Broadview
www.broadview.com.cn

Microsoft

安全技术大系

The Security Development Lifecycle
SDL: A Process for Developing Demonstrably More Secure Software

软件安全开发生命周期

[美]Michael Howard Steve Lipner 著
李兆星 原浩 张钺 译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

The Security Development Lifecycle
SDL: A Process for Developing Demonstrably More Secure Software

软件安全开发生命周期

[美]Michael Howard Steve Lipner 著
李兆星 原浩 张钺 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

对于软件安全开发生命周期（SDL）的介绍不仅讲述了一个方法论变迁的历史，还在每一个已经实践过的过程（从设计到发布产品）的每一个阶段为你提供指导，以将安全缺陷降低到最小程度。软件开发方法的发展和采用对提高微软软件产品的安全性和保密性的确卓有成效。由 13 个阶段的过程组成，统称为软件安全开发生命周期。本书将向您一一呈献。本书的特别之处在于 SDL 并不是枯燥乏味的理论，而是更具有可操作性的实践指南。SDL 有两重目的：其一是减少安全漏洞与隐私问题的数量，其二是降低残留漏洞的严重性。

本书适合以下人员阅读：一类是高级管理人员以及具体管理软件开发团队和软件开发过程的管理人员，另一类则是软件设计师和软件架构师。

版权贸易合同登记号　图字：01-2007-4303

图书在版编目（CIP）数据

软件安全开发生命周期 /（美）霍华德（Howard, M.），（美）李普纳（Lipner, S.）著；李兆星，原浩，张钺译. —北京：电子工业出版社，2008.1
（安全技术大系）
书名原文：The Security Development Lifecycle SDL：A Process for Developing Demonstrably More Secure Software
ISBN 978-7-121-05294-1

I. 软…　II. ①霍…　②李…　③李…　④原…　⑤张…　III. 软件开发－安全技术　IV. TP311.52

中国版本图书馆 CIP 数据核字（2007）第 170668 号

责任编辑：朱沭红　王鹤扬
印　　刷：北京民族印刷厂
装　　订：北京鼎盛东极装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：22.25　字数：472 千字
印　　次：2008 年 1 月第 1 次印刷
定　　价：55.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

致 谢

感谢我宽容美丽的妻子 Cheryl；我帅气的儿子 Blake 和我那活泼迷人的女儿 Paige。我爱你们。

—Michael

感谢 Anne，对她在我构建安全系统的这段时间中给予的支持和理解表示深深的爱和感激。

—Steve

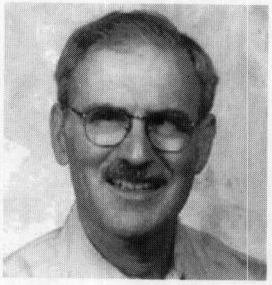
作者简介

Michael Howard

Michael Howard, CISSP，微软安全技术部资深安全项目经理。Michael 著有许多安全相关的文章和书籍，包括广受赞誉的“Writing Secure Code”（《编写安全的代码》）和“19 Deadly Sins of Software Security”，在为业内期刊撰写文章的同时，他还是 IEEE 安全与策略期刊的编辑之一。他致力于定义和传播安全教育，定义软件开发生命周期，研究新的威胁和防护措施，并协助微软产品集团开发更为安全的软件。在软件安全领域，Michael 拥有 4 项专利。

Steven B. Lipner

Steven B. Lipner, CISSP，微软安全技术部资深安全工程高级主管。Steven 负责安全开发生命周期的定义和改进，微软计划通过安全开发生命周期来增进其产品的安全性和保密性。Steven 同样负责对微软产品进行安全评估的策略和战略，从而为微软的客户们提供更为可靠的产品。Steven 拥有长达三十多年的经验，期间曾担任研究人员、开发经理以及 IT 安全方面的总经理角色。Steven 也是计算机和网络领域的 11 项专利的合作者之一。Steven 曾在 MIT 先后获得学士及硕士学位，而后参与哈佛商学院的管理开发合作项目。他不仅是美国信息安全与隐私协会专家组成员，他还以 CISSP 身份成为 ISC^2 美国专家组的一员。



推荐序

值《软件安全开发生命周期》此书中文版发布之时，在微软 Bill Gates 已经启动可信计算运动长达六年。在这一时期中，微软已经从传统的被视为只是一个提供安全性差、漏洞多的软件公司转变成为一个在缔造更为安全的软件方面成功及创新方法的领导者。当其他许多厂商仍然与上报的软件漏洞比例不断增长进行斗争之时，微软已经通过遵循本书中所描述的实践活动降低了漏洞报告的比例。

