第1章

什么是安全工程?

从人类的弯曲木材中,没有任何东西是直的。

伊曼纽尔·康德

世界永远不会是完美的,无论是在线还是在线;所以我们不要为在线设置不可能的高标准。

– 埃丝特·戴森

1.1 简介

安全工程是关于构建系统以在面对恶意、错误或意外时保持可靠。作为一门学科,它侧重于设计、实施和测试完整系统所需的工具、过程和方法,并随着环境的发展调整现有系统。

安全工程需要跨学科的专业知识,从密码学和计算机安全到硬件防篡改,再到经济学、应用心理学、组织和法律知识。从业务流程分析到软件工程再到评估和测试的系统工程技能也很重要;但它们还不够,因为它们只处理错误和不幸,而不处理恶意。安全工程师也需要一些对抗性思维的技巧,就像下棋的人一样;您需要研究许多过去有效的攻击,从攻击的开始到发展再到结果。

许多系统都有关键的保证要求。它们的失败可能危及人类生命和环境(如核安全和控制系统),对主要经济基础设施造成严重损害(自动取款机和在线支付系统),危及个人隐私(医疗记录系统),破坏整个商业部门(预付费电表),并促进犯罪(防盗和汽车警报器)。安全和安全正在成为

随着我们在所有事物中都获得软件,它们变得更加交织在一起。即使认为系统比实际情况更脆弱或更不可靠,也会产生实际的社会成本。

传统观点认为,虽然软件工程是关于确保某些事情发生（“John 可以读取此文件”）,但安全是关于确保它们不会发生（“中国政府无法读取此文件”）。现实要复杂得多。一个系统与另一个系统的安全要求大不相同。您通常需要用户身份验证、交易完整性和责任制、容错、消息保密性和隐蔽性的某种组合。

但是许多系统之所以失败,是因为它们的设计者保护了错误的东西,或者保护了正确的东西但却以错误的方式。

因此,获得正确的保护取决于几种不同类型的过程。
你必须弄清楚什么需要保护,以及如何保护。您还需要确保保护和维护系统的人员有适当的积极性。在下一节中,我将设置一个框架来思考这个问题。

然后,为了说明安防和安全系统必须做的不同事情的范围,我将快速浏览一下四个应用领域:银行、军事基地、医院和家庭。一旦我们给出了安全工程师必须理解和构建的 stu 的具体示例,我们将能够尝试一些定义。

1.2 框架

要构建真正可靠的系统,您需要具备四项要素。
有政策:你应该实现什么。有机制:密码、访问控制、硬件防篡改和您用来实施策略的其他机制。有保证:您可以对每个特定机制的依赖程度,以及它们协同工作的程度。

最后,还有动机:保护和维护系统的人必须正确完成工作的动机,以及攻击者必须试图破坏您的策略的动机。所有这些相互作用（见图 1.1）。

例如,让我们想想 9/11 恐怖袭击。劫机者成功通过机场安检拿到刀具并非机制失误,而是政策失误;安检员的工作是将枪支和炸药挡在门外,但当时允许使用刀刃最大为三英寸的刀具。政策变化很快:首先禁止所有刀具,然后禁止大多数武器（现在禁止使用棒球棒,但可以使用威士忌酒瓶）;它在许多细节上都被翻转了（禁止使用丁烷打火机,然后又允许使用）。机制薄弱,因为复合刀具和不含氮的炸药之类的东西。保证总是很差;每个月都有许多吨无害的乘客财产被扔进垃圾桶,而通过检查（无论是意外还是出于测试目的)的所有真实武器中只有不到一半被发现并没收。

大多数政府都将可见措施置于有效措施之上。例如,TSA 在乘客安检上花费了数十亿美元,这相当低效,而花费 1 亿美元用于加固驾驶舱门消除了大部分风险 [1523]。航空公司飞行员安全联盟主席指出,

大多数地面人员都没有经过筛选,几乎没有人注意看守停在地面上过夜的飞机。由于大多数客机没有门锁,因此没有什么可以阻止坏人踏上飞机并在机上放置炸弹;如果他有驾驶技能和一点胆量,他可以提交一份飞行计划并用它来做 o [1202]。然而,筛选人员和守卫飞机并不是当务之急。

