第18话

防篡改

如果按预期工作并正确使用,构建一个安全的加密系统相对容易,但构建一个在滥用或一种或多种情况下不损害其安全性的系统仍然非常困难它的子组件失败（或被“鼓励”行为不端）……这是现在唯一一个封闭世界仍然远远领先于开放世界的领域,我们在商业密码系统中看到的许多失败提供了一些这方面的证据。

– 布赖恩·格莱德曼

进入给定安全设备、系统或程序的谨慎、批判性安全思想的数量与其使用的高科技数量成反比。

– 罗杰约翰斯顿

18.1 简介

防篡改设备现在无处不在。到目前为止我们讨论的例子包括：

- 银行卡中使用的EMV芯片和手机中用于身份验证的SIM卡；
- 用作交通票的非接触式卡和用于服务控制的付费电视解码器中的智能卡；
- 用于打印机碳粉盒和游戏配件控制的芯片
  控制台配件；
- 电话、笔记本电脑和服务器中的TPM 芯片提供信任根以支持安全启动和硬盘加密；
- 用于加密银行 PIN 的硬件安全模块,不仅仅是在银行
  服务器场,但在 ATM 和一些销售点终端中；

- Android 手机中用于存储非接触式支付凭证的 NFC 芯片,以及 iPhone 中用于存储指纹和加密密钥的 enclave 芯片;

- 埋在自动售货机中的密码模块,出售从火车票到邮票到激活电表的神奇数字的一切东西;

- 各种芯片被公司用于制造控制,这些公司希望让低成本的海外制造商生产他们的产品,但不希望看到额外的产品在未经他们同意的情况下“第三班”生产并在灰色市场上出售。

市场上的许多设备都不安全。在第 4.3.1 节中,我描述了汽车远程钥匙输入设备的逆向工程如何导致班级中断,从而显着增加汽车盗窃;在第 13.2.5 节中,我描述了如何对 Mifare 卡进行逆向工程以破坏许多建筑物的锁和交通票务系统;在 12.6.1.1 节中,我描述了卡支付终端可能会受到轻微破坏,从而导致卡伪造和交易操纵攻击。

不过有些还不错。银行和政府部门使用的最好的加密模块可以承受所有已知类型的物理攻击,并且只有当人们在其上运行不安全的软件或依赖不安全的设备与用户交互时才能被击败。智能卡防篡改是在付费电视盗版者克隆用户卡与付费电视行业试图阻止他们之间的长期战争中发展起来的,并且在想要锁定其产品的公司与其他想要锁定其产品的公司之间的军备竞赛中得到磨练解锁它们。打印机墨盒的争斗在这里很重要,因为试图控制售后市场的打印机制造商和试图打入这些市场的独立墨盒制造商都在合法行事。其他黑客为律师工作,对产品进行逆向工程以证明专利侵权。

有些学者为了荣誉而破解系统,并推动最先进的技术发展。最后还有很多灰色地带。如果你找到一种解锁手机的方法,这样它就可以在任何网络上使用,这算不算犯罪?这取决于你如何做,以及你在哪个国家。

鉴于产品种类繁多且质量参差不齐,安全工程师需要了解什么是防篡改,以及它能做什么和不能做什么。在本章中,我将带您了解过去三十年的攻击和防御演变。

如果计算机无法抵抗物理篡改,攻击者可以简单地更改软件。数据中心的计算机受到物理屏障、传感器和警报器的保护。 ATM 基本上是一台装有钞票分配器和警报传感器的保险箱中的 PC,通常用螺栓固定在墙上或底座上。

在纯粹为了完整性和可用性而需要防篡改的地方,有时可以通过在不同服务器上进行复制来实现,这些服务器同时执行事务并对结果进行投票;如今,区块链和其他共识协议正在重塑这一点。 15.4 节中讨论的阈值方案也可以为密钥材料提供机密性。但是防篡改设备可以为数据提供机密性

同样,支持 SGX 和 TrustZone 等 enclave 的 CPU 的出现也为在云服务中使用加密数据进行计算提供了前景。

18.2 历史

密码学中抗篡改的使用可以追溯到几个世纪前 [1001]。海军密码本经过加权处理,以便在即将被捕获时可以将它们扔到海里;英国政府部长的助手用来运送国家文件的发送箱内衬铅以确保它们不会沉没。使用水溶性墨水打印代码;俄罗斯的一次性便签本印在硝酸纤维素上,所以如果点燃它们会猛烈燃烧;一台美国战时密码机带有自毁铝热剂。但是关键材料经常在突袭中被捕获,因此尝试自动化篡改响应过程。一些机械密码机被制造出来,打开外壳会清除密钥设置,早期的电子设备也效仿。

在臭名昭著的沃克家族将美国海军密钥材料卖给俄罗斯人 20 多年后[876],工程师们也更加关注如何在运输过程中保护密钥的问题。目标是“将密钥材料的街道价值降低到零”,这可以通过无法轻易提取密钥的防篡改设备或可以明显提取密钥的防篡改设备来实现。

纸质钥匙曾经装在“告密箱”中,旨在显示篡改的证据。当电子密钥分发出现时,一个典型的解决方案是“填充枪”:一种以受控方式分发加密密钥的便携式设备。如今,加密密钥材料的物理传输通常涉及智能卡或封装为密钥的类似芯片。您的 SIM 卡和银行卡只是最明显的例子。对关键材料的控制也获得了更广泛的目的,美国和英国政府都使用它来限制他们的网络只能使用经批准的设备。只有在系统得到适当认证后,才会提供实时密钥材料。

一旦加载了初始密钥,就可以使用身份验证协议分发更多密钥。我们这里的主题是防止篡改的物理防御。

18.3 硬件安全模块

IBM 4758(图 18.1 和 18.2)是 2000 年代初期领先的商用密码处理器,其重要性有四个原因。首先,它是第一个被评估为美国政府设定的最高防篡改级别(FIPS 140-1 4 级)[1399] 的商业产品。其次,有大量关于它的文献,包括它的历史、硬件和软件 [1795、1998、2001]。第三,因此它是一个引人注目的目标,从 2000 年到 2005 年,我和我的学生投入了大量精力来攻击它并了解残留的漏洞。第四,目前的 IBM 旗舰产品 4765 除了修复了我们发现的一些错误外,并没有太大的变化。

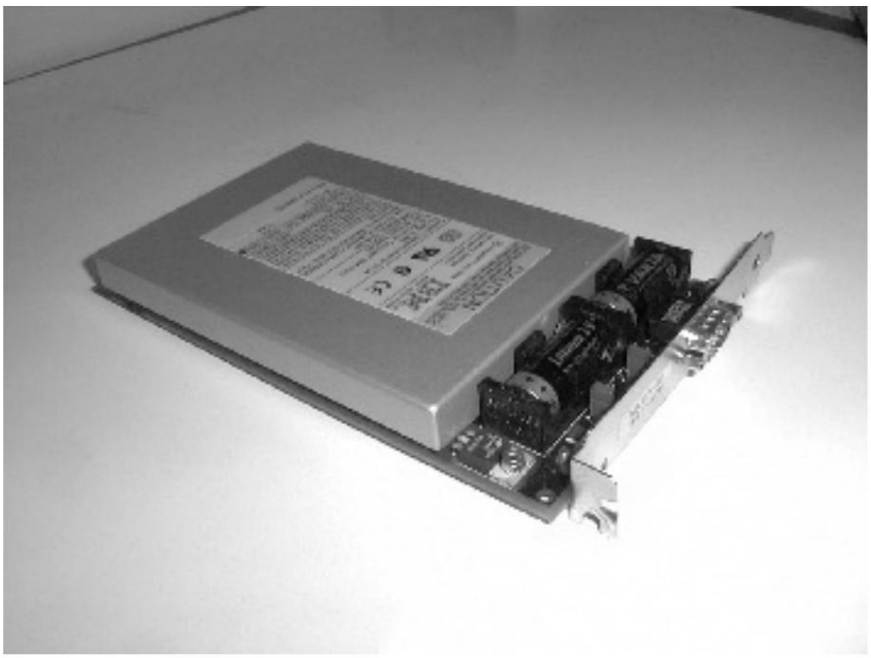

图 18.1：- IBM 4758 密码处理器（Steve Weingart 提供）

背景故事始于 1970 年代,当时米哈伊尔·阿塔拉 (Mikhail Atalla) 萌生了使用黑盒加密模块来管理银行 PIN 的想法。由于早期的 ATM 加密方案相当薄弱,IBM 开发了一种更好的块密码,它成为数据加密标准,如第 5 章所述。

随后进行了一段时间的深入研究,研究如何精确地使用分组密码来管理单个银行中的 PIN,然后在许多银行的网络中管理 PIN [1301]。银行界意识到商业操作系统可能仍然不足以保护 PIN,尤其是银行内部人员的 PIN,因此决定使用单独的硬件来管理它们。

这导致了独立加密模块或硬件安全模块 (HSM) 的开发,正如金融科技人士所说的那样。这些是微型计算机,装在坚固的金属外壳中,带有加密硬件和特殊的密钥存储器,打开外壳时会清零的静态 RAM。

最初,这只是涉及通过一些盖子开关将电源连接到钥匙存储器。因此,每当维修人员来更换电池时,他们都会打开盖子并销毁钥匙。完成后,HSM 保管人将重新加载密钥材料。通过这种方式,HSM 的所有者可以希望其密钥处于其自己可信赖的员工的唯一控制之下 。

如何破解密码处理器 (1)

明显的攻击只是窃取密钥。在早期的 HSM 中,主密钥保存在 PROM 中,这些 PROM 被加载到设备的一个特殊插槽中,以便在初始化期间读取,或者作为在控制台输入的数字字符串。 PROM 可以装进口袋、带回家和读出。明文

图 18.2：- 4758 部分打开,显示（从左上向下)电路、铝电磁屏蔽、篡改感应网和灌封材料（由 Frank Stajano 提供）

纸质钥匙甚至更容易:只需潦草地记下一份副本。

修复是共享控制 拥有两个或三个主密钥组件,并通过组合它们来制作实际的主密钥。 PROM（或纸质钥匙)将保存在不同部门控制下的不同保险箱中。

这告诉我们,共享控制是一个严重的安全可用性危害。手册可能会告诉保管人擦除活动密钥,让工程师修复设备,然后重新加载密钥。但许多资深男性过去认为触摸键盘是女性的工作,即使在今天,他们仍认为技术工作在他们之下。无论如何,谁会阅读手册?因此,管理人员经常将两把钥匙都交给工程师,以省去麻烦。在一个案例中,一名不诚实的工程师让他们使用笔记本电脑输入密钥,该笔记本电脑充当终端但已打开日志记录 [54]。我什至遇到过自动取款机的纸质万能钥匙被保存在银行分行的信件档案中,任何员工都可以在那里查找它们。

如何破解密码处理器 (2)

早期的设备很容易受到攻击者切开外壳的攻击。第二代设备通过添加光电池和倾斜开关使物理攻击更加困难。但最棘手的对手是维护工程师 他们可以在一次访问中禁用传感器并在下一次提取密钥。

到 2000 年左右,更好的产品将所有可以维修的组件（如电池)与设备的核心（如篡改传感器、密码处理器、密钥存储器和警报电路)分开。然后将核心封装到坚硬、不透明物质（如环氧树脂)的固体块中。这个想法

是任何物理攻击都会涉及切割或钻孔,这可能会被陪同工程师进入银行计算机机房的警卫发现。至少它应该留下事后篡改的证据。这是 FIPS 标准下的中级评估所需的保护级别。

如何破解密码处理器 (3)

然而,如果一个有能力的攻击者可以在短时间内不受监督地访问设备 而且,现实地说,这就是维护工程师可能拥有的,因为守卫不明白发生了什么 然后封装设备核心不够。例如,您可以用小刀刮掉灌封胶,然后将逻辑分析仪上的探针放到其中一个芯片上。理论上,刮掉粘性的环氧树脂应该会损坏里面的元件;实际上,这只是耐心的问题。 RSA、DES 和 AES 等密码算法具有这样的特性,即可以在计算期间监视任何位平面的攻击者可以恢复密钥 [860]。

