第19话

侧通道

两支军队的嗡嗡声静静地响起， 固定的哨兵几乎接
收到彼此守望的秘密耳语;火回应火,通过它们淡淡的
火焰,每场战斗都看到了对方棕褐色的脸。

– 威廉·莎士比亚,亨利五世,第四幕

优化包括采用一些有用的东西,然后用几乎可以用但更便宜的东西代替它。

罗杰·李约瑟

19.1 简介

计算机和电话等电子设备会以各种方式泄露信息。侧信道是指信息通过某种并非为通信而设计或旨在用于通信的介质意外泄漏的地方;隐蔽通道是故意泄漏的地方。侧信道攻击无处不在,其中3-4 次造成了数十亿美元的损失。

1. 首先,存在传导或辐射的电磁信号,它们可以在本地和偶尔在更远的范围内损害信息。从1960 年代开始,这些“暴风雨”袭击导致北约各国政府每年花费数十亿美元用于防护设备。冷战结束后,人们开始意识到通常没有人在倾听。

2. 其次,侧通道会在单个设备上的任务之间或紧密耦合的设备之间泄漏数据;这些可以利用功率和时序信息,也可以争夺共享系统资源。 1990 年代后期差分功率分析的发现使智能卡在银行和其他地方的部署推迟了 2-3 年,因为人们意识到当时销售的所有卡都容易受到攻击。

3. 第三起价值数十亿美元的事件始于 2018 年 1 月,宣布了“幽灵”和“熔断”攻击,这些攻击利用推测执行使 CPU 上的一个进程能够窥探另一个进程,例如窃取其密码键。这可能会迫使所有超标量 CPU 在 2020–5 年重新设计。

4. 存在利用共享本地物理资源的攻击,例如当手机侦听在附近的键盘上输入的击键时,或者实际上是在其自己的触摸屏上的键盘上输入的击键 无论这种感应是通过麦克风、加速度计和陀螺仪完成的,甚至相机。另一个例子是激光脉冲可以在麦克风上发出咔嗒声,因此可以通过窗口向家庭助理发出语音命令。到目前为止,针对手机和其他物联网设备的侧信道攻击还没有扩大到产生重大影响 但这种攻击越来越多。

5. 最后,还有利用共享社会资源的攻击。一个例子是从通信模式、位置历史甚至只是知道他们何时去度假来识别一个假定匿名的数据集中的某人。这导致了许多糟糕的政策决定,以及关于个人数据是否可以充分匿名以逃避隐私法的许多一厢情愿的想法。既有可耻的数据泄露,也有抱怨数据应该更多地用于研究和其他用途。很难用美元来衡量它的价值,但它在医学研究等领域意义重大,正如我们在第 11 章中讨论的那样。

多年来,我们已经了解旁路,但一直低估其中一些的重要性,同时花费不合理的资金来防御其他的。想要长期保护系统而不忽视真实和可扩展的威胁或浪费金钱追逐影子的安全工程师需要了解基础知识。

19.2 排放安全

发射安全或 Emsec 是关于防止使用妥协发射(即传导或辐射电磁信号)的攻击。担心 Tempest 的主要是军事组织,计算机和其他电子设备发出的杂散射频会被对手接收并用于重建正在处理的数据。这也成为投票机的一个问题,在一个荷兰团体发现他们可以在远处分辨出选民在投票机上选择了哪个政党之后,并且在自动取款机上也展示了攻击(尽管这些并没有真正扩展).

有源和无源发射安全措施都与电磁兼容性 (EMC) 和射频干扰 (RFI) 密切相关,它们可以意外地破坏系统,以及电磁脉冲 (EMP) 武器,可以故意破坏它们。 (我在关于电子战的章节中更详细地讨论了这些问题。)随着越来越多的日常设备连接到无线网络,并且随着设备获得更多的传感器,所有这些问题 RFI/EMC、边信道和电子战威胁 可能会变得更糟。

19.2.1 历史

电话线之间的串扰是 19 世纪电话先驱们所熟知的,他们的双线电路堆叠在支撑杆上的多层交叉树上。他们学会了每隔一段时间交叉电线,使每个电路成为双绞线。串扰于 1884-85 年首次引起军方的注意,而已知的第一个战斗功绩是在 1914 年。现场电话线被铺设用于连接陷入佛兰德斯泥泞中的部队,并且经常与敌人的战壕平行跑数英里几百码之外。第一次世界大战早期的电话电路是单芯绝缘电缆,它使用接地回路以将电缆的重量和体积减半。很快发现漏电引起串扰,包括来自敌方的消息。监听站很快建立起来,保护措施也被引入,包括使用双绞线电缆。到 1915 年,电子管放大器已将漏电监听范围扩大到电话 100 码和摩尔斯电码 300 码。人们发现,无人区那一团乱麻的废弃电报线提供了如此良好的通讯渠道,而且泄露的电讯如此之多,以至于清理它成为一项耗费生命的任务。到 1916 年,前线 3000 码范围内的接地回路已被废除 [1380]。

情报界在第二次世界大战前后发现了对加密设备的侧信道攻击,当时贝尔向美国政府出售了一台混合器,用于将一次性磁带添加到电报流量中,并发现明文以密文形式泄漏。整个 1950 年代,美国和英国都在努力抑制他们自己的密码机发出的电磁和声音。从 1957 年开始,出现了一台名为 KW-27 的机器,它对 Tempest 排放“提供了相当好的保护”。 1960 年,在英国首相在加入欧洲经济共同体的谈判期间下令监视法国大使馆之后,他的安全部门的科学家注意到来自大使馆的加密流量带有微弱的明文信号,并建造了设备来恢复它。到 1960 年代,北约开始制定 Tempest 标准;美国和英国向他们的欧洲盟友提供了选择性的、不完整的安全建议,这样他们就可以继续监视他们。与此同时,俄罗斯人在利用杂散发射方面发展得非常熟练,并对所有这些进行监视。当美国人和英国人意识到这一点时,他们使用手动一次性密码本作为秘密及以上级别的 trac 的权宜之计,然后开始将加密设备放在易受攻击的大使馆的屏蔽室中 [600]。在 Willis Ware 于 1967 年和 1970 年 [1985 年,1986 年] 的兰德公司报告中,有一个简短的公开提及计算机数据可能泄漏的可能性。之后,排放安全成为机密话题,1980 年制定的北约秘密标准在 2000 年才解密。

与此同时,英国“电视检测车”中的测向设备将家用电视机本地振荡器信号泄漏的杂散射频作为目标,电视所有者必须每年支付许可费以支持公共广播服务。 1985 年,荷兰研究员 Wim van Eck 发表了一篇文章,描述了如何使用改进的电视机在远处的 VDU 上重建图片,计算机数据也可能泄露这一事实引起了公众的注意 [601]。 1987 年,安全部门举报人彼得赖特 (Peter Wright) 泄露了法国密码机泄漏的故事 [2047]。

排放安全和相关主题的已发表研究在 1990 年代开始流行,

正如我稍后将讨论的那样。

19.2.2 技术监督与对策

在我们深入研究 Tempest 攻击的细节之前,值得注意的是,使用电磁频谱的最简单和最广泛的攻击不是利用无害设备的意外射频辐射,而是攻击者引入监听设备,或者（最近)当目标设备被恶意软件破坏时。无论它在传输或存储过程中受到加密和访问控制的保护有多好,大多数高度机密的信息都会以语音或笔记本电脑或电话上的击键形式出现。如果现阶段能被对方擒获,那么后续的任何防护措施恐怕也帮不上什么忙。

市场上有各种各样的漏洞:

- 在低端,几十美元就能买到一个简单的无线电麦克风,您可以在拜访目标时把它贴在桌子底下。电池寿命是这些设备的主要制约因素。它们的射程通常只有几百码,寿命为数天至数周。

- 下一步是从主电源、电话线或其他外部电源获取电力的设备,因此可以无限期地持续使用。作为一个历史例子,英国安全局在苏伊士危机期间进入了埃及驻伦敦大使馆,并修改了电话以在职员将当天的密钥设置输入密码机时进行监听 [600]。一些现代等效物夹在键盘电缆中,看起来像一个连接器;其他人看起来像电源适配器,但会将音频和视频传回给它们的所有者。警察秘密进入小组在严重犯罪嫌疑人的家中和汽车中安装此类窃听器。大多数现在使用移动电话技术:它们可以被视为定制手机,可以在通话时收听和观看。

