

文章编号: 2095-2163(2020)05-0228-03

中图分类号: TP311.5

文献标志码: A

计算机软件开发中主动防御技术的应用实践

曾俊义

(惠州城市职业学院, 广东 惠州 51600)

摘要: 为了提高软件开发的稳定性、安全性,可以充分利用主动防御技术。针对软件的实际情况,确定需要服务的应用程序。通过将主动防御技术运用在计算机软件开发中,起到了良好的防御作用,软件的使用也更加安全。文章对主动防御技术的应用进行了分析,为计算机软件开发提供一些参考依据。

关键词: 计算机; 软件; 开发; 主动防御技术

The application practice of active defense technology in computer software development

ZENG Junyi

(Huizhou City Vocational College, Huizhou Guangdong 51600, China)

[Abstract] In order to improve the stability and security of software development, we can make full use of active defense technology. Identify the applications that need services based on the actual situation of the software. Through the application of active defense technology in computer software development, it plays a good defense role, and the use of software is more secure. This paper analyzes the application of active defense technology and provides some references for the development of computer software.

[Key words] Computer; Software; Development; Active defense technology

0 引言

随着信息技术的发展,软件开发的工作也不断增加。在开发软件的过程中,了解具体功能需求,也要在设计上防止被恶意攻击。使用主动防御技术,通过分析网络攻击来对安全问题进行预测,并针对可能存在的一些网络安全隐患,开展主动性的防御,使软件的使用更加安全。

1 关于主动防御技术

主动防御是指在入侵行为对系统产生影响之前,主动进行预警和防御的一种技术,由多种可实现网络安全主动防御的技术构成,将这些技术进行组合、排列,形成完善的主动防御技术体系,降低网络安全风险。主动防御是建立在基础网络安全基础上的一种技术,其作用和目的是保护传统网络的安全。在开发软件的过程中,为了避免产生安全风险,可充分利用主动防御技术来提高软件的安全性,防止隐私和信息被泄露和篡改。在目前的软件开发过程中,主动防御技术的使用已经成为了一种重要的趋势^[1]。

2 计算机软件开发中主动防御技术的应用

2.1 分析和了解软件领域的需求

在软件的设计和开发过程中,首先要了解软件

的领域需要,同时针对使用服务的应用程序进行分析。在这个过程中,要充分利用软件体系结构的理念,采取结构化的模式对问题空间、用户需要进行统筹安排,同时借助特性的形式来对软件需求进行展现。将特征看成是需求空间中的实体单元,借助描述特征的各种变化性依赖关系,能够更好的划分软件领域需要。科学合理的分析软件领域需要,就要对特征之间的联系进行再次研究,包括约束关联、交叉关联等等,针对变化性的关联进行展示。在二次使用阶段,借助对领域特征订制,形成和软件特征相符的信息。

在分析软件领域需求的过程中,利用查询注册中心的服务情况,按照接口来阐述信息,使用一些传输协议和服务绑定实施功能。据此来构建服务的平台,促使命令被发送至服务消费端口,实施远程服务。为了使服务信息者对访问进行了解,也要将服务接口信息传递至注册中心。借助文献法来分析了解软件领域,计算公式为:

$$D_e = \sum_i \omega \sqrt{d \times i}.$$

其中, $\sum_i \omega$ 表示采用文献法获得的计算因素, D_e 表示软件领域需求。在计算中,没有进行定向分

作者简介: 曾俊义(1979-),男,本科,讲师,主要研究方向:计算机信息技术。

收稿日期: 2020-03-09

析。具体分析了用户的需要之后,可利用查询存储有服务信息库的注册端,便能搜索到需要的接口参数。

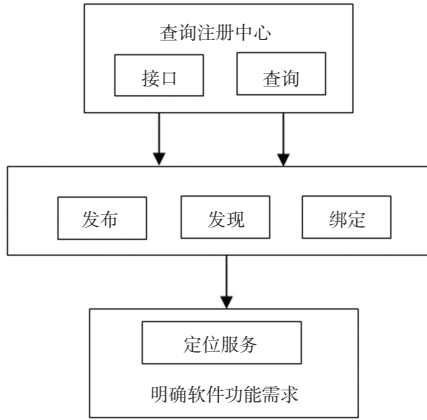


图1 查询和搜索的流程

Fig. 1 Process of query and search

综上所述,可按照服务需求提供搜索服务功能,借助相关的数据库对用户需要的服务接口参数进行查找、搜索。基于服务功能的结构,开展各种不同的操作,比如发布、发现、绑定、使用等。不仅如此,通过了解软件的功能需求,合理设计总体结构,能促使软件的功能需要得到满足,实现服务的流程化组织。设计软件的结构,属于非常重要的基础工作^[2]。

