计算机系统安全

Chapter 7: 机密性策略

主要内容

- 7.1 什么是机密性模型
- 7.2 Bell-LaPadula模型
  - 7.2.1 BLP步骤1
  - 7.2.2 BLP步骤2
- 7.3 DG/UX System

7.1 机密性策略

- 目标: 防止非授权的泄漏信息
  - 处理信息流

    信息的动态变化过程中保护信息不被泄露

- 多级安全模型
  - 防止信息从高安全级流向低安全级
  - Bell-LaPadula 模型是很多模型的基础

主要内容

- 7.1 什么是机密性模型
- 7.2 Bell-LaPadula模型
  - 7.2.1 BLP 步骤1
    - 1）信息的安全级
    - 2）读信息
    - 3）写信息
    - 4）基本安全定律
  - 7.2.2 BLP 步骤2
- 7.3 DG/UX System

7.2.1 BLP模型, 步骤 1

1）信息的安全级

- 信息安全级别：线序
  - 绝密Top Secret: highest
  - 机密Secret
  - 秘密Confidential
  - 公开Unclassified: lowest

- 主体的安全许可 *L*(s)
- 客体的安全级 *L*(o)

7.2.1 BLP模型, 步骤 1

Example

security level	*subject*	*object*
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	Ulaley	Telephone Lists

- Tamara 可读哪些文件？
- Claire 可读哪些文件？
- Ulaley 可读哪些文件？

- Tamara 可读所有文件
- Claire 可读logs和lists
- Ulaley 可读lists

7.2.1 BLP模型, 步骤 1

2）读信息

范长龙

许其亮

中共中央
军委副主席

中共中央军委委员

常万全

房峰辉

张阳

赵克石

张又侠

吴胜利

马晓天

魏凤和

7.2.1 BLP模型, 步骤 1

2）读信息

- 信息向上流动, 非向下流动
  - “上读” 不允许, “下读” 允许
  - “禁止上读” 规则

- 简单的安全条件(Step 1)
  - 主体 s 可以读客体 o：iff $L(o) \leq L(s)$ 且s对o有读权限
    - 当且仅当 iff
    - 包含强制访问控制(安全级关系)和自主访问控制 (读权限)

7.2.1 BLP模型, 步骤 1

3）写信息

范长龙

许其亮

中共中央
军委副主席

中共中央军委委员

常万全

房峰辉

张阳

赵克石

张又侠

吴胜利

马晓天

魏凤和

7.2.1 BLP模型, 步骤 1

3）写信息

- 信息向上流动, 不向下流动
  - 允许“向上写”, 不允许“向下写”
  - “禁止下写” 规则

- *-属性 (Step 1)
  - 主体可以写客体 *o*， iff $L(s) \leq L(o)$ 且主体s 对 *o*有写权限
    - 包含强制访问控制 (安全级) 和自主访问控制 (写权限)

7.2.1 BLP模型, 步骤 1

4）基本安全定理(步骤1)

- 如果一个系统初始于一个安全状态;

  系统的每次转换,都满足步骤1的基本安全条件, 和*-属性;

  那么系统的每个状态都是安全的

Chapter 7: 机密性策略

- 7.1 什么是机密性模型
- 7.2 Bell-LaPadula模型
  - 7.2.1 BLP 步骤1
  - 7.2.2 BLP 步骤2
- 7.3 DG/UX System

7.2.2 BLP模型, 步骤2

- 安全级的概念扩展，对客体分类
- 安全级(*级别, 分类*)

- 例
  - (Top Secret, { NUC, EUR, ASI })
  - (Confidential, { EUR, ASI })
  - (Secret, { NUC, ASI })

7.2.2 BLP模型, 步骤2

1）格序

- A是安全级,C是安全分类
- (A, C) *dom* (A', C') iff $A' \leq A$ 和 $C' \subseteq C$

  dom: 控制

- 安全级集合 $L = A \times C$, *dom* 形成格序
  - *最小上界*$lub(L) = (max(A), C)$
  - *最大下界*$glb(L) = (min(A), \varnothing)$

7.2.2 BLP模型, 步骤2

1）格序

- 例

  (Top Secret, {NUC, ASI}) *dom* (Secret, {NUC})

  (Secret, {NUC, EUR}) *dom* (Confidential,{NUC, EUR})

  (Top Secret, {NUC}) ¬*dom* (Confidential, {EUR})

