在信息技术和计算机技术高速发展的现阶段，它们拥有的各种强大优势被广泛的应用于各个领域当中，不仅可以为人们提供各种获取信息的便利通道，更是在工业建设方面以及产能优化的各个方面发挥其最大的作用。现如今，计算机已经成为了人们生活中最重要的一部分，也是生产及工业中必不可缺的重要组成部分。但是我们在计算机的实际应用中，无论是技术方面，还是安全隐患和安全措施方面都存在着相应的问题需要有效的措施去解决。

通常情况下计算机的运行环境都是较为安全的，它可以容忍一定的网络病毒的入侵。但是一旦有黑客入侵、人为因素的影响或者计算机本身收到了外界因素的影响，那么其可以抵御病毒，木马的能力下降，就会为病毒等的入侵提供可乘之机。病毒主要是通过文件的复制、文件的传送、程序的运行等实质性的操作来进行传播。在平时的使用中，硬盘、光盘、网络是传播计算机病毒、木马的主要途径。随着计算机网络和软件的广泛使用和普及，为病毒等的快速传播创造了便利的条件。一旦发生病毒入侵等问题，就会对计算机本身以及内部的运行文件造成直接性的损伤，甚至使个人的隐私或者机密泄露、更严重的就会造成系统的瘫痪。病毒的存在对于计算机和软件的使用来说是致命的，它能使计算机和软件本身无法按照用户指定的命令正常的运行，更会对其行业的安全性发展带来阻碍作用。我们在使用计算机和软件的过程中，大多数用户是缺乏安全意识的，这样就会导致小的病毒在计算机中正常运行，通过长时间的积累后病毒的威胁就会被不断扩大，产生更大程度的负面影响。如计算机的运行速率下降、信息丢失等，使计算机系统始终处于难以在安全控制的范围内安全启动。虽然信息的丢失对于部分人来说可能不会带来致命性的威胁，但是经济损失是在所难免的，这就需要我们提前做好预防的工作，在使用计算机及软件的过程中积极进行查杀病毒的操作，使其运行的环境始终处于安全的状态下。

无论是在人们的日常生活中还是企业的运营中，在使用计算机或软件时信息泄露的事件一旦发生造成的后果都是较为严重的，导致信息泄露的原因事实上是具有量化特性的。第一，用户在使用软件及计算机等的相关模块时并不存在对信息的保护意识，更有可能无法正确的发现并辨别安全隐患，这样就会使得计算机在使用中的保护意识存在缺失性，让病毒的入侵变得更加便捷。除了这种发生在用户本身的问题以外，计算机和软件本身存在漏洞，其根本原因是因为信息系统在创建开发的过程中的研发工作不到位导致的。我们应当在实际使用的过程中不断强化和提高用户的安全意识，实时性的开展杀毒工作，尽量避免信息泄露问题的发生。其实，部分系统为用户提供相应的服务时，是会提供安全检测的，但是这种能够实现安全检测的装置存在统一的弊端，那就是只有在安全问题发生后才会提供相应的安全检测，做出预警反应。这样虽然可以保证一定的安全性，但是相对的也降低了系统的预防性应用设施的效果。预防问题未能很好的解决，事后的预警工作也不能起到良好的效果，更无法从根本上解决源头的问题，避免其安全性问题的发生。为了更好的优化，我们就需要强化系统的事前预警功能，这样能更好的保证软件运行的安全性。

随着计算机等技术的发展，研发高效率的防病毒软件和补丁需要的是高效率的信息处理功能和较低的成本，高代价的开发给病毒的发展创造了有利便捷的条件。病毒也存在发展，随着病毒不断的更新换代，我们需要不断地完善软件和计算机的病毒查杀和预防系统，及时更新补丁，不给病毒入侵的机会。同时，正版的软件也非常重要，它能提供更安全的运行环境，对于重要的文件一定要实施备份，以防病毒入侵造成文件数据丢失。

对于人们来说其实最重要也最无法避免的问题就是信息泄露。在2018年，重大数据泄露事件屡见不鲜，虽然没有出现像2017年那样全民恐慌的勒索病毒，但是媒体曝光的数据泄露事件的数量却远远超过以往，个人敏感数据遭泄露的人数以亿计算，例如Facebook、Aadhaar等数据泄露事件都造成了巨大的影响和损失。其实数据泄露问题涉及到的不仅仅是经济上的损失，更重要的是会涉及到法律问题，我国近年来也是更加完善了法律对其的约束。为了保护用户的信息安全，要求用户在使用各种软件时都要增强自己对于信息安全防范的意识，尤其是对于密码的安全防范意识，要避免简单密码或易泄露密码，同时我们还应该定期更换自己的密码。除了在用户方面，在开发者方面，研发团队在开发软件时更应该增强保密功能，设置多重保护，保证用户信息的安全。同时开发者也要注意细节的问题，避免因为失误造成的损失。

