산업제어시스템의 역할기반 접근제어 표준화 및 연구 동향

박 경 원
동국대학교 정보통신공학과

임 대 운
동국대학교 정보통신공학과

Ⅰ. 서 론

전기, 수도 등의 산업기반시설은 외부와 물리적으로 독립되어 있고, Modbus, Profibus, RS-485, RS-422 등과 같이 제어시스템 별로 특화된 프로토콜 및 물리적 인터페이스를 사용하기 때문에 사이버 위협 및 공격으로부터 비교적 안전하다고 인식되어 왔다. 하지만, 2010년 산업제어시스템(ICS, Industrial Control System)을 대상으로 한 '스턱스넷'의 사례가 확인되면서, 물리적으로 독립된 산업기반시설이라 하더라도 더 이상 안전하지 않다는 것이 확인되었다. 또한, 산업제어시스템의 효율성과 상호 운용성 등을 높이기 위해 공개 표준이 사용되고 외부 망과의 연결에 대한 요구에 의해 물리적인 인터페이스도 통신망에 대중적으로 사용되는 이더넷이 지원됨에 따라, 침입의 경로가 다양해지고 취약점도 늘어날 수 있는 상황이 되었다.

산업 제어시스템 효율성과 상호 운용성 제고를 위해 공개 표준 사용 및 외부 망과의 연결성 확대로 인해 침입 경로가 다양해지고 취약성이 증가하는 상황이 되었다.

1997년부터 IEC (International Electrotechnical Commission)는 산업기반시설에 대해 사이버 위협에 대응하기 위한 보안의 필요성에 대해 논의를 진행하였으며, 1999년에 구성된 IEC TC 57의 Working Group 15에 의해 산업제어시스템의 보안을 위한 IEC62351 표준이 2007년에 발표되었다[1]. IEC62351은 전력시스템의 통신 네트워크와 시스템 보안을 위한 표준으로 디지털 서명을 통한 데이터 전송의 인증, 인증된 접근의 보장, 도청의 예방, 재생 및 스푸핑 공격 방지, 침입 탐지 등의 기능을 지원한다.

본고는 산업제어시스템의 역할기반 접근제어 (RBAC : Role Based Access Control)를 규정하는 IEC62351-8을 살펴보고 RBAC 관련한 연구 동향을 소개한다.

Ⅱ. 역할기반 접근제어 표준

1. 역할기반 접근제어 개요

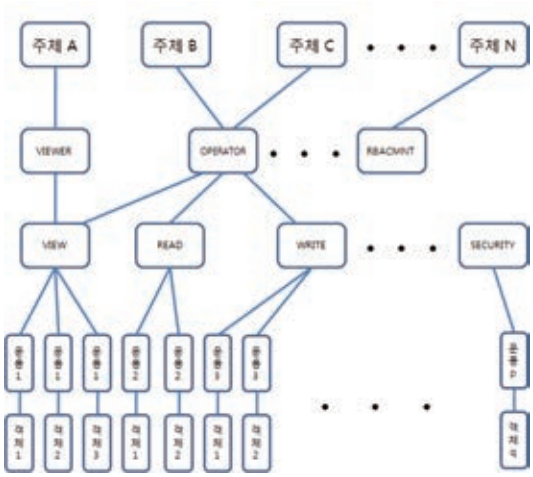
기존의 운영체제에서 널리 사용되고 있는 접근제어는 정보의 유출, 변조 및 시스템 자원의 파괴 등의 위험을 최소화하기 위한 기법이다. 특히 산업제어시스템의 경우에는 인증을 통해 모든 자원에 접근할 수 있는 사용자 모델(All-or-nothing super-user model)에 대한 대안으로 RBAC이 도입되고 있다. RBAC은 사용자가 업무를 수행하기 위해 필요한 최소한의 권한만 부여하는 것을 원칙으로 하며, 이를 통해 보안 정책, 네트워킹, 방화벽, 백업 시스템 운영 등에 있어 보안성을 향상 시킬 수 있다. 〈표 1〉은 RBAC을 설명하기 위한 용어를 정의한다.

