安全性、可靠性与系统性能评测

数据安全与保密

加密体系

- 两种密钥体制：
    1. 对称密码体制
    2. 非对称密码体制
- 对称密码体制：对称密码体制又称为**秘密密钥体制（私钥密码体制）**，加密和解密采用**相同的密钥**（或者可以通过一个推导出另一个）
    - 优点：加密**速度快**，通常用来**加密大批量**的数据
    - 缺点：需要**管理的密码多**
    - 常见的对称密钥技术：
        1. **DES**：是一种迭代的分组密码，**输入/输出都是64位**，使用一个**56位的密钥**和附加的**8位奇偶校验位。**攻击DES的主要技术是穷举。由于DES的密钥长度较短，为了提高安全性，出现了使用**112位密钥**对数据进行三次加密的算法，称为**3DES**
        2. **IDEA算法**：其明文和密文都是64位，密钥长度为128位
- 非对称密码体制：非对称密钥技术（公钥算法）。非对称密钥技术是指加密密钥和解密密钥完全不同，并且不可能从任何一个推导出另一个
    - 优点：适应开放性的使用环境，可以实现数字签名与验证
    - 缺点：使用RSA来加密大量的数据则速度太慢，因此RSA广泛用于**密钥的分发**、**数字签名**中
    - 最常见的非对称密钥技术：**RSA。**它的理论基础是数论中**大素数分解极其困难**

身份认证技术与数字签名

- 数字签名就是只有**信息的发送者**才能**产生**的**别人无法伪造**的一段**数字串**，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明
- 数字签名使用了**公钥加密**领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种运算，一个用于**签名**，另一个用于**验证**
- 数字签名算法：
    1. Hash签名
    2. DSS签名
    3. RSA签名
- 数字签名原理与过程：
    1. 发送者首先将原文用Hash函数生成128位的消息摘要
    2. 发送者用自己的**私钥对摘要再加密**，**形成数字签名**，把加密后的**数字签名附加在要发送的原文后面**
    3. 发送者将**原文和数字签名同时传给对方**
    4. 接收者对收到的信息用Hash函数生成新的摘要，同时用发送者的**公开密钥对消息摘要解密**
    5. 将解密后的摘要与新摘要对比，如两者一致，则说明传送过程中信息没有被破坏或篡改

数字证书

- **CA是数字证书的签发机构，它是PKI的核心**

- CA是负责签发证书、认证证书、管理已颁发证书的机关
- CA要制定政策和具体步骤来**验证、识别用户身份**，并**对用户证书进行签名**，以确保证书持有者的身份和公钥的拥有权
- **CA是可以信任的第三方**
- 数字证书的内容：CA《A》=CA｛V，SN，AI，CA，UCA，A，UA，Ap，Ta｝
    1. V---证书版本号
    2. SN---**证书序列号**
    3. AI---用于对证书进行签名的算法标识
    4. CA---签发证书的CA机构的**名字**
    5. UCA---签发证书的CA的**唯一标识符**
    6. A---用户A的名字
    7. UA---**用户A的唯一标识**
    8. Ap---用户A的公钥
    9. Ta---证书的有效期

SSL

- 端口号为：443
- SSL(安全套接层协议)及其继任者TLS (传输层安全协议)是一种安全协议，为网络通信及数据完整性提供安全保障；SSL和TLS是**工作在传输层的安全协议**, 在传输层对网络连接进行加密
- SSL协议的两层结构：
    - SSL握手协议（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等
    - SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持

SET（Secure Electronic Transaction，安全电子交易）协议

- SET协议称为安全电子交易协议
- 美国Visa和MasterCard两大信用卡组织共同制定了应用于Internet上的以银行卡为基础进行在线交易的安全标准--SET
- 它采用**公钥密码**体制和**X.509数字证书**标准，保障网上购物信息的安全性

HTTPS（安全套接字层上的超文本传输协议）

- 以安全为目标的HTTP通道，简单讲是HTTP的安全版
- HTTPS是工作在应用层的协议

PGP：邮件加密软件

- PGP是一个基于**RSA公钥加密体系的邮件加密软件**
- PGP可**用于文件存储的加密**
- PGP承认两种不同的证书格式：PGP证书和X.509证书

防火墙

- 是一种位于内部网络与外部网络之间的网络安全系统。它依照特定的规则，允许或是限制传输的数据通过
- 实现防火墙的产品主要有两大类：
    1. 网络级防火墙

2. 应用级防火墙

- 网络级防火墙：网络级防火墙也称为**过滤型防火墙**，是一种具有特殊功能的**路由器**，采用**报文动态过滤技术**，**能够动态地检查流过的TCP/IP报文或分组头**，根据企业所定义的规则，决定禁止某些报文通过或者允许某些报文通过，允许通过的报文将按照路由表设定的路径进行信息转发。相应的防火墙软件**工作在传输层与网络层**
    - 状态检测防火墙：又称动态包过滤，是在传统包过滤上的功能扩展。状态检测防火墙在网络层由一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此作为依据决定对该连接是接受还是拒绝。这种技术提供了高度安全的解决方案，同时也具有较好的性能、适应性和可扩展性
- 应用级防火墙：应用级防火墙也称为**应用网关型防火墙**，目前已大多**采用代理服务机制**，即采用一个网关来管理应用服务，在其上安装对应于某种服务的特殊代码（代理服务程序），在此网关上控制与监督各类应用层服务的网络连接
    - 应用级防火墙有4种类型，适合于不同规模的企业内部网
        - 双穴主机网关
        - 屏蔽主机网关
        - 屏蔽子网
        - 应用代理服务器
    - 它们共同点是需要有一台主机（称之为堡垒主机）来负责通信登记、信息转发和控制服务提供等任务

