Communications of the IIMA

Volume 11 | Issue 4 Article 5

2011

Provisional Access Control Model for Mobile Ad-Hoc Environments: Application to Mobile Electronic Commerce

Heechang Shin
Iona College

Donald Moscato
Iona College

Provisional Access Control Model for Mobile Ad-Hoc Environments: Application to Mobile Electronic Commerce

Heechang Shin
Iona College, USA
hshin@iona.edu

Donald Moscato
Iona College, USA
dmoscato@iona.edu

ABSTRACT

Role-based Access Control (RBAC) became popular because it can handle the complicated enterprise-wide access requests while traditional access control models such as mandatory access control and discretionary access control cannot. However, it is not suitable for a mobile environment because (i) there is no central trusted authentication entity that activates each user's roles, (ii) there are not many roles involved in such environment, and (iii) access control decisions depend on specific actions to be performed before the decision is taken. In this paper, we introduce a provisional authorization model with location-based predicates embedded in the policy specification languages. It includes three classes of location-based conditions such as position-based, movement-based, and interaction-based conditions. As a result, users can specify their own privacy/security policies in a mobile ad-hoc environment such as mobile auction markets.

Keywords: Access control policies; location-based services (LBS); mobile commerce; security/privacy; ad-hoc

INTRODUCTION

Mobile devices with wireless communication capabilities have become part of our lives. In a *mobile environment*, compared to the *static* desktop environment, network resources are constantly accessed through these devices while users are still moving. In this new mobile environment, it is easy to form a mobile ad-hoc network where neighboring mobile devices are forming a self-configuring network connected by wireless links. Examples include vehicular ad-hoc networks (VANETs) where neighboring vehicles communicate important information on road conditions or ride-share, social networks for finding friends, navigation advice in transportation, asset tracking, and mobile collaborative work. Especially, application to mobile electronic commerce is in our particular interests such as online ad-hoc auction market environment where auctioneers allow bidding from neighboring potential buyers.

In this environment, each mobile user is treated as a *peer* because one can retrieve data from one's neighboring mobile devices, and at the same time, one can provide the information as the

other people request the information that she brings. This *local search-and-discover* action is performed by each peer without connecting to the centralized server.

In order to protect one's own resources, each peer specifies its own security/privacy policies. In a mobile peer-to-peer environment, access control decision depends on *(i)* specific actions performed before the decision is taken and *(ii)* also *spatio-temporal* attributes. First, connection between peers is arbitrary; and thus, it would be more appropriate if the access control decision is based on the conditions that the resource-holding peer has. For example, in online ad-hoc auction market, an auctioneer allows bidding of only serious users who meet the criteria such as reading and signing the contract beforehand. Second, access control decisions are also based on current locations (i.e., spatial attribute) of neighboring peers within the specific time durations (temporal attribute). For example, in location-based services (LBS) applications, a mobile user wants to receive promotion deals only if the current location of the user is within a certain distance from the merchant during the evening hours in order not to be overwhelmed by spam mails from merchants.

The Role-based access control (RBAC) model is popular because it can handle complicated enterprise-wide access requests where the traditional access control models such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC) cannot handle. In RBAC, a role denotes a job function, and permissions to perform certain operations are assigned to specific roles instead of users. Then, each user is assigned to particular roles. Although facilitating resource sharing with enforcing security/privacy policies in a static environment has been discussed (Maruoka, Memati, Barolli, Enokido & Takizawa, 2008; Park, An, & Chandra, 2007; Park & Hwang, 2003; Ravichandran & Yoon, 2006; Silva et al. 2005), it is not applicable to a mobile ad-hoc environment due to the following reasons.

