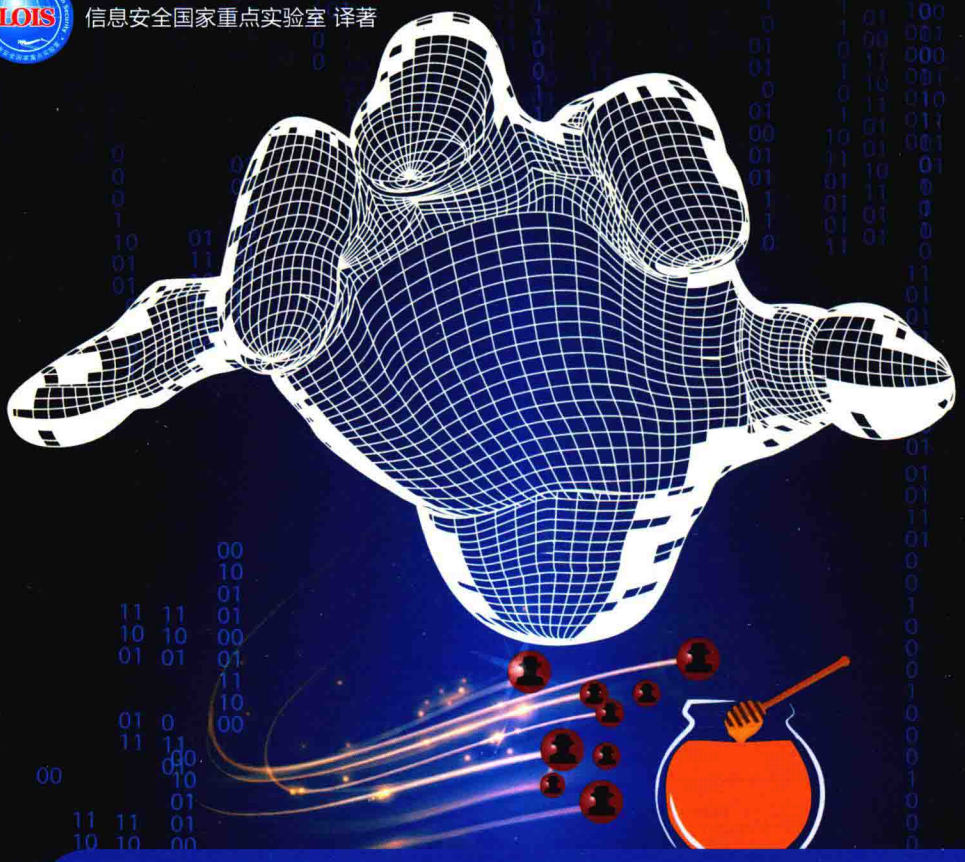
HZ BOOKS
华章科技

信息安全国家重点实验室 译著



网络空间欺骗

构筑欺骗防御的科学基石

Cyber Deception

Building the Scientific Foundation

[美] 苏西尔·贾乔迪亚（Sushil Jajodia）
V.S.苏夫拉曼尼（V.S. Subrahmanian）
维平·斯沃尔（Vipin Swarup）
克利夫·王（Cliff Wang） 著

马多贺 雷程 译

机械工业出版社
China Machine Press

网络空间欺骗

构筑欺骗防御的科学基石

Cyber Deception

Building the Scientific Foundation

[美] 苏西尔·贾乔迪亚（Sushil Jajodia）
V.S.苏夫拉曼尼（V.S. Subrahmanian）
维平·斯沃尔（Vipin Swarup）
克利夫·王（Cliff Wang） 著 马多贺 雷程 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络空间欺骗：构筑欺骗防御的科学基石 /（美）苏西尔·贾乔迪亚等著；马多贺，雷程译．
—北京：机械工业出版社，2017.1
（信息安全技术丛书）
书名原文：Cyber Deception: Building the Scientific Foundation

ISBN 978-7-111-56869-8

I. 网… II. ①苏… ②马… ③雷… III. 互联网络－诈骗－预防－研究 IV. D588

中国版本图书馆 CIP 数据核字（2017）第 108934 号

本书版权登记号：图字：01-2017-0504

网络空间欺骗：构筑欺骗防御的科学基石

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：张梦玲　　责任校对：李秋荣
印　刷：北京市荣盛彩色印刷有限公司　　版　次：2017 年 8 月第 1 版第 1 次印刷
开　本：186mm×240mm　1/16　　印　张：16
书　号：ISBN 978-7-111-56869-8　　定　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

