第 3 卷◆第 2 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

计算机软件开发中安全技术的运用之研究

高奘
Tencent Americas
DOI:10.12238/acair.v3i2.13564

[摘　要] 随着科技的发展,计算机功能越发丰富,人们对计算机依赖程度逐渐增加,使用率不断提高。为了扩大计算机功能,技术人员加大对计算机软件开发力度,然而计算机软件在给人民生活带来便利的同时也存在着不同程度的安全隐患。网络信息安全的核心在于保护数据,本文将聚焦于计算机软件开发中安全技术的运用,阐述安全技术在计算机软件开发中的必要性,分析当前计算机软件开发运用中存在的安全威胁,探讨安全技术在计算机软件开发中的运用现状,并深入分析安全技术在计算机软件开发中的关键技术,为计算机软件开发过程中提高软件整体安全性和可靠性做出指导。
[关键词] 计算机；软件开发；安全技术；运用
中图分类号：TB664　文献标识码：A

Research on the application of security technology in Computer Software development

Yan Gao
Tencent Americas

[Abstract] With the development of science and technology, computer functions are more and more rich, people rely on computers gradually increased, the utilization rate continues to improve. In order to expand the computer function, technical personnel to increase the development of computer software, but the computer software brings convenience to people's life at the same time there are also different degrees of security risks. The core of network information security is to protect the data, this paper will focus on the application of security technology in the computer software development, expounds the necessity of security technology in the computer software development, analyze the current development of security threats, discusses the application of security technology in computer software development, and further analyze the key technology in computer software development, to improve the overall security and reliability of software in the computer software development process.
[Key words] computer; software development; security technology; application

计算机在推动社会发展中起到至关重要的作用,随着数字化进程的加快,大量信息通过网络进行传播与交互,但是任何事情都具有两面性,计算机在带给人们便利的同时也带来安全隐患,主要针对计算机软件的数据安全,数据在传输、储存过程中可能面临数据篡改、数据泄露、复制拦截等问题,导致机密数据泄露,给企业和个人带来巨大的经济损失[1]。如今,计算机软件安全技术已成为维护系统稳定运行和保障用户数据安全的重要技术手段之一。安全技术的运用不仅能够保护软件免受恶意攻击,确保数据的完整性和保密性,还能提升软件的稳定性和可靠性,避免未授权的访问、使用、修改、破坏,从而为用户提供更加安全、可靠的服务。

1 计算机软件开发运用中存在的安全威胁

1.1恶意软件病毒

常见的恶意软件病毒有木马病毒、蠕虫病毒,木马病毒主要通过伪装成合法的软件或文件,通过诱导用户下载和安装来潜入系统。一旦运行,木马病毒会在用户不知情的情况下在后台执行恶意操作,如窃取用户的账号密码、个人信息等。蠕虫病毒能够自我复制并通过网络传播,无需依赖宿主文件。但是一旦感染会迅速感染大量计算机,占用系统资源,导致网络拥塞和系统性能下降,严重影响网络安全运行,甚至导致企业关键业务系统瘫痪[2]。

病毒的传播途径主要是网络传播、移动存储设备传播。当用户在浏览恶意网站时脚本可能会自动下载并运行病毒程序。或者用户在接收和打开来自不明来源的电子邮件附件时,附件中的病毒也会感染计算机。

1.2数据泄露与窃取

1.2.1外部攻击导致的数据泄露

外部攻击多为网络攻击,例如攻击者在Web应用程序的用户输入框中输入特定的SQL语句,绕过登录验证,直接获取并篡改用户数据库中的信息。

1.2.2内部人员疏忽导致的数据泄露

内部人员在处理数据时可能存在将包含敏感信息的文件发送到错误的邮箱地址；在使用公共网络时未采取加密措施进行数据传输；员工在离职时未妥善处理工作设备上的敏感数据等问题,导致数据泄露。

1.3身份认证与授权漏洞

1.3.1身份认证漏洞

许多用户在设置密码时为了方便记忆,会选择简单的密码,这些简单密码也叫弱密码,很容易被攻击者通过暴力破解或字典攻击等方式破解。其次一部分计算机软件没有设置多种密码保护,密码重置过程中没有对用户身份进行充分验证,导致攻击者通过伪造用户身份信息来重置其他用户的密码。

1.3.2授权漏洞

在一些软件中会根据不同的用户角色设置不同的使用权限,但是有些软件权限设置不合理,给普通用户过高的权限,使其能够访问和修改系统的关键配置文件或敏感数据。或者在用户角色变更时,没有及时调整相应的权限,导致离职员工仍然保留着较高的权限,可能会对系统安全造成威胁。还有些软件存在权限滥用的情况,系统管理员利用自身权限查看、窃取其他用户的隐私数据,为了个人利益对系统数据进行非法修改。