〈그림 1〉은 주체, 역할, 권한, 운용, 객체의 관계를 나타내며, 본고에서 사용자와 주체 그리고, 객체와 자원은 각각 같은 의미로 사용된다. IEC 62351-8에서 사용자의 역할은 관찰자(VIEWER), 운영자(OPERATOR), 엔지니어(ENGINEER), 설치자(INSTALLER), 보안관리자(SECADM), 보안감사(SECAUD), RBAC관리자(RBACMNT)로, 권한은 VIEW, READ, DATASET, REPORTING, FILEREAD, FILEWRITE, FILEMGT, CONTROL, CONFIG, SETTINGGROUP, SECURITY로 사전 정의

산업제어시스템의 경우 인증을 통해 모든 자원에 접근할 수 있는 사용자 모델에 대한 대안으로 RBAC이 도입되고 있다. RBAC은 사용자가 업무를 수행하기 위해 필요한 최소한의 권한만 부여하는 것을 원칙으로 하며, 이를 통해 보안 정책, 네트워킹, 방화벽, 백업시스템 운영 등에 있어 보안성을 향상시킬 수 있다.

〈표 1〉 역할기반 접근제어 용어

구분	내용
주체 (Subject)	사용자 또는 자동화된 에이전트
역할 (Role)	조직 내에서 정의된 업무의 기능
권한 (Right)	특정한 객체들을 접근할 수 있는 특권(Privilege)의 집합
운용 (Operation)	실행 가능한 기능
객체 (Object)	시스템 자원



〈그림 1〉 역할기반제어 관계도

하고 있다.

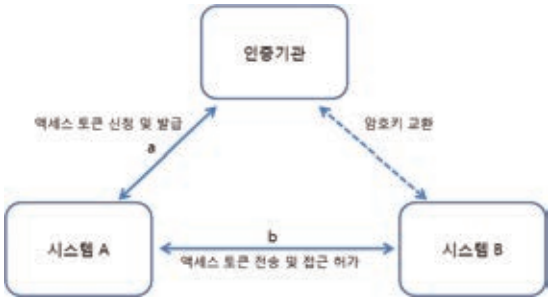
〈표 2〉는 IEC 62351-8에서 제시한 역할에 할당된 권한을 보여주고 있다. 예를 들면 VIEWER의 경우 VIEW, REPORTING의 권한을 갖고, OPERATOR의 경우 VIEWER의 권한 외에 READ와 CONTROL의 권한이 추가된다. 또한, 주체 및 역할 그리고, 권한은 필요에 따라 추가될 수 있다.

RBAC은 역할의 성격에 맞는 접근 권한을 사전에 정의하고 새로운 사용자를 추가하는 경우 사용자가 수행해야하는 업무에 맞는 역할을 부여함으로써 사용자의 권한을 직접 지정하는 기존의 방법에 비하여 권한의 부여 및 회수가 용이하고 보안성도 강화된다는 장점을 갖는다.

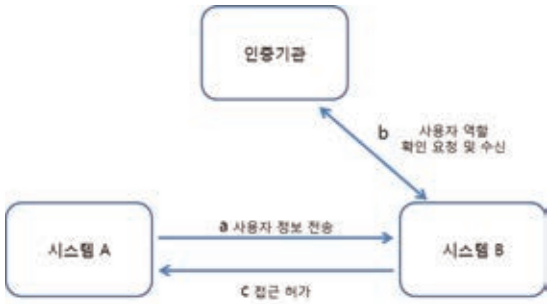
2. 접근제어모델

IEC62351-8은 시스템 A의 사용자 UA가 원격지 시스템 B의 자원을 접근하고자 하는 경우, 시스템 B가 신뢰할 수 있는 인증기관으로부터 사용자 UA의 역할을 확인하는 방법을 Push 모델과 Pull 모델로 제시한다.

〈그림 2〉는 IEC62351-8에서 제시된 Push 모델의 동작을 나타낸다. 단계 a에서 사용자 UA가 시스템 B의 자원을 접근하기 위해서 신뢰된 인증기관으로부터 자신에게 부여된 역할과 관련한 정보가 저장된 엑세스 토큰을



〈그림 2〉 Push mode



〈그림 3〉 Pull model

발급받아야 한다. 엑세스 토큰은 변조되지 않기 위해서 암호화된 상태로 사용자 UA에게 발급되며 재생 공격에 대비하기 위해서 유효 기간이 짧아야 한다. 인증기관과 시스템 B는 신뢰할 수 있는 채널을 통해 엑세스 토큰을 검증하기 위한 암호키를 교환한다고 가정한다. 단계 b에서 사용자 UA가 액세스 토큰을 시스템 B에 전송하면, 시스템 B는 키 K를 이용해서 액세스 토큰을 검증하고 UA의 역할과 관련한 권한을 허가한다. Push 모델의 프로세스는 커베로스(Kerberos) 인증 방식과 유사하며, 시스템 B는 시스템 A를 통해 주체의 역할을 전달받기 때문에, 시스템 B의 부하가 경감된다는 장점이 있다.