为什么会做出这样的政策选择?很简单,对决策者的激励有利于对有效控制的可见控制。结果就是 Bruce Schneier 所说的“安全剧院” 旨在产生安全感而非现实的措施。大多数参与者还有夸大恐怖主义威胁的动机:政客“吓唬选票”(正如奥巴马总统所说),记者出售更多报纸,公司出售更多设备,政府官员建立自己的帝国,和安全学者获得资助。结果是,恐怖分子对民主国家造成的大部分损害都来自反应过度。幸运的是,随着时间的推移,选民们明白了这一点,现在 9/11 事件后的 19 年 浪费的钱更少了。当然,我们刚刚了解到,我们社会的复原力预算本应更多地用于为大流行病做准备。它位居英国风险登记册的首位,但恐怖主义在政治上更具吸引力。更合理地管理优先事项的国家取得了更好的结果。

安全工程师需要了解这一切;我们需要能够将风险和威胁放在背景中,对可能出现的问题做出现实的评估,并为我们的客户提供良好的建议。这取决于对各种系统随着时间的推移出现的问题的广泛理解;什么样的攻击有效,它们的后果是什么,以及它们是如何被阻止的(如果这样做值得的话)。历史也很重要,因为它会导致复杂性,而复杂性会导致许多失败。了解现代信息安全的历史使我们能够理解它的复杂性,并更好地驾驭它。

所以这本书充满了案例。为了说明这一点,我将在这里举几个有趣的安全系统的简短示例,以及它们的设计目的是防止什么。

1.3 示例 1 – 一家银行

银行运行着许多对安全至关重要的计算机系统。

1. 银行的运营依赖于核心簿记系统。这保留了客户账户主文件以及大量记录进出交易的日志。这里的主要威胁是银行自己的员工 ;每年约有 1% 的银行分行员工被解雇,主要是因为轻微的不诚实行为(平均盗窃金额只有几千美元)。传统的防御来自几个世纪以来不断发展的簿记程序。例如,一个账户的每笔借记都必须与另一个账户的贷记相匹配;所以钱只能在银行内转移,不能创造或销毁。此外,大额转账通常需要两个

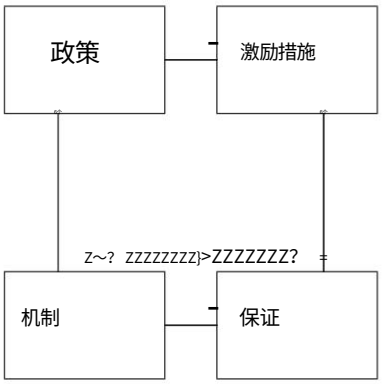

图 1.1：- 安全工程分析框架

人授权他们。还有用于寻找异常交易量或交易模式的警报，并且员工需要定期休假而无法访问银行系统。

2. 一张公众脸是银行的自动取款机。根据客户的卡和个人身份证号码验证交易 以抵御外部和内部攻击 比看起来更难！当当地恶棍（或银行职员 ）发现并利用系统中的漏洞时，在各个国家/地区发生了许多“幻影提款”流行病。自动柜员机也很有趣，因为它们是密码学的第一个大规模商业用途，并且它们帮助建立了许多密码标准。为 ATM 开发的机制已扩展到商店的销售点终端，卡支付在很大程度上取代了现金；并且它们已经适用于其他应用，例如预付费公用事业仪表。

3. 另一个公众形象是银行的网站和手机应用程序。大多数客户现在在网上而不是在分行处理他们的日常业务，例如账单支付以及储蓄账户和支票账户之间的转账。

自 2005 年以来，银行网站受到网络钓鱼的严重攻击 客户被邀请在虚假网站上输入密码。
一旦犯罪分子开始攻击客户而不是银行，1990 年代设计的标准安全机制就变得不那么有效了，因此许多银行现在向您发送带有验证码的短信。骗子的反应是去电话店，假装是你，然后买一部窃取你电话号码的新电话。这场军备竞赛提出了许多引人入胜的安全工程问题，混合了来自身份验证、可用性、心理学、运营和经济学的元素。

