计算机安全漏洞的动态检测

王鹏 / 吉林市红十字中心血站

摘 要：随着国家经济的发展以及科学技术的提高，计算技术也开始不断得到普及。计算机技术和网络技术在给人们提供了便利的同时，其自身的安全隐患也让人们的生活受到了困扰。由此可见，需要建立相应有效的安全体系对计算机软件的安全漏洞进行检测和防护，防止不安全因素对计算机软件的损害。本文就计算机安全漏洞动态检测技术进行了以下分析和探讨。

关键词：计算机；安全漏洞；动态检测

在计算机的组成中，软件是结构体系中十分重要的一个内容，软件的安全性在很大程度上也影响了软件的性能，从而影响了计算机的使用。所谓计算机安全漏洞，就是计算机系统软件以及协议在实现过程中或者计算机系统安全策略存在的一些问题和缺陷。在计算机软件中，安全漏洞的出现，会导致计算机系统受到入侵，对计算机的安全性造成严重影响。如何对安全漏洞进行检测，并对漏洞进行修复，也是目前计算机信息安全领域中的一个难题。

1 计算机安全漏洞动态检测的概述

在计算机系统中，安全漏洞是计算机系统自身的一些缺陷和问题，这些缺陷和问题的出现，计算机系统也会因此受到侵袭和攻击。这些安全漏洞大多与计算机软件的开发工作中，开发人员人为失误有关。对于计算机安全漏洞，主要存在以下几个特点：（1）软件的编程过程中，逻辑错误是常见的一个问题，大多是因为开发人员失误所致。（2）在软件的数据处理过程中，比数值的计算中逻辑错误较为常见，相比中等程度模块，过大模块以及过小模块的错误率更高。（3）计算机安全漏洞与系统环境存在十分密切的联系，不同的系统以及不同的软件设备和版本在安全漏洞的种类上也会不一样。（4）计算机安全漏洞与时间的联系也十分密切，在时间的影响下，旧漏洞会逐渐得到修复，然而新的漏洞也会不断出现。由此可见，计算机系统的安全漏洞情况将会长时间的存在，因此需要采取合理的措施对其进行控制和检测。

2 计算机安全漏洞动态检测技术

计算机安全漏洞动态检测技术主要是在源代码保持不变的情况下，对计算机程序缺陷进行检测，其对运行环境进程有所要求，因此需要对计算机运行环境进程进行修改。在计算机安全漏洞动态检测技术上，主要存在以下几种技术：

2.1 非执行栈检测技术。在目前，攻击事件中，以栈为基础的攻击发生率日益增加。这主要是因为计算机操作系统中，大多数的栈具有可执行性，另外栈存储着内部变量，这也使得攻击率大大增加，攻击方可以通过将恶意代码注入栈中，即可攻击对方计算机系统。另外，攻击栈的技术目前较为完整，这也让栈成为了主要的攻击对象。在对此类攻击的防范中，主要目标是让栈中的恶意代码得不到执行，从而防止栈受到攻击。然而，这种防范方法要求对计算机的操作系统进行修改，加上栈出现不可执行的情况，计算机的自身性能也会受到影响。对于一些存在栈以及堆溢出漏洞的程序，可以通过栈溢出从而是程序向攻击代码跳转，代码置于堆上，执行栈没有实际代码，而是堆中的执行代码。非执行栈检测技术要求对计算机操作系统的内核进行修改，将栈页标设置为不可执行。

非执行栈检测技术仅可以检测栈攻击并对其进行组织，在检测的全面性上还不够完整。攻击方如果将恶意代码的数据段注入栈中，非执行栈检测技术则会失效。另外，这项技术在兼容性方面还存在一系列的问题。

2.2 非执行堆和数据检测。在堆中，因为程序运行动态分配过程中所存的区域，数据段已将其初始化，加上堆以及数据段在非执行时对计算机软件的运行存在影响，因此非执行堆和数据检测技术的发展也不断受到阻碍。堆和数据段在不执行代码的情况下，攻击方的恶意代码也将不会被执行，同时将这种技术与非执行栈技术相互配合，能够实现对计算机安全漏洞的有效检测和保护。然而，非执行堆以及数据检测技术在实施上要求对计算机内核进行大量修改。然而，这项技术的可行性也得到了很多人的肯定，其能够检测和抵御所有在进程内存中注入的恶意代码攻击。然而，这项技术在堆以及数据段代码的动态生成模式进行了改变，因此也让程序出现了不兼容的情况。

2.3 内存映射检测技术。一些攻击方可以利用NULL结尾字符串覆盖内存，从而对系统进行攻击。对于这种情况，可以随机将代码页进行内存地址的映射，从而使这种依靠地址猜测的方法无效。比如，在缓冲区的溢出漏洞中，攻击方一般要寻找内存的目标进程地址，并利用自身创造的数据覆盖该地址。然而这种地址主要是系统自身计算所得出的，因此通过内存映射检测技术，将代码页进行随机地址映射，则会增加攻击方的难度。然而对于内存映射检测技术，也需要修改系统内核，将系统的代码页在低内存的空间内映射。对于内存映射检测技术，其能够检测和阻止内存地址跳转的攻击。然而对于新代码注入和执行的攻击则无法进行检测。另外，因低端内存大小受限，因此在代码页映射上，也无法实现所有代码页的低端内存映射。

