第22话

手机

我很少需要诉诸技术攻击。公司可以花费数百万美元用于技术保护,如果有人基本上可以打电话给某人并说服他们在计算机上做一些降低计算机防御或泄露他们正在寻找的信息的事情,那就浪费了。

– 凯文·米特尼克

隐私与隐藏无关　隐私与人的成长和代理有关。

– 克里斯托弗·怀利

保护手机、它们支持的应用程序生态系统以及它们所依赖的电信网络是现代世界的核心。首先,在 iPhone 推出后的十年里,世界从通过 PC 或笔记本电脑访问互联网转向使用智能手机,并增加了数十亿新用户。整个业务部门在转向应用程序时正在发生革命性变化;地球上 55 亿成年人中,有 50 亿人拥有手机,其中 40 亿人拥有智能手机。其次,从智能音箱到汽车的新一代联网设备与手机非常相似,通常使用相同的平台并共享相同的漏洞。第三,手机现在提供了身份验证的基础:如果您忘记了密码,您会收到一条短信来恢复它　因此可以窃取您短信的人可能会花您的钱。

第四,移动网络对其他基础设施至关重要:电力公司在维修故障时依靠手机指导他们的工程师,所以如果电话系统在电力恢复后几小时内出现故障,那就是一个真正的问题。最后,还有公共政策。虽然智能手机通过提供银行服务等服务彻底改变了第三世界穷人的生活,但它们也有助于监视和控制。

电话生态系统非常复杂,要掌握它,安全工程师不仅需要加密和访问控制等一般安全知识,还需要了解 Android 和 iOS 等特定平台,还需要了解移动和固网.电信安全的历史

具有指导意义。早期的攻击是由 enthusi asts（“电话飞客”）对电话公司进行的，目的是获得免费电话；然后电话系统的漏洞被骗子利用来逃避警方的窃听；然后引入了收费电话，这带来了大规模的欺诈行为；然后，当电信市场自由化时，一些电话公司开始对彼此的客户进行攻击；一些电话公司甚至互相攻击。

由于各种原因，在每个阶段采取的防御措施往往不够充分。同样的剥削循环随后在互联网上重演 业余黑客接着是关于窃听的争论，接着是公司和用户之间的欺诈和争斗；当两者走到一起时，我们看到了许多复杂的相互作用。现在，我们看到针对银行系统的基于电话的欺诈行为迅速增加，窃取人们个人信息的不良应用程序以及关于 5G 基础设施对国家安全影响的激烈政策辩论。

安全工程师如何解决这个问题？

手机作为一个平台的安全性取决于很多因素，我将在两个主要标题下进行处理。

1. 首先，它所连接的网络是否以某种方式受到损害，无论是通过某种窃听还是通过破坏手机网络身份的 SIM 卡交换攻击。

2. 其次，存在设备本身是否受到威胁的问题，无论是通过在操作系统中生根的恶意软件，还是通过安装潜在的恶意应用程序或库。

电话安全曾经是第一个，但现在主要是第二个。

22.1 对电话网络的攻击

滥用通信可以追溯到几个世纪前。在 Rowland Hill 爵士发明邮票之前，邮资由收件人支付。不请自来的邮件成了一个大问题 尤其是对名人来说 所以收件人可以检查信件并拒收，而不用付钱。人们很快想出了在信件封面上发送短信的方案，但他们的通讯员拒绝了。引入了法规来阻止这种情况，但从未真正有效 [1460]。

电报产生了第二组滥用行为。早期的光学电报使用信号量或日光仪工作；人们会贿赂操作员，或者通过望远镜观察最后一个日光仪站来“破解本地环路”，以便在当地博彩公司之前了解哪匹马赢了。在这里，通过立法解决问题的尝试也以失败告终 [1818]。当电报降低成本时，问题变得更糟；更大的通信量，以及内置于服务之上的更大的灵活性，导致了更多的复杂性和更多的滥用。

电话也一样。

22.1.1 对电话呼叫计量的攻击

早期的电话计费系统容易被创造性滥用。

- 在 20 世纪 50 年代,某些系统中的操作员必须通过聆听硬币掉落在金属板上的声音来判断电话亭客户已经付款,因此人们练习用一块金属敲击硬币箱以敲击正确的音符。

- 起初,接线员无法知道来电是从哪部电话打来的,所以她不得不询问来电者的号码。他可以提供其他人的电话号码 然后谁会被起诉。运营商开始回拨以验证国际电话号码,因此人们制定了社会工程攻击（“这里是 IBM,我们想预订到旧金山的电话,因为时差,我们的总经理可以接受今晚在家吗?他的号码是 xxx-yyyy ）。因此,公用电话线路会发出警告以提醒接线员。但英国的实施有一个错误:通过公用电话呼叫接线员的客户可以短暂按下其余部分,随后他将重新连接（通常是不同的接线员）,这次没有警告电话来自公用电话。然后他可以在任何地方打电话并向任何本地号码收费。

- 早期系统还通过一个或多个脉冲发出硬币进入的信号,每个脉冲都包括在线路中插入一个电阻,然后是一个短暂的开路。在一些大学,有进取心的学生安装了“魔法按钮”,可以在学生会的电话亭中模拟这种情况,这样人们就可以免费打电话了。 （在这种情况下,账单交给了学生会,对于学生会来说,魔术按钮并不是那么有趣。）

对收费表的攻击已经持续了一个多世纪。大多数国家在 1990 年代将他们的公用电话从硬币转为芯片卡以降低硬币收集和破坏行为的成本,但正如我在第 18.5 节中所说的那样,一开始的设计通常很糟糕,恶棍卖了很多假电话卡直到它得到固定的。

其他攻击涉及所谓的夹式攻击:将电话物理连接到其他人的线路上以窃取他们的服务。在20世纪70年代至90年代,国际电话非常昂贵,一些外国学生将电话夹在住宅线路上,以便给家里打电话,而毫无戒心的房主可能会收到巨额账单。在给出拨号音之前,挪威电话公司让客户驻地设备向交换机验证自身 [994]。

这家英国电话公司并不像挪威电话公司那样开明,并且制定了拒绝窃听的政策,因此它可以向受害家庭收取电话费。这偶尔会造成侧面损伤,克拉姆灵顿的一个家庭就会发现这一点。他们遇到麻烦的第一个迹象是听到他们线路上的对话。接下来是警方的访问,他们说有人投诉骚扰电话。投诉人是三位女士,她们的一位数字都与这个家庭据称制作了大量数字的数字不同

电话。检查这家人的账单时,也有人拨打过一串号码,结果发现是公用电话;这些都是在骚扰电话的同时突然开始的。当家人后来向电话公司投诉故障时,他们的连接被重新路由,这就解决了问题。

电话公司维修工程师的一份报告指出,该家庭的线路在配电柜处被篡改,但这是违反教义的,该公司后来声称该报告有误。原来附近住着一个毒贩,他窃听了他们的电话线是为了用公用电话给他的快递员打电话,这似乎是一个合理的推论。

通过使用无辜家庭的电话线而不是他自己的电话线,他不仅节省了电话费,而且更有可能逃避警方的监视。

但警察和当地电话公司都拒绝进入毒贩居住的房子,声称这太危险了 尽管毒贩此时已被判入狱六年。这家挪威电话公司拒绝了为辩方就夹式电话作证的邀请。结果是该用户因拨打骚扰电话而被定罪,该案件被广泛认为是误判。

从无绳电话窃取拨号音是该主题的另一个变体。
在 1990 年代,这在巴黎变得如此普遍,以至于法国电信打破了电话公司的传统并宣布它正在发生,声称受害者正在使用易于欺骗的非法进口无绳电话 [1097]。这有点厚颜无耻,因为大多数设备似乎只是将手机序列号发送到基站,而不是使用 DECT 安全机制,后者使用法国阿尔卡特公司获得专利的加密技术。这些机制是专有的,但结果证明存在多个弱点,正如 Erik Tews 在对它们进行逆向工程后于 2012 年记录的那样 [1871]。DECT 身份验证基于弱分组密码;机密性使用弱流密码(稍微复杂一点的 A5/1 版本,我将在下面第 22.2.1 节中描述),通常需要234次努力才能破解;有弱随机数发生器;而协议故障包括中间人攻击和重放攻击,在这种攻击中,您进行静默呼叫以收集密钥流以解密您之前记录的呼叫。据说德国情报部门使用 DECT 对新兵进行信号收集和密码分析方面的培训。自从 Tews 的作品发表后,DECT 标准机构建议改用 AES,但尚不清楚有多少供应商会受到影响。要点是,对于附近有能力的对手,无绳电话无法为您提供安全保障,而且随着 1990 年代加密货币战争期间出现的标准,您应该别无所求。至于夹式欺诈,自从 Skype 和 WhatsApp 等服务使长途电话变得便宜以来,它已基本消失。

社会工程学提供了另一种方法。一个骗子打电话给你,假装来自 AT&T,并询问你是否用你的电话卡多次拨打秘鲁的电话。当你否认时,他们说,为了冲销费用,你能确认你的卡号是123-456-7890-6543吗?不,你说(如果你不是很警觉),它是 123-456-7890-5678。现在 123-456-7890 是您的电话号码,5678 是您的密码,这样骗子就可以向

你。

收费电话服务在 1990 年代迅速增长,导致诈骗犯想出各种花招让人们打电话给他们:寻呼机信息、招聘广告、关于亲戚的虚假紧急信息、带有 0900 接入号码的“低成本”电话卡、你的名字。事实上,欺骗人们拨打收费号码的业务使骗子能够磨练他们现在用于网络钓鱼攻击的技术。加勒比地区的 809 区号曾经是针对美国用户的骗子最喜欢的掩护;许多人不知道“国内”号码(美国+1 国际直拨代码内的号码)包括相对便宜的美国和加拿大以外的国家/地区。尽管现在很多人都知道 +1 809 是“外国的”而且更贵,但更多加勒比区号的引入,例如开曼群岛的 +1 345,使得发现此类骗局变得更加困难。

电话公司建议他们的客户“不要给陌生的电话号码回电话” 但这有多实用呢?正如银行现在训练他们的客户点击营销电子邮件中的链接,从而使他们容易受到网络钓鱼攻击一样,我也接到了电话公司打来的垃圾营销电话 尽管我在拒接电话名单上。政府通常会设立弱监管机构,避免试图监管高价运营商,声称这太难了;时不时地,一切都会爆炸。在 2000 年代后期,所有主要的英国电视公司(包括国有 BBC)最终都因在各种节目中让观众打电话和投票而被罚款。其中许多都被记录下来,所以这些电话都是徒劳的 [1323]。自 1920 年代无线电广播兴起以来,广播电台的电话诈骗一直是世界范围内反复出现的问题,并且在 1950 年代电视成为主流后变得更糟 [2050]。这也是一种反复出现的模式,即最大的骗局通常是由“受人尊敬的”公司而不是俄罗斯黑帮经营的。

22.1.2 对信令的攻击

“电话窃听”一词指的是对信号的攻击以及纯粹的电话欺诈。直到 20 世纪 80 年代,电话公司都使用带内工作的信号系统,方法是在承载语音的同一电路中发送音调脉冲。我听说的第一次攻击可以追溯到 1952 年,到 1960 年代中后期,美国和英国的许多爱好者已经找到了重新路由呼叫的方法。先驱之一乔·恩格雷西亚 (Joe Engresia) 拥有完美的音调,他在孩提时代就发现,他可以通过吹口哨拨打长途电话的背景音来拨打免费电话。他天赋较差的同事使用自制的音调发生器,其中最常见的被称为蓝盒。诀窍是拨打一个 0800 号码,然后发送一个 2600Hz 的音调,在远端清除线路 也就是说,断开被叫方的连接,同时让主叫方与交换机连接的中继线。来电者现在可以输入他真正想要的号码,无需付费即可接通。电话窃听是在湾区扎根的计算机黑客文化的根源之一,并在个人计算机的发展和演变过程中形成 [1222]。史蒂夫·乔布斯 (Steve Jobs) 和史蒂夫·沃兹尼亚克 (Steve Wozniak) 在涉足计算机领域之前首先构建了蓝盒 [722]。

