第14章

监控和计量

管理是没有算法的。哪里有算法,哪里就有管理。

罗杰·李约瑟

市场不是资本主义的发明。它已经存在了几个世纪。这是文明的发明。

- 米哈伊尔·戈尔巴乔夫

14.1 简介

除了我们在上一章讨论的防盗警报器之外,您的家中可能还有许多其他监控设备:电表、婴儿监视器、烟雾探测器、健身器材、健康追踪器和联网设备。

您还可以通过预付邮资标签从您家中的预付费公用事业仪表在线购买某些计量系统的价值。越来越多的系统关注监测和计量人类活动,实际上也关注自然环境。他们走了很远的路。蒸汽机先驱詹姆斯·瓦特 (James Watt) 不仅销售发动机,还销售发动机。他使用一个密封的计数器来获得专利许可,该计数器可以测量发动机的转数。他的检查员不时阅读这些内容,并向客户收取版税。

使用密码学和防篡改的电子系统已经取代了大多数旧的机械系统,并开辟了各种新的应用。票务规模巨大,从交通票到体育赛事再到优惠券;我的票务案例研究是用于燃气和电力的预付费仪表。然后我将转向车辆系统。其中最熟悉的可能是出租车计价器,但由于它们正在被电话应用程序取代,我将主要讨论行驶记录仪
欧洲和澳大利亚使用的设备,用于记录卡车和长途汽车司机的速度和工作时间,而在美国,记录银行卡车的进出。我的第三个案例研究是宵禁标签,在美国用于在审判前监视犯罪嫌疑人,在英国用于在释放后监视假释犯。我的第四个是用于邮寄信件的电子邮资计价器

包。

这些新应用程序中的许多都遵循传统的 IT 行业口号“周二发布并在第 3 版之前获得正确”。我们确实有物联网安全通用标准的开端，例如 ETSI 标准草案 EN 303 645，它列出了通常的母亲和苹果馅饼 stu ，例如没有默认密码、保护加密密钥、可更新软件、最大限度地减少攻击表面并允许用户删除个人信息[640]。但是将基本原理转化为良好的工程需要付出努力，我们可以从已经经历过至少一次攻击和防御迭代的应用程序中学到很多东西。我希望本章中的案例研究能够提供一些必要的背景洞察力。

你会记得，为了打败防盗警报器，做一个就足够了
它看起来不可靠。仪表增加了更多的微妙之处。

当我们讨论银行金库中的警报时，我们主要关注对通信的攻击（尽管传感器失灵也很重要）。但许多计量系统的物理暴露程度要高得多。出租车司机可能希望仪表读数比实际工作的里程数或分钟数多，因此可能会操纵它过度测量。对于行车记录仪，情况恰恰相反：卡车司机通常想要超速行驶，或者长时间危险地工作，因此希望行车记录仪忽略一些驾驶。公用事业消费者可能希望他们的仪表忽略一些通过的电力或天然气。刑事被告和假释犯可能想逃避宵禁令。在这种情况下，监视对象可能会导致设备出现错误读数，或者干脆发生故障。还有各种地下市场。

许多计量和监控系统也与证据有关。
对手可以通过操纵通信（例如通过重播旧消息）或谎称其他人已经这样做来获得优势。对于邮政邮资系统，攻击者造成失败是不够的（因为那样他就不能邮寄他的信件）。我们需要了解真正的威胁。邮政主要关注阻止批发欺诈，例如贿赂邮政员工将一卡车邮件放入系统的不正当直销商。该系统可能看起来像是为阻止外部欺诈而设计的，但它真正的重点是内部。

14.2 预付费仪表

在许多系统中，用户可以在一个地方支付令牌 无论是幻数、带磁条的纸板票、显示二维码的应用程序，甚至是可充值的芯片卡 并使用存储的值别的地方。示例包括交通票、图书馆的复印卡、滑雪胜地的缆车通行证以及大学宿舍的洗衣机代币。

主要的保护目标通常是防止代币被大规模伪造。复制一张票并不难，复制一个幻数很容易。如果我们使所有令牌唯一且所有设备都在线，则可以防止此类骗局。但这使事情变得脆弱；如果人们不能上车

在移动网络黑点中,或者如果数据中心出现故障,则无法使用滑雪缆车或洗衣机,这可能会损害业务并造成真金白银。所以重放和伪造检测有时必须离线完成。但是,如果我们简单地使用通用主密钥对我们所有的代币进行加密,那么恶棍就可以从被盗的终端中提取它并开始销售代币的业务。我们有哪些选择?

在大多数票务系统中,程序欺诈很容易发生。搭便车的人可以在地铁站跳栏杆;电表可以有一个旁路开关连接在它上面。但大多数人不会作弊,除非有人通过工业化使它看起来简单和安全。为了最大限度地增加收入,小额欺诈至少应该带来一些不便,而且 更重要的是 应该有机制来防止任何人大规模伪造门票。

我要讨论的第一个例子是预付费电表。我之所以选择这个,是因为我有幸参与了一项为南非 300 万户家庭通电的项目(这是纳尔逊·曼德拉上台时做出的中央选举承诺)。 [93] 中详细描述了这项工作。截至 2019 年 12 月,我们开发的 STS 规范已在 98 个国家/地区的 6800 万米中使用。大多数经验教训直接适用于其他票务系统。

14.2.1 公用事业计量

无法获得信贷的住户使用预付费电表购买燃气和电力服务(图 14.1)。在过去,它们是投币式的,但收集硬币的成本导致供应商转而开发基于代币的电表。

这项技术是由欠发达国家推动的,最引人注目的是南非,在那里它成为国家优先考虑的乡镇电气化;由于许多房屋是非正式建造的,业主甚至没有地址(更不用说信用等级),预付款是唯一的出路。

在纳尔逊·曼德拉担任总统期间安装了超过 200 万个仪表,现在估计有 1000 万个在使用。装机量最大的是印度尼西亚3500万台,在非洲、亚洲和拉丁美洲以及一些发达国家都很常见;北爱尔兰的大多数电表都是预付款。典型的发达国家可能有大约 10% 的家庭使用预付费电表,因为他们正在领取福利金或受到法院判决。

顾客去商店购买一个代币,它可以是一张卡片、一张带磁条的纸板票或一个 20 位数字的幻数。南非的大多数电表都使用幻数。这对顾客来说很方便,因为可以在超市收银台、ATM、电话或网上购买车票。

令牌实际上只是一条或多条指令,使用电表独有的密钥加密,并表示类似“电表 12345 – 分配 50KWh 的电力!”当信用额度用完时,电表会中断供电。一些代币也具有工程功能。可以使用特殊令牌来更改价格:如果电力公司在白天和晚上收取不同的费率,则电表可能需要更新相关价格和费率变化的时间。

在英国的电表中,使用智能卡的电表数量大约是使用磁票的两倍。前者不使用 STS 标准,但能够向电力公司报告消耗模式、篡改尝试等。磁票计价器和幻数计价器没有这样的反向通道。目前有一个项目是用智能电表替换大多数欧盟国家的所有电表,这些电表通过无线电链路报告读数和其他数据,并且可以远程设置为预付费模式。其他国家已经安装了智能电表,结果喜忧参半。我稍后会回到他们身边。

图 14.1：- 预付费电表（由 Schlumberger 提供）

预付费用是欠发达国家快速为数百万家庭供电的唯一途径。在发达国家,主要的激励措施是减少坏账和其他管理成本。另一个好处是节能。在大多数电表都是预付费的地区,电力消耗最多可降低 10%,因为其成本对住户来说变得更加突出。

14.2.2 系统如何工作

预付费电表的安全要求似乎很简单。代币应该不容易伪造,而真正的代币不应该在错误的仪表上工作,或者在正确的仪表上工作两次。通常的策略是将每个令牌绑定到一个唯一的仪表,这样就不能在两个不同的仪表中使用相同的幻数,并且还使用序列号或随机数使每个令牌唯一,以便相同的令牌不能在同一个仪表上使用两次。但是,将这个简单的想法发展成一个强大的系统需要大量的经验。

每个仪表都有一个加密密钥来验证其来自自动售货机的指令

机器。早期的系统每个社区都有一个,通常在当地商店。
它有一个销售密钥KV ,它是一个社区的主密钥,每个电表都有一个设备密钥KID ,通过在销售密钥下加密其电表 ID 得出:

孩子= {ID}KV

这与第 4 章中针对停车场门禁设备描述的关键多样化技术相同,并且在所有代币都在本地购买的情况下效果很好。但现实生活通常要复杂得多。在英国,电力行业放松管制导致数十家电力公司从发电机处购买电力,然后通过公共基础设施将电力出售给家庭,因此电表在具有不同税费结构的多家电力公司之间改变所有权。在南非,很多人通勤距离很远,所以他们想在他们工作的地方买票。因此,我们从协议开始,将客户电表密钥从“拥有”电表的售货站发送到另一个站,并以相反方向传递销售数据以进行平衡和结算,有点像 ATM 网络。 2007年,我们推出了网上售卖;中央服务器有一个硬件安全模块和所有的销售密钥,因此客户可以通过互联网或手机购买一个神奇的数字。

