第16章

防伪印刷和印章

印章的好坏取决于将其放在公文包中的人。

– 卡伦·斯帕克·琼斯

如果您不知道如何破解它,您就无法保证安全。

– 马克韦伯托比亚斯

16.1 简介

许多计算机系统在某种程度上依赖于安全印刷、包装和密封来保证其保护的重要方面。

- 大多数安全产品都可以被击败,如果对手可以在您安装它们之前得到它们。密封件和防篡改包装通常有助于可信分发,即向用户保证产品自出厂以来未被篡改。

- 我们看到监控系统（例如公用事业仪表和行驶记录仪）通常如何使用密封件来让用户更难篡改输入。无论密码学多么复杂,密封件的失败都可能是系统的失败。

- 由于对 Mifare 及其一些后续产品的攻击,我还讨论了如何克隆大多数建筑物门禁系统中使用的非接触式卡。如果您在让工程师进入您的托管中心之前要仔细检查他的 ID,那么最好在查看 ID 的同时以电子方式阅读它。即使使用电子身份证,安全打印仍然很重要。

- 总的来说,使证书防篡改而不是防篡改可能是一个更现实的目标:如果有人拆开他们的智能卡并取出钥匙,他们应该无法将其重新组装成可以通过仔细检查的东西。防伪印刷在这里可以提供帮助。

除了印刷和封印技术的这些直接应用之外,现代彩色扫描仪和打印机可以轻松地用于制造还过得去的伪造品,这开辟了另一条战线。自 20 世纪 90 年代后期以来,印钞机一直在推广数字保护技术 [253]。这些包括阻止合规扫描仪和打印机被用于伪造的水印,以及可以在自动售货机中检测到伪造的不可见版权标记 [830]。同时,彩色复印机和打印机的供应商在其打印输出中嵌入了取证跟踪代码,其中包含机器序列号、日期和时间 [621]。因此,数字世界和“有趣墨水”的世界越来越近了。

16.2 历史

海豹有着悠久而有趣的历史。在关于银行系统的章节中,我讨论了簿记系统如何起源于粘土片或大疱,美索不达米亚的新石器时代仓库管理员使用粘土片作为农产品收据。

5000 多年前,bulla 系统被改编为通过让仓库管理员在带有他的标记的粘土信封中烘烤 bulla 来解决纠纷。

在古代地中海和中国,印章被用来鉴定文件。在纸张出现之前,它们在中世纪的欧洲被用作社会控制的手段。车夫会在一个收费站得到一个铅封,然后在下一个收费站上交,而朝圣者会从神社得到铅标记,以证明他们已经去朝圣了(事实上,年轻的古腾堡通过发明一个在铅封中嵌入镜子碎片以防止伪造和保护教会收入的方法)[825]。即使在手写签名成为信件的主要认证机制之后,印章仍然作为次要机制存在。直到 19 世纪,信件才被放入信封中,而是折叠多次并用热蜡和印章戒指密封。

在中国、日本和韩国,印章仍然是重要文件的首选认证机制。在其他地方,重要文件上的公司印章和公证人印章、一些国家元首用于立法档案副本的国家印章,以及一些欧洲国家对电子签名的需求,都保留了它们以前重要性的痕迹符合欧盟 eIDAS 标准的性质。

然而,到 20 世纪中叶,在西方,它们在文件中的使用已经变得不如它们用于验证包装重要。

从散装商品到包装商品的转变,以及品牌重要性的日益增长,不仅创造了更好的质量控制的潜 ,而且也带来了坏人可能篡改产品的脆弱性。美国遭受了篡改事件的流行,特别是软饮料和医疗产品,导致 1993 年报告的病例达到 235 例的高峰 [1027]。这有助于推动许多制造商使产品防篡改。

自 20 世纪 80 年代中期以来,软件复制的便捷性以及消费者对技术复制保护机制的抵制,导致软件公司越来越依赖包装来阻止假冒者。那只是

在防止伪造高价值品牌商品（从香水和香烟到飞机备件再到药品)方面的更大市场的一部分。简而言之,大量资金投入到密封件和其他种类的安全包装中。

不幸的是,大多数海豹仍然很容易被打败。典型的印章由带有防伪印刷的基材组成,然后将其粘在或绑在被密封的物体周围。所以首先要看防伪印刷。如果整个印章很容易伪造,那么再多的胶水或绳子也无济于事。

16.3 安全打印

拿破仑在 1800 年代初期将纸币以及不记名证券和护照等其他有价值的文件引入欧洲,从而引发了安全印刷商和伪造者之间的一场战斗,这场战斗展示了掠夺者和猎物共同进化的许多特征。摄影（1839 年)帮助了进攻者,然后彩色印刷和钢蚀刻（1850 年代)帮助了防守者。

近年来,彩色复印机和廉价扫描仪已被全息图和其他光学可变设备所对抗。有时双方都涉及同一个人,例如当一个政府的情报部门试图伪造另一个政府的护照 - 甚至是其货币时,就像双方在第二次世界大战中所做的那样。

有时,钞票设计者会屈服于泰坦尼克号效应,过分相信最新技术,过分相信某些特定的技巧。一个例子来自 1990 年代伪造的英国纸币。这些钞票有一条窗线 一条穿过纸张的金属条,宽约 1 毫米,每隔 8 毫米到达纸张表面。所以当你在反射光下看这张钞票时,它似乎有一条金属点线穿过它,但当你举起它并通过透射光看它时,金属条是黑色和实心的。复制这被认为是困难的。然而,一个犯罪团伙想出了一个漂亮的黑客。他们使用廉价的烫印工艺在纸张表面铺上金属条,然后用白色墨水在上面印上实心条的图案,使预期的金属图案可见。他们在审判中被发现在几年的时间里伪造了价值数千万英镑的钞票 [697]。英国纸币现在正在被改用塑料纸币,这是澳大利亚首创的一个过程。