电话窃听始于强烈的意识形态因素。在那些日子里,大多数电话公司都是垄断企业 规模庞大、不知名且反应迟钝。在

在美国,AT&T 是一个滥用垄断的公司,以至于法院最终将其解散;欧洲的大多数电话公司都是政府部门。国内电话线曾被盗用的人发现他们被指控了。如果向你女儿求爱的那个年轻人（你不知道)是一个电话飞客,他没有为他打给她的电话付费,你会突然发现公司试图勒索这个年轻人的名字或付款。电话公司也与国家安全保持一致。

许多国家/地区的电话飞客发现了信号代码或开关功能,使警察或间谍能够在他们舒适的办公桌上窃听您的电话,而无需派出接线员来窃听。回到越南战争和学生抗议的时代,这是煽动性的事件 。电话飞客是反主流文化的英雄,而电话公司则与黑暗势力携手并进。

由于只要电话信号在带内传输就无法阻止蓝盒攻击,电话公司花费数年时间和数十亿美元转向带外的称为 SS7 的信号系统,在 e等在普通订户无法轻松访问的私人互联网上。渐渐地,一个地区接一个地区,世界对蓝盒攻击关闭了大门。这迫使攻击者成为内部人员。

22.1.3 攻击交换和配置

一旦电话交换机变得可编程,第二波攻击就针对计算机。通常,这些是交换机中 LAN 上的 Unix 机器,其中也有具有管理功能（如调度维护)的机器。通过攻击其中一台防护较差的机器,phreak 可以穿过 LAN 并侵入交换设备 或侵入其他辅助系统,例如用户数据库。有关 PacBell 在这方面经验的调查,请参阅 [388];关于 Bellcore 的,请参见 [1059]。

使用这些技术,可以找到未列出的电话号码,可以在用户不知情的情况下转接电话,并且各种恶作剧成为可能。 1985-88 年,加利福尼亚电话飞客凯文·波尔森 (Kevin Poulsen) 获得了 PacBel 的许多交换机和其他系统的根访问权限:这显然涉及入室盗窃和黑客攻击（他最终被判密谋拥有十五个或更多假冒、未经授权和被盗的访问设备).

他做过一些小事,比如为名人获取未公开的电话号码,以及从洛杉矶广播电台 KIIS-FM 赢得一辆保时捷。每周 KIIS 都会给第 102 位来电者送一辆保时捷,因此 Poulsen 和他的同伙封锁了所有拨打电台 25 条电话线的电话,只保留了他们自己的电话线,打了第 102 次电话并取回了保时捷。他还被指控非法窃听和从事间谍活动;这些指控被驳回。事实上,联邦调查局对他的打击如此之大,以至于有人指控该机构与电话公司之间存在不正当关系,就像“你在需要时用窃听器挠我们的背,我们会调查你的黑客问题” [690]。

FBI 的敏感性确实凸显了这样一个事实,即外国情报机构利用对电话公司计算机的攻击来进行远程窃听。

[388]中提到的一些攻击来自海外,并且在上下文中可能会使用此类技巧使整个电话系统崩溃

美国国家安全局担心信息战攻击 [727, 1106]。进口电话交换机而不是自己建造电话交换机的国家只能假设他们的电话交换机存在供应商政府已知的漏洞。 （在 2001 年入侵阿富汗期间,喀布尔有两个交换站:一个旧的机电交换站和一个新的电子交换站。美国空军只轰炸了第一个。）

许多真正的攻击涉及内部人员,他们错误配置系统以通过特殊号码提供免费电话。当电话公司为额外电话提供服务的边际成本为零时,这并不重要,但随着 1990 年代增值服务的激增,以及随着电话公司之间现金支付的放松管制,它变得严重 [460]。在一次让人想起 Poulsen 的黑客攻击中,英国电信的两名员工在一次电话会议中每人赢得了十张协和式飞机的票后被解雇,而在这些电话会议中,每千个电话中只有一个随机选择的电话本应通过 [1914 年]。

至于局外人,除了波尔森之外,另一位“黑客大亨”是凯文米特尼克,他因一系列入室盗窃被捕并被定罪,这也使他成为联邦调查局追捕的目标。他们最初认为他是一名外国特工,滥用美国电话系统窃听敏感的美国目标。正如我在第 3 章中提到的,他出狱后作证说,他几乎所有的功绩都涉及社会工程。他写了一本关于欺骗的书,成为经典 [1325]。在国会作证时,他引用了本章开头的话：“公司可以花费数百万美元用于技术保护,但如果有人基本上可以打电话给某人,或者说服他们在计算机上做一些事情,那么这就是浪费了。降低计算机的防御能力或泄露他们正在寻找的信息”。与其他公司一样,电话公司很容易受到粗心的内部人员和恶意的内部人员的攻击。

快进到 2020 年,一个令人担忧的发展是 switch ing exploits 的增长。许多电信公司现在为企业客户提供 SS7 访问权限,例如,如果他们想发送批量 SMS 消息以验证客户身份。

通过访问交换结构,他们可以玩 Poulsen 和 Mitnick 在 1980 年代玩的那种游戏。例如,如果我想破解你的 Gmail 帐户,我会向你的移动服务提供商发送一条消息,说你已经漫游到我的网络中。然后我开始在谷歌恢复账户,它会发送一条短信来重置你的密码。正如我在 3.4.1 和 12.7.4 节中提到的,这现在正被积极用于银行欺诈； 2016 年在德国首次使用它从银行客户那里窃取资金,当时他们在不知情的情况下被转移到另一个网络； 2019 年伦敦也发生过类似的欺诈行为 [489]。 SS7 也被沙特阿拉伯的 MNO 滥用来追踪在美国的沙特持不同政见者 [1054]。发达国家的大多数主要电信公司现在都使用一些 SS7 防火墙,并根据他们的漫游协议允许或拒绝远程访问。如果有这样的协议,远程电信公司授予 SS7 访问权限的公司可以窃取手机以获取其 SMS 消息,或者让它进行收费欺诈。如果有单个用户的投诉,取证可能会很困难;你能做的最好的事情可能是寻找漫游费用。如果有上千个案例,银行可能会主动去找运营商。但是银行和他们的批量 SMS 承包商正在向运营商支付 SS7 访问费用,从而打开以前封闭的系统。简而言之,我们曾经认为攻击涉及

SS7 是民族国家的保护区,但现在已不再如此。

22.1.4 不安全的终端系统

现代电话网络的下一个主要漏洞是不安全的终端设备和功能交互。

语音邮件有许多漏洞,无论是作为客户端的答录机还是现在常见的云服务。

漏洞利用从诱骗某人拨打收费电话号码开始,然后升级为记者和其他人通过许多人懒得更改的默认 PIN 来入侵语音信箱。最臭名昭著的案件是 2002 年 3 月 21 日英国女学生米莉道勒被谋杀。 2011 年,一名为当时默多克帝国的英国旗舰《世界新闻报》工作的调查员侵入了米莉的语音信箱,在此过程中干扰了警方的调查,并可能导致她的一些消息被删除,让米莉的家人误以为她还活着。由此引发的愤怒导致该报停刊,多项刑事定罪 包括 2014 年戴维·卡梅伦 (David Cameron) 的公关人员安迪·库尔森 (Andy Coulson) 入狱,安迪·库尔森 (Andy Coulson) 曾任《世界新闻报》编辑 以及对新闻标准的公开调查。

但真正利用不安全终端系统的大型欺诈往往以公司和政府部门为目标,因为他们有能力支付大笔电话费。到 1990 年代中期,对企业专用交换分机系统 (PBX) 的攻击已成为一项大生意,每年给企业造成数十亿美元的损失 [467]。 PBX 通常配备用于重新归档呼叫的设施,也称为直接拨入系统接入 (DISA)。公司的销售人员可以拨打 0800 号码,输入 PIN 或密码,然后利用大公司可以享受的低长途电话费率再次拨打电话。

如您所料,这些 PIN 会被恶棍所知并进行交易 [1352]。
结果称为拨通欺诈。

在许多情况下,PIN 由制造商设置为默认值,客户从未更改过。许多 PBX 设计也有固定的工程密码,允许远程维护访问,谨慎的人认为任何 PBX 都至少有一个后门,以便执法和情报机构轻松访问(据说,作为出口许可的条件) .此类功能会被发现并被滥用。在一个案例中,苏格兰场的 PBX 遭到破坏并被犯罪分子用来重新拨打电话,使苏格兰场损失了 100 万英镑,他们为此起诉了他们的电话安装商。骗子从未被抓到 [1868]。犯罪分子的动机之一是获取不会被窃听的通信。作为此类犯罪受害者的企业发现警方不愿调查,电话公司也无济于事 他们不喜欢他们的账单有争议 [1624]。

在一个臭名昭著的案例中,参与劳动力市场敲诈勒索的中国歹徒 将来自中国福建的非法移民偷渡到英国 侵入了英国地区议会的 PBX,并用它重新拨打了价值超过 100 万英镑的中国电话。在一些工人死亡后,该团伙被警方解决了;涨潮时他们正在莫克姆湾采贝类

进来淹死了他们。该委员会现在已经发现其电话账单中的差异,并起诉电话公司要求退款。电话公司争辩说,它不应该受到指责,即使它提供了不安全的 PBX。在这里,歹徒也不仅对省钱感兴趣,而且对逃避监视感兴趣。 （事实上 ,他们通过阿尔巴尼亚的一个受损的 PBX 将他们的电话路由到中国,因此最有可能被这些机构监控的电话的跨境部分是在他们的收集系统不会接触的号码之间;苏格兰场的案件似乎也使用了同样的伎俩,骗子通过美国拨打电话。）

除了这些案例之外,拨号欺诈主要是由收费服务驱动的,而且骗子与收费线路运营商勾结。大多数公司不了解保护其“拨号音”的必要性,即使他们想保护也不知道如何保护。 PBX 通常由对安全知之甚少的公司电信经理运营,而安全经理通常对电话知之甚少。随着公司电话网络采用 VOIP 技术并与数据网络融合,这种情况正在发生变化。全球企业遭受的 PBX 欺诈损失估计从 2011 年的 49.6 亿美元下降到 2017 年的 38.8 亿美元,其中约一半现在是 VOIP 而不是传统的 PBX [91]。

利用不安全的终端系统也会影响国内用户。高价移动恶意软件于 2006 年出现,当时红色浏览器蠕虫通过向俄罗斯发送 5 美元的 SMS 来套现 [941];这在 Android 出现后得到了扩展,我们将在 22.3.1.4 节中讨论移动恶意软件。现在电话越来越多地用于诸如投票、确保进入公寓楼、检查罪犯是否遵守假释条款以及验证金融交易等任务,更多的动机被创造出来,用于更有创意的恶作剧,并且特别是对于破坏来电显示的黑客攻击。自 2000 年代初以来,就一直有人警告称,来电显示黑客攻击、短信欺骗和对 SS7 信号的攻击可能被用于欺诈。现在这已成为现实,我们将在本章后面更详细地讨论它。

22.1.5 特征交互

电话操作通常涉及功能交互。

- 华盛顿州 Clallam Bay 惩教中心的囚犯只被允许拨打对方付费电话,他们发现了一个有趣的系统漏洞利用,电话公司 (Fone America) 引入该系统来自动处理对方付费电话。系统会拨打所拨号码,合成语音会说：“如果您愿意接受来自……（来电者姓名)的对方付费电话……请在您的电话上按两次数字 3。”囚犯应该说出他们的名字,以便机器记录和插入。

  作为一项附加功能,该系统能够用西班牙语发送问候语。囚犯照做了,当被要求表明身份时,他们说：“如果你想用英语听到这条消息,请按 33。”这种方法经常有效,以至于他们可以接通公司的 PBX,并说服接线员给他们一条外线。华盛顿大学多次被这个骗局击中[696]。

- 许多目录查询服务会将您连接到他们的电话号码

刚刚为您提供的一项高级服务,适用于无法在驾驶时拨号的驾车者。它还可用于破坏依赖端点识别的机制。尽管有呼叫限制,顽皮的孩子还是用它来拨打性热线,而顽皮的成年人用它来防止他们的配偶看到家庭电话账单上的情人号码 [1456]。

- 呼叫转移是许多骗局的来源。在过去,它被用来恶作剧,比如孩子们对电话公司接线员进行社会工程,将他们老师的电话转接到性热线。如今,它既可以是专业的,也可以是令人讨厌的。例如,欺诈者可能会告诉受害人通过拨打一系列数字来与银行确认他们的电话号码 这会将来电转接到攻击者控制的号码。

