第12章

银行和簿记

与愚蠢对抗,众神自己也徒劳无功。

JC弗里德里希·冯·席勒

正如狗回到他的呕吐物,傻瓜也回到他的愚蠢。

– 箴言 26:11

12.1 简介

无现金支付行业是冠状病毒大流行的赢家之一,因为全世界的人们都放弃了现金,转而使用卡和电话支付。

底层银行系统的范围从支付卡处理和家庭银行业务到高价值银行间汇款,再到跟踪所有情况并在事后结算的后端簿记系统。从股票交易到交易支付,都有专门的网络,其中许多也对其他公司开放。较大的公司拥有反映银行许多功能的内部簿记和现金管理系统。

出于多种原因,此类系统对安全工程师很重要。首先,它们是核心专业能力。您需要了解交易处理才能解决更广泛的欺诈问题,本章将为您提供路线图。您还需要了解基于簿记的内部控制,因为这些不仅会在出现问题时发出预警,还会推动企业风险管理。您必须能够就 Gramm-Leach-Bliley、Sarbanes-Oxley 和 PCI DSS 进行对话,才能在您的 CFO 中赢得信誉。当你提出保护机制时,你可能首先被问到的问题之一就是它们将如何帮助高管履行对股东的信托责任。

其次,簿记带动了计算机行业。第一台军用和学术界之外的计算机是 Leo,它从 1951 年开始为里昂连锁咖啡屋做簿记。银行业迅速成为计算应用最密集的领域,并通过

1960 年代的簿记自动化。因此,簿记系统的保护具有重要的历史意义和现实意义。它还为我们提供了一个很好理解的保护模型,其中机密性几乎没有作用,但记录的完整性（及其一旦创建后的不变性)至关重要。

银行系统应防止客户相互欺骗或银行;应防止银行职员欺骗银行或其客户;而且它提供的证据应该足够好,以至于他们中没有人可以诬告他人作弊而逃脱惩罚。银行业和簿记业率先使用双重控制,现在也称为多方授权。

第三,交易处理系统　无论是 50 美元的 ATM 取款,还是 1 亿美元的电汇　都是将商业密码学作为军方之外的独立学科推出的应用程序。他们推动了加密算法和协议以及智能卡等支持技术的发展。许多有指导意义的错误首先是在金融密码学领域犯下的（或者至少是公开记录的）。

最后,我们在本世纪建立的许多全球规模的系统都是为了规避在它们所取代的本地和手动系统中已经发展了几个世纪的制衡机制而设计的。谷歌的使命是通过破坏以前对位置、规模、信心和版权的隐式和显式控制,使世界上所有的信息都可用。优步计划通过规避全球数千个城镇的出租车法规,成为全球出租车公司。毫不奇怪,无论是在欺诈和滥用的压力下,还是在立法者的压力下,一家成功的初创公司往往不得不重新制定控制措施。

在本章中,我将首先描述用于跟踪资产和管理腐败员工风险的记账系统;其他任何规模的公司也使用此类会计系统。然后我将描述用于银行间支付的国际资金转移系统。接下来,我将介绍 ATM 系统,它是银行业的公众形象,其技术也被用于公用事业仪表等应用。接下来我将讲述信用卡的故事,它已成为主要的在线支付机制。然后我将继续介绍最近的技术进步,包括非接触式支付、电话支付和开放式银行业务。

12.2 簿记系统

簿记似乎是在公元前 8500 年左右在中东发明的,紧随农业 [1663 年] 之后。当人们开始生产剩余的食物时,他们就开始储存和交易。突然,他们需要一种方法来跟踪哪个村民在公共仓库里放了什么。首先,每个单位的食物（羊、小麦、油……)都由一个粘土标记或布拉表示,它被放在一个粘土信封里,用仓库管理员的图案滚动密封,然后在窑里烤。当农夫想要取回他的食物时,饲养员在目击者在场的情况下打开了封条。　(这可能是已知最古老的安全协议。)到公元前 3000 年左右,这导致了书写 [1515] 的发明;又过了一千年,我们发现了期票、提单等等价物。大约在

同时,金属锭开始用作中间商品,通常由化验师密封在大泡中。公元前 700 年,莉迪亚国王克罗伊索斯开始直接冲压金属,从而发明了硬币 [1551]。到了伯里克利的雅典,一些富有的人开始从事银行家业务 [772]。

图 12.1：- 粘土信封及其内容代表 7 罐油,来自乌鲁克,今伊拉克,ca。公元前 3300 年（由 Denise Schmandt-Besserat 和卢浮宫博物馆提供）

下一个重大创新可以追溯到中世纪。随着黑暗时代的结束和贸易开始增长,一些企业变得太大,一个家族无法管理。最早的公认的现代银行可以追溯到这一时期;通过在许多城市设有分支机构,他们可以为贸易融资。

但是,如果公司的发展超出了所有者家族的直接监管能力,他们就必须从外部聘请管理人员。为控制欺诈风险而发展起来的机制是复式簿记。历史学家发现了 12 世纪开罗的犹太商人创建的复式记账记录 [1691],尽管有关该主题的第一本书直到 1494 年才出现 [522]。

12.2.1 复式簿记

复式簿记背后的想法很简单:每笔交易都记入两本不同的账簿,一本记为贷方,另一本记为借记。例如,当一家公司向客户赊销价值 100 美元的商品时,它会在销售账户中记入 100 美元的贷方,并在应收账款账户中记入 100 美元的借方。当客户付款时,将贷记应收账款账户（从而减少“应收款项”的资产）,并借记现金账户。（会计学校教授的原则是“借方为收款人,贷方为贷方”。）

在一天结束时,账簿应该平衡,即加起来为零;资产和负债应该相等。在除了最小的公司之外的所有公司中,书籍

由不同的文员保管。

我们安排事情以便每个分支都可以单独平衡。每个收银员都会平衡他们的现金托盘,然后将其锁在保险库中过夜;现金分类帐中的借方应该恰好平衡他们收集的实物纸币。所以大部分舞弊需要两人或多人串通,而这种分担责任原则,也称为双重控制或多方授权（MPA）,辅以审计。年终不仅要审计账簿,还要抽查;检查员可能会在没有通知的情况下突然来到一个分支机构,并坚持在员工回家之前平衡所有的账簿。

技术于 1879 年问世,当时俄亥俄州代顿市的詹姆斯·里蒂 (James Ritty) 的“清廉收银员”专利推出了带有铃铛和纸带的收银机。 Ritty 是一名酒馆老板,他的员工偷了他的钱。他将自己的专利卖给了约翰·H·帕特森 (John H. Patterson),后者创立了国家收银机公司,该公司不仅成为银行和簿记设备的领先供应商,还剥离了 IBM,后者一直主导着计算机行业,直到 1990 年代微软取代了它。

12.2.2 银行簿记

银行是较早采用计算机进行簿记的人。从 20 世纪 50 年代末和 1960 年代初的支票处理等应用程序开始,他们发现即使是当时速度慢且昂贵的计算机也比文员大军便宜得多。 1960 年代,银行开始向企业客户提供自动化薪资服务。 ATM 机在 1970 年代大量出现,第一个在线银行系统出现在 1980 年代;基于网络的银行业务随后出现在 1990 年代。

然而,今天灵活的在线系统仍然依赖于传统的后台自动化。

美国、欧洲和大多数发达国家的法律不仅要求银行而且所有上市公司都必须有有效的内部控制,并要求高管对其负责。这些法律是信息安全机制投资的主要驱动力。用于簿记的计算机系统通常声称可以实现复式记账主题的变体,但质量参差不齐。职责分离功能可能只是用户界面中的一个表皮,而底层数据对技术人员开放以供操作 。例如,如果分类账都只是一个数据库的视图,那么具有物理访问权限和数据库编辑工具的人可能会绕过控制。 Sta 也可能会注意到漏洞并加以利用。例如,一家银行不审核地址更改,直到收银员发现他可以更改客户的地址,发行额外的银行卡,然后再将其更改回来[54]。所以我们需要研究机制,而银行业是自然而然的起点。

传统的核心银行系统有许多数据结构:一个账户主文件,其中包含每个客户的当前余额以及过去大约 90 天的交易记录;一些分类账,通过系统跟踪现金和其他资产;从提款机、柜员站、商户终端等收到但尚未过账到分类账的各种交易日志;以及记录谁在何时何地做了什么的审计追踪。使用的系统

英国大型银行自上个世纪以来基本没有变化,但增加了一些外围设备,尤其是电话银行业务1。

核心银行软件会将日记帐中的交易应用到各种分类账和账户主文件中。因此,当客户走进一家分行并向他们的储蓄账户支付 100 美元时,出纳员将进行一项交易,将 100 美元记入客户的储蓄账户,同时将相同金额记入现金分类账,记录抽屉中的金额.

传统上,这是在批处理过程中连夜完成的,但越来越多地涉及实时在线处理,因此事情可能会更快出错。所有分类账总和应始终为零这一事实提供了重要的检查。如果银行（或其分支机构之一)失衡,警报将关闭 ,一些处理将停止,检查员将开始寻找原因。因此,想要增加自己账户余额的程序员必须从其他账户取钱,而不是通过调整账户主文件凭空创建。正如传统企业有不同的分类账由不同的文员管理,因此银行数据处理部门将有不同的开发团队负责不同的子系统。

此外,所有代码都要经过内部审计员的审查,并由单独的测试部门进行测试。一旦获得批准,它将在没有开发环境但只有批准的目标代码和数据的生产机器上运行。 （与编写它的开发人员不同的团队运行生产系统的原则现在在 DevOps 的新世界中受到压力。）

12.2.3 Clark-Wilson 安全策略模型

尽管此类系统自 1960 年代以来已经发展,但其安全策略的正式模型仅在 1987 年由 Dave Clark 和 Dave Wilson（前者是计算机科学家,后者是会计师)[436] 引入。在这个模型中,一些数据项受到限制,因此它们只能由一组特定的转换过程进行操作。

更正式地说,有一些特殊的程序可以输入数据 从不受约束的数据项或 UDI 转换为受约束的数据项或 CDI;完整性验证程序 (IVP),用于检查任何 CDI 的有效性（例如,账面余额）;和转换程序（TP）,在银行案例中可以将其视为保持平衡的交易。在一般情况下,它们维护 CDI 的完整性。他们还将足够的信息写入仅附加 CDI（审计跟踪)以重建交易。访问控制是通过三元组（主题、TP、CDI)实现的,它们的结构使得多方授权策略得以实施。在[47]的公式中:

1. 系统将有一个 IVP,用于验证任何 CDI 的完整性;

1如今大多数零售银行交易都是通过电话查询余额,通常由从核心系统获取定期更新的前端处理。这最大限度地减少了核心系统的负载,也最大限度地减少了当它出现故障时的投诉。

2. 将 TP 应用于任何 CDI 必须保持其完整性；

3、一个CDI只能被一个TP改变；

4. 受试者只能在特定的CDI上发起特定的TP；

5. 三元组必须对主题执行适当的职责分离策略；

6. UDI上的某些特殊TP可以产生CDI作为输出；

7. TP的每次应用都必须引起足够的信息来重构它
写入特殊的仅附加 CDI；

8. 系统必须验证尝试启动 TP 的主体；

9.系统必须只让特殊主体（即安全人员)进行
授权相关列表的更改。

许多事情值得一说。首先，与 Bell-LaPadula 不同，Clark Wilson 模型涉及维护状态。除了审计跟踪之外，这对于双重控制通常是必要的，因为您必须跟踪哪些交易已被部分批准 例如那些仅由一名经理批准并等待一秒钟签字的交易。

其次，模型并不能解决所有问题。它抓住了状态转换应该保持不变量（例如平衡)的想法，而不是状态转换应该是正确的。这种模式不会阻止您将现金存入错误的银行账户。

第三，难题仍然存在，即：我们如何控制来自不诚实员工的风险 ？规则 5 说必须支持“适当的职责分离政策”，但没有说明这意味着什么。事实上，很难在会计文献中找到任何关于如何设计内部控制的系统讨论。

在实践中发生的情况是，四大会计师事务所有一份他们向审计客户推送的控制清单 一家典型的公司可能有一份清单，其中包含大约 300 项必须维护的内部控制，具体取决于它所在的行业。这些为了应对事件、恐惧和监管要求，列表会越来越长。许多控制是正式的合规性而非真正的风险降低，有些实际上是有害的。我在 3.4.4.3 节中讨论了四大审计师如何在 1990 年代抓住 NIST 的建议让人们每月更改密码；在撰写本文时（2020 年），他们仍在推动审计客户这样做。然而，面对证据，NIST 多年前撤回了它的建议，英国的 GCHQ 也建议公司不要使用过期密码。

有原则的内部控制方法是可能的，而且确实是可取的。
在下一节中，我将尝试提炼在银行业和咨询业的采煤工作面以及最近在大学治理方面的工作经验。

12.2.4 设计内部控制

多年来，会计行业、立法者和银行业监管机构推动了各种簿记和内部控制标准

器。在美国,有发起组织委员会 (COSO),一组会计和审计机构 [461]。然而,自我监管未能阻止互联网时代的过度行为,在安然公司倒闭后,美国立法者以 2002 年萨班斯 - 奥克斯利法案 (SOX) 的形式进行了干预。SOX 监管所有美国上市公司,使得负责财务报告的准确性和完整性的高级管理人员,其真实性必须由 CEO 证明;保护举报人,他们是内部欺诈信息的主要来源;并让管理人员负责维护“适当的财务报告内部控制结构和程序”。它还要求审计师披露任何“重大缺陷”。

SOX 的大部分合规成本被认为来自内部控制。早些时候,1999 年的 Gramm-Leach-Bliley 法案 (GLBA) 在许多方面放宽了银行监管,但要求银行拥有安全机制来保护信息免受可预见的安全性和完整性威胁。连同医疗领域的 HIPAA 和我将在第 12.5.2 节稍后讨论的 PCI DSS,GLBA 和 SOX 推动了信息安全和内部控制方面的大量投资。这些法规有助于巩固四大会计师事务所对公司内部控制政策的影响力。

在本节中,我们的重点是技术方面。现代风险管理系统通常要求公司识别和评估其风险,然后建立控制措施以减轻风险。公司通常会有一个风险登记册,其中包含许多页面的主要风险项目,例如“由于内部人员未经授权进行大量银行交易而导致营运资金损失”(我将在第 27.2 节中对此进行更详细的讨论)。其中一些将通过保险等非技术措施得到缓解,但所有这些风险都应该在高级管理人员中有一个风险负责人,其中一些风险最终将由 CIO 负责2

审计员的工作将由国际审计和保险标准委员会的“国际审计标准 315”[950] 推动。 ISA 315 侧重于组织账目中由于错误或欺诈导致的重大错报风险。审计师应该了解企业及其内部控制系统;他们将识别重要账户(如现金)、每个账户的重要断言(如存在)和影响它们的重要业务流程(如销售),以及这些流程包含的控制。然后,他们会考虑每个断言可能是错误的风险以及风险是否重大。那么你如何设计适当的控制?最新版本的 ISA 315 对此有相当多的页面,但它们大多有些笼统3,因此它们的解释通常取决于会计师事务所。

正如我们将在第 3 部分中讨论的那样,有两种基本方法可以确保安全性免受错误影响和安全性抵御攻击。您可以自上而下地工作,从您不希望发生的坏事列表开始,例如“大量未经授权的电汇”,然后列举可能的原因并确定控制措施以减轻风险;或者您可以自下而上地工作,从可能失败的事情开始,例如“一名员工被勒索”,找出可能造成的伤害,然后再次确定适当的控制措施。你可能经常需要

2 有关英国银行风险治理的描述,请参阅金融行为监管局的
报告 2016 年针对 Tesco 银行的欺诈 [687],我将在第 12.6.3 节中对此进行讨论。
3 参见第 A6、A123–181、A198、A224–229 段和附录 3 第 15–24 段

使用这两种方法。在支持审计时,您需要注意财务报表所依赖的认定的风险。但是,您不能忽视可能影响公司运营能力的其他风险,例如数据中心的损失。内部控制不会是您安全状况的全部。

确定了需要通过职责分离来缓解的风险后,您可以通过两种方式做到这一点:双重控制(也称为多方授权)和功能分离。

在双重控制中,两个或多个委托人共同行动以授权交易。典型的军事例子是核指挥系统,这可能需要两个军官在控制台中同时转动他们的钥匙,而控制台中的任何一个都相距太远而无法触及两个锁(我将在第 15.4 节中详细讨论)。

典型的民用例子是银行开具保函,如果另一家银行的贷款出现问题,保函可以承担损失。

担保特别容易发生欺诈。如果您可以让 A 银行为您从 B 银行贷款给您的企业提供担保,那么 B 银行将监管您的账户,而 A 银行的资金将面临风险。拥有伪造或腐败担保的骗子可以慢慢地掠夺 B 银行的贷款账户,只有当他们违约并且 B 银行向 A 银行要钱时才会发出警报。您不希望单个经理能够发行这样的工具4。

通过职责的职能分离,两个或更多的工作人员以互补的方式处理交易。典型的例子是企业采购。直线经理做出采购决定并告知采购部门;那里的职员提出了采购订单;店员记录货物到达;发票到达账户;会计人员将其与采购订单和商店收据相关联并开出支票;客户经理在支票上签字。

然而,它并不止于此。直线经理现在在该内部账户的月度报表中记入借方,他们的老板审查账户以确保可能实现部门的利润目标,内部审计部门可以随时下班审计部门的账簿,并且当外部审计员每年进来一次时,他们将检查随机选择的部门样本的账簿。最后,当发现欺诈行为时,公司的律师可能会竭尽全力收回资金。

该模型可以概括为预防-检测-恢复。对这三个分支中每一个的依赖将取决于应用程序。如果检测可能会延迟,因此恢复可能会很困难 就像腐败的银行担保 你会付出额外的努力来预防,也许使用双重控制。在预防困难的地方,你可以让检测足够快,恢复足够有力,以提供威慑力。这里最经典的例子就是银行的收银员很容易拿走现金,所以你每天在他们回家之前数一下钱。

基于簿记的管理控制不仅是最早的安全系统之一;它催生了大量的管理科学和民法。

4如今,问题不仅仅是两位经理是否会串通一气,或者其中一位冒充另一位,而是恶意软件是否可能接管他们的两个帐户。我将在 12.3.3 节中进一步讨论这个问题。

当角色是现有业务流程的补充部分时,控制最有效,并且一些流程已经发展了几个世纪以支持它们。控制不仅与这些过程交织在一起,而且存在于公司的文化背景中。在瑞士银行,几乎所有东西都有两个经理的签名,而美国人则宽松得多。在大多数国家/地区的银行中,员工可以从一项任务随机转移到另一项任务,并被迫休一周甚至两周的假期,没有电脑或建筑物访问权限,至少每年一次。这在大学里是不可接受的 但在学术界,可以偷的东西要少得多。