Foreword 推荐序一

21 世纪的信息化进程，正以“彻头彻尾彻里彻外”的形式，以前所未有的速度、深度和广度，走向人类社会（人）、信息网络（机）与物理世界（物）的深度融合。人的社会属性已延伸到网络世界，同时网络社会的安全事件也深刻影响着人类社会及其社会生产活动。因此，如何保障网络空间安全是当前信息安全研究面临的重要挑战。当防御者在利用云计算 IaaS、PaaS、SaaS 架构来探索构建“海、网、云”协同防御体系时，黑客已经公然推出了 HaaS（Hacker as a Service，黑客即服务）的创新模式，悄悄踏上了攻击服务化的快车道。在现实的安全实践中，网络空间“人、机、物”的防御天平严重倾斜，“人”作为网络空间中的一部分，其交互行为对网络系统产生的安全影响鲜有讨论。所谓的“舆情分析”“行为分析”和“社会感知”等基于分析的安全技术，效果差强人意。正如美国陆军研究实验室计算机应急响应团队负责人安吉洛·本基文加所说：“那些如痴如醉仰望星空意欲预测未来的人们，他们以为眼中观察的星星都是当下之物，殊不知那可能是亿万年前已经消失的星球留下的残余光影。与此类似的，一些计算机安全‘专家’也在醉心于分析、挖掘网络中的海量异常事件，却拒绝承认这是‘马后炮’的做法。攻击已经发生、损失已经造成、黑客已经离场、事件未必再次重演，因此等到事后再穷追不舍地研究，于事无补。这些‘专家’的安全防御思想完全是错误的。”用所谓的事后分析方法去研究网络空间的“人”，何尝不是类似的徒劳无功。

为了抵御网络空间中的“人”，最核心的是在防御体系中融入“交互”这个关键要素。在实时场景的交互过程中，人可以倾其所能与对手博弈。古有诸葛亮用兵如神，一场以小博大、以弱胜强的“空城计”，令世人叹为观止，成为欺骗防御的千古经典。如果没有空城之上军师独自抚琴与城下千军万马形成的瞬间情景交互，空城很可能成为铁蹄下的烂城。本书同样按照交互程度对欺骗能力进行评估，所以才有了“低交互蜜罐 / 高交互蜜罐”“独立蜜罐 / 嵌入式蜜罐”等分类。

欺骗之法如兵法：“运用之妙，存乎一心。”如要透过玄妙的欺骗之术建立严谨的理论体系，

不是一件容易的事情。

数学是科学的基础，一切科学问题最终都要归结为数学问题。信息安全领域中，通常将安全性等价映射为数学难题。本书最基本的贡献在于将看似纷繁复杂而又极为具体的欺骗实例，抽象为更加严谨的数学问题，用数据工具来阐述其科学原理。一个欺骗防御系统设计的好不好，一个欺骗策略是不是有效，并不是定性地解释为欺骗故事编撰得多么生动、多么以假乱真，而是应该将其用数学理论来定量评估。一个欺骗系统不能保证所有敏感信息都不泄露，但是只要攻击者成功辨别信息真假的概率等价于胡乱猜测其真假的概率，欺骗防御系统的安全性就有了概率论这个理论依据，这也是采用数学工具指导欺骗防御系统设计的科学基础。

“求安全理论之真，务信息保障之实”是新时期信息安全国家重点实验室的指导方针。当前，网络空间安全新思想、新工具、新技术方兴未艾，特别是欺骗性防御技术才刚刚起步，构建欺骗防御的科学基础更是任重道远。译者在信息安全国家重点实验室从事移动目标防御（MTD）、网络空间欺骗等新兴防御技术研究。力求通过翻译、推荐本书，能使国内的更多学者参与其中，共同夯实欺骗防御的理论体系，促使其在网络空间安全保障中发挥更大的作用。