16.3.1 威胁模型

一如既往,我们必须在威胁模型的背景下评估保护技术。从广义上讲,威胁可以来自大型组织（例如一个国家试图伪造另一国的钞票）,来自中型组织（无论是每月伪造数百万美元的犯罪团伙还是在葡萄酒上伪造标签的经销商）,业余爱好者使用他们在家里或办公室拥有的设备。

在钞票业务中,二十世纪最后几年的最大增长领域是业余伪造。知识在印刷业传播

如何制造大量钞票的高质量伪造品,人们可能认为这会提高专业伪造品的水平。但是高质量彩色扫描仪和打印机的普及给许多人带来了诱惑,在那个需要凌乱的湿墨水的日子里,他们做梦也想不到从事伪造工作。业余爱好者曾经被认为是一个小麻烦,但自从大约 1997 年或 1998 年以来,他们已经占了美国发现的大部分伪造品。业余伪造者数量众多,因此很难对付;他们大多工作规模很小,以至于他们的产品需要很长时间才能引起当局的注意;而且他们不太可能有犯罪记录。他们出示的票据往往不足以通过银行出纳员,而是在黑暗嘈杂的夜总会等场所发出。

业界将伪造纸币或文件的检查分为三种不同的级别 [1935]:

1. 初步检查是由未经培训且缺乏经验的人员执行的,例如公众成员或商店的新收银员。往往初级督察没有动 ,甚至是负动 。

   如果他拿到一张感觉有点不对劲的钞票,他可能会尝试将它传递出去,但不会仔细观察它,以至于不得不决定是成为同谋还是去报告它的麻烦;

2. 二次检查是由有能和有积极性的人在现场进行的,例如对银行结进行经验丰富的银行出纳员或对产品标签进行培训的制造商检查员。

   这个人可能有一些特殊设备,例如紫外线灯、带有化学试剂的笔,甚至是扫描仪和 PC。然而,该设备在成本和体积上都将受到限制,并且会被严重的造假者完全理解;

3. 第三次检查是在制造商的实验室或发钞银行进行的。设计安全印刷(甚至可能是底层工业流程)的专家将在现场,并提供大量设备和支持。

安全印刷技术的现状可以总结如下。让假冒产品通过初级检查通常很容易,而如果产品和检查流程设计得当,则通过三级检查通常是不可能的。因此,二次检查是战场 除了钞票印刷等少数应用,现在注意集中在初级水平,限制是技能,最重要的是,动 。二级检查员在现场可以检测到哪种假冒产品的主要限制与所需设备的体积和成本有关。

16.3.2 防伪印刷技术

传统的安全文件使用多种印刷工艺,包括:

· 凹版,一种使用雕刻图案以强大的量将油墨压在纸上的工艺,留下凸起的油墨印象,具有很高的

定义。这通常用于纸币和护照上的滚动工作；

- 凸版印刷，将油墨滚到凸起的类型上，然后将其压在页面上，留下凹陷。纸币上的数字通常以这种方式印刷，通常有不同尺寸的数字，并使用不同的油墨，以防止使用现成的编号设备；

- 称为同步印刷机的特殊印刷机，可将正面和背面的所有油墨同时转移到纸张上。正反面印刷因此可以准确对齐；图案可以部分印在正面，部分印在背面，这样当纸币对着光时它们可以完美匹配（透视套准）。

  据信，在廉价的彩色印刷设备上很难再现这一点。
  Simultan 印刷机也有特殊的管道，使墨水颜色沿线变化（彩虹）；

- 用于背书文件或密封照片的橡皮图章
  给他们；
- 还用于密封照片和银行卡的压纹和层压材料推高了伪造成本。压印可以是实体的，也可以使用激光雕刻技术将照片刻印到身份证上；

- 水印是在纸张中加入保护功能的一个例子。
  它们是更透明的区域，通过在制造时改变纸张的厚度而插入到纸张中。许多其他特殊材料，如荧光线，也用于类似目的。

更现代的技术包括：

- 现代塑料钞票首先在澳大利亚推出，允许在透明窗口中嵌入各种特征；

- 光学可变墨水，可根据视角从绿色变为金色；

- 具有磁性、光致变色或热致变色特性的墨水；
- 只有使用特殊设备才能看到的印刷特征，例如需要放大镜才能看到的美国钞票缩微印刷，以及紫外线、红外线或磁性油墨印刷（最后一种用于美国钞票的黑色印刷）；

- 金属线和箔，从简单的虹彩特征到箔颜色复制，再到具有光学可变效果（如全息图和动态克)的箔。全息图通常是光学制作的，看起来像胶片后面的固体物体，而运动图是由计算机制作的，可能会从略微不同的角度显示许多惊人的不同视图；

- 屏幕陷阱，例如太暗而无法正确扫描的细节，以及包含正确尺寸细节的别名带结构，以与普通扫描仪和复印机的点分离形成干扰效果；

- 数字版权标记可能不同于通过直接傅里叶变换缩微打印隐藏的图像,也可能会被彩色复印机、扫描仪或打印机识别并使其停止的专有扩频信号。最著名的是南十字星形的黄色星星图案,它嵌入了许多禁令结的设计中,并阻止兼容的扫描仪和打印机对其进行处理;

- 独特的库存,例如 Sandia 提出的在制造过程中随机散布光纤的纸,这样每张纸都有一个特征图案,可以使用条形码在文档上进行数字签名和打印 [1746]。

100美元钞票的设计见[1367];关于假钞的研究,分析哪些特征提供了哪些证据,请参见 [1936]。

一般来说,纸币的真伪不能轻易地通过检查单个安全特征来确认。许多较旧的技术和一些较新的技术都可以通过初步检查的方式进行模仿。凹版印刷和凸版印刷的触觉效果会磨损 ,因此弄皱和弄脏伪造的钞票是标准做法,熟练的钞票伪造者会用淡淡的灰色印刷来模仿水印(尽管水印对业余爱好者来说仍然出奇地有效)。全息图和运动图可能容易受到使用电化学技术制作机械副本的人的攻击,否则恶棍可能会从头开始制作他们自己的原版副本。