- 1946 年,一班小学生向美国驻莫斯科大使展示了一个奇特的装置,该装置在米德堡的国家安全局博物馆展出。那是美国国玺的木制复制品,大使把它挂在他官邸办公室的墙上。 1952 年,人们发现它包含一个共振腔,当被建筑物外的微波照射时,该共振腔可充当麦克风,并转播他办公室中发生的对话。直到冷战结束,莫斯科的大使馆经常受到微波照射,因此该技术的变体可能仍在使用。

- 错误也被植入设备中。 1984 年,在美国驻莫斯科大使馆的 IBM Selectric 打字机中发现了 16 个错误;每个存储八个按键,然后在一次突发中传输它们。

  从那时起,在键盘和键盘电缆中设计和部署了许多键盘记录器,使用各种各样的传感器和侧通道 [1331]。

- 激光麦克风的工作原理是将激光束照射在进行目标对话的房间内的反射或部分反射表面,例如窗玻璃。声波在调制反射光的表面引起振动,这可以在远处被拾取和解码。

- 然而,现在全球范围内的大部分监控可能都是由蠕变软件完成的 由熟练的攻击者远程安装在目标手机上的软件,或者由胁迫或操纵他人的家庭成员安装,有时甚至作为雇佣条件。

技术监视对策 (TSCM) 专家将拥有一整套工具来提供针对此类攻击的保护。

- 更好的监视接收器每隔几十秒扫描一次从大约 10 KHz 到 3 GHz 的无线电频谱,并寻找无法解释为广播、警察、空中交通管制等信号。可以从其功率谱中发现直接序列扩频,并且通常会在连续扫描的不同频率处观察到跳频。突发传输效果更好。但监控接收器的有效性受到使用与合法手机相同的频率和协议的漏洞的限制。许多组织试图禁止使用手机,但大多数都放弃了;由于太多人离开,甚至皇家海军最终也不得不允许水手将手机留在船上。

- 非线性结检测器可以近距离发现隐藏的设备。它广播微弱的无线电信号并侦听设备中的晶体管、二极管和其他非线性结对信号进行整流时产生的奇次谐波。但是,如果错误已植入合法设备中或附近,则非线性结点检测器就没有太大帮助。还有一些昂贵的错误设计为根本不会重新辐射。

- 打破视线,例如在实验室周围种植树木,可以有效对抗激光麦克风,但通常不切实际。

- 可以通过跟踪模式检测仅使用普通建筑物 wifi 的隐藏无线摄像头,研究人员为此目的开发了应用程序 [415]。

- 一些设施有屏蔽室,因此即使引入了虫子,它们的信号也无法在外面听到[132]。在北约国家,绝密材料应该保存在安全隔离信息设施 (SCIF) 中,该设施具有物理安全和隔音功能,并定期清扫漏洞;如果威胁评估表明有能力的有动机的对手可能已经足够接近,则 SCIF 也可能具有电磁屏蔽。英国需要屏蔽室,研究人员才能访问政府持有的敏感个人数据,例如税务记录。

有供应商出售带有声学和电磁屏蔽的预制房间。但这比看起来要难。新的美国大使馆

在发现建筑物中有大量麦克风后,莫斯科的大楼不得不被废弃,英国反情报部门决定拆除并重建一座新总部大楼的大部分,耗资约 5000 万美元,一名员工其中一名建筑承包商被发现与临时爱尔兰共和军有过往往来。

· 在奥巴马政府以窃听美国官员手机为由驱逐了三打俄罗斯外交官之后,据报道俄罗斯人甚至通过窃听官员手机在未屏蔽的 SCIF 中窃取了对话 [579]。

技术的发展正在稳步地让窃听者的生活更轻松,而防御者的生活更难。随着越来越多的设备获得智能和短程无线电或红外通信 随着“物联网”成为“目标互联网” 通过现有设备而不是需要的设备进行攻击的范围越来越大安置的目的。这不仅仅是因为您的笔记本电脑、平板电脑或手机可能正在运行 creepware 来录制音频并在以后上传。美国国家安全局禁止在其建筑物内使用 Furby 玩具,因为 Furby 会记住(并随机重复)在它面前说过的话。 Cayla 会说话的娃娃在德国被禁止,因为陌生人可以用它来远程听孩子说话,也可以和他们说话。

但是还有许多更微妙的方式可以利用现有的电子设备。

19.3 被动攻击

我们将首先考虑被动攻击,即对手利用提供给他的电磁信号进行攻击,而无需他做任何努力来创建它们。我暂时排除光信号,稍后再将它们与声学攻击一起讨论。

从广义上讲,电磁攻击有两类。信号可以通过某种电路(如电源线或电话线)传导,也可以作为射频能量辐射。这些被军方分别称为“劫持”和“暴风雨”。它们并不相互排斥; RF 威胁通常具有传导成分。例如,计算机发出的无线电信号可以被主电源接收并传导到附近的建筑物中。

19.3.1 通过电源线和信号线泄漏

每个硬件工程师都知道高频信号无处不在,您需要努力阻止它们引起问题。传导信息泄漏可以通过精心设计、适当过滤电源和信号电缆来抑制。但民用设备只需屏蔽得足够好,不干扰无线电和电视即可;防止任何可利用的信息泄漏是一项艰巨的任务。

用军事术语来说,红色设备（携带机密数据)必须通过过滤器和屏蔽与黑色设备（可以直接向外界发送信号)隔离。具有红色和黑色连接的设备,如密码机,很难正确使用,而屏蔽设备往往只能少量供应,为政府市场制造。但成本并不止于此。空军基地的操作室可能有数百根电缆从中引出;将它们全部过滤,并实施严格的配置管理以保持红/黑分离,可能会花费数百万美元。承包商费用昂贵,因为所有工作人员都需要许可 用于排放安全的北约标准 SDIP-20（以前称为 AMSG 720B)被分类。

19.3.2 射频信号泄漏

1972 年,当我第一次在格拉斯哥学校的计算机中心学习编程时,我们有一台时钟频率为 1.5 MHz 的 IBM 1401。在机房调谐到这个频率的收音机会发出响亮的哨声,这取决于正在处理的数据。有些人将其用作调试辅助工具。一位学校同事有一个更好的主意:他写了一组不同长度的子程序,这样通过按顺序调用它们,计算机就可以演奏一首曲子。我们从来没有想过这可以用来恶作剧和娱乐。

现在转向更现代的设备,直到 2000 年代初用作监视器的 VDU 自然地发射电视信号 用当前显示的图像调制的 VHF 或 UHF 无线电信号。电子束电流被视频信号调制,视频信号包含许多点率的谐波,其中一些与金属部件产生共振,并且比其他的辐射更好。给定宽带接收器,这些发射可以被拾取并重组为视频。

Wim van Eck 发现了这一点,并于 1985 年将其公开 [601];设备设计在他的论文中进行了讨论,并在 [1105] 中进行了更详细的讨论。与流行的看法相反,更现代的平面显示器通常也很容易窥探。典型的膝上型电脑有一条串行线,通过铰链从系统单元连接到显示器,并传输视频信号（图 19.1）。

其他研究人员开始尝试窥探从传真机到屏蔽 RS-232 电缆再到以太网的所有事物 [534, 1796]。Hans Georg Wolf 展示了一种 Tempest 攻击,可以从八米外的自动提款机恢复卡和 PIN 数据 [1095]。大多数商业部门只是忽略了这个问题,因为屏蔽和干扰等反制措施很难做到,而且成本高昂 [143]。军方的专业知识和设备仍然属于机密,在国防领域之外无法获得。

最后,在 2006 年 10 月,一个反对电子投票机的荷兰团体证明,用于收集荷兰 90% 的选举选票的机器可以在几十米的距离外被窃听 [785]。这导致荷兰政府要求对投票设备进行暴风雨测试,使其达到“1 区 - 12dB”的水平。

区域系统的工作原理如下。认证为 Zone 0 的设备不应发出任何可在一米距离内利用的信号;它应该保护数据免受电子窃听,即使对手在隔壁房间,而且墙壁是像石膏板一样脆弱的东西。 Zone 1 设备在 20 米的距离内应该是安全的,因此荷兰的“Zone 1”