因此,高端产品需要配备防篡改屏障。一个早期的例子出现在 20 世纪 80 年代中期的 IBM μABYSS 系统中,它使用 40 号镍铬合金线环松散地缠绕在设备周围,因为它被嵌入环氧树脂中,然后连接到传感电路 [1998]。该理论认为,铣削、蚀刻和激光烧蚀等技术会破坏电线,擦除按键。但是环氧树脂线材技术在使用喷砂时容易受到缓慢侵蚀;当传感线在灌封表面可见时,可以在其周围连接分流器。 2018 年,Sergei Skorobogatov 成功地使用酸蚀刻和掩蔽相结合的方法在 Vasco Digipass 270 上暴露了电池供电的芯片,这表明只要有不错的实验室技术,你确实可以攻击由环氧树脂电线保护的带电电路 [1781]。

IBM 的下一个主要产品 4753 使用了金属屏蔽层和印有导电油墨图案的薄膜,周围环绕着化学性质相似的更耐用材料。当时的想法是,任何攻击都极有可能破坏膜。 4758 有一个改进的篡改传感膜,其中四个重叠的锯齿形导电图案被掺杂到聚氨酯片中,该聚氨酯片被灌封在化学相似的物质中,因此侵入设备的攻击者甚至难以检测到导电路径,更不用说连接到它。这种灌封围绕着金属屏蔽层,金属屏蔽层又包含加密核心。该设计在 [1795] 中有更详细的描述。

如何破解密码处理器 (4)

下一类攻击利用了内存剩余,即许多计算机内存保留了一些已存储在那里的数据痕迹。一旦某个安全模块使用相同的主密钥运行了几年,它们的值就会被写入设备的静态 RAM 中。上电时,大约 90% 的相关内存位会采用先前存储的秘密密钥位的值,这足以恢复密钥 [107]。

1至少这是理论;经验表明,要求最低工资的警卫确保某些奇异设备的专家使用某些工具而不是其他工具来修理它有点过分。

内存剩余不仅影响静态和动态 RAM,还影响其他存储介质。相关的工程和物理学问题在 [837] 和 [840] 中进行了讨论,2005 年,Sergei Skorobogatov 发现了如何从微控制器中的闪存中提取数据,即使它已被“擦除”多次 [1770];不管你喜不喜欢,闪存芯片中的磨损均衡处理器已成为您可信赖的计算基础的一部分。 RAM 内容也可能被电离辐射烧毁,因此辐射感应或硬化也可能有意义。

如何破解密码处理器 (5)

计算机内存也可能因低温而冻结。到 1980 年代,人们意识到在低于 -20o C 的温度下,静态 RAM 内容可以在断电后保留几秒钟。在液氮的温度下,这会延长到几分钟。因此,攻击者可能会冻结设备、切断电源、切断篡改感应屏障、提取包含密钥的 RAM 芯片,然后在测试装置中再次启动它们。

2008 年,Alex Halderman 及其同事将其发展为对 PC 和手机中加密密钥的冷启动攻击 [854]。现代 DRAM 可在断电后将内存内容保留几秒钟,在低温下甚至更长;通过使用冷冻喷雾冷却内存,然后使用轻量级操作系统重新启动设备,通常可以读取密钥。除非有在断电时将密钥置零的机制,否则磁盘内容的软件加密可能会被破解。即使将密钥保存在诸如 TPM 之类的特殊硬件中也是不够的,如果它所做的只是限制您可以猜测硬盘加密密码的次数,然后在您获得正确的密码后将主密钥复制到主内存,以便CPU 可以完成剩下的工作。您需要真正了解加密芯片为您提供的保证 我们将在“高级密码工程”一章中更详细地讨论这个问题。

不管怎样,更好的加密设备都有温度和辐射警报。但是现代 RAM 芯片表现出各种各样的内存剩磁行为;随着特征尺寸的缩小,剩磁似乎变长了,而且即使在标准产品线中也是如此。因此,尽管您的产品可能通过使用给定品牌的 SRAM 芯片的剩磁测试,但它可能无法通过一年后购买的相同品牌芯片的相同测试 [1768]。

这显示了依赖某些组件的属性的危险,而对于其制造商而言,该属性并不重要。

HSM 警报的主要限制类似于我们遇到的更一般的警报。误报率和漏报率之间存在权衡 ,因此在安全性和鲁棒性之间存在权衡。振动、电源瞬变和电磁干扰可能是一个问题,但温度是最糟糕的。如果无法通过正常的分销渠道可靠地发送冷冻自毁的设备,因为飞机持有的温度可能低至-40oC。 (我们在 eBay 上购买了加密模块,发现它们在到达时就死了。)

军用设备制造商有相反的问题:他们的套件必须在 -55o到 +155o C 之间进行额定。一些军用设备使用保护性引爆;内存芯片被封装在钢罐中,铝热剂装药量经过精确计算,可以在不导致气体从罐中释放的情况下破坏芯片。同时满足防篡改、耐温、辐射硬化、

运输安全、重量和成本可能很重要。

如何破解密码处理器 (6)

对加密硬件的下一组攻击涉及监视设备发出的射频和其他电磁信号，甚至向其中注入信号并测量其外部可见效果 。这种被称为“暴风雨”、“功率分析”、“旁道攻击”或“发射安全”的技术是一个很大的主题，我将在下一章专门讨论它。

就 4758 而言，该策略是采用坚固的铝屏蔽并对电源进行低通滤波，以阻止内部用于计算的频率下的任何信号外出。这种屏蔽位于篡改感应膜内部，以防止对手切开一个可以用作天线的槽。

如何破解密码处理器 (7)

我们从未弄清楚如何攻击 4758 的硬件。我们在高端系统上看到的攻击涉及利用逻辑而非物理缺陷。一个硬件安全模块，Chrysalis-ITS Luna CA3，其密钥令牌的软件由 Mike Bond、Daniel Cvr ˇ cek 和 Steven Murdoch 进行了逆向工程，他们发现了允许引入未经身份验证的“客户验证密钥”的代码，并用于证明出口活键[283]。最近，在 2019 年，Gabriel Campana 和 Jean-Baptiste B´edrune 通过对软件开发工具包附带的 HSM 模拟器进行模糊测试，发现了对 Gemalto Safenet Protect Server PSI-E2/PSE2 的缓冲区溢出攻击，然后检查了这个在真正的 HSM 上，并编写代码上传任意固件，该固件是持久的并且可以下载所有秘密[203]。

这并没有发生在 IBM 的 4758 上，它有一个经过正式验证的操作系统。但它的大多数用户都运行了一个名为 CCA 的银行加密应用程序，该应用程序在 [915] 中有所描述。 Mike Bond 和我发现 CCA 向主机公开的应用程序编程接口 (API) 包含许多可利用的缺陷。结果是，有权访问主机的程序员可以向安全模块发送一系列命令，从而导致其泄露 PIN 或密钥。这些漏洞主要是以前的加密设备遗留下来的，4758 用户需要向后兼容，而实际上大多数其他安全模块更糟糕。此类攻击很难阻止，因为 Visa 会不时强制执行新的加密操作以支持新的支付网络功能，这些操作会在整个安全模块群中引入新的系统漏洞能力 [22]。一些 HSM 现在有两个 API：一个是供应商试图保持清洁的内部 API（但需要具有导入和导出密钥的能力），另一个是实施 HSM 用于支持的任何行业标准的外部 API .

两个 API 之间的软件可能是可信的，但如果外部 API 不安全，则很难使其可信。实际上，它必须预测并阻止 API 攻击。如此多的银行为安全 HSM 支付高价，他们将其用于正式合规，同时实际上依赖其他访问控制机制来保护设备免受攻击。甚至有专业公司出售防火墙以保护 HSM 免受基于软件的危害。我将讨论 API 攻击

高级密码工程一章中有详细说明。

18.4 评价

在我们继续讨论更便宜的设备之前,先对 HSM 的评估进行一些评论。当 IBM 推出 4753 时,他们在相关白皮书 [9] 中提出了以下攻击者分类:

1. 第 1 类攻击者 “聪明的局外人” 通常非常聪明,但可能对系统了解不足。他们可能只能使用中等复杂的设备。他们经常试图利用系统中现有的弱点,而不是试图创造一个弱点。

2. 第 2 类攻击者 “知识渊博的内部人士” 具有丰富的专业技术教育和经验。他们对系统的各个部分有不同程度的理解,但有可能访问其中的大部分内容。他们通常拥有高度精密的分析工具和仪器。

3. 第 3 类攻击者 “受资助的组织” 能够组建具有相关和互补技能的专家团队,并得到大量资金资源的支持。他们能够深入分析系统,设计复杂的攻击,并使用最先进的分析工具。他们可能会使用 2 级对手作为攻击团队的一部分。

在这个方案中,典型的微控制器旨在阻止聪明的外来者;早期的 4753 旨在阻止知识渊博的内部人员,而 4758 旨在(并经过认证)阻止受资助的组织。顺便说一句,这种分类有点过时了。我们看到 1 类攻击者租用 3 类设备。现在的 3 级攻击者不仅是国家实验室,还有您的商业竞争对手甚至大学安全团队。在我们的例子中,我们有具有数学、物理、软件和银行业背景的人,我们有友好的制造商给我们提供他们竞争对手产品的样品供我们破解。

FIPS 认证计划由获得美国政府许可的实验室运营。最初的 1994 年标准 FIPS 140-1 规定了四个保护级别,其中 4 级最高,而在 2001 年推出的下一版本 FIPS 140-2 中仍然保留了这一级别。级别之间存在巨大差距4级和3级;该级别的设备通常很容易被专家攻击。事实上,IBM 工程师关于评估的原始论文提出了六个级别 [2001]; FIPS 标准采用其中的前三个作为其级别 1-3,并将建议的级别 6 作为其级别 4(4758 设计师 Steve Weingart 在 [2000] 中讲述了这个故事)。这个差距通常被称为 3.5 级或 3+ 级,是 1990 年代到 2019 年许多更好的商业系统的目标。此类设备试图将 1 级攻击社区拒之门外,同时让 2 级攻击变得困难且昂贵对于第 3 类。

关于是否放弃 FIPS 140 转而支持 ISO 19790 的磋商已经进行了大约十年 这一举措得到了供应商的支持,尤其是那些

在美国以外。 FIPS 方法的批评者指出,它没有涵盖非侵入式安全,例如缓冲区溢出和 API 攻击;它的角色概念与公司中的人类参与者相关,而不是其他系统组件;它未能涵盖某些边信道分析方法;它通常针对过时的技术； FIPS 标准包括双椭圆曲线确定性随机位生成器,已知包含 NSA 后门； NIST 发布实施指南而不是定期更新标准 [1410],因此更改过于频繁。

最终,美国商务部放弃并批准了一个更新版本 FIPS 140-3,它只是简单地参考了 ISO 标准 19790:2012 和 24759:2017,并指定了一些改进。这于 2019 年 9 月生效,2021 年 FIPS 140-2 下的测试将停止。

18.5 智能卡和其他安全芯片

虽然有数以万计的 HSM 在使用,但仍有数十亿个独立的单芯片加密模块包含非易失性内存、I/O（通常是 CPU）、一些专用逻辑和保护内存不被读出的机制。大多数被包装成卡片,而有些看起来像实体钥匙。

它们的范围从低端的交通票,到现在随大多数计算机和电话一起提供的智能卡和 TPM,再到付费电视卡和附件控制芯片,旨在尽可能长时间地抵御有能力的有动机的对手的攻击。

已经开发了许多攻击;我们已经讨论了 Mifare 卡和车钥匙损坏的后果。付费电视用户卡尤其受到了密集的攻击,因为它们通常有一个通用的共享密钥,因此攻击者可以通过妥协制造大量假卡,而银行智能卡的破解只会让攻击者掠夺特定的银行账户。打印机墨盒中的附件控制芯片也保护了很多“价值”,并在攻击和防御方面推动了真正的创新。在本节中,我将讲述芯片级安全性如何演变的故事。

