第13章

锁和警报

因为如果一个人看得太久,他很可能会睡着。

- 法式培根

最大的错误,我应该说,是没有意识到。

托马斯·卡莱尔

13.1 简介

现在大多数安全工程师都专注于电子系统,但不能忽视物理保护。首先,如果您要就公司的整体风险管理提供建议,那么墙壁和锁是一个因素。其次,由于向具有电气工程或计算机科学背景的人传授物理安全基础知识比反过来更容易,因此物理和逻辑保护之间的交互通常由系统人员来管理。第三,您经常会被问及对客户安装的意见 这些安装可能是由对系统问题知之甚少的承包商建造的。

您需要能够提供知情但外交的建议。第四,如果坏人获得物理访问权,无论是在工厂、运输过程中还是安装前,许多信息安全机制都可能被攻破。第五,许多机械锁最近被“碰撞”完全破坏,这是一种简单的秘密进入技术;他们的制造商似乎常常没有意识到使他们的产品能够被快速绕过的漏洞。最后,许多正在取代它们的电子锁很容易受到攻击,要么是因为它们使用的密码已被破解(例如 Mifare classic),要么是因为机械和数字组件的集成不佳。

许多物理安全只是常识,但也有一些不明显的曲折,而且最近技术取得了重大进展。

关于如何减少设施周围的犯罪发生率,有来自犯罪学和建筑学的有用想法;其中一些也可能会进入系统设计。在防盗警报器方面有一个非常有趣的案例研究。

例如,为了打败防盗警报器,只要让它停止工作就足够了,或者甚至只是让警卫相信它已经变得不可靠了。这为拒绝服务攻击提供了新的视角。正如我们已经看到旨在执行保密性的军事消息传递系统和旨在保持记录真实性的簿记系统一样,监控为我们提供了需要可靠可用的系统的经典示例。如果我的银行金库里有窃贼,那么我不太在乎还有谁知道（所以我不担心保密性）,或者是谁告诉我的（所以真实性不是主要问题);但我非常关心告诉我的尝试不会被挫败。从历史上看,大约 90% 的计算机安全研究是关于机密性的,大约 9% 是关于真实性的,1% 是关于可用性的。但实际的攻击 以及公司的信息安全支出 往往是相反的,更多的花在可用性上,而不是真实性和机密性的总和上。最重要的是,警报系统可以让我们了解可用性。

13.2 威胁和障碍

物理安全工程与数字安全工程在本质上没有什么不同:您执行威胁分析,然后设计一个涉及设备和程序的系统,然后对其进行测试。你根据与客户商定的标准对其进行评估,这在 2019 年可能意味着银行总部大楼有一个规范,其中规定了五年的维护成本、建筑软件渗透测试和安全政策 [350]。入口控制和警报的设计和测试由基于以下的策略驱动:

阻止 检测 报警 延迟 响应

设施可以使用硬方法（例如混凝土墙)或较软的方法（例如不显眼)来阻止入侵者。然后它将有一层或多层屏障和传感器,它们的作用是阻止偶然的入侵者,检测蓄意的入侵者,并使他们难以过快地进入。这将辅之以旨在及时响应现场的警报系统。由于屏障将有供授权人员进出的门,因此将有入口控制,可以是从金属钥匙到生物识别扫描仪的任何东西。最后,这些措施将得到运营控制的支持。例如,您如何应对您的设施经理将他的家人扣为人质?

正如我之前提到的,让员工接受双重控制并将其融入他们的工作文化的方法之一是,这些控制可以保护他们,也可以保护资产。您需要将安全的操作方面嵌入到公司的文化中,否则它们将无法正常工作,这不仅适用于计算机种类,也适用于物理安全。在物理、业务和信息领域获得统一的操作安全性也很重要:如果一个坏人可以将虚假的交货订单偷偷带入您的系统,并发送一个快递员从前台领取钻石。这也是为什么作为信息安全专家,你必须付出代价的另一个原因

也注意身体方面。

13.2.1 威胁模型

一个重要的设计考虑因素是攻击者的技能水平、设备和动机。正如我们在一个接一个的上下文中看到的那样，安全性不是一个标量。问“设备 X 安全吗？”是没有意义的。没有上下文：“在什么环境中针对谁安全？”

在没有“国际标准窃贼”的情况下，我所知道的最近的
工作分类是由一位美国陆军专家开发的 [173]。

- Derek 是一名 19 岁的瘾君子。他正在寻找一个低风险的机会
  偷一些他可以在下一次修复时出售的东西。

- 查理今年 40 岁，有七次入室盗窃罪。
  在过去的 25 年中，他有 17 年是在监狱里度过的。虽然不是很聪明，但他很狡猾，经验丰富；他在里面的咒语中学到了很多“知识”。他从小商店和郊区的房子里偷东西，拿走他认为可以卖给当地围栏的任何东西。

- 布鲁诺是一名“绅士罪犯”。他的生意主要是偷艺术品。作为掩护，他经营着一家小型艺术画廊。他在墙上挂着（伪造的）艺术史大学学位，并在 18 年前因抢劫而被定罪。

  入狱两年后，他改了名字，搬到了这个国家的另一个地方。他偶尔为了解他过去的情报机构做“黑包”工作。他想涉足计算机犯罪，但到目前为止，他所做的最多的事情就是破解锁和篡改警报。

- Abdurrahman 领导着一个由十几名特工组成的小组，其中大多数都接受过军事训练。
  他们可以获得武器和炸药，并得到他的祖国提供的博士级技术支持。阿卜杜拉赫曼本人在其军事学院的 280 名学生中排名第三。他的任务是与该国的海外对手打交道，通常是秘密进入他们的住所或办公室安放监听设备或在他们的电脑和手机中安装恶意软件。他的机构和政府正在考虑的可能任务之一是窃取钚。他认为自己是个好人而不是坏人。

所以 Derek 不熟练，Charlie 熟练，Bruno 熟练且可能得到清洁工等不熟练的内部人员的帮助，而 Abdurrahman 不仅熟练而且拥有大量资源。他甚至可能得到一名或多名被收买的熟练内部人员的帮助。（的确，如今许多恐怖分子勉强达到查理的水平，但如果假设查理是您需要担心的最高级别的攻击者，那么设计核电站是不明智的。现在您的核电站的数十家承包商正在将他们的系统迁移到云端，你可以打赌其中一个将容易受到有能力的有动机的黑客的攻击。）

社会学家关注德里克，犯罪学家关注查理，军方关注阿卜杜拉赫曼，而我们主要关注布鲁诺。他不是

最高级别的“平民”罪犯:这种区别可能属于那些为贩毒团伙洗钱的顽固的银行家和律师,或者是那些为在线犯罪团伙编写恶意软件的人。但银行和计算机房的物理防御往往是为布鲁诺设计的。

13.2.2 威慑

首先要考虑的是您是否可以防止坏人试图闯入。如果可以的话,让您的资产匿名且不显眼是个好主意。它可能是郊区的一座不起眼的建筑;在香港这样的地方,房价高得离谱,它可能是一个不起眼的办公大楼的半层楼。