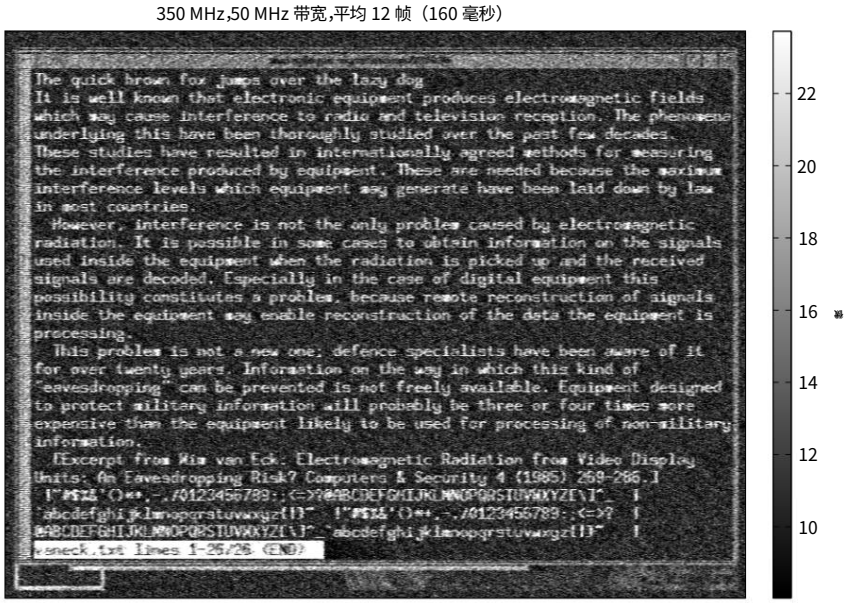

图 19.1：- 来自东芝笔记本电脑的 RF 信号通过三层石膏板墙重建了几个房间之外的信号（由 Markus Kuhn [1104] 提供）。

- 12dB 标准意味着投票机不应向 5 米外的窃听者泄露任何关于投票内容的数据。 2区和3区分别表示120米和1200米。德国人在 2007 年作为 [343] 简要公布了分区的技术细节。这份文件随后被撤回，也许是因为美国人反对。但其中的所有内容都已经在公共领域，除了区域限制曲线，考虑到近场和远场之间的差异，这是距离小型偶极子或环形天线 20m、120m 和 1200m 之间的最坏情况相对衰减掉落 。任何称职的 RF 工程师都可以对其余部分进行逆向工程。

自冷战结束削减军事预算以来，区域系统已被政府广泛使用。政府正视这样一个事实，即几乎没有攻击，除了对手可以真正接近的高价值目标，例如外交使团。斯诺登文件显示，美国的主要 Tempest 目标是联合国驻纽约的外交使团，即使在那里，此类技术也仅用于针对少数几个无法使用恶意软件破坏其计算机的国家。

各国政府意识到他们一直在浪费数十亿美元来屏蔽一切，而成本削减迫使他们对几乎所有事情都使用商用现成 (COTS) 设备。 COTS 设备在测试时往往处于 2 区，一些特别嘈杂的套件位于 3 区。通过了解哪些设备会辐射什么，您可以将最敏感的数据保存在距离设施周边最远的设备上，并且仅在您需要时才屏蔽 stu真的不得不。分区大大降低了排放安全的成本。

Markus Kuhn 和我开发了一种成本较低的保护技术，称为“软 Tempest ，在一些产品中部署了一段时间，来自电子邮件加密

化程序到荷兰投票机 [1105]。它使用软件技术来过滤或屏蔽来自计算机系统的信息承载电磁辐射。我们发现来自 VDU 的大部分承载信息的 RF 能量都集中在频谱的顶部，因此我们通过使用合适的低通滤波器对其进行卷积，去除了标准字体傅里叶变换的前 30%（参见图 19.3 和 19.4）。

图 19.3 – 普通文本

图 19.4 – 文本低通滤波

这对用户看到的屏幕内容几乎没有影响。图 19.5 和 19.6 显示了来自图 19.3 和 19.4 的两个视频信号的屏幕照片。

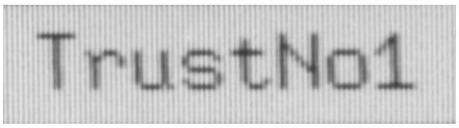

图 19.5 – 屏幕，普通文本

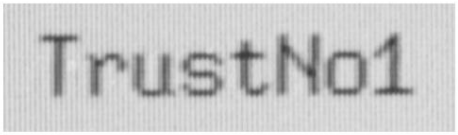

图 19.6 – 屏幕，过滤文本

然而，如图 19.7 和 19.8 中的照片所示，发射的 RF 的差异非常大。正如 Tempest 监测接收器所看到的，这些显示了潜在的危害性辐射。

在 VDU 上使用 Soft Tempest 技术转化为区域的差异 [108]。对于现代平面屏幕，可以做的事情更少，但对于某些设备，可能仍然会有有用的收获。

图 19.7 – 普通文本页面

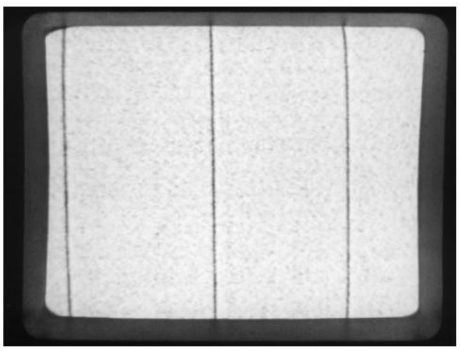

图 19.8 – 过滤文本页面

但是，攻击者可以使用主动和被动技术。我们在 IBM 1401 上观察到的现象 合适的程序可以将计算机变成无线电广播发射器 很容易在现代计算机上重新实现。图 19.9 和 19.10 显示了当视频信号是 2 MHz 的 RF 载波，用 300 和 1200 Hz 的纯音调制时 PC 屏幕的样子。

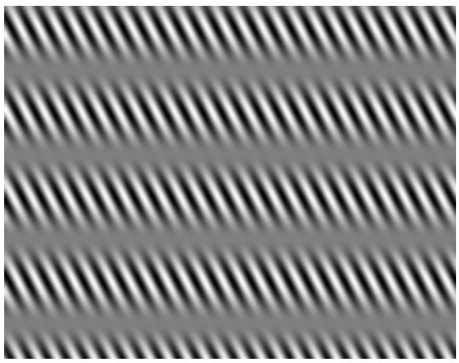

图 19.9 – 300 Hz AM 信号 图 19.10 – 1200 Hz AM 信号

使用此类技巧,恶意软件可以感染与互联网隔离的机器,并将数据泄露到附近隐藏的无线电接收器[1105]。情报界也知道这一点:1995 年的一部电视纪录片中曾报道过中央情报局在经济间谍活动中使用基于软件的射频攻击 [1062]。美国国家安全局根据 FOIA 要求解密的材料 [986] 显示,代码字 Teapot 指的是“调查、研究和控制来自电信和自动化信息的故意危害性辐射(即那些被恶意诱导或激怒的辐射)”系统设备。”恶意软件的可能性是 Tempest 测试不仅涉及被动监听被测设备的原因之一,而且还向其中注入模拟最坏情况攻击的信号,在该攻击中,对手使用软件漏洞接管设备并试图建立一个隐蔽通道[252]。

最后一类经典 Emsec 攻击是利用附近 RF 源意外诱发的 RF 辐射,美国军方称之为 Nonstop [132]。如果在手机附近使用处理敏感数据的设备,则手机的发射器可能会在设备中感应出电流,这些电流通过非线性结效应与敏感数据进行调制并重新辐射。因此,过去禁止在机密设备 5 米范围内使用手机。不间断攻击也是 Emsec 对船舶和飞机的主要担忧;在这里,如果攻击者可以靠得足够近以进行被动 Tempest 攻击,其造成的危害可能比偷听要严重得多,但是由于军舰和飞机通常携带非常强大的无线电和雷达,因此必须注意它们的信号不意外地被对敌人有用的东西调制了。在一个案例中,苏联间谍船被发现在关岛 3 英里范围之外窃听美国军事数据。