18.5.1 历史

智能卡是从 70 年代中期到 80 年代中期在法国开发的;有关早期历史,请参见 [832]。从 20 世纪 80 年代后期开始,它们开始大规模使用,最初是作为 GSM 手机中的用户识别模块 (SIM) 和卫星电视台的用户卡。它们于 1994 年开始在法国和南非用作银行卡,随后在英国和挪威进行了试用;这导致了我在有关银行业务和簿记的章节中提到的 EMV 标准,并从 2003 年开始在欧洲其他地区部署,大约从 2015 年开始在美国部署。

智能卡是一个独立的微控制器,微处理器、存储器和串行接口集成在单个芯片中并封装在塑料卡中。银行业使用的智能卡使用标准尺寸的银行卡,而现代手机使用的智能卡尺寸要小得多。智能卡芯片也以其他方式封装。在美国政府使用的 STU-III 保密电话中

1987 年至 2009 年,每个用户都有一个“加密点火钥匙”,包装成外观和感觉都像一把实体钥匙;一些预付费电表和付费电视机顶盒采用了相同的方法。内置于计算机主板中以支持可信启动的 TPM 芯片基本上是带有并行端口的智能卡芯片,因此 TPM 可以验证是否使用了正确的软件来启动计算机。非接触式智能卡包含一个智能卡芯片和一个环形天线;大多数汽车钥匙都是相同想法的稍微复杂的版本,增加了电池以提供更大的范围。在下文中,我将主要忽略封装形式因素,仅将单芯片密码模块称为“智能卡”或“芯片卡”。

除了银行卡,最广泛的应用是手机 SIM。这些手机通过 SIM 为每个用户进行个性化设置,其中包含您在网络中验证自己身份的密钥。在从付费电视机顶盒到智能电表的其他应用中可以找到使用便宜的卡来个性化更昂贵的电子设备的策略。该设备可以为全球市场批量生产,而每个用户都可以获得一张卡来支付服务费用。如果攻击成功,卡也可以相对快速且便宜地更换。

18.5.2 架构

典型的智能卡由一个最大 25 平方毫米的硅芯片组成,其中包含一个微处理器(较大的芯片在卡弯曲时更容易损坏)。便宜的产品有一个 8 位处理器,例如 8051 或 6805,而更昂贵的产品有一个模块化乘法电路来进行公钥加密,或者有一个 32 位处理器,例如 Arm,或者两者兼而有之(硬件加密更容易防止侧信道攻击)。高端的也往往有一个硬件随机数发生器。还有串行 I/O 和存储器层次结构 ROM 或闪存用于保存程序和不可变数据,闪存或 EEPROM 用于保存客户数据,例如用户帐号、加密密钥、PIN 重试计数器和值计数器;和 RAM 在计算期间保存瞬态数据。

内存受普通计算机标准的限制;在设备外部,唯一的连接是电源、复位、时钟和串行端口。 ISO 7816 中指定了物理、电气和低级逻辑连接以及文件系统(如访问协议)。提供了几种主要的软件架构,包括在底层的应用程序编程数据单元(APDU))由 ISO 7816 定义,它允许读者通过 Multos 操作系统直接调用特定的应用程序到 JavaCard,卡可以运行用 Java 语言的子集编写的应用程序,而你(和你的地下对手)可以用于编写自定义应用程序2。

您甚至可以购买覆盖 SIM 智能卡 160 微米厚,顶部和底部都有触点,您可以在 JavaCard 中对其进行编程以对其他智能卡进行中间人攻击(您将覆盖层粘贴在目标设备的顶部)。

2JavaCard 已悄然成为全球部署最广泛的操作系统之一
世界上售出超过 60 亿张卡片 [1250]。

18.5.3 安全演进

1986 年,当我还是一名银行家时,第一次听到智能卡供应商的推销时,我问这个设备为什么是安全的。我确信,由于制造卡片所需的机器成本为 2000 万美元,就像制造钞票一样,系统必须是安全的。我不相信这一点,但没有时间或工具来证明这种说法是错误的。后来我从行业高管那里了解到,直到 1995 年左右,他们的客户都没有准备好为严格的安全性买单,因此直到那时他们都依赖于设备的小尺寸、设计的隐蔽性以及芯片测试工具的不可访问性使攻击更加困难。不管怎么说,只要只是用来做SIM卡,就没有能干的有上进心的对手。通过破解我的 SIM 卡,我所能实现的就是能够将通话费用计入我自己的帐户。

改变这一切的应用是卫星电视。电视运营商在大片区域（例如整个欧洲)广播他们的信号,并为每个订户提供一张卡片来计算破译他们付费频道所需的密钥。由于运营商通常只购买一两个国家的电影版权,他们无法在其他地方销售用户卡。这创造了一个黑市,可以在其中出售伪造的卡片。一个关键因素是,欧洲人多年来从英国卫星广播中收看的“星际迷航”在 1993 年突然被加密。在一些国家,例如德国,无论价格如何,都无法合法获得。这激发了许多热衷于寻找漏洞的年轻计算机科学和工程专业学生。另一个因素是一些国家,尤其是爱尔兰和加拿大,还没有禁止销售伪造的付费电视卡的法律;加拿大直到 2002 年才这样做。

因此黑客可以公开出售他们的产品。

这很快产生了连锁反应 。据报道,第一起涉及克隆智能卡的大型金融欺诈发生在大约一年后,即 1995 年 2 月/3 月。
肇事者瞄准了一张用于向葡萄牙农民提供燃料回扣的卡,与加油站合谋,这些加油站将其他燃料销售登记到伪造的卡上,以换取一部分收益。据报道,收益约为 3000 万美元 [1330]。

如何破解智能卡（一）

最早的黑客攻击是针对协议而不是卡片本身。
例如,一些早期的付费电视系统为每个客户提供一张可以访问所有频道的卡,然后通过无线方式发送消息以取消客户在介绍期后未订阅的那些频道。这开启了一种攻击,在这种攻击中,在智能卡和解码器之间插入一个设备,以拦截和丢弃发往智能卡的任何消息。因此,您可以在供应商无法取消您的服务的情况下取消订阅。同样的攻击也发生在德国的电话卡系统上,妓院和寻求庇护者的旅馆出售手工制作的芯片卡 [1813, 184]。

如何破解智能卡 (2)

由于智能卡使用外部电源,并将加密密钥和值计数器等安全状态存储在 EEPROM 中,因此攻击者可以冻结 EEP

通过移除编程电压VP P来获取 ROM 内容。早期的智能卡在专用触点上从读卡器接收VP P。因此,通过用胶带覆盖这种接触,持卡人可以防止价值计数器减少。对于一些公用电话芯片卡,这给出了无限个单位。

解决方法是使用电压倍增器从电源电压VCC内部生成VP P。然而,这并非万无一失,因为电路可能会被攻击者破坏,例如用激光射击。除了绕过值控制之外,他们还可以绕过 PIN 重试计数器,一个接一个地尝试每个可能的 PIN。因此,谨慎的程序员不会只询问客户 PIN 并在失败时递减计数器。您递减计数器,检查它,获取 PIN,验证它,如果它是正确的,然后再次递增计数器 3。

如何破解智能卡 (3)

另一种早期攻击是使用扫描电子显微镜 (SEM) 读取芯片表面的电压。当时在大学中发现的低成本 SEM 无法在超过几十千赫兹的频率下进行电压对比显微术,因此攻击者会减慢时钟速度。在一张卡中,攻击者发现他们在重置后通过适当的事务读取了 RAM 内容,因为工作内存未归零。

现代智能卡处理器有一个看门狗定时器或其他电路来检测低时钟频率并重置卡,或者使用动态逻辑。并且攻击者有时可以通过重复重置卡并对其计时 n 次,然后 n+1 次,等等来单步执行程序。但与防盗警报器一样,在误报和漏报之间需要权衡 。廉价的读卡器在卡上电时时钟频率可能会剧烈波动,从而导致许多误报。最终,卡片获得了内部时钟。

如何破解智能卡 (4)

一旦付费电视运营商阻止了简单的攻击,盗版者便转而进行物理探测。除了电路的微观尺度、芯片表面的薄玻璃钝化层和通常是某种环氧树脂的灌封之外,早期的智能卡没有防止物理篡改的保护措施。拆封芯片的技术是众所周知的,并在半导体测试的标准著作中进行了详细讨论,例如 [197]。在大多数情况下,一毫升发烟硝酸足以溶解环氧树脂。

探测站由连接了微型操纵器的显微镜组成,用于将精细探针放置在芯片表面上。它们在半导体行业用于测试生产线样品,并且可以买到二手的(见图 18.4)。他们可能有专门的附件,例如用于在芯片钝化层上打孔的激光。

探测攻击的通常目标是处理器的总线。如果可以记录总线跟踪,则可以跟踪程序的运行。 (曾经推荐卡在重置后立即计算内存校验和的行业惯例 给出所有代码和数据的完整列表。)所以

3这种防御性编程在计算的早期很常见,当时计算机使用阀门而不是晶体管并且每隔几个小时就会发生故障。那时候,如果你屏蔽 o 三位,你会检查结果不超过七位,只是为了确定。

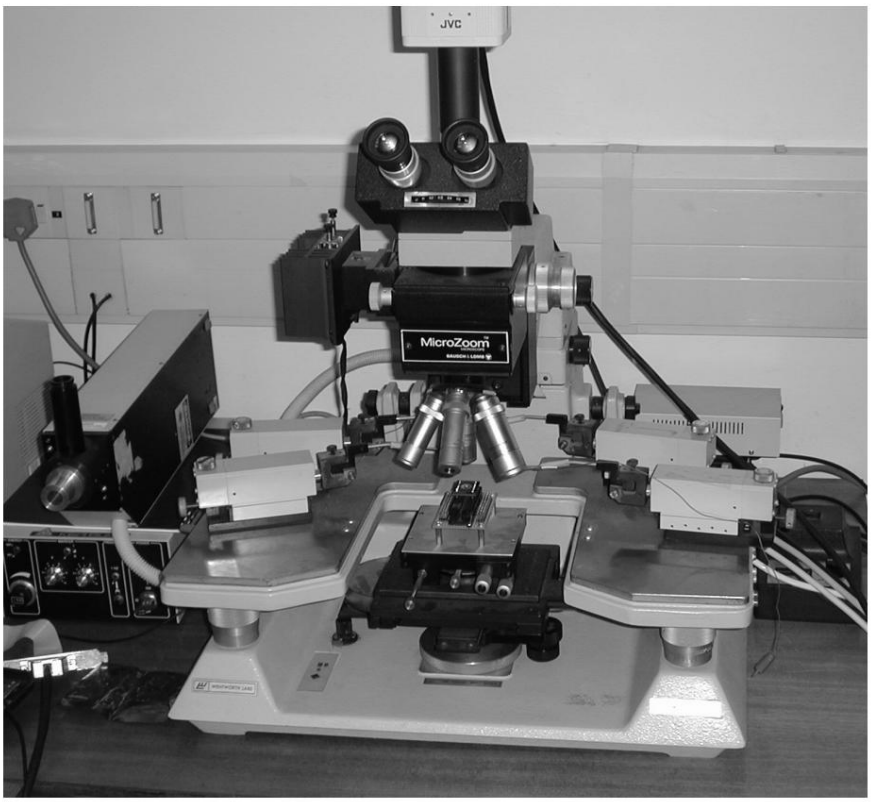

图 18.4： 我们的探测站

攻击者将找到总线并将其公开以供探测（见图 18.5）。如果芯片使用像 AES 和 RSA 这样的算法，那么除非有某种防御机制来掩盖计算，否则即使是一条总线的踪迹也足以重建密钥 [860]。

