第15章

核指挥和控制

在德国和土耳其,他们看到了特别令人痛苦的场景。跑道上停着一架德国（或土耳其)快速反应警戒飞机,满载核武器,驾驶舱内有一名外国飞行员。飞机已准备好在最早的警告下起飞,核武器也已全面投入使用。美国控制的唯一证据是一名孤独的 18 岁哨兵,他手持卡宾枪站在停机坪上。当德国机场的哨兵被问及如果飞行员突然决定紧急起飞（通过个人任性或通过德国指挥部绕过美国指挥部的命令）,他打算如何保持对核武器的控制时,哨兵回答说他会射击飞行员;阿格纽指示他发射炸弹。

– 杰罗姆·维斯纳 (Jerome Wiesner),向肯尼迪总统报告古巴危机后的核武器指挥与控制

15.1 简介

未经授权使用核武器或核技术扩散可能造成的灾难性危害,已导致美国和其他核大国花费巨额资金保护核弹头以及支持性基础设施、工业和材料。

核军备控制是国际外交的核心:虽然朝鲜现在拥有核弹,但南非和利比亚被说服放弃核弹,伊朗的计划已被停止（通过外交和网络手段）,而伊拉克和叙利亚已经拥有了他们的核武器大规模杀伤性武器计划被强制终止。

数量惊人的核安全专业知识已经公布。事实上,即使这被认为是可取的,也有多少可以保密的限制。许多国家有能力生产核武器,但

决定不（日本、澳大利亚、瑞士……）因此保持对民用核材料的控制。许多真正的不扩散力量是文化上的，是多年来通过外交和核大国的克制建立起来的，这些核大国自 1945 年以来就禁止使用这些武器，即使在面对无核国家的失败时也是如此。这是由国际原子能机构 (IAEA) 强制执行的国际协议支持的，例如《不扩散条约》和《核材料实物保护公约》[949]。

民用反应堆每年生产大约 10 吨钚，如果人类要长期依赖核能，那么我们将在反应堆中燃烧它，并将其作为燃烧铀。因此，我们必须以激发国际信心的方式保护这些事实 不仅是在政府之间，而且来自越来越多持怀疑态度的公众1。

范围广泛的安全技术已从核计划中剥离出来。
美国能源部武器实验室 桑迪亚、劳伦斯利弗莫尔和洛斯阿拉莫斯 已经工作了两代人，以使核武器和材料尽可能安全。我已经提到了他们的一些更普通的衍生产品，从发现超过 12 位的密码在战场条件下无法使用到高端防盗警报系统。将光纤缠绕在要保护的设备上并使用干涉效应检测小于一微米的长度变化的技巧也是他们的一个技巧 它被设计成环绕军械库中的弹头并发出警报如果它们中的任何一个被移动，都不会失败。

在后面的章节中，我们将看到更多的核起源技术。例如，虹膜识别 已知最准确的个人生物特征识别系统，现在用于印度的 Aadhar 身份识别系统 是利用美国能源部的资金开发的，用于控制进入钚库，以及大部分专业知识防篡改和篡改传感技术最初是为了防止滥用被盗武器或控制设备而发展起来的。 9/11 之后，美国及其盟国采取了许多积极措施来控制核扩散，包括：

1. 2003 年 3 月入侵伊拉克，宣战理由是伊拉克拥有大规模杀伤性武器；

2. 2003 年 12 月利比亚同意放弃未申报的武器
   程序；

3. 2004年，巴基斯坦核计划高级科学家阿卜杜勒·卡迪尔·汗帮助叙利亚、利比亚、伊朗和朝鲜等多个国家掌握武器技术，并瓦解了他的网络；

4. 2007 年 9 月 6 日以色列在 Deir-ez-Zor 附近的疑似叙利亚反应堆遭到轰炸的“盒子外”行动；

1 例如，英国政府在 2007 年严重尴尬，当时其钚库存的安全性受到著名科学家的批评 [1626]，而在 2018 年，议会公共账户委员会再次批评武器计划的设施摇摇欲坠、劳动力老龄化、专家人员短缺地方性资金和实际问题 [1560]。

5. 伊朗与美国、英国、俄罗斯、中国、法国、德国和欧盟达成的 2015 年联合全面行动计划

武器计划。

并非所有的努力都取得了成功,朝鲜就是一个明显的例子,它于 1994 年与美国签署了一项条约,以停止武器开发以换取石油运输和帮助发展民用核能。这在 2003 年崩溃了,之后平壤退出了《不扩散核武器条约》并发展了武器。这段历史让许多人担心特朗普政府 2018 年放弃与伊朗的协议（尽管伊朗遵守协议)可能产生的长期影响。然后还有它在 2019 年放弃了与俄罗斯的《中程核力量条约》（尽管这是俄罗斯作弊的结果）;以及巴拉克奥巴马于 2010 年签署的新 START 条约将于 2021 年 2 月到期,除非美国在 2020 年 11 月选出一位同意续签该条约的总统。