4. 幕后是高价值的消息传递系统，用于在银行之间转移大笔款项；进行证券交易；签发信用证和

担保;等等。对这样一个系统的攻击是高科技犯罪分子的梦想 我们听说朝鲜政府通过对银行的攻击窃取了数百万美元。防御是簿记控制、访问控制和密码学的混合体。

5. 银行的分支机构可能看起来很大、稳固和繁荣,让客户放心他们的钱是安全的。但石头立面是戏剧而不是现实。如果你带着枪走进去,出纳员会把你能看到的所有现金都给你;如果您在夜间闯入,您可以在几分钟内用砂轮打碎保险箱。有效控制以报警系统为中心,报警系统连接到安保公司的控制中心,安保公司的工作人员通过视频检查情况并在必要时报警。密码学用于防止强盗操纵通信并使警报看起来像是在说“一切都好”,而实际上却不是。

我将在后面的章节中介绍这些应用程序。银行计算机安全很重要:直到 2000 年代初,银行是许多计算机安全产品的主要民用市场,因此它们对安全标准产生了巨大影响。

1.4 示例 2 – 军事基地

军事系统是 20 世纪的另一个技术驱动力,因为它们激发了政府从 1980 年代初开始资助的计算机安全方面的大部分学术研究。与银行业一样,应用程序不止一种,而是多种多样。

1. 军事通信推动了密码学的发展,可以追溯到古埃及和美索不达米亚。但仅仅加密信息通常是不够的:看到用其他人的密钥加密的 trac 的敌人可能会简单地定位并攻击发射器。低截获概率 (LPI) 无线电链路是一个答案;他们使用的技巧现在已在日常通信中采用,例如蓝牙。

2. 从 1940 年代开始,政府在电子战系统上投入了大量资金。试图干扰敌方雷达同时防止敌人干扰你的雷达的军备竞赛导致了许多复杂的欺骗技巧、对策和反对策 其战略的深度、微妙性和范围在其他地方仍然找不到。

   早在勒索者开始针对银行家、博彩公司和游戏玩家的网站之前,欺骗和拒绝服务攻击就已经成为现实。

3. 军事组织需要保密一些信息,例如情报来源和未来行动计划。这些通常被标记为“最高机密”并在单独的系统上处理;它们可能被进一步限制在隔间中,因此只有少数人知道最敏感的信息。多年来,人们一直在尝试执行信息流规则,因此您可以将文件从机密存储系统复制到绝密命令系统,但反之则不行。管理多个

具有信息流限制的系统是一个难题,花费数十亿美元试图实现军事安全自动化帮助开发了您现在在手机和笔记本电脑中拥有的访问控制技术。

4. 保护核武器的问题导致了许多很酷的安全技术的发明,从可证明安全的身份验证系统到光纤警报传感器,再到使用生物识别技术识别人员的方法 包括现在用于识别身份的虹膜模式识别所有印度公民。

安全工程师还是可以从中学到很多东西的。例如,直到最近,军方还是少数需要维护数十年的软件系统客户之一。现在,软件和互联网连接正在进入汽车等对安全至关重要的消费品领域,软件可持续性正成为一个更广泛的问题。 2019 年,欧盟通过了一项法律,要求如果您销售带有数字组件的商品,则必须将这些组件维护两年,如果客户有合理的期望,则必须维护更长时间 这意味着汽车和白色家电需要维护十年.如果您正在为将销售 7 年的汽车或冰箱编写软件,您将不得不维护它近 20 年。你应该使用什么工具?

1.5 示例 3 – 一家医院

我们从银行家和士兵转向医疗保健。医院有许多有趣的保护要求 主要与患者安全和隐私有关。

1、安全可用性对于医疗设备来说很重要,绝不是一个可以解决的问题。据估计,安全可用性故障导致的死亡人数与道路交通事故的死亡人数相当 例如,美国每年有几万人死亡,英国也有几千人死亡。最大的一个问题是用于向患者滴注药物的输液泵;一家典型的医院可能有六个品牌,所有品牌的控制都略有不同,因此更有可能出现致命错误。安全可用性与安全性相互作用:还被发现可被黑客入侵的不安全设备更有可能下令产品召回,因为监管机构知道当敌对行动成为可能时,公众对风险的偏好会大大降低。因此,随着越来越多的医疗设备不仅需要软件,还需要无线电通信,安全敏感性可能会带来更好的安全性。

2. 患者记录系统不应让所有员工看到每个患者的记录,否则可能会侵犯隐私。事实上,自本书第二版以来,欧洲法院已裁定患者有权将其个人健康信息限制在参与其护理的临床人员中。这意味着系统必须实施诸如“护士可以在过去 90 天内随时查看在其部门接受过护理的任何患者的记录”之类的规则。这可以是

