概论

网络空间定义

网络空间是除空天地海之外的第五空间，包含了三个基本要素：
·第一个是**载体**，也就是通讯信息系统
·第二个是**主体**，也就是网民、用户
·第三个是构造一个**集合**，用规则管理起来，我们称之为“网络空间”

网络空间安全定义

网络空间安全涉及到网络空间中的**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**。这里面包括：

- 要保障系统本身的安全
  防治、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的**各种通信系统及其承载的数据不受损害。**
- 要防止利用信息系统带来别的安全隐患
  对这些信息系统的滥用会引发的**政治安全、经济安全、文化安全、国防安全**的相关问题。

我国网络空间安全有关政策制度和方法

1. 《中华人民共和国**网络安全法**》
2. 《中华人民共和国**密码法**》
3. 网络安全等级保护制度2.0系列标准
4. 《关键信息基础安全保护条例》
5. 《中华人民共和国**电子签名法**》
6. 《中华人民共和国**数据安全法**》
7. 《中国人民共和国**计算机系统安全保护条例**》
8. 《公安机关互联网安全监督检查规定》

网络空间安全卡脖子问题

操作系统：
在**操作系统层面**中国如果**无法实现自主可控**，面对源源不断的漏洞风险。
芯片：
在**设备、工艺和材料**三个方面还与国外存在差异
真正意义上的实现网络空间安全：

- 自主可信；
- 关键基础设施安全
- 大力培养网络安全人才

国内外网络空间安全学科建设的主要内容

- 密码学
- 系统安全
- 网络安全
- 内容安全
- 信息对抗
- 新的网络空间安全研究方向……

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对应的明文信息。

主要具体研究内容

①对称密码
②公钥密码
③Hash函数
④密码协议
⑤新型密码
⑥密钥管理
⑦密码应用

网络安全

定义：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。

主要具体研究内容

①网络安全威胁
②通信安全
③协议安全
④网络防护
⑤入侵检测与态势感知
⑥应急响应与灾难恢复
⑦可信网络
⑧网络安全管理

系统安全

定义：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。

主要具体研究内容

①系统的安全威胁
②系统的设备安全
③系统的硬件子系统安全
④系统的软件子系统安全
⑤访问控制
⑥可信计算
⑦系统安全等级保护
⑧系统安全测评认证
⑨应用信息系统安全

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。

主要具体研究内容

①内容安全的威胁
②内容的获取
③内容的分析与识别
④内容安全管理
⑤信息隐藏
⑥隐私保护
⑦内容安全的法律保障

信息对抗主要的研究内容

①通信对抗
②雷达对抗
③光电对抗
④计算机网络对抗

系统安全

基本要求

- 可用性：保证授权用户对系统信息的可访问和使用。
- 完整性：保护信息不被未经授权的实体更改和破坏。
- 机密性：保护信息不受未经授权的访问和泄漏。

定义

确保以电磁信号为主要形式的、在计算机网络化系统进行自动通信、处理和利用的信息内容，在各个物理位置、逻辑区域、存贮和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性的，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。

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。**

物理安全

物理安全又叫实体安全（Physical Security），**是保护计算机设备、设施**（网络及通信线路）**免遭**地震、水灾、火灾、有害气体和其他**环境事故**（如电磁污染等）**破坏的措施和过程**。

环境安全、设备安全和介质安全

环境安全：系统**所在环境**的安全，主要是场地与机房。
设备安全：主要指**设备的防盗、防毁、防电磁辐射泄露、防止线路截获**、抗电磁干扰及电源保护等。
介质安全：包括**介质数据的安全**及**介质本身的安全**

实际问题：硬盘忽然掉电会损坏硬盘和数据吗？

在意外断电的时候，磁盘控制器会利用空气动力和一些电容的余电，将磁头移到着陆区里面降落，从而保证不会划伤盘片。着陆区也是硬盘没事干时，磁头的休息区。

容错与实现方法

容错技术是指在一定程度上容忍故障的技术，也称为故障掩盖技术（Fault Masking）。采用容错技术的系统称为容错系统。
容错主要依靠冗余设计来实现，它以增加资源的办法换取可靠性。
冗余技术可分为：硬件冗余、软件冗余、信息冗余和时间冗余。