核控制不仅仅适用于弹头和制造弹头所需的裂变材料。 9/11 之后,我们了解到基地组织曾谈论过“脏弹” 一种将放射性物质散布到城市街区的装置 它可能不会杀死任何人,但可能会导致恐慌,而在金融中心可能会导致巨大的经济损失。因此,在 2007 年,GAO 调查人员成立了一家虚假公司,并从核监管委员会获得了许可证,授权他们购买同位素。许可证打印在普通纸上;调查人员修改了它以改变他们被允许购买的材料数量,然后用它订购了数十个含有镅 241 和铯 137 的水分密度计,这些水分密度计本可以用于脏弹 [1112]。由于对恐怖主义的恐惧,核材料的控制已经加强,并在经济中更广泛地传播。

核安全不断地教导我们有关保证限度的教训。
例如,很容易假设,如果您不希望发生的某个动作由于人为错误而发生的概率为十分之一,那么通过让五个不同的人进行检查,您可以将概率降低到十万分之一。美国空军也这么认为。然而,在 2007 年 10 月,一架从北达科他州迈诺特空军基地向路易斯安那州巴克斯代尔运送巡航导弹的飞机误装了六枚装有实弹头的导弹后,六枚美国氢弹失踪了 36 小时。所有导弹都应该由储存区的处理人员检查,并根据时间表（已过时)进行检查,地勤人员在移动任何导弹之前等待检查完成,（他们没有）,由地面机组人员检查导弹（他们没有从玻璃舷窗看弹头是真弹头还是假弹头）,由司机将识别号报给控制中心（那里没有人费心去检查）,最后由领航员检查在他的飞行前检查期间（他没有用实弹看机翼）。飞机起飞,飞往路易斯安那州,降落,在无人看管的情况下在跑道上停留了 9 个小时,然后地勤人员赶到卸载导弹并发现它们是活的 [187, 549]。这说明了共享控制的限制之一。人们会依赖他人而懈怠 这一教训在医疗安全领域也广为人知。事实上,在美国空军的案例中,事实证明飞行员已经用他们的“非正式”时间表取代了官方程序

自己的。那么,您如何才能设计出不会以这种方式失败的系统呢?

在本章中,我描述了核安全环境和一些可能在其他地方应用(或构成威胁)的技巧。它是从公共资源中收集而来的 但即便如此,仍有一些有用的教训可供吸取。

15.2 命令与控制的演变

第一颗用于战斗的原子弹是投在广岛的“小男孩”。它的安全性是临时凑合的。它带有三个雷管,一旦飞机升空,武器主管就应该用红色的活雷管代替绿色的假雷管。然而,一些重载的 B-29 在从他们使用的基地天宁岛起飞时坠毁了。埃诺拉·盖伊的武器主管、海军上校迪克·帕森斯估计,如果飞机坠毁,底火可能会爆炸,引爆炸弹并摧毁该岛。因此,他在突袭前一天练习拆除和重新安装底火 大约一条面包大小的火药装药 这样他就可以在 takeo 之后安装它。

条令已经远离即兴创作,如果有的话,我们现在处于另一个极端,机制和程序由来自不同机构的多位专家进行测试、演练、演练和分析。这是一个进化过程。当武器在 1950 年代开始由单座战术飞机携带并且挂在机翼下而不是挂在炸弹舱时,再也不可能手动插入一袋火药了。

有一个组合锁的动作:飞行员将在起飞后通过将 6 位代码输入带有金属线密封盖的特殊键盘来启动炸弹。这启用了一些中央控制;飞行员可能只有在升空后才能获得密码。

但 1950 年代的技术和程序控制都是原始的。

15.2.1 肯尼迪备忘录

古巴导弹危机改变了这一切。苏联 B-59 是一艘狐步舞级柴电潜艇,它于 1962 年 10 月 27 日遭到攻击,当时由航空母舰伦道夫号和 11 艘驱逐舰组成的美国战斗群开始在附近投放深水炸弹。这些是练习弹,投下是为了迫使潜艇浮出水面进行识别;但是船长瓦伦丁·萨维茨基认为他受到了攻击,战争已经开始,所以他应该发射一枚核鱼雷来摧毁航母。但这只有在船上的三名高级船员同意的情况下才能完成,幸运的是,其中一位 Vasily Arkhipov 拒绝了。最终潜艇浮出水面并返回俄罗斯。

这使得世界大战可能意外爆发的风险对美国决策者来说非常突出,肯尼迪总统命令他的科学顾问杰罗姆维斯纳进行调查。他报道说,美国有数百枚核武器存放在希腊和土耳其等盟国,这些国家不是特别稳定,偶尔会互相打架。这些武器受到象征性的美国保管部队的保护,因此这些武器没有物理原因

不能在危机时刻抓住。还有一些人担心美国官员未经授权使用核武器 例如,如果当地指挥官在压力下认为“只要他们知道华盛顿的情况有多糟糕,他们就会让我们使用炸弹。”在 [1825] 中,我们找到了本章开头引用的段落。

肯尼迪的回应是国家安全行动备忘录 no。 160 [217]。它下令,美国随后分散给北约指挥的 7,000 件核武器,无论是在美国还是在盟军的监管下,都应该通过技术手段得到美国的积极控制。尽管这项政策以保护美国核武器不受外国人侵害为由卖给了国会,但对疯狂的“奇爱博士”(或现实生活中的萨维茨基船长)的担忧实际上排在威斯纳的首位。

