计算机软件安全检测存在的问题及方法

聂闻华

国立台中科技大学，台湾

摘要：针对计算机软件安全检测问题，本次研究结合我国计算机软件安全检测技术的发展现状，首先对软件安全检测存在的问题进行系统分析，在此基础上，对计算机软件安全检测实现方法进行全面研究，为推动我国计算机软件安全检测技术的发展奠定基础。研究表明：对于我国计算机软件安全检测技术而言，主要存在缺乏综合分析框架、多元化检测人员不足以及检测方法滞后等问题，常见的计算机软件安全检测方法有静态检测方法、动态检测方法以及故障注入检测方法等，通过完善网络安全系统，有利于推动我国计算机软件安全检测技术的进一步发展。

关键词：计算机软件；安全检测；问题分析；方法研究；动态检测

在使用计算机软件的过程中，安全检测技术十分关键，对软件进行安全检测的主要目的是帮助用户在使用软件的过程中规避各种类型的风险问题，最终保障计算机系统以及用户信息的安全性，目前，计算机领域的相关技术已经取得了较大的发展，同时，各种类型的软件威胁问题也逐渐显现，软件使用过程中的安全隐患风险提升[1]。针对该种类型的问题，本次研究主要是对目前软件安全检测领域存在的问题进行系统分析，提出软件安全检测的实现方法，为推动计算机软件安全的进一步发展奠定基础。

1 计算机软件安全检测存在的问题分析

（1）缺乏综合分析框架

对于各种类型的计算机软件而言，在使用的过程中可以充分发挥其特点，最终的目的是满足用户的各种需求，在对软件进行检测的过程中，需要从综合性的领域出发，对软件使用过程中可能存在的问题进行全面的分析，同时，还需要根据软件的基本特点，对其检测方法进行合理选择。在另一方面，各种类型的计算机软件已经经过了大量的更新，因此，在对其进行检测的过程中，也需要对检测形式进行一定的更新，以此防止软件检测过程中出现局限性问题。在检测工作开始之前，需要制定合理的检测形式，检测形式的制定需要结合软件的基本特点以及使用时间，此时才能全面提高软件检测的准确性[2]。

（2）多元化检测人员不足

软件检测工作的专业性较强，对于检测人员的要求相对较高，检测人员需要完成的工作项目也相对较多，例如需要进行安全分析、质量检测等，事实上，如果只依靠相对较为单一的检测内容，很难对软件进行准确的检测，针对该种类型的问题，需要对软件安全检测的团队进行合理的配置。通过对目前我国软件检测人员进行调研发现，大多数检测人员掌握的相关知识相对较为单一，部分检测人员的工作经验不足，这严重阻碍了软件检测领域的发展，同时，在进行软件检测的过程中还容易引发其它类型的问题。在另一方面，软件检测工作相对较为灵活，检测流程也相对较为简单，但是对于检测人员而言，对于自身的工作内容并没有正确的认识，检测过程中的监督措施也严重不足。

（3）检测方法滞后

通过对软件检测方法进行调研发现，大多数的检测方法相对较为固定，软件检测工作还需要对软件进行合理的更新，但是在软件更新的过程中，也缺乏有效的保障性措施，尽管用户在使用软件的过程中对于软件的认可度相对较高，但是在软件更新以后，由于缺乏保障性措施，会导致出现多种类型的问题，最终使得用户对软件的认可度降低。在另一方面，在进行软件检测之前，工作人员需要对软件进行全面的分析，

并根据软件的特点以及用户的需求，制定合理的软件检测解决方案[3]。

2 计算机软件安全检测实现方法研究

（1）静态检测方法

所谓的静态检测方法主要是使用各种类型的程序分析方法，对软件的代码进行全面的检测以及分析，最终发现软件代码中存在的问题，事实上，静态检测防范的分析形势也可以分为三种类型，分别是类型推断类型、约束分析类型以及数据分析类型，通过使用不同类型的分析形势，可以对代码中潜在的问题进行筛选。该种方法使用相对较为便捷，但是，该种方法在使用的过程中也存在一定的局限性，问题筛选的过程中存在一定的盲区。

（2）动态检测方法

在使用动态检测方法的过程中，需要对计算机的运行环境进行充分的利用，最终实现软件数据深度分析的目的，同时，还可以对计算机运行过程中的问题进行合理的判断。事实上，该种类型的方法主要是对软件的运行环境进行检测，应用过程中的优势相对较多，但是，在使用该种方法的过程中，需要对计算机的源码进行一定的更改，以此确保计算机的运行状态不会出现较大的变化，计算机中大量的数据信息也不会受到影响，由此可见，使用动态检测方法的安全性相对较高。

（3）故障注入检测方法

对于故障注入检测方法而言，其需要使用软件多次故障问题时间间隔的最小值，对软件使用的寿命进行判断，一般情况下，计算机软件的使用寿命都相对较长，但是软件在出现故障问题以后，其使用寿命必然会受到严重的影响，同时，故障问题还会影响计算机的元件以及硬盘，在计算机出现死机问题以后，其软件必然无法正常运行。通过使用故障注入检测方法，可以对软件出现风险问题的概率进行估算，对常见的软件故障问题进行分类分析，以便工作人员可以制定针对性的措施，全面保障软件运行的安全性。

（4）完善网络安全系统

完善网络安全系统的方法相对较多，常见的方法为数据加密、安装杀毒软件以及使用防火墙。在数据加密方面，大量的软件中含有数据信息，在数据信息出现泄漏问题或者数据缺失的前提下，软件将无法正常使用，通过对数据进行加密，可以有效保障软件长期处于正常运行状态。在杀毒软件方面，大量的病毒会潜藏在软件中，病毒的存在也会对软件运行产生影响，因此，需要在系统中安装杀毒软件，定期对杀毒软件进行更新，这也是保障软件安全的重要措施。在防火墙方面，其主要的目的是防止软件的代码被恶意篡改，通过使用多样化的安全技术，并制定科学的安全防护方案，可以有效推动软件安全的全面发展。

3 结论

综上所述，用户在使用计算机软件的过程中，可能会出现大量的安全风险问题，这就需要全面加强软件的检测工作，目前，我国在软件检测领域已经取得了较大的发展，但是仍然存在一定的问题，因此，需要对软件安全检测方法进行更新和完善，并建立网络安全系统，全面确保软件的安全性。

参考文献

[1]孙互平.目前计算机软件安全检测存在的问题及处理方法探讨[J].电子技术与软件工程,2013(18):108.

[2]孙海松.关于计算机软件安全检测存在问题及措施的研究[J].网友世界,2014(04):1-2.

[3]王璟.计算机软件安全检测中存在问题及防御对策[J].计算机光盘软件与应用,2014,17(23):62+64.