First of all, existing RBAC cannot be directly applicable to a mobile ad-hoc environment since peers are constantly moving over time and the policies are updated based on time and space. A naïve solution would use a trusted party which authenticates each user and makes an access control decision. However, this is not practical especially for mobile ad-hoc environment where participating peers are not predetermined and do not have the capability to connect to the central server. Also, it creates an issue with scalability of the system because the trusted server must be able to deal with all the access control requests and evaluates each peer's security policies. Considering the fact that these policies are based on space and time as well as specific actions that each peer has performed, overheads to the system to enforce these policies would not be scalable. Also, RBAC is not suitable because in such a context, there are not that many roles involved. As the word "peer" represents, in most cases, each user has the same privileges: for example, for file sharing environment, every user is authorized to access the contents as long as she has access to the system. Finally, in a mobile environment, the connection between peers is arbitrary, and thus, it would be more appropriate if the access control decision is based on the conditions that the resource-holding peer has. Usually, the conditions are specific actions that have been performed by the resource-requesting peers, and these specific actions as *provisions*.

Provisional authorization models have been proposed where an access control decision is based on the provisions of requesting users (Jajodia, Kudo, & Subrahmanian, 2001; Kudo & Hada,

2000). However, the generic provisional authorization model does not address the nature of the peer's mobility issues. Let us consider the following motivating example.

Motivating Example: Consider the situation of a mobile ad-hoc auction market. A mobile seller creates a mobile auction place for mobile customers who are within a shopping mall. Auction models consist of a set of business rules and security policies such as ending conditions and confidentiality of the bidding information (Jajodia et al., 2001). In a sealed-bid auction, submitted bids must be kept secret, and any submission after the closing time must be rejected. The provisional authorization model with support to location-based predicates deals with these security policies in a structured way. Bidders can submit their bids while within their stay at the shopping mall. The bidding information is kept secret because the seller encrypts the bidding data with a cryptographic key, and the system timestamps the bid. There are two kinds of participants: supplier and bidders. First, the supplier fills in the item to be auctioned, the closing time of the auction, and the minimum price acceptable. Then, the auction information is published in the mobile ad-hoc networks located within the shopping mall. Any mobile peer who is interested in the item can submit a bid specifying the item and a bidding price. This bidding information is accommodated if the bidding ending time is not reached, and the bidding price is higher than the current bidding price. The seller can fill-in "No Good" in the status field if the current time is after closing time and the maximum price of all the bids is lower than the minimum price.

In the mobile ad-hoc environment, security/privacy policies are spatio-temporal in nature as we discussed earlier: a peer is interested in the resources within the specific neighboring region and during a specific time interval without the actual knowledge of peers' identifiers. For example, in mobile electronic commerce, sellers are interested in the buyers who are currently located in the same shopping mall. In order to limit properly the control of resources, the provisional authorizations must incorporate the spatio-temporal specifications within its model. In this paper, we introduce the provisional authorization models with location-based predicates embedded in the policy specification language in order to support mobile ad-hoc environments. Therefore, security can be even enforced more powerfully and efficiently by using provisions and location predicates.

RELATED WORK

Jajodia et al. (2001) introduce provisional authorization model, where access is granted only if certain conditions are satisfied; and Bettini, Jajodia, Wang, & Wijesekera (2003) extend this idea by introducing obligations in addition to provisions. Here, provisions are conditions that must be satisfied (i.e., certain actions to be performed) before an access is granted; obligations are conditions or actions that must be fulfilled after the access decision. They proposed a rule-based framework to select the appropriate set of provisions and obligations based on numerical weights and on semantic relationships among them. More recent work (Dougherty, Fisler, & Krishnamurthi, 2007; Hilty, Pretschner, Basin, Schaefer, & Walter, 2007) investigate the use and enforcement of such obligations.

Although there have been quite number of research work for facilitating collaboration among distributed users, relatively few works have concentrated on controlling access to the mobile ad-hoc environment. Most collaborative systems give all participants the same rights to all objects, and expect that access issues will be controlled by a social protocol (Palomar, Tapiador, Hernandez-Castro, & Ribagorda, 2008). Generic access control models have been studied extensively in non-collaborative domains. Especially, RBAC model (da Silva, Gaspary, Barcellos, & Detsch, 2005; Maruoka et al., 2008; Park et al., 2007; Park & Hwang, 2003; Ravichandran & Yoon, 2006;) is popular because it can handle complicated enterprise-wide access requests where the traditional access control models cannot handle effectively. In this approach, the client/server scheme has been used for each access request. Each user request needs to connect to the server in order to acquire the access authorization. The main limitation is the feasibility since the server must handle all the access requests, which becomes the bottleneck of the system. Also, in the case of mobile P2P environments, it is insufficient to have role permissions based on object types.

