Applying RBAC Security Control Model to Manufacturing and Logistics Service Platform

Moon Sun SHIN[1], Yong Wan JU[2], Hyun Kyu Kang[1], Seon Phil JEONG[3]

[1] Dept. of Computer Engineering, Konkuk University,
268 Chungwon-daero, Chungju-si, Chungbuk, 380-701, Republic of Korea,
msshin@kku.ac.kr (*Corresponding Author*); hkkang@kku.ac.kr.

[2] Division of Industry Development, Korea Internet & Security Agency,
Songpa-gu, Seoul,138-950, Republic of Korea,
ywju@kisa.or.kr

[3] Division of Technology and Science, BNU-HKBU United International College,
China,
spjeong@uic.edu.hk

Abstract: The recent RFID-based logistics environment enables significant improvement of business efficiency. However, to support an efficient logistics processing service in the RFID-based international logistics service platform, it is required security risk analysis and security control model. In this paper, we have analyzed and figured out requirements of the security for the efficient international RFID-based logistics service. It is possible to construct own security policy for each enterprise using RBAC. The security policy includes definition of subjects, objects, permissions, roles, role hierarchy and constraints of the enterprise. And we proposed an RBAC-based security control model, reflecting security requirements in an international logistics process and constraints of the access control model have been represented as UML. We presented example scenario and implemented the prototype system for the verification of the proposed security model for international logistics. The proposed security control model is useful to reduce business risk in international logistics.

Keywords: RFID, International Logistics, RBAC, Security Control, Access Control Constraints.

1. Introduction

The RFID (Radio Frequency Identification) system uses wireless telecommunication technology, making it feasible to identify RFID tag information without direct contact. Therefore, it has more advantages than the previously used bar code system. In other words, it is possible to read multi-tags at a time, by using frequency, without having to have direct contact with the tag. Due to such an advantage of RFID, it is now being generalized to apply so-called customized services, which can manufacture and deliver products based on diverse requirements from customers, by utilizing RFID. Various business solutions based on RFID are appeared and optimized for SCM (Supply Chain Management) [1]. It is now feasible to acquire visibility of the flow of products, in the course of manufacture, or a distribution system. Using RFID improves work efficiency, and enables more effective management of stocks and tracing of products in overall logistics movement. A further advantage is offered, in that the level of integrity can be enhanced, while reducing the loss rate of the product [2, 3]. However, a priority is to solve the issue of security of logistics information for an efficient logistics processing service in the RFID-based international logistics service platform. Security policies and privacy issues need to be addressed, as diverse types of threat occur, based on characteristics of the RFID-based logistics environment, including piracy, location tracing, and physical attack, as well as threats to the security of product information.

These threats serve to impede the development and distribution of technology for the management of the RFID technology-based logistics environment. EPCglobal Network provides standards for the structure, meaning and delivery method of RFID tag information [2]. And each company manages all the information derived from the EPCglobal Network. Here, EPCglobal Network is able to enhance efficiency of the delivery and dispersed management of EPC (Electronic Product Code) information, but is not capable of removing all of the threatening factors.

In this paper, we propose an RBAC-based security control model in order to protect and guarantee the integrity of products and reliability of the international logistics service platform based on RFID.

RBAC based security model can be used in the architecture of the EAF(Enterprise Application

Framework) for each enterprise to construct its own security policy such as roles, permissions, sessions and constraints of the organization. Existing RFID-based international logistics platforms could become exposed to threats and security risks. Therefore we need flexible security control model for the protection of not only RFID threats but also enterprise level risks. RBAC is a powerful and flexible security access control model. So it can be applied to solve these problems.

The rest of the paper is organized as follows. Section 2 describes the security guideline of the RFID system. We explain requirements of security in the EPC network application service based on RFID in section 3 and figure out security analysis in section 4. In section 5, we propose an RBAC-based security control model for the international logistics process and represent constraints of access control using UML. And section 6 contains example scenario and implementation of the proposed security model. Lastly a brief conclusion is presented in section 7.

2. Related Works

The EPCglobal architecture framework is to be serviced for a mutual goal that intensifies the distribution/supply network by using EPC. EPCglobal network is a system that grants an identification number on a product based on RFID technology and EPC code, and conveys information related to the product for suppliers and consumers, by connecting a storage space of information into the network. In other words, EPCglobal network serves as a standard that makes it feasible to collect more than one EPC data from multiple-data resources, such as RFID reader, and report them in diverse form, by filtering and grouping them according to customized order from consumers, and to store data processed on the EPC IS (Information Services). EPCglobal network provides independence between application business logics and infrastructure components.

In various fields of application, an RFID application system operating based on the EPCglobal network is applicable on the basis of an Inter-Enterprise Architecture frame, as shown in Figure 1. Regardless of being a form of open network or closed network, the basic structure operates as an application service, through connection with an enterprise subsystem [1, 2].

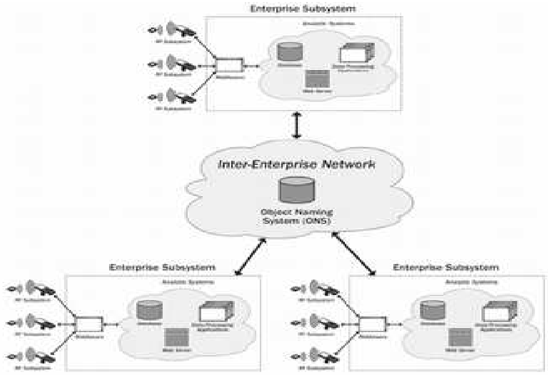


Figure 1. Inter-Enterprise Architecture of RFID-based EPCIS (from NIST report)

The security control in EPCglobal security guideline is designed in order to reduce business risk related to the RFID system [3]. System management for security control indicates a policy required for RFID system management and maintenance for security, and this is related to risk evaluation, system design, and system certification, etc. In other words, important data, such as personal information, should be stored in the enterprise subsystem, instead of a tag, and be searchable by using the tag ID. Only an authorized person is eligible to access this. Therefore, in terms of costs, encryption and access control are more efficient to be implemented on the enterprise subsystem, rather than on the RF subsystem. However, if using an identifier of EPC format that has already been exposed, attackers might be able to intercept important information, and the enterprise subsystem also faces the risk of being exposed to attack on data through a network.

