Contextual Role-based Security Enhancement Mechanism for 2G-RFID Systems

Wan Tang*, Jin Ni†, Min Chen‡ and Ximin Yang*
* Computer Intelligence Lab, College of Computer Science, South-Central University for Nationalities, Wuhan, 430074 China
† School of Physics and Electronics, Henan University, Kaifeng, 475004 China
‡ School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074 China
E-mail: *{tangwan, yangximin}@scuec.edu.cn, †lilynee822@gmail.com, ‡minchen@ieee.org
Corresponding authors: Min Chen and Ximin Yang

***Abstract*—This paper investigates the use of second-generation radio frequency identification (2G-RFID) technology to enable better quality of service in future networks. With encoded rules as mobile codes stored in radio frequency identification (RFID) tags, the system extendibility and practicability can be effectively improved. However, due to the openness of the mobile codes, the realization of conveying intelligence brings a critical issue, i.e., how to prevent mobile codes from being misused or abused to avoid malicious attacks, which cause the disruption of backend systems. We address this issue by the use of role-based access control (RBAC) through introducing context-aware computing. Then, we propose a two-level security enhancement mechanism (2L-SEM), i.e., joint contextual-authentication-based and role-analysis-based secure middleware design. According to the given contextual restrictions in terms of time and location, the proposed mechanism filtrates illegal and invalid mobile codes contained in the RFID tags. Finally, a typical case study is given to illustrate the deployment of the proposed 2L-SEM within a 2G-RFID system. The experimental results show the effectiveness of guaranteeing the safe execution of mobile codes in the 2G-RFID system.**

***Keywords* RFID, context-aware computing, role-based access control**

I. Introduction

The Internet of Things (IoT) is intended to be rich in context awareness, realized by various object sensing and information gathering technologies, such as radio frequency identification (RFID), wireless sensor networks (WSNs), etc. As a main technology for conveying the terminal information of object identification, the RFID system is a main component of the IoT. The information stored in the RFID tag is intrinsically passive, static and non-intelligent in the traditional RFID system, which is referred as the first-generation RFID system (1G-RFID-Sys) [1]. Therefore, it neither suits the dynamics of the IoT environment, nor has the intelligent decision-making ability to enable smart services with quick response in IoT. Chen et al. proposed an evolution of a 1G-RFID-Sys to a second-generation RFID system [1], [2], or 2G-RFID-Sys, in which the RFID tags contain not only static information, such as object identification and description, but also "mobile code", which is a type of encoded procedural directive that is able to intelligently "notify" the system what operations or services should be provided in special occasions. The use of mobile code enables the 2G-RFID-Sys to be more extendible, reliable, and intelligent than the original 1G-RFID-Sys.

With encoded rules stored as mobile code in the tag, the capability of 2G-RFID-Sys is enhanced to act upon sensitive context changes and adapt services according to the dynamics of networks and end-user requirements. In the 2G-RFID reader, an identification filter (ID-filter), is used to check the ID information of tags. It provides security by maintaining a list of IDs that represents the validity of tags [1]. However, the security service provided by the simple ID-filter is limited, and a security enhancement mechanism should be designed to improve the security capability in the backend system (BS). In 2G-RFID-Sys, the security requirements have two aspects, namely, static information security and mobile code security. The dynamic information security, or mobile code security, means that the legal code is only executed by the authorized BS and evaluated in terms of validity.

Recently, research has been mainly focused on RFID data privacy protection which shows that well-used data security policies can guarantee static information security for low-cost passive tags. In addition, mutual authentication [3], light-weighted cryptographic algorithms [4], collision-resolution protocols [5], etc., can control RFID readers' access to tags, and hence, can ensure the integrity and credibility of tag information with minimum information leakage, and legality of tag owners. Zhou et al. proposed a smart RFID keeper (SRK), which controls reader's unauthorized access to tags based on blocking technology [6]. Canard et al. presented the first security model for RFID authentication/identification privacy-preserving systems [7]. Huang proposed an effective scheme to enhance the security and privacy about passive RFID tags [8]. Burstein et al. applied mobile agents to the highly dynamic and variable context of the healthcare emergency decision-support domain [9], however, location awareness was not implemented. These research is suitable for static tag information protection, but inefficient for eliminating potential security hazards in the 2G-RFID-Sys.