- 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。
- 软件冗余：用于测试、检错的外加程序。
- 信息冗余：增加信息的多余度，使其具有检错和纠错能力。
- 时间冗余：重复地执行指令或一段程序而附加额外的时间。

可信计算

可信：可靠加安全
硬件系统安全和操作系统安全是信息系统安全的基础，密码技术、网络安全技术等是关键技术。
只有从芯片、主板等硬件结构和BIOS、操作系统等底层软件作起，综合采取措施，才能比较有效的提高微机系统的安全性。

可信计算思想：
首先建立一个信任根。

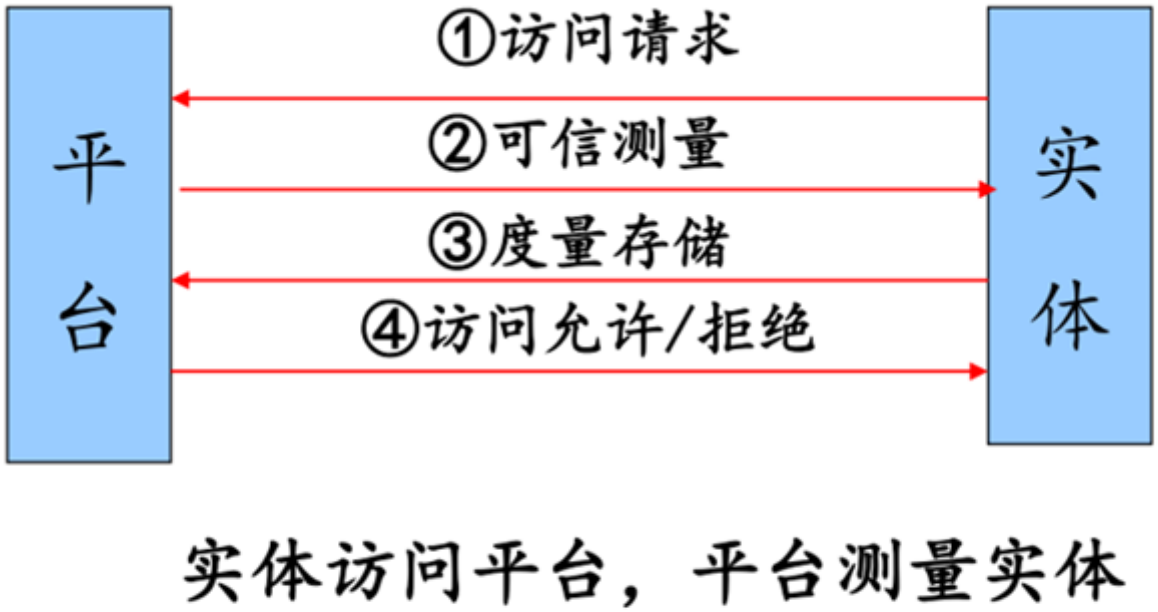
信任根的可信性由物理安全和管理安全确保。

再建立一条信任链。

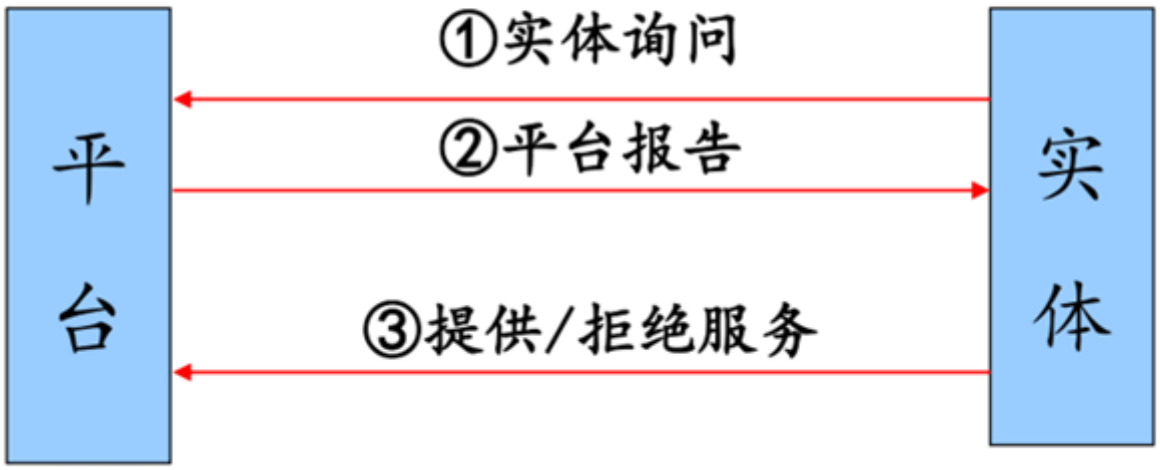
从信任根开始到硬件平台、到操作系统、再到应用，一级认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。

可信计算的思想源于社会

实现方法：（怎么进行可信计算/可信计算流程、思想）



实体访问平台，平台测量实体



实体询问平台，平台提供报告

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。指操作系统无错误配置、无漏洞、无后门、无特洛伊木马等，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。

