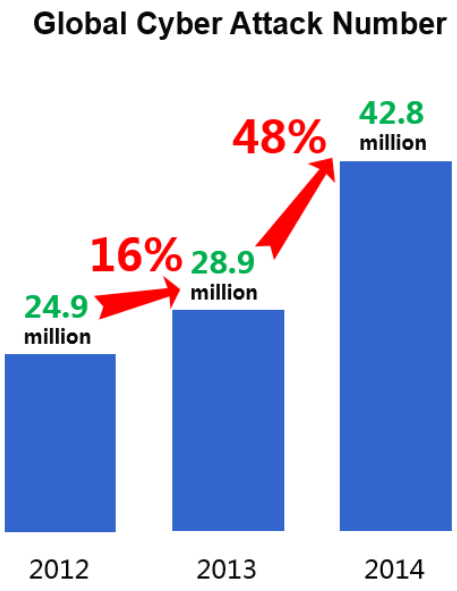
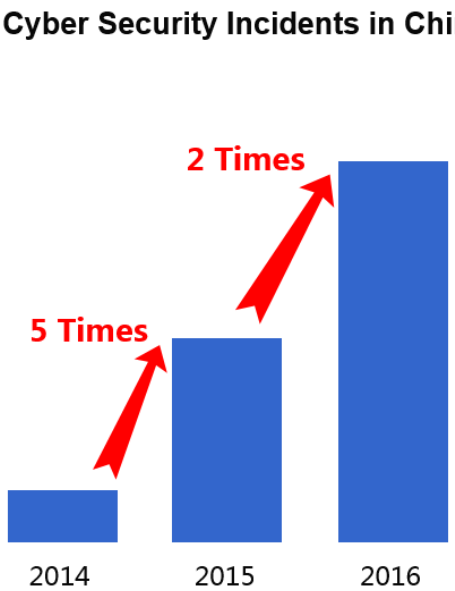
360° 剖析黑客如何入侵你的汽车

汽车的发展被认为是手机后的另一个智能终端，不可否定从PC到手机的更迭造就了信息时代的更迭和从互联网到移动互联网的更新，产品和企业也从PC时代的微软英特尔到手机时代的谷歌苹果演变。下一个时代是什么，下一个产品由谁主导，我拭目以待。没有人怀疑未来是万物互联的时代，在万物互联的大生态下，汽车俨然被认为是下一个改变人类生活的智能终端。

世界上许多最具创意和深度挖掘的公司正在竞相将其推向市场，并且有很大的理由相信他们将产生的经济和社会成就是巨大的。但任何变革在技术除了获益之外，都会带来新的挑战和风险。交通运输方面面临的最大威胁之一就是车辆网络安全。而且随着互联网连接，用户认证，智能设备和电路在很大程度上体现在新一代车辆的运行中，但与信息技术部门不同，操作系统的变化，调整，新工具和软件无法推广到生产线和用户已经在路上，任何事情即将实时响应。相比之下，变化的速度仍然很慢，对于汽车行业来说，这对确定安全漏洞有重大的影响，以及修复和修复安全漏洞所需的措施。

一、汽车网络安全的现状





上图显示了历年来网络安全在汽车方面的影响变化，去年有两名白帽黑客远程控制了一辆吉普切诺基，当然这次“事故”只是潜在的危险，并没有造成严重的损失，随后克洛斯勒召回了140万辆车。

