

适用于分布式系统的多级安全访问控制策略

马铭鑫¹, 史国振², 王亚琼³, 王豪杰³, 成文文²

(1. 西安电子科技大学网络与信息安全学院, 陕西 西安 710071;

2. 北京电子科技学院信息安全系, 北京 100070;

3. 西安电子科技大学通信工程学院, 陕西 西安 710071)

摘要: 针对分布式信息系统的资源共享及安全互操作问题, 在多级安全模型基础上加入管理平台和中间件模块, 提出一种适用于分布式系统的多级安全访问控制策略, 保证数据机密性和访问过程安全可控。用 XACML 语言对安全策略进行标准化描述, 并对策略进行安全性和灵活性分析。

关键词: 分布式系统; 多级安全; 管理平台; 中间件; XACML

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109.x.2017.00184

Multilevel secure access control policy for distributed systems

MA Ming-xin¹, SHI Guo-zhen², WANG Ya-qiong³, WANG Hao-jie³, CHENG Wen-wen²

(1. School of Cyber Engineering, Xidian University, Xi'an 710071, China;

2. School of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China;

3. School of Telecommunications Engineering, Xidian University, Xi'an 710071 China)

Abstract: A multilevel secure access control strategy for distributed system was proposed, which could guarantee the data confidentiality and security, through adding platform and middleware modules. The security policy was described in the XACML language, and the security and flexibility of the policy were analyzed.

Key words: distributed systems, multilevel security, platform, middleware, XACML

1 引言

随着 Internet 的飞速发展, 计算机和通信网络已经渗透到人们生活中的各个方面, 分布式信息系统^[1]凭借可靠性高、灵活性强以及扩充性好等特点得到越来越广泛的应用。分布式信息系统之间需要进行大量数据通信和信息交互, 因此面临信息窃取、非法修改等威胁, 如何确保网络资源的安全共享和互操作已成为研究的重要课题。多级安全^[2]作为强制访问控制^[3]的有效手段, 其

“不上读不下写”的安全特性可以控制数据按照级别只能从低向高流动, 确保敏感数据不泄露, 可以安全有效地解决跨域分布式系统之间的信息互操作, 保证合法用户对网络信息资源受控正确地使用, 限制非法用户的入侵和蓄意破坏。

2 相关工作

访问控制^[4]的主要功能是允许合法用户访问和使用系统受保护的资源和服务, 并防止非法用户的访问和合法用户的非法访问。对分布式系统

收稿日期: 2017-05-10; 修回日期: 2017-06-27。通信作者: 史国振, sgz1974@163.com

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0800304); 北京市自然科学基金资助项目 (No.4152048)

Foundation Items: The National Key Research Program of China (No.2016YFB0800304), The Natural Science Foundation of Beijing (No.4152048)

访问控制技术的研究始于 20 世纪 90 年代初分布式系统开始大量出现的时候^[5]。随着分布式技术迭代更新,安全管理机制发展遇到瓶颈,信任管理^[6]成为新的研究突破点。信任管理是说明和解释安全策略的统一方法,为安全策略提供标准、通用的机制^[7],允许对安全重要的动作进行直接授权。因此系统在实施访问控制之前,制定其安全策略十分重要。文献[8]提出一种基于风险的访问控制模型,通过风险值及其波动幅度动态调整用户的访问权限,实现了分布式系统隐私保护的机制,但未体现多级安全策略。文献[9]通过引入可信度量机制提出基于可信计算的多级安全策略(TCBMLSP, trust computing based multilevel security policy),保证主体行为可信和多级信息安全流通,但未通过非传递不干扰信息流理论对其进行建模与安全性证明。为提高分布式环境下多级安全实施的正确性和可行性,文献[10]提出了分布式可信计算基(DTCB, distributed trusted computing base),实现了细粒度的多级安全访问控制和信息流控制,并采用组合无干扰模型对齐进行形式化安全证明,但灵活性欠缺。文献[11]从理论角度制定分布式控制系统和分级系统的研究计划,讨论建模、多级控制的分布式通信方式,但没有具体实现方法。随着理论的成熟,更多的安全策略被应用到实际系统中,文献[12]提出一个安全框架,解决了预算和时间约束下分布式数据库的安全需求,通过使用多级安全数据库管理系统在不同站点复制不同的预定义安全策略,实现每个系统在进入操作模式之前通过严格的安全扫描。文献[13]提出了基于分布式顶点中心范式的多级强制向导算法,并在 Giraph 平台上实现,展示了安全策略算法的有效性和可扩展性。文献[14]提出一个新的多层次分级模型,可以自动识别不同层云服务的攻击类型和风险评估,保证数据隐私,但是未体现出可监管性。在对分布式文件系统的安全需求进行详细、全面的分析后,本文以多级安全模型为基础,提出一种适用于分布式系统的多级安全访问控制策略,兼顾灵活性、可扩展性和第三方可监管特性。用 XACML 语言对安全策略进行清晰准确描述,并进行必要的安全性证明,有效解决分布式系统域间安全互操作问题。

