

网络通信中面临的4种安全威胁

■ 截获：窃听通信内容

■ 中断：中断网络通信

■ 篡改：篡改通信内容

■ 伪造：伪造通信内容



网络层 — ARP欺骗

■ ARP欺骗 (ARP spoofing) , 又称ARP毒化 (ARP poisoning) 、ARP病毒、ARP攻击

■ ARP欺骗可以造成的效果

□ 可让攻击者获取局域网上的数据包甚至可篡改数据包

□ 可让网络上特定电脑之间无法正常通信 (例如[网络执法官](#)这样的软件)

□ 让送至特定IP地址的流量被错误送到攻击者所取代的地方

□

ARP欺骗 — 核心步骤举例

- 假设主机C是攻击者，主机A、B是被攻击者
- C只要收到过A、B发送的ARP请求，就会拥有A、B的IP、MAC地址，就可以进行欺骗活动
- C发送一个ARP响应给B，把响应包里的源IP设为A的IP地址，源MAC设为C的MAC地址
- B收到ARP响应后，更新它的ARP表，把A的MAC地址 (IP_A, MAC_A) 改为 (IP_A, MAC_C)
- 当B要发送数据包给A时，它根据ARP表来封装数据包的头部，把目标MAC地址设为MAC_C，而非MAC_A
- 当交换机收到B发送给A的数据包时，根据此包的目标MAC地址 (MAC_C) 而把数据包转发给C
- C收到数据包后，可以把它存起来后再发送给A，达到窃听效果。C也可以篡改数据后才发送数据包给A

ARP欺骗 — 防护

- 静态ARP

- DHCP Snooping

- 网络设备可借由DHCP保留网络上各电脑的MAC地址，在伪造的ARP数据包发出时即可侦测到

- 利用一些软件监听ARP的不正常变动

- ...

DoS、DDoS

■ DoS攻击（拒绝服务攻击，**Denial-of-Service** attack）

□ 使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问

■ DDoS攻击（分布式拒绝服务攻击，**Distributed Denial-of-Service** attack）

□ 黑客使用网络上两个或以上被攻陷的电脑作为“僵尸”向特定的目标发动DoS攻击

□ 2018年3月，GitHub遭到迄今为止规模最大的DDoS攻击

■ DoS攻击可以分为2大类

□ 带宽消耗型：UDP洪水攻击、ICMP洪水攻击

□ 资源消耗型：SYN洪水攻击、LAND攻击

DoS、DDoS防御

- 防御方式通常为：入侵检测、流量过滤、和多重验证
 - 堵塞网络带宽的流量将被过滤，而正常的流量可正常通过
-
- 防火墙
 - 防火墙可以设置规则，例如允许或拒绝特定通讯协议，端口或IP地址
 - 当攻击从少数不正常的IP地址发出时，可以简单的使用拒绝规则阻止一切从攻击源IP发出的通信
 - 复杂攻击难以用简单规则来阻止，例如80端口遭受攻击时不可能拒绝端口所有的通信，因为同时会阻止合法流量
 - 防火墙可能处于网络架构中过后的位置，路由器可能在恶意流量达到防火墙前即被攻击影响
 - 交换机：大多数交换机有一定的速度限制和访问控制能力
 - 路由器：和交换机类似，路由器也有一定的速度限制和访问控制能力

DoS、DDoS防御

■ 黑洞引导

- 将所有受攻击计算机的通信全部发送至一个“黑洞”（空接口或不存在的计算机地址）或者有足够能力处理洪流的网络设备商，以避免网络受到较大影响

■ 流量清洗

- 当流量被送到DDoS防护清洗中心时，通过采用抗DDoS软件处理，将正常流量和恶意流量区分开
- 正常的流量则回注回客户网站

传输层 — SYN洪水攻击

■ SYN洪水攻击 (SYN flooding attack)

□ 攻击者发送一系列的SYN请求到目标，然后让目标因收不到ACK（第3次握手）而进行等待、消耗资源

■ 攻击方法

□ 跳过发送最后的ACK信息

□ 修改源IP地址，让目标送SYN-ACK到伪造的IP地址，因此目标永不可能收到ACK（第3次握手）

■ 防护

□ 参考：[RFC 4987](#)

传输层 — LAND攻击

- LAND攻击（局域网拒绝服务攻击，Local Area Network Denial attack）
 - 通过持续发送**相同源地址和目标地址**的欺骗数据包，使目标试图与自己建立连接，消耗系统资源直至崩溃
- 有些系统存在设计上的缺陷，允许设备接受并响应来自网络、却宣称来自于设备自身的数据包，导致循环应答
- 防护
 - 大多数防火墙都能拦截类似的攻击包，以保护系统
 - 部分操作系统通过发布安全补丁修复了这一漏洞
 - 路由器应同时配置上行与下行筛选器，屏蔽所有源地址与目标地址相同的数据包

应用层 — DNS劫持

- DNS劫持，又称为域名劫持

- 攻击者篡改了某个域名的解析结果，使得指向该域名的IP变成了另一个IP
- 导致对相应网址的访问被劫持到另一个不可达的或者假冒的网址
- 从而实现非法窃取用户信息或者破坏正常网络服务的目的



- 为防止DNS劫持，可以考虑使用更靠谱的DNS服务器，比如：114.114.114.114

- 谷歌：8.8.8.8、8.8.4.4

- 微软：4.2.2.1、4.2.2.2

- 百度：180.76.76.76

- 阿里：223.5.5.5、223.6.6.6

- HTTP劫持：对HTTP数据包进行拦截处理，比如插入JS代码

- 比如你访问某些网站时，在右下角多了个莫名其妙的弹窗广告