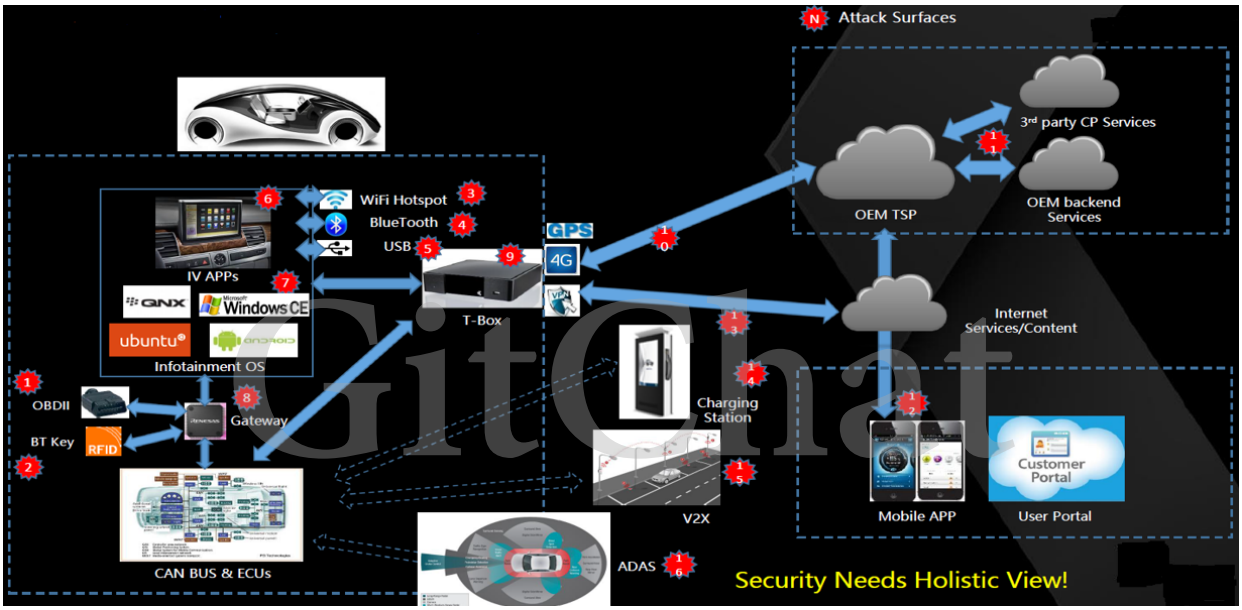
今年已经看到欧洲最大的汽车俱乐部（ADAC）的研究人员展示了无钥匙的“舒适锁定”机制在市场上的普及程度，无疑是技术精明的小偷。在阿尔法罗密欧，雪佛兰，福特，蓝

旗亚，欧宝，标致和雷诺等大众汽车集团中，可以使用廉价且易于使用的硬件工具绕过整个车辆系列的锁定机构。

车辆网络安全的核心挑战之一是汽车的各种ECU通过内部网络连接。