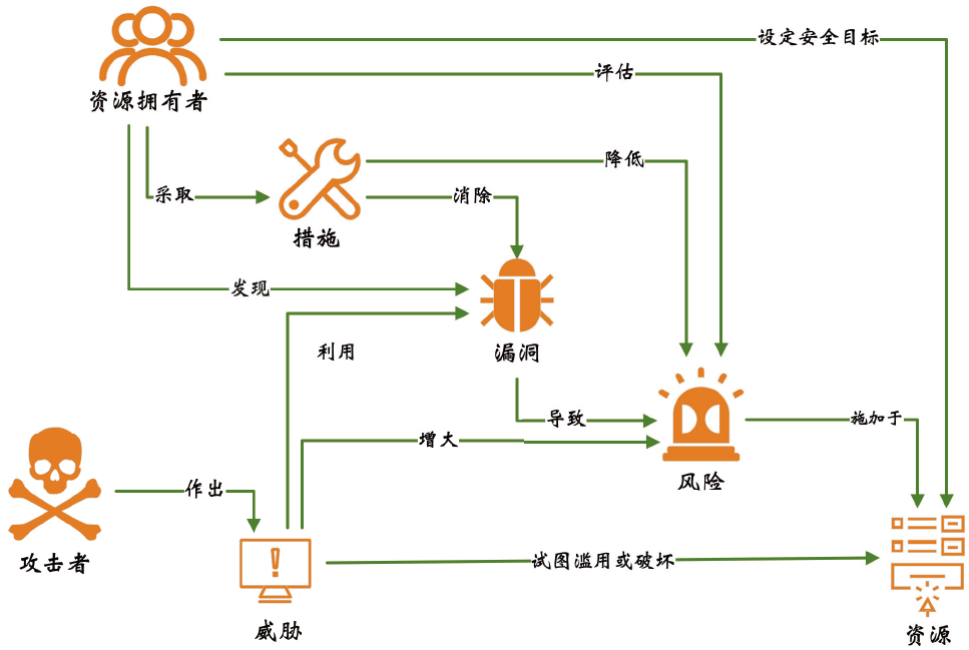
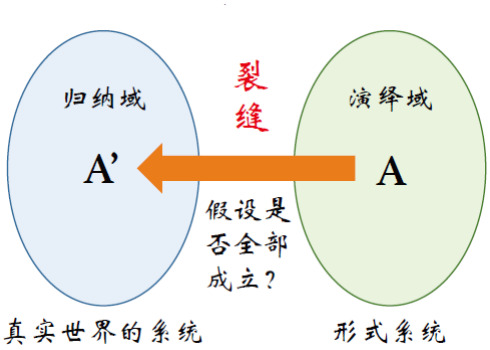
概论

网络空间安全要素模型 ★★★★★



归纳域与演绎域 ★★★★



解释 一个现实系统是否满足一个演绎模型的假设是无法形式证明的，只能证伪，即发现假设或前提不成立，因此结论也不成立。

例子 演绎域A中假设攻击者不会在夜间发起攻击，但是我们在归纳域A'中观察到攻击者在夜间发起了攻击，从而结论不成立。

网络攻击

攻击的进化 ★★★

- 孤立的安全事件
- 规范化/标准化的攻击
- 黑色产业链

黑客的分类 ★★★★

- 社区黑客
- 技术黑客（白帽）
- 经济黑客（黑帽）
- 政治黑客
- 政府黑客

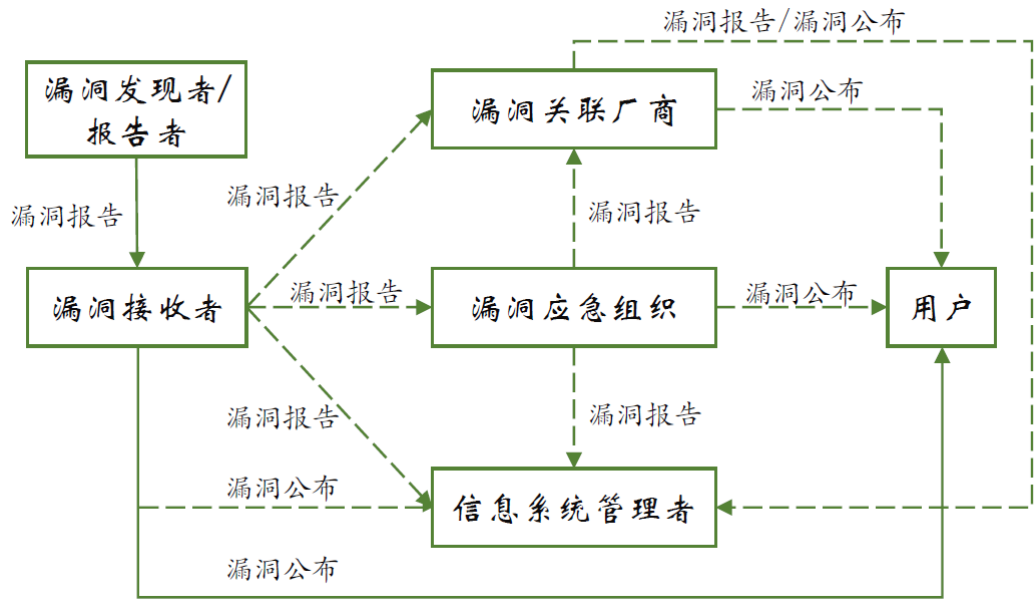
> 安全漏洞定义★★★

系统设计、实现或运行管理中存在的缺点或弱点。这些缺点或弱点可被利用来违背系统的安全策略

> 漏洞的披露★★★

- 行业内交流
- 面向社会公众

可以帮助防御方改进防御措施，也方便攻击方利用漏洞信息实施攻击



首先通知系统或设备的生产厂商，一段时间后通知管理部门，管理部门给厂商一段时间改进，最后对外发布安全漏洞的信息及修补建议

> 安全漏洞的生命周期★★★★

- 产生
- 发现
- 暴露
- 曝光
- 成熟
- 消亡

漏洞原因 ★★★★

- 设计漏洞：IP协议对IP地址的无条件信任、路由劫持
- 实现漏洞：缓冲区溢出、跨站脚本、SQL注入
- 管理漏洞：域名的残留信任

公共漏洞与暴露库 CVE ★★★★

一个漏洞字典。

公共漏洞枚举库 CWE / 公共平台枚举库 CPE ★★★

CWE 将安全漏洞按照研究视角、开发视角、系统架构视角分类

CPE 是为产生安全漏洞的信息系统、设备和开发工具进行标准分类

网络杀伤链 ★★★★

- 侦察：搜集信息，包括网络扫描、社工
- 武器化：定制攻击程序
- 投放：发送攻击程序
- 漏洞利用：触发攻击程序，获取主机权限
- 后门安装：安装后门，消除入侵痕迹
- 命令与控制：建立通信，实现交互能力
- 意图实现：执行目标任务

ATT&CK 模型 ★★★★★

ATT&CK 知识库

- 战术（Tactic）：攻击周期中攻击者的近期目标
- 战术（Technique）：攻击者大道战术目标所使用的手段
- 过程（Process）：攻击动作构成的链条，记录攻击者使用的技术和其它元数据的文档

ATT&CK 企业网络环境的战术

- 侦察：手机攻击目标的相关信息
- 资源开发：建立可以用于支持行动的资源
- 初期入侵：在目标网络中获得第一个立足点
- 执行：在本地或远程执行攻击者控制的代码
- 坚持：通过对访问控制策略的修改，使得攻击者能够持续存在于目标环境中
- 权限提升：使得攻击者在目标环境中获得更高访问权限
- 防御逃避：使攻击者能够规避在目标环境中存在的检测功能和防御功能
- 凭证访问：使攻击者可以访问或控制目标环境中某个系统、域或服务的访问凭证，例如口令

- 发现：攻击者可以获得目标环境中系统和内部网络的更多信息
- 横向移动：攻击者利用凭证访问和发现战术收集到的信息，对被攻击环境中的其它系统实施渗透攻击
- 收集：发现并获取目标环境中的敏感数据
- 指挥与控制：支持入侵攻击的交互过程
- 渗透：将收集到的有价值信息取回
- 影响：操控、终端或摧毁被攻击系统或其中的数据

ATT&CK 模型

- 技术对象：特定攻击技术的唯一标识，描述其相关细节
- 对手组对象：已经曝光的攻击者。分为命名的入侵集、威胁组、威胁者组、战役
- 软件对象：工具、例程、恶意代码

> 主动进入与被动进入★★★

主动进入：针对有漏洞服务程序的攻击，SQL 注入

被动进入：鱼叉钓鱼、第三方软件/平台发起的间接攻击（供应链攻击、水坑攻击）

> 路径 / 配置劫持★★★★

攻击者利用系统在文件搜索时的顺序劫持漏洞或注册表等配置管理程序的访问控制漏洞，将攻击程序注入特权进程空间中允许，从而达到提权的效果

- Windows：DLL加载顺序攻击（将恶意DLL放置在合法DLL的目录位置上）
- MacOS：系统动态库劫持攻击（指定搜索路径查找dylib）
- Windows：注册表配置劫持

> 木马后门★★★

- 计划任务建立与删除
- 获取主机信息
- 注册表操作
- USB设备感染
- 键盘记录
- 获取当前窗口 title
- 获取运行进程信息
- 检测杀软及运行环境
- 比特币行为监控
- 勒索
- DDos
- 向远程控制器发送数据
- 接收远程控制器指令，执行指定操作

> 木马的类型★★★★

- 基于可执行程序的木马：exe / DLL （WannaCry）
- 基于引导区的木马：（暗云）
- 网站木马（Webshell）：（水坑攻击、网络钓鱼）分为大马、小马、一句话木马

