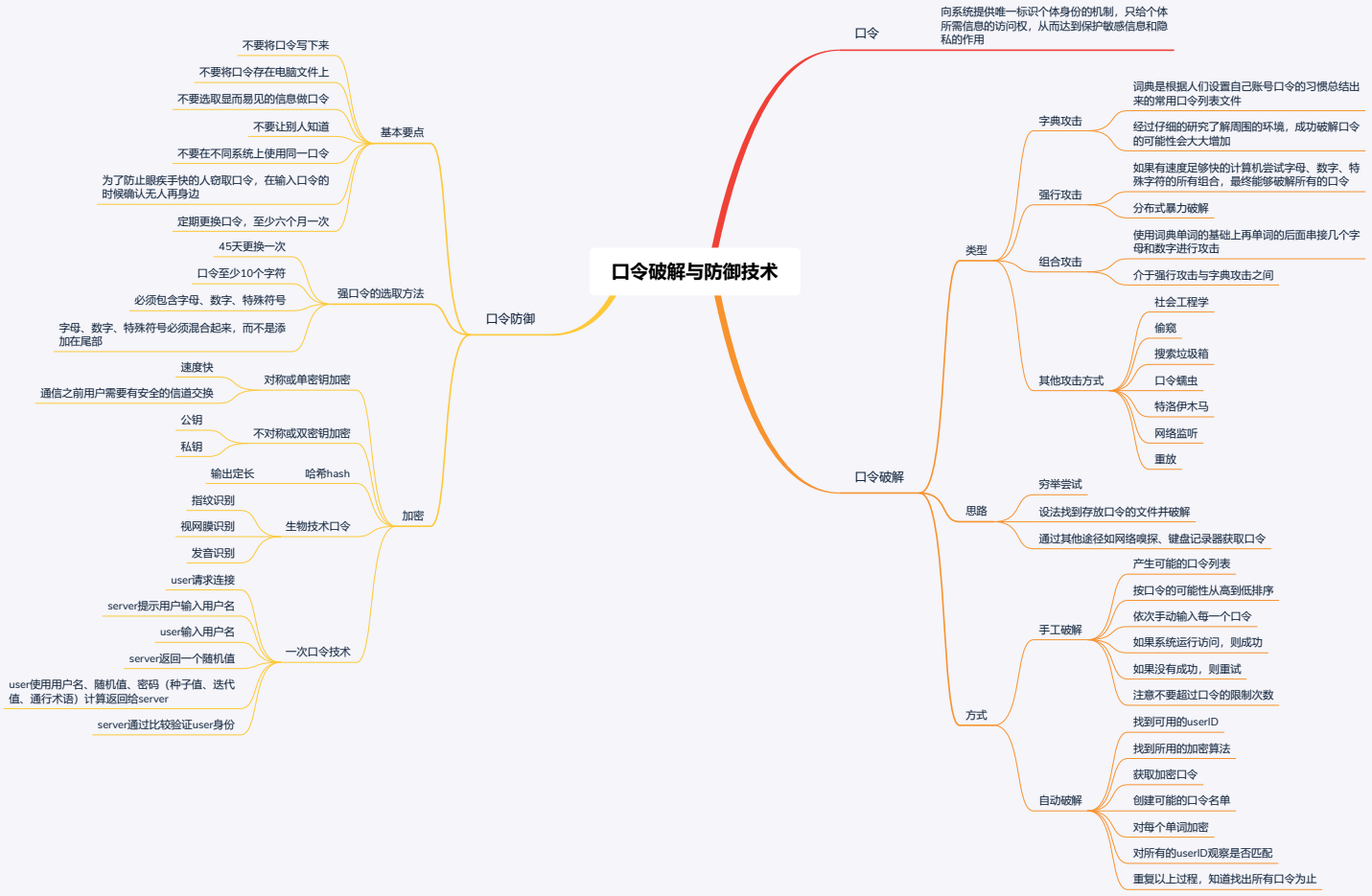
口令破解与防御技术
口令
向系统提供唯一标识个体身份的机制，只给个体所需信息的访问权，从而达到保护敏感信息和隐私的作用
口令破解
类型
字典攻击
词典是根据人们设置自己账号口令的习惯总结出来的常用口令列表文件
经过仔细的研究了解周围的环境，成功破解口令的可能性会大大增加
强行攻击
如果有速度足够快的计算机尝试字母、数字、特殊字符的所有组合，最终能够破解所有的口令
分布式暴力破解
组合攻击
使用词典单词的基础上再单词的后面串接几个字母和数字进行攻击
介于强行攻击与字典攻击之间
其他攻击方式
社会工程学
偷窥
搜索垃圾箱
口令蠕虫
特洛伊木马
网络监听
重放
思路
穷举尝试
设法找到存放口令的文件并破解
通过其他途径如网络嗅探、键盘记录器获取口令
方式
手工破解
产生可能的口令列表
按口令的可能性从高到低排序
依次手动输入每一个口令
如果系统运行访问，则成功
如果没有成功，则重试
注意不要超过口令的限制次数
自动破解
找到可用的userID
找到所用的加密算法
获取加密口令
创建可能的口令名单
对每个单词加密
对所有的userID观察是否匹配
重复以上过程，知道找出所有口令为止
口令防御
基本要点
不要将口令写下来
不要将口令存在电脑文件上
不要选取显而易见的信息做口令
不要让别人知道
不要在不同系统上使用同一口令
为了防止眼疾手快的人窃取口令，在输入口令的时候确认无人再身边
定期更换口令，至少六个月一次
强口令的选取方法
45天更换一次
口令至少10个字符
必须包含字母、数字、特殊符号
字母、数字、特殊符号必须混合起来，而不是添加在尾部
加密
对称或单密钥加密
速度快
通信之前用户需要有安全的信道交换
不对称或双密钥加密
公钥
私钥
哈希hash
输出定长
生物技术口令
指纹识别
视网膜识别
发音识别
一次口令技术
user请求连接
server提示用户输入用户名
user输入用户名
server返回一个随机值
user使用用户名、随机值、密码（种子值、迭代值、通行术语）计算返回给server
server通过比较验证user身份