国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

国之重器出版工程
网络强国建设

学术中国·院士系列
未来网络创新技术研究系列

Dynamically-enabled
Cyber Defense

动态赋能网络空间防御

杨林　于全　编著

国工信出版集团　人民邮电出版社
POSTS & TELECOM PRESS

国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

动态赋能网络空间防御

Dynamically-enabled Cyber Defense

杨林 于全 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

动态赋能网络空间防御 / 杨林，于全编著. -- 北京：人民邮电出版社，2018.7
国之重器出版工程. 学术中国·院士系列. 未来网络创新技术研究系列
ISBN 978-7-115-48561-8

Ⅰ. ①动… Ⅱ. ①杨… ②于… Ⅲ. ①计算机网络－网络安全 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第102676号

内 容 提 要

本书提出了基于动态赋能的网络空间防御，深入剖析了系统同源同质带来的问题，归纳总结了当前动态化技术发展的基本现状。以整个被防御的信息系统实体层次结构为依托，从自身内部的硬件平台、软件服务、信息数据和外部的网络通信4个方面分别研讨了目前主流的动态化防御技术，探讨其可能的演进路线，梳理与现有安全技术产品的关系，并对这些技术的安全增益、系统综合效率等方面进行宏观分析和讨论。

本书主要面向对动态赋能的网络空间防御感兴趣的电子信息相关专业的研究生和从事网络安全科研工作的学者及工程技术人员，可作为电子信息相关研究生课程的教材，也适合于从事相关研究的科研工作者阅读与参考。

◆ 编　　著　杨　林　于　全
责任编辑　代晓丽　刘　琳
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：710×1000　1/16
印张：18.25　　2018年7月第1版
字数：338千字　　2018年7月河北第1次印刷

定价：128.00元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

《国之重器出版工程》
编辑委员会

专家委员会委员（按姓氏笔画排列）：

于　全　中国工程院院士

王少萍　“长江学者奖励计划”特聘教授

王建民　清华大学软件学院院长

王哲荣　中国工程院院士

王　越　中国科学院院士、中国工程院院士

尤肖虎　“长江学者奖励计划”特聘教授

邓宗全　中国工程院院士

甘晓华　中国工程院院士

叶培建　中国科学院院士

朱英富　中国工程院院士

朵英贤　中国工程院院士

邬贺铨　中国工程院院士

刘大响　中国工程院院士

刘怡昕　中国工程院院士

刘韵洁　中国工程院院士

孙逢春　中国工程院院士

苏彦庆　“长江学者奖励计划”特聘教授

苏哲子　中国工程院院士

李伯虎　中国工程院院士

李应红　中国科学院院士

李新亚　国家制造强国建设战略咨询委员会委员、中国机械工业联合会副会长

杨德森　中国工程院院士

张宏科　北京交通大学下一代互联网互联设备国家工程实验室主任

陆建勋　中国工程院院士

陆燕荪　国家制造强国建设战略咨询委员会委员、原机械工业部副部长

陈一坚　中国工程院院士

陈懋章　中国工程院院士

金东寒　中国工程院院士

周立伟　中国工程院院士

郑纬民　中国计算机学会原理事长

郑建华　中国科学院院士

屈贤明　国家制造强国建设战略咨询委员会委员、工业和信息化部智能制造专家咨询委员会副主任

项昌乐　“长江学者奖励计划”特聘教授，中国科协书记处书记，北京理工大学党委副书记、副校长

柳百成　中国工程院院士

闻雪友　中国工程院院士

徐德民　中国工程院院士

唐长红　中国工程院院士

黄卫东　“长江学者奖励计划”特聘教授

黄先祥　中国工程院院士

黄　维　中国科学院院士、西北工业大学常务副校长

董景辰　工业和信息化部智能制造专家咨询委员会委员

焦宗夏　“长江学者奖励计划”特聘教授

前 言

互联网是 20 世纪人类最伟大的技术发明之一。自诞生以来，历经半个世纪的发展，互联网已成为驱动全球经济社会发展的重要基础设施，深刻地改变了人们的生产、生活方式。然而，利益与风险总是并存，网络攻击像梦魇一样伴随着信息化的过程，如影随形，无法摆脱，网络安全已成为影响人类社会发展的全球性问题。

