

信息技术导论

题 目：信息的安全以及保护 班 级：2015级软件工程班

姓 名：封姝鸿

学 号：2015010703012

指导教师：周桂贤

试验时间：2015.12.10

信息的安全以及保护

在这个发达的社会，随着信息化的社会发展，信息在社会中的地位和作用越来越重要，每个人的生活都与信息产生、存储等有着密切的关系，信息安全在信息社会中扮演着一个极其重要的角色。信息安全将直接关系到国家安全、经济发展、社会稳定和人们的日常生活。随着信息时代的发展，人们信息安全意识在不断提高，病毒和黑客对计算机的影响，使得信息系统的安全问题越来越受关注，也就成了很多人关注的事情。

所谓“安全”就是在客观上不会造成威胁，在主观上不形成恐惧。不同的时代人们对信息安全的理解是不同的，在20世纪60—70年代，人们关注的是通信保密，就是在通信信道上的数据不被非法窃听，于是人们开始研究密码算法。到了20世纪80年代，计算机的性能得到很大的提高，应用范围也得到了扩展，计算机就已经遍及世界各个角落。到目前为止人们逐步共识的信息安全应包括如下含义：

1. 信息具有可靠性：是网络信息系统能够在一定的时间内在要求的条件下完成规定的任务的特性。
2. 信息具有可用性：指网络信息可被授权实体访问并按需求是用的特性。
3. 信息具有保密性：是指网络信息不会泄露给没有授权的计算机用户。
4. 信息具有完整性：指如果网络信息没有被授权，那么就不能对它进行改变。
5. 信息具有不可抵赖性：指在网络信息系统的信息交互过程中，确信参与者的真实同一性。
6. 信息具有可控性：是对信息的传播及内容具有控制力的特性。

除了这些之外，信息安全还包括鉴别、审查追踪、身份认证、授权和访问控制、安全协议、密匙管理、可靠性。

既然出了问题就要解决，于是对信息安全进行研究，在这里信息安全研究又分为以下几个层面。1、信息系统的可靠性。2、信息系统本身的问题。3、网络安全技术。4、数据或信息的安全保护。

那是什么危害着信息的安全呢？在这里我们就会谈到计算机病毒。计算机病毒是一种最为奇特的人类智慧的结晶，病毒就像幽灵一般游荡在计算机的领域当中，几乎每一个计算机用户都会被无处不在的计算机病毒所困扰。既然出现了问题就要有解决的方法，所以反病毒的技术也在不断的提高，但是反病毒总是落后于新病毒产生的。然而作为一个计算机使用者，应随时预防好病毒的侵入，当他们出现时应该以最快的速度最彻底的消灭它们，这些对于一个计算机使用者是非常重要的。下面我们就进一步了解一下计算机病毒吧。

计算机病毒并不是天然存在的，是某些人利用计算机软硬件所固有的脆弱，编制具有特殊功能的程序。它与生物学上的“病毒”同样具有传染和破坏的特性。那么它是怎么样传染的呢？计算机病毒主要是通过存储介质、网络传输、运行程序等方式进行，由此导致的主要传播途径有以下几种：

1. 磁盘：磁盘携带起来很方便，为了计算机之间互相传递文件，经常会移动磁盘，这样就会将这台机器上的病毒传播到另一台计算机上，这是病毒传播的一种途径。
2. 光盘：光盘的存储量大，所以很多软件都会被刻在光盘上，以便互相传递。光盘在制作过程中可能会将带毒文件刻录在上面。如果是只读光盘，即使上面有病毒也不能清除。
3. 网络：在计算机日益升级的今天，网络已成为病毒传播最主要的途径。在网络环境下，人们通过网络传递文件、信件等，这样不仅加快病毒的传播速度，又因为资源共享，人们在网上下载免费、共享文件，使病毒传播的影响在不断的增加。

