Machine Translated by Google

第28话

保证和
可持续性

有两种构建软件设计的方法。一种方法是让它变得如此简单,以至于显然没有任何缺陷。

另一种方法是让它变得如此复杂以至于没有明显的缺陷。

– 托尼霍尔

安全工程师是科技的诉讼律师。
我们只有在出现问题时才会得到报酬,而且我们总能找到问题所在。

– 戴夫韦斯顿

改进就是改变;完美就是经常改变。

- 温斯顿·丘吉尔

28.1 简介

我在本书中涵盖了很多材料,其中一些非常棘手。但我把最难的部分留到了最后。这些是保证的问题 系统是否会工作;它的表亲合规性 你如何让其他人满意;和可持续性 它将持续工作多长时间。您如何决定运送产品?您如何将安保和安全案例出售给您的保险公司?

您需要维护多长时间,费用是多少?

2020 年的新变化是可持续性。在 2008 年版中,我将这一章称为“评估与保证”,并在结尾指出漏洞披露和产品更新的完善流程开始与上市前测试一样重要。当时的重点是像通用标准这样的测试和评估方案。那个世界现在已经奄奄一息:因为五年前有人花了 100,000 美元找了一个评估实验室来测试设备就应该是安全的,如今大多数人会觉得这种想法很古怪。

Machine Translated by Google

保证不再是静态的。

十年前,我们知道如何制作两种类型的安全系统。我们有电话和笔记本电脑之类的东西,它们包含软件并且可以在线,但由于软件每月打一次补丁,所以有点安全。我们有汽车和医疗设备之类的东西,它们包含软件但不在线;您在将它们出售之前对它们进行了死亡测试,然后希望获得最好的结果,因为修补意味着物理召回。现在我们已经开始把汽车和医疗设备放到网上,所以它们也必须在网上打补丁。

常见平台中报告的漏洞数量如此之多,以至于我们必须自动化该过程。正如我们在上一章中所描述的,软件开发生命周期已经变成了 DevOps,然后是 DevSecOps;系统的在线组件使用持续集成进行维护,而外地组件需要定期升级。

对于新产品,可以通过有能力、有动力的人是否对系统进行足够的打击来粗略地衡量保证。但是你如何定义“足够”?您如何定义“系统”?你如何对待保护错误事物的人?你如何处理可用性?太多的系统是为经验丰富的专业人士设计的,但对于普通人来说太棘手或者不能容忍错误。一旦他们上场,伤害索赔或欺诈纠纷就会开始滚滚而来。

在十年前的安全工程中,我们经常从评估的角度谈论保证,这是关于你如何收集证据来说服你的老板、你的客户和(如果需要的话)陪审团,它确实有效(或者它在过去的某个特定时间确实有效)。正如我们一再看到的那样,事情往往会失败,因为一位委托人承担了保护成本,而另一位委托人则承担了失败的风险。通用标准等第三方评估计划本应使这些风险更加透明并减轻风险,但最终却充当了责任盾 尤其是在公共部门和银行业等受监管行业。保护机密信息的系统需要满足广泛的合规要求,并且必须在攻击面使用经过评估的产品;对于支付系统,情况大致相同,只是细节有所不同。评估是由合规性驱动的。

合规性仍然是安全设计和投资的主要驱动力,但它不太重视在特定信任边界要求经过评估的产品。细节因行业而异。当我们审视医疗系统、汽车或飞机时,我们会发现由安全驱动的监管制度开始将安全纳入其中。一般业务系统的政策由四大审计公司制定,支付系统由 PCI 制定。我们在前面的章节中谈到了他们的一些具体要求;我们将在这里尝试整合一些更广泛的问题和原则。

在本书的开头,在图 1.1 中,我提出了一个框架
基于激励、政策、机制和保证的安全工程。

- 正如我们一再看到的那样,激励措施至关重要。它们通常不属于正式的保证过程,但却是必须在其中定义安全策略的环境中最关键的部分。

- 政策经常被忽视,正如我们所见:人们往往最终保护

Machine Translated by Google

错误的事情,或者以错误的方式保护正确的事情。我们在本书的第 II 部分花了很多时间探索不同应用程序的安全策略。

- 机制可能独立于政策,但可以通过使某些政策选项更易于实施而与其相互作用。

- 保证是我们对系统不会以特定方式发生故障的可能性的估计。该估计可以基于许多因素,例如用于开发和维护它的过程;开发和维护它的人;以及具体的技术评估,例如故障率、错误报告、违规报告和保险索赔的统计数据。传统上它是关于评估的 考虑到商定的安全策略和机制的强度,产品是否得到了正确的实施。

错误是否已被发现并修复?你能量化平均故障时间吗?如今,它越来越多地与供应商的未来承诺有关。

系统会修补多长时间,修补的力度有多大?

到 2008 年本书的第二版时,我注意到最大的缺失因素是可用性。大多数系统故障都有重要的人为因素。

可用性是上述框架中的一个交叉问题:如果处理得当,它对政策有微妙的影响,对机制的选择有很大的影响,对系统的测试方式有很大的影响。它跨越单个产品:事故的一个常见原因是不同的产品有不同的用户界面,我们稍后会回到这个问题。然而,设计者往往将保证简单地视为没有明显的错误,并在设计技术保护机制时没有停下来考虑人的弱点。 (有一些例外:簿记系统旨在应对错误和欺诈。)

可用性不仅仅是最终用户的问题,也是开发人员的问题。许多漏洞的出现是因为安全机制太难理解或太难使用。开发人员通常不使用操作系统访问控制,而只是以管理员权限运行他们的代码;当手机不允许这样做时,他们会不断要求他们的应用程序获得太多权限;密码学通常使用 ECB 模式,因为它是许多加密库的默认模式。

客户和供应商在价值链的多个点需要不同的东西。监管并不总是有帮助,因为政府有自己的多个议程,而且经常相互冲突:情报机构、安全监管机构和竞争主管部门各执一词。保险游戏就是在这个险恶的环境中上演的。

因此,保证是一个政治和经济过程。它也是一个动态过程,就像代码或文档的开发一样。正如您的代码和规范中存在错误一样,您的安全和安全策略也会出现问题,从而导致测试套件中出现遗漏和错误。因此,保证正在稳步从作为一个单一的项目完成的事情转变为持续发展的另一个方面。

有了这个警告,从评估的经典问题开始是有帮助的
在单个项目中构建的静态产品。

Machine Translated by Google

28.2 评价

产品评估解决了我们在 8.3.3 节中讨论的柠檬市场问题:当客户无法衡量质量时,劣质产品会驱逐优质产品。几代人以来,安全一直是柠檬市场。 1853 年出版的一本关于锁匠的书以窃贼已经知道为由公开了这一行业的“秘密”。只有锁匠的顾客是无知的 [1895]。现代消费级产品,从防病毒软件到手机应用程序,在技术上远远超出了大多数消费者的评估能力。如果他们只是依赖品牌名称,供应商还不如购买广告而不是雇佣安全工程师。至于专业产品,科技专业可能会聘请足够多的博士来进行评估,但银行不会 甚至货币中心银行也不行1。在前面的章节中,我们讨论了一些静态安全标准示例,各种产品都根据这些标准进行评估和认证。银行和政府是认证安全产品最热衷的购买者之一。

这可能是 50 年前计算机安全起步的地方,但随着计算机最终无处不在,我们也必须看看其他行业。数十个行业都有自己的安全标准,安全机制越来越多地与这些标准交织在一起。我们已经在第 23.8.1 节中讨论过电力传输和分配。道路车辆软件的安全标准已经发展了数十年;我们在 14.3.3 中谈到了卡车。现在卡车和汽车都有多个辅助驾驶系统并连接到互联网,因此它们具有关键的安全性和安全性要求。同样的情况也发生在医疗设备和其他许多方面。

我将通过一些案例研究来探讨这一点。两个重要的问题是评估是由依赖方还是第三方进行,标准是静态的还是动态的。

28.2.1 警报和锁

美国保险业于 1894 年成立联合测试实验室,警惕电灯泡的火灾隐患;它于 1901 年作为 Underwriters Laboratories 成立,这是一家制定消防安全和其他标准的非营利组织,并于 1913 年 [1916 年] 开始批准安全产品。其他国家也有类似的机构。评估人员花费固定预算的精力寻找缺陷并撰写报告,之后实验室要么批准设备,要么拒绝它,要么要求进行一些更改。

由于保险业承担了火灾和盗窃的大部分成本,因此激励措施在某种程度上是一致的,尽管在实践中这些实验室的大部分收入来自测试费。一种风险是惰性:标准可能跟不上进步。对于高安全性的锁,2000 年的实验室可能会要求 10 分钟的防撬时间,更不用说碰撞了。

我们在第 13.2.4 节中描述了碰撞工具如何改进到足以成为

1 在我 20 多岁和 30 多岁的时候,我在银行业工作,当我去银行间安全标准委员会时,房间里只有大约四个人知道我们在说什么 其中一个来自 IBM。从那时起,金融科技变得复杂了一个数量级。

Machine Translated by Google

到 2010 年成为主要威胁,而且选秀权也变得更好了。我们还在第 13.2.3 节中描述了经认证可抵抗攻击 10 分钟的银行金库如何被现代角磨机或燃烧棒在更短的时间内摧毁。一些国家（例如德国)的保险实验室已经准备好在攻击变得更好时撤销认证;在美国,他们似乎不愿意这样做,也许是因为害怕被起诉。一个行业容忍不断变化的标准的意愿可能取决于它的结构:一个拥有少数大公司的成熟行业比一个不断发展的竞争性行业更容易拖泥带水。

28.2.2 安全评价制度

为了应对重大事故或丑闻,安全标准往往一次出现一个行业。在美国,药品和医疗器械的安全由 FDA 监管,该机构于 1906 年由西奥多·罗斯福总统在记者揭露专利药品行业的滥用行为后成立。事实证明,美国最畅销的药物只是一种硫酸和松节油的稀溶液 制造起来确实很便宜,但味道却很糟糕,以至于人们相信它对他们有好处 [2050]。至于航空安全,第一步是在1931年,当时美国顶级橄榄球教练克努特·罗克尼因结构故障导致飞机失事身亡,引发舆论哗然,国家运输安全委员会成立。在 1956 年两架客机在大峡谷上空坠毁导致两架飞机上的 128 人全部遇难后,艾森豪威尔总统后来成立了美国联邦航空局 [684]。至于汽车行业,它几十年来一直设法不承担安全责任。供应商竞相用铬来装饰汽车,而不是为汽车安装安全带,直到拉尔夫纳德 (Ralph Nader) 的书《任何速度都不安全》促使国会于 1970 年成立国家公路交通安全管理局 (NHTSA);它的权力和影响随着接二连三的安全丑闻而增长。

欧洲于 1985 年将一系列国家法律整合到产品责任指令中,按行业部门增加了进一步的法规和安全机构。从那时起,欧盟已发展成为世界领先的安全监管机构,其机构制定了从航空、铁路信号到玩具等行业的安全标准 [1148]。以汽车为例,欧洲通常要求由独立实验室2进行安全测试,而美国则不需要;但大多数美国供应商也对他们的美国模型进行了独立测试,因为欧洲制定了“行业规范” ,美国法院在出现问题时根据该规范评估侵权案件。从这个意义上说,欧洲已经成为“监管超级大国” 。

欧盟的总体安全战略是通过与行业工作组和游说者协商制定一套标准,并每七到十年更新一次。许多造成严重危害的产品,例如汽车,必须获得明确的批准,通常是在独立实验室进行测试之后。玩具等危险性较低的商品需要自我认证:供应商在产品上贴上“CE”标志,以声明其符合所有相关标准。

这消除了供应商在不合规时可能使用的一些借口

2 欧洲将型式批准委托给成员国,其中大多数拥有型式批准机构,将测试委托给专业实验室。在德国,这是 TUV。一些较小的国家/地区拥有 TAA,允许制造商在 TAA 检查员在场的情况下进行自己的测试。

Machine Translated by Google

产品造成事故;它还用于从汽车制动器到工业压力阀的各种组件。

28.2.3 医疗器械安全

安全监管是一个复杂的生态系统,在许多方面都不完善。例如,医疗器械安全问题在欧美一直存在争议。这在 1980 年代变得突出,当时 Therac 25 医疗加速器中的错误导致三名患者死亡,另外三名患者受伤。

原因是一个软件错误,该错误表现为可用性问题:如果操作员太快地编辑机器的参数,他们可能会使机器进入危险状态,从而向患者提供过多的辐射。即使在今天,这个案例研究也是我的软件工程专业学生的固定读物 [1149]。

图 28.1：- 两个显然是同一型号的输液泵（图片由 Harold Thimbleby 提供）

当今最致命的医疗设备可能是输液泵,用于给医院的病人静脉注射药物和其他液体。许多致命事故都是可用性故障。看看图 28.1:这些都声称是“BodyGuard 545”,但要增加左侧机器的剂量,您按“2”,而在右侧按“5”。急诊室可能有来自六家不同供应商的设备,所有这些设备都具有不同的用户界面。医生和护士偶尔会按错按钮,输错剂量,或者将八小时输血的剂量一次输完 然后患者就会死亡。输液泵造成的死亡人数与汽车造成的死亡人数差不多,英国的死亡人数为数千人,美国的死亡人数为数万人 [1878 年]。

这当然可以用标准来解决吗?嗯,有标准。例如, litres 应该用大写字母 L 标记,所以它不会被误认为是 1 ,但您可以在右侧图像中看到,虽然 0L/h 符合此要求,但 500ml 没有。那么为什么不强制执行该标准呢?