7.2.2 BLP模型, 步骤2

级别、排序

- 步骤2中：安全级L是偏序关系
  并非所有安全级之间可以进行比较

- 步骤1中 “dom” 含义是 “greater than”
  “greater than” 是全序

7.2.2 BLP模型, 步骤2

2）读信息

- 信息向上流动, 不能向下流动
  - “读高于本级信息”不允许, “读低于本级信息”允许

- 简单安全条件 (Step 2)
  - 主体 s 可以读客体 *o*：iff *L*(s) *dom L*(*o*) 且 s 对 *o* 有读权限
    - 包含强制访问控制和自主访问控制

7.2.2 BLP模型, 步骤2

3）写信息

- 信息向上流动,不向下流动
  - “上写” 允许, “下写” 不允许

- *-Property (Step 2)
  - 主体s能写客体o，iff $L(o)$ *dom* $L(s)$ 且s对o有写权限
    - 包含强制访问控制和自主访问控制

7.2.2 BLP模型, 步骤2

4）基本安全定理（步骤2）

- 1）如果一个系统初始于一个安全状态;
  2）系统的每次转换,都满足步骤2的基本安全条件, 和*-属性;
  3）那么系统的每个状态都是安全的

  - 证明: 对转换过程做归纳
  - 基本安全定理：包括简单安全条件、*_属性和自主访问控制

7.2.2 BLP模型, 步骤2

5）问题

- Colonel的安全标签 (Secret, {NUC, EUR})
- Major的安全标签 (Secret, {EUR}) clearance

Colonel如何给Major下达指令信息？

Clearly absurd!

7.2.2 BLP模型, 步骤2

6）解决上级向下写问题

- 对主体，定义最大级别, 当前级别
  - *maxlevel*(s) *dom curlevel*(s)

- 例
  - Major 是客体 (Colonel 要写入信息)
  - Colonel 的 *maxlevel* (Secret, { NUC, EUR })
  - Colonel 的 *curlevel* to (Secret, { EUR })

  - *L*(Major) *dom curlevel*(Colonel)
    - Colonel 可以向 Major 写信息

主要内容

- 7.1 什么是机密性模型
- 7.2 Bell-LaPadula模型
  - 7.2.1 BLP 步骤1
  - 7.2.2 BLP 步骤2
- 7.3 DG/UX System

