入侵检测方法一般可以分为基于特征的入侵检测和基于异常的入侵检测两种。

基于特征的 IDS 维护一个所有已知攻击标志性特征的数据库。每个特征是一个与某种入侵活动相关联的规则集，这些规则可能基于单个分组的首部字段值或数据中特定比特串，或者与一系列分组有关。当发现有与某种攻击特征匹配的分组或分组序列时，则认为可能检测到某种入侵行为。这些特征和规则通常由网络安全专家生成，机构的网络管理员定制并将其加入到数据库中。

基于特征的 IDS 只能检测已知攻击，对于未知攻击则束手无策。基于异常的 IDS 通过观察正常运行的网络流量，学习正常流量的统计特性和规律，当检测到网络中流量的某种统计规律不符合正常情况时，则认为可能发生了入侵行为。例如，当攻击者在对内网主机进行 ping 搜索时，或导致 ICMP ping 报文突然大量增加，与正常的统计规律有明显不同。但区分正常流和统计异常流是一件非常困难的事情。至今为止，大多数部署的 IDS 主要是基于特征的，尽管某些 IDS 包括了某些基于异常的特性。

不论采用什么检测技术都存在“漏报”和“误报”情况。如果“漏报”率比较高，则只能检测到少量的入侵，给人以安全的假象。对于特定 IDS，可以通过调整某些阈值来降低“漏报”率，但同时会增大“误报”率。“误报”率太大会导致大量虚假警报，网络管理员需要花费大量时间分析报警信息，甚至会因为虚假警报太多而对报警“视而不见”，使 IDS 形同虚设。

7.7 一些未来的发展方向

本章介绍了网络安全的主要概念。网络安全是一个很大的领域，无法在这进行深入的探讨。对于有志于这一领域的读者，可在下面几个方向做进一步的研究：

(1) 椭圆曲线密码 ECC　目前椭圆曲线密码已在 TLS 1.3 的握手协议中占据非常重要的地位。此外，在电子护照和金融系统中也大量使用椭圆曲线密码系统。在互联网上已有许多关于椭圆曲线密码的资料。限于篇幅，无法在本书中进行介绍。

(2) 移动安全(Mobile Security)　移动通信带来的广泛应用（如移动支付，Mobile Payment）向网络安全提出了更高的要求。

(3) 量子密码(Quantum Cryptography)　量子计算机的到来将使得目前许多使用中的密码技术无效，后量子密码学(Post-Quantum Cryptography)的研究方兴未艾。

(4) 商密九号算法 SM9　为了降低公钥和证书管理的复杂性，早在三十多年前提出的标识密码(Identity-Based Cryptography)，现在又被重视。标识密码把用户的标识（如手机号码）作为公钥，使得安全系统变得易于部署和管理。2008 年标识密码算法正式获得我国密码管理局签发为商密九号算法 SM9。此算法不需要申请数字证书，适用于互联网应用的各种新兴应用的安全保障，其应用前景值得关注。

本章的重要概念

- 计算机网络上的通信面临的威胁可分为两大类，即被动攻击（如截获）和主动攻击（如中断、篡改、伪造）。主动攻击的类型有更改报文流、拒绝服务、伪造初始化、恶意程序（病毒、蠕虫、木马、逻辑炸弹、后门入侵、流氓软件）等。
- 计算机网络安全主要有以下一些内容：机密性、端点鉴别、信息的完整性、运行的