(1)

信息安全的三要素：机密性，完整性，可用信性

机密性：往往通过访问控制阻止非授权用户获得机密的信息，通过加

密变换阻止非授权用户获知信息内容

完整性：通过访问控制阻止篡改行为，同时通过消息摘要算法来检验

信息是否被篡改。

可用信：是信息资源服务功能和性能可靠性的度量，涉及各方面的因

素，是对信息网络总体可靠性的要求

(2) 主要威胁有：意外事件和人为攻击两大类，精心设计的人为恶意攻击威胁最大

包括：信息泄露，非授权的篡改，拒绝服务，非法使用，假冒，抵赖，

网络与系统攻击，恶意代码，自然灾害，人为失误或故意破坏。

(3)

拒绝攻击服务：是指攻击者通过发送大量服务或操作请求使服务程序难

以正常运行的情况，

破坏了可用性A：这是由于在拒绝攻击服务下，普通用户会无法得到随时可提

供的信息资源。

缓冲区溢出攻击：属于针对于主机的攻击，利用堆栈结构，通过写入超过预定

长度的数据造成溢出。

破坏了机密性与完整性，可靠性，可用性。当主机遭受缓冲区溢出攻击，若使主机root

权限被得到，则正常的服务器功能会遭受破坏，内部资源也会暴露，所存储的数

据可被修改。

(4) 手机上的访问控制：

① 一般广。智能手机在刷机时需要获得root权限，此时通过设置中获取root权限时便是一种改变身份认证并成为超级用户 superuser 的情况，此时是在此处应用了访问控制的技术 从厂家接取权限

② 在智能手机应用APP中，如有许多APP存在会员尊享特权项目，在身份认证中改变判断用户的属性位给予改用户相应的权限，如非法的用户需注册，合法非VIP用户只能访问部份资源，合法的VIP用户可访问更多资源。