好吧,FDA 的工程工作预算大约是每台设备半天,而且供应商不会给工程师实际的设备来玩。这只是一份文书工作审查 3。此外,可用性不属于 FDA 的范围。这个

3通过比较,当我和同事帮助评估专为小型商店和房屋等低后果风险设计的防盗警报器时,我们的预算是两个人-周。

Machine Translated by Google

我听说,这是行业游说“减少繁文缛节”的结果。将两种不同的设备作为同一产品销售是将合规成本降至最低的常见策略。

最近以 ISO/IEC 62366-2 的形式出现了医疗器械可用性工程的国际指南,该指南于 2018 年生效。

这是一个重大的进步,涵盖了很多领域,但可用性是一个巨大的领域。新标准非常基础,并详细解释了制造商不应该只是在法律警告传单中列出危险,甚至在设备上用告示突出它们 他们应该真正尝试减轻它们,并在这个过程中了解他们的设备如何很可能被使用和滥用。

它描述了工程师可以使用的许多评估技术,但“对医疗设备类型的经验不足”只是其可能导致使用错误的因素列表中的一个要点。制造商会发现所有这些都很昂贵,并且毫无疑问会与他们的律师讨论真正需要做的事情。仅数字输入的安全性是一个复杂的领域 [1879];每个供应商可能都应该培训这方面的专家,以及许多其他技术,但许多供应商只会尽可能少地做他们认为可以逃脱的事情。最后,可用性评估现在将包含在制造商提交给监管机构的大量文书工作中,至少在美国以外是这样。但尚不清楚当护士也使用竞争对手设备的不同界面时所产生的混乱是否会得到应有的重视。

这一切都在告诉我们,上市前测试不足以确保医疗设备安全 您还需要勤奋的上市后监督。在有关有缺陷的乳房植入物的丑闻之后,这于 2017 年开始在整个欧洲引入 [233]。在英国,关于致畸药物和盆腔网状植入物的进一步丑闻引发了独立药物和医疗器械安全审查,该审查在 2020 年记录了数十年来对安全的漠视,并在许多其他事项中建议监管“需要进行实质性修订,特别是与不良事件报告和医疗器械监管有关 [503]。 2020 年 5 月,一项新的欧盟医疗器械法规 (2017/745) 应该要求上市后监控系统和匿名事件报告的公共数据库;实施推迟到 2021 年 5 月。

而在 2020 年 6 月,英国议会通过了一项药品和医疗器械法案,该法案将使大臣们能够在英国退欧后修改现有法规。
然而,那里的情绪音乐是为了让英国成为对制药公司和医疗设备制造商更具吸引力的地方,而不是让患者更安全的地方。
在英国的国民健康服务体系中,安全专家很难成为职业4。

现在这是一个有趣的问题。如果输液泵杀死的人和汽车一样多,或者 在美国 和枪支一样多,为什么人们不更加努力,因为他们关心道路安全和枪支管制?好吧,危害既低调又分散。在您当地的医院,此类事故每月可能导致不到 1 人死亡,而且其中许多人不会被注意到,因为使用输液泵的人往往病得很重。当他们被发现时,他们更有可能被归咎于护士,而不是购买泵的医疗主任

4英国 NHS 于 2016 年成立了医疗保健安全调查部门,但它会调查被告知的内容,通常必须对其调查结果保密,并且没有或寻求强制执行权力来要求其他医疗保健组织进行更改 [875] .

Machine Translated by Google

在与销售人员共进午餐后,来自六家不同的供应商。
作为医院的死亡原因,记录在案的安全可用性故障不会进入前 20 名,因此不会引起政治家或媒体的关注。

（例外情况是安全故障具有安全角度,因为人们确实对敌对意图非常敏感。我将在下面的第 28.4.2 节中讨论这个问题。）

在事故及其原因更为明显的行业中,用户界面的标准化得到了更好的管理。道路交通事故相当明显,而且大多数人都会开车,因此车祸及其原因是人们谈论的话题。现在汽车的控制是相当标准的,油门在右边,刹车在中间,离合器在左边。事情并不完美;如果你赶时间,你可能会租一辆汽车,沿着高速公路行驶 o ,然后在夜幕降临时努力寻找电灯开关。但它曾经更糟。 1930 年代的一些汽车在中间有加速器,而第一辆量产汽车 Model T Ford 有一个手油门和踏板换档,就像摩托车一样。普通的现代司机很难从租来的停车场租到这样的车。

28.2.4 航空安全

航空业仍然有更强大的安全激励措施:客机价值八九位数,坠机事故是头版新闻,导致飞行员和乘客丧生,航空公司首席执行官甚至可能失去奖金。飞行员会注意事故报告,并且需要在他们驾驶的每种飞机上进行训练。这导致供应商对驾驶舱设计进行标准化,从波音 757 和 767 开始,它们从一开始就设计得非常相似,以至于接受过其中一架培训的飞行员可以驾驶另一架。如果同样要求护士对每个输液泵进行类型评级,那将花费真金白银,医院高管会关注,供应商最终会效仿波音公司,并且可以挽救很多生命。

然而,我们也发现航空监管失灵,波音 737Max 坠机事件就是一个例子。自从波音公司在 1997 年收购了 McDonnell Dou Glas 并成为美国唯一一家制造大型飞机的公司后,美国联邦航空管理局开始认识到它在支持波音方面的作用。该公司的工程师被允许接手美国联邦航空局过去所做的大部分安全评估和认证工作。收购的一个更有害的影响是麦克唐纳道格拉斯的高管接手,公司将总部从西雅图搬到了芝加哥,不再由工程师管理,而是由财务人员管理,他们已经摧毁了一家工程公司,他们的目标是现在是从新的垄断中榨取最大的利润。波音公司的传统工程文化被边缘化,被偷工减料 [729]。随后在印度尼西亚和埃塞俄比亚发生了两起坠机事故,造成 346 人死亡。原因让人想起上一代的 Therac 案例:软件中的设计错误表现为危及生命的可用性故障。

为了与最新型号的空中客车公司竞争,波音公司需要尽快提高 737 的燃油效率,这意味着必须在更靠前的位置安装更大的发动机,否则就需要重新设计机身,以至于出于监管目的,这将是一架新飞机,并且需要更长的时间才能获得认证。新的发动机位置使飞机

Machine Translated by Google

高速时更难配平,因此波音公司在飞行控制计算机中添加了称为机动特性增强系统 (MCAS) 的软件以弥补这一点。

MCAS 软件需要知道飞机的迎角,关键的设计错误是依赖一个迎角传感器而不是两个,尽管这些传感器经常被地面操作员和鸟击损坏。实施错误是,如果迎角输入不正确,飞机可能会进入飞行员需要在操纵杆上拉大约 50 公斤的重量以保持飞机水平的状态。安全分析中的错误使情况更加复杂:未预料到 MCAS 软件的意外激活。结果,波音公司没有进行适当的故障模式和影响分析,软件的行为甚至没有记录在飞行员手册中。飞行员没有接受过如何诊断问题或将 MCAS 关闭 的培训。波音公司对飞行员应对驾驶舱紧急情况的能力感到自满,因为许多警报同时响起 [1055]。

该公司还因 2009 年在荷兰发生的一起类似坠机事件而逃脱了欺凌调查人员的惩罚,并最初希望将印度尼西亚坠机事故归咎于飞行员失误 [857]。美国联邦航空局通过向所有已知的美国飞机运营商发送紧急适航指令来应对坠机事故,其中包括在飞机飞行手册中插入警告通知 [665]。 ;然而,警告飞行员两个传感器之间存在分歧的警告灯已成为航空公司的一个选项,就像汽车的天窗一样,并且可以禁用 MCAS 的开关的操作被改变以使其不那么直观 [155]。一些美国飞行员记录了投诉,其中一位将手册描述为“几乎是犯罪性的不足”[139];但美国联邦航空局认为此类投诉仅与航空承运人的运营有关,并未对它们进行全球安全危害分析 [664]。

在埃塞俄比亚发生第二次坠机事故后,其他国家的监管机构开始将 737Max 停飞,FAA 无法再保护他们。到 2020 年 3 月冠状病毒大流行关闭了商用航空销售,波音公司的销售额损失了 187 亿美元,市值损失了 600 亿美元。就生命损失和经济损失而言,这在一定程度上是世界上有史以来最大的软件故障。该修复于 2020 年 8 月获得批准,不仅涉及软件更改,以便 MCAS 读取两个迎角传感器,并且每次飞行仅部署一次,并且杆力有限;但是程序上的变化,以便在飞行前检查两个传感器;飞行员培训的更新;以及法规变更,以便 FAA 而不是波音公司在制造后检查每架飞机 [592]。

在分析安全性时,仅将其视为技术测试问题是不够的。心理、激励、制度和权力也很重要。游说者的力量,以及监管者被他们应该监管的行业所控制的风险,对测试制度可以实现的目标设置了真正的限制。随着时间的推移,为风险评估和降低风险而设计的措施变得工业化,并趋向于成为合规问题,然后公司寻求以最低成本通过。停止将问题视为“航空航天工程”与“软件工程”或“安全工程”与“安全工程”的区别也很重要。如果你想成为一名优秀的工程师,你需要尝试理解整个系统的每个方面

Machine Translated by Google

可能是相关的。

28.2.5 橙皮书

第一个严肃的计算机安全测试制度是橙皮书 可信计算机系统评估标准 [544]。我们在 9.4 节中谈到了这一点,我在那里描述了美国国防部试图通过它推广的多级安全模型。橙皮书评估于 1985 年至 2000 年在美国国家安全局进行,评估对象是建议供政府使用的计算机系统和加密设备等安全产品。在激励方面,这是一个集体依赖方计划,就像保险一样。

橙皮书及其配套文件分三个等级列出了多个评估等级。 C1 意味着有一个访问控制系统； C2 对应于精心配置的商业系统。在下一个频段中,B1 表示强制访问控制； B2 添加了隐蔽通道分析、从用户到 TCB 的可信路径以及严格的渗透测试;而 B3 要求 TCB 必须是最小的、防篡改的,并接受正式的分析和测试。在最高频段,A1 添加了形式验证的要求。 （很少有系统达到那个水平。）

系统的评估等级决定了可以在其上处理的信息传播范围。我在第 9.6.2 节中给出的示例是,评估为 B3 的系统可以处理未分类、机密和机密或机密、机密和最高机密的信息。

在编写橙皮书时,国防部认为他们为高保证计算机支付高价是因为市场太小,希望通过安全标准扩大市场。但橙皮书评估遵循政府工作惯例。政府用户会希望对某些产品进行评估;国安局会派人去做;鉴于传统的公务员谨慎和拖延,这可能需要两到三年的时间;该产品如果成功,将加入评估产品列表;账单被纳税人捡走了。评估过的产品总是过时的,所以市场很小,价格也居高不下5。

其他政府也有类似的想法。欧洲国家制定了信息技术安全评估标准 (ITSEC),这是一项旨在帮助其国防承包商与美国供应商竞争的共享计划。这引入了一个有害的创新 评估不是由依赖方（政府)安排的,而是由供应商安排的。供应商开始货比三家,寻找可以让他们的产品最轻松运行的实验室,无论是通过提出更少的问题、收取更少的费用、花费最少的时间,还是以上所有。

承包商可以获得商业许可评估机构 (CLEF) 的批准,理论上,如果 CLEF 偷工减料,其许可证可能会被撤销。从未发生过。

5 直到今天,大多数政府都没有希望购买技术并支付数倍于市场价格的费用,如果他们使它发挥作用的话。原因比标准更广泛、更深刻。例如,请参见第 10.4.4 节关于耗资 110 亿英镑的英国国家卫生服务现代化项目的失败,以及第 23.5 节关于耗资 60 亿美元的五角大楼联合战术无线电系统的失败。

Machine Translated by Google

28.2.6 FIPS 140 和 HSM

20世纪美国政府推行的第二个评估方案是NIST的FIPS 140方案,用于评估密码处理器的防篡改能力。这旨在帮助银行业和政府,正如我在第 18.4 节中所述,它使用许多独立实验室作为承包商。 1994年推出至今风头正劲,深受美国密码设备客户青睐。

