1 网络信息安全与保密综论

1.1 网络信息安全与保密的内涵是什么？

网络信息安全与保密是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。从技术角度看，网络信息安全与保密是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。网络信息安全与保密的重要性有目共睹。特别是随着全球信息基础设施和各国信息基础设施的逐渐形成，国与国之间变得“近在咫尺”。网络化、信息化已成为现代社会的一个重要特征。网络信息本身就是时间，就是财富，就是生命，就是生产力。实际上，网络的快速普及、客户端软件多媒体化、协同计算、资源共享和开放、远程管理化，以及电子商务、金融电子化等已成为网络时代必不可少的产物。

事物总是辨证统一的。科技进步在造福人类的同时，也带来了新的危害。从某种意义上讲，网络信息系统的广泛普及，就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。网络信息系统中的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。网络信息安全与保密便是这些众多新课题中最具代表性的例子。

根据《汉语大词典》（罗竹风主编）的解释，“安全”有两层含义：其一是指“平安，无危险”；其二是指“保护、保全”。

“保密”，则指“保守事物的秘密，不使泄漏”。仅仅根据词典的解释，“网络信息安全与保密”的含义是比较明确的。但是，在具体的工程应用和社会实践中，情况就相当复杂了。

1.1.1 网络信息安全与保密的技术特征

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的技术特征主要表现在系统的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性可以用公式描述为 $R = \mathrm{MTBF}/(\mathrm{MTBF} + \mathrm{MTTR})$，其中 R 表示可靠性，MTBF 表示平均故障间隔时间，MTTR 表示平均故障修复时间。因此，增大可靠性的有效思路是增大平均故障间隔时间或者减少平均故障修复时间。增加可靠性的具体措施包括：提高设备质量，严格质量管理，配备必要的冗余和备份，采用容错、纠错和自愈等措施，选择合理的拓扑结构和路由分配，强化灾害恢复机制，分散配置和负荷等。

网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。

生存性是在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏

是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

2.可用性

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认，访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制），业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞），路由选择控制（选择那些稳定可靠的子网，中继线

或链路等），审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息)。

3.保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即，防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括：防侦收（使对手侦收不到有用的信息），防辐射（防止有用信息以各种途径辐射出去），信息加密（在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息），物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施,保护信息不被泄露)。

4.完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障，误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码），人为攻击，计算机病毒等。

保障网络信息完整性的主要方法有：

(1) 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段；

(2) 纠错编码方法：由此完成检错和纠错功能，最简单和常用的纠错编码方法是奇偶校验法；

(3) 密码校验和方法：它是抗窜改和传输失败的重要手段；

(4) 数字签名：保障信息的真实性；

(5) 公证：请求网络管理或中介机构证明信息的真实性。

5. 不可抵赖性

不可抵赖性也称作不可否认性。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。即，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送的信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等。

1.1.2 网络信息安全与保密的层次结构

网络信息安全与保密的结构层次主要包括：物理安全、安全控制和安全服务。

1. 物理安全

物理安全是指在物理介质层次上对存贮和传输的网络信息的安全保护。物理安全是网络信息安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。一方面，在各种软件和硬件系统中要充分考虑到系统所受的物理安全威胁和相应的防护措施；

另一方面，也要通过安全意识的提高、安全制度的完善、安全操作的提倡等方式使用户和管理维护人员在物理层次上实现对网络信息的有效保护。目前，该层次上常见的不安全因素包括三类：

(1) 自然灾害（比如，地震、火灾、洪水等），物理损坏（比如，硬盘损坏、设备使用寿命到期、外力破损等），设备故障（比如，停电断电、电磁干扰等）。此类不安全因素的特点是：突发性、自然性、非针对性。这种不安全因素对网络信息的完整性和可用性威胁最大，而对网络信息的保密性影响却较小，因为在一般情况下，物理上的破坏将销毁网络信息本身。解决此类不安全隐患的有效方法是采取各种防护措施，制定安全规章，随时进行数据备份等。

(2) 电磁辐射（比如，侦听微机操作过程），乘机而入（比如，合法用户进入安全进程后半途离开），痕迹泄露（比如，口令密钥等保管不善，被非法用户获得）等。此类不安全因素的特点是：隐蔽性、人为实施的故意性、信息的无意泄露性。这种不安全因素主要破坏网络信息的保密性，而对网络信息的完整性和可用性影响不大。解决此类不安全隐患的有效方法是采取辐射防护，屏幕口令，隐藏销毁等手段。