In the ubiquitous environment, applications are context-aware and use-centric. Context-aware computing is an ability of these applications to detect and react to the various environments [10]. Therefore, this paper introduces context-

aware computing to expand role-based access control (RBAC) and enhance the security mechanism. RBAC is an approach to restricting system access to authorized users, and is sometimes referred as role-based security [11]. RBAC allows policies to be specified in terms of subject roles, each of which can be viewed as a set of subjects with the same permissions, rather than strictly in terms of individual subject identities [12].

In this paper, we categorize tags by role, i.e., the users are categorized by role as one tag belongs to one user. In order to categorize tags in which the mobile code is stored, we actually divide users into different categories of roles. The role is typically determined by several context-aware kinds of information, e.g., time, location, and historic service that the mobile code requested. Based on the roles categorized according to contextual restrictions, this paper proposes a two-level security enhancement mechanism (2L-SEM) which operates in two phases, as follows:

- *Contextual authentication*: on the reception of a mobile code from the RFID reader, the information is verified in order to ensure it satisfy pre-existing rules based on contextual constraints in BS, where the code is interpreted, otherwise, it is refused to be executed. This phase can detect the mobile code written by the user who injects a virus code, rather than write a service code.
- *Role analysis*: though some intrusive users can replicate mobile codes that can pass through the authentication phase, the contextual information of the malicious user does not correspond to the role of the legal user, thus, the system can identify such malicious user to protect the legal user during this phase. Once the "immediate role" has conflict with the "profile-based role", the BS will prevent executing the code.

Based on the contextual restriction and the concept of role, the 2L-SEM-based system can prevent misuse and abuse of mobile codes, and eliminate illegal and invalid mobile codes for 2G-RFID-Sys.

The rest of this paper is organized as follows. In Section II, taking into account the location and time usability, the restrictions for mobile code usability are discussed in detail, in addition, the 2L-SEM is proposed. Section III describes and evaluates a distributed security solution for the 2L-SEM-based system through a special application case. Finally, our work is summarized in Section IV.

II. Two-Level Security Enhancement Mechanism

In this section, we first provide some presentations of the contextual restrictions, and then propose a two-level security enhancement mechanism (2L-SEM) based on expanded RBAC.

A. Contextual Restriction

To constrain the usability and validity of mobile code, this paper defines two types of contextual restrictions, i.e., location restriction and time restriction.

$d \rightarrow 0|1|2|3|4|5|6|7|8|9$
$year \rightarrow [* \mid d]^4$
$month \rightarrow [* \mid d]^2 :: \$month \neq *^2 \Rightarrow \$month \in [1..12]$
$day \rightarrow [* \mid d]^2 :: \$day \neq *^2 \Rightarrow \$day \in [1..31]$
$weekday \rightarrow 1|2|3|4|5|6|7[, weekday]$
$weekdays \rightarrow * \mid weekday$
$hour \rightarrow [* \mid d]^2 :: \$hour \neq *^2 \Rightarrow \$hour \in [0..23]$
$minute \rightarrow [* \mid d]^2 :: \$minute \neq *^2 \Rightarrow \$minute \in [0..59]$
$second \rightarrow [* \mid d]^2 :: \$second \neq *^2 \Rightarrow \$second \in [0..59]$
$Date ::= < year > - < month > - < day >$
$Time ::= < hour > : < minute > : < second >$
$DateTime ::= Date - weekdays - Time$

Fig. 1. Time variable construction grammar

1) Location Restriction: is the constraint for mobile code's location validity. In this paper, location validity indicates whether a mobile code can be activated, and is related to the present position of the RFID tag that maintains the mobile code and belongs to one user. That is to say, if the location is other than the user's usual location in a non-authorized area, the mobile code cannot be activated by any BS, even if the mobile code is authenticated and usable.