  所以银行的回调机制就失效了。

- 可以通过各种方式利用电话会议。例如,在某些国家/地区,足球流氓被实行宵禁,要求他们在比赛期间呆在家里,并通过拨打缓刑服务来证明这一点,该服务会验证来电显示。因此,您让您的合作伙伴通过试用服务和您的手机设置电话会议。如果缓刑官问起人群的噪音,你告诉他那是电视,你不能把它关小,否则你的伙伴会杀了你。 (如果他想给你回电话,你可以让你的搭档转接电话。)

22.1.6 网络电话

在 IP 语音 (VOIP) 中,语音流量经过数字化、压缩并通过 Internet 路由。这在 1970 年代有实验性的开端;产品于 1990 年代开始出现,从 2000 年代中期开始成为大企业。如今,大多数传统电话都已数字化并通过属于电话公司的 IP 网络发送,因此从技术意义上讲,现在几乎所有电话都是“VOIP”。但是,虽然我的家庭电话假装是一部普通的旧电话,但我的实验室电话现在是一个天生的 VOIP 设备,提供电话会议和我不理解的各种其他复杂功能。

最流行的 VOIP 协议,即会话启动协议 (SIP),有其自身的漏洞 [2069],但主要是通过不良配置受到攻击,许多参与者都在不断扫描这些漏洞; PBX 每天可以收到超过一百万条消息,试图注册为分机,然后尝试拨打欠发达国家的高成本号码 [1271]。正如我在第 22.1.4 节中指出的那样,到 2017 年,针对公司 PBX 系统的 VOIP 欺诈每年约为 20 亿美元 [91]。与安全性的更广泛交互变得复杂。公司安全政策可能导致防火墙拒绝通过 VOIP 流量。当前的政治争论是关于机器人呼叫,如果他们通过 VOIP 进行呼叫,则可以更容易地隐藏来电显示。 FCC 在 2020 年投票坚持要求电信公司在 2021 年 6 月底之前实施一套协议 STIR/SHAKEN,该协议通过 SIP 对呼叫者进行身份验证 [326]。另一个监管问题是政府希望通过 VOIP 服务进行的紧急呼叫能够可靠地工作,并提供有关呼叫者位置的信息。但是 IP 数据包流可以来自任何地方,没有人拥有足够的互联网来保证服务质量。尽管 VOIP 听筒看起来像电话而且可以工作

就像电话一样,如果断电 ,您的服务也会断电。然后你被迫退回到移动网络。所以现在默认的应急系统是移动网络而不是传统网络。

22.1.7 电话公司的欺诈

电话欺诈不仅仅是不正当的客户对电信公司实施长途电话欺诈,并利用电信公司没有真正动机强化的机制来欺骗其他客户的故事,还有许多不道德的电信公司的骗局。典型的骗局是 cramming,一家流氓电话公司向不知情的用户收取大量小额费用。计费是在电话公司垄断的时代设计的,通常是国有的,并假设电话公司相互信任:如果公司 A 创建呼叫数据记录 (CDR),表明电信公司 B 的客户呼叫了他们的用户,他们只需将其传递给支付费用的电信公司 B。 （它没有动机狡辩,因为它得到了削减。）

我自己就是试图填鸭的受害者。在巴塞罗那度假时,我妻子的包被抢了,所以我们打电话取消了她放在包里的电话。几个月后,我们收到了一张SIM卡最近在西班牙产生的几十美元漫游费的要求。很可能,这家西班牙电话公司只是简单地向他们以前见过的号码塞入一些费用,因为他们知道他们通常会逃脱惩罚。我妻子的前 MNO 坚持说,即使她取消了号码,她仍然要为几个月后向其收取的电话费负责,并且必须付清费用。我们之所以免于指控,只是因为我在一次学术研讨会上遇到了公司的首席执行官,并且能够让他的私人办公室解决这个问题。没有这种访问权限的客户通常会吃亏。

事实上,英国电话公司对投诉的回应是为客户提供“保险”以防止欺诈性收费。他们可以逃脱惩罚,这是一个明显的监管失败。有很多变体:如果您在美国拨打 800 号码,公司可能会说“我们可以马上给您回电吗?”如果您同意,则您将被视为已接受费用,费用可能很高。如果您在通话过程中响应语音提示,也会发生同样的情况。

另一个问题是猛击 未经用户同意擅自更改其服务提供商。假设塞满和猛击只是由不守规矩的小型操作员完成的,那将是错误的。 AT&T 是最严重的违法者之一,不仅因为猛烈抨击而被罚款,还因为伪造订户签名以使他们看起来好像同意切换到他们的服务而被罚款。他们在德克萨斯州伪造订户已故配偶的签名时被捕。

还有一个是利用国际电话进行溢价诈骗。
国内收费号码的滥用导致许多国家的监管机构迫使电话公司向用户提供收费号码屏蔽服务。

电信公司通过将收费号码伪装成国际号码来避开这个问题。我在第 22.1.1 节中提到了使用加勒比号码的诈骗,来自小国家的许多其他电话公司也参与其中。此类骗局得益于一项国际协议（内罗毕公约）,该协议阻止电话公司选择性地屏蔽国际目的地。来自政府的建议

报纸仍然警告提防“wangiri”骗局,在这种骗局中,您接到的电话只响一次,希望您回拨国际收费号码。然而这些似乎已经停止了； 2020 年对机器人电话的广泛研究没有发现它们的证据 [1543]。诈骗可能从电信平台转移到应用生态系统的原因有很多;诈骗与监管之间的相互作用是复杂的。

到智能手机出现时,电话公司已经习惯于从提供高价值服务中分一杯羹,从伦敦的停车计时器到芬兰的渡轮票。随着恶意软件在手机上广泛传播,控制被破坏手机的僵尸网络牧民可以通过短信支付商品和服务费用。智能手机革命使许多新服务成为可能,支付方式也从短信支付转变为通过应用程序支付。短信滥用已经到了谷歌和苹果都不允许普通应用程序发送或接收短信的地步。我们可能会停下来想想这个行业的经济状况。

为什么电信公司从来没有感受到照顾客户的责任?

22.1.8 电信安全经济学

电话和有线电视公司的固定成本非常高,而边际成本非常低。建立一个全国性的网络需要数十亿美元,但处理额外电话或电影下载的成本基本上为零。正如我在经济学一章中讨论的那样,这有几个含义。

首先,存在着主导企业市场的趋势。多年来,大多数国家都认为电话服务是“自然垄断”,由政府经营;主要的例外是美国,旧的 AT&T 系统受到严格监管。在 AT&T 因反托拉斯案而解散以及玛格丽特·撒切尔 (Margaret Thatcher) 在英国将 BT 私有化之后,世界转向了一种不同的受监管竞争模式。细节因国家而异,但总的来说,某些行业（如手机)有固定数量的允许竞争者;其他（例如长途服务)免费供公司参与竞争;和其他（例如本地环路供应)仍然是垄断,但受到监管。

其次,竞争性行业（如长途电话)的价格迅速下降至接近于零。某些行业因应用程序而变得更具竞争力:Skype 和 WhatsApp 让国际电话基本免费。

在许多电信市场,结果是定价混乱 产品不断变化,新产品提供慷慨的介绍性折扣以与低成本供应商竞争,但随后又偷偷提高了价格。宽带接入与移动服务和电视产品不断捆绑在一起。如果您不厌其烦地不断查看价格,您可以获得划算的交易,但通常是以服务冷漠为代价的。如果您没有时间仔细检查您的宽带和手机账单,您可能会遇到一些令人不快的意外。

22.2 移动化

自 1981 年作为昂贵的奢侈品诞生以来,手机已成为重大技术成功案例之一。到 2020 年,我们现在拥有超过 50 亿用户;据说仅在 2019 年就售出了超过 10 亿部手机。在发达国家,大多数人至少拥有一部手机,许多新的电子服务都建立在它们之上。发展中国家的增长也很迅速,那里的有线网络经常破旧不堪,人们习惯于等待多年的电话服务。在许多地方,移动网络的到来将村庄与世界连接起来。这带来了很多好处,也带来了新的犯罪。随着技术的发展和部署,两者都稳步发展。

手机安全随着滥用的发展而发展。第一代移动电话 (1G) 使用模拟信号,手机只是通过无线链路 1 以明文形式发送其序列号。因此,恶棍们制造了设备来从附近的电话中捕获这些号码,或者对电话进行重新编程以从附近的其他电话中窃取 ID。主要客户之一是电话销售业务,它会窃取电话服务并低价转售,通常卖给想给家里打电话的移民或学生。电话销售接线员会在已知的摊位上用克隆手机闲逛,他们的客户会排队等候给家里打电话几美元。呼叫销售市场与匿名通信的犯罪市场相辅相成:人们侵入手机以在每次通话中使用不同的身份。这些被称为不倒翁,警察特别难以追踪 [944]。 1G 电话没有对语音进行加密,因此任何人都可以随便用无线电接收器窃听电话,尽管如此,来电者匿名的可能性导致他们被用于犯罪。对序列号的需求迅速增长,满足它的难度越来越大,即使是在机场等大量手机开机的地方进行窥探也是如此。因此价格上涨,并且除了被动聆听之外,主动方法也开始被使用。

移动电话是蜂窝电话:运营商将服务区域划分为多个小区,每个小区由一个基站覆盖。移动设备使用信号最强的基站,并且有一些协议可以在客户四处走动时将呼叫从一个小区转移到另一个小区。早期的主动攻击包括一个假基站,通常位于高速公路桥梁等有大量过往交通的地方。当手机经过时,他们听到了更强的信号,并试图通过发送序列号和密码进行注册。

尝试了各种机制来减少欺诈数量。大多数操作员都运行入侵检测系统来监视可疑的活动模式,例如移动速度过快或呼叫量或持续时间的快速增加。沃达丰还使用了 RF 指纹识别,这是一种军用技术,在该技术中,由于手机无线电发射器的制造差异而产生的信号特征被用于识别各个设备并将它们与所要求的序列号联系起来 [776]。

1在美国系统中,有两种:一种用于设备,一种用于用户。

22.2.1 全球移动通信系统

第二代手机（2G)采用了数字技术。全球移动通信系统 (GSM) 成立于 1987 年,当时有 15 家公司加入了 GSM 协会,并获得了欧盟的政治支持;这项服务于 1992 年推出。GSM 的设计者着手保护系统免受克隆和其他攻击:他们的目标是 GSM 至少应该与有线系统一样安全。他们做了什么,他们如何成功以及他们失败的地方,创造了一个有趣的案例历史。

该行业最初试图对构成 GSM 协议核心的密码和其他保护机制保密。这没有用:一些最终泄露了,其余的则通过逆向工程被发现。我将在这里简要描述它们。移动网络由无线接入网（RAN)和核心网（CN)组成,每个移动网络都有两个数据库,一个包含自己移动设备位置的归属位置寄存器（HLR)和一个访问位置寄存器（VLR）) 用于从其他网络漫游的移动设备的位置。这些数据库使传入呼叫能够被转发到正确的小区。

这些手机是商品,使用用户识别模块 (SIM) 进行个性化设置 这是您在注册网络服务时获得的智能卡,您可以将其加载到手机中。可以认为 SIM 包含三个数字:

1. 可能有您用来解锁的个人识别码
   卡片;
2. 有一个国际移动用户识别码（IMSI）,一个唯一的
   映射到您的手机号码的号码;
3. 最后是订户验证密钥Ki,这是一个 128 位数字,用于验证 IMSI 并为您的家庭网络所知。

还有一个手机序列号,即国际移动设备识别码 (IMEI)。用于向网络验证手机的协议运行如下（参见图 22.1）。上电时,SIM 发出 IMSI,手机将其与 IMEI 一起发送到最近的基站。

IMSI 被中继到订户的 HLR,后者生成五个三元组。每个三元组包括:

- RAND,随机挑战;
- SRES,回应;和
- Kc,一个加密密钥。

该算法是 RAND 在 SIM 的身份验证密钥Ki 下加密,给出与Kc连接的 SRES：

$$\{RAND\}Ki = (SRES|Kc)$$

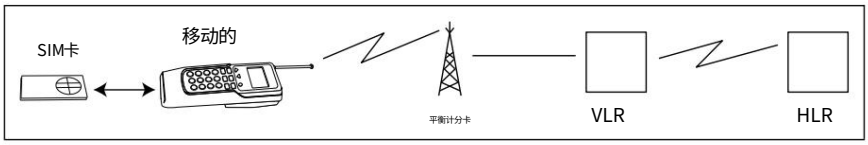

图 22.1：- GSM 认证系统组件

加密方式由发行方决定;一个名为 Comp128 的早期标准被证明是不安全的 [1971, 1972],因此发行人现在使用散列函数或使用 AES 的构造。

无论如何,三元组被发送到基站控制器 (BSC),后者现在将第一个 RAND 提供给移动设备。它将此传递给计算 SRES 的 SIM。移动设备将其返回给基站,如果它是正确的,则移动设备和基站现在可以使用加密密钥Kc进行通信。因此,整个身份验证协议如图 22.2 所示运行。

SIM卡！ HLR IMSI
HLR ! BSC（兰德、SRES、 Kc）、...
平衡计分卡！ SIM RAND
SIM !平衡计分卡 SRES 平
衡计分卡 !移动{trac}Kc

图 22.2 – GSM 认证协议

该协议中存在多个漏洞。首先,基站未经认证,因此窃听者很容易使用虚假基站来拦截电话。这种设备在欧洲被称为 IMSI 捕捉器,在美国被称为 StingRays,现在是标准的执法设备 2。其次,在大多数国家,基站和 VLR 之间的通信在微波链路上未加密3。这允许情报机构进行批量拦截,并且在许多情况下可以访问欺骗或解密 trac 所需的三元组。

GSM 的引入引起了犯罪模式的重大转变。身份验证机制使手机克隆变得困难,因此恶棍转而使用偷来的信用卡购买手机,使用偷来的身份或贿赂 siders [2034]。抢劫是下一个问题,媒体报道了大量关于孩子因手机而被抢劫的故事。 1995 年至 2002 年间,手机犯罪确实增加了 190%,但为了保持这一背景,订户数量在同一时期增加了 600% [865]。一些盗窃行为是欺凌行为 孩子拿走小孩子的手机;有些是保险欺诈,订户将手机掉在马桶里并报告手机被盗,因为他们的保险不包括意外损坏;但是盗窃的核心是抢劫者拿走手机并将它们卖给栅栏。许多围栏要么在授权访问用于重新编程 IMEI 的工具的手机商店工作,

2设计 2G 时,一个基站占满整个房间,成本为 10 万美元,因此忽略中间人攻击似乎是合理的。如今,它所需要的只是一个低成本的软件无线电。

3设备可以加密trac,但一般电话公司没有动力
打开加密。

手机中的序列号,或者与将手机运送到国外的有组织犯罪分子有联系4。

预付费手机大约从 1997 年开始出现,使该行业迅速扩展到没有信用评级的人群,包括富裕国家的穷人和贫穷国家的每个人。到 2008 年,预付费占墨西哥市场的 90%,但在美国占 15%。在 2010 年代,数十亿人不仅可以打电话和发短信,还可以使用在线信息和支付服务。

预付费电话也使匿名通信变得实用。这些问题不仅包括逃避警方的窃听,还包括欺诈、跟踪、勒索、欺凌和其他类型的骚扰。但是,预付费电话只有在不非常努力的情况下才能保护您免受警察的伤害。大多数犯罪分子对停止 trac 分析所需的操作纪律水平一无所知。正如我已经说过的,一名所谓的 9/11 策划者在使用与另一名基地组织成员使用的同一批次的预付费 SIM 卡时被捕;在 21/7 伦敦爆炸案失败后,一名可能的炸弹袭击者逃往罗马,在那里他被立即抓获。他在途中更换了手机中的 SIM 卡;但通话记录不仅显示来自 SIM 卡的 IMSI,还显示来自手机的 IMEI。如果全世界的警察都在追捕您,那么仅仅更换 SIM 卡是不够的。运营安全需要对网络的运作方式有一定的了解。

除了鉴权,2G还应该提供另外两种
保护 位置安全和通话内容的保密性。

位置安全机制是当移动设备注册到网络时,它会获得一个临时移动用户标识 (TMSI),作为其在该网络中的地址。这是一个轻量级的机制;它被伪装成不同网络中的基站的 IMSI 捕捉器轻而易举地击败了。

一旦身份验证和注册完成,2G GSM 还通过加密手机和基站之间的通信来提供一些通话内容机密性。语音被数字化、压缩并切碎成数据包;每个数据包都通过使用从加密密钥Kc和数据包编号生成的伪随机序列进行异或运算来加密。欧洲常用的算法是A5/1。这是一种流密码,与 Comp128 一样,最初是秘密的;和 Comp128 一样,它被泄露了,很快就发现了对它的攻击 [248]。到 2000 年代中期,执法供应商开始销售可以在一秒钟内破解密钥的设备,使监视团队能够收集所有 GSM trac 并对其进行解密,这样他们就可以挑选出感兴趣的对话。手机还支持一种更弱的算法,称为 A5/2,该算法已获得出口到非欧盟国家 5 的许可,并且几乎可以立即被破解。正如我在上面第 22.1.1 节中提到的,无绳电话的 DECT 标准有些相似,但也很弱。世界各地的主要大国大使馆都有屋顶结构,表明用于捕获本地电话流量的天线,斯诺登文件证实了美国国家安全局

4在最近的智能手机设计中,IMEI 应该是不可更改的;一些安卓
手机将其保存在 TrustZone 中。

5 当澳大利亚使用 A5/2 时出现了争吵。

在美国外交使团收集本地电话记录。

除了被动批量收集之外,有针对性的主动收集还可以利用协议技巧。

GSM 供应商推出了第三种密码 A5/3,它基于称为 Kasumi 的强块密码,并成为第三代移动电话的标准。但是存在一种利用初始算法协商是明文形式这一事实的降价攻击。 IMSI 捕捉器只是告诉手机使用较弱的密码。 Elad Barkan、Eli Biham 和 Nathan Keller 意识到这可以追溯完成 [171]。如果你在跟踪一个使用他的手机的嫌疑人,你会记录通话,包括质询和响应的初始协议交换。一旦他完成,你就打开你的 IMSI-catcher 并让他注册到你的假基站。 IMSI-catcher 告诉他的手机使用 A5/2 而不是 A5/1,并且适当地设置了一个密钥 IMSI-catcher 发送了之前使用的挑战。所以手机生成和之前一样的密钥Kc 。由于它现在被用于弱密码,它可以被快速破解,从而可以访问已经记录的对话。

A5/2 现已退役;不能使用 A5/1 或 A5/3 的手机以明文通信。然而,A5/1 很容易被现代设备破坏。

电话公司、设备供应商和 ISP 现在被迫为当地执法部门提供访问权限,但其他国家通常也希望访问权限,而且窃听设施的设计往往很差,以至于可能被滥用 [1707]。 2004 年 5 月,身份不明的人(据推测来自美国国家安全局或中央情报局)在雅典奥运会期间窃听了希腊总理和该国大约 100 名政治、执法和军事精英的手机,破坏了窃听Voda fone 希腊网络中内置的设施。沃达丰及其设备供应商爱立信都被处以重罚 [1550]。我和同事几年前就警告过这个问题 [4],而斯诺登的披露表明它正在稳步恶化。我将在第三部分中更详细地讨论它。

不管怎样,最终效果是,虽然 2G GSM 安全机制被设计为在允许使用 A5/1 的国家提供比有线网络稍微好一点的保护,而在其他地方提供的保护稍差一些,但它们现在在任何地方都提供稍微差一点的保护,因为第三方可以工业化的一系列漏洞利用。

22.2.2 3G

第三代数字移动电话最初被称为通用移动通信系统 (UMTS),现在被称为第三代合作伙伴计划(3gpp,或简称 3G)。首字母缩略词 3gpp 仍然用于 4G、5G 及以后的标准机构。 3G 于 2003 年至 2004 年投入使用,并将于 2022 年退役,之后无法使用 4G 或 5G 的移动设备应该会退回到 2G。这可能主要发生在人口稀少的农村地区,在那里安装更新的 4G 和 5G 技术以及他们需要的更大的回程传输是不经济的。

3G在无线电接入网络上使用扩频技术,而不是标准2G的9.6kb/s和2.5G的几十kb/s

变体 (GPRS),3G 数据速率为每秒数十万比特。 3G 的愿景是实现各种移动服务,从移动电视到可以随时随地上网的笔记本电脑。它为智能手机革命奠定了基础。

总体安全策略在 [1976] 中描述,安全架构在 [1961] 中。密码算法 A5/1 和 A5/2 被 A3 取代,A3 基于一种名为 Kasumi [1021] 的块密码,而 A3 又基于 Mitsuru Matsui 的一种名为 Misty 的设计,该设计现已经受了二十年的公众审查 [1245]。所有密钥现在都是 128 位。密码学用于保护消息内容和信令数据的完整性和机密性,而不仅仅是内容机密性,并且保护从手机运行到核心网络,而不是简单地运行到本地基站。因此,从基站或微波回程中获取密钥或明文不再是攻击。身份验证现在是双向的,而不是单向的。从理论上讲,这将消除流氓基站的漏洞,IMSI 捕捉器将不再起作用。实际上,它们工作正常,因为它们只是告诉目标手机回退到 2G 操作。3G 还具有用于本地拦截的适当接口 [1962]。

在基本的 3G 身份验证和密钥协议 (AKA) 协议中,身份验证从手机运行到访问者位置寄存器。归属位置寄存器现在称为归属环境 (HE),SIM 称为 UMTS SIM (USIM)。家庭环境像以前一样选择随机挑战 RAND,并使用 USIM 认证密钥Ki对其进行加密,以生成响应 RES、保密密钥 CK、完整性密钥 IK 和匿名密钥 AK。

$$\{RAND\}K = (RES|CK|IK|AK)$$

还有一个 HE 和 USIM 已知的序列号 SEQ。在 RAND 和 SEQ 上计算 MAC,然后通过使用匿名密钥对序列号进行异或运算来屏蔽序列号。质询、预期响应、机密性密钥、完整性密钥和掩码序列号组成验证向量 AV,从 HE 发送到 VLR。然后 VLR 向 USIM 发送挑战、掩码序列号和 MAC； USIM 计算响应和密钥,揭开序列号,验证 MAC,如果正确则将响应返回给 VLR。

USIM卡！ HE IMSI（可以选择加密）
他！ VLR RAND、XRES、CK、IK、SEQ AK、MAC VLR！ USIM RAND, SEQ AK, MAC
USIM ! VLR 电阻

图 20.4 – 3gpp 认证协议

3G 标准规定了许多其他特性,包括身份和位置隐私机制、与 2G 的向后兼容性、从 HE 到 VLR 的加密身份验证向量的机制,以及各种可选加密机制的协商。

与 2G 一样,它的设计目标是安全性应与有线网络相媲美 [922],并且最终效果是适度的改进:尽管有针对性的攻击,但更高质量的机制可以防止空中链路上的大量窃听IMSI 捕手仍然通过利用回退来工作。在一些国家,警察在最初几年很难利用第三代手机,因为他们必须将自己的系统与网络运营商的系统集成在一起,以便在任何规模大于战术的情况下开展行动。

22.2.3 4G

第四代移动网络于 2009 年首次推出,到 2019 年占移动用户的大部分（80 亿中的 42 亿)[981]。它们始终使用 IP,这与具有电路交换核心网络的 2G 和 3G 不同。无线电接入网络从 3G 的扩频方案转变为频域均衡 (FDE) 方案,尽管存在多径无线电传播（回声）,但仍可实现非常高的比特率。更高的数据速率使谷歌地图和 Snapchat 等应用程序运行得更好,并使视频流应用程序成为可能。实际上,在 2010 年代发展了一系列标准,支持高达每秒数十兆位的兆位带宽。

4G 安全标准通过将加密限制在手机和基站之间的链接而从 3G 退回,尽管公平地说,大多数应用程序现在在应用程序层加密数据。身份验证和密钥协议 (AKA) 协议与 3G 非常相似,尽管术语有所改变。