19.3.3 出了什么问题

正如埃德·斯诺登所证实的那样,Emsec 对敌对国家大使馆的威胁是真实存在的。英国在一个敌对的阿拉伯国家的大使馆曾经位于办公楼的二楼,该办公楼的一楼和三楼由当地秘密警察 Mukhabarat 占据;如果这就是你作为外交前提所得到的,那么屏蔽所有电子设备(除了用于欺骗的设备)将是解决方案的一部分。这不会是全部;您的清洁人员 将由 Mukhabarat 支付费用,因此他们会帮助您放松设备的

暴风雨垫圈,就像它们在房间里更换电池一样。

至于防御方面,2007 年 4 月发生了一起丑闻,当时洛克希德马丁公司在美国海岸警卫队船只上安装设备时忽视了 Tempest 标准。文件留在了海岸警卫队深水项目的网站上,最后出现在一个活动家网站 cryptome.org 上,该网站已关闭一段时间。这些文件不仅讲述了排放安全缺陷的故事 错误的电缆类型、违反电缆分离规则、不正确的接地、缺少过滤器、红/黑违规等 而且还讲述了一个更普遍的拙劣工作。这些船还存在船体裂缝、不防水的户外收音机、未提供规定的 360 度覆盖范围的安全闭路电视装置等等 [501]。这导致了国会调查。这些文件提供了对 Tempest 和 Nonstop 认证程序的一些见解。

最近的发展是对智能手机的 Tempest 攻击。
这样的设备没有设计要求来抵抗坐在隔壁房间的有能力的有动机的对手,并且有像样的无线电设备;因此,当 Gabriel Goller 和 Georg Sigl 在 2015 年描述了如何使用被动射频监控从远处的智能手机中提取私钥时,也就不足为奇了 [778]。此类攻击的主要困难在于手机的时钟频率通常会随工作负载而变化;如果这个频率可以以某种方式固定(例如通过恶意软件),那么攻击就会变得容易得多 事实上,它们会减少到标准的定时攻击,我现在将描述这种攻击。

19.4 计算机之间和计算机内部的攻击

在关于多级安全的章节中,我提到 Butler Lampson 在 1973 年指出的隐蔽通道可能允许处于高位的进程向低位发出信号 [1125]。举个简单的例子,高进程可以在时间ti保持一些共享资源忙碌,以表示密钥的第 i 位为 1。 ,那么高进程可以通过填满磁盘驱动器或使用大量 CPU 周期来发出信号(有些人称前者为存储通道,后者为计时通道,尽管实际上它们通常可以相互转换).

还有许多其他因素,例如顺序进程 ID、共享文件锁和文件的上次访问时间 以多级安全方式重新实现所有这些是一项艰巨的任务。也可以通过引入噪声来限制隐蔽信道容量。为此,一些机器具有随机化的系统时钟。但一些隐蔽信道容量几乎总是存在 [808]。

在经典的多级安全系统中,将隐蔽信道带宽降低到每秒一位被认为是一个很好的结果。这将使泄露许多绝密卫星图像变得困难,但泄露 256 位加密密钥当然是微不足道的。这是美国国家安全局传统上怀疑软件加密的原因之一。在软件可以在网络上发起通信的分布式系统中,隐蔽通道更难分析和阻止。 DNS 支持隐蔽通道,例如,由于该服务的合法使用而难以阻止,但恶意软件已使用它来泄露信用卡号码 [1371]。这样的渠道很容易

足够的带宽来走私加密密钥。

在 20 世纪 90 年代中期,侧信道研究因发现
对智能卡和其他加密实现的新型攻击。

19.4.1 时序分析

1996 年,Paul Kocher 表明,许多公钥算法（如 RSA 和 DSA)的实现会随着时间的推移而泄露密钥信息 [1064]。在进行求幂时,软件通常一次一位地逐步执行秘密指数,如果下一位是 1,则它会进行乘法运算。Paul 的想法是一次一位地猜测指数,研究这种猜测对时序测量的影响,看看它是否减少了它们的方差。这种巧妙的信号处理技术不断完善。到 2003 年,David Brumley 和 Dan Boneh 使用 OpenSSL 实施了针对 Apache 的定时攻击,并展示了如何通过定时大约一百万次解密来从远程服务器提取私钥 [330]。一些公钥算法的实现使用盲化来防止此类攻击（OpenSSL 确实提供了它作为一个选项,但 Apache 没有使用它）。事实上,有一系列针对 SSL/TLS 的定时攻击;尽管该协议在 1990 年代后期已被证明是安全的,但自实施以来每年大约发生一次攻击,主要是使用侧信道。

对称密钥块密码也很容易受到攻击。 John Kelsey、Bruce Schneier、David Wagner 和 Chris Hall 在 1998 年指出,后来成为 AES 的算法 Rijndael 容易受到基于缓存未命中的定时攻击 [1034]。攻击者可以通过预测猜测值是否会导致 S-box 查找缓存未命中,并根据观察结果验证这一点,来验证对第一轮密码输出的猜测。从那时起,许多研究人员稳步改进了这种攻击,并且可以通过观察数百次加密来破解 AES 的简单实现 [1489、232、1483]。许多加密库和工具包都容易受到攻击;您需要弄清楚它们是否是您的应用程序的问题,如果是,您将要做什么。泄漏的不仅仅是算法;协议和实现功能,如填充和错误处理也泄漏秘密。

19.4.2 功率分析

定时攻击可以在远处发挥作用,但如果您可以靠近目标设备,您可以做的事情就更多了。智能卡制造商从 20 世纪 80 年代就意识到信息可能会通过电源线泄露,并为各种防御措施申请了专利;到 1990 年代初期,付费电视黑客和一些政府机构似乎已经知道,可以通过简单地测量抽取的卡片电流来收集信息。称为功率分析或轨道噪声分析,这可能只涉及在地线中插入一个电阻器并在其两端连接一个数字存储示波器以观察设备的电流消耗。在图 19.11 中可以看到这种电源轨迹的示例。这显示了如何通过一次猜测一个字节并在正确的字节是正确的字节时寻找不同的电源轨迹来从微控制器中提取密码

猜到了。

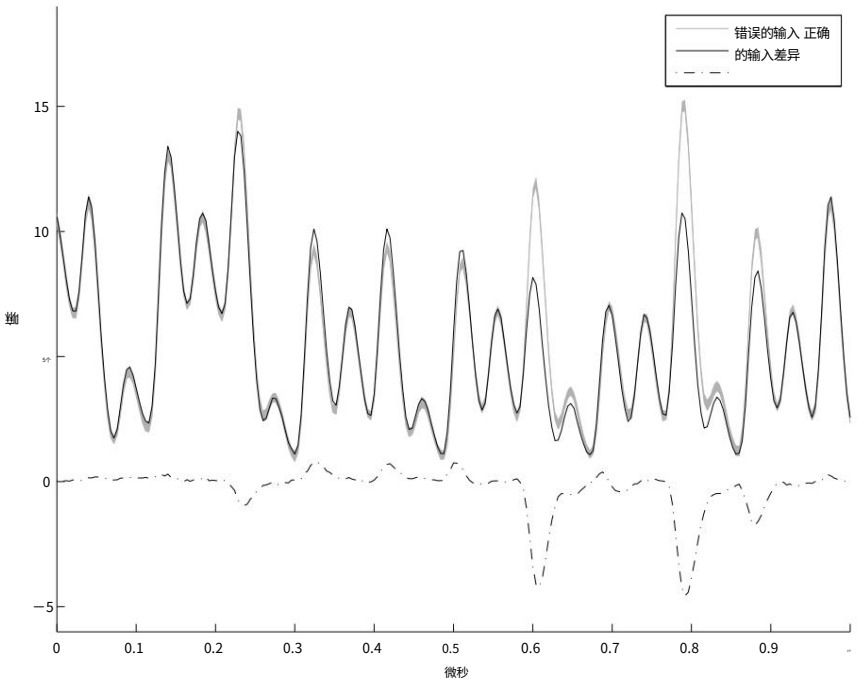

图 19.11:在 256 次单次尝试猜测存储在汽车防盗器核心微控制器中的服务密码的第一个字节期间测得的电流图（由 Markus Kuhn 和 Sergei Skorobogatov 提供）。

