自由访问控制的安全性:研究综述*)

余 杰[1] 李舟军[2] 陈火旺[1]

(国防科技大学计算机学院 长沙 410073)[1] (北京航空航天大学计算机学院 北京 100083)[2]

摘 要 自由访问控制(DAC)是大多数操作系统保护机制的核心,DAC 的安全性研究关注对象的权限是否被泄漏给未授权主体。本文介绍了 DAC 安全性研究的相关工作,重点讨论了三种典型的 DAC 模式及其安全性分析。现有的模型在 DAC 定义上还存在争论,同时对安全性的分析也存在不足。研究满足 DAC 定义且安全性可判定的访问控制系统,是一个重要的研究方向。

关键词 自由访问控制,安全性,重标记,格局

Research on Safety of Discretionary Access Control

YU Jie[1] LI Zhou-Jun[2] CHEN Huo-Wang[1]

(College of Computer, National University of Defense Technology, Changsha 410073)[1]

(College of Computer, Beihang University, Beijing 100083)[2]

Abstract Discretionary access control (DAC) is the kernel of most protection mechanism, and the research on safety of DAC concerns whether rights can be leaked to unauthorized subjects. In this paper, we introduce the related work of the research on safety of DAC, and emphasize three typical DAC schemes and the safety analysis of them. Existing schemes is ambiguous on the definition of DAC, and has some shortage on the safety analysis. It is an important research direction that giving an access control system which satisfies the definition of DAC and the safety of which is decidable.

Keywords Discretionary access control, Safety, Relabel, Configuration

1 引言

访问控制技术是系统安全研究的重要组成部分,其早期研究主要用于集中式系统,尤其是操作系统的安全保护。访问控制机制可以限制对关键资源的访问,防止非法用户进入系统及合法用户对系统资源的非法使用。随着 Internet 的发展,大量分布式系统出现,访问控制的研究重点转向分布式系统安全。

目前主流的访问控制策略有三种[1]:自由访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC)。自由访问控制策略允许系统用户自由决定授予或撤消其他系统主体对其所属某个对象的访问权限;强制访问控制策略,从全局的角度对系统内保护对象进行访问控制,对象访问权限的决策依据对象的分类和用户的分类来完成,最典型的例子是由 Bell 和 LaPadula 提出的 BLP 模型;基于角色的访问控制策略,引入了角色的概念,在用户和访问权限之间建立一个中间层,它主要应用在分布式系统[12]。

安全性分析(Safety Analysis)主要关注权限(rights)是否会被泄漏给未授权的主体。MAC 严格地限定系统用户对系统对象的访问,其安全性分析比较容易,因此,关于访问控制的安全性研究主要集中 DAC 上。DAC 的优点是其自主性为用户提供了极大的灵活性,从而使之适合于许多系统和应用。但也正由于这种自主性,在 DAC 中,信息总是可以从一个实体流向另一个实体,即使对于高度机密的信息也是如此,因此如果自主访问控制不加以控制就会产生严重的安全隐患。例如,用户 S_1 可以将其对实体 O 的访问权限传递给用户 S_2,从而使不具备对 O 访问权限的 S_2 也可以访问 O,这样的结果是易于产生安全漏洞,因此自主访问控制的安全级别较低。

访问控制模型中的安全性分析由 Harrison 等在 1976 年首先提出,之后大量的研究致力于提出一种可判定安全性的访问控制模式,如文[3~16,18]。由近期在 IEEE 安全和私密会议(Proceedings of IEEE Symposium on Research in Security and Privacy)上发表的文[15,20]可以看出,DAC 的安全性研究又重新被重视起来。当前,典型的安全性研究主要针对 HRU[3]模式、SS[15]模式和 GD[2,20]模式三种。本文第 2 部分会重点介绍这三种模式及其安全性研究。

在介绍 DAC 的安全性研究现状之前,要先阐述一下访问控制矩阵。访问控制矩阵是访问权限表示的关键,访问表、能力表等都是它的简化变形。访问控制矩阵的行表示主体,列表示对象。主体指一个活动的实体 S_i,可以是一个处理过程、用户或机器。对象指一个被主体访问的受保护的实体 O_i,主体也可以看作被其他主体访问的对象。每个对象都有一个称之为名(name)的唯一标识。主体所拥有的对对象的访问权限可以通过分属该主体和该对象的行和列的相交点元素来表示。