> DDos 攻击的直接方法机制 ★ ★ ★ ★

攻击者操纵攻击节点直接向受害者发送攻击报文，造成服务器失效。有一个明确的消耗对象

分类：链路层直接泛洪攻击（ARP缓存溢出）、基于 TCP/IP（SYN Flood）、应用层（ReDos）

> DDos 攻击的反射方法机制 ★ ★ ★ ★

以受害者主机为源伪造攻击保温并发送给第三方主机

分类：链路层（Smurf）、网络层（CharGen、NTP）、应用层（SSDP、Memcached）

僵尸网络

> 潜代码/恶意软件/恶意代码 ★ ★ ★

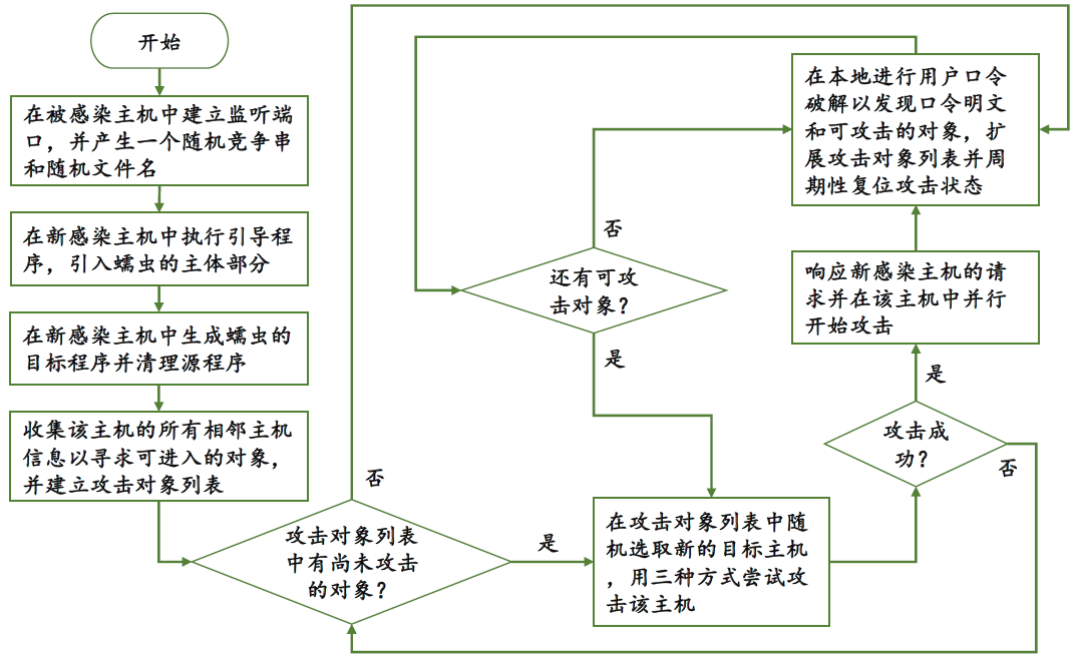
指故意编制或设置的，对网络或系统会产生威胁或潜在威胁的大妈

常见的有：病毒、蠕虫、木马、僵尸网络、逻辑炸弹

隐蔽代码：指在用户不知道的情况下安装的代码

> Morris 蠕虫 ★ ★ ★ ★

工作机制



存活机制

- 生存竞争
- 定期自我复制
- 重复感染
- 攻击“前小后大”

