第一章

CIA

C：机密性confidentiality避免未授权信息的泄露：加密、访问控制、身份验证、授权、物理安全

I：完整性integrity信息不被改变：备份、校验和、数据纠错码、保护元数据

A：可用性availability及时且容易访问信息：物理保护、计算冗余

AAA

保证：提供管理和信任：策略、权限、保护

真实性：声明的不可否认性：数字签名

匿名：确保特定的记录或者交易不归因于任何个体的属性：数据聚集、数据混淆、使用代理、使用化名

窃听-机密性

修改-完整性

拒绝服务-可用性

伪装-真实性（网络钓鱼-机密性和匿名）

抵赖-保证

追踪-匿名

开放式设计（安全只依赖于对密钥的保密）、不公开即安全（安全依赖于保密加密算法）

特权分离

最小特权

访问控制模型（最小权限原则）（访问控制矩阵主体为中心、访问控制表客体为中心、权能主体为中心）

基于角色的访问控制

对称密码系统（共享密钥密码系统）AES（缺点：每两个人需要一个密钥）

公钥密码系统（缺点：运行速度慢）

中间人攻击

蛮力解密攻击（唯一解距离）

加密散列函数（数字签名和文件系统的完整性）

消息认证码（MAC） h（K || M）提供完整性保护

数字证书、证书颁发机构CA

效率和可用性

字典攻击、设置安全密码

社会工程（利用人的弱点）假托（打电话冒充Alice改密码）、诱饵（停车场扔U盘）、相等补偿（为Alice提供服务骗取密码）

源于编程错误的脆弱性（缓冲区溢出）

第二章

锁（弹子锁、管状锁和径向锁、晶片弹子锁、密码锁）

更改钥匙和主控钥匙

撬锁、撞锁、钥匙印痕

旁路攻击

有k个钥匙坯，m个上弹子，n个下弹子，可能的钥匙数为k \* n^m个

身份验证技术

条形码

磁条卡（三条磁道）脆弱性在于容易读取和复制

智能卡（电路板上有微处理器）差分功耗分析

SIM卡（挑战-响应协议）

RFID（无线射频识别，非接触）（跳码和遥控汽车，问题在于同步）（护照，加入纸张就会泄露信息）

生物特征识别（普遍性、独特性、永久性、可收集性）特征向量

针对计算机的直接攻击

环境与事故

窃听（搭线窃听、射频辐射、光辐射、声音辐射、键盘记录器）

TEMPEST（计算机信息泄露安全防护技术）三级保护

自生系统（Live CD）防范：设置BIOS密码

计算机取证（冷启动攻击：DRAM在冷的环境衰减速度减慢）

ATM（ATM受到破坏时，ATM采取机制使得现金不可用，如标记染色或者损毁）

黎巴嫩圈套、分离器

投票机

物理入侵检测

视频监控、人为因素和社会工程

第三章

虚拟机（实现方法：模拟、虚拟化）

监控、管理、日志

虚拟内存攻击（非正常关机，外部引导另一个操作系统查看虚拟内存文件）

密码盐（字典攻击的搜索空间为2^B\*D其中B是随机盐的位数，D是字典攻击的单词列表大小）（每个用户的盐是固定的，不同用户的盐互不相同）

访问控制项ACE与访问控制列表ACL（权限升级）

文件描述符（父进程没有关闭文件描述符调用，从而使子进程也可以访问该文件）

符号链接与快捷方式（攻击者创建一个到密码文件的符号链接来欺骗程序）

通过DDL注入恶意代码（动态链接）

算术溢出

栈的缓冲区溢出（覆盖返回地址并写入恶意代码，当程序调用结束并返回时，便会去执行恶意代码）（攻击者面临的问题：猜测返回地址的位置）（NOP Sled）（跳转：程序跳转时地址存储在寄存器，通过修改寄存器从而修改跳转的地址）（返回到libc的攻击：强制程序调用一些函数，并通过修改地址达到目的。其优势在于在堆栈中没有任何代码，所以即使堆栈被标记为不可执行，也可以发动攻击）

缓冲区溢出的保护机制（canary，检查canary是否被修改判断缓冲区是否溢出）（地址空间布局随机化）

格式化字符串攻击

检查时间问题（access和open之间修改访问文件的路径）

第四章

内部攻击（后门：为调试插入后门、故意的后门）（逻辑炸弹：根据一定的逻辑执行恶意操作）（防御：避免单点故障、使用代码走查、使用归档和报告工具、限制授权和权限、重要系统的物理安全、监控员工行为、控制软件的安装）

计算机病毒（自我复制的计算机代码、需要协助来自我复制）（潜伏阶段、繁殖阶段、触发阶段、行动阶段）（类型：程序病毒文件病毒、宏病毒文档病毒、引导区病毒）（防御：特征码检测、检测与隔离）