FIPS 140 有两种主要的故障模式。第一种是它涵盖了加密设备的硬件,而不是其软件,而且许多 FIPS 140 评估设备（即使是最高级别的设备)运行的应用程序都存在内在漏洞。如第 20.5 节所述,银行标准机构强制要求弱算法、遗留操作模式和易受攻击的 API 以实现向后兼容性。解决这个问题的方法是越来越重视支付行业的自律计划 PCI 制定的标准,我在第 12.5.2 节中对此进行了描述。

第二个是 FIPS 140-1 标准由于历史原因在第 3 级和第 4 级之间存在很大差距,我在 18.4 节中讨论过。 FIPS 140 3 级很容易获得（您只需将电路封装在环氧树脂中,使其无法随意探测)并且一些 3 级设备不太难损坏（您只需用刀刮掉 环氧树脂）。 4 级真的很难,只有少数设备达到了这个等级。许多供应商的目标是业界非正式地称为“3.5 级”。由于这在 FIPS 标准中没有任何正式表达,公司在与美国以外的客户交谈时通常依赖通用标准。

28.2.7 通用标准

这为通用标准奠定了基础。 1989 年苏联解体后,军事预算被削减,未来的对手会从何而来尚不清楚。最终,美国及其盟国同意废除其国家计划,代之以单一标准 信息技术安全评估通用标准 [1396]。

这项工作在 1994-1995 年基本完成,欧洲 ITSEC 模型战胜了橙皮书方法。除最高级别外的所有评估均由 CLEF 完成,应该在所有参与国家/地区得到认可,供应商为此付费。

创新是支持多种安全策略。通用标准并不期望所有系统都符合 Bell-LaPadula,而是根据保护配置文件 (PP) 评估产品,保护配置文件是针对一类产品的一组安全功能要求和保证要求。您可以将其视为详细的安全策略,但面向产品而不是系统,并扩展为几十页的详细信息。操作系统、访问控制系统、边界控制设备、入侵检测系统、智能卡、密钥管理系统、VPN 客户端、投票机,甚至是识别家庭垃圾桶最后一次清空时间的转发器都有保护配置文件。任何人都可以提出保护概况并对其进行评估

Machine Translated by Google

由他们选择的实验室。这并不是说国防界放弃了多级安全,而是试图通过让商业公司也将其用于其他目的来使其自己的评估系统成为主流。但评估完全取决于衡量的内容和方式。安全的某些方面被明确排除在外,包括密码学、发射安全（因为北约标准被分类)和管理程序（这对可用性测试来说是个坏消息）。

通用标准取得了一些有限的成功。其评估用于智能卡、硬件安全模块、TPM 和电子签名设备等专业市场,在这些市场中,行业尽职调查规则（如 PCI)或法规（如电子签名法)提出了合规要求。由 SOG-IS（高级官员组织 信息安全） 欧盟国家情报机构代表组成的委员会 运营的非正式卡特尔,对此类设备的评估在一段时间内保持诚实。

然而,CC 在欧洲以外的运作有点像个笑话,甚至在欧洲内部,它也被公司和国家利用该系统进行破坏。英国于 2019 年退出。

28.2.7.1 血淋淋的细节

要详细讨论通用标准,我们需要一些行话。被测产品称为评估目标 (TOE)。进行检查的严格程度是评估保证级别 (EAL),范围可以从 EAL1（功能测试已足够)一直到 EAL7（不仅需要全面测试,还需要经过形式验证的设计）。商业产品通常获得的最高评估级别是EAL4,尽管2020年在CC认证的1472个产品中有85个产品达到EAL6或以上,并且许多智能卡被评估为EAL4+,即EAL4加上一项或多项更高的要求水平。

从头开始设计时,想法是首先制定威胁模型,然后创建安全策略,将其细化为保护配置文件 (PP) 并对其进行评估（如果合适的配置文件尚不存在） ,然后执行同样的安全目标,然后最后评估实际产品。保护配置文件由安全要求、其基本原理和 EAL 组成,所有这些都针对一类产品。它应该以独立于实现的方式表达,以实现跨产品和版本的可比较评估。安全目标 (ST) 是针对特定产品的保护配置文件的改进。人们可以评估 PP 以确保其完整、一致且技术上合理,ST 也是如此。评估结果提交给国家当局,后者通常是当地信号情报机构的防御部门。最终结果是注册保护配置文件和认证产品目录。

有一种写 PP 或 ST 的程式化方式。例如,FCO_NRO 是与通信 (CO) 相关的功能组件（因此称为 F） ,它指的是不可否认来源 (NRO)。其他类别包括 FAU（审计)和 FCS（加密支持）。

还有目录

· 威胁,例如 T.Load_Mal – “数据加载故障:攻击者

Machine Translated by Google

可能会恶意地在设置数据中产生错误,从而危及 TOE 的安全功能”

- 假设,例如 A.Role_Man –“角色管理:TOE 的角色管理以安全的方式执行”(换句话说,开发人员、运营商等自行其是)

- 组织政策,例如 P.Crypt_Std “加密标准:加密实体、数据认证和批准功能必须符合 ISO 和相关行业或组织标准”

- 目标,例如 O.Flt_Ins –“故障插入:TOE 必须能够抵抗通过插入错误数据进行的重复探测”

- 保证要求,如 ADO_DEL.2 “修改检测:开发者应记录将 TOE 或其部分交付给用户的程序”

保护配置文件现在应该包含一个基本原理,它通常由表格组成,显示每个威胁如何被一个或多个目标控制,以及在相反的方向上,每个目标如何被威胁和环境假设的某种组合所必需。它还将证明选择保证级别和机制强度要求的合理性。

掌握这一点的最快方法可能是阅读核心 CC 文档本身,然后是一些概要文件。质量差异很大。例如,自动提款机的保护配置文件,用管理语言编写,带有剪贴画,“选择不包括任何安全策略”,并且遗漏了许多在 1999 年编写时众所周知的问题 [340]。 2007 年的投票机配置文件 [563] 更多是用政治家的语言写的,但至少清晰度合理 6。

智能卡的保护配置文件强调通过对承包商施加 NDA、粉碎废物等来维护芯片设计的机密性 [650],而在实践中,大多数对智能卡的攻击使用探测或功率分析攻击,而芯片掩码的知识与此无关。正如我在第 18.6.4 节中讨论的那样,这已经发展成为一场政治争端:智能卡供应商已经推动评估实验室要求所有加密产品都能够抵御“高级持续威胁”。战斗已经结束,因为保证要求 AVA_VAN.5 本质上要求整个开发环境应该是气隙的,就像情报机构的绝密系统一样。气隙本身并不能阻止有能力的对手,正如伊朗人发现 Stuxnet 和美国人发现斯诺登一样。但它给依赖 Github 和其他基于云的系统的普通 IT 公司带来了真正的不便。这就是重点:智能卡公司不希望 HSM 或 enclaves 侵占他们的市场。

6这似乎是为了支持法国公司出口人口登记系统的动力,正是这些而不是实际的投票机才是选举中真正的弱点 正如我在第 7.4.2.2 节中讨论的那样。

Machine Translated by Google

28.2.7.2 通用标准出了什么问题

到 2008 年本书第二版问世时,业界人士对通用标准有很多抱怨,我在那里讨论了它,我在这里更简要地更新了它。

- 多年来最大的抱怨是流程的成本和官僚作风。如今,想要销售 HSM 等设备的初创公司将不得不花费数百万欧元和数年的努力来完成这一过程。在实践中,CC 已经成为保护已建立的卡特尔的护城河。

- 下一个最大的问题是,除了避免“技术物理”方面(例如 Emsec 或加密算法)之外,CC 还忽略了管理安全措施,这意味着实际上忽略了可用性。通常,用户界面被认为是别人的问题。

- 保护配置文件由其赞助公司设计以操纵市场。
  我在上面提到了智能卡公司如何要求 HSM 供应商也使用气隙系统来推高他们的成本。游戏通常会导致不安全的产品:供应商编写他们的 PP 来涵盖他们可以轻松完成的事情。他们可能会评估引导代码,但会将大部分操作系统留在范围之外。回忆一下 20.5 节中描述的对 HSM 的 API 攻击;一些易受攻击的 HSM 已通过 CC 认证,类似的故障也出现在其他 CC 认证产品中。

- 有时保护配置文件可能是合理的,但它们映射到应用程序的方式却并非如此。在第 26.5.2 节中,我讨论了欧洲 eIDAS 法规,该法规要求企业识别使用智能卡制作的数字签名性质,并鼓励政府要求它们进行交互,例如提交纳税申报表。正如我在第 18.6.1 节中讨论的那样,此应用程序的主要问题是缺少可信接口。由于这个问题太难了,所以它被排除在外,最终结果是在您的 PC 中发送到您的智能卡的任何病毒或特洛伊木马上都有一个“安全”签名。这个洞适当地涂上了几层软糖。 PP 是为智能卡编写的,用作“安全签名创建设备”;其他 PP 出现在 HSM 和签名激活模块 (SAM) 中 将要签名的数字对象传递给它们的服务器软件。 HSM 加上 SAM 被评估为合格的签名创建设备 (QSCD) [29]。但服务提供商使用的前端服务器软件仅经过审核,未经过认证,如果幸运的话,手机或平板电脑上的应用程序可能会安装 RASP 作为恶意软件反制措施,正如我在第 12.7.4 节中讨论的那样.这就是游说者可以实现的目标:整个认证机制已被扭曲以允许帐篷内的 Docusign 等服务,只要他们使用 CC 认证的 HSM 来保存他们的签名密钥。

- CC 声称不采用任何特定的开发方法,但实际上采用瀑布方法。根据经验,政策的发展方向得到了认可,但宣布对 PP 或产品的重新评估不在范围之内。所以他们无法应对

Machine Translated by Google

正常的安全开发生命周期,或者使用每月获得安全补丁的商业产品。 （FIPS 也是如此;在可用的标准中,只有 PCI 可以应对更新。）

- 标准是技术驱动的,而在大多数应用程序中,业务流程应该推动保护决策。我们正在通过艰难的方式了解到,出于各种原因,手工标记的纸质选票比投票机要好得多。安全是系统的属性,而不是产品的属性。

- 评估的严格程度因国家而异,德国通常被认为是几乎不可能的困难,荷兰则处于中间位置,而西班牙和匈牙利则让他们的 CLEF 轻松应对。体制内没有人能在不引起外交事件的情况下真正公开说这话,所以它无法修复。费用也各不相同,在德国进行评估的费用可能是您在匈牙利支付的三倍。

- Common Criteria 品牌没有得到很好的保护。我在第 12.6.1.1 节中描述了 VISA 声称已根据通用标准评估过的 PIN 输入设备是如何不安全的； GCHQ 的回应是,由于评估没有在他们那里注册，而且这些设备也没有声称是“CC 认证”的,所以这不是他们的问题。因此,供应商可以继续将有缺陷的终端描述为“CC 评估”。企业不会容忍这种滥用其商标的行为。

- 更一般地说,没有关于责任的内容：“在认可中使用评估结果的程序不在CC 的范围之内”。

在本书的第二版中,我认为通用标准评估有点像橡皮拐杖。这种装置有各种各样的用途,从通过从容易上当受骗的政府那里骗钱来赢得法官的同情,到敲打人们的脑袋。只是不要试图对其施加严重的影响。

28.2.7.3 协同保护配置文件

为了应对这些批评,协作保护配置文件 (cPP) 于 2015 年开始出现。其想法是从 EAL 级别转向针对每一类安全设备的单一保护配置文件,并将该配置文件开发为在政府和学术界的投入下,行业中公司之间的协作努力 [462]。希望是阻止安全评估在竞争公司之间的战略博弈中被滥用。通过浏览 CC 网站上的评估产品目录，现在可以在 2020 年看到其结果。法国和德国的供应商仍然提供许多智能卡,以及电子签名创建设备等相关产品,其证书为 EAL4+ 或 EAL6;那是 SOG-IS 卡特尔的遗产。

然而,在欧洲之外,CC 系统已经完全被供应商的利益所占据。美国公司提供许多防火墙、路由器和其他网络产品,根据行业 cPP 进行评估;和日本企业

Machine Translated by Google

提供一系列打印机和传真机。那么什么是安全传真机 它对传真进行加密吗?一点也不;它的行为与您期望的传真机一样（如果您足够大,可以记住它们）。简而言之,cPPs 已经成为一种营销机制,现在正在破坏传统的 CC 核心。想要销售电子签名系统的公司可以让他们根据被认为是 EAL4 的 cPP 进行评估,大多数客户无法分辨这与根据旧规则进行的 EAL4+ 评估之间的区别 。

28.2.8 “最大自满原则”

有大量关于标准经济学的文献,因为在许多情况下人们必须在它们之间做出选择。如果你是一个聪明的少年,你是申请一所顶尖大学并冒着获得二等学位的风险,还是应该去当地大学成为一名明星?在这两种情况下,您是否应该担心成绩膨胀会侵蚀您学位的价值?如果你正在为一家初创公司筹集资金,你应该从商业天使那里获得资金,还是尝试让知名风险基金参与?一家 IT 供应商想知道是否要进行某种认证,面临着类似的选择。甚至国家也在玩认证游戏。大型服务公司的欧盟总部都设在爱尔兰,因为长期以来都柏林的政策是拥有欧洲最宽松的隐私监管制度,以及最低的公司税。处理此类游戏有哪些选择?

