국제 물류 서비스 플랫폼의 정보 보호를 위한 RBAC 기반 접근제어 보안 모델+

신문선*, 황정희**, 황익수*** 김현철***
*건국대학교 컴퓨터시스템전공
**남서울대학교 컴퓨터학과
***한국무역정보통신(주)
e-mail:msshin@kku.ac.kr

RBAC based Security Model for EPC Global Network

Moon-Sun Shin*, Jeong-Hee Hwang**, Ik-Soo Hwang***, Hun-Chul Kim***
*Dept of Computer Science, Kon-Kook University
**Dept of Computer Engineering, Nam-Seoul University
***KTNET

요 약

RFID기반의 국제물류 서비스 플로우상에서 나타나는 보안 요구사항으로 태그 보안, 물류 보안, 인증, 접근제어 등이 있으며 특히 물류정보보안과 사용자 인증 및 접근제어를 위해서 물류정보 데이터베이스를 위한 보안모델이 필요하다. 본 논문에서는 RBAC에 기반한 강화된 접근제어 모델을 제안하며 이는 EPCglobal Network 과 같은 분산 환경의 다양한 사용자들 및 물류정보 관리에 효율적이며 보안관리에 있어 용이성을 제공할 수 있어 향후 EPC IS에 Security Module로 구현 및 적용이 가능하다.

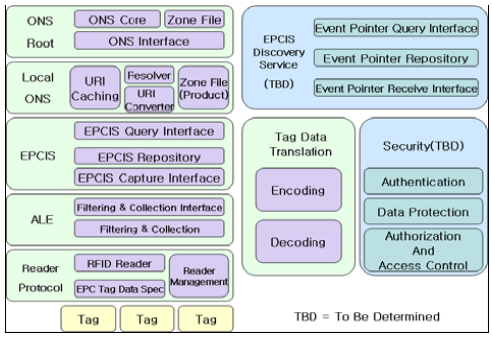
1. 서론

RFID기반의 국제 물류 서비스 플랫폼에서의 보안 요구사항을 분석해보면 제품 정보에 대한 보안뿐만 아니라 도용, 위치 추적, 물리적 공격 등 RFID 기반 물류 환경의 특성상 나타나게 되는 여러 가지 위협에 대한 보안 요구사항이 존재한다. 또한 물류 정보와 사용자 정보관련 데이터베이스 보안 등의 보안 요구사항이 요구되고 있으며 이러한 위협요소들은 국제 물류 환경의 기술발전과 보급을 저해하는 요인이 되고 있다.

EPCglobal Network는 거대한 물류환경에서 EPC정보의 분산관리와 전달 효율성을 높일 수 있으나 많은 위협이 존재하며 기업과 기관의 보안계층으로만 위협요소를 모두 제거할 수 없다. 특히 국제물류 서비스 플로우상에서 나타나는 위협에 대한 태그 보안, 물류 보안, 인증, 접근제어 등의 보안문제에 대한 해결책은 현재 미비한 단계이다.

(그림 1)은 EPCglobal Network Architecture Framework 이다. EPC가 기록된 Tag, Tag의 정보를 읽어들이는 장치인 리더, 리더로 읽은 Tag 정보를 정제하고 취합, 중복된 정보의 제거와 정보의 그룹화 등의 역할을 하는 ALE(Application Level Events), 정제된 EPC정보를 저장하고 제공하는 구실을 하는 EPC IS(Information Services), EPCglobal Network 상에서 글로벌 검색서비스를 제공하는 ONS(Object Naming Service)[7], EPCglobal Network에서 물류 정보사용자가 EPC에 대한 정보를 찾고 이에 접근할 수 있도록 하는 역할을 하는 EPCIS Discovery Service로 구성되어 있다. 현재 EPCIS Discovery Service 개념 단계의 논의만 되고 있으며, 그 외 물류 정보의 보안을 담당하는 Security 부분 또한 아직 개념 단계의 논의만 되고 있다.

Security 관련 부분은 크게 Authentication, Data Protection, Athorization & Access Control 로서 정의되어 있으나 TBD(To Be Determined 인 상태이다.



