加密

对称加密 对称加密是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以 很容易地推导出另一个

对称加密算法的优点是：使用简单、加密解密快捷高效，

其致命弱点是：加密强度不高、密钥分发困难

非对称加密

在非对称加密体系中，密钥是成对出现的，一对密钥包括一个公钥和一个私钥。如果用公开密 钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有 用对应的公开密钥才能解密

优点在于：解决了对称密钥加密强度不高及密钥分发困难的问题，

缺点是：加密速度极慢。所以非对称加密算法通常只对极小的数据量进行加密，如对信息摘要进行加 密，或用于加密对称密钥

Hash函数和信息摘要

计算过程：输入一个长度不固定的 字符串，返回一串定长的字符串（又称为Hash值），单向Hash函数用于产生信息摘要

信息摘要简要地描述了一份较长的信息或文件，

它可以被看做是一份长文件的“数字指纹”，

对于特定的文件而言，信息摘要是唯一的，而且不同的文件必将 产生不同的信息摘要

信息摘要可以用于创建数字签名。

数字签名

通过一个单向函数对要传送的报文进行处理，得到用以认证报文来源并核实报文是 否发生变化的一个字母数字串

数字签 名则可以解决否认、伪造、篡改和冒充的问题（数据的完整性和不可抵赖性）

使用非对称加密技术（公钥算法）

发送者A的私钥对信息摘要加密完成签名。接收者B收到使用A的公钥解密，成功则表明信息是A发的

数字证书是由一个权威机构证书授权中心（CA）发行的

最简单的证书包含一个公开密钥（公钥）、名称以及证书授权中心的数字签名。

其中证书授权中心的数字签名是用它自己的私钥完成的，而它的公钥也是公开的，大家可以通过它的公钥来验证该证书是否是某证书授权中心发行的，以达到验证数字证书的真实性。

数字证书

密钥只是一串数字或字符，并不能通过密钥得知它的主人是谁。这样就生了安全隐患，所以提出了数字证书的概念。

数字证书简单一点理解，就是密钥与身份信息的结合体

非对称加密技术的提出，解决了密钥传输的问题

密钥分为公钥与私钥

计算机病毒与木马

恶意代码主要分两类，即病毒与木马

病毒：一段可执行的程序代码，通过对其他程序进行修改，可以感染这些程序，使其含有该病 毒程序的一个复制

计算机病毒的生命周期包括4个阶段：

潜伏期（不做任何事，等待激活事件，并非所有病毒都有 该阶段），

繁殖阶段（也就是传染阶段，开始复制复本），

触发阶段（也就是开始执行破坏性工作 的阶段），

执行阶段（功能完成）

木马：实质上是一个网络客户端/服务器程序，是一种基于远程控制的黑客工具

其主要特征包括：

不需要服务端用户的允许就能够获得系统的使用权；

程序体积十分小，执行时不会占太多的资源；

执行时很难停止它的活动，并且不会在系统中显示出来；

一次启动后就会自动加载在系统的启动区，在每次启动时能够自动运行；

一次执行后会通过更换文件名之类的方法来隐藏自己；

实现服务端用户无法显示执行的动作

木马通常由服务器端和客户端组成，服务器端将运行在被控制的主机中，而客户端则是攻击者用来远程控制的主要工具

病毒的分类

系统引导型病毒：又称开机型病毒，是藏匿和感染硬盘的第一个扇区，即平常我们所说的引导扇区。引导型病毒籍由引导动作而侵入内存

文件型病毒：文件型病毒通常寄生在可执行档（如 \*.COM，\*.EXE等）中。当这些文件被执行 时，病毒的程序就跟着被执行

目录型病毒：这一类型病毒通过装入与病毒相关的文件进入系统，而不改变相关文件，它所改变的只是相关文件的目录项

蠕虫病毒：蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通 过网络和电子邮件

宏病毒：一种寄存在Office系统文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的 宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上

病毒种类命名

系统病毒

系统病毒的前缀为：Win32、PE、Win95、W32、W95等。这些病毒的一般共有的特性是可以 感染windows操作系统的 \*.exe 和 \*.dll 文件，并通过这些文件进行传播