操作系统的安全威胁

- 不合理的授权机制
- 不恰当的代码执行
- 不恰当的主体控制

主流操作系统安全的解决方案

- 身份认证机制
- 访问控制机制
- 数据保密性
- 数据完整性
- 系统的可用性
  操作系统安全的核心是访问控制

软件安全

当前的网络安全问题可粗略的分为：计算机病毒、恶意软件、软件漏洞、软件后门

软件漏洞分析

漏洞从发现到产生实际危害的整个过程可分为**漏洞挖掘、漏洞分析、漏洞利用**三个阶段。

软件安全问题解决方案

- 软件漏洞分析
- 病毒对抗技术
- 黑盒测试
- 白盒测试

大数据面临的安全问题

- 受到攻击风险高
- 隐私信息泄露风险
- 传输过程的安全隐患
- 大数据的存储管理风险

大数据安全解决方案

- 大数据安全审计
- 大数据脱敏系统
- 大数据脆弱性检测
- 大数据资产梳理
- 大数据应用访问控制

云计算安全问题

- 产品漏洞
- 隐私权限泄露
- 黑客攻击
- 服务中断

物联网安全

根据其层次架构分为：感知层安全、网络层安全、应用层安全。

网络安全

主要内容：

<table>
<tr><th>协议栈</th><th>网络攻击</th><th>攻击共性特征</th><th>协议栈的缺陷</th><th>防御</th></tr>
<tr><td>链路层</td><td>• 帧嗅探
• ARP污染</td><td rowspan="3">①攻击者进行身份欺骗，伪装成原通信会话的合法参与方