2 研究现状

Harrison 等首先提出了 HRU 模式并证明了其一般意义下的安全性是不可判定的[3],之后,大量的研究关注于 DAC

*)本文受到国家科学基金项目(60473057,60573057,90604007)的资助。余 杰 硕士研究生,研究方向为分布式信任管理;李舟军 博士,博士生导师,主要研究方向为高可信软件理论与技术,安全协议验证与网格安全,数据控制与生物信息学;陈火旺 院士,博士生导师,主要研究方向为软件理论与软件工程。

的安全性研究。Sandhu 等人提出了一种示意性的保护模型，并证明了如果包含循环创建(cyclic creates)则其安全性是不可判定的[4~8]。Bertino 等人引入时态逻辑，提出了支持周期约束和瞬时推理的新的 DAC 模型，但其并未论证该模型的安全性是否可判定[11,12]。文[11,12,14]也对 DAC 中的安全性进行了讨论。Solworth 和 Sloan 提出了一种基于标记和重标记的分层 DAC 模型，并论述了安全性是可判定的[15]。Li 等人重新定义了 DAC 及其安全性，并证明了 GD 模型的安全性是可判定的[20]。本节将介绍三种典型的 DAC 模式及其安全性分析，关于其不足将在第 3 部分讨论。

2.1 HRU(Harrison, Ruzzo and Ullman) 模式

定义 1.1(HRU 模式[3]) 一个保护系统(Protection System, PS)由有穷权限集合 R 和有穷命令(command)集合 C 组成。

其中权限包括：own, read, write, execute 等。命令由条件和原子操作组成，如图 1 所示，其中 $m\geqslant 0, n>0$。原子操作(op)包括：enter r into (X_s, X_o), delete r from (X_s, X_o), create subject X_s, create object X_o, destroy subject X_s, destroy object X_o。

```
command α(X1, X2, ...Xk)
 if
      r1  in (Xs1,Xo1)     and
      r2  in (Xs2,,Xo2)    and
          ...
      rm  in (Xsm ,Xom)
 then
      op1
      op2
      ...
      opn
 end
```

图 1 HRU 的命令格式

定义 1.2(格局 configuration) 一个保护系统 PS 的格局定义为一个三元组(S, O, P)，其中 S 指当前主体集合，O 指当前对象集合(S 是 O 的子集)，P 是当前的访问控制矩阵。

定义 1.3(格局的迁移)

1) $Q_1 \vdash_\alpha Q_2$ 当且仅当 Q_1 逐个经过 α 中的所有操作之后到达 Q_2

2) $Q_1 \vdash Q_2$ 当且仅当 存在命令 α 使得 $Q_1 \vdash_\alpha Q_2$

3) $Q_1 \vdash^* Q_2$ 其中 $\vdash^*$ 是 $\vdash$ 的自反传递闭包，即 0 步或多步使用 $\vdash$

定义 1.4(权限泄漏) 命令 α 从格局 $Q=(S, O, P)$ 泄漏权限 r 是指：从格局 Q 执行时，能够通过命令 α 中某条原子操作的执行向访问控制矩阵原来不含有权限 r 的单元中插入 r。

定义 1.5(安全性) 初始配置 Q_0 对权限 r 不安全是指：存在一个格局 Q 和一条命令 α，使得

1) $Q_0 \vdash^* Q$ 并且

2) α 从格局 Q 泄漏权限 r

定义 1.6(单操作 mono-operational 保护系统) 一个保护系统称为单操作的是指：它的每条命令都只包含一个原子操作。

Harrison 等人提出并证明了如下结论：

定理 1.1 存在一个算法可判定：一个特定的单操作保护系统在特定的初始配置 $Q_0=(S_0, O_0, P_0)$ 下对特定的权限 r 是否安全。

单操作系统有两个简单的性质：1)在导致权限泄漏的计算路径上，可以删除 delete 和 destroy 命令；2)重复的 create 命令可以被删除。要证明定理 1.1，可先证明单操作保护系统的任何计算序列在利用上述两性质化简后的长度都不会超过 $g(|S_0|+1)(|O_0|+1)+1$，其中 g 是系统的权限数量；然后，再通过动态调度算法进行优化后，就能在初始访问矩阵的多项式时间内判定出该系统对权限 r 是否安全。

