网络信息安全:一局持续变化的恒久棋局

潘柱廷

北京启明星辰信息安全技术有限公司,北京 100193

摘要 网络信息安全是一个持续变化的博弈棋局。本文从南向(技术领域)和北向(观念和管理)两个方面,探究这个棋局的本质性结构。仿照医学的分科模式,将网络安全领域分解成多个子领域,并探究各子领域的内在规律和关键人群。

关键词 网络空间安全;信息安全;黑客

1 网络信息安全是一个什么棋局?

“古之欲明明德于天下者,先治其国;欲治其国者,先齐其家;欲齐其家者,先修其身;欲修其身者,先正其心;欲正其心者,先诚其意;欲诚其意者,先致其知;致知在格物,物格而后知至,知至而后意诚,意诚而后心正,心正而后身修,身修而后家齐,家齐而后国治,国治而后天下平。”——《大学》

把《大学》中的修齐治平,引申到网络信息安全的格局中,就是要向内参修“格物、致知、诚意、正心”,在外践行“修身、齐家、治国、平天下”。

安全是一个古老的话题。原始人要在自然和野兽的包围中追求生存安全;在冷兵器、游牧农耕的时代,个人家族之间、部落国家之间争夺以土地为标志的空间;在热兵器、工业和大航海贸易时代,对于土地和市场的争夺变成了全球化;而在信息化时代,发展和争夺都信息化了、网络空间化了。在信息安全研究领域,已经开始习惯采用“网络空间 Cyber Space”这个词汇了。在网络空间中的安全问题,就称之为网络信息安全或网络空间安全。

安全是一场持久的博弈。信息化时代到来之后,技术推动了网络信息安全这个新棋局的形成。随着技术的发展变迁,网络信息安全这个棋局一直在持续地变化着。这是一个持续变化的恒久棋局。

1.1 安全是有立场、需担当的

网络信息安全是一个多方博弈的棋局,而且入局的弈者很多。并且这局棋还是一个局中局,有国家间的大局,也有机构和个人面对的中局和小局。

修身,个人所面临的围绕个人信息和个人计算的个人信息安全。

齐家,《大学》中的“家”指家族,在这里把其对应为个人所在的机构,也就是机构安全问题。可以是企事业机构或政府机构,当然也可以是一群人的群落。

治国,就对应为国家内部的网络信息安全,也就是基于公共基础设施安全的社会信息安全和秩序。

平天下,这里就对应为国家作为一个整体,面临国际环境下的国家自身安全以及对国际和平与秩序的维护。

如果借用儒家的“仁爱”之说,这“网络空间之仁爱”是有远近和高下之分的。“远近”就是内外之别,是亲疏之分,是立场立于内、立于亲。技术是无国界的这种论调,在安全领域是行不通的。“高下”就是责任,是担当。当一个人或者一个组织要更多地跨出自己的亲疏界限,去更多地满足其他人其他机构的诉求,这就是责任,是担当。这是所谓“高尚”。在网络空间安全的格局中,若每个人都能够很好地仁爱自己和亲近者,且能有一部分人去保护整体,从而形成整体格局的稳定和秩序。

1.2 安全的本质性结构

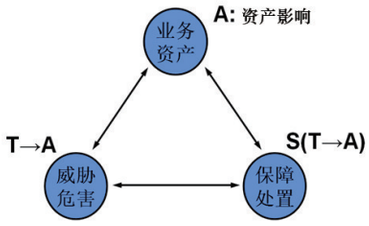
在IT领域的各分支中,网络信息安全具有区别于其他分支、特有的根本结构。一般IT领域的问题,常常可归结为两要素问题:“需求”和“需求被满足”;但是,安全永远是一个三要素互相交织、博弈的课题。这三个基本要素就是:业务和资产、威胁和危害、保障和处置(图1)。

安全的独特之处就在于:有难以控制、难以意料的“威胁和危害”一方,自然就要有针对之的“保障和处置”这一方,这两者与业务资产一起形成了一个三方博弈关系。在网络信息安全的弈局中,A类、T类、S类都会成为入局的各方。ATS安全三要素所代表的入局的各方,立场各异,印证了“安全是有立场的”。

收稿日期:2016-05-30;修回日期:2016-06-30

作者简介:潘柱廷,教授级高工,研究方向为网络信息安全技术及战略研究策划、技术管理等,电子信箱:jordan@venustech.com.cn

引用格式:潘柱廷. 一局持续变化的恒久棋局——网络信息安全[J]. 科技导报, 2016, 34(14): 107-112; doi: 10.3981/j.issn.1000-7857.2016.14.012



