# 路由器如何泄露你的秘密：Wi-Fi网络中的TCP劫持攻击

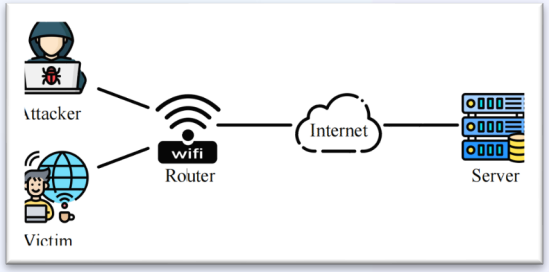
——**杨宇翔**，冯学伟，李琦，孙琨，王自强，徐恪

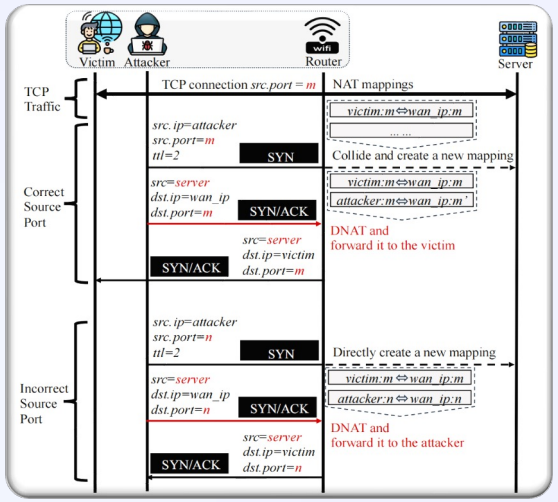
## 背景

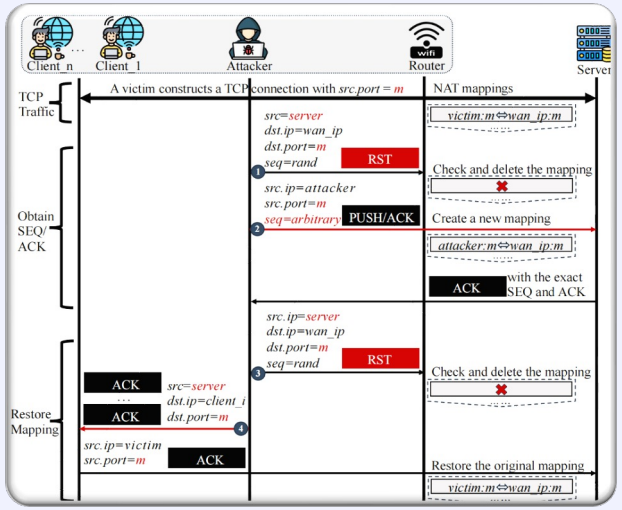
随着无线安全机制（如WPA2/WPA3）的部署和其他保护策略（如AP隔离、ARP防护、流氓AP检测）的采用，同一Wi-Fi网络中的off-path攻击者（即无法控制路由器）难以获得其他客户端与外部服务器之间的通信信息。

