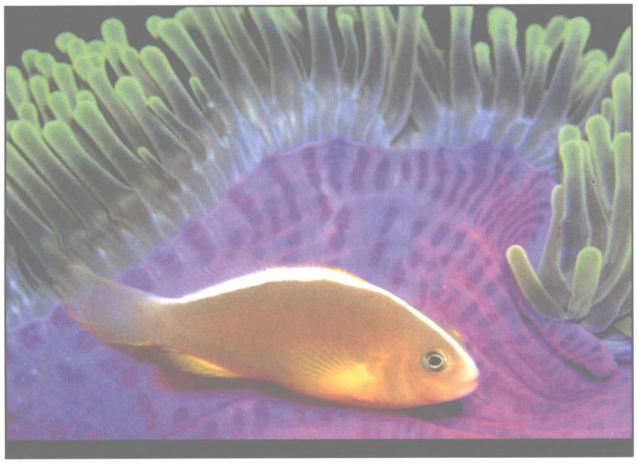
WILEY symbian

移动终端软件开发系列丛书

symbian OS平台安全

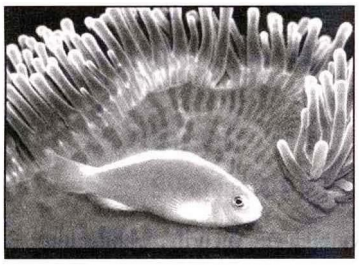
——用Symbian OS安全架构进行软件开发



〔英〕Craig Heath 等 著
张文波 译

人民邮电出版社
POSTS & TELECOM PRESS

移动终端软件开发系列丛书



symbian OS平台安全

——用Symbian OS安全架构进行软件开发

〔英〕Craig Heath 等 著
张文波 译

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Symbian OS平台安全：用Symbian OS安全架构进行软件开发 /（英）希思（Heath, C.）等著；张文波译. —北京：人民邮电出版社，2009.4
（移动终端软件开发系列丛书）
ISBN 978-7-115-19603-3

Ⅰ. S… Ⅱ. ①希…②张… Ⅲ. 移动通信－携带电话机－应用程序－程序设计 Ⅳ. TN929.53

中国版本图书馆CIP数据核字（2008）第213447号

版 权 声 明

移动终端软件开发系列丛书

Symbian OS 平台安全——用 Symbian OS 安全架构进行软件开发

◆ 著 [英] Craig Heath 等
译 张文波
责任编辑 王建军
执行编辑 戴如梅

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鸿佳印刷厂印刷

◆ 开本：787×1092 1/16
印张：12 2009 年 4 月第 1 版
字数：261 千字 2009 年 4 月北京第 1 次印刷

著作权合同登记号 图字：01-2008-5732 号
ISBN 978-7-115-19603-3/TN

定价：36.00 元

读者服务热线：(010)67119329 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内 容 提 要

本书描述了移动设备上平台安全的背景和需要，介绍了支撑 Symbian OS 安全架构的概念，如“信任”、“能力”和“数据锁定”等核心原则；介绍了如何在安全平台上开发应用程序；阐明了作为平台安全行业“网守”的应用程序证书和签名的概念。对于那些希望为基于 Symbian OS v9 的畅销手机开发或移植应用程序的人们来说，所有这些信息都至关重要。

本书对于涉及 Symbian OS 的各级开发人员——从设备制造商，到商用 Symbian OS 手机应用程序的开发者，再到参与手机采购或基于 Symbian OS 手机的移动网络服务设计的安全专家，都很有用。

——献给我的母亲Iris Heath，她于2005年12月30日平静地去世，享年89岁。

关 于 本 书

Symbian Press 很高兴为您带来这本记录了 Symbian 平台安全项目工作成果的书。该项目已经进展多年，现在我们终于有机会来公开展示 Symbian OS 安全架构的增强特性。

本书描述了平台安全的原理及实现，它记录了 Symbian 为保护手机的完整性和敏感数据、控制对敏感操作的访问而实现的各种机制。

本书描述了移动设备上平台安全的背景和需要，对支撑 Symbian OS 安全架构的概念也作了介绍，如“信任”、“能力”和“数据锁定”等核心原则；接下来本书介绍了如何在安全平台上开发应用程序：开发环境，如何编写安全的应用程序、服务器程序和插件，如何在设备之间安全地共享数据；还阐明了作为平台安全行业“网守”的应用程序证书和签名的概念。所有这些信息对于那些希望为基于 Symbian OS v9 的畅销手机开发或移植应用程序的人们都至关重要。

