开源软件安全问题与对策

李 昕[1,2] ，陈智俐[1,3]

（1. 湖南财经高等专科学校，湖南 长沙 410205；

2. 中南大学信息科学与工程学院，湖南 长沙 410083；3. 湖南大学软件学院，湖南 长沙 410082 ）

摘 要：该文分析了开源软件的技术优势与安全问题以及人们的某些误解，讨论了针对其各种安全隐患应采取的对策，提出了提高开源软件安全性的方案。

关键词：开源软件；安全；对策

A Brief Discuss on OSS Safety Problem & Solution

LI Xin[1,2], CHEN Zhi-li[1,3]

(1.Hunan College of Finance and Economics, Changsha 410205, P.R.China;2.nformation Science and Engineering College of Centre South University, Changsha 410083, P.R.China;3.Software College of Hunan University, Changsha 410082, P.R.China)

Abstract: This paper analyzed the technical advantages and safety problems of Open Source Software, and discussed some policies on such problems, then proposed some solutions to promote the safety of Open Source Software.

Key words:OSS;Safety;Solution

20世纪90年代以来，以Linux为代表的开放源代码软件随着互联网的兴起得到了飞跃性的发展，其性能、兼容性和界面友好性都大为改善。目前，无论是在基础领域的操作系统、数据库、中间件、开发工具，还是在应用领域的ERP、CRM、电子商务，开源软件都提供了强大的支持和丰富的选择。开源软件已给软件产业带来了惊人的变化，也得到了越来越广泛的应用。然而，在发展的同时，开源软件也一直承受着众多的误解，特别是在其安全性问题上更是颇受怀疑。本文从开源软件的优势入手，剖析了种种对开源软件安全问题的误解，并提出了进一步加强提高开源软件安全性的技术策略。

1 开源软件的优势

开源软件由于其独特的开放源代码的开发模式，在安全性方面具有众多与生俱来的优势：

1.1 开放代码有助于改善代码质量

在典型的闭源代码开发项目中，源码是封闭的，软件中的错误或失误有可能被开发者无意间忽略或有意悄悄掩盖；相反，开源软件通过同行审查这样的环节，使每一行代码都处在众多参与者的共同关注下，每一行代码又关联到了开发者的个人声誉，开发者会竭尽全力改进代码，其开发团队也会非常注重提高项目管理水平。

1.2 开放代码有助于快速修改错误

由于开放代码软件会得到成千上万开发者的审查，因此发现错误并修正它们只需很少时间，而闭源软件的维护只有原开发者独自承担，周期自然比较长。

1.3 开源有助于促进安全技术的应用发展

有关安全的新理论、新技术在开源编程者中更易被实践和进一步创新。他们乐于探索现有技术的缺点，并修正安全性较差的旧代码，引入新技术加以替代，代码安全性逐渐得到改善。而在商业性闭源开发中，往往由于交货周期紧迫等商业上的原因难于采纳最新的安全技术，更难于有所创新。

1.4 开源软件具有较好的安全等级

开源软件安全等级对于最终用户完全透明，用户可以确定该软件是否能真正满足需要，而封闭代码软件的最终用户却难以直接评估整个系统的安全等级，只能通过测试来间接体现。只有开放源代码，最终用户才可以彻底检查代码安全性，排除后门、木马等危害的存在，保证其符合自身利益。对于关系到国家政治军事目的的重要基础软件，开源软件的代码可审查性更为国家用户提供了必要的安全信心。

尽管开源软件在安全性方面具备了上述诸多明显优势，但在实践中还是遭遇了种种“误解”。

2 对开源软件的种种“误解”

对开源软件的“误解”一直都在伴随着开源软件的不断发展而变化，其中许多都集中在开源软件的安全性方面。其中影响最广的几个观点可以一一分析如下。

2.1 “通过分析开放的源代码能找到系统的安全漏洞”

从程序分析的角度来看，分析系统的源代码的确可以发现其安全漏洞。但许多闭源软件的漏洞在源代码

基金项目：本文受湖南省教育科学“十一五”规划课题[编号 2006XJ150]资助

保密的情况下仍可以被人发现，不开放源代码并不能保证安全漏洞不被发现。黑客固然可以发现漏洞，众多的开发者也可以发现漏洞，而且会以很快的速度改进代码，堵住漏洞，同时通过开源社区等形式来迅速公布其改进，提高了系统整体安全性，就减小了黑客可能造成的危害。

2.2 “开放的就是不安全的”

日常观念中，“安全”往往和“不开放”、“保密”、“隐蔽”联系在一起。但历史上所谓“秘密”的加密算法总是会被破解的，而现行主流的加密算法（如DES）大都是算法公开而密钥保密，其安全强度依赖于密钥的长度。算法可以被攻破，协议可以被解析，企图靠封闭和隐秘达到安全很不可靠，而“公开方法将保证更好的安全性”这个看似矛盾的观点在实践中已被证实很久了。