(그림 1) EPCglobal Architecture Framework

현재의 EPCglobal Network 상에서 물류정보의 보안문제는 물류정보 시스템을 구축하는 기업이나 단체에 의해 제안되고 있지만 연구가 활발하게 이루어지는 실정은 아니다. 또한 EPC Network 상에서 물류정보 접근제어에 관한 국내외 연구들이 수행되고 있으며, 국외에서 진행된 연구

+ 이 연구는 지식경제부 uGLP성장동력기술개발사업(한국무역정보통신)의 지원에 의하여 연구되었음

내용으로는 독일 홈볼트 대학에서는 EPCglobal Network 상에서의 전반적인 보안 위협요소에 대한 해결방법들을 설명하고 있다. 주된 해결방법으로 Virtual Private Network를 이용하는 방법, Transport Layer Security를 이용하는 방법, 기존 DNS의 보안체제인 DNSSEC(DNS Security Extensions)의 이용하는 방법 등을 제시하고 있지만 광범위한 EPC Network 상에서 적용함에 비용의 증가와 관리에 대한 문제점을 우려하였다.

IBM Almaden Research Center에서는 EPCglobal에서 개념단계의 논의 중인 Discovery Services에 대해 상세히 설명하면서 EPC Network 상에서의 물류정보 보안에 대해 EPC Network 상에서 Business partner에게만 물류정보를 제한하여야 한다고 언급하면서 그 해결책으로 EPC IS에서 기존 접근제어 기법 중 역할 기반 접근제어와 같은 접근제어 모델을 적용하여야 할 것으로 방법론 제시만을 하고 구체적인 설계나 구현에 관해서는 전혀 언급을 하고 있지 않다.

따라서 본 논문에서는 EPC Network 상에서 물류 정보와 사용자 정보 보호를 위하여 역할기반 접근제어모델에 기반한 강화된 접근제어 보안 모델을 제안한다. 이는 RFID 기반의 국제 물류 서비스 플랫폼에서의 신뢰성과 제품 무결성을 보장하기 위한 정보보호 서비스 모델로서 EPCglobal Network 과 같은 분산 환경의 다양한 사용자들 및 물류정보 관리에 효율적이며 보안 관리에 있어 용이성을 제공할 수 있어 향후 EPC IS에 Security Module로 구현 및 적용이 가능하다.

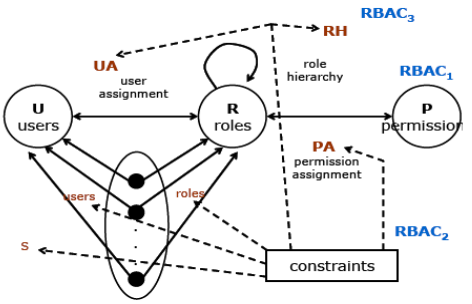
본 논문의 구성은 다음과 같다. 2장에서는 RBAC에 대하여 간략히 소개하고 3장에서는 국제물류서비스플랫폼을 위한 RBAC기반 접근제어 모델을 제안하고 4장에서는 결론및 향후 연구에 대해서 논의한다.

2. RBAC(Role Based Access Control)

RBAC 모델을 이용한 접근제어 기술은 정보보호의 기본 분야중의 하나로 보안관련 시스템과 다양한 컴퓨팅 환경에서 적용되고 있는 기반기술이다. 특히 국외에서는 RBAC모델의 역할(Role) 개념을 사용하여 엔터프라이즈급의 대형 시스템에서 사용자가 자신의 책임범위 안에서 허가된 자원만을 접근 가능하도록 한다. 각 컴퓨팅 환경에 따라 접근 주체와 객체가 각기 상이하기 때문에 각 컴퓨팅 환경마다 상이한 RBAC 모델 적용 방법이 필요하며. 유비쿼터스 환경에서의 접근제어, 애플리케이션 수준의 접근제어, 개인정보 프라이버시 보호 등을 위해서는 RBAC 모델에 대한 지식, 적용방법, 접근제어 정책의 구성과 운영, 다른 보안 기술과의 연동 등의 기술적 연구에 많은 관심이 모아지고 있다. 특히 RBAC은 대단위 네트워크의 복잡성과 보안관리의 용이성 비용감소 등에 큰 효과가 있어 다양한 환경에서 적용되고 있다.