林东岱研究员

信息安全国家重点实验室主任

2017 年 7 月

Forword 推荐序二

当前，信息技术的普及和深度应用已成浩荡之势。我国作为拥有超过 7 亿网民的网络大国，如何利用信息与网络技术的发展大潮借势而起、乘势而发，已成为建设网络强国的关键。随着“震网”“斯诺登”事件的不断曝光，网络攻击复杂化、智能化、自动化的特点可见一斑，网络安全问题日益严峻。习近平在网络安全和信息化工作座谈会上深刻指出：“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”他特别强调：“网络安全的本质在对抗，对抗的本质在攻防两端能力的较量。要以技术对技术，以技术管技术，做到魔高一尺、道高一丈。”网络空间防御作为保证网络安全的关键，无论在方法理论、体系构建，还是技术实施等方面都在不断推陈出新。不同于以往“封门堵漏”的被动防御思想，网络空间防御正朝着主动防御的思想策略发展演变。无论是通过增加内生安全实施主动免疫的可信计算理论，亦或是通过增加网络系统不确定性以提高攻击成本的拟态防御技术，它们都是对主动防御思想策略的不同诠释，网络空间欺骗防御正是在这种探索下提出的。网络空间欺骗防御不同于以往追求构建完美无瑕的系统以抵御攻击的思路，而是一种通过不断变换系统特性、限制脆弱性暴露、欺骗攻击视图、增加攻击成本等方法，以提升防御有效性的主动防御新技术。正如《孙子兵法》中所述：“兵者，诡道也。故能而示之不能，用而示之不用，近而示之远，远而示之近。”

本书是 IEEE 院士 Sushil Jajodia 和 AAAI 院士 V.S. Subrahmanian 等人，继《Moving Target Defense》出版后的又一力作。作者在网络空间防御研究方面极具前瞻性和很高的专业水准，是网络空间欺骗防御的开拓者和实践者。本书对网络空间欺骗科学问题进行了一系列重要探索，从网络空间欺骗防御的架构、欺骗防御的工具、欺骗防御的部署实施、欺骗防御的人为因素，以及欺骗防御效果的度量评估等方面系统地介绍了网络空间欺骗防御的理论体系与技术，反映了当今国际网络空间欺骗防御领域顶尖研究团队的最新研究进展和成果。

本书译者作为我国网络空间安全防御的后起之秀，敏锐地洞察到了网络空间欺骗防御的

前沿思想和优秀实践，依据对网络空间欺骗防御思想的深刻理解，结合自身在网络空间欺骗防御实践方面的技术积累和切身体会，深入浅出地阐释了网络空间欺骗防御的深奥理论和技术细节。在网络空间欺骗防御思想不断发展、欺骗防御技术逐步成熟之际，翻译了这样一本系统、权威的网络欺骗防御书籍，不仅有助于网络空间安全领域从业人员加深对网络空间欺骗防御理论和技术的理解，更为网络空间安全学科专业建设与人才培养增添了浓墨重彩的一笔，应该说恰逢其时，很有意义。

张红旗教授

解放军信息工程大学密码工程学院副院长

2017 年 7 月　于郑州

Forword 推荐序三

欺骗是人类天性的一部分，也是人类作为高智商生灵的独特表征。欺骗一直存在于人类活动的各个方面，如战争、体育、游戏、爱情等，从古绵延至今五千年。欺骗本身是中立的和中性的，是善是恶，取决于使用这项技能的目的。不过在网络空间的信息对抗中，欺骗技术长期为恶意攻击者利用，而往往被忠厚的防御者所忽视。

网络空间威胁两极分化严重：一方面，伴随互联网的发展和黑客论坛的繁荣，攻击知识和渗透工具广泛传播，攻击门槛越来越低，脚本小子级别的黑客攻击泛滥；另一方面，“道高一尺魔高一丈”，长期的防攻对抗也迫使网络攻击向着专业化水平发展，甚至国家队级别的 APT 攻击也多次粉墨登场。洋葱路由（Tor）、暗网（Darknet）等利器日臻完善，震网病毒（Stuxnet）、魔窟勒索软件等 0day 漏洞利用层出不穷，混淆、隐匿、伪造、钓鱼等欺骗手法更是愈加绝妙。

反观信息对抗的防御方，以特征检测为核心的静态防御，逐渐力不从心。主要原因是信息不对称，攻击者对防御方的安全策略了如指掌，而防御规则无法洞察攻击者眼花缭乱的伎俩以及深藏不露的动机。虽然安全防御技术也在不断发展，例如，被人们寄予厚望的量子保密通信、后量子密码等，但是这些技术距离大规模应用仍有一段长路。