当 1988 年英国银行卡上引入莎士比亚的全息图时,我作为一家银行的代表参观了工厂,并自豪地被告知,由于该行业需要第二个供应来源,他们提供了一套备用印版一家大型安全印刷公司 而他们的这个竞争对手完全无法制造出可接受的箔纸。 (莎士比亚箔片是第一个商业上使用的全彩色衍射全息图,并且会随着视角的变化而移动)。一个无法伪造的设备,即使是一家拥有真正印版的大型防伪印刷公司,也不能伪造,必须提供全面保护吗?但是当我七年后访问新加坡时,我在跳蚤市场买了一张类似(但更大)的莎士比亚全息图。这显然是制造商的吹嘘,如果他愿意,他可以伪造英国银行卡。到那时,一位警务专家估计,中国有超过 100 名伪造者能够制造出可以接受的伪造品[1440]。

当聚合物钞票引入英国时,2016 年 5 英镑钞票和 2017 年 10 英镑钞票,我们被告知它们是不可伪造的。但到 2018 年,我们被告知如何识别伪造品。一名受害者报告说,“我仔细观察,发现大笨钟不见了,序列号的一部分和女王的脸都消失了 。当我将它与我已经拥有的真钞进行比较时,我还看到银条是绿色的 [1611]。那年晚些时候,有进取心的恶棍开始使用 塑料 20 英镑纸币,尽管正式的 20 英镑纸币要到 2020 年才会发行。

因此技术在不断发展,依赖单一的保护技术是不明智的。即使一种防御被完全击败(例如,如果金属箔的机械复制变得容易),您至少有一个完全不同的技巧可以依靠(例如光学可变墨水)。

但设计一份安全文件比这要难得多。保护、美观和稳健性之间存在复杂的权衡,业务重点也可能发生变化。多年来,钞票设计者的目标是防止伪造品通过二级或三级检查,而不是更常见的初级检查。很多时间都花在了培训人们正确检查文件的困难上,而没有足够的注意去研究像 ban knote 这样的产品的典型用户实际上是如何下意识地决定它是否可以接受的。换句话说,技术重点取代了业务重点。

迄今为止吸取的教训是[1935]:

- 安全特征应传达与产品相关的信息。因此,最好用彩虹色墨水来印刷钞票的面额,而不是一些没人看的模糊特征;
- 安全特征显然应该属于它们所在的位置,因此它们嵌入到用户对对象的认知模型中;
- 它们的效果应该是明显的、明确的和可理解的;
- 他们不应该有可以提供基础的现有竞争对手
  模仿;
- 它们应该标准化。

这项工作值得更广泛的关注,因为钞票社区是我们行业中为数不多的对安全可用性投入了大量思考的子学科之一。 (我们一遍又一遍地看到,安全产品的主要缺点之一是可用性被忽视了。)当涉及到护照等纸币以外的文件时,还存在与该国政治环境有关的问题以及将使用它们的社会的习俗 [1293]。

可用性在二线检查期间也很重要,但这里的问题更加微妙,并且集中在检查员必须遵循的过程中,以区分真品和假货。

对于纸币,理论是您设计的纸币可能具有 20 个不向公众宣传的特征。银行职员等二级检查员了解许多功能。在适当的时候,这些将被伪造者所知。随着时间的推移,越来越多的功能被揭示出来。

最终,当它们全部曝光时,纸币将停止流通并被替换。如果重点从手动验证切换到自动验证,则此过程可能会变得更加困难。窃取自动售货机、将其拆解并读取软件的小偷,可以获得对当前使用的支票的完整准确描述。曾经花几周或几个月这样做,他会发现第二次要容易得多。因此,当中央银行告诉制造商二级数字水印(或其他)的秘密多项式,并且得到部署时,他可以窃取另一台机器并在几天内获得新数据。因此,与手动系统相比,故障可能更加突然和彻底,功能生命、死亡和重生的循环可能比过去更快。当然,另一种可能性是开发

一些国家完全转向卡支付,这是瑞典和芬兰等富有的早期采用者的路径。

对于产品包装,典型的商业模式是发现伪造样品并将其带到实验室,科学家在那里找到它们不同的地方
也许全息图不太正确。然后为现场检查员制作工具包,以便外出追踪来源。如果这些套件体积庞大且价格昂贵,则可以部署的数量就会减少。如果有来自不同公司的许多不同不同的伪造检测设备,那么就很难说服海关人员使用它们中的任何一个。在塑料产品收缩包装上打印单个显微紫外线条形码等想法经常失败,原因是进行验证所需的显微镜、笔记本电脑和在线连接的成本。与纸币一样,您可以获得具有多种功能的更强大的系统,但这进一步推高了读取设备的成本和体积。

对于金融工具,尤其是支票,改动比从头开始复制或伪造要大得多。在众多骗局中,不法分子通过预付定金或现金预订然后取消订单等伎俩,从商家那里获得了真实的支票。受害人按时寄出一张支票,该支票被改成更大的金额,通常使用现成的家用溶剂。标准对策是使用会在溶剂存在下变色和流动的墨水进行背景打印。但保护并不完整,因为去除激光打印机碳粉的技巧(甚至是打字机校正色带等简单的东西)。一个有进取心的恶棍甚至向他的受害者赠送了经过特别挑选的墨水容易去除的钢笔 [8]。

