Resolving Policy Conflicts for Cross-Domain Access Control: A Double Auction Approach*

Yunchuan Guo[1,2], Xiyang Sun[1,2], Mingjie Yu[1,3], Fenghua Li[1,2], Kui Geng[1], and Zifu Li[1](✉)

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
lizifu@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China,
[3] School of Cyber Security, University of Science and Technology of China, Hefei ,China

Abstract. Policy-mapping mechanisms can efficiently help to realize the exchange and the sharing of cross-domain information at low cost. However, due to concerns over policy conflicts, if not sufficient incentives, most selfish domains are often disinterested in helping others to implement policy mapping cooperatively. Thus an appropriate incentive mechanism is required. In this paper, we propose an incentive mechanism to encourage selfish domains to take part in policy mapping and resolve policy conflicts. Formulating conflict resolution as a double auction and solving Bayesian Nash equilibrium, we design the optimal asking/bidding price scheme to maximize the benefits of the domains involved. Simulations demonstrate that our approach can efficiently incentivize selfish domains to take part in cooperation.

Keywords: Cross-Domain Collaboration · Conflict resolution · Incentive mechanism · Double Auction.

1 Introduction

Cross-domain collaboration, which enables multiple organizations or systems in domains via the networks (e.g., Internet, mobile Internet, and Internet of things) to work together to achieve their own or common goals, has been widely used in various applications, such as E-government, healthcare [12] and remote offices[2]. Through cross-domain collaboration, one can directly access the resource of the other domain without the time-consuming manual authorization, thus increasing work efficiency. To securely realize cross-domain collaboration at low cost, the mapping of access control policies has been recently proposed to logically connect the involved domains without rebuilding a new collaboration system. In this approach, one autonomous domain's roles are mapped to the roles of the

* Supported by the National Key Research and Development Program of China (No.2019YFB2101702),the National Natural Science Foundation of China (No. U1836203) and the Youth Innovation Promotion Association CAS (2019160).

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

other domain. Through this approach, the authorized user of the first domain is automatically allowed to access the resource of the second domain, thus improving interoperability. However, because policy mapping breaks the security boundaries of inter-domain and causes a large amount of policy conflicts [14], domains that carry out policy mapping are suffering from an increasing number of security events, e.g., data breach, data corruption, and privacy leakage. To prevent and mitigate these events, one important thing that should be done is to design an efficient scheme of conflict resolution to achieve a tradeoff between security and interoperability.

Motivation: However, the existing schemes of conflict resolution for cross-domain policy mapping cannot efficiently work without sufficient incentives, because most autonomous domains are selfish and they are often uninterested in resolving policy conflicts (as a result, they do not participate in cross-domain collaboration) for the following reasons: (1) *Autonomy losses.* In most cases, resolving policy conflicts causes autonomy losses. For example, as shown in Fig.1(a), role-based access control(RBAC) is used to assign permissions for users in domains A and B, where domain A has two roles (i.e., r_1 and r_2) and r_1 inherits all permissions of r_2. Domain B has one role (i.e., r_3). To achieve interoperability, we assume that r_1 of domain A and r_3 of domain B are mapped to r_3 of domain B and r_2 of domain A, respectively, as shown in Fig 1(b). Under this assumption, a conflict called cyclic inheritance between r_1 and r_3 will be caused, as shown in Fig.1(c). To resolve this conflict, one possible scheme is to delete the inheritance relationship between r_1 and r_2 (i.e., role r_1 no longer inherits the permissions of role r_2), as shown in Fig.1(d). From this example, we can see that conflict resolution will decrease autonomy.

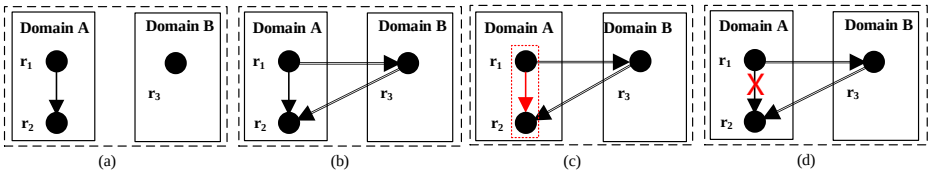

Fig. 1: (a) RBAC policy graph of domain A and B used in Autonomy losses. (b) RBAC policy after policy mapping. (c) RBAC policy conflicts between domain A and B. (d) RBAC policy after conflict resolution.

(2) *Privacy issues.* In existing schemes, the third party is often required to be responsible for mapping policies between domains and resolving their conflict. To complete its task, the third party has to obtain access control policies of both domains involved (i.e., the accessing domain and the accessed domain). However, because these policies often contain a lot of private or confidential information, both the involved domains are unwilling to disclose their policies to the third party. For example, if a policy specifies that George can access top-secret files, then it can be inferred that George is a sensitive person. Due to the above reasons, a selfish domain is unwilling to participate in the cross-domain collaboration without appropriate incentives. Therefore, an incentive mechanism

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

is required to incentivize the involved domain to participate in policy mapping and conflict resolution.