A:资产影响(S也是A之部分)
T:威胁和危害(T是A的映射)
S:保障和处置(S是T的函数)

图1　安全的3个基本要素

所有的安全问题,都应就这三方面阐述清楚,否则无从谈起其思考的完备性。

比如,用ATS安全三要素视角考虑云计算安全问题。

要素A:建立对云计算的系统形态、业务模式、技术特点等的深入认识。例如虚拟机的弹性分配和迁移模式的影响、云计算数据中心网络结构特点等。

要素T:梳理针对云计算系统的攻击方法,例如针对虚拟化系统的虚拟机逃逸攻击技术,针对云计算的计算和网络传输的资源特点进行的专项拒绝服务攻击、虚拟机病毒感染等。

要素S:针对识别出来的T,寻找最利于保护A的相关技术和方法。例如虚拟网络安全域划分模式、虚拟化安全网关设备、静态虚拟机映像病毒检测等。

把A-T-S三方面反复斟酌思考,云计算安全的问题就会越来越清晰明确。

不管是网络信息安全的专业从业者,还是安全的需求者,都需要用ATS三要素来梳理自己的思路和行动。

1.3　网络信息安全的格物致知

《大学》中的"格物、致知、诚意、正心",是向内参修的学问。

"苟日新,日日新,又日新"。"知其所止"。"此谓知本,此谓知之至也"。

"致知"到底需要知道什么呢?《大学》谈到了3个方面,一是要"知新",知道一切都在变化,了解和研究最新的;二是要"知止",知道所止,知道界限、度、目标等,知道内涵和外延。三是要"知本",知道本末、轻重、缓急,知道如何选择。

知新、知止、知本可以说也是网络信息安全领域"致知"的递进台阶。而知本的本,就在"格物"。

"所谓致知在格物者,言欲致吾之知,在其物而穷其理也。"

致知在格物。格物就是穷其理,就是对于人们关心的对象(物或事物)的内在规律进行深入的探究。此所谓"穷其理"。而且,在不同子领域,其内在规律不同。

《诗》云:"穆穆文王,於缉熙敬止!"为人君,止于仁;为人臣,止于敬;为人子,止于孝;为人父,止于慈;与国人交,止于信。

知止,对于不同的角色,其"止"是不同的。致知是有主体的,也就是"到底'谁'去知道那些'知'?"。在不同的领域中,都有该领域的"应格之物、需穷之理"(即所谓的核心技术和内在规律),该领域也会有一个特定人群能达到该领域的致知之境(成为关键人群)。

想要在网络信息安全的一个领域中达成所需所求,就一定要找到最适合去"致知"的关键人群,并在这个人群中找到最适合的、比较强大的那个人,并由这个人或者这群人来主导这个领域,才能获得成功。

1.4　安全发展的驱动力——极客和黑客

IT发展的驱动力来自于需求,就像其他领域的发展需求一样。这种需求有的是人的基本生理需求;有的来自于身边"衣食住行"这样的日常占有(拥有)需求;有的来自于军事和战争这样的争夺性需求;有的来自于社会治理、国际关系这样的控制性需求(维持既有格局的需求)。

而这种来自需求的驱动力并不是均匀分布的;并不是大众的需求都能带来相同的变化驱动力(很多需求都并不被常人意识到,就像驾马车的车夫没有对火车的需求)。

带来技术变革和产业变革的需求,来自于极客Geek,那些追求极致的人群。就像爱迪生要试验电灯泡的灯芯,乔布斯啃着苹果孵化了iPhone,谷歌旗下DeepMind的一群人造出AlphaGo来和李世石下围棋等。

极客是那些想从内部扩展卵茧的那股力量,一旦某个幸运的"行动极客"真的打破了卵壳和茧缚,就会带来断代式的技术或产业蜕变。当然,还有来自基础理论和基础技术研究领域的"科学极客",会为行动极客解决破茧的理论和技术可能性。例如:爱因斯坦的相对论为核技术的突破提供了理论保障;图灵机的抽象计算模型、香农的《信息论》、冯·诺依曼的《博弈论》等为计算机打下理论基础。

在网络信息安全领域,除了极客的推动力——这种由内而外的发展力量之外,还有一种力量是自外而内的力量。这种极致的破坏力来自于黑客Hacker。来自于外部的侵袭力量和这种力量的研究者们,促动了网络信息安全防御力量的发展,就像外部的寒热和菌毒强化了人体的免疫能力。

极客和黑客是推动网络信息安全发展的力量。他们甚至会突破并掀翻现有的棋局,创立出新的博弈格局。

而在非常需要安全能力的机构里是否诚意聘请了这样的极客和黑客呢?