过去,支票欺诈的价值是信用卡欺诈的数倍,而且由于每天处理的支票数量巨大,因此也很难处理。

这使得除非数量非常大,否则无法进行审查。在远东,人们使用个人印章或签字印章来签署支票,低成本的自动验证是可能的 [929]。然而,对于手写签名,具有可接受的错误率的自动验证仍然超出了现有技术水平(我将在 17.2 节中讨论)。企业的未来是将付款转移到银行转帐;德国是这里的早期采用者,到 2000 年代初基本上抑制了支票欺诈。 SEPA 支付现在使电子支付比欧元区的支票支付更快、更便宜。

当然,文件变更不仅仅是银行业的问题。大多数伪造的旅行证件是经过改动而不是从头开始伪造的。名称被更改,照片被替换,或者页面被添加和删除。出于这个原因,发达国家已在很大程度上转向基于芯片的护照;来自没有电子护照的国家的游客可能必须获得包含芯片或指向存储旅行者生物特征的在线数据库的签证。

16.4 包装和密封

供应链安全涉及包装和密封问题。根据洛斯阿拉莫斯漏洞评估小组的定义,印章是“一种篡改指示装置,旨在留下不可擦除的、明确的未经授权进入或篡改的证据”。

大多数密封件的工作原理是在基材上应用某种安全印刷以获得标签,然后将此标签固定到要保护的材料上。应用范围从药品到货物集装箱再到投票箱。

其他产品遵循相同的总体理念,但使用不同的材料;在底部,我们发现塑料带很容易收紧,但如果不切割就很难松开,而在顶部,有光纤环绕着受保护的物体,并通过附加的激光标签主动监测是否拉伸。

16.4.1 基板属性

一些系统向基板材料添加随机可变性。我们提到了用光纤装纸的技巧;还有水印磁学,其中随机的高矫顽信号被嵌入到卡片条中,随后可以使用标准的低矫顽设备读取和写入卡片,而不会干扰独特的随机模式。这些被用于瑞典的银行卡、韩国的电话卡以及我大学某些建筑物的门禁卡。

冷战期间的军备控制也使用了类似的想法。许多武器和材料都有独特的表面;参见例如图 16.1 的纸张表面。其他材料表面可以做的独一无二;例如,可以使用小型炸药在坦克枪管上腐蚀一个补丁。

使用激光散斑技术测量图案,并将其记录在日志中或作为机器可读数字签名附加到设备上 [1749]。

这使得识别重型火炮等资本设备变得容易,其中识别每个枪管足以防止任何一方作弊。您甚至可以使用激光散斑来验证一张纸,将其表面粗糙度编码成一种代码,该代码对折痕、干燥、涂鸦甚至烧焦具有鲁棒性 [332]。那里的问题是找到一个应用程序,您可以在该应用程序中证明在流程的每一端使用昂贵的扫描仪是合理的。

16.4.2 胶水问题

虽然标签的独特性可能是其制造的副作用,但大多数封条仍然通过将安全印刷标签固定在目标物体上来发挥作用。这就提出了一个问题,即美丽的彩虹色印刷艺术品如何以一种很难去除的方式附着在粗糙的物体上。

在防篡改包装的特殊情况下,附件是工业过程的一部分;它可以是带有弹出按钮或可打开 盖子的加压容器。通常的答案是使用比密封基材本身更结实的胶水,这样密封会撕裂或至少在以下情况下明显变形

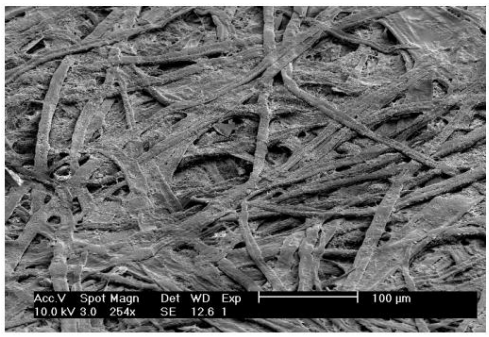

图 16.1：- 纸的扫描电子显微照片（由 Ingenia Tech nology Ltd 提供）

拉开。饮料瓶盖下的铝箔密封和药丸的泡罩包装就是这种情况。

然而,在大多数产品中,实现都相当糟糕。许多密封件很容易仅使用手动工具和一点耐心直接移除。

拿一把锋利的刀,用自密封信封中接下来的几封信进行试验。许多这样的信封应该撕开,而不是剥开;为此,翻盖上可能切有几个垂直槽。但这种希望得到的篡改证据通常假设人们会通过将信封口盖从身体上拉回来来打开它们。通过稍微抬起信封盖并前后移动刀子,通常可以在不损坏信封盖的情况下切断胶水,从而打开信封而不会留下可疑痕迹。

（有些胶水应该先用吹风机软化,或者冷冻后变得更脆弱。）或者打开另一端的信封,那里的胶水没有设计成轻度防篡改。无论哪种方式,您都可能会得到一个在仔细检查时看起来有点皱巴巴的信封。如果很明显,请熨平褶皱。这种攻击通常对初级检查有效,可能无法通过三次检查,并且很可能会通过二次检查:无论如何都会在帖子中发生皱折。

市场上的许多海豹都可以使用类似的简单技巧来打败。一个臭名昭著的例子是在瑞士和奥地利使用的小插图或高速公路收费贴纸。在那里,你必须支付道路通行费,为此你会在挡风玻璃上贴上一张贴纸,证明你已经支付了一年的会费,如果你租车的话,则支付时间更短。如果您撕下挡风玻璃上的标签以在另一辆车上使用,一些墨水会随附在挡风玻璃上,而另一些则会粘在挡风玻璃上。因此,人们通过在仪表板上来回刷动贴纸,在粘贴之前弄脏胶水。现在这已成为犯罪行为,如果被抓到会被罚款 [1468]。

16.4.3 PIN 邮件

许多银行现在在特殊印刷材料上印刷客户 PIN。过去,PIN 邮递员使用多部分文具和冲击式打印机;您通过撕开信封并抽出一张上面有 PIN 码的纸条获得了 PIN 码

