

计算机软件开发安全技术应用研究

姚胜鑫, 付大乐

武汉东湖学院 湖北武汉

【摘要】 计算机网络技术的系统化发展, 促进了各行各业的发展, 各行业都在不断应用计算机软件开发技术, 促进自身转型升级, 并研发出多样化的新型软件满足人们的需求, 更好地为社会发展服务。但是计算机网络技术在发展中也有自身的缺陷, 尤其是网络安全, 因此, 各行业在研发计算机软件时, 需要注重引用安全技术, 确保计算机使用性能的充分发挥, 提高计算机软件开发程序的稳定、可靠性。主要浅析安全技术计算机软件开发中的应用, 并针对计算机软件开发中的安全问题进行了分析, 通过安全技术提升计算机软件开发水平和质量。

【关键词】 安全技术; 计算机软件; 网络; 安全技术

Application on Security Technology of Computer Software Development

Shengxin Yao, Dalei Fu

Wuhan Donghu University, Wuhan, Hubei

【Abstract】 The systematic development of computer network technology has promoted the development of all walks of life, all industries are constantly applying computer software development technology, promote their own transformation and upgrading, and developed a diversified new software to meet people's needs, better serve for social development. But the development of computer network technology also has its own defects, especially network security, therefore, various industries in the development of computer software, need to pay attention to the reference of security technology, to ensure the full play of computer performance, improve the stability and reliability of computer software development programs. It mainly analyzes the application of security technology in computer software development, and analyzes the security problems in computer software development, and improves the level and quality of computer software development through security technology.

【Keywords】 security technology; computer software; network; security technology

随着计算机网络的出现, 人类的生活发生了翻天覆地的变化, 各种生产、管理的效率和品质都在不断提高, 为人类的发展带来更多的价值。

1 实施安全性技术目标

安全技术是电脑软件发展中必不可少的一项重要技术, 它的目的在于处理各类人为干扰的原因, 以保证电脑使用程序的安全性, 防止电脑受到电脑的病毒入侵, 同时也能有效地防止电脑受到电脑使用者的恶意攻击, 从而有效地防止电脑在使用时出现的各类意外事件。计算机信息被盗、病毒入侵、上网过程受到的恶意入侵等, 都会对计算机的正常工作造成很大的威胁, 所以, 在计算机的发展过程中, 必须采用科学的技术来保证计算机的安全

与稳定性。

2 电脑软件的发展问题

2.1 计算机硬件和软件设备损坏

在研制电脑软件时, 必须对软件及软件进行全面的检验, 一旦出现故障或损坏, 将会对电脑的发展造成一定的冲击, 甚至会使电脑无法正常工作, 从而造成资料遗失、延迟开发, 甚至会对整体的电脑造成损害。据以往经验研究, 电脑设备损坏状况比较复杂, 人为因素, 设备电路故障, 线路老化, 自然因素等。若不加以有效地加以管理, 可能会使电脑系统出现故障、电脑系统瘫痪、部分工作中断, 给使用者带来直接的经济损害。

2.2 在处理 and 传递过程中, 很可能遭到恶意的

袭击

在进行数据处理的过程中, 在传递数据的过程中, 存在着多种危险。所谓“被动”, 就是当一个电脑程式在执行时, 由于没有足够的安全措施和防护措施, 很可能会遭到恶意的入侵, 从而导致信息泄漏和信息传输遭到窃取。该方法既能干扰数据的传递, 又能使数据的内容被盗用, 但对整个电脑的网络并无多大的危害。主动式的袭击是在信息传递和处理过程中对各种信息进行篡改、拦截, 从而干扰信息的正常工作。

2.3 计算机硬件和软件技术水平低

目前电脑软件市场秩序混乱, 制度不健全, 盗版和不满足开发要求的大量软件, 使得部分电脑软件的研制和生产过程中遇到了许多问题。此外, 有些网站经营者为节约开支、追逐利润, 购买部分山寨软件, 对正品进行恶意诽谤, 使得软件行业中充斥着各种类型的产品, 从而极大地提高了软件的泄漏几率。在应用电脑软件的过程中, 若不定期地对各种软件、硬件进行维护, 防范各种隐患, 清除垃圾, 也会对资讯的安全性造成一定的不利影响。

