**导论**

网络空间定义：

网络空间是除空天地海外的第五空间，包含了三个基本要素

1. 载体，即通讯信息系统
2. 主体，即网民，用户
3. 构造一个集合 用规则管理起来，我们称之为网络空间

网络空间安全涉及到在网络空间中的电子设备、电子信息系统、运行数据、系统应用中存在的安全问题，分别对应四个层面： 设备、系统、数据、 应用。（保障本身的安全，防止带来别的隐患）

针对这些风险，要采取法律、管理、技术、自律等综合手段来应对， 而不是仅仅是技术手段

没有网络安全就没有国家安全，没有信息化就没有现代化。 ”

网络安全现状问题

Ø 工业基础网络设施中关键应用或系统的故障将可能导致人员伤亡、严重的经济损失、基础设施被破坏、危及公众生活及国家安全。

Ø 目前的网络服务存在的风险和威胁正阻碍着企业信息化、电子商务和电子政务普及的进程。

Ø 网络隐私遭到侵犯的现象层出不穷， 网络隐私的重要性也逐渐被大众所重视，被社会各界所关注。

Ø 信息战是为夺取和保持信息权而进行的斗争，对国家军事、经济的抗

衡起着举足轻重的作用。

网络安全事件

1. 网络病毒：美国蠕虫病毒
2. 工业控制
3. 网络服务：ddos攻击
4. 隐私保护：字节跳动公司

网络空间安全卡脖子问题

1. 操作系统
2. 芯片（设备，工艺，材料三个方面）

面对卡脖子问题怎么做

1. 自主可信

2.关键基础设施安全

3.大力培养网络安全人才

国内外主要大学网络空间安全学科建设情况和发展过程

1.美国一流大学已建立起完善的网络安全学科核心课程体系，课程主题以实用性和行业发展为导向，包含 丰富的实践项目经验。

2.英国核心课程体系具有多学科交叉融合的特点

3.澳洲、亚洲知名大学的网络安全研究生核心课程设置从理论、实践等方面出发,培养全面的网络安全相关人才.

国外网络空间安全人才培养的特点分析

1把网络空间安全人才培养放在国家战略 高度重视

2教育体系覆盖面广、专业度高

3多部门联动培养

4完善的人才评价机制和激励制度

协议栈中信息传递的纵向传递和横向安全

纵向传递：↓

应用层: 最基本的功能是向该层用户提供透明的和可靠的数据传送基本服务

arp 嗅探监听

传输层:

网际层: 网络层介于传输层和数据链路层之间，向传输层提供最基本的端到端的数据传送服务

源地址假冒攻击

IP分片攻击原理: 当互联网上的两台远程主机进行数据传输时，如果传输路径上的各跳间，存在不同的链 路最大传输单元（Maximum Transmission Unit, MTU），那么可能会发生IP分组分片 （IP fragmentation），以满足链路MTU的要求

( 拒绝服务攻击

 污染攻击

 安全策略逃逸) IPSec协议

网络入侵检测系统IDS 域内路由安全 域间路由安全

数据链路层:

横向安全:

1 DNS劫持

2 ARP污染: 针对以太网地址解析 协议（ARP）的一种攻击技术.可让攻击者成为中间人（Man-in-the-Middle, MITM），获取局域网上的数据包，甚至可篡改 数据包，同时迫使受害主机无法正常接收报文

3 嗅探监听: 网络嗅探（Sniffers）是一种网络流量数据分析的手段，常见于网络安全攻防技术使用，也有用 于业务分析领域

网络嗅探具有两面性：

 网络管理员使用嗅探器，通过捕获分 析网络流量，进行高效的网络管理

 恶意攻击者使用嗅探器，攫取网络中 的大量敏感信息，进行网络攻击

恶意的网络嗅探，取决于攻击者的位置 和攻击能力：

 共享网络传输链路场景下，攻击者的 恶意嗅探监听

 攻击者控守了网络设备，对流经的流 量进行拦截嗅探

4 地址伪造: IP地址伪造通常是攻击者需具备的基本能力和手段，也是进行后续恶意数据注入、连接劫 持等攻击行为的基础条件，如TCP连接劫持攻击、DNS污染攻击等

路由劫持

5 TCP连接劫持、DoS攻击

ids特点匹配，异常检测

网络空间安全学科的主要研究方向

1. **密码学**

密码学由密码编码学和密码分析学组成

密码编码学主要研究对明文信息进行编码以实现信息隐蔽

密码分析学主要研究通过密文获取明文信息。

1. **系统安全**

是从系统的底层和整体上考虑信息安全威胁并采取综合防护措 施。它研究系统的安全威胁、系统安全的理论、系统安全的技术和应用

1. **网络安全**

针对不同的应用在网络的各个层次和范围内采取防护措施，以便 能够对各种网络安全威胁进行检测发现，并采取相应的响应措施，确 保网络设备安全、网络通信链路安全和网络的信息安全。

案例：

l 2001年中美黑客大战

l cSDN遭到黑客攻击，600多万个明文的注册邮箱被迫裸奔。

l 勒索病毒

l DD0S攻击

1. **内容安全**

广义的内容安全既包括信息内容在政治、法律和道德方面的要求，也包括信息内容的保密、知识产权保护、隐私保护等诸多方面。

案例：

利用图片传播隐含信息；自然语言处理与舆情分析；盗版，非法下载侵害知识产权；泄露用户隐私信息

1. **信息对抗**

信息对抗是从对方信息系统中获取有用信息， 削弱、破坏对方信息设备和信息的使用效能，保障己方信息设备和信 息正常发挥效能而采取的综合战术、技术措施，其实质是斗争双方利 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。

信息对抗研究信息对抗的理论、信息对抗技术和应用。

案例：鑫诺卫星被攻击事件；无人机；电子对抗与干扰

1. **新的网络安全研究方向**……

网络空间安全学科是在计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科的基础上交叉融合发展而来的

**1.系统安全**

系统安全的基本要求;

1.可用性：保证授权用户对系统信息的可访问和使用。

2.完整性：保护信息不被未经授权的实体更改和破坏。

3.机密性：保护信息不受未经授权的访问和泄漏。

系统安全的定义

物理安全：计算机与网络的设备硬件自身的安全，就是信息系统硬件的稳定性运行状态。

运行安全：运行过程中的系统安全，就是信息系统软件的稳定性运行状态。

信息安全（数据安全）：信息自身的安全问题，包括对信息系统中所加工、存储和网络中所传递数据的泄露、仿冒、篡改以及抵赖过程所涉及的安全问题。

系统安全措施

（注意：决不能低估法律、教育、管理的作用，许多时候它们的作用大于技术）

法律措施

教育措施

管理措施：包括信息设备、机房的安全管理，又包括对人的安全管理，其中对人的管理是最主要的。

技术措施：硬件系统安全、操作系统安全、密码技术、网络通信安全、数据库安全……

硬件系统和操作系统安全是基础，密码、网络安全等是关键技术

“三分技术，七分管理。”

目前，计算机网络系统安全的最大威胁之一是计算机网络的安全监管。

**2.物理安全**

物理安全定义：

保护计算机设备设施免遭火灾，水灾，地震及各种环境事故破坏的措施和过程

主要包括：

1. 环境安全：场地和机房（防盗报警，安全监控，温度湿度，用电安全，管理制度）
2. 设备安全：设备的防盗防毁，抗电磁干扰，电源保护等
3. 介质安全：介质数据的安全（防止记录的数据不被窃取破坏）和介质本身的安全（防盗防毁防霉）