印象深刻。从冲击技术到激光技术的转变导致许多公司发明了信纸,您可以从中拉出一个标签来读取 PIN。这个想法是,就像印章不能在不留下可见证据的情况下移动一样,使用这种文具,如果不留下可见证据,就无法提取秘密。一种典型的机制是在印有模糊图案的纸上贴上一块贴片,上面还有一层粘合膜,上面印有 PIN。薄膜后面是纸上的一个模切标签,可以用模糊的背景将其拉开,使 PIN 可见。

我的学生 Mike Bond、Steven Murdoch 和 Jolyon Clulow 在寻找这些产品的连续版本的漏洞时获得了一些乐趣。早期的产品可以通过将它们举到光线下来阅读,因此光线以大约 10 度的角度掠过表面;不透明的墨粉在闪亮的胶膜上清晰可见。下一次攻击是将印刷品扫描到 Photoshop 中,并从底层印刷品的灰色中过滤掉碳粉的浓黑色。另一个是热转印;将一张白纸放在邮寄袋上,然后用熨斗熨烫。还有一个是使用吸墨纸和有机溶剂进行化学转移。这项工作于 2004 年向银行业报告,最终于 2005 年发表 [284]。银行现在已经发布了邮寄者的测试标准。然而直到今天,我们仍在不断收到 PIN 码易于阅读的邮件。

这是一个不起作用但仍然存在的系统示例。如果骗子知道我要办一张新银行卡,并且可以从我的邮件中窃取,他就会同时拿走银行卡和 PIN。很难想象“防篡改”PIN 邮件程序可以防止任何真正的攻击。它有时可能会阻止家庭成员意外获悉 PIN;同样,可能偶尔会有客户在没有撕开标签的情况下读取了 PIN,提取了很多钱,然后声称他没有这样做,在这种情况下,银行可能只会说“所以起诉我们”并否认自己的邮寄者。但与花在所有这些精美文具上的金额相比,这些威胁是微不足道的。这种行为的驱动因素可能是合规性;重新思考冲击式打印机时代发展起来的卡片计划规则、审计程序和保险检查太麻烦了。

16.5 系统漏洞

我们现在从针对特定打印技巧和胶水的特定威胁转向系统级威胁,其中有很多。

在我们当地的游泳池,拥挤是通过在繁忙时段向游泳者发放腕带来控制的。每 20 分钟左右就会发出不同的颜色,并且不时地要求所有持有某种颜色手环的人离开。表带由蜡纸制成。在一端,它的一侧有印刷图案和序列号,另一侧有胶水;纸张被横切,如果您不小心将其撕下 o ,它就会被完全毁坏;参见图 16.2。 （这类似于某些机场使用的行李封条。）

最简单的攻击是通过供应商的网站,每盒 100 个腕带的价格约为 8 美元。如果你不想花钱,你可以使用每个乐队

图 16.2：– 来自我们当地游泳池的腕带印章

一次,然后从不同的方向交替拉动它,轻轻地松动它 ,得到照片中显示的结果。印刷品被弄皱了,但完好无损;池畔服务员看不到损坏,实际上可能是由于粗心使用造成的。关键是,小心地修理两次对密封件造成的损坏很难与天真的用户修理一次造成的影响区分开 。一种更强大的攻击方法是根本不从密封件上取下背衬胶带,而是使用安全别针或您自己的胶水将其固定。

尽管如此,腕带密封件非常适合用途。几乎没有作弊的动机:一口气游完两个小时的奥林匹克候选者会在游泳池不拥挤的时候使用。他们还买了一张季票,这样他们就可以随时出去买一条新的腕带。但它说明了许多可能出错的事情。客户是敌人;盖章的是客户;密封重复使用的影响与随机失效的影响没有区别;未使用的印章可以在市场上购买;还可以以低廉的成本制造假印章； 有效检查不可行。

（然而,与许多用于高价值工业应用的密封产品相比,这种游泳池密封件仍然更难破解。）

16.5.1 威胁模型的特点

在军事系统中,对手是不忠的士兵,或者是对方试图破坏你装备的特种部队。在核监测系统中,可能是东道国政府试图从获得许可的平民那里转移裂变材料

反应堆。对于投票机,大多数攻击来自选举官员。

一些最困难的密封任务出现在敌人将应用密封的地方。一个典型的业务应用是公司将其某些产品的制造分包出去,并且担心承包商生产的货物数量会超过约定的数量。生产过剩是全球假冒商品价值的主要来源;肇事者可以获得经授权的制造过程和原材料,灰色市场提供了自然的分销渠道。即使发现此类欺诈行为 更不用说向法庭证明它们了 也可能很困难。

化妆品等高价值商品的典型解决方案可能涉及从多家不同公司采购包装材料,这些公司的身份对运营总装厂的公司保密。其中一些材料可能以各种方式嵌入序列号(例如通过激光雕刻在瓶玻璃上,或使用仅在紫外线下可见的墨水在玻璃纸上印刷)。可能有一种在线服务,制造商的现场代理可以借此验证在商店随机购买的样品的序列号,或者包装上可能有一个数字签名,将所有不同的序列号链接在一起以供离线检查。

密封件可以单独实现的目标是有限的。有时品牌所有者本人就是坏人,例如葡萄园将一千箱实际上是由外购混合葡萄制成的葡萄酒错误地标记为年份。

因此,每瓶南非葡萄酒都带有政府监管的印章和唯一的序列号;在这里,印章并不能证明欺诈,但会使不诚实的酒商更难逃避检查和审计等其他控制措施。

密封机制的设计通常必须考虑互补的控制过程。

检查可能比人们想象的要难。在灰色市场购买假冒商品的分销商认为它们是真品,可能会在没有任何犯罪意图的情况下开始欺骗检查员。在存在灰色市场问题的地方,从“Fred”处购买的产品将迅速推给客户,确保检查员只能在他的库房中看到授权产品。此外,分销商可能完全一无所知;兜售假货的可能是他的员工。一个众所周知的骗局是航空公司工作人员在访问市场不受监管的国家时购买假冒香水、手表等,然后在飞行中向客户出售 [1142]。航空公司仓库(以及飞机降落后的免税车)中的库存将全部为正品。因此,让代理商出去购买样品通常是必不可少的,并且密封机制必须支持这一点。

