安全技术经典译丛

The Craft of System Security

系统安全工艺

(美) Sean Smith
John Marchesini 著

黄清元 李化 译

- 权威专家旁征博引，深入剖析安全体系的竭诚之作
- 最新的系统安全及其薄弱点的详细说明；为全面认识安全体系，拥有解决问题的敏锐思维铺路搭桥
- 内容涉猎广泛，叙述客观、生动，见解独到

PEARSON Education

PEARSON Addison Wesley

清华大学出版社

安全技术经典译丛

The Craft of System Security

系统安全工艺

(美) Sean Smith
John Marchesini 著

黄清元 李化 译

清华大学出版社

北 京

北京市版权局著作权合同登记号　图字：01-2009-0838

图书在版编目(CIP)数据

系统安全工艺/(美)史密斯(Smith，S.)，(美) 马舍西尼 (Marchesini，J.) 著；黄清元，李化 译.
—北京：清华大学出版社，2009.4
(安全技术经典译丛)

书名原文：The Craft of System Security

ISBN 978-7-302-19472-9

Ⅰ.系… Ⅱ.①史…②马…③黄…④李… Ⅲ. 安全工程 Ⅳ.X93

中国版本图书馆 CIP 数据核字(2009)第 016296 号

责任编辑：王　军　王　婷
封面设计：久久度文化
版式设计：孔祥丰
责任校对：成凤进
责任印制：杨　艳

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：24.75　**字　数**：602 千字
版　　次：2009 年 4 月第 1 版　　**印　　次**：2009 年 4 月第1 次印刷
印　　数：1～4000
定　　价：49.80 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：028208-01

译 者 序

设计安全系统是非常困难的，有很多要考虑的因素：

- 工艺师必须考虑整个系统，包括很多不同层次的硬件和软件技术、用户接口设计、制造、销售、维护，以及法律、标准、社会实践、心理学(很可能还有其他我们忽略的事情)。
- 系统组件和应用日新月异，你走过30年前造的桥吗？(当然！)但是你会否信任30年前设计的密码系统？你会把一个10个月前才打过补丁的PC挂在Internet上吗？
- 造桥中所使用的科学与工程很好理解，与此相比，“安全性”仍然是一个需要继续研究的领域。安全系统的含义是什么？如何评估系统的安全性？如何达到系统安全？

系统安全非常复杂，到处都是折衷。但是，很少有方法能够告诉开发人员是否确实达到了目标。不幸的是，当前的技术并没有给予系统开发机构任何定义明确且可接受的有效方法。研究人员不得不依赖于自身的判断、创新性和经验，当然，也要依赖工具。正是这一原因使我们认为，安全系统开发如同艺术和工程守则一样，仍然是一个工艺问题。

希望本书有助于增强你在该领域的判断、创新性和兴趣。我们有意提供了详尽的参考文献引用，以便于读者能够知晓更多前人的研究工作。尽管阅读不能完全替代自身的经验，但是，我们期望它能够帮助你避免重蹈覆辙，尽可能消除系统常见的缺陷。最后，希望读者朋友们已经发现了一些工具来协助工作，我们鼓励读者持续关注这类工具，即使这些工具可能来自于比较奇特的领域，如自动形式化方法、AI、人/设备交互等领域。

最后，我们希望本书能够让你始终有一种怀疑的态度，这对于成功开发安全系统是必要的。如果你不能很好地了解你的敌手，那么开发安全系统将是一件非常困难的工作。参考文献中有各种实例，人们对这些实例进行了深入剖析，提出了一些准则，也有可能形成了一些错误的观点。很多时候，这些实践产生了比较有趣的结果，我们鼓励读者从不同的角度来思考你使用和开发的系统，要不断地问自己：“我想知道如果...，将会发生什么”。

未来社会依赖系统安全。我们需要熟练的安全设计师来保证系统安全，未来属于你们。

前　言

“我认为这本《系统安全工艺》是当今市面上最棒的软件安全书籍之一。其内容广而深、覆盖的内容有密码学、网络构建、操作系统、Web、人机交互、以及如何通过改进硬件来提高软件系统安全性。简而言之，本书适合所有系统安全从业者，并且也可以选作大学计算机科学课程的教材。”