(3) 操作失误（比如，偶然删除文件，格式化硬盘，线路拆除等），意外疏漏（比如，系统掉电、“死机”等系统崩溃）。此类不安全因素的特点是：人为实施的无意性和非针对性。这种不安全因素主要破坏网络信息的完整性和可用性，而对保密性影响不大。解决此类不安全隐患的有效方法是：状态检测，报警确认，应急恢复等。

2. 安全控制

安全控制是指在网络信息系统中对存贮和传输的信息的操作和进程进行控制和管理，重点是在网络信息处理层次上对信息进行初步的安全保护。安全控制可以分为以下三个层次：

(1) 操作系统的安全控制

操作系统的安全控制包括：对用户的合法身份进行核实（比如，开机时要求键入口令），对文件的读写存取的控制（比如，文件属性控制机制）。此类安全控制主要保护被存贮数据的安全。

(2) 网络接口模块的安全控制

在网络环境下对来自其他机器的网络通信进程进行安全控制。此类控制主要包括身份认证、客户权限设置与判别、审计日志等。

(3) 网络互联设备的安全控制

对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。此类控制主要通过网管软件或路由器配置实现。

需要指明的是，安全控制主要通过现有的操作系统或网管软件、路由器配置等实现。安全控制只提供了初步的安全功能和网络信息保护。

3.安全服务

安全服务是指在应用程序层对网络信息的保密性、完整性和信源的真实性进行保护和鉴别，满足用户的安全需求，防止和抵御各种安全威胁和攻击手段。安全服务可以在一定程度上弥补和完善现有操作系统和网络信息系统的安全漏洞。安全服务的主要内容包括：安全机制、安全连接、安全协议和安全策略等。

(1) 安全机制

安全机制是利用密码算法对重要而敏感的数据进行处理的一系列技术和方法。比如，以保护网络信息的保密性为目标的数据加密和解密；以保证网络信息来源的真实性和合法性为目标的数字签名和签名验证；以保护网络信息的完整性，防止和检测数据被修改、插入、删除和改变的信息认证等。安全机制是安全服务乃至整个网络信息安全系统的核心和关键。现代密码学在安全机制的设计中扮演着重要的角色

(2) 安全连接

安全连接是在安全处理前与网络通信方之间的连接过程。安全连接为安全处理进行了必要的准备工作。安全连接主要包括会话密钥的分配和生成及身份验证。后者旨在保护信息处理和操作的对等双方的身份真实性和合法性。

(3) 安全协议

协议是多个使用方为完成某些任务所采取的一系列的有序步骤。协议的特性是：预先建立、相互同意、非二义性和完整性。安全协议使网络环境下互不信任的通信方能够相互配合，并通过安全连接和安全机制的实现来保证通信过程的安全性、可靠性和公平性。

(4) 安全策略

安全策略是安全机制、安全连接和安全协议的有机组合方式，是网络信息系统安全性的完整的解决方案。安全策略决定了网络信息安全系统的整体安全性和实用性。不同的网络信息系统和不同的应用环境需要不同的安全策略。

1.1.3 网络信息安全与保密的不同含义

与其他概念不同的是，网络信息安全与保密的具体含义和侧重点会随着观察者的角度而不断变化。比如：

从用户（个人用户或者企业用户）的角度来说，他们最为关心的网络信息安全与保密问题是如何保证他们的涉及个人隐私或商业利益的数据在传输过程中受到保密性、完整性和真实性的保护。避免其他入（特别是竞争对手）利用窃听、冒充、篡改、抵赖等手段对其利益和隐私造成损害和侵犯，同时用户也希望其保存在某个网络信息系统中的数据，不会受其他非授权用户的访问和破坏。

从网络运行和管理者角度来说，他们最为关心的网络信息安

全与保密问题是如何保护和控制其他人对本地网络信息的访问、读写等操作。比如，避免出现“陷门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等现象，制止和防御网络“黑客”的攻击。

对安全保密部门和国家行政部门来说，他们最为关心的网络信息安全与保密问题是如何对非法的、有害的或涉及国家机密的信息进行有效过滤和防堵，避免非法泄露。机密敏感的信息被泄密后将会对社会的安定产生危害，对国家造成巨大的经济损失和政治损失。

从社会教育和意识形态角度来说，他们最为关心的网络信息安全与保密问题是如何杜绝和控制网络上不健康的内容。有害的黄色内容会对社会的稳定和人类的发展造成不良影响。

1.1.4 网络信息安全与保密的环境变迁

网络信息安全与保密还会因为不同的应用环境得到不同的解释。大体上可以分为：

(1)运行系统安全

即保证网络信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，硬件系统的可靠运行，操作系统的安全，电磁信息泄露的防护等。安全的运行系统侧重于保证网络信息系统的正常运行。避免因为系统崩溃和损坏而对存贮、处理和传输的信息造成破坏和损失。避免由于电磁泄漏，产生信息泄露，干扰他人，或被他人干扰。运行系统安全的本质是保护系统的合法操作和正常运行。