不同的指令具有截然不同的功耗曲线,正如您所见,功耗还取决于正在处理的数据。在许多情况下,主要的数据相关贡献来自总线驱动器晶体管,它们非常大（见图 18.7 的顶部）。根据设计,对于状态改变的总线的每一位,电流可能会在数百纳秒的时间内变化数百微安 [1298]。

因此,攻击者可以看到总线上每个数据字节与前一个字节（转换计数)之间差异的汉明权重。在某些设备中，每个数据字节的汉明权重也可用 [1303]。

EEPROM 读取和写入可以提供更强的信号。如果错误的 PIN 猜测导致 PIN 重试计数器被递减,这可能会导致电流消耗急剧增加,因为电荷泵准备写入内存（此时,攻击者甚至可能重置卡并尝试另一个 PIN）。

这种泄漏的影响不仅限于密码提取。了解（或猜测)密码是如何实现的攻击者可以获得有关卡秘密的重要信息,并且在许多情况下可以推断出所用密钥的值。 1998 年,保罗·科赫 (Paul Kocher) 将这一点强烈地引起了业界的注意,当时他将为定时攻击开发的信号处理思想改编为一种有效的技术,以从一组电源轨迹中提取分组密码（如 DES)中使用的密钥位,在不知道卡软件的任何实现细节的情况下 [1065]。这种技术被称为差分

功率分析,涉及将一组功率轨迹划分为子集,然后计算这些子集的平均值的差异 。如果子集与感兴趣的信息相关,则差异应为非零 [1067]。

作为一个具体的例子,攻击者可能会收集数百条目标卡的交易痕迹,其中明文或密文都是已知的。然后他们猜测一些密码的内部状态。在 DES 的情况下,每一轮密码都有八次查表,其中当前输入的六位与密钥的六位异或,然后用于查找 S-的四位输出盒子。因此,如果是攻击者可以访问的密文,他们将在最后一轮猜测到 S-box 的六个输入位。然后根据这个猜测将电源轨迹分为两组并同步。

然后计算并比较平均迹线。两条平均迹线之间的差值称为差分迹线。

对目标 S-box 的 64 个可能的六位输入中的每一个重复该过程。正确的输入值 将功率迹线分成两组,每组具有不同的 S-box 输出值 通常会给出具有明显峰值的差分迹线。然而,错误的猜测会给出随机排序的迹线,因此差分迹线看起来像随机噪声。通过这种方式,可以找到进入相关 S-box 的六个密钥位,然后是最后一轮密码中使用的其他密钥位。在 DES 的情况下,这给出了 56 个密钥位中的 48 个,因此可以轻松找到其余部分。

业界没有预料到这种攻击,当时市场上的所有智能卡都容易受到攻击 [1065]。由于它是一种非侵入性攻击,因此可以通过修改后的终端设备对毫无戒心的客户携带的银行卡进行攻击。因此,一旦攻击者不厌其烦地了解了一张卡并设计了一个木马终端,大量的卡可能会以很小的边际成本被攻破。

Paul 的发现将智能卡在银行业的部署推迟了两三年,而人们却在进行防御工作。事实上,他的公司已经为许多最好的专利申请了专利,并最终将它们授权给大多数加密货币供应商。

一些在协议级别工作;例如,银行卡的 EMV 协议（从 4.1 版开始)要求用于计算交易 MAC 的密钥是通过加密计数器从卡上主密钥派生的会话密钥。这样,就不会使用同一个密钥生成在卡外可见的两个密文。其他防御措施包括随机时钟,使跟踪对齐更加困难,以及掩蔽,您在每一轮中引入一些偏移量并重新计算 S-box 以补偿它们。这样,密码的实现在每次调用时都会发生变化。对于公钥算法,屏蔽的理由更为充分,因为它们还有助于减轻故障攻击,我将在下面讨论这一点。更昂贵的卡具有用于模乘法和 DES/AES 的专用加密引擎。

测试设备的 DPA 抗性并不简单； Paul Kocher 在 [1066] 中进行了讨论,2011 年的一篇调查文章在 [1067] 中讨论了攻击和防御的实用性。

主题有很多变体。基于高速缓存未命中的攻击可以测量功率以及加密所需的时间,因为未命中会激活大量电路来读取非易失性内存;你无法阻止对 AES 的缓存攻击

只是通过使用定时器来确保每次加密都需要相同数量的时钟周期。另一种变体是使用不同的传感器:David Samyde 和 Jean-Jacques Quisquater 创建了电磁分析,他们在芯片表面移动一个微小的拾取线圈来拾取本地信号,而不是简单地依赖整个设备的电流消耗[1568]。而且,正如我在上一章中提到的,DPA 可以与光学探测相结合； Sergei Skorobogatov 的光学增强位置锁定功率分析使用激光照射单个目标晶体管进行一半的测试运行,不仅可以访问汉明计算权重,还可以访问单个目标位 [1771]。

功率分析的壮观演示出现在 2016 年,当时 Eyal Ronen、Colin O aA ZFlynn、Adi Shamir 和 Achi-Or Weingarten 在开发出改进的功率分析攻击以检索 AES这些灯用于验证固件更新的密钥 [1614]。飞利浦还犯了其他几个错误:依靠单一的 AES 密钥（存在于数百万低成本设备中)来保护更新,对 CBC 和 MAC 使用相同的密钥,以及他们使用的光链路协议中存在两个错误。由于更新可以通过 ZigBee 进行传播,恶意软件可以通过连锁反应从一盏灯传播到另一盏灯;作者表明,在巴黎这样的城市,有足够的灯使这种连锁反应能够自我维持,就像核裂变一样。

2019 年最先进的技术可能是模板攻击,攻击者在其中仔细研究设备的电流绘制以获得感兴趣的指令,并构建多元高斯分布,给出给定指令、操作数、结果和状态。

有关详细信息,请参见例如 Marios Choudary 和 Markus Kuhn [419]。也可以使用特殊的硬件工具来捕获噪声较小的电源轨迹,这是电源分析中的一个重要因素 [1783]。

19.4.3 毛刺和差分故障分析

1996 年,Markus Kuhn 和我报告说,许多智能卡可能会因在其电源或时钟线上插入瞬变或毛刺而损坏 [106]。例如,早期银行应用中使用的一种智能卡具有不可接受的高时钟频率仅在多个周期后才触发重置的功能,因此瞬变不太可能导致误报。您可以用两个更窄的脉冲替换单个时钟脉冲而不会导致复位,但会强制处理器执行 NOP 而不是它应该执行的指令。这会引发选择性代码执行攻击,攻击者可以跨过跳转指令以绕过访问控制,或者利用卡自身代码中的小工具构建自己的程序。

次年,Dan Boneh、Richard DeMillo 和 Richard Lipton 注意到,如果可以引入随机错误,许多公钥加密算法就会严重崩溃 [285]。例如,当进行 RSA 签名时,秘密计算 S = h(m)d (mod pq) 执行 mod p,然后 mod q,然后合并结果,因为这要快得多。但是如果卡片返回一个有缺陷的签名Sp ,它是正确的模 p 但不正确的模 q,那么我们将有

$$p = \gcd(pq, 硒_{p} \quad 时(米))$$

这会立即破坏系统。

同样在 1997 年,Eli Biham 和 Adi Shamir 指出,如果我们可以将给定的内存位设置为零（或一）,并且我们知道在内存中保存密钥的位置,我们可以通过加密找出密钥,将前导位置零,进行另一次加密并查看结果是否不同,然后将下一位置零,依此类推 [246]。事实证明,光学探测只是解决此问题的工具 [1648],并且使用激光一次一个地将密钥位设置为零现在已成为一种常规的逆向工程技术。

激光引起的毛刺不仅限于对芯片的攻击。事实证明,如果你向 MEMS 麦克风发射激光,就像在手机和谷歌 Home 和亚马逊 Alexa 等语音控制数字助理中使用的那样,它会记录一次点击。 Kevin Fu 及其同事发现,通过用口头命令调制激光指示器,他们可以在几十米外激活此类设备　因此他们可以通过从花园的窗户照射激光指示器来命令 Alexa 打开房屋的前门 [1844].