位置很重要;一些街区的犯罪率比其他街区低得多。
这在一定程度上与附近的其他财产是否受到保护有关,以及骗子判断哪些财产受到保护的难易程度。如果业主只是安装可见的警报器,他们可能会将犯罪重新分配给他们的邻居;但是,让罪犯被捕而不是仅仅发送到隔壁的隐形警报可以阻止整个社区的犯罪活动。例如,伊恩·艾尔斯 (Ian Ayres) 和史蒂文·莱维特 (Ian Ayres) 和史蒂文·莱维特 (Ian Ayres) 研究了 Lojack 对汽车盗窃的影响,这是一种无形地嵌入汽车中的无线电标签,如果汽车被盗,警察可以找到它们。在很多汽车都装有 Lojack 的城镇,偷车贼很快就会被抓获,拆解被盗汽车以获取零件的“拆车店”也被关闭。艾尔斯和莱维特发现,虽然安装 Lojack 的司机每年支付大约 100 美元,但他这样做的社会效益 减少其他人遭受的汽车犯罪 是 1500 美元 [148]。这同样适用于房地产;许多房屋都装有可以悄悄报警的高级警报器的社区对于窃贼来说是一个危险的工作场所。

事实上,自 1990 年代初期以来,美国、英国和许多其他国家/地区的财产犯罪已大幅下降。

但这还不是全部。自 1960 年代以来,出现了大量关于使用环境设计来转移和阻止威胁的文献。其中大部分是在低收入住房的背景下演变而来的,因为犯罪学家和建筑师了解到哪些设计或多或少地增加了犯罪的可能性。 1961 年,伊丽莎白伍德敦促建筑师提高居民对公寓单元的可见度,并创建人们聚集的公共空间并保持公寓入口可见,从而促进社会监督;看不见的区域更容易受到伤害 [2036]。 1972 年,奥斯卡·纽曼 (Oscar Newman) 将其发展为“防御空间”的概念:建筑物应“释放居民潜在的领地意识和社区意识”[1435]。小院子比大公园好,入侵者更容易被发现,居民也更容易挑战。与此同时,Ray Je ery 开发了一个基于心理学而不是社会学的模型,因此考虑了个体罪犯之间的广泛差异;它反映在我们的四个“模范”恶棍身上。入侵者并不完全相同,也不都是理性的 [1609]。

Je ery 的“通过环境设计预防犯罪”具有影响力,并挑战了许多关于威慑的老式想法。老前辈喜欢明亮的安全灯;但它们会产生眩光和阴影,恶棍可以潜伏在其中。最好有一个文明的门面,窗户可以俯瞰人行道和停车场。在过去,带刺的旋风围栏

电线被认为是一件好事;但他们传达出缺乏个人控制。活动频繁的带野餐座位的公共区域具有更大的威慑作用 。树木也有帮助,因为它们让共享区域感觉更安全（也许是对祖先环境的回归,在草地上种有一些树木帮助我们看到掠食者的到来并躲避它们）。访问也很重要;防御空间应该有单一的出口点,这样潜在的入侵者就不会被困住。例如,已经发现闭路电视摄像机只能在停车场等只有一个出口的设施中阻止犯罪 [766]。多年来还开发了许多技巧,从使用过往车辆来提高现场能见度到在窗户下种植低矮的荆棘丛。栏杆可以比墙壁更好地形成障碍,正如您可以透过它们看到的那样。关于这些的建议可以在现代标准中找到,例如 [324]。

另一个有影响力的想法是 George Kelling 和 Catherine Coles [1029] 的破窗理论。他们指出,如果一栋建筑物的窗户破了而且没有修好,破坏者很快就会破坏更多,也许擅自占地者或毒贩会搬进来;如果垃圾留在人行道上,那么最终人们会开始在那里倾倒垃圾。所以问题应该在问题还小的时候解决。凯林被聘为顾问,帮助纽约清理遭到破坏的地铁,并激发了警察局长威廉布拉顿的零容忍运动,后者打击了公共场所饮酒者、清洁工和其他滋扰行为。纽约的轻微犯罪和严重犯罪均大幅下降。

犯罪学家仍在争论下降是由于零容忍,还是其他同时发生的变化,例如人口统计 [1151] 和携带权法 [1188]。

在罗纳德·克拉克 (Ronald Clarke) 的情境犯罪预防理论中可以找到一组相关的思想。这是建立在 Je ery 和 Newman 的工作基础上的,并且比财产犯罪更广泛;它提出了一些原则,通常通过增加风险和努力、减少奖励和挑衅以及消除借口来减少犯罪。它的重点主要是从产品和日常生活中设计犯罪;它是务实的,由应用程序驱动 [440]。它涉及对特定威胁的详细研究;例如,汽车盗窃被认为是许多不同的问题,例如未成年人兜风、夜间盗窃回家以及专业团伙盗窃汽车拆解或销往国外 这些威胁最好通过相当严厉的措施来应对不同的措施。这种实证研究可能会被具有社会学背景的犯罪学家批评为缺乏“理论”,但正在获得影响力并且与安全工程师所做的不远。本书中讨论的许多机制很容易适合应用程序级机会减少的框架。

该框架自然可以在需要时将环境控制扩展到其他主题。因此,如果您计划将托管中心的匿名性作为针对针对性攻击的防御措施,则您必须考虑如何限制知道这些场所位置的人数。至少,那是传统的方法;但这可能不是最后的决定。许多公司已经完全转向第三方云服务,不再有托管中心。这可以节省物理安全成本,以及系统管理员的工资和电费。

13.2.3 墙壁和障碍物

一旦你决定了你将使用什么环境特征来阻止 Derek 或 Charlie 试图闯入你的站点,以及你如何让 Bruno 更难找到他应该闯入你的哪些站点,你就会遇到问题设计物理屏障。

您的首要任务是弄清楚您真正想要保护的是什么。在过去,银行常常竭尽全力让劫匪的生活变得非常艰难,但这有其局限性:劫匪总是威胁要射杀客户。因此,到 1980 年代,理念已经转变为“给他能看到的所有现金”。

这种理念已经传播到其他零售业。 1997 年,星巴克在三名员工在一次拙劣的抢劫中被枪杀后,对人身安全进行了审查。他们决定将保险箱从经理办公室移到商店前面,并使这些保险箱不仅对员工、顾客和路人非常显眼,而且还通过闭路电视让控制室显眼。附带的好处是改善了客户服务。新设计在美国的许多地点进行了测试,增加的销售额和减少的损失带来了良好的投资回报 [505]。我注意到越来越多的人将车钥匙放在家里的前门内,而不是放在床头柜上。

如果有人半夜闯入你家偷你的车,你真的要和他们肉搏吗?