这种选择最有影响力的模型是 2006 年 Josh Lerner 和 Jean Tirole7 发表的一篇关于论坛购物的论文。他们的模型是一个三阶段博弈,赞助商选择一个证明者,然后证明者研究产品并可能要求一些改变,最后最终用户决定购买或不购买 [1143]。最大的问题是认证机构之间的竞争是会产生更好的标准,还是会导致逐底竞争。在大多数情况下,最大自满原则会胜出:所有者寻求单一认证机构的认可,并抵制让他们改进产品的尝试。只有在某些情况下,竞争才能提高质量。一个例子是非政府组织竞争认证产品的可持续性:在那里,认证者比赞助商更关心用户的结果,并且所需的财产不受单个赞助商的强烈控制。另一个是精英大学之间的竞争:学生没有市场力量,足够多的雇主会为精英毕业生支付溢价,因此剑桥有足够的动力与牛津、麻省理工和伯克利竞争。

参与者不仅仅是赞助商、认证者和
用户,事情变得更加复杂。

认证游戏发生在一个更大的生态系统中。一家公司推出了一些新产品并将其出售给一些客户。然后,客户需要一个标准和一些测试来满足他们的审计员的要求。他们可能希望发明人将产品许可给他们已建立的供应商,或至少许可给第二个供应商。其他发明家涌入,突然之间就有了一个专利池。这些公司为了获得他们的专利进行了漫长而艰难的谈判,以最大化他们的专利使用费份额;这通常会导致可怕的标准

7Tirole 因这项工作以及市场力量和监管方面的许多其他工作而获得 2014 年诺贝尔奖。

Machine Translated by Google

安全且难以修复（请参阅第 14.2.4 节关于智能电表;还有更多示例）。专利池可能成为阻止新市场进入者的卡特尔;此投诉是针对 5G 周围的 GSMA 标准提出的（请参阅第 22.2.4 节）。 GSMA 还因其网络设备安全保证计划 (NESAS) 而受到批评,在该计划中,供应商支付仅需几天的安全评估费用（由于大流行,现在允许远程审核）。简而言之,产业战略并没有像垄断或卡特尔那样优化伟大的产品。

在市场由垄断者主导的情况下,客户和政治压力可能最终导致垄断者关注安全,垄断者将一些安全外部性内部化甚至可能是理性的（参见第 27.5.3 节中的 Microsoft 案例）.但在一般情况下,对于某些步骤由卡特尔主导的复杂供应链,这可能要困难得多。

安全认证的复杂性大致是 (a) 依赖方 如果东西被黑客攻击有风险的人 可能是客户、第三方,如保险公司或公众 (b) 赞助商可能是供应商、客户、依赖方或(c) 测试人员可以在价格或质量上进行竞争,这意味着他们可以在不失去认证机构（可能是政府实体或行业)的许可的前提下,达到最低质量门槛协会 (d) 可能有不止一个认可机构,加上它们之间的政治。因此我们可以有多个间接层,我们有时甚至会就“谁对验证者进行验证”展开竞争。为了理解事物,我们必须详细查看实际案例。

在 CC 评估的产品在 EAL4 或以上的情况下,例如智能卡和 HSM,假设 Alice 的公司向 Bob 的银行出售产品并让验证者 Charlie 说它是安全的,之后 Bob 的客户 Dorothy 欺骗另一个客户 Eve 并潜逃。当 Eve 现在在法庭上向 Bob 索回她的钱时,评估如何改变事情？ Bob 会争辩说他没有疏忽,因为他按照行业标准运营,因此不承担赔偿 Eve 的责任。如果查理在他的系统上签署了 o ,这个论点就更加有力了。查理的角色与其说是技术权威,不如说是责任盾牌。所以爱丽丝只会努力工作以满足查理。查理将与他的竞争对手竞争,一场逐底竞争将随之而来。现实生活中的结果是,支付卡品牌成立了 PCI 来接替查理的角色。我们在第 12.5.2 节中讨论了此类标准如何转移银行业的责任:它们比商人更能保护银行（惊喜,惊喜）。

对于电子签名设备,正如我们在上文第 28.2.7.2 节中讨论的那样,智能卡行业的游说促使欧洲通过了签名法,该法赋予使用认证产品创建的签名特殊的效力,即使这些签名是不安全的。 Docusign 等在线服务签名提供商的游说也让他们加入了进来。最终的效果不是安全而是税收。 （要在某些欧盟国家/地区提交纳税申报表,您必须通过此类服务对其进行签名,从而在您的税务会计师费用中额外增加 20 欧元。）

那么认证应该是自愿的吗?一个有趣的案例研究是 Ben Edelman 对 Trust-e 计划的网站认证。他发现经过认证的网站更有可能试图将恶意软件加载到您的计算机上,而不是更少。逆向选择把方案变成了负面信号

Machine Translated by Google

质量:实力较弱的供应商对他们的网站进行了认证,而知名消费品牌则不屑一顾 [612]。原因是Trust-e认证是自愿的,成本低,认证的技术门槛也低。

但是,尽管行业游说团体喜欢谈论“减少繁文缛节”,但有多少人会对彻底废除政府支持的安全或安保标准或机构感到高兴?在实践中,游说者试图抓住监管者而不是废除它们。许多监管制度既起到护城河的作用,可以防止在位者太容易受到初创企业的挑战,也可以起到责任保护的作用。例如,我们在第 17.3 节中讨论了亚马逊、微软、谷歌和 IBM 如何限制面部识别软件的销售 这是他们最具争议的产品 直到它受到监管。

28.2.9 后续步骤

自英国脱欧以来,英国和欧洲出现了分歧。欧洲通过了网络安全法案(第 2019/881 号条例),该法案加强了欧洲网络和信息安全局 (ENISA) 并将其置于其战略的中心。 ENISA 将充当专业知识中心,并与银行、航空、能源和电信领域的部门监管机构以及数据保护机构保持联系。我预计从长远来看,这将非常重要,因为安全和安保监管正在融合,并且不可避免地会由汽车、飞机、医疗设备、铁路信号等的标准机构按部门进行管理。我稍后会回到这个。

至于信息安全产品的认证,它的做法可谓是“再接再厉”:它正在建立一个由ENISA领导的欧盟网络安全认证框架,该框架将接任顶级认证机构。它应该“有助于避免相互冲突或重叠的国家网络安全认证计划的增加,从而降低在数字单一市场运营的企业的成本”[655]。它将适用于服务和流程以及产品。正如我在 2020 年写的那样,细节仍在制定中,但目的是欧盟成员国的赞助机构将在三个级别进行认证,从“基本”开始,这需要供应商自我评估是否符合标准并承担责任对于合规性,从涉及安全功能验证的“大量”到涉及 ENISA 从 SOG-IS 接管目前评估为 EAL4 及以上的智能卡/HSM/电子签名工具包的“高”。

英国政府多年来一直关注认证问题,并参与推动cPP,以试图使认证更加标准化。但到 2017 年,他们得出的结论是,该标准对于安全而言既不必要也不充分,并且 GCHQ 从 2019 年起退出赞助商。它不再许可 CLEF 或批准认证,尽管英国组织可能会继续使用在其他地方创建的认证8。它长期以来有自己的国家产品认证计划,现在被称为商业

8我在 Donut 的一个间谍说“我们绝对承认来自任何生产国的任何 CC 证书,就好像它是我们自己的一样,我们的保证流程为该证书分配了它应得的权重 :-)”

Machine Translated by Google

产品保证 (CPA),但目前唯一保持 CPA 认证的消费产品是第 14.2.4 节中讨论的智能电表。未来的立法将要求物联网设备的基本安全,包括禁止默认密码和软件更新机制的要求;这是与 ETSI 一起完成的,导致欧洲标准草案 ETSI EN 303 645 V2.1 [646]。

现在的方向是着眼于过程而不是产品,这既适用于为英国国家基础设施开发关键设备的公司,也适用于更普遍的情况。一般计划 Cyber Essentials 是针对提供 IT 服务或处理个人信息的政府承包商强制执行的。

已经有用于安全管理的 ISO 27001 标准,我们在 12.2.4 节中提到过:这很昂贵,已被大型会计师事务所转化为收入来源,而且与 CC 一样毫无用处。几乎所有的大型安全漏洞都发生在获得 ISO 27001 认证的公司,审计员说有些事情是可以的,但事实并非如此。审计员必须依赖公司告诉他们的内容,而不知道如何保护其系统的公司只会说“我们有一个很棒的 X 流程”,而他们不知道。为什么一个小企业主要为此付出数万美元,除非他们需要它来竞标政府合同?为什么政府要征收这样的税?因此,Cyber Essentials 计划侧重于最基本的知识 ,并且只需花费 300 英镑即可获得经过验证的自我认证。它的目标是中小型企业,但第一批真正获得认证的公司是银行和电话公司等大公司,它们希望将每一个流苏都添加到他们的企业尽职调查中。

随着政府争吵不休,我们看到了私营部门标准 Bitsight 的出现。回想一下,在第一章中,我曾说过,在企业界,可信系统通常意味着保险公司可以接受。还记得在第 2.2.1.6 节中我们如何描述 NSA 如何拥有一个名为 Mugshot 的系统,该系统可以在 Internet 上爬行以寻找易受攻击的系统,以及另一个名为 Xkeyscore 的系统,它使网络战士能够在感兴趣的目标附近找到易受攻击的系统?

好吧,Bitsight 为私营部门拍摄 Mugshot,但它不是攻击公司的系统,而是通过计算有多少服务器没有及时打补丁,以及有多少其他可见的妥协指标来评估公司的网络安全风险。他们已经开始主导保险市场评估,因为在周期性的保险业利润受到挤压并且无法再让客户填写有关其网络安全实践的长问卷的时候,他们给出了单一的数字评级。这在 Lerner-Tirole 模型中是有道理的,因为 Bitsight 有动力保持领先于可能的竞争对手,就像一所精英大学一样。与政府和审计公司推动的大多数计划相比,他们的评级为生态系统带来了更多的诚实,但也有一些有趣的副作用。例如,服务公司现在不太愿意赞助学校的夺旗比赛;如果 Bitsight 爬虫在您的 IP 地址空间中发现一个易受攻击的系统,您将其设置为此类练习的目标,它可能会将您的 Bitsight 评级降低 10% 以上,这可能会让您失去真正的业务。

认证产品和业务流程就这么多。在下一节中,我们将从故障分析、错误跟踪、跨产品依赖性、开源软件和

Machine Translated by Google

开发团队。

28.3 可靠性的度量和动态

随着可靠性成为终身财产,我们需要更好的方法来衡量它。我们知道这通常是开发团队的职能;我们在 27.5.3 节中讨论了能力成熟度模型。要获得安全的代码,您需要聘请具有适当技能组合的聪明人,让他们在共享项目上一起工作,以便他们学会一起工作。在此过程中,您可以通过提供反馈和不断改进流程和工具来衡量他们的表现并加以改进。但是你如何进行测量呢?