该服务器直接向 700 万客户销售商品,还通过约 10,000 个在线自动售货机和商店等在线销售点销售商品。

统计平衡用于检测非技术损失,即通过电表篡改或未经授权连接到电源电缆而导致的电力盗窃。

我们将可能供应 30 间房屋的馈线电表的读数与这些房屋的代币销售进行比较。但顾客囤票,抄表员在抄表时撒谎,所以这种差异是一个嘈杂的信号。您可以将其用作调查团队的线索来源,并作为簿记系统的统计检查,仅此而已。

在某些情况下,自动售货机被盗并被用来与公用事业公司竞争。消除这种“幽灵供应商”通常意味着更改所有本地仪表中的密钥;那里还有一些被盗的机器,由犯罪集团操作。对策是在自动售货机的安全芯片中保持信用余额,该芯片还保护自动售货机密钥和外部计量密钥。余额随着每次销售而减少,只有在现金存入银行时才再次记入贷方;然后,运营公司发送一个幻数,用信用值重新加载芯片。因此,我们有一个会计系统,由销售点的价值计数器执行,而不是由保存在公用事业服务器上的分类帐数据执行。然而,战略方向是集中化,以节省管理经销商的精力和费用,并且运营商已经用在线自动售货机取代了在线自动售货机,这些自动售货机可以从中央服务实时获取代币。

14.2.3 出了什么问题

与防盗警报器一样,环境稳健性至关重要。除了巨大的温度范围(南非和欧洲大陆一样多变

美国)许多地区有严重的雷暴:电表可以被认为是一个微处理器,上面附有 3 公里的避雷针。

当电表被闪电击毁时,客户抱怨并因他们所说的仍未使用的价值而得到信任。因此,他们的下一步是将带电的电源线插入电表,以尝试模拟闪电的影响。如果令牌插槽下的电路被破坏,一种仪表将提供无限的信用,因此服务拒绝攻击非常有效,因此变得流行起来。

这是变得更糟。索韦托的孩子们观察到,当出现断电时 电压从 220 伏特下降到 180 伏特 一种特定品牌的电表得到了最大的信任。很快他们就将钢链扔到 11KV 馈线上,并将附近的所有电表计入。由于未指定掉电测试,因此未发现此错误。发达国家的环境标准不足以在非洲使用。在不得不拉出 100,000 米并重新修整后,负责的公司几乎破产了。

还有许多其他错误。一种电表不提供特定数量的电量,而是以某某费率提供这么多的电量。

售货员发现可以将 tari 设置为一个微小的数额,并且计价器几乎可以一直运行。另一个允许退款,但仍可以使用退款令牌的副本。另一个仪表只记住最后输入的令牌序列号,因此通过交替输入两个令牌的副本,它可以无限期地充电。

与其他地方一样,真正的安全漏洞是由偶然发现并以相当机会主义的方式加以利用的错误和失误造成的。一些漏洞被放大并花费了数百万美元来修复。

我们在 [93] 中写到的其他经验教训是:

- 只要您控制营销渠道,预付款可能既便宜又简单,但是当您尝试通过便利店、银行和超市等第三方出售代币时,它可能会变得昂贵、复杂和有风险;
- 如果您没有在第一时间获得正确的安全基础设施,那么改变它可能会很昂贵 就像需要在远处的商店出售电表代币以支持通勤者的情况一样;
- 如果可以的话,回收技术,因为它可能有更少的错误。我们需要的大部分东西都是从提款机世界借来的;
- 使用多位专家。一个专家通常无法涵盖所有问题,即使是最优秀的专家也会遗漏一些东西;
- 您绝对需要长时间的现场测试。这是许多错误和不切实际的地方首先会被发现。

在最初部署后的几年里吸取的主要教训是设计出可扩展的欺诈,这意味着集中化。程序漏洞仍然存在;例如,由于任何公司都可以成为经销商,在市场上购买电表和自动售货站,不法公司可以在社区住宅区设置流氓电表,并引导租户向他们购买代币

反而。因此,预付款并不能完全消除对良好的老式审计、能源平衡和检查的需求 它也不能完全解决欠发达国家的地方腐败或更广泛的国家控制问题。

我们所学到的知识最终形成了 STS 规范,现在全球数十家制造商都在使用这些规范。不过,一个妥协确实反咬我们一口。 STS 仪表中的日期翻到 2024 年,那是 1990 年代初期我们开展这项工作时的遥远未来 1。现在近 100 个国家/地区有 6000 万个电表,公用事业公司将花费数亿美元来为每个客户提供一张特殊的钥匙更换票以管理翻转。 (关键变化的积极方面是,剩下的幽灵自动售货机最终将停止营业。)因此,在设计新系统时,请考虑可持续性,而不仅仅是“这个系统在未来 30 年内是否可行”? 但是“这在接下来的 100 年里会好吗?”你可能只是活得够尴尬!

14.2.4 智能电表和智能电网

在 2000 年代初期,计量行业开始推销智能仪表的概念 一种与中央服务器进行实时通信的仪表,以便可以远程读取。这早在 1970 年代就已获得专利,但后来发展成为一个更广泛的概念,不仅涉及计费和预付费(如果需要),还涉及细粒度定价、停电报告和电能质量监测。自动抄表 (AMR) 被高级计量基础设施 (AMI) 取代;后者具有双向通信,因此可以远程向仪表发送命令。定价可能很复杂,包括一天中的时间和需求响应费率。出售给公用事业的好处包括降低账单成本和更容易收债。向政府提出的案例包括减少高峰需求,从而减少所需的发电站数量。市场营销人员谈论“智能电网”,兴奋地谈论您的电表能够控制家用电器并与市场协商实时收费。

一个更清醒的说法是,智能电表可以通过让用户更加意识到他们用了多少电来收回成本,从而节省资金。对电表供应商的好处是用成本至少为 50 美元且可持续使用 15 年的产品替换成本为 15 美元且可持续使用 50 年的产品。

智能计量存在许多问题。研究人员首先提出了对进入公用事业的细粒度消费数据的普遍隐私担忧;如果将电表设置为按分钟甚至按秒监测用电量,公用事业公司就可以计算出家里有多少人,他们什么时候吃饭,什么时候洗澡,什么时候睡觉。这导致了对掠夺性营销的直接担忧,以及对第三方访问的间接担忧 无论是通过执法令、滥用授权访问,还是可能不可避免地入侵广告生态系统。这引发了关于测量时间粒度以及仪表中应保存多少数据的争论

1我们必须将所有内容都放入一个 20 位令牌的 66 位中,虽然我们想在计数器中增加一个位来获得额外的 31 年,但这意味着时间单位为 2 分钟而不是一分钟,这会使同时为一个仪表出售多个代币变得棘手。但我们确实有先见之明,可以在密钥更改时重置计数器。

与集中。然后我们注意到,在一个国家的所有家庭中放置一个可远程控制的 o 开关会造成重大的网络战争威胁;如果敌人可以关闭你的电力供应,他们可以迅速关闭你的经济,或者勒索你 [105]。这导致了国家安全机构的争先恐后。但也许最大的问题是围绕着不同利益相关者的不同动机。公用事业公司希望出售大量能源,而政府则希望节省能源并减少高峰需求。那么谁会赢呢?

先驱是意大利,ENEL 公用事业公司于 2001 年开始在该国安装智能电表。他们主要担心的是电力盗窃,尤其是在意大利南部,那里的执法人员被派去断开非付费客户的电源,但受到歹徒的威胁。智能电表使违约者能够远程切换到预付款制度。这被视为成功,游说者开始工作。

智能电网的概念随着 2007 年的《能源独立与安全法案》成为美国的政策,并在奥巴马总统拨款 45 亿美元用于其发展作为《美国复苏与再投资法案》的主要措施时引起了公众的广泛关注;欧洲议会紧随其后的是 2009 年的一项法律,要求成员国在 2012 年之前对智能计量进行经济评估,如果他们发现它有益,则要求在 2022 年之前使用它(到 2020 年采用 80%)[652]。许多国家和许多美国公用事业公司现在已经启动了国家或区域智能电表计划,我们有一些成功(如西班牙)和失败(包括英国和安大略)的经验。

虽然美国公用事业往往是受监管的地方垄断企业,但欧洲模式具有竞争性发电、受监管的输配电垄断以及竞争性零售商。电表属于配电网运营商还是零售商是历史偶然事件。事实证明,在配电商拥有电表的地方,用智能电表替换所有电表很简单,因为承包商一次可以完成整条街道,并且电表可以通过与变电站的电力线通信连接到公用事业.在西班牙,公用事业公司成立了一个买方联盟,并坚持每个供应商的电表都可以与其他所有供应商的头端配合使用,因此他们获得了每台电表成本低于 50 欧元的商品硬件。

然而,在零售商拥有电表的国家,事情并没有那么简单。激励措施存在一个严重的问题:如果智能电表要通过节能来为自己买单,那么将它们置于零售商的控制之下是没有意义的,零售商通过最大化能源销售来实现利润最大化。德国进行了诚实的评估,认为智能电表不经济,并放弃了该项目。不幸的是,英国奋力前行。其能源和气候变化部已经在 2004 年、2007 年和 2008 年进行了经济评估,显示投资回报为负。他们并没有被吓倒,而是扩大了关于成本、收益、电价和利率的假设,在 2009 年得出了积极的评估,并承诺英国不仅要为电力引入智能电表,还要为天然气引入智能电表 [883]。