Let $\mathbb{C}_L$ be the location restriction set, if (1):

$$\forall m \in \mathbb{M}[\exists l \in \mathbb{C}_L \Rightarrow (m, l) \in \mathbb{M} \times \mathbb{C}_L] \quad (1)$$

is satisfied, mobile code m is available at location l. Thus, the location restriction function for the mobile codes in set $\mathbb{M}$ can be defined as (2):

$$\text{Location}(m \in \mathbb{M}) = \left\{ c \mid \wedge \left\{ \begin{array}{l} c \in \mathbb{C}_L \\ (m, c) \in \mathbb{M} \times \mathbb{C}_L. \end{array} \right\} \right. \quad (2)$$

It should be noted that the location restriction is independent to the specific location definition.

2) Time Restriction: is the constraint placed on the number of captured activated times and the activated time of a mobile code. A mobile code will not be activated when the captured time cannot satisfy the time restriction, or it has been activated more times than that allowed by the time restriction. There are two types of time restrictions, namely, continuous time and periodic time restrictions. If the activated time is constrained within a continuous time interval, it will treat the continuous time interval as a continuous time restriction, otherwise, if the activated time is aperiodic in a pre-given time interval, the period is a time restriction for the mobile code.

Prior to giving the definition of the time restriction, the time variable is defined based on a time pattern, which consists of some components (e.g., year, month, day, hour, second, etc.) and combination form (i.e., DataTime) of time variable. The time pattern is represented via the time variable construction grammar, as defined in Figure 1.

In the construction grammar, if the value of a field in a time variable is a "*" string, it means that the sub-variable can be an arbitrary legal value. Then, we define that a time range variable is an ordered pair $< t_1, t_2 >$ composed of

two time variables t_1 and t_2, and the time judging function InTimeRange is defined as follows:

$$\text{InTimeRange}(t^v, < t_1, t_2 >) = \begin{cases} \text{Ture} & t^v \geq t_1 \wedge t^v \leq t_2 \\ \text{False} & others \end{cases} \tag{3}$$

In (3), if the time variable t^v is within the time range $< t_1, t_2 >$, then the value of function InTimeRange is True; otherwise, it is False.

We denote by $Count$ the maximum times that a mobile code can be activated within a duration time, which is from time t_1 to time t_2. Therefore, according to the previous definition, where the time restriction consists of a maximum number of executed times and an activated time for the mobile code, the time restriction pattern for the mobile code can be denoted as $< t_1, t_2, Count >$. This paper also denotes by $\mathbb{C}_T$ the time restriction set. If (4):

$$\forall m \in \mathbb{M}(\exists c \in \mathbb{C}_T \Rightarrow (m, c) \in \mathbb{M} \times \mathbb{C}_T) \tag{4}$$

is satisfied, the mobile code m can be activated for at most $Count$ times within the given time range $< t_1, t_2 >$ under the time restriction c. Therefore, time restriction function of role r can be defined as (5):

$$\text{ActTime}(r \in \mathbb{R}) = \{c \mid c \in \mathbb{C}_T \wedge (r, c) \in \mathbb{R} \times \mathbb{C}_T\}. \tag{5}$$

B. Security Enhancement Mechanism

In this section, this paper categorizes different tags by role based on expanded RBAC, and designs a BS secure middleware, i.e. 2L-SEM, to ensure the usability and validity of the mobile code through two phases: contextual authentication and role analysis.

1) Contextual authentication: , authenticates the usability of mobile codes from the 2-FRID reader.