Other researchers have proposed ways to incorporate the concept of trust to RBAC (Chakraborty & Ray, 2005; Ya-Jun, Fan, Qing-Guo, & Rong, 2005). The general idea in these works is that the access privileges of a user depends on his trust level. However, the applicability of these models to mobile environments remains to be investigated. For mobile environments, (Khambatti, Dasgupta, & Ryu, 2004) investigated role-based trust model in the context of digital libraries. Each peer keeps its own list of book profile that she wants to share with others. If this profile matches with someone who keeps the book, the information is used for sharing his or her book. However, the usage of role is limited because a role simply denotes the trustworthiness, which is different from the perspective of this paper since different roles may specify different policies. Trust based access control is developed in the context of a P2P file-sharing network. A peer has the right to download files from other peers, but a resource holding peer can control the prospective downloads of its file. However, the access control is determined by the trustworthiness and performance of peers instead of their roles. Thus, the model cannot classify peers with different functionalities. Recent work by (Toahchoodee, Abdunabi, Ray, & Ray, 2009) is close to our work. They proposed a trust-based RBAC model for pervasive computing systems. Users (humans or their representatives and devices) are evaluated for their trustworthiness, and roles are associated with a trust range indicating the minimum trust level that a user needs to attain before it can be assigned to that role. An access control request is granted for users whose trust level passes the minimum trust level. However, access control decision is still made in the central server, thus not applicable to the mobile ad-hoc environment.

Some cryptographic-based mechanisms have been suggested to solve the problem of content distribution (Dodis & Fazio, 2002; Eschenauer & Gligor, 2009; Fiat & Naor, 1997; Libert, Paterson, & Quaglia, 2012). They focus on cryptographic technique for implementing compliant authorized domains. A distributed access control model is addressed in (Lopez, Oppliger, & Pernul, 2004) through the idea of authentication and authorization infrastructures. However, since there is no control on what others can do and cannot through delegation, delegation may cause issues.

Our work is orthogonal to all of the above work because they are not applicable to a mobile ad-hoc environment, as they cannot support location-based conditions, and access control decisions depend on specific actions to be performed before the decision is taken rather than roles.

AUTHORIZATION MODEL FOR MOBILE AD-HOC NETWORKS

Traditional access control uses the model that a user makes an access request of a system in some context, and the system either authorizes the access request or denies it. However, today's rapidly expanding environments, such as electronic commerce, make such models that authorize or deny a request overly simplistic and not accommodating Jajodia and Wijesekera (2004). In this section, we introduce generic provisional authorizations and how location-based conditions are embedded in the provisional authorization models in order to support the mobile ad-hoc networks.

Provisional Authorization Models

This section introduces a provisional authorization model proposed by Jajodia and Wijesekera 2004. When clients submit an access request, the authentication module is invoked, which verifies if the user is the one that she claims to be. Then, the access request is provided to the provision evaluation module, which finds the conditions under which the requested access can be honored. Next, the condition under which the access may be granted is passed to an order specification module that yields a set of ordering constraints on the actions involved. Finally, the ordering constraints are handed off to a provision verification module to check if any conditions were previously fulfilled by the requester and, if so, simplifies the condition and waits for reduced conditions to be fulfilled by the requester before final authorization.

Representation of the Policy Rules: The security policy rules are written using a number of predicates, such as cando, do, and dercando (Jajodia & Wijesekera, 2004).

1. A ternary predicate cando(*o*, *s*, *a*), representing grantable or deniable requests where *o*, *s*, and *a* are object, subject, and a signed action term, respectively.
2. A ternary predicate dercando(*o*, *s*, *a*), with the same arguments as cando representing authorizations derived by the system using logical rules of inference.
3. A ternary predicate do, with the same arguments as cando, representing the access control decisions made by the system.
4. A propositional symbol error indicating violation of an integrity constraint.
5. The predicate in(*x*, *y*, "hierarchy name") is used to specify properties of subject and object hierarchies.