比看起来更难。 （美国 HIPAA 立法制定了更简单的合规标准,但仍然是信息安全投资的驱动力。）

3. 病历通常被匿名用于研究,但这很难做好。仅仅对患者姓名进行加密是不够的:诸如“向我展示所有在 2003 年 10 月 19 日接受心房颤动治疗的 1953 年出生的男性”这样的查询应该足以针对前首相托尼·布莱尔,他当天被紧急送往医院接受治疗接受心律不齐的治疗。弄清楚哪些数据可以有效地匿名化是很困难的,而且随着我们获得越来越多的社会和背景数据,它也是一个不断变化的目标 更不用说远近亲戚的基因数据了。

4. 新技术会引入鲜为人知的风险。医院管理人员了解需要备份程序来处理断电;即使主电源和供水出现故障,医院也应该能够处理伤员。但在 2017 年 5 月英国的几家医院的机器被 Wannacry 恶意软件感染后,他们关闭了网络以限制进一步感染,然后发现他们不得不关闭事故和急诊科 因为 X 射线不再从医院传播将 X 光机装在一个信封中送到手术室,但要通过一个位于遥远城镇的服务器。因此,网络故障可以阻止医生操作,而电源故障则不会。有备用发电机,但没有备用网络。平均而言,云服务可以使事情更可靠,但故障可能更大、更复杂且相关。冠状病毒大流行引发的一个问题是附件控制:一些医疗设备会验证其备件,就像打印机验证墨盒一样。虽然供应商声称这是为了安全,但实际上是为了他们可以收取更多的备件费用。

但它带来了脆弱性:当供应链中断时,事情就更难修复了。

稍后我们将更详细地研究医疗系统安全性（以及安全性）。
这是一个比银行 IT 或军事系统更年轻的领域,但由于在所有发达国家中医疗保健占国民生产总值的比例高于其中任何一个,因此它的重要性正在增加。在强制报告的国家,它也一直是隐私泄露的最大来源。

1.6 示例 4 – 家

您可能认为典型的家庭不会运行任何安全系统。但只要停下来想一想。

1. 您可能会使用我已经描述过的一些系统。您可以使用基于网络的电子银行系统来支付账单,您可以在线访问您的医生的手术室,以便您可以重复开处方。如果您患有糖尿病,那么您的胰岛素泵可能会与您床边的扩展坞通信。您的家庭防盗警报器可能会发送

每隔几分钟向安保公司发送加密的“一切安好”信号,而不是在发生事情时唤醒邻居。

2. 您的汽车可能装有电子防盗器。如果它是在 2015 年左右之前制造的,那么当您按下钥匙上的按钮时,汽车就会解锁,这会发送加密的解锁命令。如果是较新的车型,您无需按任何按钮,只需将钥匙放在口袋里,汽车就会向钥匙发送加密挑战并等待正确的响应。但是取消按钮意味着如果你把钥匙放在前门附近,小偷可能会使用无线电中继来偷你的车。

自从这项技术被引入以来,汽车盗窃案急剧上升。

3. 您的手机通过类似于车门锁和防盗器中使用的加密质询-响应协议向网络验证自己,但警察可以使用虚假基站（在欧洲称为 IMSI-catcher,在America as a Stingray)来收听。而且,正如我上面提到的,许多电话公司对向声称手机被盗的人出售新 SIM 卡并不在意;所以骗子可能会窃取您的电话号码并用它来袭击您的银行帐户。

4. 在 100 多个国家/地区,家庭可以获得预付费电表和煤气表,他们使用从 ATM 或在线服务购买的 20 位代码进行充值。它甚至可以在 o -grid 上运行;在肯尼亚的村庄,无法支付 200 美元购买太阳能电池板的人可以每周支付 2 美元购买一个,并使用他们用手机购买的代码解锁它产生的电力。