定理 1.2 一个特定保护系统 PS 在特定的初始配置下对特定的权限 r 是否安全是不可判定的。

由图灵机理论[21]，任意的图灵机 T 是否最终会到达终止状态是不可判定的。证明定理 2 的核心技巧就是将保护系统 PS 模拟为图灵机 $T_mM=\langle K, \Sigma, Z, \delta, q_0, B, F\rangle$，其中，PS 的权限泄漏表示为到达终止状态，PS 的权限集 R 表示为状态集 K 和字母表 Z，用 PS 的命令来模拟动作函数 δ。

定理 1.3 没有 create 命令的保护系统的安全性问题可以在多项式时间内判定。

2.2 SS(Solworth and Sloan) 模式

Solworth 等人提出了基于标记和重标记(labels and relabelling)的 SS 模式[15]。SS 模型认为，访问控制设计可以分为三层结构：第一层是通用访问控制模型，该层可以是一般意义下的程序语言，也可以是更严格的模型；第二层是第一层的参数化，通过参数化实现一个访问控制模型；第三层通过初始化主体和对象让系统能够正确运转。由于较低层包含较高层，所以如果低层模型满足安全性，则高层一定是安全的。

SS 模型的主要思路是：先给对象加标记，再将拥有标记的对象的访问权限授予某些组(group)，最后通过判断某个主体是否属于这些组来判断其是否具有对某对象的特定访问权限，如下所示。

$$Objects \xrightarrow{label} objects\ labels \xrightarrow{auth} groups \xrightarrow{members} subjects$$

标记(label)用来定义各个主体在对象上操作的权限，每个对象都有一个标记。有两个不相交的标记集合：组标记(Group Labels)和普通对象标记(Ordinary Object Labels)。每个标记都被映射到三个组：读其标记对象的组、写其标记对象的组和执行其标记对象的组。

重标记规则(relabel rules)用来重置权限。用 $rl_n(t, t')$ 来表示非组之间的重标记规则，用 $rl_g(t, t')$ 来表示组之间的重标记规则。如规则 $rl_n(\langle *u, *\rangle, \langle *u, *\rangle)=g$ 表示允许组 g 的任何成员重标记同一个主体之间的标记。

Solworth 等人证明了以下结论：

引理 2.1 从一个特定的格局出发，已存在的主体 U_0 是否能够成为组 g 的成员是可判定的。

该引理是后面证明模型安全性的关键。

引理 2.2 存在一个算法，不仅能够判定从一个特定的配置出发，已存在的主体 U_0 是否能够成为组 g 的成员，还能给出一组已存在的用户集合，要使 U_0 成为 g 的成员，则其中必须有一个主体集合的所有主体都要执行重标记操作。

定理 2.3 存在一个算法，不仅能够判定从一个特定的配置出发，主体 U_0 是否能够获得对象 o 的权限 r，还能给出一组已存在的用户集合，要使 U_0 获得对象 o 的权限 r，则其中必须有一个主体集合的所有主体都要执行对组标记(group labels)的重标记操作。

2.3 GD(Graham and Denning)模式

Li等人重新定义了DAC及其安全性[20]，其定义如下：

定义3.1(访问控制模型) 一个访问控制模型由四元组组成$\langle \Gamma, \Psi, Q, \vdash \rangle$，其中$\Gamma$是状态集合，$\Psi$是状态迁移规则集合，$Q$是查询集合，$\vdash: \Gamma \times Q \rightarrow \{true, false\}$用来定义一个命题逻辑公式在某个状态是否为真。

定义3.2(访问控制系统) 一个基于某个模式的访问控制系统是用如下四元组表示的状态迁移系统$\langle \gamma, \psi, Q, \vdash \rangle$，其中$\gamma \in \Gamma$是指起始状态或当前状态，$\psi \in \Psi$描述状态迁移规则。

定义3.3(Security Analysis) 四元组$\langle \gamma, \psi, T, \Box\phi \rangle$，其中$\phi$是原子命题公式，$T$表示可信任集合，$\Box$是时序逻辑算子[21]，表示从当前时刻以后。上述四元组为真，当且仅当对所有γ'，若满足$\gamma \vdash_{\psi}^{*} \gamma'$，则$\gamma' \vdash \phi$，即在$T$中的用户不首先发起状态迁移时，在$\psi$下从$\gamma$可达的所有状态都满足安全不变式$\phi$(Security invariant)。