〈그림 3〉은 IEC62351-8에서 제시된 Pull 모델의 동작을 나타낸다. 단계 a에서 사용자 UA가 시스템 B의 자원을 접근하기 위해서 사용자 UA는 아이디와 패스워드와 같은 사용자 정보를 시스템 B로 전송한다. 단계 b에서 시스템 B는 사용자 UA의 역할을 인증기관에게 직접 요청하여 전달받는다. 이 방법은 사용자 정보만으로 시스템 B의 자원에 대한 접근 권한을 가질 수 있게 되는 것으로, 시스템 A가 사용자에 대한 액세스 토큰 정보를 보관하지 않는다는 장점이 있다. 하지만, 시스템 B가 항상 신뢰할 수 있는 채널을 통해 인증기관에 접근이 가능한 온라인 상태여야 하며, 사용자-역할 할당과 역할-접근 권한 할당을 모두 조합하여 처리해야 한다는 부담이 있다.

3. 액세스 토큰의 구조

RBAC은 여러 사용자를 등록, 수정 및 삭제하고 사용자에 따라 역할을 할당하고 관리하는 것이 핵심이라고 할 수 있다. 앞서 설명한 바와 같이 IEC62351-8의 Push 모델은 시스템 A와 B 그리고 인증기관 간에 사용자 정보, 역할 정보 등을 전달하기 위해서 액세스 토큰을 사용한다. 액세스 토큰은 X.509 ID 인증 방식과 X.509 속성 인증 방식, 그리고, 소프트웨어로 구현하는 방식으로 구현될 수 있다. X.509 인증 방식은 공개키 기반(PKI)의 ITU-T 표준으로 인증서를 발행하기 위한 인증기관의 정밀한 계층적 시스템을 취하고 있으며, X.509 속성 인증

〈표 2〉 IEC62351-8에 제시된 역할-권한 할당

Value	Role \ Right	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMGMT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
〈0〉	VIEWER	X			X							
〈1〉	OPERATOR	X	X		X				X			
〈2〉	ENGINEER	X	X	X	X		X	X		X		
〈3〉	INSTALLER	X	X		X		X			X		
〈4〉	SECADM	X	X	X			X	X	X	X	X	X
〈5〉	SECAUD	X	X		X	X						
〈6〉	RBACMNT	X	X					X		X	X	
〈7...32767〉	Reserved	For future use of IEC defined roles.										
〈-32768 .. -1〉	Private	Defined by external agreement. Not guaranteed to be interoperable.										

방식은 누가 서명하고 인증서의 유효성에 대한 입증 시도 등을 했는지를 확인할 수 있는 기능과 다른 토폴로지를 지원하는 유연성을 추가한 확장 기능을 가지고 있다. 그리고, 소프트웨어로 구현하는 방식은 커베로스 인증 방식에 쓰이는 것과 비슷하며, 컨트롤러 기반의 저사양의 산업제어시스템을 위해 사용될 수 있다. 액세스 토큰에는 사용자 정보와 역할 정보 외에도 각 구현 방식에 따른 암호화 정보도 포함하고 있다. X.509 ID 또는 속성 인증방식을 사용하는 경우에는 서명 알고리즘과 서명 값이 추가되어야 하며, 소프트웨어로 구현하는 경우에는 해쉬 알고리즘과 키의 길이, 해쉬 값 정보가 추가되어야 한다.

4. 액세스 토큰의 전송

RBAC에 사용되는 액세스 토큰의 전송 방식은 세션 기반 전송 방식과 메시지 기반 전송 방식으로 구분된다. 세션 기반 전송 방식은 TLS 등과 같이 두 시스템 간에 인증체계를 가진 통신망이 구축되어 있는 경우 적용 가능하며, 메시지 기반의 경우에는 RBAC의 자격 증명이 각각의 메시지 내용에 암호화되어 있다.