——Edward Bonver ，CISSP(信息系统安全认证专业人员)、Symantec 公司产品安全的资深 QA 工程师

“这将会是一次有趣的、令人兴奋的阅读：该书囊括了各种有关计算机安全应用和误用的实例，是一本独特而新颖的书籍。我期望本书能够激发广大学生朋友投身到安全技术领域中来；同时，该书还能够满足安全专家们的需要。”

——L.Felipe Perrone，Bucknell 大学计算机科学系教授

过去，仅有专家对计算机安全感兴趣，但是，现在它已经成为社会中每个人都需要关注的内容。生活中经常需要计算，一旦计算机遭到破坏将会引发非常严重的后果。但试图掌控计算中的全部细节问题几乎是不可能的，参与计算的多个方面都存在复杂性问题，如独立构件和计算硬件、操作系统、应用程序、网络协议，以及使用这些系统的人为因素等。

安全是每个人都应关注的问题，一个非常直接的问题是如何让每个参与者都明白安全方面的知识和安全的重要性。从软件工程师、经理、律师，以及任何其他人的职业生涯可以看出，研究者和从业者不仅需要关注安全涉及的广度，还需要关注其深度，如安全的发展趋势和准则等。

现在，安全研究文献过多关注于系统管理、密码学体制、桔皮书或者 NSA 标准，计算机科学研究人员和计算机安全从业人员能够轻易地发现详细描述某些特定工具的书籍，这些工具可以用来对系统安全性进行评估，但是，这些书籍并没有向读者阐述更为本质的问题：人们为什么要开发这些工具？如何和何时使用恰当的工具来解决特定的问题。此外，现有文献也无法辅助人们开发出安全的系统，很多工具能够有效地辅助系统审计员进行审计，但对于安全系统开发人员则没有帮助。

本书弥补了现有文献的不足。描述了现代安全开发人员所需的工具，解释了人们为什么要开发这些工具，并阐述如何使用这些工具来解决实际问题。我们希望本书能够给予研究人员足够的实践知识，同时能够使开发人员对这些问题的本质有深入的了解。这些工具对于了解系统安全设计是很必要的。

如何得到安全方面的知识？人们可以通过阅读大量书本或者电子书籍来获取足够的知识，但是很多人没有这样的时间。此外，那些资料往往重点阐述的是当前的系统细节问题，有很强的时效性，当读者阅读完之后，这些资料很可能已经过时。

本书来源于 Sean Smith 在系统安全方面所开设的一个大学课程(John Marchesini 协助完成了教学)：为那些仅修过一门安全课程，并开始专业职业生涯的学生提供正确的安全教育。我们希望本书能够有助于这些学生深入了解应对当前和未来安全挑战所必需的知识，本书通篇都描述了安全开发人员的相关经验，并阐述了我们总结的一些教训。

在 Web 刚出现的时候，本书的一个作者曾在政府安全实验室工作，那时，一些思维比较超前的政府部门开始考虑使用 Web 这种新的媒介来向广大人群发布服务。该经历为我们提供了后续所述的一些重要教训。计算技术保持爆炸性发展，影响着每一个人，包括计算机科学家。若将 1994 年的家庭或者办公计算环境以及 Web 技术与今天的这些技术进行比较，就会发现计算机的飞速发展。但是，我们需要从系统的社会影响来看待安全问题。在开发、部署、操作、管理，或者使用这些影响社会的系统时，就必须考虑其中的安全问题。

另外，本书的另外一位作者则从事安全软件产业，将安全产品销售给银行、航空、政府部门。他的这一经历使我们明白提供商为什么要周期性地为软件打上安全补丁。软件提供商需要尽可能快地发布具有新特性的产品，在开发周期的每个阶段，安全性都与这一目标冲突，需求分析阶段倾向于关注新的特性(由此带来复杂性问题)，而不是健壮性；设计阶段通常关注于良好的界面和重用性，而不是耐用性；实现阶段通常关注速度，而非可靠性；质量保障阶段一般关注功能测试，而非穿透测试。由此产生的结果是，提供商所销售的产品既不健壮、耐用，也不安全可靠，更没有测试软件是否能够有效抵御恶意用户的攻击。BugTraq[Sec06][1] 的主要目标就是关注这些产品所存在的问题。如果人们希望能够开发出打破这种模式的系统，那么就需要对这些类型的问题有深入的了解。