许多现实世界的攻击现在结合使用主动和被动方法。在上面的第 19.3 节中,我讨论了光学增强的位置锁定功率分析,它使用激光在功率分析期间部分电离目标晶体管。并且您可以使用电源毛刺在短时间内大大增加芯片的光发射,以区分特定的内存写入,正如我在第 18.5.5 节中讨论的那样。

19.4.4 Rowhammer、CLKscrew 和 Plundervolt

一个非常严重的芯片级侧通道是 DRAM 内存内容可能泄漏到相邻行中。 2014 年,CMU 的 Yoongu Kim 及其同事发现 2012 年和 2013 年生产的 DRAM 容易受到干扰错误的影响;重复访问现代 DRAM 芯片中的一行会导致物理相邻行在一致可预测的位位置发生位翻转,这种攻击现在称为 Rowhammer [1048]。次年，Mark Seaborn 和 Thomas Dullien 发现应用程序代码如何利用此硬件故障来获得内核特权 [1694]。在那之后的一年,Kaveh Razavi 及其同事展示了如何使用该技术将强公钥替换为弱公钥　其效果是一个虚拟机可以通过破坏其 OpenSSH 公钥来攻击共同托管的目标机器-密钥身份验证,并且还通过从可信密钥伪造 GPG 签名来破坏软件更新机制 [1587]。易受攻击的 DRAM 类型仍在广泛使用,攻击可以针对许多不同的软件机制,因此它们可能会存在一段时间。供应商提供的第一代硬件缓解措施包括目标行刷新 (TRR),其中 DRAM 芯片控制器刷新行以阻止最常见的锤击模式； Pietro Frigo 及其同事构建了一个模糊器来分析 42 个具有 TRR 防御的芯片,并发现了对其中 13 个进行攻击的其他模式 [725]。 2020 年,Andrew Kwong 及其同事发现该机制可用于读取和写入；

攻击者可以利用 Rowhammer 引起的位翻转与相邻行中的位之间的依赖关系来推断这些位 而且,即使 ECC 内存检测并纠正每个位翻转 [1114],这种方法也有效。

使用频率和电压的动态缩放,CPU 也容易受到硬件故障注入的影响。为了省电,许多现代 CPU 会根据负载改变频率,并适当调整电压。 2017 年,Adrian Tang、Simha Sethumadhavan 和 Sal Stolfo 发现了 CLKscrew 攻击,他们对 Nexus 6 上的 Arm 处理器进行超频以击败 TrustZone,提取加密密钥并提升权限 [1858]。 2019 年,Kit Murdock 及其同事发现了 Plundervolt:英特尔酷睿处理器中一个未记录的电压缩放接口被利用来导致欠压,从而导致乘法和 AES-NI 操作出现故障,从而允许使用故障分析提取 RSA 和 AES 密钥,如以及从 SGX exclaves [1366] 泄漏任意内存内容的指针算法错误。

尽管 Arm 和 Intel 发布了针对 CLKscrew 和 Plun dervolt 的微代码补丁,但我们可能会期待其他相同类型的 CPU 攻击。 Rowhammer / RAMBleed 攻击仍然是一个问题。从长远来看,硬件安全将需要更多的防御设计。这并非微不足道:仅仅增加 DRAM 刷新率就会增加设备功耗,不太积极的频率调整也会增加。发现 Rowhammer 的两位科学家 Onur Mutlu 和 Jeremie Kim 建议,当内存控制器关闭一行时,它会根据芯片的可靠性调整概率来刷新相邻的行 [1369]。这可能反过来会增加系统级别的复杂性。随着公司将设备推向物理学设定的边界,新的芯片技术中将潜伏更多的侧通道,因此需要一种更有原则的方法来保护半导体安全。芯片供应商正在艰难地学习他们需要在设计时让优秀的安全工程师参与进来,而不是仅仅希望稍后修补 stu 。当在流行的半导体工艺或广泛使用的 CPU 级别出现故障时,修复成本很高。

19.4.5 Meltdown、Spectre 和其他 enclave 侧通道

最近袭击芯片制造商（以及整个信息安全世界)的海啸是基于 CPU 微体系结构的一系列攻击。故事始于 2005 年,当时 Colin Percival 发现 AES 缓存未命中可能被攻击者用来观察同一 Intel CPU 上另一个超线程中的加密操作;通过将数据拉入 L1 缓存,然后稍后测量访问相同数据需要多长时间,您可以查看您的数据是否被另一个超线程驱逐 [1508]。两年后,Onur Ac i cmez、Cetin Kaya Ko 和 Jean-Pierre Seifert 发明了分支预测分析 (BPA)。现代高性能 CPU 具有超标量架构,在该架构中,CPU 不再一次获取并执行一条指令,而是拥有一条流水线,可以提前获取多达 12 条指令,并尝试预测代码将采用哪个分支。 BPA 使间谍线程能够通过观察 CPU 的分支预测状态从并行加密线程中提取密钥;一次错误的预测当时被罚了 20 个周期;在最好的情况下,可以通过观察单个签名 [13] 来提取 RSA 私钥。其他人探索了其他缓存行为;在

2015 年,Fangfei Liu、Yuval Yarom 及其同事表明,L3 缓存提供了实用的素数和探测跨核攻击,能够恢复 GPG 私钥 [1176]。到 2017 年,Cachezoom 攻击允许攻击者从 SGX 飞地中提取密钥 [1328]。最近的此类攻击是 Dayeol Lee 及其同事发起的 Membuster 攻击,它使用操作系统特权来引发缓存未命中,从而泄漏数据 [1134]。 （英特尔的回应只是简单地宣布此类攻击超出范围。)在这个领域,经过十多年的努力,许多想法汇集在一起； CPU供应商应该更加关注。

最具影响力的攻击是 2018 年初披露的 Meltdown 和 Spectre。它们都利用推测性内存读取,并建立在之前关于 prime-and-probe、分支预测和缓存侧通道的工作之上。他们是如此严重,以至于英特尔和 Arm 都宣布他们将重新设计他们的 CPU 来阻止他们;但这需要数年时间,与此同时,软件缓解措施（如果可用)可能会导致某些工作负载性能下降 15%,并且偶尔会重启。鉴于全球数据中心消耗的电力可能占所有电力的 3%,这可能是一个大问题。

Meltdown 在内存访问和权限检查之间创建了一个竞争条件,并通过缓存侧通道读出禁止的内存。它是由多名研究人员独立发现的,他们负责任地向芯片制造商披露了他们的发现,然后整合了他们的结果 [1172]。芯片制造商在 2017 年的大部分时间里都在秘密修复漏洞。

Spectre 同时被披露,也被许多相同的团队发现。它实际上是一个（不断增长的)漏洞家族,利用分支预测逻辑,这是推测执行的一个特例。该逻辑试图猜测在条件跳转后将采用哪条代码路径,流氓软件可以训练它进行错误预测。然后 CPU 将获取永远不会执行的指令,如果其中一些执行禁止的操作 例如当用户程序读取受保护的内核内存时 那么受保护的页面可能会从缓存中获取。即使它们从未被读取 因此访问控制检查从未完成 这提供了一个可靠的定时边信道,使攻击者能够观察加密密钥材料 [1069]。简而言之,即使 CPU 的执行在形式上是正确的,各种较低级别的优化也会使时序依赖于秘密数据,并且出现了一系列 Spectre 变体来利用这一点。 Meltdown 直接读取目标进程的数据,而 Spectre 则诱使目标进程通过侧通道泄露其数据。

Spectre 系列攻击不断增加;在 Spectre 被宣布后不久,研究人员发现了一个名为 Foreshadow 的变体,它破解了英特尔处理器上许多 Spectre 没有的功能,包括 SGX 和系统管理模式 [338]。 2019 年的安全会议带来了一系列利用微妙的微架构特征的其他攻击:Zombieload、Fallout、Smotherspectre 和 RAMBleed 仅举四例,而 2020 年带来了 Load Value Injection,它结合了 Meltdown 和 Spectre [339] 的想法,以及 CrossTalk,这使得 CPU 中的一个内核可以攻击另一个内核 [1570]。现在所有的 CPU 都使用分支预测 除了最小的 而且变得如此复杂以至于有很多侧通道。在设计时找到它们并不容易,因为芯片制造商为验证他们的设计而开发的工具只是检查逻辑是否给出了正确的答案 而不是检查需要多长时间。原因

