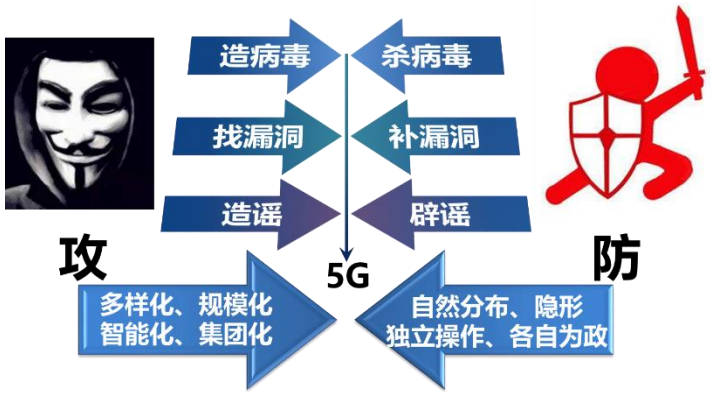
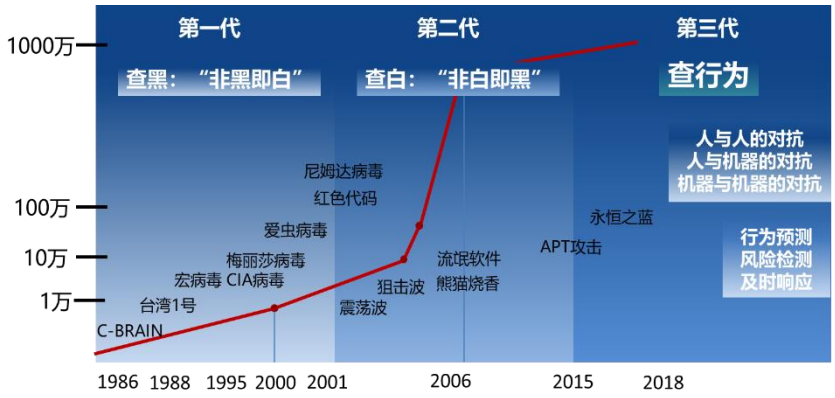
网络安全博弈建模需求与基本模型

引言

- 网络安全攻防对抗的本质是攻击者和防御者之间的攻防策略博弈





- 网络安全的本质是攻防对抗
- 5G环境下网络安全的影响跨越物理域、逻辑域、社会域和认知域，现有的网络安全防御难以有效应对

- 当前网络空间遗留了较多的漏洞，迫切需要系统的理论来支撑[1]。
- 美国也指出网络空间安全缺乏对网络空间安全现象的基本规律、理论以及理论基础模型的科学理解[2]。

Source: 奇安信《新时代、新安全、新发展》报告，2019.06

[1] 英国国家网络安全计划
[2] Pino R E. Network science and cybersecurity[M]. Springer, 2014.

引言

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 网络安全科学研究现状

美国 2011年起设立五年为一期的“联邦网络空间安全研究与发展策略计划”，拟从**经济学和博弈**的角度探索**网络空间安全科学**问题

英国 2011年启动五年为一期的“国家网络安全计划”，研究网络安全威胁和漏洞，提高网络攻击恢复能力

英国 2013年建立网络空间安全科学研究所，伦敦大学学院（UCL）等6所高校从**科学角度**研究网络空间整体安全

美国 2012年安全与隐私科学计划资助建立“网络空间安全实验室”，将网络空间安全研究提升为**网络空间安全科学**

欧洲 5G-PPP组织2015年启动5G-Ensure立项，联合芬兰国家技术研究中心等18家研究机构，旨在构建5G安全迭代愿景

中国 2016年科技部启动国家重点研发计划“网络空间安全” 重点专项

欧美等信息大国已初步开始了从科学角度建立和发展网络空间安全理论的探索

引言

- 网络空间安全——攻击者与防御者之间的攻防策略交互
- 博弈论为各种网络攻防的信息结构、参与者、行为和持续时间提供了一种定量的分析框架
- 基于博弈论建立安全科学：博弈论作为一门系统科学，可建模防御欺骗的本质、可转移性和普遍性
- 适当的博弈模型分析不同的网络攻防——识别各种攻防特征并采用合适的博弈模型来刻画此特征

第一节：网络空间安全攻击

- 攻击：试图破坏计算机或通信网络的机密性、完整性和可用性，或获得（部分）控制权的网络活动

Security Service	Sample Threats and Attacks
Confidentiality	information theft, unauthorized access, identity theft, stealing corporate secrets
Integrity	altering websites, compromising data, implanting backdoors and trojans
Availability	denial-of-service (DoS) attacks
Control	(partial) control of system, e.g. account and root access

❖攻击方法

➢ 基于物理和硬件的攻击方法

- impersonating computer technicians and carrying away sensitive hardware, or by an employee of a government organization forgetting disks with valuable information in a train on the way home, or by a disgruntled employee stealing the entire customer database of a multinational company stored on a simple CD.
- Encryption of sensitive information on hard disks and other storage media is strongly recommended uniformly by all security experts

➢ 基于软件的方法

- exploiting vulnerabilities in software：the interconnected nature of networks, especially the Internet, increases the number of potential attackers by orders of magnitude when compared to physical attacks
- virus, worm, and trojan without distinction under the umbrella of malware (malicious software).

❖ 攻击方法（续）

➢ 基于

- man-
- interc
- their
- crypt
- can b
- Physi

➢ 基于

- Soci
- Argu

he attacker
ties without
thentication
n

REQUEST FOR URGENT BUSINESS RELATIONSHIP

I am making this contact with you on behalf of my colleagues after a satisfactory information we gathered from an international business directory.

My colleagues and I are members of the Contractor Review Committee of the Nambutu National Petroleum Corporation (NNPC). I have been mandated by my colleagues to look for a trustworthy company/individual into whose account some funds is to be transferred. The funds in question is $25.5M (twenty five million, five hundred thousand US dollars) now in a dedicated account with the Central Bank of Nambutu (CBN). The above funds arose from the over-invoicing of some supplies and oil drilling works which have been executed and concluded. The fund is therefore free to be transferred overseas.

The underlisted shall be required from you immediately by fax:- **the beneficiary's name and confidential telephone and fax numbers, the full name and address of company/beneficiary**. All necessary particulars of the bank account where you wish the contract sum to be transferred (**account number, bank address, the telephone, fax and telex numbers of the bank**).

Immediately we receive the requested information from you, we shall put up an application for fund & transfer to the appropriate ministries and departments in favor of the beneficiary (you or your company).

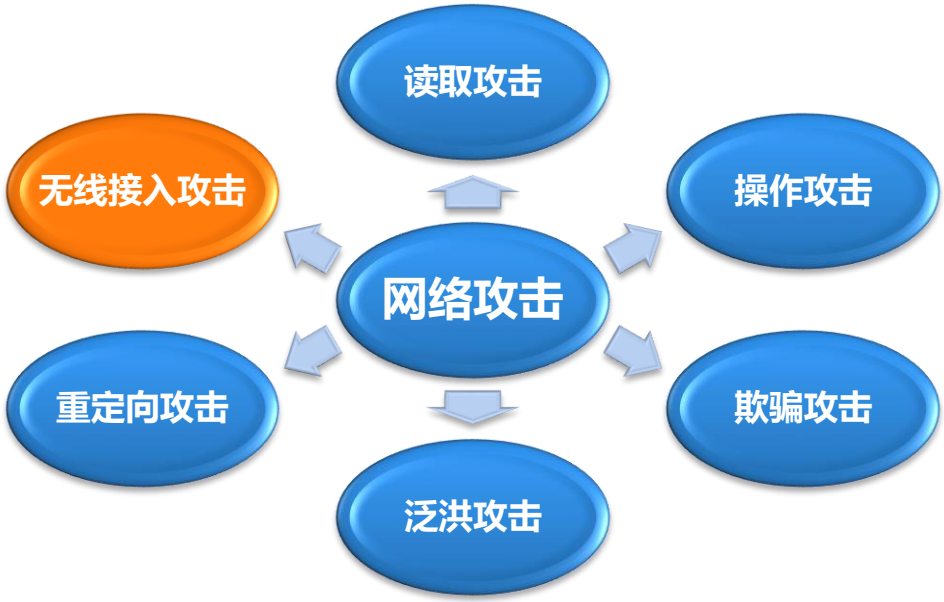
Please, we implore you to treat this deal with utmost confidentiality. As civil servants, we would not want any exposure. Do not go through the international telephone operator when lines are busy. Always dial direct.

