网络安全

第二章 系统安全、风险评估理论与应用

黄 玮

温故

- 基本术语
  - —安全是什么？CIA的内涵？
  - —资产、威胁、风险、漏洞、影响、攻击
- 安全策略和安全机制
  - —声明和实现
- P2DR模型
  - —安全是持续循环、动态变化过程
- 等级安全保护
  - —安全操作系统分级

知新

- 操作系统中的
  - —安全策略：访问控制策略
  - —安全机制：访问控制机制
- 通用弱点评价系统——CVSS
  - —Common Vulnerability Scoring System
- 风险评估的基本原理与案例分析

本章内容提要

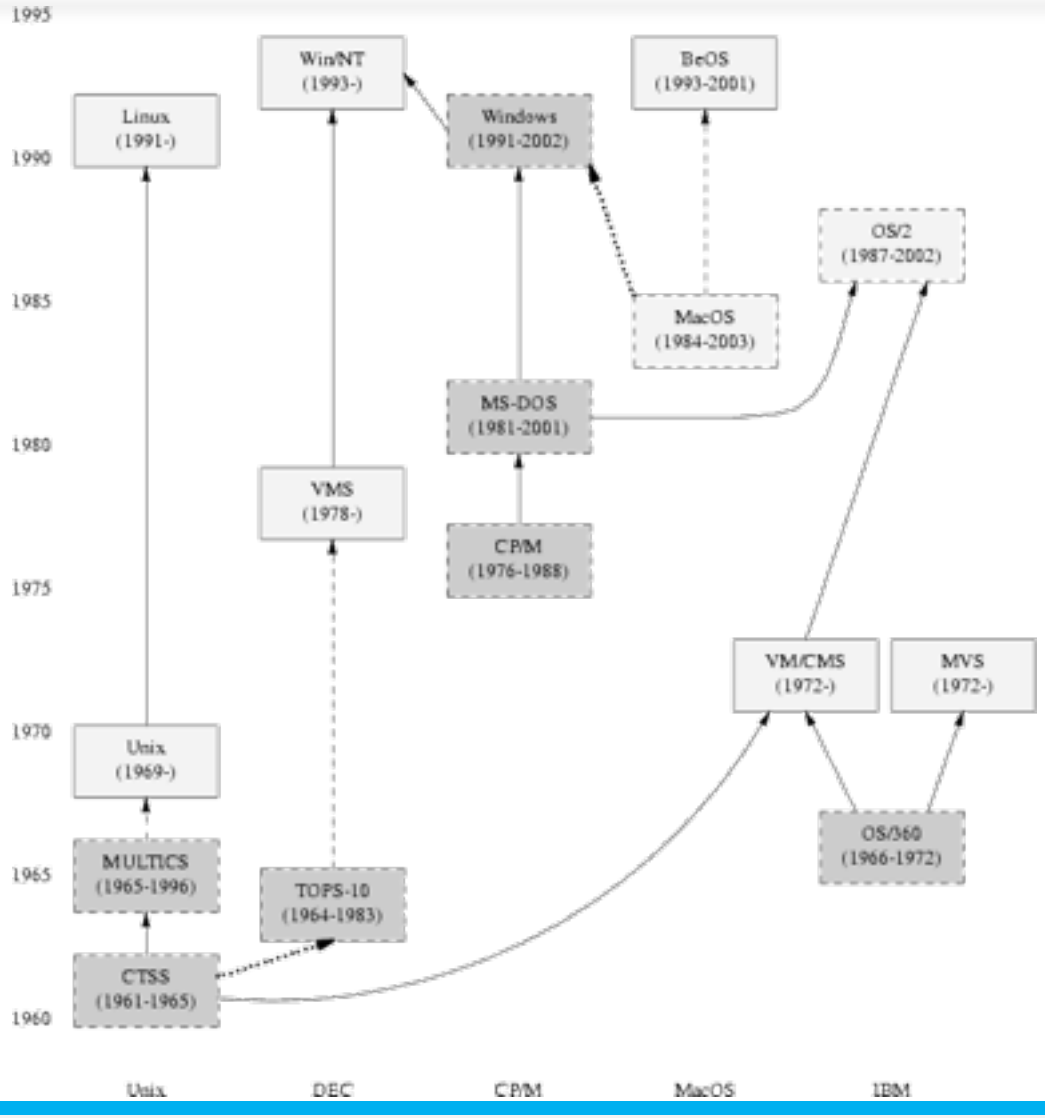
一.操作系统简史

二.数字标识理论

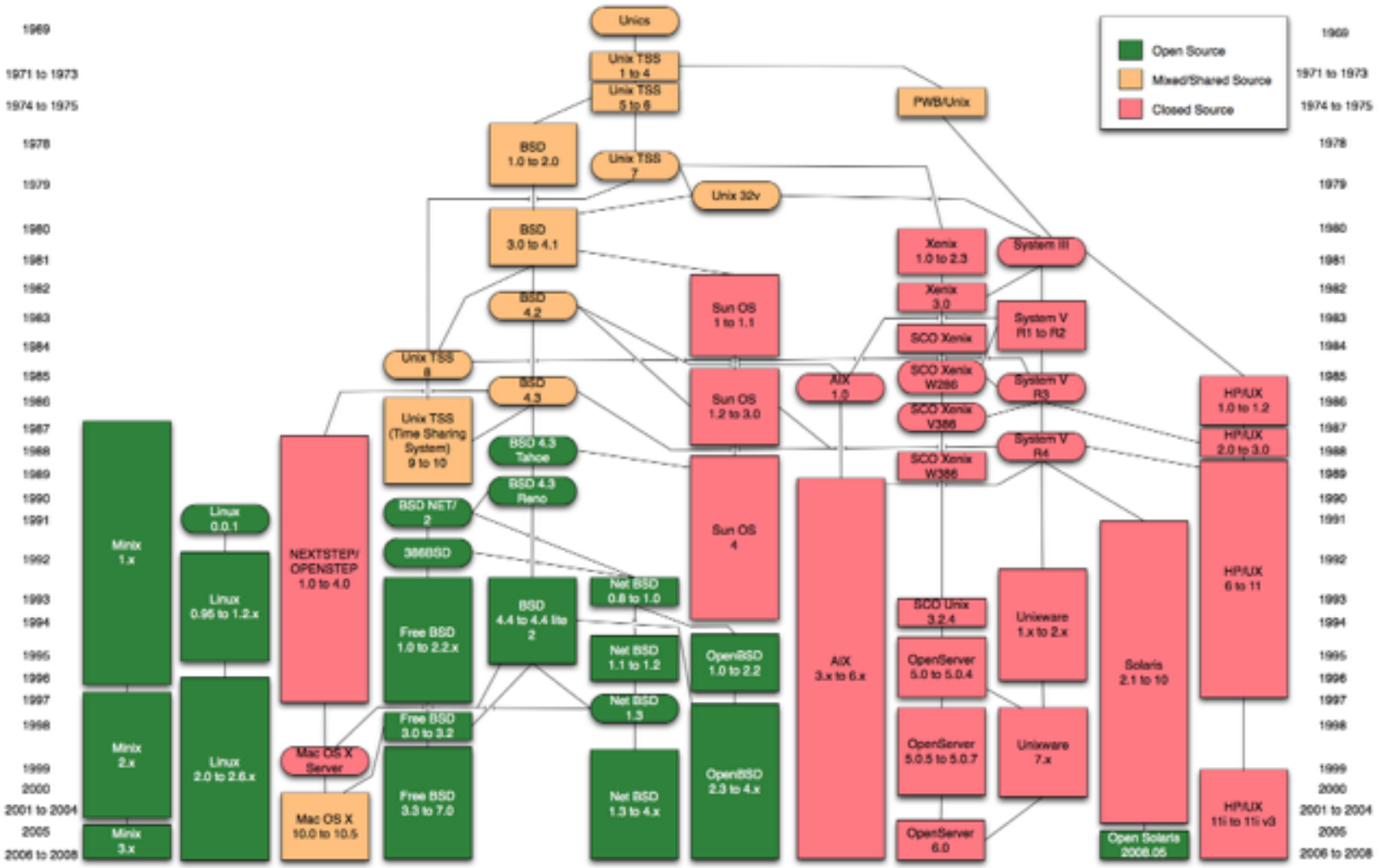
三.访问控制理论

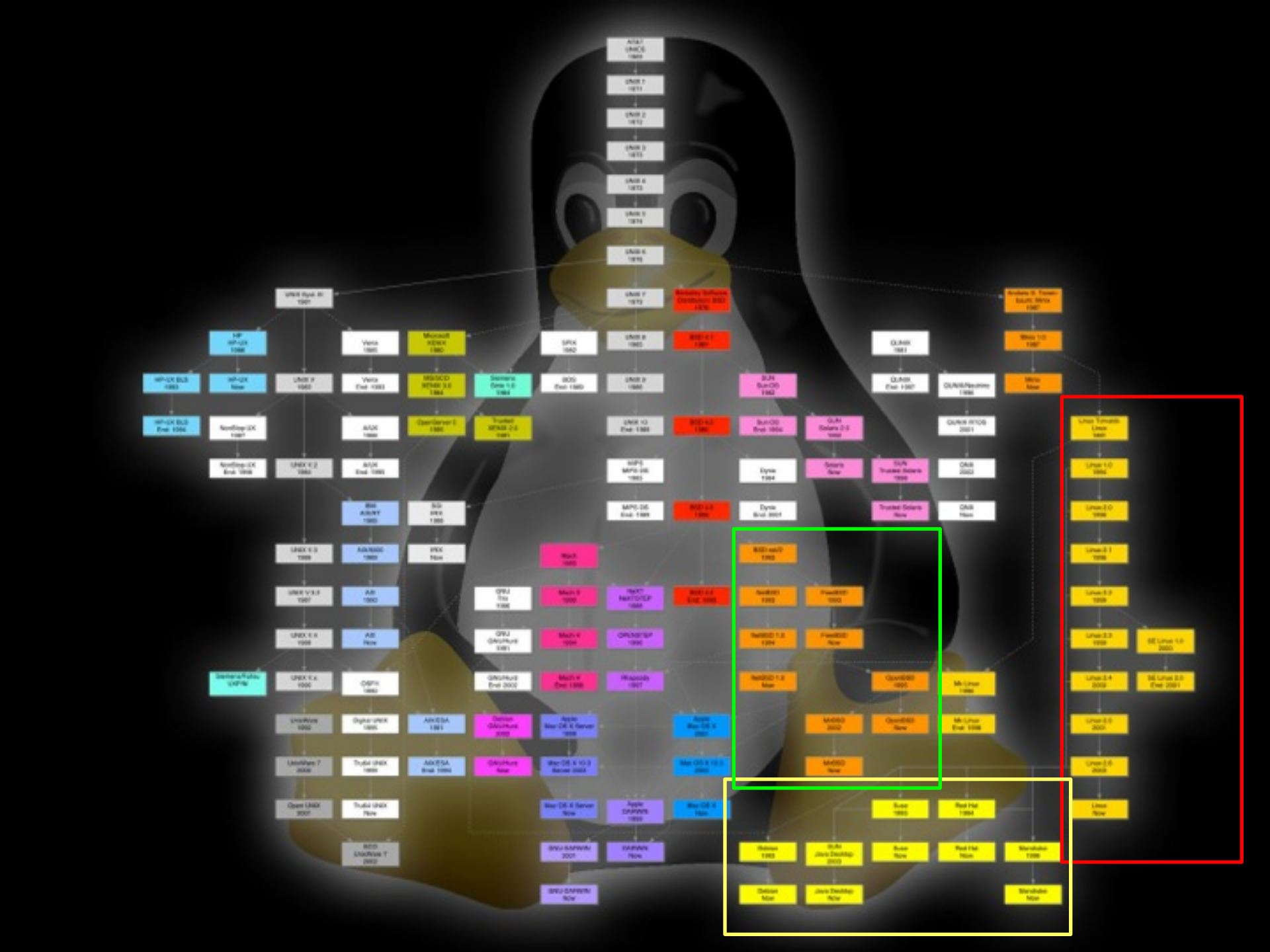
四.风险评估理论与实践

近代操作系统简史


1995
1990
1985
1980
1975
1970
1965
1960
Linux
(1991-)
Win/NT
(1993-)
Windows
