关于计算机软件安全检测技术的研究重点分析

张绍龙
（西安职业技术学院　陕西　西安　710072）

摘　要：随着时代的不断进步人们对计算机的应用越来越广泛，随之其安全问题也是人们一直关注的焦点。计算机软件安全漏洞，指的是在电脑内部软件中出现安全风险，如不能及时对其加以补救，就会造成计算机信息损失。本章将首先阐述计算机软件安全漏洞的分类，及其进行计算机软件内部安全检查工作的基本原则；然后，对计算机安全测试技术做出了详尽的分析，给出了开展计算机安全测试技术工作的具体对策。
关键词：计算机软件；安全检测技术；研究重点

Analysis on the Key Research Points of Computer Software Security Detection Technology

Zhang Shaolong
(Xi ' an Vocational and Technical College, Xi ' an, Shaanxi 710072)

Absrtact: With the continuous progress of the times, people use computers more and more widely, and its security is also the focus of attention. Computer software security vulnerabilities refer to the security risks in computer internal software, which will cause computer information loss if they cannot be remedied in time. This chapter will first describe the classification of computer software security vulnerabilities, and the basic principles of internal security inspection of computer software; Then, it makes a detailed analysis of computer security testing technology, and gives the specific countermeasures to carry out computer security testing technology.
Key words: computer software; Safety detection technology; Research focus

在应用的进程中，必然都会面临着计算机软件安全性问题，为保证计算机系统的正常使用，就必须进行病毒攻击防范措施，有效维护计算机软件的信息安全，这也是目前在计算机软件开发进程中十分关键的问题。为保证顺利使用计算机软件，必须全面注意计算机软件的安全，以防止在运用计算机软件过程中，遭受各种问题的冲击。也只有通过全面研究计算机软件安全情况，并针对具体问题提出更完善的防护方法，才能够逐步改善计算机软件的安全。

一、计算机软件的安全问题

（一）设备管理问题

软件研发工作毕竟还是要依靠于计算机的硬件设施上面，而在正常工作时基础设施的管理工作也是如今大部分公司比较重要的，安全问题。主要是由于硬件时代性跟不上环境的迅速变化，近些年大部分公司实体计算机的操作系统都由 Window7 转变为 Window8 再到了 Window10，但部分公司并未针对操作系统做出重大改变还是采用了老旧的基础设施，在简易性和安全层面都滞后于时间，而只是抱着一个自以为没有会攻击“老古董”的心理从事基础设施管理工作[1]。另外，在故障处理领域，老旧器件的长时间应用本就会导致电路老化，突然死机等现象，而失效后使用的相关材料会慢慢被人废弃，需要继续进行更新就比较麻烦。

（二）系统漏洞问题

计算机软件问题，在计算机软件研发与使用过程中有着相当广泛的普遍性，而且往往很易被掌控和规避，这就要求了计算机软件企业在其研发过程中，必须对于系统的正常运行和管理有着高度的要求，而有些较为特殊的技术需求往往会导致企业在具体的软件开发过程中，发生了难以预测的系统漏洞现象。所以，系统漏洞现象作为计算机软件中较为重大的安全问题，极大地干扰了客户的应用感受，也对于在工作过程中，对于整个计算机系统的正常运行产生了不同程度的阻碍，而且系统漏洞的出现还将严重危害使用者的个人资料和客户的隐私权。随着技术的发展，现阶段针对各种入侵形式的杀毒软件及其防火墙系统不断涌现，而具体的攻击方式及其威胁类型也会相应发生变化，必须在实施的进程中，持续地加强对其的研究和保护[2]。

二、计算机软件漏洞的产生原因

在电脑系统运行流程中，电脑操作系统漏洞一般具有以下的一些特点，细节特征包括：(1) 电脑操作系统实际上只是由一些个程式构成，在程式的编写流程中，程式员自己原因造成的代码编写出错，让程式产生逻辑性出错，就可以产生渗漏，这属于他人各种因素造成的软件安全渗漏。(2) 在电脑管理系统的运作流程中，程式可以产生逻辑性问题，而逻辑性问题一经发生，操作系统一旦无法有效地复原，就会使其相关程序也遭到了伤害，从而提高逻辑性问题的出现几率。(3) 计算机软件在使用的整个过程中，也会受到使用环境的影响，一旦操作系统本体出现出错，就可以连带操作系统里面的一些计算机软件受到负面影响，进而增大信息安全渗漏[3]。(4) 系统漏洞和使用期限之间有着必然的联系，但由于操作系统使用期限的增长，当部分缺陷得到修补的时候，还可以产生一些另外的缺陷。

