实验整理：

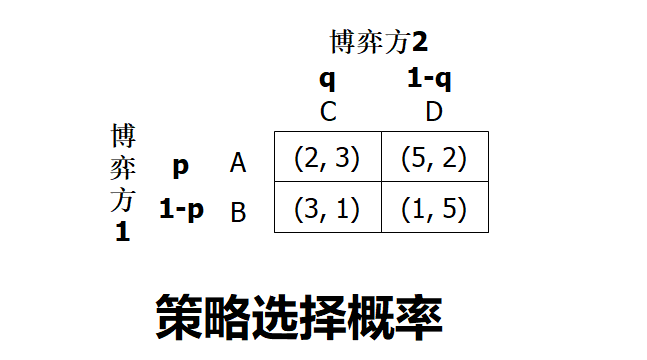
·博弈论是研究冲突对抗条件下最优决策问题的理论，包含三个基本要素

·参与人 （例如黑客、网络管理员）

·策略集 （例如 {使用DoS攻击、不使用DoS攻击})

·收益函数 （例如 网络服务质量）

·混合策略纳什均衡：在多人参与的博弈中，假设每个参与者按一定概率配置选择策略，如果任何一个参与人单独改变其概率配置都不会提高收益的数学期望，则该状态构成混合策略纳什均衡。



PPT整理：

第2组

·对抗性样本（Adversarial Examples）：

对抗性样本一般通过添加微小扰动形成，与原样本高度近似。在人看来两者难以区别，而模型的输出却截然不同。

·白盒（white-box）：

攻击者对模型有全面的了解，包括输入、架构、参数、输出、损失函数以及输出的解码结果。

白盒假设下，对抗样本的构造过程与模型的训练过程正好相反：

模型训练是固定输入样本，迭代优化模型参数；

样本构造是固定模型参数，迭代优化输入样本。

第3组

·安全推理：服务器持有神经网络模型，客户端持有需要分类的数据。服务器模型和客户端数据作为输入，计算分类，但双方都不学习除最终分类之外的任何信息。

第4组 浏览隐私漏洞

·泄露用户隐私信息的方式：随时监视受害者的游览器上有哪些标签页，正在游览器上游览哪个标签页通过以上两点，攻击者就可以随时监控你的游览记录，获取用户隐私，

对受害者造成不可预估的影响。

·解决：Site isolation是一种网站隔离机制，通过在同一浏览器中使用不同的进程来隔离访问不同网站的活动，以提高浏览器的安全性和隐私保护。

在很长的历史中，浏览器一直是一个单进程的应用程序，这就导致其在可靠性和安全性上有很大的弱点。一旦浏览器访问一个网站时崩溃或挂起，则整个浏览器必须退出和重启；如果恶意网站利用内存漏洞获取了进程控制权，那么这个受控的浏览器就可以攻击网络上的任意一个网站。

·跨站浏览隐私泄露：攻击者可以找出浏览器中加载了哪些站点，监控用户如何在这些敏感站点之间花费时间。

·在不产生实际网络请求的情况下加载一个网址：使用一个不安全的端口，使用磁盘缓存中的静态内容。

第5组

·视频剪辑对基于PPG的生物特征认证进行欺骗攻击

·PPG：基于频率的特征，它的一阶导数和二阶导数是生物特征认证的有用特征。

·攻击者可以访问包含受害者脸部视频来获取PPG信号

· Karimian基于泄露的信号使用微分方程和高斯函数将任意PPG信号的模型参数转换为受害者的模型信号，以欺骗认证系统。

第7组

·Replicated State Machines (RSM)：一种分布式系统设计模式，用于实现在多个节点之间复制相同状态的状态机。状态一致性，确保所有节点上的状态对象保持同步。

·缺点：节点过多时，验证交易需要大量计算资源，达成共识需要大量通信资源。

·记账：用户发起交易，包括转账、部署智能合约等操作。交易被广播到网络中的所有节点。节点根据交易信息，更新本地账本状态，并将交易验证结果广播到网络中的其他节点。

·验证：验证的规则根据不同的区块链协议而异，但通常会验证交易的有效性、签名正确性、转账人账户余额是否充足等内容。如果交易被验证通过，则节点会将其添加到待打包交易池中，等待进一步的处理。

·创建区块：当待打包交易池中的交易数量达到一定阈值，或者一定时间过去后，节点会开始创建新的区块。节点会从待打包交易池中选取一些交易，组成新的区块，并且添加一些元数据，如时间戳、前一区块的哈希等信息。节点会对新的区块进行哈希运算，得到一个唯一的区块哈希值。

·达成共识：新的区块被广播到网络中的其他节点。其他节点对新的区块进行验证，如果验证通过，则认可该区块的有效性，并将其添加到自己的本地区块链上。如果不同节点产生了不同的区块，那么就需要通过共识算法来解决。具体的共识算法因区块链协议而异，比如比特币采用的是工作量证明（PoW）算法，以太坊正在逐步转向基于权益证明（PoS）的共识机制。