3 计算机软件的安全性技术

3.1 IDS 技术

入侵探测技术作为一种重要的技术, 在计算机的工作中起着重要的作用, 它能够保证网络的正常运转, 在受到攻击的时候, 能够及时的对其进行分析 and 辨识, 并且能够跟踪到自身的攻击, 并依据其真实的跟踪效果来进行科学的处理。通过引入 IDS 技术, 可以对计算机运行系统、网络结构等进行综合的研究, 从而为系统中遇到的各类问题提供技术保证。通过 IDS 的统计分析, 可以有效地监测到网络的工作状态, 对网络的攻击做出快速的响应, 并及时预警, 并制定相应的对策。至于 IDS, 它结合了很多尖端的技术, 将人工智能技术引入到了实际的应用中, 它可以实时监测整个电脑的运行状况, 从而能够识别出所有的不正常现象, 从而确保了使用者的信息的安全性。此外, 本技术还可以用于其它领域, 从主机的角度来看, 它能实现对主机的自动识别, 并对系统的资料进行周期性的查询, 从而实现了对主机的实时监控。它还能对计算机网络安全进行防护^[2]。

3.2 防火墙技术

在软件研发中, 如果受到外界的入侵, 可以从安全的观点出发, 通过建立内外网络的防火墙来实现对软件的全面保护, 从而提高软件的安全性。由于防火墙技术具有很好的抵御攻击的特性, 所以, 在电脑软件的设计中, 可以充分利用防火墙技术来保证程序的安全和信息的流通。此外, 在使用防火墙技术的时候, 还必须要设定一些权利, 例如, 通过访问访问, 可以让防火墙在最短的时候, 将所有的危险都给过滤掉, 从而减少电脑系统的安全性。

3.3 Security Technology

在计算机软件的发展过程中, 可以采用密码技术来保护计算机的软件。在计算机软件的研制过程中, 利用密码技术可以对某些关键的资料进行密码或对某些实际资料进行隐蔽处理, 从而能有效地防止信息的遗失和损坏。利用信息的密码技术, 能够在信息中构成一层双重防护, 防止被黑客或病毒入侵, 从而降低信息的泄漏, 从而有效地保护使用者的权益。此外, 该技术还能满足用户的需要, 保障用户的个人隐私。在某些特殊文件传输、程序文件传输中, 首先要对文件进行密码处理, 然后才能传输, 防止黑客、病毒等入侵, 同时防止电脑程序被攻击, 保障使用者的个人资料。

3.4 漏洞修复技术

计算机软件的研制工作具有系统、周期长、反复检测的特点, 在这一进程中, 各种计算机设备、组件、内部芯片、运行系统等都会发生一定的损坏, 从而导致各种漏洞、损坏的设备和程序得以正常运行。这些问题若及时发现和解决, 将会引发各种安全隐患和经济损害, 必须通过对各种系统、程序的漏洞和损坏进行及时的修补, 从而达到最大限度地恢复电脑的网络性能, 保证使用者的电脑能够安全地操作。另外, 在电脑软硬件的应用上, 要从总体上进行设计, 制定合理的维修计划, 强化电脑软件的防护, 从而提高电脑软件的使用年限。

3.5 防制计算机的技术

电脑病毒种类繁多, 传染性强, 病毒侵袭危害大, 难以识别, 电脑网络一旦被病毒侵袭, 将会导致电脑的整体瘫痪, 所以要采取病毒防御技术, 对病毒进行反击和处理。所谓的“病毒防御技术”, 就是一种新型的技术, 它可以控制和消灭任何的病毒, 在电脑的开发过程中, 首先要设置一个病毒防

御系统,然后在系统的运转过程中,启动一个系统,来探测不同的病毒,同时阻止隐藏的病毒。在实际的程序运行中,通过分析和追踪病毒的状态,从而判定电脑的程序是否被病毒所影响,从而实现自动处理。