付费电视卡行业使用的第一个防御措施是为每张卡赋予多个密钥或算法，并安排一些事情，以便只有当前使用的那些才会出现在处理器总线上。每当盗版卡出现在市场上时，都会通过无线方式发出命令，使合法卡从以前未使用的内存中激活新密钥或算法。这样，盗版者的客户将遭受服务损失，直到可以重复攻击并且可以分发新的盗版卡或更新 [2064]。

如何破解智能卡 (5)

这种策略被 Oliver K¨ommerling 的内存线性化攻击打败了，在这种攻击中，分析师破坏了芯片的指令解码器，使得诸如跳转和调用之类的指令 它们改变了程序地址而不是递增它 被破坏了[1078]。一种方法是将控制线上的接地微探针放在指令锁存器上，这样无论上电时碰巧有什么指令，都会重复执行。现在可以从总线读取内存内容。事实上，有一次

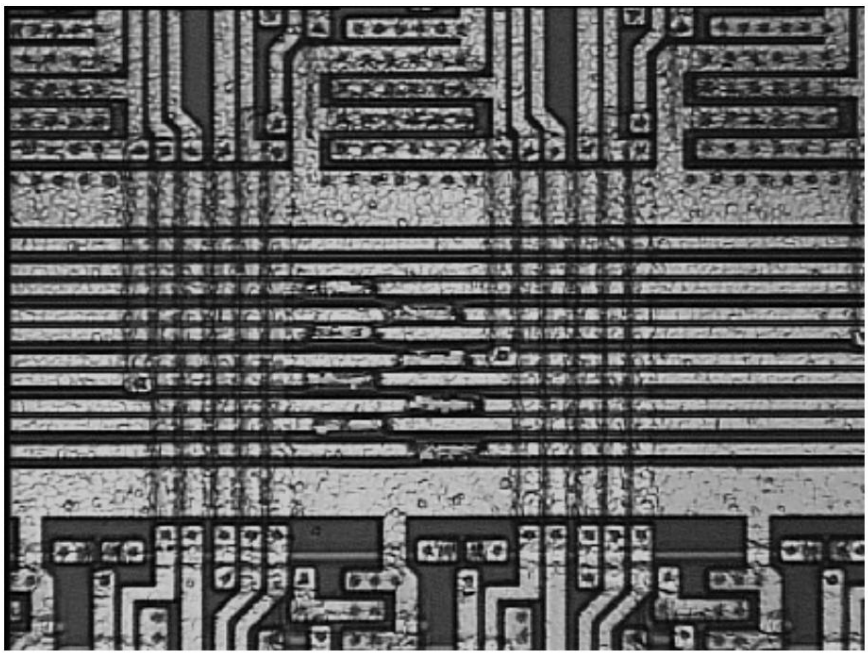

图 18.5：– ST16 智能卡的数据总线准备通过激光照射钝化层挖掘八个沟槽进行探测（照片由 Oliver K¨ommerling 提供）

一些设备的 ROM 和 EEPROM 是已知的，攻击者可以跳过不需要的指令并使设备只执行他们选择的指令。所以只要一根探针，就可以让卡片执行任意代码，理论上可以让卡片在串口输出自己的秘钥资料。这可以被认为是面向返回编程攻击的早期版本。但是探测总线上的内存内容通常更方便。

在指令解码器中通常有几个地方，接地针将阻止控制流中的程序更改。所以即使没有完全理解，内存线性化通常可以通过反复试验来实现。

一个特别容易受到攻击的智能卡系列是 Hitachi H8/300 架构，它有一个 16 位总线，如果最高有效位等于 1，则 CPU 将始终执行单周期指令而没有任何分支。因此，通过用激光照射 MSB 总线，可以轻松读出内存 [1781]。其他基于 RISC 内核的 CPU 也容易受到此影响。一些更现代的处理器有阻止内存线性化的陷阱，例如重置卡的看门狗定时器，除非它们自己每隔几千条指令重置一次。

内存线性化是故障感应攻击的一个例子。还有很多其他的例子。故障可以通过多种方式注入处理器，从硬件探测到电源瞬变和激光照明。一个常见的目标是测试电路。一个典型的芯片在工厂执行的 ROM 中有一个自检程序，允许所有内存内容

被阅读和验证。在某些情况下,芯片中的保险丝会熔断以阻止攻击者使用该设施。但是攻击者可能会导致此机制出现故障 无论是通过翻转闪存中的位[1776],还是只是找到保险丝并用两个探测针桥接它[302]。在其他情况下,测试例程受密码保护,可以在 [1775] 中找到。

我们在 5.7.1 节中注意到 RSA 算法在出现故障时是脆弱的;只需一次激光发射即可使签名模 p 正确而模 q 错误,从而使攻击者能够分解密钥 pq。 Adi Shamir 指出,如果 CPU 在其乘法单元中出现错误 即使只是一次计算 ab = c,其结果在单个位中始终返回错误 那么你可以设计一个用于解密的 RSA 密文(或用于解密的 RSA 明文) signature) 以便计算将正确完成 mod p 但错误地 mod q,再次使您能够分解密钥 [1705]。因此,细心的程序员总是会检查关键计算的结果,并认真思考可能会披露哪些错误消息。

如何破解智能卡 (6)

付费电视卡行业接下来尝试的是整合硬件加密处理器,以迫使攻击者重建硬件电路而不是简单地克隆软件,并迫使他们在盗版卡中使用更昂贵的处理器。在第一个这样的实现中,加密处理器是一个封装在卡中的单独芯片,它有一个有趣的协议故障:它总是会计算出解密当前视频流所需的密钥,然后将它传递给 CPU将决定是否将其传递给外界。黑客只是窃听了两个芯片之间的电线。

下一个版本在 CPU 本身中内置了加密硬件。如果这仅包含几千个门,则攻击者可以从显微照片中手动追踪电路。但是对于更大的门数和深亚微米工艺,成功的攻击需要严肃的工具:你需要蚀刻或磨掉芯片的层,拍摄电子显微照片,并使用图像处理软件重建电路 [269]。现在可以租用设备,也可以购买电路重构软件;现在短缺的资源是熟练的逆向工程师。

到 20 世纪 90 年代后期,一些盗版者开始让商业逆向工程实验室为他们重建芯片。这些实验室的大部分业务来自代表芯片制造商的竞争对手分析集成电路,寻找专利侵权行为。他们还反转用于配件控制的芯片,因为这样做是为了兼容性而不是盗版是合法的。许多实验室位于加拿大,在那里复制付费电视卡直到 2002 年才构成犯罪(尽管至少有两起此类实验室被付费电视运营商起诉的案例)。一些实验室现在在中国,外人更难驾驭其法律体系。

如何破解智能卡 (7)

1995 年,STM 开创了一种新的防御措施,即芯片表面的保护罩。
这是一条蜿蜒的传感器线,顶部金属中的锯齿形圆形接地线

层。一旦芯片上电,任何断路或短路都会被检测到,随后芯片将覆盖按键。

传感器网状防护罩确实会增加攻击成本。一种旁路是用针将传感器线固定到VDD ,但这可能很脆弱;和其他供应商有多个带有真实信号的传感器线路。所以如果你切割它们,你必须修理它们,而完成这项工作的工具是聚焦离子束工作站 (FIB)。这是一种类似于扫描电子显微镜的设备,但它使用离子束而不是电子束。通过改变束流,它可以用作显微镜或铣床,分辨率低于 10 纳米。通过引入一种被离子束分解的气体,您可以铺设精度为几十纳米的导体或绝缘体。有关可用于逆向工程的 FIB 和其他半导体测试设备的详细说明,请参阅 [1233]。

FIB 在各种应用中都非常有用,从半导体测试到冶金和法医学再到纳米技术,它们在物理和材料科学实验室中随处可见,而且可以以大约一百美元一小时的价格租用。

有了这样的工具,就可以直接攻击未通电的护盾。直接的方法是通过网格钻一个孔到承载所需信号的金属线,用绝缘体填充它,在绝缘体的中心钻另一个孔,用金属填充它,并在顶部镀一个触点 通常几微米宽的铂金“X”,然后用探针台上的针接触它(见图 18.6)。还有更多的技巧,例如使用电子显微镜的电压对比和反向散射模式来精确计算切割位置,这样您就可以禁用整个网格部分。

约翰·沃克 (John Walker) 在 [1975] 有一个关于如何使用这些技巧来打败盾牌的视频教程

许多其他防御措施可以迫使攻击者做更多的工作。一些芯片具有碳化硅或氮化硼保护涂层,这会迫使 FIB 操作员缓慢移动,而不是通过电荷的积累损坏芯片。带有保护涂层的芯片在马里兰州米德堡的国家安全局博物馆展出。

如何破解智能卡 (8)

1998 年,当 Paul Kocher 宣布了一种称为差分功率分析 (DPA) 的新攻击时,智能卡行业为之震惊。这依赖于这样一个事实,即不同的指令消耗不同的电量,因此通过测量芯片消耗的电流,可以提取密钥。智能卡制造商从 1980 年代就知道这在理论上是可行的,甚至为一些粗略的对策申请了专利。但是 Paul 提出了有效的信号处理技术,使它变得简单,我将在下一章中进行描述。他想出了基于时间的更简单的攻击;如果加密操作不占用相同数量的时钟周期,这也可能会泄露密钥材料4。功率和定时攻击是边信道攻击的例子,其中

4在更大的处理器上,情况可能更糟;许多研究人员在 2000 年代开发了基于缓存未命中的 AES 等加密算法的攻击,而在 2018 年,我们遇到了利用瞬态执行的 Spectre 和 Meltdown 攻击。请参阅侧面的章节

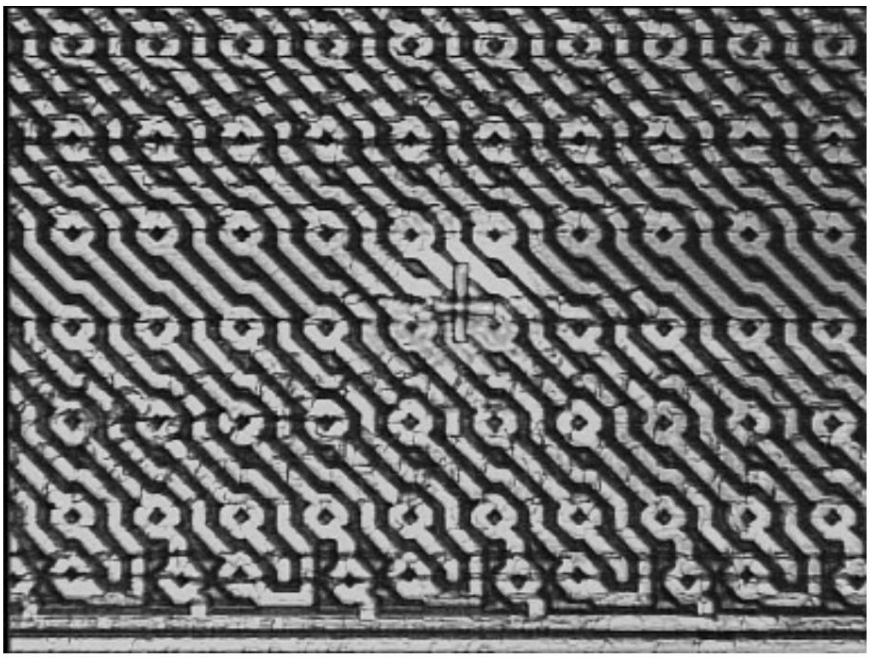

图 18.6：– 带有 FIB 十字的 ST16 智能卡的保护网,用于探测下方可见的总线（照片由 Oliver K¨ommerling 提供）

对手可以在密码计算期间观察到有关处理器状态的一些额外信息。事实证明,1998 年市场上的所有智能卡都极易受到 DPA 的攻击,这阻碍了该行业几年的发展,同时制定了对策。