本书的内容对于涉及 Symbian OS 的各级开发人员，从设备制造商，到商用 Symbian OS 手机应用程序的开发者，再到参与手机采购或基于 Symbian OS 手机的移动网络服务设计的安全专家，都很有用。

关 于 作 者

Craig Heath，第一作者

Craig 从 1988 年开始在 IT 安全领域工作，曾在 Santa Cruz Operation 公司担任 SCO UNIX 安全架构师，在 Lutris Technologies 公司担任 Enhydra 企业 Java 应用服务器安全架构师，他于 2002 年加入 Symbian，在产品管理和战略部工作。

Craig 于 1993 年成为开放组织安全论坛（原来的 X/开放安全工作组）的成员，并从 1999 年开始主持指导委员会的工作。他对多项已经公布的安全标准都有贡献，这些标准包括 XBSS（基准系统安全要求）、XDAS（分布式审核）和 XSSO（单点登录）；他还参与了 POSIX、IETF、Java 社区进程（JCP）和开放移动联盟（Open Mobile Alliance）的标准制定工作。Craig 于 1984 年毕业于沃里克大学，获计算机科学学士学位。

Craig 是 *Security Design Patterns* 一书（*www.opengroup.org/bookstore/catalog/g031.htm*）的合著者，开放组织（Open Group）的 *Guide to Digital Rights Management* 一书的第一作者（*www.opergroup.org/bookstore/calalog/g052.htm*）。

Andy Harker

Andy 拥有电子系统荣誉学士学位，他在电信软件领域工作了 17 年，曾参与过多个项目，如 FDDI-2、移动呈现和可用性系统、分布式实时中间件和光交换。

他于 2002 年加入 Symbian 并设计和开发了数字版权管理基础架构（内容访问框架），现在是密码服务技术领域的高级技术架构师，该技术领域为 Symbian OS 提供加密、密钥和证书管理、认证及软件安装服务。

在业余时间，Andy 喜欢摆弄三维图形渲染。当他想彻底逃离键盘时，就去照顾他的 400 升鱼缸中的热带鱼；如果他足够走运，会与伴侣丽贝卡和潜水好友去潜水，偶尔也会去水底拜访更大的鱼。

Geoff Preston

Geoff 于 2000 年从沃达丰加入 Symbian 来领导产品测试组织，在转到营销部门后，他引入了 Symbian 的 Catalyst 项目，与一批合作伙伴共同在 Symbian OS 上开发引人注目的第三方应用程序。最近，Geoff 和他的团队开发并发布了行业领先的证书项目 Symbian Signed。Geoff 在移动技术、网络拓扑和运营方面的背景意味着他会积极与 Symbian 的运营合作伙伴打交道并参加相关标准论坛。

Geoff 在赫尔学习，之后在中东、远东和北美生活致力于一系列通信系统的工作。他先加入了摩托罗拉，为其新的 GSM 基础设施工作，后来加入了英国的一家小型网络运营商（Racal-Vodafone）帮助启动新的 GSM 网络。

Geoff 居住在英格兰的威尔特郡，他与 Anne 结婚并和她有了一个女儿 Thea。

Jonathan Dixon

Jonathan 在过去 7 年中一直为 Symbian 工作，在一系列技术领域和任务中开发软件。在用了两年时间开发 Symbian 的蓝牙和红外线协议栈后，他花了一段时间研究重新设计套接字服务器架构，该重新设计的架构随后在 Symbian OS v9 中首次亮相。在两年时间里，他作为高级技术顾问在 Symbian 的专业服务部门工作，帮助 Symbian 授权伙伴推出手机产品，如索爱 P910i 和摩托罗拉 A1000。在最近 15 个月中，他一直作为系统架构师帮助实现 Symbian 的平台安全架构。

Jonathan 以信息系统工程一等工程硕士毕业于伦敦帝国大学。他是一个热心的滑雪爱好者和自行车爱好者，他把所有能够腾出的时间都用于骑自行车旅游或与他的妻子爱玛骑着心爱的双人自行车 Dobbin 一起长途旅行。Jonathan 感谢 Keith Robertson 不但给了他这么多能写的东西，而且教会了他如何写然后让他继续写下去。

Mark Shackman

Mark 以计算学科一等荣誉学位毕业，随后获得了数字系统硕士学位，后来又获得了研究生教育证书。在从事了 6 年教学和在摩根斯坦利工作一段时间后，他于 1997 年作为从事 SDK 内容和安装技术的作者加入了 Psion 软件。

