中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 3
Authentication Technologies

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- 3.1 Overview
  - Introduction to Authentication Technologies
  - The Weak/Strong Authentication Scheme
  - The Application of Authentication Technologies
  - The Attack to Authentication
  - The Security Guidelines to Protect Authentication Schemes
- **3.2 Public Key Infrastructure**
  - Introduction to PKI
  - PKIX
  - The Management of PKIX
  - Public Key Certificate
  - Trust Hierarchy Model

Outline

- **3.3 Kerberos**
  - What is Kerberos
  - Description
  - Kerberos Process
  - Drawbacks & Limitations
- **3.4 X.509**
  - What is X.509
  - History and Version
  - Certificate
  - Security problems
  - Application

3.2 Public Key Infrastructure

3.2.1 Introduction to PKI

- **What's PKI**
  - PKI (公钥基础设施) provides well-conceived (精心设计的) infrastructures to deliver security services in an efficient and unified style. PKI is a long-term solution that can be used to provide a large spectrum of security protection.
  - What PKI can do
    - ✧ generate digital certificates.
    - ✧ manage the certificates, certificate statuses, and the business element.
    - ✧ involve symmetric key cryptography for different purposes
    - ✧ other security purposes.

3.2 Public Key Infrastructure

3.2.1 Introduction to PKI

- **What's PKI**
  - PKI 的概念
    - ✧ PKI 是一组服务和策略，提供了一个将公钥和用户身份唯一绑定的机制，以及如何实施并维护这个绑定相关信息的框架；
    - ✧ PKI 是一个通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份的体系。
  - PKI 的主要功能
    - ✧ 签发数字证书以绑定证书持有者的身份和相关的公开密钥
    - ✧ 为用户获取证书、访问证书和吊销证书提供途径
    - ✧ 利用数字证书及相关的各种服务 (证书发布、黑名单发布等) 实现通信过程中各实体的身份认证，保证通信数据的完整性和不可否认性

3.2 Public Key Infrastructure

3.2.1 Introduction to PKI

- **What's PKI**
  - PKI 技术已经获得广泛应用，典型应用如：
    - ✧ 虚拟专用网络 VPN
      - ◌ VPN 是一种构建在公用通信基础设施上的专用数据通信网络，利用网络层安全协议 (如 Ipsec) 和建立在 PKI 上的加密与数字签名技术来获得机密性保护。
    - ✧ 安全电子邮件
      - ◌ 可以利用 PKI 实现电子邮件的安全要求，包括机密、完整、认证和不可否认性。目前发展很快的安全电子邮件协议 S/MIME，是一个允许发送加密和有签名邮件的协议。该协议采用了 PKI 数字签名技术并支持消息和附件的加密，无须收发双方共享相同密钥。

3.2 Public Key Infrastructure

3.2.1 Introduction to PKI

- **What's PKI**
  - PKI 技术已经获得广泛应用，典型应用如：
    - Web 服务安全
      - 为了解决 Web 服务的安全问题，在两个实体进行通信之前，先建立 SSL 连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议在协商时完成了对服务器和客户端基于证书的身份认证 (其中对客户端的认证是可选的)。

3.2 Public Key Infrastructure

3.2.1 Introduction to PKI

- **What's PKI**
  - PKI 场景：一个 B/S 架构下安全浏览网页的例子

(1) Web 服务器 W 生成一对私钥/公钥 (WR, WU) 并向认证机构 C 申请一个数字证书 X，证书中包含了 WU；C 保证 WU 是 W 的公钥；证书 X 用 C 的私钥 CR 加密作为数字签名；C 的公钥 CU 是公开声明的；