2.2 软件应用结构的设计

了解软件领域需求后,还要设计软件的应用结构。首先明确软件系统的需求规定,并据此进行应用设计。为了促使软件的使用效率得到提升,可充分考虑资产池里的反复构建、廉洁自律,促使面向对象的一些因素得到划分和改变。对软件应用结构设计,包括权限命名、界面构建、资源建立等。针对这些元素进行验证之后,促使应用结构被划分为可发布的软件包,内部权限的获取有:设备维持活动、相关隐私信息、网络访问实施。在软件的运行过程中,没有产生关联特征的权限,则表示无法对软件参数、用户使用产生一定的影响^[3]。

在软件设计过程中,需要对整个过程进行连接,而且拥有一致性的工具、平台。软件应用结构开发和设计,需要为设计、运行、维护提供一致性的工具且兼容软件的众多特点。同时采用自底向上的设计方法,将软件的中间结构当成是重点。也可采取可视化的设计方法,提供实时展示的功能。软件运行时,可设置相应的权限和门槛,使软件的应用访问具有一定的限制。使用软件采用权限的过程中,也要检查和测试。检查的公式:

$$DC = \frac{\partial}{Y_i \times t} - \sum_n 0.$$

其中, ∂ 表示了信息核对元素; DC 表示权限判断因素,值小于 ∂ , 则表示用户没有权限,不能进行访问,相反则可以访问; $Y_i * t$ 表示了访问拦截元素; $\sum_n 0$ 表示权限调用元素。在进行计算时,没有进行定向分析。

若是用户没有使用软件的权限,会提示有安全问题,且开展一定的检查工作,并且传递信息,软件页面也会重构,按照 HDU 模拟判断规则,针对 UI 页面进行诠释,提高软件的便利程度。借助编译的方式将系统外部文件纳入到应用程序里,在使用软件的过程中对数据进行阐述。按照各种描述对特征进行分析,高效率的加载软件资源,同时压缩字符串。在编译程序资源过程中,压缩字符串,可促使其在二进制代码里开展工作。

二进制代码的代入公式为:

$$\Delta F_j = \sum_{i=1}^c Q(R \times e_i).$$

其中, $\sum_{i=1}^c Q$ 表示二进制转换元素, ΔF_j 表示二进制代码体系, $R \times e_i$ 表示资源。

促使计算结果得以编译,且被放在相对的目录中,软件兼容各种相关资源(图片、字符串等),同时根据软件对象种类的差异提供各种不同的服务,借助参数和各种文件来创建资源,最终建立完整的软件结构,为主动防御技术的开发和使用奠定基础。

2.3 计算机软件开发中主动防御技术的应用

了解软件领域的需求,建立了软件结构,便可以对软件主动防御实施开发。要充分利用分层技术,提高软件开发的效果。分层技术能借助客户端页面达到一定的要求,能将用户的信息进行有效的传递、进行发送。分层技术还提供业务处理、数据库处理功能,使软件设计更加便利。界面层借助客户端,更好的对客户端进行处理,将相关的数据传递给业务层。业务层审核数据之后,会进行反馈,并对数据进行交换,通过代码模式和 PC 端联系。在这种情况下,可借助中间件技术来提升软件系统的稳定性,并测试软件,避免其中产生安全问题。而后进行入侵检测,分析是否有侵入现象,通过入侵检测流程来完成检测,使软件应用更加安全。入侵检测算法的公式:

$$W_e = \sum_m^n Q_{k \rightarrow i} + T_e.$$

其中, $\sum_m^n Q_{k \rightarrow i}$ 表示检测入侵元素, W_e 表示领域入侵的现象, T_e 表示入侵检测判断元素。借助这样的方式,可分析软件有没有被入侵,有没有产生安全风险,从而进行主动防御。在主动防御的过程中,也要对软件进行自动优化和改进,使软件结构更加完善。