세션 기반의 경우, 초기 인증 및 권한을 부여하기 위한 명령 교환 시, 일련의 바인딩 암호를 수행하기 위한 시간이 소요된다. 상기 과정은 세션 당 한 번만 실행이 되고, 인증을 받고 난 후에는 빠른 동작이 가능하다는 장점이 있지만, 여러 사용자 마다 별도의 세션을 생성해야 한다는 단점을 가지고 있다.

메시지 기반의 경우, 메시지 내에 암호화되어 저장된 역할 증명의 내용을 확인하기 때문에, 동일한 전송 계층 및 혼합된 다른 역할을 가진 접속에 대해서 세션에 의존적이지 않아 별도의 세션을 구현하고 유지하는 부담이 적다는 장점이 있는 반면에 각 메시지 단위로 디지털 서명을 생성하고 검증하기 위해 많은 시간이 소요된다는 단점이 있다.

세션 기반과 메시지 기반 전송 방식은 서로 상반적인 장단점을 가지고 있기 때문에, 시스템 설치 환경을 고려하여 전송 방식을 적용해야 한다.

Ⅲ. 역할기반 접근 제어 연구 동향

시스템이 확장됨에 따라 관리해야 하는 자원은 많아지게 되며, 이를 지원하기 위한 많은 정책과 요구사항이 생기게 된다. RBAC이 사용자마다 허가된 접근 권한에 대해 역할이라는 중간 매개체를 두어 사용자-권한 할당의 수를 줄일 수 있을 뿐만 아니라, 권한 부여의 편의를 제공하는 등 효율적이고 안정적으로 관리하기 위해 만들어졌음에도, 다양한 요구를 수용하기 위한 정책을 수립하고 운용하기 위한 연구는 계속 되고 있다. 본 장에서는 여러 가지 RBAC의 확장 기법, 검증 단계의 프레임워크 등의 관련 연구 동향을 소개하기로 한다.

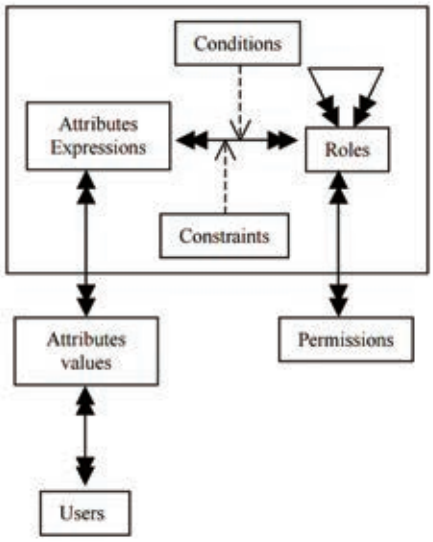
산업제어시스템이 확장되면서 관리해야 하는 자원이 많아지며, 이를 위한 많은 정책과 요구 사항을 관리해야 한다. RBAC을 통해 사용자-권한 할당 쌍의 수를 줄일 수 있지만, 다양한 요구 수용을 위한 정책 수립 및 운용에 대한 연구가 지속될 필요가 있다.

기존 RBAC의 정책보다 조금 더 다양하게 생성하고 유지하기 위한 방법으로 GRBAC (Generalized RBAC) 모델이 연구되었다. GRBAC은 접근 제어 결정 단계에서 사용자 역할, 자원 역할, 환경 역할 등으로 구분하고 이를 이용하여 다양한 사용자, 자원 및 시스템 상태에 대한 보안 관련 정보를 취합하고 구성하는 방식이다[2].

- 사용자 역할 – 일반 RBAC과 유사한 의미로서 보안 정책을 정의하는데 사용될 수 있으며, 사용자의 보안 관련 특성을 추상화함
- 자원 역할 – 자원의 종류 또는 민감도 등 자원의 다양한 속성을 추상화함
- 환경 역할 – 접근 제어의 중재를 위해 사용될 수 있으며, 시간, 시스템 부하 등과 같은 환경 정보를 수집함
- 트랜잭션 – 〈SRole, ORole, ERole, op〉의 포맷을 가지고 있으며, 세 역할의 정보를 이용하여 수행할 특정 동작을 결정함

예를 들어 "A"라는 사용자(SRole)가 "B"라는 자원(ORole)에 대해 "주중에만"(ERole) "쓰기"(op)가 가능하

〈그림 4〉 TRBAC 구조



〈그림 5〉 RB-RBAC model

도록 한다고 구성을 하면, 그에 해당하는 정책은 〈A, B, 주중, 쓰기〉 와 같이 표현될 수 있다.