蠕虫病毒 蠕虫病毒的前缀是：Worm。这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带 毒邮件）等

木马病毒、黑客病毒 木马病毒其前缀是：Trojan，黑客病毒前缀名一般为 Hack

脚本病毒的前缀是：Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。

脚本病毒还会有如下前缀：VBS、JS

宏病毒 宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是： Macro，第二前缀是：Word、Excel其中之一

后门病毒 后门病毒的前缀是：Backdoor。该类病毒的共有特性是通过网络传播，给系统开后门，给用户 电脑带来安全隐患

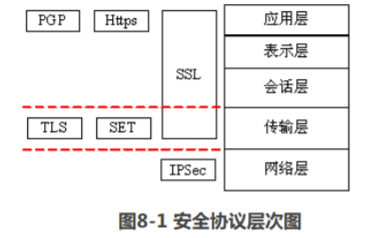
病毒种植程序病毒 这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来 的新病毒产生破坏

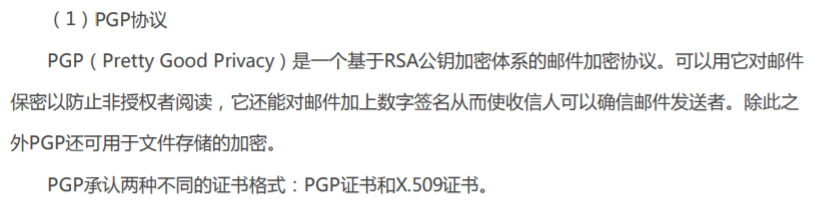
破坏性程序病毒 破坏性程序病毒的前缀是：Harm。这类病毒的共有特性是本身具有好看的图标来诱惑用户点 击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化C盘

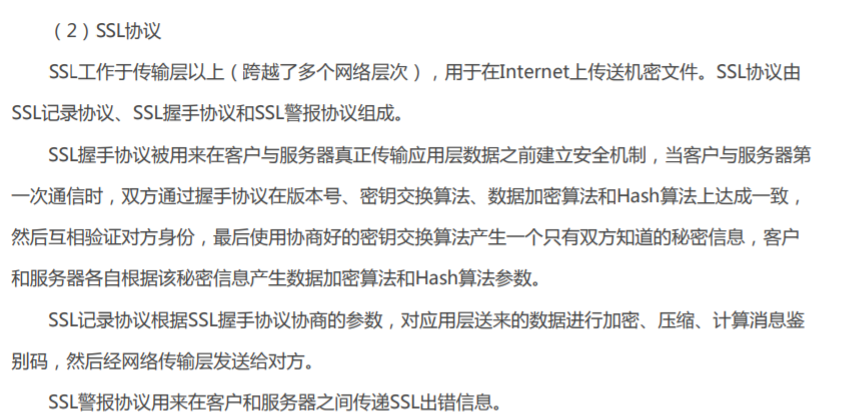
玩笑病毒 玩笑病毒的前缀是：Joke。也称恶作剧病毒。这类病毒的共有特性是本身具有好看的图标来诱 惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用 户电脑进行任何破坏

捆绑机病毒 捆绑机病毒的前缀是：Binder。这类病毒的共有特性是病毒作者会使用特定的捆绑程序将病毒 与一些应用程序如QQ、IE捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会 表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害