2　网络信息安全各领域的其理其人

网络信息安全是一门强调应用实践的技术,而且特别强调对抗性实践。所以,从安全应用者的视角,将自己所立足的安全问题(不管是个人信息安全、机构信息安全、关键信息基础设施安全、国家网络主权等)进行领域分解。各个分领域都有需要"穷其理"的关键规律和特色,还有该领域关键的人群。

2.1　网络信息安全的领域划分

网络信息安全的领域划分,就好像一个医院要将内科、外科、心血管科、烧伤科、妇科、小儿科、检验科、放射科等等划分开建设,形成一个综合性医院。有的划分依据医疗人群、有的划分依据人体的系统和器官、有的划分依据疾病形态、有的划分依据医疗方法。这种划

分方法并不是一刀切的整齐划一,而是要让科室划分有利于调动组织、分配资源、驱动活动、平衡轻重。

网络信息安全,由(ATS三要素中)不同的业务资产(A),依据其不同的业务属性、技术属性可以将网络信息安全分成很多不同的领域。例如:Web网站安全、工业控制系统安全、云计算安全、大数据安全等。另外,也有从威胁危害(T)的视角分解出来一些领域,这些领域关注如何解决这些问题,例如防病毒、网络入侵检测、抗拒绝服务攻击、APT(高级持续性威胁)防护等。还有些是从保障处置(S)的角度分解出来的一些领域,这些领域重点强调所使用的防护技术类别,例如:加密、鉴别认证、信息安全管理体系等。

每个子领域也都有自己特有的规律和特点以及特有的关键人群。

建议,如果需要在某个技术领域做出一个重大决策,一定要征求这个领域的关键人群的意见。

2.2 密码技术领域

密码在古代就被用于传递秘密消息。在近现代战争中,传递情报、指挥战争、外交斗争均离不开密码。密码一般用于通信传输过程中和存储中的信息保密。使用的密码技术和密码产品对信息进行加密保护或者安全认证,是当今现实生活中最常见的安全防护手段。密码在为党、政、军各级领导机关提供秘密通信的同时,已广泛应用于经济、科技、文化和社会生活的各个领域。例如日常使用的身份证、银行卡等,均采用了密码技术。

密码已有几千年的历史。在很长一段时间里,密码都是作为一种隐蔽通信技术。密码学成为一门完整的、成熟的学科,还是20世纪50年代的事情(图2)。

密码理论和技术实现了由传统密码到现代密码的重大变革,现代密码是通信、计算机和密码的结合,它融合了对称密码和非对称密码等多种密码技术,可以实现信息保密、抗抵赖签名、安全认证等多种功能。密码体制与功能由单一化阶段经多元化阶段,走向集成化阶段,密码系统建立在芯片上已成为发展趋势。

密码技术其实已经成为几乎每个安全领域中必备的基本要素(不管是否突出),任何两个或多个安全实体之间形成信任、信用、绑定等结构性关系时,里面都少不了密码技术的支持。例如,最近广受关注的"区块链"技术、勒索软件问题等都和密码技术密切相关。

国内密码产业发展比较成熟。国家密码管理局目前已经向社会公布非对称密码算法SM2、散列算法SM3、对称算法SM4等及系列密码协议规范。截至2016年2月底,商用密码通用产品已达到1509项款,商用密码产品销售许可单位共817家。涵盖了密码芯片、密码板卡、密码机、密码系统、密码模块等不同的种类。密码产业年产值近100亿元人民币。