The usability is determined by several kinds of information about the mobile code, such as who wrote it, when and where it was written, and the valid period. Upon the reception of a mobile code, the information is verified to ensure the satisfactory of pre-existing rules based on the contextual constraints in BS. Achieved the authentication, the code is acceptable, otherwise, it is refused to be executed.

It is assumed that each role corresponds to a logical 2G-RFID tag group. The tags belonging to the same group play the same role and have similar mobile code sets, each tag can play one or more roles, and each role can be played by one or more tags. Permission for a role is the authorization of mobile code execution. Tags and mobile codes are associated through roles, and the relationships between these objects (i.e., tag, role, and mobile code) are many-to-many mapping. Let $\mathbb{T}$, $\mathbb{R}$, and $\mathbb{M}$ be a non-empty finite tag set, a non-empty finite role set, and a non-empty finite mobile code set, respectively. Let t be a tag, r be a role, and m be a mobile code. If (6) is satisfied, mobile code m maintained in tag t belongs to role r, and then it is valid to the BS.

$$\forall(t \in \mathbb{T} \wedge r \in \mathbb{R} \wedge m \in \mathbb{M})\exists[(t, r) \in \mathbb{T} \times \mathbb{R} \wedge (r, m) \in \mathbb{R} \times \mathbb{M}] \tag{6}$$

Thus, for corresponding mobile code usability, this paper formally defines a restriction model as a 5-tuple $(\mathbb{T}, \mathbb{R}, \mathbb{M}, \mathbb{C}, f)$ where $\mathbb{C}$ is a set of authorization and restriction rules, and is associated with the special application system, f is the mapping from the tag set $\mathbb{T}$ to the mobile code set $\mathbb{M}$ and constrained by $\mathbb{C}$. The constrained mapping f is described as follows:

$$f(t \in \mathbb{T}) = \{m \mid \exists[(r, m, c) \in \mathbb{R} \times \mathbb{M} \times \mathbb{C}][(t, r) \in \mathbb{T} \times \mathbb{R} \wedge (r, m) \in \mathbb{R} \times \mathbb{M}]\} \tag{7}$$

The location restriction set $\mathbb{C}_L$ and time restriction set $\mathbb{C}_T$ are both the subsets of $\mathbb{C}$.

2) Role analysis: , checks whether a mobile code of a tag is a legal and valid member of the role or not.

Even the mobile code goes through the authentication phase, the tag will be invalid or inactive for the system. For instance, if two users with the same tag IDs, are waiting for service requested by the mobile code in different locations at the same time, one of them is an invalid member of the role, and the BS should prevent executing the code, and any following communication cannot be activated.

Before describing the policy of role analysis in 2L-SEM, we categorize the tag state, which is used to indicate the tag's active state in the system, into three types (i.e., attendee, actor, and absentee). Let $\mathbb{T}$ denote a non-empty finite tag set, SoT denote the state of tag t, and then

$\text{SoT}(t \in \mathbb{T}) \in \mathbb{T}_{state} = \{attendee, actor, absentee\}$.

In this paper, expanding the role concept in RABC, we classify the membership of a role into three types, i.e., potential member (pMember), admissive member (aMember), and valid member (vMember). Let t be a tag, r be a role, and c be a contextual restriction rule maintained in BS. Assume the sets $\mathbb{R}$, $\mathbb{M}$, $\mathbb{T}$, and $\mathbb{C}$ are same as that defined in the 5-tuple restriction model. The three types of role membership are defined as follows.

$$\text{pMember}(r \in \mathbb{R}) = \{t \mid t \in \mathbb{T} \wedge (r, t) \in \mathbb{R} \times \mathbb{T}\} \tag{8}$$

$$\text{aMember}(r \in \mathbb{R}) = \left\{t \mid \wedge \begin{cases} t \in \text{pMember}(r) \\ \text{SoT}(t) = attendee \end{cases}\right\} \tag{9}$$

$$\text{vMember}(r \in \mathbb{R}) = \left\{t \mid \wedge \begin{cases} u \in \text{aMember}(r) \\ \text{SoT}(t) = actor \\ \forall(r, c) \in \mathbb{R} \times \mathbb{C} \Rightarrow t \prec (r, c) \end{cases}\right\} \tag{10}$$

where $t \prec (r, c)$ means tag t satisfies restriction c of role r.

