07-08-Security

Created on 20220605.

Last modified on 2022 年 6 月 5 日.

目录

Chapter 1　密码学

Chapter 2　信息安全技术

2.0.1　系统安全分析

保密性，【最小授权，防暴露，信息加密，物理保密】完整性，【安全协议，校验码，密码校验，数字签名，公证】可用性，【IP 过滤，路由选择控制】不可抵赖，【数字签名】

安全的五个基本要素　机密性 (确保信息不暴露给未授权的实体或进程)　完整性 (只有得到允许的人才能修改数据，并能够判别数据是否已被篡改)　可用性 (得到授权的实体在需要时可访问数据)　可控性 (可以控制授权范围内的信息流向和行为方式)　可审查性 (对出现的安全问题提供调查的依据和手段)

加密

对称，【加密和解密秘钥一样】【加密强度低，秘钥分发困难】DES, 替换 + 移位，速度快；3DES，56 位的 K1 和 K2，K1 加–K2 解–K1 加 AES，RC-5, IDEA，

非对称，【加密和解密秘钥不一样】【加密速度慢】RSA, Elgamal，基础是 Diffie-Hellman 秘钥交换算法；ECC，背包算法，Rabin，D-H 等

摘要

单向散列函数，单向 Hash 函数，定长的散列值。MD5, SHA,SHA 更长更安全。

数字签名

A：我的名字–》信息摘要–》我的私钥加密得到签名；对方：1）收到明文名字–》信息摘要;【数字签名，识别身份的作用】2）收到的签名，用 A 的公钥解密，得到信息摘要；【验证】3）比较上述两个摘要是否相等。

数字信封与 PGP

A：原文，对称加密；秘钥用 B 的公钥加密后发送给 B。B：收到电子信封，用私钥解密信封，去除秘钥解密出原文。

秘钥用加密时间长的复杂的非对称加密。

PGP 证书，是电子邮件、文件存储加密。可以将文件用 PGP 加密后存到云盘，更安全。

数字证书：秘钥与数字签名结合在一起。CA 机构颁发。验证数字证书上颁发机构的签名。

【试设计】邮件要加密传输，最大附件 500M，发送者不可抵赖，第三方截获的话无法篡改。

发送端 A：邮件正文 –》随机秘钥 K，对称加密–》邮件密文；邮件正文–》信息摘要–》数字签名（私钥）–》摘要密文；秘钥 K –》数字信封技术，非对称加密（公钥）–》信封；

接收端 B：信封–》非对称加密（私钥）–》秘钥 K 邮件密文–》随机秘钥 K，对称加密–》邮件正文；邮件正文–》邮件摘要摘要密文–》解密签名（公钥）–》邮件摘要，与上一步的摘要验证；

病毒

引导区：。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。宏：TaiwanNo.1，Nuclear 宏病毒木马：冰河，ICMP 类型的木马，灰鸽子和蜜蜂大盗，PassCopy 和暗黑蜘蛛侠蠕虫：震网（Stuxnet）

2.1 数据安全

Chapter 3　容错计算技术