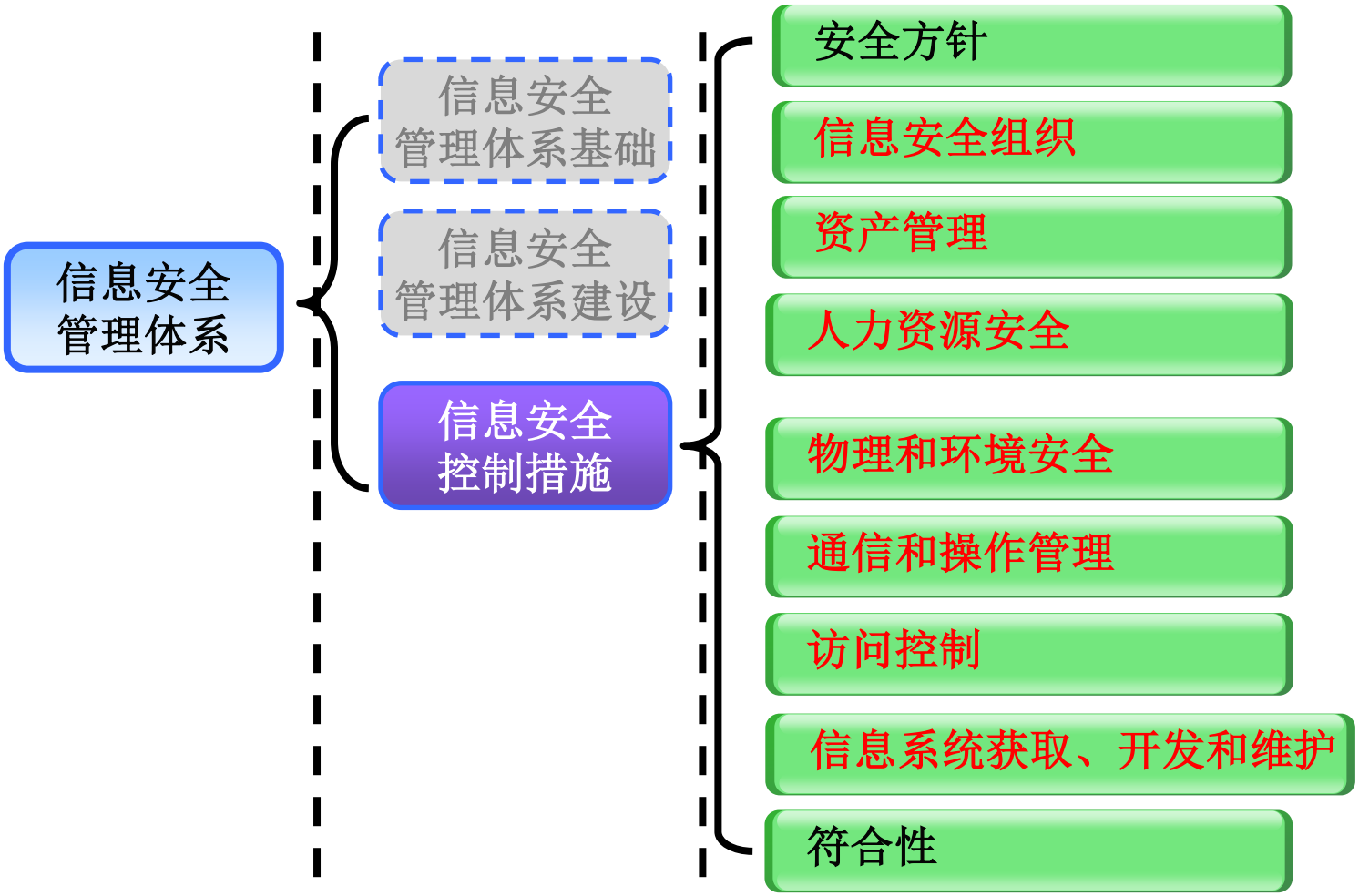
远离网络威胁，保护信息安全

现代教育技术中心

课程内容


信息安全管理体系
信息安全管理体系基础
信息安全管理体系建设
信息安全控制措施
安全方针
信息安全组织
资产管理
人力资源安全
物理和环境安全
通信和操作管理
访问控制
信息系统获取、开发和维护
符合性
知识体
知识域
知识子域