在欧洲以外,在多家零售商拥有电表的地方也出现了同样的问题。新西兰将智能电表作为可选项,计算出只有大房子才值得使用。在安大略省,就像在英国一样,政府继续推进,导致代价高昂的失败,记录在 2014 年年度报告中

审计长的报告 [1197]。该省通过建立一个中央系统来收集所有仪表读数并将其提供给零售商和监管机构，从而与 73 家当地配电公司打交道。该系统的目标，即削减高峰需求，根本没有实现；政客们准备容忍的从高峰到低谷的价格变化不足以改变行为。 2005 年（部长们宣布该项目一年后）准备的安大略省成本效益分析结果将收益高估为 6 亿美元，而收益最多为 8800 万美元，而成本则激增至 20 亿美元；最大的零售商在设备和支持它们的系统上每米花费超过 500 美元。总的来说，能源规划非常糟糕，以至于该省最终将多余的电力卖给了美国，为密歇根州和纽约州的公用事业提供了数十亿美元的补贴。

在英国，智能电表已经演变成可能是有史以来最大的民用项目灾难。历届政府（工党、联盟和保守党）承诺到 2020 年推出智能电表，因为没有人愿意被指责为不“环保”。在我看来，浪费 200 亿英镑而不节省任何能源，并取代本可以产生实际节约的更好的项目，这几乎是你能得到的最不环保的做法。该项目的每一层都镀金，每个家庭最多有四个设备：用于燃气和电力的智能仪表、将它们连接到无线网络的家庭集线器，以及一个家庭显示器，以便账单支付者可以跟踪消费情况. （该项目始于 2009 年，当时人们开始使用智能手机，但由于过于僵化而无法改用应用程序。）部长们沿用了安大略省的中央抄表服务器路线，但仍然有一位英国住户接受了一家供应商的智能电表，并且然后为了省钱而转向不同的供应商，此后通常必须提交手动读数。第二代电表的国家标准花了数年时间才达成一致，而且大多数已部署的电表都由不兼容的旧型号组成；供应商为在那里获得自己的专利而奋斗了多年，而官方没有技术知识或政治支持来齐心协力。 2010 年代中期，一旦我们指出敌对国家可以在紧张时期简单地关闭英国家庭的电力，安全机制就会在恐慌中进行改造 [105]。威胁要揭露该项目失败以及可能的成本从 110 亿英镑增加到 230 亿英镑的告密者受到监禁 [919] 的威胁。国家审计署随后在 2018 年底报告说，该项目大大低于预期：计划到 2020 年底更换 80% 的英国仪表，但只完成了 1250 万，还有 3900 万尚未完成做[1391]。更重要的是，当客户更换供应商时，70% 的仪表会失去功能（您每年都必须这样做才能获得合理的价格）。如果政府遵循其宣布的让每个人都使用第二代电表的战略，那么所有这些旧电表都将不得不更换；根据 2019 年 11 月的一份报告，只有 230 万米是新的。节省成本的可能性不大，因为到 2020 年代，该行业将不得不支持良好的老式电表、多种类型的过时智能电表和新型智能电表。至于节能，没有任何迹象。 （如果政府使用电表让每个人都提前付费，政府可以节省大量能源，但这不在议程上，并且可以使用更便宜的工具来完成。）除了计费之外，没有人将数据用于任何其他用途。而现在官方只是不想知道：用 NAO 报告的话来说，“该部门目前没有计划在

部署完成。”

关于智能电网的最后两点评论。当电表制造商在 2000 年代末大力推进营销时,人们热切地谈论电表通过创建需求响应和改进测量来帮助稳定电网。

事实证明,经验丰富的电力工程师当时表达的怀疑是有道理的。随着发电能力从连接到核心传输网络的大型纺纱机转移到嵌入更广泛的配电系统中的数十万台风车和太阳能电池板,电网确实变得更加脆弱。最近的大规模停电,例如 2016 年 9 月 28 日在南澳大利亚和 2019 年 8 月 9 日在英国,都是级联故障,由当地问题(澳大利亚的风暴和英国的雷击)导致频率变化率引起超过安全限值,导致进一步卸载,从而导致欠压和进一步卸载。每种情况下的一个复杂因素是,现在我们在人们的屋顶上嵌入了大量发电容量,卸载负载不像以前那样有效。

结论并不是我们需要智能电表,即使是在变电站级别,而是我们需要在系统中增加惯性 这意味着购买电池或同步调相机。我们还需要让其余的基础设施更能容忍中断。英国对 2019 年停电的大部分政治愤怒来自伦敦通勤者被困在火车上数小时。发生这种情况是因为 60 列西门子 Desiro 级列车在本应以 48.5Hz 跳闸时以 49Hz 跳闸,其中一半由于软件错误而无法重启。让他们重新开始工作需要技术人员带着笔记本电脑上门2。

需求响应也应该有助于减少高峰需求。
智能电表无处可用。许多国家现在都有容量市场,电网运营商可以在几秒到几分钟的时间尺度上购买额外的兆瓦,但这些市场使用专用系统运行。例如,拥有备用柴油发电机并且必须每月运行半小时以确保它们仍然工作的数据中心运营商,在需要时启动它们是有偿的。在较温暖的国家/地区,有些人允许在需求高峰期间将空调关闭半小时 ,从而获得电费折扣。最终,一旦数量充足,电动汽车充电器也将为此做出贡献。但是执行此操作的设备始终与主要公用事业仪表分开;任何创办容量公司的企业家都不想卷入受监管的混乱局面。

至于你的家庭中心的智能电表营销愿景,谈判能源价格并关闭你的炊具或热水器以应对价格飙升,这与商业现实相去甚远。销售炊具和加热器等产品的公司确实在其中安装了 CPU 和通信设备,但它们与公司自己的服务器通信,而不是与其他设备通信;政客们允许零售价格飙升以匹配容量市场的想法是天真的。智能电表在英国所取得的成就只是让数万名抄表员失业,而账单支付者为此付出了 200 亿英镑的代价。安大略省也是一样,但尾随零少了一个。

2由于国家安全规则,英国火车和铁路信号不允许进行无线软件升级,因为铁路被认为是关键的国家基础设施。
这也意味着安全补丁需要几天时间才能发布。干得好,军情五处!

14.2.5 票务欺诈

交通票务是一个比公用事业计量更大的应用，但我不知道有任何关于火车、公共汽车和地铁车票故障模式的严肃和公开的研究。就伦敦而言，放松对铁路的管制导致火车公司通过在他们获得较大比例收入的车站预订来操纵门票销售的问题；如果你正在设计一个在供应商之间分享收入的系统，你应该尝试设计出利益相关者作弊的动机。在第 13.2.5 节中描述的 Mifare Classic 崩溃后也出现了恐慌；伦敦交通局争先恐后地添加入侵检测系统以检测欺诈行为。

我们确实有一些真实欺诈数据的一种票务类型是航空公司品种。在 2010 年代，出现了一个以欺诈手段获得的机票和转售机票的渠道的生态系统。获得机票的方法多种多样，从盗用信用卡到航空公司和旅行社的不诚实人员，再到窃取飞行里程和被黑的预订系统；营销渠道包括垃圾邮件、联盟营销、向移民社区销售和向人类追踪器销售。 Alice Hutchings [936, 937] 记录了所有这些。关键因素是，与地铁票不同，机票对于这样一个生态系统的发展具有足够的价值；虽然有些顾客知道他们得到的是假机票，但他们中的很多人都是傻瓜，所以你不能逮捕所有持无效机票登机的人。

现在，我将研究一类应用程序，其中的攻击比对电表的攻击更为严重且持续时间更长。威胁模型包括传感器操纵、拒绝服务、会计欺诈、程序失败和操作人员腐败。这个典型的研究领域是车辆监控系统。

14.3 出租车计价器、行驶记录仪和卡车限速器

许多系统被设计用来监视和控制车辆。最熟悉的可能是您汽车中的里程表。购买二手车时，您会担心汽车是否已计时，即指示里程是否减少。随着里程表变得数字化，计时成为一种计算机欺诈[391]。一个相关的问题是修整，即更换或重新编程发动机控制器。这样做有两个基本原因。首先，发动机控制器作为远程钥匙输入系统的服务器，保护大多数现代汽车免遭盗窃，如第 4 章所述；所以如果你想在不偷钥匙的情况下偷车，你可能会在街上更换控制器，或者拖车然后更换或重新编程控制器。其次，人们重新编程他们汽车的发动机控制器以使它们开得更快，而制造商不喜欢这种做法，因为烧坏的发动机会增加保修索赔。因此，他们试图让控制器更加防篡改，或者至少是防篡改。

这种军备竞赛在[624]中有所描述。

许多车辆现在保存日志，这些日志会在使用期间上传给制造商

服务。通用汽车公司于 1990 年开始为一些车辆配备黑匣子以记录碰撞数据。到 1999 年记录公开时,已有约 600 万辆汽车安装了仪器,这一披露引起了隐私活动家的抗议 [1938]。事实上,有一整场会议 ESCAR 都专门讨论汽车电子安全问题。 2019 年,随着人们对自动驾驶的兴趣日益浓厚,车辆安全再次成为热门话题3。

