
侵占、损毁、篡改、丢失国家秘密：未经授权，擅自侵占、损毁、篡改或丢失国家秘密，或者故意不报告、隐瞒国家秘密的丢失。
违反保密规定传递国家秘密：未经授权，违反有关保密规定，传递国家秘密给未经授权的人员或组织。
利用国家秘密从事非法活动：利用掌握的国家秘密从事犯罪活动、危害国家安全、损害国家利益或者侵害公民、法人和其他组织的合法权益。
违反法律规定保护国家秘密：未按照法律规定采取必要的措施，保护国家秘密，造成国家秘密泄露或者丢失的。

4. 根据《中华人民共和国密码法》，我国的密码分为哪几类？
核心密码、普通密码、商用密码

5. 根据《中华人民共和国数据安全法》，国家建立数据分类分级保护制度，分类分级的主要依据是什么？
数据关联的国家安全、经济安全和社会公共利益：数据涉及国家安全、经济安全和社会公共利益的程度，包括但不限于国家秘密信息、关键基础设施数据、重要行业数据等。
数据的经济价值和社会影响：数据的价值和影响力，包括但不限于商业秘密、个人财产信息、公共服务数据等。
数据的个人隐私和个人权益：数据涉及个人隐私和个人权益的程度，包括但不限于个人身份信息、健康信息、通信记录等。

第四次作业

1. **古典密码分哪些种类？哪些古典密码采用了移位代换？哪些古典密码采用了置换变换？**

古典密码主要有两种加密方式：置换和替换
替换的有：凯撒密码、维吉尼亚密码、普莱费尔密码、Hill 密码
置换的有：栅格换位、矩形换位、费纳姆密码

2. **为什么说一次一密在理论上安全的？一次一密在实际应用中存在什么问题？**

因为密钥本身随机，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。
但这需要建立庞大的随机字母集，工作量巨大，而且存在密钥分发的问题。

3. **简述一个保密通信系统的数学模型由哪几部分组成？**

1.信源：发送明文
2.加密器：接收来自信源的明文，利用密钥进行加密并发送密文
3.信道：密文传输的途径
4.解密器：利用密钥解密密文，并把解密出的明文发送给信宿
5.信宿：接收来自解密器的明文并保存
6.攻击者：拦截获取明文或密钥

4. **随着新技术的发展，密码学面临哪些新的安全挑战？**

1.云计算/存储对密码学的新挑战：用密码感知数据存在；确保数据的安全性；确保用户的隐私；

2.大数据对密码学的新挑战：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）
3.物联网对密码学的新需求：密码要适应数据多样性、网络多样性、多层次、适应各层次的资源差异较大，需要多密码、多密钥、多安全级别、跨域互联互通。
4.新型计算机对密码学的新挑战：量子计算机和 DNA 计算机的发展，强大的计算能力可以攻破现有的许多密码算法
5.区块链核心技术的突破还需要依赖密码技术底层算法、协议的突破，区块链核心技术的攻关将长期伴随着密码技术的突破。

5. **信息隐藏和信息保密有何本质区别？**

信息隐藏：隐匿信息的存在。
信息保密：隐匿信息的真意。

第五次作业

1. **密码体制从原理上可分为哪两大类？这两类密码体制在密钥的使用上有何不同？**

可分为单钥加密体制，双钥加密体制

单钥加密体制：加密密钥和解密密钥相同，是对称加密体制

双钥加密体制：在加密和解密的过程中分别使用不同的密钥，是非对称加密体制

2. **密码攻击有哪些类型？有哪些方法？**

唯密文攻击：破译者具有密文串 y 和加密算法

已知明文攻击：破译者具有明文串 x 和相应的密文串 y 和加密算法

自适应选择明文攻击：破译者具备选择明文串 x 并构造出相应的密文串 y，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 y、加密算法、可选择密文串 y，并构造出相应的明文

方法：

穷举攻击法（强力攻击法）

数学攻击法（差分密码分析、确定性分析法--线性密码分析、确定性分析法--插值攻击方法、统计分析法）

物理攻击法（侧信道攻击）

3. **公钥密码系统的三种应用是什么？公钥密码系统对应的数学难题有哪些？**

应用：密钥的分配和管理、数字签名和身份认证、数据加解密

数学难题：模合数平方根困难问题，大数因子分解难解性，计算离散对数难解性，基于有限域上计算离散对数的困难性，椭圆曲线离散对数难解性。

4. **什么是身份基密码、属性基密码和同态密码？**

身份基密码：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。

属性基密码：由模糊身份签名发展而来，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。

同态密码：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，成为保护数据安全，提高密文处理分析能力的关键技术。