②攻击者伪造请求，并观测、判断目标对请求的响应，推理出受害通信会话的状态信息

③攻击者依据推理出的会话状态信息，伪造可被原会话接受的数据包，注入原合法数据流中，进行恶意攻击</td><td rowspan="3">①网络地址可伪造

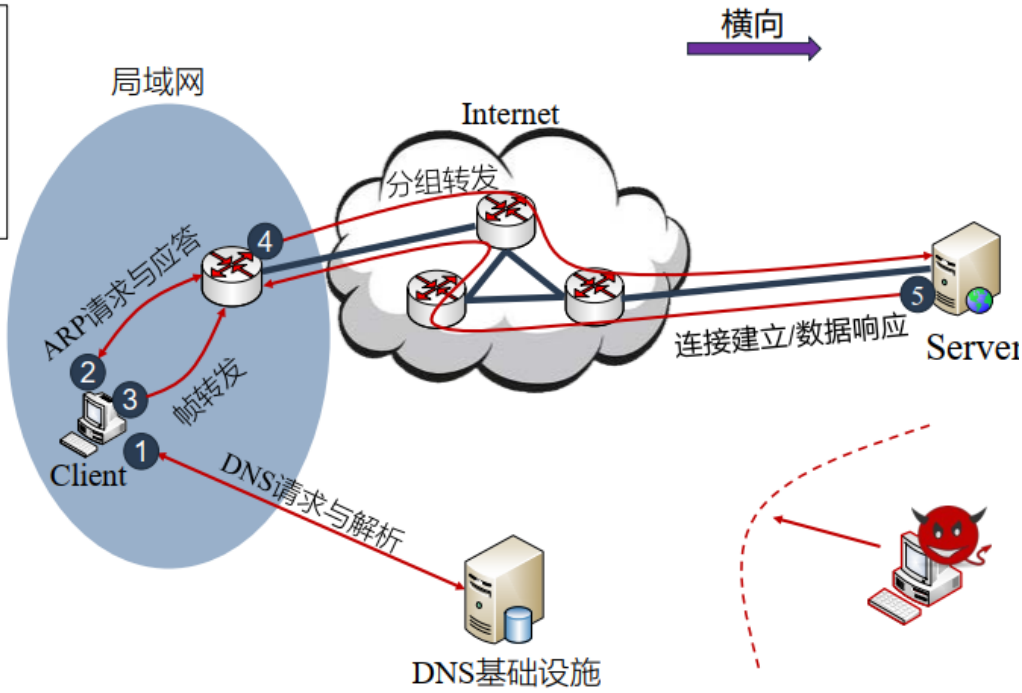
②系统随机化程度不够</td><td rowspan="3">① 真实地址 与真实身份

② 网络系统 随机化</td></tr>
<tr><td>网络层</td><td>• IP地址欺骗
• IPID误用
• IP分片误用
• ICMP误用
• 路由劫持</td></tr>
<tr><td>传输层</td><td>• TCP劫持
• TCP DoS</td></tr>
</table>

协议栈中的消息的横向安全：

局域网中的client远程访问Server时，在数据传递处理的每一步，都有可能产生安全问题

1. DNS劫持
2. ARP污染
3. 嗅探监听
4. 地址伪造、路由劫持
5. TCP连接劫持、DoS攻击



- ARP欺骗与污染（原理）

  ARP欺骗，又称ARP污染，是针对以太网地址解析协议的一种攻击技术。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

  拓扑示例

  局域网中的两台主机 A 、 B ，以及他们的 IP 地址和 MAC 地址：主机A的IP地址为192.168.1.1，MAC地址为0A-11-22-33-44-01，主机B的IP地址为192.168.1.2，MAC地址为0A-11-22-33-44-02。

  A 、 B 间正常的 ARP 解析过程：

  第1步： A 主机在本地 ARP 缓存中，检查主机 B 的 MAC 地址

  第2步：如果没有找到，询问192.168.1.2的硬件地址将 ARP 请求帧广播到本地网络上的所有主机

  第3步：主机 B 确定 ARP 请求中的 IP 地址与自己的 IP 地址匹配，将主机 A 的 IP 地址和 MAC 地址映射，添加到本地 ARP 缓存中

  第4步：主机 B 将包含其 MAC 地址的 ARP 回复消息，直接发送回主机 A

  第5步： A 收到回复，用主机 B 的 IP 和 MAC 地址映射更新 ARP 缓存

  安全问题

  在 ARP 回复时，主机 A 并不会验证 ARP 回复包的真实性。由此引出一个局域网攻击方式 ARP 欺骗：恶意主机 C ，企图冒充 B ，欺骗 A

  恶意节点 C 进行 ARP 欺骗，污染攻击 A 的 ARP 缓存：

  第1步：主机 A 要和主机 B 通信，主机 A 发出 ARP 包询问谁是192.168.1.2？请回复192.168.1.1。

  第2步：主机 C 向主机 A 发送 ARP 应答报文，我是192.168.1.2，我的地址是0A-11-22-33-44-03

  第3步：当 A 收到 C 发来的 ARP 回复消息时，会用主机 B 的 IP 和 C 的 MAC 地址映射，更新 ARP 缓存，从而实现了攻击者 C 对 A 发往 B 的流量的劫持