5. 最重要的是,家提供了一个人身安全和隐居的避风港。
这正在以多种方式发生变化。窃贼不像住户那样担心锁,因此警报和监控系统可以提供帮助;但监控也变得无处不在,许多家庭购买了 Alexa 和 Google Home 等系统来听人们说什么。随着语音和手势界面的普及,各种其他小工具现在都配备了麦克风和摄像头,并且语音处理通常在云端完成以节省电池寿命。到 2015 年,奥巴马总统的科学技术顾问委员会预测,很快地球上每个有人居住的空间都会有连接到少数云服务提供商的麦克风。 （美国和欧洲对隐私法应如何处理这一问题有着截然不同的看法。）不管怎样,你家的安全可能会依赖于你几乎无法控制的远程系统。

在接下来的几年中,此类系统的数量将迅速增加。根据以往的经验,其中很多都会设计得很糟糕。例如,2019 年,欧洲禁止使用未加密通信方式与供应商的云服务通信的儿童手表;窃听者可以下载任何孩子的位置历史记录,并让他们的手表拨打世界上任何号码。发现这一点后,欧盟下令立即安全召回所有手表 [901]。

本书旨在帮助您避免此类结果。要设计出安全可靠的系统,工程师需要了解有哪些系统、它们如何工作,以及 至少同样重要 它们在过去是如何失败的。

土木工程师从一座倒塌的桥梁中学到的东西远比从一百座屹立不倒的桥梁中学到的要多;在安全工程中也是如此。

1.7 定义

安全工程中使用的许多术语直截了当,但有些术语具有误导性,甚至引起争议。相关章节中有更详细的技术术语定义,您可以使用索引查找。在本节中,我将尝试指出主要问题所在。

我们需要澄清的第一件事是系统的含义。在实践中,这可以表示:

1. 产品或组件,例如加密协议、智能卡或电话、笔记本电脑或服务器的硬件;
2. 以上一项或多项加上操作系统、通信和其他基础设施;
3. 以上加上一个或多个应用程序(银行应用程序、健康应用程序、媒体播放器、浏览器、账户/工资包等 包括客户端和云组件);
4. 以上任何一项或全部加上 IT 人员 ;
5. 以上任何一项或全部加上内部用户和管理;
6. 上述任何或所有加上客户和其他外部用户。

上述定义之间的混淆是错误和漏洞的肥沃来源。从广义上讲,供应商和评估者社区关注第一个和(偶尔)第二个,而企业将关注第六个(偶尔是第五个)。我们会遇到许多系统的例子,这些系统被宣传为安全,甚至被认证为安全,因为硬件是安全的,但当特定应用程序运行时,或者当设备以设计人员未预料到的方式使用时,它们会严重崩溃。忽视人为因素,从而忽视可用性问题,是安全失败的最大原因之一。所以我们一般会使用定义6;当我们采取更严格的观点时,从上下文中应该清楚。

下一组问题来自于对球员是谁以及他们试图证明什么缺乏明确性。在关于安全和密码学的文献中,安全协议中的主体由(通常)连续的首字母选择的名称来标识 很像飓风,只是我们使用交替的性别。所以我们看到很多语句,例如“Alice 向 Bob 验证了自己的身份”。这使事情更具可读性,但可能会以牺牲精度为代价。我们是说 Alice 向 Bob 证明她的名字实际上是 Alice,还是她证明了她有特定的证书?

我们的意思是认证是由人类 Alice 完成的,还是由充当 Alice 代理的智能卡或软件工具完成的?在那种情况下,我们确定它是

爱丽丝,也许不是爱丽丝借给她卡的卡罗尔,或者偷了她手机的大卫,或者黑了她笔记本电脑的夏娃?

我所说的主体是指担任任何角色的自然人,包括操作员、委托人或受害者。我所说的人是指自然人或法人,例如公司或政府 1。

委托人是参与安全系统的实体。这个实体可以是一个主题、一个人、一个角色或一件设备,例如笔记本电脑、电话、智能卡或读卡器。委托人也可以是通信通道(可能是端口号或加密密钥,具体取决于具体情况)。

委托人也可以是其他委托人的复合物;例子有一个组(Alice 或 Bob)、一个连词(Alice 和 Bob 一起行动)、一个复合角色(Alice 充当 Bob 的经理)和一个委托(Bob 在 Alice 不在时充当她的角色)。

请注意,组和角色是不一样的。我所说的一个组是指一组负责人,而一个角色是由不同的人连续承担的一组职能(例如“尼米兹号航空母舰上的值班指挥官”或“现任总统”)冰岛医学协会”)。委托人可以在多个抽象级别上考虑:例如,“Bob 在 Alice 不在时代表她”可能意味着“Bob 的智能卡代表 Bob 在 Alice 不在时代表 Bob”,甚至是“Bob 在 Alice 不在时操作她的智能卡”.