计算机病毒除了传播方式多种多样，还具有多种特征。1、传染性，具不具有传染性是判别一个程序是否为计算机病毒的最重要的文件。传染性是指病毒具有把自身复制到其他程序中的特性，只要一台计算机被感染计算机病毒，如果不及时处理，那么病毒就会在这台机子上迅速扩散，然后的大部分文件会被感染，如果这台机子再和其他机子传输文件那么另一台也会被感染。2、非授权性：一般正常的程序是由用户调用，然后由系统分配资源，完成用户交给的任务。然而病毒具有正常程序的所有特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，它会在正常程序执行前执行，病毒是动作、目的对用户是未知的，是未经用户允许的。3、隐蔽性：病毒一般具有很高的编程技巧、短小精悍的程序。通常附在正常程序中或磁盘比较隐蔽的地方，也有个别会以隐含文件形式出现。 正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到上百万台电脑中。4、潜伏性：大部分病毒在感染系统之后不会马上发作，它可以长期隐藏在系统中，只有在满足其特定条件时才启动其表现模块。这些病毒在平时都会隐藏得很好，只有在发作日才露出真面目。5、破坏性：所有病毒只要侵入系统，都会对系统或者应用程序产生不同程度的影响，轻者会降低计算机的工作效率，占用系统资源，严重者导致系统崩溃。恶性病毒则目标明确，或破坏数据、删除文件，或加密磁盘，格式化磁盘，有点对数据产生不可挽回的破坏。

前面我们提到网络病毒，那么网络病毒又有哪些呢？1、木马病毒：特洛伊木马是一种黑客程序，一般它并不破坏受害者在硬盘上保存的数据，而是悄悄的躲藏在被它感染的计算机中，只要这台计算机开始上网，黑客就能够通过因特网渠道来找到这台计算机，当开始在自己的计算机上远程操纵它时，窃取用户的上网账号和密码不易被察觉，并且随意修改和删除文件用户也可能并没有察觉。2、蠕虫病毒：蠕虫病毒和一般病毒存在很大的差别。随着网络的发展，蠕虫病毒可以在短短的时间内感染整个网络，从而造成网络瘫痪。蠕虫病毒的主动攻击和突然爆发这两个特性经常使人们手足无措。因为蠕虫病毒的感染目标是互联网内的全部计算机。3、黑客程序：一般的黑客程序都存在攻击性，它能够利用计算机上的漏洞远程操作控制计算机，更严重的是直接破坏计算机的程序；黑客程序一般会在用户的计算机中植入一个木马病毒，与木马病毒相互合作从而对计算机的安全构成威胁。4、网页病毒：网页病毒是利用计算机浏览的网页来进行破坏的病毒，它寄生在网页中。5、手机病毒：手机病毒能够导致用户的手机死机、关机、资料自动删除，对外发送垃圾邮件和自动拨打电话等，并且还会导致SIM卡和芯片损坏等。

面对如此多的病毒，我们应该采取一定的措施来预防。

1. 不要随便浏览不熟悉的网站，当我们打开一些网站时，总会淡出很多窗口。
2. 安装最新的杀毒软件，处理常见的恶意网页代码，还要及时对杀毒软件升级,这样才能保证你的计算机是受到保护的。
3. 安装防火墙。防火墙是根据连接网络的数据包来进行监控的，也就是说，防火墙就相当于一个严格的门卫，掌管系统的各扇门（端口），它负责对进出的人进行身份核实，每个人都需要得到最高长官的许可才可以出入，而这个最高长官，就是你自己了。
4. 要及时更新系统的漏洞，不要给病毒机会，不然病毒就会侵害你的计算机。

5.不能随便打开陌生的电子邮件附件，如果要一定要打开的话，就以纯文本方式阅读信件，现在的邮件病毒也是很猖狂，大家应该多留点心，对于陌生人的邮件，能不回复的则选择不回复，避免感染病毒。收到电子邮件时要先进行病毒扫描，不要随便打开不明电子邮件里携带的附件。

6.对公用软件和共享软件要谨慎使用，使用U盘时要先杀毒，以防U盘携带病毒传染计算机。

7.从网上下载的所有文件，必须先对它进行扫描，杀灭病毒，再对它使用。

8.对重要的文件要做备份，如果该文件遭到病毒的侵害，就很难再对修复了，造成不必要的损失。对已经感染病毒的计算机，可以下载最新的防病毒软件进行清除。

每个人的信息都是非常重要的，在这个信息化的社会，信息安全也至关重要，所以信息安全的保护也很重要。大家应该携手创造一个安全的信息化时代，为计算机营造一个美好的环境。作为一个软件工程学生，几乎每天都要和计算机打交道，如果不能很好的掌握计算机的信息保护，那么在以后的工作中将会遇到很多问题。我们也必须要做好信息系统安全教育，学习安全知识，使人们的安全意识能跟上高速发展的信息时代，加强安全管理。