- 网络监听和嗅探

  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

链路层功能

- 将数据组合成帧
- 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
- 提供数据链路通路的建立、维持和释放的管理

网络层功能

- **分组与分组交换**
- **路由**
  路由（routing）是通过互联的网络，把信息从源地址传输到目的地址的活动
  路由安全包括域间路由安全和域内路由安全
- **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

源地址假冒攻击（原理）

IP地址用于唯一的标识互联网上的一个网络通信接口
网络层的源 IP 地址假冒攻击 ,是最常见的一种针对 IP 协议的攻击
通常， IP spoofing 也是进行复杂网络攻击，如会话劫持， DNS 污染、 TCP 劫持等攻击，的能力基础和先决条件
攻击原理:
Host1和Host2为正常合法通信的两台主机，IP 地址分别为： x . x . x . x 和 y . y . y . y恶意攻击者 Attacker，其真实 IP 地址为 Z . Z . Z . Z , Attacker 企图冒充 Host ， 发动源 IP 地址伪造攻击，Attacker 生成恶意分组，发送给主机Host2并且将分组的源地址指定为 x . x . x . x
最终的后果是：Attacker 欺骗了主机Host2，使其误认为这些分组来自于合法的远程通信端 Host 1；Attacker 也隐藏了自己的真实地址和身份，避免被追踪溯源

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，那么可能会发生IP分组分片
所有的IP分片到达目的接收端后，接收 端对这些分片进行重组， 还原出原来的 IP分组， 再提交给上层进行处理
分片的重组依赖于IPID字段， 而原始IP 分组是否允许被分片， 取决于Flags字段中的DF位

IP分组的这种**先分片、再重组**的机制，为攻击者暴露出了IP层的一个攻击面。

IP碎片攻击

- 拒绝服务攻击
  理论上一个IP分组的最大长度是65535字节， 攻击者可以发送一个长度超过65535字节IP分组，迫使接收端在对分片重组时，出现缓冲区溢出漏洞，造成异常错误
- 污染攻击
  在原始报文被分片、传输过程中，攻击者伪造一些分片，注入到正常分片流中， 篡改原始报文内容，从而形成对合法流量的污染
- 安全策略逃逸
  通常网络防火墙会对IP分片进行重组， 然后审查其中的恶意载荷。 但防火墙和接收端主机往往存在重组策略不一致现象， 即当分片出现重叠时， 二者可能会采用不同的覆盖策略
  因此， 攻击者可以通过设置合理的分片偏移， 逃逸防火墙的审查， 但形成对接收端的破坏

为了避免IP分片，提出了一些相关技术标准：“路径MTU发现”机制

IPSec协议

即Internet协议安全性，是一种开放标准的框架结构，通过对IP协议的分组进行加密和认证，来保护基于IP协议的网络传输
IPSec（互联网协议安全）是一个安全网络协议套件，用于保护互联网或公共网络传输的数据。IETF在1990 年代中期开发了 IPSec 协议，它通过 IP网络数据包的身份认证和加密来提供 IP 层的安全性。

两种安全机制：认证AH、加密ESP

认证机制

提供数据源认证、 数据完整性校验和防报文重放功能，它能保护通信免受篡改， 但不能防止窃听， 适合用于传输非机密数据

加密机制

提供加密、数据源认证、数据完整性校验和防报文重放功能。

工作模式

- 传输模式
  只是传输层数据被 用来计算AH或ESP头， AH或ESP头以及ESP 加密的用户数据被放置在原IP包头后面
- 隧道模式
  用户的整个IP数据包 被用来计算AH或ESP头， AH或ESP头以及 ESP加密的用户数据被封装在一个新的IP数据包中

网络入侵检测系统

IDS主要分为两类：

- 基于特征匹配的IDS
  基于专家知识或经验， 预定义攻击行为特征或规则，然后对网络流量或主机行为进行匹配，如果匹配成功，则判定为攻击事件
  优点： 误报率低，检测速度快
  缺点： 无法识别未知攻击，存在漏报
- 基于异常检测的IDS
  首先通过学习建模的方法，构建网络或主机的正常行为基线。然后结合当前网络或主机态 势进行判断，如果网络或主机的行为偏离该基线，则判断发生了入侵或攻击，进行告警
  优点：可以识别未知攻击
  缺点：存在误报，检测速度慢

