无线信号旁的那把“小锁”，是怎么回事？ | 运维实战家

锐捷网络 锐捷网络

近日，小锐收到这样的反馈：

“为什么手机上有的无线信号有显示小锁标识，有的没有呢？”

“我都进行web认证了，为什么手机上还是显示不安全的网络呢？”

……

出现这些问题的原因是什么，那把小锁、不安全网络到底是怎么回事？ 请容小锐详解。

常见的智能手机终端苹果手机无线网络显示标识：

> 安卓手机上的无线网络显示标识：

可以发现手机终端显示无线网络信号旁边有的有小锁标识并显示加密字样；有的没有小锁，安卓机还会显示开放网络，苹果机则是显示不安全的网络。

手机上查看无线网络列表的时候就能看到各个无线信号的状态了，此时终端还没有接入无线，手机终端是如何知道各无线信号是否配置了接入验证的？关于这些显示呈现，手机终端又是如何实现的呢？

带着这些疑问，好学的小锐开始了求知之旅。口说无凭，小锐决定结合配置和报文来进一步分析，还真让小锐发窥探到“天机”，且听小锐娓娓道来。

首先小锐对终端接入无线到上网阶段的过程进行了整理，如下：

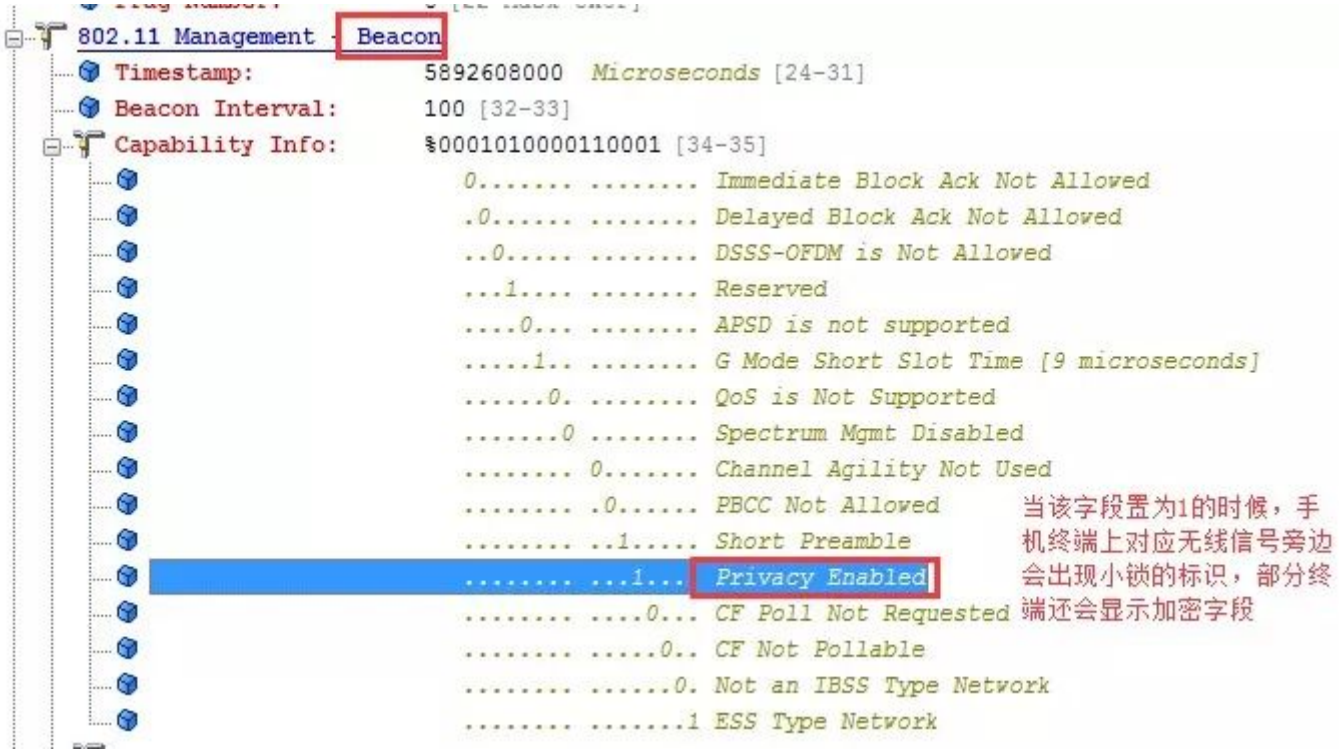
终端接入无线都需要经过扫描、认证（此处认证跟日常提到的802.1x认证等不是一个阶段）和关联阶段，之后才涉及到密码接入以及802.1x认证、web认证等多种接入验证。