设计内部控制系统是高度跨学科的。财务总监、人事部门、律师、审计人员和系统人员都从不同的方向来解决问题,提供部分解决方案,无法理解彼此的控制目标,事情就这样水落石出中间。人为因素常常被忽视,当乐于助人的下属或专制经理规避控制以完成工作时,系统最终会变得脆弱。将控件与文化相匹配并激励人们使用它们很重要;经营较好的银行向员工出售管理控制权,作为保护他们免受勒索和绑架的手段。正如我们在第 3 章中提到的,组织中的员工只有这么多的合规预算 他们只准备花费这么多的时间和精力来执行妨碍安全的仪式。在其目的被遗忘或变得无关紧要之后,成为仪式的控制也可能会被实施多年。你必须了解所有这些,并明智地使用合规预算来实现文化上可行的效果。亲密同事之间缺乏信任的文化尤其难以维持(这也是跨业务部门划分职能控制可能更有效的另一个原因)。

正如您将尝试要求多个银行家批准一笔大额交易一样,您可能希望要求多个工程师批准代码在实时系统上运行。但由于多种原因,这很难彻底做到。首先,许多接口提供单点故障。二是分责制管理过于繁琐。您可以小心地使其可审计 5。第三,双重控制通常需要持久状态,这与程序员希望通过使事务原子化来使事情简单化的愿望相矛盾。由于需要管理该状态,因此总会有一些受信任的系统管理员需要完全访问权限才能完成工作。第四,随着公司转向将开发和运营集成为 DevOps,然后添加安全性使其成为 DevSecOps,他们最终可能会拥有更值得信赖的员工。至少,随着越来越多的信任转移到源代码审查阶段,信任的位置可能会发生变化。第五,有突发事件。 ATM 系统在周末出现故障,ATM 团队的值班工程师从家里访问实时系统以修复错误。您记录此类访问并让您的审计员盯着日志,就像系统管理员一样。最后,你的顶级工程师不可避免地会比你的审计师知识渊博得多,如果他们真的想做坏事,他们也可以做坏事。

所以总有工程师可以进行欺诈。系统管理员可能

5 旧式银行系统建立在 IBM 操作系统 MVS 之上,它可以让系统管理员做任何事情,除了查明审计员正在监控他们的哪些活动 [224]。

创建两个影子用户,他们之间授权大额支付,或者支付系统维护者可能会将额外的支付放入队列中。他们被抓到的地方是平衡控制在一两天后发出警报,而他们汇款到的银行的洗钱控制使他们无法逃脱。我将在 12.3.3 节中进一步讨论这个问题。重要的是,预防 - 检测 - 恢复模型中的功能控制通常比共享控制更重要,因为它们将专有技术和访问权分开。但要使功能分离发挥作用,需要将这些机制设计到应用程序中,因此它们可能是专有的、晦涩难懂的,而且与操作系统自带的机制相比,测试得不够充分。您可以分离多少知识是有限的。有些人必须了解这一切,例如安全架构师和首席审计师。

同样的分析也适用于业务流程本身。有些人最终不得不快速做出高价值的决定,并且必须了解交易的所有方面。在一家真正的银行,你可能会发现三十或四十个你必须信任的人 首席执行官、首席交易员、高级系统管理员和其他一些人。重要的是要知道他们是谁,尽量减少他们的数量,给他们高薪,并谨慎地观察他们。

关于双重控制的最后一点是,它在组织界面上变得脆弱。一个例子是加利福尼亚州的银行在安装了新的处理设备后突然开始忽略支票有两个签名的请求 [1621]。一些组织不愿意向竞争对手展示谁是值得信赖的签约人以及签约金额。然后是争议解决:“我的两位经理说钱已经寄出!” “但我的两个人说不是!”

12.2.5 出了什么问题

盗窃和欺诈可以采取多种形式。一般公司的大多数盗窃都是内部人员造成的,而自动化似乎正在使此类事件变得越来越少且规模越来越大。

12.2.5.1 内部欺诈

当大多数银行家在分行工作时,英语世界的银行每年解雇大约 1% 的员工 。典型的犯罪行为是轻微的挪用公款,造成几千美元的损失。没有人找到一种有效的方法来预测哪个 sta 会变坏;以前忠诚的员工可能会因离婚等冲击而离职,或者被任命为他们无法忍受的新经理。

每年损失几百名出纳员只是做生意的成本。现在大多数员工都在呼叫中心工作,这些数字正在下降;他们打交道的客户是随机分配给他们的,所以很难与朋友勾结。

现在员工也更难出售客户的个人信息,因为员工必须引导客户完成安全问题才能访问他们的记录。经营良好的银行的工作人员通常被禁止将电话甚至笔和纸带入呼叫中心,这样他们就不会将数据泄露给任何外部人员

规模6。

著名的内幕案例包括：

- 英国最近最大的银行诈骗案是由格拉斯哥东区的黑帮 Feezan Hameed 制止的。 “Fizzy”在 2016 年因在 2013-15 年间从英国劳埃德银行的商业客户那里窃取至少 1.13 亿英镑而被判刑 11 年，其中仅追回 4700 万英镑7。他颠覆了两名发现目标公司的员工 通常是账户中超过 100 万英镑的中型公司。Fizzy 然后会打电话给企业主或财务总监，声称来自银行，通过阅读他们最近的几笔交易来“验证”自己，并要求他们通过计算他们的授权码来“验证”自己。第二因素设备。在他这样做之前，他会以他们的身份登录并设置一批五位数的大笔付款。他从受害者那里得到的代码将释放批次 [820]。

- HSBC 的一名密码重置职员与不明身份的人合谋更改 AT&T 用于访问其在 HSBC 的银行账户的密码。新密码用于向离岸公司转移超过 2000 万美元，但未从中恢复。店员是一个脆弱的年轻人，在内部考试失败后被聘为重置密码；法院宽恕了他，他获刑五年 [1569]。

  据称，一名 AT&T 员工密谋掩盖交易，但这位先生被判无罪。

- 2010 年代一个快速增长的银行欺诈涉及中型公司的鱼叉式网络钓鱼账户员工，并接管了几个员工账户。拥有两个文员的个人电脑比收买两个文员要简单，而且如果一个公司的个人电脑都具有相同的配置和更新状态，这可能不会太难。由于银行可能会特别注意大额交易，因此游戏通常是在公司通知之前支付大量四位数的款项。在美国，第二天没有注意到欺诈性付款的公司通常得不到补救。一次典型的攻击可能会净赚 50 万。

12.2.6 行政舞弊

所有著名的大型金融诈骗案 九位数及以上 都涉及高级内部人士。巴林银行的倒闭就是一个很好的例子：经理们未能控制流氓交易员尼克李森，他们被表面上交易利润所带来的奖金的贪婪蒙蔽了双眼。其他例子包括股权融资丑闻，其中一家保险公司的管理层在其计算机系统上创建了数千名假人，为他们投保，并将保单出售给再保险公司；以及罗伯特·麦克斯韦 (Robert Maxwell) 掠夺英国《每日镜报》(Daily Mirror) 报纸养老基金的事件。受害人的高管严重疏忽，如

6此类 opsec 规则使呼叫中心更难让员工在家工作在 Covid 大流行期间。

7全面披露：我作为其中一家受害公司的专家证人，我们不得不威胁要起诉劳埃德银行要回我们的钱。

Barings 的案例,或者是肇事者,例如 Equity Funding 和 Maxwell。
这些模式重复;例如,富国银行在 2020 年因在客户不知情的情况下开设数百万个账户而被罚款 30 亿美元,就像在股权融资案中一样 [699]。

经济学家和会计学教授将此类问题分析为代理问题:委托人 A 聘请代理人 B 管理资产,并想知道如何监控和评估 B 的绩效。无论委托人是银行的首席执行官,代理人是打算实施欺诈的经理,同样的原则也适用;或者委托人是否由股东组成,代理人是首席执行官。从理论上讲,内部控制和内部审计部门是首席执行官用来跟踪更多基层员工的工具,而外部审计师是股东用来跟踪首席执行官和高级管理人员的工具。

这就是理论。 Alexander Dyck、Adair Morse 和 Luigi Zingales 在对 1996 年至 2004 年间针对上市美国公司的 230 起公司欺诈案件的调查中分析了这种做法 [596]。在萨班斯-奥克斯利法案之前,只有少数欺诈行为被授权发现它们的人揭露:14% 由审计师和 6% 由 SEC 揭露。大多数是由具有其他激励措施的行为者发现的:19% 由员工发现,16% 由行业监管机构发现,14% 由金融分析师发现,14% 由媒体发现。证券交易所监管机构、商业银行和保险承销商以完全缺席而著称。在萨班斯-奥克斯利法案之后,强制执行者的表现略有改善,但仍略高于总数的一半。他们对激励的分析表明,具有最强举报动机的行为者(例如卖空者)最不活跃,而最活跃的员工通常有负面激励,因为他们被解雇了。这表明主导因素是谁真正知道发生了什么。其次,奖励促进披露:除了萨班斯-奥克斯利法案的影响,许多政府行为者(如税务人员)奖励举报人,具有积极的影响。

理论上,外部审计师由董事会的审计委员会任命,该委员会由一名外部董事担任主席;但谁任命外部董事?根据我的经验,外部董事往往与 CEO 友好,而审计师则不遗余力地与 CFO 闲聊8。他们提供廉价的审计服务让他们踏入大门,并从咨询中赚取真金白银;几十年来,这是一个结构性问题,最终在 2020 年 2 月,英国财务报告委员会下令将审计和咨询分开 [1049]。大型审计公司通过推销他们自己最喜欢的控制列表而不顾客户的实际风险,对信息安全世界产生了有害影响。他们通过吹毛求疵和服从来最大化他们的收入; Sarbanes-Oxley 法规使美国上市公司平均每年花费超过 1 美元的审计费用。

除了纯粹的经济激励之外,老板们发现很难应对高级同事无能或不诚实的证据。有很多关于信息回避的文献,我在第 3.2.4 节中提到过:人们不愿意学习会导致他们痛苦、压力或额外的事情

8 安然公司倒闭后的法律内斗摧毁了其审计师亚瑟安德森,将“五大”审计公司减少为“四大”;现在,审计员竭尽全力避免对欺诈承担责任。

工作。而管理者不愿面对的风险,往往是他们无法控制的。巴林银行的任何人都不想认为他们的明星交易员尼克·利森可能是个骗子;流行音乐去了银行。技术无法减轻此类风险;如果有的话,他们可能正在成长。

12.2.6.1 Post Oce 案例

高管们也可能不愿意相信他们的会计系统可能出现任何系统性错误。即使他们怀疑,也有一种社会反应是在批评下团结起来,律师可能会建议客户否认一切。

这里值得研究的案例是英国 Post Oce 会计系统的失败。 Post Oce 不仅运送信件,而且还是一家重要的金融机构,其大部分分支机构都由副邮政局长经营 通常是在其经营场所设有专营 Post Oce 柜台的店主。为了控制它们,Post Oce 建立了一个名为 Horizon 的会计系统,该系统存在多个错误,导致许多特许经营商被收取他们不欠的钱。成千上万的人的生活被毁了;有些人失去了生意并破产了,有些人被错误地解雇了,还有一些人因为他们没有犯下的欺诈行为而入狱。最终 587 名副邮政局长起诉了 Post Oce,并于 2019 年 12 月赢得了道歉和 5800 万英镑。法官发现 Horizon“远不是稳健的”[185]。

据我所知,这是第一个也是唯一一个会计系统在激进诉讼中受到适当考验的案例。许多法律体系假定会计系统正常运行,除非有人可以提供相反的证据,而这可能很难:很多法律努力都是为了迫使邮政局让索赔人访问软件及其软件文档,以便他们的专家可以对其进行检查。顺便说一句,特许经营商的总损失似乎在数亿美元左右;他们可能会获得 5800 万英镑和解协议中的 1100 万英镑,其余部分将交给律师和为诉讼提供资金的对冲基金。Post Oce 的大多数员工都减薪了,而 CEO Paula Vennels,一位受命的部长,得到了大幅加薪 [354]。她最终离开了。软件供应商富士通可能最终会支付和解费用,但这可能需要进一步的诉讼。

12.2.6.2 其他故障

大多数会计系统失灵并不那么引人注目,但也有许多失灵对金融和其他公司的运营能力产生重大影响。

我们将在本章处理支付以及后面章节的其他应用程序时看到更多示例,但这里是一个开始示例。

1. 随着时间的推移,计算机系统变得越来越复杂,它们积累了一些杂物,使它们变得更加脆弱和难以维护。软件工程师将此称为技术债务:这意味着更改变得更慢且成本更高,并且从故障中恢复可能很复杂 [41]。簿记系统也不例外。例如,2012 年 6 月,650 万

Natwest Bank 的客户在软件升级出错后不得不恢复数周的服务。人们身无分文滞留在海外，一些公司发不出工资。该银行被罚款 4200 万英镑 [686]；由于它在 2008 年的崩盘中破产，当时它主要归英国政府所有。如果服务故障再持续一周，它很可能会再次破产，让纳税人损失数百亿美元并造成广泛的破坏。因此，对关闭货币中心银行的灾难性失败的恐惧是真实存在的。但是，用一个新系统替换一个笨拙的旧核心银行系统是一项需要数年时间、耗资九位数的重大项目，它本身也存在战略风险。

作为一个年轻人，我参与了几个这样的项目：他们有他们的紧张时刻。

2. 我们在食物链的下游发现了类似的项目风险。我们大学的会计系统在 2000 年代初被更换，一个本应耗资 300 万英镑的项目却花费了 1100 万英镑。我们最终起诉了安装它的会计师事务所，并发布了一份详细的错误报告 [691]。

3. 多年后，该系统仍然难以使用，原因可能令人感兴趣。在我们大学，35 名财务人员在财务系统设计方面的发言权超过 1,500 名教授。职员更关心，因为他们一直在使用它，而我们教授可能每周使用一两个小时。文员节省的时间少于教授浪费的时间，但集中的兴趣通常会获胜。

因此，即使您的簿记系统使用标准核心来强制执行平衡和完整性的基本 Clark-Wilson 属性，仍有很多工作要做
错误的。

12.2.6.3 生态有效性

仅仅检查书籍内部是否一致是不够的。您还需要检查它们是否符合外部现实。影响现代审计要求和实践的一系列丑闻始于 1938 年 McKesson and Robbins 的倒闭，这家著名的药物和化学公司报告的资产为 1 亿美元9。事实证明，记录的资产和库存的 20%不存在。总裁菲利普·穆西卡 (Philip Musica) 原来是一名走私犯，之前有欺诈罪。他与他的三个兄弟一起，利用虚假的外国毒品业务夸大了公司的数字，涉及一家虚假的货运代理和一家虚假的蒙特利尔银行。审计员在没有询问公司老板的情况下接受了 McKesson 的账目；他们没有检查库存，没有与客户核实应收账款，也没有考虑公司内部的职责分离 [1616]。

下一代的著名案例是 1963 年的色拉油丑闻，涉及联合原油精炼公司的破产以及罗伯特·肯尼迪 (Robert F. Kennedy) 对其首席执行官蒂诺·德·安吉利斯 (Tino de Angelis) 的起诉。联合公司从美国运通公司和其他公司借了几百万美元的大豆油作抵押

9 2020 年约为 18 亿美元

实际上主要是水,并用它来进行大量的期货交易 [1442]。
美国运通公司的股票在举报人告诉它欺诈后下跌了 50%;它损失了 5800 万美元。 （沃伦·布伊特随后购买了该公司 5% 的股份并发了大财。）

所有大公司都必须接受审计的要求使审计公司卷入了每一次重大的财务丑闻。我已经提到了安然,它在 2001 年的失败导致了萨班斯-奥克斯利法案的出台,然后在 2008 年发生了金融危机,部分原因是交易复杂的金融衍生品,而这些金融衍生品最终证明是基于近乎一文不值的抵押贷款。目前为某些支付和簿记应用程序推广的区块链系统的一个问题是,虽然数学结构可以保证一致性和共识,但没有任何关于所提及的资产是否可靠甚至存在的信息。因此,当您看到一家银行谈论区块链来登记抵押贷款时,您可能会有些怀疑,智能合约将允许金融创新。我将在 20.7 节中回到这个问题。

本书于 2020 年 7 月付印时,最近的丑闻是 Wire card。作为一家支付服务公司,它已经开始处理向色情网站、在线赌场和其他普通银行不会接触的商家的卡支付。它迅速成长,取代了 Dax 30 中的德国商业银行德国 30 家最大上市公司的指数,并在德国被誉为能够挑战硅谷的罕见本土公司。但在 2020 年 6 月,当它试图收购德意志银行（德国最大的银行,市值约 200 亿美元)时,Wirecard 的审计师安永透露,其声称资产的四分之一,据称在菲律宾持有,约 21 亿欧元,找不到。

（安永三年来未能与其银行家核实其银行报表,而是依靠公司自己提供的“屏幕截图” [1834]。)该公司申请破产,其首席执行官马库斯布劳恩被捕。一系列使用它来处理支付的金融科技初创公司停止了交易,导致德国境内外的数百万持卡人无法取款。然而,早在 2008 年 [1256],投资者和监管机构就忽略了无数危险信号。更糟糕的是,当英国《金融时报》在 2019 年发表了对 Wirecard 可疑会计做法的分析时 指出其迪拜子公司似乎没有客户,一家所谓的菲律宾子公司的地址是一家小型巴士公司,另一家是一名退休海员,其新加坡子公司的举报人报告说他们被命令伪造账目 [1283] 德国监管机构 BaFin 的回应不是调查该公司,而是开始对记者进行刑事调查并禁止卖空公司股份[610]。多年来,BaFin 一直在为公司辩护而不是调查他们的批评。这是欧洲历史上最大的欺诈案之一,摧毁了超过 200 亿欧元的表观股东价值以及公众对德国金融监管的信心。在途中,Wirecard 收购了 Moodys、Credit Suisse 和 Softbank 等公司。令人惊讶的是,麦克森和罗宾斯的教训竟没有受到重视;检查海外现金余额确实应该是审计 101. 然而,审计行业存在持续存在的结构性问题,从审计师向首席财务官推销产品到几乎所有工作都由初级人员完成的事实 [703]。

12.2.6.4 控制调整和公司治理

内部控制结构往往保守、昂贵和无效的主要原因是,虽然理论上组织根据经验制定它们,但在实践中,这种经验是通过审计师卡特尔传递的。从理论上讲,这背后有一些治理。 [?] 中对内部审计标准进行了调查;最具影响力的是发起组织委员会 (COSO) 的风险管理框架,该委员会是一组美国会计和审计机构 [461]。这是判断您的系统是否用于美国公共部门或被在美国股票市场上报价的公司使用的标准。 COSO 模型不仅针对内部控制,还针对财务报告的可靠性和法律法规的遵守情况。

它的基本过程是一个进化循环:在给定的环境中,您评估风险、设计控制、监控其性能,然后再次循环。 COSO 比硬系统设计问题更强调企业文化的软方面,因此可以将其视为管理和记录系统演进过程的指南。从理论上讲,其核心包括高级管理层检查其控制政策是否正在实施并实现其目标,如果没有,则进行修改。在实践中,审计师已经抓住了它。

管理认证信息系统审计师 (CISA) 考试的信息系统审计与控制协会 (ISACA) 对 COSO 进行了改进,称为信息和相关技术的控制目标 (CobiT),它更加国际化 [946]。它从内部审计的技术方面延伸到人事管理、变更控制和项目管理。更具体的标准来自审计师对特定部门法规的解释,例如美国上市公司的 Sarbanes-Oxley、美国金融部门公司的 Gramm-Leach-Bliley、美国医疗保健提供商的 HIPAA 和居民个人信息的 GDPR欧盟成员国。而且,正如我们在有关银行业务和簿记的章节中指出的那样,PCI 贸易协会制定的标准管理与支付卡相关的数据。还有关于安全管理的 ISO 27001。无论您或您的客户从事何种行业,都值得关注不断发展的网络安全标准。其中许多是标准,因为每个人都可以就它们达成一致,所以它们绝不足够。好吧,每一次重大违规都涉及一家拥有 ISO 27001 认证的公司;审计员说有些事情没问题,但事实并非如此。我们将在 28.2.9 节中回到这个问题。

12.2.7 寻找弱点

如果您曾经负责组织中的安全性,您不应该只考虑哪些组件可能会因故障而导致足够严重的损失,从而对底线产生重大影响。你也需要考虑人,以及他们的外部关系。您的哪些经理可以通过与客户或供应商勾结来欺骗您的公司?分行经理是否可以利用伪造的抵押品向其堂兄经营的不正当企业借钱?他会不会把人寿保险单卖给不存在的人并伪造他们的死亡证明?运营经理可以收受贿赂吗

来自供应商?您的呼叫中心员工是否可以将他们处理过的帐户中的数据出售给网络钓鱼团伙,这些团伙使用这些数据冒充您的公司向您的客户提供服务?很多事情都可能出错。你必须弄清楚其中哪些重要,以及你如何找到答案。记住每年有 1% 的员工陷入诱惑的老经历。请记住,信任的人可能会伤害您。谁可以伤害你,如何伤害你?