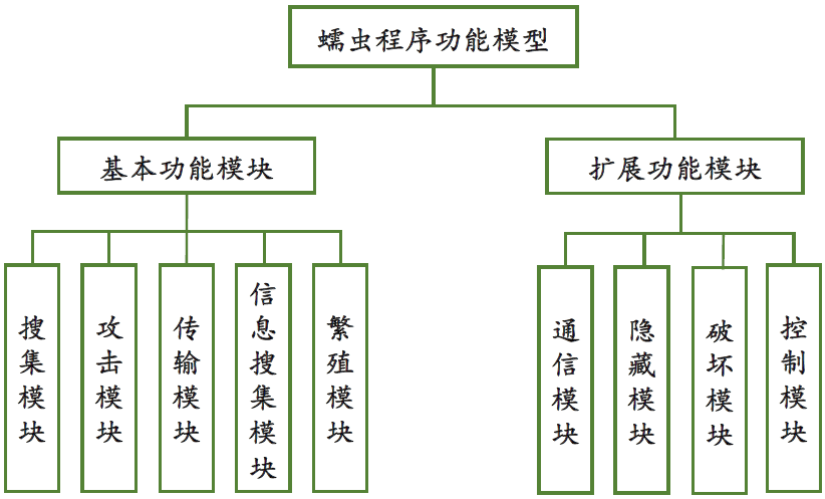
特点

- 具备强大的成功渗透能力
- 口令破解使其引发Dos攻击
- 具备较高自主性，不具备远程控制能力
- 较弱的清除入侵痕迹能力
- 具有环境依赖性

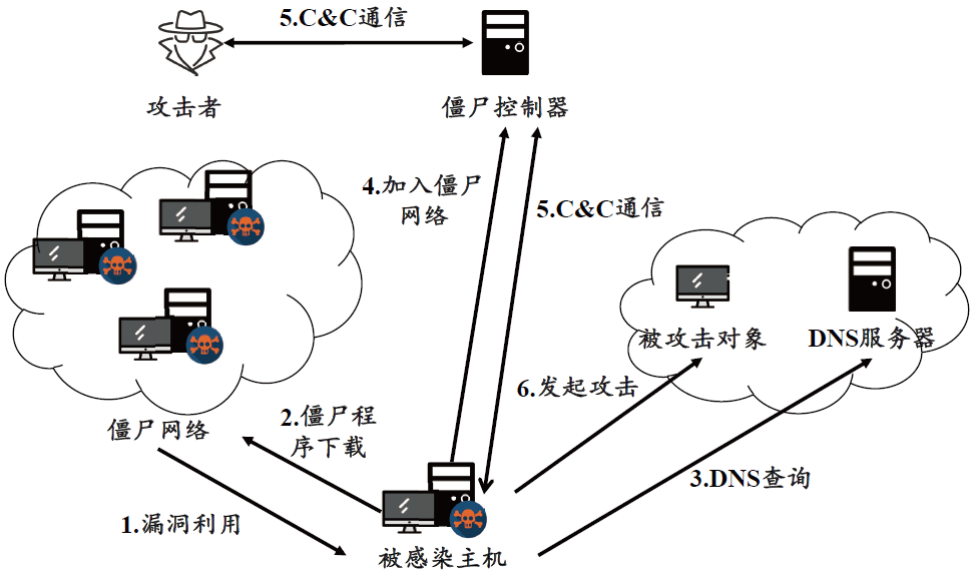
> 网络蠕虫的传播机制★★★

- 通过 IP 地址寻找目标：顺序扫描、选择性随机扫描、基于路由的扫描
- 通过域名寻找目标：目标列表扫描、被动式扫描

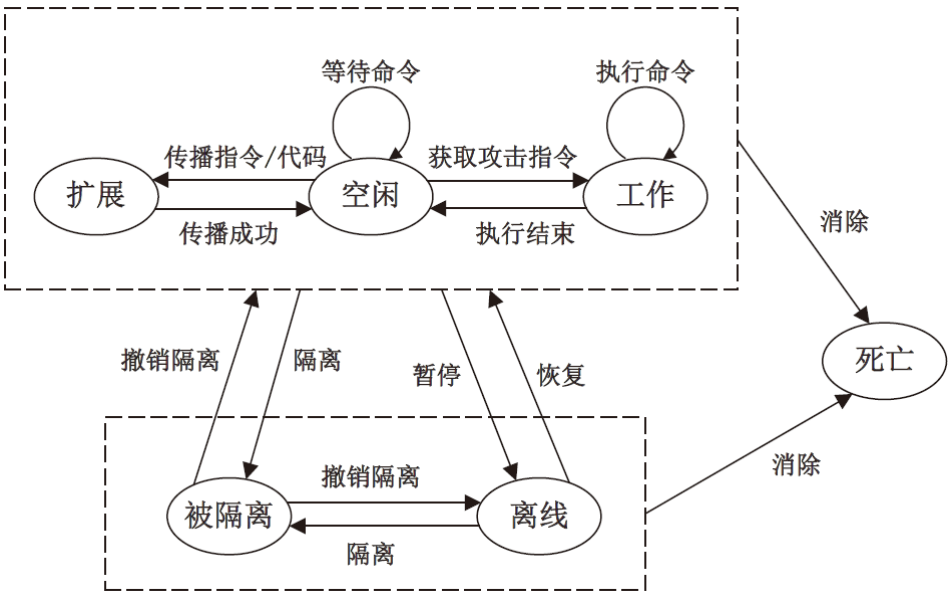
> 蠕虫的功能★★★



Zombie 的工作流程★★★



僵尸网络的生命周期模型★★★★



> 僵尸网络的三个基本行为特征 ★ ★ ★

- 扩散
- 重复
- 分布

> 僵尸网络基本控制结构 ★ ★ ★ ★

- 直接控制结构：IRC / HTTP
- P2P结构
- 无结构型：每次通信通过扫描对端完成
- 基于代理：隐藏真正的C2服务器

> 僵尸网络的生存机制 ★ ★ ★

> 切换机制 ★ ★ ★ ★ ★

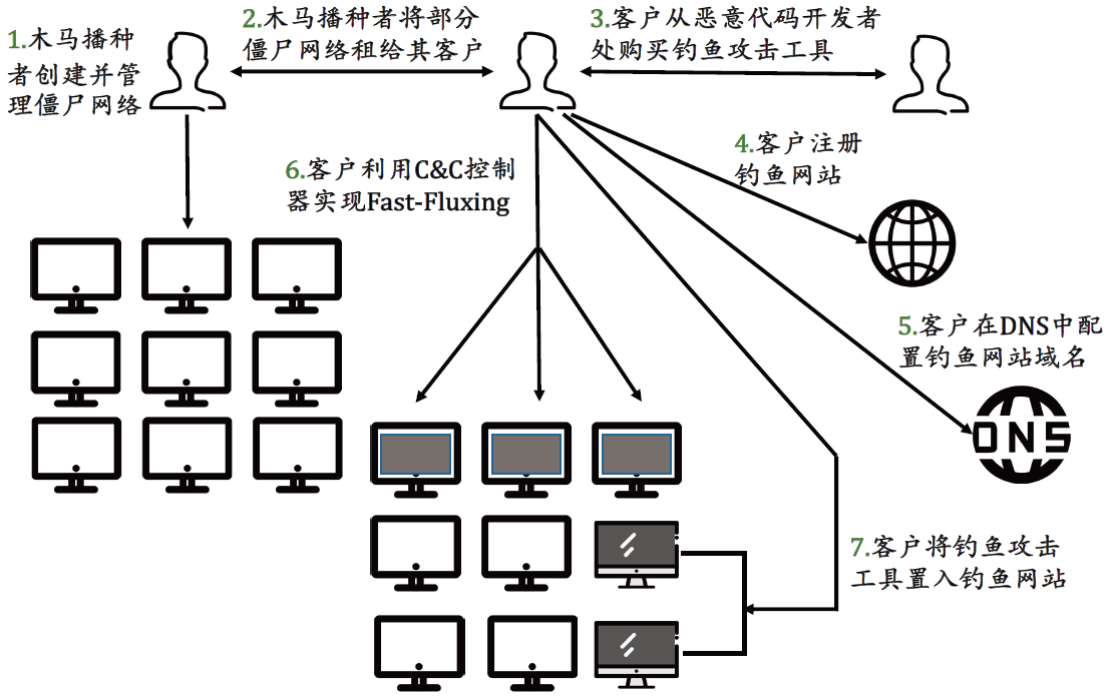
- IP Fluxing：A 记录（描述一个域名与一个 IP 地址的绑定关系）的生存期特别短
- Domain Fluxing

黑产

> 运作模式 ★ ★ ★

- 对内：合作和暗网
- 对外：社会工程学方法

> 黑产的分工合作 ★ ★ ★ ★



> 暗网 ★ ★ ★

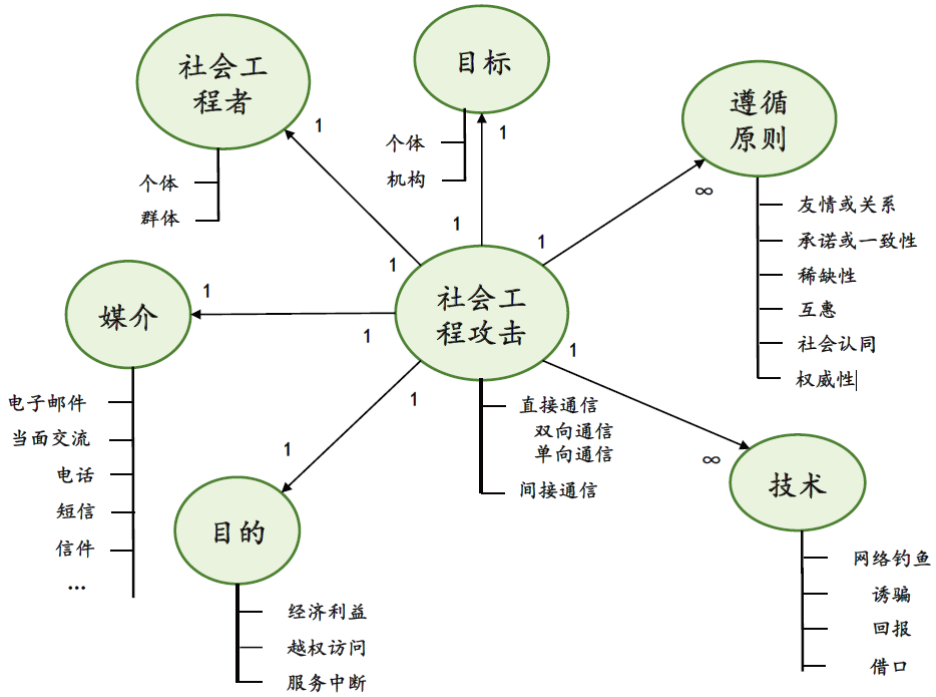
是一种覆盖网络，只能用特殊软件、特殊授权或对计算机做特殊处理才能访问，通常使用非标准的通信端口和传输加密保护