Thanks for your anticipated co-operation.
Best regards,
XXX

第一节：网络空间安全攻击

❖ 网络安全攻击分类

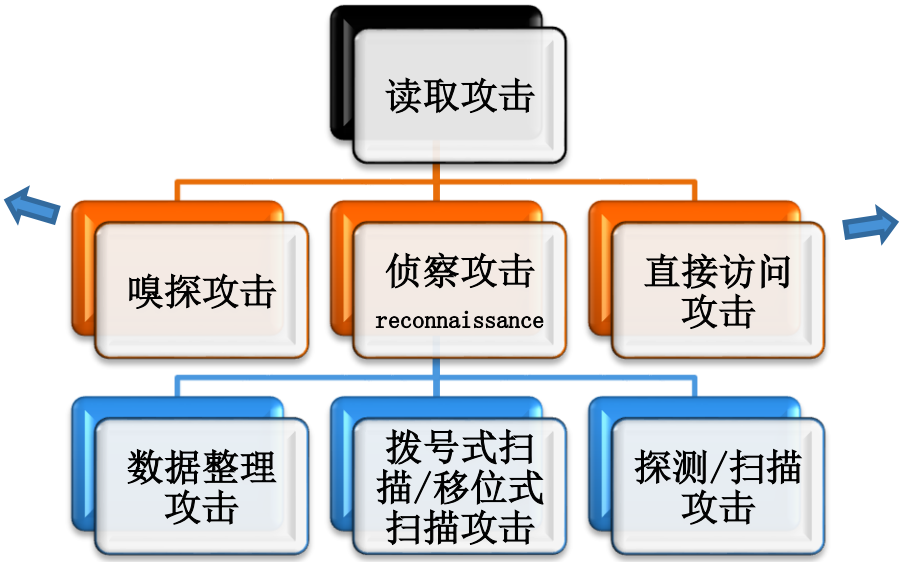
- 主动攻击：攻击者访问其所需要信息的故意行为，主动地做不利于网络主体的事情，比如远程登录到指定机器的端口查看/篡改信息
- 被动攻击：收集信息而不是进行访问，数据的合法用户一点也不会察觉到这种活动。被动攻击包括嗅探、欺骗等攻击方法



❖ 读取攻击：从被攻击者处获取信息的相关攻击

- 获取组织结构的ip地址，在地址范围内进行端口扫描和漏洞弱点扫描，入侵有弱点的主机并获取信息

- 读取信息获得情报，使攻击者了解目标系统
- 受嗅探信息须以明文而不是密文的形式发送
- 攻击信息：认证信息、网络管理信息、机密事务等
- 工具：ethereal，wireshark等
- 嗅探也是一种极好的故障排查工具



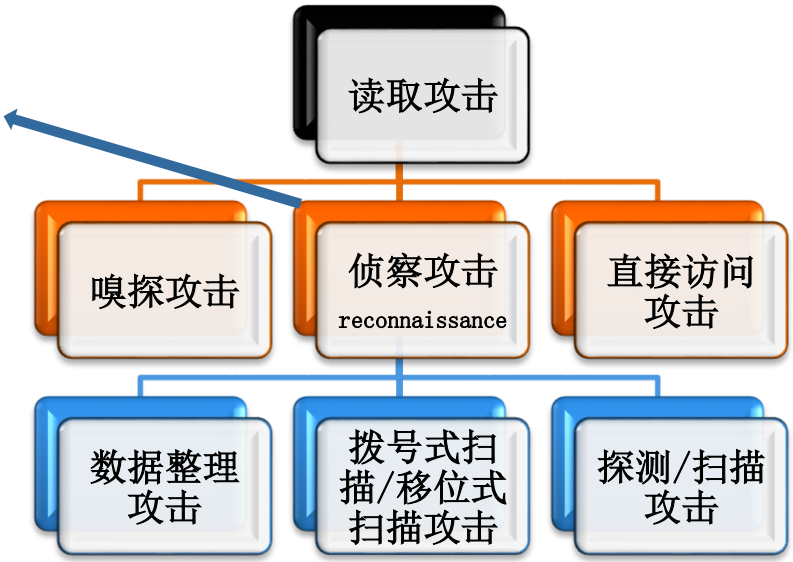
- 包含攻击者试图直接访问网络资源的所有攻击
- 攻击者穿越防火墙后，利用直接访问攻击登录到曾受防火墙保护的系统中，就可以发起不限次数的其他攻击，最常见的是操纵攻击

第一节：网络空间安全攻击

❖ 读取攻击：从被攻击者处获取信息的相关攻击

- 获取组织结构的ip地址，在地址范围内进行端口扫描和漏洞弱点扫描，入侵有弱点的主机并获取信息

- 攻击者事先汇集目标的信息，侦察攻击可采用主动方法和被动方法，成功的侦察攻击可以提高后续攻击的成功。



- 所有对网络攻击的第1步，通常采用**whois**、**Finger**等工具和**DNS**、**LDAP**等协议获取目标的一些信息，如域名、IP地址、网络拓扑结构、相关的用户信息等

- 扫描攻击包括地址扫描和端口扫描等，通常采用**ping**命令和各种端口扫描工具，获得目标计算机的一些有用信息，例如机器上打开了哪些端口，这样就知道开设了哪些服务，从而为进一步的入侵打下基础。

第一节：网络空间安全攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 操作攻击：在 OSI 模型的某层对数据进行操作的攻击

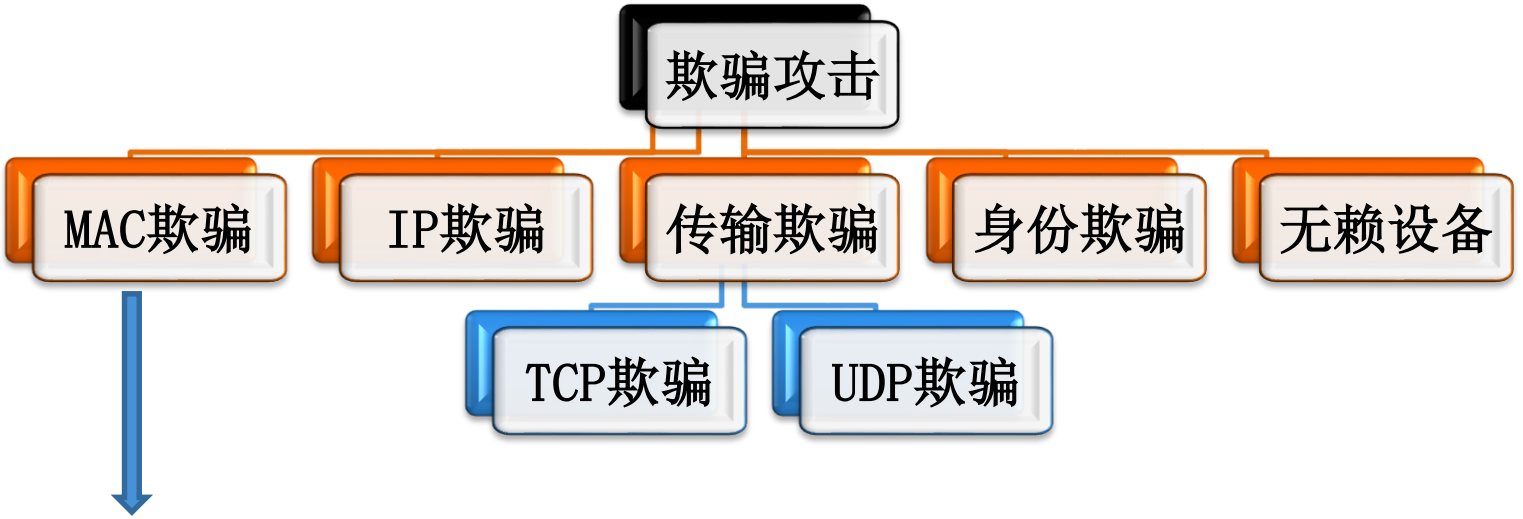
- 网络操纵
  - IP 分片攻击，对流量进行蓄意分片，以绕过基于网络（IDS 或防火墙）或基于应用程序的安全控制。Fragroute工具
  - 源路由攻击，攻击者利用源路由选择在网络中选择攻击路径。可以利用 IP、TCP 和UDP 协议进行攻击。
  - 除了第 3 层和第4 层操纵，攻击者还可以修改第2 层信息，进行虚拟LAN 跳转或其它本地网络攻击的目的。
- 应用程序操作
  - 在应用层执行的攻击，主要利用应用程序设计或实施方案中的缺陷，典型攻击：缓冲区溢出攻击

