homework1

吴承泽 SA23011083

Chapter1

1、如果你的网络服务器被黑客远程控制，列举3个可能被破坏的安全属性，并解释理由。

可能破坏的3种属性包含 **机密性、完整性、可用性**，理由如下所示：

机密性：

黑客在网络服务器中可能非法访问了服务器中的信息，导致信息被未授权的用户（黑客）访问，从而获知信息内容。

完整性：

黑客在网络服务器中可能篡改生成、传输或存储的信息，导致数据完整性或系统完整性被破坏，使得网络服务器数据被污染。

可用性：

网络服务器被黑客远程控制后，黑客修改服务程序内容，导致服务器宕机无法再随时提供信息资源服务，此时破坏了可用性。

2、简述RFC2828安全服务的定义，例举Windows10系统的3种安全服务。

RFC 2828对安全服务做出了更加明确的定义：安全服务是一种由系统提供的对资源进行特殊保护的进程或通信服务。Windows系统下的安全服务包括：

1）**Windows Defender**，Windows自带的杀毒软件和恶意软件防护工具。

2）**Windows防火墙**，阻止未经授权的网络访问，提供基本的网络安全。

3）**BitLocker**，BitLocker是Windows的全磁盘加密工具，用于保护硬盘上的数据免受未经授权的访问。

3、简述网络安全防护主要目标的“五不”。

网络安全防护的主要目标可以归结为“五不”：**进不来、拿不走、 看不懂、改不了、走不掉。**

1)“**进不来**”：使用访问控制机制，允许授权用户访问，阻止非授 权用户进入网络，从而保证网络系统的可控性和可用性；

2)“**拿不走**”：使用授权机制，实现对用户的权限控制，同时结合 内容审计机制，实现对网络资源及信息的可控性；

3)“**看不懂**”：使用加密机制，确保信息不暴露给未授权的实体或 进程，从而实现信息的保密性；

4)“**改不了**”：使用数据完整性鉴别机制，保证只有得到允许的人 才能修改数据，从而确保信息的完整性和真实性；

5)“**走不掉**”：使用审计、监控、防抵赖等安全机制，使得破坏者 走不掉。并进一步对网络出现的安全问题提供调查依据和手段， 实现信息安全的可审查性。

Chapter3

1、在腾讯会议系统中，对称密码技术和公钥密码技术适合应用在哪几个阶段？说明理由。

公钥密码技术适用于身份验证阶段，在会议系统中用户登录的过程可以通过存储在服务器中的公钥与本地私钥进行协商验证，确保参与者的身份以及安全地交换对称密钥，以便于后续加密数据。

对称密码技术适用于数据传输加密阶段，在会议系统中用户若登录并交换密钥后，系统中在网络上传输的数据流可以通过对称密钥来加密解密数据，确保数据传输中的安全性和完整性。

2、简述散列函数MD5的碰撞问题。既然MD5存在碰撞问题，为何http://mirrors.ustc.edu.cn/ubuntu-releases/16.04/ 仍然给出MD5值作为完整性验证的依据。

http://mirrors.ustc.edu.cn/ubuntu-releases/16.04/ 仍然给出MD5值作为完整性验证的依据：

1）由于历史遗留问题，MD5曾经是常用的完整性验证工具，尤其是在早期互联网时代。许多网站和软件在过去使用MD5值来验证下载文件的完整性。尽管现在存在更强大的哈希算法（如SHA-256），但一些网站可能仍然保留MD5作为一种兼容性选项，以继续支持旧有的用户和系统。

2）MD5值相对较短，易于计算和传输。对于小型文件或网络资源，MD5仍然可以提供足够的安全性。因此，一些网站可能认为它足够满足其需求，而不必使用更复杂的哈希算法。

3）MD5易于验证，对于计算资源紧迫的机器，使用MD5算法验证所占有的计算资源将小于使用安全性更高的加密算法所使用的的计算资源，而对于安全性要求不高的用途上MD5会更适合。

4）镜像文件的数据量较大，难以找到相同的MD5序列，而且由于ubuntu镜像为操作系统，本身具有极为精细的功能，对于功能的正常使用（如安装）也是完整性验证的过程，攻击者难以精心伪造这一功能的同时还构造相同的MD5序列。

3、简述用RSA公钥算法实现数字签名的过程。

RSA公钥算法：

- **密钥计算方法：** 选择两个大素数p和q (典型值为1024位) 计算 n=p*q 和 z=(p-1)* (q-1) 选择一个与 z 互质的数，令其为 d 找到一个 e 使满足 e*d =1 (mod z) 公开密钥为 (e, n)，私有密钥为 (d, n)。
- **发送方生成数字签名方法：**发送方使用哈希函数（如SHA-256）对发送消息进行处理，生成一个摘要，使用RSA中的私有秘钥 (d, n)对哈希进行加密，形成数字签名，与原始消息组合后一同发送给接收方。
- **接收方验证数字签名方法：**接收方收到消息和数字签名后，使用发送方的公钥进行解密，得到消息的哈希值，再通过相同的哈希函数对接收到的消息进行处理，得到一个哈希值，对得到的哈希值与发送过来解密后的哈希值进行比较，若匹配则证明消息完整。

4、用PGP加密某个文件，如果接收该加密文件的用户为1个，加密文件的大小为24kB；如果接收该加密文件的用户 为10个，请问加密文件的大小是原来的10倍(240kB)吗？为什么？

不一定，加密文件中包含了IDEA算法对明文加密的密文和RSA算法对密钥加密的密文，当需要将加密文件发给多个用户时，明文加密的部分仅生成一份，而密钥加密的密文根据各个用户的公钥生成多份加密对称密钥组合起来。如果加密文件用户为1个，此时加密文件中的24kB包括公钥对称密钥的加密与对称密钥对明文的加密，而接收加密文件用户为10个时，此时加密文件大小为10个公钥对称密钥的加密与对称密钥对明文的加密，由于对密钥的加密的大小会远小于明文加密的大小，此时整个加密文件的大小不应为原来的10倍。