16.5.2 防炮击措施

封印是否贴合被封物,也取决于基层人员的诚信与勤奋程度 。我在第 14.3.2.2 节中提到,在卡车限速器系统中,变速箱传感器是如何使用一根电线固定的,校准车库用一个用特殊钳子压接到位的铅盘密封。败笔是贿赂修车厂的技工,以错误的方式缠绕电线,这样当传感器从变速箱上拧下时,电线

会松动,而不是收紧和破坏密封。这比参加业余雕刻家课程更简单,这样您就可以制作印章模型并用青铜锻造一对密封钳。

盖印章的人可能粗心大意,也可能腐败。一些机场在使用值机队列附近的机器对托运行李进行 X 光检查后,会对托运行李进行胶带密封。在大约一半的情况下,对我的行李进行了这种处理,胶带固定得不好;要么它没有穿过手提箱和盖子之间的紧固件,要么它的一端脱落,要么箱子有几个大到足以容纳炸弹的隔间,但只有一个紧固件是密封的。但无论如何,机场安检主要是剧院。

许多关于密封件的有趣研究都集中在可用性上。一个大问题是检查应该检查密封件的工作人员是否真的这样做了。 Gundecking 是一个海军术语,指的是那些假装履行职责但实际上倒在炮甲板上冒烟的人。因此,如果您的任务是检查抵达港口的数千个集装箱上的封条,您如何确保您的员工 真正检查每一个?

一种方法是在每个容器密封中包含一个带有加密密钥流生成器的小型处理器,该生成器每分钟左右生成一个新数字。那么检查员的任务就是巡视所有进港集装箱,并记录它们显示的编号。如果检测到篡改事件,设备将擦除其密钥,并且不能生成更多数字。如果您的检查员没有从其中一个容器中带回有效的密封代码,您就知道有问题了,无论是它还是他。这种封条也被称为“反证据”封条:其想法是存储设备未被篡改的信息,并在发生篡改时将其销毁,不让对手伪造任何东西。

粗心和腐败相互作用。如果足够多的员工在申请或验证印章时粗心大意,那么如果我贿赂他们中的一个,由此产生的缺陷本身并不能证明不诚实。

16.5.3 随机失效的影响

当密封件因完全无辜的原因而破裂时,也会产生类似的效果。
例如,当对卡车发动机进行蒸汽清洁时,限速器密封件经常会破裂,因此如果交通警察能找到的所有证据都是密封件破裂,司机就不会因篡改而被起诉。 (卡车司机知道这一点。)

打开密封得过于严密的信封后,间谍可以用写着“海关打开”或“在运输途中爆裂由邮政局封存”的贴纸再次合上。他甚至可以用胶带把它封起来,然后在正面潦草地写上“投递到错误的地址再试一次”。

必须仔细考虑此类失败和攻击的后果。如果保护目标是防止产品的大规模伪造,那么偶尔的破损可能无关紧要;但如果是为了支持起诉,自发的密封失效可能是一个严重的问题。在极端情况下,过分相信密封件的坚固性可能会导致误判并破坏密封产品的证据(以及商业)价值。

我的例子来自我详细描述的宵禁标签

在第 14.4 节中。在那里,标签供应商对其产品的防篡改功能做出了宏大的营销声明,但在法庭上受到质疑时拒绝提供样品供辩方测试。当他们的控制令不再合理时,恐怖主义嫌疑人被释放,最终标签公司因犯罪不当行为失去了合同:他们向司法部收取了为死者或入狱人员贴标签的费用,并最终支付了数百万英镑罚款,他们的审计员也是如此 [193]。

16.5.4 材料控制

另一个常见的漏洞是密封材料的供应不受控制。公司印章就是一个很好的例子。在英国,这些通常由两个金属压花板组成,它们被插入特殊的钳子中,用于压接重要文件。几家供应商生产这些印版,一位订购了数百张印版的律师告诉我,从未进行过检查。

虽然为“Microsoft Corporation”订购印章可能会有一点风险,但为几乎任何鲜为人知的目标制作印章应该很容易:您所要做的就是写一封看起来像是来自法律的信件公司。盖章的真正目的不是为了防止伪造,而是让律师事务所能够对必须盖章的文件收取额外费用。

一个更严重的例子是制药业对泡罩包装的依赖,有时辅以全息图和变色油墨。

所有这些技术都可以免费提供给任何愿意购买它们的人,而且它们也不是特别昂贵。或者想想一些快递公司使用的塑料信封,它们设计为在打开时会拉伸和撕裂。只要你能走在街上,在车站拿起原始信封,它们就不可能阻止任何花时间和思想计划袭击的人;他可以在包裹通过快递网络之前或之后更换包装。

这也是一个“城市神话”,如果信封口盖用用拇指指甲擦过的胶带加固,警察和安全部门就无法无痕地打开信封(我最近从一家银行收到了一些文件,这些文件已经被以这种方式密封)。这并不完全可信 即使没有警察实验室发明出一种神奇的溶剂,但 19 世纪的沙皇警察已经使用叉形棍子将信件卷在密封的信封中,以便可以将其拉出、阅读,然后放入返回[1001];那里乃至整个欧洲的写信人都使用字母锁定 复杂的折叠、切口和印章系统,他们希望这样可以使篡改变得明显 [366]。

