网络空间安全复习

# 什么是安全？

网络空间是人造的电磁空间，其以终端、计算机、网络设备等为载体，用户通过在其上对数据进行创造、存储、改变、传输等操作，以实现特定的活动。

在网络空间中，人、机、物可以被有机地连接在一起进行互动，可以产生影响人们生活的各类信息，包括内容信息、商务信息、控制信息等。

**主体**：人们以用户的身份在网络空间中活动

**载体**：终端、计算机、网络设备等载体进入网络空间

**资源**：人类处理的对象是数据

**活动**：数据创建、存储、改变、传输等操作

正确性：Good Input ⇒ Good Output，预期的输入会得到预期的输出

安全性：Bad Input ⇏ Bad Output，意外的输入，系统不会因此故障，系统越复杂越脆弱

机密性（**C**onfidentiality）：保证信息内容不被非授权者获取与使用，保证数据在传输和存储过程中不被获取和解析。

完整性（**I**ntegrity）：保证数据在传输、存储过程中不被非法修改。

可用性（**A**vailability）：可被授权人正常使用，信息系统在恶劣工作环境下正常运行，系统随时为授权人提供服务。

其他：**真实性**（保证信息是真实可信的，发布者不被冒充，来源不被伪造），**不可抵赖性**（对出现的安全问题提供调查的依据和手段）

# 什么是网络空间安全？

网站

中度可信度描述已自动生成

主要包括新技术安全及应用、应用安全、数据安全、网络与系统安全、物理安全。

物理安全包括环境安全、线路安全、电磁安全、设备安全。

# 什么是网络攻击？

网络攻击是指任何**非授权**的攻击者通过计算机网络**入侵目标系统**的行为，包括查看、偷取、控制、修改、破坏、影响系统正常运行或服务等行为。

# 网络攻击分类

**主动攻击**：攻击者访问其所需信息的故意行为。可能导致某些数据流被篡改或产生虚假的叙述句。合法用户一般能觉察到这种攻击。主要包括**阻断攻击**、**伪造攻击**、**篡改攻击**、**重放攻击**、**拒绝服务攻击**等。

**被动攻击**：攻击者收集信息而不是进行修改，主要通过截取、窃听未经授权的信息，合法用户一般不能觉察到这种攻击。主要包括**窃听**、**流量分析**、**破解加密数据流**等。

**有效攻击**：攻击能对目标系统造成实际影响和后果，攻击者一般提前知晓目标系统存在的安全漏洞，针对其漏洞发起的针对性攻击。主要包括**注入类**、**提权类**、**控制类**等攻击。

**无效攻击**：攻击不对目标系统造成实际影响和后果，攻击者不知晓目标系统的情况，一般通过各种工具进行尝试。如**扫描类**等攻击。

**已知攻击**：攻击者披露或者安全人员披露的攻击行为。已知攻击默认其信息已公布，攻击者和防御者皆可使用。已知攻击模式指已披露的攻击者的攻击策略、攻击方法、攻击路径等。

**未知攻击**：**已知攻击的变种**（产生未知的攻击样本）、**针对新漏洞的攻击行为**（零日攻击）、**新型攻击行为**（未知的攻击方式）、**未知攻击模式**（已知攻击的不同组合模式、未知的攻击模式等）。

**控制窃取**：通过漏洞、后门、钓鱼等入侵系统，用户无感。你能用我也能用。

**损毁擦除**：入侵后通过wiper等途径擦除文件或硬盘，对文件造成损坏。我能用你不能用。

**降效致瘫**：通过过度消耗资源，让正常业务不能使用。我不能用你也不能用。

# 常见的基础攻击

电子邮件钓鱼、密码爆破、端口扫描、SQL注入、水坑攻击等

**勒索攻击**：勒索攻击以邮件、程序牛马、网页挂马的形式进行传播，一旦感染则利用各种加密算法对文件进行加密，被感染者一般无法解密，黑客威胁受害者支付赎金以解锁数据或恢复系统。

**APT攻击**：高级持续性威胁（Advanced Persistent Threat，APT），又叫高级长期威胁，是一种复杂的、持续的网络攻击，包含三个要素：**高级**、**长期**、**威胁**。**高级**是指执行APT攻击需要比传统攻击更高的定制程度和复杂程度，需要花费大量时间和资源来研究确定系统内部的漏洞；**长期**是为了达到特定目的，过程中“放长线”，持续监控目标，对目标保有长期的访问权；**威胁**强调的是人为参与策划的攻击，攻击目标是高价值的组织，攻击一旦得手，往往会给攻击目标造成巨大的经济损失或政治影响，乃至于毁灭性打击。