(2) 网络系统信息的安全

比如：用户口令鉴别、用户存取权限控制、数据存取权限和方式控制、安全审计、安全跟踪、计算机病毒防治、数据加密等。

(3) 网络信息传播的安全

即网络信息传播后果的安全。比如，对不良网络信息进行有效过滤。网络信息传播的安全侧重于防止和控制非法、有害的信息传播。避免公用网络信息系统中大量自由传输的数据失控。网络信息传播安全的本质是维护社会道德、国家法规和人民利益。

(4) 网络信息内容的安全

它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用网络信息系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。网络信息内容安全的本质是保护用户的利益和隐私。

由此可见，网络信息安全与保密是一个很复杂的问题，它与被保护的对象密切相关。还有一种观点认为，网络信息安全与保密包括以下几个方面：物理安全、人员安全、符合瞬时电磁脉冲辐射标准、信息安全、操作安全、通信安全、计算机安全、工业安全等。网络信息安全与保密的本质是在安全期内保证数据在网络上传输或存贮时不被非授权用户非法访问，但授权用户却可以访问。

1.2 网络信息安全与保密的威胁有哪些？

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中的存储与传输的数据安全问题更为关注。如果因为安全因素使得信息不敢放进因特网这样的公共网络，那么办公效率及资源的利用率都会受到影响，甚至使得人们丧失了对因特网及信息高速公路的信赖。

事物总是辨证的。一方面，信息系统的网络化提供了资源的共享性、用户使用的方便性，通过分布式处理提高了系统效率和可靠性，并且还具有可扩充性。另一方面，也正是以上特点增加了网络信息系统的不安全性。

1.2.1 恶意攻击

网络信息的安全与保密所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威 胁 。

自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些无目的的事件，有时会直接威胁网络信息安全，影响信息的存储媒体。但此类威胁和破坏不是恶意的，故不在讨论之列。

本书重点讨论人为威胁。此种威胁，通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，造成不可估量的经济和政治上的损失。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故），另一种是以计算机犯罪为代表的有意威胁，即恶意攻击。

虽然人为的偶然事故没有明显的恶意企图和目的，但它会使信息受到严重破坏。最常见的偶然事故有：操作失误（未经允许使用、操作不当、误用存储媒体等），意外损失（电力线路搭接、漏电、电焊火花干扰），编程缺陷（经验不足、检查漏项、水平所限），意外丢失（被盗、被非法复制、丢失媒体），管理不善（维护不力、管理薄弱、纪律松懈），无意破坏（犁地割线等无意损坏）。

人为的恶意攻击是有目的的破坏。恶意攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如：修改、删除、伪造、添加、重放、乱序、冒充、制造病毒

等）。被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦收、截获、窃取、破译和业务流量分析及电磁泄露等。

由于人为恶意攻击有明显企图，其危害性相当大，给国家安全、知识产权和个人信息带来巨大的威胁。人为恶意攻击具有以下特性：

智能性　从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高，许多人都是具有一定社会地位的部门业务主管。他们在攻击前都经过了周密预谋和精心策划。

严重性　涉及到金融资产的网络信息系统恶意攻击，往往会由于资金损失巨大，而使金融机构、企业蒙受重大损失，甚至导致破产。同时，也给社会稳定带来震荡。如美国资产融资公司计算机欺诈案，涉及金额 20 亿美元之巨，犯罪影响震荡全美。在我国也发生过数起计算机盗窃案，金额从数万到数百万元人民币不等，给国家金融资产带来严重损失。

隐蔽性　人为恶意攻击的隐蔽性很强，不易引起怀疑，作案的技术难度大。一般情况下，其犯罪的证据，存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。相反，犯罪行为人却可以很容易地毁灭证据。计算机犯罪的现场也不像是传统犯罪现场那样明显。

多样性　随着计算机互联网的迅速发展，网络信息系统中的恶意攻击也随之发展变化。出于经济利益的巨大诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻击手段不断翻新，新的攻击目标涉及偷税漏税、利用自动结算系统洗钱以及在网络上进行盈利性的商业间谍活动，等等。

国际互联网上以人为恶意攻击为代表的高技术犯罪的另一大发展趋势是网络犯罪集团化。由于网络上的安全机制不断加强，今后的网络犯罪将需要比今天高得多的技术力量，这种客观要求