(1991-2002)
BeOS
(1993-2001)
OS/2
(1987-2002)
MacOS
(1984-2003)
MS-DOS
(1981-2001)
VMS
(1978-)
CP/M
(1976-1988)
VM/CMS
(1972-)
MVS
(1972-)
Unix
(1969-)
OS/360
(1966-1972)
MULTICS
(1965-1996)
TOPS-10
(1964-1983)
CTSS
(1961-1965)
Unix
DEC
CP/M
MacOS
IBM

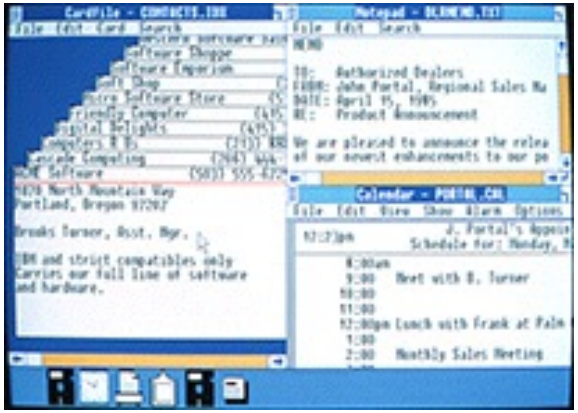
Unix系统简史——源代码授权协议角度

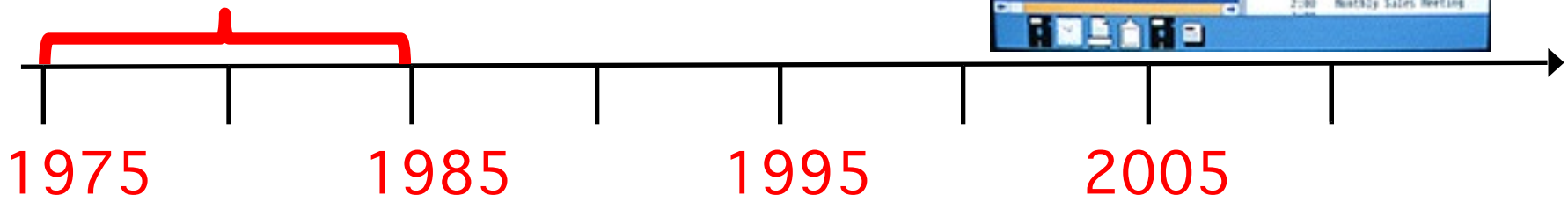




Windows的历史（1/4）

- Microsoft的起步
  - —创始人：Bill Gates & Paul Allen
  - —1980年6月：Steve Ballmer受雇负责公司运营
  - —1981年推出运行MS-DOS的IBM PC
    - C:\ 开始流行
- Windows 1.0
  - —1982-1985 （研发历史3年）





