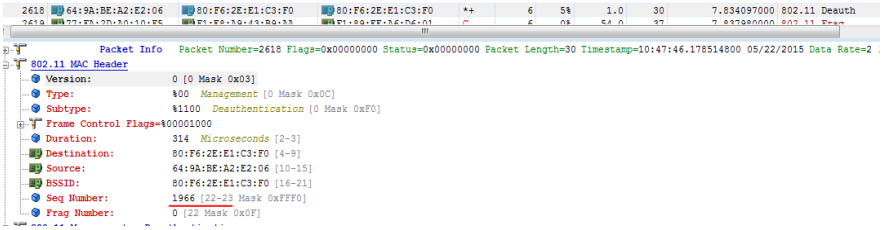
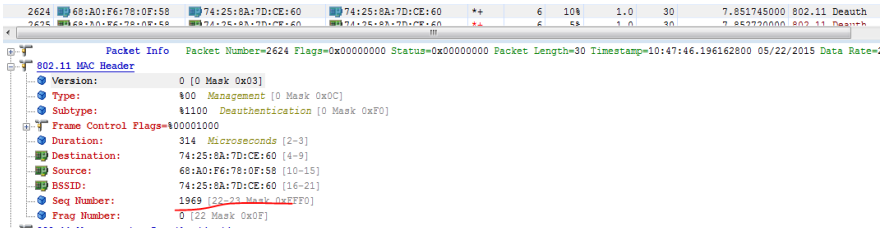
某局点wlan网络排查Deauth攻击的经验案例

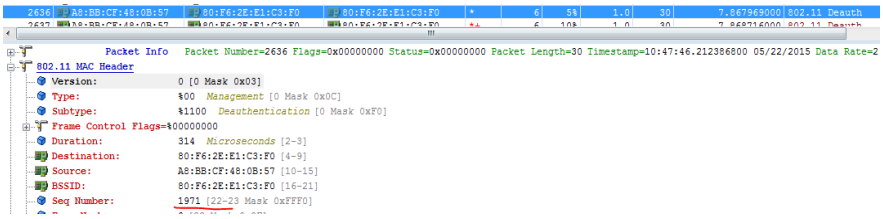
wlan接入　攻击检测及防范　余晨　2015-12-15 发表

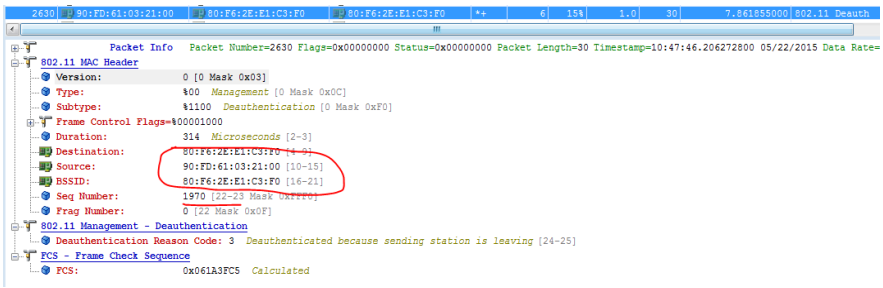
某局点wlan网络2.4G终端出现频繁掉线重连的现象，现场使用手机共享出一个无线网络供电脑上公网，该信号也出现了非常高频率的断线重连，怀疑现场存在wlan干扰或者攻击。

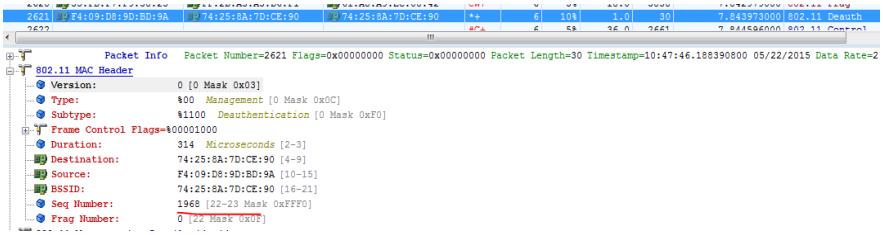
通过空口抓包，大量client的deauth同时出现，而且是发往不同的BSSID，并且deauth的seq number是连续增加的（不同client），这看着很不正常，很像是有人挨个仿冒client发送deauth。

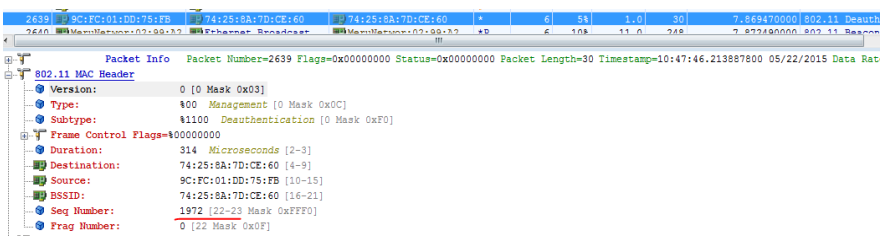












这种攻击防护手段有限，802.11为此专门出了个标准802.11w，起作用是client关联过程中是管理报文进行单独的密钥协商（目前管理报文都是明文），这样别人就无法仿冒deauth了。但需要client也支持802.11w才行，现在绝大多数终端不支持。

首先根据攻击行为推测，这个应该不是有其他厂商AP检测到rouge AP之后的反制行为，因为如果是rouge AP反制，一般会模仿AP给sta发deauth，而这里明显不是。所以这里更像是一个专门的攻击行为

。

想要定位这个攻击源的话，目前能做的就是人肉定位了：

1.先确认这个攻击源覆盖的AP范围，也就是根据掉线客户端所连的AP确认出这个攻击源在哪几个AP附近，可以先大略确认出一个范围。

2.然后在这个范围内，如果能够人肉排查是最简单的，就是挨个地方检查一下，比如可以按照电源插孔检查，这个攻击源总得用电源吧。看看有没有可疑的设备（如果攻击行为是24小时的，那就找24小时开机的设备，范围更小）。

3.如果上一个人肉排查的效果不好，那就麻烦一点了。

4.找一台笔记本，安装无线模拟发包的工具，冒充客户端发送数据报文，同时空口抓包，如果这个也能抓到这个所冒充的客户端的deauth，那肯定是仿冒的（因为模拟客户端我们设置为发送数据报文，绝对不会发deauth），全部过滤出来。

之所以要找一个笔记本模拟客户端，就是为了钓鱼这个攻击源的报文，因为它是变换mac的，只能用这个办法才能准确找到哪些是属于它的报文。

5.连续变换几个位置，重复步骤4，根据得到的不同位置的deauth的rssi，大略推测攻击源的位置，然后进一步人肉筛查。

6.如果觉得上述推测不好做或者不准确，那就得用更麻烦的办法了，找到这个酒店的工勘图，设置00原点，找至少三个准确的位置采样

7.然后把采样数据输入无线定位计算公式，利用无线定位的公式计算攻击源在工勘图中的位置（相当于人肉模拟AE定位）

最终，现场通过抓包发现Deauth 攻击源在局点大楼4层走廊尽头信号最强，基本确认在大楼对面建筑物内，且deauth信道维持在channel 6，现场将所有的AP放到了 1、11两个信道，deauth攻击问题得到解决，终端接入正常。