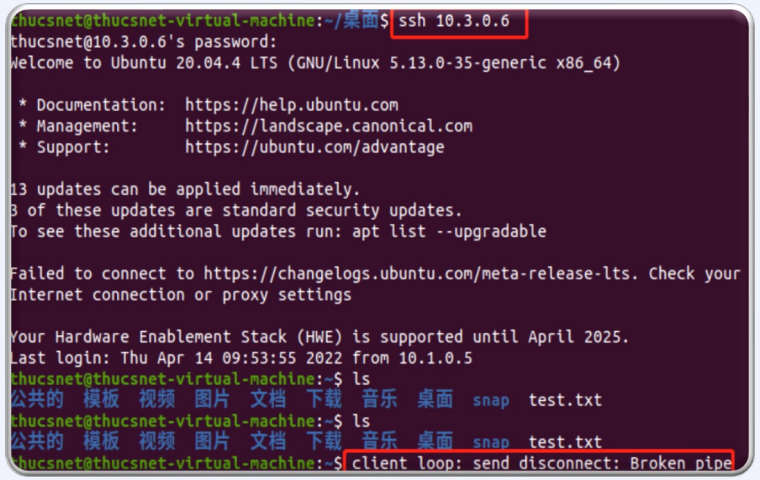
## 发现

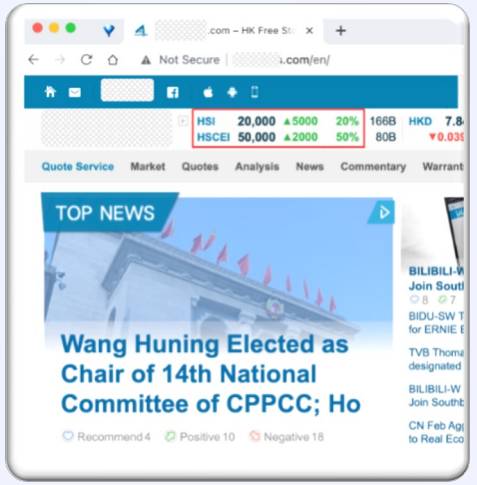
在本工作中，我们发现路由器在NAT时采用了**端口保留策略，不检测TCP报文的序列号，且未开启反向地址验证**，使得Wi-Fi网络中的恶意攻击者能够劫持其他用户与外界服务器TCP的通信。图1显示了该攻击的威胁模型。




## 攻击步骤

- 探测路由器的外部IP地址并扫描潜在受害者客户端；
- 基于路由器采用**端口保留策略**和**缺乏反向地址验证**漏洞，发送伪造的TCP SYN和SYN/ACK报文，来推断client和server之间是否存在TCP连接。
- 基于路由器**缺乏TCP序列号检查**和**缺乏反向地址验证**漏洞，利用伪造的RST数据包清除路由器原有NAT映射，并重建新的映射，从而拦截服务器发送给受害者的TCP报文，获取其中的序列号和确认号。

## 攻击效果

- **TCP拒绝服务攻击**：终止受害者 TCP 连接，如阻断加密连接（SSH等）；
- **TCP劫持攻击**：截获服务器响应，如从FTP服务器下载私人文件；
- **TCP注入攻击**：向受害者客户端回复伪造响应，如HTTP缓存污染。

# 路由器如何泄露你的秘密：Wi-Fi网络中的TCP劫持攻击

——**杨宇翔**，冯学伟，李琦，孙琨，王自强，徐恪

## 路由器测试

我们总共对**30家厂商的67款主流路由器**进行了测试，发现其中来自24家厂商的52款路由器容易受到该攻击的影响(包括360、Aruba、Amazon、Huawei、 Linksys、TP-Link、biquiti、Xiaomi、 H3C等厂商)，测试结果如下表：

## 实证研究

我们对**93个真实世界的Wi-Fi网络**进行了广泛的测量研究，发现75个（81%）真实Wi-Fi网络容易遭受该攻击影响。我们的案例研究表明，终止SSH连接、从FTP服务器下载私人文件和注入虚假HTTP响应包平均需要**17.5**、**19.4**和**54.5**秒，成功率分别为**87.4%**、**82.6%**和**76.1%**。

## 漏洞披漏

我们负责任地向受影响的厂商上报了该漏洞。截至目前，已收到 OpenWrt 社区和**七个路由器厂商**（即 TP-Link、华为、小米、360、Mercury、Ubiquiti 、Linksys）的确认。此外，我们还被分配了针对不同供应商的**10个CVE编号**（即TP-Link、Linksys、Mercury、锐捷、D-Link、Comfast、H3C、OpenWrt、Wavlink和360）。

