



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**
  - Introduction
  - Description
  - Kerberos Process
  - Drawbacks & Limitations
- **3.4 X.509**
  - What is X.509
  - Certificate
  - Security problems
  - Application



- 两种看法
1. 电子证书, 二进制文件
  2. 一个完整的公钥基础设施

## 3.4 X.509

---

### 3.4.1 What is X.509

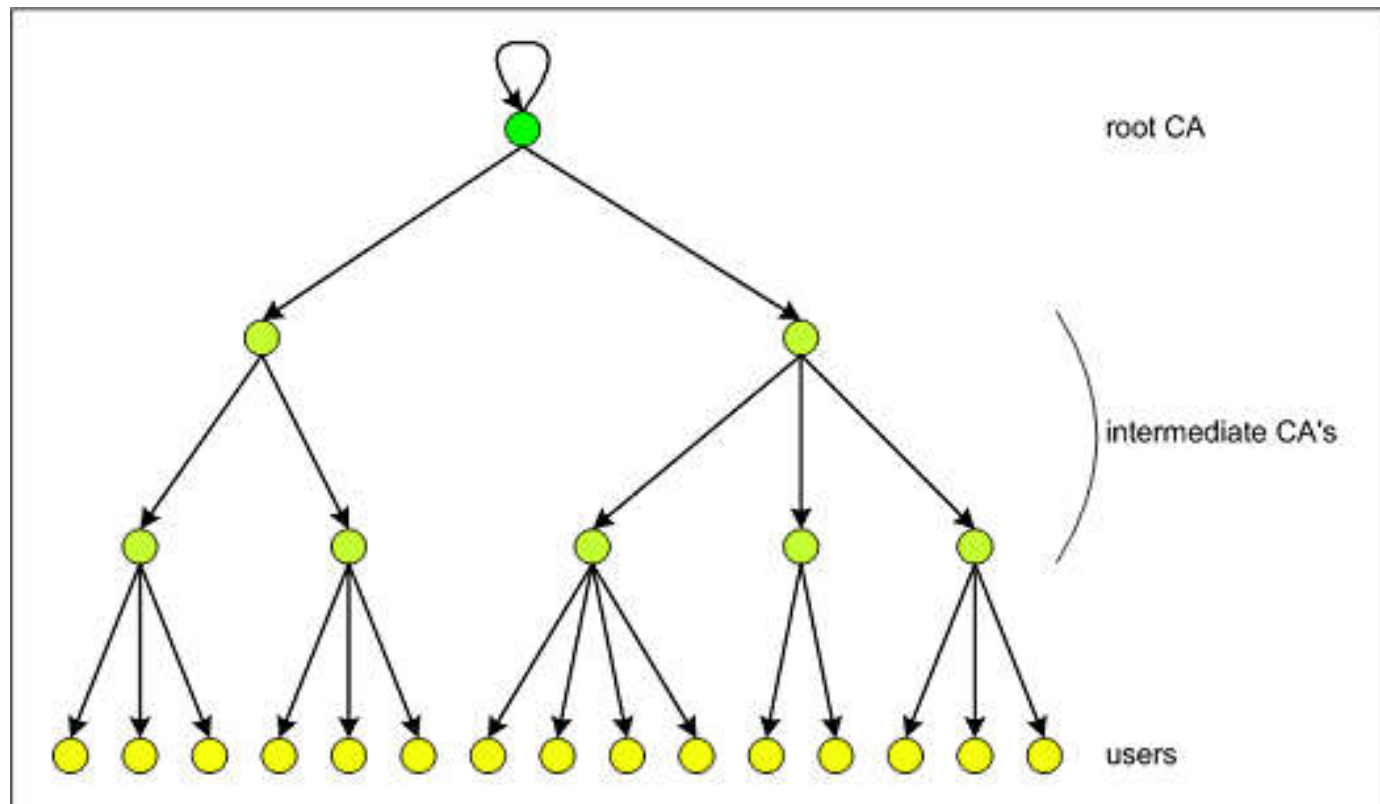
- **X.509**
  - X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO, 单点登录) and Privilege Management Infrastructure (PMI, 特权管理基础架构).
  - X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
  - Key words
    - ✧ Certificate
    - ✧ CA (Certificate Authority)
    - ✧ Hierarchy