Existing incentive mechanism can be roughly divided into two categories: non-game-theoretical approaches [3,19] and game-theoretical approaches[5,6]. In the first approaches, contract mechanisms (e.g., reward contract[3] and judge contract[19]) are often adopted to predefine a set of reward rules to motivate individuals to fulfil their promise agreed in the contract and maximize their utility. For instance, Cruz *et al.*[3] adopted Ethereum's smart contract to encourage nodes to verify trans-organizational utilization of roles. Zhang *et al.* [19] designed a judge contract to analyze and penalize subjects' misbehavior and incentive the accessed objects to facilitate the validation of subjects' identity in the Internet of Things. However, in these approaches, a participant often ignores the competitive behavior of other participants and cannot make reasonable decisions. Considering rational individuals, a large amount of efforts are spent on designing the game-theoretical approaches to evaluate the competitive behavior of all participants and select the rational action to maximize its utility. Considering the community-structured behavior, Ren *et al.* [5]designed an evolutionary game-theoretic framework to incentive users to protect privacy information in OSNs, and Fang *et al.* [6]proposed an auction-based incentive mechanism to encourage co-owners to carry out a privacy agreement. However, existing incentive mechanism are not suitable for cross-domain collaboration because they ignore interoperation and autonomy.

Contribution: To address the above problem, we investigate conflict resolution from the aspects of the game. Our main contributions are as follows.

(1) Considering the selfishness of domains and inter-domain competition, we formulate an incentive mechanism for conflict resolution of cross-domain policy mapping as a double auction game and propose a conflict resolution framework of cross-domain policy mapping.

(2) After analyzing factors that impact the cost of the accessed domain and value of the accessing domain, we solve Bayesian Nash equilibrium under the assumption the incomplete information and design the optimal asking/bidding price scheme to maximize their interests.

(3) A series of experiments are carried out on a simulated dataset and the experimental results show that our proposed algorithm can efficiently incentivize domains to participate in conflict resolution.

The rest of this paper is organized as follows. In Sect. 2, we discuss the related work. In Sect. 3, we introduce the problem statement and our basic idea. Sect. 4 formulates the value and the cost in conflict resolution and analyzes its influencing factors. We conduct a double auction game in Sect. 5. Simulations and their analysis are given in Sect. 6. We draw a conclusion in Sect. 7.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

2 Related Work

From the aspect of the number of resolution parties, the existing conflict resolution for access control can be divided into two categories: resolution within a single party and resolution among multiple parties.

2.1 Conflict Resolution within a singleparty

In this approach, conflict resolution is often formulated into a single-objective or multi-objective optimization problem to maximize the overall goal (e.g., highest precedence [8], resource consumption [18], and policy consistency [16]).

Considering the applicable laws, Huynh *et al*. [8] minimized the rule graph to resolve the conflicts between regional regulations and patient wishes, and selected the policy with the "highest" precedence (with regard to priority, specificity and modality) as the final policy decision. After translating access behaviors into the canonical representation of query spaces, Yahiaoui *et al*. [16] used fine-grained algebra expressions to infer and resolve the conflicts of policies and maximize the consistency of attribute-based access control policies. Rather than using inference to seek the solution [16], Omar *et al*. [11] adopted an answer set programming to search for the candidate resolution and calculate their priority. Extending Petri nets with both time and resource factors, Zeng *et al*. [18] designed three efficent strategies (i.e., start-early priority strategy, waiting-short priority strategy, and key-activity priority strategy) to resolve the conflict of emergency response processes and minimize resource consumption. To minimize the worst-case performance of services conflicts in smart cities, Ma *et al*. [9] designed an integer linear programming to generate serval resolution options and adopted a signal temporal logic to evaluate the performance of these options. Although the above schemes can efficiently resolve policy conflicts caused by individual mistake, they ignored individual interest and cannot deal with the policy conflicts caused by the conflict of interest of stakeholders.

2.2 Conflict Resolution among multiparty

From the aspect of interests of stakeholders, the existing schemes can be roughly divided into two categories: conflict resolution with optimizing collective interests and conflict resolution with optimizing individual interests.

Conflict resolution with optimizing collective interests. In this approach, the centralized platform regarded multiple domains as a whole and selected the scheme that maximizes their whole benefits as the final policy. Along this line, Shafiq *et al*. [14] adopted an integer programming (IP) to approximately avoid conflicts and maximize the global interoperation in the case of an acceptable autonomy loss. To assign permissions without conflicts, Zhu [20] *et al*. formulated the problem of maximizing the resolution performance into a linear programming problem and adopted the CPLEX optimization package to solve this problem and obtain the approximate optimal solution. Similarly, Samadian *et al*. [13] developed a dynamic programming algorithm with a polynomial-time complexity

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

to resolve the contingent conflicts. Although the above schemes can maximize the collective interests, they suffer from two problems: (1) A centralized platform is required to collect the privacy-sensitive policies of the involved domains. As a result, the privacy-sensitive domains are reluctant to provide their policies to the centralized platform. (2) The selfish domain often hopes to maximize not the collective interests but its own interests. Thus, the selfish domain is unwilling to resolve conflicts cooperatively.

