第24章

版权和 DRM

很高兴你的 PC 是不安全的 这意味着在你购买它之后,你可以闯入它并安装任何你想要的软件。

你想要什么,而不是索尼、华纳或美国在线想要什么。

– 约翰·吉尔摩

24.1 简介

版权一直是数字时代备受争议的问题之一,并推动了数字版权管理 (DRM) 的发展。 1990 年代和 2000 年代,好莱坞和科技行业之间发生了一场大战;到2010年基本解决了。我们赢了;音乐和电影行业的权力从 EMI 和 Universal 等公司转移到 Apple、Spotify、Amazon 和 Netflix 等公司,而 Amazon 垄断了图书市场 首先是实体书,然后是电子书。从技术上讲,世界从享受 CD 和 DVD(许多人过去共享)和卫星广播电视(有些人过去破解)等本地媒体的音乐和视频,转向了订阅管理相当简单的宽带流媒体服务。我认真考虑过将这一章从第三版中删除,而只是让您在线参考第二版的章节,因为在技术上没有太多可说的。经过深思熟虑,我决定对其进行编辑,以提供 2020 年以来的背景。正如我在第 9 章中描述的多级安全系统基本上已经过时,但推动了军事计算机安全的发展,并以许多微妙的方式影响了当今的安全格局,所以也版权战争留下了自己的印记。 DRM 仍在使用:电子书、iPhone 上的 Fairplay 系统使复制歌曲更加困难,浏览器中的 HTML5 使复制 Netflix 视频更加困难。非常相似的技术被用于游戏平台,使玩家更难使用瞄准机器人,保护云平台上的用户数据,以及手机安全,其中运行时应用程序自我保护 (RASP) 用于保护银行和其他应用程序免受恶意软件侵害那根电话。我们行业为保护游戏卡带而采用的配件控制机制现在使用密码学来支持数十个业务部门的业务模型。我放弃这个的最后一个理由

这一章是版权战争成为我们共同的安全文化的一部分,即使你还太年轻不能参加,你偶尔也会发现了解我们这些白胡子在喋喋不休的事情会很有帮助。

在政治层面,自从威廉·廷代尔（剑桥大学出版社的创始人之一)因印刷英文圣经而被烧死之前,信息控制一直是政府关注的中心。从 1709 年安妮法令开始的现代版权法的建立,到 18 世纪关于新闻审查制度的斗争,再到启蒙运动和美国宪法的制定,这种敏感性一直在持续。版权和审查制度之间的联系时常被技术所掩盖,但有重现的习惯。版权机制的存在是为了防止信息落入未付费的人手中,而审查员则防止信息落入不信任的人手中。在 ISP 被迫安装过滤器以防止其客户下载受版权保护的材料的情况下,这些过滤器通常也可用于阻止煽动性材料。

在 20 世纪,文学版权、电影和音乐的所有者积累了大量财富,从而产生了强烈的控制欲。随着互联网的兴起 ,音乐和电影行业担心销量会因数字复制而流失,并游说制定甜心法律 美国 1998 年的数字千年版权法 (DMCA) 和欧洲的一系列知识产权指令 为以下机制提供特殊法律保护:执行版权。从那以后,这些法律已被用于各种其他目的,从关闭网络钓鱼网站到阻止人们重新填充打印机墨盒,甚至是修理损坏的设备。

这些法律的表面目标是从 1990 年代开始在 Windows Media Player 等产品中使用的 DRM,以及自 2017 年以来在兼容 HTML5 的浏览器中使用的 DRM,以控制音乐和视频的复制。 DRM 的基本思想是通过加密文件使文件不可复制,然后单独提供一个“许可证”,这是使用用户唯一的密钥加密的媒体文件的密钥,加上一些“权限管理语言”中的声明关于用户可以对内容做什么。呈现媒体内容的应用程序被信任遵守这些。我还将快速浏览一下历史并描述一些有趣的变体,例如卫星电视加密系统、版权标记和叛徒追踪。与 2008 年本书第二版问世时相比,DRM 现在的相关性较低,但仍有一些应用程序,我将在后面描述。

所有这一切都混杂着一些严重的政策问题。很难使 DRM 与开源软件兼容,除非您拥有可信赖的硬件（例如 enclaves 或 TPM）,或者一旦被逆向工程就立即修补的闭源沙箱。计算机行业抵制 DRM,但好莱坞和音乐行业强迫我们引入它,说没有它他们就会被毁掉。我们警告他们 DRM 会毁了他们,但他们不听。音乐不再由 Universal 和 EMI 等公司经营,而是由 Apple 和 Amazon 等公司经营 向流媒体的转变让 Spotify 等新公司加入了这一行列。但是,DRM 引入了严重的隐私问题,这些问题并没有随着流媒体而消失。它不再是 Microsoft 中的许可证管理服务器,知道你听过的每首音乐曲目,以及你看过的每一部电影,它现在是 Apple 或 Spotify 或 Netflix 的流媒体服务器。

24.2 版权

版权保护多年来一直困扰着电影、音乐和图书出版行业。空白录音带和录像带是否应该征税,其收益将分配给版权所有者,在许多国家/地区存在着长期而激烈的争论。追溯到 19 世纪,人们担心摄影术的发明会摧毁图书出版业。第十八次看到图书出版商试图关闭公共借阅图书馆,直到他们意识到他们正在创造大众识字率并推动销售;而在 16 世纪,活字印刷术的发明被当时的大多数当权者(从王子、主教到手工艺行会)视为颠覆性的。

我们稍后会回到这些历史例子。但我将从软件保护开始 因为大多数导致 DRM 的版权问题从 1980 年代开始就出现在 PC 和游戏软件市场上。

24.2.1 软件

早期计算机的软件是由硬件供应商或编写它的用户免费提供的。 IBM 甚至在 1960 年代制定了一项计划,其用户可以借此共享他们编写的程序。 (大多数商业程序过于专业化,文档太少,或者难以适应。但研究中使用的软件被广泛共享。)因此,保护软件版权不是问题。几乎所有拥有计算机的组织都规模庞大、声名显赫;他们的软件往往需要熟练的维护。还有计算机局服务 当今云计算的先驱 使用大型机计算自己工资单的大型机所有者会将其作为一项服务提供给其他公司。在那里,您购买的是服务,而不是软件。

硬件成本是主要因素。

当小型计算机在 1960 年代问世时,软件成本变得很高。
硬件供应商开始对其操作系统收取额外费用,第三方系统公司如雨后春笋般涌现。首先,他们主要卖给你一个完整的定制系统 硬件、软件和维护 所以盗版仍然不是什么大问题。到 20 世纪 70 年代中期,他们中的一些人已经将定制系统变成了软件包:最初为一家面包店编写的软件将经过参数化并出售给许多面包店。当时最常见的版权纠纷是当一个程序员离开你的公司加入竞争对手时,他们的代码突然获得了你的一些功能;那时的问题是他是否带走了代码,还是重新实现了代码。

解决此类问题的一种方法是查看软件胎记 特定实现方式的特征。例如,关于人们是否从早期 IBM 个人电脑的 ROM 中复制软件的诉讼开启了寄存器的压入和弹出顺序,因为软件是用汇编语言编写的。这与文体学领域相结合,在文体学领域,人文学者试图通过分析写作风格来确定作者身份1。更多的

1密码分析家威廉弗里德曼和他的妻子伊丽莎白受雇于一位古怪的百万富翁,以查明培根是否写过莎士比亚。他们得出的结论是,他

最近,自然语言处理社区编写了剽窃检测工具,通常通过根据文本中出现的最不常见的词对其进行索引来识别一段文本 [879];到 1990 年代,这导致出现了试图从恶意软件作者的编码风格中识别其作者的工具 [1099]。代码风格仍然是一个活跃的研究领域[370]。

随着时间的推移,人们发明了许多与软件有关的有用的东西。因此,购买了一台用于库存控制的小型计算机(或签订了办公室服务时间合同)的公司可能会想要运行统计程序并准备管理报告。与此同时,机器的安装基数变得足够大,软件共享不再只是偶尔发生。因此,一些配方公司开始设计执行机制。一个常见的方法是检查处理器序列号;另一个是定时炸弹。 1981 年,当我在一家销售零售库存控制系统的公司工作时,我们每隔几个月就会收到一条消息,内容是“故障号。 WXYZ 请致电技术支持”。 WXYZ 是许可证序列号的加密版本,如果来电者声称来自该客户,我们会给他们一个密码,以便在接下来的几个月内重新启用系统。 (如果没有,我们会派一个销售人员过来。)如果“客户”理解,这个机制很容易被击败,但实际上它运作良好:大多数时候是一个低级别的店员得到了故障信息并打电话给我们的 oce。

当 20 世纪 70 年代末和 80 年代初微型计算机的到来创造了一个大众市场,软件公司开始发布不需要技术支持即可安装和运行的产品时,软件版权侵权才真正开始成为一个问题。最初的反应各不相同。 1976 年,即微软成立一年后,比尔·盖茨 (Bill Gates) 有一封著名的公开信,他在信中抱怨说,只有不到 10% 的微型计算机用户为 BASIC 付费 [722]。

“谁在乎从事这项工作的人是否得到报酬?”他问。 “这公平吗?”
他的信总结道:“没有什么比能够雇用十名程序员并用优质软件淹没业余爱好市场更让我高兴的了。”

对公平竞争的呼吁只到此为止,接下来该行业解决了迷你机和早期微型机之间的主要区别 后者没有处理器序列号。尝试了三种通用方法:将唯一性添加到机器中,在其中创建唯一性,或者使用偶然已经存在的任何唯一性。

1. 添加硬件唯一性的标准方法是加密狗 一种连接到 PC 的设备,可以被软件询问。最简单的只有一个序列号;最常见的是执行一个简单的挑战-响应协议;而一些高端设备实际上执行了计算的一些关键部分。

2. 早期一个非常普遍的策略是让软件以一种抵制简单复制的方式自行安装在PC 的硬盘上。例如,硬盘的某个扇区将被标记为坏扇区,并且将代码或数据的关键部分写入那里。现在,如果使用标准实用程序从硬盘复制产品,则不会复制坏扇区,而且复制也不会起作用。同一主题的变体是要求

没有。 [1001]。

存在以某种方式定制的主磁盘,例如以奇怪的方式对其进行格式化,甚至用激光在其上烧孔。不过,总的来说,应该区分保护副本和保护母版;通常要求人们可以根据需要制作备份副本,但不能制作副本的副本（这称为副本生成控制）。

3. 1988 年出现了许可证服务器,基本上是一台被编程为充当公司网络上所有机器共享的加密狗的机器,它支持更复杂的商业模式,例如使公司能够购买在其上运行程序的权利一次最多 20 台机器,并使多家软件公司能够通过同一许可证许可其产品

服务器。

4. 我在 1989 年开发的一款产品对 PC 进行了指纹识别 有哪些扩展卡、多少内存、什么类型的打印机 如果配置变化太大,它会要求用户拨打求助热线。令人惊讶的是,普通 PC 中有多少个唯一标识符;以太网地址和磁盘控制器的序列号只是比较明显的。因此,您可以将软件绑定到给定的机器指纹;广告跟踪器至今仍使用类似的技术。

针对这些防御措施中的大多数的通用攻击是使用调试器检查软件并删除对复制保护例程的所有调用。许多爱好者这样做是为了运动,并竞相在软件产品发布后尽快将未受保护的版本发布到网上。

即使是拥有软件许可副本的人也经常会得到未受保护的版本,因为它们更容易备份,而且通常更可靠。你可以通过将关键代码放在不可复制的地方（例如在加密狗、许可证服务器或现在的云中)来阻止这种情况,但这场军备竞赛告诉每个人,如果你不这样做,那么有调试器的孩子总是会崩溃你的计划最终。这就是游戏机和 iPhone 等封闭平台仅运行签名代码的原因之一。

供应商还使用了心理技术。

- 许多商业程序的安装例程会将注册用户的姓名和公司嵌入到屏幕上,例如工具栏中。这不会阻止盗版者分发以假名注册的副本,但会阻止合法用户向同事随意提供副本。直到今天,当我从许多学术期刊上下载论文时,pdf 中都可以看到我所在大学的名称和序列号。

这些是版权标记的示例,我将在稍后详细讨论。

- 行业人士乐于讲述组织因未能获得未付费的关键升级而陷入困境的故事。

- 如果早期的 Microsoft 软件（Multiplan、Word 或 Chart)认为您是在调试器下运行它,它会显示消息“邪恶之树结苦果”。现在正在破坏程序磁盘。然后它会寻找软盘上的零轨道并“rrnt, rrnt, rrnt”。

在 20 世纪 80 年代后期,市场出现分裂。游戏市场转向硬件保护,最终由封闭架构的游戏机主导,其软件以专有卡带的形式出售。由于消费者对产品的标价比对其总拥有成本更敏感,因此从软件的后期销售中补贴控制台是有意义的。这导致配件控制,其中硬件保护用于控制售后市场;它被销售打印机和许多其他产品的公司采用。我们将在 24.6 节中详细讨论它。

商业软件供应商从加密狗转向高价值产品的许可服务器,例如用于设计从芯片到船舶的一切事物的 CAD 软件。技术支持对于此类产品通常至关重要,因此它们可能作为软件和服务的捆绑销售。但出于多种原因,供应商通常不再尝试使用技术手段保护大众市场产品。

- 除非您准备花钱购买加密狗硬件来执行您的一些关键代码,否则大众市场软件中的机制将被那些认为这是智力挑战的人击败,并且未受保护的代码将被匿名发布。

- 保护很麻烦。多个加密狗妨碍或相互干扰。软件保护技术妨碍了备份和恢复;它们还会导致来自不同供应商的软件不兼容,在某些情况下无法驻留在同一台机器上。 （正确执行此操作的难度是许多使用许可证管理的公司使用 Flexlm 的原因之一。）

- 许多供应商宁愿不必担心软件是授权给用户（在这种情况下他可以将其迁移到新机器)还是授权给机器（在这种情况下他可以出售二手计算机)安装软件）。由于这两种做法都很常见,因此使一种或另一种变得非常困难的机制会导致问题。可以处理这两者的机制（例如加密狗和许可证服务器)往往很昂贵。

- 计算机病毒的出现迫使企业客户对软件卫生进行投资,因此不能轻易容忍随意复制。几年之内,反病毒程序在任何情况下都让复制保护机制的日子变得更加艰难,因为非标准操作系统的使用往往会引发
  - 警报。

- 骚扰个人用户并不能赚到多少钱,因为他们通常只是随意使用产品并且会把产品扔掉而不是付钱。

- 一定程度的共享对业务有利。获得工具的盗版副本并喜欢它的人通常会购买普通副本,或说服他们的雇主购买。 1998年比尔·盖茨甚至说：“虽然中国每年售出约300万台电脑,但人们并不为软件付费。不过,总有一天他们会的。只要他们要偷,我们就希望他们偷我们的。他们会有点上瘾,然后我们会在未来十年的某个时候弄清楚如何收集”[755]。