第六次作业

1. **什么是 OSI 安全体系结构？列出并简要定义安全服务和安全机制的分类，并简述安全服务与安全机制之间的关系。**

OSI 安全体系结构是一种网络安全框架，它主要包括三部分内容，即安全服务、安全机制和安全攻击。规定了五方面的安全服务：认证、数据保密性、数据完整性、访问控制和非否认服务。

安全服务是一种用来增强数据处理系统安全性和信息传递安全性的措施或服务。目的在于使用 1 种或多种安全机制来阻止攻击。其包括：
认证服务：提供关于某个实体(人或事物)身份的保证
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
数据机密性服务：机密性是指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
数据完整性服务：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
非否认服务(不可抵赖性)：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

安全机制包括：
加密：将明文数据通过一定的加密算法转换成密文数据，以保障数据的机密性。
数字签名：使用私钥签名，公钥进行证实用户身份
访问控制：限制用户访问计算机系统和网络资源的机制。
数据完整性：保障数据在传输和存储过程中不被算改、损坏或丢失的机制。
认证交换：实现对等实体的认证鉴别。
路由控制：防止不利的信息通过路由。
公证：由第三方参与数字签名，它基于通信双方对第三方都绝对相信。
流量填充：填充冗余的业务流量来防止攻击者对流量进行分析。

安全服务与安全机制有着密切的关系。安全服务体现了安全系统的功能；而安全机制则是安全服务的实现。
一个安全服务可以由多个安全机制实现；而一个安全机制也可以用于实现多个安全服务中。

2. 基本的安全威胁有哪些？

窃听、信息泄露、病毒感染、木马、蠕虫等恶意代码的攻击、非法使用、完整性侵犯、拒绝服务、假冒、流量分析、其他

3. 列出并简要定义被动攻击和主动攻击的分类，并简述被动攻击和主动攻击之间有何区别？

被动攻击：对所传输的信息进行窃听和监测。其包括：
消息内容泄露：传输的信息遭到窃听和截取
通信量分析：业务流量被攻击者获取分析

主动攻击：恶意篡改数据流或伪造数据流等攻击行为。其包括：
伪装：攻击者冒充合法用户或系统以诱骗其他用户或系统提供敏感信息或授予对受限区域的访问权限。
重放：捕获传输的信息并进行反复修改与发送
更改消息内容：截获传输的信息并对信息进行一定的更改
拒绝服务：通过流量或请求使系统或网络无法访问其目标用户

4. 网络攻击的常见形式有哪些？什么是缓冲区溢出攻击？

常见形式：口令窃取、欺骗攻击、缺陷和后门攻击、认证失效、协议缺陷、信息泄露、指数攻击、拒绝服务攻击。

缓冲区溢出攻击：通过造成缓冲区溢出并用指定地址覆盖返回地址而进入指定程序的方式来获得系统权限。

5. 什么是 P2DR 模型？

P2DR 模型是可量化的、可由数学证明的、基于时间的的安全模型，包含安全策略、防护、检测和响应

安全策略是 P2DR 安全模型的核心,所有的防护、检测、响应都是依据策略实施的;
防护主要是预防安全事件的发生,发现存在的系统脆弱性和防止意外威胁和恶意威胁;
检测是 P2DR 中一个非常重要的环节,是静态防护转化为动态防护的关键,动态响应和加强防护的依据,同时也强制落实安全策略的工具;
响应在安全系统中占有重要的地位,是解决安全潜在威胁最有效的方法。

第七次作业

1. 防火墙的类型有哪些？各类防火墙的特点？

类型：包过滤防火墙，电路级网关防火墙，应用级网关防火墙
特点：
包过滤防火墙：对外出数据包进行身份记录，便于下次让具有相同连接的数据包通过。对已建连接和规则表
进行动态维护。能够感觉到新建连接与已建连接之间的差别。
电路级网关防火墙：电路级网关不允许端到端 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。监视两主机建立连接时的握手信息。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。
应用级网关防火墙：针对每个服务运行一个代理。对数据包进行逐个检查和过滤。在更高层上过滤信息自动创建必要的包过滤规则。

2. 防火墙有哪些控制功能？防火墙的局限性有哪些？什么是 DMZ？

控制功能：服务控制，方向控制，用户控制，行为控制。
局限性：防火墙作为一种保护网络安全的设备，必须部署在受保护网络的边界处。使用防火墙需要考虑今后网络的扩展性，以防其不能适应新的应用环境。
防火墙软件作为一种安全工具，必须不断地升级与更新才能
应付不断发展的入侵手段。
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。