**DDos攻击**：Distributed Denial of Service，分布式拒绝服务攻击是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击，企图通过大规模互联网流量耗尽攻击目标的网络资源，使目标系统无法进行网络连接、无法提供正常服务。

**僵尸网络**：攻击者利用恶意软件感染的大量计算机，将这些计算机当作傀儡，通过远程发号施令控制这些计算机进行攻击活动。

**蠕虫攻击**：蠕虫是一种可以自我复制的代码，并且通过网络传播，通常无需人为干预就能传播。蠕虫病毒入侵并完全控制一台计算机后，就会把这台机器作为宿主，进而扫描并感染其他计算机。

# 攻击技战术框架

网络杀伤链模型：

目标侦察→武器研制→载荷投递→渗透利用→安装植入→命令控制→任务执行

ATT&CK模型：

Adversarial Tactics, Techniques, and Common Knowledge，对抗战术、技术和公共知识

手机屏幕截图

描述已自动生成

# 身份认证

身份认证就是验证主体真实身份与其所声称身份是否相符的过程。主要有三个方面：

你是谁？指纹、人脸、笔迹、声音、虹膜、DNA等

你有啥？动态口令设备、IC卡、身份证、USB Key等

知道啥？密码、知识、口令等

身份认证就是**确保身份的真实性**，确保操作者的物理身份和数字身份相对应，用于抵御假冒攻击。

对称加密认证：双方都需要知道同一份密钥。A向B出示密钥以证明他是A，B核查A出示的密钥以确认他是A。

非对称加密认证：双方为自己维护一份公钥和一份私钥。公钥对所有人开放，私钥只有自己知道。A向B传递信息时，先用B的公钥进行加密，然后将密文发送给B，B再使用自己的私钥进行解密。

冒充发送：C冒充A向B发送信息。C利用B的公钥加密一段信息并发送给B，B无法知道这段信息来自于C还是A。

此时需要利用A的私钥来对一段信息摘要做加密得到数字签名，B收到加密信息后，利用A的公钥对数字签名进行检验，以此来确定是不是A发送的信息。

冒充公钥：A和B需要交换公钥，如何确保A收到的就是B的公钥？

找可信任的第三方机构（CA）来帮助确认。B向CA申请，CA将B的公钥、证书的有效期、持有者等信息打包成证书，并使用CA的私钥进行签名。A收到证书后，使用CA的公钥验签，从中获取B的公钥。

# 访问控制

访问控制是在保障授权用户能获取所需资源的同时，拒绝非授权用户的安全机制。

一般是针对越权使用资源的防御措施。防止对任何资源进行未授权的访问。

禁止未经授权的使用、泄露、修改、销毁信息以及颁发指令等。包括非法用户进入系统、合法用户对系统资源的非法使用两个方面。

# 防火墙

**包过滤防火墙**：在传输层和网络层对包进行拦截

优点：对分组的IP地址、TCP/UDP协议和端口进行分析，处理速度快，易于配置。

缺点：难以抵御欺骗类攻击；逐包策略检查导致性能急剧下降；无法抵御应用层攻击。

**应用代理防火墙**：在应用层拦截

优点：可以感知和检查应用层行为（举例：可以根据邮箱地址是否属于白名单来拦截，甚至可以根据邮件内容是否包含敏感词来拦截）；安全控制粒度更细；可以针对每条应用流进行分析。

