试论计算机软件安全漏洞检测技术

庄义曼
丰县人力资源和社会保障局　221700

[摘　要]随着信息技术的进一步应用，我国各个领域实现了信息化发展，并且应用程度在不断加深。在这样的发展背景下，信息系统的安全性成为人们广泛关注的话题，以此强化企业生活活动的安全性。基于此，本文就以计算机软件安全漏洞监测技术为研究内容，深入分析了当前计算机软件安全漏洞产生的原因以及带来的威胁，之后阐述了安全漏洞的特点，最后就计算机软件安全漏洞检测技术进行了总结，以期能够促进提升计算机软件的安全性。

[关键词]计算机；软件安全；漏洞监测技术
【DOI】10.12252/j.issn.2096-6288.2021.11.1045

前言

现阶段，计算机在各个领域中的应用程度越来越深入，其安全性能也受到广泛地关注，一旦存在漏洞出现问题，便会影响计算机系统的正常运行，进而影响人们的生产活动。同时，在计算机系统应用的过程中，也出现一些安全漏洞问题，给人们带来损失。在这样的大背景下，安全监测技术人员需要深入研究有效避免计算机系统出现安全问题的技术，减少或杜绝安全漏洞和安全隐患。

一、计算机软件安全漏洞的形成原因

计算机软件存在的安全漏洞很难从根本上消除，只能在实际使用过程中，及时发现漏洞，并进行修补。计算机软件安全漏洞形成的主要原因可以分为以下几种情况：其一，计算机软件的研发过程，涉及的人为因素比较多，需要进行大量的计算，因此，不可避免的会存在一些计算性错误，如果没有进行修正，就会在计算机软件中形成安全漏洞。其二，在计算机软件研发的过程中，也会存在一些逻辑性错误，当软件中的逻辑程序越复杂时，其出现安全漏洞的概率就会提升，进而导致计算机软件形成安全漏洞。其三，在计算机软件运行的过程中，如果环境发生变化，与可能会诱发安全漏洞。结合这三点原因可以得出，计算机软件中的安全漏洞难以实现一劳永逸，只有在使用过程中注重检测，及时发现、及时解决。

二、软件安全漏洞给计算机带来的威胁

在实际的应用中，计算机已成为企业重要信息的储存和传递工具，直接影响企业的正常经营。在这样的背景下，计算机的使用必须注重安全性和稳定性。但是就基本特征上来看，计算机软件本身就存在一定的危险性和脆弱性。除此之外，计算机软件漏洞存在的敏感性，使其在整个系统中表现出较强的攻击性，会对整个计算机系统的正常运行造成影响。通常情况下，人为操作的影响或其他因素会给计算机软件带来一定的影响，导致安全漏洞的形成，要么形成功能性的漏洞，要么形成安全性的漏洞。与功能性漏洞相比，安全性漏洞所引发的安全威胁更具代表性。计算机软件出现安全性漏洞时，会发出错误指令，其中含有恶意代码等，也是人们经历的主要的计算机安全问题。随着计算机软件技术的深入应用，网络安全性也受到了极大的关注，成为计算机发展过程中的重要课题内容。然而不容忽视的是，依然有部分计算机用户忽略计算机软件的安全，导致计算机出现多种多样的软件安全漏洞。针对这些问题，我们需要从最基础的部分入手，全面提升计算机安全监测技术，以此提升计算机软件的安全性能。

三、计算机安全漏洞的特点

（一）受人为因素影响较大

通过分析近年来发生的计算机软件安全问题，不难发现大部分安全问题是由于人为因素引起的。而其中大部分是不法分子借助自己研发的技术，对计算机软件系统施行的攻击和破坏，以此达到他们的不法目的。但是，从根源来看，还是由于软件研发过程中，软件程序存在问题，导致代码编程中存在逻辑性错误，进而给不法分子制造了实施破坏的机会。从问题的出现，到安全问题的形成，无处不体现着人为因素的作用。因此，在计算机软件安全问题方面，程序研发人员需要注重提升自己的研发技能，提升编程的逻辑性，避免给不法分子提供可攻击的机会。

（二）应用中融入出现逻辑性错误

数据处理工作是计算机软件应用中的重要内容，而这部分工作容易造成计算机软件出现逻辑或计算的错误。当计算机软件出现数据或逻辑性错误时，往往是应为存在一些不合理的模块。在这样模块中，中等模块出现错误的概率比较小。比如，如果数据库的压缩软件库ZLIB中的库中代码解释的长度大于1，那么就会导致漏洞，容易引发安全问题。

（三）漏洞难以从根本上消除

在应用计算机软件的过程中，一旦发生安全漏洞问题，技术人员需要进行及时地修复，避免计算机系统受到黑客或者病毒的攻击，对计算机的安全性造成较大的影响。同时，计算机一旦受到黑客或者病毒的攻击，便需要进行及时地修复。然而其修复工作存在一定的难度，此外修复的过程中，还会引发新的安全漏洞问题。因此，计算机软件漏洞安全问题存在的时间比较长，而且修复难度比较大，难以从根本上解决这些问题。这就需要人们在日常使用计算机的过程中，注重做好病毒监测和防控工作，一旦发现问题需要及时开展修复工作，避免出现其他的漏洞，对计算机软件系统造成严重影响。