3 模型概述

本文以多级安全模型为基础,加入管理平台和中间件模块形成安全策略,提高模型的安全性和可扩展性,实现分布式信息系统之间安全高效的信息交互。

3.1 模型基本要素

主体(S, subject): 指用户、进程,如式(1)所示。

$$S = \{s_1, s_2, \dots, s_n\} \quad (1)$$

客体(O, object): 指文件、数据、程序、存储器段等,如式(2)所示。

$$O = \{o_1, o_2, \dots, o_n\} \quad (2)$$

安全等级(security level): 是主体、客体的梯度安全标记,包括主体、客体密级(classification)和范畴集(category)。主体、客体密级表示主体、客体保密性的敏感程度,如式(3)所示;范畴集表示组织中部门或类别的集合,如式(4)所示;系统中所有主体和客体均分配了密级和范畴集,如式(5)所示。

$$C = \{c_1, c_2, \dots, c_n\} \quad (3)$$

$$K = \{k_1, k_2, \dots, k_n\} \quad (4)$$

$$F = \{f \mid f \rightarrow C^S \times C^O \times K^S \times K^O\} \quad (5)$$

访问控制矩阵(access matrix): 用矩阵的形式描述任意时刻系统中自主授权状态,如式(6)所示。

$$M = \begin{bmatrix} m_{11}, \dots, m_{1j} \\ \vdots \quad \ddots \quad \vdots \\ m_{i1}, \dots, m_{ij} \end{bmatrix} \quad (6)$$

访问属性集(attribute set): 描述主体访问客体的方式,如式(7)所示。其中执行(E, execute),只读(R, read),添加(A, append),读/写(W, write)。

$$AS = \{E, R, A, W\} \quad (7)$$

系统状态(state): 表示多级安全系统所有可能的系统状态,如式(8)所示。用 b 表示在系统状态 v 下,主体 s 对客体 o 的访问属性权限,如式(9)所示。

$$V = \{v_1, v_2, \dots, v_n\} \quad (8)$$

$$b \in S \times O \times AS \quad (9)$$

多级安全特性^[3] (multilevel security property): 多级安全特性定义系统状态的安全性, 体现多级安全策略, 如式(10)~式(12)所示, 包括自主安全性、简单安全性和*-性质。

状态 $v = (b, M, f)$ 满足自主安全性, 如式(10)所示。

$$\forall (s_i, o_j, AS) \in v, v \in M_{ij} \quad (10)$$

状态 $v = (b, M, f)$ 满足简单安全性, 如式(11)所示。

$$\begin{aligned} x = e; x = a; or \\ (x = r \text{ or } x = w) \text{ and } (f_1(s) \geq f_2(o), f_3(s) \geq f_4(o)) \end{aligned} \quad (11)$$

状态 $v = (b, M, f)$ 满足*-性质, 如式(12)所示。

$$\begin{aligned} \forall s \in S, o_1 \in b(s : w, a), o_2 \in b(s : r, w) \\ \Rightarrow f_2(o_1) \geq f_2(o_2), f_4(o_1) \geq f_4(o_2) \end{aligned} \quad (12)$$

3.2 模型新增模块

为了摆脱传统多级安全集中式管理的约束, 本文通过加入管理平台模块和中间件模块提高多级安全的可扩展性和安全性, 实现了分布式系统之间信息安全交互和对分布式信息系统的安全管理。

管理平台 (platform): 是独立、可信、可监管的第三方, 负责协调各个跨域分布式系统的安全管理工作。主要功能包括: 对分布式信息系统中的用户和文件进行定级; 采用公钥密码技术保证访问请求/应答的安全信息交互; 记录用户的历史访问信息, 供日后进行安全审计。