Representation of Provisions: Provisions are specified with the following form:
$\oint$: Head ← Body (1)
where $\oint$ is a predicate for provisions. Jajodia et al. introduce a provisional authorization specification language pASLL (Jajodia et al., 2001). pASLL is based on the declarative, polynomially evaluable authorization specification language ASL. The following set of rules model provisional accesses for an online store:

1. register(*s*, *customer*): cando(*items*, *s*, *+buy*) ← in(*contract*, *Contracts*)
2. upgrade(*s*, *prefCust*): dercando(*item*, *s*, *+buy*) ← cando(*item*, *s*, *+buy*)
3. payFees(*s*, $50): do(*item*, *s*, *+buy*) ← cando(*item*, *s*, *+buy*)
4. payFees(*s*, $40): do(*item*, *s*, *+buy*) ← dercando(*items*, *s*, *+buy*)

The first two rules allow a customer to purchase by registering and further allow the customer to upgrade her registration to a preferred customer. Next two rules state that the purchase price of an item is $50 for a non-preferred customer and $40 for a preferred customer. Therefore, a customer has the choice of either remaining in the non-preferred category with paying $50, or registering as a preferred customer and paying $40 per item (Jajodia et al., 2001).

Supporting Location-based Predicates

The provisional authorization model does not provide the location-based predicates within the model. Thus, it cannot handle the security policies where the location-based predicates are specified. Ardagna et al. 2006 proposed the location-based conditions that can be used in access control policies. The main advantage of the proposed model is that the model can be embedded in any currently available access control system to support location-based predicates without the necessity to introduce new specification languages. Also, the proposed model's stipulated location-based predicates are well defined.

The model proposes three main classes of location-based conditions:

- position-based conditions on the location of the user: for instance, to evaluate whether a user is in the proximity of other entities
- movement-based conditions on the mobility of the users such as their velocity, acceleration, or direction where they are headed.
- interaction-based conditions relating multiple users or entities: for instance, the number of users within a given area.

The location-based predicates are expressed as Boolean queries, and their evaluation returns a triple [bool_value, confidence, timeout]. The bool_value is based on either True or False if a user access request asks whether a user is located inside a given region. Because none of the current technology fully ensures the exact user location (Horsmanheimo, Jormakka, & Lahteenmaki, 2004), there exists uncertainty about location information. The confidence expresses the level of reliability that the location information is guaranteed to be accurate within the specified intervals. Also, the assessment (True or False) of the user request has a time validity interval specified by a timeout parameter.

The model includes the following predicates

- A position predicate inarea evaluates whether a user is located within a specific area.
- A position predicate disjoint evaluates whether a user is outside a specific area. Of course, disjoint is the equivalent to the negation of inarea.
- A position predicate distance evaluates whether the user lies within a given distance from the specified entity. The entity involved in the evaluation can be either stable or moving.
- A movement predicate velocity evaluates whether the user speed lies within a given range of

velocity.

- An interaction predicate density evaluates whether the number of users currently in an area lies within the interval specified.

Location-based Predicates	Evaluation Result	Description
inarea(Alice, Newark)	[True, 0.9, 2011-11-09_11:10am]	Alice is located in Newark with a confidence of 90%. Such an assessment is to be considered valid until 11:10am of November 11, 2011.
velocity(Alice, 70, 90)	[True, 0.8, 2011-11-03_03:00pm]	Alice is traveling at a speed included in the range [70,90] with a confidence of 80%.

Table 1: Examples of Location-based Predicates.

Table 1 shows the example of location-based predicates. The example presents position-type predicates and movement-based conditions.