Windows的历史（2/4）

- 1987 – 1992：Windows 2.0 – 2.11

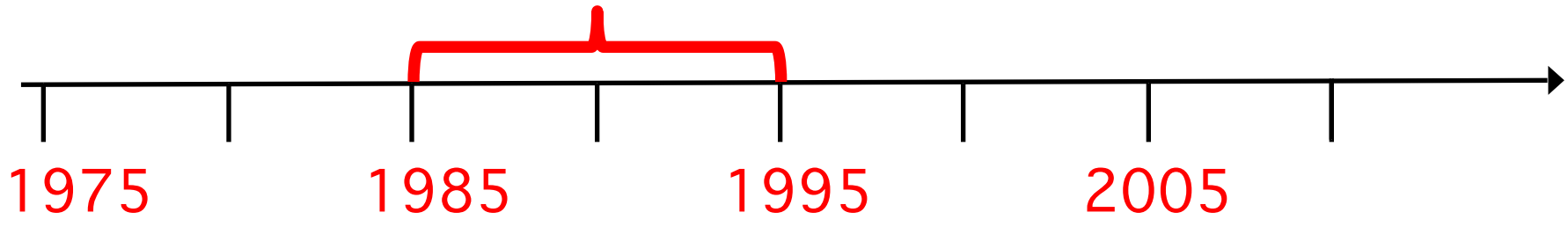
  —窗口更多，速度更快

- 1990 – 1994：Windows 3.0 – Windows NT

  —实现图形效果

- 1995 – 2001: Windows 95

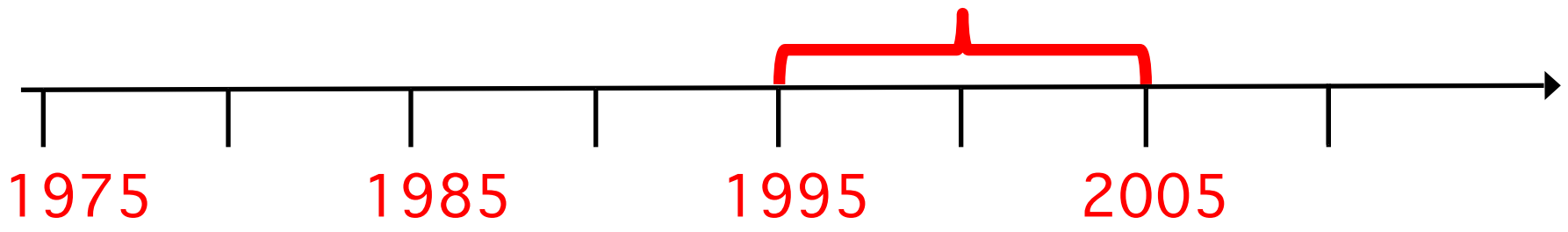
  —个人电脑和 Internet 蓬勃发展



Windows的历史（3/4）

- 1998 – 2000： Windows 98, Windows 2000, Windows Me
- 2001 – 2005： Windows XP

—稳定、易用且快速



Windows的历史（4/4）

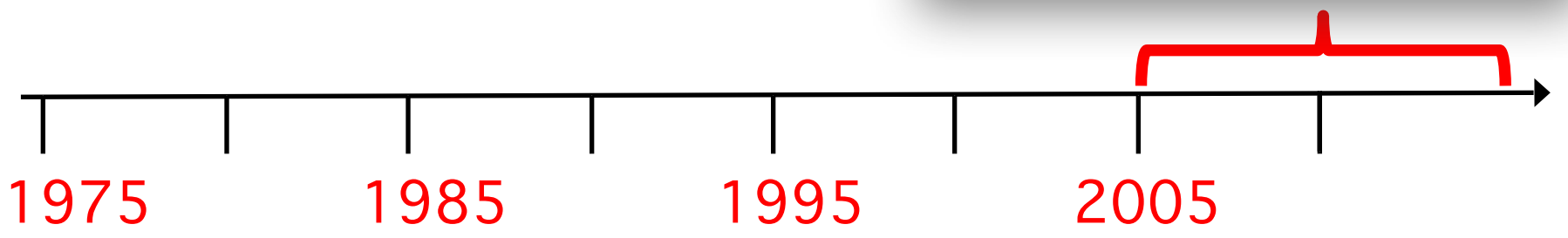
- 2006 – 2008: Windows Vista

  —安全智能

- 2009 – 2012： Windows 7

- 2012.2.29 ： Windows 8

  —移动化



本章内容提要

一.操作系统简史

二.数字标识理论

三.访问控制理论

四.风险评估理论与实践

定义

- 实体
  - —Entity
  - —业务操作的发起者（主体）或对象（客体）
- 标识
  - —Identity
  - —对实体的数字化指代
  - —又称“数字标识”

数字标识的意义

- 对信息安全相关实体建立标识体系是构建信息安全系统的基础工作之一
  - —身份认证
  - —访问控制
  - —安全审计
  - —网络协议

常见的数字标识技术

- 系统实体标识
  - —系统资源标识
  - —用户、组和角色标识
  - —与数字证书相关的标识
- 网络实体标识
  - —主机、网络和连接标识
  - —网络资源标识
  - —连接及其状态标识

系统实体标识

- 操作系统
  - —文件标识
    - 文件名和存储路径
  - —进程标识
    - 进程号：PID
- 数据库系统
  - —数据表标识
    - 数据库名和表名

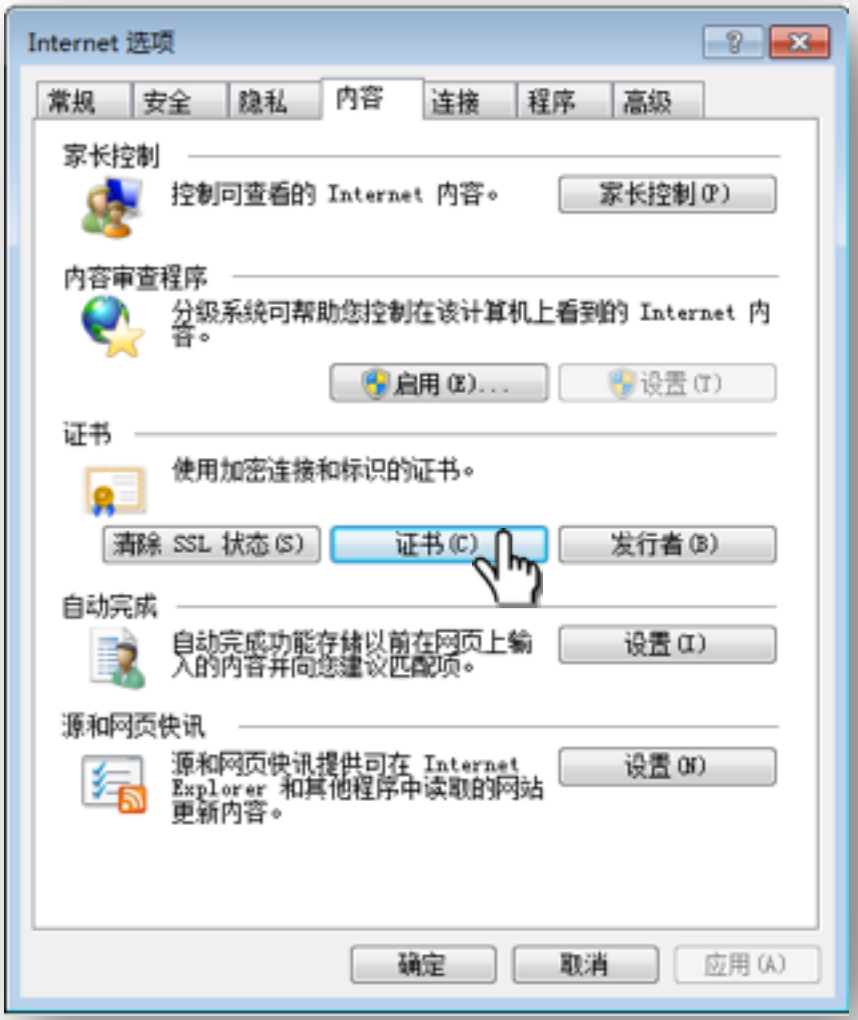
用户、组和角色标识

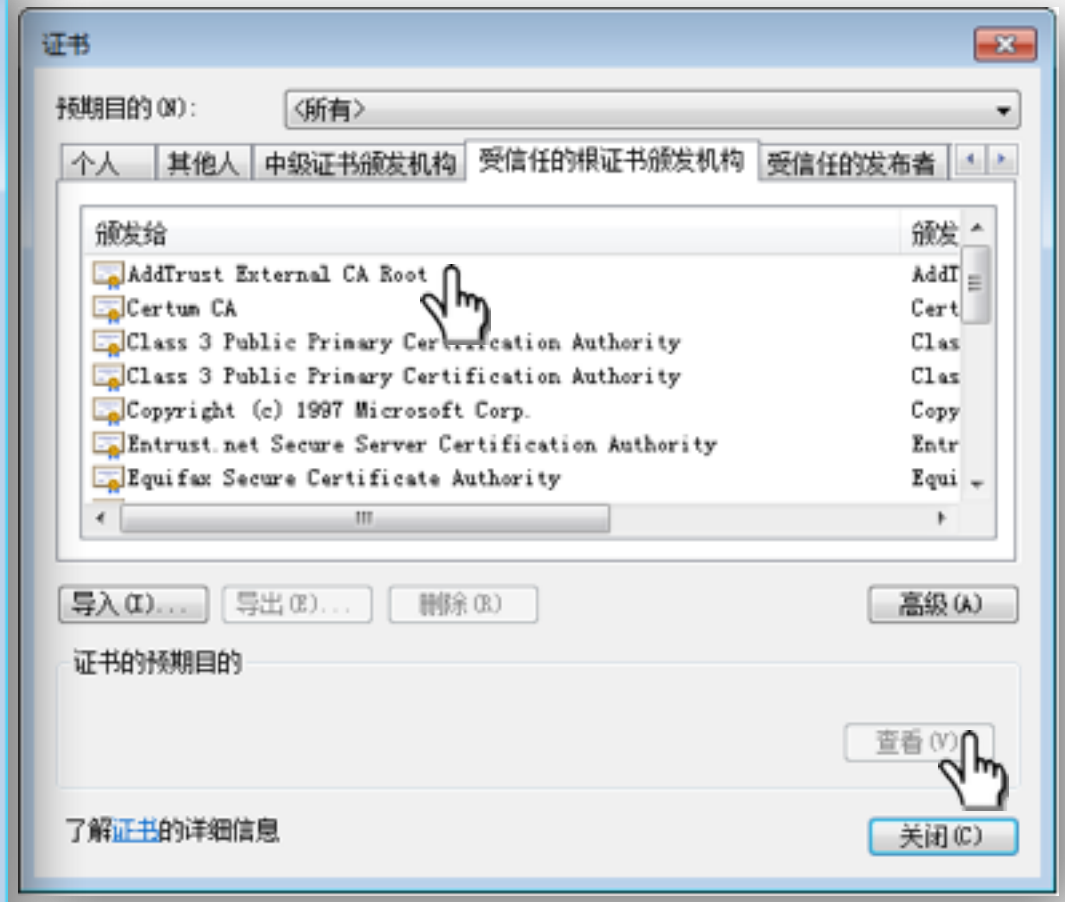
- 用户
  - —用户号：UID
- 用户组
  - —用户组号：GID
- 角色标识
  - —特殊用户分组