攻击传统上被归类为侵入式攻击,例如机械探测,它涉及穿透钝化层,以及非侵入式攻击,例如电源分析,它不影响卡。非侵入式攻击可以进一步分类为对手需要访问设备的本地攻击,如功率分析;以及她可能在任何地方的远程攻击,例如定时攻击。但这还不是全部。

如何破解智能卡 (9)

由于特征尺寸的缩小,机械探测技术变得越来越难。下一个要开发的攻击技术是光学探测。第一份报告来自桑迪亚国家实验室,他们在 1995 年描述了一种使用激光直接读出电压的方法 [32]。自 2001 年以来,光学探测已发展成为一种有效且低成本的技术,这主要是由我在剑桥的同事 Sergei Skorobogatov 开发的。2002 年,Sergei 和我报告了使用安装在探测站显微镜上的照相闪光枪在 IC [1782] 的选定晶体管中引起瞬态故障。光使硅电离,导致晶体管导通。一旦你了解光电导并学会将光聚焦在单个晶体管上,通过从闪光枪升级到激光,这就可以进行许多直接攻击。例如,

渠道。

可以通过触发锁定其保护状态的触发器来打开微控制器。这提供了一种新方法,不仅可以引起瞬态故障攻击,如 RSA 等脆弱的密码系统,还可以在空间和时间上精确定向和控制故障。

2002 年晚些时候,谢尔盖报告说使用安装在同一台廉价显微镜上的激光器直接读取微控制器的内存。基本想法很简单:如果你用激光照射晶体管,就会产生光电流并增加器件的功耗 除非它已经导通了。因此,通过在设备上扫描激光,您可以绘制出哪些晶体管处于关闭状态,哪些处于开启状态。我们将其发展成为一种相当可靠的读取触发器和 RAM 存储器的方法 [1648]。我们将我们的攻击命名为半侵入性分析,因为它介于现有的侵入性和非侵入性类别之间。

它不是侵入性的,因为我们不会破坏钝化;但我们确实去除了环氧树脂,所以它也不算是非侵入性的。

从芯片正面进行的光学探测在大约五年的时间里一直保持着最先进的技术水平。到本书第二版(2007 年)时,智能卡供应商正在使用 0.18 和 0.13 微米工艺,通常有七个金属层。从芯片表面直接进行光学探针攻击变得很困难,这与其说是因为特征尺寸,不如说是因为金属层挡住了路。此外,芯片的庞大尺寸和复杂性让人很难知道瞄准哪里。胶合逻辑增加了难度 本质上是随机布局布线。

较旧的芯片具有清晰可辨的块,仅通过观察就可以了解很多有关它们的结构和组织的信息。公交线路可以被挑选出来并作为攻击的目标。然而,图 18.7 中的 SX28 看起来就像一个随机的门海。唯一容易区分的特征是 EEPROM(左上角)和 RAM(右上角)。找到 CPU、指令译码器和总线需要一些工作。

我在第二版中写道,“目前的两个漏洞窗口是内存和背面。”从那以后的十年里,这些为我们的篡改实验室提供了主要研究目标。

如何破解智能卡 (10)

一旦低于 0.35μ,后方攻击就是实用的半侵入式选择。您使用波长约为 1.1μ 的红外激光穿过芯片背面,硅是透明的。对于 65nm 以下的特征尺寸,您需要使用机械抛光和化学蚀刻的某种组合将芯片减薄至 2–5μ;现在有提高分辨率的特殊方法,如硅浸透镜。一个物理限制是您无法获得超过几 MHz 的带宽,因为电荷载流子重新组合需要时间。

背面攻击有时可用于通过直接观察来提取 ROM 内容,但主要技术是光学故障感应 (OFI),现已成为标准的安全测试程序。硅浸没透镜使 OFI 攻击能够继续产生低至 28 纳米硅的单粒子干扰,即使激光光斑尺寸约为 1 微米 [593]。 2019 年目前的大多数智能卡倾向于使用约 90 纳米,最小的约 65 纳米 [1862]。

三大厂商都发布了40nm产品。所以OFI会继续

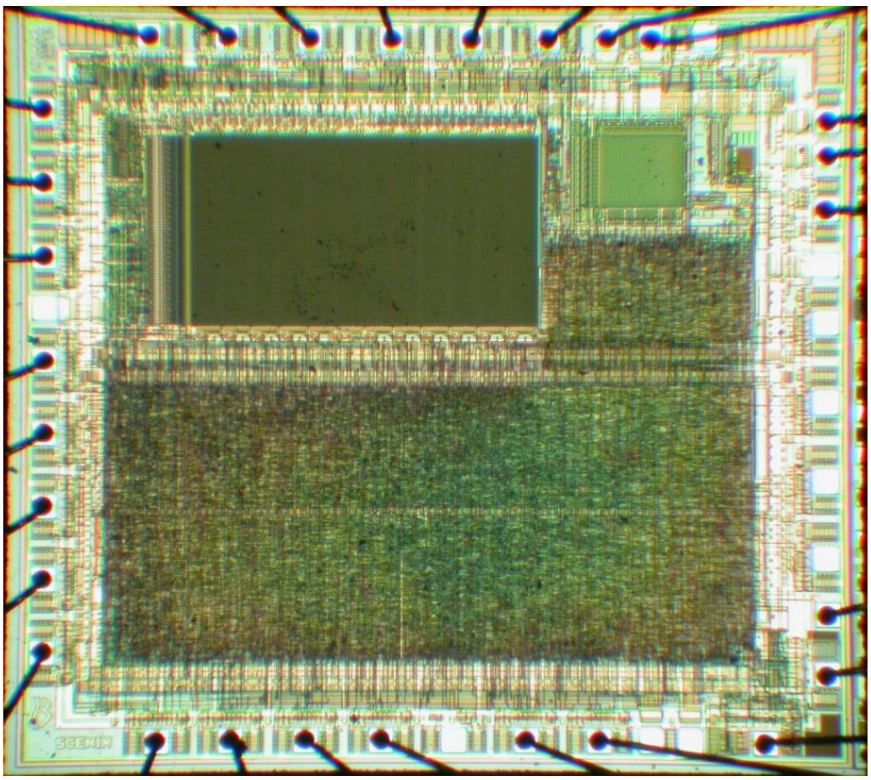

图 18.7：- 带有“胶合逻辑”的 SX28 微控制器（由 Sergei Sko robogatov 提供）

要实用一段时间。

对于更小的特征尺寸,您必须接受您在空间和时间上的目标往往是模糊的,并且您可以将激光与另一种更精确的技术结合使用。这里的一个起点是光学增强的位置锁定功率分析。通过点亮存储单元的 n 个通道，通过功率分析从状态变化中观察到的信号会增加;在更高的光照水平下,甚至可以检测到读取访问。这使得更具选择性的分析成为可能[1771]。

如何破解智能卡 (11)

到 2010 年,大多数安全芯片中的逻辑都是胶合逻辑,几乎没有可辨别的特征,但由于闪存需要高电压和大型电荷泵,因此闪存阵列很大且易于识别。芯片制造商担心,通过使用激光干扰电荷泵,针对具有单独VP P 编程电压的芯片的攻击可能会被重新发明。因此,他们试图通过在写入内存时使用每块仅验证操作来制作安全闪存,从而阻止内存损坏和内存回读访问的利用。 Sergei 的碰撞攻击受到第 13 章描述的锁碰撞攻击的启发。正如锁碰撞迫使柱面进入所需状态一样,闪存碰撞迫使总线线路进入所需状态,因为它们报告内存验证的结果 [1774]。

但也许最近最重大的突破是在 2016 年,当时 Franck Courbon、Sergei Skorobogatov 和 Chris Woods 发现了如何使用最新一代扫描电子显微镜来自动直接读取闪存和 EEPROM。由于存储单元根据浮栅中数百个电子的存在或不存在来存储位,因此在不使用为此目的设计的电路的情况下读取它们是很棘手的尤其是当使用由数十亿个电子组成的电子束时,目标是通过芯片的背面。 （我们曾经将其与用吹灯阅读重写本进行比较。）

使其工作需要非常仔细的样品制备、支持被动电压对比 (PVC) 的 SEM、微调扫描采集和高效图像处理 [480]。使用此类工具和技术,现在可以从典型的智能卡或其他安全芯片中读出 256K 的闪存或 EEPROM,并且可能有六个单位错误。早在 2000 年,4758 的设计师 Steve Weingart [1999] 就预测到了这一点； PVC 使之成为现实。

对智能卡行业的影响是现在可以读取芯片的整个内存。逆向工程是弄清楚 CPU 的指令集、内存是如何加密的等等。

如何破解智能卡 (12)

中国的逆向工程服务现在每门收费 30 美分,因此蛮力方法是将整个芯片逆向并放入模拟器中,而无需尝试详细了解它。鉴于典型的智能卡有 100,000 个门,这意味着您可以花 30,000 美元购买一个模拟器。然后你有各种各样的选择。一旦您充分了解了特定类型的一张卡,每张卡的克隆成本现在就是内存提取的成本。您还可以使用模拟来寻找边信道攻击、计划 FIB 编辑或对设备进行模糊测试并寻找其他漏洞。

由于智能卡是计算机,它们有时会遭受常见的计算机攻击,例如通过发送过长的参数字符串来覆盖堆栈。早在 1996 年,英国 NatWest 银行在支付试验中使用的 Mondex 卡就拥有经过正式验证的操作系统。然而,直到 2019 年,软件攻击才对至少一张 SIM 卡起作用。民族国家攻击者使用恶意短信将恶意软件下载到目标用户的 SIM 卡中,以便跟踪他们的位置 [575]。

18.5.4 随机数生成器和 PUF

许多加密芯片都提供了随机数生成器、物理不可克隆功能或两者兼而有之。

硬件随机数生成器 (RNG) 用于生成协议和会话密钥。弱生成器导致了许多灾难性的安全故障,其中一些出现在本书中。不良随机数会导致重放攻击,而弱会话密钥可能会破坏 ECDSA 等加密算法中的长期签名密钥。在 20 世纪 90 年代,流行的是算法随机数生成;这被称为伪随机数生成器 (PRNG)。加密芯片可能有一个特殊的密钥生成密钥,用于反加密模式;操作系统通常有类似的东西。但是,如果计数器被重置,则

重复输出;这个主题有几种变体。我还提到了 NIST Dual-EC-DRBG,它内置于 Windows 中,似乎包含一个 NSA trapdoor [1734]； Ed Snowden 后来证实,NSA 向 RSA 支付了 1000 万美元,以便在许多科技公司许可的工具中使用该标准 [1290]。

硬件随机数发生器通常量化抖动或使用一些亚稳态源,例如交叉耦合反相器对。众所周知,这种发电机很难测试;温度、电源电压和辐射等外部噪声可能会引发故障。 NIST SP800-A/B/C 等标准要求通过测试电路运行 RNG 输出。加密产品通常将来自环境和内部的多个来源的随机性混合在一起 [838],这是最高级别认证的要求。

这些来源的组合方式通常是关键,人们应该提防那些试图过于聪明的设计 [1033]。还必须注意硬件 RNG 通常是专有的、晦涩的设计,有时特定于单个晶圆厂,因此很难检查设计是否合理,更不用说它不包含微妙的后门了。保守设计的一个例子可能是自 2012 年以来在英特尔芯片中使用的设计,它结合了硬件 RNG 和随后的软件 PRNG [856]。

加密芯片的制造通常涉及将序列号和加密密钥加载到闪存或 EEPROM 中的个性化阶段。这是另一个攻击点:Ed Snowden 报告说,GCHQ 已经破解了 Gemalto 用于个性化卡片的机制,并获得了数百万 SIM 卡中的密钥副本。因此,有人可能会问,是否可以使用永远不会离开设备的固有密钥来制造芯片。每个芯片都会创建一个私钥并导出公钥,供应商将在个性化过程中对其进行认证。但这需要时间,而且似乎还需要芯片上有一个RNG。还有别的办法吗?