基于对每一个上报给微软的安全漏洞“根源”进行的分析，软件安全开发生命周期（SDL）致力于找出安全漏洞根源的一般性趋势，并采取一种务实的方法，如考虑采用相关工具或者过程以防止同类问题将来再度发生。对SDL的持续改进加以提炼并进行合理规划，这一明智之举使得微软能够成功地应对安全研究机构的种种技巧以及战术方面的变化。

所有的软件开发人员，从独立软件开发商到企业业务应用开发人员，都面临着一种压力，就是既要迅速地开发软件又要满足高的安全期望。通过将工程师所需的信息以一种简明扼要、可操作的形式，而不仅仅是一种可快速有效应用的针对工程师所用到的软件开发方法论框架展现出来，以一种易于理解的方式展现的 SDL 中所包含的信息则可被开发团队快速并有效采纳。当然本书中所提到的材料主要是描述用于微软 Windows 平台的开发，但相关概念与技巧则适用于任何平台或编程语言。

我曾经与本书的作者一起共事，并在过去的四年间致力于创建并成功实施 SDL。令人激动的是，微软成功地在其软件中降低了安全漏洞。现在微软所采用的同样的信息则可面向所有工程团队，共同分享并应用以改善其软件的安全性。

Eric Bidstrup
Microsoft Corp.

译者序

软件安全——最后的堡垒

译完这本早在2006年7月份即已在美国出版的软件安全书籍，掩卷沉思，我的目光再次落在Hard Copy的封面之上的“Security Development Lifecycle”。数年来，安全这一关键词始终相伴我左右：

- 2004年与好友Lance、Youyou一起参加X'Con正式踏入安全圈；
- 2005年先后撰写“中国国家信息安全的几点思考”、“应用安全，大有可观”等文章，并成为中国计算机报的专栏作者；此时，开始关注如何从“业务”角度分析安全问题、并寻找解决之道；
- 2005年末协同Robin、Colababy等好友共同组建“中国信息安全专业人士俱乐部”，致力于促进信息安全圈不同层面人士的技术、管理、价值观点等交流活动；先后在北京、上海等多次举办俱乐部的专题研讨活动；其中更对业务中的安全风险进一步加深了理解；
- 2006年与加拿大友人协作撰写“信息安全——敦科尔克大撤退”一文，引起诸多关注，由此开始关注“安全+价值+业务”三者之间的关系，走上以“技术+管理”相结合的信息安全探索之路；并对部分安全实践活动加以总结，撰写“中国银行业——六国毕、四海一”一文，获得诸多好评；密切关注软件安全方向研究的进展，并逐步整理、积累软件安全方面资料（其中就包括对于“Security Development Lifecycle”一书的学习与实践），同时以微软特邀安全专家身份参与多次软件安全方面的演讲会议；
- 2007年参与并以项目负责人身份进行安全咨询项目，主要是以ISO27001信息安全管理体系ISMS建设为主的咨询项目，该类咨询项目旨在帮助客户管控全面的信息安全风险，使客户符合国际通行的标准规范；同时也负责部分技术咨询项目，在此过程中，客户对于软件安全的需求进一步促使我加深理解，通过多次实践终于初步形成具有特点的软件安全咨询体系。这一体系所涵盖的服务目前仍属于初级阶段，仍不够严谨，需要客户、业务主导方以及更多同仁的共同参与方能日臻完善。

微软，作为可信计算的倡导者以及在软件安全方面的领导者之一，无可否认将其Windows Vista、Office 2007等产品开发过程中的安全实践总结并以图书形式与更多IT管

理者、开发人员、测试人员等分享，这一点是非常令人激动的。为了让更多的中国读者能够更容易理解、学习本书中所述及的软件安全实践活动，译者与微软的友人、电子工业出版社等偕同将此书中文版推出，以飨读者。

因为时间仓促，不免文中诸多疏漏，谨谢电子工业出版社的许艳、王鹤扬二位编辑，细心审校，方能顺利成书。同时微软 Eric Bidstrup 在百忙之中为中文版作序，微软安全专家 Richard.Yi 大力协助，解决不少过程中的问题，使我可顺利完成翻译工作。

同时非常感谢上海安言信息技术有限公司（最可信赖的信息安全及 IT 咨询顾问）的所有同事们，尤其是 Robin、Colababy、Yuan、Zhang 等人，他们的帮助、关心以及在软件安全实践中的合作使得我可以更好地理解、接近该书作者所希望表达的最真实想法，在此对他们表示衷心感谢！