例子：丝绸之路

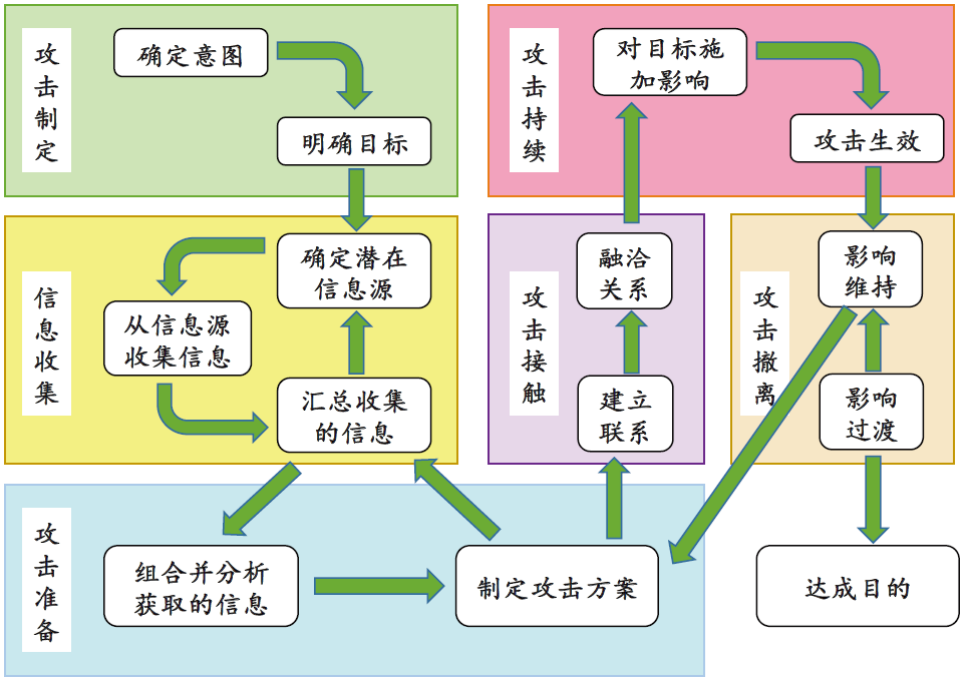
> 社会工程攻击 ★ ★ ★ ★

社会工程学：心理学的分支，研究如何有道人的思维方向和决策选择

> 社会工程攻击的本体论模型 ★ ★ ★ ★



社会工程攻击流程★★★



社会工程攻击手段★★★

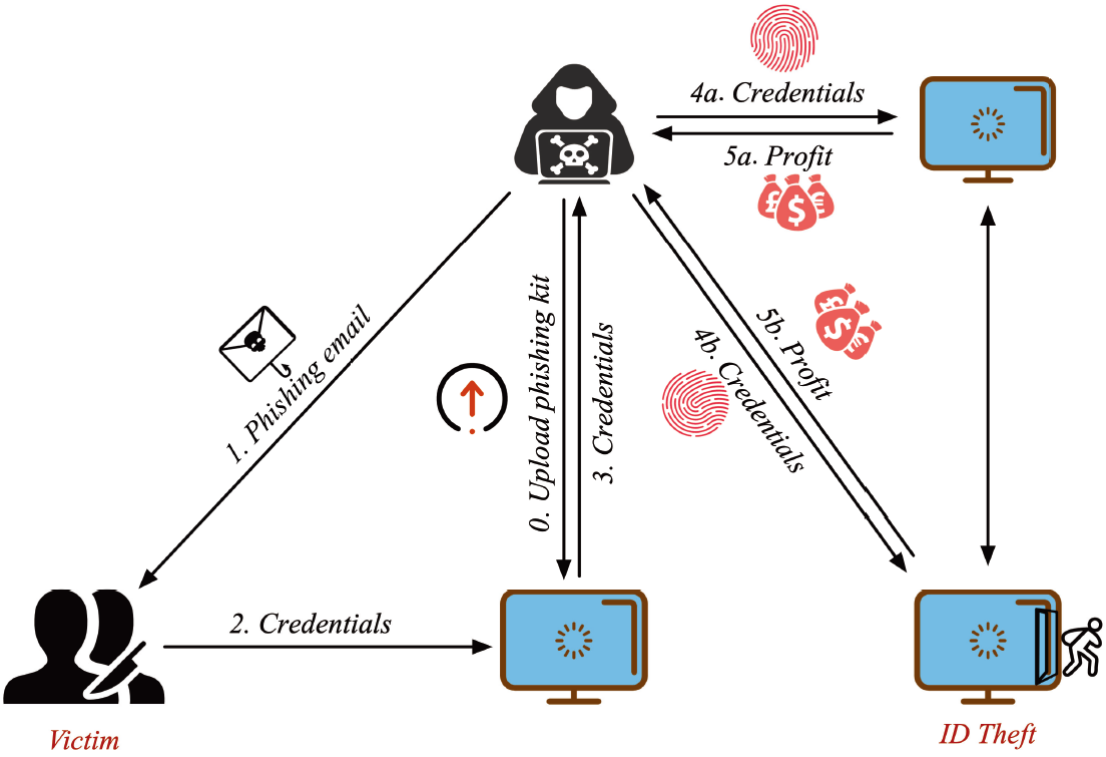
- 物理手段
- 心理手段

网络钓鱼★★★

利用社会工程方法和技术手段窃取消费者个人身份数据和金融账户凭证

- 社会工程方法：发送欺骗性电子邮件引导收件人访问伪造的网站
- 技术手段：将犯罪软件植入用户个人电脑中

> 鱼叉攻击★★★

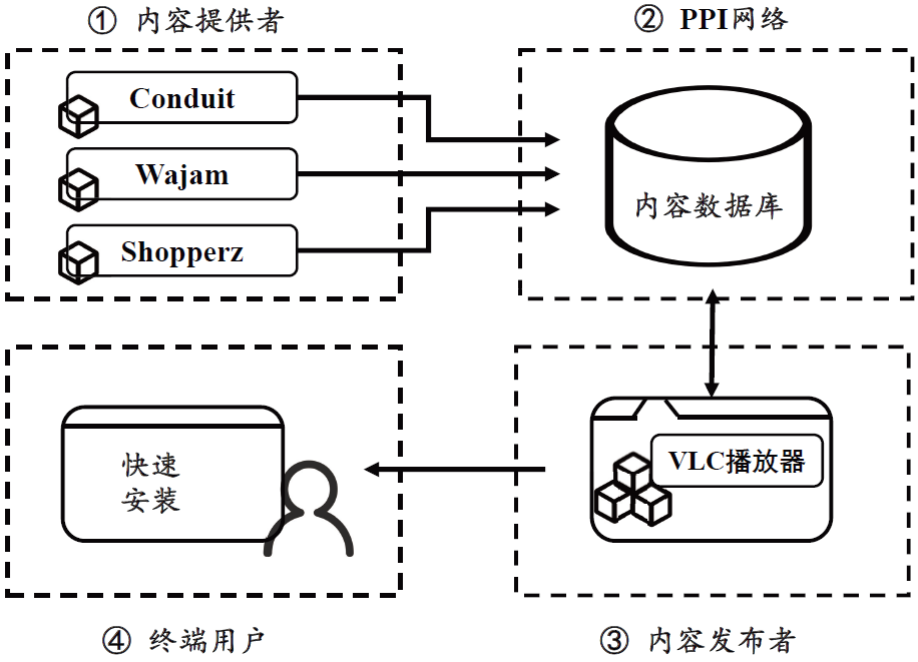


> 网络钓鱼的基本攻击方法★★★★

- 访问欺骗：要求行动攻击、相似诱骗攻击、搜索引擎攻击
- 恶意代码注入：信息收集、会话拦截、数据篡改
- 信息注入：水坑攻击

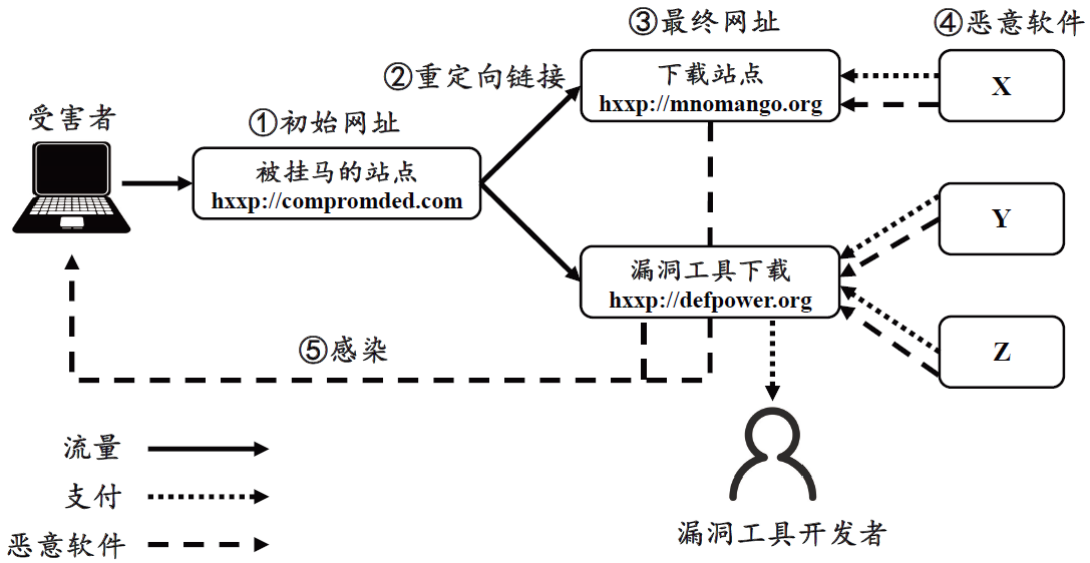
> PPI 模式★★★

按下载量付费



基于流量的 PPI★★★★

基于用户系统中存在的安全漏洞进行下载器的安装



面向销售的黑色产业链★★★★

- 广告发布
- 点击支持
- 销售实现

隐私信息盗取★★★★

- 撞库：收集泄露的密码组成一个列表，并通过这个列表登录不同的网站
- 拖库：侵入一个网站并下载其用户数据库
- 洗库：在黑市上出售有价值的用户数据

勒索软件 ★ ★ ★

利用各类技术对用户的设备、数据等进行锁定或加密，并据此直接向用户进行敲诈勒索

勒索软件的基本工作机制 ★ ★ ★ ★

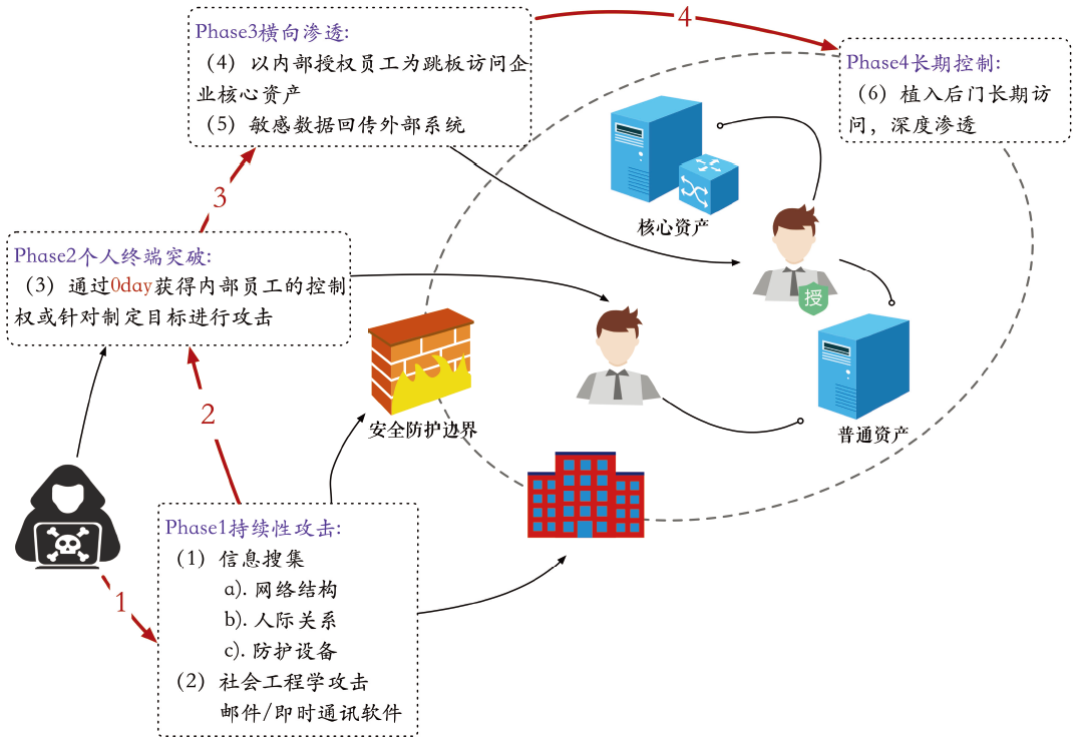
- 垃圾邮件传播
- 水坑攻击传播
- 捆绑传播
- 移动存储介质传播
- 漏洞传播
- 定向攻击

勒索软件的密钥管理机制 ★ ★ ★ ★

- 在用户域解密
- 在攻击者域解密

APT 攻击 ★ ★ ★ ★

高级持续性威胁攻击。指攻击者长期持续地对特定高价值目标进行打击



APT 攻击形式 ★ ★ ★

- 黑客入侵

- 社会工程：鱼叉式攻击、水坑攻击

入侵检测

> 监测点★★★

- NIDS：基于网络地入侵检测系统。采集网络信道中传输的全保温流量
- HIDS：基于主机的入侵检测系统。采集主机中各种对象活动的日志信息和存储数据文件的特征信息，只能对这台被保护的主机进行入侵检测