역할기반 접근제어는 조직의 구조와 연동하여 직책 혹은 역할에 따라 보안 등급이 부여되고 사용자는 특정 직책을 부여받으면 그에 대응하는 권한을 획득한다. 따라서 직책 혹은 역할에 따른 권한이 조직의 보안 정책에 따라 결정되면 각 사용자는 역할만을 배정 받게 된다. 사용자가 역할을 부여받거나 역할들간의 계층구조 등으로 발생되는 복잡성은 역할기반 접근제어모델에서 관리가 되므로 보안관리가 용이해진다.

RBAC 모델은 사용자가 조직의 정보자원을 임의로 접근할 수 없도록 하는 것이다. 사용자는 역할을 부여받았을 때에만 그 역할에 상응하는 권한을 가지게 된다.즉 사용자는 역할의 수행에 필요한 최소한의 자원에 대한 접근만이 허용된다. (그림 2)는 RBAC 모델을 도식화한 것이다. 기본 구성 요소는 사용자(U:User)와 하나 혹은 그 이상의 객체에 대한 특정 접근 모드의 승인을 나타내는 역할(R:Role), 사용자 배정(UA: User Assignment)와 인가 권한(P:Permission), 세션(S:Session) 이다.



(그림 2) Role Based Access Control Model

RBAC은 정보시스템에서 접근제어를 위한 방법론이다. 사용자의 권한과 권한부여의 관리를 용이하게 하기위해 개발되었다. 따라서 RBAC을 적용하면 권한부여가 용이해지며 관리에 드는 비용 감소효과와 보안강화에 효율적이다. 또한 파트너와의 정보상호운용성을 강화시킬 수 있으며 새로운 네트워크 레벨의 RBAC 서비스가 가능하며 궁극적으로 조직의 모든 사용자들에 대한 서비스를 개선할 수 있게 된다. 따라서 다음 장에서 RFID기반의 국제 물류 서비스 플랫폼을 위한 RBAC 기반 보안모델을 제안한다.

3. 국제물류서비스 플랫폼을 위한 RBAC 기반 보안 모델

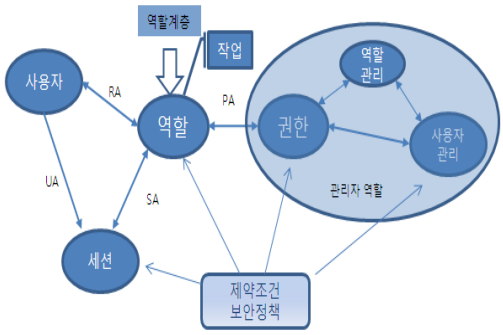
RBAC을 적용한 보안관리는 방대한 네트워크 환경에서 복잡한 권한 부여를 단순화함으로써 보안 관리에 드는 비용과 시간을 감소시켜준다. RBAC을 EPCGlobal Network에 적용하기 위해서는 다양한 상업적, 이질적 환경에서의 역할(Role)과 타스크(Task)에 관한 설계 및 다양한 조직의 보안 정책을 반영할 수 있도록 하는 유연성이 필요하다.

다음 표 1은 제안한 모델의 구성요소에 대한 정의이다.

<표 1> 제안모델의 구성요소 정의

U(User) : 사용자 집합 R(Role) : 역할 집합 T(Task) : 작업집합 단, 역할은 작업으로 구성가능 P(Permission) : 권한 집합(read, write, execute, append, delete, update) S(Session) : 세션 집합 C(Constraints) : 제약조건 집합 SP(Security Policy) : 보안정책 집합 MR(Manager Role) : 관리자 역할 RH(Role Hierarchy) : 역할 계층 UA,PA,SA,RA,TA : 사용자 할당, 권한 할당, 세션할당, 역할 할당, 작업할당

국제물류서비스플랫폼에서 적용하기 위해서는 비즈니스 파트너를 안전하게 수용할 수 있는 역할과 권한 관리 및 사용자 관리가 강화된 RBAC 모델을 설계하였다. 기존의 관리자 역할에서의 보안 관리를 수행한 것과 유사하게 권한 생성 및 역할 생성 사용자 생성 및 역할 관리 등 보안 관리 기능을 세분화하였다.