(2) W 向客户端浏览器 B 发送数字证书 X；

(3) B 用 C 的公钥 CU 认证数字证书 X 确实是 C 发布的；

(4) B 产生一对私钥/公钥 (BR, BU)，利用数字证书 X 中包含的 WU 去加密 BU，然后将公钥密文 M 发给 W；

(5) W 使用自己的私钥 WR 解密 M，得到 BU，然后 W 使用 BU 加密网页 P，将得到的秘闻网页 P_M 传给 B；

(6) B 使用自己的私钥 BR 解密 P_M，恢复明文网页 P。

3.2 Public Key Infrastructure

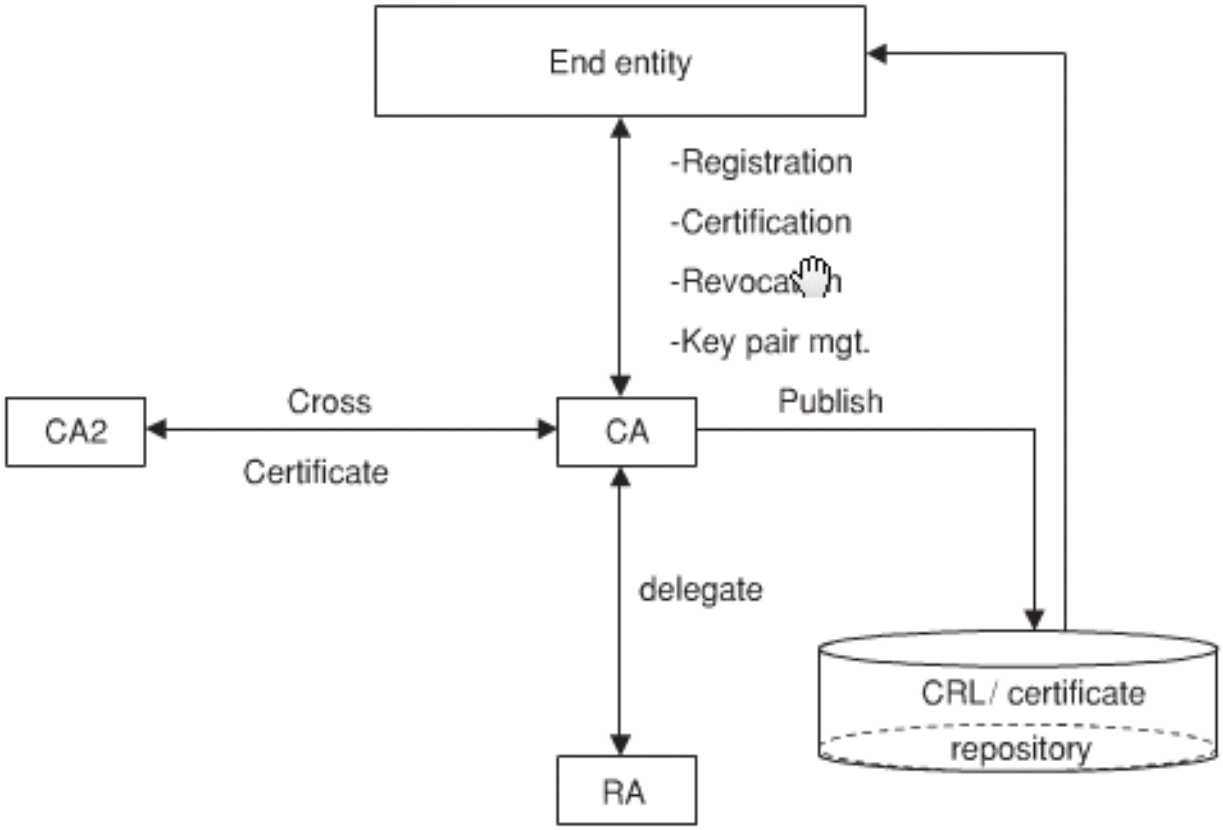
3.2.2 PKIX

- **What's PKIX**
  - The PKIX (Public key infrastructure X.509) model defines the elements that comprise a PKI including components, documents, and policy instruments.
- **The Component of PKIX**
  - PKIX components integrate four major components:
    - ✧ the End-Entity (终端实体)
    - ✧ Public Key Certificate (PKC, 公开密钥证书)
    - ✧ Certification Authority (CA, 证书授权机构/认证机构)
    - ✧ Certification Repository (CR, 证书仓库)

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**



3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - End-entity (终端实体)
    - ✧ the user/consumers of the PKI-related services, such as subscribers, network devices, processes, or any other entity that has applied for and received a digital certificate for use in supporting the security and trust in transactions to be undertaken.
  - PKC (公钥证书)
    - ✧ PKC is a digital document that is associated with and end-entity. It provides a means of identifying end-entities of their identities to public keys.