OSI 层	功能	TCP/IP 协议
应用层(Application layer)	文件传输，电子邮件，数据加密	TFTP，HTTP，SNMP，
会话层(Session layer)	的联系	没有协议
传输层(Transport layer)	提供端对端的接口	TCP，UDP
网络层(Network layer)		IP，ICMP，RIP，OSPF，BGP，IGMP
数据链路层(Data link layer)	传输有地址的帧，错误检测功能	SLIP，CSLIP，PPP，ARP，RARP，MTU
物理层(Physical layer)	以二进制数据形式在物理媒体上传输数据	ISO2110，IEEE802，IEEE802.2

- 操作攻击：在 OSI 模型的某层对数据进行操作的攻击
  - 应用程序操作（续）
    - 缓冲区溢出是应用程序弱点的表现，应用程序开发人员未对应用程序所占用的内存地址作足够的绑定检查时会发生缓冲溢出
    - 往程序的缓冲区写超过其长度的内容，造成缓冲区的溢出，破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的
    - 存在于各种操作系统、应用软件，通过缓冲区溢出进行的攻击占所有系统攻击总数的**80%**以上
    - 导致程序运行失败、系统死机、重新启动等后果，可以利用他执行非授权的指令，甚至可以取得系统特权，进而进行各种非法操作。
    - 例如：如果弱点的应用程序是以**root** 身份运行的，成功的缓冲区溢出攻击通常会导致攻击者获得**root** 权限。

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

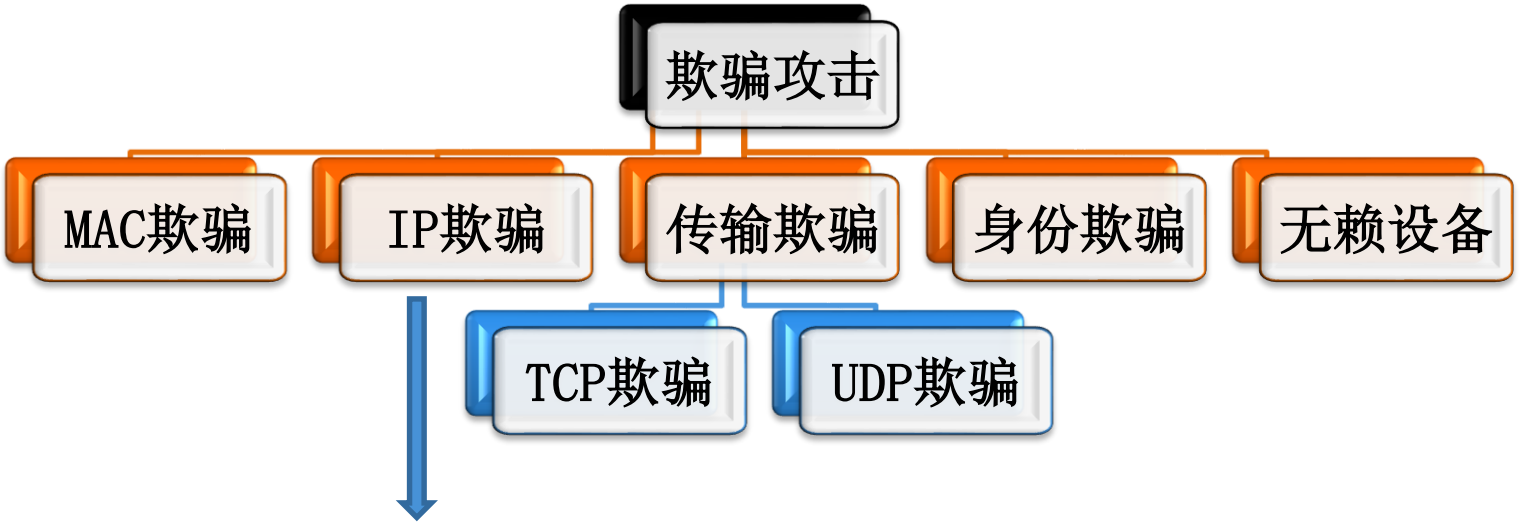
- 欺骗攻击：导致用户或系统中的设备认为信息是来自于实际上未发出该信息的来源的攻击



- 攻击者将自己的 **MAC** 地址改为受信任系统的地址，在以太网环境中，交换机上的**CAM** 表可以跟踪**MAC** 地址、**VLAN** 和**MAC** 地址所连接的端口，攻击者将目标**MAC** 地址改为另一个与交换机相连的系统的地址时，**CAM** 表将得到更新，交换机主认为某台机器从一个位置移动到另一个位置。前往目标**MAC** 地址的流量都会发送给攻击者。**MAC**欺骗非常适合于只接收数据而不主动发送数据的系统

第一节：网络空间安全攻击

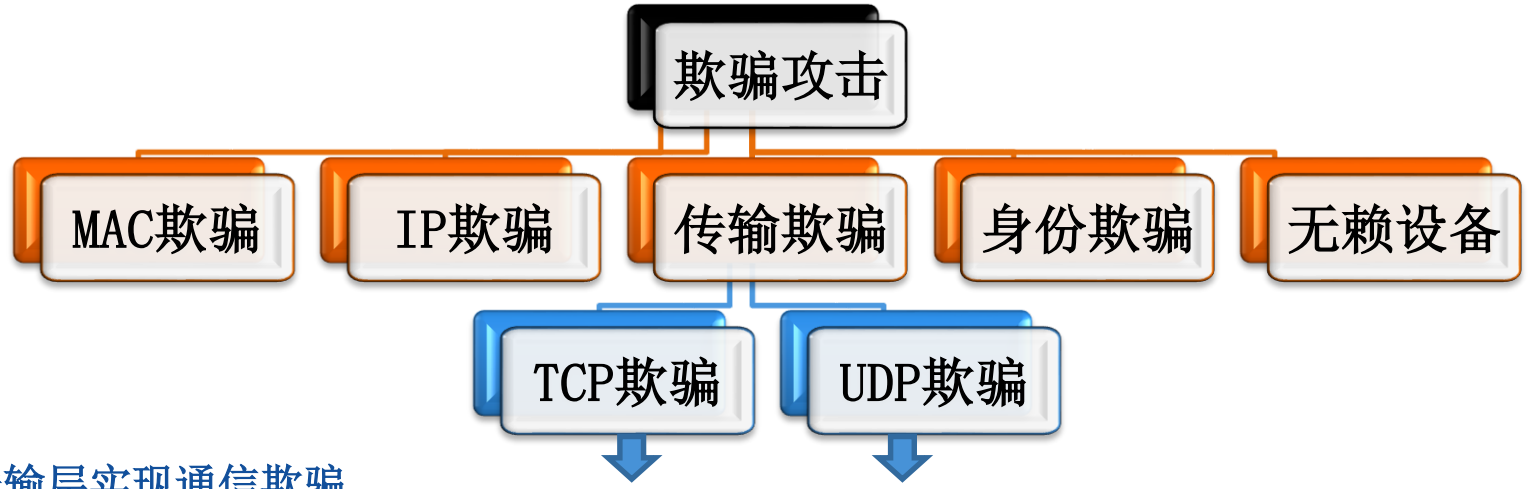
- 欺骗攻击：导致用户或系统中的设备认为信息是来自于实际上未发出该信息的来源的攻击



- 攻击者伪装成被信任的IP地址来获取目标的信任。主要针对防火墙的IP包过滤以及LINUX/UNIX下建立IP地址信任关系的主机实施欺骗。
- 攻击者进入系统的原始数据包驱动器中就可以发送带有 IP 报头的数据包。加密机制只有在需要加密通信以访问 IP层的系统中才能用作保护机制，
- 例如，采用IPSec进行通信的金融应用程序不会接受任何主机的原始IP连接，无论是合法的还是假冒的，这种加密系统概念也适合于传输欺骗。