中间件 (middleware): 是分布式信息系统的管理平台之间的信息交互接口, 通过信息加密和解密、身份认证和口令校验等方式完成两者之间信息的安全交互。

4 多级安全策略

为了保证分布式系统信息跨域互操作的安全性和灵活性, 对用户访问行为进行约束, 本文在多级安全模型基础上制定一种安全策略, 保证主体对客体实施访问控制时必须遵循一定的规则, 确保系统安全性。

4.1 策略元素

将多级安全策略中涉及的参与元素用数学符号表示, 具体元素的中文含义、英文含义和符号表示如表1所示。

表1 安全策略元素表示

元素中文含义	元素英文表示	元素符号表示
主体	subject	s
客体	object	o
密级	classification	c
范畴	category	k
安全等级	security level	selv
地域	district	dist
系统	system	sys
请求	request	req
反馈	response	res
操作	operation	op
口令	password	pass
授权	permission	per
主体前缀	—	s_
客体前缀	—	o_

4.2 安全策略详述

本文为解决分布式系统之间不同等级用户和文件安全互操作问题, 提出一种多级安全策略, 以 $Dist_x$ 域下 Sys_1 系统的用户 S_3 想要访问 $Dist_y$ 域下 Sys_1 系统的文件 O_8 的实现为例, 安全策略详细步骤如图1所示。

Step 1 等级映射: 管理平台通过综合评估对分布式系统用户 S_3 和文件 O_8 进行重新定级, 但是并不改变用户和文件原有等级, 而是将评定结果映射到管理平台的等级映射表 (LML, level mapping list), 如图2所示。

Step 2 主体访问请求: 用户 S_3 访问文件 O_8 , 发起访问请求 $s_req(s_dist_x, s_sys_1, s_3, s_selv, o_dist_y, o_sys_1, o_8, o_selv, op)$, 依次将 req 中主体区域、系统、用户名、用户安全等级、文件名和访问方式等信息进行填充, o_selv 暂不填充, 因为此时 S_3 并不知道 O_8 的安全等级, 然后通过中间件将请求信息分别用管理平台和分布式系统的公钥加密发送。

Step 3 客体本地查询: $Dist_y$ 区域 Sys_1 系统的中间件收到 $Dist_x$ 区域 Sys_i 系统的用户 S_3 的访问请求后, 对请求信息解密认证, 然后根据 O_8 文件名去本地文件系统数据库查找 O_8 相关信息, 得到 O_8 的安全等级。