定义3.4(Safety Analysis) 四元组$\langle \gamma, \psi, T, \Box \rightarrow \text{hasRight}(s, o, r) \rangle$，其中hasRight$(s, o, r)$为真当且仅当在当前状态，主体$s$和对象$o$存在，$r$是系统中的一个权限，并且$s$拥有对$o$的权限$r$。访问控制系统是安全的，当且仅当在$\psi$下从$\gamma$可达的所有状态中，hasRight都为假。

Li等人根据其定义的模式描述方法，将GD模式描述如下：

1. 存在一个区别于一般主体的全局主体u。

2. 权限集$R=\{own, control\}+R_b+R_b^*$。

3. 状态集Γ，GD模式中状态γ用当前状态的主体集、对象集和访问控制矩阵表示。每个状态必须满足以下约束：每个对象至少属于(own)一个主体；只有主体之间有控制(control)关系；u存在于每个状态，且不属于任何主体，不被任何其它主体控制；除u以外的任何主体仅仅属于一个其它主体；每个主体都能够控制自己；除u以外的任何主体最多被一个其它主体控制；主体之间的拥有(own)关系不存在环。

4. 状态迁移规则Ψ，GD模式的状态迁移命令如下，其中第一个参数i是发起本次命令执行的主体：transfer r(i, s, o)；transfer r*(i, s, o)；transfer own(i, s, o)；grant r(i, s, o)；grant r*(i, s, o)；grant control(i, s, o)；grant own(i, s, o)；delete r(i, s, o)；delete r*(i, s, o)；create object(i, o)；destroy object(i, o)；create subject(i, s)；destroy subject(i, s)。

Li等人提出了一个算法isSafeGD(γ, ψ, w, T)用来判定GD模式下一个访问控制系统的安全性，并得出如下结论：基于GD模式的系统的安全性是可判定的，并且isSafeGD最坏可以在$O((|S_\gamma| * |R_\psi|)^3)$内判断出给定系统是否安全。

3 不足及展望

在1976年Harrison等提出访问控制模型中的安全性分析之后，DAC的安全性研究从未中断过，并由此产生了很多访问控制模型[3~16,18]，但还存在如下问题：

(1)关于DAC的定义

文[22]指出，DAC的核心是：一个独立的用户或用户操作的程序可以明确指定其它用户或其运行的程序拥有的对信息的访问权限。某些文献将DAC等价于HRU模型[10,14]，某些文献将其等价于GD模型[20]，而Solworth等人则声称SS模型可以实现DAC的全部功能[15]。对DAC定义的理解，决定了对其安全性分析的结果。

(2)安全性分析

现有的安全模型都存在各自的问题，HRU模型本身不能保证其任意情况下的安全性；Li等人指出SS模型存在缺少对移出对象和主体的支持、不能确保一个对象仅有一个拥有者等不足；而GD模型中，control属性仅用于删除被控对象的某些属性，而且其一旦被赋予给某个主体，则无法更改。

由于管理比较容易，以前访问控制的研究和应用主要集中在MAC，如今，分布式应用的迅速发展，对DAC的需求逐渐变大。当前许多基于DAC的访问控制系统由于安全性的原因，都作了一些限制。研究可判定安全性的DAC系统，正成为一个热门的研究方向。对DAC安全性的研究，首先要弄清DAC的定义，然后再分析其安全性，保证任意实体对任意对象的访问权限都是可判定的。

结束语 自由访问控制是大多数操作系统保护机制的核心，它允许对象拥有者自由决定将对该对象的什么访问权限赋给谁，从而为获得保护决策提供了很大的灵活性。本文概述了DAC安全性研究的相关工作，并重点介绍了至今为止三种典型的DAC模式及其安全性分析。

DAC的安全性研究近来又重新成为令人关注的话题，现有的模型和分析还存在一些不足，如何改进这些问题，研究满足DAC定义且安全性可判定的访问控制系统，是一个重要的研究方向。