7.3 DG/UX System

- 提供强制访问控制
  - MAC 标签指明安全级
  - 有缺省标签, 也可定义标签

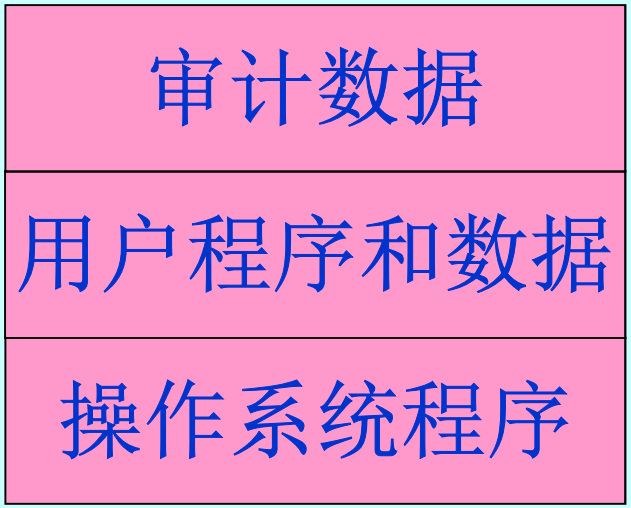
- 初始
  - 主体的标签：指定为用户, 保存在授权与鉴别数据库中

  - 客体在创建时建立标签
    - 显式标签，是属性的一部分
    - 隐式标签，从父目录获得

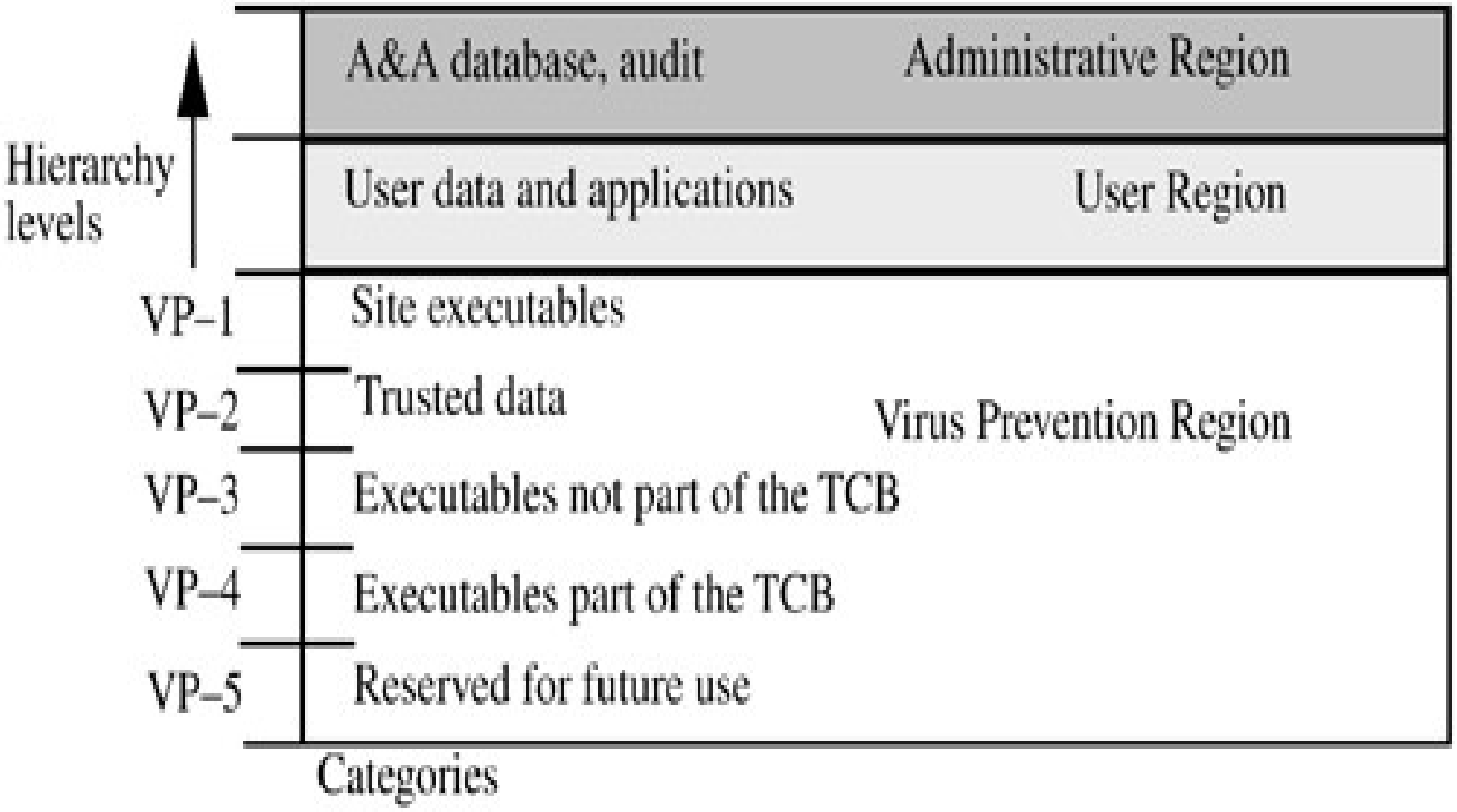
7.3 DG/UX System

操作系统程序 | 用户程序和数据 | 审计数据

如何定义安全级？



7.3 DG/UX System



7.3 DG/UX System

1）目录的标签问题

- 进程 *p* (MAC_A标签) 想创建文件*/tmp/x*
  /tmp/x 已经存在，MAC标签为MAC_B
  并且 MAC_B dom MAC_A

创建失败

●补救措施：

在某目录中，仅相同MAC标签的程序可在该目录中创建文件

现在编译器不能工作，不能传输邮件

7.3 DG/UX System

2）多级目录

- 目录下有子目录, 每个子目录一个标签
  - 子目录对用户透明，用户不可见子目录
  - p 创建 */tmp/x*，*其实创建的是/tmp/d/x* ， *d* is 是MAC_A标签对应的目录
  - 所有 *p*指向*/tmp*的参考文件均改为指向*/tmp/d*

7.3 DG/UX System

2）多级目录

- *进程 p* 运行：cd */tmp/a*, cd ..
  - 系统调用stat(“.”, &buf) 返回真正目录的inode号
  - 在DG/UX系统中，系统调用 dg_stat(“.”, &buf) 返回*/tmp*的inode