安全博弈的这种动态特性使其表现出了与其他类型工程(如修桥和制造保险箱)不同的特点。人们在修桥时，会计算需要承受的力量，购买合适的材料，然后根据规范来修桥。而在安全开发中，模块老化的速度比较快，有时候超过预期，有时候则是非常快。正是这一事实要求我们在开发安全产品时，应持续保持警惕，抓住其中的本质。这也是我们写这本书的原因。

本书的组织结构

本书第 I 部分介绍了计算机安全的历史背景；第 II 部分介绍了现代计算技术的基本情况；第III部分描述系统安全防护的基本构成模块；第IV部分讲述如何使用系统安全防护模块来构建安全的现代计算应用环境；第 V 部分描述了改变未来系统安全的新工具和新趋势。

[1] [Sec06]为参考文献标记，详见本书最后“参考文献”中[Sec06]里的内容。

第 I 部分：历史背景

第 I 部分介绍系统安全的发展历史。今天，计算机已经渗透到人类生活的方方面面。然而，就在 10 年前，将计算技术从实验室引入到真实世界的过程才刚刚开始。军事和国防是最早应用计算技术的领域，也是发展计算技术的资金来源。这些领域传统上将敌方的行为提取为侦察、破坏以及战争行动，这种认识被带入到计算环境中，引起了人们对计算机安全新问题的很多思考。有些人将这些认识奉为圣经，不容挑战和扩充；有些人则完全忽略这些问题。我们认为折衷考虑是最好的选择。

安全概述 本章的介绍是展开深入讨论的基础。第 1 章首先讨论了两个术语——“安全(security)”和“系统(system)”的含义，“系统”的标准含义是指提供简单信息应用的计算机，“安全”应该包括几个方面：保密性 (confidentiality)、完整性(integrity)和可用性(availability)。我们也将探讨基本的访问控制/保护(主体、域、客体)和描述谁在什么时候能对哪些对象执行什么操作的访问控制矩阵，然后讨论了访问控制矩阵的理论基础和实际意义。

旧约 一部分安全团体认为，计算机安全问题在几十年前就已经解决，主要依据是美国国防部发起的一项被称之为桔皮书(DoD85)的项目。当 Roger Schell 在 2001 年 10 月对这一观点表示赞成时，一些激进的观众称他为“旧约预言者耶利米”，建议严惩那些将人们的认识带入歧途的团体。不论赞同与否，我们都需要了解 Schell 的观点，本书第 2 章讨论了 Schell 的观点。

旧准则，新环境 第 3 章将探讨第 1 章和第 2 章的观点和认识是如何应用到现代计算环境中的，以及曾失败的地方。我们看到，如果不小心使用“保密性-完整性-可用性”这一三段论，系统安全所需的重要方面将无法得到保证，我们使用“正确性”这一词语作为替代来刻画安全防护行为。本章还将探讨建立系统安全边界的困难。本章将批评桔皮书的观点，尽管其中的有些观点仍然是正确的。最后将回顾其他系统的设计准则，以及它们如何继续应用到新的计算环境中。

第 II 部分：安全与现代计算场景

在了解计算机安全的发展史后，我们将探讨传统安全认识对当前的影响。第 II 部分主要讲述开发应用中需要关注的安全要素。

操作系统安全 操作系统为用户提供了利用计算机操作其他信息的接口。因此，操作系统是用户抵御内部和外部攻击的第一道防线，它定义和限定了用户的操作行为。第 4 章描述了操作系统安全防护的基本结构和工具，介绍了安全的基本准则并探讨了其在 Windows 和 UNIX 系统(包括 OS X、Linux、BSD 和 Sloaris)中的应用。

网络安全 当计算机互联时，安全需求将会有所不同。第 5 章介绍了互联的基本要素，以及安全管理员需要关注的一些主要领域。同时还探讨了新的无线组网技术——在 4 年前还非常少见的无线技术，该技术已经成为新笔记本的标准配置。对于旅馆、工业园区以及大学来说，不提供无线联网技术就如同不提供电力一样落后。然而，新的技术也带来新的风险：正如我们已经认识到的一样，在有线网络中可以保证安全的应用，在无线网络环境中其安全性却无法得到保证；人们通过搜索和访问通信范围内配有蓝牙的设备可以改变会议令人厌烦的情况，但这可能会无意间导致自己暴露在开放的外部环境中。