这有两个主要方面:可靠性增长,因为随着时间的推移系统通过测试和错误修复变得更加可靠,以及漏洞披露,因为错误被发现并且可能会或可能不会被修复。

28.3.1 可靠性增长模型

随着系统在实验室和现场进行更多测试,可靠性的提高引起了更多人的兴趣,而不仅仅是软件工程师;核、电气和航空航天工程师都依赖于可靠性模型和指标。

在最简单的情况下 测试人员试图找到系统中的单个错误 一个合理的模型是泊松分布:在 t 次统计随机测试后错误仍未被发现的概率 p 由 p = eEt给出,其中 E 取决于关于它影响的可能输入的比例[1175]。因此,当系统的可靠性由单个错误决定时 比如当我们正在寻找系统中的第一个错误或最后一个错误时 可靠性增长可能呈指数级增长。

但广泛的实证研究表明,在大型复杂系统中,第 t 次测试失败的可能性与eEt不成正比,而是与 k/t 成正比(对于某个常数 k)。所以可靠性的增长要慢得多。这首先记录在 IBM 大型机操作系统的错误历史记录中 [18],并已在许多其他研究中得到证实 [1198]。由于 k/t 的故障概率意味着大约 t/k 的平均故障间隔时间(MTBF),可靠性随测试时间线性增长。这个结果通常被安全关键系统社区表述为“如果你想要一百万小时的平均故障间隔时间,那么你必须测试(至少)一百万小时”[355]。这一直是反对开发复杂、关键系统的主要论据之一,这些系统在使用前无法进行全面测试,例如里根总统的“星球大战”弹道导弹防御计划。

k/t 行为的原因出现在 [249] 中,并在更一般的假设下通过观察为理想气体建模而开发的麦克斯韦-玻尔兹曼统计数据也适用于统计独立的错误 [312] 得到了证明。

该模型给出了许多其他有趣的结果。如果您可以假设错误在统计上是独立的,那么 k/t 可靠性增长是最好的:您需要一百万小时的测试才能获得一百万小时的 MTBF 的规则是不可避免的,直到某个常数倍数取决于最初的

Machine Translated by Google

代码质量和测试范围。这可以看作是“墨菲定律”的一个版本:在选择过程中幸存下来的缺陷数量最大化。

这些统计数据给出了软件进化模型与生物物种在选择压力下的进化之间的巧妙联系,其中“错误”是降低适应性的基因。正如软件测试尽可能减少与所应用的测试一致的错误数量一样,生物进化使一个物种能够以最小的早期死亡成本适应变化的环境,同时尽可能多地保留多样性以帮助物种在未来的环境冲击中生存.例如,如果一群兔子被蛇捕食,它们将被选择为警觉性而不是速度。

它们的速度可变性将保持不变,因此如果狐狸到达附近,兔子种群的平均奔跑速度会在选择性捕食下急剧上升 9。

进化模型还指出了从可重用软件组件(如对象或库)获得的可靠性增益的基本限制;经过良好测试的库仅仅意味着总体故障率将由新代码主导。它还解释了安全关键系统社区的观察结果,即测试结果通常是一个较差的性能指标 [1175]。测试人员测量的失败时间仅取决于程序的初始质量、测试范围和测试次数,因此它几乎没有提供有关程序在另一个环境中的可能性能的更多信息。

还有一些结果出乎意料,但回想起来却很明显:例如,每个错误对整体故障率的贡献与包含它的代码是经常执行还是很少执行无关 直觉上,执行得少的代码也测试得少.最后,不同的测试人员应该并行而不是串行地处理一个程序。

因此,复杂的系统只有在经过不同测试人员的长时间测试后才会变得可靠。这为经过试验和测试的机械设计提供了优势,因为我们获得了关于它如何失败的统计知识。大众市场软件开始大规模使用以进行全面测试,尤其是在开始向供应商发送崩溃报告后。开发团队使用回归测试意味着每个新构建都可以在一夜之间执行数十亿个测试用例。可以随时监控迁移到云的服务是否出现故障。

那么可靠性的限制是什么?首先,由平台业务模型决定的新版本中的新代码引入了新错误,其次,对抗性行动导致攻击和防御之间存在显着的不对称。

让我们举一个简单的例子。假设 Windows 等产品有 1,000,000 个错误,每个错误的 MTBF 为 1,000,000,000 小时。假设 Ahmed 为伊朗革命卫队工作,开发工具来打入美国陆军的网络,而 Brian 是 NSA 的人,其工作是阻止 Ahmed。所以他必须在 Ahmed 之前了解这些错误。

艾哈迈德只有六个人,所以他一年只能做 10,000 小时的测试。 Brian 拥有完整的 Windows 源代码、数十个博士学位、监督

9 更正式地说,自然选择的基本定理说,一个物种具有高基因变异可以更快地适应不断变化的环境[695]。

Machine Translated by Google

商业评估实验室,CERT 的内部轨道,与其他五眼联盟成员国的信息共享协议,以及政府计划向电力和电信等关键行业派遣顾问,以找出如何破解它们（对不起,建议他们如何保护他们的系统）。这一切加起来相当于每年 100,000,000 小时的测试。

一年后,Ahmed 发现了 10 个漏洞,而 Brian 发现了 100,000 个。但是 Brian 发现 Ahmed 的任何一个 bug 的概率只有 10%,而他找到所有 bug 的概率可以忽略不计。 Brian 的错误报告会变得如此火爆,以至于微软会找到一些借口停止修复它们。换句话说,攻击者有热力学站在他这一边。

在现实生活中,漏洞是相关的而不是独立的;如果 90% 的漏洞都是堆栈溢出,并且您引入了堆栈金丝雀和 ASLR 等编译器技术来捕获它们,那么出于建模目的,可能只有一个漏洞。然而,花了好几年的时间才修复那个问题,而且新的问题一直在出现。因此,如果您实际上负责陆军安全,就不能只依赖于几年前购买的一些商用现成产品。避免统计陷阱的一种方法是简单性 正如我们在第 9 章中看到的那样,它最终意味着诸如强制访问控制之类的策略、诸如多级安全邮件防护之类的体系结构,以及其他许多东西。更现代的方法是一个学习系统,它可以观察出什么问题并快速修复它。这反过来意味着警惕的网络监控、漏洞报告、漏洞披露和快速修补 正如我们在第 27.5.7 节中描述的那样。

28.3.2 恶意评论

当您真的想要保护财产时,设计和实施受到敌意审查是至关重要的。最终会是这样,如果在系统投入使用之前完成,它可能会更便宜。正如我们在一个又一个案例中看到的那样,攻击者的动机至关重要;希望系统通过的人的友好评论与认真尝试破坏它的人的贡献相比基本上是无用的。这就是由供应商支付的来自多个竞争评估者之一的评估的基本原因,如通用标准和 ISO 27001,从根本上被打破了。 （回想一下我们在第 12.2.6 节中讨论的审计师长期无法发现雇用他们的高管的欺诈行为。一位通过做空 Wirecard 赚取 1 亿美元的对冲基金经理 Jim Chanos 说：“当人们问我们时,谁是审计师,我总是说‘谁在乎？’ 几乎所有的欺诈行为都经过了一家大型会计师事务所的审计。”[30]。）

要进行恶意评论,您可以用金钱或荣誉来激励攻击者。第一个例子是 NASA 用于载人航天飞行的独立验证和验证 (IV&V) 程序;承包商被雇来搜索代码,并为他们发现的每个错误支付奖金。第二个例子是核指挥与控制的评估,桑迪亚国家实验室和美国国家安全局竞相寻找彼此设计中的漏洞。另一个是在 IBM,它有两个团队,一个在纽约,另一个在美国,多年来一直在密码学领域保持领先地位。

Machine Translated by Google

北卡罗来纳州,他们会试图打破彼此的工作,就像剑桥和牛津每年都试图赢得划船比赛一样。另一个是谷歌的零项目,该公司致力于在其依赖的产品（如 Linux)和竞争对手产品（如 iOS)中寻找漏洞,并在提前 90 天通知后积极披露漏洞,以迫使他们被固定。这得到了超过 97% 的修复 [589]。

学术界的评论充其量属于这一类。我们学者通过打破 stu 赢得我们的马刺,并通过发明新型攻击获得最高荣誉。我们互相竞争 剑桥对伯克利对CMU对魏茨曼。不过,既定的最佳实践是用金钱来激发恶意审查,特别是通过漏洞赏金计划,供应商为报告漏洞提供巨额奖励。正如我们在上面第 27.5.7 节中提到的,Apple 为任何无需用户点击即可破解 iOS 内核的人提供 100 万美元;这是 iOS 安全性的一项重要指标10。

加强学术审查或漏洞赏金计划的一种方法是
公开你的设计和实现,这样全世界都可以寻找错误。

28.3.3 免费和开源软件

安全机制是否应该接受审查?历史共识是它们应该如此。第一本关于密码学的英文书由奥利弗·克伦威尔 (Oliver Cromwell) 的密码学家约翰·威尔金斯 (John Wilkins) 于 1641 年撰写。在“Mercury, or the Secret and Swift Messenger”中,他用“如果所有那些容易被滥用的有用发明因此应该被隐藏起来,那么没有任何艺术或科学可以合法地公开”来证明讨论密码学是合理的。

奥古斯特·科克霍 (Auguste Kerckho) 在 1883 年的“La Cryp tographie Militaire”首次阐述了密码工程,建议密码系统的设计方式应使其在对手学习所使用的技术时不会受到损害:安全性必须仅取决于键 [1042]。在维多利亚时代,辩论还涉及锁匠是否应该讨论锁的漏洞;正如我在 13.2.4 节中提到的,一本书的作者指出,锁匠和窃贼都知道如何开锁,只是顾客一无所知。在第 15.8 节中,我讨论了甚至在核安全中也发现的部分开放性。

自由开源软件 (FOSS) 运动将这种开放理念从算法和架构扩展到实现细节。

许多安全产品都有公开的源代码,其中第一个可能是 PGP 电子邮件加密程序。 Linux 和 FreeBSD 操作系统以及 Apache 网络服务器也是开源的,并被广泛依赖:Android 在 Linux 上运行,Linux 在世界数据中心也占主导地位,而 iOS 基于 FreeBSD。

开源软件并不完全是最近的发明。在计算的早期,大多数系统软件供应商都发布了他们的源代码。这种情况在 1980 年代初开始消退,当时诉讼压力导致 IBM 采用

10根据这个指标,地球上最安全的系统可能是比特币,因为任何人只要能破坏签名机制,就可以窃取数十亿美元。

Machine Translated by Google

其大型机软件的“仅目标代码”政策,尽管受到用户的严厉批评。自 2000 年以来,钟摆又摆回来了,而 IBM 是开源的坚定支持者之一。

有许多支持开放软件的有力论点,也有一些反对。首先,虽然许多封闭系统是以结构化方式开发的,具有初始开发和后期升级的瀑布模型或螺旋模型,但世界正在朝着更敏捷的开发风格发展,埃里克雷蒙德将这种紧张局势描述为“大教堂和集市”具有影响力的 1999 年同名书 [1584]。其次,系统变得如此复杂,工具链变得如此之长,以至于您试图破解的错误通常不在您编写的代码中,而是在您所依赖的操作系统甚至编译器中,因此您希望能够在那里也能很快找到错误,要么修复它们,要么自己贡献一个修复。第三,如果世界上每个人都可以检查和使用该软件,那么就更有可能发现和修复错误;用 Raymond 的名言来说,“对许多人来说,所有的错误都是浅薄的”。第四,在这样的产品中插入后门也可能更加困难(尽管人们已经被发现尝试,现在一个漏洞可以卖到七位数)。最后,出于所有这些原因,开源非常有助于增强信心。

专有软件行业争辩说,虽然开放有助于防御者发现错误以便他们修复它们,但它也有助于攻击者找到错误以便他们可以利用它们。许多开放产品可能没有足够的维护者,因为典型的志愿者发现开发代码比寻找漏洞更有价值(尽管漏洞赏金开始改变这一点)。其次,正如我在第 28.3.4 节中指出的那样,不同的测试人员发现不同的错误,因为他们的测试重点不同。

由于志愿者会查看一些很酷的代码,例如密码,聪明的间谍或漏洞赏金猎人会查看一些无聊的代码,例如设备驱动程序。实际上,主要漏洞潜伏多年。例如,PGP 版本 5 和 6 中的编程错误允许攻击者在密钥持有者不知情的情况下添加额外的托管密钥 [1700]。

那么究竟是进攻者得到的帮助更大,还是防守者得到的帮助更大呢?在可靠性增长的标准模型下,我们可以证明开放性同样有助于攻击和防御[74]。因此,在给定的应用程序中,开放方法还是专有方法最有效将取决于该应用程序是否以及如何偏离标准假设,例如独立漏洞。最后,你必须出去收集数据;例如,对 OpenBSD 操作系统中发现的安全漏洞的研究表明,这些漏洞之间存在显着相关性,这表明开放性是一件好事 [1488]。

那么利益的平衡在哪里呢? Eric Raymond 对开源软件经济学的有影响力的分析 [1585] 提出了产品是否可能从开源方法中受益的五个标准:它基于共同的工程知识而不是商业秘密;对故障敏感的地方;需要同行评审以进行验证的地方;不同的用户将合作查找和删除错误,这对业务至关重要;其经济性包括强大的网络效应 。安全性通过了所有这些测试。

法律经济学学者彼得·斯怀尔 (Peter Swire) 解释了为什么政府

Machine Translated by Google

本质上不太可能接受披露:尽管出于互操作性和信任原因,竞争力甚至促使微软开放了很多软件,但政府机构玩不同的游戏,例如扩大预算和避免尴尬 [1853]。然而即使在那里,安全争论也开始盛行:从大约 1999 年的试探性开始,美国国防部已经开始拥抱开源,特别是通过我在 9.5.2 节中讨论的 SELinux 项目。

因此,虽然开放式设计既不必要也不足够,但它通常会有所帮助。重要的一阶问题是有能力的人在检查和测试你构建的东西时付出了多少努力 以及他们是否告诉你他们发现的一切。在这里做的谨慎的事情是有一个慷慨的错误赏金计划。还有一个越来越重要的二阶问题:如果您的业务依赖于 Linux,难道不应该至少让您的几个工程师参与其开发人员社区,这样您就知道发生了什么事吗?