即使保证透明胶带会在信封上留下明显的标记,人们也不得不假设警方的信封蒸煮部门没有类似信封的库存,并且收件人会足够敏锐地发现伪造的信封。鉴于可以轻松扫描带有公司徽标的信封,然后使用便宜的彩色打印机进行复制,这些假设相当雄心勃勃。不管怎样,桌面彩色打印机的到来已经让很多组织停止使用预打印文具。

这使伪造者的工作变得容易得多。

16.5.5 不保护正确的东西

如果价值代币以两种不同的方式对价值进行编码,您可能会期望犯罪分子利用任何差异,或者实际上是创造差异。在 1980 年代后期,随着银行引入读取磁条的授权终端,信用卡变得容易伪造,而大多数商家用来打印凭证供客户签名的压印机使用压印,大多数商家将签名的凭证存入银行就好像它们是支票一样。改变磁条而不是压印的骗子击败了这个系统。也有涉及部分改变的攻击。例如,信用卡曾经有全息图,但由于它们只覆盖最后四位数字,攻击者可以随时更改其他十二位数字。当银行用于生成信用卡号的算法为人所知时,这只涉及压平、重印和重新压印卡的其余部分,这可以通过廉价设备完成。

此类攻击现已过时,因为不再使用旧的 Addressograph 草稿捕获机。无论如何,所有全息图都说“这曾经是一张有效的卡”,大多数银行现在已经停止使用它。

最后,食品和药品生产商经常使用收缩包装或泡罩包装,如果设计得当,业余爱好者很难将其伪造得足够好以经得起仔细检查。然而,在选择保护措施时,你必须非常清楚威胁模型 是伪造、篡改、复制、模拟、转移、稀释、替代还是其他什么? [1524] 如果威胁模型是带有装满毒药的注射器的精神病患者,那么简单的泡罩包装或收缩包装是不够的。真正需要的是一种篡改传感膜,即使是微小的穿透,它也会做出明显且不可逆转的反应。 (这种膜存在,但对于消费品来说仍然太贵了。我将在防篡改章节中讨论它们。)

16.5.6 检查的成本和性质

业内有很多关于坏人用其他东西替换银行卡上的全息图的故事 比如兔子而不是鸽子 店主的反应只是说:“哦,看,他们改变了全息图!”这不是对全息图的批评,而是应用心理学和公共教育的更深层次的问题。当新纸币面世时,银行家们很担心 每个人都熟悉新纸币的那几周可能是伪造者的大好时机。

一个相关的问题是护照、驾照、信头、公司印章和包装的种类繁多。没有真品样品对比,检验或多或少局限在初级水平,容易造假。尽管银行职员有印有外国钞票图片的书籍,移民官员也有类似的外国护照图片,但通常只有粗略的安全特征信息。骗子经常通过腐败手段获得真正的护照和身份证(而不仅仅是来自欠发达国家。)哦,没有真正的实物样本意味着无法正确检查触觉方面。

2006 年 3 月在圣巴巴拉举行的第 7 届安全密封研讨会上,索尼娅·特鲁希略 (Sonia Trujillo) 进行了一个有点令人震惊的实验。她篡改了

三十种不同的食品和药品中的九种,仅使用低技术攻击,并邀请了 71 位篡改检测专家来区分它们。每个受试者都被要求从他们认为已被篡改的 10 件产品中准确挑选出 3 件。专家们的表现并不比随机的好,尽管他们中的大多数人花费的时间比他们被引导到每个产品的 4 秒要长得多。如果连专家都无法检测到篡改,即使他们被告知篡改已经发生,那么普通消费者有什么机会呢?

因此,公众或工作人员只需最少的培训就可以检查印章,而且无需访问在线数据库,这仍然是一种理想,而不是现实。防篡改包装的主要目的是让客户放心;次要目的包括最大限度地减少产品退货、尽职调查和减少陪审团裁决的规模。阻止无能的篡改者可能就在某个地方。

严肃对待伪造问题的公司,如奢侈品制造商,已经采用了印钞机开创的许多技术。但高价值的产品包装比纸币更难保护。熟悉度很重要:人们对他们经常接触的东西有一种“感觉”,比如当地的钱,但不太可能注意到他们很少看到的包裹有什么问题 比如高档化妆品或一瓶昂贵的葡萄酒。出于这个原因,保护包含电子产品的大部分工作已转移到在线注册机制。一些产品为此目的获得了电子设备,而其他已经拥有电子设备的产品正在获得 wifi 芯片。

一种可能性是招募公众作为检查员,检查的不是包装,而是唯一的序列号。供应商可以将这些号码打印在产品标签上,而不是将这些号码隐藏在 RFID 芯片中,而那些担心他们是否买到正品的人可以打电话来核实。这通常可以使激励措施更好地协调一致,但可能比看起来更难。例如,当 Microsoft 首次发布其反间谍软件测试版时,我将其安装在家庭 PC 上 其 Windows 副本立即被谴责为邪恶。现在 PC 是在正规商店购买的,我根本不需要解释这个的麻烦。我特别不喜欢他们最初的谈判立场,即我应该给他们更多的钱。最终他们给了我们另一个 Windows 副本。但在那之后我们没有购买另一台 Windows 机器。

16.6 评估方法

该讨论提出了一种系统的方法来评估特定应用的密封产品。而不是只是问,“你能用明显的方法以外的其他方法去除密封吗?”从设计和现场测试到制造、应用、使用、检查、销毁和最终退役,我们都需要遵循它。以下是一些应该问的问题:

- 如果印章是伪造的,谁应该发现它?如果是公众,那么他们多久会看到真正的印章?供应商是否进行了适当的实验以确定可能的错误接受率和错误拒绝率?如果是您在现场的检查员,他们的设备和培训费用是多少?

这些检查员（公共或专业)发现和报告缺陷的积极性如何?