3.6 安全性分析技术

运用安全技术构建一个统一的解析平台架构,以掌握当前的计算机软件发展状况;在构建系统的时候,要对整个系统的运行情况进行分析,并依据系统的要求,确定系统的组织架构;一个特定的安全集成解析系统包括:信息采集器、检测系统、监控接口、数据库和服务器,在该系统的分支上设置采集器,完成对网络数据、系统记录的检测,而采集器则包括感应器和监控器。该系统主要是利用一种先进的测试方法来整合和存储收集到的信息,然后按照服务端的请求请求进行查询,把满足要求的信息传递到服务器上。数据库主要分为三类:事件数据库、知识数据库和用户数据库,其中以安全集成解析平台和安全集成分析平台为中心,对各类安全信息进行风险识别、监控、预警、审计、配置等功能。监控界面是一个由安全管理人员控制的用户界面,它的安全性问题很多,必须要有一个科学的方法来解决,例如可以调整参数,识别警告信息等。

3.7 安全性鉴定技术

采用模块化的思想,对计算机的系统进行了优化,从而保证了系统的安全性。在这里,硬件驱动器主要负责控制电脑的外设工作状态,向内的应用软件传送信息,而操作系统则是利用其他技术,并能提供各种接口、存储器等辅助设施。上述的驱动程序采用安全验证技术,构成了一种以计算机系统为中心的操作系统,它可以对电脑底层的硬件进行监控,从而保证电脑的高级应用,从而实现安全、高效的开发。

3.8 指纹技术

指纹技术是目前电脑中比较常用的一种技术,它具有生物特性,要想通过指纹来访问特定的网页,就必须要有相应的数据库来实现。

4 结论

为了保证计算机系统的安全稳定运行,保证计算机系统安全稳定,应用各种安全技术来提高系统的安全性能,保证用户信息安全,保证计算机程序

运行安全。此外,安全技术的运用需要结合具体的具体条件来进行,针对各种安全隐患和风险需要及时发现、分析和处理,以保证使用者的权益不受到损害。

参考文献

- [1] 孟蓝茹,石郡儒.计算机软件安全检测存在的问题及应对措施[J].信息记录材料,2021,22(07):72-74.
- [2] 丁勇.安全技术计算机软件开发中的应用研究——评《计算机安全技术》[J].现代雷达,2021,43(01):95.
- [3] 陈中凯.试论在计算机软件开发中数据库安全设计的应用实践[J].信息系统工程,2020(12):119-120+122.
- [4] 郭庆,黄勇.基于信息安全环境分析计算机软件的开发及应用[J].通讯世界,2015(19):282-283.
- [5] EJ/T 1058.2-2005, 核电厂安全系统计算机软件 第2部分:预防软件导致的共因故障、软件工具和预开发软件的使用[S].
- [6] EJ/T 1058.2-2005, 核电厂安全系统计算机软件.第2部分:预防软件导致的共因故障、软件工具和预开发软件的使用[S].
- [7] 刘长军,在用压力管道检验验收、安全评估技术及计算机软件开发研究.上海市,华东理工大学,2000-12-01.
- [8] 《工业企业危险辨识、控制、动态安全评价技术及计算机软件开发》科研成果在上海通过劳动部主持的技术鉴定[J].工业安全与防尘,1996(03):1-20.
- [9] 《工业企业危险辨识、控制、动态安全评价技术及计算机软件开发》成果内容介绍[J].工业安全与防尘,1996(03):2-4+8.

收稿日期: 2022年9月18日

出刊日期: 2022年10月25日

引用本文: 姚胜鑫, 付大乐, 计算机软件开发安全技术应用研究[J]. 国际计算机科学进展, 2022, 2(3): 39-41.

DOI: 10.12208/j. aics.20220043

检索信息: RCCSE 权威核心学术期刊数据库、中国知网(CNKI Scholar)、万方数据(WANFANG DATA)、Google Scholar 等数据库收录期刊

版权声明: ©2022 作者与开放获取期刊研究中心(OAJRC)所有。本文章按照知识共享署名许可条款发表。<http://creativecommons.org/licenses/by/4.0/>



OPEN ACCESS