- 竞争导致成本下降,从而降低了盗版的吸引力。以工具为例,Borland 于 1983 年推出了 Turbo Pascal,震惊了整个行业。在此之前,一个典型的语言编译器的价格约为 500 美元,而且附带的文档非常糟糕,你不得不再花 50 美元买一本书告诉你如何使用它。 Borland 的产品售价 49.95 美元,在技术上优于微软的产品,并且附带的手册与第三方产品一样好。 (所以,和许多其他人一样,一旦我听说了它,从朋友那里借了一本,试用并喜欢它,我就出去买了。)更有利可图的商业模式。

该行业随后求助于法律。软件主要受版权法保护;当您编写软件(或一本书或一首曲子)时,版权现在会自动存在,如果他人未经您的许可进行复制,您有权起诉他们要求赔偿损失。具体细节因国家/地区而异,但只有在商业规模上侵犯版权才往往构成犯罪。所以版权所有者可以向个人和小企业发送不愉快的信件,但实际上在小额索赔法庭上以几美元或几英镑或几欧元起诉他们是不经济的。但是,针对大规模用户,版权执法可能是值得的。事实上,当 IBM 在 1969 年将其硬件和软件业务分开时 在美国政府提起诉讼,声称将软件与硬件捆绑在一起巩固了他们的市场主导地位之后 他们做出了一个战略决定,不使用任何技术版权执行机制,因为他们会对顾客来说很麻烦,而且对付聪明的小偷也无济于事,所以他们会转而依赖法律 [1793]。

1988 年,微软跟随 IBM 的脚步引领行业发展,成立了贸易组织(如美国的商业软件联盟),对纵容广泛使用未授权软件的大公司进行了高调起诉。随后通过威胁信件骚扰中型企业甚至小型企业,要求他们提供公司执行版权政策的详细信息 基本上是要求他们签署批准的软件审计计划,否则就有被执法队突击搜查的风险。

业界发现,法律不仅提供了执法工具,而且还设定了限制。 1993 年,英国斯肯索普的一家软件公司主管因对系统“进行未经授权的修改”而根据英国的《计算机滥用法》被定罪。他们的客户必须定期在他的软件中输入解锁码,否则软件就会冻结,无法访问数据。

但是当他使用这种机制来强制支付有争议的发票时,法院认为他做得太过火了,他最终留下了犯罪记录 [455]。

由于 Oce 的无处不在,微软当时已经成为企业部门的负担,其大部分收入来自拥有超过 25,000 个许可证的客户。除了 Oce 之外,它还销售许多用于网络管理和其他任务的高价值产品,因此与 CAD 公司一样,它转向许可服务器。尽管这些仍然可以通过反汇编应用程序代码来解决,但随着代码变得越来越大,这变得越来越困难,并且在其中一些公司被起诉后对大公司没有吸引力。然后,当 2003 年补丁星期二到来时,在未经许可的软件上运行的想法变得疯狂。对于个人软件,重点转移到在线注册上:你可以设计你的产品

让客户与您的网站互动 无论是下载音乐、最新汇率还是安全更新。然后可以通过监控在线注册的产品序列号2来检测大规模的商业假冒行为。

我在 2008 年的本书第二版中写道：“软件即服务可能是软件（或任何其他可以在线直播的内容)的最终版权保护或 DRM:你不能购买,冻结您正在运行的版本,或者离线使用它。您还可以控制所有客户的数据,从而获得令人印象深刻的锁定”。这正是自 2010 年代初以来软件行业趋同的模式。将部分或全部功能放在云端可以带来成本和可靠性方面的真正优势,我将在第 27.5.5 节中讨论。然后通过订阅销售软件,复制保护问题就消失了。

24.2.2 自由软件,自由文化?

在过去,软件是共享的,这在学术界和其他研究科学家中仍然存在,他们发展了许多实践社区,在这些社区中,软件可以自由共享并由连续的贡献者改编。

这继续支持当时的主导平台,最初是指 IBM。例如,在 20 世纪 70 年代,英国政府推动英国学术界购买 ICL 计算机； ICL 是英国的冠军,成立于 1960 年代,当时政府将计算机行业国有化以将其从 IBM 手中“拯救”出来。然而,我们学术界想要 IBM 大型机,因为世界各地的其他学术界已经编写了可以在他们的硬件上运行的软件,即使大多数是用 FORTRAN 等高级语言编写的,移植它也是一件麻烦事。 1970 年代家用电脑的出现和 1981 年个人电脑的出现发展了越来越广泛的软件爱好者社区,他们分享我们的工作,无论是通过在朋友或俱乐部中实际传递软盘,还是通过早期的公告板系统和其他拨号网络。

1983 年,IBM 停止为其产品提供源代码,引入了“仅目标代码”的政策,其他供应商也纷纷效仿。这使得理解我们所依赖的平台和工具变得更加困难,并导致在许多方面遭到反对。两年后,麻省理工学院的工程师理查德·斯托曼 (Richard Stallman) 对无法将新的 Xerox 打印机与本地维护安排相集成感到恼火,因为 Xerox 不提供打印机驱动程序的源代码。他宣布了构建自由操作系统的 GNU 项目,并帮助创立了自由软件基金会 (FSF),该基金会推动了自由软件的理念。自由软件意味着用户应该能够出于任何目的运行它,研究它是如何工作的,改变它,并重新分发它 包括改进或修改的版本。一个口号是“自由言论,而不是免费啤酒”,但自由软件有多种形式。 FSF 提倡 GNU 通用公共许可证 (GPL),它具有以下特性:任何采用 GPL 许可软件并使其可用的人都必须提供源代码

2一旦他们完成了产品注册,微软发现在德国销售的 Oce 副本中有三分之一是假冒的,并追踪到距离我们几英里外的剑桥一家小工厂。几乎所有工厂的员工都不知道这个骗局 他们认为该公司是真正的微软供应商。他们为自己的产品感到自豪,他们的销售人员使用它来尝试从其他软件公司那里获得 CD 复制业务。

他们改编的代码在相同的许可下公开可用 病毒式传播的财产也被称为“copyleft”。 1988 年,加州大学在限制较少的 BSD 许可下发布了 Unix 的伯克利发行版,该许可只允许任何人出于任何目的使用该软件。

这样的许可安排是必要的,否则由 500 名不同的人在 20 年内编写的操作系统将包含属于他们版权的代码,因此他们中的任何人都可以上法庭行使他们的权利来阻止某些第三方使用它。专有软件供应商可以获得他们雇用的工程师编写的代码的版权3,但是志愿者维护的项目呢?开放许可有助于避免相互冲突的主张。

在整个 1990 年代,关于它们各自优点的争论很多,但这两种方法都得到了广泛使用。 Linux 于 1991 年在 GPL 下首次发布,而 Berkeley Unix 衍生出了 FreeBSD 和其他在 BSD 许可下可用的变体。正如我们在访问控制一章中提到的,Linux 是构建 Android 的平台,而 FreeBSD 则演变为 OSX 和 iOS。其他自由软件许可证是为 Apache 和其他社区开发的,公共许可证从软件迅速传播到其他创造性活动:例如,BSD 的一个变体被改编为维基百科。

软件和文化都涉及许多人的适应性和累积性贡献。传统音乐家有时会创作新曲子,但更多时候会改变现有曲子;即使是新作品也会借鉴现有词汇中的短语。 DJ 从其他人那里翻录曲目并将它们混搭成新的作品。小说家重复使用旧故事情节和人物刻板印象,而喜剧演员则重复使用旧笑话。法律并不总是能很好地处理这个问题,因为它往往是为大公司的利益而不是为社区而制定的。因此,音乐公司会迫使音乐家创作具有干净版权的全新曲调,而不是遵循传统并改编老玩家的最佳曲调。

学术界也是我们建立彼此工作成果的地方,还有一个更进一步的转折点,那就是我们从使用我们工作的人数而不是付费人数中获得认可。如果许多其他数学家在其他结果中使用他们的定理,数学家就会出名,如果很多人使用我们的软件,计算机科学家就会得到认可。这与出版商造成了真正的紧张关系。事实上,从 1970 年代开始,许多计算机科学家使用 FTP 服务器和后来发明的网页,使我们的代码和出版物都可以免费在线获取。我们倾向于忽略为发表论文而必须与学术期刊签署的版权协议 或者如果我们小心的话,我们会划掉协议中的“排他性”条款,那时候出版商从不检查的纸质形式.

1994 年发表了一些具有实际影响的出版物。 Andrew Odlyzko 计算出美国政府每年在数学上花费大约 1 亿美元

3法律因国家/地区而异。在某些国家,例如美国,您拥有雇员编写的程序的版权,而在其他国家,您必须将其作为雇佣合同中的条款;和承包商完全是另一回事。自大流行封锁以来,我的一半团队都在不同国家/地区的家中工作。签订书面协议确实是谨慎的做法。

（通过支付教授的薪水和研究生的津贴)和每年 1 亿美元的数学营销（用于期刊和会议的资金,加上数学家为期刊出版商赚取利润而投入的无偿劳动) [1459]。如果出版完全在线并且所有论文都可供所有人阅读,也许可以增加实际数学上的花费。四分之一个世纪之后的许多争论,大多数政府和慈善资助者坚持他们支付的研究是对所有人开放的（尽管期刊通过向作者收取版面费并要求大学图书馆购买订阅而幸存下来用于在线访问他们的过往目录）。

第二篇论文更为人所知,是 EFF 创始人约翰·佩里·巴洛 (John Perry Barlow) 的一篇论文,他也是感恩而死乐队 (Grateful Dead) 的词作者。他指出,由于数字技术复制的边际成本为零，“信息希望免费”（他将此归因于 Stewart Brand）。随着互联网使人们能够跨越国界交换文件,思想的物理容器（书籍、CD)和管辖权都在消失。他警告公司法律部门不要试图通过武力保护那些不再受实际效率或普遍社会同意保护的东西,并警告美国将版权合规写入贸易条约：“理想情况下,法律批准已经形成的社会共识。”他呼吁公司开发适合信息时代的商业模式。他的乐队 Grateful Dead 让人们从 1970 年代开始录制他们的歌曲,并成为最吸引人的体育场之一。他建议其他行业探索现场表演和服务的模式,而不是销售比特包 [170]。

在 20 世纪 90 年代后期的互联网繁荣时期,版权战线上出现了激烈的辩论和创新。除了关于书籍、期刊、音乐和电影的争论 我们很快就会回到这些 人们越来越意识到共享基础设施和工具的必要性。通信基础设施的许多通用组件,例如 BGP、DNS 和 SMTP,首先是在纳税人的费用下实施并发布的,而且公司经常发现他们需要向公地添加更多代码。例如,在 Netscape 于 1994 年推出第一个流行的 Web 浏览器之后,Microsoft 通过免费赠送自己的浏览器 Internet Explorer 来扼杀他们,并试图通过当时称为 Internet Information Server 的产品在服务器端建立垄断它于 1995 年推出。其他竞相在不断发展的电子商务行业建立影响力的公司对微软榨取所有价值的前景感到非常震惊,以至于他们建立了 Apache,它在次年成为领先的网络服务器。这可能是有史以来最重要的软件之一,因为这意味着微软无法在网络的早期控制链接的两端,因此他们无法将其变成他们可以从中提取的专有内容租。结果,网络保持开放多年,谷歌和 Facebook 等公司也有可能继续发展。 （我们现在可能会与他们进行政策斗争,但同时发生了很多创新。）

从政策到机制,当软件工程师 或书籍作者或音乐家 将作品置于公共领域时,我们可能会附加一系列条件。一些作者很高兴他们的作品可以被任何人使用,所以选择 BSD 风格的许可证;其他人希望他们的工作

保留在公地而不是被合并到封闭的专有产品中,所以更喜欢 GPL;学术界通常希望我们的 stu 被使用,前提是我们被认为是创造者。 2001 年,拉里·莱西格 (Larry Lessig) 创立了知识共享 (Creative Commons, CC) 来为此带来一些秩序;它提供了一组许可证,这些许可证对此进行了参数化,并使您能够指定如何使用您的作品。例如,您可以指定用户是否可以与他人分享您的工作;是否允许商业用途;他们是否必须给你适当的归属;他们是否可以改编并以此为基础,如果可以,他们是否必须在与原始版本相同的许可下分发他们的贡献。这些许可证现在在软件之外广泛使用。事实上,我的大部分学术论文都是在 CC 许可下提供的,而且我与本书出版商的协议规定,我可以在手稿发送出版 42 个月后免费在线提供所有章节。如果您为这本书付费,我将不胜感激,但我希望它可供所有人使用 即使最新版本在延迟后才上线。

1996 年美国《通信规范法》(CDA) 第 230 条出现了重大进展。这让在线服务提供商摆脱版权法的束缚,声明“交互式计算机服务的提供者或用户不得被视为其他信息内容提供商提供的任何信息的发布者或发言人” 使像谷歌和面子书成为可能,让公司律师去追逐个人文件共享者。

服务公司应该在没有通知的情况下删除侵权内容;实际上,边界很难监管,而且激励措施是不正当的(第 230 条在他们为造假者投放广告时庇护他们 [1830])。

我们稍后会在本章和第 26 章中再次讨论这个问题。

因此,对于软件和人类创造力的其他产品,存在许多可供选择的商业模式。一种是免费增值:您赠送产品的基本版本,并销售高级版本。 (即使这本书以 PDF 文件的形式在线免费提供,您也必须为印刷书籍付费。)另一种方法是免费提供您的软件,并通过销售服务、广告或充当间谍软件来赚钱并出售有关用户的数据。您可以将它们结合起来:让客户沉迷于您的免费产品,然后向他们出售更多存储空间或无广告体验。这些模型在软件领域的成功 Linux 行业靠咨询生存,谷歌靠广告生存 暗示了其他在线业务的类似方法。

在2008年本书的第二版中,我当时提出“好莱坞问题的解决之道在于商业模式的改变”。随着第三版于 2020 年 8 月付印,纽约时报正在哀叹好莱坞的死亡 [1791]。领导好莱坞的华纳电影公司的高管被解雇,但没有通常的金色降落伞;他们不再是宇宙的主人,而是成为一家电话公司视频制作部门的员工。

电影业已经从批发业务转变为以最大化订阅收入为核心技能的零售业务,批发业务通过池边握手与发行商进行交易。唯一保持知名度的工作室是迪士尼,它很早就成功过渡到订阅模式 这或许得益于史蒂夫·乔布斯成为其最大股东和主要董事会董事。