其次,确定了保护目标后,您必须决定出于何种目的以及在何处设置边界或边界。最近一个增长的行业是车辆陷阱,以防止汽车或卡车靠近标志性目标,无论是携带炸弹还是撞倒观光者。但是,以牺牲普通威胁为代价来关注罕见但“令人兴奋”的威胁是错误的。

许多建筑物的墙壁很坚固,但屋顶很容易被穿透;也许恐怖分子会在您的大门处引爆自己而无济于事,但环保抗议者可能会通过爬上屋顶、挖一个洞并丢下一些燃烧物来削弱您的晶圆厂并使您损失数亿美元的生产

报纸。

为此,诸如 NIST、建筑五金制造商协会、美国保险商实验室及其在其他国家/地区的同等组织对墙壁、屋顶、保险柜等具有过多的测试结果和标准。基本思想是评估屏障能够抵抗拥有特定资源(通常是手动工具或电动工具)的攻击者的时间。普通建筑材料根本不会提供太多延迟;你用大锤在不到一分钟的时间内穿过一堵空心砖墙,不管你在前门上的锁有多贵,特警队都会用攻城锤把门从铰链上砸下来。强盗也可以。因此,数据中心、银行金库等的设计者偏爱钢筋混凝土墙、地板和屋顶,以及钢制门框。但是,如果坏人可以在整个周末不受打扰地工作,那么即使是混凝土也无法将他们拒之门外。在英格兰最大的入室盗窃案中,一群老年罪犯于 2015 年在哈顿花园一家保险箱公司的 20 英寸混凝土墙上钻孔,并盗取了 1400 万英镑的钻石。

四年后,头目被抓获,审判中揭露了他如何冒充电话公司工程师来篡改安全系统,然后使用手机干扰器来阻止警报信号 [1547]。

请注意,认证锁具、保险箱和保险库的组织通常会对攻击工具做出过时的假设。您的汽车方向盘上的锁经过认证,可以抵抗男人将其重量压在上面;但是偷车贼已经学会了使用脚手架,这样可以提供杠杆来打破它。典型的银行金库经认证可抵御攻击十分钟,但您当地的消防部门可以使用现代角磨机在两分钟内通过。如果坏人有合适的炸药,他们几乎可以在几秒钟内炸毁任何东西。另一个问题是热喷枪或燃烧棒,它可以快速切开大多数屏障材料:安全工程师使用这些东西进入密码丢失的保险库。强盗也可以得到它们。因此,不能孤立地看待障碍。您必须了解有关威胁的假设,以及您可以依赖的入侵检测和响应。

13.2.4 机械锁

近年来,锁匠行业因暴露出许多低成本机械和电子锁的脆弱性的发展而受到严重打击。

其中第一个是颠簸。这种技术使许多机械锁能够被不熟练的人使用现在容易获得的工具快速打开而不会造成损坏。它的主要目标是最初由 Linus Yale 于 1860 年获得专利的弹子锁（见图 13.1）。这实际上在古埃及使用过,但耶鲁大学重新发现了它,它通常被称为“耶鲁锁”,尽管现在许多其他公司也生产它们。

图 13.1：– 切开的弹子锁（由 Marc Weber Tobias 提供）

这些锁的外壳内装有一个圆柱形插头,并通过多个销钉组防止旋转。每个堆栈通常由两个或三个引脚组成,一个在另一个之上。底针或键针与按键直接接触;它后面是一个弹簧加载的顶部销或驱动销,它迫使底部销在键槽中尽可能向下。当插入正确的钥匙时,每个堆栈中顶部销和底部销之间的间隙与插头的边缘对齐,形成一条剪切线;现在可以转动插头了。一个典型的房屋或办公室锁可能有五个或六个销子,每个销子可能在十个不同的位置有间隙,理论上钥匙多样性为 105或 106种可能的钥匙不同。由于机械原因,实际数量会更少

公差和键切割限制。

多年来人们就知道,只要有特殊工具,就可以撬开这样的锁。

您可以在 MIT Lock Picking Manual [1896] 或 Marc Weber Tobias [1891] 等论文中找到详细信息:基本思想是使用张力扳手稍微拧动插头,然后使用开锁器操纵销钉直到它们都沿着切变线排成一行。这些技术已被锁匠等专家使用多年;但是他们需要大量练习,并且在许多司法管辖区拥有这些工具是非法的(美国的法律,请参见 [1893])。直到最近,人们普遍认为开锁只对投资银行和大使馆等高价值目标构成威胁。

新的发现是,攻击者可以插入一个特制的凹凸钥匙,每个凹凸钥匙的每个齿都设置在最低的销位置,并且其肩部略微圆润。 (这种钥匙也被称为“999”钥匙,因为所有的牙齿都处于最低位置,或咬合,即数字 9。)然后入侵者可以用指尖轻轻扭转钥匙,然后用橡皮轻敲钥匙头槌。冲击使销向上弹起;施加的扭力使它们在弹簧将它们向下推回时粘住,但在圆柱体边缘有间隙。最终效果是只需轻敲几下木槌,就可以打开锁。

这个技巧已经为人所知多年,但由于更好的工具和技术而变得更加有效。它由 Barry Wels 和 The Open Organization Of Lockpickers (TOOOL) 的 Barry Wels 和 Rop Gonggrijp 撰写的 2005 年白皮书宣传,该组织是荷兰“锁具运动”组织(现在称为业余锁匠 [2008])。电视报道向广大观众传播了这一信息。专家的观点是,碰碰桌子会开锁,可能会带来严重的后果 [1892]。例如,发现美国邮箱的锁很容易打开,美国国内市场70%的弹子锁也很容易打开。荷兰报纸和随后的宣传引发了一场军备竞赛,供应商生产更复杂的设计,业余锁匠报告其中许多人受到碰撞攻击。我们现在在我的实验室里有开锁工具包,这样学生们就可以在开放日玩它们了。他们喜欢它!

几乎所有的金属锁都坏了。当我在银行业工作时,Medeco 的锁被认为是不可撬的(甚至经过认证),并被用来保护保存银行最重要的加密密钥的硬件安全模块。公司在高安全性锁具市场占据主导地位。Medeco 在键中进行切割的角度上使用二次键控。在这个“双轴”系统中,有角度的切口会旋转销以接合滑块。 2005 年,Medeco 推出了 m3,它也有一个简单的侧边栏,形式为切入按键侧面的滑块。然而在 2007 年,Tobias 报告了对 m3 和双轴锁的攻击,使用弯曲的曲别针设置滑块,然后结合碰撞和撬动来旋转插头 [1894]。

居士能做什么?作为实验,我更换了自己的前门锁。我在一个小时车程范围内的一家商店里能找到的唯一高安全性产品竟然是来自以色列的重新命名的 Mul-T-Lock 设备。尝试安装了两次,第一次卡住了;然后,家庭成员花了大约一周的时间来学习使用更复杂的门栓,这很容易

如果操作不慎,将无法打开。下一次有情报背景的人来拜访我们时,他说在英国只有毒贩才会装这种锁;所以如果警察路过,我可能最终会作为嫌疑人出现在他们的数据库中。锁没有磨损好;几年后它开始张开,当我取下它时,我注意到一些滚珠轴承已经出来了。

这种对我的家庭安全的可疑改进使我花费了 200 英镑,而标准产品则为 20 英镑;实际上,窃贼总能破窗而入,我们的实际保护仍然更多地取决于我们的位置和我们的狗,而不是五金制品。事实上,Yochanan Shachmurove 及其同事调查了康涅狄格州格林威治的居民,并建立了一个模型,说明家庭盗窃案如何随着所采取的预防措施而变化;锁和死栓基本上没有影响,因为总是有其他进入方式,例如窗户。最有效的威慑力量是警报和明显的占用迹象,例如车道上的汽车 [1709]。

商业公司的情况稍微好一些（但也不多）。美国高安全性锁的常用标准 UL 437 和 ANSI 156.30 规定了防撬和防钻孔,但不防碰撞;虽然防撬锁通常更难碰撞,但这并不能保证。