1.4系统漏洞与攻击

利用系统漏洞是攻击者攻击的重要途径之一,通过寻找漏洞来获取系统的控制权或访问敏感数据。例如,2017年Windows系统出现的“永恒之蓝”网络安全漏洞,该漏洞允许攻击者在无需用户交互的情况下远程传播恶意软件,与WannaCry、NotPetya等勒索病毒结合能够在短时间内迅速蔓延至全球范围内的大量计算机。据统计,这些攻击波及了超过100个国家和地区,影响了数十万台设备,包括个人电脑、企业内网、政府机构、医疗机构、教育机构等,造成了巨大的经济损失和社会影响。攻击者一旦成功就可以获取目标系统的最高权限,可以随意安装恶意软件、窃取敏感信息、篡改或删除数据,甚至将受感染的设备纳入僵尸网络以进一步发动其他攻击。

1.5第三方安全风险

有些企业在与第三方开展合作时,需要信息共享,如果合作伙伴的安全措施不到位,可能会导致数据信息泄露。其次,在签订合同时,如果合同中对于数据安全责任的界定不明确,也容易出现安全风险。一旦数据发生泄露,双方可能会出现责任相互推诿的情况,企业很难采取有效的措施来挽回数据泄露造成的经济损失和声誉损失[3]。

2 安全技术在计算机软件开发中的运用现状

不同的企业对于安全技术的重视程度不同。大型企业对计算机软件安全非常重视,安全技术普及程度较高,因为大型企业中含有关键业务系统,一旦遭受外界攻击损失巨大,为了保护敏感数据,大型企业一般会成立专门的计算机安全部门,结合企业需求制定安全策略,将安全需求贯穿整个运营过程中,从需求分析、设计、编码到测试和部署,都有严格的安全标准和规范,对当前企业计算机环境进行实时安全评估监测漏洞,并不断更新安全技术,确保公司系统稳定安全运行。

而中小企业计算机安全技术普遍较弱,主要原因是资金有限,技术薄弱,相比于计算机安全,更看重计算机软件功能,虽然会购入一些商用的安全软件产品,如防火墙、杀毒软件等,来保护企业网络和软件系统的安全,但是在数据保密和完整上还是略有欠缺,安全漏洞监测和修复较大型企业频率和深度不够。

3 计算机软件开发中安全技术的运用

3.1数据加密技术的运用

信息加密技术主要体现在数据加密存储和加密传输两方面。在数据存储方面,很多企业有数据库,通过加密算法对用户数据进行加密。在一些特定的行业,如金融行业数据加密需要用到特殊的加密算法。哈希加密算法通过哈希函数将密码转换为固定长度的哈希值并存储,在验证用户身份时,重新计算输入密码的哈希值并与存储的哈希值进行比对,而不是直接存储明文密码,这样即使数据库泄露,攻击者也无法直接获取用户的原始密码,大大提高了密码的安全性。

在数据传输方面,数据加密技术可以分为对称加密和非对称加密两大类。对称加密算法(如AES算法)由于计算速度较快,适用于大量数据的加密,但其缺点是需要在发送方和接收方之间共享密钥,这带来了一定的密钥管理难度。非对称加密算法(如RSA算法)利用一对公钥和私钥来实现加密和解密,尽管加密速度较慢,但在密钥分发和管理上更加安全。在实际应用中,通常采用混合加密模式:即使用非对称加密传输对称加密的密钥,然后利用对称加密算法加密数据内容,以平衡速度和安全性。例如,在HTTPS协议中,客户端和服务器之间首先使用非对称加密交换密钥,然后使用对称加密传输数据,从而确保传输效率和安全性兼顾。

3.2防火墙的运用

防火墙是计算机软件应用最广泛的一种安全技术,可以设置一道或者多道防火墙,加强计算机系统的安全性,防止计算机软件开发过程受到攻击和干扰,给计算机软件的开发提供一个安全的网络环境。防火墙可分为多种类型,每种类型的防火墙在保护网络安全时有不同的作用,具体如下：①网络层防火墙：主要基于IP地址、端口等信息进行过滤,能够有效阻止未授权的访问,通常用于公司外网和内网之间的隔离。②应用层防火墙：通过分析应用层数据包(如HTTP、FTP等)来检测和过滤特定的数据请求。由于应用层防火墙可以识别复杂的攻击模式,如SQL注入和XSS攻击,适合在网络边界提供更深层次的安全保障。③代理防火墙:通过代理服务器将客户端与服务器分离,隐藏内部网络结构,同时可以对进入和发出的数据流进行深入分析,适用于具有较高安全需求的应用。