无线终端接入无线信号，以及进行无线数据传输，都是在空气中进行传播的。空气是移动终端（手机）和基站之间传输的介质和接口，简称空口。在空气中传输的无线报文，简称空口报文。

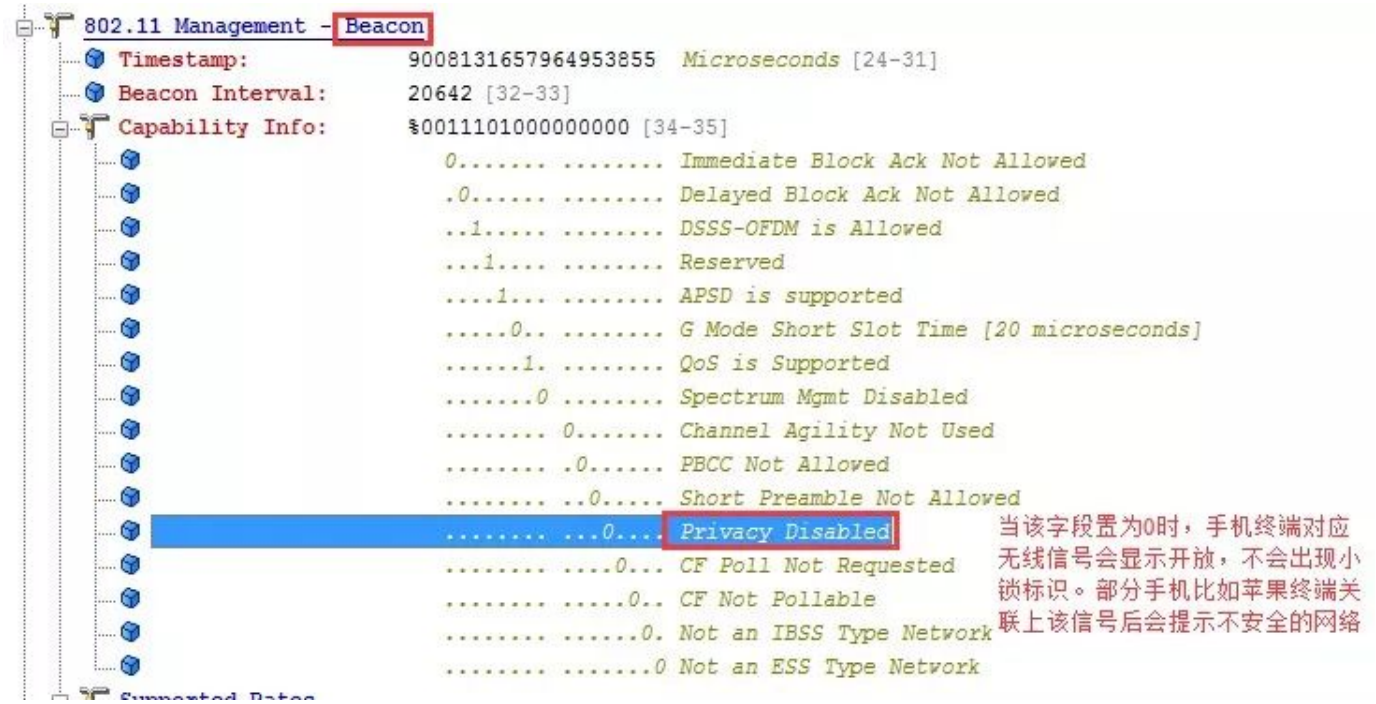
紧接着小锐结合无线设备的配置以及空口抓包，进一步分析。

通过多次空口抓包和比对无线信号的配置，小锐发现：在扫描阶段时，AP对外广播的Beacon报文中，Privacy位的状态跟手机终端无线信号后面是否有小锁等显示有关联性。

当无线信号配置为Wep、Wpa、Wpa2、Wapi、中的任意一种加密或者部署为802.1x认证时，AP广播的Beacon帧中的Privacy位会置为1，此时手机上在无线信号的wifi图标旁边会显示一把小锁标识，安卓手机还会多出加密两个字，此时对应的无线信号是加密的。