最后感谢我的家人，他们的鼓励、照顾使得我有更多精力与软件安全威胁、风险进行不懈的战斗。

译者

2007 年 11 月

序

一个周一清晨，Steve Ballmer 拿着一个笔记本电脑走进会议室。他把电脑放在我的面前，说：“帮我修好它，我明天就要。”这个周末他刚刚参加过一个婚礼，这个电脑是他的朋友——那个新郎的。他又补充道：“我整个周末都在干这个，但我还是搞不定。明天我就要把电脑还给他了！”

我们分析了这台电脑，以便找出问题之所在。之前我们也成功修复过其他电脑，但这台电脑已经彻底被病毒和恶意软件破坏。一些已知病毒可以被轻易地清除掉，但还有几个病毒是我们从来没有见过的。事实上，当第一个病毒侵入该电脑时，这台电脑就几近崩溃。我正好借此机会对此病毒的源代码进行分析。结果发现，其侵入机器的第一件事就是搜索并删除所有包含“病毒（virus）”字样的东西。当然，这其中包括所有以“反病毒（antivirus）”命名的文件。然后它将自身隐藏起来，并利用组策略的管理机制关闭了 Windows 更新功能。恶意软件狡猾地利用组策略工具禁用了几乎所有系统级权限。你试图启动杀毒软件的努力都会无功而返。因此，电脑已经彻底崩溃了。

我们最终还是修好了电脑，而且微软新近发布的一些安全和反恶意软件产品也有助于保护电脑不再受类似问题的影响，但是更多的恶意软件仍会接踵而至。安全攻击已不再局限于躲在卧室里的小青年搞搞破坏，用以炫耀，带有经济利益的攻击才是一个真正有利可图的犯罪活动。毫无疑问，一旦踏入信息安全这一战场，我们就像站在了风口浪尖，决不可行差踏错半步。这将会是一场持久战。黑客们已经超越了攻击操作系统和网络服务器的阶段，正对数据库以及与数据类型相关的程序代码虎视眈眈。如果你写的代码中含有解析器，他们就能顺藤摸瓜实施攻击。根据我们的调查以及其他行业的统计结果表明，攻击的对象已经从操作系统延伸到上层的应用程序。不仅微软的 Windows，所有的系统，包括 Linux、Mac OS X、Solaris、服务器和客户端应用以及 Web 应用，全都在劫难逃。

面对威胁，编写安全的代码是我们的杀手锏之一。当然，其他方法还包括软件默认安全配置，因其具有高伸缩性，所以即使是有漏洞的代码也不会表现得不堪一击；与此同时，安全产品也能抵御攻击或者使软件从攻击中快速地恢复。在微软，我们选定了两个主要的目标范围来摒除操作系统中的安全问题：一个是微软 Windows Server 2003，另一个则是 Windows XP SP2。这两个项目花费了数千工程师数月的劳动和无数的心血，也让我们对如何打造 Windows Vista 而反思良久。我们在这个领域的工作仍然在继续，但这些项目使得我们获益匪浅。在此若能与您分享这些收获，我们将倍感荣幸，这也是我们编写《软件安

全开发生命周期》这本书的初衷。安全不能一蹴而就，但本书中的内容能够帮助你在设计产品、管理项目、编写代码、评估风险和测试安全场景时候做得更充分，这将更好地保护你的客户。

本书的作者，Michael Howard 和 Steve Lipner，在安全产业与软件安全方面拥有超过 45 年以上的经验。Michael 和 David LeBlanc 于 2001 年 12 月出版的经典之作《编写安全的代码》（“Writing Secure Code”一书）[①]迄今已发行超过 8 万册，成为开发人员手中的不可多得的参考书，其汇集了我们在开发 Windows XP SP2 过程中的很多心得体会。在处理微软安全响应中心接到的漏洞报告，并不断改进研发方法，从根本上消除导致以上漏洞出现的原因过程中，我们获益良多。《软件安全开发生命周期》一书正是这些经验和知识的积累。本书涵盖了诸多 How-to 信息，从如何教育开发人员、如何进行安全审核到处理突发事件，这一切在本书中都有详细的阐述。