*Conflict resolution with optimizing individual interests.*A series of mechanisms (e.g., negotiation [10,17]and game [4,7]) have been proposed to express the individual interests and maximize individual interests. For instance, considering privacy preferences and the sharing requirement, Mehregan *et al.* [10] designed a negotiation mechanism to interactively adjust and revise the access permission of the shared data of online social networks (OSNs). Yang *et al.* [17] designed a local supervisory controller to observe the states (i.e., activated or inactivated) of roles of each domain and maximize resolution efficiency through selecting the prevention scheme of conflicts caused by role change. Formulating the multiparty privacy conflict in OSNs into a multi-player noncooperative game, Ding *et al.* [4] established the multiple equilibria to achieve the trade-off between privacy preference and the social influence in OSNs. Using the multiparty control game, Hu *et al.* [7] proposed an optimal conflict resolution algorithm to adjust the privacy setting in OSNs and maximize the benefits of the user who shares data.As shown above, although a large amount of efforts have been spent on resolving policy conflicts of access control, these efforts ignore the factors that affect the cost and value of the domains involved. As a result, they cannot effectively incentivize selfish domains to resolve conflicts cooperatively.

3 Problem Statement and Basic Idea

3.1 Cross-Domain Policy Mapping in RBAC

In our work, cross-domain policy mapping in RBAC is formally specified by hierarchical role graphs, where nodes of a graph can be divided into three categories: user nodes, role nodes, and permission nodes. Fig.2(a) gives an example of hierarchical RBAC roles. In this example, there are two domains (i.e., domain A and domain B), where domain A has 3 roles (i.e., r_1, r_2 and r_3), 3 users (i.e., u_1, u_2,and u_3), and 3 permissions (i.e., p_1, p_2 and p_3); Domain B has 4 roles (i.e., r_4,r_5,r_6 and r_7), 2 users (i.e., u_4 and u_5), and 3 permissions (i.e., p_4, p_5 and p_6).

As shown in Fig.2, edges between nodes can be divided into 7 categories: user-role assignment($\mapsto$), role-permission assignments($\twoheadrightarrow$), inheritance hierarchy($\rightarrow$, I-hierarchy), Activation hierarchy($\dashrightarrow$, A-hierarchy), role-specific Separation of duty(SOD) constraints ($\overset{\longleftrightarrow}{_{RSOD}}$), user-specific SoD constraints ($\overset{\longleftrightarrow}{_{USOD}}$), role mapping($\Longrightarrow$) and the induced role SOD constraint($\overset{\longleftrightarrow}{_{InducedRSOD}}$), where the edge $u \mapsto r$ represents that user u is assigned role r, edge $r \twoheadrightarrow p$ indicates that role r is assigned permission p, edges $r_1 \rightarrow r_2$ and $r_1 \dashrightarrow r_2$ represent that r_1 can inherit

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

all permissions of r_2 without activation operation and with activation operation, respectively. Edge $r_1 \overset{\longleftrightarrow}{_{RSOD}} r_2$ (called role-specific SOD constraints, RSoD)denotes no user can be allowed to simultaneously access r_1 and r_2 in the same session, and edge $u_1 \overset{r}{\underset{USOD}{\longleftrightarrow}} u_2$ (called the user-specific SOD constraint) indicates that users u_1 and u_2 are not be allowed to access role r in the same session. Edge $r_1{:}A \Longrightarrow r_2{:}B$ indicates role r_1 in domain A is mapped to r_2 in domain B, that is, r_1 is assigned the permissions owned by role r_2. Edge $r_1 \overset{\longleftrightarrow}{_{Induced RSOD}} r_2$ indicates that the new RSOD constraint between roles role1 and role2 is induced.

3.2 Conflicts Induced by Policy Mapping

For two conflict-free policies, after executing policy mapping, three types of conflicts may be induced, defined as follows.

Definition 1 (induced cyclic-inheritance conflict, iCIC.) An iCIC happens in one domain (says domain A) if after cross-domain policy mapping, at least one role (says r) in domain A inherits the permissions of roles that are senior to r.

Definition 2 (induced role-specific SoD conflict, iRSODC.) An iRSODC happens in one domain (says domain A) if after cross-domain policy mapping, a user in domain A can simultaneously can be assigned to two conflicting roles of domain A.

Definition 3 (induced user-specific SoD conflict, iUSODC). An iUSODC happens in one domain (says domain A) if after cross-domain policy mapping, two users in domain A can simultaneously access two conflicting roles.

Next, we give an example to illustrate the above conflicts induced by cross-domain mapping.

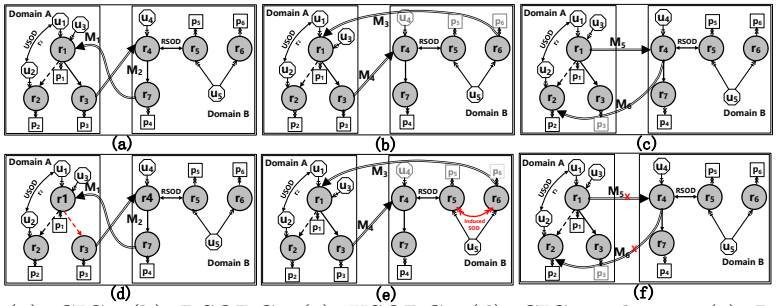

Fig. 2: (a) iCIC , (b) iRSODC , (c) iUSODC . (d) iCIC resolution, (e) iRSODC resolution, and (f) iUSODC resolution.