漏洞是网络攻防活动能够发生的前提，是网络不安全的根源，是攻防双方争夺的战略资源。信息系统是由人设计和实现出来的，人的天生惰性和认知局限性，导致漏洞无法避免，随着系统复杂性的增大，漏洞问题将更加严重。在网络攻防活动中，攻方发现漏洞、利用漏洞；防方发现漏洞、修补漏洞，降低漏洞被利用的机会。但是在漏洞面前，攻防双方是不平等的。攻方掌握了一个未公开漏洞，就可能长驱直入，直捣黄龙；防方掌握了再多的漏洞，也不敢高枕无忧。随着攻方掌握分析系统的时间越长，发现的漏洞将越来越多，系统也将越来越危险。因此，攻防双方存在严重的不对称性，小攻大防、一点攻全局防。

APT(Advanced Persistent Threat，高级持续性威胁) 是网络安全的心腹大患。Advanced 是指高级的、先进的、大投入的，强调有背景的组织行为、国家行为。Persistent 是指长期的、持续的，因此也是最为可怕的。敌手在长期地、持续地盯着你、研究你、分析你，攻方有可能比我们自己还要了解被保护的系统。攻方持续不断地发现问题，持续不断地研发出对付你的武器。我们有没有像攻方那样研究过自己的系统，持续不断地关注被保护的系统有什么安全漏洞？我们在持续不断地发展信息化，持续不断地上新项目，持续不断地建新系统，却未能持续不断地关注这些信息系统的安全。敌手在持续不断地发现问题，我们却在持续不断地积累问题。

从安全的视角看，信息系统建设还存在诸多问题。很多系统还在解决功能的有

无，无暇顾及系统自身有什么安全漏洞，更谈不上安全漏洞的监督检查，没有意识，也没有精力去关注漏洞和安全，更不会持续地关注安全。在信息系统建设过程中，人们习惯将安全体系建设等同于一般的系统建设，将安全体系构建理解为安全产品的静态堆砌，“连通即好”竟然经常成为安全就绪的标志。信息系统开通有个状态固化的过程，状态一旦固化，能力则随之固化。信息系统强调“三互”，即互联、互通、互操作，要求技术体制统一，在工程实践中则往往是以有形产品代无形体制，用同样的产品统一体制，这样的体制一经统一，能力随之统一。信息系统架构的静态性、相似性和确定性，以及信息产品的“同源、同构、同制”，给攻方刺探网络特性、掌握系统漏洞、实施攻击渗透提供了极大便利，导致信息系统始终处于被动挨打的局面，单个攻击手段一旦对局部生效，往往便能很快扩散开来，对全网造成大面积影响，一破百破，一瘫百瘫。

基于先验知识和精确识别的传统防护手段，难以应对未知漏洞和未知攻击威胁；基于静态性、相似性、确定性构建的信息系统，难以应对动态的、专业的、持续的高强度攻击。漏洞是安全问题的根源，但挖漏洞、堵漏洞却不可能成为解决安全问题的根本。挖漏洞竞赛，对防方和攻方而言，胜败游戏规则本就不平等，防方挖得再多，堵得再好，也挡不住攻方哪怕是一次防方未知的漏洞攻击。防方要想摆脱这种被动局面，就必须改变这种不平等的游戏规则，从防方跟着攻方走，改为攻方跟着防方走。网络空间动态防御是形成易守难攻不对称防御能力的很好途径。

在军事领域，动态防御的思想可谓源远流长。《孙子兵法》云：“兵者，诡道也”。意思是用兵之道，在于千变万化，出其不意。动态目标防御（Moving Target Defense）就是将“变”的思想运用于网络空间防御，其创新性在于一反常态，由阵地保卫战改为运动战或游击战。在部署、运行信息系统时，通过有效降低信息系统的确定性、相似性和静态性，增加其随机性，降低其可预见性，从而构建持续变化、不相似、不确定的信息系统，让信息系统对外呈现不可预测的变化状态，攻击者难以有足够时间发现或利用信息系统的安全漏洞，更不容其持续探测、反复攻击，从而大大提高了攻击的难度和代价。显然，这是防护策略的大转变和游戏规则的大变革，改变了网络易攻难守的不对称局面。