容错与可靠性：

可靠度：在规定的运行环境中和规定的时间内软件无失效运行的机会。

容错主要依靠冗余设计来实现

冗余技术：以增加资源的办法换取可靠性。

1.硬件冗余：在常规设计的硬件之外附加备份硬件，包括静态冗余、动态冗余。

2.软件冗余：用于测试、检错的外加程序。

3.信息冗余：增加信息的多余度，使其具有检错和纠错能力。

4.时间冗余：重复地执行指令或一段程序而附加额外的时间。

硬件容错分为： 软件容错分为：

1.硬件备份 1.恢复块方法

2.数据备份 2.N版本程序设计

3.双机容错系统 3.防卫式程序设计

4.双机热备份

5.三机表决系统

6.集群系统

**3.硬件与芯片**

芯片安全研究现状：

1.ARM架构；

2.RISC-V架构；

3.x86架构

芯片安全实例：

1. 硬件木马
2. CPU漏洞

**4.可信计算**

可信计算思想：

首先建立一个信任根。

信任根的可信性由物理安全和管理安全确保。

再建立一条信任链。

从信任根开始到硬件平台、到操作系统、再到应用，一级认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。

（可信计算的思想源于社会）

可信计算的实现方法：可信测量技术

1. 可信的测量 2.度量的储存 3.度量的报告

可信计算的平台：可信PDA

传统可信：静态度量

取得的成功：可信计算+机密计算

未来科研方向：可信计算+动态可信

**5.操作系统安全**

安全操作系统是指对所管理的数据与资源提供适当的保护级，有效地控制硬件与软件功能的操作系统。

操作系统安全是指操作系统无错误配置、无漏洞、无后门、无木马等，能防止非法用户对计算机资源的非法存取，一般用来表达对操作系统的安全需求。

操作系统面临的安全威胁：

1. 不合理的授权机制
2. 不恰当的代码执行
3. 不恰当的主体控制
4. 服务的不当配置
5. 网络协议的安全漏洞
6. 不安全的进程间通信

安全操作系统实例：方徳方舟安全操作系统

主流操作系统安全的解决方案：

1. 身份认证机制
2. 访问控制机制
3. 系统可用性
4. 数据完整性
5. 数据保密性
6. 审计

操作系统安全的核心是访问控制，主要有自主访问控制、强制访问控制、基于角色的访问控制等。

**6.软件安全**

软件安全问题的解决方案：

1. 软件漏洞分析
2. 病毒对抗技术
3. 黑盒测试：功能测试
4. 白盒测试：结构测试

软件漏洞分析：

1. 漏洞挖掘：

传统漏洞挖掘技术：静态漏洞挖掘技术（直接对目标程序进行分析不需要构造程序的执行环境但精度低、误报率高）；动态漏洞挖掘技术（模糊测试和动态污点分析）

基于学习的智能化漏洞挖掘技术（更高的准确率和完备性,消耗的人力资源相对较少）

1. 漏洞分析
2. 漏洞利用

**7.数据库安全**

数据库安全的重要性体现：

1. 数据库是重要应用软件
2. 数据库集中储存和管理着大量重要数据，如军事，政治，金融等，使得数据库成为不法 分子攻击的主要目标
3. 数据库要支持查询，插入，删除，更新等一系列操作，存储数据量大，时间长是其重要特征

数据库常见的安全问题：

1. 物理数据库的完整性
2. 逻辑数据库的完整性
3. 元素安全性
4. 可审计性
5. 可用性
6. 访问控制
7. 身份认证
8. 推理控制
9. 多级保护
10. 推理消除隐通道