计算机和软件在发布后，开发者会对其进行安全监控，安全监控系统一般是在安全事件发生后进行处理的，但是安全监控的范围是一定的。就像监控摄像头，它针对的是一定范围内的实时反映。在图像识别中，安全监控范围内的图像亮度或对比度没有发生改变，那么一般来说，所获取的图像也不会发生改变。利用图像的这一特性，我们就可以在安全事件发生时利用图像识别来判断安全性。当发生病毒入侵等异常情况时，图像相应的亮度和对比度就会发生改变，与此同时安全监控系统就可以检测到异常情况的发生，并将报告发送给安全维护系统对异常情况进行处理。这样，在保证最大程度安全性的同时，也减少了损失的发生。

以图书馆为例，由于其特殊的运行模式，业务管理模式对其安全性的要求也不一样，其开放性和共享性造成的安全问题也需要优化和解决。图书馆由于要适应学校的教学和科研特点，满足公共性资源的分享与共享，所以是开放的，相对而言，在管理层面的需求也比较复杂，但往往在复杂的需求面存在简单的问题，这就具备了图书馆系统所拥有的致命性弱点——脆弱性、开放性和易受攻击性。对于类似图书馆的公共性系统，黑客的目的一般都是窃取机密数据或破坏其系统的正常运行，黑客会对图书馆的各种联网设备进行信息轰炸，致使其服务中断，也可能入侵Web或其他文件服务器删除或篡改数据，致使系统或数据库出现故障或瘫痪，甚至完全崩溃。除此之外，黑客还会向图书馆网络系统和信息系统发送附带病毒的文件或直接病毒入侵，达到间接破坏或直接破坏系统的目的。

在内部攻击的层面上来说，来自网络内部的攻击威胁是最为严重的。使用图书馆网络的大部分是学生，所以有少数专业学生或对其技术手段感兴趣但又没有良好安全意识的的学生就会把图书馆系统作为攻击的对象。学生选择攻击图书馆是因为图书馆系统和网络对于他们来说是内网，学校的IP地址基本是在学校内部公开的，这样可以很方便的隐藏学生自己的IP地址，这样就可以肆无忌惮的对图书馆网络和系统进行泛洪等的基本攻击，并可以立竿见影的见到他们的攻击所带来的危害。其实，在内网中根据IP地址很容易就可以找到学校图书馆网络的网段，这样就很容易运用ARP欺骗、中间人攻击等攻击手段对其系统或数据库进行入侵或破坏。现在的入侵不仅仅需要专业手段，事实上，随着科技的发展，现在互联网上第三方黑客攻击软件也越来越多，方法也越来越复杂，这就为恶意行为提供更多的手段和机会，同时也使环境变得越来越不安全。例如IP碎片攻击、OOB攻击、WinNuke攻击等，但是大部分的攻击手段还是以获取IP地址为前提，进行网络攻击的。在这样的情况下，图书馆网络既要保证系统和数据库以及网络的安全运行，同时又要为教学、科研服务，共享性的需求提供条件，以满足学生学习的需求。除了内部的攻击，更为严重的是系统本身存在的漏洞威胁。图书馆使用的系统软件主要有Windows NT，Windows 2000 Server，UNIX，Linux等，windows NT和Windows 2000 Server由于系统自身存在漏洞，虽然官方网站推出了一些针对性的补丁程序，但也不可避免地容易遭到病毒的入侵或人为因素的破坏。相比之下UNIX和Linux这两个系统就显的与众不同。UNIX和Linux问世后其源代码一直处于公开状态，这就为大家不断完善它创造了有利条件，事实上相当于成千上万的专业人士对其进行了实时性的测试与优化。又因为它们其实工作在最底层的架构，所以安全性相对而言是比较高的。由于各个图书馆使用的管理系统、数据库的不同，其开发者对于软件安全性方面的关心程度不同，侧重点也不一样。如果系统和软件的开发水平比较高、比较严谨，注重细节，在安全性能上的考虑也比较周到，其针对恶意行为的防范手段也较为先进，那么其安全性就大。反之，系统和软件本身存在比较多的安全隐患，安全性自然就没那么高了。针对安全性能的提高，我们可以利用防火墙，将内网和外网进行分离，对经过它的网络数据和信息或者接收到的文件等进行扫描，过滤掉非法数据或有威胁的数据，从而禁止非授权用户进行数据访问，甚至数据纂改，但是却允许合法用户透明地访问网络资源和数据信息。目前防火墙的主要类型分为——监测型、代理型、网络地址转化——NAT、包过滤型等。事实上，应用好防火墙并对防火墙进行正确的配置将对图书馆网络和数据库以及系统软件的安全起着十分重要的作用。除了防火墙，我们还可以利用数字签名技术。现在的数字签名技术已经相当成熟，对合法用户应用数字签名也是有力的安全防范措施，并且数字签名技术运用了非对称的RSA加密等复杂且有效的密码算法，这样既保证了合法用户对数据、系统等访问的权利，也对非法入侵用户起到了有效禁止与防范的作用，更有效的阻止了内部攻击的发生。