能源部已经在研究武器安全装置。
基本原则是在武器启动之前必须感知环境的独特方面。例如,导弹弹头和一些自由落体炸弹必须经历零重力,而炮弹必须经历数千 G 的加速度。只有一个例外:原子爆破弹药。这些被设计成由地面部队带到他们的目标并使用时间引信引爆。似乎没有用于防止意外或恶意引爆的独特环境传感器的余地。

当时正在开发的解决方案是一个秘密的武装代码,它可以激活一个埋在武器中心钚坑深处的电磁安全锁。
主要的工程问题是维护。当锁暴露时,例如更换电源时,密码可能会被知道。因此,在每件武器中使用相同的代码是不可接受的。组代码是一种可能性 只有一小部分弹头共享发射代码。

根据肯尼迪备忘录,建议所有核弹都应使用密码锁进行保护,并且应该有一个只有总统或其合法继任者才能给出的“通用解锁”行动信息。问题是找到一种方法将此代码安全地转换为大量单独的发射代码,每个发射代码都可以启用一小批武器。

这个问题在 1960 年代和 70 年代变得更糟,当时的原则从大规模报复转变为“有节制的反应”。总统现在需要能够武装选定的批次(例如“德国的所有核大炮”),而不是武装所有核武器或不武装核武器。这开始将我们引向一个有些复杂的系统,尤其是当我们意识到出于维护目的我们也需要解除武装代码,以及一些在武器安全和有效指挥之间进行权衡的方法。

15.2.2 授权、环境、意图

深层次的问题是核安全系统和命令系统应该执行的安全策略。美国出现的是“授权、环境、意图”的规则。弹头要引爆,必须满足三个条件。

授权:有关武器的使用必须经过授权

由国家指挥机构（即总统及其合法继任者)执行。

环境:武器必须感知到环境的适当方面。 （对于原子爆破弹药,这一要求可以通过使用特殊容器来代替。）

意图:指挥飞机、船只或其他单位的指挥官必须明确指挥武器的使用。

在早期系统中，“授权”意味着进入设备的四个
数字授权码。

发出“意图”信号的方式取决于平台。飞机通常使用六位数的待命或“使用控制”代码。洲际弹道导弹的指挥控制台由两名人员操作,每人必须进入并转动钥匙才能发射火箭。无论实施如何,都必须有一个独特的信号;从六位代码派生的 22 位被认为是从可用性到最小化意外武装风险的许多因素之间的良好权衡 [1349]。

15.3 无条件安全认证

核指挥和控制推动了一次性验证码理论的发展。正如我在第 5 章“密码学”中所描述的,这些在概念上类似于为保护电汇汇款而发明的测试密钥,因为将密钥转换应用于消息以产生一个短的验证代码,也称为验证器或标签。由于密钥仅使用一次,因此可以使身份验证代码无条件地安全,因为它们提供的保护独立于攻击者可用的计算资源。因此,他们为身份验证所做的工作就像一次性一密本为保密工作所做的那样。

回想一下,我们仍然必须选择代码长度来限制成功猜测的概率;这可能会有所不同,具体取决于对手是试图从头开始猜测有效消息（模拟)还是修改现有的有效消息以获得另一个有效消息（替换）。在第 5 章讨论的 GCM 操作模式中,它们在2128处设置为相等,但情况并非如此。

一个例子应该可以清楚地说明这一点。假设指挥官与下属商定了一种身份验证方案,根据该方案,指令将被编码为从 000 到 999 的三位数字。该指令可能有两个值：“攻击俄罗斯”和“攻击中国”。其中一个将编码为偶数,另一个编码为奇数:这将成为密钥的一部分。消息的真实性将通过使其余数除以 337 等于密钥的第二部分的秘密数字来证明。

假设关键是：

· “攻击俄罗斯”编码为偶数，“攻击中国”编码为奇数

· 真实消息除以 337 后的余数为 12。

所以“进攻俄罗斯”是“686”（或“12”）而“进攻中国”是“349”。

一个占据了指挥官与下属通信通道,知其谋而不知秘钥的敌人,成功冒充指挥官的概率只有337分之一。

然而,一旦他看到一条有效消息（比如“12”表示“攻击俄罗斯”）,他就可以通过添加 337 轻松地将其更改为另一个,这样（前提是他理解指挥官的意图)他可以将导弹发送到其他国家。所以在这种情况下成功替换攻击的概率是 1。

与计算安全身份验证一样,无条件变体可以提供或不提供消息保密性:它可能像分组密码一样工作,或者像明文消息上的 MAC 一样工作。同样,它可以使用或不使用仲裁员。人们甚至可能需要多个仲裁员,这样他们就不必单独信任。方案还可以结合无条件和计算安全性。

例如,一个没有保密性的无条件代码可以通过使用传统密码系统简单地加密消息和认证符来添加计算安全的保密性。

身份验证在某种意义上是编码的对偶,在后者中,给定错误消息,我们希望有效地找到最近的正确消息;在前者中,我们希望找到正确的消息是不可能的,除非您已经看到它或被授权构建它。正如纠错码的设计者希望针对给定的错误恢复能力使用最短的代码长度,验证码的设计者也希望最小化实现给定欺骗概率界限所需的密钥长度。