2.4 安全共享库检测技术。对于计算机软件的安全漏洞，大多是因为不安全共享库使用所致，这是因为共享库

中图分类号：TP309

内部存在大量不安全的函数，这种函数会对计算机系统造成严重影响。安全共享库检测技术主要利用动态链接技术，并对程序运行过程中的不安全函数的使用进行拦截。另外，安全共享库检测技术还能够评估内存的上限，从而防止数据在评估边界上写入。此技术在开发和配置上较为简单，因此无需对程序进行修改。从理论上看，安全共享库检测技术能够对标准库函数为基础的攻击进行检测和保护。然而，由于其无法保证本地变量的安全，因此也使得数据段以及代码段数据溢出攻击得不到化解。另外，安全共享库检测技术对于非标准库函数也没有能力。唯一的优点是，其能够保证系统不会出现兼容性问题。

2.5 沙箱检测技术。沙箱检测技术主要是对进程访问的资源进行控制，从而对安全漏洞进行检测和防范。在系统调用函数上，如果存在多种软件调用了系统，则可能是系统受到攻击所致。在攻击之前，可以采用沙箱检测技术对该资源访问进行控制，从而使攻击得到化解。沙箱检测技术对系统的内核以及应用程序无需进行修改，然而需要对安全检测对象程序的资源访问策略进行定义，定义工作较为复杂和麻烦。此技术在检测上较为全面，能够有效对程序进行保护，然而对于重要本地变量改写方面，此技术无法发挥效用。沙箱检测技术在兼容性上并不存在问题。

2.6 程序解释检测技术。程序解释检测技术是针对程序运行过程中的检查和监视的一项技术。对于此技术而言，在性能消耗上要求较大，程序监视器在使用的过程中，虽然能够进行额外安全检测，但是其性能的消耗也十分巨大。程序解释检测技术的内核以及程序代码无需进行改变，仅仅要求在程序中对新启动代码进行重新链接，在安全策略上较为全面，能够对各种危险函数参数变化以及程序控制流程修改等攻击进行检测和阻止。

3 结束语

计算机安全问题一直十分严峻，这也使得安全漏洞检测技术得以发展。在对安全漏洞进行检测的过程中，需要对安全漏洞加以分析，运用安全漏洞检测技术，从而使计算机的安全性得到加强。

参考文献：

[1] 彭炜. 计算机安全漏洞动态检测研究[J]. 光盘技术, 2009, 2(4): 16-17.

[2] 冉崇善, 周莹. 软件设计中的安全漏洞动态检测技术分析[J]. 微计算机信息, 2010, 3(6): 78-79.

[3] 梁彬, 侯看看, 石文昌. 一种基于安全状态跟踪检查的漏洞静态检测方法[J]. 计算机学报, 2009, 3(05): 103-104.

[4] 万绪江, 班显秀, 刘小东. 网络安全的防御方法和可行性研究[J]. 电脑编程技巧与维护, 2010, 1(08): 111-112.

[5] 张迎, 宁玉文, 高东怀. 高校网站信息安全威胁与对策探析[J]. 中国教育信息化, 2010, 1(09): 142-143.

作者单位：吉林市红十字中心血站，长春 130031

《《《《《《上接第179页

及其设施，主要包括以下内容:

（1）计算机系统的环境条件

计算机系统的安全环境条件，包括温度、湿度、空气洁净度、腐蚀度、虫害、振动和冲击、电气干扰等方面，都要有具体的要求和严格的标准。

（2）机房场地环境的选择

计算机系统安装到一个合适的场所是十分重要的，安装场所能直接影响到系统的安全性和可靠性；计算机厂房的选择一定要注意外部环境的安全性、地质的可靠性、场地抗电磁干扰性，要避开强振动源和强噪声源，还需要避免设在建筑物高层和用户设备的下层或隔壁。也要注意出入口的管理。

（3）机房的安全防护

机房的安全防护是针对环境的物理灾害和防止未授权的个人或团体破坏、篡改或盗窃网络设施、重要数据而采取的安全措施和对策。为做到区域安全，首先，应考虑物理访问控制来识别访问用户的身份，并对其合法性进行验证；其次，对来访者必须限定其活动范围。

4 结束语

网络安全作为一项动态工程，它的安全程度会随着时间的变化而发生相应的变化。信息技术日新月异的今天，需要随着时间和网络环境的变化或技术的发展而不断调整自身的安全策略。总之，计算机网络安全工作是一项长期的任务，网络安全问题不仅仅是技术问题，同时也是一个安全管理问题。如何保证网络的安全，是一个值得长期研究和付出努力的问题。

参考文献：

[1] 顾巧论, 贾春福. 计算机网络安全[M]. 北京: 清华大学出版社, 2008.

[2] 吴诗豪. 计算机网络安全性研究[J]. 管理观察, 2009.

[3] 宋庆大, 颜定军. 计算机安全漏洞与应对措施[J]. 计算机安全, 2009.

[4] 方晓, 迟霄霄, 孟丹丹. 计算机网络与防范研究[J]. 计算机安全, 2009.

[5] 高晓飞, 申普兵. 浅析网络安全主动防御技术[J]. 信息网络, 2008.

[6] 武新华, 段玲华, 刘岩. 黑客防范技巧与典型应用[M]. 北京: 中国铁道出社, 2009.

[7] 王强. 计算机安全入侵检测方案的实现[J]. 计算机与信息技术, 2007.

[8] 范宝锋, 李扬继, 卢艳. 网络安全策略分析[J]. 山西电子技术, 2006.

[9] 程连生. 计算机网络安全技术探讨[J]. 科技创新报, 2009.

作者单位：内蒙古师范大学青年政治学院，呼和浩特 010051