网络安全协议

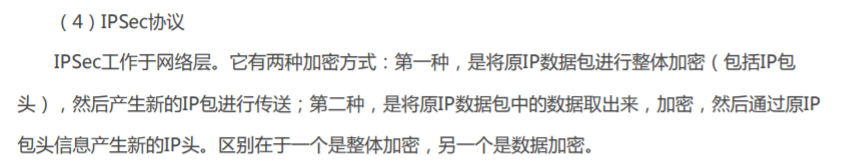


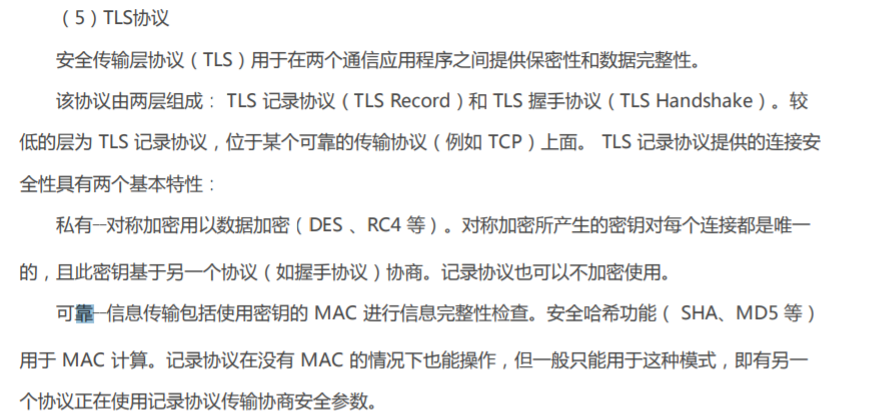






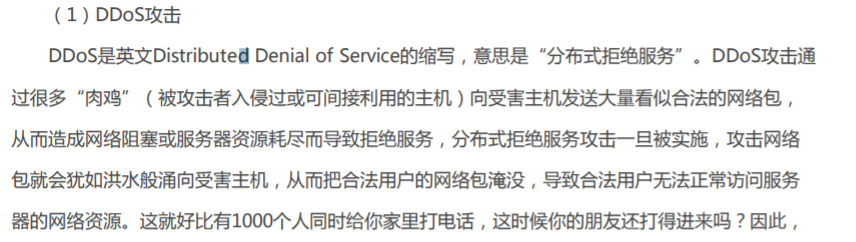
（3）SET协议 SET（Secure Electronic Transaction，安全电子交易）协议向基于信用卡进行电子化交易的应 用提供了实现安全措施的规则，SET在保留对客户信用卡认证的前提下， 又增加了对商家身份的认证