我将在第 24.5 节稍后返回版权政策,但现在让我们来看看

保护媒体内容世界的快速历史之旅。

24.2.3 书籍和音乐

1800 年,英国只有 80,000 名经常阅读的读者;直到那时,大多数书籍都是严肃的哲学或神学巨著。小说发明后,出现了一个大众图书市场,流通图书馆如雨后春笋般涌现。受过教育的阶层感到震惊,印刷商害怕图书馆会剥夺他们的销售权。但图书馆极大地激发了人们对书籍的兴趣,以至于到 1850 年,读者人数增长到 500 万人。随着人们购买他们最初从图书馆借来的书籍,书籍销量猛增。事实证明,图书馆运动是印刷商最大的盟友,并帮助为大众图书创造了一个全新的市场 [1718]。

人们复制音乐的时间比复制软件的时间长得多。帕格尼尼担心人们会抄袭他的小提琴协奏曲,所以他在排练和演出前亲自将乐谱分发给乐团,然后再收集起来。 （结果,他的许多作品都失传于后人。）

版权集体管理组织成立于 19 世纪中叶,始于巴黎;身为会员的作曲家会向场地或乐队收取表演他们作品的费用。在许多国家,这些已成为受法律支持的垄断企业;要在我们大学的音乐厅表演,你必须向表演权协会缴纳一笔税款。您可以向他们提交一个播放列表,如果您播放所有自己的作品,那么一些钱最终可能会回到您身边。许多曲子都是孤儿作品,因为作曲家的继承人不为人知,因此协会可以保留这笔钱,也可以与他们知名的作曲家分享。自由文化运动和盗版党主张限制或废除版权,以消除这种不公正现象;但是,虽然他们在一些欧洲国家赢得了一些议会席位,但在世界舞台上,他们似乎总是被版权说客打败（我将在稍后的 24.5.1 节中回到这个问题）。

当盒式录音机在 1960 年代出现时,唱片业游说（并且在一些国家得到了)对录音带征税,以分配给版权持有者。也尝试了技术措施。披头士乐队的唱片 Sergeant Pepper 包含一个 20KHz 的扰流音,理论上应该与磁带的 21KHz 偏置频率结合产生一个 1KHz 的哨子,这会破坏声音。在实践中它不起作用,因为许多唱机没有带宽来拾取扰流音。但实际上这并不重要。磁带原来不是一个大问题,因为家用设备的音质明显较差;人们主要用它们来录制音乐,以便在车里听。然后,在 1980 年代,Sony Walkman 的问世使盒式磁带成为一项大生意,虽然有一些复制,但预录盒式磁带的销售量很大,音乐行业得到了清理。

由于用于压缩音频的 MP3 格式,音频复制在 1990 年代再次成为头条新闻。以前,数字音频受其大小的保护:一张未压缩音乐的 CD 可以占用 650Mb。然而,MP3 使

人们将音轨压缩到几兆字节,而宽带使这种大小的文件可以轻松共享。到 1998 年,麻省理工学院大约 40% 的网络流量是 MP3 流量。

业界的反应是推动技术修复。这导致了版权管理行业的发展。它起源于数字出版工作以及用于保护付费电视和 DVD 的机制,所以让我们先快速了解一下。

24.2.4 视频和付费电视

录像带的早期历史是录音带历史的重演。起初好莱坞很害怕,拒绝发行电影供家庭观看。采取了粗暴的技术措施来防止复制 例如 Macrovision 系统添加了虚假的同步脉冲来混淆国内 VCR 的记录电路 这再次被证明很容易被击败。然后好莱坞对录像带出租店变得偏执,就像图书出版商对图书馆的偏执一样。再一次,图书馆变成了出版商的朋友,因为能够租借视频让人们购买录像机并激发了他们拥有自己喜欢的电影的欲望。录像机和录像带成为大众市场产品,而不是摇滚明星的玩具,到 2000 年,预录磁带的销售额占了迪士尼等公司收入的大部分。商业模式发生了变化,因此影院发行实际上只是为视频的销售做广告。

到那时,世界上许多未成年的孩子都要求他们的父母像他们的朋友一样为他们制作一套迪士尼盒带,因此录像带盗版者不得不让包装看起来很原始。这将问题简化为工业假冒问题。与在线注册开始之前的大众市场软件或今天的香水和瑞士手表一样,执法涉及派出现场代理人购买产品、寻找伪造品、追踪供应链并提起诉讼。

广播中内置了更多有趣的技术保护机制
付费电视设备。

付费电视的出现,无论是通过有线还是卫星传送,都需要有条件的访问机制,该机制允许电台运营商以各种方式限制频道的接收。如果运营商只购买了在波兰放映电影的权利,他们就必须阻止卫星覆盖范围内的德国或俄罗斯观众观看。色情频道运营商需要防止在爱尔兰等具有严格审查法的国家/地区接收色情内容。

大多数运营商还希望能够对拳击比赛等特定活动收取额外费用。

24.2.4.1 典型系统架构

早期系统的发展很大程度上取决于解码视频的硬件成本(有关机顶盒的历史,请参见 [425])。自 1970 年代以来可用的第一代系统是粗糙的模拟设备,它们使用诸如不时反转视频信号、干扰

同步,并插入尖峰以混淆电视的自动增益控制。它们很容易实施,但也很容易被击败;破解它们并不涉及密码分析,只需要示波器和持久性。

第二代系统出现在 80 年代后期,采用了模拟和数字技术的混合体:广播是模拟的,但用户控制是数字的。其中包括 Videocrypt 和 Nagravision 等系统,通常具有三个组件:

- 电视台的订阅管理服务对传出的视频进行加密,在其中嵌入各种授权管理消息 (EMM) 和授权控制消息 (ECM),并向订阅者发放智能卡等访问令牌;
- 机顶盒将有线或卫星信号转换为电视可以处理的信号。这包括对其进行解扰;
- 订户智能卡对设备进行个性化设置并控制允许机顶盒解扰的节目。它通过解释 ECM 并向机顶盒中的解扰电路提供密钥来实现这一点。

这种架构意味着复杂、昂贵的过程,如批量视频加扰,可以在具有较长产品寿命的批量生产的定制芯片中完成,而在黑客攻击后可能需要更改的密钥管理功能可以出售给客户在易于更换的低成本令牌中。如果每次系统被黑时都必须更换机顶盒本身,那么经济上的吸引力就会大打折扣4。

基本机制是机顶盒从输入数据流中解码 ECM,并将它们传递给卡。该卡对 ECM 进行解密,以获取控制消息(例如“智能卡号 123356,您的用户尚未付款,停止工作,直至另行通知”)和密钥(称为控制字),它们被传递到机顶盒。然后机顶盒使用控制字解扰视频和音频流。 [456] 中有详细的描述。

24.2.4.2 视频加扰技术

由于 20 世纪 90 年代早期可用的低成本芯片的局限性,混合系统通常通过对图像元素应用换位密码来对视频进行加扰。一个典型的方案是 Videocrypt 中使用的剪切和旋转算法。这通过在由控制字节确定的点切割它并交换左右两半来一次加扰一行视频(图 24.1):

这涉及视频信号的模数转换、缓冲器中的存储以及旋转后的数模转换 到 1990 年,这个过程几乎可以硬塞进低成本的定制 VLSI 芯片中。然而,

4现在机顶盒要几美元,而且运费占主导地位,智能卡通常只是焊接到主板上,如果出现问题,整个盒子都会被更换。

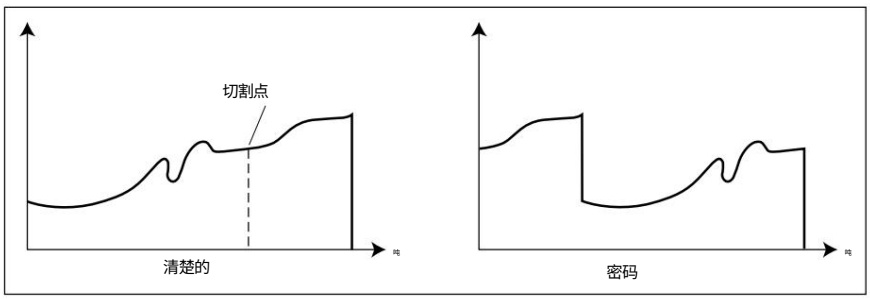

图 24.1：- 剪切和旋转置乱

这种系统的一个系统性弱点是视频是高度冗余的,因此可以使用“示波器和持久性”技术重建图像,并通过简单的信号处理来增强。这是 Markus Kuhn 于 1995 年首次完成的,需要使用大学超级计算机实时完成。图 24.2 显示了一帧加密视频,图 24.3 显示了处理后的同一帧。到 2000 年,可以在 PC 上执行此操作 [1824]。如果这种攻击在早些时候可行,它就会完全破坏系统,因为无论智能卡如何管理密钥,视频信号都可以在没有密钥的情况下被检索到。欠发达国家的一些电台仍在使用混合系统,频繁更改密钥给盗版者带来不便 他们的问题是在破解密钥时将密钥分发给他们的客户。

主要的发达国家运营商在 2000 年代初转向数字系统。这些数字系统的工作原理相同 一个带有加密硬件的机顶盒和一个用于保存个人密钥的智能卡,这些个人密钥反过来解密来自 ECM 的内容密钥。然而,加密现在通常使用块密码来保护整个数字视频流。我将在下一节中描述当前的数字视频广播系统。

混合加扰技术持续（刚好）足够长的时间。然而,他们有一些有趣的教训要教,因为他们在 1995 年之后的十年里受到了相当坚决的攻击,所以我将简要介绍一下出了什么问题。

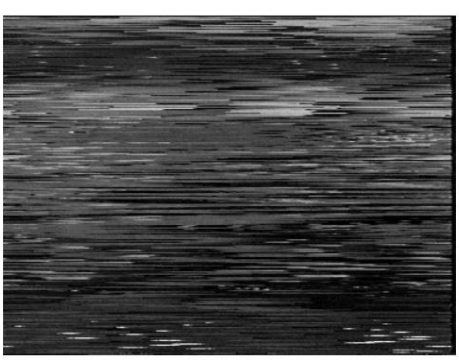

图 24.2 – 加扰后的视频帧

图 24.3 – 处理后的视频帧

24.2.4.3 对混合加扰系统的攻击

鉴于大量机顶盒可以使用控制字流来解读广播视频,下一个问题是确保只有付费客户才能获得控制字。通常,这可以通过允许和拒绝消息来完成。但可用带宽通常约为每秒 10 个 ECM。因此,向 500 万订阅者中的每一个发送一条允许消息将花费一个多星期的时间,而大多数情况下使用拒绝消息。

客户智能卡解释 ECM。如果当前节目是允许订阅者观看的节目,则使用卡中保存的主密钥并提供给机顶盒的一系列 ECM 计算出一个密钥散列 本质上是一个消息验证码 (MAC)作为控制字:

$$CW = MAC(K; ECM1,ECM2,ECM3,ECM4)$$

因此,如果订户停止支付他们的订阅,他们的卡可以通过发送一个 ECM 命令它停止发出控制字来停用;它需要访问 ECM 流才能计算控制字。如果卡片可以防篡改,只有兼容的设备才能访问主密钥 K,并且它们应该按需自杀。那么会出什么问题呢?

第一次攻击是针对协议的。由于从智能卡发送的控制字对于当前解扰节目的每个机顶盒都是相同的,一个人可以通过在智能卡和机顶盒之间放置一台 PC 来记录控制字流,并将它们发布到网上.其他人可以将加扰后的节目录像,以后再解扰[1255]。服务器如雨后春笋般涌现以应对这种键盘日志攻击,但对行业来说只是一个小麻烦;没有多少观众准备购买或构建一个特殊的适配器来将他们的 PC 连接到他们的机顶盒。拥有此类设备的爱好者发现了其他攻击,包括阻止程序,这些程序会阻止发送给您的卡的 ECM 发送给它;这样,您可以在运营商无法取消您的服务的情况下取消订阅 [1255]。

密码分析也给了一些机会。每隔半秒左右,智能卡就会为机顶盒提供一个新的控制字,并将其加载到按如下方式工作的密钥流生成器中。 Eurocrypt 系统中有两个线性反馈移位寄存器,长度分别为 31 和 29,它们会生成长线性序列。寄存器 1 的某些位用作多路复用器的地址线,多路复用器从寄存器 2 中选择一个位;该位成为密钥流序列的下一位。每个连续的输出字节都成为加扰器的一个控制字节(图 24.4)。

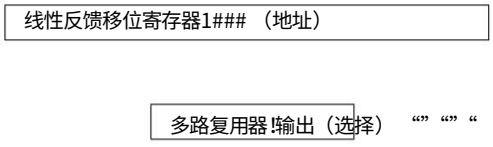

图 24.4 – 多路复用器生成器

设计者打算破解这个密码应该包括猜测密钥,因为这是 60 位长,猜测平均需要259次试验,这是不经济的 因为它必须每秒完成两次。但事实证明,密码有捷径攻击。诀窍是猜测寄存器 1 的内容,使用此地址信息将观察到的密钥流的位放入寄存器 2,如果这导致冲突,则拒绝寄存器 1 的当前猜测。(我在 1985 年发现了这种攻击,它是是什么让我对密码学产生了兴趣。)每个控制字的高阶四位左右很容易从行间相关性中推断出来 这是你真正需要努力工作的最低有效位。所以你可以使用密码分析来重建后者。但是这种计算仍然是业余爱好者而不是大众市场感兴趣的。

也许最强大的“业余”攻击利用了主密钥泄漏:某人买了一台二手 PC,出于好奇查看了硬盘,并设法取消删除了一个付费电视的完整订户管理系统操作员,包括嵌入式主密钥。这使爱好者能够编写软件来完全模拟用户智能卡事实上,它甚至可以“改进”,因此它不会在 ECM 命令时自行关闭 。

不管怎样,商业盗版者转向使用微探测技术对智能卡进行逆向工程,在 18.5 节中我描述了随后的军备竞赛。但硬件修复仅限于新卡问题,而且运营商不想每年发行超过一次新卡,因为每个用户要花费几美元,而订阅费用通常每月不到 20 美元。所以也尝试了其他防御技术。

诉讼是一种途径,但需要时间。一场针对爱尔兰海盗的诉讼败诉了,爱尔兰一度成为盗版者通过邮购方式在欧洲各地销售卡片的避风港。该行业的游说力量被用来引入欧洲法律来凌驾于都柏林之上,但这需要数年时间。到 1995 年年中,英国主要卫星电视台 (Sky-TV) 因盗版卡而损失了 5% 的收入,盗版卡主要通过都柏林的邮购方式销售。

因此,在整个 90 年代中期,海盗和运营商都在进行技术反制和反反制的战争。运营商会运送一张新卡,而在几个月内盗版者就会将其倒转并提供克隆产品进行销售。操作员会购买一些,对其进行分析,并开发使它们失效的技巧。运营商面临的问题是:当你的系统中的所有秘密都可以在几个月内被泄露时,你如何在不重新发行所有卡的情况下还能够反击盗版者?