以我在软件行业多年的经验，我能给出的最好忠告就是提醒你，安全是要付出代价的。如果现在不付出，以后它会让你加倍偿还。你会被抱怨的电话、媒体的指责、愤怒的顾客和失望的销售弄得焦头烂额。是现在就增加投入，抑或是以后再进行补救，这取决于你采用何种方式开发代码。一旦有缺陷的代码被交付之后，再想补救已是回天乏术。如果安全漏洞进入了软件的 beta 版本，那也已经无可救药。即使是在测试中能发现问题，也无济于事。当安全漏洞已经潜藏于软件之中时，软件就已病入膏肓。我希望，本书所描述的实践活动能够帮助你更有效地发现软件中存在的问题，但更重要的是，从一开始就避免这些问题的产生。

Jim Allchin
2006 年 5 月
Redmond, WA

---

① 注：电子工业出版社引进了该书的最新版“Writing Secure Code for Windows Vista”（Microsoft Press，2007），预计将于 2007 年底出版。

前　言

让我们回顾一下 2001 至 2002 年安全领域的状况，以下是当时安全方面关注的一些问题的标题和评论：

- “Gartner 推荐将微软 IIS 置于门外”（eWeek 2001a）
- “因 IIS 安全而引发的安全 bug”（eWeek 2001b）
- “微软安全的悲哀”（CNET 2002a）
- “微软安全推进乏善可陈”（CNET 2002b）

接下来，我们看看 2005 至 2006 年的情况：

- “不得不承认，微软正通过安全开发生命周期领导着软件业的前进”（CRN 2006）
- “‘微软是业界的领军人物’，Oltsik 对微软通过安全开发方法领导软件业给予肯定”（Enterprise Strategy Group 2006）
- “总而言之，近几年微软的安全公告已经大为减少”(eWeek 2005a)
- “微软：引领软件安全趋势？”(eWeek 2005b)

业界对微软态度的这一改变不是偶然的。微软进步的原因只有一个：软件开发方法的发展和采用对提高微软软件产品的安全性和保密性的确卓有成效。上述软件开发方法由 13 个阶段的过程组成，统称为软件安全开发生命周期（SDL）。本书将向您一一呈献。

本书的特别之处在于 SDL 并不是枯燥乏味的理论，而是更具有可操作性的实践指南。虽然，对于解决安全以及隐私类问题仍然不存在“银弹”，但 SDL 产生了非常积极的效应，确实能够明显减少实际代码中的漏洞数量。

最后我们必须强调的是，SDL 源于实际工作中的经验，而且它确实有效。或许安全顾问曾对你吹嘘某种先进的方法能明显提高软件安全性。至于到底能不能提高那只有天晓得！但我们可以大言不惭地说，SDL 确实能提高软件安全。当然，SDL 并不完美；但如果你确实重视安全和隐私问题，那么你就应该看一下本书中 SDL。

SDL 有两重目的：其一是减少安全漏洞与隐私问题的数量，其二是降低残留漏洞的影响。由于软件开发仅仅基于现有的安全最佳实践活动，而新的安全研究和攻击方式却永无止境，因此消除所有的安全问题和缺陷是永远不可能的。

为何你需要阅读这本书?

首先，必须说明的是，本书并非针对开发人员所写。当然，这并不代表开发人员不能阅读本书，我们的意思是，书中并没有大量的代码和可实现的最佳实践供开发人员立刻使用。本书的预期读者有两类：一类是高级管理人员、具体管理软件开发团队和软件开发过程的管理人员；另一类则是软件设计师和软件架构师。

本书的内容安排

本书分为三个部分，每个部分针对不同的读者。

第 1 部分　对 SDL 的需求

这部分提出了两个问题：其一，为什么我们要从一开始就关注软件的安全性；其二，我们如何使得这些改进获得管理层的支持。第 1 章“适可而止：威胁正在悄然改变”详细阐述了安全性和保密性为什么至关重要，以及管理层为什么难以接纳改进安全性的建议。这一章的内容所有读者都有必要了解。第 2 章“当前软件开发方法无法构建安全的软件”一针见血地指出了当前开发方法中的局限性，而第 3 章“微软 SDL 简史”讲述了 SDL 在微软兴起的渊源，并且向各级经理详细描述了哪些工作对于构建安全软件无异于水中捞月。第 4 章“从管理角度看 SDL”是专为中、高层管理者准备的，因为这一章以非技术词汇解释 SDL，从而让读者意识到实施 SDL 这一过程的投入与回报。

第 2 部分　软件安全开发生命周期过程

这部分的 13 个章节是全书的精华所在。每个章节对应 SDL 的一个阶段（从第 0 阶段开始到第 12 阶段结束），并且列出了各个阶段的需求。如果你在公司负责提升软件安全性方面的工作，如果你对整体的过程改进感兴趣，如果你是软件开发方法论研究者，抑或你需要高屋建瓴地把握企业中软件的研发过程，那么你都应该完整阅读这部分。