Security control and security policy involved with an RFID subsystem, network, and database, must allow only pre-approved roles of individuals and organizations on a RFID system operation. Protection of peripherals and subsystem that contain access control, port, and protocol of RFID, password management, RFID security education, and cipher system management, are all related to security policy. Therefore, this policy is applicable for realization of an RFID system that is related to the enterprise subsystem.

The most general technical parts of security policy for a subsystem of the RFID system are password, authorization of key-hash message, and digital signature.

Examples of risk factors of attack are unauthorized reading, writing, tag copying, user spoofing, RFID physical destruction, and unjustified behavior involving the servicing of unapproved commands. The advantage of policies for physical access control designed in order to prevent them, is that it enables to limit the possibilities of attack approaching the RFID system components. However, there exist weaknesses of attack from inside or attack of frequency interruption.

In addition, installing tags and readers in a proper location can avoid risk and interruption of electromagnetic radiation. It should be noted that users should be properly educated, to be familiar with knowledge and skills of security, how to identify unauthorized usage, and where to report, if they detect violation, etc.

Access control has many advantages to manage security control related on integrity, availability and confidentiality. Traditional access control includes MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role based Access Control). RBAC is very useful and can be applied various applications.

3. Security Requirements of an RFID System

An RFID system consists of tag, reader, server (middle-ware and application service platform), and is used by connecting with a wire/wireless telecommunication network. A tag is located on the network with information that enables subjects to be identified, and a reader collects, processes, sends, and receives information of subjects. The server implements an application process, by utilizing information of the subjects. In this chapter, it is intended to describe the security risk of tag, reader, and antenna that are major components of an RFID system, and requirements of security that specifically consider them.

3.1 Tag security

A specific password is granted on the tag for authorization, as a security control measure for a tag that contains basic product code information. A password should be assigned to each tag, since it might be used for physically protecting an ambient environment to prevent wire-tapping. In addition, different passwords should be designated between tags, to prevent them from being shared. Encryption of data is required, along with assignment of a password on the tag prior to storing data on the tag, for safety issues. In other words, it is required to prepare a measure to prevent authorized users from reading real data, if the password is somehow revealed allowing them access to the tag, by encryption of data.

It should be noted that temporary turn-off is required for the tag not suffering from frequent exchange between the reader and RF interface. This can serve as a method for reducing the risk of wire-tapping or attacks. However, such a temporary method can only be applied if it is possible to predict the number of exchanges between the tag and reader. As a particular method, it is feasible to deactivate the tag, followed by activating it once the switch turns on, so that the RF and tag can proceed with an exchange with each other. Care should be taken that the reader should perform monitoring on the tag that is continuous, and operated to immediately identify unauthorized access and unexpected data exchange

The radio frequency that transmits and receives signals related to the tag, along with such a tag security control, is related to the operation range, speed, and data transmission rate of the tag. Therefore, the movement of tags, followed by the range of operation, feasibility of frequency crash, and frequency changes, should be specifically considered.

3.2 Reader security

Standards should be followed for communication between the reader and tag. In general, a tag and reader from the same vender are generally used. There are two types of reader, wired readers and wireless readers. A wired reader is installed at a fixed location, reading the tag by accessing the reader. An example of this is the unmanned signal violation camera. The wireless type of reader is movable. All the readers have RF subsystems and interface that can communicate with the RF subsystem and enterprise subsystem, respectively. The enterprise subsystem interface supports a transmission of RFID data from the reader to a computer of the enterprise subsystem for analysis and processing.

Each reader has an acceptable power output and duty cycle. The duty cycle represents a percentage (50%, if communicating for 30 seconds in a minute) of a certain amount of time that a device emits energy. A reader communicating with manual tags requires much higher power output, than one communicating with automatic tags. A reader having a strong duty cycle is eligible to accurately read a tag from a more remote distance. However, care has to be taken on overwhelming power, which might increase the risk of wire-tapping.

In general, a reader is able to communicate with tags by using various types of antenna. In particular, detachable antennas are appropriate for selective use, depending on the requirements of the reader. Therefore, a specific communication method of tags and antennas should be understood and considered, based on the characteristics of the antenna. In addition, if multiple tags are adjacent to each other, the reader should be able to identify and process a particular tag. When a reader sends an inquiry to a specific tag, the reader should not receive a response from multiple tags at the same time. In other words, a tag should respond only if it conforms to a randomly assigned number, while the reader should make sure that there are no tags causing conflicts, and not communicate to those tags with information.

3.3 Antenna security

The most general method of security control for antennas that receive signals coming from the tag is to use a fragile antenna. This is a method of RFID tag that an antenna causes a malfunction, to prevent attackers from modifying, revising, forging or removing a tag, by making it unavailable for them to access a tag in the first place.

In addition, a proper radio frequency should be selected, depending on the business application for the use of the antenna. Using fixed frequency is a way of efficiently reducing a risk of interruption or conflicts of wireless signals.