在实际应用中,大型企业会结合使用多层次的防火墙体系,形成对外部和内部网络的立体防御,例如限制外部网络对内部敏感端口的访问,有些甚至会设置内部防火墙,将关键业务部门进行隔离,限制不同部门之间的网络访问权限,防止敏感信息在内部网络中随意传播。

3.3身份认证与授权机制的运用

随着远程办公和云计算的普及,传统基于网络边界的安全模型逐渐难以适应,零信任架构应运而生。零信任架构是一种安全模型,强调“永不信任,始终验证”的理念,即所有网络请求都需进行身份验证和授权,无论请求来源于内部网络还是外部网络。在零信任架构中,每个用户、设备和应用都必须经过多因素认证,并进行实时的权限控制,以确保只有经过授权的请求才能访问敏感数据。多因素身份认证除了传统的用户名和密码外,还会结合其他因素进行认证,如手机短信、邮箱等,对于一些重要业务可能还需要使用U盾、生物识别技术(如指纹识别、面部识别、虹膜识别等)进行身份验证。以银行为例,网上银行系统除了要求用户输入密码外,还会发送短信验证码到用户绑定的手机上,用户需要输入正确的验证码才能完成登录,对于长期未登录的用户还会要求人脸识别重新认证,以提高身份认证的安全性。其次,在访问控制中可以通过身份和访问管理工具来实现,工具允许管理人员为每个用户和设备制定访问策略,并运用安全信息和事件管理(SIEM)工具实时监控用户和设备的活动,并检测异常行为。当检测到异常行为时,SIEM工具可以触发警报并采取适当的措施,自动封锁用户或设备的访问权限。例如,企业可以通过身份验证、端点检测和响应(EDR)等技术手段来持续监控和控制数据访问,确保即使在复杂的网络环境下也能保证安全。

3.4安全漏洞扫描与修复技术的运用

计算机运行过程中需要定期进行安全漏洞扫描与修复。漏洞扫描工具可以检测操作系统、应用程序、数据库等软件组件中存在的安全漏洞。例如,在使用Nessus、OpenVAS等漏洞扫描工具对计算机操作系统、应用程序等进行全面扫描,查找是否存在未安装的安全补丁、系统配置错误等安全隐患。对于企业内部开发的应用程序,也会进行代码级别的漏洞扫描,检测是否存在SQL注入、跨站脚本攻击(XSS)等漏洞。扫描通常会按照一定的周期进行,如每周、每月等,以确保及时发现新出现的安全漏洞。当漏洞扫描发现安全漏洞后,会及时进行修复。对于操作系统和第三方软件的漏洞,通常会通过安装官方发布的安全补丁来修复。例如,当微软发布Windows系统的安全补丁时,企业的系统管理员会及时下载并安装到企业的服务器和客户端计算机上。对于企业内部开发的软件,开发团队会根据漏洞扫描报告对代码进行修改和优化。

3.5安全开发生命周期的运用

为了确保软件在开发过程中即具备安全性,大型企业已广泛运用安全开发生命周期(SDL),即将安全性作为开发流程中的重要部分。SDL包括从需求分析、设计、编码、测试到部署的每个阶段。在设计阶段,开发团队会评估潜在的安全威胁,如进行威胁建模。编码阶段,通过静态代码扫描工具检测代码中的安全漏洞。测试阶段进行动态测试,模拟实际攻击场景,确保软件能抵御各种网络攻击。SDL通过建立从源头上控制安全性的流程,有效减少软件在发布后遭遇的安全问题,从而提升产品整体的安全性。

4 结语

随着信息技术的飞速发展,计算机软件已成为各行各业发展不可或缺的工具,人工智能、大数据等新兴技术的应用使得数据安全风险等级愈发复杂。面对复杂多变的安全形势,计算机软件安全开发者要不断精进安全技术,完善对软件安全框架的设计,采用先进的加密技术保护数据的存储和传输,建立严格的身份认证和访问控制机制,加强对用户权限的控制,定期进行漏洞检查和修复,以应对不断变化的安全威胁。

[参考文献]

[1]高敏.计算机软件开发中安全技术的应用分析[J].大众标准化,2023(11):143-145.

[2]常莹,朱庆华,张燕宁.计算机软件开发中安全技术应用分析[J].信息记录材料,2019,20(7):40-41.

[3]王锐铭.计算机软件开发中安全技术研究[J].吕梁教育学院学报,2022,39(1):74-75

作者简介：

高奘(1994--),男,汉族,北京人,硕士,职称：高级软件开发工程师/Senior DevOps Engineer,研究方向：计算机软件开发和运维。