Example 1. As shown in Fig.2, we assume that: (1) in domain A, r_1 inherits all permissions of r_3, role r_2 is junior to r_1, and a user-specific SoD constraint is specified between user u_1 assigned to r_2. (2) In domain B, r_4 inherits the permissions of r_7 and a role-specific SoD constraint is specified for r_4 and r_5. Next, we give three conflicts.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

iCIC. In Fig. 2(a),if roles r_7 in domain B and r_3 in domain A are mapped to roles r_1 and r_4 respectively, then the junior role r_3 will inherit the permissions of the senior role r_1 through inheritance path $r_3 \rightarrow r_4 \rightarrow r_7 \rightarrow r_1$.Therefore, an iCIC will be induced, as shown in Fig. 2(d).

iRSODC. In Fig.2(b),if roles r_3 in domain A and r_6 in domain B are mapped to roles r_4 and r_1 respectively, then role r_6 will inherit the permissions of role r_4 along inheritance path $r_6 \rightarrow r_1 \rightarrow r_3 \rightarrow r_4$. Before the two mappings are executed, u_5 can be assigned to r_5 and r_6, simultaneously. However, after these mappings are executed, u_5 will own the permissions of role r_4. Because iRSOD conflict exists between r_4 and r_5, a new RSoD between r_5 and r_6 will be induced, as shown in Fig.2(e).

iUSODC. In Fig.2(c), if roles r_1 in domain A and r_4 in domain B are mapped to roles r_4 and r_2 respectively, thens role r_1 will inherit the permissions of role r_2 through inheritance path $r_1 \rightarrow r_4 \rightarrow r_2$. Before the policy mappings are executed, u_1 and u_2 cannot be assigned to r_2 (because there is a user-specific SoD constraints between user u_1 assigned to r_2 and u_2 assigned to r_2), simultaneously. However, after these mappings are executed, user u_1 indirectly obtains the permissions of r_2 along inheritance path $r_1 \rightarrow r_4 \rightarrow r_2$. As a result, an iUSODC between u_1 and u_2 about r_2 will be induced, as shown in Fig.2(f).

3.3 Basic Idea for Conflict Resolution

Undoubtedly, conflict resolution may cause autonomy loss. For example, to resolve the iCIC in Fig. 2(a), one approach is to revoke the permissions owned by r_3 from the permissions of role r_1, i.e., modify the inherance relationship between r_1 and r_3, as shown in Fig 2(d) and the accessed domain has to revoke its internal permissions and loses its autonomy. As a result, if domain A is selfish, it doesn't cooperatively take participate in policy mapping.

To encourage domains to cooperate, we regard policy mapping as service and propose an auction-based incentive mechanism to improve the interoperation, where the accessed domain sells its service and wins virtual credits to make up for its autonomy loss or privacy leakage. The accessing domain acting as a buyer pays for the service to the seller. As shown in Fig. 3, our auction can be divided into four steps: Policy Mapping Request, Policy Mapping Response , Asking Price & Bidding Price, and Auction, discussed as follows.

Step 1(Policy Mapping Request): The accessing domain (says domain A) requests the permissions reqPSET required by domain A to the accessed domain (says domain B) .

Step 2(Policy Mapping Response): Once the policy mapping request is received, domain B matches the requested permission reqPSET and searches the required roles in its own domain. If the match succeeds, domain B sends the matched roles to domain A; Otherwise, policy mapping fails.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

Step 3(Asking Price & Bidding Price): During asking price and bidding price, (1) Domain B evaluates the cost c of policy mapping and seals[1] the asking price p_s.(2) Domain A evaluates the value v of this policy mapping and seals the bidding price p_b.(3)Then, domain A and domain B exchange the sealed bidding price and sealed asking price, respectively.

Step 4(Auction): Domain A and domain B involved unseals the bidding price p_s and the asking price p_b. If $p_s \leq p_b$ holds, the transaction is concluded and domain A pays $\frac{p_s+p_b}{2}$ to domain B to resolve the conflicts. Otherwise, the transaction fails.

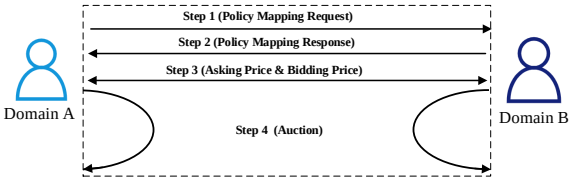

Fig. 3: Framework of conflict resolution.

4 Cost and Value in Conflict Resolution

In this section, we discuss the interoperation value of the accessing domain and the autonomy loss of the accessed domain. Next, we analyze the factors that affect value and cost.