在您拥有一个功能完备的命令和控制系统之前,必须修复很多细节。你必须想办法将关键控制机制构建到弹头中,以防止人们在不解除钥匙的情况下解除武装或拆除。您需要生成密钥并将其嵌入武器和控制设备的机制。您必须考虑攻击者可能会使用社会工程维护人员的所有方式 ,以及您将采取什么措施来阻止这种情况发生。还有一个因素是密码学的复杂性。您如何引入单向性元素,以便拆除炸弹以更换电池的维修人员最终不会知道通用解锁码?您可能需要能够从通用解锁中导出代码来解锁此特定设备,但反之则不然。更重要的是,如果危机导致您授权某些武器,您需要用于恢复和重新键入的可用机制,谢天谢地,这些武器被停用而不是使用。美国系统现在使用公钥加密来实现这种单向性,但您也可以使用单向函数。无论哪种情况,您最终都会得到无条件安全性和计算安全性的有趣组合。

身份验证研究的一个有趣的分支 是块密码的 GCM 操作模式,在“密码学”一章中进行了描述,它已成为现代密码套件中最常见的操作模式。

15.4 共享控制方案

从 20 世纪 70 年代后期开始,人们担心苏联对美国国家指挥当局的斩首袭击可能会使核武库完好无损,但核指挥和控制业务变得更加复杂。还有人担心,超过一定的准备阈值后,假设当局和战地指挥官之间的通信可以保持是不明智的,因为电磁脉冲（以及其他可能的通信攻击)可能造成损害。

该解决方案是在被称为秘密共享的密码数学的另一个分支中找到的,它有助于激发其发展。这个想法是,在紧张时期,将激活一个备用控制系统,在该系统中,军官或战地指挥官的组合可以共同武装武器。

否则,维持对大量武器的详细中央控制的问题可能变得无法解决。这方面的一个特例是潜射弹道导弹。它们的存在是为了提供二次打击能力 对一个以第一次打击摧毁你的国家的国家进行报复。英国政府担心,根据美国的原则,如果美国被摧毁,总统及其合法继任者被杀,潜艇指挥官可能无法武装他的武器。因此,英国的做法是将武装物资存放在由船员控制的保险柜中,并附上首相关于在何种情况下使用武器的信函。如果 ocers 同意,则可以发射导弹。

这怎么能概括呢?好吧,你可能只给两个人中的每个人一半的认证密钥,但是你需要两倍的密钥长度,假设即使其中一个人被收买,原始安全参数也必须应用。另一种方法是给他们每个人一个数字,然后将他们两个加起来成为密钥。这就是自动柜员机密钥的管理方式2。但这在命令应用程序中可能还不够,因为无法确定操作设备的人员是否会在不进行讨论或询问的情况下同意发动世界末日。因此,Blakley 和 Shamir 在 1979 年独立发明了一种更通用的方法 [256, 1703]。他们的基本思想如下图所示（图 15.1）。

假设英国想要执行的规则是,如果首相被暗杀,那么武器可以由任何两名内阁部长或任何三名将军或一名内阁部长和两名将军武装。为了实现这一点,让 z 轴上的点 C 成为必须提供给武器的解锁代码。我们现在通过 C 随机画一条线,并给每个内阁部长在线上的一个随机点。现在他们中的任何两个一起可以计算出直线的坐标并找到它与 z 轴相交的点 C。

类似地,我们将直线嵌入到一个随机平面中,并在平面上给每个将军一个随机点。现在任何三位将军,或两位将军加一位部长,都可以重建飞机,从而重建发射代码 C。

通过将这个简单的构造推广到 n 维的几何形状,或者

2使用加法或排他法组合密钥对 ATM 来说是个坏主意,因为它使系统容易受到攻击,我稍后将在“API 安全”的标题下讨论。
但是,在无条件安全的身份验证代码的上下文中,添加可能没问题。