Tag t, a potential member of role r, is an admissive member of role r only when it is an attendee of the system. While its state is $actor$ and its information matches the restrictions of role r, tag t will be a valid member of role r, and go through role analysis, as described by (11).

$$\begin{aligned} \text{Member}(r \in \mathbb{R}) = \text{aMember}(r) \cup \text{vMember}(r) \\ \subseteq \text{pMember}(r) \subseteq \mathbb{T} \end{aligned} \tag{11}$$

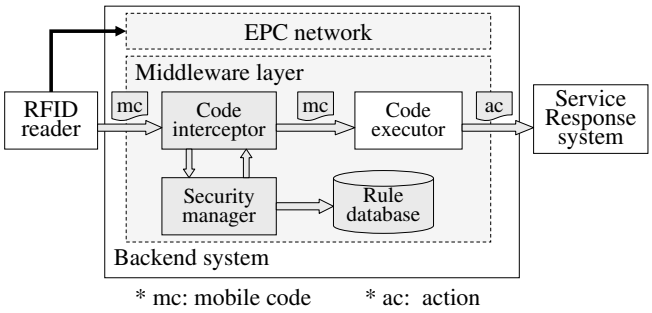


Fig. 2. Reference architecture for 2L-SEM-based system

III. Reference Architecture and Its Application

In this section, a 2L-SEM-based reference architecture is designed for 2G-RFID-Sys. In addition, a highway speed detection system is provided as an application case to illustrate how the proposed 2L-SEM can be applied and how it provides guaranteed security.

A. Reference Architecture

The given 2L-SEM-based reference architecture for the 2G-RFID-Sys is shown in Figure 2. A code interceptor is responsible for constructing audit requests relied on the context of a mobile code, which is delivered from an RFID reader, and applies these audit requests to the security manager. Then, the security manager will operate our security enhance middleware, i.e. 2L-SEM, to make a judgment regarding the request by searching the authorization and restriction rules stored in the rule database. If an authority exists and the request is in accordance with the rules, then the security manager returns a permission message, otherwise, it denies the request of the mobile code execution. When the code interceptor receives a permission massage sent by the security manager, the corresponding mobile code will be forwarded to the code executor which is coresponding to the middleware layer in the original 2G-RFID BS.

B. System Instance

In the highway management application, the 2G-RFID tag is carried by a vehicle, which is a private car but not an ambulance, stores a mobile code MC_001: "emergency: on". While the car is passing through an speed detection point equipped with an RFID reader on the highway, the availability of the mobile code stored in the tag and delivered to a BS by the reader, decides whether the BS can interpret and execute the mobile code, and then, provide corresponding service or action.

in Table I, some examples are given to illustrate the mapping relationship between the subject combination and the time restriction combination, the former includes three items: tag, role, and mobile code. More tags (e.g., Tag_001 and Tag_002) with different rule sets are both playing the same role Private Car, and the same mobile code (e.g., MC_001) is carried by different roles (e.g., Private Car and Ambulance). The time restriction combination consists of the time variable $StartTime$, time variable $EndTime$, maximum activated times, and duration time. The mobile code can be activated within a time range $<$ *StartTime*, *EndTime* $>$. However, if the value of $StartTime$ is Null, the activated time range is $< t_w$, *EndTime* $>$, where t_w is the time when the code was written in the tag. Furthermore, if the value of $EndTime$ is also Null, the mobile code can be activated within the time range $< t_w, t_w + EndTime >$. Finally, if the value of Duration time is 0, the mobile code can be activated at anytime.