4.1 Influencing Factors

Autonomy loss & false gain. For the accessed domain, policy mapping will cause not only autonomy losses but also false gains. Given domain A, we define the autonomy of managing its role at time t as the weighted sum of permissions assigned to the role, and autonomy of domain A at time t as the weighted sum of the autonomy of its all roles at the current time, formally described as follows.

$$Autonomy\ (A \mid t) = \sum_{r \in role(A|t)} \left(w_r \sum_{p \in perm(r|t)} w_p \right) \tag{1}$$

Where functions $role(A \mid t)$ and $perm(r \mid t)$ returns all roles in domain A and all permissions (including the original permissions and the inherited permissions) of role r at time t, respectively. Parameters w_r and w_p represent autonomy weights of role r and permission p, respectively.Given an autonomy function of domain A, we use function $Autochange(A) = Autochange(A \mid before\ mapping) - Autochange(A \mid after\ mapping)$ to denote autonomy change.

[1] Temporal attribute-based encryption (TABE) can be used to seal the price. Only when the pre-negotiated time is reached, the domain involved can decrypt the sealed price. TABE is out of the scope of our paper, please refer to [1] for more details.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

Autonomy losses $autoloss(A)$ and false gain $falsegain(A)$ caused by cross-domain mapping can be defined as follows, respectively.

$$autoloss\ (A) = \begin{cases} Autochange\ (A),\ if\ \ Autochange\ (A) > 0 \\ 0,\ otherwise \end{cases} \tag{2}$$

$$falsegain\ (A) = \begin{cases} |\ Autochange\ (A)\ |,\ if\ Autochange\ (A) < 0 \\ 0,\ otherwise \end{cases} \tag{3}$$

Interoperation. As shown in Section 3, if a role (say r_A) in domain A is mapped to a role (say r_B) in domain B, then interoperation of domain A will be increased. Generally, for the accessing domain, greater interoperation means a high value/benefit. In our work, the interoperation $Interoperation(A \rightarrow B)$ brought by mapping roles in domain A to roles in domain B is defined as the weighted sum of B's permissions assigned to roles of domain A, formally described as follows.

$$Interoperation(A \rightarrow B) = \sum_{r \in map-role(A)} \left(w_I(r) \sum_{p \in mapped-perm(r,B)} w_I(p) \right) \tag{4}$$

Where functions $map{-}role(A)$ and $mapped{-}perm(r, B)$ return the map roles in domain A and the obtained B's permissions of role r, respectively. Parameters $w_I(r)$and $w_I(p)$ represent interoperation weights of role r and permission p, respectively.

Privacy leakage. If a role (say r_A) in domain A is mapped to a role (say r_B) in domain B, then the privacy of domain B will be leaked. For the accessed domain, a greater privacy leakage means a high risk to suffer the malicious attack. In our work, we define the amount $PrivacyLoss(A \rightarrow B)$ of privacy leakage brought by mapping roles in domain A to roles in domain B as the weighted sum of the privacy of its all mapped permissions, formally described as follows.

$$PrivacyLoss(A \rightarrow B) = \sum_{r \in map-role\ (A)} \left(w_p(r) \sum_{p \in mapped-perm(r,B)} w_p(p) \right) \tag{5}$$

Parameters $w_p(r)$ and $w_p(p)$ represent privacy weights of role r and permission p, respectively.

4.2 Seller's Cost

Generally, more than one candidate schemes (say $S_1 \ldots S_n$) can be used to resolve conflicts[2] and cost rely on candidate schemes.As shown in Section 3, the accessed

[2] For example, as shown in Fig.2(d), there are two candidate schemes S_1={remove the mapping $r_7{:}B \Longrightarrow r_1{:}A$ or $r_3{:}A \Longrightarrow r_4{:}B$} and S_2={modify the inheritance relationship between r_1 and r_3} of resolving conflicts: if we delete mapping $r_7{:}B \Longrightarrow r_1{:}A$ or $r_3{:}A \Longrightarrow r_4{:}B$, then no conflict can be found.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

domain acts a seller.Given a candidate scheme, its cost depends on the loss caused by policy mapping, including three parts: autonomy loss, false gain, and privacy leakage.

Given the accessing domain A and the accessed domain B, we define B's service cost $Cost(A \to B)$ caused by a policy mapping from domain A to domain B as follows.

$$Cost(A \to B) = \min \{cost\,(A \to B \mid S_1), \ldots, cost\,(A \to B \mid S_n)\} \quad (6)$$

where $cost\,(A \to B \mid S_i) = autoloss\,(A \to B \mid S_i) + PrivacyLoss\,(A \to B \mid S_i) + falsegain\,(A \to B \mid \mathrm{S}_i)$ represents cost domain B's service cost if resolution scheme S_i is adopted. $autoloss\,(A \to B \mid S_i)$ denotes autonomy losses of domain B in candidate scheme S_i, $PrivacyLoss\,(A \to B \mid S_i)$ and $falsegain\,(A \to B \mid \mathrm{S}_i)$ are similar.

4.3 Buyer's Value

The accessing domain acts a buyer and its value depends on benefits caused by policy mapping, including two parts: interoperation improvements and false gain.