三、计算机软件安全检测基本概念

计算机软件的安全性能主要形成于整个计算机软件研发流程中，是整个计算机软件研发流程中的一项关键过程。通过计算机软件的测试，技术人员对程序的软件安全性有了更加充分的认识与掌握，尤其是可以及时发现程序中出现的问题与安全隐患，以便及时采取措施加以解决，提升程序安全性质量。这些办法，能够有效减少软件开发项目所存在的市场风险，提升效率，确保效益。必须指出的是，计算机软件安全性检测只能解决在应用软件程序中出现的有误，更确切地说，应用软件安全检测只有发现错误，无法解决出错。而按照测试所采用的原理，将计算机软件安全测试又分为静态检查与动态测试两类。计算机系统软件系统的可靠性测试，作为软件开发项目品质管理中的重要一环，作用一点就是提升软件开发项目实现后的主要功能和系统设计总体目标之间的统一性。从实践工作角度来看，计算机软件安全测试主要包含了三部分内容，依次为功能测试、渗透检测以及认证过程。计算机安全软件测试和他人检查应用软件之间主要的区别就是，计算机软件安全测试的主要目的是用来避免目标应用软件为超过系统设计范畴工作，而他人试验则关注于应用软件的设计任务[4]。

四、计算机软件安全检测中的注意事项

一是要制定测试方法，以确保测试方法、基本原理、流程的科学化、合理化，以及结论的实效性。同时科技人员也要全方位、深刻地掌握计算机软件设计要求和特点，根据具体环境选用合理的、科学的安全测试方式，并认真制订与之相应的、标准化的测定方法。严格执行，保证了测试成果的安全、合理。同时，承担应用软件安全测试工作的科技人员应当掌握比较全方位的应用软件安全测试理论知识和丰富的实践经验，在具体实施应用软件安全测试时，还必须有软件设计技术人员的参加，以确保安全测试产品质量。

二是做好计算机软件安全性检测环节中的数据分析工作。软件系统安全性检测是一个相当复杂的项目，软件信息越多，架构越是复杂，这阶段的数据分析压力和复杂度也就越来越大，必须针对具体情况做好代码级别、操作系统层级和应用级程度的数据分析。在每一阶段的研究中，都要有针对性地选用适当的研究方法，保证研究结论的可靠性。测试技术与监测方法是开展计算机软件安全监测时需要注意的二个因素[5]。

五、计算机软件安全检测的主要技术

（一）形式化检测技术

形式化测试技术，指的是在对计算机系统软件开展安全测试项目时，从现有的形式化标准上进行，通过对计算机系统软件进行分析与检验，从而测试出计算机系统软件的安全是否符合标准。在通过表现手法检测技术对计算机系统软件实施安全测试技术之前，一定要具备适当的规则化的形式语言，以保证表现手法检测技术在应用的环境中具有标准内容。值得注意的是，表现手法检测技术只是一个炎症性的测试方式，及时使用表现手法测试技术并不能测试出计算机系统软件中的安全问题，更不能判断计算机系统软件中并不存在安全问题。

（二）动态的软件安全漏洞检测技术

当对计算机软件的安全漏洞进行测试后，技术人员利用动态的检测工具，在不修改计算机系统源代码、二进制程序的前提下，对计算机系统内的所有软件程序进行了安全测试。在对动态检测技术进行使用时，必须根据软件进程的实际工作条件而做出适当的调整 ；但必须注意的是，在对动态检测技术进行使用后，可能会导致计算机软件中产生新的安全漏洞，但如果经过测试后的计算机软件中仍出现了安全隐患或缺陷，势必会对计算机的使用体验造成影响[6]。

（三）静态安全检测

静态安全性测试，是指针对计算机系统的内部结构所进行的安全性测试，研究计算机系统内部结构的可靠性和安全漏洞相互之间所具有的一些相似性和特征方面的相同度。计算机软件缺陷一般包括安全漏洞和错误内存性缺陷，安全漏洞一般是数据流出现的错误差别，而出现这个区别的一般是错误内存形态。而内存性泄漏则大多是由于信息本身的类别、准确性等存在问题而造成的，在检测此类泄漏时，重点是为其在存储空间中构建模块，并进行对程序代码的静态扫描，而分析时主要面对的则是程序代码的关键语句。在该检查方式下，系统程序被包含了多种不同语言，并经过对各种编程语言和数据库系统之间的有效性比对，确定编程内容中是否出现了数据错误，从而实现一定的检查目的。静态检查技术一般是在应用软件编程的帮助下，负责对应用软件编程里面的有关代码加以检查，比如源代码、二进制代号等的代码，一旦代码中出现了数据异常，就可以诊断为应用软件安全漏洞。静态测试技术下的漏洞判断标准，是测试代码的漏报率和误报率，一旦漏报率明显降低，就会出现在误报率的基础上。静态测试技术，主要是对软件程序整体情况所进行的测试，它并不能精确测定其关键特性，在测试时必须确定被测试的程序不处在正常工作状态。

