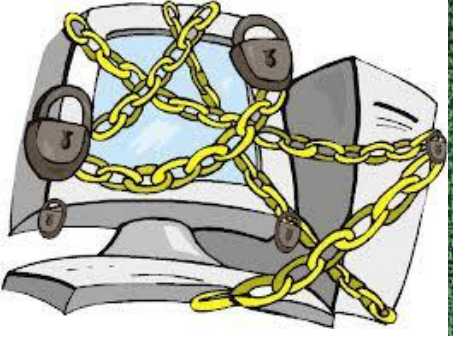


Introduction to Information Security

实验三：数字证书及其应用

Chunhua Chen, Ph.D. / 陈春华 博士
chunhuachen@scut.edu.cn
South China University of Technology

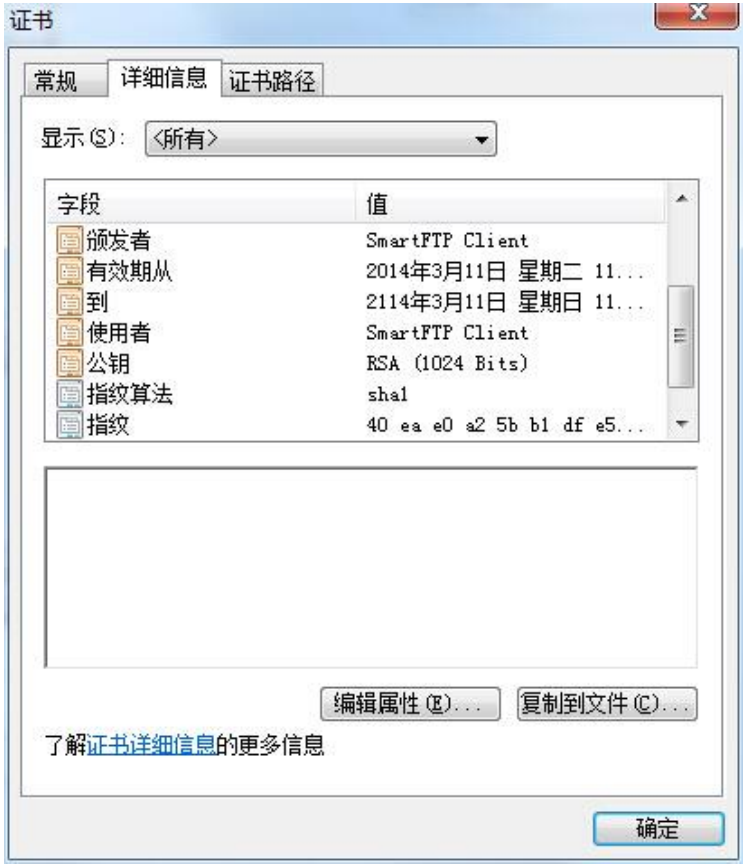
29st March 2012

公钥基础设施

- 在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。
- 因此，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。
- PKI方案：
  - 引进数字证书(Certificate)机制，并由此构建形成公钥基础设施（Public Key Infrastructure、PKI）来提供服务.

数字证书

- 数字证书是公钥钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络环境中的一种身份证，用于证明某一主体的身份以及其公开密钥的合法性。



数字证书

- 版本号： 证书所遵循的 X.509 标准的版本
- 序列号： 唯一标识证书且由证书颁发机构颁发的编号
- 有效期： 数字证书保持有效的时间段，并包含起始日期和过期日期。
- 使用者名称 ：数字证书所有者的姓名
- 使用者公钥信息： 与数字证书所有者关联的公钥以及与该公钥关联的特定公钥算法。
- 证书颁发机构的数字签名： 使用证书算法标识符字段中指定的算法以及证书颁发机构的私钥进行的实际数字签名
- 其他内容

PKI体系

- 一个完整的PKI系统必须具备证书认证机构（Certificate Authority、CA）、数字证书库、密钥备份及恢复系统、证书作废系统和应用接口（API）等基本组成部分。
  - 证书认证机构
  - 数字证书库
  - 密钥备份及恢复系统
  - 证书作废系统
  - PKI应用接口系统
- 整个PKI系统中，只有CA会和普通用户发生联系，其他所有部分对用户来说都是透明的
  - 申请/签发用户数字证书

PKI安全服务

- 认证：实体鉴别
- 密钥交换：协商会话密钥
- 消息完整性保护
- 数字签名-不可否认性服务

问题：

- CA的公钥如何安全获取？
  - CA自签发公钥证书
  - 浏览器等应用在发布中预先安装常用的CA公钥证书
  - 用户管理浏览器等应用中的证书
- 实验：利用如下技术或工具，构建PIK系统
  - EasyRSA
  - Openssl

Web和HTTPS

- 服务器端认证
- 建立安全通信信道

安全电子邮件

- 对电子邮件进行数字签名
- 对电子邮件进行加密