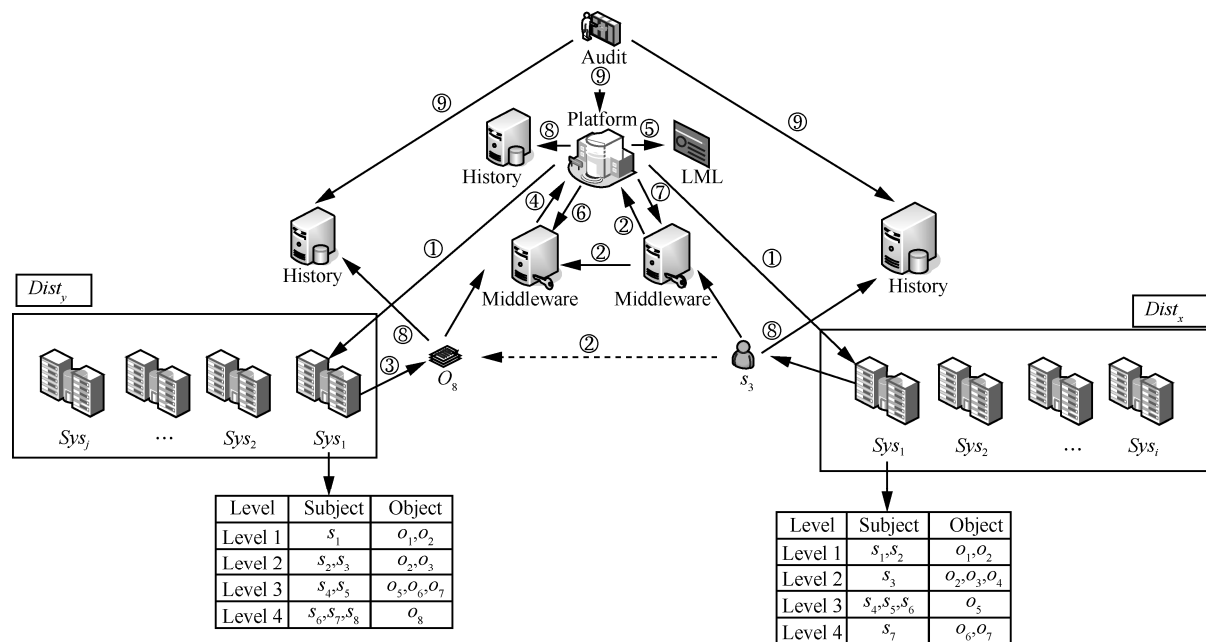


图 1 多级安全策略结构

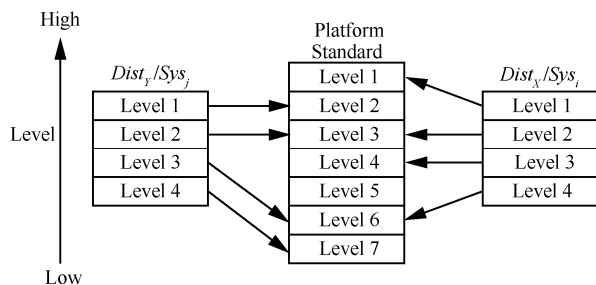


图 2 等级映射表

Step 4 客体访问请求: 文件系统 Middleware 生成一个一次性口令, 并对 req 进行反馈形成 $o_res(s_dist_x, s_sys1, s_3, s_selv, o_dist_y, o_sys1, o_8, o_selv, op, pass)$, 将文件 O_8 的 o_selv 和刚生成的 $pass$ 进行填充, 最后将 o_res 用管理平台公钥加密发送。

Step 5 管理平台授权认证: 管理平台首先将收到 step 2 和 step 4 信息进行解密, 然后进行匹配 (为了确保是同一条请求信息), 匹配成功后等级映射表 LML 根据主 s_req 和 o_res 中主体、客体信息查找对应的安全等级并根据多级安全模型进行授权判定, 得到 $permission$ 。

Step 6 平台授权客体: 管理平台将授权判定结果用分布式文件系统公钥加密返回, 文件系统对 $p_res(s_dist_x, s_sys1, s_3, s_selv, o_dist_y, o_sys1, o_8, o_selv, op, pass, per)$ 进行解密, 如果 per 为同意访问, 文件系统将文件 O_8 的 $password$ 认证接口打开, 并设置用户访问时限倒计时 5 min (超时

窗口关闭); 否则, Middleware 关闭本次访问请求。无论成功与否, 都将该次访问行为进行记录, 供日后安全审计使用。

Step 7 平台授权主体: 管理平台将认定结果用用户公钥加密返回, $p_res(s_dist_x, s_sys1, s_3, s_selv, o_dist_y, o_sys1, o_8, o_selv, op, pass, per)$, 如果 per 为同意访问, 用户 S 可以用 $password$ 访问文件 O_8 ; 否则, Middleware 关闭本次访问请求, 同样将该次访问行为进行记录, 供日后安全审计使用。

Step 8 记录访问行为: 同样地, 管理平台也会将每次访问行为都记录在案, 以独立的可信第三方身份保证每一次主体访问客体行为的真实抗抵赖性, 供日后安全审计使用。

Step 9 安全审计: 审计作为独立的第三方, 监督管理平台、分布式文件系统和用户历史记录, 负责安全审计, 供相关单位进行安全检查。

4.3 XACML 语言描述

XACML 是一种统一标准语言^[15], 用于描述访问控制策略以及访问控制请求/响应的产生过程, 不仅为整个授权过程的控制提供一系列逻辑算法, 而且还提供标准可扩展点, 使其能够很好地适用于分布式信息系统。本文从策略 (policy)、请求 (request) 和响应 (response) 这 3 个方面对上述安全策略进行 XACML 语言描述, 实现规范化和实例化。

1) Policy

Policy 是对安全策略的核心描述, 本文的访问控制授权机制采用多级安全策略, 即 <Description> 中的 multilevel security strategy access control policy, 管理平台据此对用户进行访问请求授权判决, Policy 的 XACML 描述如下。

```
<Policy>
  <Description>
    multilevel security strategy access
    control policy
  </Description>
  <Rule>
    <Description>
      The action of subject on object
      follows multilevel security policy.
    </Description>
    <Target>
      <AttributeValue>multilevel
      security</AttributeValue>
    </Target>
  </Rule>
</Policy>
```