资产清单

- 信息安全管理工作的直接目的是保护组织的资产
- 资产包括：
  - **信息**：业务数据、合同协议、科研材料、操作手册、系统配置、审计记录、制度流程等
  - **软件**：应用软件、系统软件、开发工具
  - **物理资产**：计算机设备、通信设备、存储介质等
  - **服务**：通信服务、供暖、照明、能源等
  - **人员**
  - **无形资产**，如品牌、声誉和形象

(1)对资产负责

什么叫资产安全的适当保护

适当保护的意义：黑客破解系统的代价高于该资产的价值，那么我们认为这个资产是安全的，而不需要对保护措施进行无限的投入。

知识域：信息安全控制措施

知识子域： 人力资源安全

- 理解任用前控制目标的含义，掌握角色和职责、审查等控制措施的实施方法
- 理解任用中控制目标的含义，掌握管理职责、信息安全意识教育和培训等控制措施的实施方法
- 理解任用的终止或变化控制目标的含义，掌握终止职责、撤销访问权等控制措施的实施方法

- 一句话：想方设法对不同角色和职责的人进行控制
- 本次课程最重要的内容

- 信息安全保障最大的风险：人

- 欢迎随时互动讨论

- 1、八卦一下近年大规模的信息安全事件
- 2、重点说说，信息安全最大风险-人
- 3、如何入侵一个系统
- 4、防范入侵的技巧

近年较为严重的网络入侵事件

利用漏洞入侵

永恒之蓝攻击-渗透测试带来的风险

Stuxnet（震网）蠕虫的攻击目标直指西门子公司的SIMATIC WinCC系统。这是一款数据采集与监视控制（SCADA）系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程；它运行于Windows平台，常被部署在与外界隔离的专用局域网中。

一般情况下，蠕虫的攻击价值在于其传播范围的广阔性、攻击目标的普遍性。此次攻击与此截然相反，最终目标既不在开放主机之上，也不是通用软件。无论是要渗透到内部网络，还是挖掘大型专用软件的漏洞，都非寻常攻击所能做到。这也表明攻击的意图十分明确，是一次精心谋划的攻击。