第 3 部分　SDL 参考资料

本书的最后一部分列出了 SDL 开发和编程所需要的一系列相关资源。其中的一章讲述了能够满足 SDL 安全需求的敏捷开发模式。在本书出版之前，还没有涉及安全和敏捷软件开发相关内容的文章。第 18 章“在敏捷模式中集成 SDL”将填补这一空白。

SDL 的未来发展

SDL 不是一成不变的。任何一种关注安全的软件开发过程都不能固步自封，因为安全本身瞬息万变。在微软，我们在每年的 1 月和 7 月对 SDL 进行全面更新。虽然我们的初衷是保证 SDL 能够不断采纳各种建议，以便更有效地改进软件安全性，然而现在，这种变更过程已经非常详尽了。过程顺序正如以下四段所述。

微软所有人员都在帮助改进 SDL。这种改进可以是提出某种需求或给出某个建议。对于此类需求和建议，团队都必须要在产品后续的版本实现。现在的需求在一年半载之前可能就只是一个建议，这种情况司空见惯。对此类需求和建议进行描述的文档应包含预期变更以及变更基本依据。归根结底，此类预期变更必须对提升安全性确实产生效果。我们不希望 SDL 面对一大堆善意而无用的要求穷于应付，因此如果预期变更执行后，应当至少可以避免发布五份安全公告。当然，如果某项变更有望进入实施阶段，文档中就必须详细描述如何验证以确保提出的需求得以满足的方法。这对一个测试提案的团队识别提供的准确真实的反馈来说也是不无裨益的。

接下来，SDL steering 小组会对这些提案进行评审并及时反馈给提案者。提案者本身就是 SDL steering 小组成员或者是被邀请参与其提案评审会的外部人员。

一旦开始修改草案，就会在微软内部安全人员中公开这些提案，以便集思广益。

最后，提案修订完毕并付诸实践。SDL 涵盖的所有产品都是新的需求实施的对象，因而必须将上述建议考虑在内。

考虑到 SDL 这一动态特性，本书中部分内容或许在不久的将来会被取代。书中一些材料将会在网站 http://go.microsoft.com/fwlink/?LinkId=65489 及时更新，敬请关注。

随书 CD 内容

随书 CD 中包含以下资料：

- **“基本内容”** 我们认为，每一位在软件方面有过研究的人都应该有基本的安全知识。这个在线的视频介绍和幻灯片演示就是我们认为您应该了解的最基本的安全知识。这个演示并不是要将您培养成为一个安全专家，而是为所有的软件开发人员提供入门级的教育。
- **安全风险评估文档** 第 8 章，“第 3 阶段：产品风险评估”中提及 riskassess.rtf 文档，该文档可被用于帮助安全团队关注潜在的弱点，以迅速地发现一个应用软件的风险区域。

- **banned.h** 在第 11 章，“第 6 阶段时：安全编码策略”中提到，它是一个可以包含到任何 C/C++代码中的头文件，用于快速找到代码中的违禁函数。
- **MiniFuzz file fuzzer** 在第 12 章，“第 7 阶段：安全测试策略”中有所提及。MiniFuzz 是一个用于提供文件模糊器（fuzzer）雏形的 C++源代码文件集。这个工具的目的并不是提供一个完整的模糊测试方案，而是给开发者和测试者一种感觉，理解文件模糊器是如何工作的同时，也了解如何使用 Windows 的调试的 API 来捕获代码中的错误。
- **外部攻击基本原理文档** AttackSurfaceRationale.rtf 是在第 13 章，“第 8 阶段：安全推进活动”中提到的一个简短的文档，它用于帮助安全人员理解为什么一个产品仍然具备那些默认启用的受攻击面（诸如开放的网络端口等）。

系统需求

Attacksurface.rtf 和 riskassess.rtf 这两个 Word 文档都是用 Microsoft Word 2003 创建的，但是已经可以用 Windows XP SP2 的 Microsoft Windows WordPad 和 Microsoft Word 2000 读取。系统需求与 Microsoft Word 的一样。

MiniFuzz 这个软件是用 Microsoft Visual C++ 2005 编写的，这个工程文件只能被装载到 Microsoft Visual Studio 2005 中。系统需求与 Visual Studio 2005 的一样。