Representation of Location-based Provisions

Location-based provisions are specified in the same way that non-location-based provisions do, which is shown in (1). It is important to observe that confidence plays a role for accuracy of user locations. Therefore, a threshold for confidence may need to be set up. Ardagna, Cremonini, Damiani, di Vimercati, and Samarati (2006) introduce the concept of an Extended True Table (ETT) for custom confidence thresholds for each predicate. For example, suppose the confidence threshold for the inarea predicate is [0.8, 0.9]. If the confidence is less than 0.8, the returned Boolean value is not confirmed, and the location-based condition is set to false. If the confidence level is above 0.9, then returned Boolean value is confirmed. If the threshold level is between 0.8 and 0.9, predicate re-evaluation is triggered because under the current threshold level, the returned value is not confirmed. The maximum number of tries is specified in order to prevent the deadlock situation.

Now, we have all the capabilities to specify the access control policies for mobile ad-hoc auction market. The following example is based on the work by (Jajodia et al. 2001), and we extend it by incorporating location-based provisions.

1. cando(*supplier_info*, *X*, *+rw*) ← in(*X*, *supplier*)
2. cando(*supplier_info*, *X*, *+r*) ← in(*X*, *bidder*) ^ inarea(*X*, *ShoppingMall*)
3. cando(*bid*, *A1*, *+r*) ← owner(*bid*, *A1*) ^ uid(*A1*)
4. encrypt(*Price*, *key1*)^timestamp(*Price*, *tsa1*): cando(*bidder_info*, *A1*, *+w*(*Price*)) ← not(done(*bidder_info*, *A1*, *+w*(*Price'*))) ^ uid(*A1*) ^ time(*T*) ^ field(*closing_time*, *A2*) ^ *T* < *A2*.
5. write(*winning_price*, -1): cando(*status*, *supplier*, *+w*("*No Good*")) ← current_top(*A1*) ^ field(*minimum_price*, *A2*) ^ *A1* < *A2* ^ *time*(*T*) ^ *field*(*closing_time*, *A3*)^*T* >= *A3*
6. write(*winning_price*, *A1*): cando(*status*, *auctioneer*, *+w*("*Completed*")) ← *current_top*(*A1*) ^ field(*minimum_price*, *A2*) ^ *A1* >= *A2* ^ *time*(*T*) ^ field(*closing_time*, *A3*) ^ *T* >= *A3*

The first two rules specify that the supplier can read and write any fields in *supplier_info* node, and the bidder who is in the shopping mall can read any fields in *supplier_info*. The third rule specifies that the bidder who submitted bid data can read her data. The forth rule specifies that if the bidder has not submitted a bid before the closing time of the auction is not reached, a bidder can submit a bid, if price is encrypted with time release key *key1* and timestamp from *tsa1* authority is recorded. The fifth rule specifies that if the maximum price of submitted bids is lower than the minimum price and the current time is after the closing time, the seller writes "*No Good*" in the status field in the *system_info* section, if error code is written in *winning_price* field. The last rule specifies that if the maximum price of submitted bids is equal to or greater than the minimum price and the current time is after the closing price, the supplier writes "*Completed"* in the status field in the *system_info* section, provided the highest price is written in the *winning_price* field.

DISCUSSION

We assume that the identification of a peer (user) is properly authenticated and its claimed location is properly verified . In the traditional static client/server architecture, the authentication procedure is rather standardized. However, in the mobile ad-hoc environment, it raises some issues with authentication. It mainly comes from the limited resources of mobile devices. Due to the mobile nature, the mobile devices will not necessarily be on-line to other networks except the mobile ad-hoc network. Therefore, in a typical case, a peer with resources does not have any prior knowledge about the peer who asks an access request. Thus, the authentication process is rather problematic.