这是控制维护者必须不断思考的问题。

要吸取的教训包括以下内容。

- 在不断变化的环境和需求中很难保持有效的控制
  拥有它的高级人士。
- 如果您依靠客户或员工的投诉来提醒您注意欺诈和系统故障,您最好有一个好方法让他们与您联系并让您倾听他们的意见。许多公司通过难以联系来削减成本,但这会产生后果。
- 主要接触的是公司自己的员工和承包商,所以你最好和他们中的足够多的人交谈并问一些问题,比如“如果你想诈骗公司,你会怎么做?”
- 不要只考虑交易和流程,还要考虑人、激励、社会规范和操纵或恐吓他人的权力。

  你是否期望人们在没有任何激励机制的情况下保持彼此诚实,除了举报者的风险之外别无他法?

- 没有安全策略可以实现完全合规,因为变通办法将
  人们应对现实生活所需要的。
- 这些变通办法自然会产生漏洞,因此您最好设计
  人们可以遵守的控制。
- 你最好与公司的执行领导建立工作关系,这样你就可以了解他们中的哪些人可能会承担与你的职责相关的风险,这样他们也可以了解你在做什么。

总会有残余风险。管理这些残余风险仍然是最困难和最被忽视的工作之一。采用某些特定系统是万无一失的学说是一个极其糟糕的主意 因为如果你将其失败的先验概率指定为零,那么证据就不会改变它,当它最终失败时,事情可能会变得很糟糕。更一般地说,你需要帮助公司从经验中学习。经验不仅仅意味着损失历史:需要识别和改进阻碍的控制。如果您被视为对利润的贡献,而不仅仅是另一种合规负担,那么您会被更多人倾听。例如,如果您可以修复密码重置功能以减少需要的员工 ,或改进欺诈引擎以减少公司网站拒绝购物篮的次数,董事会将更容易听取您的意见。

最后,您的风险管理系统将不得不对一种或多种合规制度表示敬意,具体取决于行业。一些行业使用国际安全管理标准ISO 27001:它要求你系统地分析风险,将不可接受的风险纳入其中。

某种形式的风险处理（控制、规避、转移）；并有一个管理流程来确保控制得到更新。在许多公司中，无论如何，这将由您的审计师推动。并且有许多特定于行业的监管制度需要处理。在医疗保健领域，您必须担心 HIPAA（请参阅第 10.4 节）；至于银行业务和支付，我们接下来会谈到这一点。

12.3 银行间支付系统

当人们想到电子欺诈时，他们通常会想到一个好莱坞场景，其中狡猾的俄罗斯黑客破解了银行的密码并将数以亿计的美元电汇到避税天堂。转账系统确实是一个犯罪目标，并且已经存在了一个半世纪。我们将首先了解用于银行间转账的系统，然后是银行客户（无论是个人还是商家）使用的系统。

12.3.1 电子商务的电报史

许多人认为电子商务是 20 世纪 90 年代中期发明的东西。
但它可以追溯到更远的地方。

政府使用古典时代的视觉信号，包括日光仪（使用镜子在接收器上闪烁阳光）、信号灯（使用移动手臂的位置来发出字母和数字信号）和旗帜。陆基系统沿着一连串的信标塔发送信息，而海军系统则在船只之间传递信息。拿破仑战争后，法国政府将其日光仪网络开放用于商业用途，很快就发生了第一起欺诈事件。在 1836 年被发现之前的两年时间里，两名银行家贿赂一名接线员，让接线员通过在传输中出现错误，让他们可以从安全距离观察到，从而秘密地向他们发出股票市场走势的信号。还设计了其他技术来表示赛马的结果。博彩公司学会了用时钟“报时”，而不是等待结果并希望他们是第一个听到结果的人。

从 1760 年代到 1840 年代，电报由许多先驱开发，其中最有影响力的是塞缪尔莫尔斯。 1842 年，他说服国会资助一条从华盛顿到巴尔的摩的试验线路。

这给人们留下了深刻的印象，以至于开始了认真的商业投资，到那个十年结束时，已有 20 家公司运营了 12,000 英里的线路。
这在很多方面都类似于 1990 年代后期的互联网繁荣。

银行是第一批大用户，他们发现他们需要一种机制来防止交易在途中被不正当的操作员更改：我在 5.2.4 节中讨论了他们为此目的开发的测试密钥系统。电报也被用来创建全国市场。纽约的商品交易商第一次可以在几分钟内了解芝加哥拍卖会的定价，到达波士顿的渔船船长可以了解格洛斯特的鳕鱼价格。这段时期的历史表明，电子商务的大部分概念和问题都为维多利亚时代的人所熟悉 [1818]。你怎么知道你在和谁说话？你怎么知道他们是否值得信赖？如何

你知道货物是否会送达,付款是否会到账? 19 世纪的答案是值得信赖的中介机构 主要是使用推荐信、担保和信用证帮助企业管理风险的银行。

到 1970 年代,银行家们开始意识到这个有价值的旧维多利亚式系统
应该进行大修了。

首先,正如我之前在 5.2.4 节中提到的,大多数测试密钥系统都容易受到密码分析的攻击;观察大量交易的人可以逐渐计算出关键材料。

二是测试钥匙系统不支持双控。秘密的桌子被保存在一个保险箱里,两个职员会坐在一起制定一个测试并检查它;但是并没有什么可以真正阻止工作人员同时对未经授权的消息进行测试。

第三,真正关心的是成本和错误。使用手动加密意味着每笔交易至少要在键盘上输入 3 次:一次输入支付银行的计算机,然后在电传室打印出一笔交易,然后手动计算测试;然后第二次发电传给收款银行,收款银行人工核对测试;然后第三次,那家银行将其输入他们自己的计算机。错误比欺诈更成问题。付款肯定可以直接从一家银行的计算机流向另一家银行的计算机吗?

12.3.2 斯威夫特

一个银行联盟在 1970 年代成立了环球银行金融电讯协会 (SWIFT),以提供更安全、有效和可控的机制来在成员银行之间发送支付指令。可以将其视为具有内置身份验证和不可否认服务以及可选加密功能的电子邮件系统。它用于每天在世界范围内运送数万亿美元的货物,其设计已被复制到处理许多其他类型资产所有权的系统中,例如证明船舶货物所有权的提单。

设计约束很有趣。银行不希望信任 SWIFT,以至于其员工可以伪造银行交易。真实性机制必须独立于机密性机制,因为当时许多国家(例如法国)禁止民用密码学来保密。不可否认功能不能使用数字签名,因为它们还没有被发明出来。最后,银行必须能够对银行间交易实施可审计的双重控制。

图 12.2 总结了 SWIFT I 的设计。通过在发送银行计算消息验证码 (MAC) 并在接收银行检查它来确保消息的真实性。过去使用双边密钥交换来管理密钥:每当一家银行在海外建立关系时,谈判的高级经理将与他的对方号码交换密钥,无论是在面对面的会议上还是之后通过邮寄到彼此的家庭住址。有两个关键组成部分可以最大限度地降低风险

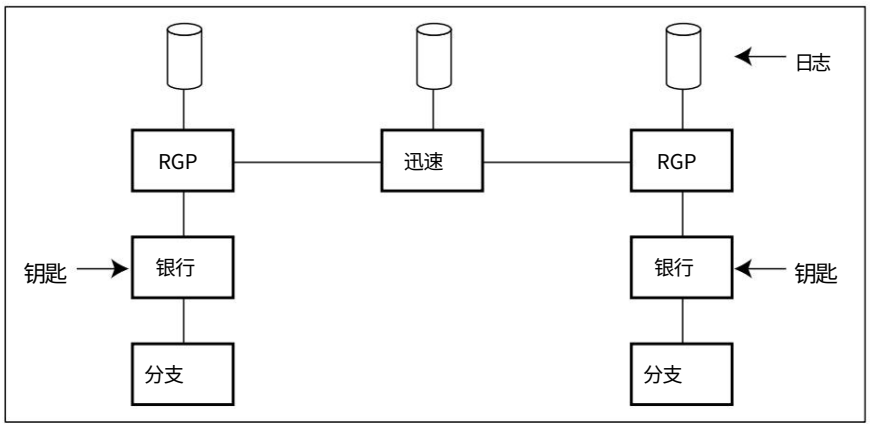

图 12.2：- SWIFT 架构

妥协,每个方向都发送一个（即使犯罪分子在银行经理的邮箱中一端读取了银行经理的邮件,也不太可能在两端都发生）。
直到两家银行都确认对方的密钥已安全接收和安装后,身份验证才会启用。

这样,SWIFT 就没有参与消息认证;只要使用的身份验证算法是可靠的,他们的任何员工都无法伪造交易。身份验证算法本应属于商业机密,但由于银行希望其安全机制成为国际标准,因此人们想出办法查看 ISO 8731 [1631]。很快,一个攻击被发现并发表在 [1545] 中。幸运的是,这次攻击需要超过 100,000 条消息才能恢复密钥　这对于封闭系统的实际攻击来说太大了,这让银行有时间迁移到更现代的机制。

尽管 SWIFT 本身在身份验证方面不受信任,但它确实提供了不可否认服务。每个国家的银行将它们的消息发送到区域通用处理器 (RGP),该处理器记录它们并将它们转发给 SWIFT,SWIFT 也记录它们并通过其所在国家的 RGP 将它们发送给收件人,后者也记录它们。 RGP 通常由不同的服务公司运营。因此,任何希望不诚实地拒绝交易的银行家不仅要破坏当地的 SWIFT 应用程序及其周围的控制,还要破坏不同国家/地区的两个独立承包商。而且日志比密码学更容易让法官理解。

保密性是一个可选的附加组件。它由银行与 RGP 节点之间以及这些节点与主要 SWIFT 处理站点之间的线路加密设备提供。钥匙在租用线路两端的设备之间手持。在保密是非法的国家,这些设备可以在不损害真实性和不可否认机制的情况下被省略 10。

10在一个国家,一家试图安装线路加密器的银行在几个小时后发现线路上出现噪音。这只出现在现场线路上,而不是备用线路上,只是在延迟之后出现,并且在两条线路之间交换设备也无济于事。银行意识到本地间谍不会容忍加密并放弃了。

双重控制由专用终端或可与其他银行系统集成的软件包提供。通常的操作方法是让三个独立的人员进行 SWIFT 交易:一个输入,一个检查,一个授权11。还有一个进一步的功能控制,您可以通过每天对照报表检查交易来核对账户。因此,通过输入控制的虚假支付指令应该会在下一个工作日发出警报。

12.3.3 出了什么问题

SWIFT 我运行了 20 年,没有收到任何针对系统本身的外部欺诈报告。在 20 世纪 90 年代中期,在对 MAC 算法的攻击发布后,通过添加公钥机制对其进行了增强:SWIFT II 仍然使用双边密钥交换,但 MAC 密钥在使用公钥加密的代理银行和 MAC 本身之间共享进一步受数字签名保护。密钥管理机制被纳入 ISO 11166,并且对该体系结构的安全性存在一些争论 [112、1631]。除了采用公钥密码术带来的信任集中化 因为中央认证机构可能错误地证明密钥属于银行,而实际上它不属于银行 至少一个早期部署采用了 512 位公钥由于美国的出口管制,RSA 公钥的使用受到限制,到 2000 年,至少有一个这种长度的 RSA 公钥被一群学生秘密分解 [43]。双边密钥交换在 2009 年被一个新系统所取代,该系统的加密机制是专有的。

消息标准正在被 ISO 20022 取代。

一旦加密货币开始强化并默认提供机密性,就会出现政治争端。 《纽约时报》在 2006 年 6 月披露,美国国家安全局正在访问整个交易流,因此美国国家安全局只是要求访问所有内容。这引起了与注重隐私的欧洲人的对抗,但最终在奥巴马总统接替布什总统之后,欧盟同意了一项条约,根据该条约美国财政部可以向 Swift 发出传票 [341]。欧洲境内的付款据称被排除在外,但由于此类付款是有针对性的,而且埃德·斯诺登 (Ed Snowden) 透露了收集的规模,因此欧洲议会和隐私权当局一再提出这个问题 12。

对银行间系统的犯罪(相对于政府)攻击并未涉及支付机制本身,而是涉及周围的业务流程。银行程序员向处理队列中插入伪造的消息确实时有发生,但通常会失败,因为他不了解业务流程。国际电汇的实际运作方式是银行相互维护账户,因此当银行 A 向银行 B 的客户汇款时,它实际上发送了一条指令“请从我们在您的账户中向该客户支付以下款项”。由于这些帐户

11由于检查器可以修改收款人和金额,这实际上只是双重控制,而不是三重控制 维护接口的程序员总是可以在那里攻击系统,除非你也可以在系统端保持职责分离。

12有人可能会问,为什么银行不只是构建具有端到端加密的新系统,而是银行监管机构要求访问银行之间的所有消息流量以及银行内部的一些流量,以执行针对内幕交易的规则。

同时具有余额和信用额度,并且由于付款可能必须通过一个或多个代理银行,因此大额付款需要人工干预才能使资金可用。还有一些过滤器可以寻找大额交易,以便银行可以将它们报告给洗钱当局 [75]。因此,一个天真的程序员如果偷偷向他在瑞士银行开设的账户进行虚假交易,通常会在他到场取款时被捕。

通过 Swift 进行的最著名的攻击发生在 2016 年 2 月 4 日至 5 日,当时朝鲜特工从孟加拉国银行窃取了 6300 万美元。他们似乎使用 Dridex 恶意软件窃取了银行员工的凭证,然后下令进行四笔交易,将 8100 万美元从该银行在纽约联邦储备银行的账户转移到菲律宾,但仅追回了 1800 万美元;其余的通过当地的赌场洗钱。另有 30 笔总价值 8.51 亿美元的交易被标记为由美联储人工审查,但未发送;另一笔 2000 万美元的款项被寄往斯里兰卡,在付款银行发现拼写错误并停止付款后被收回。这实际上并不是对 Swift 的攻击,而是对孟加拉国银行自己的 Swift 系统网关的攻击 [858]。

但是,如果您的人生目标是通过银行欺诈致富,那么您最好还是获得法律学位并担任银行经理,而不是摆弄计算机。事实上,大多数重大欺诈都利用了程序漏洞,而不是技术攻击。

- 也许第一起著名的电汇欺诈是在 1979 年,当时计算机顾问 Stanley Rifkin 从 Security Pa cific National Bank 挪用了超过 1000 万美元。他通过同意从瑞士的俄罗斯政府机构购买大量钻石来绕过管制。

  他观察到在向电汇部门口述转账时内部使用的授权码,并通过电话使用了该授权码 这是系统界面双重控制故障的典型示例。他在美国银行假期前夕进行了这笔交易,从而给了自己额外的逃生时间。他出错的地方在于,他没有计划好收集完石头后要做什么。如果他把它们藏在欧洲,然后回到美国帮助调查欺诈行为,他很可能会侥幸逃脱;实际上,他继续逃跑并被抓住了。

- 1986 年在伦敦和约翰内斯堡之间发生了一起稍微不同类型的欺诈。当时,南非政府采用两种汇率,在一家银行中,负责决定每笔交易适用哪种汇率的经理与伦敦的一位富人密谋。他们以 7 兰特兑 1 英镑的汇率汇款到约翰内斯堡,并于次日 4 兰特汇回。两周后,中央银行派出了警察。当他在交易室看到他们时,经理没有停下来取夹克就逃走了,开车越过边境去了斯威士兰,然后经内罗毕飞往伦敦。在那里,他向媒体吹嘘自己如何欺骗了邪恶的种族隔离制度。由于英国没有外汇管制,外汇管制欺诈不构成犯罪 ,因此他无法被引渡。这可能是我所知道的唯一一个罪犯不仅逃脱了数百万美元而且还为此吹嘘的案例。

· 我曾见过坏人使用保证书进行欺诈而逍遥法外。
一个国家的公司要求他们的银行为另一国家的公司提供贷款担保是很常见的。这可以设置为两家银行之间的 SWIFT 消息,甚至是纸质信件。但由于当时没有现金易手,平衡控制不起作用。如果伪造的担保被视为真实的,“受益人”可以从容不迫地从承兑银行借钱,洗钱,然后消失。只有当贷款银行意识到贷款已经变质并试图收回担保时,伪造才被发现。然后你可能会以计算机取证案件告终,因为两家银行就谁的错争论不休。

教训是要警惕任何可以打败双重控制的事情。但你需要在更广泛的背景下看待这一点。这不仅仅是系统管理、接口甚至共享控制加密的技术问题:核心是业务流程设计。通常,关键交易不会在随意检查时出现。适当的拆分控制通常需要功能分离,为此您需要在其社会和经济背景下真正理解应用程序。

12.4 自动取款机

我们的第二组课程来自研究支付卡。这个故事至少有四个组成部分:第一,自动取款机(ATM);第二,信用卡;第三,芯片卡自 2000 年代中期以来同时用作借记卡和信用卡;第四,非接触式支付,包括电话银行。