安全实现 计算最终由运行在真实机器上的真实代码完成，逻辑安全模型在真实实现时，不可避免的与预期存在差异。长期以来，计算机安全问题的一个重要来源就是系统实现时的缺

陷。第 6 章中综述了系统实现时的缺陷，包括一些常见的错误，如缓冲区溢出、缺乏反向验证、转义字符、检查时间/使用时间以及一些更为细节的问题，如开发过程、工具链问题和硬件问题。我们给出了上述问题的真实示例和一般原理，并探讨了安全编码以及其他应对措施。本章还探讨了编程语言技术和软件开发过程是如何影响安全的以及我们应当怎么做。

第III部分：安全系统的构成模块

第III部分综述了设计、开发、部署安全系统中需要关注的基本构成模块。

密码学 密码体制是当前安全系统的基本构成模块。计算机专业人员需要对这些内容有很好的理解，并能够在大型应用中使用这些工具。第 7 章介绍了标准密码学元素(公钥、对称分组密钥等)以及使用这些元素的标准方法(如 hash 函数、填充算法、混合密码学、消息鉴别码等)。我们在授课中遇到很多学生“知道 RSA”，但并不知道如何进行数字签名。

密码学破解 人们喜欢处理简单的抽象模型，但是，在真实系统中实现密码学原语时，在具体细节中通常会潜伏一些危险的问题。从抽象层次来看，这些系统没什么问题。但是，潜在危险则会破坏整个系统的实际安全性。在实现过程中，计算机专业人员需要对这些密码学原语中存在的问题有深入了解。第 8 章介绍了这方面的问题，并列举了一些案例以有助于读者提高这方面的认识。

身份认证 当系统为多个人服务时，讨论“安全系统”才有意义。第 9 章讨论了身份鉴别的基本原理以及在各种环境中鉴别人和系统的相关技术：直接机器访问，通过非信任网络或者通过非信任网络的非信任客户端。第 9 章还阐述了身份鉴别和授权之间的区别。

公钥基础设施 公钥基础设施(Public Key Infrastructure，PKI)提供了一种在通信实体之间跨空间、时间、机构建立可信通信的机制。但是，实现公钥机制的基础设施仍然有很多需要解决的问题，一些反对者甚至认为该方法天生不足。第 10 章讨论了公钥基础设施的问题空间、主要方法、使公钥基础设施部署和过程复杂化的相关问题以及反对者的观点。

标准、实施和测试 人们为什么要相信某个系统是安全的？不论对于提供商，还是对于开发者、管理者、客户来说，该问题都是一个基本问题。第 11 章讨论了穿透测试、验证和标准，阐述了这些方法如何辅助人们实现安全性和保密性，以及这些方法的不足是什么。本章中，我们阐述了自己在测试和验证中的一些经验，同时为读者提供了一些建议。

第IV部分：应用

前面章节讨论了历史和构成模块，第IV部分讨论如何将这些准则和工具应用到当前的计算环境中。

Web 及其安全 Web 技术是由一些不想去图书馆的物理学家创造的，当前它已经成为社会电子服务的核心媒介。我们讨论了 Web 的工作原理，并阐述了影响其安全性和隐私的各种威胁以及主要的解决方法。第 12 章讨论了标准方法(如 SSL 和 cookie)和一些更为复杂的方法。

我们也讨论了一些案例，在这些案例中，机构往往会无意间通过基于 Web 的服务泄露信息。例如，如果编辑阅读了本章的内容，那么他们就不会谴责某些私立学校的申请者通过攻击 ApplyYourself 网站来提前得到录取消息；如果受怀疑的学校阅读到本章，那么他们就会谴责那些许可该站点的 IT 组织，而不是草率地拒绝那些申请者。

办公工具及其安全 生产性工具，如 Microsoft 办公套件、Lotus 1-2-3 以及丰富的图形化 HTML 邮件等，几乎在所有环境中都是标准组件。但是，这些工具的丰富性和复杂性不断引发