2) Request

用户需要规范地描述和表示跨域操作的请求, 以说明自己的身份信息以及访问目标。例如, 位于上海市 (Shanghai) 档案局 (Document) 的 Alice 想要查看北京市 (Beijing) 档案局的上季度财务收入 (quarter revenue), 用 XACML 语言描述此请求过程如下。

```
<Request>
  <Subject>
    <Attribute AttributeId="Distic"
    <AttributeValue> Shanghai
    </AttributeValue>
  </Attribute>
  <Attribute AttributeId="System"
  <AttributeValue> Document
  </AttributeValue>
</Attribute>
  <Attribute AttributeId="Name"
  <AttributeValue> Alice
  </AttributeValue>
</Attribute>
```

```
<Attribute AttributeId="Category"
<AttributeValue> Finance
</AttributeValue>
</Attribute>
<Attribute AttributeId="Level"
<AttributeValue> 3</AttributeValue>
</Attribute>
```

```
</Subject>
```

```
<Object>
```

```
<Attribute AttributeId="Distic"
<AttributeValue> Beijing
</AttributeValue>
</Attribute>
<Attribute AttributeId="System"
<AttributeValue> Document
</AttributeValue>
</Attribute>
<Attribute AttributeId="Name"
<AttributeValue> Quarterrevenue
</AttributeValue>
</Attribute>
<Attribute AttributeId="Category"
<AttributeValue/>
</Attribute>
<Attribute AttributeId="Level"
<AttributeValue/>
```

```
</Object>
```

```
<Action>
```

```
<Attribute AttributeId="Option"
<AttributeValue> read
</AttributeValue>
</Attribute>
```

```
</Action>
```

```
</Request>
```

3) Response

管理平台通过 Policy 对 Request 进行安全验证授权后, 将授权结果返回给客户端。如果允许, 客户用 password 进行访问; 如果拒绝, 用户则无权访问该文件, 用 XACML 语言描述如下。

```
<Response>
  <Result>
    <Decision>Applicable</Decision>
  </Result>
```

</Response>

5 模型分析

5.1 可扩展性分析

当有新的分布式系统加入时, 根据本文提出的 LML, 只需将不同等级的用户和文件按照等级进行映射, 而不是将每一个用户和文件重新定级, 实用性较高, 依次类推, 管理平台只需对系统从总体角度上进行认定, 可以融入更多分布式系统, 体现了较高的可扩展性。

5.2 安全性分析

5.2.1 信息交互安全性

管理平台与分布式信息系统之间通信全程公钥加密, 并且 Middleware 还实现了用户认证、password 和访问时限倒计时等功能, 极大程度上保证了分布式系统之间信息交互的机密性。

5.2.2 模型安全性

由于模型中加入了 LML, 增添了原有多级安全的认证用户和信息, 因此需要对模型的安全性进行证明, 最终结果表明安全性有保障。

定义 1 当有新的分布式系统加入系统中时, 管理平台根据 LML 对其进行综合评定, 得出用户和文件的相关等级 $f_s \rightarrow f_s^*$, $f_o \rightarrow f_o^*$, 由对应的补充管理平台访问控制列表 M 得到 M^* , 其系统安全状态为安全可信, 系统状态变化如式(13)所示。

$$(b, M, f) \rightarrow (b, M^*, f^*) \quad (13)$$

即

if $f_c(s_i) \in f_s^*$, $f_c(o_j) \in f_o^*$, $m_{ij} \notin M$, 对 $req(s_i, o_j, as)$ 的处理如下。