在 Symbian 成型后，Mark 加入了连接性工程组，专门负责编写、制作、提供和支持连接性 SDK。他在 Symbian 的第一本书 *Professional Symbian Programming* 中也编写了一章内容。2001 年，他转到了工具箱组并很快成为技术架构师，负责引入新的软件包管理工具箱格式和随后的基于组件的版本。

2004 年，Mark 调到 Symbian 开发人员网络（Symbian Developer Network），以演示文稿、论文、书籍和工具的形式为开发人员提供技术支持。

Mark 感谢 Stephen Mansfield 提供审阅意见和更正，感谢 Stephen 和 Jonathan Dixon 提供技术建议和意见，还要感谢 Colin Turfus 和 Symbian 开发人员网络团队一直以来的支持，感谢 Hashem 做的所有其他事情。

Matthew Allen

Matthew 在 25 年前开始工作，那时他在小型机上使用 UNIX 第 6 版，在大型机上使用穿孔卡片和 JCL，从此之后，他一直在技术前沿工作。在 2003 年加入 Symbian 安全团队之前，他为各种项目工作，包括目录查询系统、UNIX 内核移植、自由空间光链路、分布式处理框架、SS7 调用处理和编译器开发。

Matthew 在剑桥大学鲁宾逊学院学习，在那里他获得了文学硕士学位。

Matthew 感谢他父亲的养育，感谢他妻子的宽容。

Michael Bruce

1996 年，Michael Bruce 从新南威尔士大学（澳大利亚悉尼）毕业，获机械工程荣誉学位。在制造行业从事了几年过程自动化后，他移民到英国并于 2002 年加入了 Symbian 的网络团队；随后，在转到安全团队后，成为实现新的平台安全软件安装程序的开发人员之一；最近他转到了营销部门，负责提供 Symbian Signed 所需的支持 Symbian OS v9 的工具。

当 Michael 不工作时，他喜欢旅行，尤其是到有雪的地方追逐对滑雪的热情。

Phil Spencer

Phil 对 Symbian OS 的涉足始于 Symbian OS 的前身 Psion，Psion 驱动着创造性的 Psion PDA。作为 20 世纪 90 年代早期最成功的 Psion“共享软件”作者之一，他于 1998 年夏天在 Psion 软件公司接受了一个实习职位。一年后，Phil 完成了大学入学资格考试，在进入大学之前的一年时间里，他作为“开发人员顾问”在新成立的 Symbian 公司中工作，负责向第三方开发人员提供支持、建议和指导。Phil 决定将其进入大学前的学业中断时间延长为两年，最终于 2000 年 9 月开始了在伦敦经济学院的经济学学位的学习，与此同时他继续为 Symbian 工作。

2004 年夏，Phil 以经济学荣誉学士学位毕业，返回 Symbian 全职工作并成为了开发人员内容团队的负责人。他管理的团队负责提供必要的文档和支持，以使开发人员能够了解 Symbian OS，并确保有引人注目的创造性应用程序可供 Symbian OS 手机使用。

Phil 目前居住在伦敦，他工作之余的最大兴趣是旅游。Phil 感谢他在 Symbian 和 Symbian Press 团队中的亲密同事，因为他们不仅给了他许多支持和乐趣，还帮助他在工作和大学学习的同时保持小小的清醒！

Simon Higginson

Simon Higginson 于 1999 年作为高级开发人员顾问加入了 Symbian 的技术培训团队，帮助编写了许多 Symbian OS 的培训课程，包括最近的平台安全课程。他有 19 年 IT 行业经验，曾作为软件开发人员为 GST Professional Services 公司工作，然后作为顾问为剑桥科学园的 Origin Automation Technology 公司工作。

Simon 在上学时从约克大学的计算机上开始了其计算生涯，之后他继续在剑桥大学邱吉尔学院攻读自然科学和计算机科学专业。在编写本书第 2 章时，他令人惊讶地找到了时间去竞选英国议会议员，感谢金斯林的人们选了别人，让他有时间完成工作。

Will Palmer

Will 从 2000 年 6 月开始为 Symbian 工作，最初是作为与计算机本地同步功能的开发人员，然后转到实现 SyncML 的远程同步开发团队。他一直在此领域工作，从程序员成长为技术负责人再到技术架构师。作为相关技术，他还获得了 OMA 设备管理的经验，目前他是专攻设备和

设置管理的系统架构师。

在接受C++程序员训练之前，Will在牛津理工学院学习电子工程，进入Symbian之前他为一家销售车辆跟踪软件的信息技术公司工作，开发计算机的客户端一服务器架构，也为车载手持设备开发软件，这进一步增加了他对电信领域的兴趣。