手机现在是 UE 或用户设备,而 HE/HLR 现在是归属用户服务器 (HSS)。基站功能分为演进型 NodeB (eNodeB) 基站和少量移动管理实体 (MME),后者处理 AKA 交换、做出准入决定、向基站提供会话密钥并处理执法访问.当时的想法是,MME 可以安置在受保护的空间中,或者至少可以防篡改（人们谈论过 TPM,但似乎没有运营商实施过）。

4G 的三个主要弱点是基站（或 MME)的本地流量仍然可以被任何可以接管它的人监控;用户设备的身份以明文形式发送到网络,或者使用相当弱的全球唯一临时身份（GUTI)进行屏蔽,就像它的前身 TMSI [918];并且归属网络将身份验证委托给服务网络[362]。 SS7 被称为 Diameter 的控制协议套件所取代,其中可以选择对消息进行加密,但由于运营商相互信任,因此很容易受到许多相同类型的攻击 [426]。它以较少的可滥用功能开始 o ,但他们因业务压力而退缩。

得益于 Google 在其 Messages 应用程序中的支持,Rich Communications Services (RCS) 在 2019 年变得广泛可用。它旨在用更丰富的聊天功能取代 SMS,包括地理定位交换、社交存在信息和 IP 语音。也称为 SMS+、+Message 或 joyn,它提供许多与 WhatsApp 相同的服务,但没有端到端加密,因为它是电信托管产品。许多初始实施是不安全的,因为电信公司没有正确配置它们 [1696]。

几十年来,在安全和情报界的要求下,电话安全一直很薄弱。然而,当事实证明在美国的俄罗斯特工破坏了使用一键通手机的 FBI 反情报特工的通信时,这一策略遭到了打击 [579]。我们还没有被告知它们是 3G 还是 4G,或者具体的漏洞是什么,但情况太糟糕了,奥巴马政府在 2016 年 12 月驱逐了三打俄罗斯外交官。他们还痴迷于在弗吉尼亚州兰利的中央情报局总部视线范围内的场所。

22.2.4 5G 及以后

第五代网络于 2019 年投入使用,有望在带宽和延迟方面比 4G 进一步显着改善。目前的主要驱动因素是带宽； 2018 年第三季度至 2019 年第三季度,移动流量增长了 68%,主要来自视频,预计到 2025 年增长将超过 25%,届时全球近一半的流量将是 5G [981]。同样,有一个不断发展的标准系列,其复杂性进一步增加。初始部署使用非独立模式 (NSA),该模式重用 4G 控制平面（甚至 4G 塔)但提高了数据速率。真正令人兴奋的是即将推出的独立模式 (SA)。 5G 使移动网络运营商不仅可以在现有频率上,而且可以在超过 20GHz 的毫米波频率上建设新容量,而且成本更低、更容易,这将意味着灯柱、公交车站等处的小型基站数量要多得多（这也将限制可用于进行身份验证握手的时间）。网络能源效率和区域流量可以提高两个数量级,而连接密度、移动性和数据速率可以提高一个数量级。可用性是重中之重； 2016年布鲁塞尔爆炸案后,警方手机因网络拥堵无法上网,不得不寻找wifi热点相互通话。

术语再次发生变化。每个微型基站现在都是一个分布式单元 (DU),由一个集中式单元 (CU) 控制,该单元也在现场,但算作核心网络的一部分。加密从您的设备到 CU,从那里使用 IPSec 保护到访问管理功能 (AMF),它取代了 MME 盒。身份验证和密钥协商协议非常相似（XRES 更名为 HXRES）。

一项实质性改进是,您的设备身份会通过其公钥加密发送到您的家庭网络,因此位置隐私将更难破解;我们被告知 IMSI 捕手将不再工作 6。假基站的被动和主动攻击似乎仍有可能,包括将设备降级为上一代技术的中间人攻击,并可用于耗尽能源关键设备的电池 [1712]。

但是整个核心网都上云了,包括所有的执法接入机制。移动网络运营商不再捍卫熟悉的技术,而是依赖于他们不了解的新技术,而且大多数人只会从最便宜的供应商那里购买。配置中的一个错误,所有内容都可读；除非像 SGX 这样的东西

6我们之前听说过 3G:窃听者只是强制回退到 2G。我们听说情报机构正在游说与大数据运营商合作打破这一局面。

可以工作,云提供商的政府很可能能够通过向他们而不是运营商提供授权来获得访问权限。在核心云网络中使用 SDN 带来了更多问题,其中最棘手的长期问题可能是 5G 是否会成为网络中立的终端网络,使网络运营商能够根据性能为每个应用程序定制产品（和价格）。同时,规范很复杂,实现仍然不稳定。随着标准的发展,一场斗争发生在想要操纵 trac 以打破网络中立性并在价值链上攀登的大数据运营商与想要端到端信任的大型移动网络运营商之间。理论上,trac 编辑将由进行编辑的公司签署,但似乎没有人知道这将如何运作。另一个是美国政府正试图阻止华为在中国境外获得大量安装;英国国家网络安全中心（GCHQ 的一部分)的 2019 年年度报告指出,2010-19 年间出现了重大的供应链风险,市场驱动因素不足以确保做出充分的反应 [1393]。2020年,随着冠状病毒大流行和香港“一国两制”的结束,反华情绪高涨,英国政府决定从2020年底开始禁止华为销售5G网络设备,并在2019年12月1日拆除现有设备。 2027 年,更长期的解决方案可能取决于第三次较量,即“bellheads”和“netheads”之间的较量:诺基亚和华为等采用电话行业方法和文化的公司与乐天等文化来自计算机行业,一旦它在云中,它将愉快地虚拟化所有可见的东西 [609]。

6G和7G呢?电信研究人员谈论前者看到无线电接入网络的演进,以支持对峰值带宽、延迟、服务质量和功耗有不同要求的多种应用程序 [1454];后者拥有数千颗微型卫星,可在整个地球表面部署 200Mbps 宽带。流媒体游戏、增强现实和（也许)自动驾驶汽车的到来将创造对超低延迟云服务的需求,而不是将我们的数据传输到由谷歌、Facebook、微软和亚马逊,我们可能会在每个城镇看到边缘云和服务器集群,甚至可能在用于容纳旧电话交换机的建筑物中。然后,正如 1990 年代后期的互联网繁荣迫使我们将 Web 服务划分为核心的活动进程,其余部分可以或多或少地静态提供服务并因此在 CDN 中本地缓存,我们将不得不托管一些活跃的 stu 也在本地。

22.2.5 一般 MNO 故障

不管使用的是哪一代无线电链路技术,MNO 都存在一些常见的故障,其根本原因在于行业的经济性和监管。一是对手机支持的身份验证功能的攻击迅速增加。除了我们在第 22.1.3 节中讨论的也适用于有线电信公司的 SS7 安全问题之外,移动世界还为我们带来了 SIM 交换、频道劫持和身份验证应用程序中的 cookie 窃取。其中许多都有安全经济学的根源:

系统中不同委托人之间的激励机制存在一些偏差。

在 3.4.1 节中,我们介绍了 SIM 交换攻击,攻击者说服受害者的电信公司在受害者的帐户上发行新的 SIM 卡。这可以为各种混乱打开大门;个人的生活可能会被接管其在线帐户的攻击者毁掉。名人是目标:2019 年 8 月,Twitter 首席执行官杰克·多尔西 (Jack Dorsey) 的帐户被接管了一个小时,并用来发送种族主义和反犹太主义的推文,导致评论员怀疑接管特朗普总统推特帐户的人是否会引发第三次世界大战 [1340].正如我在 12.7.4 节中提到的,SIM 卡交换攻击在 2020 年主要用于针对银行和比特币交易所的客户,并且通常涉及电话公司内部人员。然而,电话公司的反应充其量只是参差不齐。唯一使 SIM 卡交换变得更加困难的美国主要 MNO 是 Verizon [712]。但并非所有对策都能帮助所有用户:如果它们是可选的,那么公司可以更容易地免除不选择使用它们的客户的损失。第一个采取行动的 MNO 是 2003 年在南非的 MTN,它使用户能够指定第二张 SIM 卡来授权更换 SIM 卡;奇怪的是,这是我在 12.7.4 节中描述的 2007 年第一起 SIM 交换欺诈案中涉及的电话公司。电话公司还可以通过发送 IMSI 的哈希值作为对第二因素 SMS 的响应来帮助依赖方检测 SIM 交换;但很少有人这样做。我们在第 22.1.8 节中讨论了电话公司对其客户的敌对态度； MNO 在这方面与传统有线电话公司没有什么不同。

事实上,它们可能更糟,因为它们在大多数国家/地区的大多数客户都是预付款客户。

移动网络运营商及其供应商感到无法妥善保护客户安全的另一个例子是 SIMjacking。 2013 年,卡斯滕·诺尔 (Karsten Nohl) 警告说,许多正在使用的 SIM 很容易被劫持,因为内置的功能可以促进无线软件更新。业界反驳说这不是问题,因为 SIM 卡只能运行签名软件 [1582]。 2019 年,政府一直在使用它进行监视 [1107]。 MNO 与其客户的关系一直有些敌对,在许多国家/地区,他们被迫按需进行中间人攻击。当嫌疑人的手机浏览器访问未加密的 URL 时,MNO 会转而提供警方恶意软件。

这种网络注入攻击可以通过 IMSI-catchers 在战术上进行,但在 MNO 进行更方便。这种做法始于欠发达国家,但现在已经传播到德国 [1443]。我们将在第 26.2.7.3 节中讨论政府监控,以及自加密货币战争以来它在安全方面产生的紧张局势。

MNO 真正的根本问题是他们失去了对服务的控制。由于各种原因,他们无法与开发人员接触并推广他们可以从中获取价值的应用程序生态系统。他们最终被商品化了 移位者必须维护基础设施,但他们看到了他们过去享受被他人榨取的垄断利润。

22.3 平台安全

手机故事的第二部分是应用生态系统。这些解决了一些问题,也带来了其他问题:最严重的安全问题是平台本身是否值得信赖,或者您的手机是否可能违背您的利益。自从 2000 年代初期出现可编程电话以来,这一直是一个日益受到关注的问题。有关背景故事,请参阅我的书的第二版,其中描述了 2007 年的情况。简而言之,在 iPhone 出现之前,安全性在供应链上是分散的,涉及芯片设计师、芯片制造商、操作系统供应商、手机原始设备制造商和移动网络运营商在他们为 DRM 和控制权争吵时推卸责任。 MNO 不允许 OEM 与客户有任何关系。正如我在访问控制一章中所说,Arm 在 2004 年推出了 TrustZone;到 2007 年,每年在 Symbian 手机中检测到数百种病毒和蠕虫,供应商以访问控制、代码签名等方式做出回应。

苹果同时以多种方式改变了世界。首先,它打破了主机厂与客户有关系的禁忌。其次,它使第三方供应商更容易编写应用程序。第三,它使 App Store 成为平台战略的核心,通过分享音乐下载和软件来货币化。这需要一个半封闭的平台。设备可以通过 MNO 或 wifi 上网,并且可以根据需要在两者之间轻松切换。其效果是将权力从 MNO 转移到 Apple。谷歌于次年推出了 Android,其战略是让类似的平台尽可能开放 7,允许任何人为 Android 手机编写应用程序。他们旨在提供最低水平的信任,使生态系统得以发展。他们记得微软在 1980 年代初期通过提供更开放的平台从苹果手中夺取了大部分 PC 软件市场,使网络效应对他们有利,并希望在手机上做同样的事情,让 iPhone 成为富人的利基产品。这最终没有发生,我们现在拥有两个以多种方式融合的大型生态系统。

但苹果的货币化战略确实给了它更好的动力来维护其平台,iPhone 通常至少打补丁五年,而安卓产品打补丁三年,而且通常更短。

iPhone 和 Android 都采用了我在访问控制一章中描述的安全架构;这两种方法都旨在将应用程序彼此分开,并防止它们破坏平台本身。主处理器并不是全部,因为手机包含许多其他 CPU,并且在 DSP 中也发现了漏洞,这些漏洞可能会影响来自多个 OEM 的手机 [1212]。我还在侧通道一章中讨论了一个糟糕的应用程序如何使用手机的加速度计和陀螺仪来计算输入另一个应用程序的密码或 PIN,即使被拒绝直接访问屏幕也是如此。丰富的传感器和广泛的应用程序相结合,使得平台级别的安全和隐私服务变得相当复杂。随着时间的推移,Android 和 iPhone 的安全机制都得到了完善,添加了更多控件来阻止或减轻更明目张胆的滥用行为。然而,最好将它们理解为一个生态系统,而不是