因此，如果黑客设法访问易受工具的外围ECU（比如汽车的蓝牙或者信息娱乐系统），那么黑客们就可以控制关键的ECU，如制动器或者发动机，从而造成严重的破坏。

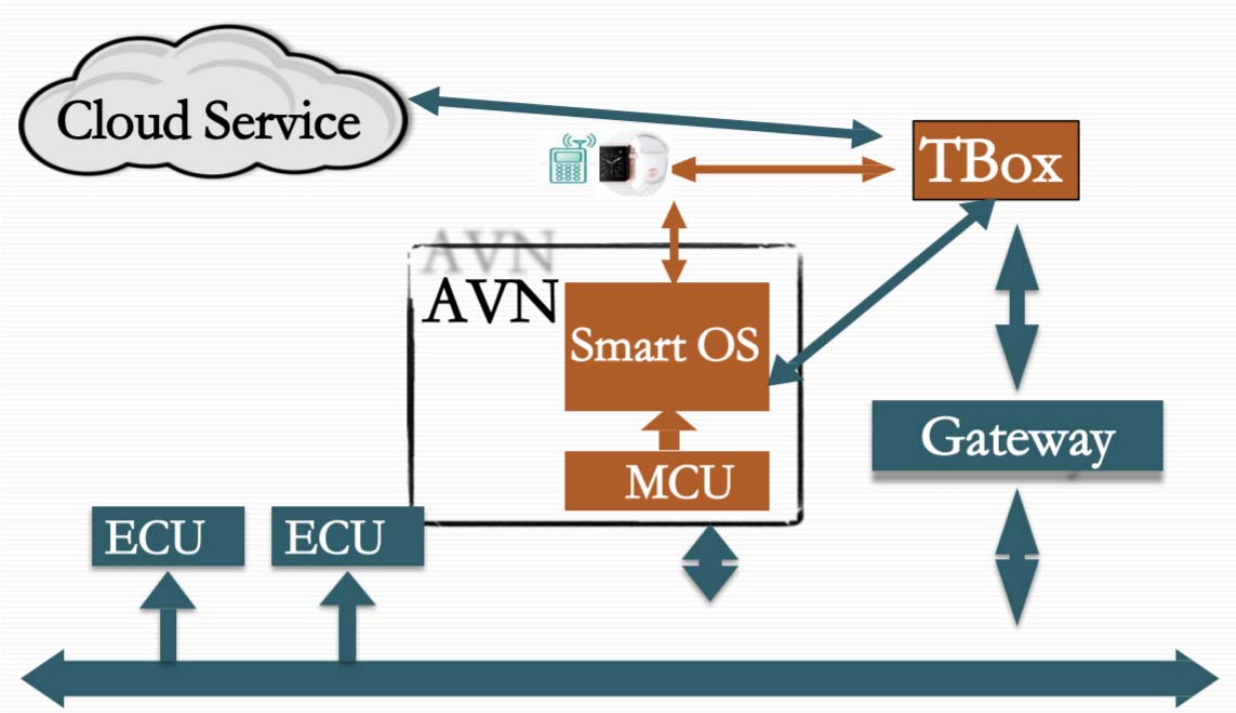
如今的汽车有多达100多个ECU，超过1亿行的代码，这就给与了巨大的供给面。当困难的是汽车制造商是从许多不同的供应商里获取ECU，意味着没有一个黑客可以控制甚至熟悉车辆的所有源代码。