其他车辆监控系统是在出厂后安装的,最熟悉的可能是出租车计价器。出租车司机有动机操纵计价器以显示更多的行驶里程（或等待的分钟数）,如果他可以侥幸逃脱的话。还有各种其他类型的“黑匣子”用于记录车辆从飞机到渔船再到装甲银行卡车的移动,它们的操作员有不同程度的篡改动机。向年轻和高风险司机销售“按需付费”保险的保险公司要求他们在黑匣子中安装卫星导航设备,让保险公司在下午沿着乡间小路行驶时每英里收取几美分的费用但是晚上在内城开车每英里几美元 [1909]。任何想在星期六晚上开车在城里转悠给女士留下深刻印象的年轻人都会有打破黑匣子的动机。

14.3.1 行驶记录仪

我要在这里使用的案例研究是行驶记录仪。这些设备用于监控卡车司机的速度和工作时间;在欧洲,传统的模拟设备从 2006 年开始被数字设备取代,一辆卡车可以使用大约十年,现在大部分车队都是数字设备。这为我们提供了一些关于此类设备如何工作以及可能发生故障的有趣数据;这是转向数字技术并没有让事情变得更好的一个例子。真正需要的不是高超的技术,而是更多的执法。

司机在开车时打瞌睡导致的交通事故比醉酒造成的事故多几倍（例如,英国的事故率分别为 20% 和 3%）。由于卡车的质量,涉及卡车的事故更有可能导致致命伤害。所以大多数国家规定了卡车司机的工作时间。虽然这些法律在美国使用称重站和驾驶员日志来执行,但欧洲国家/地区使用记录车辆速度 24 小时历史记录的行驶记录仪。直到 2005–6 年,这才记录在一张圆形蜡纸图表上（图 14.2）;从那时起,引入了数字行驶记录仪,旧系统已基本被淘汰4。

首先让我们以旧的模拟系统为基准;它仍在使用中
欧洲道路上的旧卡车和公共汽车。

模拟系统使用加载到转速表中的蜡纸图表,转速表是车辆速度表/里程表单元的一部分。它在仪器内部的转盘上缓慢转动,每 24 小时转动一次,速度历史记录由与速度计相连的细尖笔记录。和一些

3完全披露:我的一名研究生是由博世资助的。
4自 2004 年 8 月起在英国注册的车辆必须安装数字系统,自 2005 年 6 月起发放驾驶证,2006 年 8 月强制要求新车使用数字系统;其他欧盟国家的日期略有不同。

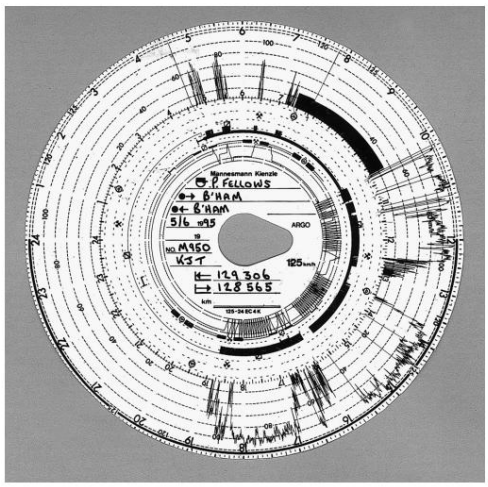

图 14.2：- 行驶记录图

不需要我们关心的例外情况,除非您有行车记录仪,否则在欧洲驾驶卡车是违法的;如果它是模拟的,你必须安装一个图表,并在上面写下你的开始时间和位置。您还必须随身携带几天的图表,以证明您已遵守相关的驾驶时间规定（通常每天 8.5 小时,并有每天休息时间和每周休息天数的规定）。如果它是数字的,则必须插入驱动卡;卡和车辆单元都保存记录。

欧洲法律还限制卡车在高速公路上的时速为 100 公里/小时（62 英里/小时）,而在其他道路上则更低。这不仅由警察限速器和行驶记录仪记录执行,而且直接由同样由行驶记录仪驱动的限速器执行。行驶记录图还用于调查其他违法行为,例如未经许可的废物倾倒,以及被车队运营商用来检测燃料盗窃。因此,卡车司机可能想要摆弄他的转速表的原因有很多。实际上,不应该聚合目标是安全工程中的一般原则。强迫卡车司机破坏他的行车记录仪以绕过他的限速器,反之亦然,这是一个设计错误　但现在这个错误已经根深蒂固,无法轻易改变。

我们要说的大部分内容同样适用于出租车计价器和其他监控设备。卡车司机希望他的车辆看起来行驶的距离更短,而出租车司机则相反。这对实际的篡改技术几乎没有影响。

14.3.2 出了什么问题

根据在引入新数字系统之前对 1060 名司机和操作员定罪的调查 [64],违规行为分布如下。

14.3.2.1 大多数行驶记录仪操作是如何完成的

大约 70% 的定罪犯罪不涉及篡改,而是利用了程序上的弱点。例如,一家在邓迪和南安普敦有经营场所的公司应该有四名司机,以便每天在每个方向上驾驶一辆车,因为距离大约 500 英里,行程大约需要 10 小时 这对一个司机来说是违法的每天做。

标准的小提琴是让两名司机在彭里斯等中间点相遇,更换卡车,并将新的纸质图表插入行驶记录仪。
因此,来自南安普敦的司机现在开着从邓迪来的车回家了。当停下来询问他的图表时,他展示了从彭里斯到南安普顿的当前图表、前一天从南安普顿到彭里斯的图表、前一天从彭里斯到南安普顿的图表,等等。通过这种方式,他可以给人一种错误的印象,即他每隔一晚都在彭里斯度过,因此是合法的。这种在工作日中途调换车辆的做法称为重影。在欧洲大陆更难被发现,那里的司机可能周一在法国、周二在比利时和周三在荷兰的一个仓库外工作。

更简单的欺诈行为包括错误设置时钟、假装搭便车的徒步旅行者是救援司机,以及将起点记录为一个具有非常常见名称的村庄 例如英格兰的“米尔顿”或西班牙的“拉霍亚”。如果停下来,司机可以声称他是从附近的 Milton 或 La Hoya 出发的。

这些技巧通常涉及司机和操作员之间的勾结。
当操作员被命令出示图表和支持文件(如工资记录、称重站单据和船票)时,他的办公室很可能会被烧毁。 (值得注意的是,有多少卡车公司在与他们院子里的卡车保持安全距离的廉价木棚中运营。)

14.3.2.2 篡改供应

第二大欺诈类别,约占总数的 20%,涉及篡改行驶记录仪的电源,包括干扰电源和脉冲电源、电缆和密封件。

最早的行车记录仪使用旋转电缆 直到 1980 年代初期汽车中的速度计也是如此 这很难摆弄;如果卡住卡车的里程表,很可能会剪断电缆。最近的模拟行驶记录仪是“电子的”,因为它们使用电缆而不是旋转线。输入来自变速箱中的传感器,该传感器在传动轴旋转时发送电脉冲。这使摆弄变得更加容易!一种常见的攻击方法是将传感器拧松大约十分之一英寸,这会导致脉冲停止,就好像车辆是静止的一样。为防止这种情况,传感器使用电线和铅封固定到位。安装工被贿赂逆时针而不是顺时针缠绕电线,这导致它在拧下传感器时松开而不是折断。事实上,印章是发给车间而不是个体装配工的,这使得起诉变得复杂。

但是大多数小提琴仍然简单得多。司机将电缆短路或用烧断的保险丝更换行驶记录仪保险丝。 (一位制造商试图

通过将卡车的防抱死制动系统放在同一个保险丝上来阻止这个把戏。
许多司机宁愿早点回家,也不愿驾驶安全的车辆。)图 14.2 中的图表中有电源中断的证据:上午 11 点左右,有几个地方的外部迹线指示的速度突然从零变为超过 100 公里/小时。这些表示电源中断,除非距离轨迹中也存在不连续性。那里,单位

是开放的。

14.3.2.3 篡改仪器

第三类欺诈是篡改行车记录仪本身。
此类别中的典型违规行为是校准错误,通常是与安装人员合谋完成的,但有时是由司机破坏设备上的密封件造成的。
这相当于约 6% 的违规行为,但在 1990 年代有所下降,因为数字通信的引入使得篡改电缆变得更容易。

14.3.2.4 高科技攻击

调查时的篡改艺术状态是图 14.3 中的设备。照片左侧的塑料圆筒标有“电压调节器 日本制造”,但肯定不是电压调节器。 (它似乎是在意大利制造的。)它被拼接到行驶记录仪电缆中,并由驾驶员使用遥控钥匙进行控制。第一次按下导致指示速度下降 10%,第二次按下导致下降 20%,第三次按下导致其降至零,第四次使设备恢复正常运行。

这种设备占定罪的比例不到 1%,但据信其使用更为广泛。它很难找到,因为它可以隐藏在卡车电缆线束的许多不同位置。警察拦下了一辆装有这种装置的超速卡车,却找不到它,他们很难定罪:密封的、显然经过正确校准的行驶记录仪与他们的雷达或照相机提供的证据相矛盾。