Banned.h 是在 Visual Studio 2005 的环境下编写的，但是已经在 Visual C++ 2002、Visual C++ 2003、Visual C++ 2005 和 GCC 3.4.x 下测试通过。

最后，“基本内容”中的视频演示要求具备 Windows Media Player 7 或更高版本，Windows Media 9 解码器，Internet Explorer 6 和 XML Parser 4.0 Service Pack 1（光盘中均已包含）。

致谢

如果没有微软内外的许多朋友帮助，这本书是根本不可能面世的。在此感谢那些审核草稿、提出批评和在某些方面提出正确分析和建议的所有人员。

接下来要感谢的是微软安全性工程和通信小组中的一些同事。每天和工程小组一起致力于 SDL 的美好前景的同事们，他们是：Adel Abouchaev、Allen Jones、Bryan Nealer、Chris Walker、Dave Ross、David Ladd、Eric Bidstrup、George Stathakopoulos、Greg Wroblewski、John Lambert、Jon Ness、Matt Thomlinson、Mike Mitchell、Mike Reavey、Neill Clift、Nicholas Judge、Shawn Hernan 和 Tina Knutson。

还要感谢一些朋友通过微软提供了反馈意见，他们是：Akshay Aggarwal、Amy Roberts、Bill Ramos、Bjorn Levidow、Christopher Budd、David LeBlanc、Irada Sadykhova、Jason Garms、JC Cannon、John Gray、Jon Wall、Manoj Mehta、Peter Torr、Rose Bigham、Talhah Mir 和 Todd Webb.

我们的一些客户用他们的实际经验纠正了我们的一些观点和注释，他们是：Adam Shostack、Alan Krassowski (Symantec)、Charles Chandler (NetIQ)、Hugh Thompson (Security Innovations)、Kyle Randolph (Citrix)、Michael Angelo (NetIQ)和 Mukesh Kumar (SafeCo)，在此对他们也表示感谢。

Virgil Gligor，Maryland 大学的电子和计算机工程的教授，对我们的草稿进行了外部的技术复审。由于 Virgil 在构建安全系统方面有多年的经验，其丰富的学识、严谨的观点，都使我们最终的书稿增色不少。

微软的可信计算学术咨询委员会在激发我们创作这本书方面起了至关重要的作用，Virgil 也是其中一员。我们曾经请这个委员会对一篇关于 SDL 的论文（Lipner and Howard 2005）进行评审，他们还给我们提出了很多有帮助的建议，委员会的一些成员提议我们最好写一本关于 SDL 的书。这些建议是我们最终决定启动这一项目的主要原因。

最后，也是最重要的，我们要感谢微软公司的高管们，从 Bill Gates 往下，批准且授权我们在公司内部执行 SDL，并为我们提供了数千员工，以使他们意识到安全和隐私正是“完成工作任务必不可少的一部分”，从而交付更为安全的软件。

真诚地感谢你们所有人。

Michael Howard
Steven B. Lipner
Redmond, WA
2006 年 6 月

参考文献

(eWeek 2001a) http://www.eweek.com/article2/0,1759,1240915,00.asp. September 2001.

(eWeek 2001b) http://www.eweek.com/article2/0,1759,97182,00.asp. July 2001.

(CNET 2002a) http://news.com.com/Commentary+Microsofts+security+woes/2009-1001_3-808870.html. January 2002.

(CNET 2002b) http://news.com.com/Microsofts+security+push+lacks+oomph/2100-1001_3-808010.html. January 2002.

(CRN 2006) Rooney, Paula. "Is Windows Safer?" http://www.crn.com/sections/coverstory/coverstory.jhtml;jsessionid=VV1Q351RM5A1YQSNDBOCKH0CJUMEKJVN?articleId=179103240. February 2006.

(Enterprise Strategy Group 2006) Oltsik, John, Senior Analyst, Enterprise Strategy Group. "Good security news to be in short supply in 2006," *http://news.com.com/Good+security+news+to+be+in+short+supply+in+2006/2010-1071_3-6028980.html*. CNET News.com, January 2006.

(eWeek 2005a) Naraine, Ryan. "Microsoft Claims Security Win with New Development Rules," *http://www.eweek.com/article2/0,1759,1779769,00.asp*. March 2005.

(eWeek 2005b) http://www.eweek.com/article2/0,1759,1860574,00.asp. September 2005.

(Lipner and Howard 2005) Lipner, Steve, and Michael Howard. "The Trustworthy Computing Security Development Lifecycle," *http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp*. MS DN, March 2005.

目 录

第 1 部分 对 SDL 的需求