确实存在关于哪些锁设计可以抵抗碰撞的知识,但您必须寻找它。 （Tobias 的论文和 www.toool.org 是很好的起点。）

因此,购买者面临一个柠檬市场 正如人们可能从大多数锁具供应商的营销文献的光鲜、流畅和缺乏技术内容所怀疑的那样。即使是昂贵的防撬锁,建筑商或原始设备制造商也常常安装不当;有一次我不得不闯入带有 Medeco 锁的密码处理器时,我发现它转动了一个由白色金属制成的凸轮,当我们试图打开它时,它很容易弯曲。事实上,托比亚斯最近发布的一份安全警报显示,一种最流行的高安全性门栓可以通过将窄螺丝刀滑下钥匙槽,在末端抓住门栓并转动它来机械绕过,即使没有破坏锁内广泛的安全保护.这种设计已经存在了二十多年,并且在披露之前制造商并不知道该漏洞。许多高安全性安装使用类似的硬件。

最近出现的第二类问题是万能密钥攻击。这些锁匠也知道了一段时间,但由 Matt Blaze1 进行了改进和发布。万能钥匙系统的设计使得除了建筑物中每扇门的单独钥匙外,还可以有一把打开所有门的顶级万能钥匙 比如,供清洁工使用。更复杂的方案很常见;例如,在我们大楼中,我可以打开学生的门,而系统管理员和清洁工可以打开我的门。在弹子锁中,这种方案是通过在一些弹子堆上进行额外切割来实现的。因此,一些插针堆叠也将有一个中间插针,而不是在它们之间具有单个切口的顶部插针和底部插针。

万能密钥攻击是一次搜索一个额外的切割。假设我的密钥位是 557346,我走廊的主密钥是 232346。我让

1有一个有趣的回复：“几天来,我的电子邮件收件箱里全是来自锁匠的愤怒信件,其中大部分都指出我是个白痴,因为每个人都已经知道这一点,以及我不负责任的一点,因为这种方法太危险了,不能发布”。该论文是[259]。

一把带咬合 157346 的钥匙,然后在锁中试一试。它不起作用。然后我将第一个位置归档到 257346。由于 2 是第一个销的有效咬合,因此这打开了锁,并且由于它与我的用户咬合 5 不同,我知道它是该销的主钥匙咬合。我将不得不为每个销平均尝试四次咬合,如果三个销是万能钥匙,那么我将在大约十二次测试后得到一把万能钥匙。因此,万能钥匙不仅为建筑物的住户提供了更大的便利,也为严重的窃贼提供了更大的便利。这很重要,因为大多数仍然有金属钥匙的大型商业场所都使用万能钥匙。有万能钥匙系统可以抵御这种攻击 例如,奥地利锁匠 Evva 有一个系统,该系统涉及嵌入金属钥匙中的磁铁,这些钥匙更难复制。但大多数已投入使用的系统似乎都很脆弱,而 3D 打印的发明使它们更加脆弱。

机械万能钥匙系统的一大难题是撤销。钥匙持有人离开,可能不诚实或粗心。他们可能已经剪切了密钥的副本,并将其卖给了攻击者。或者有人可能已经为他们的钥匙拍了张照片,并用它来打印副本。万能钥匙攻击在这里很重要,许多昂贵的防撬锁实际上使问题变得更糟。它们通常依赖于辅助键控机制,例如侧边栏:这些键看起来像两个普通的弹子键焊接在一起,如图 11.2 所示。建筑物中所有锁的侧边栏通常是相同的(主钥匙系统通常需要共享主钥匙的锁中的公共侧边栏)。因此,如果一个坏人可以拍下属于我的一个学生的真钥匙的照片,他就可以将它变成一个碰撞钥匙,可以打开我的门,甚至是建筑物中的每扇门,如图 11.3 所示。这在大学校园里可能不是问题,那里除了书本没什么可偷的。但它绝对是针对银行、金银交易商和珠宝商的,攻击者可能会花两年时间计划袭击这些地方。如果这样的设施有一个使用侧边栏锁的万能钥匙系统,并且员工甚至被怀疑泄露了钥匙,那么谨慎的做法是更换每把锁。因此,虽然单独更换机械锁很容易,但在一栋建筑物中集成数百把锁的系统最终可能会将建筑物所有者锁定在锁供应商身上,而不是将窃贼锁在房屋外。

碰撞、坏门栓、万能钥匙攻击和 3D 打印的综合影响可总结如下。随着工具和知识的普及,像查理这样的职业罪犯将能够快速打开几乎所有房屋的锁,而且不会留下任何法医痕迹,而像布鲁诺和阿卜杜拉赫曼这样的更专业的攻击者也将能够打开大多数商业场所的锁。房子的锁可能并不重要,因为查理无论如何都会从窗户出去;但商业场所中大多数机械锁的脆弱性可能会产生更为复杂和严重的影响。

如果您的职责包括服务器机房或其他资产的物理保护,那么是时候开始考虑它们了。

图 11.2 – 侧边栏锁的钥匙

图 11.3 – 侧边栏碰撞键

13.2.5 电子锁

撤销的困难只是电子锁获得越来越多市场份额的原因之一。它们已经存在了很长时间 自 1970 年代以来，酒店一直在使用卡锁。有许多产品使用各种机制，从非接触式智能卡到密码键盘再到生物识别技术。

其中许多可以通过各种方式绕过，本书的大部分章节都可以以一种或另一种方式应用于它们的设计、评估和保证。也有一些机电锁结合了机械和电子（或磁性）元件；但是很难让锁匠、密码学和电磁机制无缝地协同工作；在您测试它们之前，您永远无法分辨。这种锁不仅比简单的金属锁或卡片锁花费更多的钱，而且经常以有趣的方式失效；有大量关于攻击它们的文献 [1839, 1291]。

但是，从使用锁来保护大型复杂场所的大公司的角度来看，问题不在于锁本身，而在于如何管理建筑物中的数十或数百把锁，尤其是当您在全球拥有数十或数百座建筑物时.

较新的建筑物开始意识到谁在哪里，使用多个传感器，并将物理访问控制与逻辑访问控制相结合。在一个理想的世界中，您会实时知道谁通过了哪扇门，并且能够将其与信息安全策略保持一致；例如，如果正在处理机密材料，如果房间内有人未经授权，您可以发出警报。建筑物可以监控物体和人；在我们实验室的一项实验中，人和设备都携带了用于位置跟踪的活动徽章 [1982]。电子系统可以完全或几乎始终在线，从而使撤销变得更加容易。除了执行安全政策外，智能建筑还可以提供其他好处，例如通过关灯和根据居住者的存在调整空调来节省能源。但这将是一个漫长的过程。

正如我们在与我合作过的一个组织中发现的那样，一个实际问题是只有少数公司销售大型门禁系统，而且它们很难定制。在一个建筑项目中，我们发现供应商的协议不支持我们理想中想要使用的套件，而且我们没有时间或人员从头开始构建我们自己的门禁系统。传统门禁供应商的运作方式与其他系统公司的运作方式相同：他们通过锁定（从经济角度，而不是锁匠意义上）赚钱。由于专有的布线系统和卡设计，您最终要花 200 美元购买一个门锁，而制造成本可能为 10 美元。锁定的主要限制是撕裂和更换整个系统的成本 因此是专有布线。