7根据监管机构的坚持,控制设备的基带软件
射频行为必须被锁定

保护选项列表。

这个生态系统确实是巨大的。到 2019 年,全球 56% 的互联网访问来自移动设备,但美国为 63%,印度为 80% [1252]。它至少包括在这两个移动设备系列本身上运行的应用程序,以及它们所依赖的后端服务。边界很难界定。我们可能必须包括应用程序开发人员与其产品捆绑在一起的广告生态系统。我们是否包括移动设备从浏览器应用程序访问的网络服务?我们是否包括语音电话,既然它正在迁移到 WhatsApp、Skype 和 Signal 等应用程序?运行移动操作系统和应用程序的其他设备（从手表到汽车)又如何呢?从应用系列开始可能是最简单的。

22.3.1 安卓应用生态系统

Android 是部署最广泛的终端用户操作系统,不仅存在于手机中,还存在于平板电脑、手表、电视、汽车和其他设备中 月活跃设备总数超过 20 亿台。它的平台安全模型由 Ren´e Mayrhofer 和 Google 的同事在 [1252] 中描述,在第 6.2.8 节中我讨论了技术架构。行动基于三方同意 :用户、开发者和谷歌都应该同意。其实现方式是,Android 不是像在传统的 *nix 系统中那样为最终用户提供用户 ID,而是使用单独的用户 ID 运行每个应用程序;私有应用程序目录中的数据由应用程序控制,而共享存储中的数据由最终用户控制,并且有强制访问控制机制以确保关键系统数据保持在平台的控制之下,除非它被root。只要这种情况没有发生,用户就不会被诱骗让不良应用程序访问或覆盖其他应用程序的数据。威胁模型包括从物理攻击和窃听到利用操作系统、库和其他应用程序中的漏洞的所有内容;假设用户会被诱骗安装恶意应用程序 [1252]。通过 Google 的 Play 商店销售的应用程序会进行恶意软件扫描（尽管扫描并不完美）。

然而,谷歌从应用程序销售中抽取 30% 的收入,并拒绝托管成人应用程序。这促使许多付费和成人应用程序供应商使用不太安全的分销渠道,例如 OEM 交易、第三方商店和他们自己的网站 [1823]。自 2014 年以来,谷歌已经提供在首次运行时上传非 Play 商店应用程序进行扫描的服务,但恶意应用程序的风险始终存在。更多的应用程序多少有些掠夺性,即使它们是由硬件供应商、MNO 和安全公司等表面上受人尊敬的企业分发的。可悲的是,用户数据已成为一种主要商品。考虑到大多数应用程序都是免费的,而且生态系统与其他任何东西一样,都是由广告收入驱动的,因此几乎没有其他期望。一个主要后果是 Android 不支持最关键的隐私权限 允许用户控制应用程序的互联网访问。 （黑莓允许用户拒绝互联网访问。)这让广告公司很高兴,否则许多用户会在安装手电筒/游戏/指南针应用程序时关闭 互联网访问。如果这让您不满意,您可以获得伪装成 VPN 的防火墙应用程序,并可以阻止其他应用程序访问互联网。但当然,大多数用户都会默认,让广告生态系统收获几乎所有的东西。

22.3.1.1 应用市场和开发商

应用程序市场减轻了一些安全问题,同时放大了其他问题。由于 Android 生态系统是开放的,任何人都可以成为开发者并通过 Play 商店分发他们编写的软件。这为新手开发者提供了一个巨大的市场,他们可以毫不费力地运行简单的应用程序。您必须将框架与 Android SDK 一起使用这一事实以可能有用的方式限制了开发人员。尽管碎片化极大地阻碍了操作系统的更新过程,但如果您使用推送更新的应用商店,则应用更新很容易。

然而,开发人员很快就会遇到技术和业务的复杂性。一些简单的应用程序只不过是用于在线后端的定制浏览器;其他人以新的方式使用手机的单一功能,例如手电筒应用程序。但是这个特征有多统一呢?您需要支持多少个 Android 版本?您需要在数百种不同的手机上进行测试吗?现在有测试框架可以提供帮助,但如果您的应用程序使用许多现代手机上丰富的硬件功能,那么碎片化就是一个真正的问题。例如,开发冠状病毒接触者追踪应用程序的人一直在努力应对不同手机之间蓝牙性能的差异。另一个例子是开发人员想要保护真正敏感的信息,例如银行应用程序中的关键材料。 Arm 希望开发人员能够使用 TrustZone,但由于 OEM、手机和软件版本之间的差异,这变得非常困难,以至于大多数人转而采用混淆方法。然后机器人提供 KeyStore,它允许应用程序将其密钥存储在 TrustZone 或安全元件或其他可用的加密处理器中,并阻止其他应用程序使用它们。一些开发人员更喜欢混淆,希望阻止恶意软件扎根于手机,从而伪装成应用程序;正如我在第 12.7.4 节中提到的,一些银行监管机构坚持这一点。

业务复杂性可能来自应用程序本身,或来自生态系统的基础经济学:平台公司、设备供应商、应用程序开发人员、应用程序发布者(添加各种广告的人)、广告网络、工具制造商和最终用户都有不同的 er奖励。付费应用、允许应用内购买的应用和免费应用有不同的规则。识别用户的规则很复杂:需要用户同意才能使用某些 UID(IMEI、IMSI、电话号码和广告 ID),但不需要用户同意,例如 MAC 地址和硬件指纹。

22.3.1.2 糟糕的 Android 实现

随着 Android 在 2010 年左右的普及,第一个系统性安全问题变得显而易见,这是许多获得许可的 OEM 的工程工作质量低下。一个例子是恢复出厂设置。二手手机交易兴旺,富裕的用户购买最新型号,而他们的旧手机最终被出售。您可能会认为,当您在手机上恢复出厂设置时,会清除您的所有个人信息,不仅会从共享存储中清除,还会从应用程序存储中清除。但是很难做到这一点,因为与典型手机上闪存的组织方式有关;可能有嵌入式多媒体卡 (eMMC) 和虚拟 SD 卡,它们具有自己的磨损均衡机制。如果 OEM 的工程师不

不厌其烦地实施安全删除,那么很常见的结果是,购买二手手机的人可以检索 Google 主 cookie 并访问与手机关联的 Gmail 帐户 [1757]。

几年来,我购买了谷歌自有品牌的 Nexus 和 Pixel 手机,并且在使用后从未出售过,但许多人通过合同获得手机补贴并锁定到移动网络运营商,然后在二手市场上出售它们 通常是在欠发达国家. (谨慎的做法是假定最不发达国家的 Android 手机已被 root 并被当地经销商安装了远程访问木马。)

这些质量问题扩展到 TrustZone 及其可信执行环境 (TEE),由各种芯片组供应商实施。例如,Qualcomm 的 TEE 系统允许受信任的应用程序 (TA) 映射到主机操作系统的内存区域,因此任何不安全的 TA 都可以让对手获得设备的根权限。

其他问题允许对其他四家供应商的 TEE 进行攻击:可信环境中使用的软件安全机制落后于现有技术水平数年,ASLR 缺失或弱,TCB 过大,调试通道信息泄漏,没有执行预防、多个侧通道以及没有好的方法来撤销恶意或易受攻击的 TA 其中有很多。有关这些问题的调查,请参阅 David Cerdeira 及其同事 [403]。

然而,Android 实施的最大安全问题是售后支持不力。许多原始设备制造商仅支持当前正在积极销售的版本;他们不愿意花费工程师时间将修复程序向后移植到旧版本。 2015 年的一项调查显示,87% 的活跃设备不安全(2011-15 年的平均值),因为它们运行的操作系统版本包含已知漏洞。在许多情况下,OEM 根本没有提供可用的修复程序 [1880]。到 2011 年,这已被谷歌确定为一个问题;如果原始设备制造商承诺修补他们的系统,该公司会向他们提供降价组件,但这几乎没有吸引力。谷歌现在为供应商和应用程序提供认证计划,但问题不仅仅是 OEM 工程工作。如果在 OpenSSL 或 Bouncy Castle 密码库中发现漏洞,则此修复程序必须传播到 Linux,然后传播到 Android,传播到每个 OEM,然后在许多情况下传播到每个移动网络运营商 因为 MNO 控制更新对于锁定到网络的电话。这些步骤中的每一个都可能需要几个月的时间,并且出于商业原因可以忽略每个步骤 [1880]。这引发了围绕协调披露的棘手问题,我们将在第 27.5.7.2 节中讨论,以及监管,我们将在本书的最后一章中讨论。

22.3.1.3 权限

正如我们在访问控制一章中指出的那样,许可从一开始就是一个棘手的问题。在 Android 的早期版本中,应用程序的清单指定了它所要求的访问权限,用户必须在安装时批准所有这些权限才能运行它。这导致了广泛的滥用,因为大多数用户只需单击批准即可完成安装,并且许多实用程序成为收集和转售您的地址簿、浏览器历史记录和其他个人数据的机器。早在 2012 年,研究表明只有 17% 的用户在安装过程中注意,并且只有 3% 的人能够回答

关于正在发生的事情的基本问题 [676]。 2015 年,Android 6 转向了 Apple 模型,即在首次使用时批准访问此类资源。事实上,对更危险权限的逐步限制比其他任何因素都更能推动平台的发展。 Android 6 还使细粒度位置访问成为一个单独的权限； Android 7 限制应用程序访问其他应用程序的元数据； Android 8 随机化 MAC 地址并强制使用单个广告 ID 进行货币化； Android 9 在应用程序处于后台模式时限制对传感器的访问,并限制对电话和通话记录的访问;和 Android 10 在后台模式下限制位置访问。

谷歌现在提供几十种权限,开发人员在向其他应用程序提供服务时始终能够定义自定义权限;数以千计的这些是由硬件供应商、移动网络运营商、安全公司和互联网浏览器定义的 [741]。这些进一步分化了生态系统,使用户（和开发人员)更难理解。

Yasemin Acar 及其同事对同意问题的分析将其分解为用户和开发人员对权限的理解和对权限的关注 [10]。双方都存在可用性和激励失败。很明显为什么掠夺性手电筒应用程序想要访问我的地址簿;许多失败更加微妙。开发人员只是想让 stu 工作以便他们可以发布它,而用户只是试图访问某些服务或其他服务。开发人员的可用性是错误的重要来源;我们已经在其他地方（例如在第 5.5 节中)注意到了这一点,但它在应用生态系统中显得更加突出,因为开发人员必须驱动应用程序框架 API 才能完成有用的工作。出于无知或困惑,有相当一部分开发人员会请求比他们需要更多的权限,这甚至适用于开发人员应该更了解的系统应用程序。 Google 未能实施故障安全默认设置； API 令人困惑且文档不足。这促使开发人员通过 stackexchange 等论坛复制彼此的代码,其程度甚至超过了传统开发8。

22.3.1.4 安卓恶意软件

由于 Android 是一个开放平台,任何人都可以为其编写应用程序,因此它吸引了大量有害软件。正如我们在 22.1.4 节中提到的,收费电话恶意软件于 2006 年与 Red Browser 蠕虫一起出现； Android 的到来使移动恶意软件从小众活动变成了主流问题。这里的定义很难,因为许多应用程序至少以不同的方式对某些人有害;在这里,我重点关注那些暗中损害安装用户利益的应用程序。我将在后面的第 22.3.1.6 节中讨论 OEM 和 MNO 安装的不良程序。

恶意软件可以是批量的或有针对性的,它可以来自私营部门的犯罪分子或国家行为者。按数量计算,其中大部分是散装私营部门的品种,其中大部分来自常规分销渠道。除了 Play Store 中的数百万个应用程序,替代市场也被广泛使用,特别是在 Play Store 受到审查的中国和伊朗等国家。这