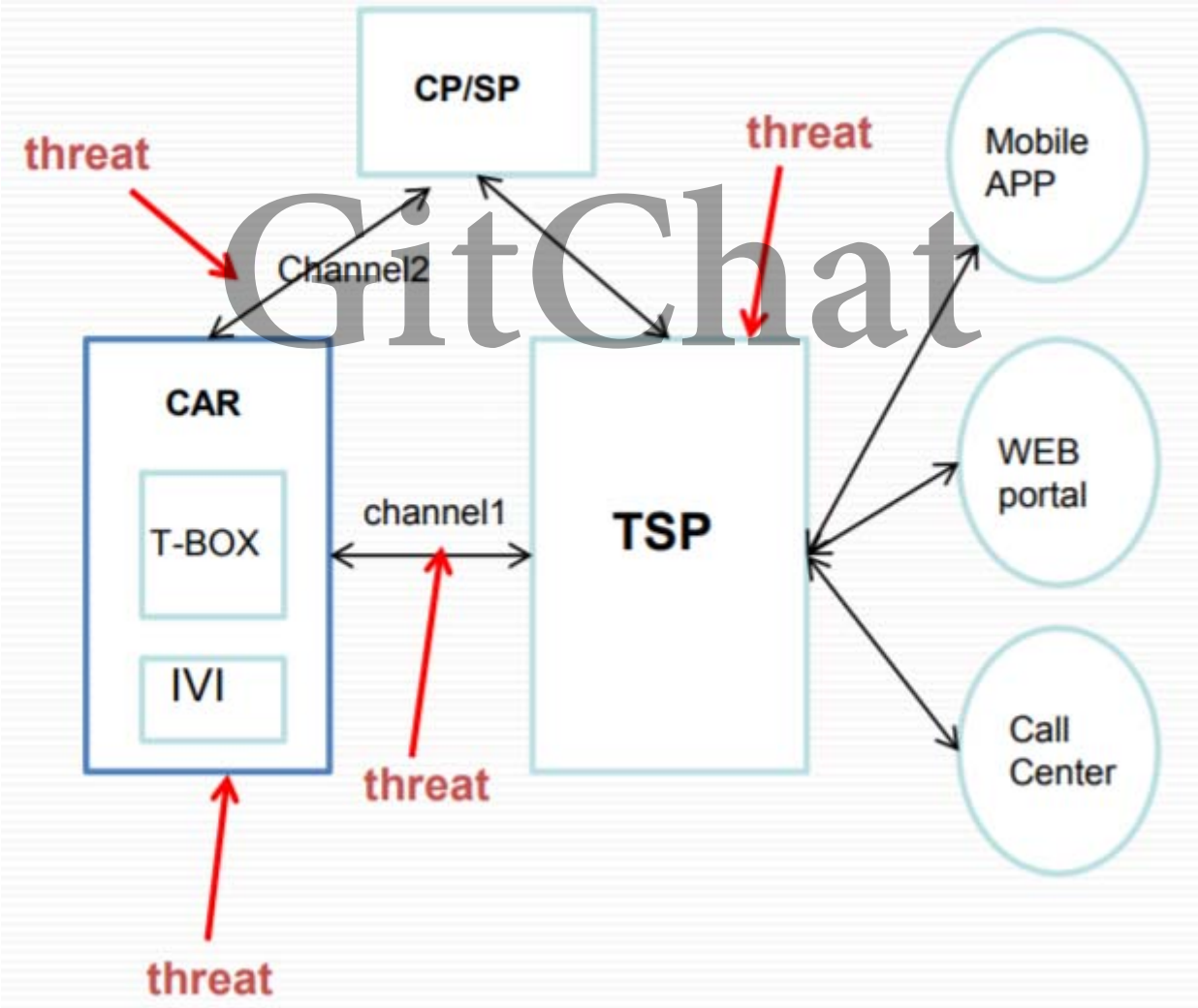
二、汽车易攻击面



汽车越来越附能也就意味着攻击汽车的点越来越多，上图中显示有很多点都是新能源汽车相对于传统汽车的“高大上”功能，比如手机的远程控制，云端的远程监控等。通信和娱乐系统特别容易受到攻击，并且可以通过逆向工程来访问API库，从而促进系统之间的数据共享。从这里，攻击甚至可以将恶意代码注入到电子控制单元（ECU）和控制器区域网络（CAN）总线中，该总线控制关键系统，如电动转向和制动。OBD设备是厂商用来诊断汽车的各种数据，该接口集成了很多ECU的CAN总线接口，通过OBD接口可以变向的访问汽车其他设备，比如雨刷，空调等，现在有很多创业公司在做基于OBD外设控制汽车，但目前做的都不温不火，甚至有些公司在基于该接口做自动驾驶的方案。

总而言之，OBD是最容易控制汽车的接口。其次连接模块也是黑客们喜欢攻击的重点，对汽车而言连接模块如WIFI，蓝牙，USB等每一次连接到车机的时候都充满着被“亲密”的风险，一旦获取到数据就可对其进行解码分析，从而按照厂商协议进行逆向操作控制汽车。最后专注下汽车联网设备，这是汽车最容易遭受攻击的方面，传统汽车的联网是由TBOX来提供，就像PC网卡的概念，插上PC使之具有联网的功能，该外设通过指定协议访问TSP服务器进行数据的收发，对黑客而言在这条链路上充满着“收获”的惊喜。以一张图来说明通过TBOX是如何控制各个ECU的。



