1. 信息安全的目标是保护网络与信息系统中信息的机密性、完整性、不可抵赖性、可用性和可控性等信息安全属性。

2. (1)信息泄露 (2)非授权的篡改 (3)拒绝服务
(4)非法使用(非授权访问) (5)假冒
(6)抵赖 (7)网络与系统攻击 (8)恶意代码
(9)自然灾害 (10)人为失误和故意破坏

3. 拒绝服务攻击：目的是使计算机或网络无法提供正常的服务。通常采用耗尽网络资源或耗尽可用的操作系统资源等方式导致合法用户的请求无法被处理。

缓冲区溢出攻击：利用缓冲区溢出漏洞，向缓冲区填充超过缓冲区容量的数据量，使溢出数据覆盖合法数据，从而导致程序运行失败，系统关机重启等后果。

拒绝服务攻击破坏了信息安全的可用性，因为拒绝服务攻击导致合法的用户无法正常使用信息系统，使信息系统的服务不能维持运行。

而缓冲区溢出攻击破坏了信息安全的可用性与可控性。因为缓冲区溢出攻击会导致程序失效和系统关机重启等，使得合法用户不能使用信息系统，同时，破坏了管理员对于信息系统的掌握与控制，因此其破坏了可用性与可控性。

4. ①对于手机中的保密资料如照片文件等，可设置输入密码后才可查看。

②某些应用想要获取手机的位置信息时，需要持有者（管理者）授予相应的权限才可以访问。