参考文献

1 徐锋，吕建. Web安全中的信任管理研究与进展. 软件学报，2002，13(11)：2057~2064

2 Graham G S, Denning PJ. Protection - principles and practice. In: Proceedings of the AFIPS Spring Joint Computer Conference, AFIPS Press, May 1972, 40: 417~429

3 Harrison M A, Ruzzo W L, Ullman J D. Protection in operating systems. Communications of the ACM, 1976, 19(8): 461~471

4 Sandhu R S. The schematic protection model: Its definition and analysis for acyclic attenuating systems. Journal of the ACM, 1988, 35(2): 404~432

5 Ammann P, Sandhu R S. Safety analysis for the extended schematic protection model. In: Proceedings of the 1991 IEEE Symposium on Security and Privacy, 1991. 87~97

6 Sandhu R S. Expressive power of the schematic protection model. Journal of Computer Security, 1992, 1(1): 59~98

7 Sandhu R S. The typed access matrix model. In: Proceedings of the 1992 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, May 1992. 122~136

8 Sandhu R S. Undecidability of the safety problem for the schematic protection model with cyclic creates. Journal of Computer and System Sciences, 1992, 44(1): 141~159

9 Bertino E, Bettini C, Samarati P. A temporal authorization model. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM Press, 1994. 126~135

10 Bertino E, Bettini C, Ferrari E, Samarati P. An access control model supporting periodicity constraints and temporal reasoning. ACM Transactions on Database Systems, 1998, 23(3): 231~285

11 Motwani R, Panigrahy R, Saraswat V A, Ventkatasubramanian S. On the decidability of accessibility problems (extended abstract). In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, ACM Press, May 2000. 306~315

(下转第288页)

险;根据建立的规程来设计与交付服务。服务提供商支持该能力的手段有:分享与使用先前合约中获得的知识,客观地度量和回报员工表现,以及监控技术基础架构。

在3级,服务商已经建立系统来形成和管理客户关系,持续地致力于服务交付的改进。这些改进,往往是产生于明确的度量和验证活动。3级服务提供商展现出关于组织目标的可度量的改进。组织学习跨合约地改进了关于组织目标的绩效。

3级能力级别包含26个实践,能力级别为3级的服务提供商已经有效地实施了所有2级和3级的实践。

4级:*主动增加价值*

能力级别处于4级的服务提供商,能够不断创新,在向客户和其他利益攸关者提供的服务中,增加巨大的统计价值和实际价值。在4级,服务提供商能够为客户和未来客户定制其方法和服务,理解客户的感受,并基于先前的经验预测其绩效。服务提供商支持该能力的手段有:系统地评价和融合技术进展;从当前比较分析的角度,以及内外部标杆的角度,设置绩效目标。

4级服务商系统地规划、实施和控制其改进,往往根据自己的绩效标杆生成这些计划。4级能力级别包含10个实践,能力级别为4级的服务提供商已经有效地实施了所有2级、3级和4级的实践。

5级:持续卓越

能力级别处于5级的服务提供商,通过对所有2、3、4级实践至少2年的2次或多次连续认证评估,表现出可度量的、持续的和一致的卓越绩效和改进。

5级能力级别不包含任何新的实践,外包商无需其它实践就可以达到5级。在动态多变的环境下,有效持续地实施所有eSCM-SP实践,就表现出全组织持续卓越的能力。

4 IT外包服务商能力改进与度量

eSCM-SP是一个"最佳实践"能力模型,它指导服务商改进其在外包生命周期中的能力,并提供给客户一种客观评价服务商能力的方法。度量是有效地的服务管理、业务流程外包(BPO)和组织改进的基础。首先,度量对于定义与跟踪服务水平是必要的,它是建立客户一供应商协议的客观标准。第二,识别组织的绩效趋势也依赖于度量和分析,它能够实现超前管理。第三,度量还支持有效的资源分配。第四,持续的流程改进基于可度量的改进得以最佳地实例化,这来自对改进机会的识别和从改进中获得的价值。第五,基于有效数据的行业研究还为以下活动提供依据:精明地选择和监控供应商,建立服务级别协议,以及进行风险管理。