当我们必须考虑更多细节时,我会更具体。

身份这个词的含义是有争议的。当我们必须小心时,我会用它来表示两个负责人的名字之间的对应关系,表示他们指的是同一个人或同一设备。例如,了解“Alice 作为 Bob 的经理”中的 Bob 与“Bob 作为 Charlie 的经理”和“Bob 作为分行经理与 David 共同签署银行汇票”中的 Bob 相同可能很重要。通常,身份被滥用为简单的“姓名”,这种滥用由诸如“用户身份”和“公民身份证”等短语根深蒂固。

信任和值得信赖的定义经常混淆。以下示例说明了差异:如果在巴尔的摩华盛顿国际机场的厕所隔间观察到一名 NSA 员工向中国外交官出售关键材料,那么(假设他的操作未获授权)我们可以将他描述为“受信任但不值得信赖 。我使用 NSA 的定义,可信系统或组件是指其故障会破坏安全策略的系统或组件,而可信系统或组件是不会发生故障的系统或组件。

信任有许多替代定义。在企业界,可信系统可能是“如果在我的手表上被黑客入侵也不会让我被解雇的系统”,甚至是“我们可以确保的系统”。但当我指的是经批准的系统、可保险系统或保险系统时,我会这么说。

机密性与隐私与秘密的定义打开了另一个蠕虫病毒。这些术语重叠,但不完全相同。如果我的邻居在我们共同的篱笆上砍掉了一些常春藤,结果他的孩子们可以看到我的花园并逗弄我的狗,那不是我的保密问题

1当我们开始必须围绕 AI 制定规则时,围绕公司的法律可能会派上用场。一个公司,就像一个机器人,可能是不朽的并且有一些功能性智能 但没有意识。你不能监禁一家公司,但你可以对其处以罚款。

入侵。对前雇主的私事保持沉默的义务是一种保密义务,而不是隐私义务。

我将使用这些词的方式如下。

- 保密性是一个工程术语,指的是用于限制可以访问信息的主体数量的机制的效果,例如密码学或计算机访问控制。

- 保密涉及保护其他人或
  组织的秘密,如果你知道的话。

- 隐私是保护您的个人信息的能力和/或权利,并延伸到防止侵犯您的个人空间的能力和/或权利(其确切定义因国家/地区而异)。隐私可以延伸到家庭,但不能延伸到公司等法人。

例如,医院的病人有隐私权,为了维护这项权利,医生、护士和其他工作人员对他们的病人负有保密义务。医院在其业务交易方面没有隐私权,但那些了解隐私权的员工可能有保密义务(除非他们援引举报权来揭露不当行为)。

通常,隐私是为了个人利益而保密,而保密是为了组织利益而保密。

更复杂的是,保护数据(例如消息内容)通常是不够的;我们还必须保护元数据,例如谁与谁交谈的日志。例如,许多国家/地区的法律对性传播疾病的治疗保密,但如果私家侦探可以观察到您与性传播疾病诊所交换加密信息,他可能会推断您正在那里接受治疗。事实上,英国的一个关键隐私案件就是这样一个事实:英国的一名模特赢得了针对一家小报的隐私诉讼,该小报刊登了一张她离开戒毒匿名组织会议的照片。因此,匿名性在隐私(或机密性)方面可能与保密一样重要。但是匿名很难。自己匿名是很困难的;你通常需要在人群中躲藏。

此外,我们的法律法规并非旨在支持匿名:警方从电话公司获得详细的账单信息(告诉他们谁给谁打过电话)比获得实际窃听要容易得多。(而且它通常更有用。)

真实性和完整性的含义也可以微妙地变化。在关于安全协议的学术文献中,真实性意味着完整性和新鲜度:你已经确定你是在和一个真正的委托人交谈,而不是重播以前的消息。我们在银行协议中有类似的想法。如果当地银行法规定支票在六个月后不再有效,则七个月前未兑现的支票具有完整性(假设未被更改)但不再有效。但是,有一些奇怪的边缘情况。例如,警方犯罪现场官员会将伪造的支票放入证物袋中,以保持伪造支票的完整性。(完整性的含义在新上下文中发生了变化,不仅包括签名,还包括任何指纹。)