数据库安全实例：

1. 数据泄露
2. 数据库漏洞

数据库安全解决方法：

1. 数据库审计
2. 数据库防火墙
3. 数据库加密
4. 数据库静态
5. 数据库动态脱敏
6. 安全标准

为何对数据库安全加密很麻烦：

1. 数据量大
2. 存储时间长，密钥应经常更换
3. 数据库要支持查询，插入，删除，更新等一系列操作，需要同态加密

数据库安全发展：

1. 数据库密文检索
2. 同态加密

**8.大数据安全**

大数据的定义：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

大数据的特点：

1. 海量的数据规模
2. 快速的数据流转
3. 多样的数据类型
4. 价值密度低

大数据面临的安全问题：

1. 受攻击风险高
2. 隐私信息泄露风险
3. 传输过程的安全隐患
4. 大数据的存储管理风险

大数据安全解决方案：

1. 大数据安全审计
2. 大数据脱敏系统
3. 大数据脆弱性检测
4. 大数据资产梳理
5. 大数据应用访问控制

**9.云安全计算**

云计算的定义：

云计算是一种可以方便的通过网络对共享的可配置计算资源池进行按需访问的模型,池中资源只需要很少的管理付出或服务提供者帮助就能快速供应和释放。

云计算安全问题：

1. 产品漏洞
2. 隐私权限泄露
3. 黑客攻击
4. 服务中断

云计算安全的研究方向：

1. 借助硬件隔离技术构造可信执行环境
2. 基于可信虚拟化技术构建可信云平台
3. 通过建立可信第三方对云计算平台进行动态可信度量
4. 以可信安全芯片的密钥管理为基础，将终端密钥管理转化为云平台密钥管理

**10.系统安全热点问题**

（物联网安全，车联网安全，空天信息安全）

物联网安全

物联网安全的层次架构：

感知层安全

网络层安全

应用层安全

作为基于互联网的新兴信息技术模式，物联网安全上升至国家安全

物联网安全威胁：

感知层安全威胁：隐私泄露威胁，物理攻击，信号泄露与干扰

网络层安全威胁：网络层协议漏洞，DDOS攻击，无线传输问题

应用层安全威胁：病毒，蠕虫，木马，远程攻击

物联网安全防护：

感知层：物理安全，接入安全，硬件安全，操作系统安全，数据安全

网络层：安全审计，加密传输，网络入侵防护

应用层：十分控制，访问控制，隐私保护，APP安全

物联网安全研究方向：

1. 去中心化认证
2. 边缘计算

车联网安全

车联网安全威胁：

网络：信息容易被窃听，网络容易被攻击

平台：车辆本身容易被攻击

组件：汽车专用微机控制器的脆弱性

车联网安全国内研究主要问题

1. 如何提高针对车联网攻击的检测及攻击响应效率？

2. 如何实现精准的网络安全测试评估？

3. 如何应对未知的智能网联车网络攻击？

4. 如何制定及时有效的智能网联车信息安全标准？

空天信息安全

案例：鑫诺卫星遭受攻击

卫星链路安全问题；可信的空天信息；传统的安全问题与非传统环境和应用的交织

**密码学**

密码算法的作用：1.加密 2. 认证

分为：密码编制学，密码分析学（密码破译）

信息安全学科的研究方向与内容

1. 密码学
2. 网络安全
3. 信息系统安全
4. 信息内容安全

传统密码体制的密钥产生 本质上是产生具有良好密码学特性的随机数或随机序列

密钥必须满足密码安全性和应用有效性

RSA密码:可用于加密，数字签名，安全易懂

数字签名应该满足的条件：

1. 签名者事后不能抵赖
2. 其他人不能伪造
3. 如果当事双方关于签名真伪发生争执，能够在公正的冲裁者面前通过验证确认其真伪

密钥分配时应该做到：

公钥：因为公钥是公开的，不用确保秘密性，要确保真实性和完整性

私钥：秘密性，真实性，完整性

**网络安全**（链路层，网络层，传输层）

协议栈中消息的横向安全：

1. DNS劫持
2. ARP污染
3. 嗅探监听
4. 地址伪造，路由劫持
5. TCP链接劫持，DOS攻击
6. 链路层安全（ARP欺骗与污染，网络嗅探与网络监听）

链路层最基本的功能：

向该层用户提供透明的和可靠的数据传送基本服务

功能：

1.将数据组合成帧

2.控制帧在物理信道上的传输 ，包括处理传输差错 ，调节发送速率

3.提供数据链路通路的建立、维持和释放的管理

ARP欺骗又称ARP污染，是针对以太网地址解析协议(ARP)的一种攻击技术，可让攻击者成为中间人，获取局域网上的数据包，甚至可篡改数据包，同时迫使受害主机无法正常接收报文

