

U 盘和 Wifi 是如何偷走我们的隐私的

王曦 2021192010

数学与统计学院

计算机伦理

2023 年 06 月 02 日

1. U 盘的被动攻击：计算机窃取 U 盘文件

U 盘里的隐私是如何泄露的

- 我们中学的时候, 老师们常用 U 盘将课件拷贝到教室的电脑上, 同学们常用 U 盘将课件拷贝到自己电脑上.
- 当你将 U 盘插入电脑, 你的隐私是如何泄露的?
- 视频演示: U Disk Theif.

2. U 盘的主动攻击: U 盘木马

U 盘木马

- U 盘下有个文件 “autorun.inf”.
- 合理、合法地利用计算机技术.

- 对策:

(1) 不将自己的 U 盘插入不可信任的计算机, 也不将不可信任的 U 盘插入自己的计算机.

(2) 用微信文件传输助手或网盘等传输文件.

(3) 虚拟机だめ: 用 NAT 桥接等方式穿透虚拟机以感染宿主机 (病毒逃逸).

3. Wi-Fi 的被动攻击: Wi-Fi 探针与“盒武器”

Wi-Fi 探针

- 手机打开 WLAN 开关: 向周围广播, 发送探测请求帧.
- 无线路由器: 发送信标帧, 告诉手机此处有 Wi-Fi 可连. 路由器在信号范围内截获请求帧, 且通过身份认证和连接许可, 即提供网络服务.
- Wi-Fi 探针: 可截获请求帧, 并获取设备的 MAC 地址, 一般不提供网络服务.
- Wi-Fi 探针可根据获取的 MAC 地址、信号强度、时间等信息定位 Wi-Fi 设备, 计算出区域内 Wi-Fi 设备的位置分布.
- 应用: 人流异常预警、徘徊人员预警、客流监测.

Wi-Fi 探针与“盒武器”

- MAC 地址只是网卡的身份证, 不属于用户的隐私信息.
 - Wi-Fi 探针获取到的 MAC 地址, 与其他手机 App 获取到的设备序列号 (IMEI)、MAC 地址、手机号码等信息结合, 查表即得某人在何区域内出现过.
 - 《中华人民共和国公安部令》中对互联网安全保护技术措施的规定: 提供互联网连接的设备需备案.
 - Wi-Fi 探针不提供网络服务, 无需备案, 且可合法购买.
-
- 手机对策: 发送探测请求帧时使用随机伪 MAC 地址.
 - Wi-Fi 探针对策: 伪造成无密码的公共 Wi-Fi 诱导用户连接, 提供网络服务, 以获取真实的 MAC 地址.
 - 治标不治本的方法: 在不信任的公共场所不打开 WLAN 开关, 尽量使用流量上网. 根本原因还是穷.

4. Wi-Fi 的主动攻击: ARP 欺骗

ARP 欺骗

- 前提: 同属一个局域网.

(1) 用 Kali 扫描网络, 对要攻击的对象所连的 WLAN 抓包, 通过弱密码字典破解获得密码.

(2) 连接对应 WLAN, 此时处于同一局域网.

- ARP 欺骗: 用 Kali 伪造网关.

(1) 接收数据但不应答: 断网攻击.

(2) 接受数据并应答: 中间人攻击.

谢 谢!

Thank you!