国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

“十二五”
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

动态赋能
网络空间防御

杨林　于全　编著

Dynamically-enabled Cyber Defense

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

"十二五"
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

动态赋能
网络空间防御

■ 杨林 于全 编著

Dynamically-enabled Cyber Defense

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，2016.7
（学术中国. 院士系列. 未来网络创新技术研究系列）
ISBN 978-7-115-41450-2

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

中国版本图书馆CIP数据核字(2016)第031258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
执行编辑　刘　琳
责任印制　彭志环

◆ 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
北京圣夫亚美印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：16　　2016 年 7 月第 1 版
字数：314 千字　　2016 年 7 月北京第 1 次印刷

定价：88.00 元

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

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，强调是有背景的组织行为、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，更谈不上持续的安全关注。

在信息系统建设过程中，习惯于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，能力随之单一。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转变，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得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，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，并对这些技术的安全增益、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

2016 年 1 月

目 录

第1章 绪 论

1.1 信息化时代的发展与危机

互联网技术自问世以来，先是用在军事、教育和科研部门，后来迅速向政治、经济、社会和文化等各个领域渗透。网络就把人类从工业时代带进了信息时代，其速度之快，出乎人们的预料。在短短几十年里，网络已彻底改变人类社会的面貌和人们的生产生活方式。

1.1.1 信息化的蓬勃发展

当前，信息技术发展的总趋势是以互联网技术的发展和应用为中心，从典型的技术驱动发展模式向技术驱动与应用驱动相结合的模式转变。一方面，家用电器和个人移动终端都向网络终端设备的方向发展，形成了网络终端设备的多样化和个性化，逐步改变了曾经计算机网络一统天下的局面；另一方面，电子政务、远程教育、电子商务等技术日趋成熟，互联网对个人生活方式的影响逐步深化，从基于信息获取和沟通娱乐需求的个性化应用，发展到与医疗、教育、交通等公用服务深度融合的民生服务。与此同时，随着“互联网+”行动计划的出台，互联网将带动传统产业的变革和创新。未来，在物联网、云计算、大数据等技术应用的带动下，互联网将加速农业、现代制造业和生产服务业转型升级，形成以互联网为基础设施和实现工具的经济发展新形态。

今天，中国已成为网络大国。仅以互联网为例，自 1994 年互联网正式引入我国以来，在短短 20 多年时间里，我国互联网迅速发展，普及率已超过世界平均水

平，互联网已成为我国重要的社会基础设施。据中国互联网络信息中心（CNNIC）统计数据，截至 2015 年 6 月，我国网民规模达 6.68 亿人，手机上网用户数达 5.94 亿，中国域名总数为 2 231 万个，其中，.CN 域名总数为 1 225 万个，网站总数为 337 万个。统计显示，各种网络应用十分活跃，网民的人均周上网时长达 25.6 小时，每天上网约 3.7 小时。搜索引擎用户规模达 5.36 亿人，网络新闻用户规模达 5.55 亿人，网络购物用户规模达 3.74 亿人，其中，团购用户规模达 1.76 亿人，使用网上支付的用户规模达 3.59 亿人，使用过网上预订机票、火车票、酒店或旅游度假产品的网民规模达 2.29 亿人，互联网理财网民规模达 7 849 万人，即时通信用户的规模达 6.06 亿人，微博客用户规模达 2.04 亿人。

移动互联网发展迅速，手机网民规模继续保持增长，网民上网设备逐渐向手机端集中。随着手机终端的大屏化和手机应用体验的不断提升，手机作为网民主要上网终端的趋势进一步明显。移动商务类应用发展迅速，助力消费驱动型经济发展。移动互联网技术的发展和智能手机的普及，促使网民的消费行为逐渐向移动终端迁移和渗透。由于移动终端即时、便捷的特性更好地契合了网民的商务类消费需求，伴随着手机网民的快速增长，移动商务类应用成为拉动网络经济增长的新引擎。

物联网概念更加深入人心，物联网正成为经济社会绿色、智能、可持续发展的关键基础和重要引擎。物联网应用仍处于发展初期，物联网在行业领域的应用逐步广泛深入，在公共市场的应用开始显现，M2M（Machine to Machine，机器与机器）通信、车联网、智能电网是近两年全球发展较快的重点应用领域。M2M 是率先形成完整产业链和内在驱动力的应用，车联网是市场化潜力最大的应用领域之一，全球智能电网应用逐步进入发展高峰期。不远的将来，我们还将从今天的物联网（Internet of Things，IOT）时代步入万物互联（Internet of Everything，IoE）的时代，所有的东西将会获得语境感知、增强的处理能力和更好的感应能力，创作出无限可能。