第一节：网络空间安全攻击

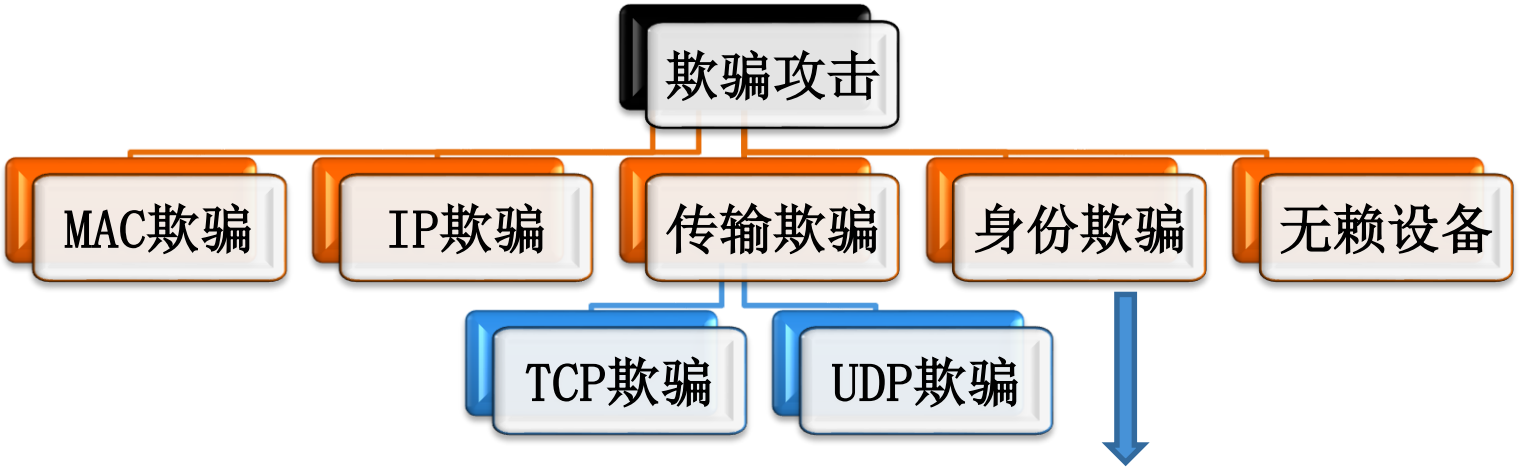
- 欺骗攻击：导致用户或系统中的设备认为信息是来自于实际上未发出该信息的来源的攻击



- 传输层实现通信欺骗
- **UDP欺骗：UDP报头结构简单，是系统安全中最薄弱的环节。SNMP、syslog、TFTP等管理应用程序都使用UDP作为其传输机制。**
- **TCP欺骗：TCP协议是面向连接的协议，TCP协议中的32bit序列号是特定于连接的，该序列在操作系统中是伪随机的，很难预测。攻击者通过在真正的客户机与服务器之间通过认证后插入会话来伪装成受信任的客户机。在攻击者无法看到客户机与服务器之间交换数据包的情况下，此类攻击非常难以实现，但是一旦从客户机与服务器之间的路径上的位置发起攻击时，其破坏力极大。**

第一节：网络空间安全攻击

- 欺骗攻击：导致用户或系统中的设备认为信息是来自于实际上未发出该信息的来源的攻击



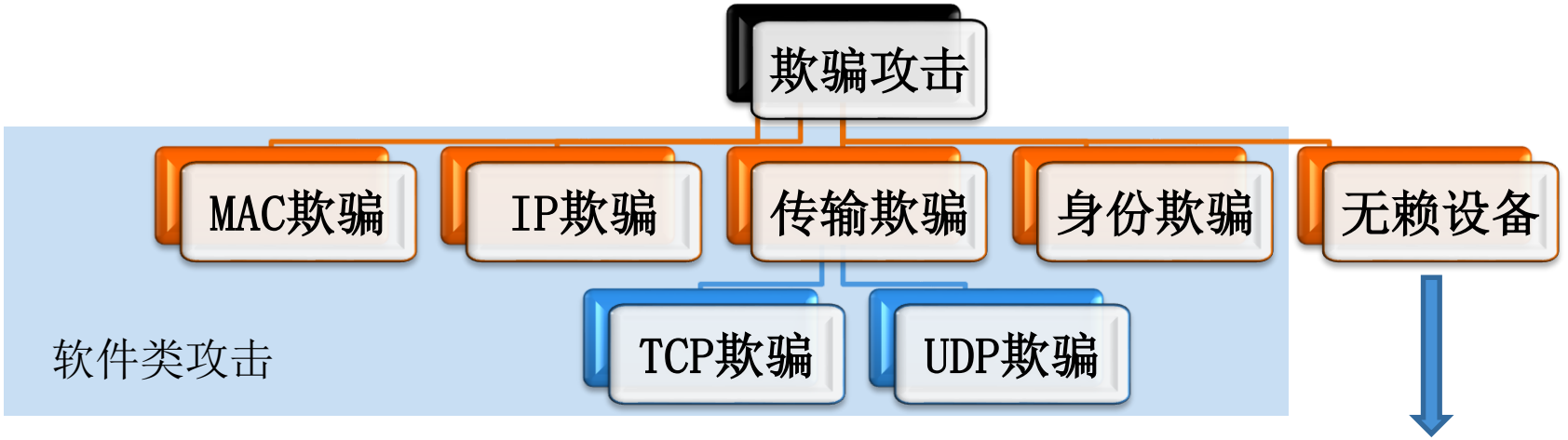
- 身份欺骗包含密码破解、暴力登录尝试、数字证书偷窃和伪造等方式。身份验证机制可由下列方法实现：
- 1）明文用户名和口令（telnet）
- 2）预共享密钥（WEP）
- 3）经过加密的用户和口令（SSH）
- 4）一次性口令（OTP）
- 5）公钥加密系统（PGP、IPSec）

最不安全

最安全

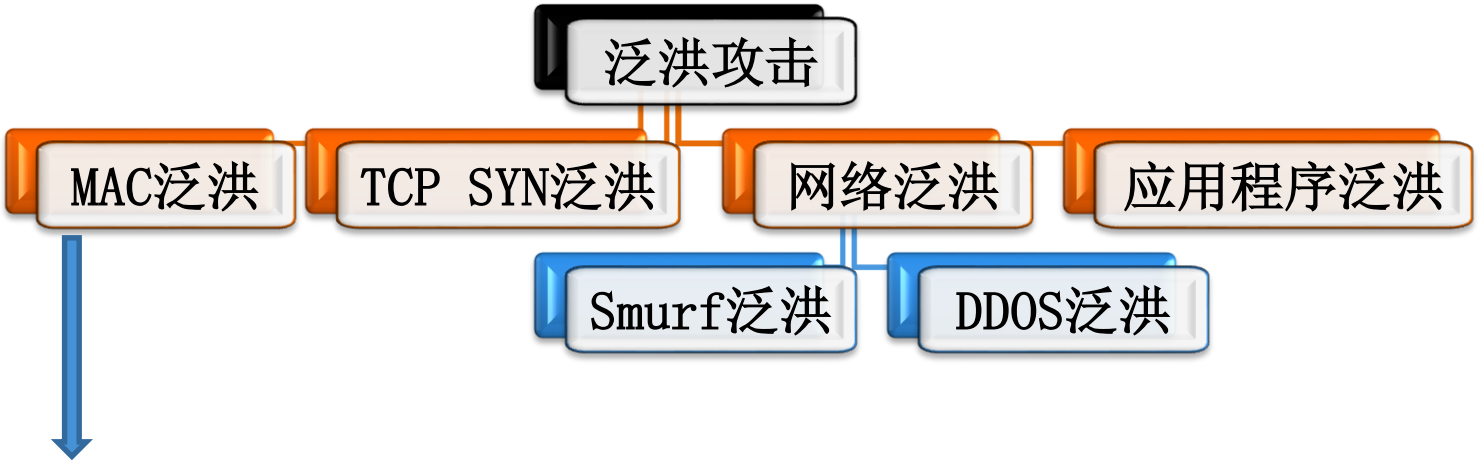
第一节：网络空间安全攻击

- 欺骗攻击：导致用户或系统中的设备认为信息是来自于实际上未发出该信息的来源的攻击



- 将无赖设备添加到网络中，使设备成为合法的身份进行攻击。例如DHCP 攻击
- 无赖设备在网络中确定IP寻址方案，搜索HTTP代理服务器，创建一条隧道式连接与攻击者相连。使远程攻击者以本地用户身份出现发起攻击
- 无赖设备攻击需要攻击者实际接触到目标网络