NIDS

优势

1. 部署方便，成本较低
2. 网络视角不同与主机视角
3. 不易受到攻击者破坏
4. 攻击未达主机，检测及时，响应快速
5. 独立于所保护的主机与系统

劣势

1. 根据网络流量特征进行检测，检测性能依赖与规则的完备性与准确性。
2. 不了解所保护主机，无法判断警报的实用性。
3. 处理加密会话比较困难。

HIDS

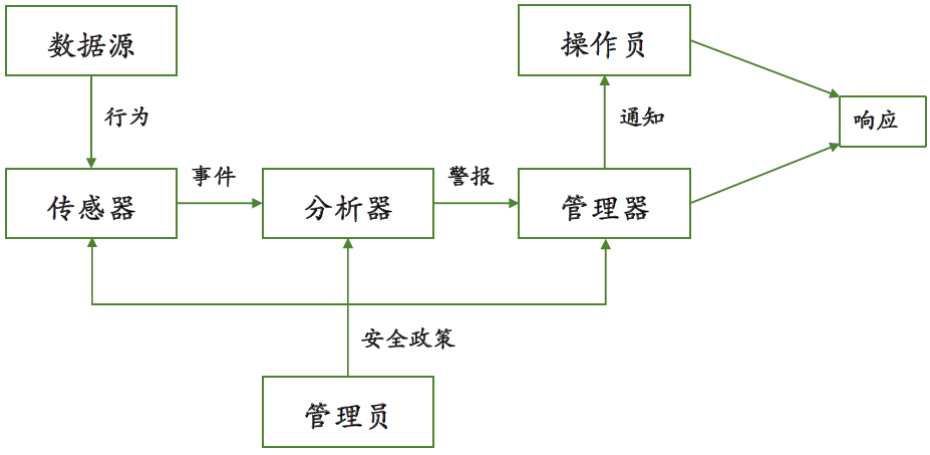
优势

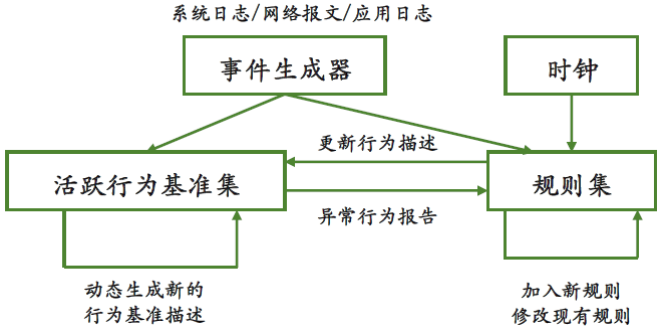
1. 基于主机日志，掌握细节，有助于准确判定
2. 精细地监视主机系统的各种行为与改变、以发现不当之处
3. 比NIDS功能简单、运行开销小、对硬件环境的要求低
4. 可检测不经过网络的攻击

劣势

1. 与所保护主机处于同一运行环境，依赖于本地系统的可靠性
2. 不能阻止成熟的攻击者抹去入侵之后的日志记录
3. 无日志记录的攻击是盲区
4. 安装于所保护主机，耗费资源；引入安全管理困扰

> 网络入侵检测的基本模型★★★★





检测精度★★★

- 误报：假阳性
- 漏报：假阴性
- 基率谬误：个体因为忽视事物发生的概率而做出的错误判断
- 准确率

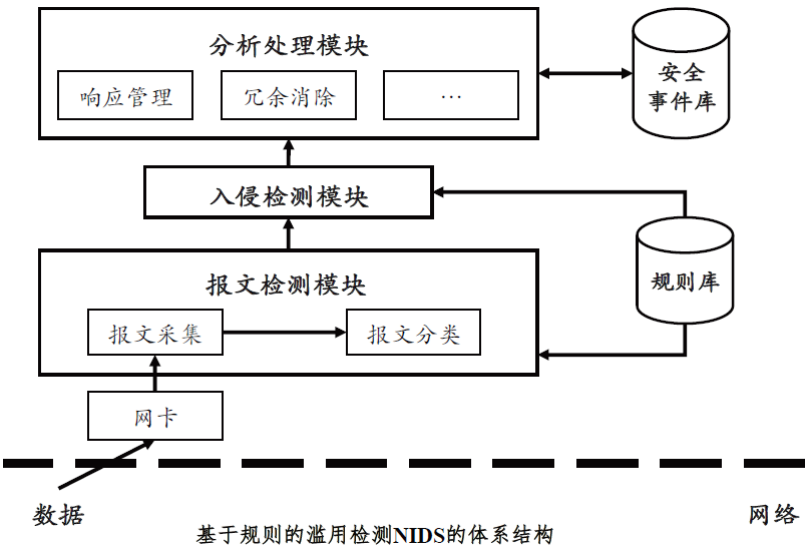
异常行为★★★

数据中不符合预期的行为模式

网络滥用检测★★★

根据已知的攻击特征检测入侵，可以直接检测出入侵行为

滥用检测基本架构★★★



基于规则的滥用检测NIDS的体系结构

数据采集方法★★★

从网络信道中获取传输的报文或其副本，从中提取网络层协议报文

- 广播侦听：局域网中
- 端口映射采集：NIDS 与被保护对象不在同一以太网段中，但汇接于一个公共的以太交换机
- SDN 端口镜像
- 分光采集
- 软件实现：2-copy、0-copy

> 检测规则 ★ ★ ★

侧重点

- 报文负载
- 协议与应用语义

> Snort 检测规则 ★ ★ ★

划分为两个部分：规则头和规则选项

规则头：

- 规则操作：alert、log、pass、activate、dynamic
- 协议
- IP 地址和端口号
- 方向操作符

规则选项：

- 报文特征描述选项
- 规则本身说明选项
- 规则匹配后动作选项
- 某些选项的修饰

> 报文分类 ★ ★ ★

分析器对采集到的报文依据报文中报头部分和/或数据部分的内容在检测规则中寻找匹配

- 面向报头字段
- 面向报文数据部分

> BM 算法 ★ ★ ★ ★

- 坏字符规则

  当文本串中的某个字符跟模式串的某个字符不匹配时，称其为坏字符

  此时模式串向右移动，移动的位数=坏字符在模式串中的位置-坏字符在模式串中最右出现的位置

  若模式串中无坏字符，则位置为-1

- 好后缀规则

  当字符失配时，后移位数=好后缀在模式串中的位置-好后缀在模式出纳上一次出现的位置

  若好后缀没有再次出现，则为-1

> 冗余消除 ★ ★ ★

单个警报信息不完整，逐个警报分别相应也不合理，需要通过警报关联发现重点和核心问题

> 基于相似性的关联判定 ★ ★ ★

- 基于警报属性值：使用距离函数计算
- 基于时序信息：设定时间窗口

计算简单且开销小，语义简单不能发现因果关系

> 基于因果关系的关联判定 ★ ★ ★

- 将因果关系记录为有向图
- 使用机器学习方法：需要有足够数量和质量的训练数据支持

> 蜜罐 ★ ★ ★

是一种安全资源，价值在于被扫描、攻击、攻陷

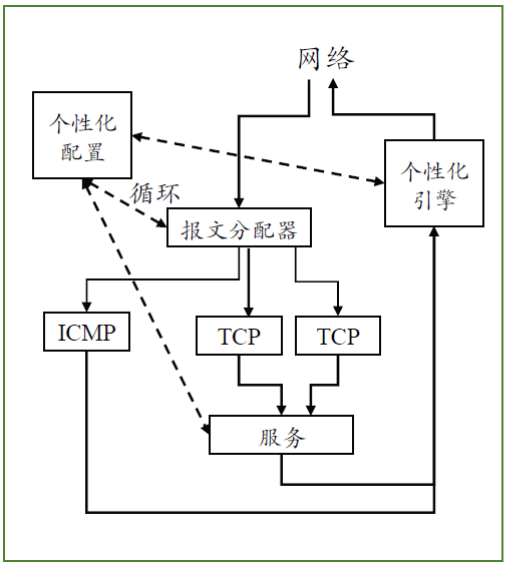
> 蜜罐的分类 ★ ★ ★

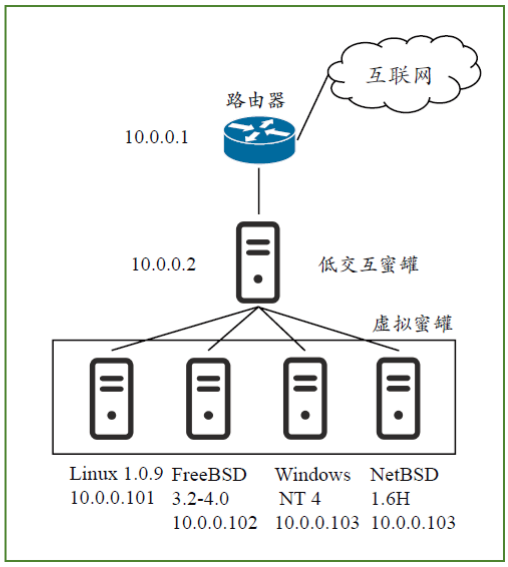
- 应用目的：产品型、研究型
- 交互度：低交互、中交互、高交互
- 实现形式：物理蜜罐、虚拟蜜罐

> 蜜罐的部署 ★ ★ ★

- 放在防火墙外面：消除防火墙后出现系统被攻陷的危险性、捕获不到内部攻击者
- 放在非军事区（DMZ）：攻击者一般选择此处做跳板，采集到的攻击类型有局限性
- 放在防火墙后面：信息量最多，引入新的威胁，需要区别对待

> 蜜罐的实现 ★ ★ ★





> 蜜罐的核心机制 ★ ★ ★

- 欺骗环境构建机制
- 威胁数据捕获机制
- 威胁数据分析机制

网络安全防御

> 系统的可生存性 ★ ★ ★

系统在有意外、攻击和故障的条件下能够及时完成其被指派任务的能力

- 性质保持
- 整体性能保持

可生存性需要考虑 R3A

- 对攻击的抵御能力
- 具有检测和评估损失的能力
- 服务的恢复能力
- 自适应性

> 可生存性相关工作 ★ ★ ★ ★ ★

- 入侵防范：在系统的各个层次建立兼顾的屏障以抵御网络入侵攻击
- 入侵检测：以尽可能低的漏报率和误报率来检测出现在本地系统中的攻击，发现那些对其它系统有影响的安全事件
- 入侵容忍：在丧失部分系统和功能的情况下，是系统最大化地保持关键运行的能力

> 网络的纵深防御★★★

步数网络入侵检测系统、主机入侵检测系统、防火墙等

> 漏洞扫描★★★

- 检测联网主机允许外部访问的服务种类。通过观察某个端口是否可以交互，来判断对应的服务是否可用
- 进一步获取这个服务实现的某些指纹信息，然后利用先验知识来判断对方是否有漏洞可以利用