A RF system operator is able to adjust the RF energy level transmitted from the reader or active tag, and to prepare for the security. In other words, some types of antenna are specifically designed to adjust the direction of RF energy that has been transmitted, which is a feasible means of preparing for the security. In addition, it is to prepare a measure for installing an electromagnetic shielding device on a range of electromagnetic wave regarding an antenna, and to restrict it. It is an important issue to block movements of antennas from outside, by preventing RF signals from being transmitted into a non-protected area.

Considering such security factors of the antenna, it is feasible to minimize interruption of other electromagnetic waves, and to reduce the risk of wire-tapping, by selecting a specific antenna that meets the requirements of the reader, and entails a wide enough range for communication with the tag.

3.4 Security requirements of network

Security requirements should be specifically considered for the RFID enterprise subsystem and enterprise system that constitute the EPCglobal network to deal with a security threat, in order to provide a reliable and safe international logistics service platform.

Basically, the RFID system should protect privacy and network security. A security mechanism that guarantees non-disclosure, integrity, fusibility, undeniable issue, and certification is required, and is inevitable in each session of information flow. Figure 2 presents the data flow of an RFID enterprise subsystem, and indicates the requirements of security that are to be followed. Security technologies, including certification skills between RFID tag and reader, symmetry-key for transmitting or receiving data in a safe manner between tag and reader, and key management, such as the use of a public key, is required for network security for privacy protection entailing prevent wire-

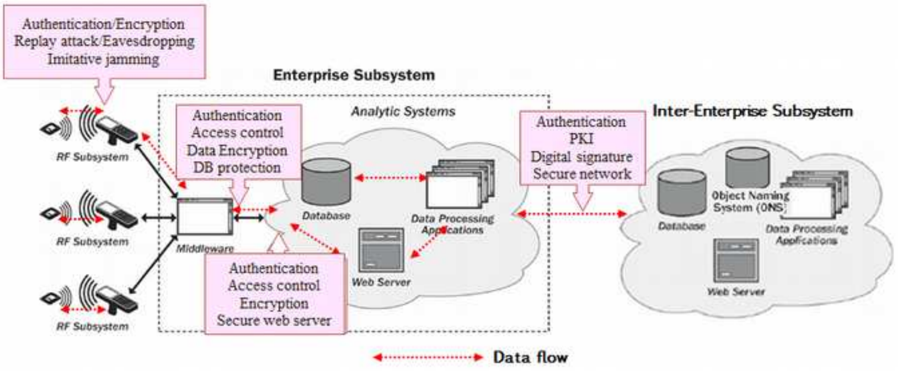


Figure 2. Data flow and security controls in an RFID system

tapping, forged tag, illegally copied tag, fake reader and guarantee for confidentialness of information leaked due to hacking. This is because there are security issues in the RFID system tag itself, in the section connecting tag and reader, between the reader and the local server, and in the server itself.

4. Analysis of Security Control in International Logistics Process

It is intended to analyze hazardous factors in the international logistics process, based on the logistics process of export/import between Hong Kong and Japan, which was started by the TLS (Transport and Logistics Services) business action group owned by EPCglobal. This business has been performed to investigate shipment information that was used for export/import based on RFID technology, and to require visibility as to how export/import logistics have been managed between Hong Kong and Japan by utilizing EPC/RFID [6].

The items produced by forwarding agents are packed, and moved to a warehouse, after loading them on a truck. Here, tags are applied for printing first, and then proceed to tagging onto each box. In addition, tagging information is forwarded to EPCIS in Hong Kong. Boxes are placed on a palette, loaded on a truck, and passed through the gate of the warehouse. Products grouped in a palette are loaded on a container, followed by closing the container door, and application of e-Seal on the door. At this time, data in the box should be forwarded to EPCIS in Hong Kong.

The tag information of a box, e-Seal information, and load information are all combined together, being forwarded to EPCIS in Hong Kong. Container vehicles pass through the gate of the warehouse on arrival at the port terminal, and containers are loaded onto a ship to be delivered. Ships sail to Japan from Hong Kong. Containers are unloaded from a ship arriving to the port terminal, and, at this time, the e-Seal information of the container is captured on the EPCIS.

The container e-Seal on the vehicle is read at the container yard gate, capturing it on EPCIS. Container vehicles are moved through a forwarder, and e-Seal is read at the gate entrance, and the door of the warehouse. All these items of information are stored in EPCIS in Japan. Freight in the container is unloaded at a warehouse, and a tag of box and palette are read, to confirm and determine real freight and the shipping advice.

Vehicles coming out of a warehouse are confirmed through e-Seal at the gate. E-seal is read at a gate by the receiver of freight, and vehicles are confirmed via e-Seal, when they arrive at the gate. Whether freight is damaged or not is checked through e-Seal, attached on the door of vehicles.

Figure 3 shows the potential vulnerabilities for EPCglobal Network that can occur in the process flow of international logistics export. Security control of hazardous factors that can occur in each process phase is as follows.