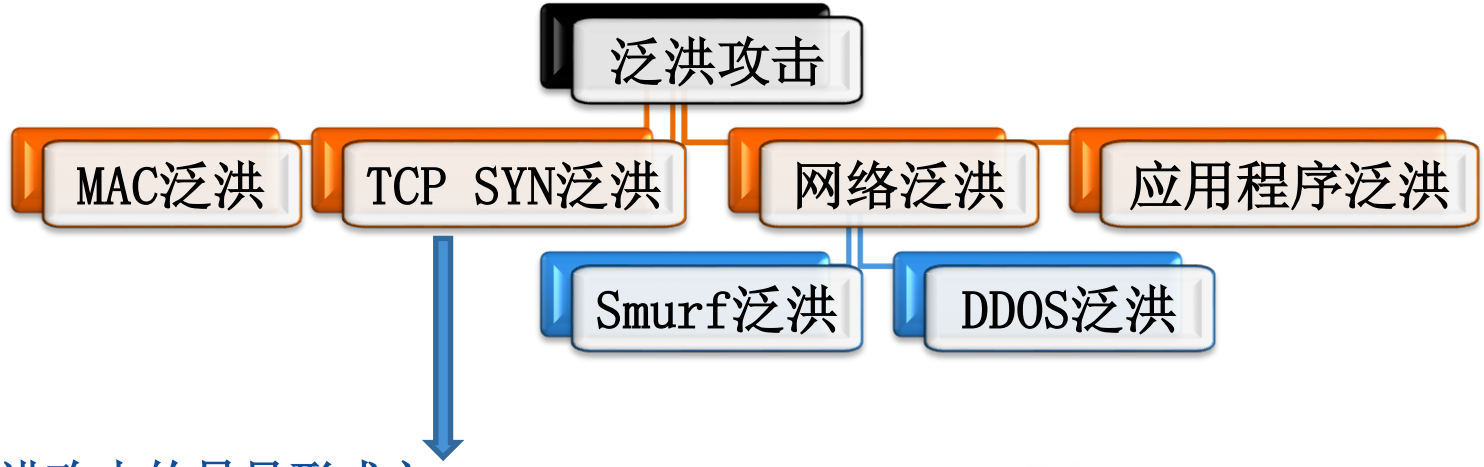
❖ 泛洪攻击：向某些网络资源发送过量的数据的攻击



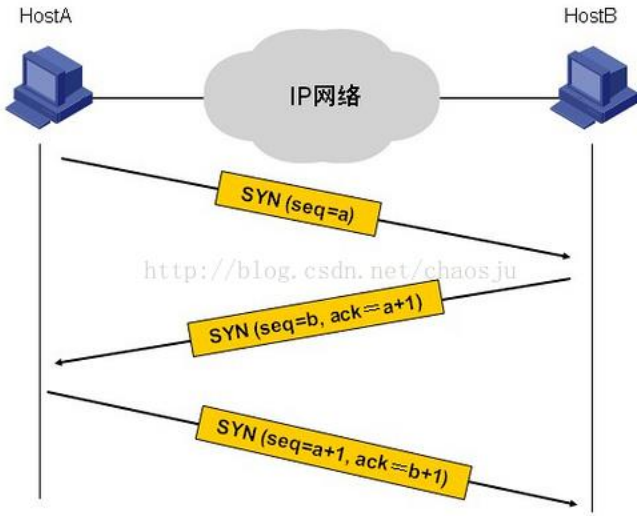
- 以假冒的源 MAC地址和目的地址将数据包从攻击者的系统发送到以太网链路上，用于占领MAC地址在CAM上的位置，由于CAM表容有限，当CAM填满后，其它主机就只能在本地LAN上进行泛洪，使攻击者可以对这些帧进行嗅探

第一节：网络空间安全攻击

❖ 泛洪攻击：向某些网络资源发送过量的数据的攻击

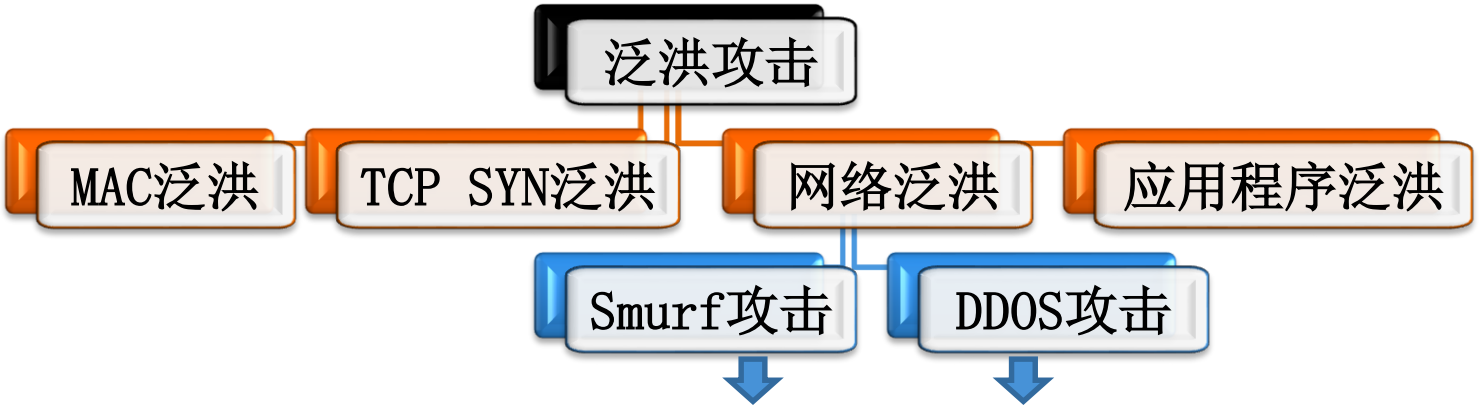


- 泛洪攻击的最早形式之一
- 发送一个**TCP SYN**数据包，不对其响应送回的**SYN-ACK** 确认，收到**SYN** 数据包的服务器将一直将边接保持开放状态，服务器还会定期重新发送**SYN-ACK**数据包，在拆除连接之前，默认情况下最多发**4** 次。攻击者发起 **TCP SYN** 泛洪攻击时，会向某个系统发出数千个连接请求，以耗尽服务器的所有可用内存，这会使用服务器崩溃。



第一节：网络空间安全攻击

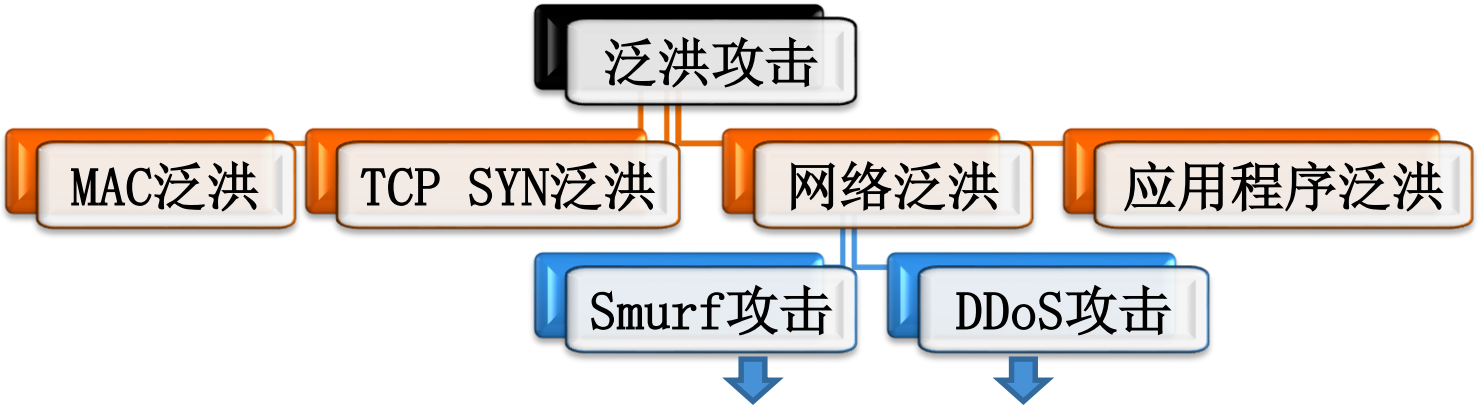
❖ 泛洪攻击：向某些网络资源发送过量的数据的攻击



- 针对网络的**internet**链路设计的消耗网络链路可用带宽的攻击
- **Smurf** 攻击：发送**ICMP**应答请求包，目的地址设为受害网络的广播地址，最终导致该网络的所有主机都对此**ICMP**应答请求做出答复，导致网络阻塞。如果将源地址改为第三方的受害者，最终将导致第三方崩溃。若攻击者向包含**100** 台主机的的网络发出**768kbit/s**的广播**ping**数据，当回程流量发送到受攻击网络中时，这将变成**76.8Mbit/s**的数据流，回弹的网络越大增幅就越大
- 路由器上使用命令**no IP directed-broadcast**可以阻止网络成为**smurf**攻击的源头