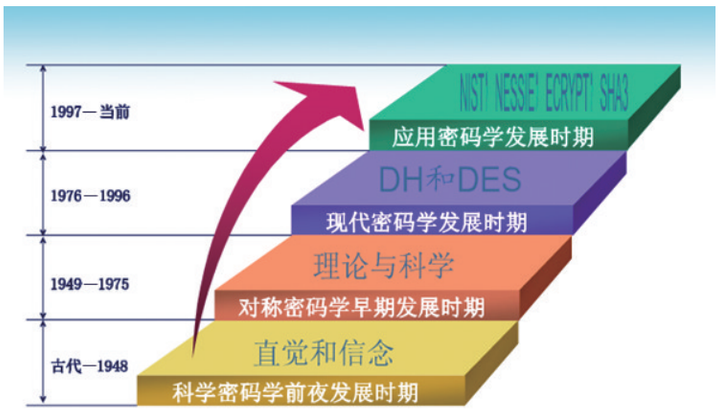


图2 密码学发展历程

自从20世纪中叶现代密码的理论、技术和应用发展,密码的关键问题逐步聚焦为两个根本问题:算法、计算能力。

算法就是数学算法,密码的基础就是某个数学模型、某个定理、某个公式;密码设计就是发现一种算法,密码分析就是破解这个算法。掌握和主导算法的是数学家。

计算能力决定了密码的抗破解强度,量子计算之所以受到安全界的关注,是因为其潜在计算能力和计算模式可能使得现有的密码都变得极易破解。掌握和主导计算能力的是计算科学家,一般这些人也是数学家。

所以说,数学家是密码技术关键人群,掌握着密码的命脉。

2.3 身份鉴别技术领域

身份鉴别技术(或者说用户身份认证)是网络信息系统确认访问者(用户)身份的过程。网络信息系统为各用户明确了标志(如用户名),并且注册和记录了各个用户的访问权限。当用户试图访问系统时,系统会对用户身份进行鉴别,确认了用户身份后,就按照记录的访问权限授权。

对用户的身份鉴别,基本方法有3种:1)根据你所知道的信息证明你的身份;2)根据你所拥有的东西证明你的身份;3)直接根据你独一无二的生物特征证明你的身份,比如指纹、虹膜等。如果结合了两种以上的方法,就称为双因子身份鉴别、强认证。

静态口令(登录口令Password,常被俗称为登录密码),是最常见的通过"你所知"的身份鉴别技术。静态口令是用户自己设定、注册并存储在系统中;当用户登录时,系统会将用户输入的口令与系统中密文存储的口令进行对比验证。近几年,每年都会有一些大的互联网网站出现大规模的用户信息泄露,这种泄露主要指系统中存储的用户名和口令的大量泄漏。俗称的"拖库"就是入侵系统后将存有用户名和口令的数据库偷走。有些网站将用户名和口令直接明文存储,这更是极端危险。用加密和签名的算法保护存有用

户名和口令数据库,是最基本的防护措施。

动态口令技术是最典型的“所拥有”模式的身份鉴别。用户携带一个能够显示持续变化的口令的小设备,如果该口令与用户在系统中的一个同步变化的口令相一致,就鉴别成功。

双通道鉴别,就是除了用户面对要访问的系统之外,再通过持有另一个登记的设备来达到“所拥有”的鉴别,例如短信口令表示用户持有登记的手机设备;二维码扫描鉴别其实也是同样的鉴别机制。

智能卡、USB令牌等鉴别手段是通过加密算法将用户鉴别的必要信息加密存储在这些随身小设备上,用户通过持有这些卡和令牌实现“所拥有”模式的鉴别。

指纹、静脉掌纹、虹膜、声纹等都是利用用户人体的生物特征完成鉴别。

用户鉴别并不一定是越严格越好。需要把握好鉴别认证的方便性与严格性之间的平衡。比如,虽然静态口令有很多安全隐患,对于拖库、口令暴力猜测、彩虹表攻击等目前还没有比较彻底的解决办法,但是因为静态口令是免费的,而且使用方便、易学,今后还会被长期采用。再比如,一个用户要登录多个系统,单点登录技术可以让用户只鉴别一次,后续使用体验更流畅;而Web访问过程中的cookie记录,可以使用户多次打开一个应用App的时候或反复访问一个网站的时候,不必每次都进行口令验证。虽然这样使身份鉴别的强度变弱一些,但是单点登录和cookie带来了方便确实让人难以割舍。

用户身份鉴别,是网络安全中给普通用户最直接的感受;也是黑客攻击的重灾区。对于身份鉴别的攻击,一种是对鉴别模式本身的攻击,另一种是通过对于系统的攻击达到绕过身份鉴别的目的。