他们现在发现的是,微体系结构隐蔽通道以前沉睡的死水突然成为安全研究中最热门的话题,数百名聪明的研究生突然开始努力寻找。修复他们发现的一切都需要数年时间,鉴于技术的性质,我怀疑一切都将永远被修复。例如,Arm 引入了新的屏障指令 CSDB、SSBB 和 PSSBB。例如,在 CSDB 出现在代码中之后,不能使用预测的数据或状态 [131] 推测性地执行任何指令。从 v8.5A 开始还有一个新的数据字段 CVS2,以指示存在针对对抗性预测训练的缓解措施。可能需要四年时间才能将这一切都变成硅片,而必要的支持出现在软件工具链中可能还需要几年时间 而程序员要学会使用它还需要更长的时间。许多程序员不会费心,而许多经理对这种邪恶而复杂的问题的反应将是否认。

因此,在 2020 年代,您在同时运行不值得信任的进程的 CPU 上进行的任何加密都可能面临风险。很可能所有大小的 CPU 都将获得加密处理器,其硬件引擎可以在恒定时间内执行 AES、ECDH、ECDSA 等。 （但这随后打开了几个新的蠕虫罐头,正如我们将在高级密码工程一章中讨论的那样。）

19.5 环境侧信道

在过去的二十年里,出现了大量利用人类行为和设备环境的旁道攻击。此类攻击也利用声学、光学、设备运动和组合;一旦攻击者弄清楚如何从某人打字的声音中恢复文本,他们就可以将相同的技术应用于通过其他方式（例如在网络上或通过测量设备运动)观察到的击键时间。

19.5.1 声学侧信道

正如我在第 19.2.2 节中提到的,声学安全在防止人员或设备窃听敏感对话方面有着悠久的历史。至于窃听机,第一起案例可能发生在1956年的苏伊士危机期间,当时英国人利用电话窃听器破解了埃及大使馆哈格林密码机的设置。后来有一个“民间谣言”说,这些机构能够通过记录他们发出的声音来判断某人在旧的 IBM Selectric 打字机上打字,并且可以从点阵打印机发出的噪音中恢复数据 [323] .后来证明,从 1976 年到 1984 年,克格勃确实窃听了美国驻莫斯科大使馆的 IBM 打字机,尽管他们使用的是磁性窃听器而不是麦克风 [790]。

2001 年,Dawn Song、David Wagner 和 Xuqing Tian 表明,击键时间包含的信息足以让对手仅通过观察在 SSH 下加密的 trac 即可恢复大量信息。当在交互模式下使用 SSH 时,由于每个击键都在一个单独的数据包中发送,因此加密的数据包计时提供了精确的击键间计时,甚至一个简单的隐藏马尔可夫模型也为每个击键对提供了大约一位信息

内容;他们指出,这将使攻击者在猜测他观察到其加密值的密码时获得大约 50 倍的优势 [1803]。

2004 年,德米特里·阿索诺夫 (Dmitri Asonov) 和拉克什·阿格拉瓦尔 (Rakesh Agrawal) 表明,电脑键盘上的不同按键发出的声音完全不同。他们训练了一个神经网络来识别目标键盘上按键发出的咔嗒声,并得出结论,可以从声音发射中识别出某人的打字,错误率仅为百分之几 [136]。 2005 年,李庄、周峰和 Doug Tygar 将这些线索结合起来,提出了更强大的攻击。鉴于某人在未知键盘上用英语键入文本约十分钟的记录,他们识别出各个键,然后使用按键间时间和已知的英语统计数据来确定哪个键是哪个。因此,他们可以从他们从未访问过的键盘记录中解码文本 [2072]。其他研究人员迅速加入;到次年,Yigael Berger、Avishai Wool 和 Arie Yeredor 表明,通过改进信号处理算法,声学重建可以变得更加高效 [228]。

其他人将声学分析降低到一个更低的水平:Eran Tromer 和 Adi Shamir 表明,密钥通过 PC 的声发射泄漏,主要由主板上的电容器以高于 10KHz 的频率产生 [1908]。

2012 年开始的深度神经网络革命使更多的信息能够从这些信号中提取出来,到 2016 年,Alberto Compagno 和他的同事已经表明,如果你在通过 Skype 与某人交谈时打字,他们可以重建你的很多内容。重新输入 [464]。同样在 2016 年,Mengyuan Li 及其同事表明,当您在智能手机上打字时,您的手指运动会干扰 RF 信号,从而改变 wifi 上的多路径行为,足以调制信道状态信息;这使得流氓 wifi 热点能够推断击键信息 [1162]。到 2017 年,Ilia Shu mailov 已经弄清楚手机上的一个应用程序如何通过使用设备中的两个麦克风聆听屏幕上的点击来恢复输入另一个应用程序的密码和 PIN [1731]。这种到达时间差 (TDOA) 处理以前是复杂电子战套件的领域;这是你口袋里的一个应用程序,即使在可信执行环境中实施了密码输入机制,恶意软件也无法直接窃取它,即使保护可用,它也会让流氓应用程序窃取你的网上银行密码。

19.5.2 光边信道

现在转向光学,有明显的光学旁道,例如肩窥,有人在 ATM 机上越过您的肩膀观看您的 PIN,然后掏出您的口袋; ATM 犯罪团伙还在 PIN 输入设备上方的商店天花板上使用闭路电视摄像机,甚至在停在自动取款机旁边的家具货车中。现在每个人的口袋里都有相机,书房里有 3D 打印机,物理钥匙很容易复制 即使有人在远处观看也是如此。但是还有很多很多。

你是否曾在夜晚眺望过一座城市,看到有人工作到很晚?

在他们的办公室里,他们的脸和衬衫被电脑显示器发出的漫反射光照亮了?你有没有想过是否可以从发光中恢复任何信息? 2002 年,马库斯·库恩 (Markus Kuhn) 表明答案是“一切都很好”:他将高性能光电倍增管连接到示波器,发现普通 VDU 管中使用的蓝色和绿色荧光粉发出的光会在几微秒后衰减。因此,漫射反射辉光包含大量屏幕信息,编码在时域中。因此,给定一架望远镜、一个光电倍增管和合适的图像处理软件,就可以通过解码从他的脸或衬衫散射的光来读取银行家正在注视的计算机屏幕 [1103]。 (根据埃德·斯诺登的说法,这是美国国家安全局用来监视外国大使馆的技术之一,代号为“海洋”。)

下一个标题来自 Joe Loughry 和 David Umphress,他们查看了 PC、调制解调器、路由器和其他通信设备的数据串行线上的 LED 状态指示灯。他们发现其中有相当一部分是通过光学方式传输串行数据:测试的 12 个调制解调器中有 11 个,7 个路由器中有 2 个,以及一个数据存储设备。设计人员只是在串行数据线上驱动信号灯,而没有停下来意识到 LED 有足够的带宽来将数据传输到等待中的望远镜 [1189]。

Ben Nassi 及其同事在 2020 年的最新发现是 lamphone 频道。房间里的演讲或音乐会引起悬挂的灯泡振动,可以使用望远镜和合适的光电二极管从街对面读取 [1387]。与从窗户拾取声音的激光麦克风不同,这完全是被动的,而且方向不太敏感。

19.5.3 其他边信道

热隐蔽通道于 2006 年出现,当时史蒂文·默多克 (Steven Murdoch) 发现可以远程测量的典型计算机时钟偏差显示出昼夜变化,并意识到这是环境温度的函数。他的实验表明,除非机器的所有者采取对策,否则任何可以从中提取准确时间戳的人都可以测量其 CPU 负载;这就提出了一个问题,即攻击者是否可以找到隐藏机器在世界上的哪个位置。经度来自时区,而纬度(更慢)来自季节。因此,隐藏在诸如 Tor 之类的匿名服务背后可能并不像看起来那么容易 [1356, 1358]。

正如我们在生物识别学一章中讨论的那样,人们早就知道油性指纹残留物会损害指纹扫描仪。然而,它们也会在触摸屏上留下痕迹,在这些开始用于手机后,Adam Aviv 记录了污迹攻击:这些残留物是打破 Android 设备上常用的模式锁定的非常有效的方法 [145]。