加上网络上日益增长的经济利益将诱使计算机犯罪集团，尤其是跨国犯罪集团将黑手伸向网络信息系统。届时，传统犯罪活动和网络犯罪的融合将对各国司法当局和国际反犯罪机构提出更大的挑战。

下面简要介绍一些有代表性的恶意攻击。

信息战　这是一种以获得控制信息权为目标的无硝烟的战争。信息战可以说是一种国家行为的恶意攻击。信息战的攻击目标包括各种军事命令、通信系统、能源、运输和金融等与国家的政治、经济、文化密切相关的系统。在和平时期，信息战处于绝对隐蔽状态。一旦战争爆发，信息战将出其不意地发挥出巨大的破坏力。美军在伊拉克实施的“沙漠风暴”战争便是典型的信息战战例。

商业间谍　利用国际互联网收集别国的重要商业情报，其目标是获得有价值的信息、能力、技术和对自身有利的谈判地位。在多数情况下，商业间谍属于一种集团行为的恶意攻击。

除了以信息战为代表的国家行为恶意攻击和以商业间谍为代表的集团行为恶意攻击之外，还有众多的个人行为或者小团体行为的恶意攻击。此类恶意攻击数量巨大，目的复杂。有的恶意攻击者来自窃贼、骗子、敲诈、贩毒、犯罪组织成员和其他有犯罪行为的人。有的恶意攻击者来自黑客、恶意竞争者、心怀不满的工作人员、个人仇敌等。此类恶意攻击的典型代表有：

窃听　在广播式网络信息系统中，每个节点都能读取网上的数据。对广播网络的基带同轴电缆或双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得偷听网上的数据或非授权访问很容易且不易被发现。

流量分析　它能通过对网上信息流的观察和分析推断出网上

的数据信息，比如有无传输，传输的数量、方向、频率等。因为网络信息系统的所有节点都能访问全网，所以流量的分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也有益于进行有效的流量分析。

破坏完整性　有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改。

重发　重发是重复一份报文或报文的一部分，以便产生一个被授权效果。当节点拷贝发到其他节点的报文并在其后重发它们时，如果不能监测重发，节点依据此报文的内容接受某些操作，例如报文的内容是关闭网络的命令，则将会出现严重的后果。

假冒　当一个实体假扮成另一个实体时，就发生了假冒。一个非授权节点，或一个不被信任的、有危险的授权节点都能冒充一个授权节点，而且不会有多大困难。很多网络适配器都允许网帧的源地址由节点自己来选取或改变，这就使冒充变得较为容易。

拒绝服务　当一个授权实体不能获得对网络资源的访问或当紧急操作被推迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议而引起（如，传输了错误的信号或在不适当的时候发出了信号），也可能由超载而引起。

资源的非授权使用　即与所定义的安全策略不一致的使用。因常规技术不能限制节点收发信息，也不能限制节点侦听数据，一个合法节点能访问网络上的所有数据和资源。

干扰　干扰是由一个节点产生数据来扰乱提供给其他节点的服务。干扰也能由一个已经损坏的并还在继续传送报文的节点所引起，或由一个已经被故意改变成具有此效果的节点所引起。频繁的令人讨厌的电子邮件信息是最典型的干扰形式之一。

病毒　目前，全世界已经发现了上万种计算机病毒。它们的

类型及数量大体为：DOS型10 000～11 000种、Windows型12种、UNIX型6种、宏病毒200余种、Macintosh型35种和众多的E-mail病毒。计算机病毒的数量已有了相当的规模，并且新的病毒还在不断出现。比如，最近保加利亚计算机专家迈克·埃文杰制造出了一种计算机病毒“变换器”，它可以设计出新的更难发现的“多变形”病毒。该病毒具有类似神经网络细胞式的自我变异功能，在一定的条件下，病毒程序可以无限制地衍生出各种各样的变种病毒。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加，计算机病毒已经构成了对计算机系统和网络的严重威胁。

诽谤　利用网络信息系统的广泛互联性和匿名性，散布错误的消息以达到诋毁某人或某公司形象和知名度的目的。

1.2.2　安全缺陷

假如网络信息系统本身没有任何安全缺陷，那么恶意攻击者即使有天大的本事也不能对网络信息安全和保密构成威胁。遗憾的是现在所有的网络信息系统都不可避免地存在着这样或那样的安全缺陷。有些安全缺陷是可以通过人为努力加以避免或者改进的，但有些安全缺陷则是折衷各种需要所必须付出的代价。