经营者想出了各种狡猾的把戏。其中一个更有效的是 ECM,其数据包内容由智能卡作为代码执行;这样,现有的卡库可以即时升级,并且可以利用正版卡和盗版卡之间的实施差异。任何会在两个平台上给出不同答案的计算 即使只是由于无意的时序条件 可能

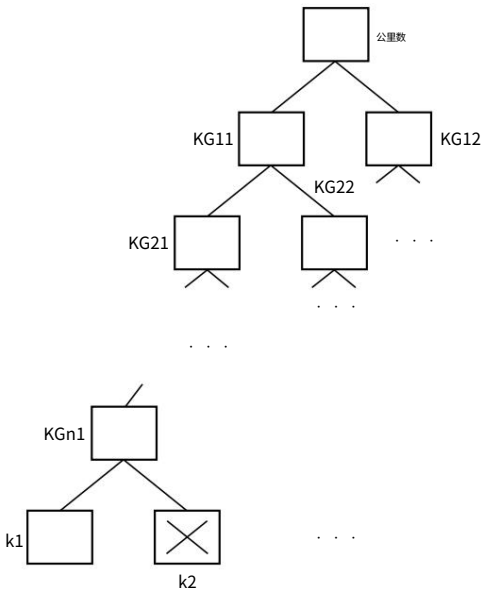

图 24.5：- 二叉吊销树

被送入 MAC 算法,使盗版卡传送无效的控制字。

其中一个系统 (Eurocrypt) 从一开始就设计了一个有效的撤销方案,值得简要了解一下。每个用户智能卡都包含一个用户密钥ki,并且有一个中间组密钥 KGij 的二叉树将用户密钥链接到当前活动的主密钥KM。每个操作卡都知道它和主密钥之间路径中的所有组密钥,如图 24.5 所示。

在这个方案中,如果（比如说)密钥k2出现在盗版卡中并且必须被撤销,那么运营商将发送一个数据包流,让所有其他用户卡计算一个新的主密钥KM。第一个数据包将是 {K0 M}KG12 ,这将让一半的订阅者立即计算 K0 ;那么在更新版本的KG11下会有一个K0加密 :{K0 M}KG011;然后这个新的组密钥 KG0 11 在 GK22 下加密;等等。结果是,即使有 1000 万客户 ,操作员也必须传输少于 50 个 [illegible] 包含多个用户密钥的盗版卡,以及如何识别泄露的密钥,而不必费心破解盗版卡。但它是一个有用的工具。

还使用了心理措施。例如,一家有线电视台播放了一个免费 T 恤的特别优惠,并阻止合法观众看到 0800 号码拨打;这让他们得到了一份海盗客户的名单。

与其他地方一样,经济因素在这里也很重要。与传统软件公司一样,付费电视盗版者的成功取决于上市时间:能够在三周内制作出 99% 正确伪造品的盗版者将消灭三个月后制作出 99.9% 正确伪造品的竞争对手。所以海盗赛跑

像合法供应商一样进行营销,盗版卡也有错误。对经济学的理解告诉我们,最好让盗版者在你拔掉他之前建立起大量的用户群,因为这让他有时间消灭他的竞争对手,而且一旦他建立起来就关掉他的卡会破坏与立即回应相比,他在更多潜在客户中的可信度更高。但如果你离开他太久,他可能会获得财务和技术资源,成为一个长期存在的问题。

付费电视行业学会了提前计划安全恢复,并在其产品中隐藏最初未使用但可以稍后激活的功能5。

最终,通过在处理器硬件中加入专有加密算法,智能卡变得更加难以伪造。由于攻击者不能简单地用探测台读出算法,而必须对芯片中的数千个门进行逆向工程,因此他们将具备攻击技术能力的实验室数量减少到屈指可数。这些实验室中有许多是通过咨询交易或其他类型的赞助而进入行业轨道的。留在帐篷外的人受到监视。强有力的执法提供了链条中的最后一环。该行业追捕主要的商业盗版者并让他们破产,无论是将他们关进监狱还是将他们淹没在诉讼中。

在 20 世纪最后一起付费电视盗版大案中,英国海盗克里斯·卡里 (Chris Cary) 因伪造 Sky-TV 智能卡而被定罪,他以 105,000 美元的价格让加拿大一家公司对其设计进行了逆向工程。他通过爱尔兰的一家幌子公司出售伪造品,当时伪造卡片还不是非法的 [1368]。因此,Sky TV 的安全顾问派了一名间谍潜入他都柏林的销售办公室,她悄悄复印了足够多的文件,以证明该行动确实是从英国进行的 [956]。英国当局不想起诉,所以 Sky 提起自诉并判处他有罪。

当当局把他关进一个开放的监狱并潜逃时,Sky 的私家侦探毫不留情地追捕他并在新西兰抓获了他,在那里他使用死者姓名的护照逃跑了 [847]。然后他最终被关进了一个合适的监狱。 Sky-TV 无情的不愉快对其他人起到了警示作用。

24.2.4.4 数字电视广播

数字视频广播 (DVB) 主要使用一套标准,这些标准自 1996 年以来经过多年发展,由 DVB 联盟控制,该联盟是一个拥有 250 多个成员的行业组织。这些标准很多而且很复杂,涉及 IPTV 和数字地面电视以及卫星电视,涉及免费服务和付费电视。 DVB 一直在取代模拟/混合系统,从 2003 年的英国和德国开始。最新的标准 DVB-T2 于 2009 年由 ETSI 颁布。

保护机制很复杂,其中一些有保密协议,但这里是一个电报摘要。 DVB 的条件访问机制类似于混合系统:内容 en

5 我们在第 16.3.1 节中讨论了印钞机如何在多年前学会将整个一系列安全打印功能,可以根据需要一次公开一个。

加密是数字的,但密钥是由用户智能卡生成的,像以前一样在 EMM 和 ECM 上运行。加密使用 DVB 通用加扰算法,该算法仅在 NDA 下可用,但在 2002 年泄露。

2011 年,Erik Tews、Julian W¨alde 和 Michael Weiner 发现了一次攻击,当时几乎不实用,因为它需要一个 8TB 的彩虹表 [1872]。智能卡未标准化(接口级别除外),因此每个广播员都可以使用他最喜欢的加密技巧和供应商;迄今为止的盗版似乎都涉及智能卡克隆,而且付费电视运营商之间还发生过各种诉讼,指控对方盗用。

付费电视,无论是有线还是卫星,在 2008 年达到顶峰,占美国家庭的 75%。将它赶下台的是 Netflix,更普遍的是转向基于宽带的在线订阅服务。

24.2.5 DVD

DVD 的历史既是好莱坞和计算机行业之间麻烦的警告,也是关于如何不进行复制保护的实物教训。

1996 年,消费电子行业推出了数字视频光盘 (DVD),后来更名为数字多功能光盘。好莱坞照例吓坏了,说除非 DVD 有一个像样的版权保护机制,否则一流的电影不会上映为了它。所以在最后一刻内置了一种称为内容加扰系统(CSS)的机制;对此的争论阻碍了 DVD 的推出,而且它是匆忙设计的。 (Jim Taylor 的标准参考文献 [1865] 讲述了 DVD 标准如何演变的故事,其中也描述了其中的大部分标准。)

DVD 具有区域编码:磁盘应该只能在来自某些指定区域列表的播放器上运行,以支持先在美国发行电影,然后在欧洲等地发行电影的传统做法,以最大限度地降低制作物理成本胶片印刷,以及胶片爆炸造成的经济损失。

但用户更愿意购买可以关闭区域编码的 DVD 播放器 。所以每个 DVD 供应商都想拥有市场上第二不安全的播放器;他们不想成为好莱坞痛打的公司,但他们希望潜在客户相信他们播放器的区域编码可能被破解。

这留下了 CSS,它在 DVD 发布时就已经知道易受攻击 [1494]。它的密钥长度为 40 位,因此该设备不会违反美国出口法规,但设计太差以至于有效密钥长度仅为 16 位。挪威少年 Jon Lech Johansen 对该算法进行了逆向工程,并为其编写了解密软件 DeCSS。行业律师对将其发布到网上的人发出禁令,但这些被视为审查制度,因此它开始出现在美国以外的网站、T 恤、歌曲和其他传统上享有宪法保护的言论形式中6。这只是让它传播得更广,让好莱坞看起来很愚蠢 [1127]。他们的律师犯了错误,说服了政府

6在第一版和第二版中对CSS以及如何破解它进行了完整的描述
这本书的;由于 DVD 正在重蹈恐龙的覆辙,因此我在这一版中放弃了它。

挪威起诉约翰森。 2003 年,他在上诉中被判无罪。

另一组问题来自 PC 是一个开放平台的事实。 DVD 联盟要求制作 DVD 播放器软件的人混淆他们的代码,这样就很难进行逆向工程。有关系统软件混淆技巧的论文适时出现 [141]。但这种封闭的方法与 Linux 发生了冲突,Linux 是已经被数百万人使用的开源 PC 操作系统。 DVD 联盟的理念与向 Linux 社区提供 DVD 驱动程序并不一致。

因此,随着带有 CD 驱动器的 PC 在商店中开始被装有 DVD 驱动器的 PC 所取代,Linux 用户社区要么不得不打破 CSS,要么放弃使用 Linux 转而使用 Windows。在这种情况下,有人搞清楚 CSS 和 DeCSS 的出现只是时间问题。

无论如何,DVD遵循了通常的模式:好莱坞害怕,拒绝发行他们最好的电影;为防止复制而采取的技术措施,很快就被破坏了;然后诉讼。我在 2001 年写道:“一个通情达理的人可能希望制片厂最终会再次明白过来,并通过销售 DVD 赚到很多钱。当然会有复制,但这还不是完全微不足道的 即使是 DSL 调制解调器也需要数小时才能将 4Gb DVD 电影发送给朋友,而且 PC 磁盘空间也是一个问题。”这实现了;尽管一些工作室坚持了一两年,但他们都加入了 DVD 的行列,到 2008 年第二版时,迪士尼的大部分收入都来自 DVD 销售。

2007 年,HD-DVD 和 Blu-Ray 之间发生了一场格式大战,两者都使用更短波长的激光来更密集地编码信息,每张磁盘最高可达 50Gb,因此有人试图推销更高密度的光学媒体。两者都使用了我在本书第二版中描述的高级访问内容系统 (AACS)。然而,只有 Playstation 3 完全实现了蓝光,而 HD-DVD 根本没有得到真正的关注。

它们作为分发媒体被宽带的发展摧毁,作为存储媒体被 USB 记忆棒的成本下降摧毁。

24.3 通用计算机上的 DRM

Victor Shear 在 1980 年代获得了自毁软件的专利,他的公司成立了 InterTrust [1793]; Olin Sibert、David Bernstein 和 David Van Wie 在 [1735] 中描述了他们的 DigiBox 系统。这使 DRM 机制能够反映真实世界的所有权,这样我就可以卖给你一张照片,你可以在收到收据后解密它;更重要的是,你可以把它给别人,之后你就不再拥有它了。

Intertrust 是众多公司中最成功的一家,这些公司在 20 世纪 90 年代中期致力于研究如何控制通过 Internet 向使用个人计算机的客户销售和分销数字商品[7]。最初的应用包括分发报纸和科学期刊的文章 [315],

7 InterTrust 专利是 20 世纪仅有的四项导致九位数易手的计算机相关专利之一,其他三项分别是哈佛虚拟内存专利、RSA 公钥专利和 Fraunhofer MP3 专利。

尽管人们一直认为,一旦网络具有足够的带宽,音乐和视频就会随之而来。

基本问题是,PC 作为通用计算机,原则上可以复制任何文件并将其发送到任何其他计算机;与模拟复制不同,副本是完美的,因此可以从一份原件制作数百万份副本。

从内容供应商的角度来看,PC 所有者是“敌人”这一事实使问题更加复杂。音乐产业认为无限复制会毁了他们的生意;计算机行业告诉他们,DRM 在通用计算机上本质上是不可能的,因此他们最好采用一种新的商业模式。音乐和电影行业,尽管规模只有计算机行业的十分之一,但在国会中的影响力要大得多(一位微软人抱怨说,普通国会议员更愿意与麦当娜合影,而不是与比尔合影),而且他们仍然控制着对计算机行业希望他们的 PC 和手机能够播放的音乐和视频。结果是推动了 DRM。

24.3.1 Windows 媒体权限管理

Windows Media Player (WMP) 是 DRM 的早期部署,在 Windows 98 发布时取代了早期的媒体播放器。它使用户能够播放音乐、观看视频和查看照片,具有从 MP3 播放器支持到卡拉 OK 歌词同步等各种功能。它引入了 Windows Media 权限管理 (WMRM),其工作方式如下。

一家想要销售数字媒体的商店使用内容密钥对每个项目进行加密,并将加密文件放在链接到他们网站的流媒体服务器上。
为了访问媒体对象,客户必须获得一个许可证,该许可证由对象标识符、许可证密钥种子和一组权利管理语言的指令组成,这些指令说明了他们可以用它做什么;他们可以播放多少次,是否可以将其刻录到 CD,等等。许可证由许可证服务器生成,并使用客户的 WMP 应用程序生成的公钥加密。许可证获取可能涉及注册或付款,但也可能在后台悄无声息地发生[1558]。

该架构类似于付费电视条件访问,因为保护音乐或视频的批量加密任务与密钥管理的个人任务分开,因此不必为每个客户重新加密视频。正如付费电视智能卡在密钥泄露或密钥管理机制受损时可以更换一样,WMRM 的密钥管理功能是在软件的“个性化黑盒”(IBX) 组件中执行的,该组件可根据需要进行更换在 Windows 更新过程中。

IBX 内部构件不时被逆向工程 [1693]。
客户的私钥被黑匣子遮蔽并隐藏在文件中;客户之前获得的许可证保存在许可证商店中;内容密钥使用客户的公钥加密;由于微软必须从黑客攻击中恢复过来,因此协议会不时进行调整。我在第 6.2.5 节中描述了在 2000 年代初期,Microsoft、Intel 和其他一些大公司如何组建可信计算组以尝试将 DRM 正确地构建到

电脑架构。由于商业和技术原因,该尝试失败了,但导致了用于可信引导的 TPM 芯片、Arm 处理器中的 TrustZone 飞地,并最终导致了英特尔芯片中的 SGX 飞地。