Given the accessing domain A and the accessed domain B, value of $A\,Value(A \to B)$ induced by a policy mapping as follows.

$$Value\ (A \to B) = Interoperation(A \to B)\ \text{-}\ falsegain\ (A \to B) \quad (7)$$

5 Double Auction Game and Its Analysis

In our work, we formulate conflict resolution in cross-domain collaboration as an auction game, where cooperation with resolving conflicts is regarded as service, the accessing domain plays as a buyer, and the accessed domain plays as a seller. In this game, the key aspect is to ask price p_s and the bid price p_b to maximize the interests of the involved domains. In our game, the accessing domain and the accessed domain bid at the same time. If the asking price p_s is less than or equals the bidding price p_b, then the auction concludes at the trading price $\frac{p_s+p_b}{2}$; otherwise, the auction fails, where (1) the asking price p_s depends on cost c of a seller and buyer's value v predicted by the seller, (2) the bidding price p_b relies on value v to the buyer and seller's cost c predicted by the buyer.

5.1 Double Auction with incomplete information

In the above auction, if the seller knows the service value to the buyer and the buyer also knows the seller's service cost, then this auction is complete. However, in practice, service cost and service value are often private information of a seller and a buyer, respectively. Thus, the assumption of incomplete information is more reasonable. That, although the seller does not accurately know the value to the buyer and the buyer does not know the seller's cost, the probability distributions of cost and value are assumed to be their common knowledge. In

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

our work, both cost and value are assumed to obey the two-parameters Burr XII distribution ,which is widely adopted in the economic field [15].

The probability density function of two-parameter Burr XII function with shape parameter α and τ is as follows.

$$burr(c \mid \alpha, \tau) = \frac{\alpha\tau c^{\tau-1}}{(1+c^{\tau})^{\alpha+1}}, c \geq 0, \alpha \geq 1, \tau \geq 1 \tag{8}$$

Now if $\alpha > 1$, then $burr(c \mid \alpha, \tau)$ is a unimodal function which peak at $c = \left(\frac{\alpha-1}{(\alpha\tau+1)^{\tau+1}}\right)^{\frac{1}{\alpha}}$.If $\alpha = 1$, $burr(c \mid \alpha, \tau)$ is an L-shape function. The culmulative distribution function of two-parameters Burr XII is as follows:

$$Burr(c \mid \alpha, \tau) = 1 - \frac{1}{(1+c^{\tau})^{\alpha}} \tag{9}$$

In this paper, the cost c and the value v have the truncated Burr XII distribution over an interval [0, U] ,that is, their probability distribution function is given by:

$$truncated - burr(c \mid \alpha, \tau) = \frac{burr(c|\alpha,\tau)}{Burr(U|\alpha,\tau) - Burr(0,|\alpha,\tau)}, 0 \leq c \leq \mathrm{U}, \alpha \geq 1, \tau \geq 1 \tag{10}$$

We assume that the asking price p_s of a seller and the bidding price p_b of a buyer are proportional to cost c and value v, that $p_s(c) = \beta_s c$ and $p_b(v) = \beta_b v$ and where $\beta_b > 1$ and $0 < \beta_s < 1$ are linear parameters. Given the above assumption, we can calculate the expected benefits $E_{accessed}(p_s, p_b(v))$ of the accessed domain and the expected benefits $E_{\text{access}}(p_s(c), p_b)$ of the accessing domain, as follows.

$$E_{\text{accessed}}(p_s, p_b(v)) = E\left[\frac{p_s + p_b(v)}{2} - c \mid p_b(v) \geq p_s\right] \tag{11}$$

$$E_{\text{access}}(p_s(c), p_b) = E\left[v - \frac{p_s(c) + p_b}{2} \mid p_s(c) \leq p_b\right] \tag{12}$$

5.2 Bayesian Nash equilibrium

Because the above game is incomplete, we should solve Bayesian Nash equilibrium, where Bayesian Nash equilibrium is defined as follows: the strategic combination $(p_s^*(c), p_b^*(\mathrm{v}))$ is a Bayesian Nash Equilibrium if $p_s^*(c) = \max_{p_s} E_{accessed}(p_s, p_b(v))$ and $p_b^*(\mathrm{v}) = \max_{p_b} E_{\text{access}}(p_s(c), p_b)$. Next, we solve it.

According to statistical probability , we have the following formula:

$$\begin{aligned} p_s^*(c) &= \max_{p_s} E_{accessed}\ (p_s, p_b(\mathrm{v})) = \max_{p_s}\left[\frac{p_s + E[p_b(v)|p_b(v)\geq p_s]}{2} - c\right] Prob\{p_b(v) \geq p_s\} \\ &= \max_{p_s}\left(\frac{p_s}{2} - c\right)\left(1 - \frac{1}{\left(1+\frac{p_s}{\beta_b}^{\tau}\right)^{\alpha}}\right) + \frac{1}{2}\int_{\frac{p_s}{\beta_b}}^{U} \beta_b \frac{\alpha\tau x^{\tau}}{(1+x^{\tau})^{\alpha+1}} dx \end{aligned} \tag{13}$$

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

$$p_b^*(v) = \max_{p_b} E_{access}\ (p_s(c), p_b) = \max_{p_b} \left[v - \frac{p_b + E[p_s(c)|p_s(c) \le p_b]}{2} \right] Prob\{p_s(c) \le p_b\}$$
$$= \max_{p_b} \left(v - \frac{p_b}{2}\right) \left(1 - \frac{1}{\left(1 + \frac{p_b}{\beta_s}^{\tau}\right)^{\alpha}}\right) + \frac{1}{2} \int_0^{\frac{p_b}{\beta_s}} \beta_s \frac{\alpha \tau x^{\tau}}{(1+x^{\tau})^{\alpha+1}} dx \tag{14}$$

Since the integral part of Formula(13)and Formula(14) cannot be calculated, we convert it power series(the center of the series is equal to zero) as the approximate solution, gives.