传输层安全

传输层的基本功能如下：

- 分割与重组数据
- 按端口号寻址
- 连接管理
- 差错控制和流量控制、纠错的功能
  常见的传输层协议主要包括两类：TCP（Transmission Control Protocol）和UDP （User Datagram Protocol）

拒绝服务攻击

最常见的DoS攻击有**计算机网络带宽攻击**和**连通性攻击**:

- 带宽攻击指以极大的通信量冲击网络，使得所有可用 网络资源都被消耗殆尽
- 连通性攻击指用大量的连接请求冲击计算机，使得所 有可用的操作系统资源都被消耗殆尽

TCP劫持攻击

TCP劫持攻击是指，一个TCP连接外的的非法攻击者，将自己伪造的TCP报文，注入到TCP连接双方的合法数据流中，进而对连接进行攻击破坏

- 伪造控制报文、如RST报文等，恶意阻断该连接
- 伪造数据报文，污染数据流

TLS协议（传输层安全性协议）

通常在TCP等传输层协议之上运行，提供以下三个安全功能:

- 加密： 阻止第三方对传输数据的窃听
- 身份验证：确保交换信息的各方是他们声称的身份
- 完整性：验证数据是否伪造而来或未遭篡改过

网络攻击的共性特征

攻击者可以进行身份欺骗，伪装成网络通信的一端
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

协议栈的不当设计

两个共性特征映射到实际的网络系统中，本质上是利用了当前协议栈中的两个基础安全缺陷

- 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
- 网络地址可伪造， 缺乏合法性验证
- 网络状态信息可预测推理，缺乏足够的随机化