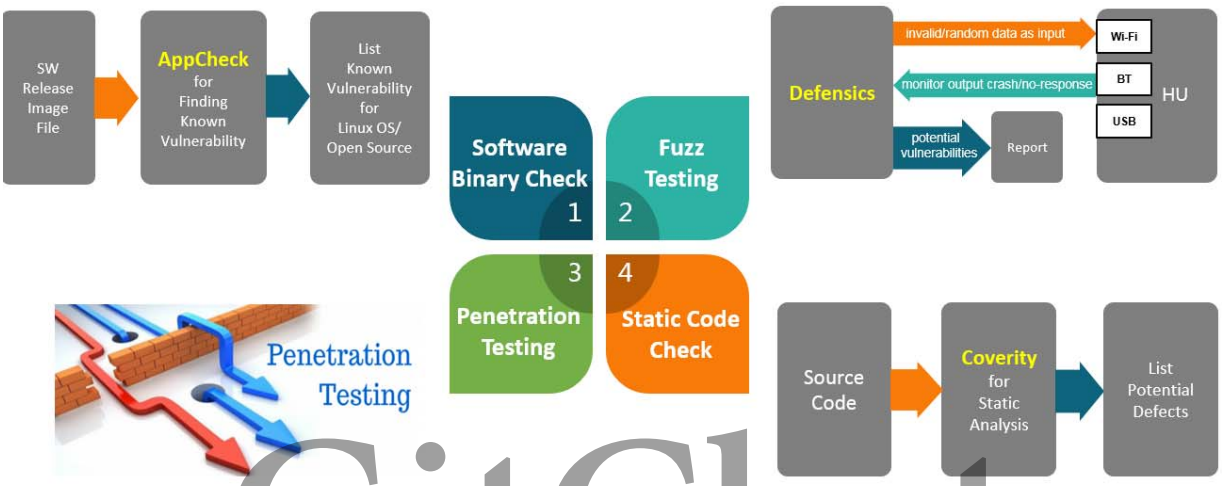


连接TSP服务器中有很多可被破解的危险，控制汽车的手机app，网络浏览器，甚至电话都是可以参考点，通过车联网的网络破解比目前的PC，移动互联网的破解相对容易是因为汽车是个发展更新很缓慢的产品，很多汽车厂商的服务器甚至都没有提供安全加密的算法，当然网络攻击只是入侵汽车的步骤之一，汽车攻击相对于PC或者手机难以攻击的点在于汽车本身是个集成度很高的产品，里面有大量不同厂商的ECU，每家零部件供应

商或者整车厂都有一套自己的车载协议，而且这些协议是不公开的，这是黑客们攻击汽车最难以逾越的屏障，同时也是汽车最安全的一道保护层。

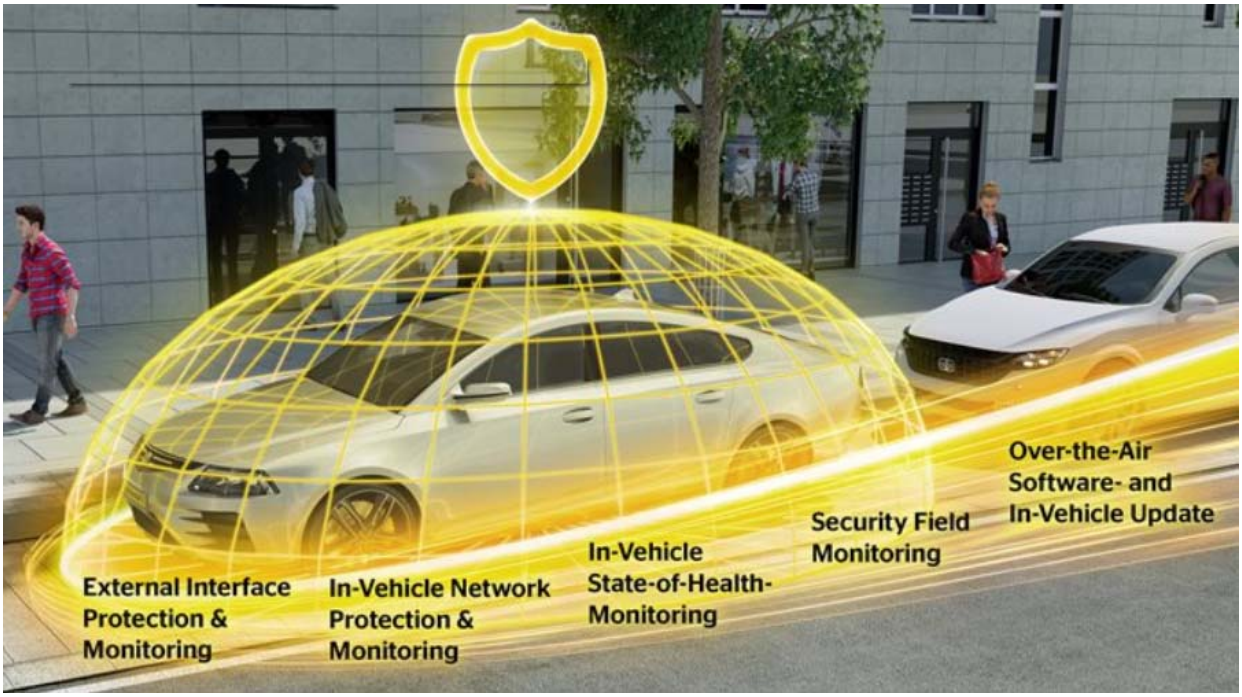
三、汽车的安全策略

安全是个矛与盾的相对概念，没有绝对的安全，理论上来讲每一次的安全防护黑客都是可以破解的。这里从不同的角度尽量给大家介绍下在汽车上路之前甚至上路后都有哪些安全措施。