·改变区块链：区块链是一个不断增长的链式结构，新的区块会被添加到链的末端。如果某个节点要更改区块链的某个旧区块的数据，那么就需要对后续的所有区块进行重新计算，这个过程需要消耗大量的计算资源。如果网络中有多个节点尝试更改同一个旧区块，那么共识算法会判定哪个更改是有效的，哪个是无效的。

·区块链面临的威胁：双重花费，因为不公平丢弃交易，需要一个公平的对抗性调度器，单个节点发生错误或缓慢，交易没有正确签名或不同块间冲突，假设同步容易受到攻击，依赖于领导者，错误的共识算法

第8组 我知道你的社交网络账户：用于设备身份关联的新型攻击架构

·SN-SN关联攻击指跨社交网络关联攻击：可利用社交网络节点的结构相似性(用户的好友信息)关联同一用户在不同社交网络中的帐户。

·DS-SN关联攻击：设备系统状态 -> 社交网络关联攻击。用户经常在移动设备上访问社交网络会产生丰富的设备特征，可利用移动设备上的侧信道信息对目标进行去匿名化。

·步骤1: 通过零权限恶意应用程序从受害者的设备获取系统状态

·步骤2: 推断设备中的活动转换

·步骤3: 推断触发的相应社交网络事件

·步骤4: 根据设备触发的推断事件和从目标社交网络抓取的公开可用事件，将受害者

的设备与其社交网络帐户相关联。

·有效性评估：DS-SN关联攻击

·收集系统状态信息的Java恶意应用程序

·用于活动转换推理与社交网络事件推理的Python后端

·用于爬取社交网络公开数据，进行设备-账号匹配的Python爬虫

·威胁模型：是指攻击者可以通过安装在受害者设备上的恶意应用程序在没有特殊权限的情况下完成推理攻击。

第10组

·云端存储的优势：便于管理，可扩展性强，成本效益高

·安全问题：云端的数据访问此时对潜在的不可信实体是可见的，应对键值对进行加密

·访问模式攻击：如频率分析

·推断出键值

·识别出某一键值何时被访问

·检测并识别出键值访问频率的变化

·Pancake是保护键值存储免受访问模式泄漏攻击的系统。采用频率平滑方式、具有较小的带宽开销。适用于高性能数据存储设计。

·频率平滑中采用的四种技术

·选择性复制

·虚假访问

·查询批处理

·动态适应

·F作为伪随机函数和E作为（随机化）认证加密方案的密码安全性。这确保了密钥F（k，j）看起来是随机的，并且没有任何关于值的泄漏。

第11组

·新的恶意软件样本无法提前被分类，使得静态逆向工程仍被需要。静态逆向工程分析恶意软件手动且乏味。

第12组

·DNS缓存污染攻击：

·伪造攻击：伪造一个恶意的DNS响应，欺骗递归解析器去接受它。缓解措施：增加DNS数据包的随机性。

·分片整理攻击：被分片的DNS响应包中的第二个分片段并不包含DNS和UDP报文中的报头，可以避开针对伪造攻击的防御措施。

第13组

·黑盒攻击是指攻击者只能通过输入和输出来了解模型，而无法获取模型的内部信息。更接近于实际应用环境中的攻击情况

·白盒攻击则是指攻击者拥有对模型的完全访问权限，包括模型的结构和参数等信息。更好地理解模型的内部结构和漏洞。

·非目标攻击旨在使模型的预测出现错误，但攻击者并不关心预测的具体类别。测试模型的鲁棒性或者破坏模型的性能。

·目标攻击的目标是让模型将输入预测为特定的类别。欺骗模型、某些检测算法或者破坏安全系统。

第15组

·边缘计算也称为边缘处理，是一种将服务器放置在本地设备附近网络技术, 这有助于降低系统的处理负载，解决数据传输的延迟问题。这样的处理是在传感器附近或设备产生数据的位置进行的，因此称之为边缘。

第17组

被动观察——嗅探攻击

主动延迟——TCP劫持攻击

第19组

·同态加密

·密文空间具有特定的算符，与明文空间的算符一一对应

·多数同态加密属于公钥系统

·加密和计算只需要公钥

·解密需要私钥

第21组

·防御策略

·差分隐私（Differential Privacy ，DP）：通过往查询结果中加入随机噪声r，使得邻接数据集D与D′经过同一查询后的结果并非确定的具体值，而是服从两个很接近的概率分布，这样攻击者无法辨别查询结果来自哪一个数据集，保障了个体级别的隐私性。

·知识蒸馏（Knowledge Distillation ，KD）：将泛化能力从较大的模型（原始模型）转移到较小的模型（蒸馏模型），而不导致效用退化。一旦提炼出来的模型被训练好，它就可以在许多场景下取代原始模型，因为它的计算效率更高，对资源的依赖性更少。