而没有上述这些加密配置时，AP广播的Beacon帧中的Privacy位会置为0，手机上该无线网络旁边不会显示小锁标识，当苹果手机关联上该不加密的信号时会提示不安全的网络，跟无线信号是否开启了mab认证或者web认证无关。而安卓手机未关联前则会显示开放这两个字，关联后除了已连接不会有其他提示。此时对应的无线信号是开放的。



通过上面的说明，相信大家对于手机终端上无线信号的显示情况已经了解了。大家可能会有新的疑问，无线信号是否配置加密有什么影响呢？数据传输安全吗？为什么苹果手机会提示不安全的网络呢？

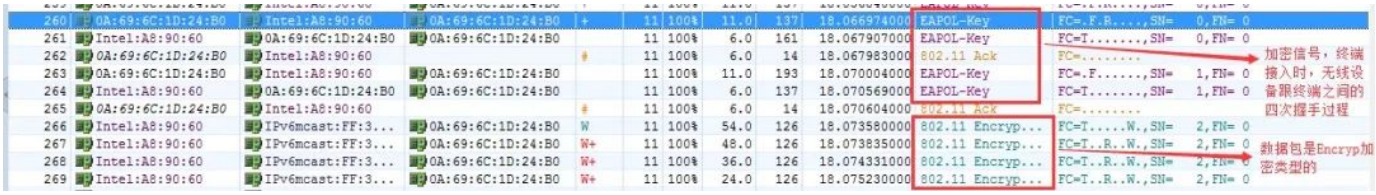
小锐继续抓取空口报文，抓取终端的数据报文：发现**当空口是开放的时候，抓包可以看到终端的数据报文，协议和内容都可以看出来；**

到目前为止，小锐可以确定部署了web认证但是却反馈不安全网络的无线信号，是因为空口是开放的，空口传输的数据报文是明文传输的。

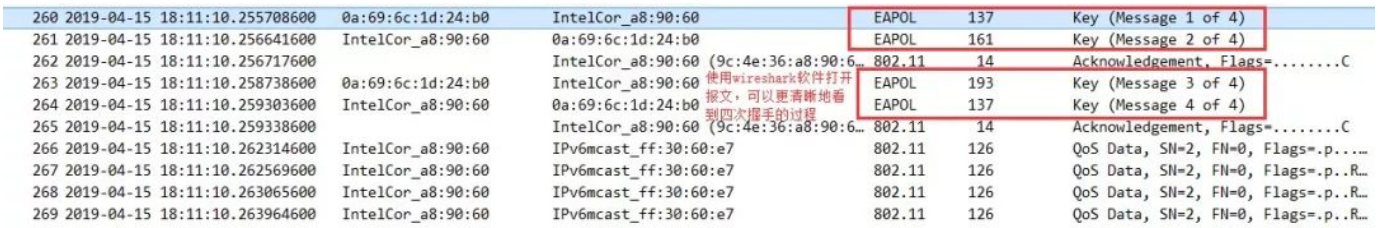
看到这里，可能大家不禁会有疑问，web认证到底有什么作用呢？小锐是这么认为的：web认证是对终端能否使用网络做的授权，web认证成功之前终端可以接入无线网络，也会获取到ip地址，但是无法上网，只有web认证成功之后才可以使用无线网络。

那么在部署了web认证的网络中，如何让空口报文传输更加安全呢？可以考虑在对应的无线信号上同时配置上wpa/wpa2加密，这样终端数据在空口传输的时候就是加密的，终端需要先输入密码接入无线之后再进行web认证。