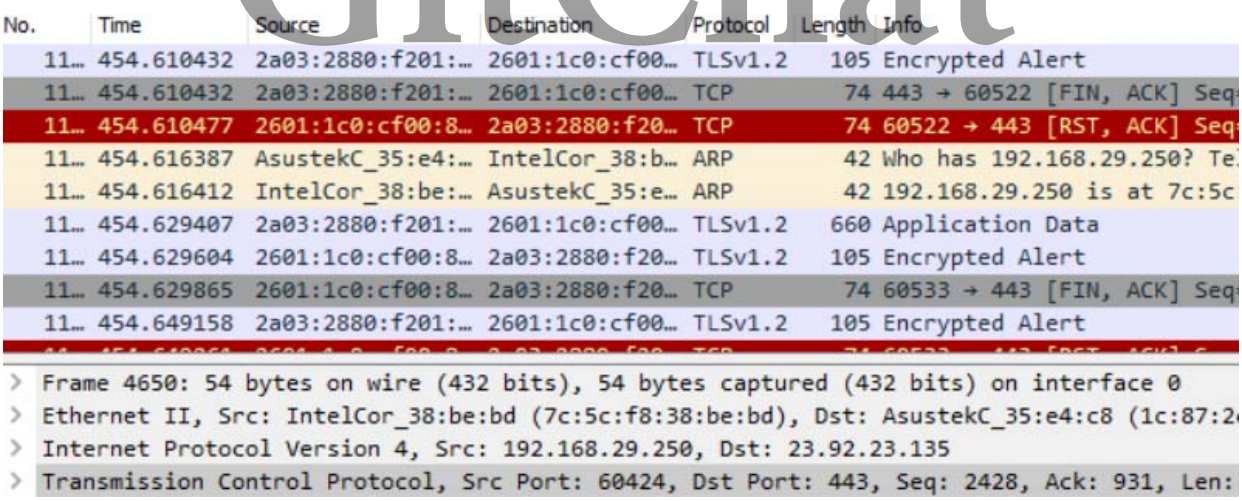
首先是软件开发阶段的安全保证，包括静态检查，这里有很多公司可以使用，比如代码静态检查的coverity工具，可以有效检查代码的漏洞。其次代码发布前对其进行本地化的测试检查，根据黑客有可能的入侵手段进行模拟重现，保证出现的漏洞封杀在摇篮，最后根据供应商方案进行trust zone的渗透测试。总而言之每家公司的解决方案都不一样，这里我以端到端开发的解决方案为例展开网络安全是如何从组件开始的，之所以采用端到端方案是确保在任何时候都有可能达到最高的安全程度。从产品开发的第一天开始考虑网络安全，从而首先不会出现潜在的安全漏洞。不仅要考虑初始开发，而且考虑整个产品生命周期。举例来讲可以不断检查CAN总线上的异常通信，并对各个控制单元之间的通信进行加密，永久监控车辆系统的当前状态也可以增加更多的安全性，把检测结果定期向安全中心报告，以便检车车队的安全漏洞，这样可以快速开发和实施安全补丁，可以通过OTA技术更新快速导入，无需进行维修中心的访问。总而言之网络安全可以从五个方面进行保护：