网络嗅探是一种网络流量数据分析的手段

网络嗅探具有两面性：

网络管理员使用嗅探器 ，通过捕获分析网络流量 ，进行高效的网络管理

恶意攻击者使用嗅探器 ，攫取网络中的大量敏感信息 ，进行网络攻击

1. 网络层安全

网络层介于传输层和数据链路层之间，向传输层提供最基本的端到端的数据传送服务

网络层具备的功能包括：

分组与分组交换

路由

网络互联

网络连接复用

差错检测与恢复

服务选择

网络管理

分片与重组

1. 源地址假冒攻击
2. IP分片攻击
3. 拒绝服务攻击
4. 污染攻击
5. 安全策略 逃逸
6. IPSec协议

两种安全协议：认证；加密

两种工作模式：传输模式，隧道模式

1. 网络入侵检测系统IDS

两类IDS:基于特征匹配；基于异常检测

1. 域内路由安全
2. 域间路由安全
3. 传输层安全

传输层主要负责提供不同主机应用程序进程之间的端到端的服务

常见的传输层协议主要包括两类：TCP和UDP

传输层的基本功能如下：

1.分割与重组数据

2.按端口号寻址

3.连接管理

4.差错控制和流量控制、纠错的功能

网络攻击共性特征分析：

1.攻击者可以进行身份欺骗 ，伪装成网络通信的一端（身份欺骗）

2.攻击者可以进行推理猜测 ，成功构造出可被通信对端接受的数据报文（数据猜测）

协议栈的不当设计：

一是网络地址缺乏足够的真实性验证 ，可以被恶意伪造

二是网络系统在实现和部署过程中， 随机化程度不高 ，致使网络的状态信息可被恶意攻击者预测推理

协议栈安全的基本防御原理：

1.基于真实源地址的网络安全防御

2.增强协议栈随机化属性

**大数据与AI**

大数据：具有4V特征的数据集（volume，velocity,variety,value）

大数据特征：volume，体量 velocity,速度 variety,多样性 value，价值密度

大数据面临的问题（4V）

1. 海量的数据规模
2. 快速的数据流转
3. 多样的数据类型
4. 巨大的数据价值

人工智能未来

• 类人智能

• 仿真大脑

• 心灵模型

• 知识推理

• 情感模拟

• 意识力

• 创造力

大数据与人工智能：

1. 大数据为人工智能提供了数据基础
2. 人工智能为大数据提供了分析模型
3. 算力为大数据和人工智能提供了计算基础
4. 大数据加强和证实了经验主义人工智能的路线，理性主义应融入经验主义的框架

**大数据和AI自身的安全**

可能带来的危害

1. 威胁物理环境安全
2. 威胁人身财产安全
3. 威胁国家社会安全

• 数据安全性

-- 指人工智能算法所依赖的数据的安全性

• 模型安全性

– 指人工智能算法或模型的自身安全性

• 环境安全性

– 指人工智能算法或模型在训练、实现或运行时，依赖的外部环境的安全性

A.人工智能本身面临的数据安全

• 训练阶段数据污染

• 运行阶段数据异常

• 模型窃取攻击还原训练数据

• 开源框架导致数据泄露

B.人工智能应用导致的数据安全

• 个人数据过度采集

• 放大数据偏见，导致社会歧视

• 数据资源滥用，加大治理风险

• 数据智能窃取风险

C.人工智能应用加剧的数据治理

• 数据权属：个人和行业

• 数据违规跨境风险

• 对抗样本

• 白盒攻击：修改模型

• 黑盒攻击：修改数据

• 后门攻击

• 篡改训练数据

• 篡改模型参数

• 木马样本数据

• 深度伪造

• 可解释性

**基于大数据和AI的安全**

1. **人工智能助力网络攻击**
2. 恶意代码免杀
3. 基于生成对抗网络框架IDSGAN生产恶意流量
4. 智能口令猜解
5. 新型文本验证码求解器
6. 自动化高级鱼叉式钓鱼
7. 网络钓鱼电子邮件生成
8. Deeplocker新型恶意软件
9. Deepexploit全自动渗透测试工具
10. 基于深度学习的DeepDGA算法
11. 基于人工智能的漏洞扫描工具
12. **人工智能助力网络防御**
13. 恶意软件检测
14. 未知加密恶意流量检测
15. 恶意网络流量检测
16. 基于人工智能检测恶意域名的方法
17. 运用机器学习检测恶意URL
18. 新型网络钓鱼电子邮件检测
19. 基于人工智能的网络安全平台
20. 基于机器学习的通用漏洞检测方法