> 基于 TCP 的端口扫描★★★★★

- TCP connect扫描：调用connect。不需要特权就可以调用，速度快，但容易被察觉并过滤
- TCP SYN扫描：发送 TCP SYN 报文，若返回 TCP ACK/SYN 则说明开放，若返回 TCP RST 则不可达。不留痕迹，但扫描者需要有超户权限
- TCP FIN扫描：发送 TCP FIN 报文，关闭情况下会返回 TCP RST，开放状态下会忽略。一些情况下开放关闭都会返回 TCP RST，扫描不够隐蔽，会被基于阈值检测的防火墙或 NIDS 发现拦截
- TCP 空闲扫描：探测将是主机 IP 及当前 IP ID；伪造一个以僵尸主机位源地址的 TCP SYN 报文，发送给主机，若返回了报文，则会导致 IP ID 改变；若端口开放，则+2，若关闭或过滤，则+1

> UDP ICMP 端口扫描★★★★★

发送UDP 报文，若返回 ICMP-PORT-UNREACH 报文，则对应端口关闭。

需要发送多个报文确认状态，速度较慢，且接收需要超级用户权限

> 扫描对象选择★★★★

- 遍历性扫描：顺序扫描、选择性随机扫描、拓扑扫描
- 针对性扫描：基于目标列表的扫描、基于路由的扫描、基于 DNS 的扫描

> 扫描方式★★★★★

- 水平扫描：针对一个端口号，一定范围内的主机
- 垂直扫描：针对一个主机的所有端口
- 显示扫描
- 隐式扫描：被动式扫描、基于间接通信的扫描、TCP空闲扫描

> 扫描工具 nmap★★★

采用垂直扫描

- 主机发现
- 端口扫描
- 服务侦测
- 系统侦测

> 扫描工具 zmap ★ ★ ★

全球互联网安全扫描

- 不支持脚本
- 无状态请求方法，有更高的并发扫描效率
- 每次发送多个报文
- 随机方式生成扫描地址（乘法循环群）
- 对每个扫描任务设置一个任务密钥，作为 识别一句

> 攻击图 ★ ★ ★

由一系列攻击行为构成，描述了攻击者在网络系统中利用系统脆弱性进行渗透，逐步提升权限的过程

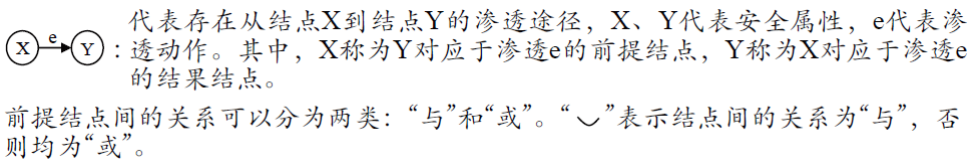
采用有向图来表示，分为状态列举表示法和渗透依赖表示法

能够检测安全扫描不能直接发现的系统脆弱性以及脆弱性之间的关系

- 目标模型构建
- 攻击图构建
- 攻击图分析

> 基于攻击图的评估方法 ★ ★ ★

- 根据安全漏洞的特征在系统中寻找匹配，这部分是直接的安全漏洞
- 寻找漏洞之间的关联关系及系统配置之间可能导致漏洞的关联关系



> 协同防御 ★ ★ ★

综合 IDS 的检测结果或在 IDS 间共形检测信息

> 入侵检测组件协同场景 ★ ★ ★

- 分析

- 互补
- 互纠
- 核实
- 调整
- 响应

> 入侵协同阻断系统 ★ ★ ★

拦截流量或攻击交互。常使用防火墙或其它攻击拦截技术

> 基于 GrIDS 的系统防御 ★ ★ ★ ★

支持 IDIP 协议的系统，又称为网关。是进行入侵检测协同和攻击拦截的基本单位

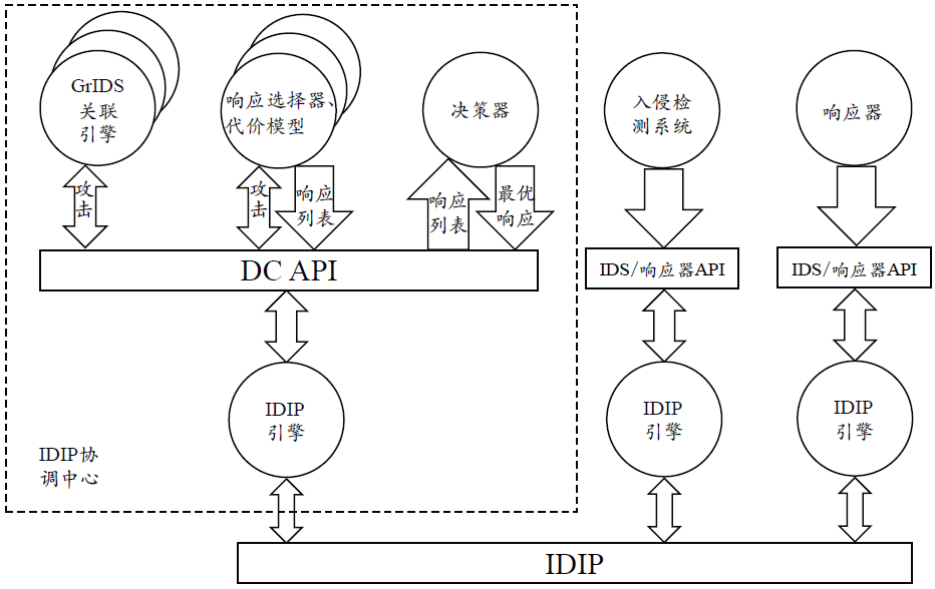
> CITRA 的系统架构 ★ ★ ★ ★

在网络边界内追踪入侵者、组织或者减少入侵造成的后续破坏、汇集入侵活动情况

工作原则：使得响应是高成功率的、短期的；基于代价模型进行响应选择计算

优势：集中控制和分布式实施结合，具有良好的适应性和灵活性

核心组件：GrIDS、DC（攻击聚合、相应选择、响应优化）



网络攻击阻断

> 防火墙 ★ ★ ★

是网络之间一种特殊的访问控制措施，用于隔离互联网的某一部分，限制这部分和互联网其他部分之间数据的自由流动

> 防火墙的基本架构 ★ ★ ★

> 防火墙的实现 ★ ★ ★

- 网络设备中的软件模块：ACL功能
- 主机中的软件工具：代理、个人防火墙
- 独立设备：基于交换机的独立设备、数据包级或者应用级的过滤器

> IP 级防火墙 ★ ★ ★ ★

报文过滤防火墙，位于网络层，通常在路由器实现，报文过滤只根据 IP 地址和端口号

过滤规则记录在访问控制列表中（ACL）

对报文可以转发、报错、丢弃、备忘

> 过滤规则 ★ ★ ★

- 内向流量：源在外宿在内
- 外向流量：源在内宿在外
- 内向服务：服务器在外客户在内
- 外向服务：服务器在内客户在外

> 规则处理 ★ ★ ★

> 状态检测 ★ ★ ★

状态：通信会话的存在条件

> 状态检测防火墙 ★ ★ ★ ★

不仅检查 IP 报头内容，还检查 TCP/UDP 或更高层协议报头内容

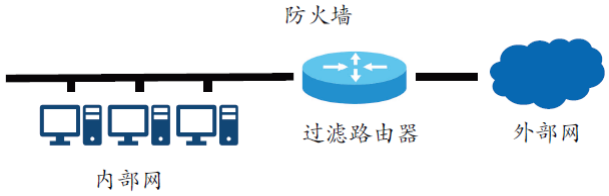
以 TCP 连接为过滤单位

再系统内部建立允许通过连接或流的状态信息表，每个连接按形如源 IP 地址、宿 IP 地址、源端口、宿端口、传输协议的五元组进行标识

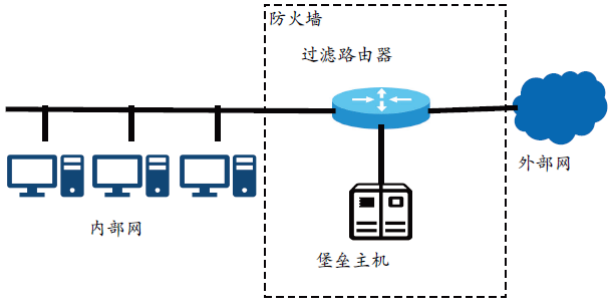
只需对每个连接的第一个报文进行过滤规则检查，其后报文的处理根据状态表来确定

> 防火墙的使用★★★

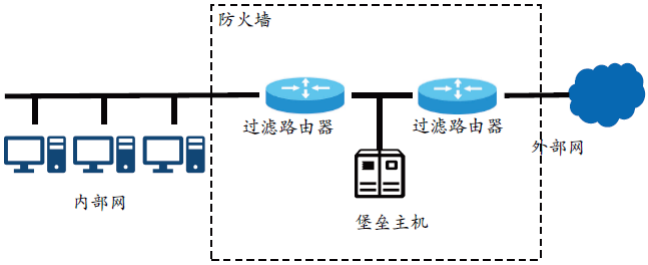
- 路由器过滤方式（有孔过滤）：实施成本低、增加边界路由器负担、不能防范基于非正常使用方式的流量