身份鉴别技术关键人群:密码专家、鉴别架构设计师。

2.4 系统漏洞和渗透攻击领域

系统漏洞和渗透攻击领域可以比喻为医院的内科。

这里的系统主要指一个主机系统、设备系统、软件系统等(不包括网络系统)。对系统攻击的目的是控制系统、获得超越限制的权限,进而就可对系统采取进一步的攻击举措。

20世纪末最受关注的被攻击系统是Windows操作系统、Unix类操作系统;进而各款数据库管理系统、Web应用系统等都成为被攻击目标。在手机和移动互联网逐渐获取主流地位时,手机操作系统iOS和安卓就成为了主要目标。例如,当苹果iPhone手机操作系统iOS升级一个新版本时,整个安全圈就都开始期待新“越狱”方法的出现。对系统的攻击,一般要先挖掘系统漏洞,并找到漏洞利用的渗透攻击方法。

当发现漏洞后,特别是严重的漏洞,系统厂商就要马上开发漏洞补丁,并为用户提供安全更新。当年“微软XP停服事件”的起因,就是微软声明将停止对于Windows XP操作系统的安全补丁升级服务。

漏洞扫描工具是进行漏洞检查的常用工具。另外对于主机系统的安全检测,也包括要发现系统中隐藏的、被植入的恶意代码,例如病毒、木马等。发现了病毒和木马就要进行查杀。

不把这个领域称作“主机安全领域”,而称为“系统漏洞和渗透攻击领域”,就是因为这个领域的关键人群就是系统的漏洞挖掘和漏洞利用渗透设计者——这类人俗称是拥有黑客技术的人。任何没有经过比较充分的漏洞挖掘和渗透攻击测试的系统,都是不可靠不安全的。

系统厂商也在系统的强壮性方面与系统攻击者进行对抗。比如,系统地址空间的缓冲区溢出漏洞曾经是操作系统的主要漏洞类型,之后系统厂商开发了地址随机化技术,就系统性地解决了缓冲区溢出漏洞的漏洞利用问题。

而当“震网病毒”事件中系统的攻击者将目标锁定为西门子的工业控制系统之后,就带动了整个安全产业对于工业控制系统安全的再认识。

系统漏洞和渗透攻击关键人群:拥有黑客技术的人,他们才是整个领域的领跑者。

2.5 网络结构安全领域

更愿意把网络结构安全领域比喻成医院的外科或者骨科。

网络是大型系统的骨骼和传输通道。网络是以网络设备为节点,并通过有线或者无线的传输通道连接起来。这些节点就是网络设备和主机。典型的网络设备有交换机、路由器、防火墙等。虽然网络设备也都是网络中的节点,但由于这些网络设备对外的接口和管理界面相对单一,对其漏洞挖掘和直接攻击并不是很多,网络主要是作为攻击流的途经通道。

当然,现在也有针对网络协议和网络结构的攻击。比如,分布式拒绝服务攻击DDoS,就是通过控制大量僵尸主机而形成一个攻击网络集团,同时向一个目标发起访问,将网络带宽拥塞,将被攻击目标主机资源耗尽,让服务无法访问到。为了对抗这种洪流式的攻击,除了要通过增加网络带宽、提高主机性能之外,被访问网络也需要构建一些疏导性结构,比如通过CDN内容分发网络来响应带宽访问的尖峰压力。

纵深防御是安全界一个主流思想,其中一种重要的纵深就是网络结构形成的空间纵深。一般大型网络都会非常注重网络拓扑结构的设计,特别是有秩序地划出安全域(依据安全等级和安全关系划分网络区域),安全域边界则用防火墙等安全网关构建防护边界。如果要从外向内访问到内部重要和敏感的系统,都会经过多层安全网关的过滤和检查。如果两个网络安全域要通过一个相对不信任的网络区域建立通信,常常会采用通信加密技术构建VPN(虚拟专用网)完成。

随着云计算、虚拟化技术的发展,一种被称为SDN软件定义网络的新网络形态出现了。其首先在大型数据中心网络中得到应用,SDN网络能够根据网络传输的需要,动态调整网络拓扑结构。

网络结构安全关键人群:网络架构师和性能工程师。

网络和网络结构安全的关键性问

题就是网络的连通问题,而网络连通可以衍生出来两个问题:一个是网络(连通)结构,另一个是网络传输性能(这很类似现实中的交通运输)。网络结构安全领域中,也有两类关键人群。

一类是网络性能工程师。主要是提高网络设备的性能。CPU性能有摩尔定律,与摩尔定律相联系的另一个网络定律是吉尔德定律,即主干网带宽的增长速度至少是运算性能增长速度的3倍(即每8个月增长1倍)。网络性能也是安全的一个重要延伸。