如果一个软件或者网站被恶意攻击、破坏，那么就存在一种机制——权限最小化机制，权限最小化机制能够有效的将潜在损害最小化，降低其造成的伤害及损失。常见的权限最小化实践包括，普通管理员/系统管理员等角色管理、文件只读权限/文件访问权限等访问控制、进程/服务以所需最小用户权限运行等。当开发者进行软件的设计时，安全性设计人员可以提前评估软件的行为及功能所需的最低限度权限及访问级别，按等级划分区域，从而合理的给相应区域分配相应的权限。如果程序存在特定情况必须要较高级别的权限或最高权限，也可以考虑特权赋予及释放的机制，但必须做到身份及等级区域的认证。这样一来，即便程序或软件本身遭到攻击或破坏等恶意行为时，也可以将损失降到最低。例如，在Windows系统中的网络进程、本地服务、用户进程等的权限都比较低且它们之间是互相独立的，分别为NETWORK SERVICE、LOCAL SERVICE、user权限，只有核心的重要进程是使用SYSTEM权限的。在最新版本的OFFICE程序中，打开不可信来源的文档或文件时，系统会将其默认为不可编辑的文件和文档，同时也是默认为不可执行的代码的，这样子，即使存在缓冲区溢出漏洞等系统缺陷存在，也不会轻易的执行shellcode等恶意代码，以免造成不必要的麻烦与损失。

除了权限最小化，还有默认安全配置。默认安全配置在用户熟悉设备软件或系统的安全配置选项之前不仅仅有利于更好的帮助用户更熟悉的掌握安全配置的经验，同时也可以确保应用程序和软件系统在初始状态下的确处于较安全的状态。而用户也可根据实际使用软件功能和系统功能的情况而决定应用程序和软件系统的安全与隐私的等级水平是否降低，是否能保证安全性。事实上，在Windows 7之后的Windows操作系统中，DEP(数据执行保护)默认是开启的。用户可设置选项改变DEP的状态，来默认安全，保证其系统的安全性。在Windows操作系统升级到Windows 10系统时，默认启用安全防护软件Windows Defender，用户可选择关闭，但当其开启时，就会默认保证系统的安全性。

与默认安全相似，纵深防御也是在开发者开发软件和系统时设计安全方案时的指导思想。纵深防御其实包含两层含义。第一，纵深防御要在各个不同的层面、不同的方面实施相对应不同层次的安全方案，避免出现疏漏，发生不安全事件与行为，针对不同层次的安全方案之间也需要相互配合，构成一个整体，积极防御恶意行为。第二，要在正确的地方做正确的事情，即在解决根本问题的部分或层次实施针对性的安全方案，更有目的的进行安全防御。总而言之，纵深防御并不是同一个安全方案要做两遍或多遍，而是要从不同的层次、不同的角度对系统和软件做出整体性的解决方案，保证安全性。主要的可以是针对XSS的防护，除了要对用户输入的特殊符号进行过滤和预处理，还要区分用户的输入是否是富文本，进而进行相应的编码操作，在输入的过程当中过滤的同时也在输出时进行过滤操作，同时性保证安全性问题。但即使做了十足的过滤、预处理、编码等安全防护工作，为了更进一步的确保能够缓解甚至避免XSS攻击，Web站点也可以对Cookie和浏览器等联网设备启用HTTP-Only属性，确保即使发生了XSS攻击，也可以阻止通过脚本访问Cookie的操作，以保证用户信息的安全性，避免出现信息泄露等问题。