7.3 DG/UX System

3）加载没有标签的文件系统

要求: 文件系统客体（文件）必须有MAC标签

1）文件系统的根有显式的MAC标签

2）如果mount到一个无标签的文件系统, 其标签为mount点的标签，隐式继承其父亲的MAC标签

3）创建客体的硬链接，客体必须有显示标签；如果没有显示标签，把隐式标签转为显示标签

4）如果目录的标签要改变，子目录的隐式标签转为显示标签

5）系统解析符号链接时，客体标签就是符号链接目标的标签

7.3 DG/UX System

3）客体标签

- 问题: 客体有2个名字
  - */x/y/z, /a/b/c* 指向同一个客体
  - *y* 有显式标签 IMPL_HI
  - *b* 有隐式标签 IMPL_B

- 情况1: 硬连接
- 创建硬连接需要有显式标签
  - 如果标签为隐式, 需将标签改为显式

含义：移动文件时需将标签改为显式

7.3 DG/UX System

3）客体标签

- 情况2: 当mount到文件系统时，硬连接存在
  - 该路径上的所有客体标签均为隐式: 路径下的隐式标签都相同
  - 改变目录标签时，在改变前需将儿子的标签改为显式

7.3 DG/UX System

3）客体标签

- 符号连接是文件, 规则同文件的规则
- 当解析符号连接时, 符号连接的标签为其指向文件的标签
  - 系统需要访问符号连接本身的标签

7.3 DG/UX System

4）MAC标签的使用

- 执行简单的安全条件(读)
- 不完全执行*-属性(写)
  - 进程的MAC必须等于客体的MAC
  - 仅在同安全级下可写
- 实际使用中进行完全限制

7.3 DG/UX System

5) MAC 元组

- 客体级别:采用MAC范围表示

- MAC范围是指具有上界和下界的标签(label)
  - 必须满足：上界 dom 下界

  - Examples

[(Secret,{NUC}), (Top Secret,{NUC})]

[(Secret,∅), (Top Secret,{NUC,EUR, ASI})]

[(Confidential,{ASI}), (Secret,{NUC,ASI})]

7.3 DG/UX System

6) 客体 和 元组

- 客体必须有MAC标签
  - 可以是MAC元组，也可以是安全标签
  - 二者都有, 元组级别高于label

- Example
  - Paper has MAC range:
    [(Secret,{EUR}),(Top Secret,{NUC,EUR})]

7.3 DG/UX System

6) 客体 和 元组

- 进程可以读客体，需满足下面条件:
  - 客体的MAC范围(*lr*, *hr*); 进程的MAC标签*pl*
  - *pl dom hr* ，对客体有读权限

- Example,假定主体对客体有读权限

  Peter主体标签(Secret,{EUR})

  paper文件标签(Top Secret,{NUC,EUR})

  Peter不能读paper文件

  - Paul标签(Top Secret,{NUC, EUR, ASI})

    paper (Top Secret, {NUC, EUR})

    Paul可读paper

7.3 DG/UX System

6) 客体 和 元组

- 进程可以写客体，需满足:
  - 客体MAC范围(*lr*,*hr*); 进程MAC级别*pl*
  - 进程对客体有写权限
  - $pl \in (lr, hr)$

- Example，假定主体对客体有写权限
  - Peter级别(Secret, {EUR})

    paper MAC范围(Top Secret, {NUC, EUR})

    Peter可写paper
  - Paul (Top Secret, {NUC, EUR, ASI})

    paper级别(Top Secret, {NUC, EUR})

    Paul不可写paper

关键点

- 机密性模型限制信息的流动
- Bell-LaPadula模型为多级安全模型
  - 是计算机安全的基石

作业

* 1: Why is it meaningless to have compartments at the UNCLASSIFIED level (such as (UNCLASSIFIED, { NUC }) and (UNCLASSIFIED, { EUR }))?
* 2: Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

  1) Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).

  2) Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).

  3) Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).

  4) Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).

  5) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

作业

* 3: Prove that any file in the DG/UX system with a link count greater than 1 must have an explicit MAC label.
* 4: In the DG/UX system, why is the virus prevention region below the user region?
* 5: In the DG/UX system, why is the administrative region above the user region?

* 下一章：完整性策略
* Reading

  Introduction to Computer Security

  Chapter 6. Integrity Policies