网络攻击

DDoS攻击与ARP欺骗攻击



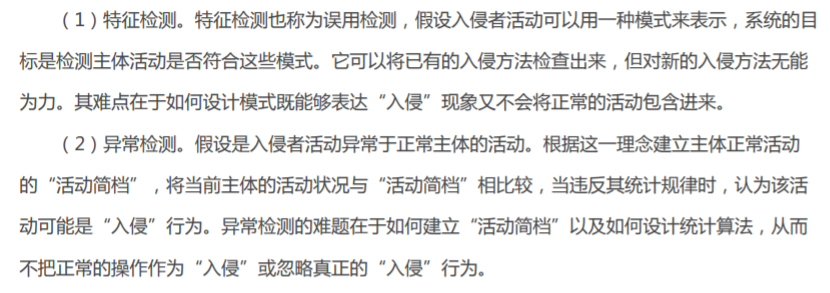
（2）ARP欺骗攻击

修改IP地址和MAC地址的映射关系，使发送给正确主机的数据包发送给另外一台由攻击者控制的主机

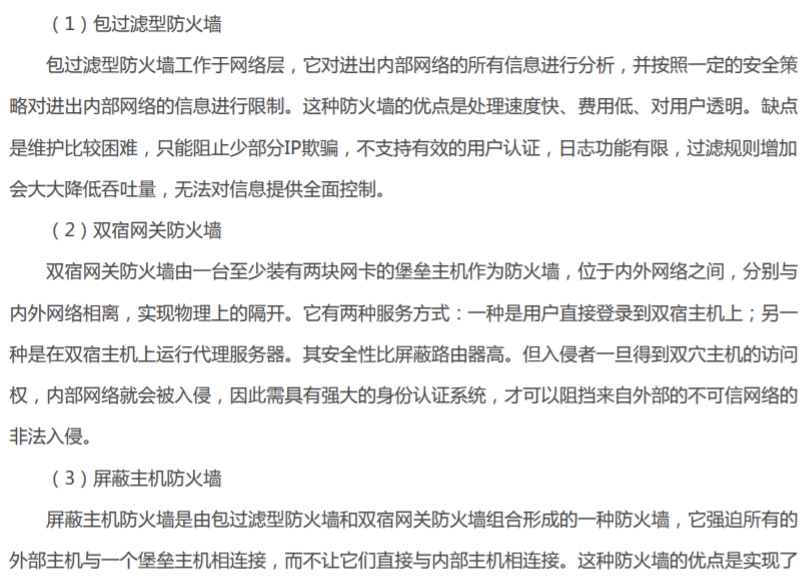
入侵检测

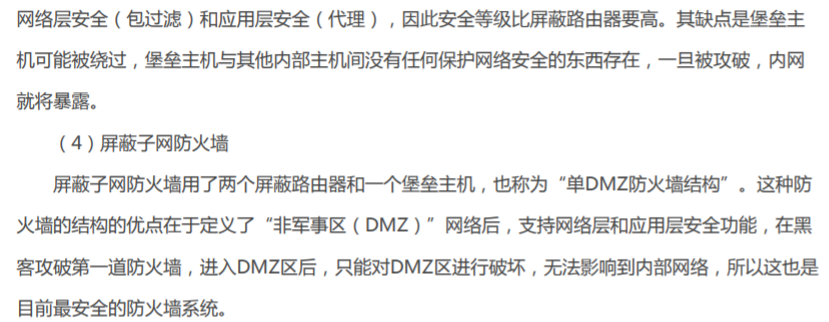
一种能够及时发现并报告系统中未授 权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术

违反安全策略的行 为有：入侵—非法用户的违规行为；滥用—用户的违规行为



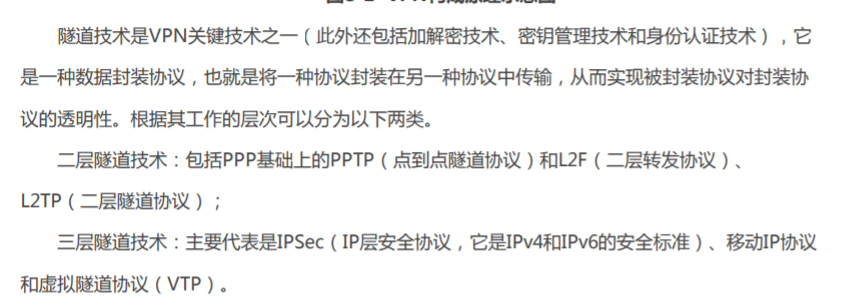
防火墙



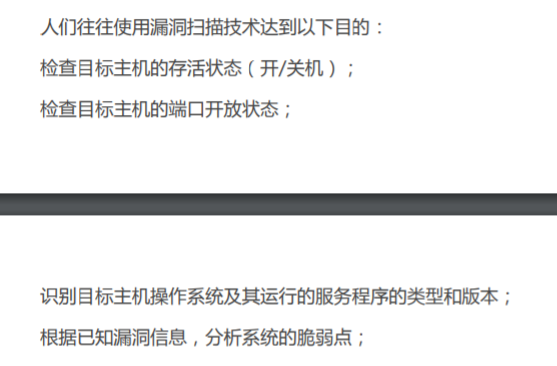


VPN

虚拟专用网（VPN）是企业网在因特网等公共网络上的延伸，它通过一个私有的通道在公共网 络上创建一个安全的私有连接



漏洞扫描



错题：

CIH病毒是一种能够破坏计算机系统硬件的恶性病毒，有时还会破坏计算机的BIOS

特洛伊木马一种秘密潜伏的能够通过远程网络进行控制的恶意程序，它使控制者可以控制被秘 密植入木马的计算机的一切资源和行为, 计算机感染特洛伊木马后的典型 现象是有未知程序试图建立网络连接

漏洞扫描系统是一种自动检测目标主机安全弱点的程序，漏洞扫描系统的原理是根据系统漏洞 库对系统可能存在的漏洞进行一一验证。黑客利用漏洞扫描系统可以发现目标主机的安全漏洞从而 有针对性的对系统发起攻击；系统管理员利用漏洞扫描系统可以查找系统中存在的漏洞并进行修补 从而提高系统的可靠性。漏洞扫描系统不能用于发现网络入侵者，用于检测网络入侵者的系统称为 入侵检测系统

数字签名是对签 名真实性的保护

网络安全体系设计是逻辑设计工作的重要内容之一，数据库容灾属于系统安全和应用安全考虑范畴

包过滤防火墙对数据包的过滤依据包括源IP地址、源端口号、目标IP地址和目标端口号

用户获取网站的数字证书后通过验证CA的签名和确认数字证书的有效性，从而验证网站的真伪

每个数字证书在诞生时，CA中心就会对证书做一个数字签名，这个数字签名正是我们验证 一个证书是否为合法证书的唯一标识