28.3.4 过程保证

近年来,越来越少强调以产品为中心的保证措施,例如测试,而更多地强调过程措施,例如谁开发了它以及如何开发它。任何做过系统开发的人都知道,一些程序员编写的代码中的错误比其他人少一个数量级。也有一些组织编写的代码比其他组织好得多。有能力的公司试图聘用优秀人才,而优秀人才更愿意为重视他们并雇用志趣相投的公司工作。

虽然高质量和低质量开发人员之间的一些差异取决于人才,但许多是由工作文化决定的。根据我自己的经验,一些 IT 部门缓慢而官僚,而另一些 IT 部门则充满活力。领导事项;就像用钱人取代波音的工程领导层导致 737Max 灾难一样,我看到当 IT 部门的 CIO 被官僚取代时士气崩溃。另一个问题是,随着时间的推移,工程师的质量有下降的趋势。一个因素是魅力:许多聪明的毕业生想为初创公司而不是大型科技公司工作,或者为活跃的金融科技和对冲基金工作,而不是无聊的老式货币中心银行。另一个是人口统计:1990 年代初期的微软充满了长时间工作的年轻工程师,但十年后,许多人兑现了他们的股票期权并离开了,而其余的人大多成家立业并工作时间。一旦公司停止增长,晋升就很缓慢; IBM 有句谚语:“唯一离开的人是好人”11。银行和政府机构也有类似的问题。一些公司试图通过评级系统来解决这个问题,该系统要求管理人员每年解雇效率最低的 10% 左右的团队成员,但这对士气造成的损害是可怕的;人们把时间花在吹牛而不是写代码上。保持高效的工作文化是真正困难的问题之一,而且数量惊人的大公司在这方面做得很差。我们在第 27.5.3 节中讨论过的能力成熟度模型是一种工具,可以帮助优秀的管理者将优秀的团队凝聚在一起并随着时间的推移不断改进。但

11 作为一名前 IBM 员工,我喜欢那个!

Machine Translated by Google

仅靠它自己是不够的。整个公司环境都很重要,从饮水机聊天到最高领导层。使命是做伟大的工程,还是只是为华尔街赚钱?当然,每家公司都假装有使命,但大多数都是假的,而且工作人员一眼就能看穿。

一些老式公司信奉 ISO 9001 标准,该标准要求他们对设计、开发、测试、文件编制、审核和管理控制的流程进行一般性记录。更多详细信息,请参见 [1937];整个顾问和审计师行业都陷入了困境。

与我们在上面第 28.2.9 节中讨论的 ISO 27001 一样,它是装饰性的而不是有效的。充其量它可以为渐进式流程改进提供一个框架;但通常这是一种打勾的练习,只是用更多官僚主义的混乱来取代混乱。正如敏捷开发方法取代瀑布方法一样,ISO 9001 也正在被能力成熟度模型取代。从保证的角度来说,这归结为值得信赖的供应商。

但可信赖的供应商很难证明。政府认证机构不能被视为歧视,因此项目退化为打勾。正如我们在上文第 28.2.8 节中讨论的那样,私人认证计划有加强卡特尔或逐底竞争的趋势。在这两种情况下,咨询公司和审计公司都将流程工业化以最大化他们的费用收入,我们又回到了起点。如果你擅长你的工作,你如何做到这一点?

做高质量工作的小企业通常在向最挑剔的客户销售产品时做得更好 少数大公司足够聪明,能够欣赏他们所做的事情。简而言之,您通常必须自己成为专家才能真正了解质量提供者是谁。

那么动态呢?如果质量难以衡量,质量激励参差不齐,质量提升困难重重,那么进化产品的保证水平又有什么用呢?它们会像牛奶,还是像酒 [1488]?他们会随着年龄的增长而变得更好,还是会消失?

简单的答案是您必须进行实际测量。系统的质量可能会提高,也可能会下降。如果产品增强引入新错误的速度等于发现和删除旧错误的速度,它甚至可能会找到一个平衡点。有几个研究团体在各种应用程序和环境中测量系统的可靠性、可用性和可维护性。根据经验,新系统的可靠性通常会随着更活跃的错误被发现和修复而提高一段时间,然后在几年内保持平衡,然后随着代码变得复杂和更难维护(软件工程师有时甚至称为衰老)。然而,如果维护代码的公司仍然从中赚到足够的钱,并且有动力关心质量,他们可以通过重写变得过于混乱的部分来解决这个问题 这个过程被称为重构。简而言之,现实世界是复杂的。模型只能带你走这么远,你必须研究系统在实际使用中的行为方式。

测量带来了它自己的问题。一些供应商收集并分析关于他们的产品如何失败的大量数据 例如微软、谷歌和苹果等平台公司 但只向外部提供选定的数据,为专业的第三方评估人员创造市场,从

Machine Translated by Google

学术界的科技出版社。其他公司说得少得多,为 Bitsight 等评级公司创造了机会。众所周知,医疗保健行业对患者受到伤害的证据守口如瓶,他们的律师可能需要工作多年才能立案。但在医疗设备等应用中,监管机构有足够的公共利益进行干预以提高透明度,正如我们在上文第 28.2.3 节中指出的那样,欧盟最近修改了医疗设备监管法律以强制进行售后市场监督。由于现在大多数软件都在应用程序而不是平台中,并且经常在或支持设备中,这让我们考虑安全监管。

28.4 安全与保障的纠缠

正如我们在 28.2.2 中讨论的那样,政府对从汽车到铁路信号以及从医疗设备到玩具的多种设备的安全进行监管。随着软件渗透到一切事物中,并且一切事物都连接到云服务,安全监管的性质正在发生变化,从简单的上市前安全测试到在软件将定期修补的多年服务生命周期内维护安全和安全。我们已经看到这是如何与安全纠缠在一起的。我们在 23.8.1 节讨论了智能电网,在 14.2 节讨论了智能电表,在 13.3 节讨论了建筑警报。

我相信,安全与保障的日益纠缠对我们的领域来说是如此重要,以至于自 2017 年以来,我们已经合并了一年级本科生的安全与保障教学,正如我在第 27.1 节中提到的那样。安全是一个比安全更多样化的主题。虽然安全工程是一门相当连贯的学科,但随着时间的推移,安全工程已经分裂为飞机、公路车辆、船舶、医疗设备、铁路信号和其他应用的独立学科。正如我在 27.3 节中讨论的那样,我们仍然可以从安全工程师那里学到很多东西,并且安全工程师也开始必须学习安全性。这将是一个漫长的过程。由于冠状病毒封锁,这些讲座现在可以通过视频公开获得 [89];我现在希望我多年前就把我的讲座放在网上。

促使我们将安全和安全教学结合起来的是我们在 2015-6 年为欧盟所做的一些工作,这些工作研究了一旦计算机无形地嵌入到任何地方后安全监管将会发生什么。欧盟是全球数十个行业的主要安全监管机构,因为它是最大的市场并且比美国政府更关心安全。 Ocials 想知道这个生态系统将如何适应“物联网”,在“物联网”中,漏洞(无论是旧的还是新的)可能会被远程大规模利用。许多以前只考虑安全性的监管机构也将不得不开始考虑安全性。

2015 年欧盟面临的问题是如何使从汽车和飞机到医疗设备、铁路信号和玩具等数十个行业的安全监管现代化,并酌情引入安全监管。监管目标各不相同。在本书中,我们讨论了安全如何在许多不同的部门失败以及潜在市场失灵的性质。

在不同的环境中,安全监管机构可能希望提高攻击者的成本并减少他们的收入;降低防御成本;减少影响

Machine Translated by Google

安全故障;使保险公司能够有效地为网络风险定价;并降低攻击的社会成本和社会脆弱性。

安全监管机构似乎更直截了当。他们倾向于忽视每次市场失灵背后的经济微妙之处,而将重点放在伤害和死亡上,然后是直接的财产损失。至少对于死亡,你会认为我们有不错的统计数据,但优先级是由公众对不同类型伤害的关注来调节的。正如我们所讨论的,与一千人一次死于医疗设备事故相比,公众对一百人同时死于飞机失事更为震惊。然而,当黑客表明他们可以通过 wifi 进入并将几种型号的 Hospira Symbiq 输液泵输送的剂量更改为可能致命的水平时,FDA 发布了一项安全建议,告诉医院停止使用它 [2066]。它没有发布关于 300 多个模型的建议,这些模型仅受到我们在第 28.2.3 节中讨论的安全问题的影响。当你停下来想一想,这是相当惊人的。一名安全监管机构忽视了一个每年导致数千名美国人死亡的问题,同时对迄今为止尚未造成任何人死亡的安全加安全问题感到恐慌。

也许人们直觉地理解了我们在第 27.3.6 节中讨论的原则:如果对手可以设计触发它所需的输入组合,那么百万分之一的偶然发生致命事故的可能性并不能提供太多保证.

这种模式在第二年继续存在,当时 FDA 在报告称该设备可能被黑客攻击后,在美国召回了 465,000 个 St Jude 心脏起搏器进行固件更新。由于设备故障的风险很小,因此更新需要去医院就诊。该报告本身是有争议的,因为它是由一家卖空圣裘德股票 [1838] 的投资公司推动的。

欧盟已经在医疗器械安全方面开展了工作,并于次年更新了其医疗器械指令,要求“根据最先进的技术水平开发医疗器械软件,同时考虑到开发生命周期、风险等原则”管理,包括信息安全、验证和确认”,以及“设计和制造的方式尽可能防止未经授权的访问,这可能会妨碍设备按预期运行”[653]。本文并未涵盖所有基础知识,但它是有用的第一步;它将于 2021 年生效。

28.4.1 汽车电子安全保障

由于谷歌和特斯拉等公司对自动驾驶汽车的兴趣激增,道路安全在 2010 年代中期推动了人们对安全与安全融合的兴趣。继 2012 年使用深度神经网络在计算机视觉领域取得突破后,进展迅速。关于实验车辆早期事故的第一条消息是在 2015 年左右与我在第 25.3 节中描述的对抗性机器学习的突破性研究以及我在第 25.2.4 节中描述的备受瞩目的吉普切诺基黑客事件同时出现的。自动驾驶汽车突然成为热门话题,不仅是股市投资者和安全研究人员的话题,也是安全问题。恐怖分子能否入侵他们并将他们驱赶到人群中?他们可以通过在建筑物上投射欺骗性图像来获得相同的结果吗?如果孩子们可以用他们的手机从学校叫车回家,有人会破解它来绑架他们吗?和

Machine Translated by Google

道德如何 如果一辆自动驾驶汽车即将撞车,并且可以在杀死一名乘客或两名行人之间做出选择,它会怎么做?它应该做什么?让我们一步一个脚印地处理安全和保证方面的问题。

道路安全是安全监管的一个重大成功案例。根据 Ralph Nader 的著作“任何速度都不安全”[1370],美国国会成立了国家公路交通安全管理局 (NHTSA)。它最初认为对新车型进行碰撞测试就足够了,但发现需要强制召回后来发现不安全的车辆 12。在 2009 年雪佛兰 Malibu 和 1959 年雪佛兰 Bel Air 之间的碰撞测试的消费者报告视频中可以清楚地看到这些影响。 Bel Air 的客舱被压碎,假人司机被刺穿在方向盘上;一个人类司机会被杀。得益于 50 年的进步,Malibu 的乘客舱依然完好无损;前部缓冲带吸收了大部分能量,安全带和安全气囊固定了假人驾驶员,人类驾驶员会走开 [472]。我向我的一年级学生展示这段视频,以强调安全工程不仅是为了减少错误的可能性,而且是为了减轻错误的影响 。视频所展示的几十年的进步不仅涉及多个国家的工程、游说和标准制定,还涉及安全活动家与行业之间的许多争论。在行业内,一些汽车制造商试图领先,而另一些则拖后腿。汽车安全还涉及驾驶员培训、禁止酒后驾驶和驾驶员工作时间过长的法律、改变围绕此类行为的社会规范、道路交叉口设计的稳步改进等等。它已经发展成为一个庞大而复杂的生态系统。随着汽车变得更智能、连接性更强,这现在必须得到发展。

在 2010 年代,汽车逐渐获得更多辅助技术,从泊车辅助到自适应巡航控制,再到自动紧急制动和自动车道保持。我在第 25.2 节中描述了像谷歌和特斯拉这样的公司如何推动一项研究计划将这些系统结合在一起,从而实现自动驾驶。他们自己的辅助技术功能存在各种错误;我在第 23.4.1 节中讨论了自适应巡航控制的盲点。有些也容易被利用:查理·米勒和克里斯·瓦拉塞克破解了吉普车的泊车辅助功能,将其开出道路。销售有限自动驾驶功能的公司,如特斯拉,经历了开始削弱公众信心的事故。我在第 25.2 节中讨论了自动驾驶汽车的一些安全隐患。我们也讨论了安全的可用性方面。特斯拉的“自动驾驶仪”要求驾驶员集中注意力并将一只手放在方向盘上,以保持控制并避免发生事故。但由于它在大部分时间都能正常行驶,许多司机并没有这样做,其后果有时是致命的,而且具有新闻价值。

即使在 2020 年,虽然更好的自动驾驶系统可以在高速公路上很好地驾驶汽车,但它们在较小的道路上可能会不稳定,在环形交叉路口和草地边缘行驶时会感到困惑。那么我们应该如何测试它们的安全性呢?