微软随Windows Server 2003推出信息权限管理（IRM）,旨在将DRM扩展到普通用户;这个想法是对文档或其他数字对象的访问控制将由其创建者保留。所以 DRM 不仅有利于好莱坞,也有利于好莱坞。我可以给你发一封电子邮件,你只能阅读,不能复制,一个月后就会消失。我们的愿景是,这将得到整个 Windows 生态系统中可信计算机制的支持,并方便地加强生态系统以应对来自 Linux 或 Google 文档等挑战的挑战。不过,美国公司不喜欢这种锁定,微软无法让操作系统机制发挥作用。如今,在基于云的系统（如 Oce365 或 Gmail)中实现这种分布式使用控制很容易,但要跨这样的生态系统工作就太难了;因此,如果让 Trusted Computing 发挥作用,我们离可能达到的水平不远了。

WMRM 随后在 Windows 10 中被 PlayReady 取代,PlayReady 是微软更新的“媒体文件防复制技术”。 WMP 在最基本的情况下用于提供流媒体服务、支持音乐订阅服务和地理链接服务,例如 MLB.com,它使除球队主场以外的任何地方都可以观看美国职业棒球大联盟的比赛 为此,版权通常已出售给当地电视台。

24.3.2 Fairplay、HTML5 和其他 DRM 系统

微软的产品是相当典型的权限管理系统。在 iPod 及其媒体播放器 QuickTime 中推出的 Apple 的 FairPlay 也有在主密钥下加密的音乐。当购买一首曲子时,客户会收到用随机会话密钥加密的主密钥,以及用他的 iTunes 播放器的 RSA 公钥加密的会话密钥。会话密钥在线备份在 Apple 的服务器上。与 Windows 一样,不时出现一些解锁受保护内容的程序,Apple 也适时升级了 iTunes。 Apple iTunes 在 2020 年被 Apple Music 取代。

一些公司的权利管理系统是彻头彻尾的滥用,2005 年索尼的 XCP 系统出现了一个特别极端的案例。用户第一次将带有该系统的 CD 插入 PC 时,会出现最终用户许可协议;如果用户拒绝,CD 将被弹出,如果他们接受,CD 将加载并隐藏一个 Rootkit,拦截所有对 CD 驱动器的访问,并阻止任何其他媒体播放器播放 Sony 音乐。 Microsoft 将其归类为恶意软件,并通过 Windows Defender 和恶意软件删除工具 [1307] 将其删除。后来发现,索尼甚至在他们的 Rootkit 中包含了一些侵犯他人版权的软件。

2012-14 年,万维网联盟 (W3C) 争论是否采用 HTML5,它在浏览器中提供沙箱以支持带 DRM 的多媒体内容,以及加密媒体扩展 (EME) 作为软件的一种手段,这引起了重大争议在沙盒中与在线许可证管理器进行通信。当他们最终在

2014 年,W3C 主席 Tim Berners-Lee 因采用未来排除开源浏览器的标准而遭到猛烈批评。自 2017 年以来,浏览器需要从 Google 获得“Widevine”DRM 软件的许可才能支持 Netflix 等服务。 Mozilla 是最后一个切换的主要浏览器,因为他们得出结论认为拒绝只会导致大多数用户切换浏览器。 2020 年,谷歌停止向开源浏览器提供这项技术;此后,所有新浏览器都必须是专有的; EFF 在 2012-4 年的辩论中就预测到了这一点 [571]。

2020 年的另一项发展是微软推出“双重加密”,这是一种 DRM,使银行等受监管行业更愿意将敏感数据保存在 Oce365 / Azure 云中:内容密钥保存在本地设备上,但整个过程是与 Microsoft 的访问控制结构集成 [432]。微软运营的 DRM 是否会阻止持有 FISA 授权的 FBI 特工访问微软云上的数据是一个有趣的问题;我想只有在下一个斯诺登出现时我们才会知道答案。

24.3.3 软件混淆

正如我已经提到的,早期的软件保护机制使用软件模糊来隐藏密钥并检查机器指纹、加密狗和许可证服务器的存在。有反汇编器且手头有时间的孩子往往会打败这样的把戏,因此在可能的情况下,公司会将一些关键功能转移到云端,转移到可信赖的硬件,或两者兼而有之。

但这并不总是可能的,到 2020 年,关键应用程序包括运行时应用程序自我保护 (RASP)。正如我在第 12.7.4 节中讨论的那样,这是一些移动应用程序开发人员使用的一组技术,用于保护可能已被恶意软件 root 或越狱的手机上的应用程序。 Face book 使用它来保护在欠发达国家使用其 Android 应用程序的客户,在这些国家,许多 Android 手机都是二手的,没有补丁支持并且通常由当地销售代理商获得 root 权限。根据欧洲中央银行的授权,RASP 正成为欧洲银行应用程序或它们所依赖的身份验证应用程序的强制要求。在这两种情况下,目标都是保护加密密钥免受对设备进行 root 操作的攻击者的攻击。这也是 1990 年代产品（如 Windows Media Player)的威胁模型。

早期曾尝试编写混淆编译器来生成防篡改软件;在 [141] 中描述了一个早期的 Intel 项目,并导致了在早期软件 DVD 播放器中使用的工具。正如我在之前的 24.2.5 节中所描述的那样,这些被适当地打破了,并导致英特尔转向可信计算并最终转向 SGX,正如我在 6.3.1 节中所描述的那样。

理论计算机科学家撰写了许多关于混淆和不可区分性的论文; Boaz Barak 及其同事在 2001 年的一个开创性结果表明,我们不能编写具有强大和可持续保护属性的混淆编译器 [166]。但是 与其他不可能性导致的安全性（如恶意软件检测)一样 随之而来的问题是,即使完美的混淆在理论上是不可能的,实际的混淆对于某些目的来说是否足够好。

微软采用了一种安全更新理念:Windows Media Player 的密钥管理代码隐藏在 IBX 中并四处移动,因此它可能上个月在 Windows 错误处理程序中,下个月可能在一个不起眼的设备驱动程序中。恶意软件编写者采取了类似的轨迹。正如我在第 21.3.5 节中所述,他们经常通过包含多态标头的加壳器运行代码来混淆代码,该加壳器反过来解密恶意软件主体。密钥和标头都不同 erer,使恶意软件更难识别。如果维护人员有能力和积极性,有时可以使这样的方法工作得很好。但是,很多时候,它们不是;从销售商那里购买 RASP 的天真的公司应该做好最坏的打算。

主要的安全研究会议往往不接受关于混淆的论文,因为他们将其视为战术军备竞赛,而不是科学知识的积累。尽管如此,仍有一个小型研究社区致力于混淆,截至 2020 年,保护用于身份验证或解密的引擎的最新技术是实现一个具有奇怪指令集的虚拟机,在其中实现加密,然后进一步混淆虚拟机本身(自定义操作码早在 1990 年代就已用于 Sky-TV 智能卡)。评估这样的方案,甚至猜测要打破它需要多少努力,仍然是一个真正的问题 [555]。如果 RASP 测试人员尽管尝试了两周仍无法提取加密密钥,那么这并不能保证您不会遇到尝试了一个月 8 的人。反编译工具和技术一直在改进,许多工程师一生中的大部分时间都在试图弄清楚其他人的代码实际上做了什么。有些人获得了这方面的真正诀窍,但他们可能不在您的合规性测试实验室工作!因此,柠檬市场是意料之中的。

综上所述,这还有一些不那么重量级的方面。一些工具在缩小和优化 Java 字节码时混淆了它;ProGuard 就是其中之一,作为 Android SDK 的一部分分发。娱乐方面,还有国际混淆 C 代码竞赛,人们在尝试隐藏功能的过程中乐在其中。

24.3.4 游戏、作弊和 DRM

游戏是最早的应用程序之一 当世界上第一台合适的计算机 EDSAC 开始运行时,研究生们就开始为它编写游戏。几十年来,电脑游戏一直是一门大生意。

它们推动了 20 世纪 70 年代的家用电脑热潮,进而催生了 PC 行业;游戏机一直是微处理器和存储芯片的巨大市场;和游戏 无论是在控制台还是 PC 上 在很大程度上推动了计算机图形学的发展 [2056]。 2001 年美国游戏销量超过电影票房销量;随着游戏转移到网上,游戏公司开始销售订阅服务,而不仅仅是一次性门票 [280]。

8我亲自承受伤疤。早在 1990 年代,英特尔就付钱让我们花两周时间破解由其内部混淆编译器 Beelzebub 生成的原型 DVD 播放器二进制文件。我们只进行了大约一半,然后该公司向其客户吹嘘“剑桥无法打破这个”。乔恩·莱赫·约翰森 (Jon Lech Johansen) 后来花了一个月的时间盯着代码并破解了它,让我们看起来很愚蠢 但至少英特尔最终看起来更愚蠢。

当任天堂将控制台游戏带入家庭时,他们通过以后销售软件卡带和其他附加组件来补贴控制台,因此在控制可以使用哪些附件方面付出了很多努力,正如我稍后在第 24.6 节中讨论的那样； PC 游戏软件的版权保护也是一个大问题。

然而,转向在线电脑游戏已经减轻了这些担忧。由于游戏逻辑的关键部分运行在服务器上,客户端软件可以免费赠送,剩下的问题就是玩家是否能获得不公平的优势。

游戏玩家作弊的方式有很多种 [2057]。有些游戏禁止勾结,例如契约桥牌,而且很难阻止在在线平台上玩游戏的人使用完全独立的渠道作弊。在现实世界中,由经验丰富的玩家组成的陪审团会审理作弊指控,他们会就结果是否比诚实比赛中的预期更好发表看法。即便如此,一些决定多年来仍存在争议:玩家可能很幸运,而一起玩了多年的伙伴可能会下意识地交流而不是尝试。在线游戏可以提供帮助,因为您可以拥有用于统计分析的在线记录、许多玩家使用同一张牌的在线锦标赛,以及人们与许多合作伙伴而不是一个合作伙伴一起玩的新游戏形式。

其他游戏需要合谋,例如涉及多人团队的冒险游戏。正如我在第 8.6.8 节中讨论的那样,到 2020 年,这些是目前最大的 DDoS 出租服务市场。球员通常是小学生,花几美元就可以在关键时刻让对方球队的关键成员下线。

第三种作弊策略是从计算机游戏的本质中产生的。例如,在战术射击游戏中,成功应该取决于玩家的战术和射击技巧,而不是游戏机制。然而,游戏的物理模型总是存在缺陷,通常是由于网络延迟和游戏设计师用来处理它的优化而引入的。例如,您通常会期望在射击决斗中,如果您的网络延迟最低,或者如果您先移动,您就会有优势。然而,许多游戏客户端使用的预测算法会缓存附近玩家的信息,因此如果你跳到一个角落,看到你的敌人并开枪射击,那么你的网络连接越慢,他看到你并做出反应的时间就越长。迈克邦德创造了“新战术”一词来指代球员下意识地利用这种异常现象 [280]。这本身可能不是作弊,但近年来玩家已经开始故意操纵网络连接来制造人为延迟,无论是传入数据包以延迟其他玩家,还是我们的传出数据包以查看其他玩家将要做什么。

这将我们带到了经典游戏作弊之一,即拥有您自己的代码以实现自动化和支持。人们已经编写了各种各样的工具,从重复点击开火按钮的简单例程（破解游戏中你可以物理开火的速度是一个因素)到拦截传入网络数据包的代理,识别坏人,检查你的传球,并优化他们的目标。这些瞄准机器人具有不同的复杂程度,从执行所有目标获取和射击的代码,到仅提高瞄准性能的人工控制版本。它们可以作为代理连接到数据包流、图形卡甚至客户端代码中。

同一主题的另一个变体是 wall hack,玩家修改他的

看穿墙壁的软件 例如,通过改变图形软件使它们半透明而不是不透明。这样的黑客攻击是可能的,因为第一人称射击游戏通常会向游戏中的所有玩家发送原始位置信息,然后将其留给客户端软件根据本地物理模型进行渲染。

销售第一人称射击游戏的游戏公司认为瞄准机器人和其他客户端黑客严重破坏了其他玩家的乐趣,因此他们使用各种加密、身份验证和 DRM 机制来减少作弊,同时也减少作弊的感知 这几乎对操作员造成损害[281]。诸如 Punkbuster 之类的防护软件自 2000 年以来一直存在,使用反病毒技术来检测对游戏代码或其所依赖的驱动程序的挂钩尝试。 Steam 等大型游戏平台有自己的 DRM 机制,试图阻止瞄准机器人和其他游戏作弊,并通过让客户更难转售游戏来保护自己的收入 [1288]。正如我在上一节中所讨论的,这是一场持续不断的战斗,并且一些技术(例如人为延迟)很难完全解决。

然而,游戏是值得信赖的客户端软件的应用之一,其保护涉及类似 DRM 的机制,已经变得根深蒂固,尽管大多数现代游戏都被锁定到客户帐户并且它们的大部分逻辑现在都在服务器上运行。服务器通常还加强了分析,以检测赛后作弊行为,就像在专业桥牌锦标赛中一样。

24.3.5 点对点系统

从 20 世纪 90 年代后期开始,点对点文件共享成为在线分发音乐的主要方式之一。一旦人们在他们的计算机上安装了 CD 驱动器并连接了宽带,他们就可以复制和分享他们最喜欢的曲目。 1999 年,18 岁的辍学者肖恩·范宁 (Shawn Fanning) 通过创建 Napster 服务彻底改变了音乐行业,该服务使人们能够相互共享 MP3 音频文件 [1381]。 Napster 没有将文件集中保存,这会招致法律诉讼,Napster 只是提供了一个索引,以便想要某个特定曲目的人可以找出其他人拥有它并准备分享或交易。它吸引了数千万用户,但好莱坞的诉讼于 2002 年 9 月将其关闭。Gnutella 和 Freenet 等系统随后借鉴了抗审查系统世界的思想,建立了没有中央节点的网络,中央节点可以被关闭法律攻击[439]。紧随其后的是其他系统,例如 Kazaa 和 Bittorrent。

我是早期抗审查系统 Eternity Service 的设计者。当一个早期的匿名转发器 anon.penet.fi 被用来发布一条令山达基教徒不安的消息并在他们获得法院命令迫使其运营商披露用户的真实电子邮件地址与他们在他的系统上使用的假名 [881]。

作为该案例主题的信息包含他们教会前任牧师的一个 adavit,大意是一旦成员被完全启动,他们就会被告知其他人类正遭受错误意识的折磨;事实上,耶稣是坏人,路西法是好人。

好吧,历史上有许多宗教谴责其竞争者既受骗又邪恶的例子。山达基教的创新是声称

他们的经文就是他们的版权,所以举报人的泄密是侵犯版权。他们在许多司法管辖区都逃避了这一争论,直到最终荷兰的一家法院通过允许那里的一个非政府组织发布所谓的“Fishman adavit”来制止这种争论。