与数字证书相关的标识

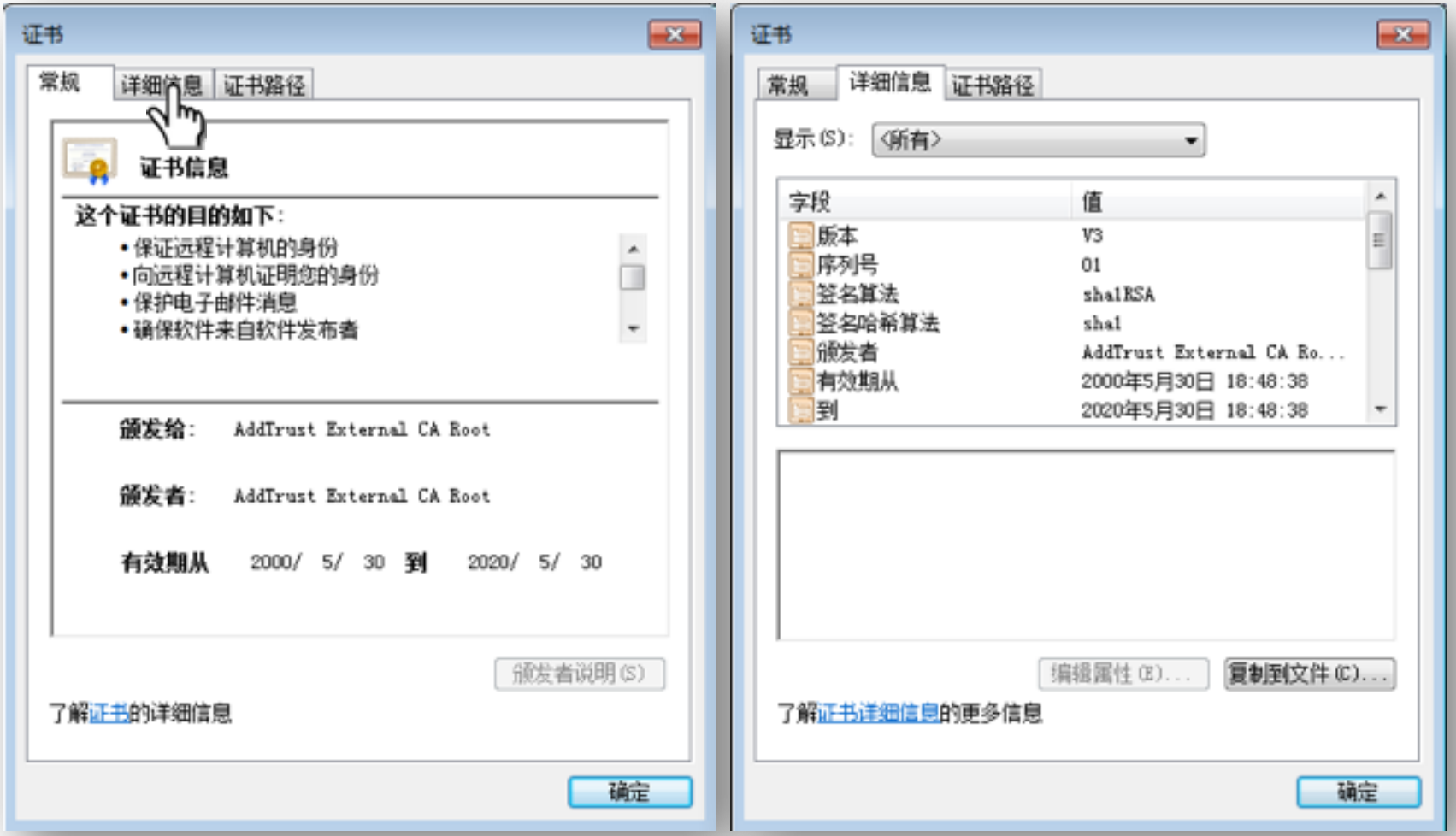
- 数字证书用于绑定证书所有者情况及其公钥
  - —在数字签名和认证中用于向签名验证者或身份认证者提供这些信息
- X.509证书
  - —基本信息
  - —辅助信息
- 数字证书通常由证书签发者对证书签名
  - —基于数字证书的标识具有抗篡改的特性

数字证书实例(1/2)


Internet 选项
常规
安全
隐私
内容
连接
程序
高级
家长控制
控制可查看的 Internet 内容。
家长控制(P)
内容审查程序
分级系统可帮助您控制在该计算机上看到的 Internet 内容。
启用(E)...
设置(T)
证书
使用加密连接和标识的证书。
清除 SSL 状态(S)
证书(C)
发行者(B)
自动完成
自动完成功能存储以前在网页上输入的内容并向您建议匹配项。
设置(I)
源和网页快讯
源和网页快讯提供可在 Internet Explorer 和其他程序中读取的网站更新内容。
设置(N)
确定
取消
应用(A)


证书
预期目的(N):
<所有>
个人
其他人
中级证书颁发机构
受信任的根证书颁发机构
受信任的发布者
颁发给
颁发
AddTrust External CA Root
Certum CA
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
Copyright (c) 1997 Microsoft Corp.
Entrust.net Secure Server Certification Authority
Equifax Secure Certificate Authority
导入(I)...
导出(E)...
删除(R)
高级(A)
证书的预期目的
查看(V)
了解证书的详细信息
关闭(C)

数字证书实例(2/2)


证书
常规
详细信息
证书路径
证书信息
这个证书的目的如下:
• 保证远程计算机的身份
• 向远程计算机证明您的身份
• 保护电子邮件消息
• 确保软件来自软件发布者
颁发给: AddTrust External CA Root
颁发者: AddTrust External CA Root
有效期从 2000/ 5/ 30 到 2020/ 5/ 30
颁发者说明(S)
了解证书的详细信息
确定
证书
常规
详细信息
证书路径
显示(S): <所有>
字段
值
版本 V3
序列号 01
签名算法 sha1RSA
签名哈希算法 sha1
颁发者 AddTrust External CA Ro...
有效期从 2000年5月30日 18:48:38
到 2020年5月30日 18:48:38
编辑属性(E)...
复制到文件(C)...
了解证书详细信息的更多信息
确定