1.1.2 信息化的美好体验

信息技术发展不断带来各种惊喜。在信息时代的今天，无数新生的信息产品就像竞相绽放的花蕊，给人无限美好的感觉，给个人工作生活的方方面面带来新奇而美好的体验，或方便、或快捷、或丰富、或时尚。

网购让你足不出户买到满意商品。还有什么东西不能在网上买到吗？恐怕已经很少了。现在，当你乔迁新居后，只需要通过电脑或手机，进入一家电商的主页，根据自己的需要搜索到心仪的电器，下单即可，剩下的就是在家等着收货，电商会派人上门安装调试，而几年前，你可能还要揣着大把现金跑到一个较远的电器城，挨家比较各种电器的性能和价格，选定电器后自己找车运回家。

微信让沟通变成零距离。不知何时，你已经不再使用QQ和亲戚朋友联系了，你习惯了微信，随时有感而发，发个朋友圈，随时看到好友发的各种信息。突然有一天，微信里面蹦出一个群，里面有好多熟悉的名字，都是毕业多年未联系的大学同学，这些同学们分布在祖国各地或是国外，但是从同学群建立的那一刻起，你们之间的距离变成在手机屏幕上点几下的距离。有一天下班回家，你发现年迈的母亲也学会了玩微信，她捧着平板电脑，兴奋地和远方的亲戚视频聊天，在随后的几天，她把好久不联系的亲戚朋友都挨个联系了一遍。

打车软件让你出行更方便。为待在一个像北京这样的超大型城市因摇不上号而无法买车，打车也不太好打，于是滴滴打车、快的打车出现了，它能迅速通知到周围几百台出租车，很快有司机和你联系，一分钟之后，一辆的士来到你跟前。

互联网金融助力理财、创业。过去两年，阿里巴巴、百度、腾讯等互联网企业纷纷推出金融服务和产品，在支付、借贷、汇兑、理财等传统金融领域攻城略地，种种迹象表明，互联网正加速向金融领域进军。事实上，互联网金融正从单纯的支付业务向转账汇款、跨境结算、小额信贷、现金管理、资产管理、供应链金融等传统金融业务领域渗透。以小额信贷为例，数据显示，中国电商小贷累计贷款规模2014年已达2 300亿元。可以预期，未来将有更多涉及小微企业的贷款业务将依托阿里小贷这样的电商平台完成。

小小的手环给你带来健康的生活方式。手环可以记录你的睡眠、运动等数据，让你随时掌握自己身体状况，成为健康小秘书。你可以给自己设定目标，比如，每天行走8 000步，你可以设置提醒，保证每天都能达到目标。手环会做专业统计，告诉你在哪个时间段，你行走了多少公里，消耗了多少千卡热量，估算所消耗能量相当于一瓶可乐或者一个煎蛋，成为减肥者的福音。手环会将你的运动数据与云端其他用户做比较，告诉你的步数超过百分之多少的其他用户。手环还会告诉你昨晚你睡了几个小时，深睡几个小时，让你有数据来评价自己的睡眠质量。

你会因为出行没有买到火车票而烦恼，却不能一直在电脑前守着等待有人退票，于是抢票软件出现了，输入你要的车次，它会替你完成抢票工作。

当你的小孩到了上学年龄，你为了他即将离开你的视线而放心不下时，儿童手表出现了，通过定位，你随时可以知道他在哪里，他有需要时也可以和你通话。

诸如此类的惊喜还可以列举很长一大段。上面这些可能还只是开始，今后还会有更多的惊喜出现。

1.1.3 信息化带来的危机

互联网既是“机会之窗”，给人们带来诸多便利和好处，又是“易受攻击之窗”，存在巨大的隐患风险。社会对互联网的依赖性越强，网络信息的安全就越重要，

网络攻击带来的威胁就越严重。随着互联网向社会各行各业的渗透，绝大多数国家的通信网、电网、金融业、运输系统等网络都已经连成一体，形成一个巨大的网络，给各国带来巨大的安全风险。网络没有边界，但对于一个主权国家而言，保护关系国计民生的重要国家关键基础设施和民用网络是巨大的挑战。世界上几乎所有国家都一致认为，目前网络空间非常脆弱，漏洞百出，网络安全令人担忧。