我们选择了一个卡系统来控制对建筑物部分的访问，并使用了 Mifare 非接触式智能卡，因为它们可以从多个门禁供应商处获得。由同一组织运营的其他建筑物使用了该系统，它允许更复杂的访问控制策略，这些策略是一天中时间的函数。在 oce 门本身，我们有金属门钥匙，只有一个矩阵指定哪个钥匙打开哪个锁（这意味着如上所述的主钥匙系统）。该组织希望

及时迁移到更全面的电子系统,一旦他们能够获得能够使体面的系统集成成为可能的组件 - 例如在建筑物的标准以太网上运行的价格合理的门锁。

然后,在 NXP Semiconductors 销售的底层卡系统 Mifare Classic 上发现了一次攻击。这使用了一种称为 Crypto-1 的专有密码,由于 1990 年代加密战争期间实施的出口管制,其密钥被限制为 48 位,我在 26.2.7 中对此进行了讨论。 Mifare Classic 还有其他缺陷,包括弱随机数生成器和通过错误消息泄露密钥流材料的协议。虽然主要用于交通票务,但它也有数万座建筑物的安装基础,并得到几家主要建筑物门禁控制供应商的支持。

Mifare Classic 在 2007 年由 Karsten Nohl 和 col leagues [1450] 部分逆向工程； Flavio Garcia 和奈梅亨的同事在第二年完成了这项工作,发表了对芯片的完整分析,并展示了如何破坏荷兰所有公共交通工具票中使用的版本 [747]。

恩智浦试图让法院禁止这项研究,但失败了。这些针对 Mifare 的攻击的效果是迫使运输系统部署入侵检测系统来检测逃票者;对门禁系统的影响是卡钥匙变得容易复制。任何拥有适当设备并临时拥有钥匙的人都可以制作一份工作副本,就像使用传统金属钥匙一样。更重要的是,一个巧妙的攻击者可以部署一把假锁并复制任何通过它的人的钥匙。这将包括清洁工,他们的钥匙可以打开建筑物中的所有锁,以及安全巡逻人员,他们的钥匙可以打开公司所有建筑物中的所有锁。您甚至可以将非接触式读卡器放入咖啡杯中,将其举至胸部高度,以克隆将钥匙挂在挂绳上的人的钥匙。

一些锁具供应商受到严重打击。一家供应商以接近成本的价格向酒店出售锁具,并通过以每把钥匙 1 美元的价格出售替换卡存货来赚取利润。 Mifare 的突破意味着来自台湾的竞争对手可以以几美分的价格出售兼容的库存,从而破坏他们的商业模式。恩智浦对此作出回应,推出了一款在卡片上添加数字签名的产品,这样锁就可以分辨出它虽然是一把弱钥匙,但却是一把真正的弱钥匙。

对于拥有数十座建筑物并使用由普通卡 卡操作的 Mifare 锁的组织来说,结果是要转向更安全的锁,他们必须立即更换所有锁和卡,或者坚持使用生产了两个系列的 NXP后继卡。第一种是“加固”的经典卡,它们仍然使用较弱的 Crypto 1 密码,但修复了使初始攻击更容易的实施错误;但由于底层密码很弱,这些密码也被破解了 [1316]。第二条产品线使用了更好的算法,例如 DESfire 卡,使用双密钥三重 DES。然而,David Oswald 和 Christof Paar 迅速发现了对 DESfire [1484] 的定时攻击。创业锁供应商开始生产可以应对多个产品线的读卡器,部分缓解了这个问题;一个人不仅可以应对 Mifare,还可以应对 NFC（适用于 Android 手机)和蓝牙（适用于 Apple 制造的手机,它将 NFC 芯片锁定到 Apple pay）。其他人正在采用新技术,例如我在第 4.3.1 节中提到的用于 UWB 无线电的新 802.15.4z 标准。

简而言之,恩智浦通过将其客户迁移到新产品但在安全方面付出了一些代价,设法维持了大部分锁定。这产生的一些外部效应被更警觉的读卡器供应商捕获。然而,对于身为建筑师或建筑服务经理的传统锁具购买者而言,整个领域已经变得过于复杂。这也是 CISO 的安全工程团队也需要对物理安全感兴趣的另一个原因。

13.3 报警

警报不仅仅用于处理入室盗窃。它们的应用范围从监控超市的冷冻温度（这样员工就不会“意外地”关闭冷冻柜,以期得到食物带回家）,一直到冲突地区的简易爆炸装置,这些装置通常是诱杀装置-被困。但是,在盗窃和保护服务器机房、银行金库或艺术画廊的背景下讨论它们很方便。警报还为我们解决更广泛的服务拒绝攻击问题打下了良好的基础,从游戏到电子战,这是一个无处不在的问题。

建立警报的标准因国家和不同类型的风险而异。与锁一样,您通常会聘请专业公司来完成此类工作;但您必须了解技术问题。我自己的专业经验范围从自动取款机内置的警报,到大型风险（例如批发珠宝商)的警报系统使用的通信安全,再到用于保护银行计算机的系统

房间。

服务器机房中的警报受到很好的保护,不会被篡改（至少不会被外人篡改）。所以我将以一家美术馆作为我的案例研究。这有保护珍贵物品并展示它们的有趣设计问题。在白天,攻击者可以作为公众成员进来,我们假设攻击者是布鲁诺　受过教育的专业艺术窃贼。电影编剧对布鲁诺的看法是他组织了对警报的狡猾攻击,花了几天时间仔细研究市政厅的建筑计划：

如何偷画（一）

> 毕加索的一幅画被一个小偷从一个装有“最先进”警报系统的画廊偷走了,小偷移走了十几块屋顶瓦片,并从绳子上下来,以免激活地毯下的压力垫。
>
> 他抓起这幅画,没有碰到地板就爬了出来,并被委托盗窃的富有歹徒付钱。

新闻界喜欢这种 stu　,它确实时有发生。
现实既简单又陌生。让我们系统地研究威胁情景。

13.3.1 如何不保护一幅画

设计报警系统时的一个常见错误是被最新的传感器技术迷住了。市场上有许多令人印象深刻的研究 ,例如您可以将光纤电缆环绕在受保护的物体周围,如果电缆拉伸或松弛小于 100 纳米（千分之一毫米）,它就会发出警报。现代科学不是很了不起吗?因此,天真的美术馆老板会买几英尺的这种神奇电缆,将其粘在他的奖品毕加索的背面,并将其连接到报警公司。那会发现坐在水手长椅子上的家伙。那你怎么打败它呢?嗯,这很容易。

如何偷画（二）

> 布鲁诺以游客的身份进来,躲在扫帚柜里。凌晨一点,他出现,抓起这幅画,朝消防出口走去。
> O 发出警报,但那又怎样!不到一分钟,他就会骑上摩托车。十二分钟后警察赶到时,他已经走了。

警报很少与建筑物入口控制很好地集成在一起。许多设计师没有意识到,除非您能够明确说明白天进入该场所的所有人员,否则您最好对“留守”恶棍采取预防措施 即使这只是一次巡视画廊关闭后。严格的人身安全意味着对人的严格控制。事实上,在 1978 年,RSA 密码系统的首次使用记录并不是为了加密通信,而是为工作人员使用的凭据提供数字签名,以通过爱达荷福尔斯钚反应堆的进入壁垒。证书包含体重和手部几何形状等数据 [1747, 1751]。但我仍然对我访问过的大多数安全站点的建筑物入口控制被轻易击败感到惊讶 无论是通过温和的技术手段,比如坐在别人的肩膀上通过入口亭,还是（通常）通过帮助人们扶着门开着。

