计算机软件安全检测技术探究

王建华

国核信息科技有限公司

[摘　要]伴随着科技的快速发展,计算机开始成为人类生活和社会生产各领域中极其重要的工具,可以有效提高人们的生活质量和学习效率。所谓计算机软件安全检测,就是保证计算机软件工作正常、安全运行的重要基础保障。本文从计算机的安全检测技术着手,根据可能对计算机产生威胁问题深度分析,最终提出安全检测技术策略的运用,以供参考。

[关键词]计算机;软件安全;检测技术

【DOI】10.12252/j.issn.2096-6288.2020.04.1292

计算机在工作生活中的大量使用为人们提供了便利,软件的不断研发使其呈现多元化态势,软件功能的涉及范围很广,大体有商业用途与私人专用两类,不管计算机软件的功能如何使用,都大幅度地提升了生产工作的效率,同时加快了计算机的改进步伐。但与此相对应,计算机软件的大规模使用令客户的信息安全遭到破坏,隐私与安全大大减少,因此针对软件系统制定规范的制度与检测标准,才能实现计算机软件未来的安全性发展。

一、计算机软件安全检测技术的必要性

对计算机中的软件进行安全检测的目的就是防止计算机遭到病毒的入侵,确保用户的个人信息得到保护,计算机中涉及到的财产也有相应的保障,在目前软件泄漏私人数据频频发生的时期,计算机的安全检测发挥着关键作用,只有通过有序的检测,才能发现计算机使用过程中的缺陷,在与标准进行对比后及时修理,分析后续数据的稳定性。

二、计算机软件安全检测的主要技术

（一）形式化检测技术

形式化检测技术主要采用了有限状态语言和动作语言,通过在软件数字模型中增加状态语言功能,软件的规格说明就可以以更加形式化的方法加以说明,在实际应用的过程中,不但要进行基本定理的证明,而且还要进行模型的检测。通过形式化检测我们可以得知计算机的安全性能是否符合计算机的运行标准。利用模型检测方式,把软件系统的特性有效地用逻辑表达,进而可以利用状态空间搜索来检测软件安全特性。

（二）随机检测法

随机检测法具体是指,在计算机软件展开安全检测环节,对有可能出现的安全隐患进行排查,如果随机检查的数据表明计算机存在安全隐患,计算机会迅速的将系统内的信息进行加密,从另一方面来看,这样能够大大提升计算机的系统安全性,在一定程度上可以防止电脑病毒对计算机的破坏。就当前的计算机杀毒发展状况而言,目前一般的杀毒都是采用了计算机安全检测的随机检测技术,在采用安全软件之前,用户就需要确定好自己的使用参数。在一个计算机里最好只设置一次杀毒,而若是在一个人使用的计算机里同时下载或安装了多个病毒查杀软件,那样就会让计算机的运行速度明显地降低。与此同时,计算机用户在使用计算机时,必须定期对病毒查杀软件进行升级,养成更新安全检测系统的习惯,保障安全检测系统充分发挥其自身的保护作用。

（三）故障注入检测技术

故障注入检测技术是运用了逆向保护的方式,对计算机系统进行高速且有效的保护,在计算机的运行过程中,把故障写入计算机系统,从而达到测试目的,判断计算机使用环境是否安全。该技术应用能够彰显检测技术智能化特色,对于软件安全领域检测技术开发中也有着一定重要性,可以更迅速地判断软件实际使用时,会不会存在安全漏洞和使用风险,并对其中存在的漏洞进行技术处理以更全面的提高计算机软件的故障风险抵抗能力,进而更大幅度的改善计算机软件的总体安全特性。

三、全面提高计算机软件安全检测技术的有效措施

（一）合理选择检测方法

在实际的计算机安全检测技术的使用过程中,相关的技术人员需要对软件的类型进行详细的了解,然后根据软件的功能以及性能来选择适合的安全检测技术。同时,技术人员还需要根据检测过程当中的各种突发情况,进一步的对安全检测技术进行一系列的调整。为了能够更好的完成这一项工作,这样才能更好的找出科学的检测方法,最大限度的提升安全检测技术在计算机软件检测过程中的使用安全性和有效性。

（二）利用系统进行分析检测

在进行软件安全检测的过程当中,相关的技术人员还要充分的考虑软件系统的问题,对各种软件问题进行安全检测。通过这样的方法不仅能够及时的掌握软件当中存在的各种问题和漏洞,同时也能够提升系统的使用有效性。为了能够更好的利用系统来完成计算机软件的分析和检测,相关的工作人员必须要不断地加强对系统的了解,并采取有效的措施不断的对软件和安全检测技术进行优化,这样才能够取得更好的检测效果。

（三）提高专业人员的素质

在计算机软件的安全检测过程中,所有的工作都是由安全检测技术人员来进行。因此,相关部门必须提高对安全检测人员的要求,不断的提升安全检测人员的整体素质和工作水平。这样才能够更好的完成计算机软件的安全检测任务,从而有效的提升计算机软件的整体安全性。为了能够使安全检测人员更好的适应各种全新的安全检测技术,相关部门需要定时的为安全检测人员安排一系列的专业化培训,并在培训的过程当中不断的培养安全检测人员的突发事故应急处理能力。当然,相关部门还可以在内部推行良性的竞争机制,最大限度的激发安全检测人员的工作积极性和工作热情,这样能有效的提升计算机软件安全检测的整体效率和水平。

结束语:

在人们对计算机软件要求不断提高的当下,计算机软件的类型越来越复杂,各种源代码的不断增加使得相关的工作人员在进行软件维护时很难兼顾所有问题。在这种情况之下,计算机软件很容易出现各种形式的安全漏洞,这无疑降低了计算机软件使用的安全性。软件是计算机使用过程中不可或缺的重要组成部分,是计算机得以正常运行的基础。为了保证计算机的使用安全性,相关部门应加强计算机安全检测技术的研究力度,不断推新一系列的计算机安全检测技术,从而为计算机安全检测技术的全面发展奠定良好基础。

参考文献:

[1]张飞.计算机软件安全检测技术探究[J].信息与电脑(理论版),2016.01.180-181.

[2]刘露.浅议计算机软件安全检测技术[J].数字技术与应用,2016.05.204.

[3]贺岚.计算机软件安全检测技术及相关问题研究[J].信息与电脑(理论版),2016.21.40-41.