容错技术

提高计算机可靠性的技术可以分为避错技术和容错技术。避错是指预防和避免系统在运行中出错。容错就是当计算机由于种种原因在系统中出现了数据、文件损坏或丢失时，系统能够自动将这些损坏或丢失的文件和数据恢复到发生事故以前的状态，使系统能够连续正常地运行。

冗余技术

- 实现容错的主要手段就是冗余。冗余是指所有对于实现系统规定功能来说是多余的那部分的资源
- 主要的冗余技术包括：结构冗余、信息冗余、时间冗余、冗余附加技术
- **结构冗余**：
    - 结构冗余按其工作方式，可分为：
        - 静态冗余：常用的有**三模冗余**和**多模冗余**。静态冗余通过表决和比较来屏蔽系统中出现的错误
        - 动态冗余：动态冗余的主要方式是多重模块待机储备，当系统检测到某工作模块出现错误时，就用一个备用的模块来顶替它并重新运行。须有检测、切换和恢复过程，故称其为动态冗余
            1. **热备份系统**中，两套系统**同时、同步运行**，当联机子系统检测到错误时，退出服务进行检修，而由热备份子系统接替工作
            2. **冷备份的子系统**平时停机或者运行与联机系统无关的运算，当联机子系统**产生故障时**，人工或自动**进行切换**，使冷备份系统成为联机系统。在运行冷备份时，不能保证从程序端点处精确地连续工作
- **信息冗余**：在实现正常功能所需要的信息外，再**添加一些信息**（奇偶校验码、冗余校验码），以保证运行结果正确性的方法
- **时间冗余**：使用附加一定时间的方法来完成系统功能。附加的时间主要用在**故障检测、复查或故障屏蔽上。**时间冗余**以重复执行指令（指令复执）或程序（程序复算）来消除瞬时错误带来的影响**
- **冗余附加技术**：指为实现上述冗余技术所需的资源和技术，包括程序、指令、数据、存放和调动他们的空间和通道等

- 故障的恢复策略一般有两种，分别是**前向恢复**和**后向恢复**
  - 前向恢复是指使当前的计算继续下去，把系统恢复成连贯的正确状态，弥补当前状态的不连贯，这需要有错误的详细说明
  - 后向恢复是指系**统恢复到前一个正确状态**，继续执行，这种方法显然**不适合实时处理场合**

软件容错

- 软件容错的主要目的是提供足够的冗余信息和算法程序，使系统在实际运行时能够及时发现程序设计错误，采取补救措施，以提高软件可靠性，保证整个计算机系统的正常运行。
- 软件容错主要技术：
  - **恢复块方法**：**后向恢复策略。**恢复块方法是一种动态的故障屏蔽技术，采用后向恢复策略。它提供具有相同功能的主块和几个后备块，一个块就是一个执行完整的程序段，主块首先投入运行，结束后进行验证测试，如果没有通过验证测试，系统经现场恢复后由一后备块运行
  - **N版本程序设计**：N版本程序设计是一种静态的故障屏蔽技术，采用前向恢复的策略，其设计思想是用n个具有相同功能的程序同时执行一项计算，**结果通过多数表决来选择。n份程序必须由不同的人独立设计，使用不同的方法，不同的设计语言，不同的开发环境和工具来实现。目的是减少n版本软件在表决点上相关错误的概率**
  - **防卫式程序设计**：防卫式程序设计的基本思想是通过**在程序中存储错误检查代码和错误恢复代码**，使得一旦错误发生，程序能撤销错误状态，恢复到一个已知的正确状态中去。其实现策略包括**错误检测**、**破坏估计**和**错误恢复**三个方面

系统可靠性评价

可靠性计算

- 串联系统：各个子系统的可靠性分别用R1，R2，…，Rn表示

  - 系统的可靠性为：R=R1 X R2 …. X Rn
  - 系统的失效率为：λ = λ1 + λ2+…+ λn
- 并联系统：假如一个系统由2个子系统组成，只要有一个子系统能够正常工作，系统就能正常工作，设系统各个子系统的可靠性用R1，R2，…，Rn表示
- 系统的可靠性为：R= 1- (1- R1) ×（1- R2）×…×（1- Rn)
- 系统的失效率=1/（无故障时间*（1/1+1/2+……1/n））

模冗余系统

- m模冗余系统由m个（**m=2n+1为奇数**）相同的子系统和一个表决器组成，经过表决器表决后，m个子系统中占多数相同结果的输出作为系统的输出
- m模冗余系统的可靠性：

$$\sum_{i=n+1}^{m} C_m^i R_0^i (1-R_0)^{m-i}$$

$$\mathbf{R=}\quad C_3^2 \times 0.8^2 \times (1-0.8)^1 + C_3^3 \times 0.8^3 \times (1-0.8)^0$$