第一节：网络空间安全攻击

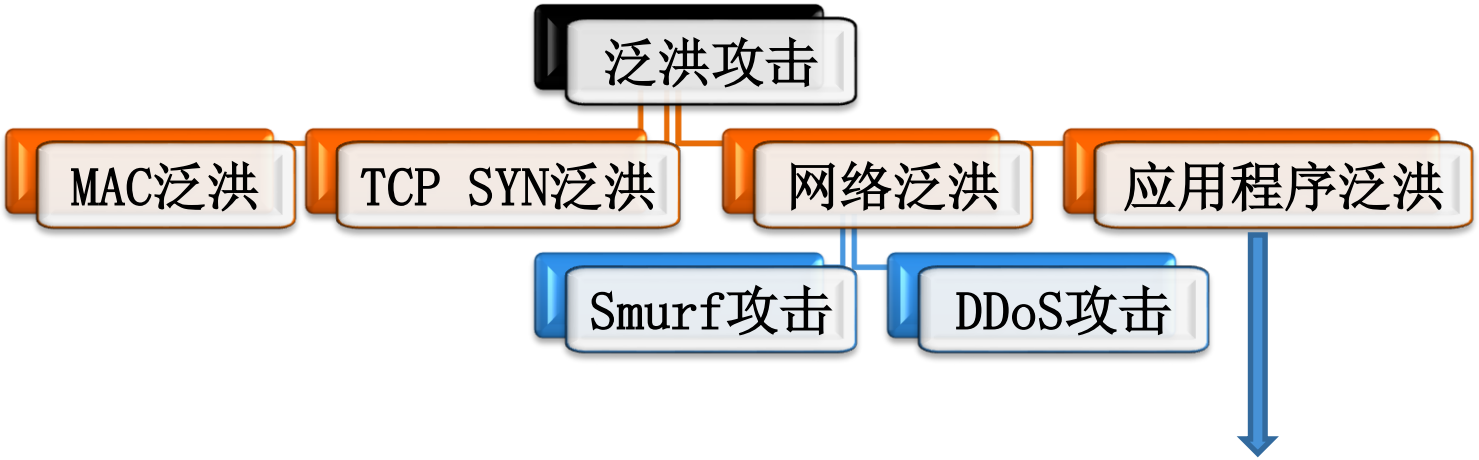
❖ 泛洪攻击：向某些网络资源发送过量的数据的攻击



- DDoS攻击：基于DOS的特殊形式的拒绝服务攻击，是一种分布协作的大规模攻击，利用一批受控制的机器向一台目标机器发起攻击，破坏性巨大
- 1)攻击者侵入系统，将DDoS主探系统软件安装在系统中
- 2)主探系统感染internet部分，受感染的系统成为其代理系统
- 3)攻击者伺机将攻击指令发送给主控系统，主控系统操纵代理系统，对某个IP地址进行泛洪攻击
- 4)受攻击的网络将淹没在假冒的网络流量中，合法请求得到处理的可能性极小

第一节：网络空间安全攻击

❖ 泛洪攻击：向某些网络资源发送过量的数据的攻击



- 消耗应用程序或系统资源的攻击，最常见的应用程序泛洪是垃圾邮件
- 包括在服务器上持续运行CPU密集型应用程序，利用持续不断的认证请求对服务器进行泛洪攻击。

第一节：网络空间安全攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 无线接入攻击：针对无线接入网/无线信号的攻击
  - 窃听（eavesdropping）：主动/被动截取无线保密信号
  - 干扰（jamming）：发送噪声信号干扰合法信号接收
  - 导频欺骗（Pilot spoofing）：在导频训练阶段发送合法终端相同的导频序列，让合法发送端认为攻击者为其通信对端，从而实现身份伪装、信息伪造/篡改（Messages falsification/tamper）。例如不可信中继可以篡改或伪造中继信号
- 物理层认证技术、物理层密钥技术、安全信道编码、安全空口技术（安全MIMO、安全中继等）

第一节：网络空间安全攻击

❖攻击者：

to personalize and abstract people with malicious intent, who try to compromise confidentiality, integrity, availability, or control of a computer network without its owner's consent or knowledge

Actor	Description
Script Kiddie	often young, no sophisticated skills, motivated by fame
'Black hat' hacker	semi-professional, criminal intent, sophisticated attack tools and programs
Cracker	modifies software to remove protection
Malicious user	inside organization, criminal intent
Malicious sysadmin	control of network, criminal intent, potentially significant damage

第一节：网络空间安全攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

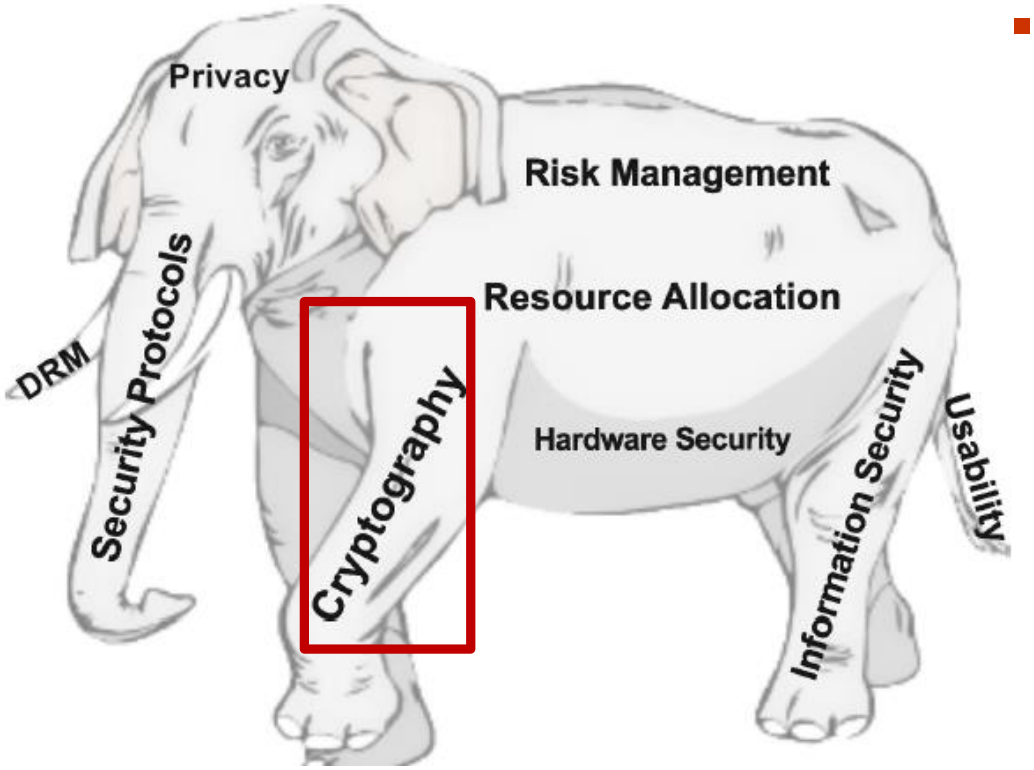
❖防御者：

- 保护网络和系统安全的任务完全在于系统管理员
- 从防御的角度来看，网络安全的一个主要问题是**缺乏动力**，这在一定程度上源于难以量化网络安全增加的价值
- 目前还没有如何评估和量化网络安全的相关标准。缺乏量化自然会影响有关防御者的决策过程

❖防御机制

- 防火墙：检查通过它们的网络流量并过滤可疑数据包，通常基于分析其属性的规则集。通过调节传入和传出流量，防火墙在网络中和网络之间保持独立的信任区域。
- 入侵检测和预防系统（Intrusion detection and prevention systems）：检测并防止针对网络系统的攻击
- 反病毒软件：识别和删除各种恶意软件，包括病毒。定期扫描存储介质和内存，寻找恶意软件的迹象并删除。