更重要的是,报警响应过程往往没有经过深思熟虑。
（过度依赖最新技术的泰坦尼克号效应常常使人们对常识视而不见。）

所以我们千万不要孤立地去想告警机制。正如我上面提到的,物理保护系统有几个步骤:阻止-检测-报警-延迟-响应,并且重点会因应用程序而异。如果我们的对手是德里克或查理,我们将主要关注威慑。

在 Abdurrahman 可能试图窃取裂变材料的那种目标上,几乎肯定会检测到攻击;主要问题是要拖延足够长的时间让海军陆战队赶到。布鲁诺是最有趣的案例,因为我们不会有军事预算来阻止他,而且有更多的场所,其捍卫者担心布鲁诺而不是阿卜杜拉赫曼。

因此,您必须仔细查看并确定更大的问题是检测、延迟还是响应。

13.3.2 传感器故障

防盗警报器使用范围广泛的传感器,包括:

- 振动探测器,用于感应栅栏扰动、脚步声、玻璃破碎或对建筑物或周边的其他攻击;
- 打开门窗;
- 检测体温的被动红外设备;
- 使用超声波或微波的运动探测器;
- 无形的微波或红外线屏障;
- 地毯下的压力垫,在极端情况下可能会扩展到在每块地砖下使用压力传感器测量整个地板。
- 摄像机,如今通常带有移动检测器甚至面部检测器,可以自动报警或向监控中心提供实时视频馈送;
- 设备上的运动传感器,从通过地震仪的简单束缚电缆到光纤环路。

大多数传感器都可以绕过。翻越围栏可以打败围栏干扰传感器;移动非常缓慢的运动传感器;通过打破墙壁来切换门窗。设计良好的传感器组合归结为技能和经验(后者并不总是保证前者)。传感器安装的标准参考文献是 [408],虽然有点过时。

主要问题是限制误报的数量。超声波在中央供暖入口等移动空气附近表现不佳,而振动探测器可能会因 trac 而变得无用。雷电等恶劣天气会触发大多数系统,而飓风不仅会带来雨水,还会导致数以千计的误报,从而淹没一个城镇的警察队伍。在某些地方,即使是正常的天气也会使保护变得困难:您如何保护入侵者可能能够越过您的传感器(甚至越过您的栅栏)2 的地点?

但无论你是在阿拉斯加还是亚利桑那,主要的困境是你离受保护的物体越近,你对环境的控制就越严密,因此可实现的误报率就越低。

相反,在外围很难降低误报率。但是要延迟入侵者足够长的时间让警卫到达那里,外围正是您需要可靠传感器的地方。

如何偷画(三)

> 所以布鲁诺接下来的进攻,就是等待一个漆黑的暴风雨之夜。他以某种方式设置了警报,注意不要被闭路电视捕捉到

2对于一个核电站的入侵者检测的指导性工作示例雪区见[173]。

或留下任何其他确凿证据证明警报是真实的。他退后几百码,躲在灌木丛中。守卫出来了,什么也没发现。他等了半个小时,再次设置了闹钟。这次守卫不打扰了,所以他进去了。

误报 无论是有意还是无意 都是行业的祸根。它们是对警报响应部队的拒绝服务攻击。电子战的经验表明,大于 15% 的误报率会降低雷达操作员的性能;大多数入侵者警报响应器的运行都远高于此阈值。故意引起的误报对于没有全天候警卫的站点特别有效。

许多警察部门有一项政策,即在某个地点发出一定数量的误报后(通常每年三到五次),他们将不再派警车到那里,直到报警公司或其他关键人员到场检查.

误报会以其他方式降低系统的性能。它们由天气条件和交通噪音等环境刺激引起的速度限制了可以有效部署的传感器的灵敏度。此外,警报行业的成功极大地增加了警报总数,从而降低了警察对虚假警报的容忍度。一个常见的策略是将远程视频监控作为第二道防线,这样报警公司的调度员就可以检查客户的房屋;许多警察部队优先处理以这种方式确认的警报 [979]。但即使是视频链接也不是万灵药。攻击者可以在同一条街道上的其他建筑物中关闭照明、生火或设置 o 警报。由于洪水或飓风,电话交换机出现故障,可能会导致投机抢劫。

在交通和天气之后,布鲁诺的下一个盟友是时间。植被长到传感器光束的路径上,栅栏变得松弛导致振动传感器不能很好地工作,犯罪团体学习新的技巧,同时哨兵变得自满。

因此,需要严密的人身保护的地点通常有几个边界:一个外围栏,以防止醉汉和野生动物进入;然后是带有埋藏传感器的平坦草地,带有红外线屏障的内部围栏,最后是一座足够大的建筑物,可以在骑兵到达那里之前延迟坏人。国际原子能机构针对拥有超过 15 克钚的场址制定的法规具有指导意义 [949]。

在大多数站点,这种保护都太昂贵了。即使你有很多钱,你也可能在曼哈顿或香港这样的地方,那里的房地产价格昂贵:如果你必须靠近交易所才能足够快地进行交易,你的银行计算机房可能只是办公楼的一层,而且你必须尽你所能保护它。一个很好的例子来自佛罗里达州的一伙珠宝窃贼,他们的目标是零售店,这些零售店与没有理由安装警报的美甲沙龙等商店共用一面墙。

他们闯入那里,然后穿过墙壁进入珠宝店 [1215]。

不管怎样,传感器和物理屏障的组合仍然只占不到一半。

13.3.3 特征交互

入侵者警报和障碍以多种方式与其他服务交互。
其中最明显的是电。停电会使许多地点一片漆黑且不受保护,因此重要的报警装置需要备用电源。不太明显的相互作用是与火灾警报和消防。

如何偷画（四）

> 布鲁诺以游客的身份参观了画廊,并在计时器上留下了一枚烟雾弹。它在凌晨一点关闭并设置火警警报,这反过来又导致防盗警报器忽略来自其被动红外传感器的信号。 （如果没有,警报调度员无论如何都会忽略它们,因为他会集中精力让消防车赶到现场。） 布鲁诺从消防出口闯入并抓住了毕加索。他可能会在混乱中逃脱,但如果他没有逃脱,他总是可以声称自己是一位热心公益的旁观者,他看到了火灾并冒着生命危险拯救了该镇无价的文化遗产。警察可能不相信他,但他们很难给他定罪。

有史以来最大的入室盗窃案 2019 年从德累斯顿的 Grune Gew ¨ olbe 盗窃了价值约 10 亿欧元的宝藏,这里是奥古斯都大帝的宝藏室和其他十几个藏有无价古董的房间。他们[469]附近建筑工地发生火灾导致当地变电站难以,当地路灯和博物馆电源都被关闭[1043]。