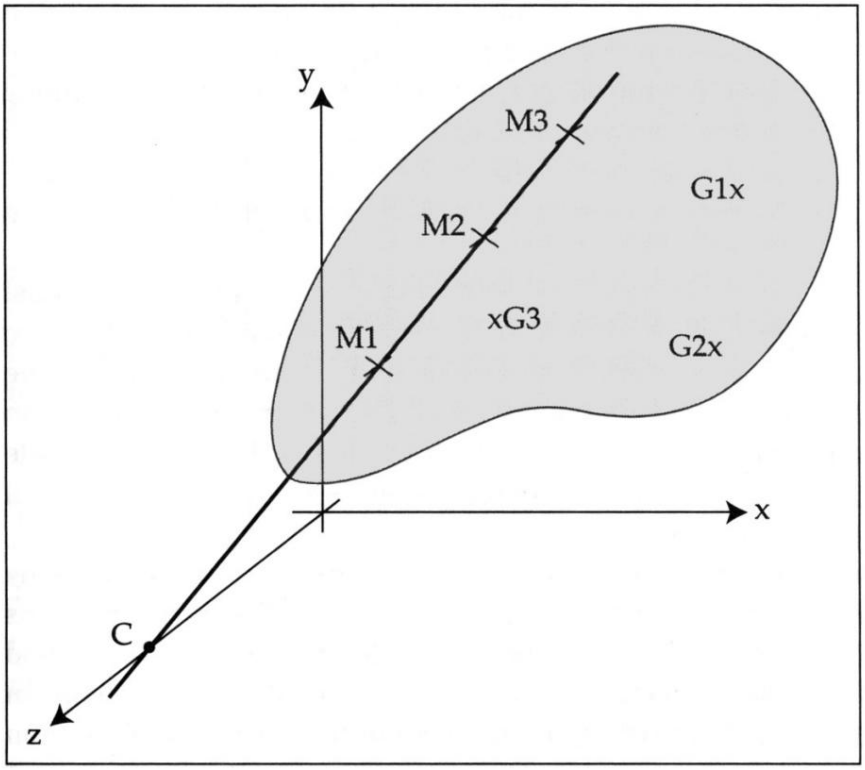

图 15.1：- 使用几何的共享控制

一般的代数结构而不是直线和平面,这种技术使武器、指挥官和选项能够以仅受可用带宽限制的复杂性连接在一起。可以在 [1829] 中找到秘密共享的介绍,在 [1750] 中可以找到更详细的说明。这激发了门限签名方案的发展,如第 5 章“密码学”中所述,并且可用于执行诸如“交易所的任何两名副总裁可以激活冷比特币钱包”等规则的产品。

在典型的军事应用中,使用二取二控制； n 必须足够大,以便至少有两个钥匙持有者准备好并能够完成这项工作,尽管有战斗损失。许多细节需要注意。例如,一个指挥官的死亡不应该让他的副手获得两半钥匙,还有各种各样的细节问题,比如谁在什么时候（在同一侧)射杀了谁。银行业大同小异;可能需要两个人才能释放大笔款项,并且您需要注意委托规则不允许两个密钥都落入一对手中。

在一些民用应用程序中,一些内部人员可能合谋破坏您的系统。典型的例子是付费电视,盗版者可能会购买几十张用户卡并对其进行逆向工程以获取他们的秘密。因此,付费电视运营商需要一个能够抵抗多个受感染用户的强大系统。

我将在有关版权的章节中更多地讨论这个叛徒追踪问题。

15.5 防篡改和 PAL

在现代武器中,螺线管安全锁已被用于保护大多数美国核装置的许可动作链接 (PAL) 所取代。关于 PAL 的已发布信息的摘要可以在 [217] 中找到。 PAL 开发始于 1961 年左右,但部署缓慢。即使在 20 年后,欧洲大约一半的美国核弹头仍然使用四位密码锁3。随着更复杂的武装选项的引入,密码的长度从 4 位增加到 6 位,最后增加到 12 位。设备开始具有多个代码,具有单独的“启用”和“授权”命令,并且还能够在现场更改代码(从误报中恢复)。

PAL 系统辅以各种编码开关系统和操作程序,对于诸如原子弹爆破弹药之类的武器,其体积和复杂程度不足以使 PAL 无法访问,武器也存储在篡改中称为 PAPS 的传感容器(用于规定动作保护系统)。其他用于防止意外引爆的机制包括故意削弱雷管系统的关键部分,以便它们在暴露于某些异常环境时失效。

无论使用何种系统组合,都有惩罚机制来阻止小偷从被盗武器中获得核当量。

这些机制因武器类型而异,但包括使坑变形并氢化其中的钚的气瓶、破坏中子发生器和氚助推器等部件的聚能装药,以及导致钚扩散而不是屈服的不对称爆炸。如果敌人的捕获受到威胁,这种自毁程序将使它们永久失效,不会屈服。销毁代码始终是优先事项。假设一个准备部署“恐怖分子”偷走一批炸弹的叛乱政府会准备牺牲一些炸弹(和一些技术人员)来获得一件可用的武器。

要执行授权维护,必须禁用篡改保护,这需要单独的解锁代码。持有各种解锁代码的设备 用于维修和射击 本身以与武器类似的方式受到保护。

[1825]中总结了保证目标:

> 目前认为,即使是拥有这种武器、拥有一套图纸并享有国家实验室技术能力的人,在不知道密码的情况下也无法成功引爆。

实现这样一个雄心勃勃的目标需要付出巨大的努力 。有几个需要护理级别的例子:

· 在测试表明 1 毫米切屑碎片在机载指挥所携带的控制装置的保护性爆炸中幸存下来后,

3Bruce Blair 说,战略空军司令部抵制新条令,并在 1977 年之前将 Min uteman 授权代码保持在“00000000”,向历任总统和国防部长撒谎 [255]。其他人说这只是使用控制代码。

软件被重写,所有的密钥材料被存储为两个独立的组件,它们被保存在芯片表面相距超过 1 毫米的地址;

· “足球”,总统身后随身携带的指挥装置,之所以这么厚,是因为担心聚能炸弹可能会破坏其保护机制。聚能电荷可以产生速度为 8000 米/秒的等离子射流,理论上可以用来禁用篡改感应电路。因此,可能需要一定的距离才能使报警电路有足够的时间将代码存储器归零。