3. 什么是入侵监测系统？入侵检测方法有哪些？

入侵检测系统的诞生就是为了让计算机能够更安全稳定的运行，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，它对系统中未经授权的用户进行攻击，对外部攻击和运行的异常都有实时的保护，它可以在网络系统被入侵之前就发现和拦截。
方法：统计异常检测方法，特征选择检测方法，基于贝叶斯推理异常检测方法，基于贝叶斯网络异常检测方法，基于模式预测异常检测方法。

4. IPsec 提供哪些服务？IPsecVPN 有哪两种工作模式，这两种工作模式有何区别？

提供的服务：对网络单元的访问控制，数据源认证，提供用于无连接服务的协议（协议）的无连接完整性，重放数据报的监测和拒绝，使用加密来提供保密性和有限的数据流保密性。
工作模式：传输模式，隧道模式。
区别：
采用传输模式时，IPSec 只对 IP 数据包的净荷进行加密或认证；封装数据包继续使用原 IP 头部，只对部分域进行修改；IPSec 协议头部插入到原 IP 头部和传送层头部之间。
采用隧道模式时，IPSec 对整个 IP 数据包进行加密或认证；产生一个新的 IP 头，IPSec 头被放在新 IP 头和原 IP 数据包之间，组成一新 IP 头。

5. 我国的网络安全划分为哪几个安全等级？每个安全等级划分的依据是什么？

用户自主保护级，系统审计保护级，安全标记保护级，结构化保护级，访问验证保护级共五级。
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。
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。
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。
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。
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。

6. 针对工业互联网的攻击发起点有哪些？有哪些具体威胁？

工业互联网安全挑战：工业互联网含有大量 CPS 设备，安全防护措施相对滞后，改进后蠕虫、病毒和木马等传统攻击方式会严重威胁工业互联网安全，而且由于工业互联网集成多类不同系统，所以存在多种攻击发起点，攻击者可以从物理层、网络层和控制层分别发起攻击。例如 Stuxnet 蠕虫利用“零日漏洞”导致伊朗核设施中的离心机故障。因此，工业互联网遭受攻击会严重影响国家安全。
具体威胁示例：美国佛罗里达州供水系统遭黑客攻击，宏碁电脑遭巨额勒索攻击，美国最大油气管道商被攻击，全球最大肉类供应商遭受勒索攻击。工控设备高危漏洞，外国设备后门，高级持续性威胁(APT)，工业网络病毒，无线技术应用的风险。

7. 物联网感知识别层面临哪些安全挑战？

物理俘获、网络窃听、Dos 攻击、节点欺骗、越权访问、假冒攻击、信息窃取

8. 我国网络安全事件分为哪几类以及分为哪几个级别？

国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》将网络安全事件分为 7 个基本分类：有害程序事件、 网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾难性事件、其他网络安全事件
《国家网络安全事件应急预案》将网络安全事件分为 4 个级别：特别重大事件（I 级）、重大事件（II 级）、较大事件（III 级）、一般事件（IV 级）

9. 计算机病毒的主要特点有哪些？计算机病毒主流检测技术有哪些？

特点：
传染性：传染性是病毒的基本特征。计算机病毒同自然界的生物病毒一样具有传染性，会通过各种渠道扩散到更多的计算机系统上，是否具有传染性是判别一个程序是否为计算机病毒的最重要条件
隐蔽性：计算机病毒通常会采用隐藏进程、文件等手段延长自己的生命周期。
寄生性：病毒通常都是附着在其它正常程序之中，类似生物界的寄生现象，当调用程序时窃取到系统的控制权，先于正常程序执行。现在这个特性正在变化
潜伏性：大部分的病毒感染系统之后不会马上发作，可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块
破坏性：任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，如降低计算机工作效率，占用系统资源，导致系统崩溃，此特性可将病毒分为良性病毒与恶性病毒
检测技术：
基于特征码的传统检测技术：采样为固定位置、采用精准匹配方式技术简单、易于实现、查杀精准速度慢、无法查杀未知病毒
基于行为的传统检测技术：针对病毒动态行为进行检测针对隐蔽性强的病毒有更好检测能力，具备查杀未知病毒能力
基于云技术的云查杀技术：将“匹配”和“基准”放在云端进行反应速度快终端资源使用大大减小基于大数据与人工智能的查杀技术：将“匹配”和“基准”放在云端进行可以根据模型匹配已知与未知病毒

