下一代 Internet 面临的安全问题

随着计算机网络和 Internet 的出现与发展，信息技术已成为 20 世纪科技领域的新宠儿。今天，Internet 已成为最大规模的全球性计算机网络，对人类的社会和经济活动产生的影响日益显著。然而，同其他学科一样，信息技术的发展也不是一帆风顺的。因冷战的需要而诞生于 60 年代的计算机网络理论和技术在经历了 30 年的发展之后，已变得越来越不能适应今天和未来网络应用发展的需要。受传统网络理论的局限，今天的 Internet 在服务质量、数据处理与传输速度等诸多方面都不能满足新的应用要求，安全问题尤为突出：网络的抗入侵和抗毁能力很低，缺乏全局协调的安全基础设施，不能满足诸如国家安全、经济竞争等重要任务的要求------因此，发展新的网络理论体系、解决网络的安全问题已经成为当务之急。

1997 年 5 月，在美国计算机研究学会上，一批来自学术界、企业界和政府部门的著名专家就下一代 Internet (NGI)所面临的挑战作了讨论。会议认为，由于网络规模的不断膨胀、可用的计算资源更多、新技术的引入和应用更新加快，因而可能会产生更多的安全问题。所以，在设法解决当前网络的安全问题的同时，还要考虑 NGI 可能面临的新的安全需求。

应重点考虑的安全问题包括计算机病毒、非法访问和攻击、服务失效攻击（如使得 WEB 服务器不能正常工作，从而影响电子商务的进行）和由配置错误所引起的故障（如 Internet 的大面积瘫痪）。具体地说，在网络安全方面的研究内容包括：

基础设施的坚定性 NGI 将沿用传统的路由协议，因此目前正在加紧研究 BGP 和 OSPF 的安全性问题，重点是路由信息的完整性和鉴别，以及对 BGP 的授权，以便使安全故障的影响面尽可能小。现在需要的是用这些技术对现有的网络设备（路由器）进行改造并逐渐向未来的网络设备过渡。

基础设施的另一些安全问题尚未提到议事日程，其中包括对利用网络控制算法和阻塞控制算法的自愈性进行攻击的防御方法（目前的算法不能分辨故障报告的真实性）；以及多址和 QOS 的授权机制等。网络的同构性导致安全性的降低，而网络的异构性则导致管理难度的增加，目前的趋势是平台的同构性。

安全政策 当前安全政策的特点是静态的、难管理、难调整、粗粒度，并且不能直接被端系统用户控制。这些安全政策往往是通过管理员在防火墙和服务器中设置访问控制来实现的，它们带来的问题是共享跨越管理域的信息变得几乎不可能，因为面向用户的安全政策管理是非常困难和低效的，所以正常用户和攻击者具有相同的数据共享范围。因此，要求安全政策的粒度可变并可强制实施，以满足动态合作的需求；并相应地改进安全管理的用户界面。这些改进需要系统软件的支持，包括可提供更细粒度访问控制的安全操作系统和强类型语言（如 JAVA）。

可移动的代码 JAVA、ActiveX 和智能代理等概念的兴起增加了对可移动代码安全性研究的要求。首要的问题是如何定义、实施和管理移动代码在本地环境中的访问控制，要细致到每个移动代码模块和每个工作站。另外要考虑移动代码的模型，还要考虑服务在本地被拒绝或降级的情形。

要研究“带证明的代码”机制，要求移动代码的编写者将该代码满足本地环境访问控制要求的证明附接在移动代码之后随之一起移动，这种证明可以是传统的、形式化方式的，也可以是一段运行代码，以保证移动代码在执行时不违反访问控制约束。移动代码在执行前，

用户或管理员可对其进行正确性检查（包括完整性检查）。

智能代理是一种特殊的移动代码，它按用户的要求代为收集数据或执行处理。因此，对于智能代理，还要考虑它的数据在传输过程中的安全性机制，对委托给该代理的用户资源的保护等问题。

入侵检测 现有的入侵检测手段是基于已知的安全漏洞并针对单个计算机或小规模网络进行的。为提供大范围的入侵检测的手段，DARPA 正在组织研究入侵检测的通用框架。另外，自纠正和自诊断系统也是研究的方向。目前的入侵检测需要较多的系统资源，包括处理时间和带宽。在不同管理域之间作追踪的协调是一件困难的事情，而且追踪还涉及合法性和个人隐私保护等法律问题。

PKI PKI 对于电子商务和移动代码等都有及其重要的作用，它能为大规模的身份鉴别、事务加密和无否认等服务提供支持。美国的社会保险署和国内收入署都在实验使用 RKI 来支持他们的业务（以满足大量用户的使用），试验提供大规模的 PKI 的方法。

需要研究的问题有：出现故障时对超大规模系统的影响；在大规模 PKI 系统中进行证书撤销的方法；不同 PKI 的互连方法，等内容。这些研究所涉及的领域包括经济、法律、社会学和技术等方面。

安全管理 改进异构安全系统的管理能力，防止因不良的管理界面而导致系统的误配置，进而导致系统的误操作。

密码学 要研究高速传输和交换环境中的加密算法和信息摘录算法及其实现（软件及硬件的形式）。要研究适用于多址环境的加密协议、密钥管理协议和签名方法。另外，密钥恢复机制（尤其在大规模环境中）要成为研究的重点，以提高在允许使用加密技术条件的密文管理能力。

操作系统 根据 CERT 的研究，50％以上的网络安全问题是由于系统（尤其是软件工程的问题）的弱点造成的，而且无法仅靠使用加密技术来克服。美国政府投资研究安全的操作系统已有 20 多年的历史，但其成果基本上没有进入民用领域，尤其是在桌面计算机方面。要研究适用于网络环境的安全操作系统，仅增加审计功能是不够的。另外要研究评价计算机操作系统安全性的标准体系。

软件工程 在许多方面，软件工程成为解决网络安全问题的核心，要在软件的设计与实现阶段就开始考虑安全问题。

网络管理 要求网络管理系统支持基础设施的坚定性，从系统的角度而不是从单个被管对象的角度考虑问题，例如支持对入侵的联合追踪。

总而言之，今天的 Internet 已不能适应新的应用在数量和性质上的需求。从当前的趋势看，网络研究正呈螺旋式的形式向前发展，网络推动应用，应用驱动网络，因此需要不断地构建试验床，用螺旋式发展的理论来理解未来的网络需求。进入 90 年代以来，计算机互联网络面临两个挑战：进一步扩大用户规模和使更复杂的新应用上网，这需要研究新的概念和网络体系结构以支持超大规模互联网络的设计、管理和应用。信息社会和正在逐渐形成的全球化知识经济形态对计算机网络提出的新要求，需要人们对现有的计算机网络功能结构进行扩充和调整，构造出新的计算机网络功能模型、协议体系结构和一系列新型的关键协议和单元技术理论。这种新的协议体系结构应不存在安全缺陷，并同时具有主动性、适应性、可扩展性和服务的可集成性等特征。这些新的理论和方法将突破传统理论的限制，可处理在规模和复杂性发生量级变化的网络信息交换问题和网络安全问题，适应超大、超高速计算机网络

的需要。这将改变目前这种需要对现有体系结构不断进行修修补补的被动状态，为从根本上解决未来较长一段时期内网络应用对计算机网络安全性、实时性、可管理性、可用性等方面的要求提供理论基础。