在eSCM-SP所有三个维度中度量都很重要:外包生命周期,能力域和能力级别。处于1级的组织有望具备业务目标集为合约设定环境,虽然它们可能不是平衡的、综合的目标集。处于2级的组织应该能够度量成本/效益,状态/进展,非一致性,以及绩效/满意度,趋于实现将客户需求适当联系于业务目标的合约目标。处于3级的组织应该能够度量绩效和趋势以实现组织目标,它以平衡的和综合的方式集成了业务目标、客户需求和改进目标。处于4级和5级的组织应该能够预测并可度量地改进流程能力。

eSCM-SP中的能力级别提供了一些稳定水平的集合,它们表现为能力改进,却在实现某个级别时经历数次反复。组织可能使用图2中的通用路线图来为合约或组织建立度量能力。在所有能力级别上,度量都应由组织的业务目标所驱动,并所收集的数据应支持理解、控制或改进。用于度量eSCM-SP中实践的通用路线图为:识别目标,确保绩效跟踪的措施,收集绩效的数据,定期根据目标评审绩效,确保当绩效趋势偏离于目标实现时所要采取的纠正性措施,采取纠正性措施,以及根据目标计划跟踪状态/进展。

小结 目前,IT外包在国内的发展可谓方兴未艾,尤其是逐渐形成了一些比较有实力的外包商。随着国外竞争者的涌入,如何提高自身服务能力成为许多IT外包服务商最为关注的话题之一。本文在分析IT外包的发展现状、理论渊源的基础上,介绍了专门针对IT外包服务商开发的能力改进与度量模型eSCM-SP,并提供了改进的路线图。希望有越来越多的企业从提高服务能力的角度出发,来实践eSCM-SP的最佳实践,为利益攸关者交付更多的价值。

参考文献

1 Paulk M C, Guha S, Hefley W E, et al. Comparing the eSCM-SP v2 and Related Models and Standards: A Comparison Between the eSourcing Capability Model for Service Providers v2 and Related Models and Standards. Pittsburgh, PA: Carnegie Mellon University

2 IT Services Qualification Center. The eSoucring Capability Model for Service Providers v2. Carnegie Mellon University, 2004

3 Control OBjectives for Information and related Technology (COBIT 3rd Edition). 2000. http://www.isaca.org/cobit.htm

4 The IT Governance Institute. COBIT: Control Objectives for Information and related Technology (3rd Edition). 2000. www.isaca.org/cobit.htm

5 BS 15000-1:20. September 2002. IT Service Management: Part 1: Specification for Service Management. British Standards Institute

(上接第277页)

12 Freudenthal E, Pesin T, Port L, Keenan E, Karamcheti V. drbac: Distributed role-based access control for dynamic coalition environments. In: Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS02), 2002

13 Osborn S, Sandhu R S, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Transactions on Information and System Security, 2000, 3(2):85～106

14 Samarati P, de Capitani di Vimercati. Access control: Policies, models, and mechanisms. In: R. Focardi and R. Gorrieri, eds. Foundations of Security Analysis and Design, volume 2171 of Lecture Notes in Computer Science, Springer, 2001. 137～196

15 Solworth J A, Sloan R H. A layered design of discretionary access controls with decidable safety properties. In: Proceedings of IEEE Symposium on Research in Security and Privacy, May 2004

16 Solworth J A, Sloan R H. Security property based administrative controls. In: Proceedings of the Ninth European Symposium on Research in Computer Security (ESORICS2004), Springer, Sept. 2004. 244～259

17 Li N, Tripunitara M V. Security analysis in role based access control. In: Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies (SACMAT 2004), 2004. 126～135

18 Soshi M, Maekawa M, Okamoto E. The dynamic typed access matrix model and decidability of the safety problem. IEICE Transactions on Fundamentals, 2004, E87-A(1):190～203

19 Li N, Tripunitara M V. On safety in discretionary access control: [Technical Report CERIAS-TR-2005-20]. Center for Education and Research in Information Assurance and Security, Purdue University, Feb. 2005

20 Li N, Tripunitara M V. On Safety in Discretionary Access Control. In: Proceedings of IEEE Symposium on Research in Security and Privacy, May 2005

21 Hopcroft J E, Ullman J D. Formal Languages and Their Relation to Automata. Addison-Wesley, Reading, Mass, 1969

22 Downs D D, Rub J R, Kung K C, Jordan C S. Issues in discretionary access control. In: proceedings of IEEE Symposium on Reserch in Security and Privacy, Apr. 1985. 208～218