本书在动态目标防御基础上，提出动态赋能网络空间防御这一概念，将“变”的思想全面应用于网络空间各个环节，用体系化的动态防御思路颠覆传统的防护思路，对信息系统全生命周期全面贯彻动态安全理念，即要求信息系统在研制、部署、运行等各个阶段，不仅要完成其自身功能，而且要在硬件平台、软件服务、信息数据、网络通信等各层次上都能变换其与安全相关的特征属性。这种变换涉及时间和空间两个维度，可能是某个属性单独变换，也可能是多个属性同时变换。通过这些变换，增强信息系统内生安全性。另外，这种动态赋能思想指导下的防御体系，不

仅是在前台实施防护，还要集约调度聚集在后台的专业资源和专业力量，将新的安全能力源源不断地向前台动态输出，提供全局赋能的新活力。从体系角度看，动态赋能就是要将静态设防的死装备，变成动态赋能的活体系，形成前台防护、后台赋能的动态主动网络空间防御体系。

动态赋能网络空间防御是对网络空间安全防御技术和体系的一种探索，是将安全能力作为信息系统自身标准属性的一种设想。未来的网络空间防御体系一定是在动态赋能思想指导下的安全体系。因此，各类系统动态化、随机化的技术、方法及其与现有防护手段的关系、贡献、兼容、演进问题，对下一代防护产品甚至信息产品带来的挑战和问题，都是本书关注的问题。

目前，围绕动态防御的相关理论研究已取得一些进展，一些关键技术的发展也使动态防御的工程应用成为可能。由于动态赋能防御研究涉及面广、难度大，目前的研究成果还较为零散、系统性不强。为了便于读者更为系统地理解动态赋能防御所涉及的技术，本书归纳总结了当前动态防御技术发展的基本现状，提出了动态赋能防御的体系架构，以信息系统的实体层次结构为依托，从系统平台、软件服务、信息数据和网络通信 4 个方面分别研讨了动态防御技术，探讨其可能的演进路线，梳理与现有安全技术的关系，并对动态赋能防御的安全增益、系统综合效率等方面进行了分析和讨论。本书期望将动态赋能网络空间防御的相关思想、技术和成果呈现给读者，将先进的理念、技术和方法落到实处，为以能力为导向的网络空间安全提供支撑，也为未来具有内生安全能力的信息系统结构设计与软 / 硬件产品开发提供参考。

希望本书的出版有助于我国网络空间安全领域相关研究人员准确把握网络空间安全的技术发展方向，为下一代 IT 基础设施的发展提供思路；有助于推动未来网络空间主动防御体系的构建，让安全不再是信息系统发展的障碍，让安全成为信息系统发展的内生能力。

由于动态赋能网络空间防御涉及面广、技术难度大且尚不够成熟，虽然我们付出了很大努力，书中仍可能存在疏漏。不当之处，敬请读者批评指正。

作 者

目 录

第1章 绪论

网络将人类从工业时代带进了信息时代，在短短几十年里，就彻底改变了人类社会的面貌和人们的生产生活方式。无数新生的信息产品给个人的工作生活带来了新奇而美好的体验，但也存在巨大的隐患和风险。网络攻击所导致的安全风险与安全威胁，像梦魇一样伴随着信息化的进程无法摆脱。在实践当中，人们逐渐认识到漏洞是安全问题的本源，其客观存在性以及现有防护的被动性使网络攻防具有易攻难守的不对称态势。为此，本书提出了动态赋能的理念，将中国传统文化中“变”的思想进行系统化、体系化的应用，设计动态变化的技术机理和体系，以期彻底改变安全防护工作长期以来的被动局面。