协议栈安全的基本防御原理

- 基于真实源地址的网络安全防御
- 增强协议栈随机化属性

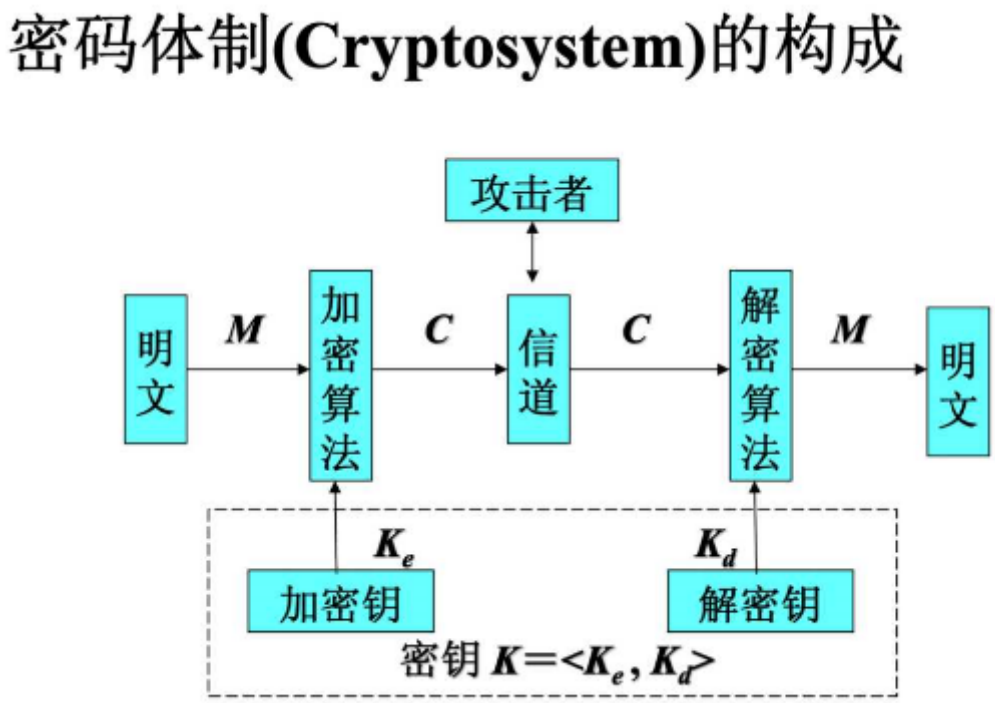
密码学

密码算法的作用——加密、认证

- 对称密码
- 公钥密码
- Hash函数
- 密码协议
- 新型密码
- 生物密码
- 量子密码等

密码学的组成

- 研究密码编制的科学称为密码编制学
- 研究密码破译的科学称为密码分析学（密码分析学俗称密码破译）
- 密码编制学和密码分析学共同组成密码学



RSA公钥密码（原理）

数字签名

一种完善的签名应满足以下三个条件:

- 签名者事后不能抵赖自己的签名;
- 任何其他人不能伪造签名;
- 如果当事的双方关于签名的真伪发生争执， 能发在公正的神裁者面前通过验证确认其真伪

AI和大数据安全

大数据与人工智能

- 大数据为人工智能提供了数据基础
- 人工智能为大数据提供了分析模型
- 算力为大数据和人工智能提供了计算基础

- 大数据证实和加强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的自身安全

- 威胁物理环境安全
- 威胁人身财产安全
- 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

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

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

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

人工智能模型安全

- 对抗样本

- 后门攻击
- 深度伪造
- 可解释性

人工智能环境安全

- AI:TensorFlow;Pytouch
- 大数据；Hadoop、Hbase、MongoDB、ElasticSearch

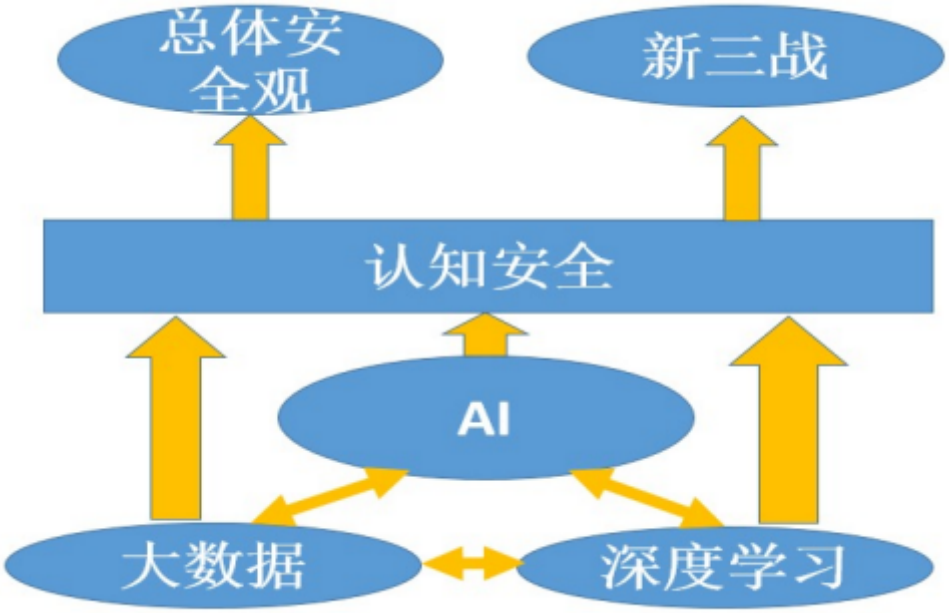
人工智能助力网络攻击

- 恶意代码免杀
- 基于生成对抗网络框架IDSGAN生成恶意流量
- 智能口令猜解
- 新型文本验证码求解器
- 自动化高级鱼叉式钓鱼
- 网络钓鱼电子邮件生成
- DeepLocker新型恶意软件
- DeepExploit全自动渗透测试工具
- 基于深度学习的DeepDGA算法
- 基于人工智能的漏洞扫描工具。