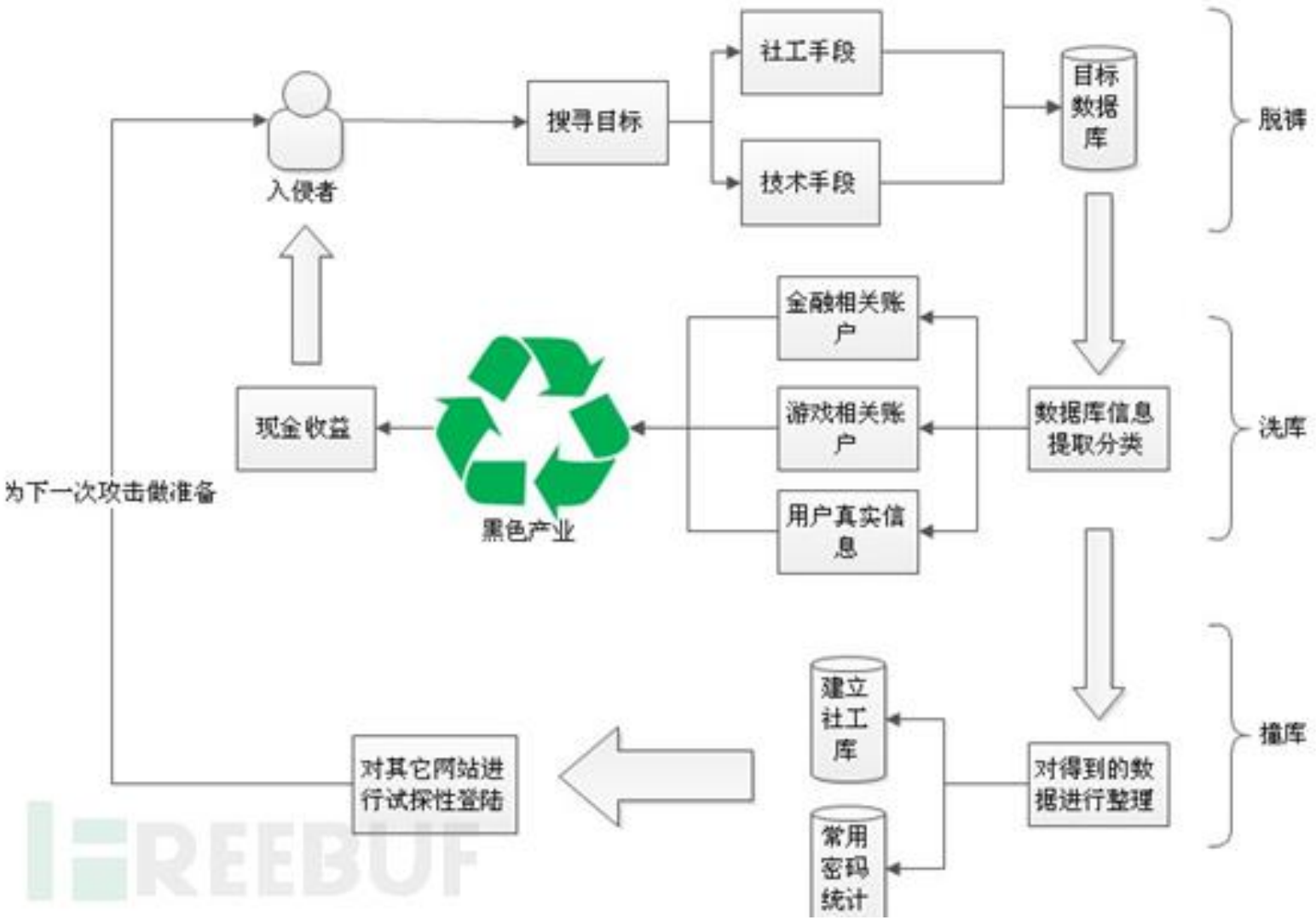
Stuxnet蠕虫利用四个漏洞都是在Stuxnet中首次被使用，是真正的零日漏洞。如此大规模的使用多种零日漏洞，并不多见。

近年较为严重的网络入侵事件

数据泄露的风险

在黑客术语里面，”拖库“是指黑客入侵有价值的网络站点，
把注册用户的资料数据库全部盗走的行为，因为谐音，也经常被称作“脱裤”，360的库带计划，奖励提交漏洞的白帽子，也是因此而得名。在取得大量的用户数据之后，黑客会通过一系列的技术手段和黑色产业链将有价值的用户数据变现，这通常也被称作“洗库”。最后黑客将得到的数据在其它网站上进行尝试登陆，叫做”撞库“，因为很多用户喜欢使用统一的用户名密码，”撞库“也可以是黑客收获颇丰。

下图是黑客，在“脱裤”“洗库”“撞库”三个环节所进行的活动。


社工手段
搜寻目标
技术手段
目标数据库
脱裤
入侵者
金融相关账户
游戏相关账户
用户真实信息
数据库信息提取分类
洗库
现金收益
为下一次攻击做准备
黑色产业
建立社工库
常用密码统计
对得到的数据进行整理
撞库
对其它网站进行试探性登陆