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - CA (证书机构)
    - ✧ the issuer of PKC and certificate revocation lists (CRL).
    - ✧ PKC are digitally signed by the CA, which effectively (and legally) binds the subject name to subject public key and the CA's public key.
    - ✧ a CA also involved in a number of administrative and technical tasks.
  - CR (证书仓库)
    - ✧ a certificate repository is a generic term used to specify any method for storing and retrieving certificate-related information such as the public key certificates issued for end-entities and the CRLs which report on revoked certificates.

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - CRL (证书撤回清单/证书吊销列表)
    - ✧ a signed document containing reference to certificates, which are decide to be no longer valid.
  - CRL issuer (CRL 签发者)
    - ✧ CRLI may be an optional entity to which a CA delegates the verification of information related to revocation, issuance and the publication of CRLs.
  - RA (注册机构)
    - ✧ a registration authority is an administrative component to which a CA delegates certain management functions. However, the RAs are not allowed to issue certificates or CRLs. (RA 是受CA委托实施某些管理功能的管理组件)

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - PKI Document
    - ✧ a PKI must be operated in accordance with well-defined policies that define the rules to perform the PKI activities appropriately. Four important documents are:
      - Certificate policy (CP, 证书策略)
      - Certificate practice statement (CPS, 证书操作规范)
      - Subscriber agreements (用户协议)
      - Relying party agreements (第三方信任协议)

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - Certificate policy (CP)
    - ✧ a certificate policy sets forth general requirements that PKI participants must meet in order to operate within a PKI. A CP is also a named set of rules that indicate the applicability of a certificate to a given application.
  - Certificate practice statement (CPS)
    - ✧ a certificate practice statement defines a comprehensive statement of practices and procedures followed by a single CA or a related set of CAs set out in a CP.

3.2 Public Key Infrastructure

3.2.2 PKIX

- **The Component of PKIX**
  - Subscriber agreements
    - ✧ a document representing an agreement between the subscriber applying and receiving a certificate and the issuing authority of the certificate. It focuses on the subscriber's responsibilities, rights, and obligations in using the certificate.
  - Relying party agreements
    - ✧ this is typically an agreement between a party that wishes to rely on a certificate and the information contained in it.