## 3.4 X.509

### 3.4.1 What is X.509

- X.509
  - Hierarchy



## 3.4 X.509

---

### 3.4.1 What is X.509

- **History and Versions**

- Version 1 (1988): issued and associated with the X.500 Standard
- Version 2 (not used widely): include Subject and Issuer identifier
- Version 3 (1996): Extensions added
  - ✧ called PKIX for *Public Key Infrastructure*
- RFC 5280

## 3.4 X.509

---

### 3.4.2 Certificate

- **Introduction**

- In the X.509 system, a certification authority (CA) issues a **certificate** binding a public key to a particular distinguished name in the X.500 tradition, or to an alternative name such as an e-mail address or a DNS-entry.
- An organization's trusted root certificates (根证书) can be distributed to all employees so that they can use the company PKI system.
- Browsers such as IE, Netscape/Mozilla, Opera, Safari and Chrome come with root certificates pre-installed, so SSL certificates from larger vendors will work instantly; in effect the browsers' developers determine which CAs are trusted third parties for the browsers' users.

## 3.4 X.509

---

### 3.4.2 Certificate

- **Structure of Certificate**

Certificate

Version

Serial Number

Algorithm ID

Issuer (CA's name)

Validity

Not Before

Not After

Subject

Subject Public Key Info

Public Key Algorithm

Subject Public Key

Issuer Unique Identifier (Optional)

Subject Unique Identifier (Optional)

Extensions (Optional)

Certificate Signature Algorithm

Certificate Signature



## 3.4 X.509

---

### 3.4.2 Certificate

- **Example of Certificate**

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 7829 (0x1e95)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,  
OU=Certification Services Division, CN=Thawte Server, CA/emailAddress=server-  
certs@thawte.com

Validity:

Not Before: Jul 9 16:04:02 1998 GMT

Not After : Jul 9 16:04:02 1999 GMT

Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala, OU=FreeSoft,  
CN=www.freesoft.org/emailAddress=baccala@freesoft.org

## 3.4 X.509

---

### 3.4.2 Certificate

- **Example of Certificate**

Certificate:

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:  
33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:  
66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:  
70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:  
16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:  
c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:  
8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:  
d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:  
e8:35:1c:9e:27:52:7e:41:8f

Exponent: 65537 (0x10001)

公钥(e,N)  
N:模底  
私钥(d,N)

## 3.4 X.509

---

### 3.4.2 Certificate

- **Example of Certificate**

Certificate:

Signature Algorithm: md5WithRSAEncryption

93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:  
92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:  
ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:  
d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:  
0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:  
5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:  
8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:  
68:9f

## 3.4 X.509

---

### 3.4.2 Certificate

- **How to get a certificate**
  - CA distributing
  - Certificate transported by link
    - ✧ Feature
      - Everyone with CA's public key can get the public key in the CA's certificate
      - Only CA can modify the certificate
    - ✧ CA can exchange their PK safely

## 3.4 X.509

---

### 3.4.2 Certificate

- **Revoke a certificate**
  - Why revoking
    - ✧ Every certificate has a validity
    - ✧ User don't think the key is secure
    - ✧ User don't trust CA
    - ✧ CA think the certificate is unsecure
  - CRL (Certificate Revocation List)
    - ✧ the certificate revoked by not out of valid time