TABLE I. PARTIAL TESTED ROUTERS FROM 30 VENDORS

| No. | Router Model | Vendor | OS | Generation | Port Preservation | Reverse-path Validation Disabled | TCP Window Tracking Disabled | TCP Close Timeout (second) | Vulnerable |
|---|---|---|---|---|---|---|---|---|---|
| 1 | TL-XDR6020 | TP-Link | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 2 | TL-WDR7620 | TP-Link | Vxworks-based | Wi-Fi 5 | ✔ | ✘ | ✔ | 1 | ✘ |
| 3 | AX3 Pro | Huawei | EMUI (Linux-based) | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 4 | AR6140E-9G-2AC* | Huawei | VRP (Linux-based) | - | ✘ | ✘ | ✔ | 10 | ✘ |
| 5 | V6G | 360 | 360OS(Linux-based) | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 6 | Magic R365 | H3C | Comware(Linux-based) | Wi-Fi 5 | ✔ | ✔ | ✔ | 10 | ✔ |
| 7 | W30E | Tenda | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 8 | RAX1800Z | China Mobile | AOS(Linux-based) | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 9 | X32 Pro | Ruijie | RGOS(Linux-based) | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 10 | Redmi RA81 | Xiaomi | MiWiFi(Linux-based) | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 11 | MW300R | Mercury | Vxworks-based | Wi-Fi 4 | ✔ | ✘ | ✔ | 1 | ✘ |
| 12 | X30G | Mercury | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 1 | ✔ |
| 13 | RAX50 | Netgear | DumaOS(Linux-based) | Wi-Fi 6 | ✔ | ✘ | ✔ | 10 | ✘ |
| 14 | RT-AX89X | ASUS | AsusWrt(Linux-based) | Wi-Fi 6 | ✔ | ✘ | ✔ | 10 | ✘ |
| 15 | E9450 | Linksys | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 16 | QUANTUM D2G | Wavlink | Linux-based | Wi-Fi 5 | ✔ | ✔ | ✔ | 10 | ✔ |
| 17 | CF-616AC | Comfast | OrangeOS(Linux-based) | Wi-Fi 5 | ✔ | ✔ | ✔ | 10 | ✔ |
| 18 | DI-7003GV2* | D-Link | Linux-based | - | ✔ | ✔ | ✔ | 1 | ✔ |
| 19 | AX3000 | ZTE | ZXR10ROS(Linux-based) | Wi-Fi 6 | ✔ | ✘ | ✔ | 10 | ✘ |
| 20 | M80* | IP-COM | Linux-based | - | ✔ | ✔ | ✔ | 1 | ✔ |
| 21 | SK-WR6640X | Skyworth | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 22 | VE5200G* | Volans | Linux-based | - | ✔ | ✔ | ✔ | 1 | ✔ |
| 23 | NBR1009GPE | Netcore | NOS(Linux-based) | - | ✔ | ✔ | ✔ | 1 | ✔ |
| 24 | Wimaster* | Wimaster | Linux-based | - | ✔ | ✔ | ✔ | 10 | ✔ |
| 25 | IK-Enterprise* | iKuai | iKuaiOS(Linux-based) | - | ✔ | ✔ | ✔ | 10 | ✔ |
| 26 | Instant On AP22 | Aruba | ArubaOS(Linux-based) | Wi-Fi 6 | ✔ | ✘ | ✔ | 10 | ✘ |
| 27 | EdgeRouter X* | Ubiquiti | Linux-based | - | ✔ | ✔ | ✔ | 10 | ✔ |
| 28 | AX1800 | JdCloud | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 29 | Cisco Meraki 64* | Cisco Meraki | Linux-based | - | ✔ | ✘ | ✘ | - | ✘ |
| 30 | eero pro | Amazon | Linux-based | Wi-Fi 5 | ✔ | ✔ | ✔ | 10 | ✔ |
| 31 | Google Wi-Fi | Google | ChromeOS(Linux-based) | Wi-Fi 5 | ✔ | ✔ | ✔ | 10 | ✔ |
| 32 | GL-MT3000 | GL.iNet | Linux-based | Wi-Fi 6 | ✔ | ✔ | ✔ | 10 | ✔ |
| 33 | pfSense 2.7.0* | pfSense | FreeBSD-based | - | ✘ | ✘ | ✔ | 90 | ✘ |

✔means that the router is satisfied with the condition, and ✘means that the router is dissatisfied with the condition.
✔means that the router is vulnerable to our attack, and ✘means that the router is immune to our attack.
* means that the model is an enterprise router which does not support Wi-Fi by itself and needs to work together with wireless access points.

TABLE III. EXPERIMENTAL RESULTS OF TCP ATTACKS IN 30 WI-FI NETWORKS.

