第 1 章

鸟瞰无线安全攻防

1.1 无线安全概述

1.1.1 无线安全的由来

“无线”安全是庞大的信息安全体系下一门很广泛的学科。当今社会，电子产品大量依靠各种无线技术，从近场通信 NFC、蓝牙 BLE、射频 RF、工控无线传输 ZigBee、无线局域网 WiFi，到手机蜂窝网络 Cellular、卫星定位 GPS、卫星通信 SATCOM，这些都属于无线技术领域，所以无线通信技术上的传输、认证、加密等安全问题，在各种设备对无线技术依赖加深的情况下变得越来越重要。从现在到未来，人类对这些技术的安全拥有足够的掌控也将是非常必要的。因此，如何正确地使用无线通信技术，并保证其安全，是每一个研发、产品、安全研究人员都要认真思考的问题。

遥想 10 年前，国内安全圈里的黑客们还在最早的无线安全时代（无线局域网、WiFi）研究与徘徊，当时破解 WiFi 密码、蹭网继而进行网络渗透是最传统的无线攻击方法。那个时代，也是无线局域网安全最火热的年代，无线安全研究者们专注于寻找性能优良的无线网卡，搭配自己优化的无线破解平台或使用 BackTrack、Kali 这类完善的环境对自己感兴趣的一个又一个无线热点进行安全评估，体会那种突破无线密码、接入目标无线网络的成就感。

随着无线攻防手段的更新，攻击方法也有了更有趣的发展，如先侦测无线客户端发出的曾经连接过的热点的 Probe 信息，再通过软 AP 程序产生相同名字热点的所谓 EvilAP 的钓鱼攻击方法，将无线目标拉入虚假的无线环境进而发起攻击，或者窃取目标网络流量中的敏感信息。独角兽团队所支持的 2015 年 315 晚会上 WiFi 安全环节的出现，也让圈里的老无线安全研究者的心为之一动。这个安全演示环节出自 DEFCON 黑客大会 Wireless Village 上有名的 The Wall of

Sheep（绵羊墙），这个项目是为了教育人们——“你很可能随时都在被监视”，同时也给那些参会的人难堪，参加安全大会还如此不注意安全，难怪被贴到绵羊墙上。绵羊墙的账号和部分隐匿的密码将被投影在专门的一个会议室内的大屏幕上，The Wall of Sheep 大约由 7 名来自北美的安全人士维护，他们每年花 2 周时间来拉斯维加斯参加 DEFCON。大会提供免费的“hostile”的网络（BlackHat 和 DEFCON 提供的无线网络）供参会者接入访问，如果接入了，那么你的所有网络活动都可能被监听和探测。

1.1.2　无线安全与移动安全的区别

现在安全行业对“无线”及“无线安全”的概念是略模糊的，多数从业者认为无线即指手机无线端，无线安全则指手机系统安全、App 端安全。这其实是不正确的，这个安全领域更应该定义为移动安全。本书所提到的无线安全则是更广义的，是指所有使用无线通信协议的无线电技术的安全，即“无线电安全”。

1.1.3　无线安全的现状

随着手机的普及和人们日益增长的随时随地无线上网的需求，针对 WiFi 的各类攻击屡见不鲜，从国内各类媒体对用户在咖啡厅等公共场所上网被钓鱼事件的报道就可以发现，WiFi 安全已经是一个社会安全问题，手机厂商、安全公司也都对 WiFi 造成用户隐私信息泄露等问题在各自能把控发力的地方下足了工夫。如苹果公司在 iOS 8 系统上增加了新的安全特性，可以使设备的无线 MAC 地址随机化，用来躲避在使用 WiFi 的过程中暴露自己手机的“物理指纹”；安全厂商也在各自的手机卫士类产品内增加了对周围无线热点评估的功能，以谋求提高用户连接 WiFi 时的安全性，使用户不受黑客无线钓鱼攻击的威胁。

那么我们只关注 WiFi 安全就可以了吗？答案是否定的，随着物联网（IoT）的持续蓬勃发展，现在的手机、智能设备对各类无线模块、传感器的需求越来越大，蓝牙、GPS、NFC 模块早已成为必备项。此时此刻，我们从安全的角度来看，整个行业对于使用这些无线技术的安全准备是不足的。

美国 Todd Humphreys 教授领导的无线导航实验室，是 GPS 安全研究领域非常领先的一个团队。早在 2012 年，Todd Humphreys 教授就在 TED 发表了演讲，呼吁公众注意 GPS 安全。在 DEFCON 23 上，中国独角兽团队的安全研究员黄琳向全球展示了如何使用低成本的软件无线电设备欺骗手机、汽车甚至无人机。Todd Humphreys 教授在 2016 年 2 月又以文章 *Lost in Space: How secure is the Future of Mobile Positioning?* 再次提出了他对于未来依赖 GPS 技术的设备在受到

GPS 欺骗攻击时抗攻击能力的疑问，以及这种攻击手段被滥用的担忧。

2016 年 2 月 18 日，是苹果公司寄予厚望的 Apple Pay 入华首日，但其实在几天之前，国内安全行业的专家们就已收到各类媒体关于 Apple Pay 这种 NFC 的交易方式是否安全的咨询。

从以上两个事件可以发现，在传统的无线局域网安全之外，更多的“无线”安全进入人们的视野和生活，我们已无法视而不见。安全从业者必须要具备在该领域安全的架构设计及风险评估能力。