Among the works to address this authentication problem in the context of mobile ad-hoc environment, DUMAS (Dynamic User Management and Access Control System) was an interesting solution by Fenkam, Dustdar, Kirda, Reif, & Gall (2002). There are two types of mobile peers: L1 peers (Peers of Level 1) and L2 peers. L1 peers are peers that maintain a security infrastructure. This includes the complete intelligence for assigning permissions, revoking permissions, and also providing authentication. To use a service protected by a L1 peer, a user must present his authorization certificates including his authentication information. L2 peers are devices lacking the resources for instantiating the full DUMAS engine. L2 peers utilize the power of L1 peers to verify authorization certificates related to the service it provides. Obviously, the main disadvantage of this architecture is that if an adhoc mobile network does not include L1 peers, authentication of consisting peers cannot be processed. However, with the reasonable number of L1 peers, the security of a system can actually work fine because at least one L1 peer in the adhoc network can provide the security environment for participating peers. However, this work does not address the location verification problem, which will be addressed in our future work.

CONCLUSION

Mobile ad-hoc environments are characterized by its local ad-hoc network formation, which can be used for searching for local resources of the users' interests. In most of cases, the local

resources are available during a limited duration of time and proximately located with the user. For example, the local search-and-discover, for example, can happen in many applications such as social networks for finding friends, navigation advice in transportation, mobile electronic commerce, asset tracking, and mobile collaborative work.

The main purpose of this paper is to develop an access control system for mobile ad-hoc environments. In this setting, each peer has its own security/privacy policies for protecting its resources. In this paper, we introduced the provisional authorization models with location-based predicates embedded in the policy specification languages. The mobile ad-hoc auction markets are used as a motivating example to explain the concept of the proposed model.

REFERENCES

Ardagna, C. A., Cremonini, M., Damiani, E., di Vimercati, S. D., & Samarati, P. (2006). Supporting location-based conditions in access control policies. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security (ACIACCS'06),* pp. 212-222. doi: 10.1145/1128817.1128850

Bettini, C., Jajodia, S., Wang, X. S., & Wijesekera, D. (2003) Provisions and obligations in policy rule management. *Journal of Network and System Management, 11*(3), 351-372. doi: 10.1023/A:1025711105609

Chakraborty, S., & Ray, I. (2006). TrustBAC: Integrating trust relationships into the RBAC model for access control in open systems. *Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, 49-58. Lake Tahoe, CA. doi: 10.1145/ 1133058.1133067

da Silva, J. F., Gaspary, L. P., Barcellos, M. P., & Detsch, A. (2005). Policy-based access control in peer-to-peer grid systems. *Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing.* Washington, DC, USA. doi: 10.1109/GRID.2005.1542731

Dodis, Y., & Fazio, N. (2002). Public key broadcast encryption for stateless receivers. In J. Feigenbaum, (Ed.), *Lecture Notes in Computer Science*: *Vol.* 2696. *Digital Rights Management* (pp. 61-80). Berlin, Germany: Springer-Vergal. doi: 10.1007/978-3-540-74835-9_25

Dougherty, D. J., Fisler, K., & Krishnamurthi, S. (2003) Obligations and their interaction with programs. In J. Biskup & J. Lopez (Eds.), *Lecture Notes in Computer Science: Vol. 4734. Computer Security: ESORICS 2007* (pp. 375-389). Berlin, Germany: Springer-Verlag. doi: 10.1007/978-3-540-74835-9_25

Eschenauer, L., & Gligor, V. D. (2009). *Method and apparatus for key management in distributed sensor networks*. *U. S. Patent No. US 7,486,795 B2*. Washington, DC: U. S. Patent and Trademark Office.

Fenkam, P., Dustdar, S., Kirda, E., Reif, G., & Gall, H. (2002). Towards an access control system for mobile peer-to-peer collaborative environments. *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, (WETICE'02)*, Washington, DC, USA, (pp 95-100). doi: 10.1109/ENABL.2002.1029995

Fiat, A., & Naor M. (1994). Broadcast encryption. In D. R. Stinson (Ed.), *Lecture Notes in Computer Science Vol. 773. Advances in Cryptology—Crypto'93* (pp. 480-491). Berlin, Germany: Springer-Verlag. doi: 10.1007/3-540-48329-2_40

Hilty, M., Pretschner, A., Basin, D., Schaefer, C., & Walter, T. (2007) A policy language for distributed usage control. In J. Biskup & J. Lopez (Eds.), *Lecture Notes in Computer Science: Vol. 4734. Computer Security* (pp. 531-546). Berlin, Germany: Springer-Verlag. doi: 10.1007/978-3-540-74835-9_35