## 3.4 X.509

---

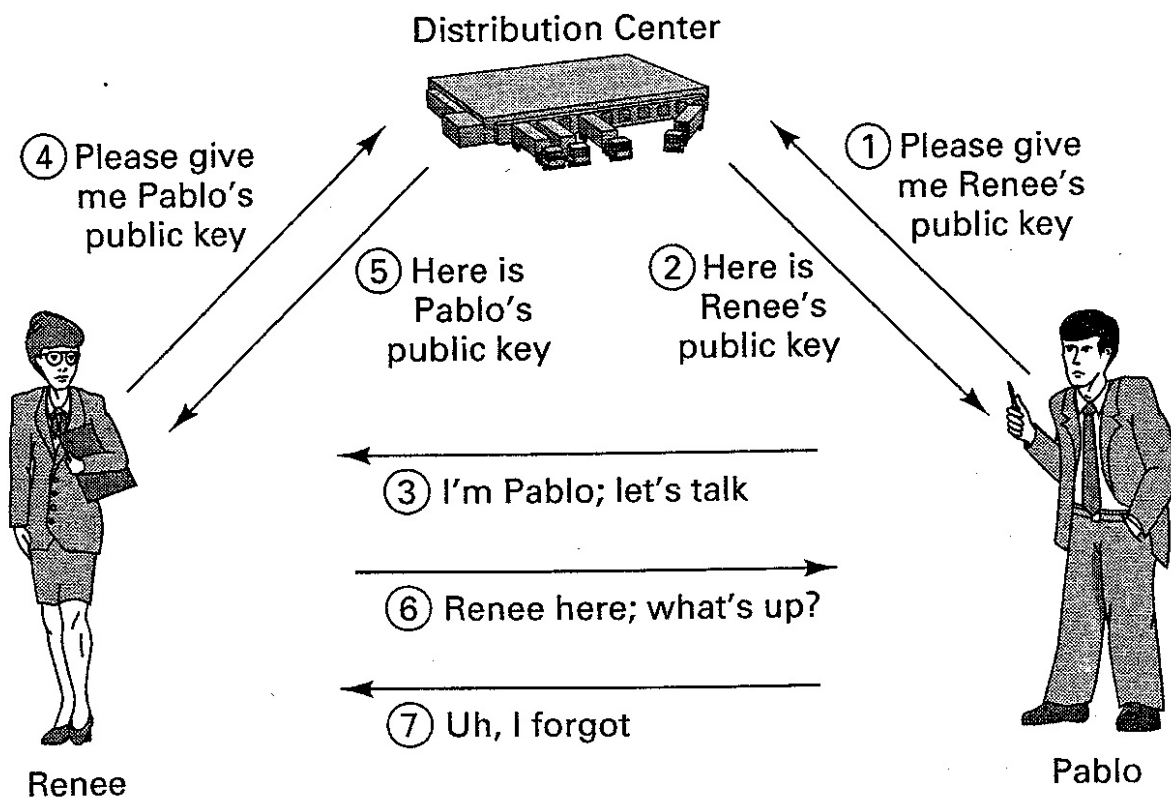
### 3.4.3 Security problems

- **Security Problems with X.509**
  - Specification
    - ✧ Complexity and lack of quality
  - Architectural flaw
  - Commercial certificate authorities
  - Implementation

## 3.4 X.509

### 3.4.3 Security problems

- **Security Problems with X.509**
  - Specification: Complexity and lack of quality



## 3.4 X.509

---

### 3.4.4 Applications

- **Applications with X.509**
  - S/MIME (Multipurpose Internet Mail Extensions)
  - SSL (Secure Socket Layer)
  - TLS (Transport Layer Security )
  - SET (Secure Electronic Trade)
  - PKI (Public Key Infrastructure)
  - .....



# Referances

---

1. William Stallings. “Cryptography and Network Security Principles and Practices”
2. Mohammad Obaidat, Nouredine Boudriga. “Security of e-Systems and Computer Networks.”
3. Tim Moses. “PKI Trust Models”(Draft)
4. [http://en.wikipedia.org/wiki/  
Public key infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)  
X.509  
X.500  
Kerberos protocol
5. <http://www.dartmouth.edu/~deploypki/applications.html>
6. <http://guides.brucejmack.biz/SOA-Patterns/WSSP/13.3X509AppDoc.htm>
7. <http://web.mit.edu/kerberos/>
8. <http://www.kerberos.org/>



## End of Chapter 3