这种关注必须扩展到实施和操作的许多细节。武器测试过程不仅包括独立的验证和验证,还包括竞争机构的敌对“黑帽”渗透尝试。即使那样,也会采取所有实际措施来防止可能的对手进入。

这些装置(包括弹药和控制装置)由武装部队进行纵深防御;经常进行零通知质疑检查;并且可以要求员工在白天或晚上的任何时间重新参加相关考试。

我在自己的章节中更详细地讨论了防篡改,因为它广泛用于银行卡和电话等应用程序。然而,防篡改、秘密共享和一次性验证器并不是唯一受益于核工业兴趣的技术。还有更微妙的系统课程。

15.6 条约验证

各种核查系统被用来监测核不扩散条约的遵守情况。例如,国际原子能机构和美国核管理委员会 (NRC) 监测获得许可的民用动力反应堆和其他设施中的裂变材料。

一个有趣的例子来自为监测全面禁止核试验条约 [1747] 而设计的防篡改地震传感器设备。此应用程序的目标是在每个签署方的测试站点中安装足够灵敏的传感器,以便以高概率检测到任何违反条约的行为(例如测试过大的设备)。这里的篡改感应非常简单:地震传感器安装在钢管中,然后插入回填混凝土的钻孔中。整个组件非常坚固,可以依靠地震仪本身以相当高的概率检测篡改事件。这种实物保护通过随机挑战检查得到加强。

由于普遍存在欺骗的假设,认证过程变得更加复杂。由于没有双方信任的第三方,而且传输的地震数据量为每天 108 位,因此使用数字签名方案 (RSA) 代替一次性认证标签。但这只是答案的一部分。一方可能总是通过说负责生成它的官员已经叛逃来否认签名消息,因此签名是伪造的。所以钥匙

一旦它被双方密封,就必须在地震包本身内产生。此外,如果一方制造设备,另一方会怀疑它具有隐藏功能。针对切割和选择品种提出了几个协议,其中一方将生产多个设备,另一方将拆除一个样品进行检查。其中一些问题后来在电子商务中重新出现。 （如果许多系统设计者在 [1747] 中阅读了桑迪亚的前加密负责人 Gus Simmons 对这些条约监控系统的描述,他们本可以避免很多悲伤。）

15.7 出了什么问题

尽管在开发高科技保护机制方面投入了大量资金,但核控制和安全系统似乎与其他任何系统一样遭受同样类型的设计错误、实施失误和粗心操作。

15.7.1 核事故

主要风险可能只是意外。我们已经发生了两起国际核和辐射事件等级为74的核事故,即切尔诺贝利和福岛的事故,以及一些不太严重的事故。位于塞拉菲尔德的英国主要废物后处理厂储存了 160 吨钚 世界上最大的储存量 几十年来一直饱受丑闻困扰。

伪造废证件;辐射泄漏已被掩盖;工人们更改了入境通行证,以便他们可以将汽车带入禁区;有破坏报告;核警察部队只能解决 10-20% 的盗窃或刑事破坏案件 [1131]。清理这一切的任务可能需要一个世纪的时间,耗资超过 1000 亿美元;同时它必须受到保护[1867]。在国防核企业的其他地方,包括核武器工厂和潜艇基地,存在重大而普遍的问题,包括破旧的设施、不称职的承包商、士气低落、项目延误、成本上升以及 20 艘旧潜艇等待处置 其中 9 艘其中仍然含有燃料 [1560]。俄罗斯的情况似乎更糟。一项关于核安全的调查描述了苏联解体后他们的安全机制是如何破旧不堪,裂变材料偶尔会出现在黑市上,举报人会受到起诉 [953]。

15.7.2 与网络战的互动

其次,越来越多的担忧是核安全可能会因网络攻击的可能性而受到破坏。即使命令和控制通道本身已经使用加密和

4定义是“具有广泛健康和环境的放射性物质的主要释放需要实施计划和扩展对策的环境影响”

此处描述的防篡改机制,可能会受到拒绝服务攻击； 2018 年,特朗普政府改变了原则,允许首先使用核武器应对此类袭击。另一个重要问题是指挥官是否可以相信他们在屏幕上看到的内容。 1983 年,在国际紧张局势时期,苏联的一个新预警系统发生故障,据报道美国向俄罗斯发射了五枚民兵导弹。

莫斯科地堡的指挥官斯坦尼斯拉夫·彼得罗夫中校认为这可能是虚惊一场,因为只发射五枚导弹是不合逻辑的,因此在卫星确认这确实是一场虚惊之前一直开火。

这可能是世界距离意外核战争最近的一次（三年前美国也曾误报）。既然我们有更复杂的系统,AI 会在我们甚至没有意识到的情况下潜入各种地方的命令链中,这样的系统故障在今天会如何发展?更不用说失败了 如果攻击我们的情报、监视和侦察 (ISR) 能力,包括监视导弹发射、检测核爆炸和传递命令的卫星,情况会怎样?