传统的信息对抗是计算和计算的对抗，寻找的是系统的弱点；欺骗防御则是人与人的对抗（防御者 vs 攻击者），寻找的是人性的弱点。正如本书所阐述的，一个欺骗防御是否能够成功，主要在于防御者能否利用攻击者的多种偏见：个人偏见、文化偏见、组织偏见、认知偏见等。而文化偏见又包含诸多内容，如权利距离指数（PDI）、个人主义与集体主义（IVC）、男权主义与女权主义（MVF）等。面临艰难抉择时，彪悍的民族热衷于决斗，而中庸的民族习惯于抓阄。以打折促销、免费中奖为幌子的诈骗手段在第三世界屡屡得手，在发达国家就未必具有诱惑力。如果敌手没有偏见，就不会失去理性，也就没有上当受骗的可能，欺骗就无从下手。

实践表明，欺骗防御是切实有效的，而且在未来的信息对抗中将扮演越来越重要的作用。即使人类进入量子计算时代，但凡人性的弱点还没有消失，欺骗和防御的故事还会不断上演。欺骗的挑战在于，一个经典的欺骗故事只能用一次，一旦完成了一次欺骗，敌手就会对这类欺骗刻骨铭心、倍加防范，想要实现帽子戏法基本不可能。这也是欺骗防御在网络对抗中的魅力所在。一个成功的欺骗，就可能力挽狂澜、扭转攻防局面，甚至因改变历史而会永垂史册。

如何将人的因素引入到信息安全的科学体系中，还需要不断的探索，本书是一个良好的开始。目前在高等院校网络空间安全学科的教学体系中，关于欺骗防御的教程基本是空白的。

欣而作序，推荐给网络空间安全专业和信息对抗领域师生和同行参阅。

李琼教授

哈尔滨工业大学计算机学院信息对抗技术研究所所长

2017 年 7 月

The Translator's Words 译 者 序

一直以来，网络安全不得不面对这样一个残酷的现实：防御者疲于应对不计其数的漏洞以求保障安全，而敌手只需要找到一个脆弱性即可实施攻击。网络攻防游戏的主动权掌握在攻击者手中。

某次于内华达 Las Vegas 参加一个网络安全国际学术会议，同城还有另外两个安全相关盛会：全球黑客大会 DEFCON 和 BlackHat。同样是安全会议，学术这边门可罗雀、冷冷清清；而一墙之隔的 DEFCON CTF 门庭若市、好不热闹。那次黑客大会使用一种大而醒目的参会胸牌。放眼望去，满大街都挤满了佩戴此胸牌的来自世界各地的参加 DEFCON 和 BlackHat 的人群，其中不乏带着小孩参会的家庭。整个赌城洋溢着一片欢乐的“黑色”节日气氛。这些不谙世事的孩子未必知道夺旗比赛的本质是什么，估计认为利用新漏洞攻击是一件很酷、很炫的事情。同样热衷于挖漏洞的不止是攻击者，即使在安全学术会议上，很多研究者也抛弃了加密、认证、隔离等正统防御方法的研究，转而去挖掘漏洞，以求快速地出成绩，酷炫地秀一把。漏洞成了备受攻防双方欢迎的“硬通货”。

漏洞是挖不完的，所以黑客威胁永远存在，这也决定了没有一劳永逸的防御方法，攻防竞赛永远存在。在写这段文字的时候，互联网世界正在被“永恒之蓝”漏洞利用勒索软件蹂躏。已经有大量的专业研究反病毒、数据恢复的同行夜以继日地进行救火，而那些被寄予厚望的所谓的威胁情报发现、各种 SRC 以及大数据分析系统因为被无视而略显尴尬。

要想改变攻防对抗的不对称格局，只有改变防御的游戏规则。移动目标防御（Moving Target Defense，MTD）正是这种变革思想的代表。与传统以封堵漏洞为核心的防御策略不同，MTD 通过不断改变目标系统的属性来动态转换其攻击面，从而提高敌手攻击的成本和代价。在虚虚实实、真真假假的转换中，网络空间不再是静止的，而成了瞬息万变的。为了扩大攻击面的转换空间，“欺骗”成为 MTD 的重要技术手段和工具。蜜罐、蜜饵、蜜标、蜜词本、无底洞文件、面包屑等欺骗元素，加之精心设计的欺骗故事和精心构建的欺骗场景，巨大的