物理不可克隆功能 (PUF) 是一种从制造过程中自然发生的变化中识别设备的方法。 80年代,桑迪亚国家实验室在被美联储询问是否可以制造出不可伪造的钞票纸时,他们想出了将光纤切碎成糊状的想法,这样你就可以通过独特的斑点来识别每张钞票模式 [1746]。这种机制应该是不可克隆的,如果它被篡改,它的行为应该会发生可检测的变化。可以为集成电路设计类似的东西吗？ 2000 年,Oliver 和 Fritz K¨ommerling 提出用金属纤维加载芯片包装并测量其特性以生成密钥,用该密钥加密芯片内容,这样钻穿包装就会破坏密钥 [1079]。 2002 年,Blaise Gassend、Dwaine Clarke、Marten Van Dijk 和 Srini Devadas 提议在硅本身中使用过程可变性,这表明环振荡器的集合可能足够混乱以至于是独一无二的 [754]。随着人们提出设计和其他人破坏它们,攻击和防御通常会共同进化。

整个 2010 年代,我们开始看到 PUF 出现在大量低成本芯片以及 FPGA 等高价值产品中。典型的“弱 PUF”在上电时根据过程可变性生成一致的随机数； SRAM PUF 读取一些 SRAM 单元的初始状态

并通过纠错用作稳定的随机 ID 或 AES 密钥来加密内存或驱动 PRNG。如果你的对手有能力反转你的电路并扫描你的闪存,PUF 可能至少会迫使他们费力地探测总线的密钥,或者一次诱导一条总线故障以使用差分故障分析。

PUF 营销通常声称要多得多,其中一项声称（以及研究目标)是一种“强大的 PUF”,它可以充当硬件挑战-响应机制。给定一个输入,它将返回一个输出,该输出对于每个芯片（和每个输入)来说都是完全不同的,可以用作本身的密码原语。例如,一个人可能会在个性化时向芯片发送一千个挑战,并存储响应以供以后进行密钥更新。请注意,这本身并不能阻止 NSA 对金雅拓的攻击,因为他们破解了个性化文件,如果使用了 PUF,他们也会获得质询响应对文件。

2020 年最先进的技术似乎是 XOR 仲裁器 PUF,它由一个多路复用器链和一个仲裁器组成。对 PUF 的挑战被输入到多路复用器的地址线,多路复用器选择一条路径让信号通过它们到达仲裁器。为了让攻击者更难计算出每条电路路径上的相对延迟,将多个仲裁器的输出异或在一起。然而,Fatemeh Ganji、Shahin Tajik 和 Jean Pierre Seifert 已经表明,可以使用合适的机器学习技术来对底层电路进行建模 [745]。同一位作者与 Heiko Lohrke 和 Christian Boit 合作开发激光故障感应攻击,由芯片的光发射引导,禁用一些仲裁器,以便更快地学习其他仲裁器,从而显着降低 PUF 的熵 [1859]。总是存在探测攻击,因为芯片上的某些例程必须能够读取 PUF 才能执行任何工作,这意味着引导加载程序或监视器。

由于这些设备通常出于个性化、保修和升级目的对供应链的各个部分开放,因此很难看出此类设备会提供什么额外保护,即使我们可以发明一种可以正常工作的设备。此外,大规模使用此类设备往往会使个性化速度变慢,协议更加复杂。最后,PUF 的强度取决于晶圆厂尽力消除的变化,因此硅工艺的变化可能会突然使 PUF 设计变得不安全。

18.5.5 更大的芯片

越来越多的大型芯片具有嵌入式安全功能,通常用于制造控制或配件控制。这些产品的鼻祖可能是 Clipper 芯片,克林顿政府于 1993 年提出用它来替代 DES。也称为托管加密标准 (EES),这是一种防篡改芯片,包含 Skipjack 块密码和旨在允许 FBI 解密使用它加密的任何 trac 的协议。当用户向 Clipper 提供一些明文和加密它的密钥时,芯片不仅会返回密文,还会返回执法访问字段 (LEAF),其中包含用户提供的密钥,该密钥在设备中嵌入的 FBI 密钥下加密。为了防止人们通过发送错误的 LEAF 消息来作弊,LEAF 有一个用“家庭密钥”计算的 MAC

由所有 Clipper 芯片共享 这些芯片必须是防篡改的,以保持 Skipjack 块密码和 LEAF 家族密钥的秘密。

正如经常发生的那样,失败的不是防篡改,而是协议。几乎在 Clipper 上市后,Matt Blaze 就发现了一个漏洞:由于用于将 LEAF 绑定到消息的 MAC 只有 16 位长,因此可以将消息密钥输入设备,直到你得到一个具有给定 LEAF 的密钥,因此可以使用 LEAF 发送一条消息,而不会向政府透露任何信息 [258]。 Clipper 被 Capstone 芯片取代,加密战争以其他方式继续,Skipjack 块密码被置于公共领域 [1400]。

本章感兴趣的是所使用的篡改保护机制,当时声称这些机制足以抵御“非常复杂、资金充足的对手”[1398]。虽然声称 Clipper 芯片是未分类的并且可以出口,但尽管多次尝试,我始终无法获得样本。它使用 Vialink 只读存储器 (VROM),其中位通过烧断芯片上金属 1 和金属 2 层之间的反熔丝来设置。高压编程脉冲用于熔化通过两个金属层之间的多晶硅的导电路径。这项技术也被用于 QuickLogic FPGA,它被宣传为公司隐藏专有算法的一种方式,并声称“几乎不可能进行逆向工程”;更多细节和显微照片出现在其数据手册 [801] 中。最近的一个变体是点击穿 PUF,其中足够高的电压被施加到一组晶体管上足够长的时间,以至于大约一半的晶体管会遭受栅极氧化层的击穿,从而产生可以读作 1 和 0 的随机故障 [422]。

Fusible links 也用在其他设备上;例如,最近的 iPhone 在片上系统中刻录了一个 AES 密钥。基本上可以通过三种方法对反熔丝器件进行逆向工程。

- 首先要看的是编程电路。所有这些芯片都有一个测试电路,用于在编程期间回读和验证比特流,许多芯片通过事后熔化单个保险丝来禁用它。

  如果你能得到样品设备和编程器,你也许可以使用差分光学探测 [1772] 找到这个保险丝。然后你用一个FIB修复它,或者用两个探针桥接它,读出比特流。这种攻击技术不仅适用于反熔丝 FPGA,也适用于闪存和 EEPROM 品种。

- 在需要读取多个保险丝的地方,例如用于存储AES 密钥的地方,蛮力方法是一次剥离芯片一层并直接读取保险丝;它们在适当的化学染色下是可见的。由于这种攻击具有破坏性,因此它通常对每个设备中不同的密钥(如 iPhone 或 spot breakdown PUF)的兴趣有限。

- 在设备实施加密算法的地方,旁路攻击可能是最快的入侵方式。大约 2000 年之前制造的大多数设备都相当容易受到功率分析的影响,虽然智能卡芯片制造商已经整合了防御措施,但更大芯片的制造商可能

更愿意避免向 Cryptography Research 支付版税,该机构为许多最好的专利申请了专利。你总是可以尝试光故障感应来一次读取密钥,自 2000 年代末以来,我们也知道如何使用光发射,我将在后面讨论。

安全 FPGA 在 21 世纪成为一项重要业务,因为公司将电子产品的制造外包给远东,但希望控制至少一个关键组件以防止过度构建和假冒。现在出售的大多数 FPGA 都具有传统存储器而不是反熔丝,因此它们可以重新编程。如果您使用将比特流存储在 SRAM 中的易失性 FPGA,您会希望将一个或多个嵌入式密钥保存在非易失性存储器中,以便上传比特流,然后在上电时解密。为了更快地启动,您可以选择将整个比特流存储在闪存中的非易失性设备。

在这两种情况下,都可能有保险丝来保护密钥材料和安全状态 [583]。但是请注意通过升级机制进行的服务拒绝攻击。例如,闪存 FPGA 可能只有足够的内存来存储比特流的一个副本,而不是两个;所以天真的方法是读入比特流一次来解密它并验证 MAC,然后第二次重新编程该部分。但是,如果第二次提供的比特流损坏,您会得到一个死产品吗?如果您允许回滚,您的客户也许可以通过重放旧比特流来逃避升级。如果攻击者让您的产品加载随机加密的比特流,这可能会导致短路并使部件变砖。所以停下来想一想是否有人会试图通过损坏的升级来破坏您的产品基础;如果是这样,您可能会考虑使用安全的比特流加载器。

您还可以考虑使用更昂贵的 FPGA,其具有足够的片上内存以同时支持新旧比特流。

第二种大芯片安全产品是内置认证逻辑的片上系统（SoC）。先驱可能是 2000 年索尼的 Playstation 2,它采用了 MagicGate,这是一种在设备的图形芯片和嵌入在合法配件中的小型验证芯片之间运行的加密质询-响应协议。游戏机制造商的商业模式包括对软件和附加存储卡收取高价,其销售商必须使用复制控制技术并向游戏机供应商支付版税;这是用来补贴控制台的初始成本。当然,售后市场运营商随后会破解他们的复制控制机制,因此索尼着手通过更好的复制控制技术来主导其售后市场。这使用了一些有趣的保护技巧;MagicGate 协议既简单（因此无法发现协议攻击)又随机（因此攻击者无法从重复交易中学到任何东西）。售后市场公司花了几年时间和数百万美元才赶上来。虽然小芯片中的验证逻辑可能需要顶部金属屏蔽、复制陷阱和布局混淆来隐藏它,但大芯片中的相同逻辑可以隐藏在数十亿个其他晶体管中。

到 2000 年代中后期,类似的逻辑出现在其他行业的片上系统产品中　有时是为了配件控制,有时是为了使一种产品能够以多种不同的性能水平出售作为一种手段的价格歧视。这种做法导致了一些有趣的边缘案例。

例如,在 2017 年,特斯拉暂时“升级”了其 S 型和 X 型汽车的电池,以便车主可以摆脱飓风厄玛 [1930] 的路径。

那么,您如何破解我们如今随处可见的魔法设备呢?
内存读出可能是最可靠的攻击路径。例如,Sergei Skorobogatov 使用新的 PVC 闪存/EEPROM 读出技术来反转 OmniPod 胰岛素泵。知道如何编程的糖尿病患者更愿意控制自己的胰岛素泵,但出于市场控制和责任原因,供应商试图阻止它们。因此,OmniPod 的片上系统与设备的授权控制器运行身份验证协议,支持糖尿病患者的非政府组织 Nightscout Foundation 希望提取密钥,以便患者可以根据自己的健康需求优化控制,而不是遵循治疗Omnipod 设计的协议。 [1778] 中描述了该分析。

第二种攻击路径是查看设备是否使用加密数据进行计算,如果是,则寻找协议故障或侧通道让路。早期的例子是 Markus Kuhn 在DS5002 处理器 [1102]。该设备率先使用硬件进行总线加密,在加载和存储数据时动态加密内存地址和内容,因此它不仅限于当时可以安装到低成本篡改传感包中的少量 RAM (1995)。
Markus 注意到处理器的一些指令具有可见的外部效应;特别是一条指令导致内存中的下一个字节输出到设备的并行端口。因此,如果您使用测试剪辑拦截处理器和内存之间的总线,您可以在指令流中的某个点输入所有可能的 8 位指令字节,直到您看到一个字节的输出。使用此技术将几个字节的加密函数列表后,您可以加密并执行一个小程序来转储整个内存内容。类似的技巧今天仍在使用,并且攻击的变体仍然有效。 2017 年,
Sergei Skorobogatov 展示了对汽车行业使用的片上系统的主动攻击,该系统使用内存加密来增加总线探测难度。通过选择性地将错误的操作码注入总线,他能够逆转加密功能 [1779]。

iPhone 提出了一个更棘手的问题。 2016 年 3 月,联邦调查局局长詹姆斯康梅要求苹果对其 iOS 操作系统进行执法“升级”,以允许访问锁定的 iPhone,声称 FBI 否则将无法解锁圣贝纳迪诺射手的手机。