（四）故障注入检测技术

故障注入测试方法主要是指利用计算机系统软件的故障模式，来在计算机系统软件中输入故障，从而使系统软件中出现的潜在安全问题快速地出现，从而完成了对计算机系统软件的安全测试任务。虽然故障注入分析方法是通过逆向分析的方法，采用引入事件的方式来诱导计算机系统软件中的安全问题出现，并对安全问题加以监测与处理，不过在具体的操作过程中，技术人员必须充分证明故障注入的正确性，防止计算机系统软件中出现更大的安全问题，从而给使用者产生严重损失。

（五）反病毒技术

计算机病毒的危害性也无须过多介绍，但近年来中国大学校内网络中的勒索病毒，还有中国知名的熊猫烧香等病毒，都已经给社会经济带来了重大负面影响。而现在主要使用的反病毒技术则为主动内核技术，是通过对操作系统内部进行修复，从而将反病毒技术变成了操作系统的底层模块，只要计算机开始正常工作便可以不停地检查病毒，而此技术也需要操作系统、网络、软件与硬件之间的无缝连接，也是未来反病毒技术的主要发展趋势，但是由于现阶段其主要技术核心已被专门设计操作系统的公司所掌握，实际效果与模块架设方式尚不明朗。还有代码辨识技术，是指现代社会运用大量的数据信息将病毒代码进行了特征辨识后，在扫描过程中通过比较代码的可疑程度，从而进行反制，利用此技术就必须构建起强大的数据库系统。

六、全面提高计算机软件安全性能质量的有效方法

（一）合理选择检测方法

在电脑安全测试的应用中，技术人员必须要熟悉应用软件的性质和种类，而后再针对应用软件的特点和作用选用较为适宜的安全测试。此外，管理人员在测量时，必须要具有应对突发性事故的意识，测试过程中如果出现突发事件工作人员必须及时对测试做出相应的改变，由此才能保证测试得以高效地实施。管理人员必须要重视训练自身的专业意识和专业技能，只有员工具备较好的专业技能素质在操作时才能保证没有出现人为失误，进而改善测试质量。安全测试人员要想良好的适应这项工作，就一定要增强自己的开发意识，如此可以使自身具备很高的程序开发水平以及相应的开发基本功，只有技术人员具备上述特点才能够针对程序的不同找到合理的测试方式，如此才能够大幅度地提高软件的安全测试技能。

（二）利用系统进行分析检测

技术人员在检查软件系统的过程中，一定要全面地考虑到软件系统出现的相关情况，并针对实际情况做出针对性的安全性检查。使用这些检查手段可以有效地找到软件中出现的缺陷和安全隐患，同时这些方法可以改善系统性的软件使用性能。要想让系统可以有效地对软件进行管理和检查，相应的人员必须要加深系统的认识，并且要了解系统的特点，进而采用科学的方法对软件和检查体系加以更新和优化，由此来改善检查成果。

结束语 ：

综上所述，由于计算机与社会生活、发展的联系日渐紧密，使计算机软件的安全问题被大众所重视。而为使计算机软件的安全性得到提高，需要对软件的安全漏洞进行必要的检测。同时，为进一步提高检测技术的应用效率，需要对其进行更为全面的分析与探究。

参考文献 ：

[1] 李世庆 . 计算机软件安全检测技术探讨 [J]. 信息技术与信息化，2021(5):172-173.

[2] 孙涛 . 计算机软件安全检测技术探讨 [J]. 科学与信息化，2021(6):63.

[3] 丁文才，韦正超，阳江，等 . 关于计算机软件安全检测技术探讨 [J]. 电脑知识与技术，2021，17(2):40-41.

[4] 卢艳静 . 关于计算机软件安全检测技术探讨 [J]. 软件，2022，43(8):104-106.

[5] 韩敬峰 . 浅析计算机软件安全检测技术 [J]. 福建电脑，2021，37(1):170-171.

[6] 余鹏 . 计算机软件安全检测技术的分析与应用 [J]. 现代信息科技，2019，3(3):154-155.

作者简介 张绍龙（1980.9-），男，汉族 ，河南淅川人，硕士，讲师，研究方向 ：计算机技术、软件工程