1. 数据接口加密
2. 车内网络总线的保护监控
3. 汽车健康数据监控
4. 安全模块如trustzone的硬件保护
5. 云端服务器的数据传输处理



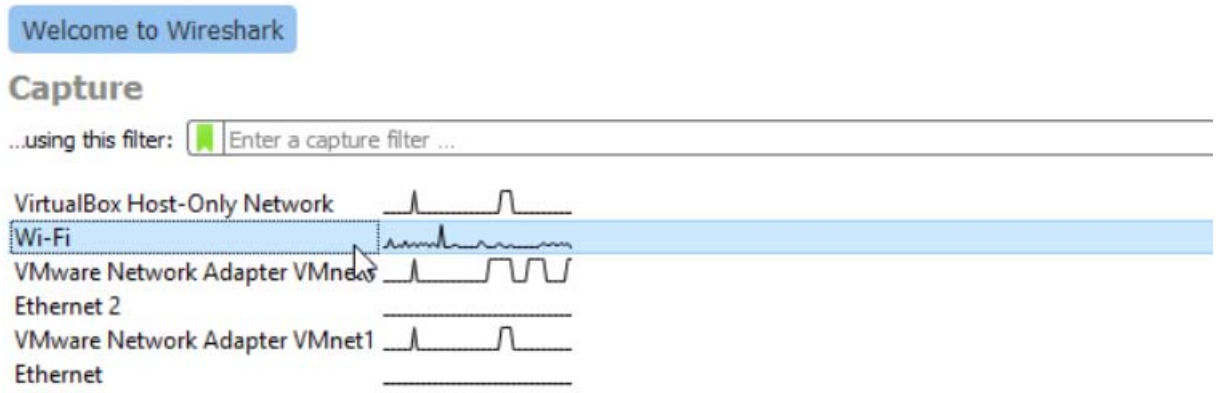
四、黑客如何攻击你的汽车

我们以攻击TBOX为例讲解如何破解TSP服务器，WIFI通常是网络的弱点，因为WIFI信号可以随处可见。还有很多路由器都包含漏洞，可以利用正确的设备和软件（如Kali Linux附带的工具）轻松利用漏洞。首先使用一个捕获，筛选和检查网络包的工具Wireshark.

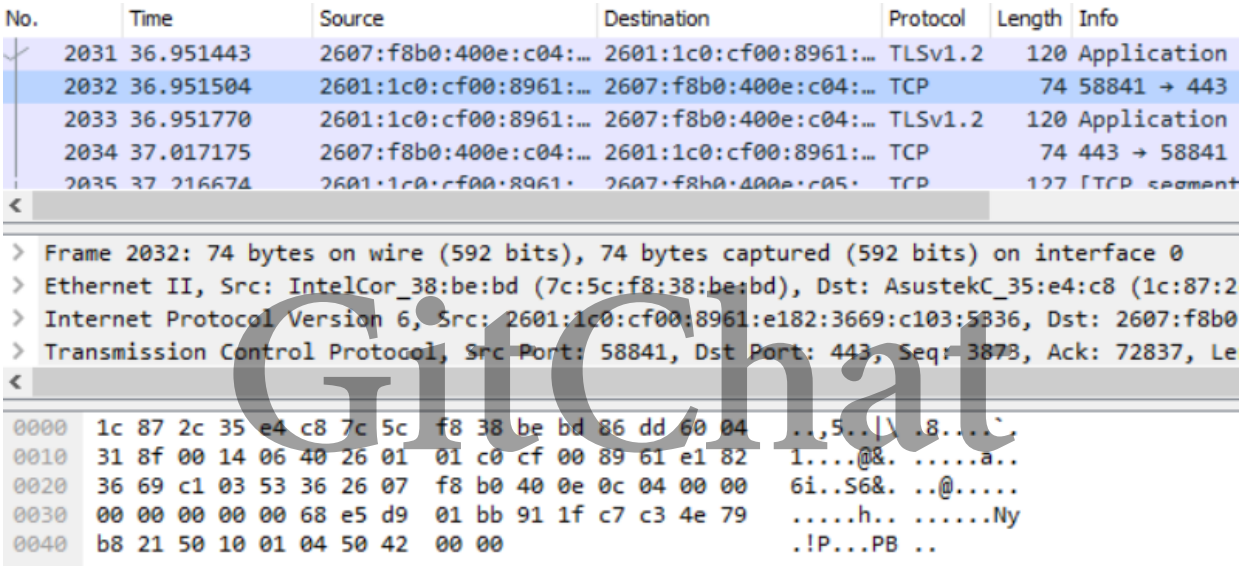


Wireshark，一种以前称为Ethereal的网络分析工具，实时捕获数据包，并以人类可读的格式显示。Wireshark包括过滤器，颜色编码和其他功能，让您深入了解网络流量并检查单个数据包。