4.1 Box and Palette: Tag Printing

It should be noted not to store, or to minimize the information that can cause invasion of privacy, such as personal information on the tag, in order to protect data stored in the tag, for convenient identification of information that has been leaked. In addition, a unique method should be created to not expose the type of identifier to be used on a tag, in order to make it impossible for attackers to predict identifiers. Prior to saving data on a tag, a password should

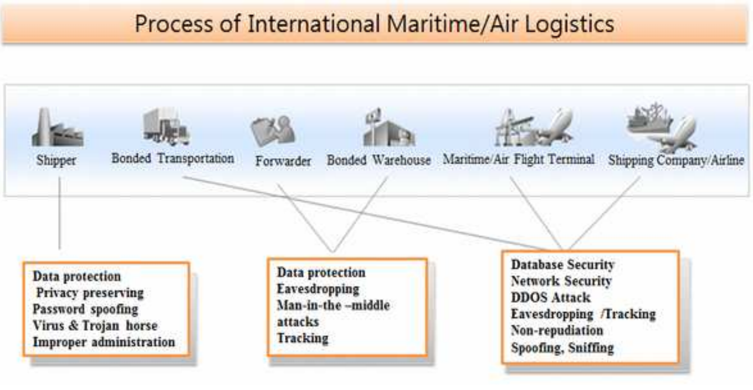


Figure 3. Security weakness in the process of international Logistics based on EPCIS

be encrypted, to prevent direct access of information. In addition, a back-up system should be prepared, to store data against loss. As a method of protecting tag data, it is plausible to prevent hazardous factors of security, by restricting the use of tag commands, or applying a kill feature for tags that are not used anymore, and this can reduce the risk of information being leaked.

4.2 Container (Truck): e-Seal

Logistics has a weakness on security in the middle of delivery. Therefore, care has to be taken. Specifically, a security control that can prevent hazardous factors, including an access of unauthorized users, DOS attack, or location tracing, is needed. For this, monitoring the steady existence of tags and operational status is required on a regular basis, so that location tracing does not become feasible without requiring additional security devices, by expecting a distance to be attacked.

4.3 Forwarder

An agreement of stipulation on MOA (Memorandum of Agreement) or MOU (Memorandum of Understanding) is required for a forwarder, a third party for export and import in the field of logistics, to maintain confidential security of a range of access for information or delivery control. In addition, it should be inspected if employees at a third party company are well informed of security control policies on a regular basis, in order to prevent information leakage.

4.4 Warehouse: Gate

It is required to prepare electromagnetic shielding devices, and a particular measure for access control, in a range of electromagnetic wave, in order to minimize physical access control at a warehouse, where products are stored.

In other words, a specific policy considering the feasibility of application of methods such as electronic shielding that can prevent movement of tag from the outside is required, to prevent RF signals from being transmitted to the outside. In addition, an additional security control is also needed, as a proper precaution for product information not to be attacked through electronic communication with tags. Deactivating tags is an example of this.

4.5 Port terminal and ship: container loading

A port terminal that loads products on a ship entails a procedure of product movement. Therefore, only authorized personnel are eligible to participate in the course of delivery of products, and should monitor whether they abide by rules of security control. In addition, if any violation of security control in a behavior or a method of loading products occurs, they should immediately report it, followed by assignment of duties for employees in charge of the system and delivery. Here, thorough education is needed, for mutual monitoring between employees for such an emergency.

In order to prepare for a case of hazardous factors and security threat that can occur in the international logistics process, a thorough

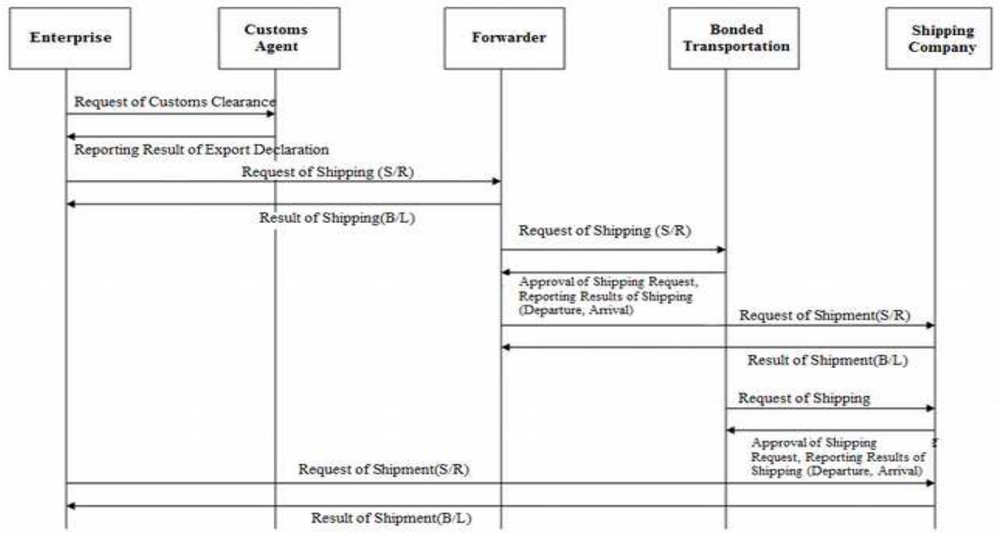

Enterprise
Customs Agent
Forwarder
Bonded Transportation
Shipping Company
Request of Customs Clearance
Reporting Result of Export Declaration
Request of Shipping (S/R)
Result of Shipping(B/L)
Request of Shipping (S/R)
Approval of Shipping Request, Reporting Results of Shipping (Departure, Arrival)
Request of Shipment(S/R)
Result of Shipment(B/L)
Request of Shipping
Approval of Shipping Request, Reporting Results of Shipping (Departure, Arrival)
Request of Shipment(S/R)
Result of Shipment(B/L)

Figure 4. Sequence diagram of the RFID-based international logistics process

measure covering all possible situations is specifically required, which considers types of tag in each phase, frequency, system certification in a network, requirement of security for user authorization, system analysis, and network.

5. Security Control Model for International Logistics Service

The basic concepts of role-based access control consist of user (U), role (R), and permission (P) [7,8]. In this chapter, we present an RBAC-based security control model for the international logistics service. The constraints of user and roles are represented in UML.