그리고 이와 유사한 방법으로 특히, 시간 정보에 의해 접근 제어 정책이 결정될 수 있는 방향에 대한 연구가 있었다. 이는 특정 역할의 사용자가 특정 기간에만 해당 역할로서 접근 권한을 갖게 하는 것으로, 예를 들어 쓰기 권한을 가진 근무자가 근무시간 동안에는 쓰기 권한을 사용할 수 있지만, 근무시간 이후에는 그 권한이 해제되어, 근무자가 책임질 수 없는 시간에 발생될 수 있는 문제를 극복할 수 있도록 하기 위한 것이다. 이를 위해 TRBAC(Temporal RBAC)이라는 모델을 이용하여 역할 사이에 시간의 종속성을 부여하였다. 〈그림 4〉를 보면, 주기적으로 역할의 활성화 및 비활성화를 하기 위해 Role Trigger Operation 이라는 개념을 사용한 것을 확인할 수 있다. Role Trigger Operation은 정해진 시간에 의해 실행 또는 연기될 수 있으며, 충돌을 해결하기 위해 활성화와 비활성화 동작에 우선순위를 부여할 수 있도록 설계되었다[3].

다양한 환경 조건에 맞는 접근 제어를 실현하기 위해서 TRBAC을 확장한 ERBAC (Event-driven RBAC)모델

〈표 3〉 IEEE DBP3에 제시된 역할-허가 할당

Value	Name	Permissions						
		Monitor data	Operate controls	Transfer data files	Change config	Change security config	Change code	Local login
〈0〉	VIEWER	Yes	No	No	No	No	No	No
〈1〉	OPERATOR	Yes	Yes	No	No	No	No	No
〈2〉	ENGINEER	Yes	No	R/W/D	Yes	No	No	No
〈3〉	INSTALLER	Yes	No	R/W	Yes	No	Yes	Yes
〈4〉	SECADM	No	No	No	No	Yes	Yes	Yes
〈5〉	SECAUD	Yes	No	R	No	No	No	Yes
〈6〉	RBACMNT	Yes	No	D	Yes	Roles only	No	No
〈7...32767〉	Reserved	For future use.						
〈32768〉	SINGLEUSER	Yes	Yes	R/W/D	Yes	Yes	Yes	Yes
〈32769 .. 65535〉	Private	Defined by external agreement. Not guaranteed to be interoperable.						

이 연구되었다[4]. 이 모델은 여러 가지 사건에 대해 조건이 충족되면, 그에 해당하는 접근 제어를 허용하는 방식으로 기존의 RBAC의 접근 제어 정책보다 세밀하게 정책을 수립할 수 있다는 특징을 갖는다. 또한 ERBAC을 이용하여 수립된 정책 간의 충돌 등을 검증하고 이를 수행하기 위한 구성을 최적화하기 위한 프레임워크로 정수 프로그래밍 기반의 추론 방법[5]의 연구가 진행되고 있다.

〈그림 5〉의 RB-RBAC (Rule-Based RBAC)[6]은 동적으로 정의된 규칙의 유한 집합을 기반으로 각 역할에 사용자를 할당할 수 있는 모델로, 사용자가 가지는 속성 값을 이용하여 조건 또는 제약 사항을 확인한 후에, 역할에 맞는 권한을 허락하는 방식으로 동작된다. 더 나아가, 역할의 계층 구조를 유도하여 그것들 사이에서 서열 관계를 가지도록 하는 속성 기반의 AB-RBAC (Attribute-Based RBAC)모델에 대한 연구로 발전되고 있다[7].

그 밖에도 미국 국립표준기술연구소에서 통합 표준을 위한 RBAC으로 4단계의 모델을 제시하고 있는데, 각 단계는 하위 단계의 내용을 수용하는 방식으로 각 보안 수준에 맞추어 적절한 단계의 RBAC 모델이 채택된다[8].