第一节：网络空间安全攻击

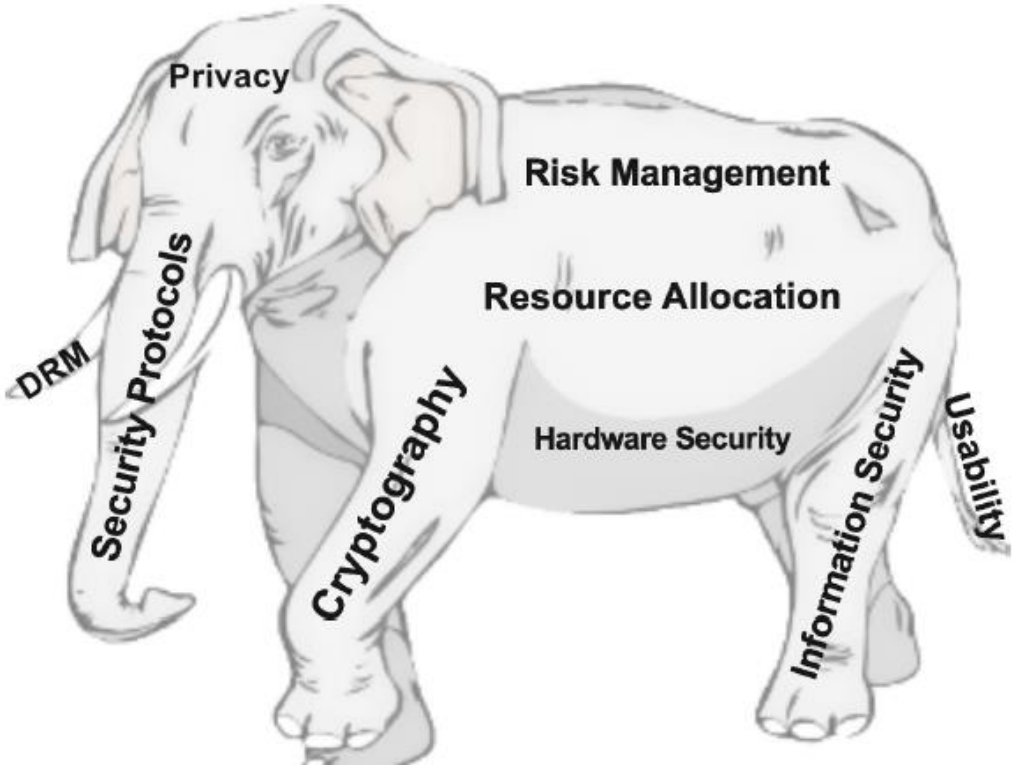


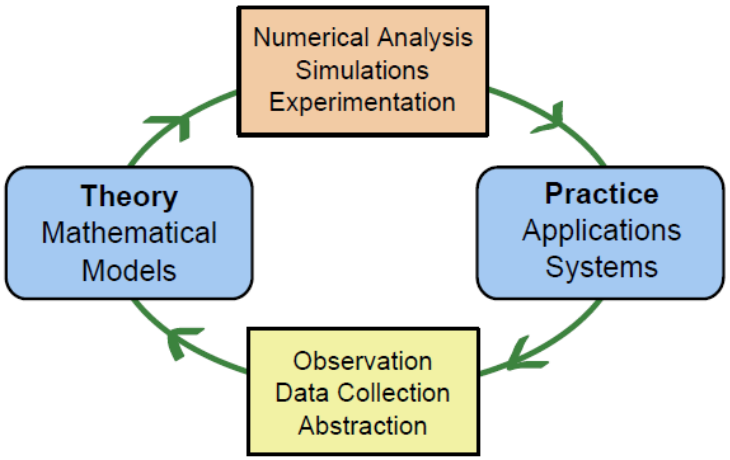
- 加密：隐藏信息
  - 保密: 确保消息内容除预期接收者外是保密的
  - 完整: 向接收者保证接收到的消息没有被改变
  - 认证: 证明身份的过程
  - 不可否认: 确保发送者确实发送了消息

- 密钥加密（经典的密码学），密钥用于加密和解密
- 公钥密码术，其中一个密钥用于加密，另一个用于解密
- 哈希函数：从给定的数据中计算一个固定大小的位字符串，即哈希值，这样数据中的变化肯定会改变散列值。因此，它们确保了完整性。

第一节：网络空间安全攻击

- 网络安全技术——盲人摸象，注重微观的技术细节，缺乏理论的指导





第二节：博弈模型分类

- 博弈论建立网络安全攻防定量分析框架的优势
  - 基于数学证明的安全：传统安全方法依赖于要么在预防性设备（如防火墙）中实现，要么在反应性设备（如反病毒程序）中实现，针对单次事件的防御
  - 可靠的防御：基于数学分析结果可以设计健壮可靠的网络系统设计防御机制抵御恶意用户/节点的自私行为（或攻击）

第二节：博弈模型分类

- 博弈论建立网络安全攻防定量分析框架的优势（续）
  - 及时行动：传统安全方法缺乏参与者的激励机制，对抗速度相当缓慢，博弈论方法使用潜在激励机制来分配有限资源，感知风险
  - 分布式防御方案：传统防御方法采用集中式判决，但现实网络中由于缺乏集中协调者，很难实现集中式的防御，博弈方法可以以个体利益为目标，实现分布式防御

第二节：博弈模型分类

- 采用博弈论建立攻防分析需注意的问题
  - 合理性：博弈建模重点在于均衡策略分析，实际系统中有限的信息/资源导致攻防双方很难采取最佳响应效果的行动，因此需要适当的行为预测理论。此外，多均衡点存在情况下的参与者很难达到一致的策略选择
  - 多层防御：一般研究下，防御者采取某一特定的防御机制，实际场景下防御者会同时采取多层防御，如何建模多层防御下的博弈模型？

第二节：博弈模型分类

- 采用博弈论建立攻防分析需注意的问题（续）
  - 可实现性：实际攻防场景下，攻击者和防御者在做攻防决策时通常会考虑许多不确定但真是存在的因素，如网络中有多少的流量，信噪比如何，节点功率如何等等。实际环境中防御者不可能完美的观测到这些信息，因此防御者需要有分析和观测环境改变的能力。此外，已有的博弈建模大多基于两个用户博弈，这一假设只有在多个攻击者/防御者有相同的策略和回报时才成立，实际系统中由于攻击者/防御者策略和回报的差异性，两用户博弈可能不成立。

填空题 3分

设置

北京郵電大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《孙子兵法》的精髓包括 [填空1] 、 [填空2] 、 [填空3]

正常使用填空题需3.0以上版本雨课堂

作答

填空题 4分

设置

北京郵電大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

完整的博弈通常包含的构成要素有 [填空1] 、 [填空2] 、 [填空3] 、 [填空4]

正常使用填空题需3.0以上版本雨课堂

作答

第二节：博弈模型分类

- 博弈论：研究多个个体或团队之间在特定条件制约下的对局中利用相关方的策略，而实施对应策略的学科
- 根据博弈参与者能否达成相互合作的约束性协议
  - 合作博弈 VS 非合作博弈
    - 区别在于相互发生作用的当事人之间有没有一个具有约束力的协议，如果有，就是合作博弈，如果没有，就是非合作博弈。
  - 静态博弈 VS 动态博弈
    - 静态博弈：博弈中参与人同时选择或虽非同时选择但后行动者并不知道先行动者采取了什么具体行动——囚徒困境（不完美博弈）
    - 动态博弈：博弈中参与人的行动有先后顺序，且后行动者能够观察到先行动者所选择的行动——棋牌类游戏

第二节：博弈模型分类

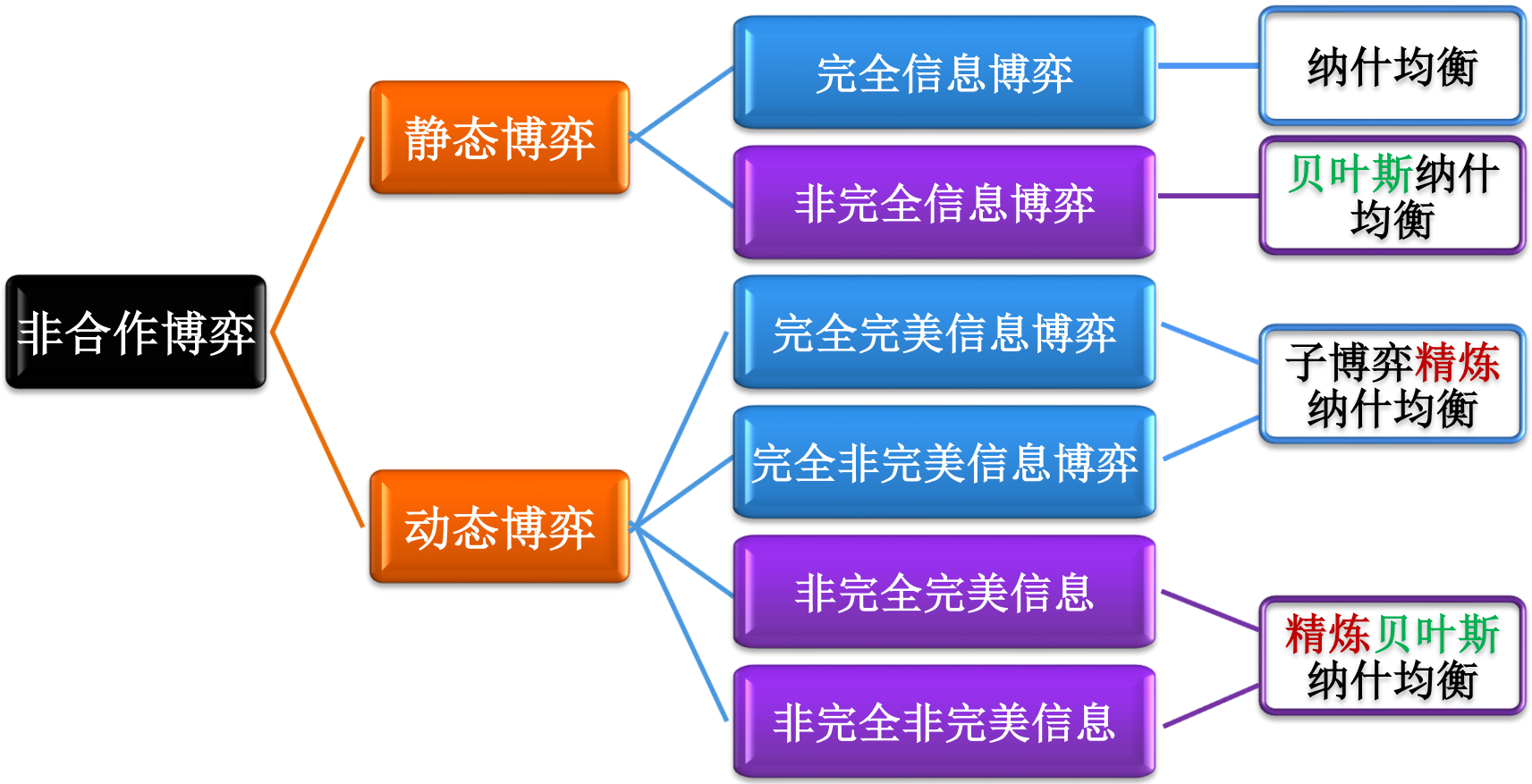
北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 根据博弈参与者能否达成相互合作的和约束性协议（续）
  - 合作博弈 **VS** 非合作博弈
  - 静态博弈 **VS** 动态博弈
  - 完美（**Perfect**）信息博弈 **VS** 不完美信息博弈
    - 完美：每个参与者都知道所有其他参与者所采取的行动（**action**），例如棋牌类游戏
    - 不完美：至少一个参与者不知道至少一个其他参与者的采取的行动，静态博弈都是不完美的