缺点：处理性能低；与应用协议高度相关；对用户不透明（举例：每个应用程序可能都需要自行制定一套防火墙策略）。

**状态检测防火墙**：在会话层拦截

优点：基于会话状态实现访问控制，提高了网络攻击难度；可以基于流指定访问控制策略；兼顾安全与性能。

缺点：安全性不如代理防火墙；无法克服应用协议的多样性

防火墙需要在性能、成本、安全三者之间寻找平衡

防火墙的不足：

防火墙作为网络边界的防护措施，**不能防范来自内部的攻击**；

防火墙**不能防范不通过它的连接**。

防火墙**不能防范利用标准协议缺陷进行的攻击**。

防火墙不能防范数据驱动式攻击。

防火墙不能防范策略配置不当或错误配置引起的安全威胁。

防火墙不能防范本身安全漏洞的威胁；

防火墙可能带来传输延迟、瓶颈及单点失效。

# 入侵检测

入侵检测是从计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象的一种机制。

**异常检测**：以入侵者活动异常于正常主体活动为假设前提，为正常主体构建正常活动的参考库，当其违反统计规律时，认为该活动是入侵行为。

**优点**：可以检测到未知的入侵；可以检测冒用他人账号的行为（异地IP登录）；具有自适应、自学习功能；不需要系统先验知识。

**缺点**：漏报相对低、误报率相对高；统计算法的计算量庞大、效率低；统计点的选取和参考库的建立比较困难。

**误用检测**：首先定义异常系统行为，然后将所有其他行为定义为正常。只有违反异常模式库时才会警告。

**优点**：算法简单、系统开销小、准确率高、效率高

**缺点**：只能检测出已知攻击，新类型的攻击影响大；模式库的建立和维护难，模式库需要不断更新。

HIDS：基于主机的入侵检测

专注于单个机器的系统内部，监视系统的全部或部分行为，检测目标是主机系统和本地用户。主要检测对象是系统日志等。

优点：审计内容全面；视野集中；适用于加密和交换环境。

缺点：影响服务器性能；依赖于审计数据或系统日志准确性和完整性；如果主机数目多，代价太大；不能监控网络上的情况。

NIDS：基于网络的入侵检测

专注于检测网络流量，监控网络关键节点的网络流量，分析数据包内容等。

优点：服务器平台独立性：监视通信流量不影响平台的变化和更新；配置简单；众多攻击标识。

缺点：不能检测不同网段的网络包；很难检测复杂的需要大量计算的攻击；协同工作能力弱；难以处理加密的会话。

# VPN（Virtual Private Network）

VPN的目标是在公用网络基础设施之上构建专用的数据通信网络。

它的核心包括两个部分：**隧道技术**和**加密技术**。

图示

描述已自动生成

本机的所有Internet流量被VPN加密，加密后通过隧道技术套一层IP header，指向VPN服务器，这部分也是加密的。

不同层的实现技术

2层：**PPTP**，L2F，L2TP

3层：**IPSEC**，GRE

4层：**SSL**

**IPSEC**：IP SECURITY

* IPSEC不是一个单独的协议，而是一系列为IP网络提供安全性的协议和服务的集合。
* IPSEC应用于**网络层（名字带”IP”）**，提供数据加密、完整性验证、用户验证和防重放保护。
* 隧道模式：对整个IP报文进行封装和加密，隐蔽源和目的IP地址
* 传输模式：只对IP报文数据载荷进行封装和加密，源和目的IP地址不加密
* AH协议：用于完整性确认、数据来源确认和防重放，不涉及加密。
* ESP协议：用于完整性确认、防重放、加密。
* IKE协议：互联网密钥交换协议。