测试防抱死制动系统 (ABS) 相当简单,因为我们了解打滑和滑水的物理原理,而且此类系统已经存在了足够长的时间,以至于我们有很长的事故历史。接下来我们有紧急制动辅助系统 (EBA),如果它认为您

12 这个故事在“汽车安全斗争”[1235] 中讲述。

Machine Translated by Google

试图紧急停车。通常的算法是,如果你在 300 毫秒内将脚从油门移到刹车,然后施加至少 2 公斤的力,它会尽快启动和停止汽车。这是一个简单的算法,但更难评估,因为它试图推断驾驶员的意图。 （我曾经无意中触发了我的,幸好我身后没有车。）

最近添加的是自动紧急制动 (AEB),如果有小孩或狗跑到您面前,它应该会停止汽车。这更难,因为你试图理解你在前方街道上看到的一切,复杂的处理同时使用传统逻辑和基于深度神经网络的机器视觉系统。正如我们在 25.2 节中讨论的那样,当前的产品既有限又质量参差不齐。添加车道保持辅助和自适应巡航控制,您的汽车可以很好地在高速公路上自动驾驶。

但是你应该如何测试呢?如果我们转向完全自主,你的风险和威胁分析必须包括人类社会中发生的许多坏事。

特斯拉在为其自动驾驶功能辩护时表示,其汽车比其他汽车更安全;截至 2020 年 6 月 23 日,在涉及其车辆的 135 人死亡事故中,只有 10 人归因于 Autopilot [1870]。不过,实际数字存在争议。一家保险取证公司对 NHTSA 提起诉讼,要求获得截至 2016 年 6 月的事故原始数据,并对其进行研究,并声称特斯拉提供并被 NHTSA 接受的分析仅考虑了 13% 的数据。正如特斯拉所声称的那样,在车辆的自动驾驶功能被激活后,安全气囊的部署并没有减少 40%,而是完整的数据显示从每百万英里行驶 0.76 次部署增加了 57% 到 1.21 [1565]。

随着时间的推移,保险业积累了所有汽车制造商的良好数据,并担心索赔成本。它担心 AEB,担心如果汽车在前面跑过兔子时急刹车,可能会发生更多的追尾事故。但在 2016 年数据开始出炉后,保险公司松了口气。当我在网上查询为配备 Autopilot 的特斯拉和同等价值的插电式混合动力梅赛德斯购买保险要花多少钱时,我得到了大致相同的答案（尽管更多的保险公司为梅赛德斯出价）。

但精算成本并不是公共政策的唯一驱动力。政客们开始担心卡车司机的工作。哲学家们开始担心伦理问题:如果在杀死行人和杀死司机之间做出选择,自动驾驶仪会保护它的司机吗?业界担心更新。机器视觉的进步如此之快,以至于您可以想象每五年必须销售一个全新的视觉单元,因为我们现在拥有的系统无法在五年前的硬件上运行。客户是否愿意每隔几年为新的自动驾驶仪支付数千欧元?

人们也更担心安全威胁,因为我们已经进化到对敌对活动很敏感。到 2020 年,我们将进行一系列安全标准化,包括我在第 27.3.5 节中提到的关于网络安全的 ISO 21434 标准草案;对 UNECE13 法规的拟议修正案,以处理联网车辆的网络安全和软件更新

13联合国欧洲经济委员会是根据 1958 年的一项条约成立的。这包括

Machine Translated by Google

克莱斯 [1921];在日本,继对丰田和本田的网络攻击之后,对整个汽车行业供应链提出了基本要求 [1243]。这一切都很好,但目标一直在移动得更快。

在布鲁塞尔,官方开始担心监管生态系统如何应对。超过 20 个机构以某种方式参与车辆安全（与美国不同,NHTSA 涵盖从汽车设计到速度限制的所有内容）。每个机构都必须聘请一名安全工程师吗?其中一些根本没有任何工程师,只有律师和经济学家。生态系统应如何发展以应对?在 2015 年柴油门排放丑闻之后,Ocials 突然不太愿意相信行业的保证,当时事实证明大众汽车在其汽车中安装了软件以在排放测试中作弊。

大众汽车和奥迪的 CEO 丢掉了工作,并面临刑事指控,还有其他十几位高管;这些公司支付了数十亿美元的法律和解金。威胁模型不再只是外部黑客,而是包括供应商本身。监管机构希望重新掌控局面。他们需要做什么?

28.4.2 使安全和安保监管现代化

我们的简报是考虑所有部门普遍存在的政策问题。很明显,欧洲机构需要网络安全专业知识来支持安全、隐私、消费者保护和竞争。但这在实践中意味着什么?为了充实这一点,Eireann Leverett、Richard Clayton 和我研究了三个我们有一定了解的行业:医疗设备、汽车和配电。我们的完整报告 [157] 于 2016 年提交,并于次年发表,连同面向学术读者的摘要版本 [1148]。完整的报告对 ISO、IEC、NIST 和其他机构的嵌入式设备的现有安全/安全标准拼凑进行了广泛分析。

这个练习让我们学到了很多我们没想到会提上日程的主题。可用性在很多方面都至关重要。过去占主导地位的安全范例是分析有限或不稳定的人类表现如何会降低原本设计良好的系统,然后找出如何减轻后果。一些国家要求 67 岁以上的司机接受医疗或重新参加驾驶考试,并坚持系好安全带和安全气囊。在安全方面,恶意进入等式:您担心 80 多岁的寡妇接到电话并被说服在她的 PC 上安装“升级”。汽车安全不仅仅是关于恐怖分子是否可以远程接管您的汽车并将其开到一些行人身上。如果一个孩子可以用她的手机叫车送她去学校,我们还要担心什么新的威胁?她是否可能被陌生人绑架或（更有可能)在监护权纠纷中被绑架?

谁的工程师需要担心她的安全　汽车公司的、网约车公司的,还是政府的?

安全工程师的任务是让即使是易受攻击的用户也能享受合理的保护,以对抗有能力的有动机的对手。你如何嵌入

欧洲和非洲的汽车制造国加上日本、韩国和澳大拉西亚,实际上是三个汽车标准化区之一,其他是美洲和中国。

Machine Translated by Google

在以前从未考虑过远距离对手的行业中的良好实践?这不仅是制定最低标准的问题,也是将安全思想嵌入标准机构、监管机构、测试设施和生态系统中许多其他地方的问题。这将是一个漫长而艰巨的过程,就像汽车安全一样。让那些通过仔细检查“英国标准手指”是否会不小心刺入电器而工作的测试工程师来从创造性恶意的角度来思考是很困难的。

我们从哪里开始?

我们提出了一些建议。委员会认为其中一些属于“太难”类别,包括将产品责任法扩展到服务,并要求不仅向安全机构和隐私监管机构而且还向其他利益相关者报告违规和漏洞。最终我们将需要法律来规范汽车数据在调查事故中的使用,特别是当汽车自动驾驶仪导致致命事故时存在责任纠纷的情况下。 （目前,供应商将数据关闭,需要通过激烈的诉讼才能获得。）没有数据,我们将无法构建学习系统。

我们的一项建议是,供应商必须针对其 CE 标志进行自我认证,以便在需要时对产品进行修补。正如我在上面第 28.2.9 节中讨论的那样,这看起来将通过技术标准 ETSI EN 303 645 V2.1 [646] 部分实现。 ETSI 是一个拥有约 800 家公司的会员组织;它可以比政府行动得更快,但仍有一定的影响力;例如,它设立了移动电话标准机构。然而,不遵守 ETSI 标准并不能授权鹿特丹的海关人员将一集装箱玩具运回中国。为此,我们需要赋予标准以法律效力。

28.4.3 2019 年网络安全法

另一项建议是欧洲应该建立一个欧洲安全工程机构来支持决策者。欧洲已经有了欧洲网络和信息安全局 (ENISA),负责协调欧盟政府机构之间的安全漏洞报告,但由于英国和法国情报机构的游说,它被流放到了克里特岛,他们不希望有同行竞争对手在欧洲机构中。英国脱欧公投改变了政治局面,使 ENISA 有可能在布鲁塞尔设立一个适当的办事处,从而承担起安全工程咨询的角色。

2019 年《网络安全法》将此正式化 [655]。正如我们在第 28.2.9 节中所述,它授权 ENISA 成为监管安全标准的中央机构,同时也成为向其他欧洲机构提供网络安全建议的主要机构。希望 ENISA 随着时间的推移建立自己的能力和影响力,并确保新的安全标准也适当关注安全性,至少包括适当的开发生命周期（这是我们的另一项建议）。

要使安全技术真正发挥作用,光有功能是不够的,测试甚至学习激励也是如此。正确的人必须信任它,它必须嵌入到社会和组织流程中,

Machine Translated by Google

这意味着在足够长的时间内与更广泛的系统保持一致并保持稳定。这意味着监管机构应该从产品测试转向整个系统的保证（这是我们的最终建议）。

28.5 可持续性

从长远来看，我们的报告认为最严重的问题是产品变得越来越不稳定。随着安全和安全漏洞得到修补，监管机构将不得不应对一个不断变化的目标。汽车机制将需要安全测试和安全测试，以及处理更新的方法。正如我们从大众汽车的惨败中看到的那样，许多传统制造商没有跟上协调披露的步伐。

大多数使用两年的旧手机都没有打补丁，因为原始设备制造商和移动网络运营商无法齐心协力。那么，我们到底要如何修补一辆在丹麦乡村使用了 10 年，然后出口到罗马尼亚的 25 岁路虎呢？这引发了一场政治斗争，因为汽车行业在六年多的时间里不想为软件补丁承担责任。

（如果您有钱，典型的欧洲汽车经销商会向您出售新车 3 年的租约，如果您不是那么富有，则向您出售经过批准的二手车。）但是，新车的内含碳成本–其制造过程中排放的二氧化碳量 – 大约等于其生命周期内的燃料燃烧量。可以预见的是，软件不是最新的汽车迟早会被禁止上路。目前，汽车报废的平均年龄约为 15 年；如果减少到六个，环境成本将是不可接受的。我们甚至不会通过从内燃机转向电动汽车来减少二氧化碳排放，因为电动汽车的内含碳成本更高；整个能源转型是基于这样的假设，即它们将至少持续与我们传统车队的 150,000 公里平均寿命一样长 [614]。

我们在欧洲机构中找到了准备好的听众。许多其他利益相关者一直在抱怨软件对消费品耐用性的影响，更新仅在短时间内可用或根本不可用。维修权活动家正在为消费电子设备在循环经济中可重复使用而开展活动，他们对科技公司试图使用“安全”机制阻止维修，甚至滥用它们试图使维修非法化感到恼火。由于经济激励和消费者期望的复杂相互作用 [1954]，物联网市场的自我调节在很大程度上是不成功的。消费者权益组织开始警告智能设备的使用寿命短得惊人：你可以在“智能冰箱”上多花点钱，却发现一年后供应商停止维护服务器时它变成了一块结冰的砖[933] .随着绿党在整个欧洲的投票份额增加，计划淘汰已经成为一个热门的政治话题。灯泡过去寿命更长；自 1901 年以来，两百周年纪念灯一直在利弗莫尔燃烧。1924 年，通用电气、欧司朗和飞利浦的卡特尔同意将灯泡的平均寿命从 2500 小时减少到 1000 小时，此后许多行业都效仿了这一行为。政府已经退缩；法国在 2015 年将缩短产品寿命定为违法行为，而在 Apple 于 2017 年承认后

Machine Translated by Google

由于它使用软件更新来降低旧款 iPhone 的速度,促使用户购买更新款,因此遭到起诉。 2020 年,它因反竞争行为收到了有史以来最高的罚款 e1.2B,尽管这也与其对待法国经销商的方式有关 [1193]。 （它以 5 亿美元解决了一项美国集体诉讼 [966]。）

安全机构已经警告我们有关“物联网”的风险,包括使用默认密码和无法修补软件的网络连接设备。事实上,当我在返回伦敦的欧洲之星火车上第一次向布鲁塞尔的大约 100 名安全和 IT 政策人员介绍我们的工作时,我了解到 Mirai 僵尸网络摧毁了 Twitter。我们很快发现它利用了具有默认密码且无法修补其软件的小米闭路电视摄像机。这完美地说明了采取行动的必要性。

在接下来的三年里,有不止一项举措试图创造一种法律手段来阻止像小米这样失败的科技公司通过修补漏洞（甚至使修补成为可能)来支持他们的产品。技术游说者阻止了前几次尝试,但最终在 2019 年,欧洲议会更新了消费者法以涵盖软件维护。

28.5.1 货物销售指令

该指令于 2019 年 5 月在欧洲议会获得通过 [656],并将于 2021 年生效。此后,销售“带有数字元素”的商品的公司必须在合理的使用寿命内维护这些元素。该措辞旨在涵盖商品本身的软件、商品所连接的在线服务以及可通过服务或直接与商品通信的应用程序。它们必须在售后至少维护两年,如果客户有合理的期望,则可以维护更长的时间。

这在实践中意味着什么?