人工智能应用问题分析：

1. 逻辑性强的漏洞难以发现
2. 算力限制
3. 数据接问题：训练数据缺乏
4. 可解释性差
5. 性能有待提高

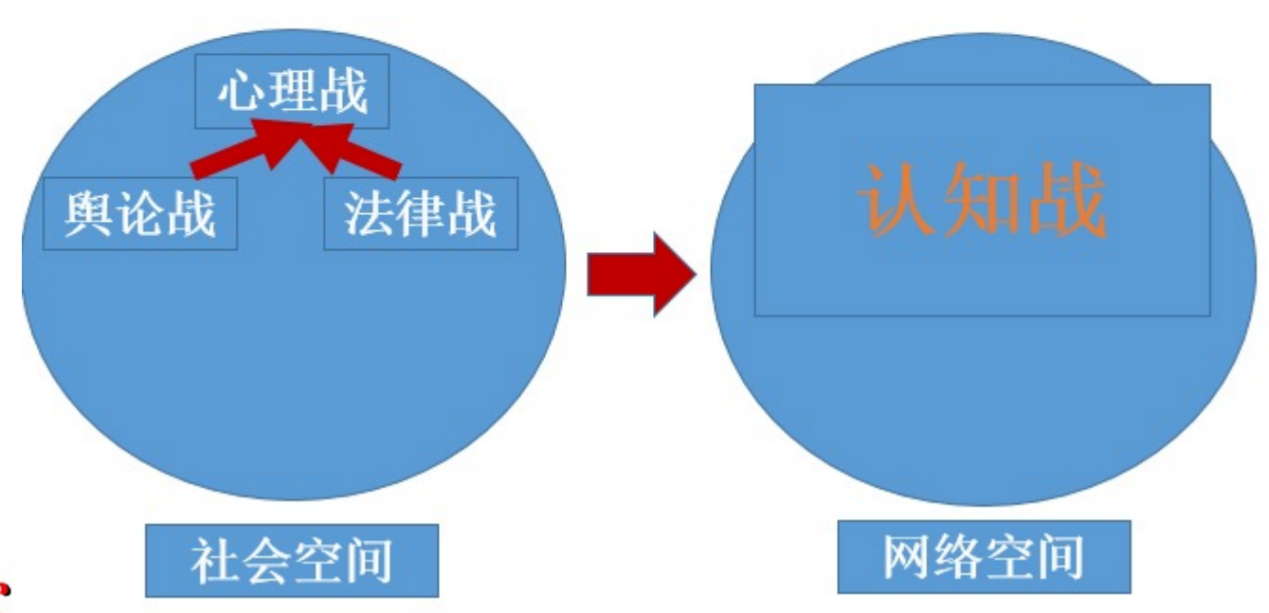
认知对抗概念:

情感和情感对抗：情感博弈

认知和认知对抗

认知对抗挑战：

1. 舆论抹黑
2. 威胁利诱
3. 法律裁决
4. 心理震撼
5. 心理扭曲
6. 谣言散播



认知对抗定位：

1. 博弈空间（物理战，信息站，认知站）
2. 网络安全（信息安全，内容安全，认知安全）
3. 网络空间治理
4. 总体国家安全观

认知对抗技术：

话题分析,属性分析，观点分析，意见分析，诱因分析，情绪分析，情绪演化，情感对话，用户画像，情报生产

认知对抗应用前景：

1. 国家安全，社会稳定
2. 舆情的监测预警引导
3. 情报
4. 网络空间话语权
5. 网络空间维稳