The RFID-based international logistics process sequence diagram has a flow, as shown in Figure 5, representing a connection of authorization of users, roles, and permission, for the information delivered from EPCIS. In order to apply it to the international logistics service platform, a specific RBAC model has been designed that is intensified, in terms of the management of role and authority safely accepting business partners.

Table 1. Definitions of the components of the RBAC based security control model

U(User) : User group
R(Role) : Role group
T(Task) : Task group, however, role can be constituted by tasks
P(Permission) : Set of permission (read, write, execute, append, delete, update)
S(Session) : Session group
C(Constraints) : Set of constraints
SP(Security Policy) : Security policy sets
MR(Manager Role) : Management role
RH(Role Hierarchy) : Role hierarchy
UA : User assignment
PA : Permission assignment
SA : Session assignment
RA : Role assignment
TA : Task assignment

Similar to the security management in the previous role of manager, functions of the security management, including creation of permission, roles, users, and role management, are subdivided. Figure 6 shows an RBAC based security control model for the international logistics service platform, on the basis of role engineering.

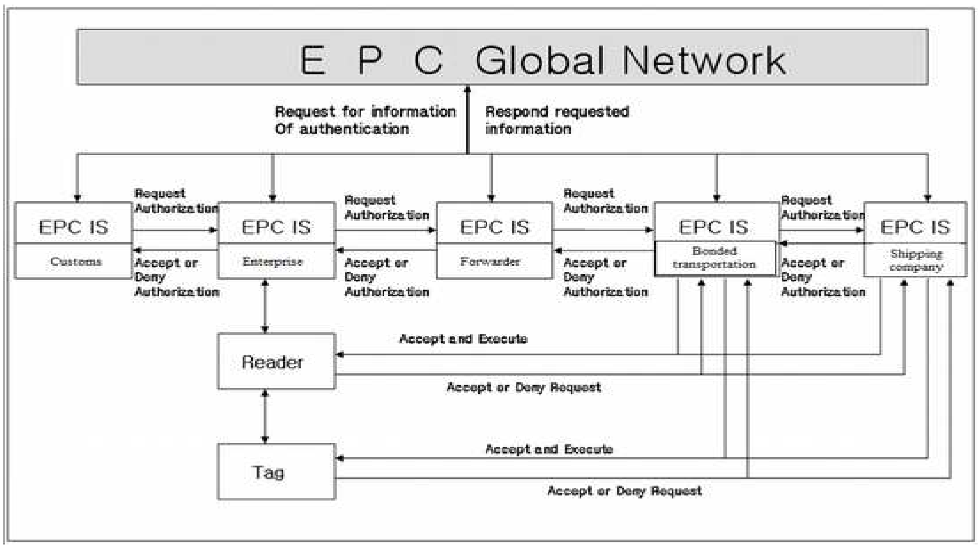


Figure 5. Process of request and response for authentication through the EPC global network

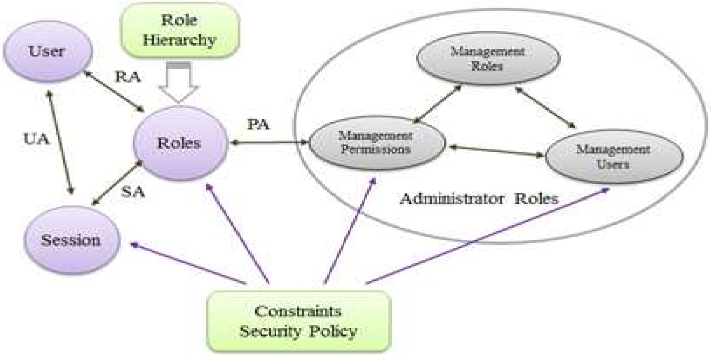


Figure 6. RBAC based security control model

Aarious constraints and security controls could be reflected in RBAC security model along with the intensified role of manager, deriving flexibility from changes in the logistics environment. In particular, the logistics environment determines whether access control of business partners is to be allowed or prohibited, aiming to rapidly reflect modified security control on the security model, followed by changes. Here, conditions of authorization and constraints as to users and roles in each phase should be modeled based on the authorization relations.

RBAC security control model simplifies the complicated procedures of granting authority in an extensive network environment such as RFID-based logistics service.[12]

The management of users, the management of roles, and management of permissions are all components of the purpose of management for security control. The proposed model can be utilized to protect users and logistics information of an organization in the logistics environment, after being realized for access control in the enterprise subsystem that serves as the role of EPCIS. In addition, they are also generalized descriptions of a security model to account for various types of security control, and to perform them.

They should be performed with a proper authority by security tools, and it has to be guaranteed to independently establish particular hardware and software and regeneration mechanism of the control according to the change of an organization. In addition, a proper procedure of implementing security control, such as performance in an external environment other than the pre-established security control in the information processing system, is required, to guarantee the certainty of the security.

Using UML, a type of modeling language that can conveniently specify RBAC control, is beneficial for expression of RBAC control in an organized and systematic manner in the application program design model [6, 7].

Figure 7 is an object diagram of security control based on an RBAC model, which represents basic components such as users, roles, permission, session, and role hierarchy, SSD (Static Separation of Duty), constraints, and DSD (Dynamic Separation of Duty). It also indicates the relationship of the role of customs, delivery, and shipment to be requested by companies in the international logistics process.

The UML diagram is represented by use-case, class diagram, sequence diagram, and object diagram, and can be also used to derive the requirements of access control, constraints, and security control on these diagrams.

In order to maximize the efficiency of the RBAC, we presented the constraints of RBAC using UML. Role engineering is what designs components of RBAC model, and properly constitutes policies in a particular organization.

Constraints of the duty separation are used to prevent conflicts with policies. Constraints of the SSD are intended to prevent conflicts that can occur when acquiring permission regarding the role against the user.