安全和隐私问题。这些工具主要用于处理电子对象，这些电子对象与纸质对象看起来很相似，而且工具还提供了与纸质对象类型的操作，用户很容易将电子对象与纸质对象同等相看，并基于这种假设来进行信任决策。但是，这种假设是不正确的，由此产生的信任决策也通常是不正确的。第 13 章对这些问题进行了探讨。

货币、时间、属性　虚拟对象并不是实体，社会系统的运行依赖于实体的属性，而我们对实体的理解已有上千年的历史。第 14 章讨论了一些问题和工具，以使虚拟位串具有与纸质货币和文档相似的属性。我们开发了很多针对传统媒介(如书籍、杂志、唱片)的技术，能够很轻易地对这些对象进行知识产权保护，而针对虚拟位串的知识产权保护技术则还不成熟，这也是虚拟位串与纸质实体之间的重要差异之一，电子位并不具备实体的自然属性，而数字版权管理(Digital Right Management，DRM)及相关领域的研究(这些研究包括水印、信息隐藏、策略表达等)主要就是为了设计和开发出一些安全系统，以抵制某些类型恶意行为，能够强制系统保持在某种，“好的”状态。

第Ⅴ部分：新工具

本书不仅关注当前安全领域的知识，也向读者介绍了一些未来的安全技术。第Ⅴ部分介绍了有望在未来扮演重要角色的计算机安全技术和工具，因此，该部分的某些章节与前面的章节相比，有些“单薄”。第 15 章和第 17 章就其本身而言，都是正在发展的研究领域，但是，经常不为安全设计人员所关注，第 18 章则介绍了最近才出现的研究领域。

形式化方法和安全　保证当代计算系统和应用程序安全的一个主要挑战是控制它们不断增长的复杂度。如果系统过于复杂以致难以理解，那么如何确信该系统确实能够安全地运行？

形式化方法能够有效地应对这类安全问题(如[CW96，Win98])。Holzmann 的 SPIN 甚至在 2002 年获得了 ACM 系统奖。计算机专业人员应当意识到，如果能够形式化描述系统的功能，并能够描述某状态如何保持“安全性”及这些属性的含义，那么，就存在一种半自动的方法来验证该系统是否具备这些属性。第 15 章讨论了这些工具。

基于硬件的安全　针对计算机安全的研究通常关注计算过程。但是，由于计算最终需要硬件支持。因此，硬件的结构和行为将从根本上影响硬件上保存的计算过程的属性。一部分计算机安全研究机构已经开始提倡并探讨了基于硬件的安全技术。最近，电子商务的出现为密码操作加速器的发展提供了市场，而企业级身份鉴别则为用户硬件令牌开辟了市场，并且计算产业界也在不断推动 TCPA/TCG 硬件的发展，从这些事实都可以看出，这类技术的可行性不断提高。第 16 章阐述了当前高级计算中设计、使用、评估基于硬件的安全技术所取得的成就。

搜索有害位　人工智能在学习和识别方面为安全技术提供了一些非常有用的工具(例如，由此产生了 Los Alamos——一个获益的研究项目)。第 17 章介绍了这些工具，并阐述了这些工具如何识别已知的有害模式和未知模式，也讨论了这些工具在系统和网络入侵以及高级应用数据中的作用。

人为因素　在很大程度上来说，计算系统的安全之所以重要，是因为人们使用这些系统来处理一些对人来讲非常重要的事情。人机交互(Human/Computer Interaction，HCI)主要研究人如何与设备进行交互：指导这一交互的原则，以及不良设计如何产生非预期的结果甚至大的灾难。第 18 章介绍了人机交互安全(HCI-Security，HCISEC)领域的研究及基本的设计原则(在 Norman 所著 *The Design of Everyday Things*[Nor02]有详细阐述)，同时也讨论了该原则在计算安全中的重要性。该领域逐渐受到安全研究人员的关注(如[AS99，BDSG04，Gar5，Smi03c，Yee04])。

结束语

最后总结了上述内容，本书的附录给出了一些来自理论计算科学的相关背景知识，以便于读者能够更好地理解本书的内容。参考文献则详细列举了本书所引用的相关参考文献，也列举了一些前沿研究的内容，不过由于受篇幅所限，更多前沿研究没有在本书中列出。尽管我们已经尽最大努力，但错误不可避免。请将您的反馈意见发送至 wkservice@vip.163.com，我们将不胜感激。

目　录

第 I 部分

历史背景