ATM 是 20 世纪最具影响力的技术创新之一。它们由发明家 Luther Simjian 于 1938 年设计,他还发明了提词器和自动对焦相机。 1939 年,他说服花旗银行在纽约安装他的“Bankamat”机器,但他们在六个月后撤回了它,称“唯一使用这些机器的人是一小部分不想与出纳员打交道的妓女和赌徒”面对面”[1743]。它的卷土重来是在 1967 年,当时伦敦恩菲尔德的巴克莱银行安装了 De La Rue 制造的机器。据世界银行称,现在有超过 240 万台机器,即每 100,000 名成年人有 41 台 [2041]。带 PIN 的卡支付现在用于商店的许多终端,包括分组密码、防篡改硬件和支持协议在内的技术最终被用于从邮政邮资盖印机到彩票终端的许多其他应用。简而言之,ATM 是让现代商业密码学和零售支付技术落地的“杀手级应用”。

12.4.1 ATM 基础知识

大多数 ATM 都使用 IBM 在 1970 年代后期为其 3624 系列提款机开发的系统的某些变体。该卡的磁条包含

平底锅：	8807012345691715
PIN 键 KP：	fefefefefefefe
DES {P AN}KP 的结果：	A2CE126C69AEC82D
{N}KP十进制：	0224126269042823
自然密码：	0224 6565 6789
偏移量：	
客户密码：	

图 12.3：- IBM 生成银行卡 PIN 码的方法

客户的主帐号 (PAN) 和到期日。称为“PIN 密钥”的秘密密钥用于加密 PAN,然后将其十进制化并截断。此操作的结果称为“自然 PIN”;可以添加偏移量以提供客户必须输入的 PIN。偏移量没有加密功能;它只是让客户能够选择自己的 PIN。该过程的示例如图 12.3 所示。

在第一批使用 PIN 的 ATM 中,每台 ATM 都包含 PIN 密钥的副本,每张卡都包含偏移量和主帐号。因此每台 ATM 都可以验证所有客户的 PIN。早期的 ATM 机也离线运行;如果您的现金提取限额是每周 500 美元,卡上会保留一个计数器。

从 20 世纪 90 年代中期开始,网络变得更加可靠,ATM 倾向于只在线运行,这简化了设计。 2003年开始磁条辅以智能卡芯片,2012年开始非接触式支付;我将在后面的部分中描述这些增强功能。但基本原则仍然存在:PIN 是使用加密技术生成和保护的。

称为硬件安全模块 (HSM) 的加密处理器位于银行的服务器机房中,负责管理客户 PIN 以执行双重控制策略。

1. 对客户 PIN 的明确值以及用于保护它们的密钥的操作始终在安全加密设备 (SCD) 中完成,因此银行员工的任何成员都无法看到他们自己以外的 PIN自己的。 SCD 包括银行服务器机房中的 HSM13以及 ATM 和其他 PIN 输入设备中的加密模块。

2. 因此,例如,卡片在带有机器的设施中进行个性化处理,以对卡片进行压花、编码磁条和初始化芯片,而 PIN 邮件则在包含连接到 HSM 的打印机的单独设施中打印。他们隔几天寄出。

3. 终端主密钥以两个印刷组件的形式提供给每个ATM,由不同的人携带到分支机构,在ATM的后键盘输入,并组合成密钥。类似的仪式（但需要三个人）用于在银行和 VISA 等网络交换机之间设置主密钥。

13或者现在,也可以在云服务提供商或其他服务承包商中使用

4.如果ATM在本地执行PIN验证,则PIN密钥在终端主密钥下加密并发送到ATM。密钥存储在本地 SCD（键盘旁边的防篡改芯片)中,它会在输入 PIN 时验证它们或对其进行加密,以便它们可以从 ATM 发送到中央 HSM 进行检查。

5. 如果银行的 ATM 接受其他银行的卡,则 PIN 将在 ATM 的 SCD 中加密并发送到银行,银行将使用与交换操作员共享的密钥对其进行解密并重新加密,例如签证。此 PIN 转换功能完全在 HSM 内完成。

VISA 同样使用 HSM 将 PIN 转换为与发卡银行共享的密钥,因此它可以由那里的 HSM 进行验证。

ATM 网络迅速变得比 Swift 大几个数量级。
它很快就连接了数万家银行和数亿持卡人,而不是被几千家银行使用。在 20,000 家银行之间进行双边密钥交换或财务结算是不可行的,因此每家银行都连接到 VISA 等交换组织提供的交换机,这些交换机的 HSM 转换流量。这些交换机还可以进行会计处理,因此银行可以通过一次借记或一次贷记为每天的交易结算账户,而不是每家都必须在数千家其他机构开设账户。

这些交换机是可信的,因此如果出现问题,后果可能很严重。这似乎大约每十年发生一次。在一个案例中,交换机管理员最终成为逃犯,而在另一个案例中,交换机上与 Y2K 相关的软件升级被搞砸了,结果一个国家的持卡人发现一两天内他们可以取款,即使他们的账户是空的。每种情况下的账单都是七位数。

在 1980 年代设计 ATM 网络和安全系统的工程师（我就是其中之一)假设犯罪分子相对老练,对系统设计相当了解,并且在选择攻击方法时是理性的。我们担心许多银行购买安全模块的速度很慢。我们担心银行偷工减料,例如在授权响应中省略验证码。我们为加密算法是否足够强大、防篡改 HSM 是否足够防篡改以及用于生成密钥的随机数生成器是否足够随机而苦恼。我们知道我们无法正确地实施双重控制:银行经理认为触摸键盘有损他们的尊严,因此他们中的大多数人不会在维护访问后自己输入 ATM 主密钥组件,而是将两个密钥组件都交给 ATM自动取款机工程师。最重要的是,我们担心修理工会弄到银行的 PIN 密钥,迫使重新发行数百万张银行卡并破坏公众对电子银行业务的信心。这是我们的世界末日情景。

世界末日终于发生了。 2017 年 12 月,南非邮政银行的一个密钥在数据中心迁移期间被盗用,当时该密钥保存在笔记本电脑上。不知何故,它被复制到记忆棒上;首席执行官也有一份。这些副本本应在目击者面前销毁,但不知何故丢失了一根棍子。从 2018 年 3 月到 2019 年 12 月,56,000 笔交易中有 5600 万兰特（340 万美元)被盗,大部分是发给穷人的卡

养老金领取者支付国家福利。 2019 年 2 月,中央银行命令邮政银行重新发行其所有 1200 万张卡,耗资 10 亿兰特（6000 万美元)[1237]。

然而,在过去 50 年中,针对基于 PIN 的支付卡的数百万起欺诈行为却变得更加多样化。

12.4.2 出了什么问题

卡支付系统具有巨大的交易量、多种多样的运营商和大量有能力的有动机的对手。银行卡欺诈的浪潮接连不断,其中的漏洞被发现、利用并最终得到修复。总体模式是,信用卡欺诈的价值随着时间的推移而增加,但在交易中所占的比例却在下降;随着系统规模和经验的增长,该系统正在慢慢变得更加安全 [91]。

第一波浪潮发生在 1990 年代初期,利用了早期磁条卡系统实施和管理不善的问题。在英国,一位多产的欺诈大师安德鲁·斯通 (Andrew Stone) 因 ATM 欺诈而被定罪 3 次,最后一次被判入狱五年半。当他偶然发现一个“加密替换”技巧时,他开始了:他将银行卡上的帐号更改为他妻子的帐号,并发现他可以使用他的 PIN 从她的帐户中取款。事实上,他可以使用他的 PIN 从该银行的任何账户中取款。发生这种情况是因为他的银行将加密的 PIN 写入了卡的磁条,但没有将其与帐号相关联。他的第二种方法是“肩窥”:他会站在受害人身后排队,观察输入的 PIN,然后捡起丢弃的 ATM 单据。当时大多数银行都在单据上打印了完整的帐号,即使没有其他正确信息,卡也可以使用。

斯通的方法通过他作为同谋训练的人传播开来,并通过他在狱中写的“Howto”手册传播开来。他（和其他)欺诈行为的大约 2000 名受害者联合起来对 13 家银行提起集体诉讼,以取回他们的钱。银行通过争辩说每个案件的事实不同 ,并将其分成数以千计的小额索赔案件,受害者没有专业知识去追究,从而打败了这一点。我是这个案例的专家,并用它写了几篇关于问题出在哪里的论文 [54、55]。随着罗马尼亚和其他地方的犯罪分子开始设计 ATM 盗刷设备并在线销售,欺诈最终在全球蔓延开来。在这里,我将总结我们学到的更重要、更有趣的课程。

1990 年代初期的大多数实际“幻影提款”似乎
有以下三种原因之一：

- 简单的处理错误会引起争论的稳定背景噪音。发达国家每人每月约有四笔交易;仅在英国,即每月 2.4 亿。如果错误率只有十万分之一,那争议就大了。即使您的核心银行系统具有良好的平衡控制,为其提供支持的外围系统也可能不稳定。

  我们追踪到的一个错误来源是,如果在从银行服务器收到确认消息之前网络出现故障,大型银行的 ATM 会再次发送交易;周期性地,服务器本身

崩溃并忘记了未结交易,导致借记被重复。我们还发现一些客户的账户被其他客户的交易扣款,而其他客户的卡交易则根本没有被扣款。 （我们过去称这些卡为“董事卡”,并开玩笑说它们是发给银行董事的。）

· 据估计,在 1990 年代,邮件失窃占所有英国支付卡损失的 30%,并且邮政控制程序多年来一直令人沮丧。例如,当我在 1992 年 2 月搬到剑桥时,我的银行通过邮局寄出的不是一张,而是两张卡片和个人识别码,而且在入侵者拿到我们公寓楼的邮件并撕毁它寻找的几天后,它们就到了对于贵重物品。2003–5 年,当磁条卡被芯片卡取代时,邮件盗窃案再次激增 见图 12.4。主要的解决办法是让你打电话给呼叫中心或访问一个网站来激活一张卡,然后才能使用它。

· 涉及不诚实或疏忽银行员工的欺诈 似乎是幻影的第三大原因。我们偶尔会遇到 ATM 服务人员在 ATM 内安装窃听器以记录客户卡和 PIN 数据的案例,还有一个案例可以追溯到 1990 年代,不正当的内部人员一次以 50 英镑的价格为被盗的卡计算 PIN。最近,我们遇到了更多的骗子案例,他们研究如何对银行呼叫中心进行社会工程,以向他们控制的地址发行新卡 [2013]。内部欺诈在英国等国家特别常见,在这些国家法律通常要求客户为欺诈行为付费,而在美国等银行支付的国家则很少见;英国银行职员知道客户投诉不会得到仔细调查。

然而,由于粗心的设计或教导,有很多欺诈行为
技术安全课程。

· 站在 ATM 队列中,观察客户的 PIN,捡起丢弃的票并将数据复制到空白卡上的肩膀冲浪技巧,于 1980 年代中期首次在纽约报道;它在 1990 年代中期仍在湾区工作。那时它已经自动化了;湾区犯罪分子使用带有运动传感器的摄像机来窥探 PIN,无论是租一间俯瞰自动取款机的公寓,还是将租来的面包车停在那里。视觉复制很容易停止:现在的标准是只在票上打印帐号的最后四位数字,自 90 年代初以来,卡片在磁条上有一个三位数的卡片验证值 (CVV)绝不能打印出来。

然而,并不总是检查 CVV。

· 由于漏洞和失误造成了很多损失。 1980 年代出售的一台 ATM 有一个“测试分发”代码,只要在键盘上输入某个 14 位数字序列,该代码就会输出十张最低可用面额的钞票。一家银行在其分行手册中印制了这一序列,三年后突然出现大量亏损。

所有使用这台机器的银行都不得不赶紧推出一个补丁来禁用测试分发交易。尽管我在

1993 年,以及 2001 年本书第一版中,类似的事件直到 2007 年仍有报道。

- 便利店中使用的某些品牌的 ATM 可以重新编程,以为他们在分发 1 美元钞票,而实际上他们在分发 20 美元钞票;它只是使用了在线手册中打印的默认主密码。任何知道这一点的路人都可以走到机器前,重新设置账单价值,提取 400 美元,然后他们的账户只被扣除 20 美元。租用机器的店主没有被告知该漏洞,而是要自己付钱 [1539]。

- 许多银行的运营安全程序很糟糕。作为一项实验,我妻子于 1993 年在目击者的陪同下进入我们银行的一家分行,并告诉他们她忘记了 PIN。出纳员帮她打印了一张新的密码邮件,打印机连接到柜台后面的个人电脑上 就这样!

  这不是我们账户所在的分支机构。没有人认识她,她提供的所有身份证明就是我们的银行卡和她的支票簿。当抢走手提包的任何人都可以走在街上,并在任何一家分行获得其中的卡的 PIN 码时,再多的加密技术也无济于事。 (该银行后来于 2008 年破产。)

- 黎巴嫩环路是一种持续工作了 40 年的技术 现在仍然适用于许多 ATM。骗子将一圈磁带(可能是旧录像带上的磁带)塞进自动取款机的喉咙里,等待受害者。卡片卡在环路中,受害者将其丢弃。骗子取回它,如果他设法看到受害者的 PIN,就会去购物。有些 ATM 有阻止这种情况发生的机制,有些则没有。

  有些银行根本不在乎:此类欺诈的一名受害者在银行大堂直接进入银行投诉,但被不想卷入的员工哄骗 。卡被盗后,发卡行责备她,最后演变成一场纠纷。

- 高科技作案手法是使用虚假终端或窃取器来收集卡和 PIN 数据。第一份报告于1988年来自美国;在那里,骗子建造了一台自动售货机,可以接受任何卡和密码,并分发一包香烟。 1993 年,两个恶棍购买了一台真正的 ATM 机和一个软件开发工具包,对其进行编程以窃取卡数据和 PIN,并将其安装在康涅狄格州的 Buckland Hills 购物中心 [988]。

- 虚假终端攻击在 90 年代蔓延到欧洲和销售点系统。我在第 4.5 节中提到,在荷兰乌得勒支,车库销售点终端上的水龙头被用来收集卡和 PIN 数据; 1994 年,伦敦的骗子建立了一个完整的虚假银行分行 [943]。

  最终,到 2000 年代中期,撇卡器在黑市上变得广泛可用。到 2015 年,一个罗马尼亚团伙被发现在墨西哥的旅游景点经营 100 台自动取款机,每月盗窃 20 美元 [1094]。磁条卡太容易复制了,卡片技术必须改变。

- 自 2010 年代中期以来,我们偶尔会看到骗子入侵 ATM 机的“头奖”攻击,以便它们继续分发账单,直到取完为止。这可能涉及用恶意软件感染 ATM,无论是在线的

或者通过物理访问 USB 端口,或物理插入流氓电子设备 [489]。

- 当内部人员进入后端系统中的其中一台服务器时,或者当其中一台服务器因不安全而失败时,偶尔会发生欺诈。这可能导致客户能够使用具有任何 PIN 的卡(如果在线 PIN 检查过程失败)或具有正确 PIN 的客户能够无限透支(如果余额查询过程失败)。其中一个失败是故意的:在 9/11 破坏了其 ATM 网络之后,市政信用合作社决定让纽约的客户在问题得到解决之前不检查余额就可以取款。这花费了 1500 万美元,最终有 118 名客户被控盗窃 [1657]。

我认为我们在 1980 年代设计 ATM 安全系统时做错的第一件事就是担心犯罪分子很聪明,而我们更应该担心我们的客户 银行的系统设计者、实施者和测试者 无法使用安全我们设计的系统。近年来,Yasemin Acar、Sascha Fahl 等人的研究表明,即使不是大多数,也有许多安全故障可以被视为程序员的可用性故障;普通程序员无法应对安全极客喜欢构建的复杂加密 API 和访问控制机制 [11]。安全极客关注加密是因为数学很有趣,但不太关注“无聊”的部分,例如创建非专家可以实际使用的工具。因此,坏人很少会破解密码。现代支付网络拥有如此多的用户,我们必须期待有机会发现那些太隐蔽而无法在测试中被发现的漏洞。

我们做错的第二件事是没有弄清楚哪些攻击可以工业化,而是专注于这些攻击。就 ATM 而言,虚假终端攻击最终大获成功。有组织犯罪参与的第一个线索是 1999 年在加拿大,在多伦多地区逮捕了数十名涉嫌东欧有组织犯罪的人物,原因是他们部署了经过篡改的销售点终端 [129、216]。大约从 2005 年开始,东欧制造的盗刷器在地下市场上销售,设计用于连接到自动取款机的喉管以读取磁条并使用微型相机或键盘覆盖层捕获 PIN。我将在下一节中更详细地讨论这些。补救措施一直从磁条卡转向芯片卡,但这已经花费了十五年多的时间,同时磁条欺诈也造成了巨大的损失。奇怪的是,从磁条 ATM 卡问世到盗刷器让它们太容易被攻击用了 40 年。正如我在第 2.3 节中讨论的那样,关键因素是犯罪分子开始专业化和组织化。

12.4.3 激励和不公正

在美国,银行承担着许多与新技术相关的风险。
在一个历史性的案例中,贾德诉花旗银行,银行客户多萝西·贾德声称她没有进行过一些有争议的提款,而花旗银行则表示,由于其系统是安全的,她一定是这样做了。法官裁定他“不准备裁定当一名可信的证人面临

机器的不利‘证词’,他在法律上也面临着无法满足的举证责任” 并把钱还给了她 [995]。美联储将这一观点纳入“E 条例”,该条例要求银行退还所有有争议的交易,除非他们能够证明客户存在欺诈行为[639]。这导致了一些轻微的滥用,但通常少于故意破坏造成的损失 [2046]。

在其他国家（例如英国、荷兰和挪威）,银行多年来一直声称其 ATM 系统绝对可靠,却逍遥法外。

他们坚称,幻影提款是不可能发生的,抱怨幻影提款的客户一定是弄错了或在撒谎。当斯通和他的追随者开始因 ATM 欺诈而入狱时,这一地位在英国受到了一定程度的破坏,并且发生了一些相当不愉快的事件。一个例子是 Munden 案例 [55]。

约翰·蒙登 (John Munden) 是我们的一名当地警员,驻扎在剑桥郡的博蒂舍姆 (Bottisham);他的节奏包括我当时居住的 Lode 村。
1992 年 9 月,他放假回家,发现自己在 Halifax Building Society 的账户空空如也。他要求发表声明,发现有六次提款,总计 460 英镑,他不记得做过这些,并提出了投诉。哈利法克斯以试图通过欺骗手段获取金钱为由起诉了他。在试用期间发现他们的 IT 有点摇摇欲坠;有争议的交易没有得到适当的调查;他们做出各种疯狂的声明,例如他们的 ATM 系统不会出现错误,因为它的软件是用汇编语言编写的。尽管如此,这是他的话反对他们的话。他于 1994 年 2 月被定罪并被停职。就在审理上诉之前,检方提供了哈利法克斯审计员的一份报告,声称他们的系统是安全的。辩方要求自己的专家能够平等地访问银行的系统。哈利法克斯拒绝了,因此法院拒绝接受所有计算机证据。案件失败了,约翰·蒙登被宣告无罪,他又重新找到了工作。