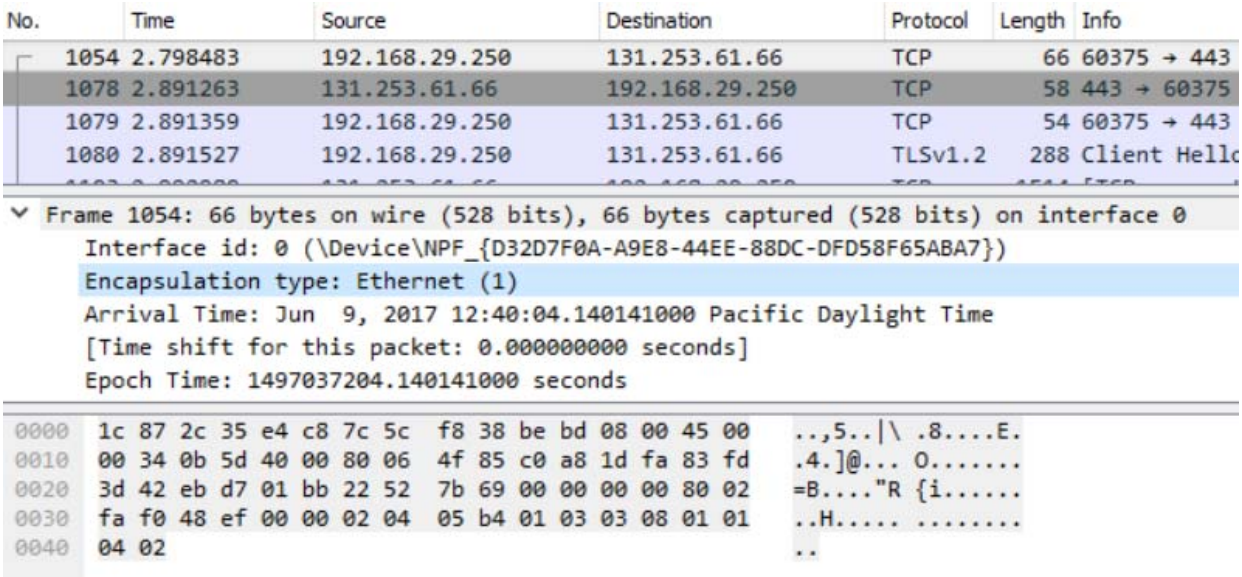
下载并安装Wireshark后，您可以启动它，然后双击Capture下的网络接口名称开始捕获该接口上的数据包。例如，如果要在无线网络上捕获流量，请单击无线界面。您可以通过单击捕获>选项来配置高级功能，但现在不需要。



一旦您单击界面的名称，您将看到数据包开始实时显示。Wireshark捕获发往或从您的系统发送的每个数据包。如果您启用混杂模式 - 默认情况下启用 - 您还可以看到网络上的所有其他数据包，而不仅仅是寻址到网络适配器的数据包。要检查是否启用混杂模式，请单击“捕获”>“选项”，并验证“在所有接口上启用混杂模式”复选框在此窗口的底部。



点击一个数据包选择它，你可以挖一下查看它的细节。



图中点击的数据是TSP服务器对应的地址，可以看出此网络的包头信息和内容。然后运用破解工具对其进行破解。第一步是创建一个包含8个大写字母的所有可能组合的密码列表。我们将在Kali Linux中使用Maskprocessor来创建密码列表。我们将通过与Aireplay ng

连接的客户端进行身份验证，与Airodump ng进行4次握手。最后一步是使用Aicrack ng强制使用密码。

1. 将使用maskprocessor生成密码列表，将每个字母的文件管道传输到一个文件，以便我们可以使用多台计算机加速强制强制密码。

   掩模处理器A ? u ? u ? u ? u ? u ? u -o /usr/A.txt

   掩模处理器B ? u ? u ? u ? u ? u ? u ? u -o /usr/B.txt

   掩模处理器C ? u ? u ? u ? u ? u ? u -o /usr/C.txt

   等。对字母表中的每个字母重复。每个文档的文件大小将约为60 GB。

2. 接下来我们要做的是捕捉与Airodump-ng的握手。我们将首先使用Airodump-ng来选择我们的目标，并检索它的BSSID并通过WiFi接入点进行广播。然后，我们将使用Aireplay-ng对连接的客户端进行身份验证以强制重新连接，这将给我们四分之一的握手需求。现在我们来启动Airodump-ng，使用以下命令找到我们的目标：

   $airodump-ng mon0

   现在选择您的目标的BSSID和通道，并使用以下命令重新启动Airodump-ng，并查找连接的客户端：

   $airodump-ng -bssid [BSSID] -c [channel] -w [filepath to store .cap] wlan0mon

   打开一个新终端，并使用Aireplay-ng为连接的客户端发出一个命令。

   aireplay-ng -0 2 -a [BSSID] -c [Client MAC] mon0

   取消认证成功和4路握手被捕获！

3. 最后使用以下命令通过Aircrack-ng强制输入密码：

   aircrack-ng -a 2 -b [路由器BSSID] -w [文件路径到密码列表] [文件路径到.cap文件]

   最终会破解密码：