1. 普遍存在的安全缺陷

网络信息系统是计算机技术和通信技术的结合。计算机系统的安全缺陷和通信链路的安全缺陷构成了网络信息系统的潜在安全缺陷。计算机硬件资源易受自然灾害和人为破坏；软件资源和数据信息易受计算机病毒的侵扰、非授权用户的复制、篡改和毁坏。计算机硬件工作时的电磁辐射以及软硬件的自然失效、外界电磁干扰等均会影响计算机的正常工作。通信链路易受自然灾害和人为破坏。采用主动攻击和被动攻击可以窃听通信链路的信息并非法进入计算机网络获取有关敏感性重要信息。网络信息系统

的安全缺陷通常包括物理网络的安全缺陷、过程网络的安全缺陷以及通信链路安全缺陷三种。一些普遍存在的安全缺陷、安全问题和安全脆弱性包括：

网络的规模　网络的规模越大，通信链路越长，则网络的脆弱性和安全问题也随之增加。网络用户数量的增加，网络的安全性威胁也随之增加。在大规模的网络信息系统中，由于终端分布的广泛性和地理位置的不同，网络分布在几百至上千公里的范围内，通常用有线信道（同轴电缆、架空明线或光缆等）和无线信道（卫星信道、微波干线等）来作为通信链路。对有线信道而言，分布式网络易受自然和人为破坏，非授权用户可以通过搭线窃听攻击侵入网内获得有关重要信息，甚至可以插入、删除信息。由于串音和电磁辐射，导致网络信噪比下降，误码率增加，信息的安全性、完整性和可用性受到威胁。无线信道的安全脆弱性更加显而易见，被动攻击几乎不可避免。

电磁辐射和电磁泄漏　计算机及其外围设备在进行信息处理时会产生电磁泄漏，即电磁辐射。电磁辐射分辐射发射和传导发射两种。当计算机设备在进行数据处理和传输时，各种高频脉冲通过各种电器元件和分布参数的耦合、调制，叠加成一个包含有用信息的频带信号，由电源线、电缆和电话线等通信链路传导出去造成信息泄漏。而当各种高频脉冲通过电路元件（电阻、电容、集成电路片等）传导时，又会向空中以电磁波的形式辐射信息，从而导致信息泄漏。在计算机中，以视屏显示器的辐射发射最为严重。由于计算机网络传输媒介的多样性和网内设备分布的广泛性，使得电磁辐射造成信息泄漏的问题变得十分严重。国外一些发达国家研制的设备能在一公里以外收集计算机站的电磁辐射信息，并且能区分不同计算机终端的信息。因此，电磁辐射已对网络信息的安全与保密构成严重威胁。

搭线　现行计算机网络的传输媒介主要是同轴电缆和现有电

话线路等，这为搭线窃听提供了可能。搭线窃听的手段主要有两种：其一，利用磁记录设备或计算机终端从信道中截获有关计算机信息，然后对记录信息进行加工、综合、分析，提取有用信息；其二，搭线者不仅截获有关信息，而且试图更改、延迟被传送的信息，从而造成更大的威胁。例如，在具有现金分配能力的自动出纳机（ATM）中，前者可以使攻击者获得为冒充合法用户所必需的信息（个人识别符、 PASSWORD等），而后者则可以使攻击者能够插入未经认可的报文以非法手段获取资金。

串音　在有线通信链路中（光纤除外），由于电磁泄漏和信道间寄生参数的交叉耦合，当一个信道进行信息传送时，会在另一个或多个相邻信道感应出信号或噪声即串音。串音也可能由网络交换中心产生。串音不但使网络内的噪声增加，传输的信息发生畸变，而且会引起传导泄漏，对信息保密构成威胁。

2　中国特色的安全缺陷

中国是一个发展中国家。我们的网络信息安全系统除了具有上述普遍存在的安全缺陷之外，还具有其他一些独具特色的安全缺陷。比如：

(1) 由技术被动性引起的安全缺陷

首先，我们的芯片基本依赖于进口，即使是自己开发的芯片也需要到国外加工。只有当我国的半导体和微电子技术取得突破性进展之后，才能从根本摆脱这种受制于人的状态。

其次，为了缩小与世界先进水平的差距，我国引进了不少外国设备，但这也同时带来了不可轻视的安全缺陷。比如，大部分引进设备都不转让知识产权，我们很难获得完整的技术档案。这就为今后的扩容、升级和维护带来了麻烦。更可怕的是，有些引进设备可能在出厂时就隐藏了恶意的“定时炸弹”或者“后门”。在非和平时期，这些预设的“机关”有可能对我们的网络信息安全与保密构成致命的打击。

再者，新技术的引入也可能带来安全问题。攻击者可能用现