国防科技著作精品译丛
网电空间安全系列

The Science of Cybersecurity and a Roadmap to Research

网络电磁安全科学与研究路线图

【美】Benjamin J.Colfer 著　宋小全 熊 军 孙 旭 等译
鲜 明 审校

NOVA
国防工业出版社
National Defense Industry Press

装备科技译著出版基金

网络电磁安全科学与研究路线图

The Science of Cybersecurity and a Roadmap to Research

[美] Benjamin J. Colfer 著
宋小全 熊 军 孙 旭 等译
鲜 明 审校

国防工业出版社
National Defense Industry Press

著作权合同登记　图字: 军 -2012 -060 号

图书在版编目（CIP）数据

网络电磁安全科学与研究路线图 / (美) 科尔弗 (Colfer, B. J.) 著 ; 宋小全等译.
— 北京: 国防工业出版社, 2013.2
（国防科技著作精品译丛. 网电空间安全系列）
书名原文: The Science of Cybersecurity and a Roadmap to Research
ISBN 978-7-118-08569-3

Ⅰ. ①网… Ⅱ. ①科… ②宋… Ⅲ. ①信息—研究 Ⅳ. ①E869

中国版本图书馆 CIP 数据核字（2012）第284624号

网络电磁安全科学与研究路线图
[美] Benjamin J. Colfer 著
宋小全　熊　军　孙　旭　等译　鲜　明　审校

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　北京嘉恒彩色印刷有限公司印刷
开　　本　700 × 1000　1/16
印　　张　14
字　　数　218 千字
版 印 次　2013 年 2 月第 1 版第 1 次印刷
印　　数　1—3000 册
定　　价　65.00 元

(本书如有印装错误，我社负责调换)

国防书店: (010) 88540777　发行邮购: (010) 88540776
发行传真: (010) 88540755　发行业务: (010) 88540717

序言

从我们使用的电话和其他一些日常用品到企业网络，再到社会经济运行依托的信息基础设施，信息技术的影响在社会各个方面已经广泛而深入。

由于美国的重要基础设施越来越依赖于公共和私有的网络，因此这些网络崩溃或失效造成对国家层面大范围影响的潜在可能性也增加了。

保护国家重要基础设施不单单是保护物理系统，更重要的是保护系统运行依赖的网络电磁部分。

为确定国家网络电磁研究与发展计划，以确保我们领先于对手并开发出在未来足以保护我们信息系统和网络的技术，本书仔细考察分析了网络电磁安全研究路线图。

第一篇：在与 DoD 和情报机构相关的所有领域中，保护计算基础设施的需求都日益凸显。由于现代计算系统在很大程度上是互联互通和互相依赖的，利用安全缺陷使其核心功能严重下降的可能性始终存在。虽然在保护网络和计算机资源上耗费了大量的精力，但目前过于依赖经验的方法成功率有限。

第二篇: 美国正处于重要的决策关头, 我们必须不间断地保护当前的系统和网络, 同时努力摆脱面前的对手, 确保下一代技术能使我们在保护关键基础设施和回应对手的攻击中处于有利地位。术语“系统”(system)广泛地用于表示系统和网络。

译者序

网络电磁空间 (以下简称网电空间) 安全研究已得到世界各国的高度重视, 美国无疑是这方面的先行者和带头人。美国政府在加强先进信息技术研究的同时, 将网电安全问题提升到一个前所未有的高度来认真对待, 其研究成果对未来全球范围内的网电理论研究具有重要影响, 吸收借鉴国外相关领域的先进理念和方法, 对推动促进我国在该领域的能力发展具有重要意义。

本书共包括两部分, 第一篇是 JASON 咨询组应美国 DoD 要求撰写的研究报告《网络电磁安全科学》, 第二篇是美国土安全部发布的《网络电磁安全研究路线图》。第一篇从理论、实验、实践等多个角度分析了网电安全作为一门科学面临的基本问题, 并重点分析了模型检测、形式化方法以及免疫学在本领域的可能应用前景, 最后对如何推动网电安全科学的发展提出了建议。第二篇主要围绕所提出的 11 个网电安全领域的难题 (如可扩展可信系统、企业级安全度量等) 展开, 以提问的形式, 从背景需求、研究现状、差距、目标、测试评估等多个角度对这些问题进行了深入探讨, 提出未来研究建议和近期、中期、长远研究路线。与国外同类书籍相比, 本书内容涉猎广泛、论证严谨、权威性高、针对性强, 能够代表美国政府和学术界当前针对网电安全领域的最前沿观点和看法, 是我国相关决策规划