Eternity Service 旨在通过在网络上分发文件片段来提供长期文件存储,并进行加密,以便托管它们的人无法分辨他们拥有哪些片段,并且只能通过重邮机制进行重建[61]。后来的版本是 Publius9,它也提供了一种抗审查的匿名发布机制 [1974]。

美国版权 Oce 将对等网络定义为计算机彼此直接链接而不是通过中央服务器链接的网络。没有可以通过法院命令关闭的服务器给音乐行业执法者带来了一个有趣的问题。音乐产业所依赖的两种策略是起诉上传者和对系统进行技术攻击。

攻击点对点系统的一种方法是通过引入修改后的对等点“遍历网络”,尽可能多地联系其他对等点,然后识别它们。在 2000 年代中期,音乐行业试图大规模骚扰用户,提起了数万起诉讼。在许多情况下,人们同意停止并停止并支付少量罚款而不是打官司;但在 2007 年 10 月,明尼苏达州德卢斯的联邦陪审团裁定 30 岁的杰米·托马斯 (Jammie Thomas) 因在 Kazaa 上分享资料而侵犯版权,并命令她为案件中涉及的 24 首歌曲每首支付 9,250 美元。为音乐行业工作的公司也将损坏的音乐文件上传到垃圾邮件发送系统(这通常是合法的),并且怀疑他们也在进行拒绝服务攻击(在许多司法管辖区是不这样的)。 2007 年 9 月,一家名为 Media Defender 的公司致力于“文件共享缓解”,其数千封内部电子邮件在一名员工将其电子邮件转发到 Gmail 并且其密码被泄露后泄露。

事实证明,Media Defender 的商业模式是每月每张专辑收取 4,000 美元,每首曲目每月收取 2,000 美元,用于“保护”涉及对 15 个 P2P 网络的 2200 万用户的攻击 [1501]。据称,点对点系统也遭到了 Comcast 的攻击,据说该公司通过发送伪造的重置数据包来破坏 Bittorrent 连接,从而中断了其客户的连接。康卡斯特可能更愿意其客户通过其有线网络收看电视,因此他们会看到其广告,但如果这些指控属实,则会引发公共政策问题:康卡斯特不是执法机构 [219]。

2020 年的情况是,一些司法管辖区遭受了这种勒索,来自有时被称为 Torrent trolls 的律师事务所:例如,在瑞典,有数万起律师要求家人支付大笔款项的案件声称他们的孩子上传了一些受版权保护的材料 [1655]。这似乎更像是地方程序法的功能;在许多国家,律师不能这么不正经,至少在

9 对于非美国读者:革命者亚历山大·汉密尔顿、约翰·杰伊和詹姆斯·马迪之子在撰写《联邦党人文集》时使用了笔名 Publius,该文集收录了 85 篇文章,于 1787–8 年在纽约州报纸上发表,帮助说服了纽约州约克选民批准美国宪法。

这种特殊的方式。

在更大的全球生态系统中,大型服务公司现在占据主导地位,版权侵权的决定性因素是根据美国 DMCA 建立的通知和删除制度,其他地方也有类似的法律。我将在 24.5 节中进一步讨论这个问题。

24.3.6 管理硬件设计权

另一个版权管理生态系统是保护在硬件中使用许可的设计。像 Arm 这样的公司通过向制造定制芯片的公司授权处理器和其他组件的设计来谋生,无论是通过设计专用集成电路 (ASIC) 还是通过使用现场可编程门阵列 (FPGA)。

硬件保护的第一个用例是当此类设备用于使产品更难伪造时,例如通过超额生产。一家相机公司获得了一个电路许可,他们将其集成到加载到 FPGA 的比特流中,然后成为他们在中国工厂生产的新相机的关键组件。他们支付了 100,000 个许可证,但市场上有 200,000 个摄像机。有两种失败模式:相机公司可能订购了额外的产品并向知识产权所有者撒谎,或者中国工厂可能在欺骗相机公司。事实上,他们可能都在作弊,每个人都决定多生产 50,000 个单位。现在,相机公司可以使用一些技术机制来阻止工厂欺骗它,例如在制造后使用序列号等对每台相机进行个性化设置 但这可能会使欺骗知识产权所有者变得更加困难。

所以第二个问题是知识产权所有者如何判断产品是否包含特定电路。相机公司可能已经为一种型号许可了处理器或滤镜,然后在没有声明的情况下也将其内置到另一种更便宜的型号中。

这些风险导致一些大型 IP 供应商更愿意将他们最好的设计只授权给其他大公司,因此小型初创公司可能处于不利地位。它们还抑制了 FPGA 的销售,FPGA 的制造商提供了通过为整个芯片分发加密比特流和更新来解决第一个问题的机制;第二个问题更难,因为芯片设计工具在信任边界内。客户需要能够评估设计和调试设计,这在控制传播方面处于紧张状态。已经有一些侧通道用于取证。半导体 IP 的所有者可以购买可疑商品的样品,然后测量芯片的精确模拟行为,例如功耗和时序,这通常可以揭示给定功能组件的存在。甚至可以特意设计组件以在其电源迹线中生成合适的信号。 (军事承包商使用类似的技术来寻找硬件特洛伊木马。)

这给我们带来了版权标记的问题。

24.4 信息隐藏

好莱坞对寻找保护版权的新机制的兴趣在 20 世纪 90 年代中期与军方对不引人注目的通信的兴趣以及公众对政府控制密码学的努力的关注结合在一起,并开始推动信息隐藏领域的快速发展。这主要是指将数据隐藏在其他数据中的技术,例如将秘密消息隐藏在 MP3 音频文件中,或者程序的序列号嵌入在某些指令的执行顺序中。

好莱坞寻求在数字音频、视频和艺术品中不引人注意地嵌入版权标记的救赎。其中包括水印、可能隐藏也可能不隐藏但难以删除的版权信息,以及作为隐藏序列号的指纹。例如,当您从 Apple 的 iTunes 音乐商店下载 mp3 时,它包含嵌入在音频中的指纹,可以识别您的身份。当时的想法是,如果您随后将副本上传到文件共享系统,版权所有者可能会起诉您。 （有些人认为指纹识别会抑制整体销售,因为它会给诚实的购买者带来法律风险。例如,亚马逊没有标记 MP3 下载 [852]。）

隐私利益在于隐写术,其目的是将消息以某种方式嵌入到某些掩护媒体中,以使其存在无法检测到。

Gus Simmons [1745] 提出的概念模型如下。爱丽丝和鲍勃在监狱里,他们想策划一个越狱计划;他们所有的通讯都通过监狱长威利。如果威利检测到任何加密信息,他将把他们单独监禁起来,从而挫败他们的计划。因此,他们必须找到某种方法将他们的秘密信息隐藏在无害的掩饰文本中。

与密码学的相关领域一样,我们假设所使用的机制为监狱长所知,因此安全性必须完全依赖于 Alice 和 Bob 以某种方式设法共享的密钥 [1753]。

与电子战有一些相似之处。首先,如果隐写术被视为一种低拦截概率的通信,那么版权标记就像是抗干扰通信:它可能使用很多相同的方法,但为了抵抗集中攻击,它可能具有更低的位速度。我们可以将 Willie 视为盗版者,他试图以导致版权标记检测器失败的方式破坏音频或视频信号。其次,最初为电子战开发的直接序列扩频等技术在信息隐藏领域得到了应用。

版权标记无需隐藏即可生效。一些电视台以明显但不显眼的方式将其徽标嵌入图片的一角,正如我所指出的,学术期刊下载也有类似的做法。但是,在下文中,我将重点关注隐藏的版权标记。

24.4.1 水印和副本生成管理

DVD 联盟开始担心数字视频或音频可以解码为模拟格式,然后再分发（所谓的“模拟空洞”）。

他们着手发明一种复制生成管理系统,该系统甚至可以使用模拟信号。这个想法是视频或音乐曲目可能是

未标记,或标记为“永不复制”,或标记为“仅复制一次”;合规播放器不会录制标记为“永不复制”的视频,并且在录制标记为“仅复制一次”的视频时会将其标记更改为“永不复制”。商业销售的视频将被标记为“永不复制”,而电视广播和类似材料将被标记为“仅复制一次”。这样,消费者可用的 DVD 播放器将允许无限复制家庭视频和时移观看电视节目,但不容易被商业盗版滥用。该机制依赖于在内容中隐藏版权标记,并在 [1167] 中进行了审查。对于每个磁盘,选择一个票证 X,它可以是一个随机数,加上复制控制信息,还可能加上一些物理介质独有的信息,例如导入轨道中的摆动。使用单向哈希函数 h 计算 h(X),然后计算 h(h(X))。在视频中嵌入 h(h(X)) 作为隐藏的版权标记。让兼容的机器寻找水印,如果它们发现一个拒绝播放曲目,除非它们提供了 h(X),它们通过散列它并将其与标记进行比较来检查。

兼容设备只会在给定 X 的情况下记录标记的轨道,在这种情况下,只有 h(X) 会写入新光盘。这样,原始介质中的“仅复制一次”轨道在新介质中变为“不再复制”轨道。

这最终以蓝光形式出现,但在市场上失败了,并且对开发人员来说是一个彻底的痛苦。

鲁棒性取决于很多因素,包括我们的老朋友、接收器操作特性或 ROC,它设置了误报和漏报之间的权衡。标记机制的漏报率低是不够的;它也需要低误报率 [1318]。如果您的播放器在您制作的孩子生日聚会视频中错误地检测到“禁止复制”标记,那么您必须购买盗版播放器才能观看。那么什么样的标记是可能的,它们对伪造、欺骗和其他攻击的抵抗力有多强?

24.4.2 一般信息隐藏技术

信息隐藏的历史甚至比密码学更早,其根源在于伪装。希罗多德 (Herodotus) 记录了希腊人和波斯人之间战争期间使用的技巧,包括将信息藏在猎人携带的野兔的肚子里,将其纹身在奴隶剃光的头上,然后允许头发重新长出,并写下它在写字板的蜡下的木制底座上 [889]。 Francis Bacon 提出了一个系统,通过交替使用两种不同的字体 [1513],以每个字母一位的方式在书中嵌入二进制信息。直到现代,大多数作家都认为隐藏机密信息比加密信息重要得多 [2021]。军事和情报组织敏锐地意识到,trac 安全通常比内容机密性更重要,并且已经使用了从间谍使用的微点到低拦截概率无线电的各种技术。

当谈到将数据隐藏在其他数据中时,该主题的现代术语如下[1521]。版权标记,或者在隐写术的情况下,嵌入文本,隐藏在产生标记文本的封面文本中,或者在隐写术的情况下,隐藏文本。在大多数情况下,在此过程中会使用额外的秘密信息;这是标记键或隐写键,

通常需要它的某些功能来恢复标记或嵌入的文本。这里，“文本”一词可以酌情替换为“音频”、“视频”等。

已经提出了各种各样的嵌入方案。

- 许多人建议在音频或视频信号的最低有效位中隐藏标记或秘密消息。这通常不是一个很好的策略，因为隐藏的数据很容易从统计上检测到（最低有效位不再与图像的其余部分相关），并且删除或替换也很简单。它也被有损压缩技术严重损坏。

- 一种更好的技术是将标记隐藏在一个或多个由密钥确定的位置。这最早是在中国古典时期发明的。发件人和收件人都有一张纸质面具的副本，上面有随机位置的孔洞。发件人会将他的面具放在一张空白纸上，在孔中写下他的信息，然后将其取下并撰写包含秘密嵌入信息字符的封面信息。这个技巧在 16 世纪由意大利数学家卡丹重新发明，现在被密码学家称为卡丹格栅 [1001]。

- 它的现代版本在.gif 格式图像中隐藏了一个标记，如下所示。
秘密密钥被扩展为选择适当数量的像素的密钥流。嵌入的信息是这些像素的颜色代码的奇偶校验。在实践中，即使图像中相当多的像素也可以将它们的颜色更改为调色板中相似像素的颜色，而没有任何可见的效果[972]。然而，如果所有的像素都以这种方式调整，那么隐藏的数据也很容易通过再次调整它们来移除。如果封面图像和嵌入方法可以安全地调整 1% 的像素，则可以获得更好的结果。然后，如果典狱长使用不同的密钥重复该过程，则会调整不同的 1% 像素，并且只有 1% 的隐藏数据位会被破坏。然后可以使用纠错码恢复这些。

- 一般来说，噪音或失真的引入 就像有损压缩一样 会在隐藏数据中引入错误，几乎与嵌入方法无关，除非添加某种纠错码。为钞票标记而提出的系统 Patchwork 使用重复代码 钥匙选择两个像素子集，其中一个通过增加亮度来标记，另一个通过降低亮度来标记。这嵌入了一位；该笔记要么使用该密钥加水印，要么不是 [225, 830]。这让人想起差分功率分析：密钥告诉你如何将输入数据分成两堆，如果密钥正确，它们就会明显不同。

- 在一般情况下，人们可能希望嵌入不止一位，并让嵌入的数据经受住非常高水平的诱发错误。因此，一种常见的技术是使用从电子战中借鉴的直接序列扩频技术 [1890]。你有许多秘密序列，每个序列编码一个特定的符号，你将其中一个添加到内容中以对其进行标记。

- 扩频编码通常在变换空间中完成,以使其效果更不易察觉,并且对常见的压缩形式更具鲁棒性。这些技术也通常与感知过滤结合使用,感知过滤强调图像或音乐轨道中最嘈杂或感知最重要部分的编码,在那里它最不突兀,并在音乐或音乐的安静段落中弱化它大片的色彩 [288]。

- 一些方案使用特定媒体的特性,例如通过将文本行向上或向下移动百分之三英寸 [315] 来标记印刷媒体的方案,或者在感知阈值以下向音乐添加额外的回声 [225] .到目前为止,此类技术似乎还没有像基于使用变换空间、扩频和感知过滤的键控嵌入的通用技术那样稳健或广泛使用。

版权标记在 20 世纪 90 年代后期取得了非常迅速的进展:人们发明了其他人破坏的标记方案,直到某些系统被纸币和 Adobe 等工具采用。从 2000 年代中期开始,人们对版权标记的兴趣随着向宽带的转移而减弱,但对隐写术和隐写分析的研究仍在继续,并与图像取证研究相结合。

24.4.3 对版权标记方案的攻击

在这本书中,我们看到了对密码系统的攻击,这些攻击偶尔涉及密码分析,但更多时候依赖于错误的假设、保护错误的东西、协议失败和实现错误。在整个技术史上,发明往往最终被用来解决与发明者最初考虑的问题有所不同的问题。版权标记在这两个方面都没有什么不同。