加密病毒、多变体病毒（用不同的密钥加密）、变形病毒（指令重排、包含无用指令）

特洛伊木马（一个程序，表面执行有用的任务，隐形执行恶意操作）

蠕虫（无需将自己注入其他程序就可以传播，且不需要与人交互）（不感染其他程序）

Rootkits（通过修改程序或者操作系统来隐藏自己）

零日攻击（恶意软件利用开发者不知道的脆弱性）（检测方法：不断扫描程序、沙箱测试）

僵尸网络（DDoS）

广告软件、间谍软件（键盘记录、屏幕截图、追踪Cookies、数据收获）

第五章

物理层：传输比特流

链路层：传输帧

网络层：传输数据包

传输层：应用程序之间的连接

应用层：提供网络服务

ARP欺骗（ARP缓存中毒从而建立中间人攻击）（预防：检查是否有相同的MAC、静态ARP表）

IP欺骗（DoS攻击）（规避防火墙策略）（TCP会话劫持）

数据包嗅探（抓包）（防御：高层协议加入加密）

NAT

TCP序列预测（仅允许单向通信）（对受害客户端进行DoS攻击、向服务器发送SYN数据包、通过预测序列号向服务器发送ACK数据包）

盲注入（单向通信中，因为IP欺骗无法接受服务器响应，但是可以对服务器执行一些命令）

ACK风暴？？？

完全会话劫持（攻击者和目标服务器或者客户端在同一个网段）（数据包嗅探可以知道序列号）（对策：加密会话、避免创建以安全验证开始而后切换到未加密的会话）

DoS攻击

ICMP攻击（ping洪水攻击：发送大量回显请求、smurf洪水攻击：将ICMP数据包源IP改为攻击目标IP，广播该数据包，则该网段中所有计算机都会向目标计算机发送一个ICMP数据包）

SYN洪水攻击（攻击者向服务器发送大量SYN数据包（第一次握手），但是却不发送ACK数据包（第三次不握手））（防御：SYN Cookies）

优化的TCP ACK攻击（攻击者发送SYN数据包之后不等服务器回应立刻发送ACK数据包）

IP回溯

第六章

DNS

网址嫁接（浏览网页、邮件重定向）、网络钓鱼

DNS缓存中毒（攻击者向DNS服务器发送DNS请求后立刻发送伪造的DNS响应，服务器接受这个伪造的响应）防御：对查询使用随机标识符、始终检查标识符、DNS请求的端口随机化、部署DNSSEC

DNS缓存中毒与生日悖论P188（攻击者需要猜测真正DNS服务器返回响应的ID）

子域DNS缓存中毒（向很多不存在的子域发DNS请求来猜测ID）（防御：只接受内网请求、源端口随机化）

客户端DNS缓存中毒P189图片ab

防火墙

黑名单（默认允许）白名单（默认拒绝）

无状态防火墙（不维护上下文、状态）状态防火墙（维护上下文、状态，如：TCP三次握手）

隧道

SSH（1TCP连接、2交换管理细节加密方法版本、3密钥交换、4身份验证）

IPSEC（传输模式只对有效载荷加密、隧道模式整个加密）

（IKE互联网密钥交换处理SA安全关联、AH头和ESP头尾、AH不可NAT但ESP可NAT）

VPN（远程访问VPN、站点到站点VPN）可以用隧道来规避防火墙

入侵检测系统IDS

网络IDS、主机IDS、被动式IDS

IDS攻击（DOS使之无法记录每个事件）

基率谬误P203（计算题）

入侵攻击的类型

端口扫描、DoS攻击、恶意软件攻击、ARP欺骗、DNS缓存中毒

检测

基于规则的入侵检测

统计入侵检测

端口扫描（TCP扫描、SYN扫描、空闲扫描、UDP扫描）

蜜罐（给一个诱饵）

无线网

WEP有线等效保密P211（密钥生成密钥流，密钥流与明文异或形成密文）（攻击：初始化向量IV重用、消息明文的CRC32、分析大量密文恢复密钥信息、ARP重新注入、**牛奶咖啡**）

WPA（预共享密钥、802.1x）

第七章

标准的HTTP协议不提供任何方式的数据加密

HTTPS采用了安全套接字层（SSL）或采用了传输安全（TLS）

SSL和TLS依靠证书来验证服务器的身份，并在浏览器和服务器之间建立加密通信信道

Cookis（内置有效期、清除Cookies）攻击：直接访问Cookie文件查找想要的机密信息、在客户端和服务端进行Cookie信息传递时候进行截取，进而冒充合法用户进行操作、修改Cookie信息，在服务端接收到客户端获取的Cookie信息的时候，对伪造过的Cookie信息进行操作