(그림 3) RBAC 에 기반한 강화된 보안 모델의 설계

강화된 관리자역할과 함께 제약조건과 보안정책을 모든 구성요소에 적용할 수 있도록 정책 반영 기능을 한층 강화하여 물류 환경에서의 상황변화에 따른 유연성과 적응성을 유도하였다. 특히 물류 환경은 이해관계에 따라 비즈니스 파트너의 접근제어가 허용되거나 금지될 수 있어 이러한 상황변화에 따른 보안정책 변경을 보안모델에 신속하게 반영하기 위해서이다.

관리사용자지정, 관리역할, 관리권한지정, 관리권한 등은 보안관리를 위한 관리목적의 구성요소들이다.

제안 모델은 EPC IS 역할을 수행하는 엔터프라이즈 서브시스템에서 접근제어를 위해 구현되어 물류환경에서의 조직의 물류 정보와 사용자정보 보호를 위해 활용되어질 수 있다. 또한 다양한 보안정책을 기술하고 이를 수행시키기 위한 보안모델의 일반화된 기술사항이다.

기술된 보안정책은 시스템 관리자 절차를 통해서 구현가능하며 수립된 보안정책들은 정보처리시스템(IT시스템)의 적절한 부분으로 각각 구현될 수 있어야 한다. 보안도구에 의해서 적절히 권한을 가지고 실행될 수 있어야 하며 변화에 따른 정책의 갱신 메커니즘과 특정 하드웨어 소프트웨어 독립적 수립이 보장되어야한다. 또한 정보처리시스템에 구현된 보안정책 외에 외부 환경적 요소에서의 수행과 실행 등의 올바른 보안정책이행과정이 있어야 보안의 확실성을 보증할 수 있다.

4. 결론

본 논문에서는 RFID 기반의 국제 물류 서비스 플랫폼에서의 효율적인 물류처리 서비스를 위해서 우선적으로 요구되어지는 보안 요구사항인 물류 정보의 보안 및 사용자 접근제어를 해결하기 위해서 RBAC에 기반한 접근제어 보안 모델 설계에 관하여 기술하였다. RBAC 모델을 국제물류서비스 플랫폼에서 적용하기 위해서는 다양한 상업적, 이질적 환경에서의 역할(Role)과 타스크(Task)에 관한 설계가 필요하며 또한 비즈니스 파트너를 안전하게 수용할 수 있는 역할과 권한 관리 및 사용자 관리가 강화된 RBAC 모델의 설계를 제안하였다. 또한 다양한 조직의 보안정책을 반영할 수 있도록 제약 조건과 보안정책을 모두 제안모델에 구성요소로 추가하였다. 향후 설계된 보안모델을 구현하여 효용성을 검증하는 연구를 계속해서 수행할 것이며 이는 RFID 기반 국제 물류 환경의 특성상 나타나게 되는 여러 가지 위협에 대한 Security와 Privacy 문제를 해결하는데 적용할 수 있는 보안기반기술로 향후 RFID기술 기반 물류 환경 관리의 기술발전과 보급에 기여하게 될 것이다.

참고문헌

[1] Ravi S. Sandhu, Edward J.Coyne, Hal L. Feinstein and Charles E. Youman. "Role-Based Access Control Models", IEEE Computer, Volume 29, Number2, pages 3847, February 1996.

[2] NIST(National Institute of Standards and Technology). "An Introduction to Role Based Access Control", December, 1995

[3] 정보통신연구진흥원. "역할기반 접근제어 컴포넌트 S/W개발 연구결과보고서", 2003.

[4] Benjamin Fabian, Oliver Günther. "Security Challenges of the EPCglobal Network"

[5] Dong Seong Kim and Jong Sou Park, "A Security Framework in RFID Multi-domain System", Workshop on Advances in Information Security (WAIS 2007), IEEE Computer Society, Vienna University of Technology, Austria, 04, 2007

[6] Jules, A. "RFID Security and Privacy: A Research Survey", IEEE Journal on selected Areas in Communications, Feb,2006.

[7] 문홍구, 한기덕, 권혁철, "EPCglobal Network 상에서 EPC IS 와 EPCIS Discovery System의 연동을 통한 물류 정보 접근 제어 방법", 한국정보과학회 가을 학술발표논문집, Vol.34, No.2(D), pp.95-99, 2007

[8] Qingfeng He, " A Strutured Role Engineering Process for Privacy-Aware RBAC Systems"