Horsmanheimo, S., Jormakka, H., & Lahteenmaki, J. (2004). Location-aided planning in mobile network trial results. In A. Markopoulos, P. Eggers, & S. Ponnekanti (Eds.), *Wireless Personal Communications 30*(2-4), pp. 207-216. Berlin, Germany: Springer-Verlag. doi: 10.1023/B:WIRE.0000049400.25243.fd

Khambatti, M., Dasgupta, P., & Ryu, K. D. (2004). A role-based trust model for peer-to-peer communities and dynamic coalitions. *Information Assurance Workshop, 2004. Proceedings. Second IEEE International*, 141- 154. doi: 10.1109/IWIA.2004.1288044

Kudo, M., & Hada, S. (2000). XML document security based on provisional authorizations. In P. Samarati (Ed.), *Proceedings of the 7th ACM conference on computer and communications security*, pp. 87-96. New York, NY: ACM. doi: 10.1145/352600.352613

Jajodia, S., Kudo, M., & Subrahmanian, V. S. (2001). Provisional authorizations. In A. Ghosh (Ed.), *E-commerce security and privacy*, pp. 133-159. Boston, MA: Kluwer Academic.

Jajodia, S., & Wijesekera, D. (2004). A flexible authorization framework for e-commerce. In R. K. Ghosh & H. Mohanty (Eds.), *Lecture Notes in Computer Science: Vol. 3347. Distributed Computing and International Technology* (pp. 336-345). Berlin, Germany: Springer-Verlag. doi: 10.1007/978-3-540-30555-2_39

Libert, B., Paterson, K. G., & Quaglia, E. A. (2012). Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In M. Fischlin, J. Buchmann, & M. Manulis (Eds.), *Lecture Notes in Computer Science, Vol. 7293. Public Key Cryptography—PKC 2012* (pp. 206-224). Berlin, Germany: Springer-Verlag. doi; 10.1007/978-3-642-30057-8_13

Lopez, J., Oppliger, R., & Pernul, G. (2004). Authentication and authorization infrastructures (AAIs): A comparative survey. *Computers & Security, 23*, 578-590. doi: org/10.1016/ j.cose.2004.06.013

Maruoka, M., Nemati, A. G., Barolli, V., Enokido, T., & Takizawa, M. (2008). *Role-based access control in peer-to-peer (P2P) societies*. Paper presented at the 22nd International Conference on Advanced Information Networking and Applications: Workshops. Washington, DC, USA.

Palomar, E., Tapiador, J. M. E., Hernandez-Castro, J. C., & Ribagorda, A. (2008). Secure content access and replication in pure p2p networks. *Computer Communications, 31*, 266-279. doi: org/10.1016/j.comcom.2007.08.015

Park, J., An, G., & Chandra, D. (2007). Trusted P2P computing environments with role-based access control. *IET Information Security 1*(1), 27-35.

Park, J., & Hwang, J. (2003). Role-based access control for collaborative enterprise in peer-to-peer computing environments. *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, USA, 93-99. doi: 10.1145/775412.775424

Ravichandran, A., & Yoon, J. (2006). Trust management with delegation in grouped peer-to-peer communities. *Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, USA, 71-80. doi: 10.1145/1133058.1133070

Toahchoodee, M., Abdunabi, R., Ray, I. & Ray, I. (2009). A trust-based access control model for pervasive computing applications. In E. Gudes & J. Vaidya (Eds.), *Lecture Notes in Computer Science: Vol. 5645. Data and Applications Security XXIII,* (pp. 307-314). Berlin, Germany: Springer-Verlag. doi: 10.1007/978-3-642-03007-9_22

Ya-Jun, G., Fan, H., Qing-Guo, Z., & Rong, L. (2005, November). *An access control model for ubiquitous computing application*. Paper presented at the Second International Conference on Mobile Technology, Applications and Systems, Guangzhou, China

This Page was Left Blank Intentionally