人员和科研技术人员了解网电安全研究现状和发展方向极具参考价值的文献。

本书第一篇的摘要和第 1 章 ~ 第 4 章由宋小全译, 第 5 章 ~ 第 6 章由冷家旭译, 宋小全对第一篇进行了初统和初校; 本书第二篇的概要简介、第 1 章 ~ 第 3 章和附录由熊军译, 第 4 章 ~ 第 7 章由孙旭译, 第 8 章 ~ 第 9 章由刘浩然译, 第 10 章 ~ 第 11 章由董平译, 熊军对第二篇进行了初统和初校; 宋小全对全书进行了统稿和校对, 最后由鲜明对全书进行逐字逐句的审译、修改。本书翻译过程中, 得到了国防工业出版社崔晓莉编辑的大力帮助和指导, 在此顺致谢忱。

我们在翻译中尽量尊重原著的风格, 矢志译得准确、严谨、流畅, 为方便读者理解还对部分特定缩略语进行了展开解释。但毕竟因水平有限, 错误和欠妥之处在所难免, 恳请读者批评指正。

译 者

2012 年 12 月

国防科技著作精品译丛 · 网电空间安全系列

国防工业出版社已出版或即将出版的国防科技著作精品译丛 · 网电空间安全系列, 请关注:

《网络电磁安全科学研究路线图》

《信息战》

《电子战》

《网电空间安全：公共部门的威胁与响应》

《网电战争 —— 安全从业者的技术、战术与工具》

《网电力量和国家安全》

《网电空间态势感知问题与研究》

《网电战基础: 在理论和实践中认识网电战基本原则》

《工业网络安全 —— 智能电网, SCADA 和其他工业控制系统等关键基础设施的网络安全》

目录

第一篇　网络电磁安全科学

第 1 章　概要 2

第 2 章　问题陈述和介绍 6

第 3 章　网络电磁安全科学概述 8

3.1　网络电磁安全属性 9

3.2　其他科学的指导 9

3.2.1　经济学 10

3.2.2　气象学 10

3.2.3　医学 10

3.2.4　天文学 11

3.2.5　农学 11

3.3　安全随时间降级 11

3.3.1　UNIX 密码 11

3.3.2　撞匙 12

3.4　保密的角色 12

3.5　网络电磁安全科学的面貌 13

3.6 相关科学 14
3.6.1 信任 14
3.6.2 密码学 14
3.6.3 博弈论 14
3.6.4 模型检验 16
3.6.5 模糊处理 16
3.6.6 机器学习 16
3.6.7 组件合成 17
3.7 科学成果的应用 17
3.8 度量 18
3.9 新技术带来的机会 19
3.10 实验和数据 20

第 4 章 模型检测 22

4.1 Spin 与 Promela 简介 22
4.2 安全领域应用 26
4.2.1 Needham-Schroeder 协议 26
4.2.2 协议的 Promela 模型 28
4.3 尺度问题 34
4.4 代码提取模型 37
4.5 与 hyper-properties 的关系 38

第 5 章 免疫系统模拟 40

5.1 生物学基础 40
5.2 从类推中学习 42
5.2.1 对于自适应响应的需求 42
5.2.2 感知形态的混合 43
5.2.3 可控实验的需求 44
5.2.4 时间尺度上的区别 45
5.2.5 对于检测的响应 45
5.2.6 最终观点 46