现有法规要求汽车和洗衣机等耐用品供应商至少供应备件 10 年,因此我们希望新的监管制度至少需要同样长的时间。事实上,该指令的序言指出，“消费者通常希望至少在卖方对不合格负责的期限内收到更新，而在某些情况下,消费者的合理期望可能会超出该期限期间,特别是在安全更新方面可能就是这种情况。”鉴于在许多国家/地区,汽车必须通过年度道路适用性测试才能继续使用,并且此类测试可能包括检查软件是否在可预见的未来打了最新补丁,我们很可能会看到对安全补丁的需求延长十年以上。

毫无疑问,当游说者试图削减成本时,会有各种各样的争论,但这是朝着正确方向迈出的一大步。在安全问题上,美国的做法通常效仿欧洲。

Machine Translated by Google

28.5.2 新的研究方向

现在不仅有明确的社会需要长期维护耐用品软件的安全和保障,而且有明确的法律要求,我敦促我的计算机科学家同行们将此作为研究的一项重大挑战。

自 1960 年代以来,由于摩尔定律,我们几乎将计算机视为消耗品。这限制了我们从最低级别的技术细节到最高级别的政策的思考。我们已经将数千个、然后是数百万个、更多的晶体管塞进了芯片,以支持更精细的流水线和缓存。我们已经知道明年的 PC 运行速度会更快,因此我们已经忍受了缓慢而低效的软件。我们对垄断不屑一顾,相信十年后的技术将与今天大不相同,因此我们可以用市场竞争代替市场竞争。我们就像一艘游轮,高兴地把垃圾扔到海里,期望我们会把它远远抛在身后。

摩尔定律现在行不通了。 Hennessy 和 Paterson 对 CPU 性能的分析表明,虽然从 1978 年到 1986 年每年增长 25%,从 1986 年到 2003 年增长高达 52%,但在 2003-11 年放缓至 23%,在 2013-15 年和 2013-15 年放缓至 12%之后是 3.5% [882]。随着聚会的结束,我们将不得不开始清理垃圾。从由 12 级 CPU 管道引起的像 Spectre 这样的边信道攻击,到我们英国媒体报道软件中积累的技术债务,一直到驱动这一切的垄断商业生态系统。

还有很多很多。许多流行的 CA 的根证书开始过期,如果这些证书嵌入到软件无法升级的设备（例如电视)中,那么这些设备基本上就变砖了 [117]。

（最受欢迎的 Letsencrypt 将于 2021 年推出。)当 CA 根证书到期时,您必须更新客户端而不是服务器来修复它们。在消费类设备中,趋势是缩短使用寿命,使加密可更新;正如我在第 21.6 节中讨论的那样,Safari 和 Chrome 等浏览器开始强制执行 398 天证书到期,这是频繁更新的另一个强烈动机。

从石化厂到变电站,许多环境都配备了不常更新的长寿命设备。建筑和土木工程项目中的系统有点混合;一些供应商正在开发预计尽可能稳定并可维护 25 年的 Linux 版本,而其他供应商则推动对整个系统进行更积极的定期更新,并告诉我们“将所有内容都放在云端”。

后一种方法与“智能建筑”模因相关,但也有其自身的缺点。一旦多个承包商和分包商需要在线访问包含建筑物完整工程信息的系统　从变电站到空调再到火灾和防盗警报器　就会出现明显的风险。其中一些承包商在国际范围内运营,因此那里的被颠覆员工或 root 机器可能可以访问数十个国家/地区的关键国家基础设施。我们对此感到满意吗?

适应新常态需要数年时间,因为这需要数百万利益相关者改变行为。我怀疑由此造成的紧张局势

Machine Translated by Google

未来十年,适应将在政策、创业和研究中发挥重要作用。

那么可持续安全研究会是什么样子呢?作为第一个试点项目,我和 Laurent Simon、David Chisnall 负责密码软件的维护。正如我在 19.4.1 节中提到的,TLS 在 20 年前就被证明是安全的,但从那以后每年大约有一次针对它的攻击,主要是通过侧通道进行的。问题之一是加密实现(例如 OpenSSL)通常具有设计用于在恒定时间内执行加密操作的代码,因此使用中的密钥不会泄漏给外部观察者,并且还会将包含密钥材料的内存位置归零或其他敏感数据,以便同一台机器的其他用户也无法推断出密钥。

但时不时地,有人会改进编译器,使其现在明白某些指令不会做任何实际工作。它优化了它们,突然之间,数百万台机器都拥有不安全的加密软件。这非常烦人;你在外面和坏人打架,突然间你的编译器作者在背后捅了你一刀,就像你背后的一个颠覆性的第五纵队。我们的工具匠应该是我们的盟友而不是我们的敌人,因此我们找出了正确解决这个问题所需的条件。像 C 这样的语言无法表达程序员的意图,所以我们想出了如何通过代码注释来做到这一点。让编译器正确执行恒定时间代码和安全对象删除被证明是非常棘手的,但我们最终以 LLVM [1758] 插件的形式获得了概念的工作证明。

还需要很多很多。从低级编译器内部结构到中级安全系统,汽车行业面临的一大挑战是将事故数据提供给可以从中学习的利益相关者。在欧洲,每年约有五万人死于道路交通事故,另有五十万人受伤。在世界范围内,每年有大约 100 万人死亡。随着汽车开始记录控制输入和传感器数据,典型事故的数据有数兆字节,但目前这些数据大多未被分析。数据越来越多地存储在供应商的服务器以及损坏的车辆中。但是,当警方调查重大道路事故时,他们目前无法从数据记录器或车辆中的 1 亿多行软件中获取大部分信息 其中一些将来自附属供应商,并且不确定的出处、版本和补丁状态。在诉讼激烈的情况下,可能会要求提供数据,但供应商不愿意共享数据,而且通常需要法院命令。

应该发生什么?我们应该以学习系统为目标。我们不断听到有人在愚蠢的事故中被自动驾驶汽车撞死的报道 例如,优步在亚利桑那州坦佩杀死了 Elaine Herzberg,因为她在路上推着一辆自行车,而它的软件只检测到人行横道上或附近的行人 [1264]。我们应该期望能够推送更新以阻止这种情况再次发生。那么补丁周期会是什么样子呢?在航空领域,事故受到监控,不仅会向飞行员和空中交通管制员等操作员提供反馈,还会向飞机和支持地面系统的设计人员提供反馈。用于监控涉及医疗设备的事故的系统的工作已经开始,尽管供应商可能会拖延时间。同样,关键是监测不良事件和收集数据的强制性系统。

Machine Translated by Google

现在路口出了好几起事故,我们就修;这就是我们目前所有的“补丁周期”,因为公路部门唯一可用的数据是每次事故的位置和严重程度,再加上主治人员报告中的几句话。随着汽车变得更加自主,汽车的学习系统也是不可避免的,但它们不会自己学习。

学习将涉及分析失败原因、积累工程知识,以及最终涉及多个利益相关者群体的政治。

首先,我们需要从汽车感知到的内容、它们决定做什么以及为什么这样做的细粒度数据。制定法律以将这些数据从供应商提供给事故调查员、保险评估员和其他利益相关者的任务摆在了前面。目前,欧盟成员国负责车辆标准的上市后监督,因此做得很少,在柴油门事件之后,有人提议赋予欧盟委员会监督权。然后就是实际构建这些系统的任务。它们将庞大而复杂,因为需要处理围绕安全、隐私和管辖权的多种相互冲突的权利。

进一步向上移动到政策层面,人们越来越一致认为技术需要更好地监管。在技术日新月异的时候,我们也许可以容忍对隐私和竞争的各种危害。如果您不喜欢 IBM 在 1980 年代的垄断地位,您只需要等到 Microsoft 出现即可;到 90 年代后期微软成为“邪恶帝国”时,拉里和谢尔盖开始了谷歌。 Google+ 对您来说太笨重了吗?不管怎样,试试 Facebook 或 Twitter。但随着摩尔定律失效,我们现在拥有的主导企业可能会在一段时间内保持主导地位 就像铁路在 19 世纪下半叶和 20 世纪上半叶的主导地位一样。在许多其他领域,技术使一些参与者能够锁定市场主导地位;正如我在 2020 年所写的那样,亚马逊是世界上最有价值的公司。我们需要更新对反垄断法的思考。有一些迹象表明这种情况正在发生 [1044]。

你希望二十年后的法律是什么样子的?安全、保障和反托拉斯的部分应该如何组合在一起?

28.6 小结

在过去,安全工程项目中的大问题是如何知道何时完成。设计了各种评估和保证方法来提供帮助。现在世界不同了 。我们永远不会结束,任何说他们已经结束的人都不应该被信任。

安全评估和保证方案在许多不同的生态系统中发展起来。美国军方产生了最初的橙皮书,并启发了密码模块的 FIPS 140 标准和通用标准,这两者都试图向企业和其他国家传播可信系统的福音。安全认证计划在许多行业中分别发展 - 医疗保健、航空航天和公路车辆仅举三个例子。供应商一直在玩弄这些系统,并努力在可能的情况下抓住监管机构。现在一切都在获取连接

Machine Translated by Google

tivity,没有安全就没有安全,这些生态系统正在融合。

在安全和保障方面,重点将从上市前测试转移到监控和响应,这将包括更新现场已有的设备和支持它们的服务。这将超越软件生命周期标准,朝着学习系统的目标迈进,该学习系统甚至可以从新的危害和攻击中快速恢复。

情况正在慢慢好转。早在 20 世纪,许多供应商就没有正确地保护信息安全。到 2010 年,更好的人在第三次或第四次尝试时或多或少地获得了成功。未来,当产品出现故障时,每个人都需要及时合理地修理,并在合理的时间内修理。

但所有这一切的代价,各种设备和服务中安全与安全的纠缠,以及它们与歧视、全球化和贸易冲突等问题的相互作用,将使这些问题日益成为全球政治的焦点。从最广泛的意义上讲,技术给我们带来的安全和安保成本将与国家主权观念以及在更实际的层面上人们通过集体行动实现那些无法通过个人行动实现的目标的能力越来越紧张或市场力量。

正如安全经济学在 2000 年代和安全心理学在 2010 年代成为热门话题一样,我预计安全政治将成为 2020 年代及以后的增长话题。

研究问题

除了我在上面第 28.5.2 节中讨论的可持续安全的巨大挑战之外,还有许多其他围绕保证的开放性问题。我们真的不知道如何在复杂的生态系统中进行保证,例如汽车与在线服务和手机应用程序的对话。第二个问题来自于这样一个事实,即随着安全和安保的世界慢慢融合在一起,就像两个星系慢慢合并一样,我们发现安全工程师和安全工程师不会说彼此的语言,有共同语言兼容的标准集,甚至是不兼容的标准化方法。

在一个又一个行业中解决这个问题需要数年时间。

另一个重大机会可能是轻量级机制可以改进实际部署的系统。太多的研究人员认为“如果它不完美,它就不好。”我们有大量的学术界人士撰写论文,内容涉及可证明的安全性、形式化方法以及由于无法扩展而无法在野外发现的隐蔽攻击。我们有大量的实际问题是由企业在开发上偷工减料而产生的。如果程序员要从 stackexchange 中窃取尽可能多的代码,我们是否需要为了公共利益而努力清理那里的示例以消除缓冲区溢出?我们是否有机会为加密库和设备权限等工具设置安全可用性标准,以便(例如)强制淘汰默认为 ECB 的库,就像 MD5 和 SHA1 一样?

另一个可能是 AI/ML 系统的测试,包括部署前和持续评估。例如,我们已经知道,深

Machine Translated by Google

神经网络和其他 ML 机制与其训练数据一起吸入偏见;由于机器视觉系统主要是根据白人的照片进行训练，因此它们在发现肤色较深的人方面普遍更差,导致人们担心自动驾驶汽车更有可能杀死黑人行人 [2026]。当学习系统涉及有争议的社会问题时,它会是什么样子?在一个并非所有生命都受到同等重视的世界中,您如何实现持续安全?我们如何确保公司做出的安全、隐私和安全工程决策接受公众监督和法律挑战?

进一步阅读

在大量纳税资金的支持下,整个行业都致力于促进安全保障业务。他们的热情甚至可以带有宗教的味道。不幸的是,写异端邪说的人还远远不够。