信息化的迅猛发展必然带来诸多网络安全威胁等伴生性问题，我国也不例外。我国基础网络仍存在较多漏洞风险，云服务日益成为网络攻击的重点目标。域名系统面临严峻的拒绝服务攻击，针对重要网站的域名解析篡改攻击频发。网络攻击威胁日益向工业互联网领域渗透，已发现我国部分地址感染专门针对工业控制系统的恶意程序事件。分布式反射型的拒绝服务攻击日趋频繁，大量伪造攻击数据分组来自境外网络。针对重要信息系统、基础应用和通用软/硬件漏洞的攻击利用活跃，漏洞风险向传统领域、智能终端领域泛化演进。网站数据和个人信息泄露现象依然严重，移动应用程序成为数据泄露的新主体。移动恶意程序不断发展演化，环境治理仍然面临挑战。

各种新设施的建成、新技术的应用、新产品的涌现，使人们在享受便利和好处的同时，也无法忽略头顶上的朵朵乌云，如果不采取有效的措施，将造成各种各样不可预料的严重后果。

（1）工控系统威胁：置国家于危险之中

工控系统现在已经普通应用于几乎所有的工业领域和关键基础设施中，涉及的方面广泛。因此，工控系统的安全问题对国民经济的正常运转和国家的安全构成重大威胁。2010 年出现的震网（Stuxnet）病毒 [1]，其攻击目标直指西门子公司的 SIMATIC WinCC 系统，这是一种运行与 Windows 平台的监控和数据采集（Supervisory Control and Data Acquisition，SCADA）系统，被广泛应用于钢铁、汽车、电力、运输、水利、化工、石油等工业系统。Stuxnet 能够控制物理系统参数，使用 PLC Rootkit 修改控制系统参数并隐藏 PLC 变动，从而对真实物理设备和系统造成物理损害。伊朗政府后来确认其第一座核电站——布什尔核电站遭到 Stuxnet 蠕虫的攻击，造成 1/5 的离心机报废。

（2）云计算平台：数据安全隐忧

云平台技术的深入发展及其对服务模式的重构，使服务无处不在。云平台服务是一种混合的服务模式，这种特征既可能引入传统的威胁，又会带来新的威胁。而云平台与传统系统平台的部署模式不同，使其更容易受到威胁，例如，2011 年 Sony（索尼）公司的 PlayStation 网络和 Sony 在线娱乐遭受一系列攻击，造成在线游戏云平台网络瘫痪，并使用户账户数据的安全受到威胁[2]。

（3）移动智能终端：知道危险却离不开

现在移动智能终端已伴随几乎每个用户的日常生活，这些设备除了可以通过

基站或无线网络连接互联网，还可以打电话、发短信、彩信、拍照、录音、导航、定位、蓝牙传输以及近场通信（Near Field Communication，NFC）。丰富的各种功能在提升终端适用性的同时，也引入了更多形态的漏洞。以短信为例，2012 年，法国黑客 pod2g 发现了存在于苹果智能手机（iPhone）所有版本中的短信欺骗漏洞[3]，利用该漏洞，任何人都可以伪造号码向任何 iPhone 用户发送短信，并将受害者的回复短信引导至伪造号码。2015 年 7 月，以色列 Zimperium 移动安全公司研究人员 Joshua Drake 发现 Android 系统核心组件 Stagefright 框架存在允许黑客执行远程恶意程序的严重安全漏洞，一旦用户接收并打开一条彩信，通过浏览器下载特定视频文件或者打开嵌入多媒体内容的网页，黑客就能入侵手机。该漏洞俨然成为 Android 系统最危险的漏洞，影响 95%的 Android 用户。

以智能手机为代表的移动智能终端携带了许多高价值的用户信息。因此，用户数的迅速增加吸引了许多厂商，包括恶意程序开发者的关注，以搜集用户信息尤其是其隐私信息为主要目的的程序不断涌现。

（4）智能手环：没开包就被强制控制

作为一款兴起没多久的高科技可穿戴智能设备，智能手环的普及率已经相当高。目前市场上的手环品牌也是五花八门，用户可选择的产品非常多，如图1-1所示。手环一般都会无巨细地记录用户的信息。很多用户一出门就会戴上他们的智能产品，黑客一旦侵入，就能轻易地得知用户的住址、工作甚至喜欢的餐厅。央视节目中有过演示[4]，使用一款软件强制与一个尚未开封使用的新手环配对，即可让手环在包装盒里执行动作。一位技术人员戴着智能手环在一个房间内活动，另一名技术人员在其他房间内破解手环，如图 1-2 所示。电脑画面中显示，佩戴手环者的一举一动均可以被实时监测，并以圆点抖动的形式展现。根据圆点抖动幅度，甚至可以判断佩戴者的运动行为。

图 1-1 五花八门的智能手环产品