主机、网络和连接标识

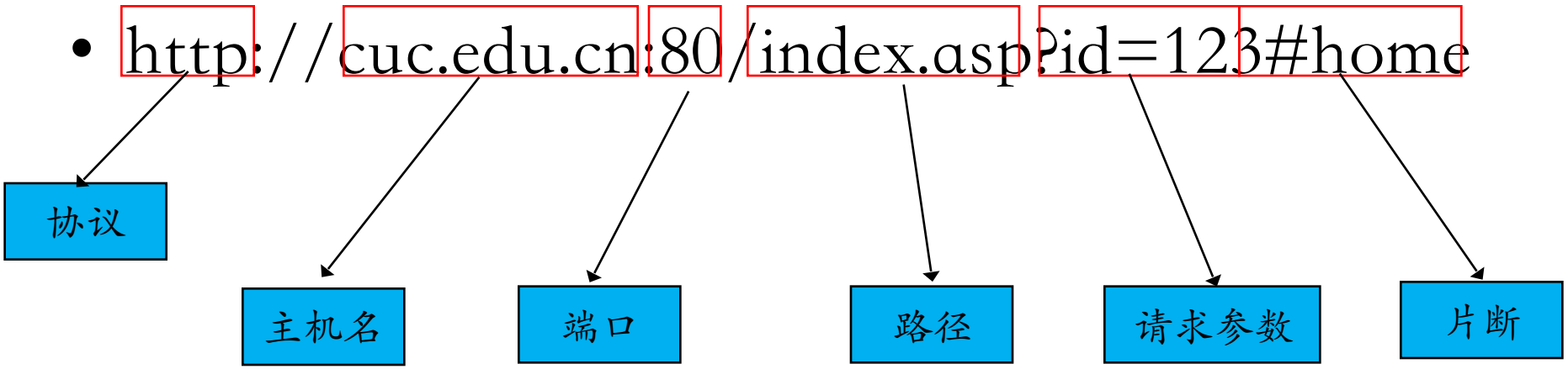
- 主机标识
  - —数据链路层：MAC地址
    - 例如：08-00-27-07-DD-0A
  - —网络层：网络地址
    - 对于TCP/IP网络，即IP地址
  - —应用层：域名地址

网络资源标识

- 统一资源定位符

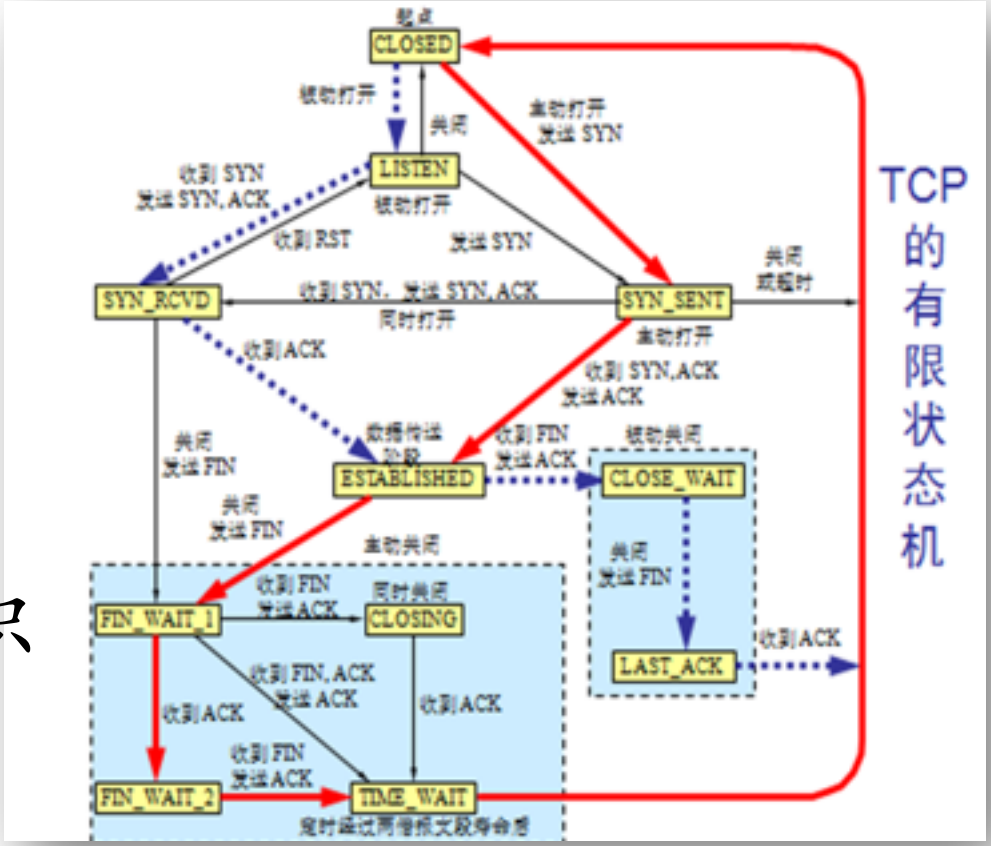
  —URL：Uniform Resources Locator

- http://cuc.edu.cn:80/index.asp?id=123#home



连接及其状态标识

- 唯一标识一个网络(会话)连接：IP五元组
  - —源IP地址
  - —目的IP地址
  - —源端口
  - —目的端口
  - —传输层协议类型
- (会话)连接状态标识



本章内容提要

一.操作系统简史

二.数字标识理论

三.访问控制理论

四.风险评估理论与实践

生活中的访问控制机制

安全专家：“报告老板，通往停车场的道路已经被我们封锁了！绝对安全！”

访问控制理论

访问控制的基本概念

- 主体

  —主动的实体，是访问的发起者，它造成了信息的流动和系统状态的改变，主体通常包括人、进程和设备等

- 客体

  —包含或接受信息的被动实体，客体在信息流动中的地位是被动的，客体通常包括文件、设备、信号量和网络节点等

- 访问

  —是使信息在主体和客体之间流动的一种交互方式

访问控制的基本概念

- 授权访问

  —主体访问客体的允许，授权访问对每一对主体和客体来说是给定的

- 安全访问策略

  —一套规则，可用于确定一个主体是否对客体拥有访问能力

  —主体对客体的操作行为集和约束条件集

- 访问控制的三要素

  —主体、客体、安全访问策略

访问控制模型

- 访问控制的三个基本面
  - —认证
    - 身份认证：客体对主体的识别认证
    - 客体和主体的身份可以随着时间、应用场景而改变
  - —(访问控制)策略实现：访问授权
    - 授权主体对客体可以正常访问
    - 非授权主体对客体无法访问
  - —访问审计
    - 记录访问历史，实现不可抵赖性

访问控制策略

- 自主访问控制
  —DAC: Discretionary Access Control
- 强制访问控制
  —MAC: Mandatory Access Control
- 基于角色的访问控制
  —RAC: Ro1e-Based Access Control

自主访问控制

- 特点
  - —已授权主体可以访问客体
  - —非授权主体无法访问客体
  - —访问授权可以自主分配（授权和取消授权）
    - A可以访问文件α，则A可以授权B也能访问文件α
- 实现方式举例
  - —访问控制列表(ACL：Access Control List)
  - —访问控制矩阵
  - —面向过程的访问控制

访问控制矩阵

访问控制矩阵示例

某系统中有2个进程和2个文件

访问权限集合：{读、写、执行、追加、属主}

	文件A	文件B	进程A	进程B
进程*A*	读、写、属主	读	读、写、执行、属主	写
进程*B*	追加	写、属主	读	读、写、执行、属主

- 属主：绝大多数现代操作系统，属主权限的拥有主体可以对所拥有的权限自行分配

强制访问控制

- 特点
  - —(操作)系统对访问主体和受控对象(客体)实行强制访问控制
  - —多级访问控制策略
  - —(操作)系统预先分配好主客体安全级别：安全标签
  - —主体访问客体时先进行安全级别属性比较，再决定访问主体能否访问该受控对象(客体)

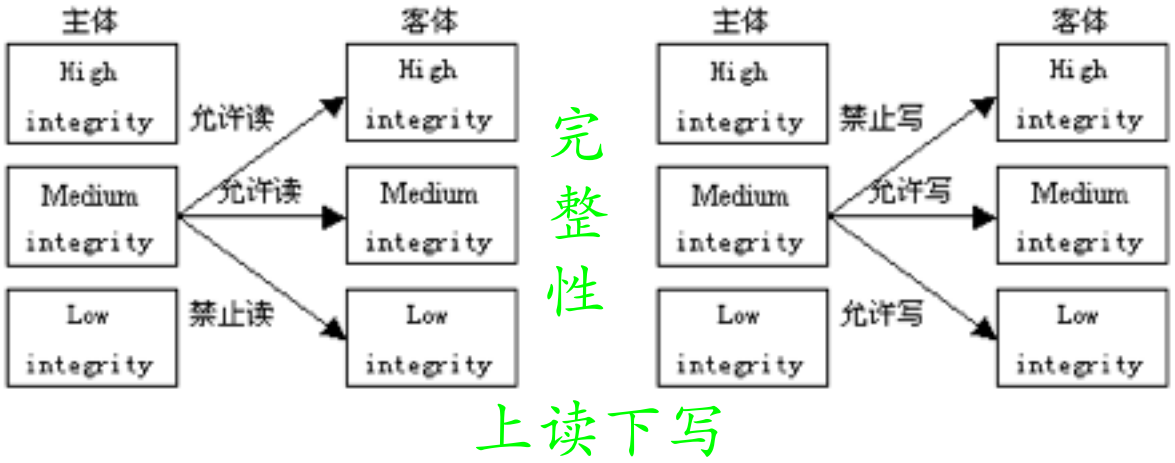
- 实现方式举例

—Lattice模型

—BLP模型

Bell-LaPadula

—Biba模型



基于角色的访问控制

- 强制访问控制模型的一种实现形式
- 但不是基于多级访问控制策略的实现
- 用户和访问权限的逻辑分离
  - —访问权限首先是与角色相关联
  - —然后角色再与用户关联
  - —从而完成基于角色的访问授权
- 用户不能任意的将访问权限传递给其他用户
  - —和DAC的最基本区别