1.2　无线安全攻防思路

1.2.1　常见攻击对象

一张门禁卡、一把无线钥匙、一个无线遥控器、一部手机、一辆汽车、一台无线呼吸监测仪、一架飞机，甚至一辆坦克、一颗卫星，只要攻击对象使用了无线介质进行数据交互，那么这条无线链路就有可能被监听、解密、重放、欺骗、劫持，甚至被入侵、被控制。看似不可能直接接触的目标，往往在无线通信层，攻击会变得如此直接。

作为一个安全评估人员，首先要做的就是确定可以评估的攻击面。以一辆汽车举例，汽车的无线钥匙系统和汽车的胎压传感系统（TPMS）多数采用 315MHz 或 433MHz 的 RF 传输数据；如果是无钥匙启动系统的汽车，则多会采用 125KHz 或 13.56MHz 的 RFID 技术；这辆汽车如果还具备 Telematics 网络连接能力，那么车机控制系统一定会具备 2G 到 4G 的蜂窝通信能力，并且本身一定还会提供 2.4&5.8GHz 的汽车 WiFi 网络，这些都是暴露在外可进行风险评估的攻击面。

1.2.2　无线安全攻击手段

无线攻击不同于传统的 Web 攻击等手段，它是一种靠尝试介入无线通道为起点，最终获取连入该无线通道并实施信号控制，或者利用网络进行更深入的渗透测试的攻击形态。对于这样的无线通信安全评估，大致可分为如下几种手段。

攻击手段之一：无线数据报文监听。使用与目标无线系统运行频率相同的监听设备对全量无线报文进行收集及数据逆向分析、解密。如监听 WiFi 使用无线网卡，监听蓝牙使用蓝牙嗅探设备，监听无线钥匙则使用 SDR 设备。将无线报文数据通过相应的方法解密后，可以深入了解整套无线系统的运作原理，找出关键的无线指令。

攻击手段之二：无线信号重放攻击。如果目标系统的无线通信协议没有设立有效的时间戳或随机性等防信号重放机制，那么当使用相应的无线设备截获一段合法合规的无线指令时，就可以通过将这段信号指令直接重放出来，影响目标系统。如截获了无线钥匙的开门指令，可以不使用钥匙，直接重放开门或关门信号，就能获得打开目标车门或其他设备的权利。

攻击手段之三：无线信号欺骗攻击。联合无线监听及解密，通过掌握目标无线协议的报文构成及关键密匙、校验方法等，直接构造合法的可通过协议认证的无线报文，影响目标无线系统的运作。

攻击手段之四：无线信号劫持攻击。通过使用协议层（如压制 WiFi 热点的软件 MDK3）或通信层（如发出特定频段噪声的信号干扰器）网络阻断的方法，也称无线拒绝服务攻击，将目标网络环境从合法领域拉入可控的虚假领域，再通过劫持上下行无线网络流量进行各类攻击。如使用 MDK3 压制一个无线客户端到一个合法无线热点的连接，迫使其接入虚假的无线热点；又如使用 3G 到 4G 信号干扰器，将手机或汽车的蜂窝网络从相对安全的网络压制到不够安全的 2G 网络环境，再被开源基站控制，继而进行上下行流量的中间人劫持攻击。

1.2.3　无线安全防范思路

无线安全防范要从攻击面去考量，可靠的通信协议、强认证、强通信加密、抗信号干扰是一套无线通信协议安全与否的核心。具体问题要具体分析，关于各类无线通信协议详细的防范方法请读者阅读后续章节。

1.2.4　无线安全趋势

如今，随着 RTL-SDR、Ettus 的 USRP 及 HackRF、Nuand 的 bladeRF 等各类软件无线电设备的价格下降、软件环境社区的完善，安全研究者已经可以轻易地拥有一块无线频谱覆盖 50MHz~6GHz 的无线信号分析“神器”，无线黑客们已经不再像当年只能利用 2.4GHz 的无线网卡进行狭窄的“无线”攻防。不得不说的是，廉价的 SDR 设备推动了无线安全领域的发展，安全研究人员借助这些设备已经从传统安全领域跨界到无线电安全领域，但与此同时也增加了被恶意利用的风险。

刀可以用来杀人，也可以用来救人。这种设备的民用化，或许导致被更多的怀有恶意的黑客所利用，以致影响、威胁到我们的生活，但同时我们也需要使用这些设备来了解、评估已经在使用的无线技术。攻与防一直在博弈，我们只有与时俱进，了解最新的攻击手段，才能优化改良现有的体系，使我们的生产生活更加安全。当年科学家们认为 6 位数字的密码已经足够安

全，但随着计算机 CPU 运算速度的提高，现如今密码的复杂度如何想必大家也有目共睹。就像 GPS 欺骗攻击这种无线信号攻击方式一样，当年研发 GPS 的科学家们怎么也不会想到，时至今日，一个普通人也可以利用一些廉价的设备发出这些科学家当年自认为只有他们的卫星才能发出的导航信号吧。

无线电技术下的攻防在未来会愈演愈烈，各种资料、设备、研究社区的丰富也使得更多的安全研究者开始踏入这个领域进行各自的研究，无线电通信安全终将成为信息安全体系重要的一环。