Privacy Access Control Mechanism for Online Social Network

[#]Ms. Sneha H. Pisey[1], [#]Prof. P.L.Ramteke[2], [*]Prof. Pranita Deshmukh[3] , [$]Prof. B.R.Burghate[4]
[#]*Dept of Computer Science & Engineering, H.V.P.M, College of Engineering & Technology, Amravati*
[*] *Dept of M.C.A PRMIT&R,* [$]*Dept. of Computer Science & Engineering, P.R.M.I.T&R Badnera*
Email ID: sneha.pisey@gmail.com, pl_ramteke@rediffmail.com, pranita.33deshmukh@gmail.com, bharatburghate@gmail.com

Abstract:

Online social networks (OSNs) have experienced tremendous growth in recent years and become a *de facto* portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Face-book and provide usability study and system evaluation of our method. The existence of online social networks that include person specific information creates interesting opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address some of the current limitations, we have created an experimental social network using synthetic data which we then use to test the efficacy of the semantic reasoning based approaches we have previously suggested.

Keywords: - Online Social Network, Security, Policy Specification and management.

1. Introduction

ONLINE social networks (OSNs) such as Face book, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs [1]. For example, Face book, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month [3]. To protect user data, access control has become a central feature of OSNs [2], [4]. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as wall in Face book, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload content into their own or others' spaces

but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Face book, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements [5]. It is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively in this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Based on these sharing patterns, a multiparty access control (MPAC) model is formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for OSNs

2. Proposed Work and Objectives:

In Proposed System we implemented a proof-of-concept Face book application for the collaborative management of shared data, called *MController*. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs [7]. Obversely, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model [8]. A proof- of-concept implementation of our solution called *MController* has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the *owner* of data, other controllers, including the *contributor*, stakeholder *and disseminator of* data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision [9].

3. Scope

On-line Social Networks (OSNs) are platforms that allow people to publish details about themselves and to connect to other members of the network through links. Recently, the popularity of OSNs is increasing significantly. For example, Face-book now claims to have more than a hundred million active users. The existence of OSNs that include person specific information creates both interesting opportunities and challenges. For example, social network data could be used for marketing products to the right customers. At the same time, security and privacy concerns can prevent such efforts in practice. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

4. Existing System

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content [6] in this paper; we pursue a systematic solution to facilitate

5. MULTIPARTY ACCESS CONTROL FOR OSNS: REQUIREMENTS AND PATTERNS

In this section we proceed with a comprehensive requirement analysis of multiparty access control in OSNs. If we consider the application is an access or, the user is a disseminator and the user's friend is the owner of shared profile attributes in this scenario**,**

a) Profile sharing: - demonstrates a profile sharing pattern where a disseminator can share others' profile attributes to an access or. Both the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes.

b) Relationship sharing: - shows a relationship sharing pattern where a user called owner, who has a relationship with another user called stakeholder, shares the relationship with an access or. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated.

c) Content sharing:- depicts a content sharing pattern where the owner of content shares the content with other OSN members, and the content has multiple state holders who may also want to involve in the control of content sharing. In another case, when Alice posts a note stating "I will attend a party on Friday night with @Carol" to Bob's space, we call Alice the contributor of the note and she may want to make the control over her notes

6. MPAC Model and policy

MODULE DESCRIPTION: Number of Modules After careful analysis the system has been identified to have the following modules [12]:

a) Owner Module

b) Contributor Module

c) Stakeholder Module

d) Disseminator Module

e) MPAC Module

a) Owner Module:

In Owner module let is a data item in the space m of a user u in the social network. The user u is called the owner of d. The user u is called the contributor of d. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

b) Contributor Module:

In Contributor module let d be a data item published by a user u in someone else's space in the social network. The contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor

c) Stakeholder Module:

In Stakeholder module let is a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u 2 T who has a relationship with another user called stakeholder, shares the relationship with an access or. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

d) Disseminator Module:

In Disseminator module let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been re-

disseminated, the original access control policies should be always enforced to protect further dissemination of the content.

e) MPAC Module:

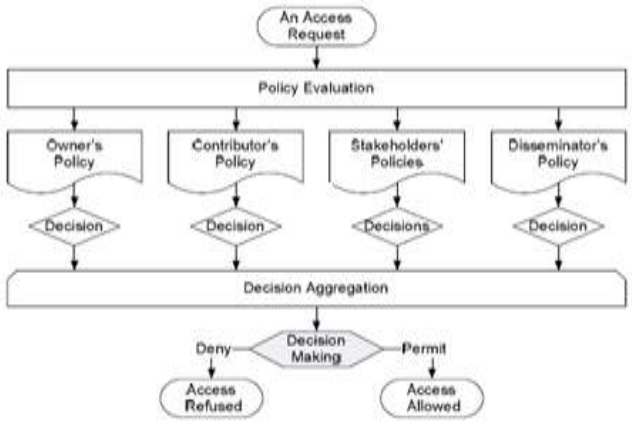
MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. Assessors Specification: Assessors are a set of users who are granted to access the shared data. Assessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

f) MPAC Policy

A multiparty access control policy is a 5-tuple *P =<controller; ctype; access or; data; effect >*, where • *controller € U* is a user who can regulate the access of *data*; • *ctype € CT* is the type of the controller; • *access or* is a set of users to whom the authorization is granted, representing with an access specification defined in Definition *data* is represented with a data specification defined in Definition and • *effect € {permit; deny}* is the authorization effect of the policy.

g) Privacy Policy Evaluation

Two step are perform for evaluation for access request model (MPAC)



Multiparty Policy Evaluation Process.

1. A voting scheme for decision making of multiparty control
2. Threshold-based conflict resolution
3. Strategy-based conflict resolution with privacy recommendation
4. Conflict resolution for dissemination control

7. IMPLEMENTATION AND EVALUATION

7.1 Prototype Implementation

We implemented a proof-of-concept Facebook application for the collaborative management of shared data; called *MController* .Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs. Obversely, our approach can be generalized to deal with other kinds of data sharing, such as videos and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. Figure shows the architecture of *MController*, which is divided into two major pieces, *Face book server* and *application server*. The Facebook server provides an entry point via the Face book application page, and provides. The application server is responsible for the input processing and collaborative management of shared data. Information related to user data such as user identifiers, friend lists, user groups, and user contents are stored in the application database. Users can access the *MController* application through Facebook, which serves the application in an iFrame. When access requests are made to the decision making portion in the application server, results are returned in the form of access to photos or proper information about access to photos. In addition, when privacy changes are made, the decision\making portion returns change- impact information to the interface to alert the user. Moreover, analysis services in *MController* application are provided by implementing an ASP translator, which communicates with an ASP reasoner.

Users can leverage the analysis services to perform complicated authorization queries. *MController* is developed as a third-party Facebook application, which is hosted in an Apache Tomcat application server supporting PHP and MySQL database. *MController* application is

based on the iFrame external application approach. Using the Javascript and PHP SDK, it accesses users' Facebook data through the Graph API and Facebook Query Language. Once a user installs *MController* in her/his Facebook space and accepts the necessary permissions, *MController* can access a user's basic information and contents. Especially, *MController* can retrieve and list all photos, which are owned or uploaded by the user, or where the user was tagged. Once information is imported, the user accesses *MController* through its application page on Facebook, where s/he can query access information, setprivacy for photos that s/he is a controller, or view photos s/he is allowed to access. A core component of *MController* is the decision making module, which processes access requests and returns responses (either permit or deny) for the requests. Figure depicts a system architecture of the decision making module in *MController*. To evaluate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the controller. Then, the decisions of all controllers are aggregated to yield a final decision as the response of the request. Multiparty privacy conflicts are resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for decision making. Otherwise, multiparty privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated sensitivity score is considered as a recommendation for strategy selection. Regarding the access requests to disseminated content, the final decision is made by combining the disseminator's decision and original controllers' decision adopting corresponding combination strategy discussed previously. A snapshot of main interface of *MController* is shown in Figure All photos are loaded into a gallery style interface. To control photo sharing, the user clicks the "Owned", "Tagged", "Contributed", or "Disseminated" tabs, then selects any photo to define her/his privacy preference by clicking the lock below the gallery. If the user is not the owner of selected photo, s/he can only edit the privacy setting and sensitivity setting of the photo.3 Otherwise, as shown in Figure, if the user is the owner of the photo, s/he has the option of clicking "Show Advanced Controls" to assign weight values to different types of controllers and configure the conflict resolution mechanism for the shared photo. By default, the conflict resolution is set to automatic. However, if the owner chooses to set a manual conflict resolution, s/he is informed of a sensitivity score of shared photo and receives a recommendation for choosing an appropriate conflict resolution strategy. Once a controller saves her/his privacy setting, a corresponding feedback is provided to indicate the potential authorization impact of her/his choice. The controller can immediately determine how many users can see the photo and should be denied, and how many users cannot see the photo and should be allowed. MController can also display the details of all users who violate against the controller's privacy setting (See Figure). The purpose of such feedback information is to guide the controller to evaluate the impact of collaborative authorization. If the controller is not satisfied with the current privacy control, s/he may adjust her/his privacy setting, contact the owner of the photo