核威胁倡议组织 2018 年的一份报告详细描述了这些担忧 [1833]。仅仅保护武器本身是不够的,因为对规划、预警或通信系统的网络攻击也可能造成灾难性后果。主要风险是由于错误警告或错误计算而导致使用;还有外部依赖性,从网络到电网。如果这些网络也用于核力量,那么对常规指挥和控制网络的攻击可能被视为战略威胁。这些问题已在特朗普政府的 2018 年核态势评估中得到承认。仅靠技术网络安全措施是不够的,因为存在重大的软性问题,例如关键人物是否会因为让他们看起来无能而受到削弱。

还可能担心对手在网络作战中的能力可能会削弱自己的威慑力,或者过度自信地认为自己的能力可能会降低攻击对手的风险。一个非北约核国家信号情报机构的一位高级官员亲自告诉我,在一次对抗中,他们“击败了”一个地区对手。不管这是否属实,这种情绪在权力走廊中表达时,会破坏威慑力并使核冲突更有可能发生。最近,美国国家人工智能安全委员会在 2019 年警告说,如果配备人工智能的系统成功跟踪和瞄准以前无懈可击的军事资产,核威慑可能会被削弱 [1415]。

不仅仅是宣布拥有核武器的国家。目前有 22 个国家拥有足够数量和质量的可用于武器的裂变材料,44 个国家拥有民用核计划（一旦阿联酋变得危急,就有 45 个）。在这些国家中,有 15 个国家甚至没有网络安全法;除非监管机构要求,否则能源公司通常不会投资于网络安全,而一些公司（和国家)并没有真正的能力。

美国/以色列使用 Stuxnet 病毒攻击伊朗在纳坦兹的铀浓缩能力,这一切对各国政府来说都非常突出。 2009 年,他们的浓缩铀产量下降了 30%,2010 年病毒曝光。它感染了离心机控制器,导致它们旋转起来然后减速,从而摧毁了大约 1000 个伊朗的

机队 4,700 人。美国政府最终于 2012 年承认参与 [1028]。

15.7.3 技术故障

也有一些有趣的高科技安全故障。一个例子是在核武器削减条约中发现的可能攻击，这导致了密码数学的一个新分支的发展　潜意识通道的研究　并且与后来的版权标记和隐写术相关。

这个故事在 [1753] 中讲述。卡特执政期间，美国曾与苏联提出一项协议，双方将合作核实洲际弹道导弹的数量。为了保护美国民兵导弹免受苏联的首次打击，有人提议用巨型卡车在 1000 个发射井周围随机移动 100 枚导弹，这些发射井的设计让观察者无法确定它们是否在移动导弹.因此，苏联人必须摧毁所有 1,000 个发射井才能成功进行第一次打击，这被认为是不切实际的。

但是，美国怎么能向苏联保证发射井场最多有 100 枚导弹，却又不让他们知道在哪里呢?提议的解决方案是，发射井将安装一个俄罗斯传感器包，该传感器包可以检测导弹的存在或不存在，对这一点信息进行签名，然后通过美国的监控设施将其发送到莫斯科。问题是只能发送这一点信息；如果俄罗斯人可以在消息中偷运更多信息，他们就可以找到完整的筒仓　因为只需要十位地址信息就可以指定现场的一个筒仓。

（还有许多其他安全要求可以防止任何一方作弊，或错误地指控另一方作弊：有关更多详细信息，请参见 [1752]。）

要了解潜意识通道的工作原理，请考虑密码学一章中描述的数字签名算法。系统范围的值是质数 p、质数 q 除 p 1 和 q 阶子的生成器 g。消息 M 上的签名是 r, s，其中 r = (gk group of F⇒ (mod p)) (mod q)，k 是随机会话密钥。从 k 到 r 的映射是相当随机的，因此希望在此签名中隐藏十位信息以秘密传输给同伙的接一个地尝试 k [illegible] 约定（例如“第 72-81 位”　）然后，尝试一个

这可能会导致安全协议出现灾难性故障。但最终，媒体上广为人知的“导弹炮弹游戏”并没有被使用。最终，中程弹道导弹条约 (MRBM) 使用了统计方法。俄罗斯人可以说“我们想看看下面的 20 个发射井”，然后他们就会打开卫星进行观察。随着冷战的结束，检查与有人驾驶飞机的检查飞行变得更加密切，双方都有观察员，而不是卫星。

不过，潜意识通道的发现意义重大。他们可能被滥用的方式包括将 HIV 状态或重罪定罪的事实放入数字护照或身份证中。如果这是不可接受的，补救措施

是使用完全确定的签名方案（例如 RSA)而不是使用随机会话密钥（例如 DSA)的签名方案。

15.8 保密还是公开?

最后,核工业提供了一个很好的保密案例。在 1930 年代,来自许多国家的物理学家自由地分享了导致原子弹诞生的科学思想,但在“原子间谍”（Fuchs、Rosenbergs 等人)将广岛和长崎装置的设计泄露给苏联之后,事情走向了另一个极端。美国采取了一项政策,即原子知识诞生于机密。这意味着如果你在美国管辖范围内并且有与核武器相关的想法,你必须保密,无论你是否持有安全许可甚至在核工业工作。这与宪法有冲突。从那时起,随着对保护问题的详细考虑,事情已经大大放松了。

“我们在新墨西哥州有一个数据库,记录了钚在非常高的温度和压力下的物理和化学特性”,一位美国前核安全负责人曾告诉我。 “我应该把它归为什么级别?