在软件的入侵检测中,也要设置防火墙功能,使风险和威胁被拦在外面,避免隐私和信息泄露。还可以采用 VPN 技术来进行加密处理,避免非法用户进入。如遇到复杂入侵和攻击现象,主动防御技术还可以按照风险种类的不同,建立信息库,利用态势划分算法,公式为:

$$q(k_e) = \frac{[r(n-1) + r]}{D * E_{i-1}}$$

其中, $q(k_e)$ 表示风险种类判断元素, E_{i-1} 表示行为库转换元素, D 表示风险种类划分元素。

构建了行为库,分析入侵现象,根据实际情况开展主动防御。因为入侵行为具有高危的特点,因此需要针对反击现象确定,避免反击时产生误差。主动防御技术对于非法入侵和攻击具有主动防御的功能^[4]。传统软件开发方法和主动防御软件开发的方法对比,如表 1。

从表 1 可以看出,与主动防御软件开发相比,传统软件开发的安全性低。由于软件开发环境越来越复杂,用户数量也在不断增加,必须采取主动防御技术

来解决风险和安全问题。主动防御的技术和方法具有一定的成效,值得推广和使用。

表 1 传统软件开发方法和主动防御软件开发安全度的对比
Tab. 1 Comparison between traditional software development methods and proactive software development security %

实验次数	传统软件开发	主动防御软件开发
5 次	20	80
10 次	27	85
15 次	29	91
20 次	40	96
25 次	51	99

3 结束语

21 世纪是一个信息技术大力发展的时代,为了满足人们的各种需求,软件开发工作也在不断进行和开展。但传统的软件开发技术,容易产生安全风险。可在软件开发和设计中采用主动防御技术,提高安全性,为用户的使用带来更多便利。

参考文献

- [1] 李伟宁,王汉高,钟伟杰. 电力信息化行业网络安全主动防御技术研究[J]. 网络安全技术与应用,2018(5):69-70.
- [2] 刘冬兰,刘新,张昊,等. 基于大数据的网络安全态势感知及主动防御技术研究与应用[J]. 计算机测量与控制,2019,27(10):229-233.
- [3] 林旺群,王慧,刘家红,等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展,2011,48(2):306-316.
- [4] 王朝栋,郑忠斌,蔡佳浩. 基于主动防御技术的工业安全诱捕系统研究[J]. 信息技术与网络安全,2019,38(10):27-30,49.

(上接第 227 页)

等运动目标的识别,搭建了基于 NI 的振动信号采集和处理的实验平台,对过零数统计分析的运动目标识别方法进行了验证,基于验证结果,设计开发了地下电缆保护预警系统,实现了对进入保护区域的施工机械的探测和报警,达到了保护地下电缆的目的。

参考文献

- [1] 彭翀翀. 基于检波器阵列的地下电缆防外力破坏系统[D]. 浙江:浙江大学,2017
- [2] 杨柳. 浅层地震勘探中的无线同步研究[D]. 成都:成都理工大学,2011
- [3] 张玉成. 高频压电振子的振动传递特性及抛光应用研究[D].

辽宁:辽宁工业大学,2015

- [4] 王文强. 桥头桩基在强夯振动波作用下的动力响应分析[D]. 山东:济南大学,2017
- [5] 张航. 基于多振动传感器的平面振动定位研究[D]. 山东:山东大学,2017
- [6] 孙洁娣. 基于多地震动传感器的管道安全监测预警关键技术的研究[D]. 天津:天津大学,2008
- [7] 刘喜亮. 基于波动方程的瑞利面波有限差分法正演模拟[D]. 湖南:中南大学,2006
- [8] 靳舜. 基于声音和震动信号特征融合的车辆识别研究[D]. 陕西:长安大学,2014
- [9] 王辅东. 地铁爆破振动在线监测系统的设计与实现[D]. 江西:南昌大学,2017