For the accessed domain 's benefit function:

$$p_s^*(c) = \max_{p_s} \frac{p_s}{2} - c - \frac{p_s}{2\left(1 + \frac{p_s}{\beta_b}^{\tau}\right)^{\alpha}} + \frac{c}{\left(1 + \frac{p_s}{\beta_b}^{\tau}\right)^{\alpha}}$$
$$+ \frac{\tau \alpha \beta_b}{2} \left[\sum_{n=0}^{\infty} \frac{(-1)^n [(\alpha+1)(\alpha+2)\ldots\ldots(\alpha+n)]}{n!(\tau n + \tau + 1)} \left(U^{tn+\tau+1} - \beta_b^{\tau n+\tau+1}\right) \right] \tag{15}$$

For the accessing domain 's benefit function:

$$p_b^*(v) = \max_{p_b} v - \frac{p_b}{2} + \frac{p_b}{2\left(1 + \frac{p_b}{\beta_s}^{\tau}\right)^{\alpha}} - \frac{v}{\left(1 + \frac{p_b}{\beta_s}^{\tau}\right)^{\alpha}}$$
$$+ \frac{\tau \alpha \beta_s}{2} \left[\sum_{n=0}^{\infty} \frac{(-1)^n [(\alpha+1)(\alpha+2)\ldots\ldots(\alpha+n)]}{n!(\tau n + \tau + 1)} \left(\frac{p_b^{\tau n+\tau+1}}{\beta_s} - 0 \right) \right] \tag{16}$$

We can easily obtain its solutions of Formula (15) Formula (16) and use either bisection or Newton's method to get the equilibrium strategy of the accessed domain and the accessing domain.

6 Experiment Evaluation

In our experiment, three scales (i.e., large-scale, medium-scale and little-scale) of RBAC policies [21] are adopted to simulate the double auction in cross-domain collaboration. In the large-scale dataset, there are 1008 users ,314 roles and 34 role-specific SOD constraints; In the medium-scale dataset, there are 503 users ,137 roles and 17 role-specific SOD constraints; In the little-scale dataset, there are 10 users ,10 roles and 1 role-specific SOD constraint. To simulate our auction, we set the parameter of the Burr XII distribution to be $\alpha = 2$, $\tau = 5$ (the two parameters fit the actual value and cost distribution), $U = 0.8$(that is upper bound of cost and value), $\beta_s = 0.95$, and $\beta_b = 1.05$(i.e., about 5% gain).

Auction benefits: For each double auction, the benefits of the accessing domain and the accessed domain are defined as $\frac{p_s+p_b}{2} - c$ and $v - \frac{p_s+p_b}{2}$, respectively.Fig. 4 shows the total benefits of the involved domains over the number of auctions. From this figure, we can see that the benefits of the domain increase with the number of auctions.Thus, a rational and selfish domain actively takes part in conflict resolution.

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

Autonomy loss v.s. Interoperation: In this experiment, we compare autonomy loss and interoperation of our approach with Shafiq's approach [14]. In Shafiq's approach, to guarantee security, an autonomous domain has to set the upper bounds of the acceptable autonomy loss. In our experiment, the upper bound is set to 10 percent and 50 percent, respectively. For simplicity, we write the two schemes corresponding to the two parameters as 10%-autonomy-loss and 50%-autonomy-loss, respectively. Fig. 5 shows the autonomy loss and interoperation with the number of role mapping. From Fig. 5, we can see that the interoperation of our approach approximates or exceeds the interoperation of the 50%-autonomy-loss scheme, while the autonomy loss of our approach approximates or is lower than the autonomy loss of the 10%-autonomy-loss scheme. In other words, our approach can approximately achieve trade-off between maximizing interoperation and minimizing autonomy loss.