8它也促使 Acar 和她的同事从开发人员的角度 [11] 来审视可用性,创建了一个重要的安全研究新领域,我在访问控制一章末尾的研究问题部分提到了这一点。

最大的单一恶意软件来源是 Play 商店,其中极少数应用程序有时是有害的,而一些替代市场有时会删除大部分有害应用程序。应用程序可能天生有害,或者它们所依赖的库可能会变坏,或者坏人可能会收购失败的应用程序公司,就像他们抢购前银行的域名一样。最近曝光的最大犯罪团伙之一通过购买 Android 应用程序并使用他们的用户数据来训练机器人然后点击广告 [1738],从而进行了数亿美元的广告欺诈;此类骗局也利用其他类型的恶意软件。测量问题非常重要,因为 60 多家反病毒公司使用不同的标准为应用程序贴上标签,并将它们归入不同的系列。任何时候都有数百个家庭在活动。

Guillermo Suarez-Tanguil 和 Gianluca Stringhini 在 2018 年进行的一项调查分析了 2010-17 年间收集的 120 万个样本,并将它们归类为超过一千个科 [1842]。自 2012 年以来,其中大部分都涉及重新打包,恶意软件开发人员使用合法应用程序（载体)并添加有害代码（附加程序）。这是通过将许多良性载体与同一恶意骑手的变体重新包装来实现工业化的。骑手可能会尝试对手机进行 root 以进行持久访问,并投放可以在命令和控制服务器的指导下赚钱的远程访问木马 (RAT),就像普通的 PC 恶意软件一样。货币化策略已经演变； 2010 年的重点是拨打高价电话,但到 2018 年,它已经转移到广告欺诈和个人信息泄露上。绝大多数骑手使用加密等混淆技巧,而只有四分之一的良性应用程序这样做（Facebook 的应用程序使用混淆来防止用户数据和密钥被恶意软件窃取,特别是欠发达国家的 RAT）。 Riders 大多是本机代码,而不是 Java（或 Kotlin,后者在 2019 年取代它成为首选的官方 Android 语言）。

银行木马在针对性更强的私营部门恶意软件中脱颖而出。一种常见的方法是覆盖攻击,其中恶意软件诱使用户允许其使用 Android 辅助功能服务,这使其能够在（例如)您的银行应用程序上构建覆盖,以便它可以在控制下捕获屏幕和输入数据远程命令服务器 [396]。一段时间以来,Android 恶意软件一直在窃取银行短信,而谷歌通过只允许批准的应用程序读取短信的权限来进行反击； 2020 年的最新发展是 Cerberus 银行恶意软件现在也可以窃取 Google 身份验证器 cookie [431]。

各州已经在情报和执法任务中使用了有针对性的恶意软件,到 2012 年,Gamma 等供应商已经生产了在多个司法管辖区发现的其产品的手机版本 [1231]。此类恶意软件还会寻求根访问权限,但会植入间谍软件。最近大量恶意软件部署的例子来自土耳其,土耳其在 2018 年使用 Turk Telekom 网络上的中间人设备部署间谍软件 [1218],还有中国为维吾尔人的手机设置网站陷阱 [393]。批量国家行为者恶意软件可能包括在某些司法管辖区强制篡改应用程序版本； .Skype 从 2005 年开始在中国只能通过本地分销商 Tom Online 使用，该公司将其重新包装以扫描中国审查员禁止的词语。

微软收购 Skype 后,他们从 2013 年开始收回控制权,但该应用从 2017 年起被禁止进入中国的应用商店 [1347]。

存在技术滥用,其中应用程序破坏了权限框架,同时又没有对手机进行 root 操作。 Joel Reardon 及其同事在一个检测过的虚拟环境中运行了 88,000 个 Android 应用程序,以寻找滥用侧信道的应用程序 [1588]。他们发现中国的两家大公司,百度和 Salmonads,使用 SD 卡作为隐蔽渠道,这样可以读取手机 IMEI 的广告可以为那些不能读取的广告存储它。他们还发现 42 个应用程序使用 ioctl 系统调用在不应该获取 IMEI 的时候获取了 IMEI,超过 12,000 个应用程序使用代码来获取 IMEI。

22.3.1.5 广告和第三方服务

手机应用程序通常会结合第三方服务来支持广告、社交网络集成和分析,用于从崩溃报告到 A/B 测试等一系列目的。此类服务甚至可以在未经用户同意的情况下跨多个应用程序跟踪用户。 Cam Scanner 就是一个可能出错的例子,该应用程序被超过 1 亿人下载,用于扫描和管理文档。在某个时候,该应用程序进行了更新,添加了一个包含恶意模块的新广告网络。负面评论促使反病毒研究人员进行调查,结果发现该模块正在向人们的手机投放特洛伊木马程序 [796]。

第三方服务是生态系统中相当不透明的部分,因为它们对用户不直接可见。 Abbas Razaghpanah 及其同事使用 VPN 应用程序进行的一项调查揭示了一些亮点,该应用程序被 11,000 名志愿者用来监控进出他们手机的流量 [1586]。他们映射了 2,000 多个广告和跟踪服务 (ATS),其中包括数百个以前没有报道过的服务,并发现有相当一部分 (39%) 进行了跨设备跟踪;前 20 名中的 17 名在网络和应用程序生态系统中都有存在。前十名中的八名在其隐私政策中保留与其他组织共享数据的权利。其中最大的是 Alphabet 和 Facebook,但其整个业务由 ATS 组成的公司,如 Chart boost、Vungle 和 Adjust,占有很大份额,但用户相对不为人知。应用程序开发人员经常同时使用多个此类服务。付费应用程序的跟踪器最少,免费应用程序的跟踪器更多,允许应用程序内购买的免费应用程序（通常是高级服务)往往最多。

Yasemin Acar 及其同事讨论了相互信任问题 [10]。应用程序开发人员必须信任广告网络,因为它们在应用程序沙箱中执行并继承其权限。广告库以各种方式利用应用程序,例如从网络服务加载不安全的代码和窃取用户的私人信息;应用程序开发人员通过伪造的点击事件从网络中窃取资金来回报赞美,就像恶意软件开发人员一样。 （边界有点模糊,就像以前在 PC 世界中一样;堆栈的几乎每一层都有掠夺性行为。）

有很多儿童应用程序未经父母同意收集个人数据的例子,违反了美国儿童在线隐私保护法

法案 (COPPA):Irwin Reyes 及其同事扫描了 5,855 个最流行的免费儿童应用程序,发现其中大多数可能因为使用第三方 SDK 的方式而违反了 COPPA;这些通常使开发人员能够禁用第三方跟踪和广告,但大多数开发人员不会这样做

打扰。更糟糕的是,19% 的应用程序使用禁止在儿童应用程序中使用的 SDK 收集个人身份信息 [1599]。这项研究导致州检察长采取法律行动,这可能会鼓励应用程序开发人员更认真地对待法律。还有其他违反欧盟 GDPR 及其电子隐私指令的做法,但欧盟监管机构似乎不愿参与,因为 ATS 行业绝大多数位于美国,相当于大量无形出口。即使从美国当局的角度来看,大多数 ATS 专家甚至没有 COPPA 政策,将法规遵从性留给了他们的客户。

大多数人都希望,如果他们为应用程序付费,他们将获得更多隐私。但鉴于开发人员依赖第三方服务进行分析和广告,这需要付出很多努力,而许多开发人员不愿意这样做。 Catherine Han 及其同事比较了同一应用程序的免费和付费版本,发现三分之一的付费版本在数据收集方面同样具有掠夺性;另外六分之一至少收集了一些相同的数据;四分之三的人使用相同的权限;几乎所有人都有相同的安全策略。在查看为家庭设计的付费/免费应用程序对时,她发现大多数付费应用程序都以与免费版本相同的方式违反了 COPPA [859]。

22.3.1.6 预装应用

Julien Gamba 及其同事研究了全球 200 多家供应商分发的固件 [741]。分销通常反映了手机 OEM 和 MNO 之间的合作关系,以及各种关联的开发商、广告网络和分销商。它们可能难以控制;已经有多个恶意软件进入的案例,以及出于商业或监管原因进行大规模数据收集的软件。一些手机还具有可能被恶意应用程序利用的诊断或支持模式。大多数预装应用程序在 Play 商店中不可用,因此似乎不属于传统框架。有些来自像 Facebook 和 AccuWeather 这样的公司,这些公司以积极收集个人数据而闻名;其中许多不是这些公司应用程序的公开版本;许多预装的应用程序使用移动分析或有针对性的广告库。更重要的是,74% 的非公开应用程序似乎没有得到更新,41% 的应用程序在 5 年或更长时间内未打补丁 [741]。许多具有敏感的自定义权限,以便执行诸如企业客户的移动设备管理、呼叫阻止和 VPN 服务等任务。行为分析表明,很大一部分预装应用程序可以访问和传播用户和设备标识符、配置和当前位置。此类应用程序联系最多的域是 Alphabet、Facebook、亚马逊、微软和 Adobe。一些预装的应用程序,特别是在较便宜的手机中,在系统分区中有用户无法轻易删除的组件,这些组件会提供烦人的广告,甚至充当特洛伊木马程序的加载程序 [1109]。

22.3.2 苹果应用生态

Apple 从一开始就在安全可用性方面处于领先地位,早在 Android 之前就提供了细粒度的访问控制,但其生态系统一直更加封闭。

当 Mac 与 PC 竞争时,它是一个硬件平台,可以对抗许多 OEM。同样的模式也出现在 iPod 上,Apple 要求 30% 的音乐销售额,并且在 Apple 推出 iPhone 时继续如此。商业模式与游戏机非常相似。 Apple 是唯一的硬件供应商,需要 30% 的软件收入,以及 30% 的在线商品和服务应用内购买。现在 Apple 在发达国家拥有一半的市场（以及四分之三的青少年）,这正在成为一个反垄断问题。每个开发者都有恐怖故事,尽管亚马逊在 2020 年 4 月获准在苹果设备上销售电影而不给苹果提成 [836],但这恰恰凸显了苹果规则的任意性。为什么像 match.com 这样的约会网站必须将销售额的 30% 交给它,而 Uber 却不需要?

Apple 将约会视为一种数字商品,但 Uber 试图通过声称它是相同的,只是司机和乘客之间的婚介服务来避免出租车监管。这些规定似乎对小公司的打击尤其严重,如果人们通过 iPhone 应用程序预订,则对因大流行而上网的音乐家、健身教练和瑜伽老师等人征收“苹果税”。

所有这一切导致 Epic Games 在美国提起反垄断诉讼,以及欧盟的竞争政策调查 [888]。

Apple 还利用其对硬件和操作系统的控制来实施权利管理机制,以保护其售后市场收入;不允许竞争的应用程序商店。该公司对开发商进行尽职调查,要求他们每年为许可证支付 99 美元。它的应用程序审查过程比谷歌的要严格得多:有广泛的自动安全测试,然后是人工审查,以确保应用程序在支付、内容和滥用等问题上遵守苹果政策。为了支持这一点,提交到 App Store 的 iOS 应用程序只允许使用公开记录的 API [1812]。因此,学术研究人员对 iOS 生态系统的研究要少得多,但仍然可以说一些事情。

对恶意软件的整体保护是所有大众市场系统中最好的,iOS 的零日远程攻击交易价值数百万美元,并在大规模使用后立即进行修补。事实上,当我们自己大学的金融部门就如何保护真正的高价值交易免受网络钓鱼征求意见时,我的建议很简单:购买一台 iPad,在其上运行银行的验证器应用程序以释放付款,仅将其用于付款,并在其余时间妥善保管。

然而,这种保护并不完全是防弹的,各种参与者都有
找到解决方法。

首先,爱好者和其他“越狱”Apple 设备的历史由来已久,首先是那些反对 DRM 的人,或者想在不向 Apple 支付 99 美元税的情况下加载自己的应用程序的人,就像他们使用 Android 一样。随着越狱的出现,Apple 对其进行了修补;所以至少该公司有动力更新其设备,而不是像典型的 Android OEM 那样在售后放弃它们。有时打补丁是不可能的,比如当漏洞是针对设备的引导 ROM 时;例如,2019 年 Checkra1n 越狱将解放 2017 年之前销售的大多数设备 [798],取证行业使用 Checkm8 越狱,它利用了从 4S 到 X 的所有 iPhone 的引导 ROM [798];正如我在第 26.5.1 节中描述的那样,这在出售给世界警察部队的法医“亭”中被广泛使用。虽然 ROM 漏洞利用不能