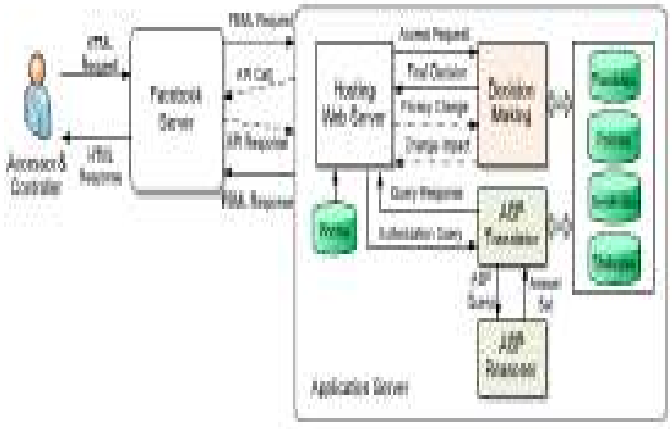


Figure a) Overall Architecture of MController Application

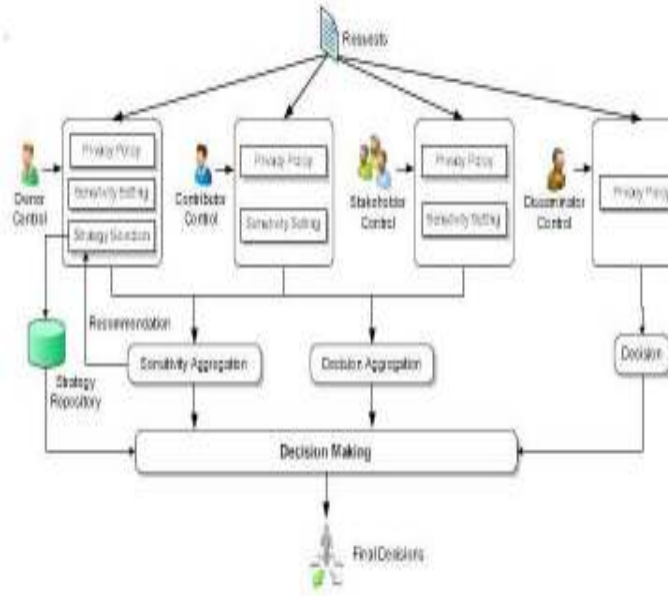


Figure b) Process Flow

7.2 System Usability and Performance Evaluation

7.2.1 Participants and Procedure

MController is a functional proof-of-concept implementation of collaborative privacy management. To measure the practicality and usability of our mechanism, we conducted a survey study (n=35) to explore the factors surrounding users' desires for privacy and discover how we might improve those implemented in MController. Specifically, we were interested in users' perspectives on the current Facebook privacy system and their desires for more control over photos they do not own. We recruited participants through university mailing lists and through Facebook itself using Facebook's built-in sharing API. Users were given the opportunity to share our application and play with their friends. While this is not a random sampling, recruiting using the natural dissemination features of Facebook arguably gives an accurate profile of the ecosystem. Before Using MController. Prior to using MController, users were asked a few questions about their usage of Facebook to determine the user's perceived usability of the current Facebook privacy controls. Since we were interested in the maximum average perception of Facebook, we looked at the upper bound of the confidence interval.

An average user asserts at most 25% positively about the likability and control of Facebook's privacy management mechanism, and at most 44% on Facebook's simplicity as shown in Table 1. This demonstrates an average negative opinion of the Facebook's privacy controls that users currently must use. After Using MController. Users were then asked to perform a few tasks in MController. Since we were interested in the average minimum opinion of MController, we looked at the lower bound of the confidence interval. An average user asserts at least 80% positively about the likability and control, and at least 67% positively on MController's simplicity as shown in Table 1. This demonstrates an average positive opinion of the controls and ideas presented to users in MController. Improvement. Besides viewing user opinions and analyzing the usability of our proof-of-concept application, we also briefly investigated the potential improvement of our application. The lowest score for MController is in the area of simplicity. On average, users found setting privacy settings for a photo more complicated in MController than Facebook. This means that while users appreciated the privacy controls of MController presented to them, it would be desirable to further simplify the process implemented in MController. This could be achieved by adopting learnbased generation of privacy settings for OSNs [10], [11].