我们不想要的东西通常被描述为黑客攻击。我将遵循 Bruce Schneier 并将 hack 定义为系统规则允许的事情,但这是其设计者未预料到和不希望发生的事情 [1679]。例如,税务律师研究税法以找出漏洞,并将其发展为避税策略;以完全相同的方式,黑帽研究软件代码以发现他们开发成漏洞利用的漏洞。黑客不仅可以针对税收系统和计算机系统,还可以针对市场经济、我们的选举领导人系统甚至我们的认知系统。它们可能发生在多个层面:律师可以破解税法,或者向上移动并破解立法机关,甚至媒体。以同样的方式,您可能会尝试通过发现加密算法中的数学弱点来破解密码系统,或者您可以降低一个级别并测量实现它的设备所消耗的功率以计算出密钥,或者向上一个级别并欺骗设备的保管人在他们不应该使用它时使用它。这本书包含了很多例子。在更广泛的背景下,黑客攻击有时是重大创新的源泉。

如果黑客变得流行,则可能会更改规则以阻止它;但它也可能会变得规范化(例子包括从图书馆到阻挠议案再到搜索引擎和社交媒体)。

我要在这里澄清的最后一件事是描述我们正在努力实现的目标的术语。漏洞是系统或其环境的一个属性,它与内部或外部威胁一起可能导致安全故障,即违反系统的安全策略。我所说的安全策略是指对系统保护策略的简明陈述(例如,“在每笔交易中,贷方和借方的总和相等,所有超过 1,000,000 美元的交易必须由两名经理授权”)。安全目标是一个更详细的规范,它规定了在特定产品中实施安全策略的方式 加密和数字签名机制、访问控制、审计日志等 并将用作衡量标准评估工程师是否完成了适当的工作。在这两个级别之间,您可能会发现类似于安全目标的保护配置文件,只是以充分独立于设备的方式编写,以允许在不同产品和同一产品的不同版本之间进行比较评估。我将在第 3 部分详细说明安全策略、安全目标和保护配置文件。一般来说,保护一词将表示诸如机密性或完整性之类的属性,以非常抽象的方式定义,以便我们在一般上下文中对其进行推理系统而不是具体的实现。

这在某种程度上反映了我们用于安全关键系统的术语,并且由于我们将不得不在越来越多的应用程序中同时设计安全性和安全性,因此将两者并排考虑是很有用的。

在安全领域,关键系统或组件是指其故障可能导致事故的系统或组件,如果存在危险 一组内部条件或外部环境。危险是危险导致事故的概率,风险是事故发生的总体概率。因此,风险是危害水平与危险和潜伏期的结合 危害暴露和持续时间。不确定性是风险无法量化的地方,而安全是避免事故发生的地方。然后我们有一个安全政策,它给我们一个简洁的声明,说明如何将风险保持在可接受的阈值以下(这可能包括简洁,例如“不要将炸药和雷管放在同一辆卡车上”,到更多

用于医学和航空的复杂政策）;在下一个级别,我们可能会发现必须为特定组件（例如飞机、飞机发动机甚至飞机发动机的控制软件)制定安全案例。

1.8 总结

“安全”是一个非常多的词,对于不同的人来说,它通常意味着非常不相容的东西。对于公司而言,这可能意味着能够监控所有员工的电子邮件和网页浏览;对于员工来说,这可能意味着能够在不受监控的情况下使用电子邮件和网络。

随着时间的推移,控制系统设计的人越来越多地使用安全机制来获得相对于其他使用它的人的商业优势,我们可以预料到冲突、混乱和语言的欺骗性使用会增加。

让人想起刘易斯卡罗尔的一段话：

> “当我使用一个词时，”矮胖子用相当轻蔑的语气说，“它的意思就是我选择它的意思不多也不少。” “问题是，”爱丽丝说，“你是否可以让单词表达这么多不同的意思。”“问题是，”矮胖子说，“哪一个才是主人 仅此而已。”

安全工程师必须对单词在不同应用程序中获得的含义的不同细微差别敏感,并且能够形式化安全策略和目标的实际含义。对于希望逃脱惩罚的客户来说,这有时可能会带来不便,但一般来说,稳健的安全设计需要明确保护目标。