第二节：博弈模型分类

- 根据博弈参与者能否达成相互合作的和约束性协议（续）
  - 合作博弈 VS 非合作博弈
  - 静态博弈 VS 动态博弈
  - 完美（Perfect）信息博弈 VS 不完美信息博弈
  - 完全（complete）信息博弈 VS 不完全信息博弈
    - 完全：每个参与者都知道所有其他参与者的策略（strategy）和回报函数（payoff），不考虑每个参与者已经采取的行动（action）
    - 不完全：至少一个参与者不知道至少一个其他参与者的策略或收益函数

第二节：博弈模型分类


非合作博弈
静态博弈
动态博弈
完全信息博弈
非完全信息博弈
完全完美信息博弈
完全非完美信息博弈
非完全完美信息
非完全非完美信息
纳什均衡
贝叶斯纳什均衡
子博弈精炼纳什均衡
精炼贝叶斯纳什均衡

第三节：非合作博弈之静态博弈

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 完全信息静态博弈

- 纳什均衡：在一种策略组合上，其他参与者不改变策略时，某参与者就不会改变策略，因为目前状态最优——囚徒困境

甲 \ 乙	坦白	不坦白
坦白	5，5	1，10
不坦白	10，1	2，2

  - 纳什均衡：双方参与者都选择坦白，结果二人同样服刑5年
  - 无论甲坦白与否，乙的最优策略都是坦白
  - 无论乙坦白与否，甲的最优策略也都是坦白

——占优战略均衡

- 占优战略均衡：占优策略就是指无论竞争对手如何反应都属于本企业最佳选择的竞争策略——智猪博弈

第三节：非合作博弈之静态博弈

❖ 不完全信息静态博弈

- 参与人的支付函数不清楚。支付函数不是共同知识，参与人不知道在与谁博弈，博弈的规则没有定义。
- 海萨尼转换——引入一个虚拟参与人“自然”。自然首先行动，决定每个参与人特征。每个参与人知道自己特征，但不知道别人特征。此方法将不完全信息静态博弈变成一个两阶段动态博弈，第一个阶段是自然N的行动选择，第二阶段是除N外的参与人的静态博弈。该转换把“不完全信息”转变成为“完全但不完美”信息，可以用分析完全信息博弈的方法进行分析。“不完美信息”指：“自然”作出了它的选择，但其他参与人并不知道它的具体选择是什么，仅知道各种选择的概率分布——贝叶斯纳什均衡

第三节：非合作博弈之静态博弈

❖ 不完全信息静态博弈

- 贝叶斯纳什均衡——参与人同时行动，没有机会观察到别人的选择。
  - 给定其他参与人的战略选择，每个参与人的最优战略依赖于自己的类型。每个参与人仅知道其他参与人有关类型的分布概率，而不知道其真实类型，因此不可能知道其他参与人实际上会选择什么战略。但是可以正确地预测其他参与人的选择与其各自的有关类型之间的关系。
  - 因此，该参与人的决策目标就是：在给定自己的类型以及其他参与人的类型与战略选择之间关系的条件下，使得自己的期望效用最大化。
- 贝叶斯纳什均衡是一种类型依赖型战略组合。在给定自己的类型和其他参与人类型的分布概率的条件下，这种战略组合使得每个参与人的期望效用达到了最大化。

第四节：非合作博弈之动态博弈

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 完全信息动态博弈

- 完美信息动态博弈——行动顺序发生；下一步行动之前所有以前的行动都可以被观察到；每一可能的行动组合下参与者的收益是共同知识
- **Stackelberg博弈**
  - 双寡头模型：两个参与者分别是**leader**和**follower**，进行的是数量竞争。**leader**先行选择产量，**follower**观察到**leader**的选择后再作选择。参与者地位的不对称引起决策次序的不对称
  - **Follower**对**leader**的最优反应

$$R_2(q_1) = \max_{q_2} U(q_1, q_2)$$

  - **Leader**的问题变成

$$\max_{q_1} U(q_1, R_2(q_1))$$

逆向归纳法

$$(q_1^*, R_2(q_1^*))$$

第四节：非合作博弈之动态博弈

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 完全信息动态博弈

- 非完美信息动态博弈——总存在某一步行动不被观察到
- 参与者1和2同时选择行动，参与者3和4观察到第一阶段结果后同时选择行动
- 子博弈——第一阶段，参与者1和2之间的博弈（静态博弈），第二阶段，参与者3和4之间的博弈（静态博弈）
- 逆向归纳法解两阶段博弈均衡解

第四节：非合作博弈之动态博弈

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 完全信息动态博弈

- 重复博弈——同样结构的博弈重复许多次，其中的每次博弈称为“阶段博弈（stage games）”
- 重复博弈可以是完全信息重复博弈，也可以是不完全信息重复博弈。
- 重复博弈中每次博弈的条件、规则和内容都是相同的，但由于有一个长期利益的存在，因此各博弈方在当前阶段的博弈中要考虑到不能引起其它博弈方在后面阶段的对抗、报复或恶性竞争，即不能象在一次性静态博弈中那样毫不顾及其它博弈方的利益。有时，一方做出一种合作的姿态，可能使其它博弈方在今后阶段采取合作的态度，从而实现共同的长期利益。

第四节：非合作博弈之动态博弈

❖ 非完全信息动态博弈

- 信号博弈——信号发送者（S）发出私人信息，信号接收者（R）在接收信息发送者的信息基础上做出决策的博弈
- 发送者S有一个给定的类型（t），发送者会观察这个没有其他人（好比说接收者）知道的类型，去从讯息堆 **M = {m1, m2, m3,..., mj}** 中选择送出一个讯息（m），然后接收者R观察这个讯息后从他可行的动作中 **A = {a1, a2, a3,...., ak}** 选一个作为反应动作（a）。接收者除了讯息之外其他都无法得知（如发送者的类型t），接着根据（t, m, a）的组合来决定双方会获得的报酬或回报。

第四节：非合作博弈之动态博弈

❖ 非完全信息动态博弈

- 信号博弈——信号发送者（S）发出私人信息，信号接收者（R）在接收信息发送者的信息基础上做出决策的博弈
- 小偷与乘客之间的博弈：小偷（S）向乘客（R）释放了谁反抗就殴打谁的信号，而乘客觉得小偷的信号是可信的，可能会有如下的几种情况：

对于乘客来说，小偷的威胁是可信的，因此，不反抗是最优的策略；对于小偷来说，乘客的不反抗下的不殴打策略最优。这一博弈的结果直接导致出现了不良的社会风气，纵容了小偷的违法行为。

本章小结

- 网络空间安全攻击类型
- 非合作博弈分类
  - 合作博弈 **VS** 非合作博弈
  - 静态博弈 **VS** 动态博弈
  - 完美（**Perfect**）信息博弈 **VS** 不完美信息博弈
  - 完全（**complete**）信息博弈 **VS** 不完全信息博弈