- 主机过滤方式（堡垒主机）：将需要外部访问的服务放置在堡垒主机中



- DMZ：DMZ 和外部网开孔，和内部网无孔。过滤表内容简单



- 网关：适用于 WAF

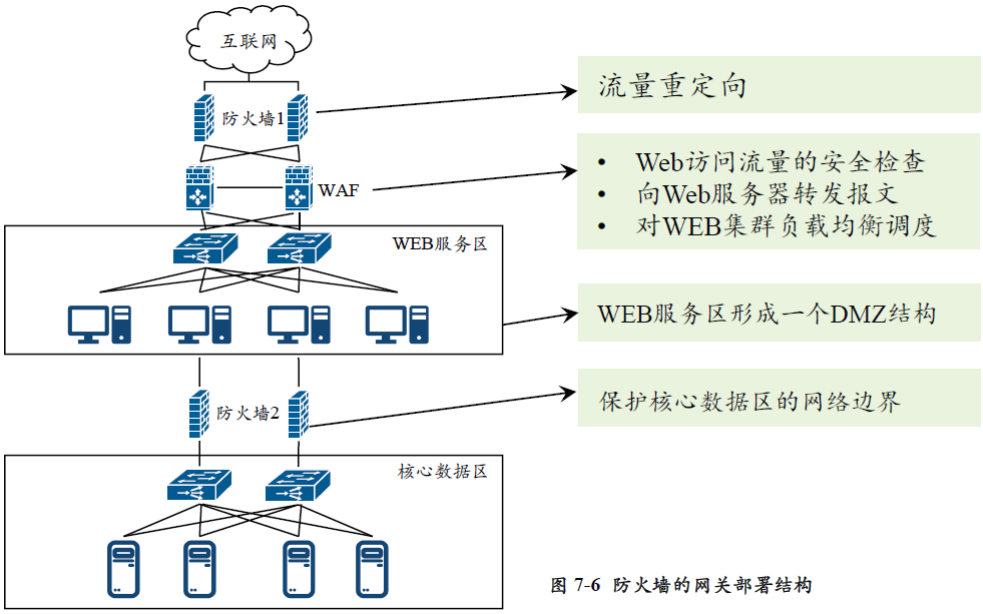


图 7-6 防火墙的网关部署结构

计算机取证★★★

- 计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与提取
- 以一种法律认可的方式鉴定、保存、分析和递交数字证据的过程
- 以一种尽可能避免扭曲、偏离的方式收集和分析数据以重构数据或重建系统中过去发生的事件
- 一门获取、保存、恢复和递交经过电子处理和存储在计算机媒体中的数据的学科

黑色郁金香事件发现过程★★★

黑色郁金香事件响应过程★★★

黑色郁金香数字取证调查过程★★★

网络安全访问

认证与鉴别★★★

鉴别是证实信息交换过程和处理对象真实性的一种手段，包括对处理对象的鉴别和对处理动作的鉴别。

鉴别包括证实处理对象的真实性、证实交互动作的真实性、证明信息的时效性

零知识证明★★★

允许用户表明他指导某个秘密而不需把这个秘密说出来，避免口令内容传递

由验证者提出问题，证明者回答问题。容易受到桥接攻击

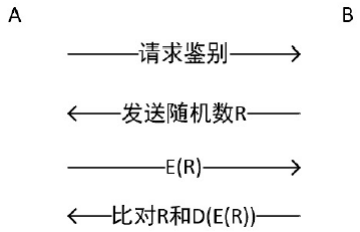
单向鉴别 ★★★

假设：对 A 而言，B 是完全可信的，B 需要鉴别 A

方法：A 使用自己的唯一性信息证明自己的身份，一般是自己的口令

- 对称加密

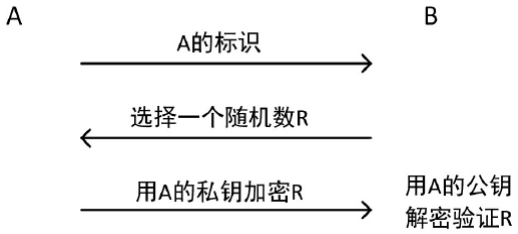
  A 和 B 共享一个密钥

  缺点：要求 B 是可靠的、密钥需要经常更换、攻击者可以冒充 B

  改进：B 向 A 发送 R 的加密形式，A 解密发回；A 请求鉴别时直接发送一个用共享密钥加密的时间标记

- 非对称加密

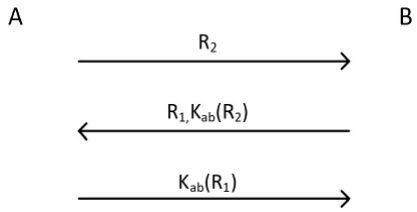
  

  特点：攻击者可以冒充 B 发送 $E_A(X)$ 作为 R 给 A，哄骗 A 解出 X

  方法的安全性依赖于所获得公钥的真实性

双向鉴别 ★★★

- 对称密钥

  容易受到中间人攻击（桥接攻击）

  措施：使用不同的密钥；使用不同的明文值，利用特征信息鉴别

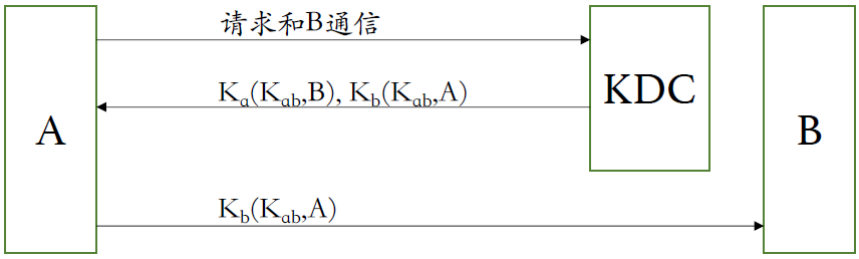
SSO ★★★★

单点登录功能

通过将可信中继的登陆映射到各个应用中，避免了用户再使用不同应用时的重复登录

> 可信中继模型★★★

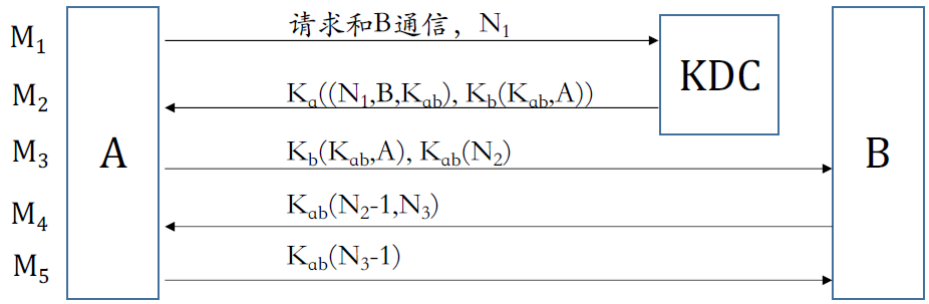
使用密钥分配中心（KDC）来保存和传递密钥



可信中继是 SSO 的主要支撑技术

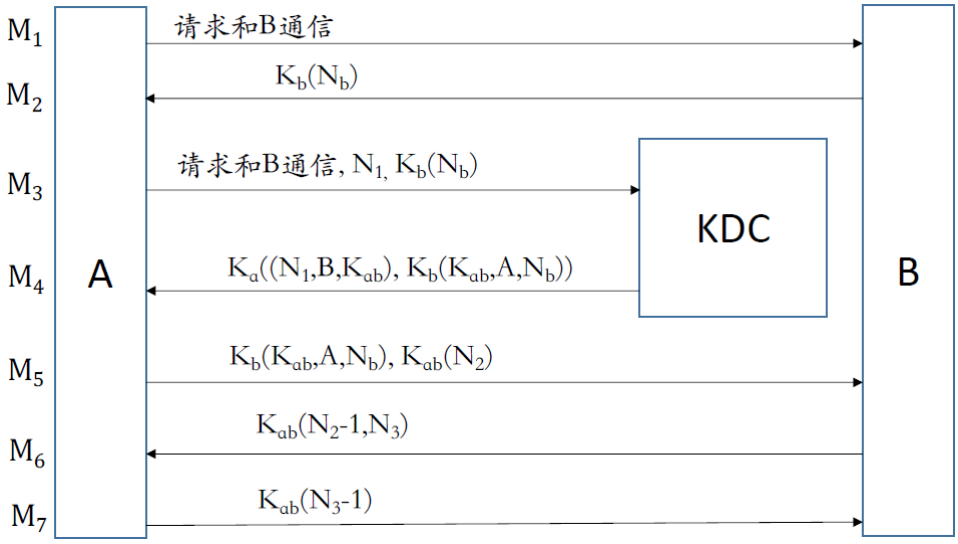
> Needham-Schroeder Scheme★★★★

密钥分配+双向鉴别



向 KDC 申请密钥和使用密钥的过程是分离的，导致基于时间差的攻击

扩展的 Needham-Schroeder Scheme



> 鉴别中的身份信息管理问题★★★

- 用户的身份是可以变化的，集中鉴别管理机制用当有能力为不同的应用系统提供不同的授权信息
- 鉴别范围的限制

> 身份管理★★★

目的是使合法用户再异构环境中能以合理的理由在核实的事件访问恰当的资源

用户首先在身份提供者（IdP）处作者测，当用户希望访问某个被保护的应用时

- 用户向应用提出访问请求
- 应用委托服务提供者（SP）提出要求；SP 将鉴别要求和授权要求提交给 IdP
- IdP 生成响应的鉴别和授权信息给 SP

> 匿名通信★★★

考虑的是发送者和接收者也是机密信息的场合。攻击者希望得到的是端系统之间的通信关系、端系统发送和接收活动信息

- 发送者匿名：消息对发送者的无关联性
- 接收者匿名：消息对接收者的无关联性
- 关系匿名：消息对发送者与接收者的无关联性
- 无连接性：消息之间的无关联性

> 广播方法★★★

通过广播实现接收者匿名，该接收者被赋予一个其它参与者不能识别的暗示地址

DC-net 可实现发送者匿名

- 由所有的端系统向信关发送一个数据。其中用户数据发送者将要发送的用户信息 S 与其它所有密钥做异或，其余发送者直接对密钥做异或
- 由信关向所有端系统广播一个数据。信关做异或得到 S 并发送