| No. | Network Mode | SSID | Router Vendor | Wi-Fi Generation | WPA2/3 Enterprise/Personal | Attack Result | Time Cost (s) | Success Rate |
|---|---|---|---|---|---|---|---|---|
| 1 | Enterprise mode | Campus 1 | Huawei | Wi-Fi 6 | WPA2-Enterprise | SSH DoS | 15.43 | 18/20 |
| 2 | Enterprise mode | Campus 2 | TP-Link | Wi-Fi 4 | WPA2-Enterprise | FTP Hijacking | 10.32 | 18/20 |
| 3 | Enterprise mode | Campus 3 | H3C | Wi-Fi 6 | WPA2-Enterprise | HTTP Injection | 48.87 | 15/20 |
| 4 | Enterprise mode | Enterprise 1 | TP-Link | Wi-Fi 6 | WPA2-Enterprise | SSH DoS | 11.56 | 16/20 |
| 5 | Enterprise mode | Enterprise 2 | TP-Link | Wi-Fi 5 | WPA2-Enterprise | FTP Hijacking | 11.43 | 18/20 |
| 6 | Enterprise mode | Enterprise 3 | Netcore | Wi-Fi 6 | WPA2-Enterprise | HTTP Injection | 87.20 | 15/20 |
| 7 | Enterprise mode | Office building 1 | TP-Link | Wi-Fi 5 | WPA2-Enterprise | SSH DoS | 9.56 | 18/20 |
| 8 | Enterprise mode | Office building 2 | iKuai | Wi-Fi 6 | WPA2-Enterprise | FTP Hijacking | 21.46 | 17/20 |
| 9 | Enterprise mode | Office building 3 | Mercury | Wi-Fi 6 | WPA2-Enterprise | HTTP Injection | 31.14 | 15/20 |
| 10 | Enterprise mode | Hotel 1 | Netcore | Wi-Fi 5 | WPA2-Enterprise | SSH DoS | 15.75 | 18/20 |
| 11 | Enterprise mode | Hotel 2 | D-Link | Wi-Fi 6 | WPA2-Enterprise | FTP Hijacking | 9.45 | 19/20 |
| 12 | Enterprise mode | Hotel 2 | iKuai | Wi-Fi 6 | WPA2-Enterprise | HTTP Injection | 71.32 | 16/20 |
| 13 | Home mode | Restaurant 1 | TP-Link | Wi-Fi 5 | WPA2-Personal | SSH DoS | 8.95 | 17/20 |
| 14 | Home mode | Restaurant 2 | Comfast | Wi-Fi 5 | WPA2-Personal | FTP Hijacking | 21.56 | 18/20 |
| 15 | Home mode | Restaurant 3 | Skyworth | Wi-Fi 6 | WPA2-Personal | HTTP Injection | 62.35 | 13/20 |
| 16 | Home mode | Coffee shop 1 | Mercury | Wi-Fi 4 | WPA2-Personal | SSH DoS | 8.98 | 17/20 |
| 17 | Home mode | Coffee shop 2 | TP-Link | Wi-Fi 4 | WPA2-Personal | FTP Hijacking | 9.29 | 18/20 |
| 18 | Home mode | Coffee shop 3 | Wavlink | Wi-Fi 5 | WPA2-Personal | HTTP Injection | 45.22 | 13/20 |
| 19 | Home mode | Shopping mall 1 | Tenda | Wi-Fi 6 | WPA3-Personal | SSH DoS | 24.23 | 18/20 |
| 20 | Home mode | Shopping mall 2 | TP-Link | Wi-Fi 4 | WPA2-Personal | FTP Hijacking | 11.44 | 19/20 |
| 21 | Home mode | Shopping mall 3 | Huawei | Wi-Fi 6 | WPA3-Personal | HTTP Injection | 78.44 | 15/20 |
| 22 | Home mode | Bookstore 1 | 360 | Wi-Fi 5 | WPA2-Personal | SSH DoS | 19.45 | 18/20 |
| 23 | Home mode | Bookstore 2 | Xiaomi | Wi-Fi 6 | WPA3-Personal | FTP Hijacking | 10.61 | 18/20 |
| 24 | Home mode | Bookstore 3 | H3C | Wi-Fi 6 | WPA3-Personal | HTTP Injection | 56.12 | 14/20 |
| 25 | Home mode | Experience store 1 | Xiaomi | Wi-Fi 6 | WPA3-Personal | SSH DoS | 16.97 | 17/20 |
| 26 | Home mode | Experience store 2 | Huawei | Wi-Fi 6 | WPA3-Personal | FTP Hijacking | 23.98 | 18/20 |
| 27 | Home mode | Experience store 3 | Xiaomi | Wi-Fi 5 | WPA2-Personal | HTTP Injection | 52.14 | 16/20 |
| 28 | Home mode | Cinema 1 | Ruijie | Wi-Fi 5 | WPA2-Personal | SSH DoS | 8.89 | 19/20 |
| 29 | Home mode | Cinema 2 | Mercury | Wi-Fi 6 | WPA3-Personal | FTP Hijacking | 11.31 | 18/20 |
| 30 | Home mode | Cinema 2 | Huawei | Wi-Fi 6 | WPA3-Personal | HTTP Injection | 54.26 | 16/20 |