在家庭生活占据主要位置之前，Will喜欢旅游。现在他幸福地拥有两个小男孩，他们帮助他磨练其在职业生涯中所需的沟通和谈判技巧。

作 者 致 谢

Craig 想要感谢：

Symbian OS 平台安全的架构师们，尤其是 Corinne Dive-Reclus、Mal Minhas、Keith Robertson 和 Andrew Thoelke，他们应该接受对本书所描述特性的大部分称赞；其他来自 Symbian 对设计有重要影响的贡献者，包括 Will Bamberg、Jonathan Harris 和 Dennis May；荣誉也应该归于进行实现、集成和测试的众多 Symbian 工程师，因为人数太多而无法逐一列出。

对设计有所贡献的合作伙伴和客户，包括诺基亚的 Timo Heikkinen、Jann Uusilehto 和 Antti Vähä-Sipila；索尼爱立信的 Johan Alm；UIQ 的 Mattias Reik；沃达丰的 Steve Babbage 和 Tim Wright；法国电信的 Didier Bégay 和 Orange 公司的 Tim Haysom。

我的合著者 Matthew Allen、Michael Bruce、Jonathan Dixon、Andy Harker、Simon Higginson、Will Palmer、Geoff Preston、Mark Shackman 和 Phil Spencer，他们完成了大部分艰苦工作。

我的经理 Richard Wloch 和我的合著者的经理 Tim Bentley、Bruce Carney、Simon Garth 和 Neil Hepworth，他们允许我们将大量的工作时间用于准备这本书。

其他贡献了相关材料或富有洞察力的意见的人们，包括 Tim Band、Ilhan Gurel、Sami Lehtisaari、Stephen Mansfield、Steve Mathews、Kal Patel 和 Jo Stichbury。

最后特别要提到的是 Phil Northam 和 Freddie Gjertsen，他们使这本书的编写过程变得轻松，并容忍了我们错过许多最终期限！

Symbian Press 致谢

Symbian Press 要感谢 Craig 的坚持；感谢 Stephen Evans 又一次宽容地为我们提供了更多资源；感谢伦敦广播公司（LBC）将我们拴到了办公桌上；还要感谢 William，因为绝对应该提到他。

前　言

在过去 10 年里我一直在手机安全领域工作，我们看到手机上使用的编程环境的功能和灵活性被极大增强，手机正在走向计算机和互联网的开放性。在同一时期还有着其他努力，这种努力不是封闭计算机和互联网的开放环境，而是至少“驯服”它们，这种驯服需要发生并且应该继续。

幸运的是，手机功能和开放性的增强是以可控方式发生的，许多因素都有利于安全。首先，在这一时期，大多数手机曾经并仍然被网络运营商购买（用于销售给其用户），他们施加于手机的安全要求有着较高的实现标准；其次，进出手机的大多数数据都涉及网络运营商，运营商有理由也有能力在网络端采取措施来控制病毒和蠕虫在客户端上的影响；最后，有一个简单的事实：Symbian OS 手机只代表了全部手机中的一小部分。

某些这类因素正在改变，最重要的变化无疑是基于 Symbian OS 和其他开放操作系统的手机的比例开始显著增加，Symbian OS 将成为恶意软件编写者的重要而值得的目标。短距离和长距离无线接口种类的日益增多意味着数据和应用程序有许多方式可以进入手机，运营商能够控制的数据比例将减少。Symbian OS 正在进入更大和更缺少控制的世界，它需要能够照顾好自己。

因此，沃达丰非常欢迎 Symbian 引入平台安全架构。我们希望有效的应用程序开发者证书方案、对 Symbian OS 最可信部分的持续审查和改进，以及与安全软件启动时和运行时的保护相互补的硬件安全特性将与平台安全一起使用，帮助确保平台安全的长期成功，这样 Symbian OS 就可以向更广泛的应用程序开发者开放，并保证能够基于开发者将承担的责任来为代码分配特权，同时用户及其手机能够被保护而不受糟糕代码和恶意企图的影响。

本书提供了平台安全架构的背景知识，这些知识将对安全专业人员有意义并指导应用程序开发人员如何最好地利用现在的安全改进，广泛采用这些实践将使整个手机行业受益，包括软件厂商、半导体厂商、手机制造商、网络运营商、内容提供商还有非常重要的手机用户！

Tim Wright
（沃达丰研究和开发集团安全技术部）

目　录

第 1 部分　Symbian OS 平台安全简介

第 2 部分　平台安全应用程序的开发

PART 1

第 1 部分

Symbian OS 平台安全简介

- 第 1 章　为什么需要安全平台
- 第 2 章　平台安全概念