第三方Cookies跟踪

会话劫持（会话ID、会话令牌编码）

网络钓鱼（URL混淆、变种Unicode攻击）

鼠标点击劫持

沙箱（应用程序或脚本在另一个应用程序中受限的运行权限）

跨站点脚本（持久性XSS例如网站留言簿、非持久性XSS例如回显搜索查询的结果网页）

XSS过滤（去除危险的符号）

跨站点请求伪造（CSRF）例如登陆攻击

防御客户端的攻击（用户安全地浏览、浏览器内置安全措施）

服务器脚本攻击（远程文件包含RFI、本地文件包含LFI）

SQL注入（通过在数据流中插入SQL命令、查询额外信息、绕过身份验证）（盲SQL注入、SQL注入蠕虫）（通过对输入进行过滤来防止SQL注入）

拒绝服务攻击DOS、分布式拒绝服务攻击DDOS

第八章

对称加密（加密和解密使用相同的密钥）

唯密文攻击（从很多密文推导出密钥和明文）、已知明文攻击（从很多明文密文对推导出密钥）、选择明文攻击（从明文推导出与明文关联的密文）、选择密文攻击（从密文推导出与密文关联的明文）

替换密码（凯撒密码、多字母替换密码、替换盒S盒）

一次一密（密钥块长度m和明文长度n相同、完全随机选择移动量ki）密钥会耗尽

线性同余发生器（不足以作为加密用的随机序列、三个连续的数就可以确定其余的值、有周期性）

希尔密码（使用矩阵）

置换密码

AES（替代DES）分组密码，每组128位。密钥长度128、192、256

AES128在明文与密钥异或后进行10轮处理。每一轮处理为：1、S盒替换2、置换3、希尔矩阵乘法4、轮密钥异或

AES定时攻击（通过不同的运行时间推导密钥）

ECB（电子密码本）（每个分组独立加密）

CBC（密码分组链接）（必须顺序加密、解密可以独立）

CTR（计数器模式）（加密解密都可以并行）

公钥加密

模逆（乘法逆元）（xy mod n = 1）（如果n是素数，在Zn中除0外，每个元素都有模逆）

模幂（x^y mod n = 1）（如果n不是素数，Zn中只有与n互质的元素的模幂等于1。正好是x与n的最大公约数等于1 的这些元素x具有模幂）（如果n是素数，Zn中的每个非0元素都有模幂等于1，且总有x^n-1 mod n = 1）

欧拉定理

RSA（安全性基于给定e和n，计算d的困难性）（缺点：若明文相等，则密文相等，Elgamal克服了这一缺点）

DH密钥交换协议K = g^xy mod p（中间人攻击：截获并修改消息）

费马小定理g^(p-1) mod p = 1

加密散列函数

抗冲突性（弱抗冲突性，强抗冲突性）

Merkle-Damgard构造

生日攻击（256bits抗冲突散列函数的安全性是128bits）

第九章

安全策略（主体、客体、操作、权限、保护）

安全模型（自主访问控制DAC、强制访问控制MAC）

BLP（不可向上读、不可向下写）（强调机密性：信息只能从低安全级别流向高安全级别）

Biba（不可向下读、不可向上写）（强调完整性：信息只能从高安全级别流向低安全级别）

低水印模型（不可向上写）

CW模型

中国墙模型（每个用户只能访问利益冲突类中的一种资源）

基于角色的访问控制RBAC（分层结构）（约束结构：静态职责分离、动态职责分离如负责人使用不同角色批准不同文件）

黑盒测试（不能看到源代码）、白盒测试（可以看到源代码）、灰盒测试（可以看到部分）

静态测试（源代码测试、二进制代码测试）动态测试（用调试器控制程序执行）模糊测试（自动向程序注入意想不到的输入）

漏洞（负责任披露、充分披露立即公开）

系统管理（用户策略、系统策略BIOS密码、网络策略防火墙）

渗透测试（模拟实际的入侵）（网络发现ping扫描、脆弱性测试端口扫描、利用已知的脆弱性）

Kerberos（身份验证服务器、票据授予服务器）

文件加密（文件密码、加密文件系统）

磁盘加密

可信平台模块（主板上的安全密码处理器）

第十章

数据库安全（两阶段提交：请求阶段、提交阶段）（推理攻击：单元抑制删除一些单元从而留下空白、推广1983.6.2->1980至1985、加噪添加随机值）

电子邮件安全（垃圾邮件：用“蜘蛛”获得地址、用开放代理来匿名）（验证码又称全自动人机区分图灵测试）（黑名单、灰名单需要发送方重传）（用机器学习内容过滤）

信用卡、数字现金（防止重复消费、防止银行了解每一笔交易信息、盲签名）、网上拍卖

数字版权管理（软件许可方案）

社交网络

投票系统（ThreeBallot）