10. 按照漏洞扫描的技术执行形式的维度划分，漏洞扫描技术分为哪些？什么是原理检测和版本检测？

漏洞扫描技术分为：扫描目标是已规模化发布的系统、应用软件或者设备；扫描目标是各种应用，以 Web 应用居多；
原理检测：对目标机的相关端口发送请求构造的特殊数据包，进而根据返回的结果信息，判断漏洞是否存在。
版本检测：系统扫描是依照漏洞库标准实施的，在标准的漏洞说明中，会详细说明该漏洞所在系统的身份信息，例如 CPE 标识的系统类型和详细版本号。此外按照惯例，系统的升级一般会更改版本号，因此在漏洞与系统版本之间就存在了关联关系。

第八次作业

1. 操作系统通常由进程管理、内存管理、外设管理、文件管理、处理器管理等子系统组成，是不是把这些子系统的安全机制实现好了，操作系统的安全目标就实现了？为什么？

不是。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。如果各个子系统无法相互配合自洽，那么在子系统间容易产生安全风险

2. 涌现性和综合特性都是整体特性，请分析说明两者的区别？

综合特性：可以分解为系统组成部分的特性
涌现性：不可还原（即不可分解）为系统组成部分的特性

3. 请对安全管理和风险的概念进行分析，以此为基础，说明在安全管理工程中为什么要遵循风险管理原则？

安全管理（Security Management）：把一个组织的资产标识出来，并制定、说明和实施保护这些资产的策略和流程。
风险（Risk）某物遭受伤害或损失的可能性。
风险管理原则可以标识威胁、评估现有威胁控制措施的有效性、确定风险的后果、基于可能性和影响的评级排定风险优先级、划分风险类型并选择合适的风险策略或风险响应，从而最大程度的避免威胁发生，减少损失。

4. 请说明针对数据库应用的 SQL 注入攻击的原理？

SQL 注入攻击就是攻击者把 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

5. 什么是跨站脚本攻击（XSS）？请分析说明跨站脚本攻击（XSS）威胁会给 Web 应用系统带来什么样的安全风险？

XSS 攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。
用户在观看网页时就会受到影响，攻击者可能得到更高的权限（如执行一些操作）、私密网页内容、会话和 cookie 等各种内容。

6. 请简要说明访问网站时涉及的 cookie 是什么东西，它是如何泄露个人敏感信息的？

cookie 是浏览器与服务器交互时，由服务器建立，由浏览器保存的一些赋值信息。
cookie 会帮把在该网站上所输入的文字信息或是一些选择和操作都纪录下来，并将信息保存在用户的硬盘上，这些信息将保存在用户的浏览器中，当下一次用户连接到这个服务器时，浏览器就可以将合适的状态发送给服务器使用。在这一过程中，如果 cookie 被窃取，就可能泄露用户的信息。

第九次作业

1. **信息内容安全的主要技术有哪些？**

1.内容获取：从网络中提取和获取相关内容
2.内容分析：对获取的信息内容进行分析处理，以提取有价值的信息和知识
3.内容网络：以内容为中心构建新型网络架构，通过内容命名等技术实现可靠安全的内容传输与共享

2. **信息内容安全威胁主要有哪些？**

一方面：内容安全所面临威胁有泄露（指对信息的非授权访问）、欺骗、破坏和篡夺等。

另一方面：一些恶意用户产生并传播的恶意内容也是网络空间面临的潜在安全威胁。

3. **典型的信息内容的获取技术有哪些？并简要说明其原理。**

1.基于自然语言理解的和文本挖掘的事件及元素抽取：利用自然语言处理的方式从文本中识别出事件的要素，事件间的联系从而构建出事件知识库。
2.基于知识图谱的文本信息与行为特征表示学习：利用知识图谱将文本信息和用户行为映射到实体、关系等概念上，从而提高信息的可理解性与可操作性。
3.基于图神经网络推理信念网络的社交网络用户认知模型构建技术：利用图神经网络，对社交网络中的用户进行建模，分析其偏好与用户间的影响与传播机制，从而预测用户行为与反应。
4.基于自然语言理解和深度学习模型的语义文本信息生成技术：利用自然语言理解分析文本信息与逻辑，借助深度学习模型生成符合语法语义和目标的文本信息。

4. **信息过滤技术有哪些分类与应用？**

1.基于内容的过滤：根据信息内容的特征与用户的兴趣或需求进行匹配，从而过滤出相关的信息。应用有新闻推送等。
2.基于用户兴趣的过滤：根据用户的行为与反馈，建立用户的偏好模型，从而过滤出符合用户兴趣的信息。应用有视频推送、音乐推荐等。
3.协作过滤：根据用户之间的相似度或关联度，利用其他用户的兴趣或评价，从而过滤出可能感兴趣的信息。应用有论坛推送、博客关联、电商推荐等。
4.主动过滤：用户主动设置过滤条件或规则，对信息流进行筛选或屏蔽，从而过滤出自己想要的或排除掉不想要的信息。应用有广告过滤，标签设置等。