还有就是建立威胁模型，威胁建模是一种分析应用程序或软件威胁的过程和方法。这里的威胁其实是指恶意用户可能会试图利用系统自身出现的漏洞以破坏系统、入侵系统进行恶意行为，但又和我们常见的漏洞并不相同。这些特殊的漏洞是一个特定的可以被利用的威胁，如缓冲区溢出、sql注入等，均会造成较大的威胁。典型的威胁建模是作为SDL设计阶段的一部分安全活动，威胁建模允许开发中的安全设计人员能够尽量在第一阶段就可以识别潜在的安全问题并实施相应的缓解措施。其实如果能在设计阶段就发现潜在的威胁有助于将威胁更全面、更有效的解决，同时也在一定程度上降低了风险，也有助于降低开发和后期维护的成本。威胁建模的一般流程分为四个部分，与系统架构师及设计人员沟通，了解设计详情；使用成熟的威胁建模方法分析当前设计方案潜在的安全问题；对潜在的安全问题提出安全建议及对潜在威胁的缓解甚至解决措施；对安全设计方案进行验证并对整个设计方案进行回顾并再次确认。比如微软使用的威胁建模方法是STRIDE威胁建模方法。为了便于安全人员以及设计人员快速便捷的进行威胁建模，微软开发了基于STRIDE威胁建模方法的SDL 的Threat Modeling Tool威胁建模工具，该工具可以帮助安全人员以及设计人员画出详细的数据流图、分析其存在的威胁、生成并导出威胁建模报告。具体化一点，STRIDE威胁建模是由微软提出的一种威胁建模方法，该方法将存在的威胁类型分为Spoofing（仿冒）、Tampering（篡改）、Repudiation（抵赖）、Information Disclosure（信息泄漏）、Denial of Service（拒绝服务）和 Elevation of Privilege（权限提升）。这六种威胁的首字母缩写即是STRIDE，STRIDE威胁模型几乎可以涵盖目前存在的绝大部分的安全问题。除此之外，对于STRIDE威胁建模方法有着详细的流程和方法，包括绘制数据流图、识别威胁、提出缓解措施、安全验证。数据流图(Data Flow Diagrams)包含外部实体(External Entity)、处理过程(Process)、数据流(Data Flow)、数据存储(Data Store)，安全人员会提前与系统架构师及设计人员沟通，尽可能详细的了解设计详情并画出数据流图，最后还需要标注信任边界（Trust Boundary）。根据不同的数据流图元素及已经确认的威胁进行划分，相应的缓解措施也不相同。例如外部实体用户的仿冒威胁，其缓解措施简单来说就是对用户的身份进行进一步的详细认证。对于一个Web应用来说，缓解仿冒威胁不仅仅需要较强的认证机制，还需要防止恶意攻击者用暴力破解、口令猜测等方法绕过认证机制直接获取内容，从而造成仿冒用户的威胁。用户仿冒威胁缓解的详细措施是，对用户访问进行帐号密码、证书等身份认证，或数字签名的身份认证；在用户帐号密码认证过程中，如果出现三次密码错误的情况，则增加验证码机制。输入验证码且正确确保一个方面后再进行身份认证；当用户认证较多次数后仍然验证失败，则在较长的一段规定时间内禁止该帐号进行登录等操作；最后用户密码必须包含数字、字母及特殊字符，且长度在8位以上，如果存在业务安全需要则增加密码过期机制，定期提醒用户修改密码。在提出缓解措施时，有的时候不仅要考虑安全问题，同时也要考虑软件的易用性和可用性，所以不同层次和方面的威胁，不同的应用场景。其缓解措施也要随之而改变以提高应用安全性的同时也能给用户带来较好的交互体验。微软等大型系统开发者和互联网开发公司对于常用的威胁给出了其常用的标准缓解措施，并在具体实施时已将常用的缓解方案及措施集成为独立的解决方案或者代码模块。可以方便同类应用直接使用，更有效、快速的缓解威胁。