3.2 Public Key Infrastructure

3.2.3 The Management of PKIX

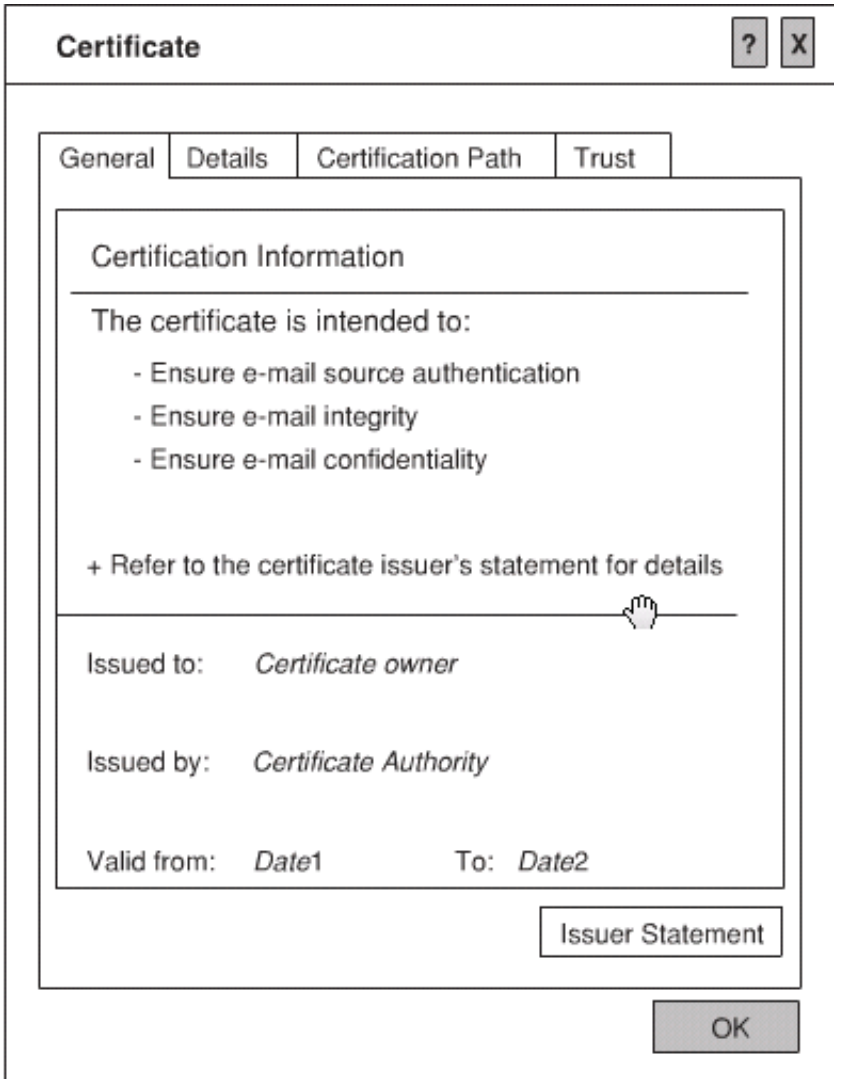
- Registration
- Initialization
- Certificate generation
- Certificate update
- Revocation
- Key pair management
- Cross-certification
- Additional management functions

3.2 Public Key Infrastructure

3.2.4 Public Key Certificate

– Form of certificate

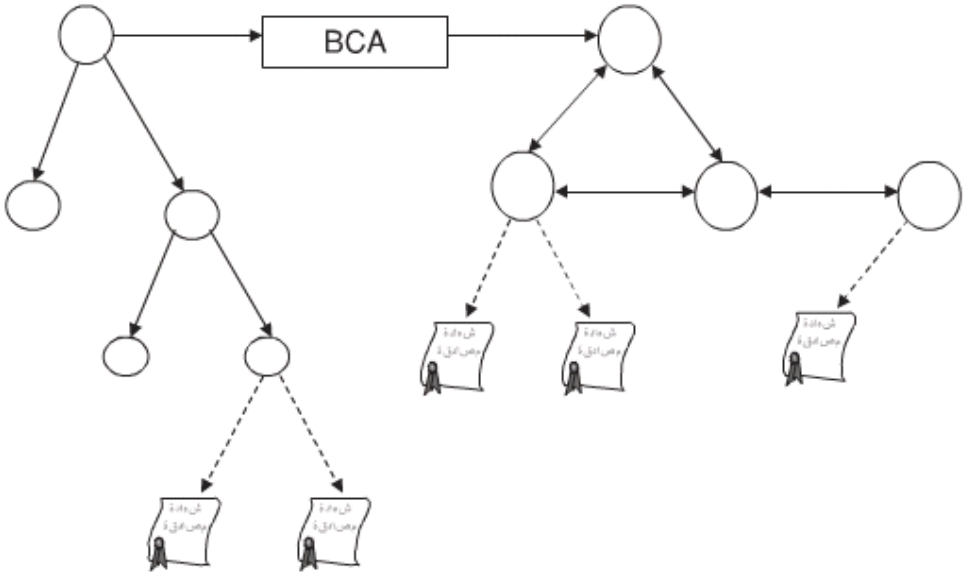
1. Certificate version
2. Serial number
3. Signature algorithm
4. Issuer
5. Validity
6. Subject
7. Subject public key info



3.2 Public Key Infrastructure

3.2.5 Trust Hierarchy Model

- Hierarchy Model 严格分层模型
- Mesh PKI 对等模型
- Bridge CA 桥接模型



End of Chapter 3.2