另一类是网络架构师。定义网络基本结构,划分安全域并设计边界安全,都是网络架构师的责任。

2.6 网络入侵检测领域

网络入侵检测领域就像医院内科中的免疫科。

在网络结构已经基本确定的条件下,要应对网络中途经的攻击流,就要采用网络流的检测分析,从中发现攻击行为,这就是广义的网络入侵发现技术。

入侵检测(intrusion detection)是对入侵行为的检测。入侵检测作为一种积极主动地安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵。入侵检测通过执行以下任务来实现:监视、分析用户及系统活动;系统构造和弱点的审计;识别反映已知进攻的活动模式并报警;异常行为模式的统计分析;评估重要系统和数据文件的完整性;操作系统的审计跟踪管理,并识别用户违反安全策略的行为。

入侵检测系统一般都分为两部分:一部分通过各种手段收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息(网络入侵检测系统就部署在网络中以旁路方式监听网络数据流)。另一部分就是将采集到的数据导入到分析中心进行分析,检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

这种分析可分成两类:特征检测和异常检测。

特征检测:将已经发现的入侵者活动提取出一种模式来表示,系统的目标是检测新活动是否符合这些模式。这种检测已知的模式,难于发现新入侵方法。这就需要不断研究和提取新特征,并通过特征库升级保障检测有效性。

异常检测:假设入侵者活动都异于正常主体的活动。根据这一理念建立正常活动模式,并比较当前活动是否异常,如有异常则可能是"入侵"行为。异常检测的漏报和误报比较多,但有时能够发现未知攻击。另外,随着数据挖掘等技术的引入,给异常检测带来了更多的能力提升。

从检测性能的角度看,随着网络带宽的加大,对于高带宽网络的检测常常不进行全流量全数据包检测,而只对数据包的元数据(meta-data)、流数据(flow)进行检测,比如,仅检测网络五元组信息、包长、时间、是否加密、协议类型、碎片程度等是否产生异常,就能发现不少可疑行为。有了深度流数据检测(DFI)的初步结果,再抉择后续的深度包检测(DPI)。

入侵检测体系中的关键人:数据分析算法工程师。分析算法工程师设计的算法确定了分析引擎的系统设计,确定了检测特征的数据结构、样本、特征提取模式等。

2.7 防恶意代码传播领域(防病毒、防木马)

防恶意代码传播领域就像医院的传染病科。

恶意代码包括计算机病毒、木马、蠕虫等代码。计算机病毒是一个程序,一段可执行码。就像生物病毒一样,具有自我繁殖、互相传染以及激活再生等类似生物病毒特征。计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。

计算机病毒在感染一个主机系统时,其实就是一个攻击渗透过程,也是利用系统的漏洞或者一个已经植入系统的木马。

这个领域的关键技术就是系统漏洞、利用漏洞的渗透、代码传播规律。

与系统漏洞和渗透领域一样,防恶意代码传播关键人群也是拥有黑客技术的人。

2.8 网络信息安全的其他科室

网络信息安全的范畴非常庞杂,在业务、威胁、保障的任何一方面出现变化,都可能衍生出一个新的领域。就像医院中的科室变化一样,并非有一个新疾病和新医疗方法就会新增一个科室。领域和科室的设置,要根据技术本身的自完整性(相对独立性)、涉及范围、资源条件等决定。

还有一些网络信息安全的领域(科室)值得点出来,列于表1。

网络信息安全的领域划分没有像医院的科室划分那样标准和广泛认同。但相信,随着网络信息安全的发展,这种类似科室划分的领域划分会逐

表1 其他网络信息安全研究领域

领域	领域简述
源代码审计	在信息系统软件的开发周期中展开安全检查。检查软件中的Bug错误和安全漏洞。可以比喻为儿科或者妇娠科。
内容安全	对信息系统存储、处理、传输、发布的内容进行安全检查。比如,舆情分析、谣言溯源、关键字过滤、信息水印、信息隐藏等都属于这个领域的技术。这可以比喻为精神科、心理科。
应急响应	这就好像医院的急诊科;也类似公共事件的应急处置。 作为应急,要把握住预防、检测定级、抑制扩散、消除、恢复、后续改进和追责等六步要领。 在互联网应急领域,中国有CNCERT/CC互联网应急协调中心。
取证	这就像刑侦中的取证、法医鉴定等。 信息取证、电子取证是为了让证据得以保全和确认,在侦查、检诉中成为被采信的法定证据。
云安全	针对云计算系统特点的攻防技术领域。