Constraint of DSD restricted the role to be promoted in the same user session. It means, the user could not activate other roles that conflict in the same session when a part of the role in DSD constraints is activated.

It is feasible to obviously represent an RBAC model in UML, but there are weaknesses. First of all, a clear classification of terms is needed, and there is no abstract package, even though an abstract package might exist in UML. An arrow used in the application key hierarchy, and the one for generalization of UML, have

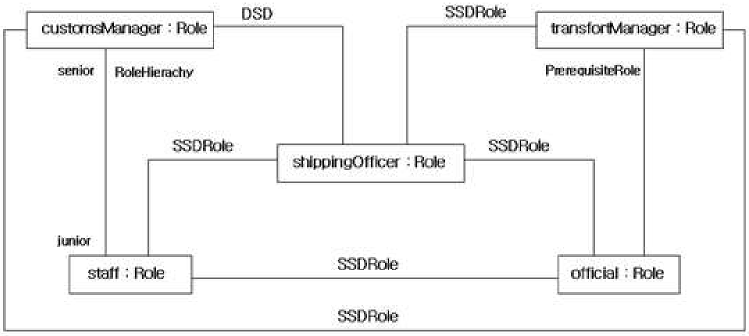


Figure 7. Object Diagram of RBAC based Security Control Model

different meanings. In addition, a technology of constraints that needs an additional extension is still insufficient.

Here we introduced an example scenario to figure out how to apply the proposed security specification in the real world and worked well. We implemented a prototype system based on this scenario. The three companies were connected to EPC IS(EPC Information Server). Figure 8 showed the example architecture of international logistics.

An 'Enterprise A' company located in Hong Kong has provided wines and they have sold them abroad. A bonded warehouse 'WH co.' stocked goods from international enterprise and shipping company 'Sailor Moon' shipped goods. The assumption was that EAF (Enterprise Application Framework) was adopted to develop the international logistics service for the three companies. Therefore the EAF had three managers: Data Manager, Security Manager, Business Event Manager. Data Manager of EAF incorporates to access external EPC IS using network sockets, and web services. Security Manager supports appropriate access control and authentication in the distributed environment. Business Event Manager provides various business process functions with related companies and customers. Figure 9 shows an example of the RH(Role Hierarchy) of the enterprise, the bonded warehouse and the shipper.

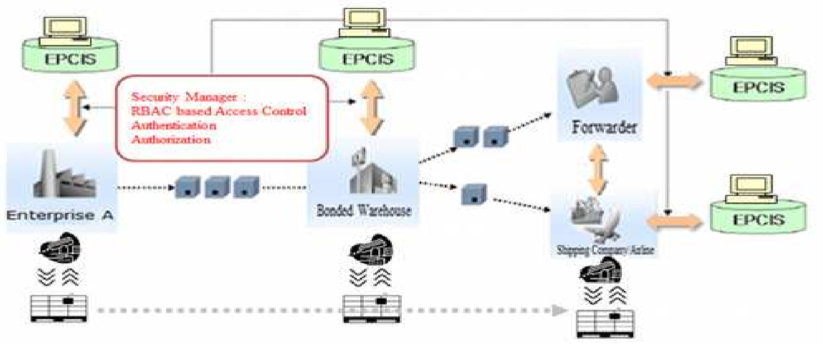
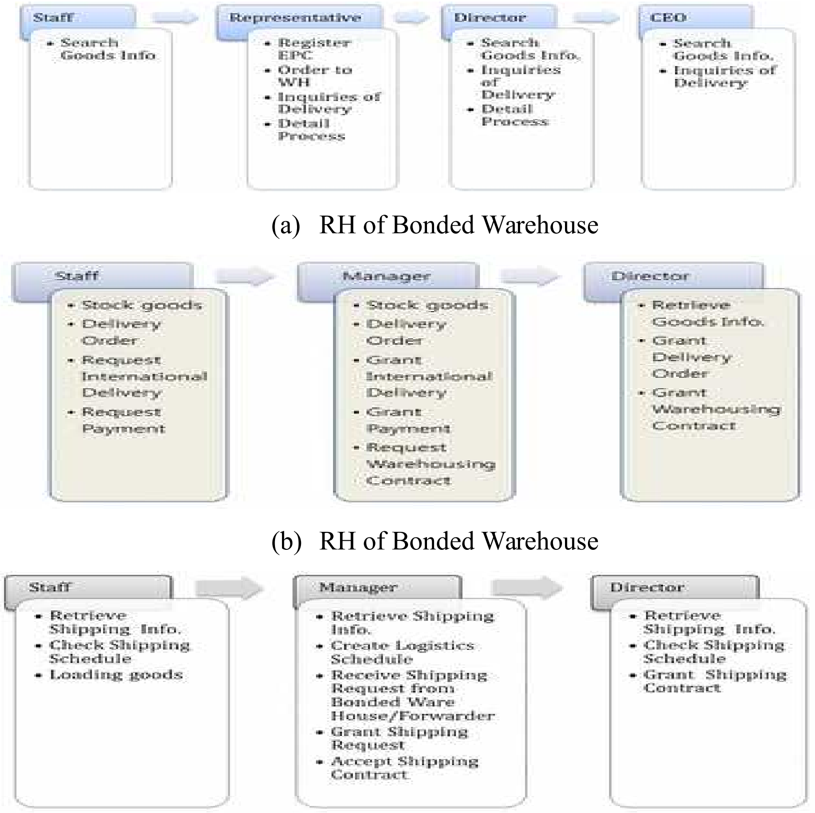