7.2.2 Performance Evaluation

To evaluate the performance of the policy evaluation mechanism in MController, we changed the number of the controllers of a shared photo from 1 to 20, and assigned each controller with the average number of friends, 130, which is claimed by Facebook statistics [3]. Also, we considered two cases for our evaluation. In the first case, each controller allows "friends" to access the shared photo. In the second case, controllers specify "friends of friends" as the accessors instead of "friends". In our experiments, we performed 1,000 independent trials and measured the performance of each trial. Since the system performance depends on other There are O(n) MySQL calls and data fetching operations and O(1) for additional operations. Moreover, we could observe there was no significant overhead when we run MController in Facebook

TABLE 1
Usability Evaluation for Facebook and MController Privacy Controls

Metric	Facebook		MController	
	Average	Upper bound on 95% confidence interval	Average	Lower bound on 95% confidence interval
Learnability	0.20	0.25	0.83	0.80
Simplicity	0.38	0.44	0.72	0.64
Control	0.20	0.25	0.83	0.80

8. Scope & Objective

On-line Social Networks (OSNs) are platforms that allow people to publish details about themselves and to connect to other members of the network through links. Recently, the popularity of OSNs is increasing significantly. For example, Face-book now claims to have more than a hundred million active users. The existence of OSNs that include person specific information creates both interesting opportunities and challenges. For example, social network data could be used for marketing products to the right customers. At the same time, security and privacy concerns can prevent such efforts in practice. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

9. CONCLUSION

In this paper, we have proposed a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called *MController* has been discussed as well, followed by the usability study and system evaluation of our method. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time-consuming and tedious tasks. Therefore, we would study inference-based techniques [11] for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

10. Technical Challenges

SN sites are perfect for illegal online activities as they consist of a huge number of users with high levels of trust among them. As a result there is a high range of security risks, threats and challenges. SN sites provide some mechanisms for privacy settings to protect users, but these mechanisms are not enough to protect the users. The top and primary privacy problem is that SN sites are not informing users of the dangers of spreading their personal information. Thus users are not aware of the extent of the risks involved. The second problem is the privacy tools in SN sites, which are not easy to use and do not offer the flexibility for users to customize their privacy policies according to their needs. The third problem is the users themselves who cannot control what other users can reveal about them such as tagging their photos or related information to other friends' profiles

11. Reference

[1] Face book Developers.
http://developers.facebook.com/.

[2] Face book Privacy Policy.
http://www.facebook.com/policy.php/.

[3] A. Besmer and H. Richter Lipford. Moving beyond un-tagging Photo privacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563–1572. ACM 2010.

[4] B. Carminati and E. Ferrari. Collaborative access control in online social networks In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing

(CollaborateCom), pages 231–240. IEEE 2011

[5] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.

[6] L. Fang and K. LeFevre. Privacy wizards for social networking sites.In Proceedings of the 19th international conference on World Wide Web, pages 351–360. ACM 2010.

[7] P. Fong. Relationship-based access control: Protection model and policy language. In Proceedings of the first ACM conference on Data and application security and privacy, pages 191–202. ACM,2011.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11, pages 103–112. ACM, 2011.

[9] L. Jin, H. Takabi, and J. Joshi. Towards active detection of identity clone attacks on online social networks. In Proceedings of the first ACM conference on Data and application security and privacy, pages 27–38. ACM, 2011.

[10] A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel. You are who you know: Inferring user profiles in online social networks.In Proceedings of the third ACM international conference on Web search and data mining, pages 251–260. ACM, 2010.

[11] B. Qureshi, G. Min, and D. Kouvatsos. Collusion detection and prevention with fire+ trust and reputation model. In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, pages 2548–2555. IEEE, 2010.

[12] A. Squicciarini, F. Paci, and S. Sundareswaran. PriMa: an effective privacy protection mechanism for social networks. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pages 320–323. ACM, 2010.