5. **什么是内容中心网络？内容中心网络的架构有哪些基本组成？**

内容中心网络摒弃以 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。实现了以内容为中心的订阅机制和语义主导的命名、路由和缓存策略。
内容中心网络的架构的基本组成有：
1.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
2.命名：内容的命名是信息对象的标识，具有全局性和唯一性。其地位与

TCP/IP 架构的 IP 地址类似
3.路由：根据内容名字将兴趣包和数据包转发到合适的节点
4.缓存：在网络中的任意节点存储和提供内容，以便响应后继接收到的相同请求
5.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

6. **针对内容中心网络架构的常见攻击有哪些？简要说明每种攻击方式？**

1.命名相关攻击：如监视列表攻击和嗅探攻击。利用命名机制获取或篡改内容的名称或元数据，从而破坏内容的保密性与真实性
2.路由相关攻击：如 DDOS 攻击和欺骗攻击。利用路由机制，大量发送无效包或发送伪造的数据包，耗尽网络资源和缓存空间，污染路由表，从而影响内容的正常转发
3.缓存相关攻击：如驱逐流行内容攻击。利用缓存机制，影响内容的缓存和分发，从而破坏内容的完整性
4.洪流攻击：类似于 DDoS 攻击，通过发送大量的请求、答复、确认数据包，从而占据网络流量，影响内容中心网络处理正常信息，使网络拥塞，功能瘫痪。
5.其他攻击：如假冒攻击和重放攻击。通过伪造或重放内容的签名或时间戳，使得用户获取错误信息和过时内容，从而危害用户的隐私与安全。

第十次作业

1. **身份认证的主要方法有哪些？并对每个方法原理进行简单描述。**
    1. 用户名/口令认证（所知）：简单易用，不需要任何硬件设备，利用口令登录即可
    2. 动态口令/一次性口令 OTP（所有）：一次性口令是根据有效期较长的共享密钥产生的变化的密码，它来源于产生密码的运算因子是变化的
    3. 挑战 — 答应认证（所有）：通过一轮应答实现服务器对用户的认证，利用一次 性随机数实现防重放攻击
    4. 基于生物特征的认证（个人特征）：利用生物统计学，根据签名、指纹、人脸、虹膜、语音等个人特征实现身份认证
    5. 图灵测试：采用的方式利用人能快速回答，而机器回答困难的问题，验证登录信息系统的是人还是自动化执行的程序
    6. 多因子认证：采取多种认证方式结合进行认证
2. **身份认证的主流标准有哪些？FIDO 认证协议的主要目的是什么？**
    1. RADIUS：由 Livingston 公司发明的，用于接入认证和计费服务

2. 在线快速身份认证 FIDO：使用生物特征识别技术代替口令对在线用户进行身份认证
3. 联盟身份管理 FIM：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，支持用户身份跨安全域链接，用户可以在一个域中认证之后，不需 要再进行独立的登录过程就可以访问另一个域的资源

FIDO 认证协议的主要目的是：实现无口令身份认证协议

3. 挑战应答认证协议为什么可以对抗重放攻击？

利用一次性随机数并要求双方时间同步，从而通过一轮应答来验证认证者的身份。

4. 什么是联盟身份管理？

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，支持用户身份跨安全域链接，用户可以在一个域中认证之后，不需 要再进行独立的登录过程就可以访问另一个域的资源。

5. 访问控制模型有哪些？

1. 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
2. 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
3. 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

6. 虚拟化主要有哪些方式？其面临的安全威胁是什么？

1. 方式：
    1. 裸金属架构虚拟化
    2. 寄居架构虚拟化
    3. 容器虚拟化
2. 安全威胁：
    1. 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
    2. 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。攻

击者首先借助恶意虚拟机访问共享硬件和缓存，然后在交替执行的过程中通过边信道信息来推断出目标虚拟机的行为，识别相应的信息，最终导致目标虚拟机内的用户数据泄露。

7. 简述区块链的数据结构，说明其为什么具有不可篡改的特性。

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。默克尔树用来存储当前区块的所有交易信息

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。

8. **简述人工智能对网络安全的影响。**
    1. 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
    2. 网络犯罪：伪造语音、图片、视频，生成虚假内容，识别验证码
    3. 隐私保护侵犯：收集、识别个人隐私，精准画像
    4. 不确定性风险：人工智能不可控，产生意外损害
    5. 智能网络攻防：自动化的网络攻防
    6. 人工智能伦理：人工智能与人类的关系，是否会取代人类