14.3.3 数字行驶记录仪

针对行驶记录仪操纵采取的对策因国家/地区而异。
在英国,卡车会停在路边接受车辆检查员的随机检查,并且可能会在全国范围内跟踪可疑卡车。在荷兰,检查员更喜欢去一家卡车运输公司检查他们的交货文件、司机的时间表、燃料记录等。在意大利,高速公路收费站的数据被用来起诉平均速度超速的司机限制(您经常可以看到卡车停在意大利收费站前)。但司机可以在不同的控制制度之间进行套利。

例如,在法国和荷兰之间运营的卡车司机可以将他的文件保存在法国的一个仓库中,荷兰车辆检查员无法获取这些文件。英国制度的弱点是,当车辆检查员拦下一辆卡车并发现违规证据时,这将导致一些人被起诉

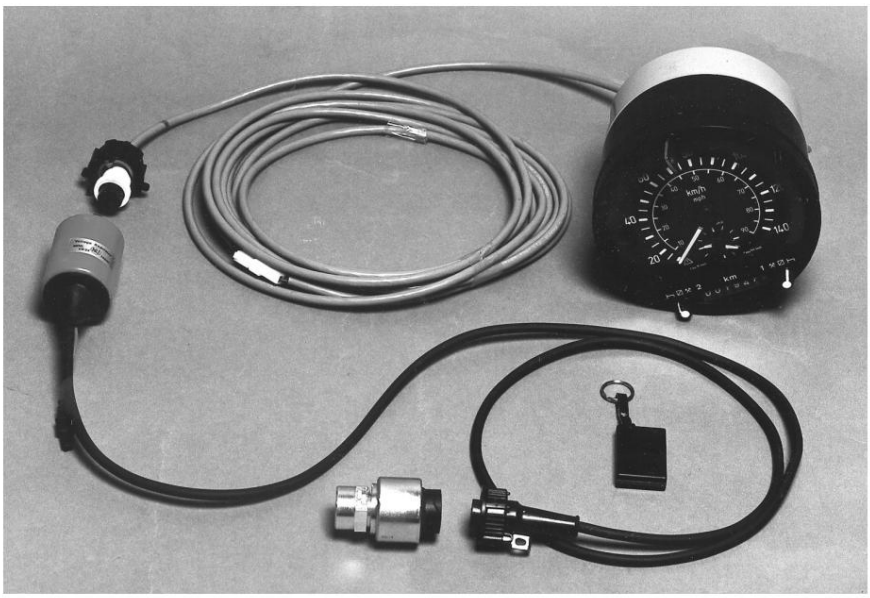

图 14.3：- 带有由驾驶员使用无线电钥匙扣控制的中断器的行驶记录仪。 （由英格兰汉普郡警察局提供）

几个月后在当地地方法院。外国司机经常不出现。

于是欧盟主动设计了一个统一的电子行车记录系统，用智能卡取代现有的纸质图表。

每个司机现在都有一张司机卡，上面记录了他过去 28 天的驾驶时间。自 2006 年以来注册的每辆车都有一个可以保存一年历史的车辆单元。还有机械师用来校准设备的车间卡，以及执法人员用来在路边读出的控制卡。 1998 年，英国交通部聘请我研究新方案并找出问题所在。

在与从警察和车辆检查员到行驶记录仪供应商和事故调查员的广泛人员交谈后，我写了一份报告 [64]。我在 2007 年编写本书第二版时重新审视了该领域；发现我大部分时间都正确地预测了问题，这让我既高兴又沮丧。然而，也出现了一些有趣的新变化。终于，在2020年的第三版中，我们可以采取更成熟的观点。

对该项目提出的主要反对意见是，目前尚不清楚数字化将如何帮助打击占总数 70% 的程序欺诈。
事实上，我们这对在邓迪和南安普顿之间“幽灵”的司机让他们的生活变得更加轻松。转换到新系统花了 14 年 比一辆卡车的寿命还长 与此同时，一家不正当的公司可以运行一辆新的数字卡车和一辆旧的模拟卡车。每个司机现在将拥有一张图表和一张卡片，每张卡片每天有五个小时，而不是他们在停车时可能会不小心弄混的两张图表。事实证明这是有根据的。到 2008 年，大约 20% 的车队配备了数字行驶记录仪 比预期的要多一些 这表明运营商

可能在需要之前就已经安装了数字设备,因为它们更容易摆弄。 2020年,司机拥有多张卡。

另一个反对意见是,由于详细的速度和驾驶时间信息的丢失,执法将变得更加困难。早在 1998 年,德国人就希望驾驶卡成为一种存储设备,以便可以包含详细的记录;由于智能卡行业的游说,法国人坚持使用智能卡。所以驱动卡内存有限,只能包含有限数量的报警事件。

14.3.3.1 系统级问题

各国对细粒度数据丢失的反应各不相同。德国寻求车队管理系统的基础设施,该系统接受数字行驶记录仪数据、现有纸质图表中模拟数据的数字化版本、燃料数据、交付数据甚至工资单,并将它们全部协调起来,不仅为卡车运输公司提供管理信息而是警方的监控数据。英国也有类似的情况,但由警方决定检查哪些公司;除非他们这样做,否则只有雇主可以获得有关违规驾驶的数据。有第三方服务公司会为那些热衷于节省时间或只是为了证明合规性的公司分析这一点。德国还引入了重型货车道路收费系统,为车队管理提供更多信息。

英国有一个自动车牌阅读器 (ANPR) 摄像头网络,最初安装在伦敦周围是为了让爱尔兰共和军的炸弹袭击更加困难;在 1997 年的耶稣受难日协议结束了这一威胁之后,车牌识别系统并没有停止使用,而是在全国范围内推广。在检测汽车逃税者的基础上这是合理的,但我们随后看到越来越多的诉讼中引用了车牌识别数据,从恐怖主义到入室盗窃,无所不包。在强制执行司机工作时间的情况下,策略是根据 ANPR 数据库验证记录的行程样本;一旦发现差异,公司的运营就会受到更严密的审查。

然而,关于隐私和国家经济利益的分歧阻碍了欧盟范围内的标准化。是否要求卡车公司下载和分析卡车数据取决于各个国家/地区。

甚至在有此要求的国家之间,仍然存在套利行为。例如,德国警察比意大利警察更积极地执行司机的工作时间规定。因此,在旧的模拟系统下,一位通常懒得在他的机器上放图表的意大利车手在翻越阿尔卑斯山时这样做了。与此同时,对面行驶的德国卡车司机拿出了他的图表。最终效果是特定国家/地区的所有司机都受到相同级别的执法。但是,如果驾驶数据是从意大利驾驶证上传的,并保存在罗马一家卡车公司的个人电脑上,那么它们将受到意大利执法级别的约束（如果罗马警方不关心德国的事故,则更少）.解决办法是治外法权;一名在德国被拦下的意大利卡车司机,如果不能出示他在过境前一周在意大利的令人满意的驾驶记录,现在可以在那里被起诉。

在英国,被拦下并被命令在地方法院出庭的外国司机通常不会出现。结果证明,真正的解决办法不是技术上的,而是法律上的。 2018 年 3 月,英国修改了法律,允许在路边进行现场罚款。以前,警察只能对正在进行的违规行为处以现场罚款,而不能对卡车或司机记录中可见的违规行为处以罚款。这一变化导致罚款增加近 10 倍 [924]。

14.3.3.2 其他问题

总的来说,从模拟到数字的转变并不是一种进步。虽然尚未收集数字和模拟设备的比较欺诈统计数据,但官方的观点是,虽然对不切实际的旅程的初始检测仍然大致相同,但数字作弊设备的复杂性使它们更难找到 [1726]。行车记录仪数字化还有其他有趣的问题。

首先,数字行车记录仪是第一个导致数字签名大量出现在法庭上的系统。多年来,安全研究人员一直在撰写带有妙语的学术论文,例如“法官然后将 X 提高到 Y 的次方,发现它等于 Z,然后将 Bob 送进监狱。”现实是不同的。

法官发现数字签名很困难,因为它们以十六进制字符串的形式出现在从车辆单元打印出来的小票上,没有经过批准的验证设备。警方通过应用“获取”证据的标准程序解决了这个问题。当他们突击搜查一家狡猾的卡车运输公司时,他们会对 PC 的磁盘驱动器进行成像,并在密封在证据袋中的 DVD 上进行复制。一份交给辩方,一份留待上诉。记录复制的纸质日志以及车辆单位的打印输出可供他们的崇拜检查。

其次,很多司机都有不止一张驾照。这在任何地方都是违法的,但这并不能阻止它!司机从朋友那里借来他们只是偶尔使用它们 例如,因为他们通常驾驶 3.5 吨以下的卡车。由于欧盟的行动自由,司机可以轻松拥有多个地址:图卢兹的让·穆兰也可能是安特卫普的让·穆兰。建立了一个名为 Tachonet 的数据库,以尝试在欧洲国家/地区捕获重复的应用程序,但它似乎效果不佳。

例如,司机可能会忘记他们在居住国之一的中间名。从 2018 年开始,成员国必须与其共享数据。

第三,出现了新型的拒绝服务攻击(以及针对变速箱传感器、保险丝等的传统攻击)。卡车司机可以通过向主电源供电来破坏他的智能卡(即使是卡车的 24 伏电压也可以)。根据规定,他可以在等待更换期间驾驶 15 天。由于静电每年至少会损坏 1% 的卡,因此很难起诉偶尔这样做的司机。