一旦喧嚣平息,银行又重新声称他们的系统是安全的,当英格兰特伦特河畔伯顿的简巴杰因抱怨幻影提款而被起诉时,同样的戏剧再次上演。她的案子在 2008 年 1 月告破。如果一个系统要提供证据,那么双重控制是不够的。它必须能够经受敌对专家的检查。银行真正需要的安全属性不是双重控制,而是不可否认性:交易中的委托人能够证明事后发生的事情。这可能是通过安装 ATM 摄像头提供的;尽管这些作为反抢劫措施在纽约州是强制性的,但在英国并未使用。

事实上,在 1992-4 年的 ATM 欺诈浪潮中,少数安装了 ATM 摄像头的银行在其他银行的压力下不得不撤回摄像头;摄像机证据威胁到银行的集体立场,即他们的系统是绝对可靠的。又过了 25 年,我在第 12.2.6.1 节中提到的 Post Oce 案例才最终使银行的系统受到彻底审查,并在高等法院被谴责为不可靠。

12.5 信用卡

导致现代卡支付系统的第二个组成部分是信用卡。在 1950 年代大莱俱乐部发明信用卡之后的许多年里,大多数银行都将信用卡视为吸引高价值客户的亏损领导者。最终,商户和持卡人的数量达到临界质量,交易量开始下降 。在英国,从 80 年代中期开始,信用卡业务突然暴利 14。

当您使用信用卡在商店购物时,交易从商家流向他们的银行(收单银行),银行在扣除通常低于 2% 的小商家折扣后付款给他们15。如果卡是由不同的银行发行的,交易现在会流向 VISA 之类的交换机,后者将其传递给发卡银行进行支付。每笔交易涉及两个部分:授权,当您在商家出示您的卡时,他们想立即知道是否给您商品,以及结算,它通过一个单独的系统流向商家,通常是两个或三个几天后。发卡行也能从商家折扣中分得一杯羹,但大部分收入来自向持卡人提供信贷。

12.5.1 信用卡欺诈

从 1950 年代到 90 年代,信用卡交易的处理方式是在多部分表格上使用卡上的压纹制作纸质销售汇票,写下金额,让客户签名,然后像支票一样处理。使用被盗信用卡进行欺诈的风险传统上由热卡列表和商户限额来管理。每个商户都有一个当地的“热卡列表”加上他们的收单银行设定的限额,超过该限额他们必须致电在线授权。在 20 世纪 80 年代,引入了电子终端,售货员可以刷卡并自动获得授权。骗子的反应是大量伪造卡片:1989 年至 1992 年间,磁条伪造从偶尔的滋扰发展到占欺诈损失总额的一半 [12]。

邮购和电话销售的引入导致商户无法检查卡的无卡交易 (CNP)。银行通过使用到期日作为密码、降低最低限额、增加商户折扣和坚持送货到持卡人地址来管理风险,持卡人地址的数字部分应该在授权时进行检查。但主要的变化是转移责任,让商家承担纠纷的风险。如果您对在线信用卡交易(或实际上根据 CNP 规则进行的任何交易)提出异议,将立即向商家扣除全部金额,并支付一笔可观的手续费。这个

14支付系统具有强大的网络外部性,就像通信技术或计算机平台一样:服务提供商必须招募足够多的商家来吸引持卡人,反之亦然,因此新的支付机制可能需要数年时间才能建立,然后突然像火箭一样起飞 .

15借记卡更便宜,即使是信用卡交易,大商户也能支付不到 1% 的费用。

无论借记是欺诈、争议还是退货,均适用。

VISA 对日益增多的卡片伪造和在线欺诈的回应是卡片验证值 (CVV) 根据卡片内容（帐号、版本号、有效期)计算并写在卡片末尾的三位数 MAC。它们奏效了:1994 年第一季度,VISA 的欺诈损失下降了 15.5%，而 Mastercard 的欺诈损失上升了 67% [386]。所以万事达卡也采用了 CVV。

它们也出现在借记卡上,在技术上与信用卡融合在一起:这是一个扩展过程,因为银行首先允许在 ATM 机上使用信用卡,然后在不同的时间让借记卡在销售点使用在不同的国家 。

骗子转向窃取 - 经营业务,在这些业务中,通过额外的、未经授权的终端刷取真正的客户卡,以获取磁条的副本,然后将其重新编码到真正的卡上。

（在 PIN 已经用于销售点终端的国家,这允许伪造的卡直接用于 ATM。)银行的回应是入侵检测系统,试图通过关联购买历史来识别犯罪企业投诉的客户。到 20 世纪 90 年代后期,更聪明的不正当企业学会了承担客户交易的成本。您在 Mafia 拥有的小酒馆喝了一杯,提供了一张卡片,在凭证上签名,却没有注意到账单上没有显示费用。一两个月后,会有一笔巨额的珠宝、电子产品甚至赌场筹码账单。

到那时你已经忘记了小酒馆,银行从来没有它的记录 [720]。

在 2000 年代初期,随着电子犯罪变得专业化,高科技罪犯变得更有组织。 2003 年在俄罗斯和乌克兰开始出现的在线犯罪论坛使恶意软件编写者、僵尸网络牧民、钓鱼网站运营商和套现专家能够相互交易并做好自己的工作。这从针对在线交易蔓延到对零售终端的攻击。论坛提供了记录磁条卡和 PIN 数据的假冒终端和窃取器,以制作卡克隆。在远东,窃听被用来收集 2000 年代中期的卡片数据 [1158]。

欧洲在 2003-5 年引入了智能卡,骗子想出了将数据从芯片卡复制到磁条卡的设备,用于仍然接受磁条交易的终端。其中一些利用了 EMV 协议中的漏洞,因此在下一节中介绍了 EMV 和芯片卡后,我会再回来讨论它们。

不管卡片是否有芯片,有许多涉及真正客户从未收到过卡片的骗局。发行前的欺诈行为包括从垃圾邮件中收到的“预批准”卡的邮件盗窃。有些应用程序是以存在但不知道该应用程序的人的名义提出的（通常被银行误传为“身份盗用” ,他们想假装是您的身份被盗而不是他们的钱 [1324]）。还有一些骗子让粗心的银行工作人员将您帐户的替换卡发送到他们控制的地址的骗局 [2013]。在客户收到账单并投诉之前,针对此类欺诈的剩余防线是自动欺诈检测,我将在第 12.5.4 节中讨论。

12.5.2 网上信用卡诈骗

现在从传统的信用卡诈骗转向网络诈骗,我首先在1987年帮助警方调查了一起网络信用卡诈骗案。在那个案子中,嫌疑人从他在超市工作的伙伴那里得到了一张热门信用卡号码列表,然后用它们从海外公司购买软件,他下载这些软件为他的客户订购。当时的热门卡片列表只包含那些在该国被滥用的卡片;在海外使用本地热卡意味着银行将背负罐头,而不是无辜的客户。

碰巧的是,嫌疑人在有足够的证据逮捕他之前就辞职了。
一场暴雨冲走了他家对面的河岸,暴露了警察为监视他而搭建的藏身之处。

大约从 1995 年开始,互联网繁荣开始,企业争先恐后地建立网站。人们担心在互联网上使用信用卡会导致大量欺诈,因为“邪恶的黑客”截获了电子邮件和网络表格并获取了数百万的信用卡号码。这些担忧促使 Microsoft 和 Netscape 引入 SSL/TLS 来加密从浏览器到 Web 服务器的信用卡交易。

实际情况要复杂一些。拦截电子邮件和网络流量确实是可能的,尤其是在端点,但可能很难大规模进行。许多网站在没有加密或弱加密的情况下运行了很多年,结果证明真正的问题不是窃听而是网络钓鱼。甚至这也是在 2004 年之后才大规模进行的;那里(正如我在第 3 章中提到的)更多的是心理学问题而不是密码学问题。 TLS 本身没有帮助,因为可以设置中间人攻击的坏人可以获得证书并加密 trac。该网站将有一个不同的域名,但期望大多数公众注意到这一点是不合理的,尤其是当银行和商家自己使用各种不同的域名时 16。

其次,大部分在线交易的信用卡号码都落入坏人之手,因为有人入侵了商家的计算机。 VISA 多年来一直有规定,禁止商户在处理完交易后存储信用卡数据,但许多商户无视这些规定。随后是支付卡行业数据安全标准 (PCI-DSS),由支付卡行业安全标准委员会 17 共同努力。 PCI DSS 规则要求保存持卡人数据(例如帐号和到期日期)18 的系统基本卫生,而根本不能存储 CVV 和 PIN 等敏感数据。

最后,执法开始发挥作用,到 2007 年 10 月,美国全国零售联合会要求信用卡公司停止强迫零售商存储信用卡数据(他们应该临时存储卡号以防退款)[1957] . PCI DSS 现在已成为接受信用卡交易的公司的重要合规部分;它提供的很少

16现在有一些技术修复,例如证书透明度,我将在
第 21.5.1 节。

17这是由 Visa、MasterCard、Amex、JCB 和 Discover 设立的;它现在也有其他利益相关者。

18持卡人数据在网络传输时必须加密,存储时必须受到防火墙和 AV 的保护;不能使用默认密码;并且您必须拥有安全策略、需要了解的访问控制、测试,以及自 2017 年以来的安全软件开发生命周期。它加起来相当多的文档和很多会计师检查它的工作。

责任保险,因为如果发生欺诈,银行通常可以责怪商家,即使商家被证明是合规的。

商家面临的其他真正激励因素首先是纠纷成本,其次是安全漏洞披露法。虽然各国之间的细节有所不同,但披露法律有所不同,因为通知客户需要花费真金白银,而且遭受违规行为的公司的股票价格可能会下跌几个百分点。至于纠纷,许多国家的消费者保护法使得拒绝交易变得容易。基本上客户所要做的就是打电话给信用卡公司并说“我没有授权”,然后商家就会背负账单。在几乎所有信用卡交易都在本地进行并且大多数交易金额都很大的时代,这是可行的。如果客户以欺诈方式拒绝交易,商家将通过法院追究他们的责任。现在很多交易都是国际化的,金额很小,通过信用卡系统验证海外地址很不稳定。

因此,拒绝交易并侥幸逃脱的机会增加了。

另一方面,一些市场领域有许多剥削客户的网站,色情网站一直是个痛处。一个常见的骗局是提供网站的“免费游览”并要求提供信用卡号码,据称是为了验证用户已超过 18 岁,然后无论如何都会向他收费。一些网站向从未访问过它们的其他消费者收费 [921]。甚至像 playboy.com 这样看似大型且“受人尊敬”的网站也因此类做法而受到批评,而在色情行业的最底层,事情是残酷的。迄今为止最糟糕的案例可能是 Operation Ore,大约 3000 名信用卡诈骗受害者因涉嫌购买儿童性虐待材料而被错误逮捕,至少一人自杀。我在第 26.5.3 节讨论了 Operation Ore 案例。

恶意网站的主要障碍是信用卡拒付。银行通常会向商家收取 100-200 美元的费用,并从他的账户中扣除交易金额。因此,如果您网站上超过一小部分交易受到客户的质疑,您的利润就会受到侵蚀。如果退款超过 10%,您的银行可能会终止您的服务。这促使商家小心谨慎 提防奇怪的订单(例如四只手表)、来自不可靠国家的订单、使用免费电子邮件服务的客户、要求加急交货等。但是让他们承担邮购交易的大部分责任并不是最理想的:银行对欺诈模式了解得更多。分担责任可能会更好,但法律体系并不擅长于此。当法律成文时,一个说客打败了另一个说客,或者在关键先例确立时,一个法律团队打败了另一个,我们就陷入了困境。

一种系统性攻击涉及渐进式猜测。所有网站都必须要求提供主帐号和到期日,但商家也可能要求提供印在卡背面的 CVV 以及持卡人地址中的数字。从一个有效的帐号开始,您可以通过在仅检查该帐号的商家网站上进行测试来猜测到期日期;然后你在也会检查的网站上猜测 CVV,然后是邮政编码数字,最后从也会检查的网站上猜测门牌号码。有足够的网站可以为 VISA 卡工作;万事达卡有中央监控,

他们在大约十次猜测失败后将一个数字列入热门列表（尽管这可能导致拒绝服务攻击）[1]。

另一种攻击是凭据刺痛，坏人从受感染的网站获得数百万个电子邮件/密码组合，并在其他可以提取价值的网站上试用它们。此类攻击，加上地下市场上越来越多的被盗信用卡数据，推动了更好的持卡人身份验证的发展，至少对于大额交易而言。

12.5.3 3DS

3D Secure 是支付卡行业设计的单点登录系统19。
当商家捕获超过某个阈值的支付交易时，他们会重定向到银行服务器，邀请客户使用密码或第二因素（例如通过 SMS 发送到他们手机的代码）来验证交易。它越来越多地用于大额支付卡交易。

3DS 迅速获得了用户，因为使用它的客户在可能的情况下要承担欺诈责任，因此商家支付的费用较少。多年来，客户入职一直是一个软肋。许多银行最初让 3DS 服务器直接登记他们的客户，并在他们的卡首次在参与商户处使用时索取密码，这个过程称为购物期间激活 (ADS)。有些甚至让客户在忘记密码的情况下重新注册，所以最初系统很容易被破解。它还让客户习惯于在 URL 与银行无关的网站上输入银行密码，一家银行甚至让客户在那里输入他们的 ATM PIN [1362]。现在，在首次推出十年后，3DS 正在转向（不兼容的）第二个版本，该版本被认可为 EMV 标准。一个因素是政府强制要求使用双因素身份验证，这导致大多数银行知道客户的手机号码。然而，基于 SMS 的双因素身份验证现在已达到其使用寿命的终点，如前面第 3.4.1 节和后面的第 12.7.4 节所述。一些 3DS 实现仍然使用银行密码。

12.5.4 欺诈引擎

人们从 20 世纪 90 年代中期开始致力于更好的金融入侵检测，到现在为止，所有接受无卡交易的任何规模的网站都有一个欺诈引擎来决定是接受还是拒绝每笔交易。有两种方法：异常检测，它使用各种阈值和其他技术来寻找异常模式，以及滥用检测，它寻找已知的欺诈模式。这两种情况的大问题都是误报。我们都有卡被封的经历，而且在很多情况下，诱因很明显。小额交易过去常常引起警报，因为他们建议小偷测试被盗的卡以查看哪些卡仍然有效。另一个问题是海外的多项交易；在 1990 年代，每当我去美国时，我的借记卡都会进行三笔交易，然后就停止工作了。现代机器学习技术已经使这种机制稍微不那么烦人了

19 它有多种品牌名称，如“Mastercard SecureCode”、“Verified by VISA”、“Amex SafeKey”和“发现 ProtectBuy”。

ing,但现代支付系统每秒处理数万笔交易的庞大规模意味着即使是 0.1% 的误报率也会引起大量客户投诉。

更有说服力的是寻找已知滥用模式的项目。例如,FICO 维护着一份最可疑 ATM 的列表。订阅其服务的银行会在交易被拒绝时通知它,无论是因为卡被盗、密码错误还是空账户。然后,ATM 被提升到“热门 ATM”列表中。当骗子将一大把被盗的卡带到 ATM 机时,它会在三四张卡中排在列表的首位,然后拒绝任何订阅 FICO 服务的银行发行的卡。骗子会认为它们不好并将它们扔掉。按发卡量计算,全球超过 40% 的银行现已订阅。

运行入侵检测系统的一个重要成功因素是激励。由于欺诈引擎,英国的网站可以拒绝多达 4% 的购物篮。如果安全是 CFO 的责任,他会将其视为成本中心并尽量减少它;但对于首席营销官来说,误报率降低 25% 意味着“销售额增加 1%”,他们会乐意为此付出真金白银。

一个好的欺诈引擎的核心往往是根据一组众所周知的威胁向量(例如错误的 IP 地址,或来自同一 IP 地址的过多登录)和一组从交易流中提取的信号质量信号(例如“卡旧但好”)。然后将这些信号馈送到对交易进行评分的机器学习系统。信号似乎是设计中最重要的部分,而不是您使用 SVM 还是贝叶斯网络。随着坏人学习新的技巧,信号需要不断地策划和更新,并且欺诈引擎需要与人工流程很好地集成。至于欺诈引擎是如何失灵的,监管机构针对 2016 年针对 Tesco 银行的欺诈行为的报告发现,工作人员未能对欺诈检测规则“运用应有的技能、谨慎和勤勉”,以及“以足够严谨的方式应对攻击,技巧和紧迫感”[687]。在这种情况下,该银行在前一天收到万事达卡关于新型信用卡诈骗的警告后未能更新其欺诈引擎。解释完芯片卡后,我们将在 12.6.3 节进一步讨论这种情况。

12.6 EMV 支付卡

自 2003 年以来最大的投资是新卡技术,银行用 EMV 智能卡取代信用卡和借记卡,随后是使用卡和手机进行非接触式支付。卡支付变得既复杂又多样化;了解它们的最好方法可能是跟踪它们的演变。

60年代出现集成电路,70年代出现微处理器时,各种人提出把它们放在银行卡里。德国人认为智能卡是由 Helmut Gr¨ottrup 和 Jurgen ¨ Dethlo 于 1968 年发明的,当时他们提出了一种用于卡的定制 IC 并获得了专利;日本人指出了有村邦隆在 1970 年的一项专利;而法国信贷

罗兰·莫雷诺 (Roland Moreno) 于 1973 年提出在卡片中使用存储芯片,而米歇尔·乌贡 (Michel Ugon) 于 1977 年提出添加微处理器。法国公司霍尼韦尔布尔 (Honeywell Bull) 于 1982 年为一种包含内存、微控制器和进行交易所需的一切的芯片申请了专利;它们于 1983 年开始用于法国公用电话,并从 80 年代中期开始用于银行业。

挪威位居第二,部分银行从1986年开始发行芯片卡。英国NatWest银行在90年代初开发了Mondex电子钱包系统,在斯温顿进行试点,然后卖给万事达卡;该软件演变为 Multos,一种仍在使用的卡片操作系统。 VISA 和 Mastercard 之间有一场专利大战。在本书第二版的第 3 章中有关于这些早期试点项目的更多详细信息。那都是很好的学习经历。但要使支付卡真正有用,它必须在国际范围内发挥作用 尤其是在欧洲,许多小国家紧密地挤在一起,那里有数百万人跨越国界进行每周一次的购物,甚至在上下班途中。因此,银行终于在 1990 年代后期聚在一起,敲定了一个标准。

12.6.1 芯片卡

EMV 标准规定了用于 ATM 和零售支付终端的芯片卡和支持协议。它们最初由 Europay、Mastercard 和 VISA 开发,然后他们成立了 EMVCo 来维护和扩展标准。芯片卡于 2003-6 年在英国推出,然后在其他欧洲国家推出,其中大部分使用 PIN 码在商店和 ATM 机上进行身份验证,导致该系统被称为“芯片和 PIN”。在美国和新加坡,现在使用带有签名的芯片卡,该系统称为“芯片和签名”。标准长达数千页;它们现在扩展到非接触式支付、在线支付等等;还有针对特定国家和个别银行的其他文件。为了理解这一切,让我们从使用带有 PIN 的 EMV 卡从商店购买商品的基本协议开始。