而当空口加密时，无线设备跟终端会先进行四次握手，之后数据报文都是加密的，无法看到数据内容，如下：



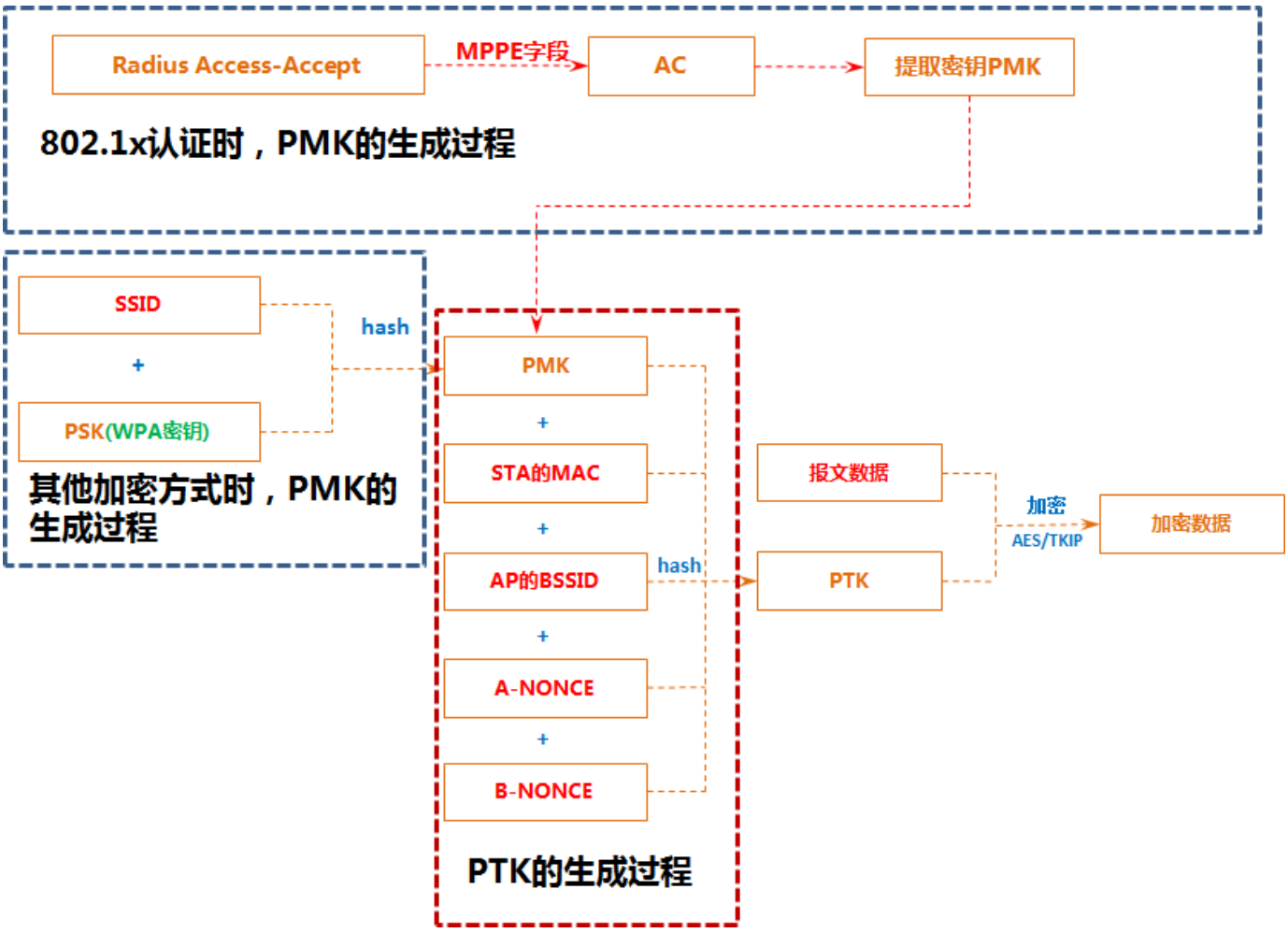
上图是使用omnipeek抓取的空口报文，用该软件打开后无法直观的看到四次握手的过程，但是可以看到数据是加密的。使用wireshark软件打开报文，可以很直观的看到四次握手的交互过程，如下：



关于四次握手的作用，小锐经过研究发现是为了最终生成PTK（成对传输秘钥）或者GTK（组临时秘钥）置于网卡。PTK或者PMK再根据一定的加密算法对数据报文进行加密和解密。报文由终端发送出去的时候，终端加密，AP解密；报文由AP发给终端时，AP加密，终端解密，数据在空口传输的时候是加密传输的。