第四,我提到过转速表上详细、冗余数据的丢失使得执行更加困难。在过去的模拟时代,当图表不正确时,经验丰富的车辆检查员有一种“感觉”,但模拟轨迹被二进制信号取代,表明司机违反了

规定或他没有。这会影响到其他执法任务;例如,类比图通常用于收集非法有毒废物倾倒的证据,因为记录的速度历史通常可以让检查员很好地了解卡车的路线。

接下来,系统中的一些卡(主要是用于设置仪器的车间卡,以及警察和车辆检查员使用的控制卡)非常强大。它们可以用来抹去不法行为的证据。例如,如果您使用车间卡将车辆单元的时钟从 7 月 10 日倒回至 7 月 8 日,则 7 月 9 日和 10 日的条目将变得不可读。因此,一些国家竭尽全力减少落入坏人之手的工作坊卡的数量。例如,在英国,卡车修理工必须通过犯罪记录检查才能获得一个;但这并非万无一失,因为通常是公司被定罪,而不正当的卡车维修公司的富有所有者刚刚成立了新公司。没有公司许可计划,虽然不法分子可以被列入黑名单,不能担任持牌公司的董事,但骗子只是躲在提名董事的背后。

14.3.3.3 复活的小鸭,或豆腐

行车记录仪世界中有一个有趣的 spin-o 。在 1990 年代后期,一项欧盟法规规定,为了阻止使用图 14.3 中所示的那种中断器,所有数字行驶记录仪都必须对从变速箱传感器到车辆单元的脉冲序列进行加密。由于这两种设备都包含一个微控制器,并且数据速率相当低,因此这在理论上应该不是问题。但是我们究竟如何分发密钥呢?如果我们只是设立一条热线电话,车库可以拨打,很可能会被滥用。长期以来,装配工与卡车司机合谋破坏系统,车库工作人员滥用求助热线获取被盗汽车的解锁数据,甚至是被盗汽车收音机的 PIN 码。

复活小鸭安全策略模型提供了一种解决方案,更通俗地说,称为首次使用信任。这得名于这样一个事实:从蛋里出来的小鸭子会把它看到的第一个发出声音的移动物体认作它的母亲:这被称为印记。同样,刚从收缩包装中取出的“新生”车辆单元可以将第一个向其发送密钥的变速箱传感器识别为其所有者。传感器在上电时执行此操作。一旦收到这把钥匙,车辆单元就不再是新生的,并将在其余下的“生命”中忠实于变速箱传感器。如果传感器出现故障并且必须更换,可以使用车间卡“杀死”车辆单元的密钥存储并将其复活为新生儿,然后它可以在新传感器上留下印记。每一次复活的行为都不可磨灭地记录在车辆单元中,以增加滥用的难度。 (这至少是理论上的 实施有些不足,因为在一个单元中,传感器重新输入密钥的错误代码与断电的错误代码相同。)

密钥管理的复活小鸭模型最初是为了处理数字温度计或其他医疗设备到医生的平板电脑或床边监视器的安全印记 [1819]。它还用于无线局域网扩展器;这些设备通常使用称为 Homeplug AV 的协议套件通过家用电源以 155Mb/s 的速度传输数据

从插入宽带集线器的设备到另一层的远程设备。
为了防止您的邻居能够使用您的 wifi,每个虚拟网络都使用您第一次插入扩展器时设置的密钥进行加密 [1437]。这个想法是,当您插入某些东西时,它应该可以正常工作;如果它与错误的网络配对,你按下一个按钮再试一次;在极端情况下,您可以通过将包装上的密钥复制到任何具有键盘的已注册设备中来手动进行安全保护。随着越来越多具有受限接口的设备加入物联网,此类协议将变得更加普遍。

14.3.4 传感器故障和第三代设备

然而,即使协议可以得到保护,传感器仍然可以被直接攻击。自数字转速表开始发货以来,为您带来中断器的人们现在有了新产品:一个包含电磁铁和电子设备的黑盒子,用于模拟变速箱。错误的卡车司机拧下他的变速箱传感器并将其放置在这个模拟器中,该模拟器带有自己的电缆和一个传感器,他将其插入他的实际变速箱中。该系统现在像以前一样运行;根据命令,它要么忠实地传递冲动,要么丢弃它们,要么过滤掉其中的一些冲动。狡猾的脉冲序列像以前一样到达行驶记录仪,但这次使用三重 DES 进行了精美的加密。安全传感比看起来更难!

这变得如此令人讨厌,以至于欧盟在 2009 年通过了一项法律,明确禁止并要求成员国检查“任何旨在破坏、抑制、操纵或更改任何数据的设备,或旨在干扰记录设备的组成部分之间的电子数据交换的任何部分,或者在加密之前以这种方式禁止或更改数据的任何部分”[652]。它还升级了规定,要求 2012 年注册的车辆配备“第三版行车记录仪”,这需要额外的运动传感器作为传感器失效的对策

14.3.5 第四代 智能行车记录仪

2014 年更新了法规,引入了智能行驶记录仪,自 2019 年 6 月 15 日起首次注册的车辆必须配备智能行驶记录仪,并增加了:

- 更好的安全机制使欺诈更加困难;
- 卫星导航系统,它将在每次行程的开始和结束时记录卡车的位置,如果行程长于此,则每三个小时记录一次;
- 路边的警察可以在车辆行驶时读取行驶记录仪数据的无线电链路

到现在为止,读者可能会对任何所谓的“聪明”事物感到某种愤世嫉俗。这些规定是朝着普遍执法方向迈出的一步,但并未要求车辆单位保留详细的 GPS 历史记录。

某些国家/地区的隐私法会使这种情况变得困难;在恶劣的情况下,例如倾倒有毒废物,当局可以随时传唤司机的手机历史记录 5。同时,供应商提供具有自动侵权检查功能的车队管理系统,向公司保证这将最大限度地减少责任。

我们将不得不拭目以待,看看这一切如何运作。

但是,需要持续 GPS 监控的实用性可能是什么?
我们可以从下一个应用程序中获得一些见解。

14.4 宵禁标签:GPS当警察

我的第三个监控计量案例是犯罪嫌疑人和假释犯戴在脚踝上的宵禁标签,以限制和监控他们的行动。它们于 1999 年在英国推出,用于减少监狱人口。大多数罪犯在服完一半刑期后获释,并在宵禁期间度过部分假释期,这通常意味着他们必须从晚上 7 点到早上 7 点呆在家里。他们在与家庭监控站通信的脚踝手镯上佩戴宵禁标签。其他人则接受社区刑罚而不是监禁,并实行宵禁。大约 20,000 名罪犯可能在任何时候都处于“待命状态”。

宵禁标签也已经传播到许多其他国家。更昂贵的标签包含 GPS 芯片,并不断向警方报告标签佩戴者的位置。在英国,宵禁禁止他们靠近学校的性犯罪者、一些警区的顽固犯罪者以及恐怖主义嫌疑人都佩戴这些装置。在法国,他们被引入家庭暴力案件 [478]。在美国,许多嫌疑人被作为保释条件提供给许多嫌疑人(其中最著名的可能是哈维温斯坦)。那里的问题是,虽然联邦政府为其囚犯的标签支付费用,但 90% 的案件是由州和城市提出的,这主要是迫使标签佩戴者支付费用。监控由两家公司主导,它们通常每天收费 10 美元,预付 350 美元。 (当政府支付时,他们每天只能得到 2-3 美元。)因此,可怜的被告负债累累,或因不支付而入狱。这是短视的,因为监狱每天的费用约为 100 美元。鉴于美国随时都有大约一百万人在监狱中等待审判,这是一个具有实际后果的政策问题;标签佩戴者的数量超过 125,000,并且自 2018 年第一步法案以来一直在上升。法官认为监控命令是免费的;他们防御性地发布它们,稳步扩大范围;三分之二的标签佩戴者是非裔美国人;与保释不同的是,如果被宣告无罪,被告不会拿回他们的钱 [1074]。

2013-6 年,我作为专家证人参与了多起宵禁案件。第一次发生在 2013 年,涉及一名因入店行窃而被定罪的妇女,她被指控篡改她的宵禁标签,因为它多次表明她晚上离开了家。对与我被告案件有关的日志的分析表明存在大量误报;其中一些有很好的解释(例如停电),但很多没有。整体画面是

5欧洲所有3.5吨以下的车辆都必须配备嵌入式电话以提供eCall紧急服务;不幸的是,这对于大型车辆来说并不是强制性的,这无疑是因为行业游说。

一种被混乱的程序和利益冲突所包围的不可靠技术。标签承包商 Serco 不仅提供标签和后端系统,还提供呼叫中心和法院系统的接口。更重要的是,如果你违反宵禁,将你带到地方法官面前的不是检察官,而是承包商 依赖于帮助设计该系统的分包商之一的专家证据。我们向法院索取了本案中的标签,以及一套用于测试的标签设备、系统规格、误报统计和审计报告。承包商立即回复说:“虽然我们仍然认为被告违反了命令,但我们已经注意到许多因素,这些因素将使我能够为了公共利益适当地停止诉讼”[83]。