渐形成共识,并稳步发展和进化。

3 北向,安全的正念与正解

常听到这样的说法,网络信息安全是“三分技术、七分管理”。虽然这种三七开的分法并不一定妥当,但这让人们意识到除各领域的技术问题之外,还有很多如战略、规划、政策和合规、供应链管理、运作管理、风险管理等重要的非技术话题。在业界,对于这类问题还有一个简单的归类就是“北向”(注:在各种模型图中,管理性内容常常画在技术性内容的上面。借用上北下南的说法,把管理的、非技术的部分简称为“北向”)。

观念是北向的。正确的安全观念、正确的解决思路对于安全工作至关重要。

安全没有所谓的“百分之百安全”,安全面对的常常是还没有发生的、潜在的问题。因此安全就引入了概率的思想、风险管理的观念和方法。“对目标有所影响的某件事情发生的可能性就是风险”,包括对目标影响的大小、事件发生的概率。风险管理就是要对影响和概率进行控制,以达到安全投入与预期损失的某种平衡。信息安全管理体系的设计依据,常常就是风险管理过程中各阶段的成果。

ATS安全三要素强调,安全是基于各自立场的多方复杂博弈。既然是博弈,博弈的对手就不像自然灾害那样的自然选择性,就不像医学中无智力的生物病毒。如果过度地、错误地套用医学上免疫系统的说法,就很容易引起误导。

要树立博弈思想,明确我们面对的对手是人或人的组织,是有智力、有技术、有资源的、活的博弈对手。

从人的本心诉求来说,总还是希望有某个人(或神)采用某种方法、利用某种神奇的设备,将问题彻底解决了。这种观念被称为称之为“银弹思维”(注:在欧洲中世纪传说中的“人狼”妖怪,用一般的枪弹是不起作用的,只有一种用银子作成的特殊子弹才能把它杀死。银弹比喻万能的终极杀器)。

在网络信息安全领域中,没有银弹。每一种技术、解决方案、工具、产品都不可能是银弹。首先,每种手段都有限制条件和功能极限;其次,每种手段都有其附带的副作用;第三,这些手段是否能够正确使用也是不确定的。也就是说,每种手段都有可能失效。

当使用的是复杂的电子设备、复杂的软件、复杂的供应链供应商网络、复杂的智能化功能、傻瓜式的使用界面,如果还要追求一把椅子一张桌子那样的安全可靠稳定,是绝对不切实际的。现今的电子设备、网络软件,是一定有Bug的,是一定有问题的。

一个没有Bug没有安全问题的设备和软件是不存在的。

如果这么一个复杂系统没有问题,或者说没有发现问题,那么一定是下面两种情况:1)这个设备和软件还没受到关注(还根本没有人琢磨其安全性);2)这个设备和软件的安全问题,被厂家或者某些人掩盖起来了。

一个好的安全的产品,应当是能够及时发现安全问题并能及时快速解决的产品。这才是安全,这就是“新安全观”。

在考虑一个复杂系统的安全时,必须采用“纵深防御”的路线。也就是在系统中安排空间纵深、时间纵深、手段多样性纵深等。体系设计必须基于一个基本点“面向失效的设计”。也就是要在某一项手段和措施失效时,在其身后还有下一个手段和措施作为补充和纵深。纵深防御思想,与军事对抗和斗争中思路非常接近。

秉持北向的正念,合理地组织南向的各个技术领域,组成适合自身的安全解决方案,这才是人们在这个持续变化的恒久安全棋局中,谋生存、谋发展的策略。

Network information security: Agame that ever changes

PAN Zhuting

Beijing Venustech Cybervision Co.,Ltd, Beijing 100193, China

Abstract The area of cyber security is like a game of chess, whose fundamental construction is explored in this paper. The area is described through the southward view which is technic oriented and the northward view that is awareness and management oriented. Referring to the medical division pattern, the author divides the area of cyber security into several sub-areas, peeks into their internal rules, and digs into the group of people who play crucially influential roles in that sub-area. The author expects to offer a view of observing the whole landscape and provides several key points which can help to draw the outline of this area.

Keywords cyber security; information security; hacker

(责任编辑 刘志远)