身份认证

- 将身份标识唯一的绑定到主体
- 外部实体能够向系统证明其身份标识唯一性的因素
  - —知道的（例如：口令或秘密信息）knows
  - —拥有的（例如：令牌或磁卡）has
  - —生物特征（例如：指纹、虹膜）is
  - —实体位置（例如：在特定终端上）where
- 以上因素可以单一使用，也可以多个同时使用

访问授权

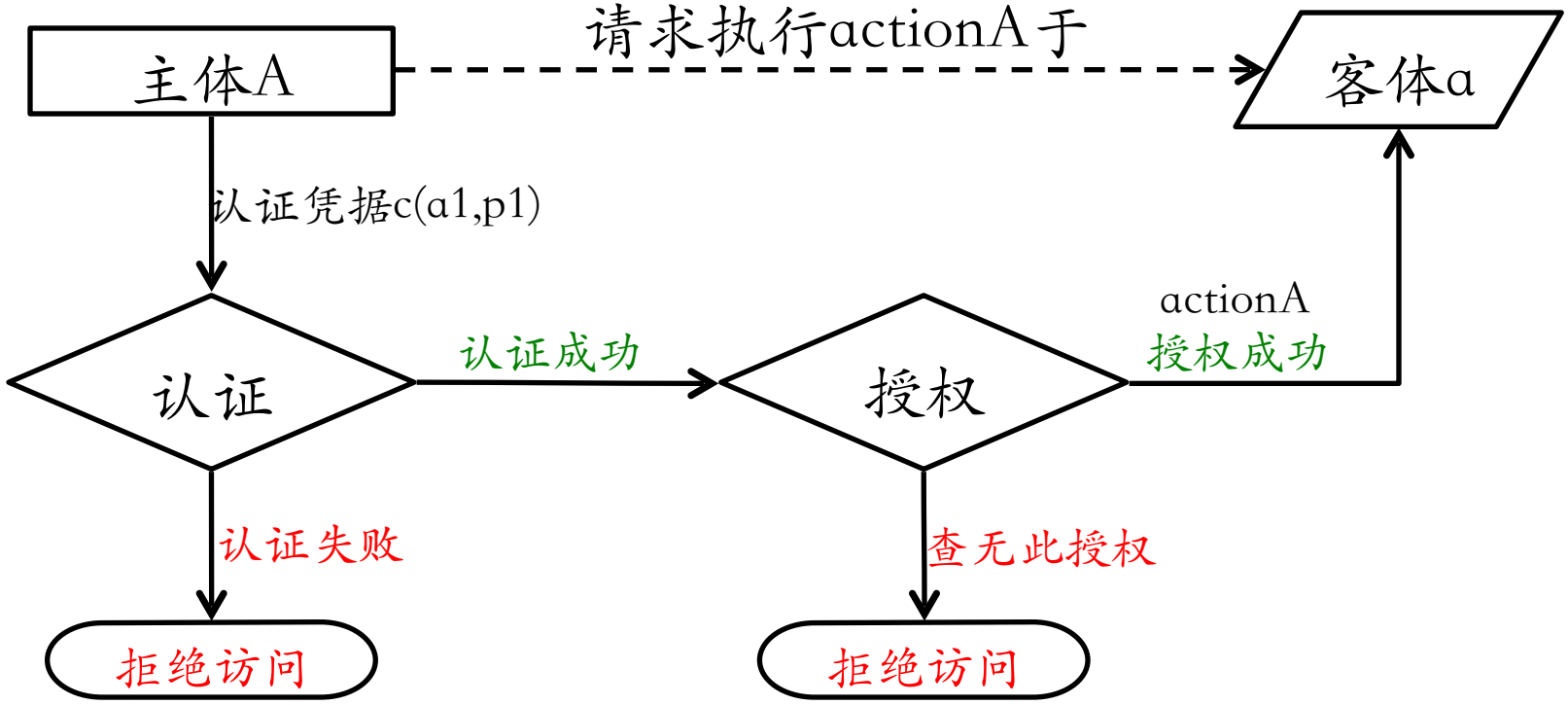
- 授权类型
  - —授予(grant)权限
    - 拥有该权限的主体可以将所拥有的客体访问权限分配给其他主体
  - —属主(own)权限
    - 客体的创建者通常都会拥有属主权限，该权限可以由创建者自己授予他人
- 权限的弱化原则
  - —主体无法将自己不具备的权限授予他人
  - —主体如果具有属主权限则不受上述原则约束

撤销访问授权

- 为何需要撤销访问授权?
  - —认证凭据丢失/被盗
  - —人员变动（离职/岗位变动等）
- 如何取消访问授权?
  - —身份认证环节：禁用/取消/删除认证凭据
  - —访问授权环节：禁用/取消/删除/修改访问控制列表中的授权项

身份认证和访问授权的关系

- 身份认证是访问授权的基础
- 没有身份认证就无法实现访问授权



访问审计

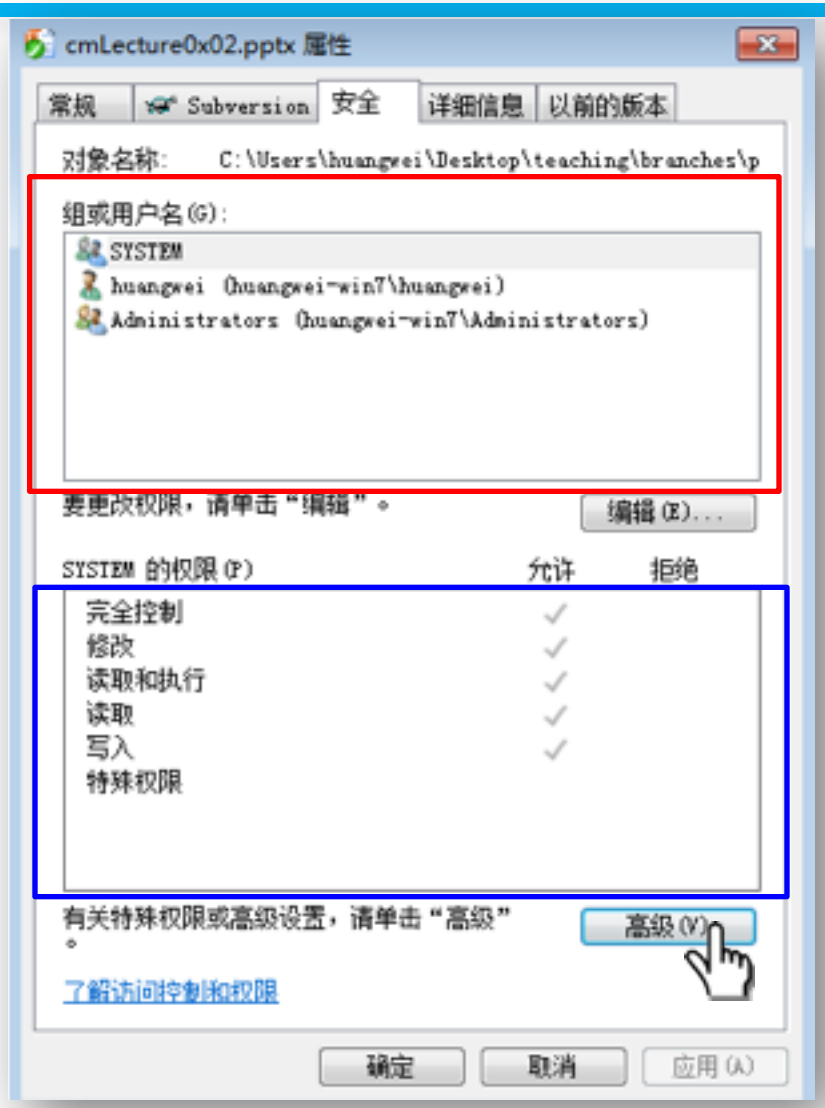
- 内涵
  - —主体对客体的访问行为会被记录，用于安全责任追查和认定
- 意义
  - —检测是否存在违反安全(访问控制)策略的行为
  - —重建安全事件
- 手段
  - —日志