谢尔盖着手证明他是错误的,到八月,他的进攻开始奏效。有问题的手机 Apple 5c 有一个带嵌入式 AES 密钥的 SoC,通过燃烧熔断链接设置;因为这些可以在电子显微镜下看到,所以读出是可能的,但会破坏 SoC。
AES 不容易受到密码分析的影响,并且加密似乎一次只对一个高速缓存行起作用,因此密码指令搜索将不起作用。但没关系,因为存在 NAND 镜像攻击。手机的非易失性存储器是一个NAND Flash芯片,其内容是加密的,一个缓存行,通过嵌入式设备密钥,这样一部手机的芯片就无法在另一部手机中读取。攻击是拆焊存储芯片,将其安装在插槽中,然后复制其内容。然后,您进行了六次 PIN 猜测,手机开始变慢(十次后锁定)。

接下来,您移除内存芯片并恢复其原始内容。您现在可以再进行六次尝试。通过更多的工作,您可以克隆芯片或构建电路板来模拟它,这样您就可以更快地猜测。详细信息可以在 [1777] 中找到。最后,FBI 使用了
Cellebrite 的一项服务,这是一个

取证公司,后来证明是在利用 iPhone ROM [793] 中的 Checkm8 错误。

我要提到的第三种攻击是光发射分析,严格来说它是一种侧信道,但我将在这里介绍它,因为它正在成为攻击高级加密芯片的主要方式之一。半导体结切换时会发射光子,而光子发射显微镜是一种成熟的故障分析技术,硅主要在 n-MOS 晶体管漏极区域附近发射近红外光。 Julie Ferrigno 和 Martin Hlavac 在 2008 年首次使用它来攻击加密实现,他们使用昂贵的单光子计数光电倍增管从过时的 0.8µ 微控制器中读取 AES 密钥,但担心他们的技术不适用于更小的技术小于 0.12µ [681]。到第二年,Sergei Skorobogatov 发现卖给业余天文学家的光电倍增管接近理想状态,并发现了升压技巧:将芯片电源电压从 1.5V 增加到 2V 可将光子输出增加六倍。他发现他几乎能够从现代芯片 Actel ProASIC3 FGPA 的内部加密引擎中读出 AES 密钥。然后,一旦建立了 AES 算法时序,并且他知道每个轮密钥需要 1.6µs,他进一步将电压增加到 2.5V,用于单个总线写入的 0.2µs,使光子输出进一步增加四倍加上时间决议,这使他能够在公共汽车上清楚地阅读轮钥匙的每个字。早在 2001 年,我就向 Actel 咨询设计时,这一切都相当尴尬。ProASIC3 采用 0.13µ 技术制造,具有 7 个金属层和闪存,我们已经内置了各种对策来阻止攻击我们当时知道;侵入式地读出来会很乏味。这是一个尖锐的提醒,即很难阻止尚未发明的攻击,一旦专家开始磨练攻击,攻击就会很快得到改善。光发射分析现在用于组合攻击:如果你想攻击一个太大而无法进行逆向工程的芯片,你可以在进行密码学时观察发射,这会告诉你在尝试故障攻击或光学攻击时将激光瞄准哪里-增强的功率分析。它还可以建议您可以在哪里放置 FIB 的几个探测点。

18.5.6 最新技术

你能在多大程度上保护单芯片产品免受有能力的有动机的对手的攻击?在 1990 年代后期,一切都坏了,在这本书的 2001 年版中,我写道,“我所知道的任何技术或技术组合都可以使智能卡抵抗熟练和坚定的渗透袭击者。”在 2000 年代,由于付费电视公司和银行业的努力,防御得到改善,所以在第二版中我写道“这几乎仍然是正确的,但是.....你可以看到一年的延迟,预算超过一百万美元,而且不确定是否会成功。”

现在,在 2019 年,摩尔定律已经失效;加密芯片大多停留在100nm左右,而半导体测试设备行业的目标是支持9nm工艺,并且仍在不断创新,例如无源电压对比显微镜;研究人员正在寻找创新的方法来使用他们的产品。所以攻击者开始迎头赶上。的范围

业也在增加。 2007 年,我们有一些智能卡原始设备制造商、一些逆向实验室和一些感兴趣的学者;现在许多芯片制造商都被他们的客户要求提供一些防篡改功能,因为从路由器到 Raspberry Pi 的产品都获得了某种安全启动功能以击败持久的恶意软件。因此,越来越多的中档产品适合研究生学习硬件逆向工程的艺术和工艺5。对逆向设备兼容性的需求不断增长,尤其是在中国,这推动了商业逆向实验室的发展。

现在市场已经足够大,人们可以靠销售专业工具(如版图重建软件和光学故障感应工作站)谋生。

结果,攻击者越来越多,也越来越有效率。我怀疑克隆智能卡的成本会稳步下降到几万甚至几千。

安全经济学仍然是一个很大的软肋,安全芯片在很多方面都是柠檬市场。购买 HSM 的银行家可能不会意识到 FIPS 级别 3 和级别 4 之间的巨大差距,并且明白有时可以用瑞士军刀击败级别 3。那里的购买动机是合规性,而在真正的安全与运营发生冲突的地方,看到旨在使合规性更容易的较弱标准也就不足为奇了。
API 安全性太难,HSM 的内部和外部 API 之间的差异使它太混乱了。 FIPS 几乎放弃而支持 ISO 19790 和通用标准下吹捧的各种保护配置文件将进一步混淆事情,英国将放弃该标准。混淆营销和责任游戏似乎将继续下去。但这有关系吗?

首先,大部分 HSM 业务正在向云端迁移,Azure 和 AWS 各自拥有大约 2,000 个 HSM,Google 正在追赶。
我们将让 3 家公司运行几千台 HSM,而不是让几千家银行每家运行几台或几十台 HSM。随着价格的下降,HSM 供应商工程师的专业知识将会流失;随着云服务提供商保护他们的数据中心,HSM 很可能被加密芯片取代。

其次,大多数智能卡市场 SIM 卡和 EMV 卡 只有适度的物理保护要求,因为完全妥协使攻击者只能利用一个帐户。你不希望一个坏的终端能够对它看到的每一张 EMV 卡进行生产电源分析攻击,但即使发生这种情况也不是世界末日,因为这就是磁条卡被克隆的方式,并且我们知道如何限制损失。付费电视市场过去常常引领创新并定制他们使用的芯片,因为一次中断就可以让盗版者卖出数十万张克隆卡。但付费电视现在正在转向有线宽带,公司了解到更安全的芯片并不是减少损失的唯一方法:更复杂的智能卡发挥了作用,但大部分改进来自对盗版的法律行动,以及来自使技术措施和法律措施有效协同。

如今,小工具制造商将他们的产品锁定在具有云服务和应用程序的生态系统中,这使得制造控制减少了对防篡改 FPGA 的依赖。

5我的同事 Franck Courbon、Markus Kuhn 和 Sergei Skorobogatov 现在正在为我们的研究生开设这样的课程。

因此,我预计尽管加密芯片的数量和种类将继续增加,但物理保护的质量将保持不变。

供应商将只花费他们需要的钱来满足认证要求,这将保持光滑并且将被博弈。安全工程师将不得不习惯于使用灰盒组件构建系统 付出一些努力,可以从中提取密钥和算法的芯片。

我怀疑配件控制仍将是最艰难的硬件战场。如今,售后市场控制不仅仅涉及打印机墨盒,还涉及车辆、医疗设备和其他高价值产品。但是,在相互验证对方的两个设备中至少有一个至少偶尔上网的情况下,保护要求远没有卫星电视那么严格。真正的问题将是如何阻止攻击规模扩大。

18.6 剩余风险

因此,安全工程师必须注意涉及防篡改处理器的系统的许多故障模式,这些系统或多或少与设备的价格或技术防篡改无关。

18.6.1 可信接口问题

上述各节中描述的设备都没有真正值得信赖的用户界面6。一些银行安全模块的正面有一个（或两个)物理锁,以确保只有拥有给定金属钥匙（或智能卡)的人才能执行特权交易。但无论您使用 2000 美元的 4765 还是 2 美元的智能卡来进行数字签名,您仍然信任驱动它们的 PC。如果它向您显示一条文字“请支付 amazon.com 47.99 美元购买安德森安全工程的副本”,而它实际发送以供签名的消息是“请将我在 13 Acacia Avenue 的房子转抵押并将收益支付给 Mafia Real Estate Inc”,那么防篡改并没有给你带来太多好处。

事实上,这可能会使您的情况变得更糟。 Nick Bohm、Ian Brown 和 Brian Gladman 指出,当你使用合格的电子签名设备时,你是在说‘我同意对所有由我现在提供给你的密钥验证的签名承担无保留的责任,我将承保任何人因依赖它而承担的所有风险”[277]。我将在后面的第 26.5.2 节中讨论它的历史和政治。欧盟 eIDAS 法规要求所有欧盟政府接受合格的电子签名,以用于以前需要纸上墨水的交易,并为签名设备的技术认证制定标准。该行业已正式生产出数十种认证产品。考虑到与纸上墨水签名相比的责任转移,除非不得已,否则任何明智的人都不会使用合格的电子签名设备。所以游说者一直在工作,一些国家现在坚持让你用他们来报税。这导致德国的研究人员仔细研究签名、签名验证服务和 pdf 文件如何

6iPhone 安全飞地处理器 (SEP) 与指纹读取器有直接链接,但其他一切都依赖于主应用程序处理器,包括 FaceID。

相互作用;如您所料,结果有些令人震惊。 Vladislav Mladenov、Christian Mainka、Kersten Mayer zu Selhausen、Martin Grothe 和 J¨org Schwenk 创建了一份由亚马逊在德国签署并得到所有官方机构支持的文件,证明您应获得 1 万亿美元的退款。他们发现了三种针对 pdf 签名的新攻击,研究了如何绕过 22 名查看者中的 21 名的签名验证,并欺骗了 8 名在线验证服务中的 6 名 [1326]。可以肯定的是,这只是冰山一角。

另一个例子来自一些人用来存储加密货币的硬件钱包。早期产品没有可信显示,因此容易受到恶意软件的攻击。后来的一些将智能卡芯片作为安全元件与驱动显示器的安全性较低的微控制器相结合。这开启了许多可能性 包括 Saleem Rashid 描述的邪恶女仆攻击,其中可以临时访问设备的人,例如酒店女仆,重新刷新微控制器软件 [1580]。在这种情况下,安全元件不知道主处理器是否正在运行受损代码。

并非总是需要可信赖的接口,因为防篡改处理器通常能够在无需对用户进行身份验证的情况下完成有用的工作。回想一下第 14 章中的预付费电表示例:在那里,防篡改处理器可以维护一个价值计数器,对每个运营商强制执行信用限额,并限制自动售货机被盗时的损失。邮政计价器的工作方式相同。在从打印机墨盒到游戏机再到预付费电话卡的其他应用中,供应商主要关心的是使用控制。

18.6.2 冲突

另一组问题是,在不同方控制下的设备上实施应用程序的情况下,您必须考虑当每一方攻击另一方时会发生什么。在银行业,发卡机构、终端所有者和客户是不同的;克隆卡、虚假终端、黑帮商人和作弊银行之间的所有互动都需要仔细考虑。

冲突和脆弱性的一个特殊来源是许多防篡改用户的商业模式使他们的客户成为敌人 例如权限管理和配件控制。他们的客户可能拥有该产品,但如果可以的话,他们有动机去篡改它。在附件控制的情况下,他们也可能有合法的权利试图打破它;在这些机制被用来限制设备寿命并因此造成环境污染的地方,他们甚至可能觉得自己有道德责任。