1) $f_c^*(s_i) \leftarrow f_c(s_i)$, M

2) 对 $req(s_i, o_j, as)$ 授权, 构造 M^* , 使

$$M^* = M \cup (s_i, o_j, as)$$

进入 (b, M^*, f^*) 状态。

else

进入 (b, M, f) 状态。

具体证明如下。

① 证明满足式(10)自主安全特性

设 $(s_i, o_j, as) \in b$

if $f_c(s_i) \in f_s, f_c(o_j) \in f_o$

满足多级安全式(10)特性

else $f_c(s_i) \in f_s^*, f_c(o_j) \in f_o^*$

$as \in M^*$

状态满足 (b, M^*, f^*) 特性。

② 证明满足式(11)简单安全特性

if $f_c(s_i) \in f_s, f_c(o_j) \in f_o$

满足多级安全式(11)特性

else $f_s^*(s_i) \leftarrow f_c(s_i), f_o^*(o_j) \leftarrow f_c(o_j)$

$$f_s^*(s_i) \geq f_o^*(o_j)$$

状态满足 (b, M^*, f^*) 特性。

③ 证明满足式(12)满足*-特性

if $f_c(s_i) \in f_s, f_c(o_j) \in f_o$

满足多级安全式(12)特性

else $f_s^*(s_i) \leftarrow f_c(s_i), f_o^*(o_j) \leftarrow f_c(o_j)$

$f_s^*(s_i) < f_c^*(o_j)$, 满足式(7)中 A 操作。

$f_s^*(s_i) = f_c^*(o_j)$, 满足式(7)中 W 操作。

$f_s^*(s_i) > f_c^*(o_j)$, 满足式(7)中 R 操作。

证毕。

6 结束语

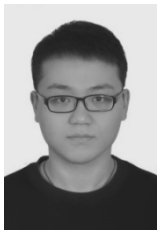
本文基于多级安全模型, 加入管理平台和中件模块, 提出一种适用于分布式系统的多级安全策略, 保证了分布式系统之间跨域操作、信息交互的安全性, 极大提高了安全策略的安全性和可扩展性。采用 XACML 语言对策略进行规范化描述, 并对策略安全性进行形式化证明。接下来, 将本文安全策略进行实现, 并应用到实际分布式系统中。

参考文献:

- [1] CHANDY K M, LAMPORT L. Distributed snapshots: determining global states of a distributed system[J]. ACM Transactions on Computer Systems, 1985, 3(1): 63-75.
- [2] BELL D E, PADULA L J L. Secure computer system: unified exposition and multics interpretation[J]. Secure Computer System Unified Exposition & Multics Interpretation, 1976.
- [3] ISO 7498-2: 1989(en)[S].
- [4] 李风华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-166.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal of Communications, 2016, 37(11): 156-166.
- [5] WOO T Y C, LAM S S. Authorization in distributed systems: a formal approach[C]//IEEE Computer Society Symposium on Research in Security and Privacy. 1992:33-33.
- [6] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust man-

- agement[J]. Proceedings of IEEE Conference security & Privacy, 1996, 30(1): 164-173.
- [7] Blaze M. The KeyNote Trust-Management System Version 2[J]. At & T Research Labs, 1999.
- [8] 李甲帅, 彭长根, 朱义杰, 等. 面向 Hadoop 的风险访问控制模型[J]. 网络与信息安全学报, 2016, 2(1): 46-52.
- LI J S, PENG C G, ZHU Y J, et al. Risk access control model for Hadoop[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 46-52.
- [9] LIU X T, LI X W, CUI X. Research on trust computing based multilevel security policy[J]. Electronic Design Engineering, 2016.
- [10] JING S, CHEN X, DU X, et al. Distributed multilevel security core architecture based on noninterference theory[J]. Journal of Computer Applications, 2013, 33(3): 712-716.
- [11] SCHUPPEN J H V. Research program for control of distributed and of multilevel systems[M]//Coordination Control of Distributed Systems. Berlin: Springer, 2015: 385-392.
- [12] BATRA N, SINGH M. Multilevel policy based security in distributed database[M]//Advances in Computing and Communications. Berlin: Springer, 2011: 572-580.
- [13] ARLEO A, DIDIMO W, LIOTTA G, et al. A distributed multilevel force-directed algorithm[C]//The International Symposium on Graph Drawing and Network Visualization. 2016:3-17.
- [14] HUSSAIN S A, FATIMA M, SAEED A, et al. Multilevel classification of security concerns in cloud computing[J]. Applied Computing & Informatics, 2016.
- [15] eXtensible Access Control Markup Language (XACML) Version 3.0[S]. 2013.

作者简介:



马铭鑫 (1992-), 男, 山西临汾人, 西安电子科技大学博士生, 主要研究方向为网络信息安全。



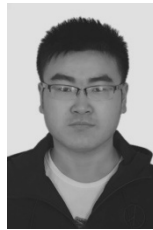
史国振 (1974-), 男, 河南济源人, 博士, 北京电子科技学院副教授、硕士生导师, 主要研究方向为网络与系统安全、嵌入式安全。



王亚琼 (1994-), 女, 山西朔州人, 西安电子科技大学硕士生, 主要研究方向为网络信息安全。



王豪杰 (1991-), 男, 山东青岛人, 硕士, 西安电子科技大学硕士生, 主要研究方向为访问控制与网络安全。



成文文 (1993-), 男, 河南济源人, 北京电子科技学院硕士生, 主要研究方向为网络安全。