几个月后,有一起案件涉及几名受“恐怖主义预防和调查措施”(TPIM)命令约束的男子。这是 2011 年推出的一项措施,允许英国政府对被认为具有恐怖主义威胁但没有足够证据对其提起诉讼的个人实施宵禁;它们在人权方面一直存在争议。许多人收到了限制行动的命令,并配备了 GPS 标签以监督遵守情况。大约六个月后,这些标签往往会损坏,于是这些人因篡改标签而被起诉并入狱。由于这是一项保密令,该模式只有在代表其中三人的伦敦律师事务所注意到后才曝光。再次,政府拒绝向专家审查任何证据,三人被无罪释放,让当时的内政大臣特蕾莎·梅感到尴尬[?]。几天后,其中一人在伦敦清真寺戴上面纱并以女性身份离开,以此逃避监视。

这引起了媒体的愤怒 [1904]。接下来的一个月,事实证明,英国的两个主要宵禁标签承包商 Serco 和 G4S 一直在大规模欺骗政府,向被释放或入狱、在国外或死亡的罪犯收取标签费,自 2005 年合同开始以来,这种情况一直在发生。他们被剥夺了合同,此事被提交给严重欺诈办公室 [1286]。 Serco 最终在 2019 年被罚款 1920 万英镑,并被勒令支付 370 万英镑的费用;其会计师德勤因对标记操作进行审计而被罚款 420 万英镑。

2014 年,另一名被移民拘留的恐怖主义嫌疑人被控篡改标签,他否认了宵禁标签的可靠性。这一次,政府决定冒险试一试。嫌疑人的律师指示我和我们材料科学部门的一位同事担任专家。我们假设佩戴沉重标签的压力会导致表带固定断裂,尤其是对于每天祈祷五次的虔诚穆斯林而言。法院正式下令我们两个人和我们实验室的一名沙特研究生安装 GPS 标签,我们安装了加速度计和应变计来监控测试。

虽然学生的标签在几天的祈祷后幸存下来,但我的标签在家里的暖气片上发现时坏了 ,而我的同事在踢足球时戴了它。该规范要求标签能够承受 50 公斤的拉力,运营公司(已从 G4S 接管业务但仍使用相同的专业分包商)声称制造标签的材料不易疲劳断裂。然而,政府“出于商业机密的原因”拒绝透露这些材料的内容

曾是。不管;对断裂的固定凸耳上的一条条子进行的测试表明,它是一种聚碳酸酯,确实会发生疲劳断裂。法院命令我们交还所有样品“以保护承包商的知识产权”,但并未对我们的专家报告施加保密令,该报告可在 [85] 中找到。这名嫌疑人也最终被法院释放。

到 2015–6 年,来自新供应商的 6 个 GPS 标签被肯特警方用于监控轻罪者。供应商最初对 GPS 精度做出了不准确的声明(销售人员不喜欢承认任何不完美的地方),并且进行了几次试验。这迫使我们研究 GPS 的安全性和可靠性,或者更广泛地说是 GNSS(这个术语不仅包括最初的美国服务,还包括欧洲伽利略系统以及俄罗斯和中国提供的产品)。

在此类服务中,一个卫星星座中的每一个都广播一个非常准确的时间信号,一个接收到四颗或更多卫星的接收器可以解算出它的位置和时间。实际上,它需要的远不止于此。首先,信号的传播取决于电离层中的条件,这些条件是可变的,除非可以根据参考站进行校准,否则会导致误差 一种称为增强的技术,用于飞机导航,可以产生 2 米的精度。消费设备的平均精度更接近 10 米,但由于多种原因,它可能会差得多。

首先,如果可见卫星靠得很近,这会降低精度,如果只有几颗卫星可见,这可能会发生。在这种情况下,您可以查看由此产生的精度稀释并使用它来估计误差。 (对于我们第一个案例中的关键修复,只有五颗卫星可见,预期误差为 45 米;您可以在网站上查看位置和时间的函数。)其次,许多消费设备(例如电话)具有可自动将设备放置在最近的道路或路径上的贴合软件。第三,更大的误差可能来自多路径 通常是当从建筑物反射的信号与直接信号竞争时。多路径和快速匹配的结合导致您的手机或导航仪在驾车或步行穿过高楼林立的城镇时从一条街道跳到另一条街道。最后,还有各种干扰,从简单地拒绝服务的弹幕干扰到更复杂的策略,例如诱饵发送,其中诱饵重新传输在另一个位置观察到的无线电频谱,导致 GPS 设备相信它在那个位置。直到最近,GPS 干扰还是政府干的事,但低成本软件无线电的出现开始传播这种乐趣。如果我是一个被盯上的歹徒,我可以使用 meaconing 来提供不在场证明:它会告诉警察我实际上出去开枪时一直在家。

如果您打算在 GPS 上开展业务,无论是直接还是依赖底层地图服务,最好不仅要了解平均误差,还要了解最坏的情况,以及可能出现此类异常值的情况6。有可能比商品设备做得更好,无论是使用专业设备还是使用巧妙的信号处理。我的一位博士后 Ramsey Faragher 创办了一家公司(焦点定位),它将干涉测量法应用于连续的 GPS 定位,以提高准确性并检测多路径和多种干扰,支持大约 1 的精度

6您应该至少雇用一名阅读该主题的工程师(例如通过 [1017])并关注相关博客(例如 https://www.insidegnss.com。

米7。

在组织层面,法庭案件让人们深入了解该技术如何在警察实践中发挥作用。很大一部分入室盗窃案都是“多发惯犯”所为 通常是有吸毒和酗酒问题的男性,他们曾多次因轻罪被定罪。 （我们的第一个案例是一名男子据称偷偷溜进某人的厨房并从冰箱里偷了一瓶酒。）看看他们中有没有人在 100 码以内,如果有,就派车去接他们。这可能有助于警方通过锁定飞行常客以延长刑期来降低犯罪统计数据;如果监狱里塞满了本应接受康复治疗或接受精神病治疗的人,或者如果它转移了对更有能力的罪犯的注意力,那么在社会上可能不太理想。

14.5 邮资计价器

我的第四个计量案例是邮资计价器。邮票于 1840 年由 Rowland Hill 爵士在英国引入,以简化邮政收费,并发展成为一种可用于特定目的的特殊货币,从支付邮资到支付某些税款以及为邮政汇票充值。到 19 世纪末,邮政系统的大量用户开始发现邮票不能令人满意,邮资计费器于 1889 年由约瑟夫·鲍曼 (Josef Baumann) 发明。它的第一次商业用途是 1903 年在挪威;在美国,亚瑟·皮特尼 (Arthur Pitney) 和沃尔特·鲍斯 (Walter Bowes) 于 1920 年获得了批准使用的仪表,并以此为基础开展了大型业务。早期的邮政计价器是模拟的,会在信件上或胶带上打印邮票（称为邮戳）以贴在包裹上。标记有日期,这样旧的标记就不会被剥离 并重新使用。每个仪表都有一个机械值计数器,由物理密封保护;每隔一段时间,您就会将仪表带到邮局进行读取和重置。防止欺诈依赖于用户将他们的邮件带到了解他们的当地邮局;店员可以检查日期和电表序列号。

1979 年,Pitney Bowes 推出了“电话重置”服务,使公司能够通过电话额外购买价值 500 美元的信用额度;实施涉及机械一次性垫,仪表包含带有连续充电代码的磁带 [477]。 1981 年,该系统升级为基于 DES 的系统,可以用任意金额为电表充电。充值代码部分是从价值计数器计算出来的 所以如果公司谎报他们使用了多少邮资,他们就无法为设备充值。

然而,这些仪表仍然会产生墨水标记。

1990 年,Pitney Bowes 的 Jos´e Pastor 建议用打印的数字签名代替邮票和邮戳 [1497]。这引起了美国邮政总局的注意,他们启动了一项计划来调查密码学是否有助于生产更好的邮资计价器。一个问题是彩色扫描仪和复印机的可用性是否会使邮票和标记太容易伪造。 Doug Tygar、Bennett Yee 和 Nevin Heintze 为他们所做的威胁分析表明,大问题与其说是伪造或复制邮票,不如说是7 全面披露:我投资了这家公司。

篡改仪表以获得额外的邮资。是大宗邮寄者腐蚀了邮政服务的员工,以便在不支付费用的情况下将卡车装载的垃圾邮件插入系统 [1912]。由于散装邮寄者会冒着引起邮政工作人员怀疑的风险 ,所以很想打断他们的交易;然后很自然地锻造了一个仪表板,其感应柱在别处。到 1990 年,美国邮政服务的损失达到了九位数,并且在整个 1990 年代,大量邮件寄件人被高调定罪,他们操纵了他们的仪表,从而获得了数百万美元的免费邮资 [265]。

这导致了一个使用数字签名的仪表的开发程序,该数字签名由邮资计费器中的防篡改处理器生成。这已发展成为可供多个竞争制造商使用的开放标准。

基本思想是,机器可读的邮戳包含发件人和收件人的邮政编码、计费器编号、日期、邮资费率、计费器曾经售出的邮资量和剩余信用额度它,全部受数字签名保护。私人签名密钥保存在仪表的处理器中,而其相应的公共签名验证密钥保存在邮政服务目录中,由仪表序列号索引。通过这种方式,邮政检查员可以在分拣场所对邮件进行批量抽样,检查每件邮件不仅已贴邮票,而且在从其表面来源到目的地的合理路线上。