对于加密信号的无线802.11的数据帧，所有的单播数据帧将会被PTK保护，所有的组播数据以及广播数据将会被GTK保护。

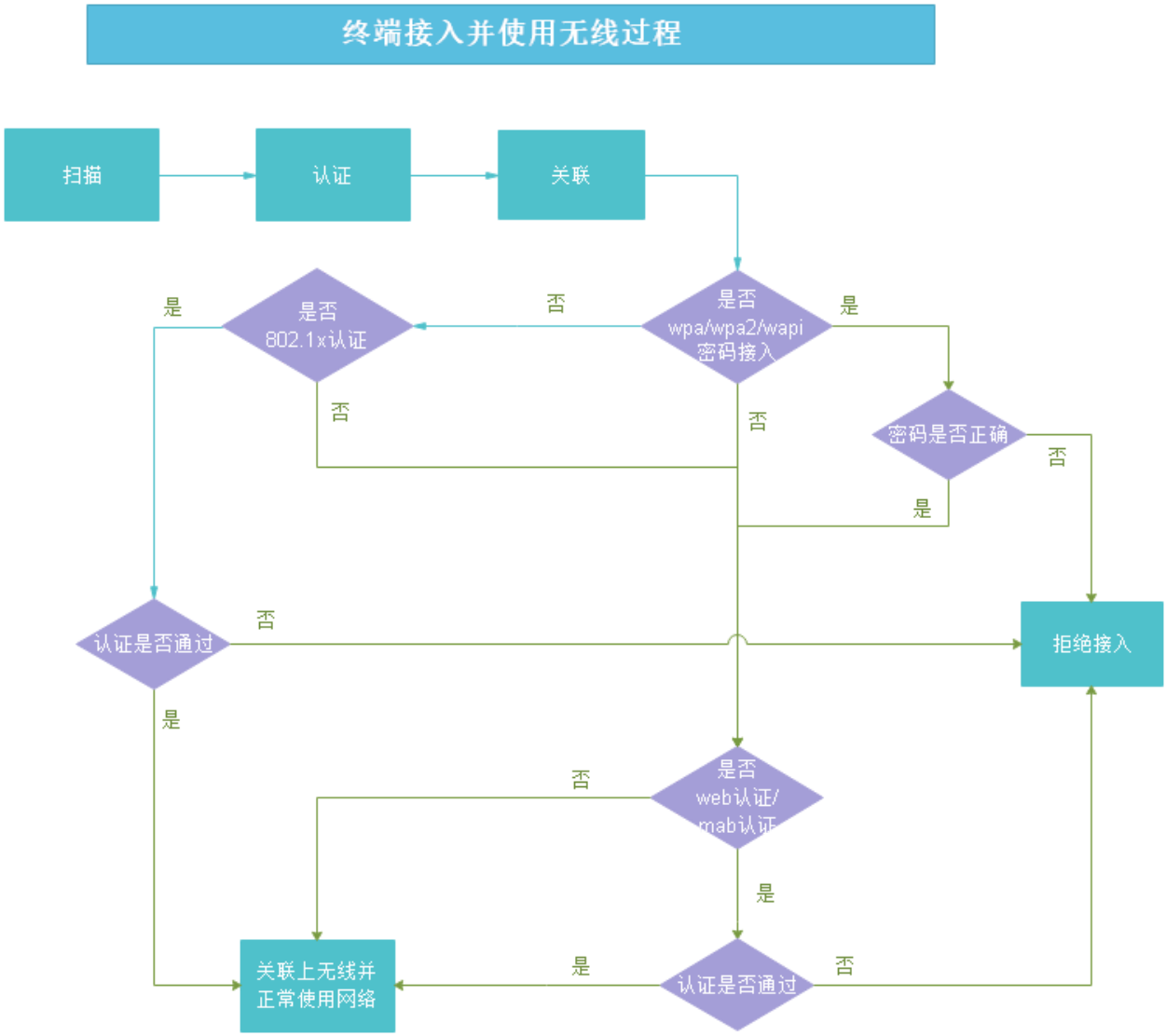
组临时秘钥GTK是在PTK的基础上生成的，而PMK（成对主密钥）是用于生成PTK的主材料。那么PMK是如何产生的呢？802.1x认证和wpa/wpa2等加密算法的PMK生成方法是否一样呢？PTK又是如何生成的呢？PTK生成过程如下：



通过上图可以看到802.1x认证和wpa/wpa2等加密算法的PMK生成方法不同，但是后面生成PTK的过程是一样的。PTK的生成过程中的A-NONCE是AP生成的随机数，B-NONCE是终端生成的随机数，由于随机数和终端STA的MAC都是不同的，所以在一个加密的无线信号中，每个STA都有一个独自的PTK。

空口抓包的四次握手过程，就是PTK的生成和协商过程，在四次握手的时候，还会生成GTK（GTK是在PTK的基础上生成的，对于GTK的生成不做过多讲述，所有的STA和AP共同拥有一个相同的GTK）。

最后，小锐针对wpa/wpa2/wapi、802.1x认证、web认证的生效顺序进行了整理（由于wep加密算法过旧且容易被破解，流程图中去掉了wep加密），附上终端接入无线并使用无线的流程如下：



“运维实战家”专栏，从技术到实践，和您聊聊运维的那些事儿，讲述运维人的“昨天、今天和明天”