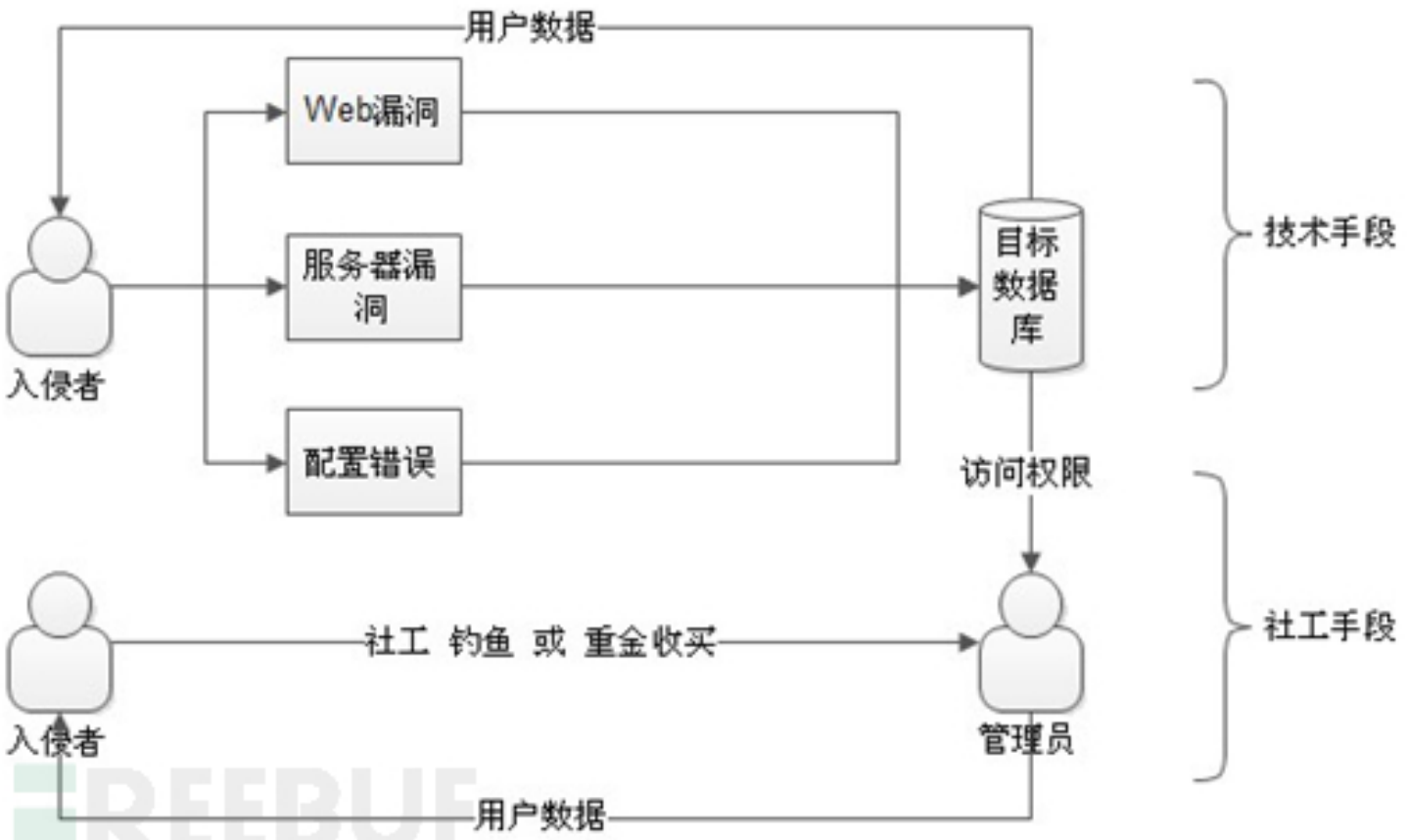
随着地下产业链日渐成熟，用户数据可以被迅速地转变成现金。

（1）用户账号中的虚拟货币，游戏账号，装备，都可以通过交易的方式变现，也就是俗称的“盗号”。

（2）金融类账号比如，支付宝，网银，信用卡，股票的账号和密码，则可以用来进行金融犯罪和诈骗。

（3）最后一些可归类的用户信息，如学生，打工者，老板等，多用于发送广告，垃圾短信，电商营销。也有专门的广告投放公司，花钱购买这些分门别类的信息。

黑客为了得到数据库的访问权限，取得用户数据，通常会从技术层面和社工层面两个方向入手。



知识域：信息安全控制措施

首先要了解人

人，是最不可靠的

- “没有一个系统是安全的”
- “人不能总藏在他的计算机后面，最大的安全漏洞并不是存在于什么程序或者服务器内，人类才是最大的安全漏洞”
- “所有黑客手段中最有效的、最伟大的幻想艺术——社会工程学”