美国于 2000 年引入了这项技术,Pitney Bowes 等传统供应商销售传统仪表,而 stamps.com 等初创公司获得了在线生成标记的许可,以便客户可以下载并在家中的计算机上打印。德国和英国在 2004 年紧随其后,加拿大在 2006 年紧随其后;其他国家纷纷效仿。到 2006 年,所有美国邮政设施都配备了读取新邮戳所需的扫描仪,下面的图 14.4 显示了一个示例。

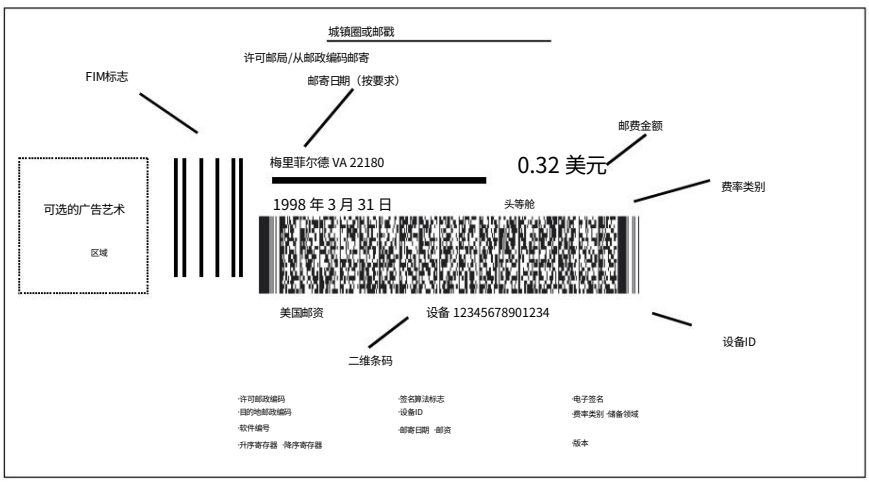

图 14.4：- 美国邮政计量表的一种新格式（由 Symbol Technologies 提供）

这种邮戳可以由直接替换的邮资计费器产生

ments的老式设备;您称量一封信,将其邮寄,然后在月底收到账单。不过,您不必将电表拿去读取,因为信用电表可以通过互联网完成,而如果您购买预付费电表,则可以通过致电呼叫中心并购买一个幻数来补充电表你的信用卡。这与本章前面讨论的预付费电表的工作方式非常相似。

也可以通过简单地指定发件人和目的地邮政编码在 Internet 上购买邮戳。这种“在线邮寄”针对的是小公司和在家工作的人,他们在购买电表时发送的邮件数量不足以让他们物有所值。计量邮资和在线邮资都比邮票便宜。通过跟踪邮件的数量和盈利能力直至本地级别,还可以更好地管理系统。因此,总而言之,数字邮政为用户和邮政服务提供了更大的灵活性。但是安全呢?

邮资计价器是效用计费模型的轻微延伸。有一个防篡改处理器,或者在仪表本身,或者在在线邮寄的情况下连接到网络服务器;这有一个值计数器和一个加密密钥。

它通过创建标记来分配价值,直到价值计数器用完,然后需要从链中更高的控制单元补充。每种情况都有一些附加功能。许多邮资计价器具有“Clark Wilson”功能,其中价值计数器实际上由两个计数器组成,一个升序寄存器 (AR) 包含计价器曾经分配的总价值,一个降序寄存器 (DR) 指示剩余信用额度。平衡控制是 AR + DR = TS,“总设置”,即该设备进行或授权的所有销售总额。如果天平出现故障,仪表就会锁定并且只能由检查员访问。

完整的威胁模型包括被盗的邮资计价器、被篡改以提供免费邮资的计价器、未经授权的人使用的真正的计价器、带有价值不足以覆盖重量和服务等级的标记的邮件,以及有效标记的简单副本。各种抽样和其他测试用于控制这些风险。微妙之处包括您如何处理认证邮件和回复邮件等功能。在从使用哪种身份验证算法到仪表必须将哪种使用数据上传回邮政服务等问题上,各国也存在差异。

一旦运营商获得了实际经验,该行业就开始从数字签名转向消息认证码。签名之所以吸引人,是因为它们优雅;但在现实生活中,签名验证是昂贵的,而且也被证明是不必要的。主要分拣场所的设备每分钟必须处理数千件邮件,而邮政服务通常将邮戳验证为离线批量操作。伪造的邮件最初会通过,只有在出现滥用模式时才会被拦截。一旦集中验证,MAC 就比签名更有意义;中央服务器具有带有主密钥的硬件安全模块,就像公用事业仪表一样,每个仪表中的主密钥多样化为一个 MAC 密钥。事实证明,两位数的 MAC 足以在系统滥用变得严重之前检测到它 [477]。

在许多国家,邮政服务将所有密码学外包给电表供应商。所以邮戳只在本国邮政系统中被验证,因为

海外系统通常会使用不同的供应商。我们还看到了多种架构。例如，加拿大在其标记上同时使用签名和 MAC。（如果你想贿赂一名邮政员工让几吨垃圾邮件进入系统，现在就在边境口岸。）

stu 在现实生活中实际上是如何崩溃的 一如既往 具有启发性。在德国邮政的“Stampit”计划中，用户购买“智能 pdf”文件，这些文件会联系邮政说正在打印，而无需与用户或其软件进行任何交互。如果卡纸，或者打印机没有碳粉，那就麻烦了。因此，用户安排影印邮票，或将其复制到一个文件中，以便在需要时再次打印。英国系统从中吸取了教训：虽然当用户 PC 报告邮票已打印时，邮票被列入灰色名单，但直到邮票出现在分拣处，灰色才变为黑色。句法上的差异很微妙：德国系统不止一次试图阻止你打印邮票，而英国系统更实际地试图阻止你不止一次使用它 [884]。

总而言之，与过去相比，邮政检查员不得不参考机械仪表读数的纸质记录，转向数字邮政仪表可以实现更好的控制。它还促进了将服务扩展到更多客户并改善邮局现金流和信贷控制的商业模式。与数字行车记录仪不同，数字邮政仪表带来了实实在在的好处。

14.6 总结

许多安全系统以某种方式关注环境的某些方面的监视或计量。它们的范围从公用事业仪表到出租车仪表、行驶记录仪和邮政仪表。我们将在后面的章节中遇到更多的计量和支付系统，例如用于在打印机墨盒打印一定数量的页面后停止工作的机制。

随着世界从模拟技术转向数字技术，许多监控、计量和支付系统都进行了重新设计。一些重新设计取得了成功，而另一些则不太成功。数字预付费电表取得了成功，因为它们使发展中国家的公用事业公司能够向甚至没有地址，更不用说信用评级的数亿人出售电力。数字行车记录仪没有那么令人印象深刻。他们只是做旧模拟系统所做的事情，但效果不佳。考虑到许多根深蒂固的利益相关者以及缺乏破坏性流程变更的机会，它们的缓慢演变也许是不可避免的，因为目标是确保成熟行业遵守现有安全法。我们的第三个例子，宵禁标签，将位置监控从车辆扩展到人类。它支持了一些创新，因为技术犯罪监控是一个新行业；它还告诉我们在大型复杂系统中使用 GPS 的一些限制。我们的第四个例子，邮资计价器，确实带来了一些有竞争力的创新，并且取得了成功。

与防盗警报器一样，监控系统的保护与可靠性密切相关。你必须长期认真地思考什么样的服务拒绝

攻击是可能的。密钥管理可能是一个问题,尤其是在您无法提供中央密钥管理设施或雇用足够多值得信赖的人员的低成本广泛分布的系统中。系统可能不得不与众多相互怀疑的各方打交道,并且通常必须在尽可能便宜的硬件上实施。许多监控设备都掌握在对手手中。如果您希望您的设计成功,则必须了解各种应用程序级的微妙之处。

研究问题

关于“物联网”的讨论很多,但供研究人员思考的具体例子却很少。此处描述的案例研究可能会有所帮助。

尽管为支付网络开发的机制(和产品)可以(并且正在)进行调整,但许多设计工作必须重做,最终结果往往存在漏洞。计量应用程序特别有用,因为普遍存在的相互不信任不仅是由相互竞争的商业实体造成的,而且是由各级不诚实的员工以及不诚实的客户造成的;以及大部分设备都在攻击者手中的事实。

同样,安全经济学家和创新学者也有问题。
为什么现有计量系统的一些数字化转型效果很好(公用事业、邮资),而另一些则不那么令人印象深刻(行驶记录仪)?为什么有些具有破坏性,因为新进入者成功地挑战了现有供应商的前任,而在其他情况下(例如邮资),现有供应商设法过渡到更好的数字系统并在来自互联网初创公司的创新竞争中幸存下来?

进一步阅读

预付费电表在[93]中有描述。行驶记录仪写在[64]中;其他与运输相关的论文出现在年度 ESCAR 汽车电子安全会议上。邮政计价器的早期工作是在 [1912] 中,美国的规定可以在 [1320] 中找到。然而,对邮资计价器安全性最详细的阐述是 Francotyp-Postalia 的 Gerrit Bleumer 所著的一本书,该书在该计划中发挥了主导作用 [265]。