从授权的角度看

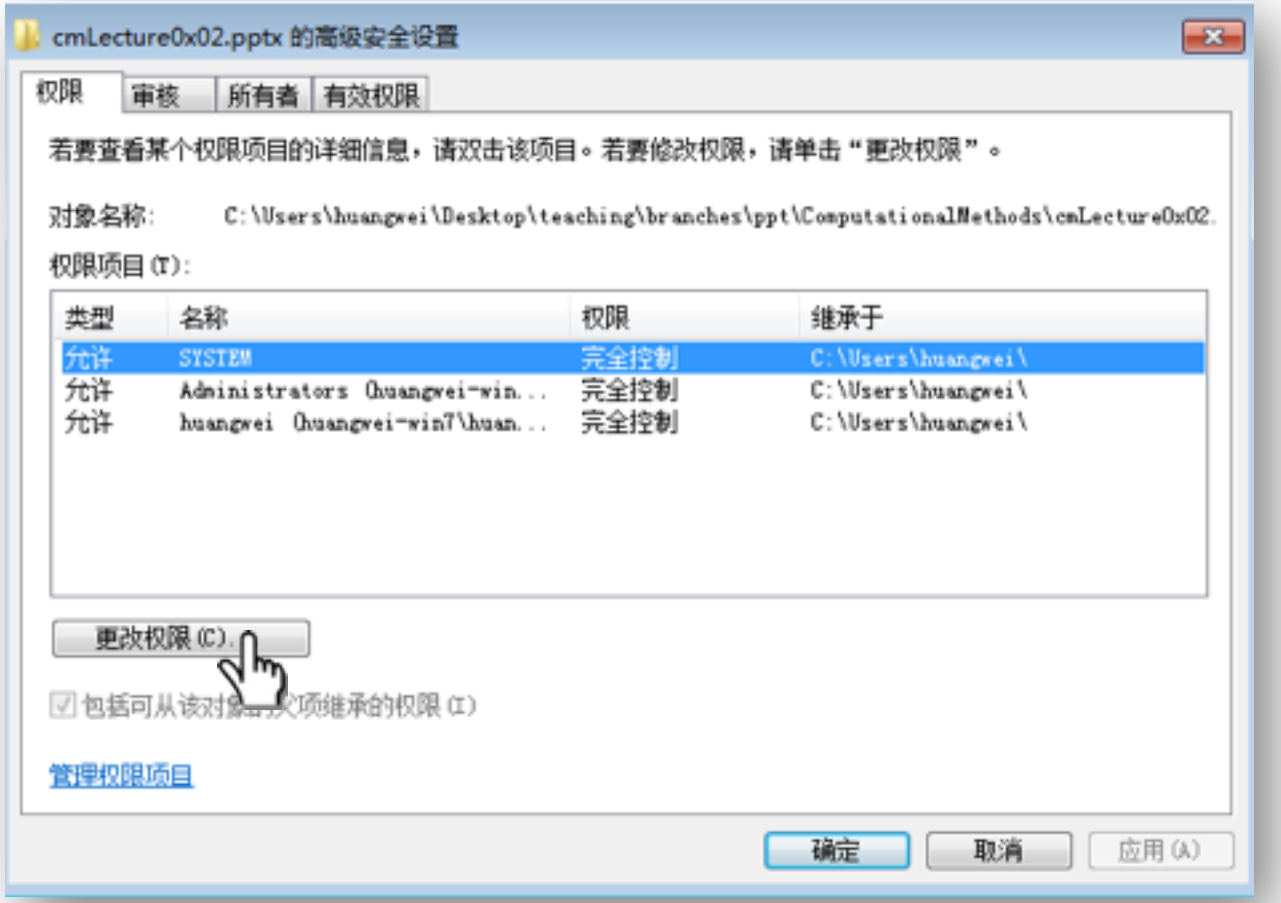
WINDOWS 7访问控制模型

有何特别之处？(1/3)

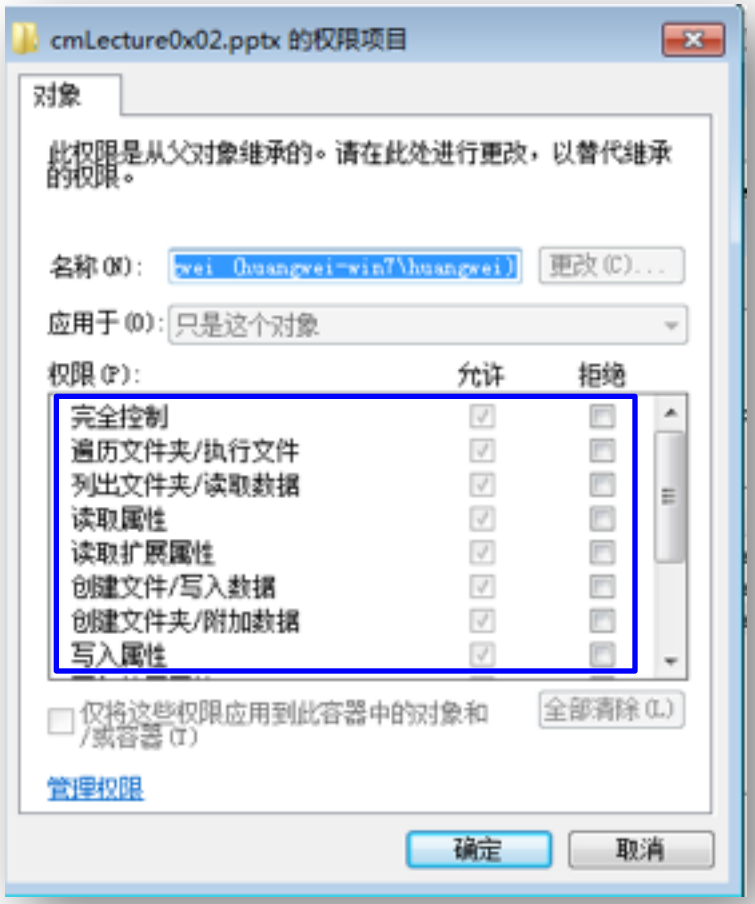
- 访问令牌
  —主体的数字标识
- 安全描述符
  —客体的数字标识

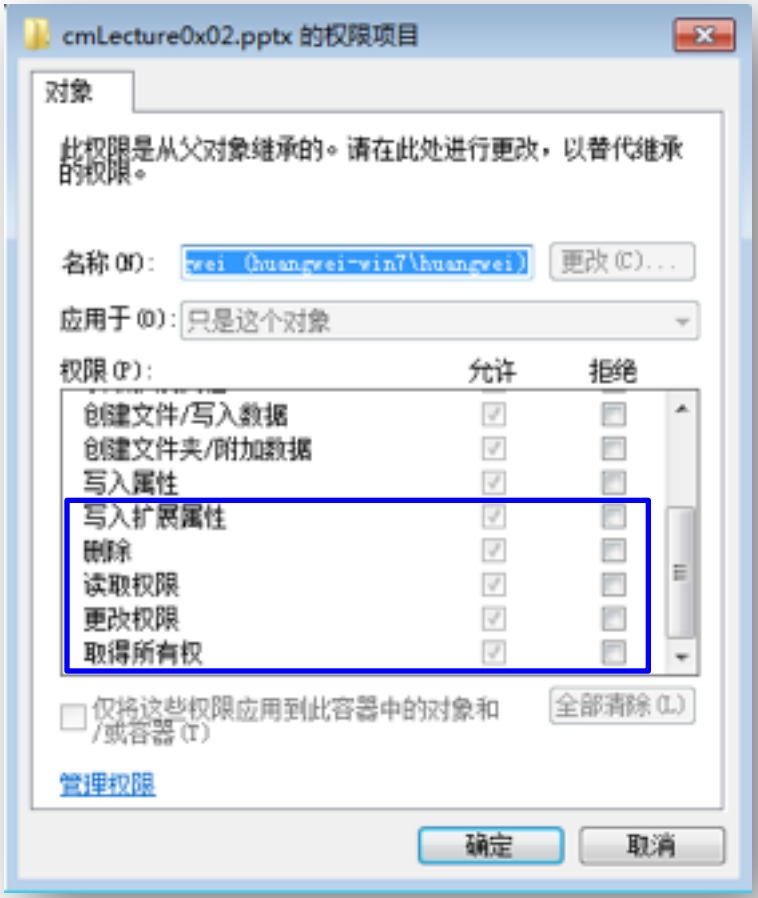


有何特别之处？(2/3)