VPN vs 代理服务器

VPN的安全性更高，因为它提供了设备与VPN服务器之间所有流量的加密，并且保护设备上的所有应用和协议。

代理服务器通常不提供加密，它只会将流量通过另一台服务器转发，只处理特定应用或服务的流量。

VPN的速度可能较慢，因为需要对数据进行加密处理，但现代VPN已经尽可能地减少了这部分工作所需的时间花费。

代理服务器不加密流量，所以理论上它的速度要更快一些。

VPN的匿名性更高，它可以全方面隐藏用户的IP地址并加密流量。

代理服务器可以隐藏IP，但通常不进行加密，匿名性不如VPN。

VPN的配置更复杂，而代理服务器的配置相对更简单，例如对某个应用程序可以直接输入代理地址和端口。

# 什么是数据安全

一方面是数据内容的安全，即使用加密算法、数字水印、监管等技术对数据内容进行保护，如数据保密性、数据完整性、数据认证性、不可否认性、数据非法复制、数据滥用等。

二是数据本身的安全，主要是采用现代信息存储手段对数据本身进行主动防护，如通过数据备份、集中存储、异地容灾等手段保证数据的安全。

常见的备份方式：

本机备份：在本机硬盘的某个位置备份文件

异机备份：将文件备份到与本机分离的存储介质，如U盘、移动硬盘等

活备份：备份到可擦写的存储介质中

死备份：被分到不可擦写的存储介质中

动态备份：利用软件功能定时备份指定文件

静态备份：按照文件进行人工备份

热备份：系统处于正常运转状态下的备份

冷备份：系统处于正常关闭状态下的备份

# 信息隐藏和数字水印的对比

**信息隐藏：**

**载体内容：**无关，一般一对一

**主要用途：**用于保密通信

**前提：**一般不告知有信息隐藏，如果怀疑有信息被隐藏，则已经不安全

**主要攻击：**隐写分析

**主要考核：**不可感知性

**数字水印：**

**载体内容：**有关，一对多

**主要用途：**用于版权标识

**前提：**可以公布有水印存在

**主要攻击：**水印擦除

**主要考核：**安全性

# 隐私保护——K匿名机制

隐私保护阶段：

数据发布、数据存储、数据分析、数据访问

在数据发布时，针对链接攻击提出的一种保护机制。

表格

描述已自动生成

表格

中度可信度描述已自动生成

# 舆情发展阶段

**事件爆发**：某个事件发生并引起了一定的关注度

**信息传播**：相关信息开始在网络上广泛传播，可能引起更广泛的关注度

**舆情形成**：公众开始对该事件产生情绪反应，形成一定的舆论

**舆情演化**：随着时间的推移，舆情可能会有新的变化和发展，公众对事件的态度也可能发生变化

**舆情消退**：事件逐渐淡化，公众的关注度和讨论热度逐渐降低

# 信息技术的安全表现

新技术安全包括助力网络攻击、助力网络防护、内生安全、衍生安全。

以人工智能为例：

符号主义＋安全：符号主义强调知识，记忆的知识错误会出现“指鹿为马”的错误，如果遇到未知的知识也会发生不可预料的错误。

连接主义+安全：对抗攻击，后门攻击，敏感数据窃取、模型参数泄露，数据源干扰攻击

行为主义+安全：机器人自我意识、机器人行为失控

人工智能**助力网络攻击**：

1. 自动化网络攻防：网络超级挑战赛（CGC），参赛队伍全由计算机组成，无人为干预，实时识别系统漏洞、自动完成打补丁和系统防御，最终实现全自动的网络安全攻防。
2. 制作虚假信息内容：DeepFake技术可以生成十分逼真的图像，此类技术用于不良图像、视频制作时，将给社会监管带来极大的难度和挑战。
3. 攻击语音识别：海豚音攻击可以影响智能汽车和智能家居的语音控制系统，通过攻击语音助手，使得被攻击系统可以打开特定的软件和安装特定的软件、实现对汽车和家居系统的远程控制。

人工智能**助力网络防护**：

1. MIT研发人工智能系统AI^2，对日志数据进行测试，与使用无监督学习方法的检测系统相比，AI^2在召回率上平均提高了3.41倍，误报率降低了5倍。

人工智能**衍生安全**：

1. 人工智能系统失误引发安全事故：自动驾驶系统识别物体出错，导致发生交通事故。

人工智能**内生安全**：

1. 人工智能模型及算法缺乏可解释性，存在对抗样本等可造成神经网络出错

# 网络安全态势感知

网络安全态势感知就是在大规模网络环境中，对影响网络态势的安全要素进行察觉获取、理解评估和未来预测。

**“态”**：当前状态，对获得的网络安全信息和事件做评估，确定攻击的真实性，理清攻击类型、性质和危害。

**“势”**：全局的发展趋势，预测未来网络安全事件的演变趋势。

**网络安全态势感知的对象：**

**感知域：**已知（配合）网络的安全态势感知，已知网络资产、拓扑、漏洞和受到的攻击等信息。

**非感知域：**未知（不配合）网络的安全态势感知。

**关键技术：**

1. 态势感知**数据采集**
2. 网络安全**事件检测**
3. 网络安全**状态评估**
4. 网络安全**事件预测与溯源**
5. 网络安全态势**可视化**

# 传统网络安全防御模式

**自卫模式：**以自保为目的的守护防御模式，不断提升自我能力，不在乎攻击者是谁。持续提升网络安全防御能力。基于网络靶场开展系统安全性持续验证与优化。

**缺点：**

新漏洞、新型攻击层出不穷，需要不断提升和巩固，仅依靠自身能力有局限。

内部攻击者、潜藏在系统内的攻击者很难发现。

**护卫模式：**以反击为目的的主动防御模式。采取手段诱导、定位、发现攻击者的存在，在攻击者实施有效攻击之前就将之封杀在萌芽之中。

**盾立方：**自卫模式+护卫模式