网络安全

网络的安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护。而从企业的角度来说，最重要的就是内部信息上的安全加密以及保护。

网络安全的重要性

计算机存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转，不可替代的，而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间，核辐射环境等等，出错率和故障的增多必将导致可靠性和安全性的降低。

随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能不足。

计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等等。

从认识论的高度看，人们往往首先关注系统功能，然后才被动的从现象注意系统应用的安全问题。因此广泛存在着重应用、轻安全、法律意识淡薄的普遍现象。许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的。

网络面临的危险

覆盖全球的 Internet，以其自身协议的开放性方便了各种计算机网络的入网互连，极大地拓宽了共享资源。但是，由于早期网络协议对安全问题的忽视，以及在使用和管理上的无序状态，网络安全受到严重威胁，安全事故屡有发生。从目前来看，网络安全的状况仍令人担忧，从技术到管理都处于落后、被动局面。

犯罪目前已引起了社会的普遍关注，其中计算机网络是犯罪分子攻击的重点。计算机犯罪是一种高技术犯罪手段，由于其犯罪的隐蔽性，因而对网络的危害极大。根据有关统计资料显示，计算机犯罪案件每年以 100%的速度急剧上升，Internet 被攻击的事件则以每年 10 倍的速度增长，平均每 20s 就会发生一起 Internet 入侵事件。从 1986 年首次出现以来，30 多年来以几何级数增长，对网络造成了很大的威胁。国防部和银行等要害部门的计算机系统都曾经多次遭到非法入侵者的攻击。

随着 Internet 的广泛应用，采用客户机/服务器模式的各类网络纷纷建成，这使网络用户可以方便地访问和共享网络资源，但同时对企业的重要信息，如贸易秘密、产品开发计划、市场策略、财务资料等的安全无疑埋下了致命的隐患。必须认识到，对于大到整个 Internet，小到各 Internet 及各校园网，都存在来自网络内部与外部的威胁。对 Internet 构成的威胁可分为两类：故意危害和无意危害。

总地来说，网络面临的威胁主要来自以下几个方面。

黑客的攻击。对于大家来说，黑客已经不再是高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展。因此，系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，黑客攻击的隐蔽性好、“杀伤力”强，这都是网络安全的主要威胁。

管理的欠缺。网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。目前，美国 75%～85%的网站都抵挡不住黑客的攻击，约有 75%的企业网上信息失窃，其中 25%的企业损失在 100 万美元以上。

网络的缺陷。Internet 的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 簇缺乏相应的安全机制，而且 Internet 最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此在安全可靠、服务质量、带宽和方便性等方面存在不适应性。

软件的漏洞或“后门”。随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免，如常用的操作系统，无论是 Windows 还是 UNIX，几乎都存在或或少的安全漏洞，众多的各类服务器、浏览器、桌面软件等都被发现过存在安全隐患。大家熟悉的“尼姆达”“中国黑客”等病毒都是利用微软系统的漏洞从而给企业造成巨大损失的，可以说任何一个软件系统都可能会因为程序员的疏忽、设计中的缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

企业网络内部。网络内部用户的误操作、资源滥用和恶意行为令再完善的防火墙也无法抵御。防火墙无法防止来自网络内部的攻击，也无法对网络内部的滥用做出反应。