它的保安人员最终在闭路电视上看到了入侵者并报了警,但他们没有及时赶到。

火灾和入侵之间的相互作用总是很困难。在核反应堆,通常有一条规则,如果发现炸弹,该地点将被封锁,任何人不得进出;以及消防安全规定,如果发生火灾,必须疏散大部分人员（也许还有一些当地居民）。这就提出了一个有趣的问题,即如果炸弹爆炸 ,则适用哪条规则。一些防火措施只有在您可以将无辜入侵者拒之门外时才能使用。许多服务器机房都有自动灭火器,这通常意味着充满二氧化碳。二氧化碳倾倒场对未经训练的人来说可能是致命的:当能见度下降到几英寸时,你必须在肺部的空气中离开房间,并且你会被倾倒场可怕的尖叫声弄得迷失方向。氮气倾倒虽然不那么引人注目,但也是致命的。氧气浓度下降不会像二氧化碳浓度上升那样引起恐慌反应。

但最严重的特征交互是在警报和通信之间。

13.3.4 通信攻击

老练的攻击者攻击通信的可能性至少与攻击传感器的可能性一样大。有时这意味着传感器和传感器之间的布线

报警控制器。

如何偷画（5）

布鲁诺走进一家美术馆，趁工作人员分心时，他切断了窗户开关的电线。那天晚上他回去自助。

您的一名员工或一名清洁工也有可能被贿赂、引诱或胁迫制造漏洞。在英国最大的抢劫案中，2006 年 2 月发生在肯特郡汤布里奇的 Securitas Cash Management 仓库，劫匪假装是警察将经理和他的家人扣为人质。然后他们强迫他让他们进来，并拿走了 53,116,760 英镑；尽管有五名劫匪被抓获并入狱，但其他人逃脱了，大部分钱也没有追回。当我在 1980 年代在银行工作时，我们小心翼翼地向我们的现金中心经理介绍了控制措施，以防止他们的家人被劫持为人质。拥有知识渊博、积极进取的后卫固然好，但双控防守必须深入贯彻。拥有有能力的防御者的高价值站点坚持要求由两个人而不是一个人来完成警报维护和测试。即便如此，双重控制并不总是足够的，尤其是当你的对手是 Abdurrahman 而不是 Bruno 时。在英国有史以来第四大抢劫案中，临时爱尔兰共和军于 2004 年 12 月在北银行绑架了两名钥匙持有人，并用枪指着他们的家人，迫使他们在第二天让他们进入银行位于贝尔法斯特的总部。恐怖分子带着 2640 万英镑逃脱，为了让大部分钱毫无用处，他们偷走的 50 英镑纸币被停止流通。另一个边缘案例是监狱系统，其中对传感器、电缆甚至建筑物结构的攻击非常频繁，因此持续的测试和检查计划至关重要。问问自己“如果我的一半员工是释放日的罪犯，我会怎么做？”和“如果我的少数员工为一个决定抢劫我的组织工作，我将如何应对？”我将在有关银行业务和簿记的章节中更详细地讨论双重控制的含义。

保护报警传感器和控制器之间通信的老式方法是物理的：为每个传感器铺设多根电线并将它们埋在混凝土中，或者使用铠装气体加压电缆。更现代的方法是加密通信 [706]。那么你如何攻击那些？

如何偷画（6）

布鲁诺打电话给竞争对手画廊，声称来自处理他们警报的安保公司。他说他们正在更新他们的电脑，所以他们可以告诉他他们的警报控制器单元的序列号吗？一名初级工程师很有帮助地这样做了 没有意识到盒子上的序列号也是保护通信安全的加密密钥。布鲁诺以 200 美元的价格购买了一个相同的控制器，现在他拥有了一个功能相同的单元，他将其连接到竞争对手的电话线上。这会继续报告“一切正常”，即使事实并非如此。

用假冒的报警设备或模仿它的计算机来代替,被称为“欺骗”。多年来一直有黑匣子欺骗各种报警控制器的报道。早在 1981 年,窃贼就盗窃了价值 150 万美元的从中国进口的玉石雕像和黄金首饰,导致进口商破产。保护其位于新泽西州哈肯萨克的仓库的警报系统被切断 。通常这会触发安全公司的警报,但盗贼将自制电子设备连接到外部电缆以确保持续电压 [861]。我在第 13.2.3 节中提到了英国最大的盗窃案是如何涉及干扰警报信号的。

使用更好的现代系统,要么保险库中的警报控制器向警报公司发送加密伪随机序列,如果它被中断,警报公司将假设最坏的情况,要么警报公司定期向控制器发送随机挑战,这些挑战被加密并返回,只是与 IFF 一样。然而,设计通常是错误的,因为工程师没有接受过安全协议方面的培训。加密算法可能很弱,或者它的密钥可能太短(无论是因为无能还是出口法规)。

即使没有,Bruno 也可以记录伪随机序列并稍微慢一点重放,这样到周一清晨他可能已经积累了五分钟的“松弛”时间来应对闪电袭击。

一个更常见的失败原因是严重的设计错误。一种是使加密密钥等于设备序列号。这通常出现在很多人都能看到的采购订单、发票和其他文件中。 (用现金购买警报控制器是个好主意。这也使您不太可能得到一个被“加标”的控制器。但大公司通常很难做到这一点。)

到目前为止,您可能已经决定不涉足美术馆业务。但我把最好的留到最后。这是对防盗报警系统最强大的攻击。它是 (3) 的变体,但不是针对传感器,而是用于通信。

如何偷画(7)

> 布鲁诺切断了他对手画廊的电话线,躲在了几百码外的灌木丛中。他数着到达的穿蓝色制服的人数,以及离开的人数。如果这两个数字相等,那么可以合理猜测保管人说过,“哦,麻烦了,我们会在早上修好它”,或者类似的词 eect。他现在知道他还有几个小时的工作时间。

这或多或少是攻击银行金库的标准方法,它也被用于计算机安装。作案手法各不相同,从简单地将卡车倒车驶入电话公司的路边接线盒,到更复杂的尝试在不同场所引起多个同时警报并淹没当地警察部队。 (这就是为什么它比仅仅敲击栅栏更强大。)

在一个案例中,新泽西州的小偷切断了三根主要的电话线,导致三个警察局以及哈肯萨克梅多兰兹 (Hackensack Meadowlands) 数以千计的家庭和企业的电话和警报设备瘫痪。他们利用这个机会

从美国经销商处窃取 Lucien Piccard 手表,批发价值 210 万美元,零售价值可能为 800 万美元 [861]。在另一起事件中,俄克拉荷马州的一名副手 sheri 在盗窃毒品仓库之前切断了塔尔萨 50,000 户家庭的电话线 [1923 年]。第三次,一个恶棍炸毁了电话交换机,中断了伦敦珠宝区数十家商店的服务。

这种使响应部队的能力饱和的一揽子服务拒绝攻击相当于核打击的盗窃行为。从电话到宽带的转变没有任何改变;一名英国窃贼现在没有切断 BT 电话线,而是切断了 BT Openreach DSL 线,这是同一根铜线,但现在传输数字信号。在有线电视公司提供宽带的地方,你切断它;因此,美国窃贼将学会如何识别康卡斯特电缆,如果它们是本地供应商的话。更重要的是,报警服务通常与宽带供应商合作,让提供传感器的公司在低成本的批量市场上竞争,他们没有动力做任何复杂的事情。