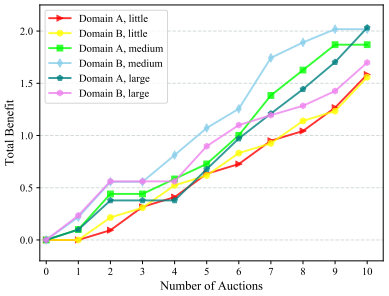

Fig. 4: Auction benefits

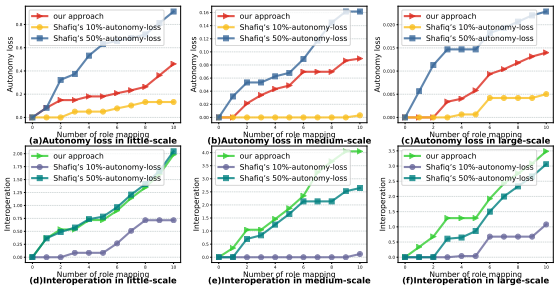

Fig. 5: Autonomy loss *v.s.* Interoperation

7 Conclusion

In this paper, we design an incentive mechanism to motivate domains to participate in conflict resolution. In detail, considering the selfishness and rationality of the involved domain,a game-theoretic approach is proposed to maximize their utility while achieving a tradeoff between security and interoperability. The simulation demonstrates the effectiveness of the conflict resolution approach.

References

1. Calistabebe, P., Akila, D.: Quantitative sørensen–dice indexed damgård–jurik cryptosystem for secured data access control in cloud. In: IOP Conference Series: Materials Science and Engineering. vol. 993, p. 012093. IOP Publishing (2020)
2. Chen, H.C.: Collaboration iot-based rbac with trust evaluation algorithm model for massive iot integrated application. Mobile Networks and Applications **24**(3), 839–852 (2019)
3. Cruz, J.P., Kaji, Y., Yanai, N.: Rbac-sc: Role-based access control using smart contract. IEEE Access **6**, 12240–12251 (2018)
4. Ding, K., Zhang, J.: Multi-party privacy conflict management in online social networks: A network game perspective. IEEE/ACM Transactions on Networking **28**(6), 2685–2698 (2020)

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43

5. Du, J., Jiang, C., Chen, K., Ren, Y., Poor, H.V.: Community-structured evolutionary game for privacy protection in social networks. IEEE Trans. Inf. Forensics Secur. **13**(3), 574–589 (2018)
6. Fang, L., Yin, L., Guo, Y., Wang, Z., Li, F.: Resolving access conflicts: an auction-based incentive approach. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). pp. 1–6. IEEE (2018)
7. Hu, H., Ahn, G.J., Zhao, Z., Yang, D.: Game theoretic analysis of multiparty access control in online social networks. In: Proceedings of the 19th ACM symposium on Access control models and technologies. pp. 93–102 (2014)
8. Huynh, N., Frappier, M., Pooda, H., Mammar, A., Laleau, R.: Sgac: a multi-layered access control model with conflict resolution strategy. The Computer Journal **62**(12), 1707–1733 (2019)
9. Ma, M., Stankovic, J.A., Feng, L.: Cityresolver: a decision support system for conflict resolution in smart cities. In: 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). pp. 55–64. IEEE (2018)
10. Mehregan, P., Fong, P.W.: Policy negotiation for co-owned resources in relationship-based access control. In: Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies. pp. 125–136 (2016)
11. Omar, I.Y., Laborde, R., Wazan, A.S., Barrère, F., Benzekri, A.: egovernment service security policy: obligation conflict resolution in xacmlv3. In: Proceedings of the International Conference on Security and Management (SAM). p. 89. The Steering Committee of The World Congress in Computer Science (2016)
12. Salehi, A., Rudolph, C., Grobler, M.: A dynamic cross-domain access control model for collaborative healthcare application. In: 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). pp. 643–648. IEEE (2019)
13. Samadian, H., Tuiyot, D., Valera, J.: Dynamic Programming Approach in Conflict Resolution Algorithm of Access Control Module in Medical Information Systems (2020)
14. Shafiq, B., Joshi, J.B., Bertino, E., Ghafoor, A.: Secure interoperation in a multidomain environment employing rbac policies. IEEE transactions on knowledge and data engineering **17**(11), 1557–1577 (2005)
15. Tadikamalla, P.R.: A look at the burr and related distributions. International Statistical Review/Revue Internationale de Statistique pp. 337–344 (1980)
16. Yahiaoui, M., Zinedine, A., Harti, M.: Deconflicting policies in attribute-based access control systems. In: 2018 IEEE 5th International Congress on Information Science and Technology (CiSt). pp. 130–136. IEEE (2018)
17. Yang, B., Hu, H.: Secure conflicts avoidance in multidomain environments: A distributed approach. IEEE Transactions on Systems, Man, and Cybernetics: Systems **PP**(99), 1–12 (2019)
18. Zeng, Q., Liu, C., Duan, H., Zhou, M.: Resource conflict checking and resolution controller design for cross-organization emergency response processes. IEEE Transactions on Systems, Man, and Cybernetics: Systems **50**(10), 3685–3700 (2019)
19. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the internet of things. IEEE Internet of Things Journal **6**(2), 1594–1605 (2018)
20. Zhu, H., Sheng, Y., Zhou, X., Zhu, Y.: Group role assignment with cooperation and conflict factors. IEEE Transactions on Systems, Man, and Cybernetics: Systems **48**(6), 851–863 (2016)
21. Zhu, T., Li, F., Jin, W., Guo, Y., Fang, L., Cheng, L.: Cross-domain access control policy mapping mechanism for balancing interoperability and autonomy. Journal on Communications **41**(9), 29–48 (2020)

ICCS Camera Ready Version 2021
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-77961-0_43