信息熵让攻击者陷入难以判别方向的防御迷阵中。因此，“欺骗防御”的本意，并非戏弄攻击者或激怒攻击者，其最重要的价值在于为 MTD 系统提供增加攻击面转换空间的手段，提高 MTD 的防御熵。欺骗防御与 MTD 的连通就此建立。理解了“欺骗防御”与 MTD 一脉相承的关系，才能理解“欺骗防御”在整个网络空间安全中的位置和价值。本书的几位作者也是《 Moving Target Defense I &II 》图书的作者，而“欺骗”是 MTD 的重要组成部分，也是更高层次上的防御智能化的核心。

“欺骗”不是防御者的专利，相反，攻击者才是这项技能的始作俑者。世界顶级黑客凯文·米特尼克（Kevin D.Mitmick）的代表作《欺骗的艺术》，数十年来在网络安全界广为传阅。书中将黑客攻击的手法汇编成册，深入剖析了网络攻击中采用的多种精湛的欺骗之术，谓之欺骗的艺术。该书已经成为学习和研究社会工程学的圣经之作。矛和盾从来都是对立统一的，欺骗也可以作防御之用。因此，需要说明的是，本书不是攻击工具，不是诈骗手册，不是黑客信手拈来的社会工程学，而是一本站在米特尼克《欺骗的艺术》的对立角度阐述欺骗防御技术的科学研究读本。

随着人工智能、博弈论等理论体系的完善，以及软件定义网络（SDN）、云计算、虚拟化等新技术的成熟，“欺骗防御”已经远远超越了蜜罐的概念。本书涵盖的内容新颖、前沿、体系完备，包括网络空间抵赖与欺骗、MTD、暗网、黑客论坛、网络匿名、嵌入式蜜罐、虚拟攻击面，甚至素有“黑客奥林匹克”之称的 DEFCON CTF 等。在这本书中还重点介绍了网络欺骗的复杂性和多面性，指出由于其复杂性而引出的新的科学问题，并提出解决这些问题的新方法。无论从学术思维还是从技术路线上，相信对网络安全研究者都有启发意义。

本译著的出版得益于 Springer 出版社和华章公司多位领导、同事的努力；几位信息安全领域备受尊敬的老师和学长的作序和鼓励，更增加了译者对 MTD 研究领域的信心。同时感谢中国科学院信息工程研究所信息安全国家重点实验室第五研究室领导和课题组老师、同事、研究生给予的帮助。译者水平有限，错漏之处在所难免，恳请批评指正。

更多建议和交流，欢迎莅临 mtdlab.org。

译者

2017 年 7 月于北京西山脚下

Preface 前　言

本书旨在为构建网络空间欺骗防御的科学基础迈出探索性的一步。在本书中，我们提出了一个最新的基础研究结果，收集了来自世界各地的顶尖研究团队关于网络空间欺骗防御的最新研究进展。本书对网络空间抵赖与欺骗防御工作、网络空间欺骗工具和技术、攻击者身份识别与检测、网络空间欺骗操作量化、无线网络欺骗策略、蜜罐部署、人为因素、匿名和溯源问题进行了严谨的分析。此外，我们不仅对网络空间欺骗的不同方面进行抽样检测，同时更突出了可用于研究此类问题的科学技术。

我们真诚地希望，本书可以激发网络安全的研究人员，基于我们现有的知识，进一步构建网络空间欺骗防御的科学基础，从而最终带来一个更加安全、可靠的网络空间环境。

Fairfax, VA, USA　Sushil Jajodia

College Park, MD, USA　V.S. Subrahmanian

McLean, VA, USA　Vipin Swarup

Triangle Park, NC, USA　Cliff Wang

致　谢 *Acknowledgements*

我们诚挚地感谢为本书做出贡献的众多研究者，特别要说的是，能够得到如此多研究者的帮助是我们的荣幸。特别感谢 Springer 的高级编辑 Susan Lagerstrom-Fife 对此项目的鼎力支持。同时还要感谢美国陆军研究办公室所授权的 W911-NF-14-1-0116、W911NF-15-1-0576、W911NF-13-1-0421 项目的资助。

Contents 目　录