Figure 8. Example Business Process Model



(a) RH of Bonded Warehouse

(b) RH of Bonded Warehouse

Staff
• Retrieve Shipping Info.
• Check Shipping Schedule
• Loading goods
Manager
• Retrieve Shipping Info.
• Create Logistics Schedule
• Receive Shipping Request from Bonded Ware House/Forwarder
• Grant Shipping Request
• Accept Shipping Contract
Director
• Retrieve Shipping Info.
• Check Shipping Schedule
• Grant Shipping Contract

(c) RH of Shipper

Figure 9. Role Hierarchies for prototype system

Four roles are needed in Enterprise A. There are three roles in bonded warehouse and shipper. Each role has tasks that have been carried out by the user who granted with role. The constraints of SoD should be essential to avoid the conflict of roles. In this scenario we need DSD(Dynamic Separation of Duty) as follows:

Staff.Session→ excludesAll(Manager.Session)
Manager.Session→ excludesAll(Director.Session)
Staff.Session→ excludesAll(Director.Session)

The Process of security mechanisms using RBAC based security model is as follows:

(1) [Authentication] *A User with Representative Role selected his Role and could log in the enterprise (bonded warehousing company / shipping company) application system by entering password of each role. The enterprise application system requests information* on *login and authority from databases.*

(2) *A User belong to enterprise ((bonded warehousing company / shipping company) carried out his job to register EPC of products on EPC IS.*

(2-1) [Access Control] If there is no permission to use EPCIS, sending product information to EPCIS would be denied.

(2-2) [Access Control] If permission is granted, the enterprise (bonded warehousing company / shipping company) application system can find the session key which was made between the enterprise application system and EPCIS

(3) [Encryption] *The enterprise (bonded warehousing company / shipping company) application system made encryption of data using the session key.*

(3-1) [Key Agreement] If there is no session key, the enterprise (bonded warehousing company / shipping company) application will make a session key by communicating with EPCIS.

(4) *The enterprise (bonded warehousing company / shipping company) application sends the encrypted form of data to EPCIS.*

(5) *EPC IS decrypts the received data that was encrypted by the enterprise (bonded warehousing company / shipping company) application.*

6. Implementation

In order to verify the proposed security model for RFID-based logistics service we implemented the prototype of an example scenario. We defined the specification of the proposed model: roles, subjects, objects, constraints and so on. Figures below demonstrated the implementation of RBAC security model introduced in the previous section. Figure 10 showed the implemented prototype system for enterprise connected to EPC IS.

Representative Role carried out to register goods on EPC IS. The user who has a role of representative makes acquisition of permission from EPC IS. If permission is granted, it is possible to make registration EPC for the trace of their product during logistics service.

After registering goods on EPC IS by the enterprise, bonded warehouse and shipping company can access goods information on EPC IS for the logistic service. The roles of the bonded warehouse company are shown in Figure 11. And Figure 12 shows the prototype system for shipping company. The constraints of the RBAC security model can be specified according to the company's policy. In our prototype system we implemented constraints of SSD (Static Separation of Duty) using tab control for selecting only one role per one session. The constraints of DSD (Dynamic Separation of Duty) also had been applied using option controls.

7. Conclusion

RFID-based international logistics environment can bring a significant efficiency for improving cost and delivery issues. In this paper, we applied an RBAC-based security control model to cover the security requirements in an international logistics process and constraints of the access control. RBAC based security control model for international logistics can be flexible used to each phase for each enterprise. For the verification of the proposed security model, we made example scenario and implemented the prototype system. We had applied the proposed security control model to each parts of the logistics service such as shipper, bonded transportation and enterprise. In the future works, we are going to extend the prototype system applying GRBAC based security model to specify the security policies needed to enterprise in EPC IS. We also extend the Security Manager in order to provide the stronger authentication between RFID tag and reader in EPC IS.