四、计算机软件安全漏洞检测技术

（一）动态化检测中的非执行栈

由于操作系统中的栈能够在应用过程中被执行以及其具有可写性，使其存在可改变的特性，进而导致在计算机软件使用过程中，存在着被攻击的可能，为安全漏洞的形成提供了环境。例如：若计算机内部环境不变，攻击人员可以将恶意代码编写进栈中，改变计算机软件原来的程序，恶意代码会在系统中寻找可以破坏计算机软件的突破口，以寻找攻击计算机软件系统的可能性，进而形成安全漏洞。为此，针对这一漏洞，计算机软件研发人员需要在软件编写的过程中，改变栈的代码形式，使其处于不可被执行的情况中。经过大量的实验和实践得出，这一方法具备较强的可行性，能够极大的降低恶意攻击者随意编写计算机软件程序的能力，进而为计算机软件的运行创造良好的环境，以此达到保护计算机软件系统的目的。

（二）动态化检测中的内存映射

在提升计算机软件安全性的工作中，字符串的有效应用起着关键性的作用。通常情况，计算机软件攻击者会使用“NULL”字符作为恶意攻击的结尾，再借助覆盖内存页的形式给计算机软件造成安全漏洞。结合这一情况，漏洞监测技术，可以通过有效控制字符串，应用内存页的映射方式，使内存页跳转至较为简单的区域，提升计算机软件的安全性能，同时需要攻击者具备较强的计算机技术才能突破这一防御，进而提升计算机软件系统的安全程度。与此同时，安全检测人员可以在不同的计算机地址中随机输入映射，加大恶意攻击者的猜测数量，使他们难以瞄准真正的攻击目标，提升计算机系统的安全性能，降低恶意攻击者对软件运行造成不良影响的程度。

（三）动态化检测中的沙箱方法

防火墙是计算机安全防护的重要措施，而沙箱技术则是一种通过构建限制方面的隔离墙实现抵挡恶意攻击的目的。在实际的防御应用中，沙箱技术表现出来的优势在于其没有改变原有的软件程序代码，只是针对外来信息进行隔离，通过抵挡外来信息，为计算机软件营造良好的内部运行空间，屏蔽恶意攻击的同时，保证计算机内部的兼容性。例如：C语言中一般不会涉及调动函数，但是若果在安全检测中，发现软件中存在着某种调动函数，则可以推断出计算机正在遭受某种攻击，此时可以借助沙箱的方式，屏蔽这一调动函数，提升阻隔的针对性。通过借助沙箱技术，计算机软件系统能够保证运行的平稳性，同时也能够免受外界的攻击。

（四）动态化检测中的安全共享库

信息共享是当下计算机软件技术发展的必然方面。在实际应用过程中，共享数据库会处于相对开放的状态，提升计算机软件系统的开放性，以此实现数据的传输和接受，在这一过程中，如果计算机的安全值比较低，则会使计算机软件系统出现安全漏洞，进而为不良攻击制造可能性。为此，在研究计算机安全漏洞检测技术的过程中，研发人员需要依据系统的实际情况，强化共享数据库的安全性，进而为计算机安全共享数据提供保障。在强化共享数据库安全性能的过程中，检测技术需要针对链接中存在的问题加以强化，进而有针对性的拦截安全性较低的函数。同时，成功拦截之后，技术人员需要针对其中存在的漏洞进行优化和完善，提升计算机软件运行的安全性。

（五）静态化检测

静态化软件漏洞检测技术的检测原理是针对计算机软件中存在的源代码进行扫描，通过扫描待测软件的相关源程序或二进制代码的方式，进而精准地发现其中存在漏洞问题，并针对这些问题加以规制，从语法、语义上对待检测程序的基本特征加以理解与分析，并从不同的角度对可能存在的不良信息进行解读，进而探寻出系统运行过程中可能具有的异常信息以及不良因素。静态化检测的具体执行过程：通过事先对计算机程序进行扫描，以此对其中存在的重要问题加以分析，并按照漏洞的衡量标准落实检测策略，进而分析出程序执行过程中的漏洞。例如：语法以及语义识别漏洞可能存在的不同角度，对其加以分析，可以提升检测的广度，并就不同的角度完善检测的针对性以及检测价值。在运用静态检测的过程中，需要应用类型推断、约束分析、数据判断等不同的思考角度，对于计算机软件在执行以及运行过程中可能存在的问题加以判断，进而实现漏洞相关问题的有效筛查。但上述的分析手段，在实际的执行过程中表现出一定的局限性，不能就全局的角度实现软件内部问题的有效分析，但静态检测的手段仍然在当今的时代中，具有一定的便捷性，可以有效提升检测效率。

结语

总之，计算机软件技术的普及，极大的提升了人们生产生活的便利性，推动社会的发展。针对人们比较关注的安全问题，研发人员需要从专业的角度进行分析，并做好计算机软件安全漏洞的检测工作。除此之外，还需要强化使用者的安全意识，注重遵循计算机软件的使用规则，避免人为操作引发的安全问题。

参考文献

[1]李云.安全漏洞检测技术在计算机软件中的应用[J].无线互联科技，2021，18（09）：76-77.

[2]徐菲.计算机软件中安全漏洞检测技术的实践研究[J].无线互联科技，2021，18（02）：41-42.

[3]陈婧.计算机软件中安全漏洞检测技术研究[J].电子技术与软件工程，2020（13）：250-252.

[4]陈健.论计算机软件中安全漏洞检测技术的应用[J].科技风，2017（7）：1.