人工智能助力网络防御

- 恶意软件检测
- 未知加密恶意流量检测
- 恶意（僵尸)网络流量检测
- 基于人工智能检测恶意域名的方法
- 运用机器学习检测恶意URL
- 新型网络钓鱼电子邮件检测
- 基于人工智能的网络安全平台AI2
- 基于机器学习的通用漏洞检测方法
- 基于深度学习的威胁情报知识图谱构建技术
- 基于混合词向量深度学习模型的DGA域名检测方法

认知对抗总结



补充

sm4是什么算法

2017年安华金和发布国内首款支持MySQL数据库的透明加密产品
（DBCoffer-MySQL TDE）采用国产SM4加密算法，相较传统AES等算法更安全可靠、合规，最大程度保证数据安全
对称算法 无线局域网标准的分组数据算法

关于网络入侵检测系统，HIDS和NIDS的区分

网络数据传输（NIDS），主机系统行为（HIDS），
HIDS全称是Host-based Intrusion Detection System，即基于主机型入侵检测系统。作为计算机系统的监视器和分析器，它并不作用于外部接口，而是专注于系统内部，监视系统全部或部分的动态的行为以及整个计算机系统的状态。
网络入侵检测系统(network intrusion detection system，NIDS)，是指对收集漏洞信息、造成拒绝访问及获取超出合法范围的系统控制权等危害计算机系统安全的行为，进行检测的软件与硬件的组合。
NIDS的目的是从网络上的TCP/IP消息流中识别出潜在的攻击行为

大数据和AI安全的联系

数据安全性
-- 指人工智能算法所依赖的数据的安全性

网络分层

物理层 (PH)、 数据链路层 (DL)、网络层 (N)、传输层 (T)、会话层 (S)、 表示层 (P)、 应用层 (A)。

协议栈中消息的纵向传递

信息由应用层发送至传输层，加上TCP/UDP头部，发送到网络层，加上IP头部，发送到链路层，再加上Link头部。

协议栈中消息的横向安全

局域网中的client远程访问Server时，在数据传递处理的每一步，都有可能产生安全问题。进行DNS请求与解析可能发生DNS劫持；进行ARP请求与应答时可能发生ARP污染；进行帧转发时可能发生嗅探监听；进行分组转发时可能发生地址伪造、路由劫持；进行连接建立/数据响应时可能发生TCP连接劫持、DoS攻击。

（开放题）怎样设置密码让黑客不容易猜到/怎样设计密码使得足够安全，而且说明安全的密码有什么特征/比较安全的密码要注意什么

为了设置一个不容易被黑客猜到的密码，可以考虑以下几个建议：

- 密码长度：密码越长越安全。建议使用至少12个字符的密码。
- 复杂度：使用多种字符类型（如大写字母、小写字母、数字和符号）组成密码。这将使密码更难以猜测。
- 不要使用常见密码：不要使用易于猜测的密码，如"123456"、"password"等。这些密码非常常见，黑客有可能使用破解工具轻易地破解它们。
- 避免使用个人信息：不要使用与个人信息有关的密码，如生日、姓名、地址等。这些信息容易被黑客获取。
- 定期更改密码：即使使用非常强的密码，也应该定期更改密码。这可以减少黑客猜测或获取密码的机会。

除此之外，安全的密码通常具有以下特征：

- 长度足够：密码长度越长越安全，建议使用至少12个字符的密码。
- 复杂度高：使用多种字符类型组成密码，包括大写字母、小写字母、数字和符号。
- 随机性强：密码应该是随机的，避免使用类似字典中的单词、常见短语或习惯用语等。
- 避免使用相同密码：不要在多个账户上使用相同的密码，这会增加黑客获取密码的机会。
- 定期更改密码：即使使用非常强的密码，也应该定期更改密码。
-

比较安全的密码还需要注意以下几点：

- 不要轻易泄露密码：密码不应该轻易泄露给他人，尤其是陌生人。
- 不要在公共场合输入密码：在公共场合，如咖啡厅、图书馆等地方，应该避免输入密码，以防止密码被窃取。
- 使用双因素认证：使用双因素认证可以进一步提高账户安全性。双因素认证通常需要输入密码以及其他验证方式，如手机短信、指纹等。

（开放题）网络安全在当下的应用