首先,卡将其凭据发送到 PIN 输入设备 (PED) 或终端,包括主帐号 (PAN) 和发卡银行签署的证书。然后终端发送不可预测的数字或随机数 N、日期 t 和请求的支付金额 X,以及持卡人输入的 PIN。卡会检查 PIN,如果它是正确的,它会计算一个身份验证请求密码 (ARQC),这是一个关于 N、 d3和 X 的消息身份验证代码 (MAC)。每条消息都有一些额外的数据di ,我们将在后面讨论。

C！ T : P AN, d1, CertKB(P AN, d1)
吨！ C : N, t, X, d2,PIN C ! T : d3,
MACKCB(d3, T, N, t, X)

ARQC 是使用卡和银行之间共享的密钥 KCB 计算的20。商家无法检查这一点,因此必须要么接受风险

20 长期密钥 KCB 实际上是用来为每笔交易生成一个派生的唯一密钥（DUKPT,读作 duck-put)作为功率分析的对策。我省略了这样的

在线支付或通过支付网络将交易发送至发卡银行。银行检查 ARQC 和可用资金,如果一切正常,则发送一个响应,其中还包括该卡的授权响应密码 (ARPC)。该卡以另一个称为交易证书的 MAC 进行响应。

EMV 允许许多选项,其中一些单独或组合是危险的,并且可以被视为构建支付系统的构建工具包,您可以使用它构建非常安全或非常不安全的系统。真正限制加密货币的是 VISA 和 MasterCard 的转换规范,因为大多数银行希望能够依靠他们的立场进行处理。在 2005-17 年间,随着一系列欺诈行为利用了安全性较低的版本,事情变得越来越严密。了解协议套件的最简单方法可能是遵循这段历史。

12.6.1.1 静态数据认证

直到 2011 年,许多国家/地区的默认 EMV 变体是静态数据身份验证 (SDA)。由于这使用不能进行公钥加密的廉价卡,因此没有卡公钥 KC,PIN 以明文形式发送到卡中。因此它仍然容易受到中间人设备的窃听,就像 EMV 正在取代的磁条卡一样。终端验证了证书和数字签名,但是没有办法验证MAC21。和以前一样,商家有一个允许在线交易的下限,因此他们不必在网络或收单银行出现故障时停止交易22。

首先,通常被利用的漏洞是与磁条卡的向后兼容性。证书最初包含伪造磁条卡所需的所有信息,随着芯片和 PIN 的引入意味着人们开始在任何地方输入 PIN,而不仅仅是在提款机上23,团伙要么设置假终端,要么使用各种窃听设备从真正的终端收集卡数据,然后通过磁条伪造兑现。最初,这些用于本地 ATM,这些 ATM 在转换期间会回退到磁条处理以实现可靠性和兼容性。

从 2000 年代后期开始,骗子将目标锁定在美国和泰国等尚未采用 EMV 的国家/地区。在图 12.4 中的黄线中可以看到这波磁条回退欺诈,它在 2006 年到 2010 年间激增。

2006-9 年的部分犯罪浪潮以加油站为目标。对我们位于剑桥的当地 BP 车库的攻击涉及安装在天花板上的闭路电视摄像机以捕获 PIN 以及窃听以获取卡数据;超过 200 名当地人发现他们的卡的副本被用于泰国的自动取款机。 BP 的竞争对手 Shell 受到的打击更大,在他们的一些 PIN 键盘被伪装成篡改的密码键盘替换后,他们一度退回到磁条操作

细节在这里,并将在后面的边信道章节中讨论功率分析。

21银行因此可以使用它喜欢的任何算法,但默认的是 DES-CBC-MAC 和最后一个块的三重 DES。

西班牙的 22 楼限制首先被削减为零,这似乎也在英国发生,这似乎很愚蠢;当电话线中断时,车站不应该停止售票,季票可能除外。

23在英国,有 900,000 个商店终端和 50,000 个自动取款机。

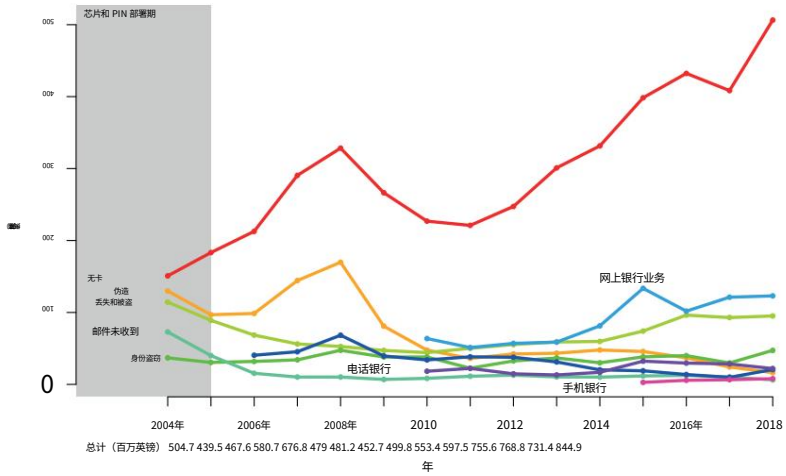

图 12.4：- 2004 年至 2018 年英国的信用卡欺诈。

成为维修工程师。最引人注目的欺诈行为是在 2008 年发现的，当时一个团伙显然在迪拜的一个仓库中截获了 PIN 输入设备，这些设备是从中国工厂运往英国和荷兰的途中，并在其中安装了微型手机，该设备将卡发送给该团伙和密码数据。英国的商店和荷兰的银行直接安装了开箱即用的新设备 这些设备立即开始将客户的数据通过短信发送到卡拉奇的服务器 [1729]。该团伙在英国被捕并受审，但由于银行拒绝提供证据，此案失败了。

因此，我和同事调查了一个密码键盘样本，发现这种攻击很容易。例如，2007 年在英国部署最广泛的终端 Ingenico i3300 有一个用户可访问的隔间，如图 12.5 所示，它可以访问电路板的底层。我们发现，可以使用弯曲的回形针轻松访问承载串行数据信号的直径为 1 毫米的过孔，回形针可以插入塑料上的孔中，而不会留下任何外部标记。因此，攻击者确实可以在终端内隐藏一个设备，该设备可以收集和中继卡和 PIN 数据。此类设备的“通用标准评估”结果毫无价值；我将在 28.2.7.2 节中讨论其失败的政治和组织原因。

此类设备现在已通过 PCI 制定的标准认证，并且日益严重的问题是软件复杂性；现在的 PIN 输入设备不再基于 8 位微控制器，而是倾向于在 Linux 或 Android 平台上构建，这些平台具有更大的攻击面。

法国遭受了一波使用“yescards”的攻击。这些卡被编程为接受任何 PIN（因此得名）并使用来自真实卡的证书参与 EMV 协议，但返回 MAC 的随机值 [179]。他们在购买零食和地铁票等低价值物品时工作得很好，那时候这些物品总是通过在线交易出售。

图 12.5：- 一根硬线穿过 Ingenico 隐蔽隔间壁上的孔插入以拦截智能卡数据。设备的正面显示在右上角。

另一类问题与身份验证方法有关。每张卡和每个终端都有一个首选持卡人验证方法 (CVM) 的优先级列表，它在补充数据d1和d2 中共享。该卡实际上可能会说：“首先尝试在线 PIN 验证，如果不支持，请使用本地 PIN 验证，如果这不可能，那么签名就可以了，如果你连签名都做不到，那你就别做了”根本不需要对客户进行身份验证 。 “无身份验证”是一个选项，这似乎令人惊讶，但它是支持没有 PIN 键盘的停车计时器等设备所必需的。除了 PIN、签名或什么都没有之外，终端 CVM 列表还可以指定设备上的身份验证，例如手机上的生物识别扫描仪。卡和终端都可以有风险管理逻辑来为不同的方法设置货币限额。但是 EMV 版本 1 有一个缺陷：身份验证方法列表本身并未经过身份验证，因此骗子可以在虚假终端攻击中操纵它 [169]。

一旦拥有中间人设备，许多攻击就成为可能。
我们的两个学生为电视节目实施了中继攻击；咖啡馆里的一个假冒终端通过无线电连接到一张假卡上。当咖啡馆里的一名记者去一个学生经营的收银台支付 5 英镑购买蛋糕时，交易被转发到另一名学生携带的假卡上，后者正在书店里徘徊，等待以 1 英镑的价格购买一本书50。 50英镑的交易

成功通过[584]。这个主题有许多有趣的变体。不过,我们在野外找不到它们,因为它们很难扩展。

不同国家/地区的欺诈规模差异很大,这表明 EMV 的实际安全性取决于背景因素和实施细节 例如当地 ATM 将在多大程度上进行后备磁条处理,当地商店开放的比例各种类型的掠夺者攻击,以及 一如既往的 激励措施。银行是否像美国那样承担欺诈风险,这让他们小心翼翼,或者他们是否能够将成本转嫁给商家和持卡人?

EMV 推出期间的一个里程碑是“责任转移”。在许多国家/地区,监管机构允许银行通过更改条款和条件来强迫商户安装 EMV 终端,这样如果不使用 EMV,商户将对有争议的交易负责,但如果使用 EMV,则银行承担责任。

在那种情况下,欧洲大部分地区的银行只会将责任归咎于客户:“你的卡被使用了,你的 PIN 码也被使用了,所以你要承担责任。”所以从理论上讲,欺诈不再是银行的问题。在实践中,欺诈增加了,如图 12.4 所示。由于在转换期间从邮件中偷走了许多卡片,欺诈最初有所增加;银行匆忙推出,因为商户为欺诈支付了费用,直到他们拥有 EMV 终端,这需要时间 24。随着商店开始配备终端机,人们习惯于在其中输入 PIN,不法分子使用不良终端机窃取卡数据来制作磁条副本,以便在 ATM 机上使用,随后假冒产品激增。不过,最大的变化是邮购和在线欺诈的激增。最终效果是,到 2007 年 10 月,欺诈比前一年增加了 26% [126]。

如果不是一些公然的操纵,欺诈数字本来会更高。从 2007 年 4 月起,英国银行客户被禁止向警方报告信用卡欺诈;这笔交易是由布莱尔政府在银行和警方之间谈判达成的,目的是压低犯罪统计数据,为此它曾两次受到议会委员会的批评。适当的欺诈报告仅在 201525 年才重新引入。您可以从 2008 年至 2016 年图 12.4 中红线的下降部分看到其影响;那些丢失的数百万美元包括大量简单地倾销给持卡人的欺诈成本。

银行还接管了调查信用卡欺诈的小型警察部门的大部分资金,因此它们对确实发生的此类起诉有一定的控制权。

12.6.1.2 ICVV、DDA 和 CDA

为了阻止磁条回退欺诈,银行从 2000 年代中期开始实施集成电路卡验证值 (iCVV),一种 CVV,即

24这导致了商人和银行之间多年的不和。

25到那时它已经达到了它的政治目的。从 2007 年到 2015 年,犯罪率稳步下降,因为它像其他一切一样在网上移动,而在线部分没有被正确计算。 2016 年,特蕾莎·梅 (Theresa May) 竞选保守党领袖时,她对党员的一项主张是,尽管将警察人数从 14 万减少到 12 万,但她仍会减少犯罪;这种说法在技术上是真实的,至少在报告的犯罪中是这样。当鲍里斯·约翰逊 (Boris Johnson) 在 2019 年接替她时,他声称在 2008-16 年担任伦敦市长期间犯罪率有所下降。这种说法在技术上什至是不正确的,因为一旦国家统计局坚持从 2015 年开始正确计算,英国报告的犯罪率就翻了一番。

芯片中的卡数据与磁条（在磁条 ATM 交易中读取)和签名条（在线使用)上的版本不同。一旦这三者都不同 ，理论上,仅芯片分离器就不能用于制作有效的磁条伪造品,即使商家通过将签名条 CVV 保存在数据库中来违反 PCI DSS 规则,然后被黑客攻击,这个 CVV 应该不足以允许磁条伪造或肯定卡伪造（这被称为通道分离）。三个 CVV 的计算方式都相同 作为 PAN 上的三位数 MAC、版本号和到期日期,使用三重 DES 计算,但在计算中使用不同的服务代码值。

动态数据认证 (DDA) 是 EMV 的当前默认变体。
它最初在德国使用,从 2011 年开始在整个欧洲使用。 DDA卡可以进行公钥加密:每张卡都有一个私钥KC,其公钥嵌入在卡证书中。密码学用于两个功能。

首先,当卡首次插入终端时,它会发送一个随机数,并对其进行签名,以确保该卡存在于终端（某处）。然后终端发送一个包含“不可预测的数字”的块和使用卡的公钥加密的 PIN,然后是交易数据,卡像以前一样返回应用程序数据密码。这会阻止 skimmers 收集PIN26。早在 2000 年代,DDA 卡的价格是 SDA 卡的两倍;卡片现在非常便宜,DDA 的主要额外成本是卡片个性化速度较慢。

联合数据认证 (CDA) 是 Rolls-Royce 的变体。它类似于 DDA,除了该卡还计算 MAC 上的签名。这使得离线操作更加安全,因为终端现在可以验证交易。它将交易数据与公钥以及执行 PIN 验证的事实联系起来 假设银行选择了在交易数据中包含 PIN 验证标志的选项。至于为什么这很重要,请考虑无 PIN 攻击。

12.6.1.3 无密码攻击

2009 年,我们收到了几位欺诈受害者的可靠投诉,称他们的卡被盗,然后在商店中用于银行拒绝退款的交易,声称他们的 PIN 已被使用 同时他们坚称 PIN 不可能被泄露。 Steven Murdoch、Saar Drimer 和我进行了调查,发现中间人设备可以告诉终端卡已接受 PIN,同时告诉卡终端已启动芯片和签名交易 [1364].一些国家的银行不使用 PIN,通常是因为监管机构不允许责任转移;英国的一些银行允许客户拒绝 PIN 并获得美国风格的芯片和签名卡。

在该协议中,卡数据d3包含一个标识PIN是否被验证的标志,终端单独向其收单银行返回一个标志,并带有相同的信息。然而,卡片标志是专有的

26 由于卡片数据仍然清晰,不法分子仍然可以通过目视收集 PIN 并尝试磁条回退,希望发卡行不检查 CVV;一些银行显然仍然没有。

发行人,而不是 EMV 标准,因此默认情况下不检查它。

2011 年 5 月,四名罪犯在法国被捕,Houda Ferrari 等人在最后一次上诉结束后于 2015 年发表了一份法医报告。
No-PIN 攻击是通过从被盗卡上切下芯片并将其粘合在爱好者智能卡的芯片下方来实现的,然后对智能卡进行编程以执行中间人攻击 [680]。该团伙使用 40 张改装卡在 7,000 多笔交易中窃取了约 60 万欧元,其中 25 张被警方没收。

一家英国银行在 2010 年底阻止了这次攻击,但该阻止在 2011 年初被移除,这可能是因为严格的错误处理导致了太多的误报(终端标志可能丢失或错误)。对我们披露该漏洞的反应有些消极;银行的贸易协会写信给大学,要求它取消一名学生的硕士论文,该学生的项目是建立一个更强大的中间人装置来调查这些问题(大学当然拒绝了)[77]。直到 2017 年,这种攻击才在英国彻底停止。但是,如果卡或商户终端是由非英国银行发行的,攻击可能仍然有效。

覆盖智能卡可能在 2018 年底在中国和可能的意大利被用于此类攻击。这些是非常薄的智能卡 - 大约 180 微米厚 - 顶部和底部都有触点。它们是在中国开发的,支持手机漫游;这个想法是您将一个贴在普通手机 SIM 卡上以提供替代方案。叠加层充当经典的中间人。这些设备是攻击的理想选择;它们广泛可用,使您不必构建繁琐的自定义硬件,并且易于使用(您可以在 JavaCard 中对它们进行编程)。

12.6.2 预演攻击

2011 年 6 月 29 日,一位在马略卡岛度假的汇丰银行的马耳他客户发现他的账户中有四笔 ATM 交易被扣款,尽管他当时持有该卡。前一天晚上,他在一家他认为员工可疑的餐厅吃过饭,想知道他的卡是否被复制了。汇丰银行拒绝给他退款。所以他联系了我们,我们建议他索取交易日志。原来,ATM 生成的“不可预测的数字”只是一个每 3 分钟循环一次的 16 位计数器。

对于DDA/CDA卡,EMV认证步骤为:

吨! C : T, N, t, X, d2, {PIN}KC C ! T : d3,
MACKCB(d3, T, N, t, X)

如果我知道在明天的日期 t 时给定终端将生成哪个“不可预测的数字”N,并且我今天手里拿着你的卡,那么我可以计算出 ARQC MACKCB(d3, T, N, t, X)那将在明天在那台机器上工作。 Mike Bond、Marios Choudary、Steven Murdoch、Sergei Skorobogatov 和我因此安装了一张支付卡,通过连接微型微控制器,

内存和时钟芯片,并调查了英国剑桥周围的自动取款机。
我们发现几乎一半的人将计数器用作“不可预测的数字”。
其他人有带有卡位的随机数生成器。然后我们回到 EMV 规范,发现终端的测试例程只需要测试人员绘制三个“不可预测的数字”并检查它们是否不同。

那么这可以在英国大规模利用吗?

下一个数据点出现在 2012 年 9 月,当时一名苏格兰水手在巴塞罗那旅游街兰布拉大道的一家酒吧点了一杯酒。他用他的 EMV 卡支付了 33 欧元,至少他是这么想的。他昏倒了,第二天早上醒来,发现当天晚些时候他在劳埃德银行的账户被扣了十笔 e3,300 的借记 当时总计 24,000 英镑。银行声称,由于芯片和密码已被使用,他有责任。他指派了聘请我们的律师,并从银行拿到了交易记录。事实证明,这十笔交易是均匀分布的,通过三个不同的收单银行提交,虽然它们是在同一个终端上进行的,但终端在这些银行中的每一个都注册了不同的特征。

这是技术操纵的明显证据,水手收回了他的钱。我们将此称为“预播放攻击”,因为其本质是记录您将在未来预订的交易,而不是重播旧交易。如果将使用相同的终端,那么正是终端生成“不可预测的数字”这一事实使得攻击变得容易 [282]。

从那以后,我们在欧洲的一些国家看到了赛前攻击的案例,通常是针对脱衣舞俱乐部和其他色情行业公司的顾客。
在英国,伯恩茅斯一家膝上舞俱乐部的一位顾客在 2014 年抱怨说,工作人员让他喝醉了,并在 13 笔交易中向他收取了 7,500 英镑 [334]。
在媒体宣传之后,还有十几名其他受害者挺身而出,其中包括那些在回到家躺在床上后遭受借记的人 [1948 年]。这表明这是一场预演攻击,而不是妓女滚动醉酒顾客的简单案例;地方当局对此感兴趣,俱乐部被“试用”六个月。然而,我们无法说服警方突击搜查俱乐部并寻找证据,最终它获得了完整的执照。 2020 年,伦敦的一家俱乐部在向客户多次收费后实际上失去了执照,一些受害者被骗上万 [1341]。事实证明,在欧洲其他地方也很难。波兰克拉科夫的一家这样的俱乐部遭到突击搜查,但警方没有寻找技术证据。终端可能以多种方式受到损害:除了糟糕的随机数生成器之外,他们的供应商可能无法修补他们的软件,现在有些甚至让运营商在他们身上运行应用程序 27。所以预演问题仍然存在,我担心最终我们会遇到一起凶杀案。玩前攻击的皮条客似乎经常在受害者的饮料中下毒,如果你对醉汉进行麻醉并让他们在妓院的沙发上睡觉,同时抢劫他们的银行账户,那么他们中的一个人迟早会吸入一些呕吐物.