> Tor★★★★

- 洋葱路由

  在报文转发的过程中改写源点信息。这种方法称为源重写技术

  洋葱路由：基于嵌套的 IP 隧道技术。第一个节点是服务代理，负责源路由的分配。每一跳收到报文后，对最外层解密，获得下一跳信息

  使用非对称密钥系统，使用各节点的公钥加密下游节点的信息

  转发出替换报头源地址可以实现发送者匿名，替代关系需要保留在中继节点

- Tor 匿名网络

  由一组可信的权威目录服务器和数千个志愿加入的路由器组成

传输中继路由器定期从某个目录服务器获取整个网络的节点信息，包括 IP 和公钥

发送者的 Tor 客户端从目录服务器获取 Tor 路由器列表，随机选取三个构成一个序列，然后封装发送

提供的是发送者和接收者的关系匿名服务，不提供数据保密服务

网络基础设施保护

> 安全的依赖性 ★ ★ ★

> 常用保护机制 ★ ★ ★

- 端口安全
- DHCP 窥探
- 动态 ARP 检测
- IP 源保护

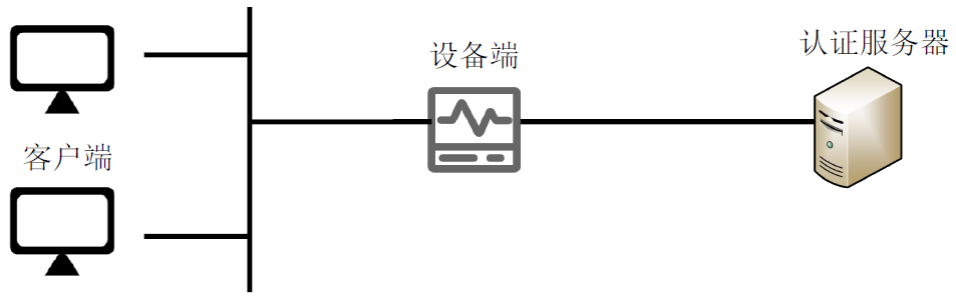
> 802.1X 基本原理 ★ ★ ★ ★

基于端口的接入控制

设备端为客户提供的接入局域网的端口有两种

- 非受控端口：发出或接收认证报文
- 受控端口：传递业务帧

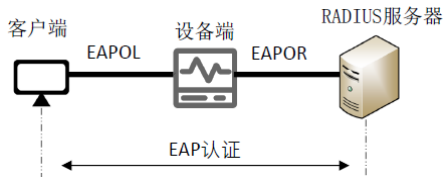
> 802.1X 基本构架 ★ ★ ★ ★



- 客户端是请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持802.1X认证的客户端软件。
- 设备端是局域网中控制客户端接入的网络设备，例如NAS，位于客户端和认证服务器之间，为客户端提供接入局域网的端口(物理端口或逻辑端口)，并通过与认证服务器的交互来对所连接的客户端进行认证。

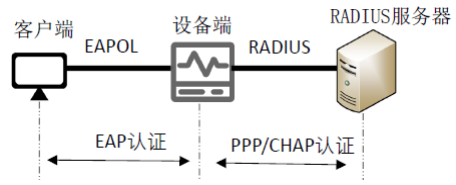
- 认证服务器用于对客户端进行认证、授权和计费，通常为RADIUS服务器。认证服务器根据设备端发送来的客户端认信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即将服务器的功能也实现在设备端。

基于 MD-Challenge 的 EAP 中继方式认证过程 ★ ★ ★

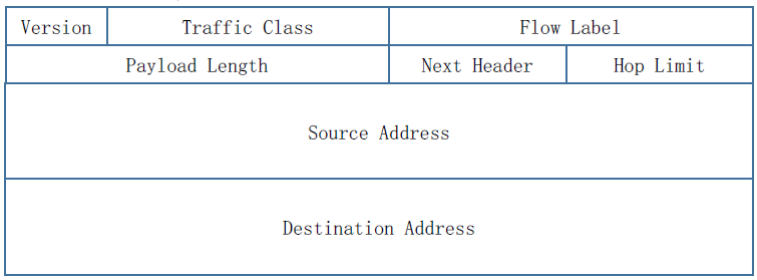


设备端仅进行中转，处理简单。但 RADIUS 服务器要支持相应的 EAP 认证方法

基于 CHAP 的 EAP 终结方式认证过程 ★ ★ ★



IPv6 报头格式及其改进 ★ ★ ★



IPsec ★ ★ ★

包括访问控制、无连接传输的完整性保护、数据源鉴别、回访报文的检测与剔除、基于加密的数据内容保密、数据流保密

主要通过鉴别头 AH、负载安全封装 ESP、密钥管理协议 IKEv2提供

服务方式：传输模式、隧道模式

实现方式：

- 集成在现有的 IP 中
- BITS：实现在已有的 IP 协议栈下
- BITW：实现在独立的加密机中

IPsec 系统架构 ★★★★

- SPD 安全策略库：存放已定义的各种安全策略，以确定如恶化分解到达和离去的 IP 流量

  类似于 ACL，主要内容是选择符（适用于谁）和处理要求

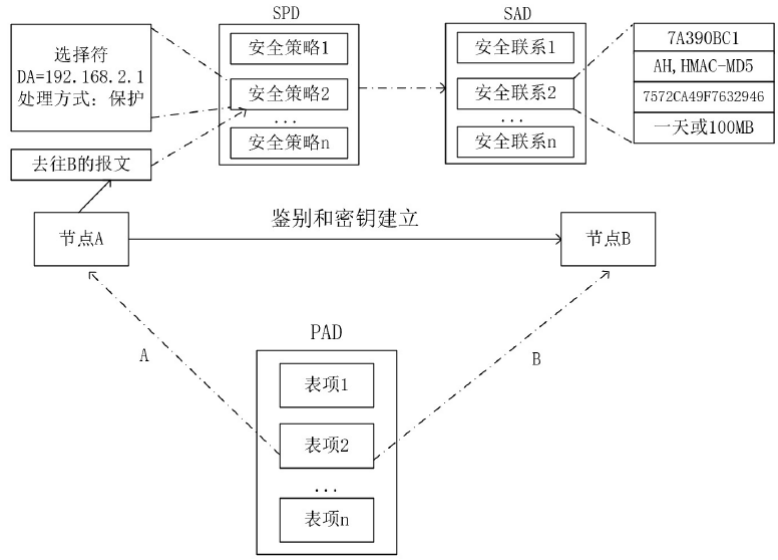
  报文处理方式有：丢弃、旁路、保护

  SPD 分为 3 各部分：SPD-S（保护）、SPD-O（离去流量旁路和丢弃）、SPD-I（进入流量旁路和丢弃）
- SAD 安全联系库：保存已建立的各个安全联系的各种参数，IPsec 的安全规程将根据这些参数来处理受保护的 IP 报文

  包括：基本参数、密码学参数、传输参数、标记参数

  查找内容：SPI、宿地址、源地址
- PAD 对等授权库：提供安全联系管理协议和 SPD 之间的对应关系

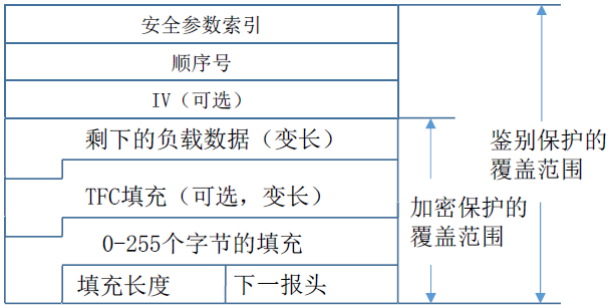
报文处理流程 ★★★



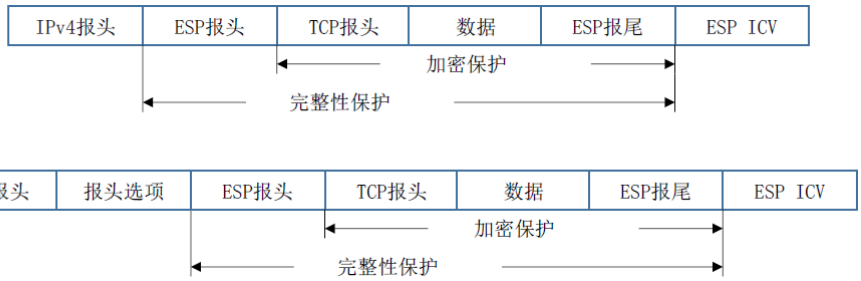
ESP ★★★

提供保密性、完整性、防回放服务

报头格式



传输模式



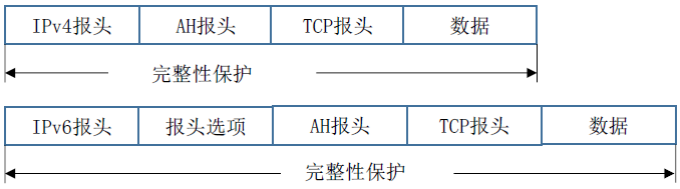
AH ★★★

提供完整性保护、IP 报文源点鉴别、防回放攻击

不提供加密服务

报头格式

传输模式



DNS 安全威胁 ★★★

- 域名解析欺骗攻击
- 失效服务攻击：路由劫持、DDos
- 服务窃取攻击
- 抢占

DNSSEC ★★★

- 增加新的安全资源记录并使用数字签名来保护域名数据库中各个资源记录的完整性
- 使用TSIG协议来实现在主从DNS服务器之间带鉴别的域拷贝和对主服务器的更新
- 增加关于公钥的资源记录以在全球互联网中形成一个统一开放的关于域名的PKI体系和DNS解析服务的信任链

DNSSEC 新增的资源记录 ★ ★ ★

DNSSEC 的信任链 ★ ★ ★ ★

- 安全的域名服务器：支持 DNSSEC 的 DNS 服务器
- 安全的解析器：支持 DNSSEC 的 DNS 解析器
- 鉴别链：描述构成域名解析路径的各个域名服务器之间的信任关系
- 鉴别密钥：供安全的 DNS 解析器用来验证解析结果签名的公钥
- 密钥签名密钥：在一个域名中用于签名保护其它鉴别密钥的密钥
- 域名签名密钥：用于域名中的域名记录进行签名保护的密钥

DNSSEC 使用 ★ ★ ★ ★

DNSSEC 部署 ★ ★ ★