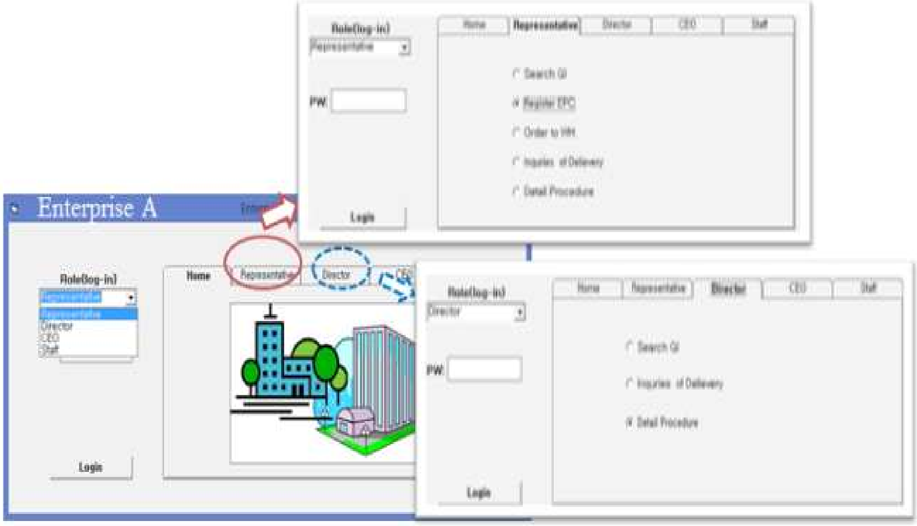


Figure 10. Prototype system for Enterprise A

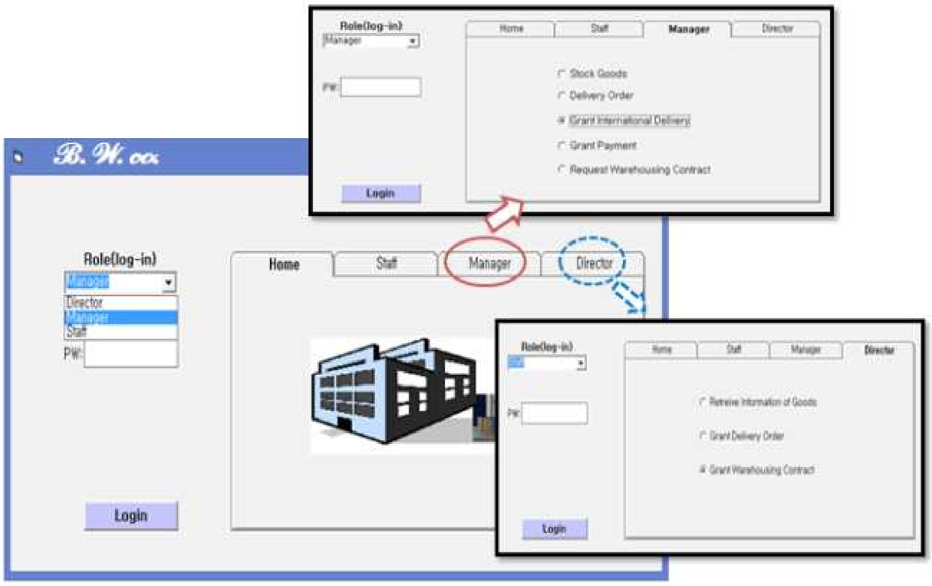


Figure 11. Prototype system for Bonded Ware House

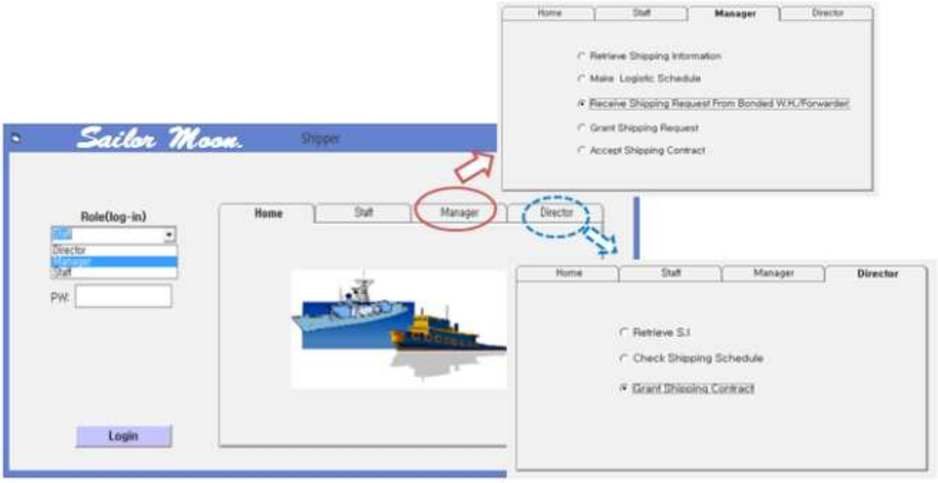


Figure12. Prototype system for Shipping Company

Acknowledgements

This paper was supported by Konkuk University 2015.

REFERENCES

1. EPCglobal. **The EPCglobal Architecture Framework Final Version & EPC Information Services (EPCIS) Ver. 1.0 Spec**. 2007.
2. CERNIAN, A., D. CÂRSTOIU, A. OLTEANU, V. SGÂRCIU, **An Integrated Cluster Analysis and Validity Test Platform for the Compression based Clustering Approach**, Studies in Informatics and Control, ISSN 1220-1766, vol. 24(2), 2015.
3. WU, M.-Y., W.-L. TZENG, **Applying Context-Aware RBAC to RFID Security Management for Application in Retail Business**, APSCC '08. IEEE, 2008.
4. REKLEITIS, E., P. RIZOMILIOTIS, S. GRITZALIS, **A Holistic Approach to RFID Security and Privacy**, In Proceeding of: SecIoT '10, 2010.
5. ŢIGĂNOAIA, B., **Some Aspects Regarding Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard**, Studies in Informatics and Control, ISSN 1220-1766, Vol. 24(2), 2015.
6. NIST, **Guidelines for Securing Radio Frequency Identification System**, 2007.
7. MAYER, N., A. RIFAUT, E. DUBOIS, **Towards Risk-Based Security Requirements Engineering Framework**, In Proceedings of REFSQ'05.
8. RAY, I., D. KIM, **Using UML To Visualize Role-Based Access Control Constraints**, In Proceedings of the 9th ACM Symposium on ACMT, 2008.
9. DENG, H.-F., W. DENG, H. LI, H.-J. YANG, **Authentication and Access Control in RFID based Logistics-Customs Clearance Service Platform**, International Journal of Automation and Computing, May 2010, Vol. 7.
10. STOJANOVIC, N., D. STOJANOVIC, **A Hybrid MPI+OpenMP Application for Processing Big Trajectory Data**, Studies in Informatics and Control, ISSN1220-1766, Vol. 24(2), 2015.
11. HE, W., Y. LI, K. CHIEW, T. LI, E. W. LEE, **A Solution with Security Concern for RFID-Based Track & Trace Services in EPCglobal-Enabled Supply**, InTech ISBN: 978-953-307-265-4, 2011.
12. SHIN, M. S., H. S. JEON, Y. W. JU, B. J. LEE, S. P. JEONG, **Constructing RBAC Based Security Model in u-Healthcare Service Platform**, TSWJ vol. 2015, Art. ID 937914, 2015.