- “你的脸皮要足够厚，那样世界就会在你的脚下”
- “人类天生胆小且容易受骗”
- “人们只看到他们愿意看到的”

- 如何入侵一个“系统”
- 最后会说说，如何防止被入侵的技巧。
- 入侵并不是用技术破译登陆密码
- 破译效率太低
- 黑客第一个技能是--学习肩窥，没底线

- 肩窥=偷看
- 破解银行卡
- 银行卡复制器+摄像头
- 哪怕是通过动作观察训练，缩小密码范围，然后再穷举破解密码

- 人们只看到他们愿意看到的
- 如何控制一个人的心理和行为
- 把一些带有暗示性的支离破碎的信息植入对方，诱导对方进行信息重构、分析和逻辑判断，形成自己的推论，并深深的信服自己。

- 作为中国千万网民中的一个，你可能觉得，我不用网银，打游戏不充钱，我没有什么被黑的价值，所以黑客是不会来光顾我的。其实不然，每一个使用互联网服务的用户，在享受快捷方便的时候，都把自己暴漏在了风险之下。不是黑客会不会值得黑你，而是你有没有可能被波及。

最后说说如何保护自己

- 首先明确自身存在人性的弱点。
- 需要养成日常安全的行为习惯，就是建立细致的行为约束管理规范。
- 资金安全，尽量使用ATM和现金消费，尽量不用要pos机消费，开设一张权限最低的银行卡作为日常消费。
- 保护好手机，选择安全系数高的型号，不要泄露验证码。苹果手机开启双重认证模式。

- （1）重要网站/APP的密码一定要独立，猜测不到，或者用1Password这样的软件来帮你记忆；
- （2）电脑勤打补丁，安装一款杀毒软件；
- （3）尽量不使用IE浏览器
- （4）支持正版，因为盗版的、破解的总是各种猫腻，后门存在的可能性很大；
- （5）不那么可信的软件，可以安装到虚拟机里；
- （6）不要在公共场合（如咖啡厅、机场等）使用公共无线，自己包月3G/4G，不差钱，当然你可以用公共无线做点无隐私的事，如下载部电影之类的；
- （7）自己的无线AP，用安全的加密方式（如WPA2），密码复杂些；

- 设置复杂密码或指纹、虹膜解锁功能，不用外置存储卡
- 离开座位锁定屏幕（Windows图标键+L键），安装防窥膜。
- 删除文件和销毁文件的技巧，使用安全加密的移动硬盘存放资料
- 不打开任何可疑文件，识别可疑的邮件，TAOBAO类似的地址钓鱼诈骗。

- 尽量避免使用社交网络、网上银行和网上购物
- 黑客可以利用社交网络的信息，装成你的朋友进行线上聊天欺诈。
- 拥有高权限的管理者不要与其他人建立亲密关系，防止被社工。
- 设置密码的技巧
- 不用简单的词语组合，生日、名字缩写

如何设置一个容易记忆的复杂密码

- 通常认为特殊字符、字母、数字组合为安全密码
- 例如：A8qh@*g！Pw

- 但是太难记忆，只好用手抄本抄录，密码遭遇物理泄露风险。

- 一套容易记忆的密码编制技巧，词意记忆密码
- 我很胖2018年我特么要减掉20公斤！
- whp2018nwTMyjd20kg!

当然你不要把这个写到你的社交网络的签名档里面

❖谢谢大家！