(污迹还有助于猜测各种触摸屏设备上使用的 PIN 甚至是你的 Tesla。)

Adam 还开发了将智能手机的加速度计用作侧通道的用途,发现用户键入时手机的摇摆运动会揭示重要信息。即使在不受控制的设置下,当用户在走路时,他的模型也可以在 5 分钟内对 20% 的 PIN 和 40% 的解锁模式进行分类

尝试[146]。 Philip Marquardt 和其他人已经使用加速度计来解码附近传统计算机键盘的振动 [1229]。 Liang Cai 和 Hao Chen 随后研究了同时使用加速度计和陀螺仪,发现后者更有效,并且让 4 位 PIN 码的猜出率比随机猜出高 80 倍 [365]。然后我和 Laurent Simon 开始尝试将相机变成一个虚拟陀螺仪,因为当您点击 PIN 码时手机会倾斜;我们发现摄像头加麦克风在击键推理方面与陀螺仪一样好[1756]。手势输入也会泄漏;输入到一个应用程序中的文本可以被其他人读取,尽管这是一种利用共享中断状态的技术侧通道[1759]。

2015 年 Apple Watch 的到来,激发了更多人研究智能手表端渠道;到今年年底,Xiangyu Liu 及其同事表明,智能手表不仅可以让您对智能手机 PIN 输入进行加速度计推理攻击,还可以重建在普通键盘上键入的文本 尽管如果您将它戴在左手手腕上的左手字母 [1177] 更准确。

这些旁路有什么大不了的吗?答案似乎是“还没有”。 Joel Reardon 及其同事研究了来自 Google Play 商店的 88,000 个应用程序,并在 2019 年报告说,虽然超过 12,000 个应用程序能够利用旁路来观察其他应用程序或系统数据,或者以他们不应该使用的方式进行通信,但实际上只有 61 个应用程序做到了所以[1588]。然而,安全工程师必须意识到,随着我们转向具有丰富传感器的智能手机等设备,我们获得了丰富的侧通道,这使得将信息限制在特定应用程序和上下文中变得越来越困难。随着我们进入一个拥有无数智能对象的世界,侧通道的数量和类型将会成倍增加。

我们可能希望有一天这会给我们带来一个令人讨厌的惊喜。

19.6 社交侧渠道

许多侧信道发生在应用层,并且经常被忽视。
一个典型的例子是,向五角大楼运送比萨饼的数量增加,泄露了即将开展军事行动的事实。一个更微妙的例子是,从访问泌尿生殖医学诊所获得的个人健康信息在英国被认为是特别敏感的,除非患者同意,否则不能与 GP 共享。在一个案例中,一名妇女去 GUM 诊所就诊的经历被泄露,因为保险公司未能召回她进行涂片检查,而她的全科医生知道该检查是到期的 [1310]。保险公司知道诊所已经做过涂片检查,所以不想再付钱。

我已经在推理控制一章中详细讨论了这些问题,不建议在这里重复该讨论。我只会指出,这也是一个具有高影响力的侧通道系列。多年来,政策制定者和科技行业都假装相信,对医疗记录等敏感数据进行去标识化处理可以使其不敏感,因此适合被视为工业原材料。事实并非如此,因为一个接一个的丑闻让我们明白了 其中包括欧盟通用数据保护条例。

社交渠道也在技术政策辩论的哲学方面发挥作用;例如,Helen Nissenbaum 甚至将隐私定义为“上下文完整性”。大多数真正造成伤害的隐私失误是由于来自一种情况（例如诊所)的信息最终出现在另一种情况（例如报纸)中。具有复杂侧通道的无处不在的设备并不是唯一的问题;在没有有效选择退出的情况下用于广告的大量数据收集会导致更多的泄漏。我将在后面的“监视还是隐私？”一章中讨论这个问题。

19.7 总结

侧信道攻击包括一系列威胁,在这些威胁中,系统的安全性可以通过破坏辐射来破坏,无论是从无意的射频还是传导的电磁信号,到通过共享计算状态的泄漏,再到现代中发现的各种传感器移动电话和其他消费设备,也通过社交环境泄露。

侧信道泄漏是一个很大的话题,而且随着我们在几乎所有事物中都获得软件和传感器,它会变得更加复杂。哪些侧信道构成真正的威胁当然取决于应用,而且大多数时候它们中的大多数仍将引起学术兴趣。但偶尔,他们会咬人。所以安全工程师需要意识到风险。

研究问题

2019 年顶级安全会议上的许多研究论文都是关于侧信道的,特别是对处理器的侧信道攻击破坏了访问控制和飞地,以及对安全芯片的侧信道攻击使 TPM 或支付卡被击败。早在 2015 年,重点就放在对手机、智能手表和其他物理设备的侧信道攻击上。

社交旁路继续受到关注并推动对隐私的研究。

随着系统变得越来越复杂,侧信道漏洞变得无处不在。更复杂的供应链使错误修复变得更加困难,有时漏洞无法修复,因为这会在性能、精力或现金方面花费太多。随着技术的磨练和软件的传播,攻击变得更加容易。这也适用于经典的 Tempest 攻击,因为软件无线电 在中频阶段将信号数字化并在软件中进行所有后续处理的无线电 不再是昂贵的军事好奇心 [1117],但现在在蜂窝无线电基地中无处不在站、GPS 接收器、物联网设备,甚至是爱好者的卧室。对机器学习兴趣的激增势必会产生影响,从通过功率分析到利用社交渠道的 Tempest 改进无处不在的攻击。很难预测哪些辅助渠道会扩大规模成为另一个价值十亿美元的问题,但可以肯定的是,其中一些会。

进一步阅读

大卫·伊斯特 (David Easter) 撰写的近期暴风雨史讲述了俄罗斯、美国、英国及其欧洲盟友之间的冷战斗争 [600]。经典的 van Eck 文章 [601] 仍然值得一读，我们关于 Soft Tempest、Teapot 和相关主题的工作可以在 [1105] 中找到。有关功率分析，请参阅 Paul Kocher [1065] 和 Thomas Messergues [1298] 的论文。对于时序和功耗分析，Paul Kocher 及其同事的原始论文是经典参考文献 [1064、1065]； Stefan Mangard、Elisabeth Oswald 和 Thomas Popp 的教科书涵盖了所有主要方面 [1214]，而 Paul Kocher 2011 年的调查论文“差分功率分析简介”解释了攻击和防御的工程细节 [1067] . Mark Randolph 和 William Diehl 在 2020 年进行的一项调查涵盖了更多近期的工作 [1576]。

为了跟上安全芯片的定时和功率攻击的进展，您确实需要关注当前的研究文献，因为攻击技术一直在改进。例如，在 2019 年 11 月，Daniel Moghimi、Berk Sunar、Thomas Eisenbarth 和 Nadia Henninger 发现对 STM 制造的 TPM 进行的定时攻击已通过通用标准 EAL4+ 安全认证，并在英特尔 CPU 中的虚拟 TPM 上进行，使他们能够提取 ECDSA键；后一种情况导致了对 VPN 产品的真正攻击 [1329]。计时攻击出现二十多年后，您仍然不能依靠认证产品或大品牌来抵御它们。

针对主流计算机硬件的攻击仍在快速发展。有关对内存的攻击，请参阅 Onur Mutlu 和 Jeremie Kim 的 2019 年关于 Rowhammer 的调查论文 [1369]。至于利用推测执行对 CPU 进行的攻击，Meltdown 和 Spectre 攻击引起了广泛关注，以至于微架构安全一夜之间从一潭死水变成了该领域最热门的研究领域之一。多年来，CPU 设计者（以及几乎所有其他人）都认为，如果硬件已经过验证，那么它就会按照手册中的说明进行操作，因此没有必要寻找错误。现在我们知道验证工具无话可说侧通道，有数百个聪明人在 CPU 上殴打。错误报告不断出现，同时 CPU 变得如此复杂，可能需要数年时间才能达到一定的稳定性。 2019 年最好的起点可能是 Clau dio Canella 及其同事在 Usenix 安全研讨会上的调查论文 [380]。 Claudio 及其同事还通过名为 EchoLoad [381] 的攻击破坏了第一代 Meltdown 缓解措施。