- 一开始,许多人解决了嵌入隐藏版权信息的问题,以便可以在法庭上证明作品的所有权。

  但这是没有问题的。律师在证明展品的所有权方面几乎从来没有任何困难;他们不依赖于可能会混淆陪审团的技术措施,而是依赖于乐队合同和模特授权表格等文件。

- 像往常一样,许多设计者忽略了 Kerckhos 的原则 系统的安全性应该在于密钥的选择,而不是所使用的算法。
  但是当标记用于证明特定数字对象是否被许可时,这意味着将它们与标记密钥一起在法庭上公开,因此可能需要使用多个密钥。

- 例如,在美国销售的彩色复印机在复印件的位模式中隐藏机器识别代码 (MIC),作为检测货币伪造者的额外手段 [2002]。施乐和佳能在 1980 年代推出,显然是在与一个或多个政府达成秘密协议后,它的存在于 2004 年在荷兰的一起法庭案件中被披露。

然后在 EFF 领导的众包工作中对机制进行了逆向工程。 MIC 是一个直径为 0.1 毫米的黄点图案,人眼几乎看不到,在 A4 彩色复印件上重复约 150 次。现在有软件可以识别并删除它,因此举报人可以在将敏感文件泄露给媒体之前对其进行清理 [1602]。

- 许多标记只是给信号增加了一些噪音。但是,如果视频中的所有帧都带有相同的标记,则可以将它们平均得到标记,然后将其减去。或者您向标记系统提供一些已知内容,并比较其输入和输出。即使在解密后立即在防篡改过程中应用标记,并且每个设备添加不同的标记,那么如果标记由在内容中离散点添加的小信号组成,对手也可以解密相同的密文与几个不同的设备进行比较,以去除标记。

- 已经尝试开发一种与公钥密码学等效的标记,以便(例如)任何人都可以插入一个只有一个委托人可以检测到的标记,或者任何人都可以检测到一个只有一个委托人可以插入的标记。如果可以在制作封面音频或视频时插入标记,则前者似乎是可行的 [494]。后者似乎更难。首先,您不能通过在图像中嵌入签名来验证图像的所有部分,因为那样您将修改它以证明它未被修改。其次,如果您尝试仅验证高阶位或显着特征,则会存在鲁棒性问题:给定一个可以检测标记的设备,攻击者可以通过对图像进行小的更改来删除它,直到解码器无法找到为止它不再 [1511, 1168],然后应用自己的签名。因此,主要努力投入到在内容的每个实例中放置不同标记的机制,因为它被解密。

- 开发了隐写分析技术来破解大多数嵌入方案。
  十多年来,人们会在信息隐藏研讨会上提出新的信息隐藏机制,但第二年它们就被破解了。最多产的攻击团队是杰西卡·弗里德里希 (Jessica Fridrich) 和她在宾厄姆顿的学生;她关于隐写术的书是关于该主题的认真工作的起点 [724]。

- 最成功的标记创业公司 Digimarc 建立了一项服务来跟踪网络上的知识产权。他们提供了让图片所有者嵌入隐形指纹的工具,并且有一个机器人可以在网上爬行寻找标记的图片并将它们报告给版权所有者。有多种方法可以解决这个问题。例如,一个标记的图像通常可以被分割成更小的图像,这些图像在网页上呈现时看起来就像原始图像,但其中不会检测到版权标记(图 24.6)[1516]。
  Digimarc 在监控广播流方面工作了一段时间;但随着时间的推移,人工智能改进到软件可以直接识别正在播放的歌曲的程度。 Digimarc 进入安全印刷领域,将其标记技术授权给中央银行作为一种伪造检测措施。例如,它出现在欧元纸币上,

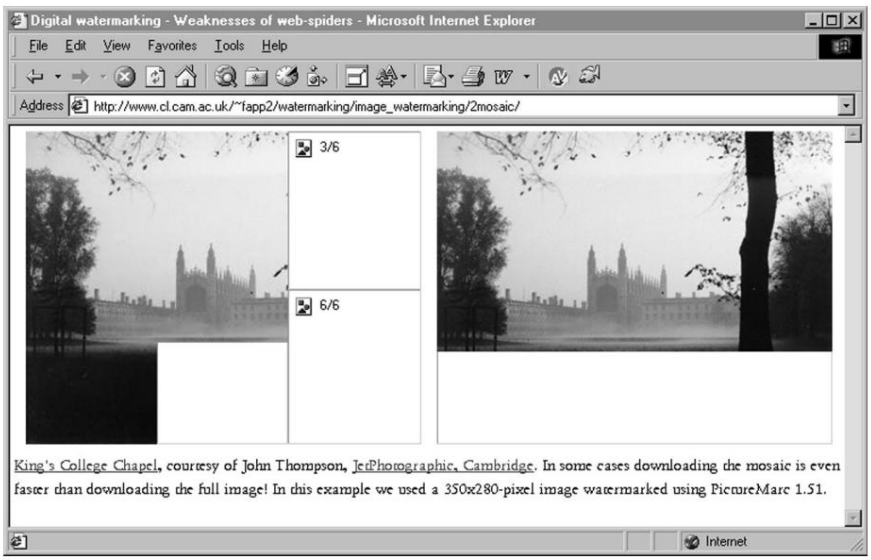

图 24.6： – 马赛克攻击（由 Jet Photographic 提供，www.jetphotographic.com）

它可以防止使用最新设备 [2061] 进行扫描或复印。 Photoshop 和 Paintshop Pro 等软件包现在拒绝处理标记的图像。 Digimarc 现在监控包装并提供标签系统。

· The most general attacks on imperceptible copyright marking schemes involve suitably chosen distortions.可以通过随机复制或删除声音样本来消除音频标记,以引入听不见的抖动;用于点击去除和重采样的技术也是强大的标记去除器。对于图像,我的学生开发了一个名为 Stirmark 的工具,它会在图像中引入与在高质量打印机上打印然后用高质量扫描仪再次扫描时相同类型的错误。它应用了轻微的几何失真:图像被轻微拉伸、剪切、移动和/或旋转了一个不明显的随机量这击败了开发时几乎所有现有的标记方案,现在是版权标记稳健性的标准基准[1516]。

有关对版权标记方案的攻击的更完整说明,请参见 [724]。
一旦标记检测算法已知,设计仍然健壮的标记方案仍然很困难。

也许扼杀版权标记的关键技术因素不是攻击,而是延迟。这对于流媒体体育赛事非常重要;在你看到进球之前,你不想听到隔壁的欢呼声。最近,媒体流标准（DASH、HLS)已经更新,以支持在完全写入以“修复”此问题之前下载媒体块。显然,用于识别谁重新流式传输流的服务器端水印会引入大量延迟。这有助于推动采用直接识别侵权材料。 2017 年,Apple 收购了 Shazam 的先驱;谷歌

为 YouTube 开发了自己的 Content ID,其中包含内容指纹数据库,其中包含有关版权声明位置的信息,当上传或直播视频时,会在该数据库中查找它们。版权所有者可以选择通过分享广告收入来通过视频获利,或者阻止它。类似的技术用于阻止因其他原因引起反感的内容:儿童性虐待材料大多使用称为 PhotoDNA 的 Microsoft 系统进行识别。

24.5 政策

在 1990 年代和 2000 年代,随着互联网的开放使复制变得容易并威胁到传统音乐,科技行业与许多“知识产权”(IP)(版权、专利和商标)所有者之间发生了激烈的政策辩论,书籍和电影出版商 10.反应包括一系列法律,从通过美国的数字千年版权法案 (DMCA) 延长版权期限到欧洲的知识产权执法指令,这些法律以许多技术和其他地方的人认为具有威胁的方式转移了权力。技术的出路是美国 1996 年《通信规范法》(CDA) 第 230 条,其中规定“交互式计算机服务的提供者或用户不得被视为其他信息内容提供的任何信息的发布者或发言人”提供者 所以平台不能对用户侵犯版权负责。这有利于信息服务公司在美国而非欧洲的发展。

美国 DMCA 确实赋予版权所有者强制 ISP 关闭包含侵权材料的网站的权力(“通知和删除”)。尽管还有一项规定(“通知并退回”)要求订户提交反通知并在 14 天内退回他的作品,除非版权所有者提起诉讼,但实际上许多 ISP 只会终止客户的作品服务而不是卷入诉讼。这不仅导致了大量使用点对点系统的音乐复制,还导致了音乐行业律师的大量删除请求,以及我们之前讨论过的 DRM 的推动。

向谷歌提出的删除请求中有一半以上来自排名前 16 位的版权所有者,其中前三名每年产生超过 10 亿的版权 其中许多指向甚至不在谷歌上的链接。许多投诉组织很少或根本没有删除他们投诉的链接,因为这些链接要么不相关,要么被判定为不侵权;有关详细信息,请参阅 Google 的透明度报告 [800]。

这具有实际的政策后果:审查一家冒充耐克的中国商店是一回事,而审查 Black Lives Matter Peckham 以回应白人至上主义者的投诉则是另一回事。

有许多副作用:例如,允许复制供个人使用的法律规则(美国的“合理使用”和英国的“公平交易”)正在被不允许的技术控制所取代。例如,当我申请扩建厨房的规划许可时,我必须提交四份当地规划图;

10 “知识产权”一词是有争议的。许多活动家反对它,认为这是企业游说者创造的宣传用语,他们希望人们开始将专利和版权视为永久的自然权利,如房地产或人权,而不是暂时的垄断。

但是我们大学图书馆的地图软件只能打印三份。
这完全是英国陆军测量局为了最大化其收入而故意采取的行动。法律控制由访问控制补充,DMCA 和类似的欧盟法律赋予这些访问控制的法律特权创造了一系列新的权利,被法律学者称为“副版权”[532]。

实际上,版权法规不再由华盛顿或布鲁塞尔的立法者制定,而是由为微软、苹果或亚马逊工作的程序员制定。
结果是侵蚀了版权使用者的权利。在一个引人注目的例子中,亚马逊悄悄地从其客户的 Kindle 中删除了乔治·奥威尔 (George Orwell) 的《1984》和《动物庄园》的一个版本,这两个版本引起了一些争议 [1831]。
这是一个发人深省的提醒,提醒您拥有一本书的实体副本与“拥有”一本电子书之间存在巨大差距 事实上,您只是从编写许可证的供应商那里购买了许可证,而您几乎没有任何权利根本。

与此同时,版权法突然与数百万人息息相关。过去它只是出版商等专家的关注点,而现在它触及每个下载音乐、时移电影或维护个人网页的人的生活。由于法律跟不上技术的发展,它所允许的和人们实际做的之间的差距越来越大。例如,在英国,翻录 CD 在手机上收听在技术上是违法的;然而,由于这是人们仍然购买 CD 的主要原因之一,英国唱片业协会(贸易机构)慷慨地表示不会起诉任何人。但是,许多过去发生在私人或不受监控的公共场所(例如在酒吧唱歌)的轻微侵权行为现在都发生在网上(例如歌曲的手机视频片段出现在某人的社交网络页面上) .约翰·德黑兰 (John Tehranian) 计算出,一名典型的法学教授每天侵犯版权的次数超过 80 次,法定罚款超过 1000 万美元 [1866]。实际上,我们之所以容忍版权法,是因为它并未针对个人强制执行。技术使执法成为可能,将版权整合到数量越来越少的公司所有者和集体管理组织中,形成了一个集中的游说团体,贪婪使滥用行为发生,摩擦增加。

版权的合并也导致收入分配不公。我已经提到了集体管理协会的问题,它实际上影响了征税场所和分配收益的方式,使富人得到很多而小人物根本没有;这在流媒体中变得更糟,流媒体的支出是播放的函数而不是用户的函数。因此,如果我的孙女每月支付 10 英镑,每天听 Ariana Grande 四个小时,而我支付同样的费用,每周听 Kathryn Tickell 两个小时,那么与其给他们每人 10 英镑(减去 Apple 的 30% 佣金),Ariana将得到凯瑟琳得到的十四倍 [1553]。这意味着你的大部分订阅 或者至少是科技公司不会采取任何方式的钱 都流向了像阿丽亚娜、艾德希兰和 Lady Gaga 这样的巨星。

还有隐私问题。在过去,人们会用现金买一本书或一张唱片;转向下载意味着谷歌、Spotify 和苹果等公司运行的服务器记录了人们观看和收听的内容,并且可以传唤。 (转向在线图书销售然后转向 Kindles 在亚马逊创造了类似的记录。)这些记录也用于营销。加拿大隐私专员的一项调查发现许多

侵入行为的例子,包括电子书软件分析个人、图书馆服务中的 DoubleClick 广告、通过 IP 地址跟踪个人的系统,以及供应商声明的隐私政策与观察到的行为之间的矛盾 包括与第三方的未公开通信 [682]。

为什么版权所有者或声称代表他们行事的大型科技公司能逍遥法外?答案在于游说的动态。

24.5.1 IP 大厅

知识产权游说团体的现代起源是辉瑞制药公司在 1970 年代努力将其药品的专利保护从美国扩展到巴西和印度等欠发达国家。 Peter Drahos 和 John Braithwaite 讲述了这段历史 [581];总之,辉瑞和其他制药公司与音乐和电影行业(希望减少盗版和复制)、奢侈品行业(希望减少廉价仿冒品的数量)以及许多其他美国参与者(包括商业软件联盟),并说服美国政府开始向其他国家施加压力,使其专利、版权和商标法与美国的法律接轨。从 20 世纪 80 年代中期开始,这主要是欠发达国家想要达成贸易协议的问题,但在 1995 年,一项与贸易相关的知识产权条约 (TRIPS) 对世界贸易组织的成员生效(WTO),随后是 1996 年世界知识产权组织 (WIPO) 的两项条约。从本质上讲,美国和欧盟联合起来欺负像印度和巴西这样的顽固国家。

这些条约的实施激起了发达国家的反对,因为人们开始意识到他们可能会受到怎样的影响 。在美国,根据 WIPO 的要求,1998 年的数字千年版权法将规避版权保护机制定为违法行为,而在欧盟,2001 年的版权指令也有类似的效果。这被视为使供应商能够创建封闭平台并控制竞争;自由和开源软件运动以及安全研究人员也将其视为一种威胁 尤其是在俄罗斯研究员 Dmitri Sklyarov 应 Adobe 的要求在美国会议上被捕之后,因为他的雇主出售了绕过密码保护的工具在 PDF 文档上。

还有许多其他引人注目的事件;例如,当美国唱片业协会 (RIAA) 试图强迫项目主席撤回 Ed Felten 和他的学生描述版权漏洞的论文时,我是 2001 年信息隐藏研讨会的项目委员会成员标记方案被吹捧为数字音乐标准 [495]。 Ed 随后在具有里程碑意义的学术自由案件中起诉了 RIAA [620]。