As shown in Table I, if the tag is carried by a private car, MC_001 can only be activated during six hours; however, it is available at anytime if it is stored in an ambulance tag. The driver of a private car is subject to an emergency situation while transporting a pregnant woman to the hospital, and then mobile code MC_001 is written in the tag carried by the car at 5:15 am in Nov. 30, 2010. After one day, the car passes over a speed detection point. The mobile code is delivered to the BS of the highway speed detection system based on 2L-SEM, where it goes through the authentication phase. However, MC_001 cannot be activated since it is only a private car, but not an ambulance, and its duration time has been exceeded six hours.

C. Performance Evaluation

In order to evaluate the proposed 2L-SEM, we established a simulation platform for the 2L-SEM-based highway speed detection system using SimJava 2.0 [13]. In the platform, the time interval of tags arriving at the reader follows an exponential distribution with mean *r*. The number of mobile codes in each tag, n_t, is in the uniform distribution on the interval [0, 20]. For a mobile code, the average server time of the rule database, t_d, obeys the exponential distribution with mean 0.2, and the average execution time of code executor t_e is 1ms. The number of mobile codes provided by system n_m is 100, and the ratio of authenticated mobile codes p_a is 90%.

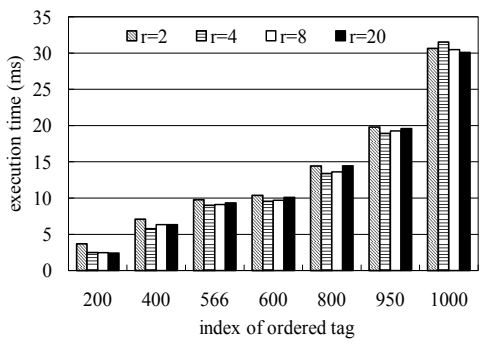
We ran the simulation four times with different tag time intervals with mean *r*(=2s, 4s, 8s, 20s), and then evaluate the performance in terms of tag execution time, average tag processing time, and rate of mobile codes execution, with the results shown in Figure 3.

First, we index the tags by their execution time. The execution time consumed in code executor of seven tags are given in Figure 3a. Based on the reference architecture given in Section II-A, in all the four cases with different tag time intervals, the average execution time of tags should be $((20/2)p_a t_e =)$9ms, and the maximum execution time of tags should be $(20t_e =)$20ms. In Figure 3a, 95% tags and 56.7% tags are executed within 20ms and 9ms, respectively. This application case can achieve the design performance, that is to say, the tag execution time of the system can be achieved via setting system parameters.

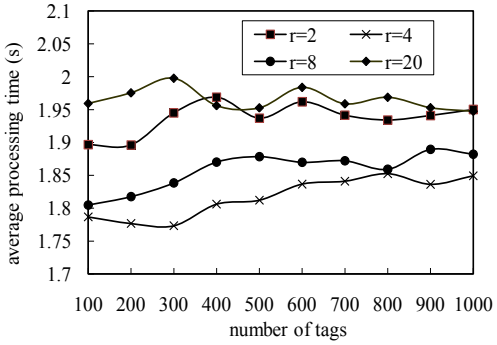
Hence, the efficiency of BS authorization and mobile codes filtering in the 2L-SEM-based system is surveyed in terms of average processing time that a tag spends in the code interceptor and security manager, and the results are illustrated in Figure 3b. As the number of tags increases, the average tag

TABLE I
MAPPING RELATIONSHIP BETWEEN SUBJECT AND TIME RESTRICTION

Tag	Role	Mobile code	StartTime	EndTime	Max activated times	Duration time
Tag_001	Private Car	MC_001	Null	Null	0	6 hours
Tag_002	Private Car	MC_002	Null	2012-12-31-*-12:59:59	0	0
Tag_003	Ambulance	MC_001	Null	Null	0	0
Tag_004	Ambulance	MC_002	2010-9-1-*-00:00:00	2010-10-31-*-12:59:59	0	0



(a) Distribution of the tags execution time



(b) Average tag processing time

Fig. 3. Performance of the 2L-SEM-based highway over-speed detection system (r: the mean of the interval time of tags)

processing time approaches 1.9s, which is approximating the average server time of the rule database, It is obvious that the efficiency of the 2L-SEM-based system is decided by the processing time of the rule database.