在 5s 之后的设备上破解用户 PIN,由于安全元素,他们可以访问那些在首次解锁后可访问的用户数据,如第 6.2.7 节所述。还有一个运营商解锁市场,您还可以假设手机由攻击者实际保管。

可以远程利用 iOS 的攻击更有价值,因为国家行为者愿意为此支付数百万美元。我们在第 2.2.4 节中描述了阿联酋如何使用这种工具来针对持不同政见者,以及沙特阿拉伯如何使用这种工具来对付 Je Bezos,他们厌恶他的报纸《华盛顿邮报》;沙特人还入侵了他们的地区竞争对手卡塔尔国王。网络犯罪分子也这样做:2019 年,谷歌的零计划揭示了 iOS 漏洞被用于感染 iPhone [204]。 Apple 总是快速修补此类漏洞,因此您的数百万只能让您访问少数目标。如果有人可能会花费一百万美元来破坏您的手机,您最好拥有几部并且不要告诉您的敌人您的私人手机号码包含您真正关心的数据9

其次,Apple 出售大公司的“企业证书”,让 iOS 开发人员绕过应用程序审查流程。这导致了滥用和口水战,Facebook 的企业证书被暂停,直到他们的应用停止违反应用商店政策;谷歌在 iPhone 上的应用程序也有类似的经历,突然大量色情、赌博和间谍软件应用程序被曝光。他们一直在滥用企业证书并隐藏在应用程序商店中 [1697]。许多不良行为者通过伪装成来自欠发达国家 MNO 的帮助热线应用程序获得了企业证书 [1170]。

第三,Apple 与 Android 类似,它不允许用户阻止应用程序访问互联网。所以我们也找到了适用于 iOS 的防火墙应用程序,但这是 iOS 隐私机制妨碍隐私的一种方式。一个应用程序甚至无法看到另一个应用程序,更不用说阻止它了,因此 iPhone 上的所有 iOS 防火墙只能阻止对广告服务器的访问。

尽管恶意软件问题没有 Android 严重,但同样的市场力量仍然存在,因此广告滥用仍然时有发生。许多流行的应用程序(包括 Grindr 和 OkCupid 等约会应用程序)与广告商共享大量数据,并且仍然允许在 Apple 生态系统中使用 [1762]。这同样适用于您可能希望更加注重隐私的应用程序,例如 VPN 和广告拦截器 隐私利用通过嵌入式广告网络进入,如 Android 生态系统 [1739]。在一个案例中,一个广告 SDK 让其作者窃取了使用它并安装在 3 亿部 iPhone 上的 1,200 个应用程序的点击次数;它的代码具有隐蔽功能,可能帮助它通过了应用程序审查过程 [1314]。尽管在 Apple App Store 中付费的应用程序比在 Google Play 商店中付费的应用程序更多(6% 而不是 4.4%),而且人们认为不显示应用程序的付费应用程序不会跟踪您,但这样的预期可能是乐观的– 在两个生态系统中。在第 22.3.1.5 节中,我提到了一项研究,该研究表明付费版本的 Android 应用程序通常仍会跟踪您。人们可能会期望 Apple 得到类似的结果,但 iPhone 是一个更难进行研究的平台。

9我认识一位大亨,他每天都会借用不同员工的手机,并让总机转接他的电话。如果那是你的策略,你最好假设它偶尔可以兼作监听设备并让你的 PA 为你携带它。面对国家对手,保持热电话和冷电话之间的分离并不简单:请参阅第 2.2.1.10 节中描述的同行系统。

苹果和谷歌一样,一直在逐步收紧应用程序所需的权限。例如,iOS13 将地理数据从安装时的“允许”细化为“允许一次”和“使用应用程序时允许”,并且还减少了使用 wifi 和蓝牙来确定位置 引起了开发人员的同类投诉 [434]。从 2020 年 9 月开始,iOS14 会将广告商身份识别 (IDFA) 从选择退出转变为选择加入,从根本上杀死它,并破坏广告商跟踪广告活动有效性的能力 据说是为了隐私,但它看起来也以牺牲谷歌、Facebook 和第三方广告服务公司为代价来推广 Apple 的广告业务 [1073]。

这两家商店存在一些共同的政治问题,例如他们都允许沙特阿拉伯男性使用的应用程序来控制他们的妻子、女儿和仆人的行动,正如我在第 2.5.4 节中讨论的那样。有时,它们确实会出现分歧。 Apple 在删除“不良”应用程序方面比 Google 更积极,尽管这有时会给他们带来负面影响。在 2019 年香港抗议活动期间,Apple 禁止了示威者用来躲避警察的众包抗议安全应用程序,声称“您的应用程序包含不合法的内容 或促进、启用和鼓励一项活动……具体来说,该应用程序允许用户逃避执法”,而谷歌则保留了 Android 版本 [1253]。

冠状病毒接触者追踪引发了另一场政治争议。 2020 年 2 月,新加坡政府宣布了一款应用程序,该应用程序将使用蓝牙记录彼此靠近的手机,这样当有人病毒检测呈阳性时,公共卫生官员可以自动追踪可能的接触者,而不仅仅是询问患者他们是谁过去一周见过面。结果证明效果不是很好,因为蓝牙不是一种很好的测距技术。如果您将音量设置为确保能看到 2 米外的人,那么您会在 10 米外看到相当多的人 这大大增加了接触者追踪器必须处理的误报数量。更重要的是,如果运行该应用程序的人口比例为 p,则患者及其联系人都在运行该应用程序的概率为p2 ,漏报率为1p2;对于新加坡,p 为 12%,因此错过了超过 98% 的联系人。到 4 月份报道时,包括英国、法国、德国、拉脱维亚和澳大利亚在内的许多其他国家/地区也已开始开发接触者追踪应用程序。他们发现对蓝牙使用的限制使得此类应用程序很难为 Android 手机编写,而对于 iPhone 来说基本上是不可能的 [437]。

当他们要求更好地访问时,谷歌和苹果拒绝了,理由是如果所有应用程序都可以进行蓝牙联系追踪,他们的客户将面临隐私风险。谷歌和苹果提供了一个用于匿名接触者追踪的 API,但从流行病学家的角度来看,这甚至没有用 [1799]。这导致了对谷歌,尤其是苹果公司的批评,因为它做出的政策决定是民选政客的工作[955]。德国改用谷歌/苹果 API,但开始要求酒吧和餐馆保留客户联系方式的列表,这样如果一位客户生病,就可以使用传统方法追踪坐在附近的人。

22.3.3 交叉问题

这两个生态系统的融合导致了越来越多的交叉问题。这些不仅适用于手机,也适用于其他物联网设备,其中许多属于 iOS 生态系统（例如 Apple 手表)或 Android 生态系统,包括恒温器、门铃摄像头、楼宇传感器和 Google Home 智能扬声器。另一个值得注意的生态系统可能是亚马逊 Alexa 的生态系统,它启动了智能扬声器产品类别（这一类别增长非常迅速,用了 4 年时间才被一半的美国人口采用,而不是智能手机需要 8 年）。其中许多设备还旨在支持应用程序生态系统,尽管数量和用途因产品而异。

除了我们在第 22.2.5 节中讨论的 MNO 和我们在上一节中讨论的贪婪的广告生态系统引起的问题之外,一个主要问题是设计不佳的应用程序。

很简单,当数十亿人将他们的财务生活、社交生活甚至性生活委托给应用程序时,编写糟糕的应用程序可能会造成真正的伤害。本书的许多其他章节都讨论了具体的应用问题。在这里,一个例子可能会成功地将事情放在上下文中。它说明了一个许多应用程序开发人员根本没有考虑清楚的问题 撤销。事实上,在协助设计支付应用程序时,我们花了大约一半的安全工程时间来详细研究我们如何应对被盗手机:当来自不同 erent 的警报传入时如何快速阻止支付利益相关者,当犯罪受害人第二天走进一家商店并购买了一部新手机时会发生什么,无论您是依靠手机店对他们进行身份验证还是让他们致电银行承包商,您将如何与手机原始设备制造商打交道他们有自己的备份和恢复服务 一大堆令人头脑麻木的细节。这就是真正的工程归结为:与您的供应链合作,并通过客户体验和可能的滥用案例进行思考。

FordPass 是我的一个例子,可以说明当您注意力不集中时可能发生的情况,该应用程序使您能够控制租来的汽车,以便您可以跟踪它、锁定和解锁它以及启动引擎 甚至在您租用汽车几个月后将其归还给租赁地 [794]。还有更多案例,但这足以说明设计不当的应用程序可能会暴露其他系统,包括安全关键系统。

来自编写不当的应用程序的威胁涵盖了机密性、完整性和可用性的整个范围。依赖于不再维护的应用程序的商品的后果是,欧盟于 2019 年通过了商品销售指令,要求具有数字组件的商品供应商将这些组件维护至少两年,如果合理的话,可以更长时间客户的期望。从 2022 年 1 月起,与汽车或洗衣机等耐用品一起提供的手机应用程序必须在最后一件产品离开展厅后维护十年。我们将在本书的最后一章进一步讨论可持续性。

22.4 小结

电话安全是一个引人入胜的案例研究。一个世纪以来,人们一直在欺骗电话公司,而自从放松管制以来,电话公司一直在大力回敬。首先,系统根本没有真正受到保护,很容易逃避收费和重定向呼叫。事实证明,为防止这种情况而采用的机制(带外信号)是不够的,因为系统复杂性的迅速增加会带来更多的漏洞。这些范围从通过 PBX 等终端设备的不良设计和管理对用户进行社会工程攻击到利用各种难以预测的功能交互。主要的颠覆性力量是收费服务的发展,使人们能够窃取真钱。

在移动领域,保护 GSM 及其第三代、第四代和第五代继任者的尝试是一个有趣的案例研究。他们的工程师专注于通信安全威胁而不是计算机安全威胁,并且以牺牲客户利益为代价来维护电话公司的利益。

他们的努力并非完全白费,而是导致了一个极其复杂的全球生态系统,该生态系统已成为重大政治斗争的主题,尤其是在 5G 基础设施的控制方面。

2020 年的主导因素是移动应用生态系统。 Android 生态系统吸引了数十万开发人员,从像 Uber 这样的公司,它们已经将应用程序构建到主要的国际业务中,通过许多成熟企业提供的应用程序和大量专业工具,再到大量的犯罪边缘。 Apple 生态系统受到更多监管,但在许多方面相似。这两个生态系统中许多看似无害的应用程序可能会以有趣的方式被滥用,它们使用的广告网络对隐私构成普遍威胁。移动应用程序生态系统、笔记本电脑等更传统平台上的应用程序以及手表和汽车等设备上的应用程序以各种方式融合和重叠,但就它们仍然不同而言,移动平台比笔记本电脑更强大地保护应用程序免受彼此影响做,平台运营商在生态系统层面做出重大安全努力 。事实上,由于大多数 Android 手机都没有安装最新补丁,因此不安全,因此繁重的工作不是在技术平台安全级别上完成的,而是在生态系统级别上完成的。

研究问题

通信、移动性、平台和应用程序之间的交互继续为有趣的研究和代价高昂的工程错误提供沃土。在过去的十年中,我们在手机应用程序生态系统中探索了很多问题,主要是在其中大多数问题发生的 Android 部分。移动性现在正在扩展到各种其他设备,从您的手表到您的汽车,并且围绕应用程序生态系统的许多问题都出现在智能扬声器和其他家用设备上。鉴于这些新兴生态系统的庞大规模,我们将需要创新的方法来自动寻找威胁和漏洞。一种方法是构建蜜罐并寻找攻击轨迹;更前卫的防御可能是分析

用于控制物联网设备并从中推断漏洞的配套应用程序 [1978]。

进一步阅读

关于世界电话系统的信息分散在大量标准文档中,这些文档可能相当繁重,而应用程序平台至少有官方指南、白皮书和开发者社区。跟上最新的漏洞利用是关注安全博客和技术媒体的问题。

我在相关章节中引用了一些针对特定子问题的很好的调查,但我不知道有任何关于整个电话安全场景的好书或调查论文。也许这是不可避免的;现在越来越多的人通过移动设备上网,而不是从笔记本电脑或台式机上网,移动安全以某种方式触及本书的大部分主题。