2.3 “开放代码没人真正去仔细分析”

众多的事例证明，在开放源码系统中，即使是很小的错误也可以被发现，只是发现的时间有早晚；而影响越大的错误，越容易被众多开发者发现并改正。

2.4 “开放源码中可放置后门”

每个开发者都可以把任意代码放进系统中，但他既不能保证放置的后门不被发现，更不能保证后门不会被堵住，还要把开发者的个人名誉置于其中冒险。开源软件可以使用代码控制系统来管理代码树，同时有许多人在检查和分析代码，这使得放置后门变得更加困难。相反，封闭源码的软件中更容易放置后门或陷阱，却难于被外人发现。

通过分析以上的种种“误解”，可以得出的结论是开放源代码与安全漏洞没有直接关系。安全漏洞的来源主要来自软件的设计、质量控制和配置使用方法，而不在于源代码是否开放。更令人不安的是，在封闭的源代码中，商业组织和国家机构很容易在上千万行的程序中设置后门而达到不可告人的目的。开源软件的使用者认为封闭源码软件并不比开放源码软件的安全性好，相反，开放源码软件更有能力和潜力提供更好的安全。

3 开源软件的安全隐患与对策

绝对安全的系统是不可能存在的。像任何其他系统一样，开源软件在实践中的确也存在一些安全隐患，但可以采取相关的对策来尽力消除，逐步提高系统安全性。

3.1 检查机制难以全面严格执行

理论上任何人都可以检查所有的软件代码，但实际上限于个人精力和能力，经过专业安全检查的软件只是少数。大多数开发者分析源代码是出于自身需要，常常无暇检查与自身工作无关的代码。

相应的对策是进一步完善开源社区的开发机制，努力建设好全面、严格的检查机制，并做好文档完整性管理，促进检查的深入进行。

3.2 检查者的技术水平差次不齐

现实中不可能期待代码检查者的技能总是会高过代码编写者，一些错误在有限的检测中很难被发现，甚至要求分析者的专业水平高于编码者。实际上，大多数错误都是在程序已经编译、测试并分发后才被发现，在实际使用中才暴露出来的。开放源码的程序通常依赖于用户报告和公共论坛来发现错误，而不是派人提前查看代码的漏洞。

相应的对策是加强开源社区的交流、培训机制，努力提高全体开发者的专业技能，并鼓励更多的人来参与发布前的代码检查测试，争取可以尽早发现漏洞。

3.3 缺乏专业安全测试

开放源码的最主要安全性优点是“多眼”现象——让更多人分析代码，可以更及时地发现和修复错误，特别是与安全性相关的错误。然而，无法保证分析开放源码的人会发现代码中的任何安全性问题，更不必说所有问题了，也无法保证发现安全性问题的任何人都会实际报告它们。

相应对策是对开源系统进行全方位安全测试。现代软件工程对软件生产过程中的测试环节给予了充分的重视，提出了一系列诸如黑盒子、白盒子测试等专业测试方法，也为软件的安全测试指明了方向。测试工作可以内部进行，还可以外包给专业的第三方测试公司(如大学、研究所和商业公司)。目前比较有影响的开源系统安全测试工具软件有两类，一类包括Secure software公司的Code Assure工具和Ounce Labs开发的Prexis工具，这两种工具能通过分析找出各种可能的安全隐患，生成详细的漏洞报告，同时指导用户如何防范；另一类包括最著名的开源社区Sourceforge提供的BogoSec工具，它能扫描全部代码并给出一个安全指标数值，从而近似地反映代码的总体安全质量，也可以使用多个独立的扫描程序对源代码进行扩展扫描，生成高级评测结果，帮助开发人员和用户从安全角度对源代码的质量进行比较判断。

3.4 软件升级维护的困境

任何用户都可以自行对开发源代码软件进行二次开发应用，这是开源软件的一大优势。但不利的是，用户的自行修改总不得不跟随着原来软件的升级而反复进行，否则就可能失去新版本的许多新功能，同时继续承受着旧版本可能的安全性威胁。新旧版本的更替不可避免地会带来用户的修改工作量。

相应对策是主动及时升级软件。软件升级包括了功能上的增加和改进以及安全性修正。得到广泛使用的开源软件有很大一部分用户是商业用户

和政府组织，他们发现的问题会及时发布，而且还会提交解决方案。主动及时对软件升级变化和信息发布进行跟踪，对保持更新同步是非常重要的。

3.5 系统的安全性依赖于系统的具体实现

安全理论与具体实践总是存在着一定距离的。受制于计算机的现行体系结构、计算资源和运行规律的束缚，不可能完美地实现安全算法的所有细节，只能用有限的手段来接近无限的理想结果。例如在设计安全系统时总是假设可以产生完全意义上的随机数，但实际上计算机至今还没有能力产生那样的随机数。