其实，对于计算机的网络信息系统和软件安全方面存在的根本性问题, 最有效、最便捷的就是要建立起相适应于软件或系统的科学的防火墙技术, 利用防火墙技术保证计算机网络系统和软件来更好的进行安全工作。计算机网络信息安全和软件安全的保障思路就是, 首先要考虑到的是数据加密的方法对于数据安全性的促进作用和保护作用, 在实际的操作当中, 可以用复杂的加密算法将数据进行加密, 结合计算机网络防火墙实现对相应数据的强化与保护。对于实际应用中的数据加密的方式, 主要是通过网络连接和相应的端口加密来进行的, 因此需要网络安全维护程序当中的控制端与协议类型来相符合实际的网络数据筛选条件, 以实现对数据的实时转发，保证数据的安全性。

防火墙中的一类重要技术就是包过滤据技术，包过滤技术主要是指有选择性的对信息或文件等进行合理的判断, 能够较准确的分辨出它们的实际意义, 并拒绝不良信息和恶意信息传输的技术。包过滤防火墙主要通过网络参考模型中的数据传输与控制技术, 来实现对相应计算机网络和计算机自身的保护，主要针对信息方面。例如, 在网络传输工作当中, 在对网络传输的目标IP进行相应的保护工作时, 能够主动获取信息传输中的目标IP, 并对其中的数据包进行必要的分析与识别，过滤掉恶意或存在风险的数据包, 以保证正确信息传输的安全性和可靠性。从另一个角度来说, 包过滤防火墙技术可以在计算机的内部形成新的监测网络体系, 从内到外对信息等进行全面的控制和监督, 从而实现过滤数据信息、更好的防御攻击和恶意行为的目的。另外, 实际的包过滤防火墙技术往往应用在路由器和电脑的主机上，除了利用它最根本的作用以外，它可以通过实际的需求选择内网封闭或者外网开放的应用形式来更好的实现对数据的监控管理。

防火墙分为两种，应用型防火墙和网络型防火墙，分别从其运用的角度来说, 网络型防火墙主要是通过网络的IP端口来进行地址转化等功能来确保与外网的连接是否正确与安全, 更需要加强对网络的实时控制，对信息进行实时监测。在实际的计算机访问网络的时候, 同时内部网络与外部网络沟通的时候, 网络防火墙发挥了主要作用, 它能够对自动的网络终端地址和相应的端口进行监督、分析、管理, 通过改变终端地址和外界网络实现与实际端口的正确安全连接来保证网络在有效的可控范围内。防火墙是保护计算机和系统整体的各项工作稳定进行的基础, 只有建立完整功能的防火墙, 才能够保证各项数据的安全性, 保护用户的隐私与个人信息，防止被窃取。任何数据进入系统中时必须经过防火墙的筛选与过滤, 这就给防火墙实现安全保护功能的发挥提供了可能性, 例如对某一频繁发送信息的IP进行锁定与信息检测, 以抵御恶意的攻击与行为。还有一种是多防火墙，多防火墙联合防御是提高安全性与可靠性的重要方法。这种技术方法结合了多种防火墙系统，采用多种类型共同配置的方式配置防火墙, 在内部将防火墙的工作内容分层次、分等级的进行设置, 以保证相互之间不受冲突。多防火墙组成的安全系统可以监控不同区域和层次的安全问题, 各个防火墙可以通过相互之间的转化, 对不良信息进和恶意信息进行分层和过滤, 达到提升系统整体安全的目的。

在实际使用的过程中, 由于使用者之间存在一定文化和专业性的差异, 他们对安全防火墙的认识也并不全面，存在一定的缺陷和匮乏。例如, 计算机网络用户会认为对防火墙设置的保护是网络形式的隐私和相应的网络性信息, 同时他们还认为防火墙能够保证网络不受外界任何因素的影响而安全运行，保护系统。但是在网络系统的专业人员看来, 防火墙技术对维护网络信息的安全和可靠具有一定的促进作用, 当在网络系统发生异常或者出现问题或被判断为出现攻击行为时, 能够保护信息和隐私。对于交流而言, 信息的传送方可以将相应的信息用加密算法进行加密处理, 建立全面的安全系统规则, 从而实现计算机网络与外界连接传输信息的机密性和安全性, 保证在不法分子入侵或破坏系统时, 无法窥探或篡改到信息的具体内容和隐私部分。

　　对于防火墙技术的有效运用与分析要从实际的科学技术和未来的发展方向出发, 将先进的科学技术与实际的防火墙技术相结合，更好的在未来的方向上去发展, 建立安全的管理系统, 使用户的实际信息和个人隐私得到可靠的保护。将安全管理与防火墙紧密结合, 对数据进行必要的检查和监测的同时, 注重对系统本身的管理, 从而不断的提高安全性、机密性和可靠性。