谁会偷它,这对他们有什么好处吗?俄罗斯人,他们自己得到了这些数据。以色列人可以想办法。卡扎菲?他到底要拿它做什么？”

随着此类问题得到解决,许多技术已被解密和发布,至少是大纲。从 20 世纪 80 年代初在科学会议上早期发布关于认证代码和潜意识通道的结果开始,人们发现公共设计审查的好处超过了对手广泛了解所用系统的好处。

许多实施细节都是保密的,包括可能有助于破坏的信息,例如设施的五十座建筑物中的哪一座包含警报响应部队。然而,大局是相当开放的,指挥和控制技术有时会提供给其他国家,包括潜在的敌对国家。减少意外战争的可能性的好处被认为超过了保密的可能好处。 9/11 之后,我们宁愿在巴基斯坦拥有像样的指挥和控制系统,也不愿冒险让一些遭受宗教狂热袭击的中层官员使用他们的武器之一来对付我们。这是 Kerckhos 学说的现代转世,该学说是 19 世纪的格言,即系统的安全性必须取决于其密钥,而不是其保持晦涩的设计 [1042]。

可以更广泛地吸取核教训。 9/11 之后,一些政府大谈恐怖分子使用生物武器的可能性,并对细菌学、病毒学、毒理学甚至医学的研究和教学实施控制。我在这些学科的教职同事对此深感不以为然。 “你不应该担心炭疽病，”英国一位顶级病毒学家告诉我。 “真正令人讨厌的是大自然母亲梦寐以求的事情,例如 HIV、SARS 和禽流感。如果这些政策意味着下次病毒降临时喀土穆没有任何有能力的公共卫生人员

尼罗河,我们会很抱歉。”可悲的是,2020 年的事件证实了这一智慧。

15.9 总结

核武器的控制,以及从通过核设施的物理安全保护国家指挥系统的完整性到监督国际军控条约的附属活动,为安全技术的发展做出了巨大贡献。

几乎不计成本地保护武器和裂变材料这一理性决定推动了许多数学和科学的发展,这些数学和科学已在其他地方得到应用。我们在本章中看到的具体示例是身份验证代码、共享控制方案和潜意识通道。本书其余部分还散布着其他示例,从警报到虹膜生物识别技术,从防篡改电子设备到密封件。

然而,即使我们可以保护授权使用核武器的指挥和控制渠道,但这绝不是全部。如果网络攻击可以通过针对一个国家的情报、监视和侦察能力来破坏人们对威慑的信心,它们仍然会严重破坏稳定。在核边缘政策时期,每一方都可能认为他们拥有未公开的网络能力的优势。鉴于自 1945 年以来美国总统已使用核威胁十几次(古巴、越南和伊拉克只是更明显的例子),我们预计每一代人都会发生几次这样的危机。

研究问题

我在 2001 年第一版的本章末尾设定的研究问题是“为这一领域开发的技术寻找有趣的应用,例如验证码”。到第二版时,分组密码的伽罗瓦计数器操作模式已经标准化,并且现在已经普及。

还有什么可能?

现在最严重的研究问题可能是硅和钚之间的相互作用。美国/以色列在 2009-10 年对伊朗铀浓缩计划的攻击为世界提供了一个在核世界中使用网络攻击的例子。此类攻击的威胁会在哪些方面增加核冲突的风险,我们可以做些什么呢?鉴于我们不能像强化命令和控制通道那样强化一切,我们可以做些什么来维持对监控等支持系统的信任,或者至少确保它们以不会导致致命错误的方式退化闹钟?

进一步阅读

由于我自己对核武器的直接经验相当过时 包括在 1970 年代从事核能力飞机的航空电子设备方面的工作
本章是根据已发表的资料和与内部人士的对话汇编而成的。美国科学家联合会是有关核武器的最佳公共信息来源之一,他们讨论了从炸弹设计到许多核武器技术解密的基本原理等方方面面 [672]。 [2045] 中也讨论了解密问题,Steve Bellovin [217] 收集了关于 PAL 的公开材料。

格斯·西蒙斯 (Gus Simmons) 是桑迪亚足球俱乐部的设计者;他是验证码、共享控制方案和潜意识通道的先驱。
他的书 [1749] 仍然是本章讨论的大多数技术资料的最佳参考。在 Doug Stinson 的教科书 [1829] 中可以找到对身份验证和秘密共享的更简洁的介绍。

许多地方都记录了核设施中的控制故障。俄罗斯装置的问题在[953]中讨论;美国的核安全由核管理委员会监督[1455];健康与安全执行官发布的季度报告 [874] 中记录了英国装置的不足之处。最好和最新的问题调查可以在公共账户委员会 2018 年的报告“国防部核计划”[1560] 中找到。至于“硅和钚之间”的相互作用,查塔姆研究所最近有一份关于该主题的报告 [27]。