cmLecture0x02.pptx 的高级安全设置
权限
审核
所有者
有效权限
若要查看某个权限项目的详细信息，请双击该项目。若要修改权限，请单击“更改权限”。
对象名称: C:\Users\huangwei\Desktop\teaching\branches\ppt\ComputationalMethods\cmLecture0x02.
权限项目(T):
类型 名称 权限 继承于
允许 SYSTEM 完全控制 C:\Users\huangwei\
允许 Administrators (huangwei-win... 完全控制 C:\Users\huangwei\
允许 huangwei (huangwei-win7\huan... 完全控制 C:\Users\huangwei\
更改权限(C)...
包括可从该对象的父项继承的权限(I)
管理权限项目
确定
取消
应用(A)

有何特别之处？(3/3)





权限定义划分更细致！！

访问令牌

- 访问令牌是与特定的Windows帐户关联的
- 访问令牌会与特定进程绑定

  —进程中的线程默认会继承该访问令牌
- 当线程访问某个对象时，Windows就会使用这个线程特有的令牌进行访问控制授权检查

安全描述符

- 安全描述符是与被访问对象关联的
  - —对象所有者(O:)
    - SID，唯一标识
  - —主要组(G:)，仅用于兼容POSIX程序
    - SID，不用于Windows程序，唯一标识
  - —访问控制列表
    - DACL (D:)： 自主访问控制列表
      包含0或多个ACE（访问控制项）
    - SACL (S:)： 系统访问控制列表
      定义系统审计规则

安全标识SID

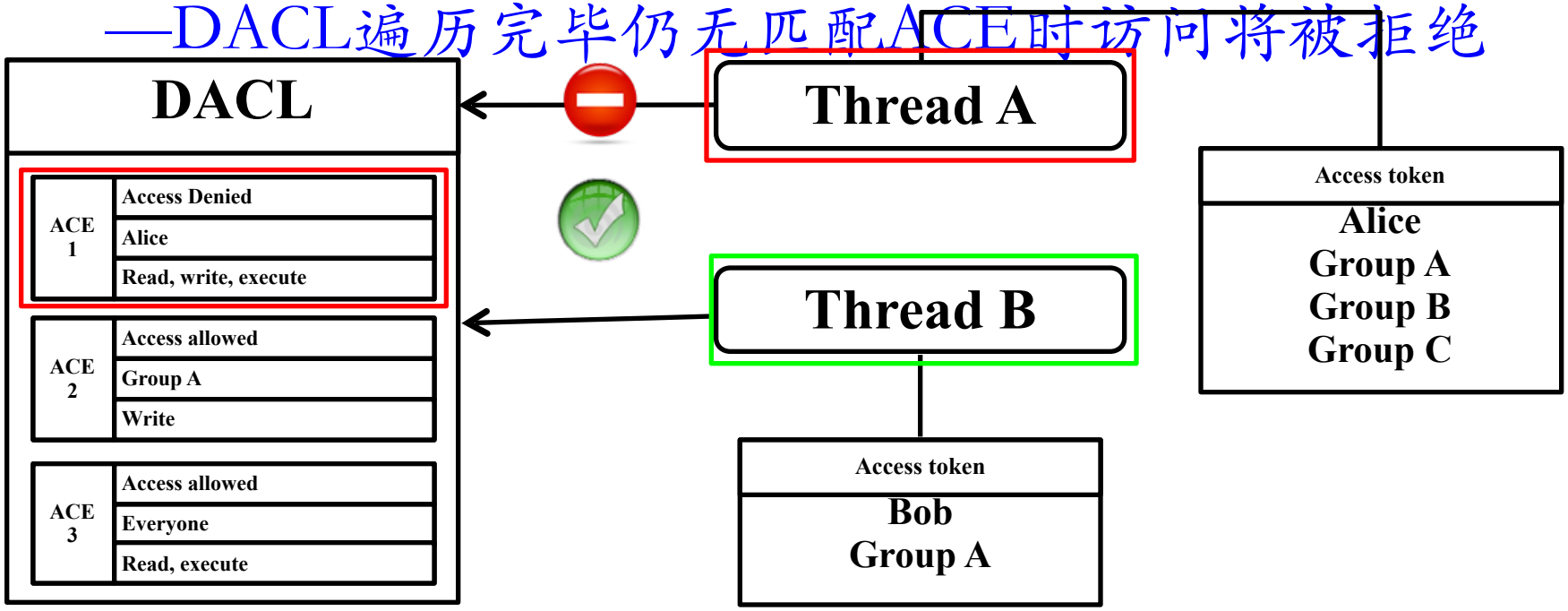
- Security Identity
- 每个SID在同一个系统中都是唯一的

```
C:\Users\huangwei>whoami /user

用户信息
----------------

用户名                 SID
====================== ============================================
huangwei-win7\huangwei S-1-5-21-1959901537-2963729105-2829771546-1000
```

- 线程访问对象时
  - —系统会顺序遍历检查DACL中的ACE
  - —匹配成功ACE即终止遍历并执行ACE标识策略
  - —DACL遍历完毕仍无匹配ACE时访问将被拒绝



本章内容提要

一.操作系统简史

二.数字标识理论

三.访问控制理论

四.风险评估理论与实践

内容提纲

- 为什么需要风险评估
- 如何量化评价一个漏洞的严重程度
- CVSS与漏洞评分
- 漏洞评分高低对实际网络安全的影响

参考文献

① M. Bishop, Computer Security: Art and Science. Addison-Wesley Professional, 2002.
   ① Chapter 2. Access Control Matrix
   ② Chapter 7. Hybrid Policies
   ③ Chapter 15. Access Control Mechanisms
   ④ Chapter 27. System Security

② 《Unix操作系统发展大事记》http://www.techcn.com.cn/index.php?doc-view-112413

③ 《Solaris 开发者安全性指南》 第3章 编写 PAM 应用程序和服务 http://download.oracle.com/docs/cd/E19253-01/819-7056/ch3pam-01/index.html

④ John R. Michener，理解 Windows 文件和注册表权限 http://msdn.microsoft.com/en-us/magazine/cc982153.aspx

⑤ Access Control Model http://msdn.microsoft.com/en-us/library/aa374862%28v=VS.85%29.aspx

参考文献

⑥ PAM configuration guide for Debian http://www.rjsystems.nl/en/2100-pam-debian.php

⑦ Windows的历史 http://windows.microsoft.com/zh-CN/windows/history

⑧ 开放漏洞与评估语言（OVAL）的基本架构 http://wiki.scap.org.cn/oval/architecture

⑨ CVSS Guide http://www.first.org/cvss/cvss-guide.html

⑩ CVSS在线计算器 http://nvd.nist.gov/cvss.cfm

课后思考题

- 生物特征身份认证方式有哪些？优缺点分析？应用场景举例
- “找回口令功能”和“忘记密码”在访问授权机制中的意义？请尝试设计一种安全的“找回口令功能”，详细描述找回口令的用户具体操作过程
- 绘制用户使用用户名/口令+图片验证码方式登录系统的流程图

  —考虑认证成功和失败两种场景

  —考虑授权成功和失败两种场景

课后思考题

- Windows XP / 7中的访问控制策略有哪些？访问控制机制有哪些？
- 用权限三角形模型来理解并描述以下2种威胁模型

  —提权

  —仿冒
- 试通过操作系统的访问控制机制来达到预防一种真实病毒的运行目的

课后思考题

- 什么是OAuth?
- 什么是OpenID?
- 试用本章所学理论分析0Auth和OpenID的区别与联系
- 如何使用0Auth和OpenID相关技术实现单点登录（Single Sign On）？