18.6.3 柠檬市场、风险倾销和评估博弈

这里讨论的每个产品类别,从 HSM 到 FPGA,再到智能卡,都有范围广泛的产品,在保护质量方面也有很大差异。许多产品都有评价,但很难解读它们。

首先,高水平保证的产品相对较少 无论是

FIPS-140 4 级或 4 级以上的通用标准。有许多较低级别的测试很容易通过,供应商可以四处货比三家实验室,让他们轻松驾车。这导致了一个柠檬市场,在这个市场中,除了最知情的买家之外,所有买家都将被诱惑去购买最便宜的 FIPS 级别 3 或 CC EAL4 产品。

其次,评估证书并不像它们看起来的那样。 2001 年购买 4758 的人可能会将其 4 级评估解释为牢不可破 - 然后当我们打破它时被吓了一跳。事实上,FIPS 证书仅指硬件,我们在软件中发现了漏洞。它也以另一种方式发生:有一个具有通用标准 6 级评估的智能卡,但它仅涉及操作系统 它在没有真正防御微探测的芯片上运行。我将在第三部分更详细地讨论评估系统的失败。

第三,虽然 HSM 倾向于根据 FIPS 进行评估,但智能卡供应商倾向于使用通用标准。争论的焦点是使用哪种保护配置文件;供应商自然希望实验室评估他们认为自己擅长的安全方面。

最后,许多公司使用安全处理器来转移风险而不是最小化风险。银行喜欢说“你的芯片和密码卡被使用了,所以这是你的错”,在许多国家,监管机构让他们逍遥法外。从医学到国防,在许多环境中,买家想要的是安全证书而不是真正的保护,而这在很多方面与评估系统的缺陷相互作用。事实上,评估产品的主要用户恰恰是那些关注尽职调查而不是降低风险的系统运营商。

18.6.4 隐蔽性安全

许多设计人员都努力为他们的密码处理器保密。您几乎总是必须签署 NDA 才能获得智能卡开发工具。保护配置文件仍用于根据通用标准评估许多智能卡,强调设计模糊性。芯片掩模必须保密,指令集架构是专有的,必须审查员工 ,开发人员必须签署保密协议 这些都推高了行业成本 [650]。默默无闻也是出口审批的常见要求,导致人们怀疑它掩盖了蓄意的漏洞。例如,我们测试的卡在指示生成私钥/公钥对并输出公共部分时始终会产生相同的值。许多包含加密的产品已被破坏,因为它们的随机数生成器不够随机 [775、576],正如我们所讨论的,NSA 让 NIST 对一个弱的生成器进行了标准化。

一些 HSM 供应商是一个光荣的例外。 IBM 的通用密码体系结构从一开始就得到了很好的记录,英特尔的 SGX 和 Arm 的 TrustZone 的核心机制也是如此。这种开放性有助于发现对 IBM 产品的 API 攻击,以及对英特尔和最近的 Arm 产品的边信道和 ROP 攻击。但大多数此类攻击已被负责任地披露,并且学习过程已改进了他们的产品。

2020 年的一场争论是开发环境是否需要气隙。多年来,这一直是智能卡 OEM 的普遍做法;我们访问过的一个实验室只有一台连接到互联网的个人电脑(涂成红色,放在基座上),因此工作人员可以预订航班和酒店。这些公司现在正在推动评估人员强调攻击者最终使用高级持续威胁拥有整个公司基础设施的风险。这会给一直在线运营的公司带来不便,因为他们将不得不重建工具链并改变工作流程。

聪明的评估者不会被这种游戏技巧所吸引。对智能卡的实际攻击几乎没有使用内部信息;他们中的大多数人都是从对零售卡进行探测攻击或侧信道攻击开始的。由于行业早年没有对自己的产品进行恶意攻击,所以产品弱小,最终被人家攻破。自 20 世纪 90 年代后期以来,一些组织(例如 VISA)指定了渗透测试 [1963]。但是激励仍然是错误的;一个明智的供应商会去任何评估实验室提供最简单的旅程。我们将在第 28.2.7.2 节中讨论评估的基本经济学和政治学。

18.6.5 改变环境

我们已经看到了功能蠕变和环境变化如何通过破坏系统的设计假设来破坏系统的例子。一个普遍的问题是“杠杆” 企业试图利用他人维护的基础设施,而没有协商适当的合同。我们已经看到,SIM 卡以前只是电话公司用来识别用户身份的一种方式,现在变成了控制银行账户访问权限的令牌。在本书的第二版中,我写道“这重要吗? .....我会说它可能没有;使用短信来确认银行交易以几乎为零的边际成本为银行和客户提供了有价值的第二个身份验证渠道。”当时,我们在南非报告了一起 SIM 卡交换攻击案例。

在接下来的一段中,我写道:“但是,一旦每个人都这样做,五年或十年后会发生什么?如果 iPhone 像 Apple 希望的那样取代 ,让每个人不仅将 iPhone 用作手机,还用作网络浏览器,会怎样?突然间,这两个认证渠道缩减为一个。”

就是这样; SIM 交换现在在美国成为主流。

这实际上与当地的法律法规有关。在大多数国家,电话公司不因未能正确验证其客户而向银行承担责任。毕竟,电话公司只是出售通话时间,被盗通话时间的边际成本接近于零。但印度是一个几乎没有 SIM 交换欺诈的国家,监管机构决定电话公司必须分担 SIM 交换欺诈的责任,并且电话公司在向他们出售 SIM 之前必须根据国家 Aadhar 数据库检查客户的指纹。

18.7 那么应该保护什么?

在如此复杂的世界中,防篡改芯片能增加什么价值?

首先,他们可以将信息处理绑定到一个物理令牌上。付费电视用户卡可以在灰色市场上买卖,但只要不被复制,电视台运营商就不会损失太多收入。这也适用于配件控制,打印机供应商希望他们的产品可以与任何原装墨盒一起使用,而不是与廉价的竞争对手一起使用。

其次,他们可以维护价值计数器,就像第 13 章讨论的邮政计量一样。即使设备被盗,它可以提供的服务总价值也是有限的。在打印机中,可以对墨盒进行编程,使其仅分配一定量的墨水,然后宣布自己干燥。

第三,它们可以减少对人工操作员的信任。他们在某些政府系统中的主要目的是“将关键材料的街头价值降低到零”。用于安全电话的加密点火钥匙应该只允许小偷伪装成合法所有者,并且只有在他们可以访问实际设备的情况下,并且只有在钥匙和电话都没有被报告被盗的情况下。同样的一般考虑也适用于 ATM 网络,它不仅实施职责分离政策,而且将很多信任从人转移到事物。

第四,它们可以保护监控安全启动的物理信任根,从而使恶意软件难以持久存在。这个任务本身不需要高等级的身体防护;针对有能力的有动机的软件攻击者的安全性是关键。一个问题是,想要在自己的设备上运行自己喜欢的 Linux 版本的激进分子是否真的必须破坏 TPM,或者他们是否可以忽略它并自行管理恶意软件风险。

第五,他们可以控制不受信任的硬件承包商生产过剩的风险:有时称为“第三班”问题,您雇用的工厂分两班为您生产设备,第三班为灰色市场销售生产更多设备。这可能涉及将部分设计嵌入到难以逆向工程的 FPGA 中,或者通过使用 TPM 来控制设备在您的生态系统中工作所需的凭据。随着物联网获得云服务和应用程序,公司正在从前一种策略转向硬件成本更低且更易于管理的后者。您只需发布与工厂运送您的产品一样多的凭据。

第六,此类技术可以控制假冒电子零件带来的一些更普遍的风险。这涵盖了许多罪过,从导致早期产品故障的廉价仿冒品到国家对手进行的复杂供应链攻击。有关调查,请参见 Guin 等人 [833]。本章中描述的技术也可用于打击假冒,许多工具也是如此。至于供应链攻击,最有害的可能是硬件木马。一个国家安全问题是,随着防御系统越来越依赖海外制造的芯片,晶圆厂可能会引入额外的电路以促进以后的攻击。例如,一些额外的逻辑可能会导致带有两个特定输入的 64 位乘法用作终止开关。自 2010 年左右以来,这一直是重要研究的主题,并且已经开发了用于硅前和硅后木马检测的机制;例如,您可以对“黄金”参考芯片和评估目标进行差分侧信道分析 [1775]。这当然假设你可以生产

值得信赖的晶圆厂中的参考芯片。有关该领域的调查，请参见 Xiao et al [2053]。

这是一份不完整的清单。但这些应用程序的共同点是可以独立于周围环境的可信度提供安全属性。但请注意：所需和提供的实际保护属性可能非常微妙，防篡改设备通常是有用的组件，而不是完整的解决方案。通用机制一次又一次地失败；安全不是您撒在系统上以防止坏事发生的某种神奇的仙尘。你需要弄清楚你想要阻止哪些坏事。如果您不小心，您会发现自己在应用程序中为智能卡和加密模块付费，而这些模块几乎没有添加；如果您真的不走运，您可能会发现该行业游说法律授权或行业标准来强制您使用他们的产品。

18.8 总结

防篡改设备和系统有着悠久的历史。可以通过多种方式保护计算机免受物理篡改，从将它们锁在有人看守的房间里，通过将它们放在篡改感应箱中，再到将它们制成带有屏蔽以防止探测和防御侧信道攻击的单芯片。

我已经讲述了硬件防篡改是如何通过一系列攻击和防御循环发展起来的故事，并给出了应用示例。安全处理器通常容易受到接口（人、传感器或系统）的攻击，但通常可以在我们需要将处理链接到物理对象并保护安全状态免受可扩展威胁的应用程序中提供价值，特别是在任何在线服务的环境中可能是间歇性的。

研究问题

防篡改处理器设计基本上有两个研究方向。
第一个问题是制造“更快、更好、更便宜、更安全”的处理器：如何将高端设备提供的保护带到成本低于一美元的芯片上？第二个与推动攻击艺术的发展有关。如何使用最新的芯片测试技术进行“更快、更好、更便宜、更新颖”的攻击？第二个问题的最佳指南可能是 Sergei Skorobogatov 2018 年的演讲，“硬件安全：当前的挑战和未来的方向”[1780]。

更广泛的研究领域是如何使用不太安全的组件构建更安全的系统。如何有效使用适度保护的芯片来阻止各种攻击扩展？

进一步阅读

我不知道有任何关于硬件防篡改知识论文的最新系统化。我和我的同事在 2005 年写了一份关于安全处理器的调查 [100],如果有点过时,它可以作为一个更详细的起点;同一时期的是关于攻击技术 [1772] 的暑期学校以及 FPGA 安全性 [583] 和微控制器安全性 [1767、1769] 的评论。

Bunnie Huang 关于破解 Xbox 的书仍然是一本好书 [930]。从行业角度来看,稍后的总结是由 Chipworks 的 Randy Torrance 和 Dick James 在 2009 年 [1897] 中提出的。

至于过去十年的研究,当前最好的论文经常出现在 CHES（关于加密）、HOST（木马和后门）、FDTC（故障攻击)和 Cardis（智能卡)等会议上。失效分析研究往往出现在 ISTFA 和 IPFA。

对于早期历史 加权密码本和水溶性墨水 请阅读 David Kahn 的书“The Code Breakers”[1001]。有关 1990 年代中后期芯片卡技术的手册,请参阅 [1578],而我们如何开始篡改那几代卡的血淋淋的细节可以在 [106、107、1078] 中找到。提到的 IBM 产品有大量在线文档 [951],您还可以在其中找到美国 FIPS 文档 [1397]。

对于现代芯片测试技术,我推荐 John Walker 在 Hardwear.IO 2019 上关于如何在逆向工程 [1975] 中使用 FIB 的主题演讲视频,以及 Chris Tarnovsky 在同一活动中关于芯片防御技术 [1862]。