- 有没有真正知道自己在做什么的人努打败这个系统?什么是失败 篡改、伪造、篡改、证据价值的侵蚀或对您的商业信誉的“公关”攻击?
- 设计团队的声誉如何 他们是否有成功击败对手产品的历史?
- 在战场上待了多长时间,取得进步使失败变得容易得多的可能性有多大?
- 还有谁可以购买、伪造或窃取密封材料?
- 盖印章的人是否粗心或腐败,如果是,
  你将如何应对?
- 密封件会保护产品的正确部分（或足够部分)吗?
- 什么是质量问题?污垢、油污、噪音、振动、清洁和制造缺陷的影响如何?该产品是否必须经受住户外天气、汽油飞溅、贴身携带或掉入一杯啤酒中?或者如果发生这样的事情,它应该做出明显的反应吗?随机密封失效的频率是多少?它们会产生什么影响?
- 如果您最终要上法庭,除您自己（或供应商)之外,对方是否可以依赖其他专家?如果答案是否定的,那么这是好事还是坏事?为什么陪审团要相信你,系统的发明者,而不是被告席上可爱的小老太太?法官会以公平审判为由放过她吗 因为反驳你的技术主张对她来说是不可能解除的举证责任?如果您将公司卖给某人,而某人又将公司卖给骗子,会发生什么情况?
- 一旦产品被使用,密封件将如何处理 您是否
  如果有人从垃圾中回收一些旧印章会感到困扰吗?

请记住,击败海豹是在愚弄人,而不是击败硬件。
因此,请认真考虑应用和检查印章的人员是否会忠实有效地执行任务;分析动机、机会、技能、审计和问责制。当封印被敌人（如合同制造的情况)或被公开腐败的人（如急于赢得卡车公司业务的车库)使用时,要特别小心。最后,不仅要从客户公司及其对手的角度,还要从无辜的系统用户和法律证据的角度考虑密封失败和检查错误率可能带来的后果。

这个全生命周期保证过程只是您需要应用于一般系统的保证过程的一个缩影。我将在第三部分中更详细地讨论这一点。

16.7 总结

大多数市售密封产品相对容易失效,当密封检查由未经培训、无动机或两者兼而有之的人随意进行时尤其如此（这种情况经常发生）。密封必须在密封件的整个生命周期内进行评估,从制造到材料控制、应用、验证和最终销毁;在关键应用程序中强烈建议进行恶意测试。印章通常取决于防伪印刷,对此可能会有大致相似的评论。

研究问题

这是一个很多想法来来去去却没有产生太大影响的领域。毫无疑问,从纳米粒子到铁磁流体再到 DNA,许多用于产品安全和假冒检测的奇特新技术都会受到吹捧;但只要市场失灵,人们忽视系统层面的问题,他们又有什么用呢?它们中的任何一个是否具有使我们能够解决初级可检查性难题的新颖特性?

自动检查系统可能是一种前进的方式。一个例子是冷链保证。疫苗等一些产品需要保持在40 摄氏度以下,并且已经在集装箱或货盘中装有记录仪,用于监测温度并识别故障。如果超过阈值,也有根据化学反应显示不同条形码的告示纸条。拥有安全关键产品的受监管行业,例如制药业,可能是尝试新想法的好地方。

一个更难的问题是如何帮助消费者在监管较少的行业中。假货和毒药大多是在零售层面引入的,而这些零售层面过去是高度分散的。但技术正在解决这个问题,也许解决方案不在于包装,而在于针对亚马逊等大型零售商采取的监管行动。据报道,它的市场和履行服务正成为许多假冒产品最受关注的分销渠道,以及被政府机构宣布为不安全、带有欺骗性标签或被监管机构禁止的产品,包括铅含量达到危险水平的儿童玩具[591]。这看起来像是成为政府与大型科技公司之间的一场大型监管战。也许这是不可避免的规模效应;如果每个人都在 Facebook 上,那么这包括世界上所有的变态、恶霸和极端分子,如果世界上所有的商家都使用亚马逊来运送他们的产品,那么可以预料到类似的事情。我怀疑,最终亚马逊将被迫雇佣数万名产品安全和合规检查员,就像 Facebook 被迫雇佣数万名内容审查员一样。但法律通常滞后于技术十五年左右,与此同时安全打印和密封将继续 尽管继续转向在线产品注册。

进一步阅读

关于防伪印刷的权威教科书是 van Renesse [1935],它不仅涉及全息图和运动图等技术技巧,还涉及它们如何在从钞票印刷到护照再到包装的各种应用中发挥作用。这是非常重要的背景阅读。

可以在许多出版物中找到有关印章的基本文字
Roger Johnston 的海豹脆弱性评估小组（例如,[989]）。

造假的历史令人着迷。从独立到南北战争,美国人使用私人银行而非政府发行的纸币,伪造行为无处不在。银行可以对付当地的伪造者,但到大约 1800 年,雕刻师、造纸商、印刷商、批发商、零售商和路人组成的网络已经出现,在佛蒙特州和加拿大边界的荒地设有避风港;美国和加拿大政府都不想承担这个问题的责任[1311]。

最近出现了 Supernote 争议。在 2000 年代后期,出现了每年价值几百万美元的伪造美元,几乎在每个方面都是完美的:它是用正确的印刷机印刷在正确的纸张上的,并且准确地跟踪了微小的变化 除了它没有使用正确的磁性和红外安全功能。美国政府指责朝鲜伪造,并以此实施制裁;其他人则认为这些票据更有可能是由中央情报局为了追踪现金流而制作的。这些纸币的数量很少,而且只在朝鲜外交官和中亚军阀等中情局感兴趣的人手中。它们经过精心设计,可以通过除货币中心银行使用的点钞机以外的所有检查,这将阻止它们大规模流通;并且出现的数量至少比伪造者生产的数量少一个数量级,并且需要生产以支付设备费用[622]。