具有讽刺意味的是,该计划的发起人曾向学术界和其他人发出公开挑战,要求打破它。下一个案例是 Bunnie Huang 的书“Hacking the Xbox”:这本书描述了作为一名麻省理工学院的学生,他是如何攻克第一版微软游戏机 [930] 中的保护机制的。

他写的这本书让他的出版商大吃一惊,但他找到了另一本书。
权利管理机制和反黑客法对自由的侵犯导致了数字权利非政府组织在许多国家的发展(其他国家已经因为“加密战争”而拥有它们;我将讨论

所有这些在第 26.2.7 节中有更详细的介绍）。

一个转折点出现在 2003-4 年,当时知识产权游说团体试图通过布鲁塞尔制定一项进一步措施,即知识产权执法指令。以其最初的形式,这将进一步加大对侵权者的处罚力度,并消除基于言论自由或合理使用的公共利益辩护的前景。

这一次,该措施的反对者设法组建了一个足够强大的对立利益联盟,该措施得到了实质性修改。

这种反对导致了第二年 EDRi 的成立,这是一个促进欧洲数字权利的非政府组织,并得到了欧洲几十个非政府组织的支持,他们意识到在布鲁塞尔进行游说是必不可少的。

知识产权游说团体的错误在于试图迫使欧洲每个国家将专利侵权定为犯罪,而不仅仅是民事案件。大型制药公司的目的是削弱那些在获得专利后生产低成本仿制药的公司。目前,药品专利持有人试图通过“长青”来延长他们的专利 申请附属的、后来的专利,通常带有可疑的衍生权利要求 仿制药制造商通过向他们的分销商提供赔偿金来应对这种情况,以免他们必须支付损害赔偿。将侵权定为刑事案件会破坏这些安排。这导致仿制药制造商以及超市、汽车零部件经销商和消费者团体强烈反对该指令。甚至软件行业也开始紧张起来:我们向微软指出,成千上万的公司认为微软侵犯了他们的专利,但没有钱在民事法庭上走到底。如果侵犯专利权构成犯罪,难道他们会去报警吗?比尔是否会在未来的欧洲之行中冒被捕的风险?当科技公司撤回支持时,将专利侵权定为刑事犯罪的尝试失败了。一个富有、强大的游说团体不会被花言巧语或大学教授和自由软件活动家的愤怒所阻止。当它遇到另一个向相反方向推进的富有、强大的游说团体时,它就停止了。

一些版权活动家希望,一旦版权到期 或者假设可以根据知识共享许可提供大量材料 那么一切都会变得平淡无奇。我对此表示怀疑。版权和专利背后的理论都是为创作者提供暂时的垄断,以增加创作的供应。最初版权是 18 年,然后是 35 年,然后是 50 年,然后是创作者的一生加上 70 年。愤世嫉俗者指出,每当米老鼠有失去版权的危险时,美国政府就会介入,增加版权期限,并胁迫其他政府采取行动。 （其他愤世嫉俗者指出,在克利理查德爵士让当时的首相托尼·布莱尔在他位于巴巴多斯的豪宅度假后,音乐表演的版权期限从 50 年延长到 70 年。）一些律师希望无限期延长版权期限,但那违反了版权所依据的社会契约,也没有解决保存问题:许多出版商未能妥善保管自己的旧目录,不得不从国家保藏馆藏中取回副本。

整理旧作品需要花钱,就像整理旧手稿一样;事实上,电影业最近发现,存档数字制作的成本实际上比他们过去支付的要高,当时他们只是把原版锁在一个旧盐矿里。只有太多的位

在数字制作过程中生成,每隔几年将它们复制到新磁盘并不便宜。从长远来看,一旦比特串不属于任何人,谁来支付维护费用?我们是否可以将现有的纳税人资助的存款图书馆系统扩展到数字资料?但由于多种原因,这些组织通常无法在数字材料方面取得很大进展,从缺乏理解到对版权法过于防御11。旧金山非政府组织互联网档案馆 (Internet Archive) 为子孙后代保存在线资料做出了非常值得称赞的努力,并且自 2006 年以来一直在运行一个开放图书馆项目。谷歌扫描了大学图书馆中的许多书籍,最终获得了一个在漫长的法庭案件后与作者和其他利益相关方的法律和解 12。因此,Google Books 可以搜索数百万册图书,并提供已失去版权的图书的全部内容。如果一本书仍然有版权,它可以让人们搜索和查看片段作为版权法允许的合理使用,但它不能在没有出版商同意的情况下出售电子版本。 （它本来想卖电子版的,只要给出版商固定的版税,就可以挑战亚马逊对图书市场的控制。） 2020 年的最新进展是图书出版商（包括 Wiley,出版商这本书)停止互联网档案馆借出电子版图书 [1000]。尽管发生了大流行,版权战争仍在继续。

24.5.2 谁受益?

正如我在第 8.6.4 节中提到的,版权战争的转折点出现在 2005 年。当年 1 月,Google 的首席经济学家 Hal Varian 在柏林的 DRM 会议上发表讲话,并询问谁将从更强大的 DRM 中受益。

他指出,在经典经济理论中,两个行业之间的技术联系通常会使集中度更高的行业（例如汽车制造商和汽车零部件)受益。但平台行业集中（当时是苹果、微软和索尼）,而音乐行业则不那么集中（四个专业和许多独立公司）:那么音乐行业为什么要期望成为更好的 DRM 的赢家?经济理论说,平台厂商应该赢得更多。音乐产业发展迅速,但到那年年底,他们受到了伤害 到那年秋天,他们泪流满面地游说英国政府和欧盟委员会对苹果公司“做点什么”,比如强迫它打开其 FairPlay DRM 方案。

在接下来的几年里,哈尔的预言成真了。音乐巨头失去了对苹果、亚马逊和 Spotify 等公司的市场支配力,而 Netflix 在视频分发方面确立了主导地位。音乐下载 有或没有 DRM 改变了音乐产业的结构和动态。

乐队过去依靠专业人士来宣传他们,但现在他们可以通过在网站上赠送专辑来自己做这件事;他们总是做

11当大英图书馆想要存档我们的非政府组织网页时,他们希望我们签署版权释放和赔偿表格,我们不能为来自第三方的材料或由已经离开或死亡的人撰写的材料做这件事。唯一可行的方法是将 stu 放到网上,如果有人提出令人信服的反对意见,就将其撤下。这就是科技公司所做的;遗留组织通常没有信心。

12The Authors Guild, Inc. 等诉 Google, Inc.； 2015 年 10 月 16 日（2d 巡回赛）;十一月 2013 年 14 日（SDNY）。

他们的大部分收入来自表演,现在他们赚的比以往任何时候都多 正如约翰·佩里·巴洛 (John Perry Barlow) 早在 1994 年就预测的那样。事实上,聪明的乐队现在拥有独立唱片公司,因为那时他们将获得更大的流媒体份额和其他收入。由于大流行,现在有一个快速增长的在线音乐会新部门,乐队在空旷的场地表演并向他们的粉丝直播,切断了订阅流媒体服务和拥有大场地的大公司 [1685].

24.6 附件控制

密码机制和权限管理技术最重要且增长最快的用途之一通常是附件控制。

故事始于 1895 年,当时 King Camp Gillette 发明了一次性剃须刀刀片,并从后来的刀片销售中补贴剃须刀。在吉列的记忆中,经济学家称这种策略为两部分定价,甚至简称为“剃须刀和刀片”模型。科技行业首先将其用于游戏机;然后它被打印机制造商采用,他们从 1996 年开始使用 Xerox N24 来补贴打印机的墨盒（有关墨盒芯片的历史,请参阅 [1822]）。

在典型的系统中,如果打印机检测到第三方墨盒或重新填充的墨盒,它可能会悄悄地从 1200 dpi 降级到 300 dpi,甚至根本拒绝工作。 2003 年,添加了有效期和墨水使用控制 [1207];现代墨盒现在以电子方式限制分配的墨水量,而不是等待它物理地用完。最新进展是区域编码:您不能在最近从英国购买的 HP 打印机中使用美国墨盒。

其他行业正在采用这项技术。例如,您可以在我们的实验室示波器中使用的 RAM 量取决于您为此支付的费用。

经过一番抱怨,欧洲监管机构决定容忍这一点,但在美国,此事由法庭决定。打印机制造商 Lexmark 起诉 SCC,后者对其打印墨盒加密进行了逆向工程,指控其违反了《数字千年版权法》。尽管他们在一审中获胜,但在 2004 年的上诉中败诉了 [1157]。在一个类似的案例中,张伯伦（制造车库门开启器的公司)起诉 Skylink（制造兼容开启器的公司)并且也败诉了,在 2004 年也失去了上诉。这使美国法律有利于密码学家的自由市场,这是之前的立场DMCA 出现了 [1647]。一家想要使用加密芯片控制其售后市场的公司可以自由雇佣它能找到的最聪明的密码学家来构建真正难以破解的认证芯片,而它的竞争对手可以自由雇佣他们能找到的最聪明的密码分析员来尝试进行逆向工程他们。

还有很多很多的例子。即使是过去从未使用过电子设备,并且出于任何目的都不需要电子设备的东西,也已经获得了芯片来实施掠夺性商业模式。有数百个例子:我在 2020 年修订本章时出现的一个例子是它们在 GE 冰箱的滤水器中的应用。在购买“智能”冰箱六个月后,Jack Busch 接到要求以 54.99 美元的价格购买另一个滤水器。事实证明,过滤水选项会自行关闭 ,除非您每六个月购买一个新过滤器,无论您是否需要。杰克适时想出了一个黑客

并出版了它 [353]。

附件控制是否令人反感?我在本书第二版中采用的观点是标准经济学的观点:取决于市场的竞争程度。如果墨盒的利润率很高,但打印机市场竞争激烈,竞争将压低打印机的价格以补偿高价墨盒 [1942]。但在许多其他行业中,它可能是反竞争的;它只取决于行业的集中程度,在赢家通吃的平台市场中,它可能特别令人反感 [73]。

从那以后我改变了主意。竞争很重要,随着一个又一个行业在其产品中采用软件并变得更像软件行业,我们看到它越来越少,具有我们在第 8 章中讨论的垄断趋势。例如,约翰迪尔现在符合其带锁的拖拉机限制授权经销商进行维修,这引起了农民的极大不满,因为他们不得不支付 230 美元的召回费用和每小时 135 美元的费用才能授权技术人员授权备件 [1070]。使用加密机制进行产品捆绑和捆绑是我们的政策制定者现在意识到他们必须处理的反竞争因素之一。就拖拉机而言,维修权法可能是必要的缓解措施之一。

可持续性也很重要,技术搭售机制通常会缩短产品寿命,导致不必要的消费。强制每六个月更换一次滤水器滤芯就是一个很好的例子;我们使用我们的大约五年。这种机制还导致产品易碎且难以维护。如果你买了一个“智能冰箱”,另一个常见的结果是,几年后,当供应商停止维护与之通信的服务器时,它就会变成一块结霜的砖。我将在 28.5 节中更详细地讨论这个问题。

covid 大流行说明了附件控制的其他副作用。
在封锁初期,一些医院没有足够的电池供重症监护临床医生使用的呼吸器使用,现在他们可以 24 x 7 不间断使用,而不是偶尔使用。市场领先的 3M 呼吸器和为其供电的电池都带有验证芯片,因此该公司可以以超过 200 美元的价格出售电池,而制造成本为 5 美元。医院很乐意以 200 美元的价格购买更多,但中国上个月将该工厂收归国有,3M 不会向其他组件供应商提供密钥。这种情况下的解决办法确实是竞争。其他供应商的呼吸器更便宜,而且不坚持使用专有电池,而在南安普顿,保罗·埃尔金顿 (Paul Elkington) 和医学院的同事设计了他们自己的呼吸器,使该设计向世界上所有想要制造它们的人开放 [623]。

幸运的是,3M 将失去他们滥用的市场主导地位,但在大流行的最初几个月里,没有足够的个人防护设备的临床工作人员付出了真正的代价。市场控制机制不仅对明天的可持续性有影响,而且对今天的安全也有影响。

24.7 总结

防止未经授权复制数字内容的技术保护在技术上和政治上都是一个棘手的问题。这在技术上很困难,因为通用计算机可以免费复制位串,而且在政治上也很困难,因为版权管理技术造成了很多附带损害。

音乐产业本身是受害者之一可能是公正的,但并不能解决持续存在的问题。这些与竞争、消费者保护和可持续性等更广泛和更深入的问题密切相关。

研究问题

2020 年围绕版权的许多棘手问题都是政策问题,而不是技术问题。如果您想从事信息隐藏或数字图像取证方面的技术工作,您可以阅读 Jessica Fridrich 的书作为起点 [724]。对于软件混淆,您可以从 2019 年 Dagstuhl 研讨会的报告开始,该研讨会由 Bjorn De Sutter 和 col leagues [555] 组织。一个跨越技术和政策的开放性问题是计算机游戏中使用的反作弊引擎的隐私。他们从您的 PC 收集什么信息,他们将这些信息发送到哪里,这是否合理?它甚至是合法的吗?

进一步阅读

像往常一样,卡恩是一本很好的历史背景读物 [1001]。 PC 时代的软件复制保护技术在 [829] 中进行了讨论; [1255] 中有付费电视系统的历史。至于信息隐藏,有 Katzenbeisser 和 Petitcolas [1023] 的书,以及 Jessica Fridrich 的书 [724]。

游戏安全性的标准参考由 Greg Hoglund 和 Gary Mc Graw [912] 编写;关于计算机游戏作弊的历史,另见 Je Yan 和 Brian Randell [2054, 2056]。

对于围绕版权和开放文化的政策问题的原则性讨论,您可以从 Pam Samuelson [1646, 1647] 和 Larry Lessig [1144, 1145] 开始。那么我建议您阅读与您相关的任何应用领域。如果你是一名学者,你应该读一读 Aaron Swartz 的悲剧 Reddit 的创始人在将数百万篇科学论文放到网上并被出版商的律师追捕后自杀 以及围绕 Sci-Hub 的长期斗争,这使得所有人都可以无视版权地获得科学论文。如果您为了赚钱而播放音乐,您可能想关注围绕流媒体的争论以及 Live Nation 和 Ticketmaster 之间的反垄断和解。如果您在酒吧播放音乐,您可能会对围绕爱尔兰音乐权利组织的争议感兴趣。

如果您是律师或政策制定者,最好与从事版权问题的非政府组织交谈。例如,欧洲数字权利 (EDRi) 的观点:“在数字环境中,公民面临来自国家的不成比例的执法措施,来自

公司和缺乏创新产品,所有这些都加深了人们对失败和非法法律框架的印象,破坏了创作者与他们所生活的社会之间的关系。版权需要从根本上进行改革,以符合目的,可预测对于创作者来说,灵活且可信。”