第 6 章 结论与建议 47
参考文献 49

第二篇 网络电磁安全研究路线图

当前信息安全研究中的困难问题

第 1 章 可扩展的可信系统 60
1.1 背景 60
1.2 未来发展方向 65

第 2 章 企业级衡量指标 (ELM) 75
2.1 背景 75
2.2 未来方向 81

第 3 章 系统评估生命周期 87
3.1 背景 87
3.2 未来发展方向 90

第 4 章 应对内部威胁 97
4.1 背景 97
4.2 未来方向 100

第 5 章 应对恶意代码和僵尸网络 108
5.1 背景 108
5.2 未来方向 115

第 6 章 全球范围身份管理 122
6.1 背景 122
6.2 未来的方向 126

第 7 章 时间关键系统的生存能力 131
7.1 背景 131

7.2 未来的方向 · · · · · 134

第 8 章 态势感知和攻击归因 · · · · · 140

8.1 背景 · · · · · 140

8.2 未来方向 · · · · · 146

第 9 章 溯源 · · · · · 154

9.1 背景 · · · · · 154

9.2 未来方向 · · · · · 157

第 10 章 隐私安全 · · · · · 162

10.1 背景 · · · · · 162

10.2 未来方向 · · · · · 167

第 11 章 可用的安全 · · · · · 172

11.1 背景 · · · · · 172

11.2 未来方向 · · · · · 178

附录 A 各主题间的相互关联 · · · · · 184

附录 B 技术转化 · · · · · 194

B.1 介绍 · · · · · 194

B.2 技术转化的基本问题 · · · · · 196

B.3 各主题特定相关问题 · · · · · 197

B.4 强制性功能 (一些说明案例) · · · · · 198

附录 C 参与路线图制定的人员列表 · · · · · 201

附录 D 缩略语 · · · · · 203

参考文献 · · · · · 206

第一篇　网络电磁安全科学

JASON

The MITRE Corporation

摘　要

JASON 应 DoD 之邀考察网络电磁安全的理论和实践, 评估是否存在潜在的基本原理从而使采用更科学的方法成为可能, 同时确定创建网络电磁安全科学的需求, 并推荐科学方法应用的特殊途径。我们的研究明确了一些与之特别相关的计算机科学的子领域, 也提出了一些进一步发展网络电磁安全科学的建议。

第 1 章

概要

保护计算基础设施在与 DoD 和情报部门有关的所有领域中都已变得意义重大。由于现代计算系统的相互连接和相互依赖的程度, 存在着利用安全漏洞使系统核心功能严重降级的可能性。

JASON 应 DoD 之邀研究网络电磁安全的理论和实践, 评估是否存在潜在的基本原理从而使采用更科学方法成为可能, 确定创建网络电磁安全科学的需求, 并推荐科学方法应用的特殊途径。我们的研究明确了一些与之特别相关的计算机科学的子领域, 也提供了一些进一步发展网络电磁安全科学的建议。

定义一门网络电磁安全科学的挑战源于这一领域的独特之处。网络电磁安全的 “世界” 是一个人造的环境, 与真实物理世界仅仅存在微弱的关联。所以无论攻击方还是防御方, 几乎不存在先天的约束。最重要的是, 与网络电磁安全相关的威胁是动态变化的, 其中, 对手的性质和议程在不断的变化, 遭遇的攻击样式随时间在不断演化, 部分是为了应对防御行动而作出的改变。因此, 没有一个科学领域能覆盖网络电磁安全所有突出的问题。然而, 它仍存在和其他一些研究领域相似的地方。网络电磁安全需要理解计算机科学领域的概念, 同样也要借鉴诸如流行病学、经济学和临床医学等的观念; 这些类比将有助于确定研究的方向。

我们的研究确定了几个与之有明确关联的计算机科学的子领域。这些子领域包括模型检验、密码学、随机论、类型论等。在模型检验中, 人们提出算法的详细描述, 然后尝试验证在特定假设下该描述的不同推论的正确性。模型检验为考察安全问题提供了一种有益的和严格的理论框架。密码学, 研究存在敌对方且敌对方的假定功率必须明确规定的通信, 今天已被

看作一个严谨的研究领域, 而且其研究方法可以为未来的网络电磁安全科学提供有益的经验。类型论则是任一种能够替代朴素集合论的形式系统, 在程序安全性推理方面也是有效的。模糊处理是一种用来伪装或打乱程序的数据路径和变量的方法, 可以帮助人们抵御某些常见的攻击模式。最后, 博弈论的思想可以帮助我们确定网络电磁防御行动的优先次序。在所有时间里保护所有的东西是不可能的, 所以必须建立关于风险的概念, 博弈论方法提供了一种推理框架。

显然, 人们希望提出计算机系统安全等级的度量方法, 但需要理解并意识到这些方法的局限性。当然可以通过记录各种现有的攻击策略来确保系统不受这些攻击的影响, 但这是一种保守的方式。对文件和关键程序的变化检测固然对识别异常有所帮助, 但将这些异常与实际的攻击关联起来还需要进行更深入的研究, 可以利用源自机器学习和事件处理等科学领域的思想。

JASON 意识到需要加快将研究成果转化为易为开发者使用的工具。有一些非常先进的方法 (如前述的模型检验、类型检测等) 能用来评估和分析现有系统的安全性能, 但目前它们还不能以开发工具的形式得到广泛的应用。对这类工具的私人开发商来说, 这个市场可能不够大, 这就需要 DoD 更加积极的支持未来的开发。

DoD 提出了一些问题作为研究的部分内容。下面我们列出了这些问题和我们的答案。

(1) *哪些科学理论、实验和 (或) 实践方法的基本原理是网络电磁安全研究团体为取得重大进展而必须采纳的? 研究团体是怎样从这些基本原理中获益的? 是否存在必须采纳的网络电磁安全科学的哲学基础?*