关于安全可用性的一个有趣的观点是,如果您的钱包或钱包中有四张或五张卡,那么如果您将它们的所有余额和信用额度加起来,再加上卡公司可能给您的额外“未经授权的透支”,

27Dixons Carphone 在 2020 年被罚款 500,000 英镑,原因是恶意软件感染了 5,390 个收银机,损害了 1,400 万人的个人数据和 560 万张卡片的数据。前一年,他们因类似的失败被罚款 400,000 英镑 [2039]。

您可能正在以汽车的价格四处走动。如果你口袋里有那么多现金,你可能不会去城里的坏地方。除非你有几个大朋友,否则你甚至可能在大街上行走都不舒服。支付卡掩盖了这种审慎的反应,使我们能够比在冷静和清醒时花更多的钱。除了欺诈之外,还有漏洞问题。例如,英国政府刚刚禁止在赌场使用信用卡。如果您正在设计一个接受受监管产品在线支付的系统,或者如果您的产品将来可能会因为它们会让人上瘾而受到监管,那么您需要解决从道德到地理定位再到仲裁的一系列问题。

12.6.3 非接触式

非接触式支付于 1997 年由美孚在美国率先推出,并于 2000 年代在从伦敦到东京的许多交通系统中采用。到 2007 年,您只需在日本地铁十字转门上触摸手机即可通过。同年巴克莱银行发行了第一张非接触式银行卡； VISA 和 Mastercard 开发了用于支付的非接触式 EMV 变体;谷歌于 2011 年使用万事达卡 PayPass 标准推出了 Android Pay28。这些早期采用者努力让商家改变他们的支付终端,而媒体和公众仍然持怀疑态度。 2014 年苹果推出 Apple Pay 时,市场出现了转机。到 2017 年,由于点击支付的便利性,卡支付在英国已超过现金支付； 2018 年,借记卡在美国超过现金,使用移动在线应用程序的美国消费者比例从 40% 上升到 60% [707]。 2020 年的冠状病毒大流行导致从现金到非接触式的进一步大规模转换,英国 ATM 交易从 1 月的 2.32 亿笔下降到 4 月的 9100 万笔,现金交易从三分之一下降到十分之一,而非接触式限额从 30 至 45 英镑。

基本思想很简单。在美国,终端生成一个“不可预测的数字”N,卡使用 KC 在选定的交易数据上生成动态 CVV 作为 3 位 MAC,并与 N 一起发送给发卡银行。为了扩展处理,CVV 密钥可以提供给收单银行的 HSM 和代表它们的服务公司。

交易限额降低了风险 2020 年,美国为 100 美元,英国为 30 英镑。一些发卡机构有一项政策,在一定数量的非接触式交易后,持卡人必须使用 PIN 进行完整的 EMV 交易;这会导致某些应用程序出现复杂情况。在英国和欧洲有一种变体,其中制作卡片以生成 ARQC,该 ARQC 可以发送到银行网络以进行随机检查。

与常规 EMV 一样,N 由终端而非银行生成,因此预播放攻击是可能的,但在大多数国家/地区,由于交易限制,这不是问题29。然而,非接触式支付从卡到手机的扩展导致了额外的复杂性,我们的系统

28完全披露:我在设计上为谷歌做了一些工作。
29在德国,您通过非接触式支付进行大额卡支付,并结合 ATM 交易中的在线 PIN 验证,但我不知道有任何预播放事件。

现在有两个卡计划的竞争提案的混搭。
在某些 Android 手机中,信用卡变成了虚拟信用卡,在执行非接触式 RF 协议的 NFC 芯片中的安全元件中的 Java Card 中实现； Apple 与 Apple 类似,但密钥材料位于 iPhone 的安全飞地中。其他 Android 手机使用主机卡模拟,其中 NFC 功能在软件中提供。 NFC 芯片或功能也开始出现在手表、手镯和其他设备中。许多使用令牌化,其中电话或其他设备由代表银行行事的在线令牌化服务提供商 (TSP) 提供令牌 30 和密钥材料。商家将交易发送给 TSP,TSP 在其 HSM 中执行适当的加密操作并将交易转发给客户的银行。

当推出非接触式卡时,通常会出现实施失败。在某些商店,如果您使用接触式交易付款但将钱包或手袋放在终端附近且里面有一张不同的非接触式卡,您可能会被收取两次交易费用。研究人员还想知道,骗子是否可以通过在街上擦过受害人的卡片时与他们进行 RFID 交易,或者在不打开信封的情况下阅读邮寄的卡片来获取信用卡号、安全代码和有效期[894]。来自纽卡斯尔的 Martin Emms 及其同事证明了这是可能的,并发现了一些更有趣的缺陷:一家英国银行甚至让您猜测 PIN;与其他人一样,外币交易的现金限额失败 [628]。2016 年 11 月 5 日,这导致了针对英国 Tesco 银行的重大欺诈,当时巴西的骗子通过在移动设备的非接触式界面上使用磁条数据发布了高价值交易。来自 8,261 个客户账户的虚假交易总计 220 万英镑,尽管最终损失仅为 700,000 英镑,但这次攻击引发了大量欺诈警报,银行的周末工作程序无法应对。直到11月7日才将欺诈交易流阻断,很多合法交易也被阻断,9日才恢复正常客服。由于这次失败以及给客户造成的困扰,监管机构对银行处以 1640 万英镑的罚款 [687]。

2019 年,Leigh-Anne Galloway 和 Tim Yunusov 发现你可以通过伪装成手机将非接触式限额从 30 英镑提高到 5500 英镑,而且还有一种可利用的预播放攻击。这些攻击利用了电话/卡/终端的复杂性。Android 手机可以有多个限制,具体取决于屏幕是关闭还是打开,以及用户最近是否进行了身份验证;并且电话和终端相互发送未经认证的标志[736]。 2020 年,David Basin、Ralf Sasse 和 Jorge Toro 发现了一种改进的中间人攻击,其中交易从被盗的卡通过两部手机路由到非接触式终端,该终端接受持卡人使用手机自己的身份验证机制进行验证的声明,例如生物识别[182]。银行的欺诈引擎可能会阻止此类攻击的规模扩大,并且它们尚未出现在统计数据中（尚未）。然而,我们仍然收到持卡人的投诉,他们的卡被盗后成为欺诈的受害者,他们声称他们的 PIN 没有被泄露,而他们的银行声称它一定已经被泄露。

30 There s a payment account reference (PAR),卡号的永久化名

我们开始看到不依赖于特定硬件但允许使用其他通道来运行协议的创新变体,例如 QR 码。我们将不得不拭目以待,看看这些是否会导致大规模的中间人攻击。

第二代 EMV 的设计者正在谈论关闭所有明文间隙,甚至添加距离边界作为选项。此类技术可以阻止此处描述的许多攻击。但是现在非接触式已经运行了几年,主要问题就比较平淡了,包括卡冲突:如果你的钱包里有三张卡,你在地铁十字转门上挥动钱包,哪一张会被扣款?卡片选择机制不够强大,无法给出可重复的答案 [1287]。这是伦敦的一个问题,如果你接入当地的交通系统但未能再次接入,你将被收取最高票价。如果进出十字转门在您的钱包中看到不同的卡片,您最终将支付最高金额的两倍。

最近的一项发展是 COTS 上的软件 PIN (SPoC),其中一种明文磁条加上高度加密的 PIN 的旧假设被推翻了:SPoC 规则是 PIN 不能受到严格保护的设备绝不能学习相关的卡数据。如果在商家的 iPhone 中输入 PIN,就像我们现在在 Apple 商店看到的那样,还有另一个组件称为安全读卡器 – PIN (SCRP),它插入手机并接受客户卡。即使手机应用程序遭到破坏,坏人也不知道 PIN 码适用于哪张卡。手机还将客户 PIN 码传递给 SCRP,在 SCRP 中加密并发送 o 进行在线验证。

还有一些方法可以在普通手机上接受非接触式支付;据推测,下一步将是通过一起点击手机来支付人们的费用,其中一个模拟卡,另一个模拟终端。在肯尼亚和孟加拉国等国家,电话对电话的直接支付已经成为数以千万计的人的家常便饭,正如我将在下面的第 12.8.1 节中描述的那样。将此类系统与 EMV 世界结合起来并使整个系统使用安全将是一个有趣的挑战。

12.7 网上银行

在信用卡和借记卡之后,支付领域的第三个线程是通过您的 PC 或手机进行银行业务。

1985 年,苏格兰银行提供了世界上第一个家庭银行服务,其客户可以使用英国电信运营的专有电子邮件系统 Prestel 进行支付。当 Steve Gold 和 Robert Schifreen 入侵 Prestel 时 如前文 3.4.4.4 节所述 它吓坏了媒体和银行家。但真正的风险很小。该系统只允许指定账户付款 你只能在你自己的账户和你通知银行的账户之间汇款,比如你的天然气和电力供应商。在早期,这意味着要去一家分行,填写一份纸质同意书,然后等到收银员检查收款人帐号。

20 世纪 90 年代初期,电话银行业务迅速发展,银行紧随其后
1990 年代后期的网站,然后钓鱼者就来了。

12.7.1 网络钓鱼

在第 3.3.3 节中,我总结了网络钓鱼的历史,从 1990 年代开始到 2003 年开始针对在线银行账户的使用。坏人从 http://www.barqlays.com 等错误域名到欺骗性域名开始使用粗略的诱饵比如 http://www.barclays.othersite.com;银行最初的反应是责怪他们的客户。随着地下犯罪论坛从 2005 年左右开始发展,支持日益专业化,就像在正常经济中一样,帮派迅速变得更加老练。一个团伙编写恶意软件,另一个团伙组织僵尸网络,我们开始看到接受热钱并洗钱的专家。通常的技术是尽可能地掠夺任何客户账户,然后将钱发送到恢复速度最慢的任何一家银行的受损账户。在 2006 年英国银行损失的 3500 万英镑中,有超过 3300 万英镑是一家银行损失的。它的一位竞争对手告诉我们,秘诀在于快速发现帐户接管并积极跟进;如果钱被送到了一个骡子的账户,他应该在他走到西联汇款之前发现他的账户被冻结了。所以洗衣工学会了避开他们。

该行业学会了尽快删除网络钓鱼网站,专业的删除公司也擅长于此。坏人用快速通量等技巧做出回应,其中钓鱼网站托管在僵尸网络上,每个回答诱饵的标记都被发送到不同的 IP 地址。

第二个战场是资产追回:骗子会想方设法把钱迅速转移到海外洗钱,而行业和执法部门会想方设法阻止他们。直到 2007 年 5 月,首选路线是 eGold,这家公司在佛罗里达州运营,但在加勒比地区有合法住所,提供不受监管的电子支付。在 eGold 被 FBI 突击搜查并关闭后,这些恶棍开始通过芬兰的银行向其在波罗的海国家和俄罗斯的子公司汇款。第三种选择是像西联汇款这样的电汇公司:钓鱼者通过提供在家工作的工作来招募骡子,并作为一家外国公司的代理赚取佣金。他们被告知他们的工作是每周收到几笔付款,扣除他们自己的佣金,然后通过西联汇款 [789] 发送余额。俄罗斯和中东也有各种电子货币服务 [75]。监管机构打地鼠仗:一个渠道关闭后,另一个渠道将开放。容易洗钱的银行 在业内被称为“骡子银行” 遭受的欺诈甚至更少,因为大团伙避免瞄准他们的客户,希望他们能作为第二个环节保持有用的时间更长链。这场战斗仍在继续,资金通过从加密货币到亚马逊礼品卡的各种方式进行洗钱。

这强调了我们在上面第 12.2.4 节中介绍的预防 - 检测 - 恢复模型的重要性。如果单靠身份验证无法完成工作,并且您无法在杀伤链中找到其他易受攻击的点,则需要加强补充它们的入侵检测机制。

12.7.2 上限

2006 年,银行宣布了基于 EMV 的双因素认证标准,并于次年推出。芯片认证程序 (CAP)31包含一个手持式密码计算器,您可以将 EMV 银行卡放入其中。您输入密码;设备获取卡进行检查;然后您可以执行三个功能之一。您可以获得一次性密码登录,您可以回答登录挑战,或者您可以验证一系列数字,通常来自收款人帐号和金额。

当前版本在 EMV 卡上使用自定义应用程序,该应用程序使用与发卡行共享的密钥来计算提供的数据和应用程序交易计数器 (ATC) 上的 MAC（不同于用于点-售交易）。响应代码是截断的 MAC 和截断的 ATC。安全性在[585]中讨论;简而言之,如果您将卡放入损坏的终端,这会生成一个 CAP 代码以登录您的在线银行服务,尽管这很难扩展,因为您通常还需要密码。 CAP 读卡器的可用性意味着劫持您的银行卡的劫匪可以索取您的 PIN 码并进行检查,而不必将您带到 ATM 机并冒着被闭路电视看到的风险。这导致了凶杀案,并且是疏忽的设计:如果您提供了错误的 PIN,其他密码计算器只会返回错误的结果,包括我在第 4.3.2 节中描述的 1980 年代的早期设计。

12.7.3 银行恶意软件

随着银行通过使用从部分密码问题到早期双因素身份验证方案的更复杂的身份验证机制,使简单的网络钓鱼攻击变得更加困难,一些坏人只是更加努力地进行说服。

即使在德国,其银行会向客户提供打印的一次性密码列表,骗子也会说服一些客户一次性输入所有密码。

其他坏人转向自动化,以银行恶意软件的形式出现。从 2007 年开始,Zeus、Torpig、SpyEye、EMotet、Trickbot 和 Dridex 等一系列恶意软件从全球银行及其客户窃取了数亿美元,并通过各种技术传播,包括 Word 宏和路过式下载。

到 2011 年,中间人攻击发展为浏览器中人攻击:当受感染 PC 的用户开始使用他们的银行账户时,浏览器恶意软件可以主动修改交易数据,以便他们看到的是 他们授权什么。这就是为什么谨慎的银行现在使用第二个因素（例如 CAP)来至少验证任何新收款人帐号的最后四位数字。不使用 CAP 的银行可能会使用专用的身份验证设备或基于电话的第二因素。

12.7.4 电话作为第二因素

对 2000 年代中期网络钓鱼浪潮的另一种反应是使用客户的电话作为第二因素。发送确认似乎很自然,

31这是发明它的万事达卡的品牌名称； VISA 称之为动态密码
身份验证 (DPA)。

例如：“如果您真的想向 Russian Real Estate LLC 汇款 7500 美元，请立即在您的浏览器中输入 4716。”这似乎提供了与 CAP 相同的好处，但具有更好的用户界面。

然而，在南非银行于 2007 年开始实施后，他们很快就发现了第一起 SIM 交换欺诈案。约翰内斯堡的一些骗子用一家照顾孤儿和弱势儿童的慈善机构首席财务官的电话号码获得了一张新 SIM 卡，并从其银行账户中盗取了 R90,460 [1514]。银行向电话公司投诉，电话公司毫不留情：电话公司卖的是通话记录，不卖银行认证服务。正如我在第 3.4.1 节中讨论的那样，此类欺诈从南非传播到尼日利亚，然后从大约 2014-5 年传播到美国，在那里它们最初被用来窃取 Instagram 帐户，并从 2018 年开始在比特币交易所抢劫人们的帐户 [1092] .

此类攻击现在涉及电话公司内部人员。在 2019 年的一起案件中，亚利桑那州图森市的一名 AT&T 承包商帮助一个 SIM 卡交换团伙从 29 名受害者那里窃取了 200 万美元 [711]。 2020 年，凯文·李 (Kevin Lee) 及其同事尝试在五家美国电话公司中的每家更换十张 SIM 卡，结果发现这很容易：对于大公司，每次都能奏效。漏洞包括通过询问最近的通话和最近的充值来验证人们的身份，这两者都可以被攻击者操纵 [1136]。另据报道，SIM 交换器通过社会工程学攻击电话公司员工，让他们在自己的 PC 上安装远程访问工具，然后使用被破坏的机器将目标电话号码重新分配给他们控制的 SIM [485]。数以万计的客户服务代表可能会粗心大意、遭到黑客攻击或从 SIM 交换团伙那里收受贿赂。有些人已经收受贿赂来解锁被盗的手机，一旦这些地下社区联系起来，我们可以预料事情会变得更糟。在德国和英国也有一些案例，攻击者利用 SS7 信令协议远程窃听目标的手机并以这种方式窃取代码 [489]（我将在第 22.1.3 节中进一步讨论） .在中国，法律要求您去手机店并出示身份证件才能购买 SIM 卡；在印度，您需要进行生物识别检查，并且电话公司还对 SIM 卡交换欺诈承担部分责任。然而，美国和欧洲的旅行方向不再是将 SMS 作为第二个因素，而是转向定制手机应用程序 32。

但正如我在 2007 年本书的第二版中所写，“双通道身份验证的安全性依赖于通道的独立性……如果每个人都开始使用 iPhone，或通过无线接入点进行 VoIP 电话，那么独立的假设被打破了。”

在欧盟，第二个支付服务指令现在要求银行使用双因素身份验证。所以它变得普遍，坏人在破解它方面得到了很多练习。但是，如果您不是在笔记本电脑上而是在手机应用程序上进行银行业务，并且使用另一个手机应用程序作为您的第二个因素，会发生什么情况？如果恶意软件扎根您的手机，它是否会接管这两个应用程序并盗用您的帐户？

在撰写本文时（2020 年），欧洲中央银行认为只要您使用运行时应用程序自我保护，两个应用程序就可以
(RASP)，这意味着您使用那种技术混淆了应用程序代码

32 银行使用硬件令牌作为第二因素或软件令牌或 SMS 的数据，
或者根本没有第二个因素，可以在 https://twofactorauth.org/#banking 找到。

1980 年代为软件版权保护和 1990 年代为数字版权管理开发的技术。这让经验丰富的安全工程师望而却步,因为这种机制的历史并不好;在关于版权和 DRM 的章节中有讲述,我在第 24.3.3 节进一步讨论了 RASP。很难保证破解混淆方案需要多长时间;任何时候都必须预期会出现中断,并且此类方案的用户最好准备好在发生时立即对其进行修补。也许攻击者可能需要做的就是填充网络堆栈中的一种方法,以获取包含身份验证交换的字符串。因此他们可能不需要提取密钥或以其他方式破坏 RASP 机制本身。

