（2）加密解密（掌握）

发信者将明文数据加密成密文，然后将密文数据送入网络传输或存入计算机文件，而且只给合法收信者分配密钥。合法收信者接收到密文后，实行与加密变换相逆的变换，去掉密文的伪装并恢复出明文，这一过程称为解密（Decryption）。解密在解密密钥的控制下进行。用于解密的一组数学变换称为解密算法。

加密技术包括两个元素：**算法和密钥**。

密码体制	数据加密技术	典型代表	特点
对称密钥体制	对称加密（私人密钥加密）	DES	加密密钥和解密密钥相同
非对称密钥体制	非对称加密（公开密钥加密）	RSA	加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密

（3）安全行为分析技术（掌握）

虽然大多数的攻击可能来自组织以外，但最严重的损害往往是由内部人员造成的，只有管理好内部威胁，才能保证信息和网络安全。

用户和实体行为分析 （User and Entity Behavior Analytics，UEBA）提供了用户画像及基于各种分析方法的异常检测，结合基本分析方法（利用签名的规则、模式匹配、简单统计、阈值等）和高级分析方法（监督和无监督的机器学习等），用打包分析来评估用户和其他实体（主机、应用程序、网络、数据库等），**发现与用户或实体标准画像或行为异常的活动所相关的潜在事件**。UEBA 以用户和实体为对象，利用大数据，结合规则以及机器学习模型，并通过定义此类基线，对用户和实体行为进行分析和异常检测，尽可能快速地感知内部用户和实体的可疑或非法行为。

从架构上来看，UEBA 系统通常包括**数据获取层、算法分析层和场景应用层**。

（4）网络安全态势感知（掌握）

网络安全态势感知（Network Security Situation Awareness）是在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示，并据此**预测未来的网络安全发展趋势**。安全态势感知不仅是一种安全技术，也是一种新兴的安全概念。它是**一种基于环境的、 动态的、整体的洞悉安全风险的能力**。安全态势感知的前提是**安全大数据**，其在安全大数据的基础上进行数据整合、特征提取等， 然后应用一系列态势评估算法生成网络的整体态势状况， 应用态势预测算法预测态势的发展状况，并使用数据可视化技术，将态势状况和预测情况展示给安全人员，方便安全人员直观便捷地了解网络当前状态及预期的风险。

网络安全态势感知的关键技术主要包括：**海量多元异构数据的汇聚融合技术、面向多类型的网络安全威胁评估技术、网络安全态势评估与决策支撑技术、网络安全态势可视化等**。

2.2 新一代信息技术及应用

1、物联网（掌握）

物联网（TheInternet of Things）是**指通过信息传感设备，按约定的协议将任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的网络**。

1.技术基础

物联网架构可分为三层：**感知层 、网络层和应用层**。**【口诀：敢裸泳】**感知层由各种传感器构成，包括温度传感器，二维码标签 、RFID 标签和读写器，摄像头，GPS 等感知终端。**感知层**是物联网识别物体、采集信息的来源。**网络层**由各种网络，包括互联网、广电网、网络管理系统和**云计算平台**等组成，是整个物联网的中枢，负责传递和处理感知层获取的信息。**应用层**是物联网和用户的接口，它与行业需求结合以实现物联网的智能应用。

2.关键技术