最重要的是构建公共语言和一整套基本概念, 据此, 研究团体可以共享理解和认识。虽然网络电磁安全是存在着对手的科学, 这些对象将随时变化, 但共同语言和协商一致的试验性协议将有助于假设的测试和概念的确认。如果出现了关于研究进展的一致意见和关于未来更有希望的研究方向, 研究团体将从中受益。同时, 必须与现实世界中的实践保持联系 (类似在医学领域从动物模型测试到可能的临床试验的一种进展)。

(2) *网络电磁空间是否存在可以形成科学研究的基础的 "自然法则"? 是否需要考虑数学抽象或理论模型?*

网络电磁安全不存在类似物理、化学和生物学中固有的 "自然法则", 本质上是一种应用科学, 由自动控制论、复杂性理论和数理逻辑等计算机科学的数学模型构成。

(3) 是否存在一种度量标准体系可用来测量一个系统、一个网络、一个任务的网络电磁安全状态并得到可重复的结果？测量理论或实践是否有助于提高我们量化网络电磁安全的能力？

多种度量标准可以有效地应用，例如现代入侵检测系统等。但必须意识到这些度量标准是基于经验和统计得出的，无法应用在没有详细规定的场景中，特别地，无法度量那些还没有观察到的事情，例如新的攻击方式。不可能对信息系统的一般行为进行安全等级非常确定的度量。度量结果的可重复性取决于是否严格遵守协议标准和判决准则。而目前，可重复性不是公布网络电磁安全结果需要考虑的首要标准。

(4) 网络电磁安全研究的科学基础是什么？传统的实验和理论研究方法在网络电磁安全上是否仍有效？是否存在解析和方法论的方法？这些方法是什么？

值得肯定的是，传统的实验研究和理论研究都适用于网络电磁安全领域。最首要的是建立起研究的协议从而可以开展可重复的实验，这些协议需要提供初始条件的清晰描述、许可的威胁种类和安全目标的确切含义。

(5) 传统科学理论和方法，例如复杂性理论、物理、动力系统理论、网络拓扑学、形式方法、数学、社会科学等，能否对网络电磁安全科学有所贡献？

传统的部分计算机科学领域在过去对于深入理解网络电磁安全起到了作用，未来仍将得到更多的重视。当创建了一个给定的系统或关键内核的安全模型，然后利用一系列精确定义的可能输入来测试各种假设时，模型检验显得特别有用。当输入空间无限时，则可以对某特定的威胁建模。密码学通过关注假设来确保保密通信是可行的。编码模糊处理技术和类型理论的应用也使我们可以更深刻地认识安全代码的构建。最后，博弈论将在安全评估方面扮演着重要角色。对 DoD 来说，保密在网络电磁防御中也是有价值的重要措施，例如，利用模糊处理技术，开发 DoD 专用安全产品，搜集和保护未公开的网络电磁攻击的数据等。

(6) 建模和仿真方法如何在网络电磁安全科学中发挥作用？

建模和仿真在很多方面都能发挥作用。一方面是利用现有的计算能力在运行的系统上持续地进行安全测试；另一方面是利用虚拟机等概念提供精确定义的试验床，以一种受控的方式来检测计算和安全系统在受到明确定义的攻击时的行为反应。

(7) 在小的、封闭的和受控的环境下，可重复的网络电磁实验是可能的，但这能否扩大到整个互联网上并得到可重复的结果呢？或扩大到可支

持 DoD 和 IC 的互联网的子网上呢?

因为对以前的小规模实验的结果没有系统性梳理,提这个问题有点为时过早。以前的大部分工作不是为着可重复性的目标开展的,重要的是首先评估这些较小规模的试验床的效用,而不是先去考虑如何扩大可控的网络规模甚至扩大到整个互联网。

(8) 为形成网络电磁安全科学领域,需要哪些步骤来发展和培育其中的科学探究?建立网络电磁安全科学研究团体又需要什么?

成立联系学术界、工业界、国家实验室和 DoD 的跨学科中心应该是重要的一步。这些中心应将研究重点聚焦到网络电磁安全问题上,特别是与 DoD 需求相关的问题上,但也将影响其他发挥重要作用的机构的行动,如 DARPA、NSA 在信息安全保障方面的努力。在所有此类机构中,为团体建立起评审过的标准协议是很重要的,这有利于团体的交流沟通和研究结果的存档。

(9) 是否有理由相信上述目标基本上是无法实现的?如果是,为什么?

每一条理由都使人相信朝着上述目标的努力能取得重大的进展。人们首先必须理解从事网络电磁安全的科研企业的性质,描述清楚研讨对象的特性。只要提出公认的论述方法,大量有价值的科学研究都能实现。考虑到网络电磁安全具有技术和社会两方面因素,即使技术活动自身不能“解决”网络电磁安全问题,它们也将起到巨大的促进作用。