12.7.5 责任

一个长期存在的争论是关于责任的。对网上银行业务的热潮导致许多银行采用合同条款,将欺诈风险置于客户身上,这与消费者法和传统银行业务相冲突 [277]。不幸的是,欧盟 2007 年和 2015 年的支付服务指令在争议解决程序中留下了漏洞33。

对在 25 个国家/地区运营的 30 家银行的银行欺诈报销条款和条件进行的一项研究表明,安全建议种类繁多,其中大部分内容含糊、不切实际甚至相互矛盾 [201]。例如,汇丰银行要求每个账户使用唯一的 PIN 和密码,这与英国银行行业协会早先建议客户将所有 PIN 更改为为其中一张卡发行的 PIN 的建议相反。它还对网上银行提出了最繁重的要求,包括必须始终手动将银行的 URL 输入浏览器。它和许多其他银行一样,要求客户使用防病毒软件;更少的人要求对软件进行最新修补。

与此同时,银行通过商业实践训练他们的客户容易受到攻击,例如告诉他们的客户泄露他们的安全数据,即使是在拨打未经请求的电话时也是如此。我个人接到过我的银行打来的不请自来的电话,说 你好,这里是 Lloyds TSB,你能告诉我你母亲的娘家姓吗?您非常想告诉他们迷路,但如果您这样做,重新激活或更换您的支付卡会很麻烦。即使安全仪式变得更加复杂,如果需要作为中间人(或浏览器)攻击,网络钓鱼者仍然可以通过它谈论标记。

然而,大约在 2015 年左右,坏人开始进化出更好的方式。

12.7.6 授权推送支付欺诈

授权推送支付(APP)欺诈是指诱使客户进行银行转账。 2017 年才开始收集数据,

33 英国银行让英国政府在第 72(2) 条中“必要地”插入:“如果支付服务用户否认授权已执行的支付交易,支付服务提供商记录的支付工具的使用,包括支付启动服务提供者(视情况而定)本身不一定足以证明支付交易是付款人授权的,或者付款人有欺诈行为或故意或重大过失未能履行第 69 条规定的一项或多项义务。

2018 年的数据与 2017 年的计算方式不同,因此我们没有在图 12.4 中显示这些数据。然而,总额为 3.543 亿英镑,仅次于远程购买欺诈,并且超过其余部分的总和。

一个典型的作案手法是寻找正在买房的人,然后发送一封看似来自他们律师的电子邮件,通知他们公司的银行帐号已更改。另一个是针对弱势老年人。在一个案例中,一名 92 岁的退伍军人被冒充他的银行 A 银行的骗子打电话,告诉他银行被黑了,因此他不得不将毕生积蓄 120,000 英镑转移到银行 B保管。两天后,他的儿子来探望并了解了事情的经过。在这个特殊案例中,他们的律师要求 B 银行出示用于开设 mule 账户的了解你的客户的文件。几天后,B银行（素有“骡子银行”之称)怯生生地退了钱。

那个受害者很幸运,但很多人就没那么幸运了。大额欺诈变得容易,因为银行使大额支付变得容易;在过去,取出 120,000 英镑至少需要安排与银行经理的会面。然而,网上银行已与即时支付系统相结合,这意味着欺诈者可以获得五位数甚至六位数的金额。在英国,这成为一个痛点,以至于议会的财政部委员会指出,快速不可撤销的支付只是错误的违约 [1361],支付服务监管机构改变了规则,以便银行现在承担部分责任。因此,进行大额银行转账变得更加复杂。即使是中等规模的交易也会被搁置;如果你想付给你的水管工几千美元来翻新你的浴室,你很可能会接到银行打来的焦急电话,并需要接受一些安全仪式。

针对公司的类似欺诈也一直在稳步增长。它们被称为商业电子邮件泄露 (BEC),现在每年造成数十亿美元的损失 [91]。在最近的一个案例中,荷兰的一家博物馆同意以 240 万英镑的价格从伦敦一家艺术品经销商处购买约翰·康斯特布尔 (John Constable) 创作于 1855 年的一幅画作,但在骗子入侵了博物馆的电子邮件帐户并发送了看似来自来自经销商。博物馆起诉经销商但败诉 [506]。受害公司受到的保护远少于消费者,但有一些缓解措施对两者都有帮助。例如,英国监管机构要求银行实施收款人确认:当您首次向新账户付款时,系统会要求您提供账户持有人的姓名,如果有误,您会收到提醒[1361]。尽管如此,现在谨慎的做法是在商业合同中对公司银行帐号进行硬编码,这样一来,如果 A 公司向骗子 C 而不是 B 公司付款,就没有争论的余地了。在德国　公司自 20 世纪以来一直使用直接银行付款　多年来,公司在信笺上打印银行帐号一直是一项法律要求。

12.8 非银行支付

除银行外,还有许多付款方式。 PayPal 是许多基于电子邮件的支付服务提供商的幸存者,这些服务提供商如雨后春笋般涌现

在互联网繁荣时期兴起,现在实际上已经成长为一家银行,提供传统和新颖的支付服务组合。更传统的服务是哈瓦拉,这个术语指的是为南亚和中东移民社区提供服务的货币兑换商,帮助他们将钱寄回家。他们与与维多利亚电报网络一起成长起来的西联汇款以及提供低成本外汇交易的更现代的支付服务提供商竞争。其中一些服务被网络犯罪分子使用,最著名的是 PayPal 和西联汇款。西联汇款对执法部门来说是一个特殊的问题,因为犯罪分子可以向其众多分支机构中的任何一个汇款并提取现金。所有此类供应商在欧盟都受到 2009 年电子货币指令的监管,该指令制定了资本和流动性规则。还有一些加密货币,例如比特币,一些监管机构目前豁免电子货币监管,我将在高级密码工程一章中讨论。

两种特殊类型的支付服务值得单独讨论:电话支付和覆盖支付,其中主要的例子是 M-Pesa、支付宝/微信支付和 Sofort。

12.8.1 M-佩萨

M-Pesa 是肯尼亚的一项手机银行服务,由 Voda fone 于 2007 年推出。它发展迅速,运营它的公司 Safaricom 现在是肯尼亚最大的金融机构。欠发达国家推出了 200 多项类似服务,其中约 20 项发生了变革;现在最大的此类服务可能是孟加拉国的 B-Kash。在 2020 年冠状病毒封锁期间,许多此类服务一直在快速增长。

M-Pesa 开始作为内罗毕和蒙巴萨的农民工向农村亲戚汇款的一种方式。在手机出现之前,这意味着邮寄现金,或者与朋友或公交车司机一起汇款 既不方便又危险,尤其是在前一年有争议的选举之后的 2008 年内乱期间。手机普及后,人们开始购买通话时间作为转移价值的手段,从那里开始向转移实际价值迈出了一小步。此类系统的安全机制往往很简单,通过 SMS 或 USSD 发送加密的 PIN、收款人和价值。

关键的成功因素在于,电话公司已经建立了由数以万计的销售代理组成的网络,这些代理可以将现金转化为数字信贷并再次返回 网络覆盖最小的村庄,这与传统银行不同。操作问题与人们错误地向错误的电话号码汇款以及将收到的 M-Pesa 付款与业务系统集成有关。

12.8.2 其他电话支付系统

许多其他国家/地区都有电话支付系统,或者拥有广泛使用的在电话上运行良好的专有支付系统。其中的一个例子是 PayPal,它将您从商家网站重定向到 PayPal,您可以在其中登录以授权付款。直到 2013 年,这是世界上

领先的电话支付系统。从那时起,领先的手机支付机制就是支付宝,这是阿里巴巴集团在中国运营的专有支付应用程序。紧随其后的是腾讯的微信支付； 2020 年,它们分别占据了中国移动支付市场的 54% 和 39%。智能手机支付在中国迅速流行起来,就像 M-Pesa 在肯尼亚所做的那样,因为过去在主要城市以外的银行业务并不令人满意 [608]。它们已成为中国的默认支付机制,并使用可视化支付渠道:商户显示二维码,客户扫描该二维码即可将正确的金额发送到正确的账户。支付宝和微信支付不仅作为商业平台运作,而且作为国家基础设施运作,自 2018 年以来受到严格监管:中国人民银行获得所有交易数据的副本 [1529]。这符合我们在 2.2.2 节中讨论的中国对信息主权的态度。这两款应用现在都支持刷脸支付,这与我在第 17.3 节中讨论的面部识别技术在中国的日益普及保持一致。印度在 UPI 也有一个低成本的电话支付系统,与国家 Aadhaar 生物识别卡相关联;在这些国家支付和身份层上有许多相互竞争的支付应用程序。

12.8.3 Sofort、开放银行

德国传统上不使用信用卡,这在人们开始网上购物时很不方便。一种方法是从网站订购商品,获取商家的银行帐户详细信息和交易参考号,去您的银行付款,然后在第二天返回商家的网站并输入付款详细信息。

..

Sofortuberweisung 在德语中是“立即支付”的意思,并着手通过工业化的中间人攻击来解决这个问题。例如,为了购买机票,您点击航空公司结账页面上的“sofort”(“立即”)按钮,该服务会打开一个框架,您可以在其中输入您的银行名称和帐号。 Sofort 然后以您的身份登录到您的银行,并向您提供银行的身份验证质询。一旦你通过了这个,它就会进入你的账户,检查是否有足够的钱,然后自己付款。然后它会重定向回航空公司,您就可以拿到机票 [79]。其效果是使网上购物更容易,但也剥夺了银行的卡交易费(商家支付的费用约为他们为卡交易支付的费用的三分之一)。

银行起诉 Sofort 不公平竞争,并煽动客户在 Sofort 网站上输入他们的凭据来违反银行服务条款。

在德国联邦反垄断局辩称银行的服务条款阻碍了竞争并且旨在排除像 Sofort 这样的新商业模式之后,他们败诉了。 Sofort 获得了银行牌照,而其他银行只需要参与竞争。

结果是欧盟的第二个支付服务指令 (PSD2),也称为“开放银行”。自 2018 年 1 月起,银行必须开放其系统,不仅是在客户要求时以标准格式向其他受监管的金融机构发布交易数据,还允许其他机构按照客户的方式行事。好处将包括银行和金融科技公司提供仪表板,让你看到你所有的资产

您拥有账户的所有银行,并在它们之间转移资金以获得最优惠的价格。缺点是欺诈和洗钱活动正在迅速转移到开放的银行渠道。如果骗子在A银行开户,充入赃款,授权金融科技B的账户操作,然后利用B让A汇款给C,A不能拒绝交易。结果是对欺诈和洗钱的传统控制变得不那么有效了。所以安全工程师的工作岗位会更多34。我们将不得不拭目以待,看看这一切将如何发展。

将基于 QR 码的支付引入 EMV 标准开启了在全球范围内扩展类似 Sofort 支付机制的可能性。除了客户出示二维码支付工具外,商户也可以通过这种方式提出支付需求,客户手机即可发起网上银行支付。 M-Pesa 等现有电话支付系统还要求客户扫描二维码或手动输入数据(如果他们的手机无法执行此操作)。这里可能有一些创新和融合的空间,所以我们必须拭目以待,看看它会如何发展。

12.9 总结

银行系统对安全工程师来说至关重要,因为这是转移赃款的方式 而且在其他方面也很吸引人。簿记为我们提供了一个面向真实性和问责制而非机密性的系统的成熟示例。 Clark-Wilson 安全策略提供了这种方法的模型,它已经发展了几个世纪。使其在实践中运作良好意味着复杂的功能分离,其设计涉及许多学科的输入。威胁模型特别强调内部人员。

通过在第一代 ATM 系统中的使用,支付系统在密码学的发展中发挥了重要作用;基于智能卡的支付的采用再次改变了欺诈格局。

最后,自 2000 年代中期以来,我们已经看到了针对电子银行系统的几波攻击 通过网络钓鱼帐户凭据、通过专门恶意软件进行的浏览器中间人攻击、通过对用作二次身份验证的手机的 SIM 卡交换攻击因素,并通过社会工程学将客户直接汇款给坏人。这些已经逐步探索了高科技和低狡猾的可能组合,并且它们教导了采用整体方法来减少欺诈的重要性。大流行病引起的动荡可能会强调这一点,但至少使用激增的机制,例如发达国家的非接触式支付和其他地方的电话支付,已经有几年的时间才能平息。

34Open Banking 意味着从旧的 ISO 8583 标准迁移到更新的 ISO 20022。
这使得 PIN 块从 8 字节变为 16 字节,从而从 3DES 变为 AES;从交易后期批量结算到实时全额结算;还有更多。

研究问题

我一直不信任大型会计师事务所的卡特尔 从 1980 年代的八大会计师事务所到现在的四大会计师事务所,经历了 3 次合并以及安德森在安然丑闻中的失败。我和一个学生曾经想知道成为大型会计师事务所的客户是否是不当行为的信号,但简短的分析并没有提供任何证据。此后,当我在管理机构或审计委员会任职时,我总是建议使用本地公司,因为它更便宜,但只有一次设法改变(从一家大公司到另一家)。当我在我们大学的管理机构任职时,我不得不忍受这个卡特尔一年来动摇我们一百万美元并且没有提供任何有用的回报;大部分工作都是由初级人员完成的。我认为德国人可能更好,因为他们的规则禁止审计师出售咨询服务,但 Wirecard 丑闻打破了这种幻想。在那起丑闻(以及许多其他丑闻)之后,英国政府仍然决定,从 2024 年起,审计公司必须将他们的审计和咨询业务分开,这样审计合伙人的报酬仅来自审计业务,而不是来自咨询的交叉补贴 [1050]。如果能奏效,那就太好了,但我看不出它如何对本书中描述的大多数具体问题产生任何实际影响,无论是本章分析的内部控制问题还是我在第 28.1 节。审计卡特尔带来了巨大的社会成本,并不完全符合我们对标准经济分析的预期35。

需要更好地理解它。

设计内部控制仍然是不科学的;我们可以使用工具来帮助我们以更系统、更不容易出错的方式来做这件事。正如许多安全故障来自用户(默认情况下被提供危险的选择)和程序员(他们被赋予访问控制和其他使用起来非常棘手的工具)级别的可用性差一样,许多内部控制失败来自于为审计师的舒适而设计的管理机制,而不是在真实组织中实际使用。我们怎样才能做得更好?

支付系统一度非常保守,自 1970 年代以来在许多方面几乎没有变化,并且随着机制从 ATM 和 HSM 转移到芯片卡和手机中的加密芯片而不断发展。随着攻击的发展(如 SIM 交换)和环境的变化(如开放式银行业务),地面也在发生变化。面对这种变化保持弹性需要努力。随着 EMV 实施的收紧,以及第二版 EMV 开始解决此处描述的残留漏洞,我们可以预期欺诈将转移到外围:通过帐户接管转移到客户;通过黑客攻击、退款诈骗、优惠券诈骗等向商家提供;通过发行前欺诈和对授权和结算系统的技术攻击,向银行转移。

如果帐户接管将变得越来越普遍,这意味着什么?我怀疑我们的监管方法需要彻底改革:责备

35 请参阅第 28.2.8 节中讨论的 Lerner-Tirole 模型,了解面临合规要求的公司通常如何选择最便宜的供应商的模型。为什么大多数大公司甚至大大学都选择著名但昂贵的公司,因为它们几乎无法检测高管是否是骗子或公司是否在资不抵债的情况下进行交易?

指责普通客户因他人设计的系统而受到伤害是错误的。但是我们该怎么办呢?我们应该追求彻底的透明度、延迟付款,还是更加重视快速资产追回?是否有一些巧妙的组合,例如使付款的速度和最终性成为付款人和收款人已知身份的函数?还是监管机构应该继续将责任推回银行,让他们自己解决?

2020 年初的背景是,由于低利率和日益激烈的竞争,零售银行赚的钱比以前少了,因此银行安全工程师被要求事半功倍。社交媒体让停机时间变得更加痛苦;如果一家银行的移动应用程序由于网关上的 DDoS 攻击而停机 15 分钟,可能会出现推特风暴,导致董事们打电话给首席运营官。这种激励措施将学生转移到云中,但这会引发更多问题;我们将在后面的高级密码工程一章中讨论云 HSM。冠状病毒大流行对支付服务提供商来说是个好消息,PayPal 的股价上涨了约一半;至于它可能会在哪些方面推动金融科技创新,可能会围绕视频展开。对于贷款等复杂和高价值的交易,视频会议不得不取代分支机构内的会议。 Monzo 等金融科技公司的最新一波浪潮已经让客户录制自拍视频作为入职流程的一部分,这样呼叫中心的工作人员就可以帮助客户从丢失或被盗的手机中找回账户,从而确认他们是同一个人谁开的账户。还有什么?

进一步阅读

Andrew Jamieson 为 Underwriters Labora tories 写了一本关于 EMV 的 100 页电子书 – 是我这里空间的十倍 [977] – 这可能是我从简短摘要到 PCI 数千页规范的有用垫脚石SSC 和 EMVco [629]。我不知道有哪本关于核心银行系统的综合书籍,尽管国际清算银行提供了许多关于支付系统的论文:最新的,我们将于 2020 年 7 月出版,分析了服务质量和注释虽然欧洲境内的支付大多需要不到 30 分钟,但多个中介机构、营业时间、时区、资本管制、流动性和古老技术的结合意味着向亚洲和非洲的支付可能需要数小时到数天 [162]。如果你打算在内部控制方面做任何真正的工作,你最好阅读 ISA 315 [950];四大会计师事务所对它的解释现在对内部控制产生了影响。我将在第 3 部分中重新讨论这个主题。

要了解实际可能出错的地方,请阅读 Horizon 案的判决 [185] 以及 Alexander Dyck、Adair Morse 和 Luigi Zingales 对公司欺诈的调查 [596]。

生成和保护 ATM PIN 的 IBM 系统在许多文章中都有描述,例如 [521] 和 [951],而早期的 ATM 网络在 [763] 中描述。有关 ATM 欺诈的基础知识,请参阅 [55];而汇丰银行内部人士的审判记录提供了电子银行系统中典型内部控制的快照 [1569]。 Jason Franklin、Vern Paxson、Adrian Perrig 和 Stefan Savage 于 2007 年对地下市场进行了首次调查 [714];

即使在那时,重点还是放在银行欺诈上,而不是毒品或恶意软件上。从那时起,关于从地下社区的社会动态 [1345] 到 Dridex 恶意软件活动 [1622] 背后的俄罗斯人的主题的丰富文献。

我和我的同事在 2012 年 [90] 和 2019 年 [91] 对网络犯罪的大型调查做出了贡献。在我们的银行欺诈资源页面上有我们小组关于银行欺诈的著作集,网址为 https://www.cl.cam.ac.uk/~rja14/banksec.html。

有关大型信用卡欺诈的权威案例研究,请参阅 FCA 2018 年对 Tesco 银行的裁决 [687]。这不仅说明了欺诈是如何进行的,还说明了控制是如何在多个点上失败的,以及监管机构是如何计算罚款的。

最后,关于美国情报机构打击恐怖主义融资的政治和立法历史及其通过秘密或立法手段获取 SWIFT 数据的努力,请参阅 David Bulloch 的论文 [341]。