相应的对策是增加额外的安全方式。开源操作系统允许用户或企业采取任何合适的方式加强系统的安全性。例如在Linux中用户就可以根据对安全性的需要建立自己的系统内核。很多安全访问控制模型和框架已经被研究和开发出来，用以增强Linux系统的安全性，比较知名的有POSIX.1e capabilities，安全增强Linux（SELinux），域和类型增强（DTE），以及Linux入侵检测系统（LIDS）等等。目前Linux安全模块（LSM）作为一个Linux内核补丁的形式提供了一个轻量级通用访问控制框架，它使得上述各种的安全访问控制模型能够以Linux可加载内核模块的形式实现出来，用户可以根据其需求选择适合的安全模块加载到Linux内核中，从而大大提高了Linux安全访问控制机制的灵活性和易用性。Linux安全模块也很有希望进入Linux 2.6稳定版本，被Linux内核接受成为Linux内核安全机制的标准，在各个Linux发行版中提供给用户使用。

4 结论

开源软件是否安全可用，最终取决于开放源码这种形式是否安全。如系统本身不安全，开源软件的可用性就将大打折扣，再奢谈其他问题也就毫无意义了。开源软件自诞生之日起就一直非常活跃地发展变化，其安全性能的提升也受到了极大的关注，成为变化焦点之一。开源软件安全性能在众多开发者的推动下不断完善，促进了开源软件在更大领域的广泛应用。

参考文献：

[1] 孟祥宏．开源软件技术安全性研究[J]. 信息网络安全，2007年7期．

[2] 梁洪亮，王旭．开放源码引发安全争议[J]．电子商务，2003.7.

[3] Gary McGraw，John Viega. Make your software behave: Security by obscurity [EB].http://www.ibm.com/ developerworks/ library/s-obs.html?S_TACT=105AGX52&S_CMP=cn-a-os.

[4] 赵亮．如何增强Linux系统的安全性[EB]．http://www.ibm.com/developerworks/cn/linux/l-lsm/part1/index.html.

作者简介：李昕（1969—），女，在职硕士研究生，副教授，主要研究方向是计算机网络、电子商务。

收稿日期：2007-11-07

蓝代斯克推出新版本的IT管理解决方案8.8

为了更有效地帮助全国各地的企业用户简化和高效率管理日益复杂的IT系统，提高IT系统的价值、增强其安全保障，全球领先的系统、安全和业务流程集成管理解决方案提供商蓝代斯克软件公司（LANDesk）正式向中国市场推出最新版本的IT管理解决方案8.8以及最新版本的LANDesk主机入侵防御系统、LANDesk应用程序虚拟化系统和LANDesk防病毒系统。以更强大更实用的功能，帮助企业机构更轻松、更高效、积极主动地管理IT系统。

蓝代斯克隆重上市的LADNesk IT管理解决方案8.8升级产品，是蓝代斯克旗舰产品的最新版本，包括LANDesk管理套件、LANDesk安全套件、LANDesk服务器管理器、LANDesk补丁管理器、LANDesk手持设备及嵌入设备管理器等这些已在中国市场上获得成功推广应用的产品的最新版本。LANDesk管理套件8.8新增了创新的实时软件分发、许可证监控、报警、配置及报告等工具，帮助客户更容易地保护和管理企业级系统，实时分析IT投资回报；LANDesk安全套件8.8提供了诸多创新功能，包括新的数据泄漏防护和无线接入点发现功能，并进一步增强已有功能，如对补丁管理、主机入侵预防（HIPS）和其他企业级功能都做了进一步的增强，帮助企业用户更有效地提高系统安全性；LANDesk主机入侵预防系统是一款基于行为的安全监控、警报及补救解决方案，比传统的反病毒软件更胜一筹，可以根据系统行为来保护计算机，防范越来越多的零日威胁、高危险的rootkit病毒及其他恶意软件基于行为的安全监控、警报及补救解决方案；LANDesk应用虚拟化系统能够帮助用户能够无缝地部署虚拟化应用软件，带来了全新的软件分发模式。

据悉，从3月25日开始，蓝代斯克将在全国18个城市举办主题为“点击之间，掌控万端”的蓝代斯克IT管理解决方案巡展活动，全方位展示蓝代斯克先进且实用的IT系统和安全管理解决方案，零距离与区域用户沟通，为区域用户提供更有效的服务。