未来的攻击可能不涉及剪断或爆炸物,而是对网络设施的分布式拒绝服务攻击。与其让本地电话交换机附近的所有警报都关闭(可以通过用警察淹没它来在一定程度上保护它),还可以关闭由同一个警报监控的数千个警报公司,或通过攻击响应链中的其他组件。这可能包括对警察通信或 4G 网络的攻击,因为这些网络比有线线路更多地用于报警通信。最小化易受攻击组件数量的一种方法是使警报通信匿名,这样就无法针对拒绝服务攻击 [1423]。

多年来,伦敦保险市场(世界上大部分主要再保险业务都在伦敦保险市场开展)的规则是,保险金额超过 2000 万英镑的场所中的警报控制器必须具有两种独立的通信方式。

传统方法是一种使用有线通信的警报和一种使用蜂窝无线电的警报;到 2019 年,我们将看到使用两种不同 4g 无线电服务的产品 。这打开了干扰的可能性,如第 13.2.3 节中提到的 2015 年哈顿花园入室盗窃案中所使用的那样。在核世界,国际原子能机构的规定规定,含有超过 500 克钚或 2 千克铀 235 的场所必须在场所内同时配备警报控制中心和武装响应部队 [949]。

在您保护的资产不是保险库而是托管中心的情况下,网络对您的运营也至关重要。如果将您连接到世界的单根光纤穿过路边的接线盒,那么拥有八英寸的混凝土墙和屋顶就没有什么意义了。您会希望至少有两条埋入式光纤连接到至少两个不同的电信公司 并且您会希望它们使用来自两个不同供应商的交换机和路由器。即便如此,对于知识渊博的对手来说,摧毁托管中心的最简单方法通常是切断其通信。这就是为什么小公司有两个中心而大服务公司有几十个的原因之一。如果您不是在云规模上运营,您可能想问问自己:谁想挖掘,谁知道去哪里,您会及时发现他们吗?

最后,值得记住的是,许多人身安全事件都是由愤怒的人进入工作场所引起的 无论是配偶、前任

员工或客户。在枪支私有化普遍的国家,你必须为射手做好准备。

13.3.5 经验教训

读者可能仍然会问,为什么一本本质上是关于计算机系统安全的书要花好几页来描述墙壁、锁和警报系统。有比显而易见的更多的原因。

- 大多数锁都可以被破解。可以对金属钥匙进行拍照,并用 3D 打印机制作伪造品,甚至是老式文件;他们打开的锁经常会被撞到。如果您可以靠近,通常可以克隆卡片钥匙。

  所以警报很重要。

- 处理拒绝服务攻击是许多安全系统设计中最困难的部分,通常也是最重要的部分。入侵者警报为我们提供了适用的知识和经验。

- 一个非常普遍的教训是必须审视整个系统 从
  通过检测、报警、延迟和响应进行威慑。

- 另一个观察结果是,最外层的外围防御是您最想依赖的防御,但也是最不值得依赖的防御。

- 漏报率和误报率(接收器操作特性)之间的权衡 也是安全工程中普遍存在的问题。

- 让警卫保持警觉是一项艰巨的工作,尤其是在几乎所有警报都是误报的工作中。典型的例子是机场安检,美国运输安全管理局将测试枪放入手提箱,无论是物理上还是使用 X 光机中的软件。他们发现,如果您在每个检查点每个轮班多次测试安检人员,只有大约 20% 的威胁可以通过,但如果您只测试一次,则这一数字会上升到 60-75% [713]。

- 不了解威胁模型 为查理设计并希望将布鲁诺拒之门外 会导致许多现实生活中的失败。您需要知道实际出了什么问题,而不仅仅是犯罪作家认为出了什么问题。

- 最后,您不能只将安全工程项目的技术方面留给专业分包商,因为关键的研究 总是会漏掉。

还有其他与报警行业的经验相关的应用。在后面的章节中,我将讨论防篡改处理器,这些处理器旨在检测渗透它们的企图并通过销毁所有加密密钥材料来做出响应。

13.4 总结

安全工程师必须处理物理保护以及计算机和密码系统。正如计算机和电信的融合见证了计算机行业的设备和方法取代了旧的电话公司做事方式一样，物理保护系统的自动化正在稳步将屏障、锁和警报的世界带入我们的轨道。向“智能建筑”的转变意味着进入控制、警报和系统安全与能源管理等相结合。此类复杂人工制品的设计、实施和管理将越来越多地成为系统安全人员的工作。

在本章中，我强调了一些值得注意的事情。首先，环境威慑很重要；建筑、景观和照明等因素可以真正降低入侵的可能性。

其次，锁并不像您想象的那么安全。秘密进入技术的最新发展导致了对大多数机械锁甚至昂贵的“高安全性”产品的攻击的广泛公开。

许多卡片钥匙系统也容易受到攻击，因为最常见的产品在 1990 年代受到美国出口管制的影响，并且用更好的产品替换它们的过程受到行业结构和激励措施的阻碍。

除非您至少了解密码学、协议和防篡改的基础知识，否则不可能知道什么是好的，什么不是；这是安全工程师的工作，而不是退休警察的工作。

第三，从已经相当自动化的物理安全的一个方面，即警报，可以学到很多东西。警报为我们提供了一个很好的系统示例，该系统的安全策略取决于可用性而不是机密性或完整性。在其他情况下处理拒绝服务攻击时，它们可以为我们提供一些有用的见解。

研究问题

在战略层面，物理安全和系统安全的融合势必会引发各种新问题。我希望那些探索信息/物理安全边界的人会发现新的研究挑战；我们将在 2020 年出版时提出的一个例子是声学侧通道的使用。给定一个像样的麦克风，你可以记录耶鲁键被推入键槽时的咔嗒声，并用它来推断键咬 [1225]。

毫无疑问，这样的结果还会更多。从安全经济学的角度来看，锁匠行业的问题将成为一个很好的论文题目：Mifare 和其他产品中发现的漏洞是如何在整个供应链中得到处理的，这是一个复杂的故事，据我所知，没有人我知道，确实系统地分析过。将此与其他复杂生态系统如何应对关键组件的安全故障进行比较可能会很有趣。

在技术层面，我们可能需要更好的机制来指定和实施可以管理物理和其他形式的策略引擎

的保护。至于低级机制,我们可以使用更好的工具来管理嵌入式系统中的密钥。正如飞利浦的一位工程师对我说的那样,智能建筑是否意味着我每次更换灯泡时都必须执行安全协议?智能建筑最终会开放吗,因为许多不同的服务公司都可以访问所有有能力的对手都必须假设有一份副本的计划?但如果你真的想让坏人不知道你核电站报警响应中心的准确位置,你如何对这些信息保密呢?您的所有承包商都会高兴地声称已通过 ISO 27001 认证,但几乎每家承认大数据泄露的公司也是如此。

进一步阅读

关于报警系统的经典参考文献是 [173],而一些系统问题在 [1423] 中进行了讨论。特定国家的资源通常可通过美国工业安全协会 [45] 等贸易协会以及当地保险业获得;许多国家都有一个非营利机构,例如美国的 Underwriters Laboratories [1916],以及对产品、安装或两者进行认证的计划。对于锁碰撞和相关主题的进展,我会关注 Tool 组、Marc Weber Tobias 和 Matt Blaze; Matt 还撰写了有关保险箱破解的文章 [261]。有关最新传感器技术的研究论文出现在 IEEE Carnahan 会议上 [952]。最后,用于监测核军备控制条约遵守情况的系统在 [1748] 中有记载。