IV. CONCLUSION

The scalability and flexibility of 2G-RFID-Sys will support more intelligent applications in the future. How to prevent mobile codes from being misused or abused and avoid malicious mobile codes is a critical issue of 2G-RFID-Sys. To address this issue, this paper made the following major three contributions, the first is providing the presentations of two types of contextual restrictions (i.e., location restriction and time restriction), which are used to represent the set of authorization and restriction rules for special application system; the second is the proposal of a 2-level security enhancement mechanism for the 2G-RFID-Sys, achieved by expanding the restraint polity of RBAC; and the third is the design of the reference architecture based on the proposed mechanism. In addition, this paper provided an application case to illustrate and verify how the proposed mechanism can provide intelligent and secure information processes for the 2G-RFID-Sys.

V. ACKNOWLEDGMENT

This research was supported by the Special fund for Basic Scientific Research of Central Colleges (ZZZ10003), South-Central University for Nationalities, China.

REFERENCES

[1] M. Chen, S. Gonalez, V. Leung, and Q. Zhang, "A 2G-RFID-based ehealthcare system," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 37–43, Feb. 2010.

[2] M. Chen, S. Gonzalez, Q. Zhang, and V. Leung, "Code-centric RFID system based on software agent intelligence," *Intelligent Systems, IEEE*, vol. 25, no. 2, pp. 12–19, Mar. 2010.

[3] F. Armknecht, A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "On RFID privacy with mutual authentication and tag corruption," in *Applied Cryptography and Network Security*, ser. Lecture Notes in Computer Science, J. Zhou and M. Yung, Eds. Springer Berlin / Heidelberg, 2010, vol. 6123, pp. 493–510.

[4] S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-tagged systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 38, no. 3, pp. 360 –376, May. 2008.

[5] D. H. Shih, P. L. Sun, D. C. Yen, and S. M. Huang, "Short survey: Taxonomy and survey of RFID anti-collision protocols," *Computer Communications*, vol. 29, no. 11, pp. 2150–2166, 2006.

[6] Z. Zhou and D. Huang, "SRK: A distributed RFID data access control mechanism," in *Communications, 2008. ICC '08. IEEE International Conference on*, Beijing, China, May 2008, pp. 2854–2858.

[7] S. Canard, I. Coisel, and M. Girault, "Security of privacy-preserving RFID systems," in *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, Guangzhou, China, June 2010, pp. 269–274.

[8] M. Rieback, B. Crispo, and A. Tanenbaum, "Keep on blockin' in the free world: Personal access control for low-cost RFID tags," in *Security Protocols*, ser. Lecture Notes in Computer Science, B. Christianson, B. Crispo, J. Malcolm, and M. Roe, Eds. Springer Berlin / Heidelberg, 2007, vol. 4631, pp. 51–59.

[9] F. Burstein, A. Zaslavsky, and N. Arora, "Context-aware mobile agents for decision-making support in healthcare emergency applications," in *Proceedings of the 1st Workshop on Context Modeling and Decision Support*, 2005, pp. 1–16.

[10] L. Barkhuus and A. Dey, "Is context-aware computing taking control away from the user? three levels of interactivity examined," in *In Proceedings of Ubicomp 2003*. Springer, 2003, pp. 149–156.

[11] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[12] M. N. Tahir, "Hierarchies in contextual role-based access control model (C-RBAC)," *International Journal of Computer Science and Security*, vol. 2, no. 4, pp. 28–42, 2008.

[13] ICSA, "Simjava 2.0," *http://www.icsa.inf.ed.ac.uk/research/groups/hase/simjava*, Aug. 2010.