- Flat-RBAC : RBAC의 본질적인 측면에서의 구현 모델이지만, 다수 개의 사용자-역할 할당과 역할-권한 할당 기능을 지원하며, 사용자는 동시에 다중 역할에 대한 권한을 사용할 수 있음
- Hierarchical RBAC : Flat-RBAC의 기능에 더하여 계층적인 역할을 지원하며, 임의 또는 제한된 계층에 대한 지원이 포함됨
- Constrained RBAC : Hierarchical RBAC의 기능에 더하여 업무 분리에 따른 제약 기능이 추가됨
- Symmetric RBAC : Constrained RBAC의 기능에 더하여 사용자-역할 할당에 효과적인 성능을 낼 수 있는 허가-역할 할당 지원

그 밖에 보안처리를 위한 사전 프로세싱에 사용하기 위한 Dual Bloom Filter를 이용한 검증 프레임워크[9]와 Role Key Layer에 서명, 확인, 암호화 등 다양한 보안 기능을 지원하는 계층적 역할키 기반의 암호화 RBAC 시스템에 대한 논문[10] 등과 같이 RBAC을 보완하고, 확장하기 위한 다양한 연구가 계속되고 있다.

Ⅳ. 역할기반 접근 제어의 산업시스템 적용 방안

IEEE DNP3 표준은 IEC62351-8에서 제시된 기본 개념을 준수하여 RBAC을 정의하고 있지만, 권한 대신에 허가(Permission)라는 용어를 사용하고, IEC 62351-8에서 제시한 역할과 권한의 관계 〈표 2〉를 〈표 3〉와 같이 수정하여 제시하고 있다[11]. 또한 DNP3에서는 전체 권한을 가지고 있는 슈퍼유저로서 SINGLEUSER라는 역할이 추가되었으며, IEC62351-8에서는 권한을 11개로 분류하였으나 DNP3에서는 권한을 7개로 축소하여 분류하였다.

DNP3의 경우 기능 코드와 객체의 조합의 수가 약 3,000개에 이르며, 개발자는 자체적으로 각 각각의 권한과 역할이 충돌하지 않도록 관리해야 한다. 특히 산업제어시스템은 각 장비의 성능보다 신뢰성이 가장 중요하고, 현장에서 사용중인 저사양의 장비에 대한 보안 알고리즘이 필요하다.

DNP3 표준에서는 각각의 권한(허가)을 어떤 운용과 객체로 연결해야 하는지에 대한 구체적인 예는 제시하고 있지 않고 있기 때문에, RBAC 구현 시 이에 대한 정책적인 접근과 연구가 필요하다. 예를 들어 DNP3의 경우 운용은 기능 코드(Function Code)로, 객체는 객체 그룹과 변형 (Object Group and Variation)으로 정의하고 있으며 기능 코드와 객체의 조합의 수가 약 3,000개에 이른다. 개발자는 자체적으로 각각의 권한과 3,000여개의 운용 및 객체를 보안적인 측면에서 충돌하지 않게 연결하고, 연결 정보를 효율적으로 관리하는 방안을 결정해야 한다.

RBAC을 산업제어시스템에 적용하기 위해서는 산업제어시스템의 특성을 고려해야한다. 산업제어시스템은 각 장비의 성능도 중요하지만, 신뢰성이 제일 중요하기 때문에, 현장에는 고도의 신뢰성 테스트를 마친 비교적 낮은 사양의 장비가 여전히 사용되고 있으며, 일괄적으로 플랫폼을 변경하는 것은 쉽지 않다. 그러므로 RBAC을 적용

함에 있어서도 기존 시스템의 통신 및 동작에 문제를 일으키지 않도록 하위 호환성을 유지하면서 보안의 수준을 높일 수 있는 방안에 대한 연구가 필요하다. 예를 들어 사양이 낮고 고도의 신뢰성이 요구되는 현장 장비가 사용되는 산업제어시스템에 RBAC을 적용하는 경우, 현장 장비와 인증기관이 항상 온라인 상태를 유지하여야 하는 Pull 모델보다는 현장 장비의 프로세싱에 대한 부담이 적은 Push 모델이 적합하다고 할 수 있다. 액세스 토큰의 구성 및 관리 측면에서도 X.509의 PKI 기반 인증서 방식보다는 소프트웨어 기반의 액세스 토큰을 구현하는 방법도 고려되어야 하며, 액세스 토큰의 전송 방법에 있어서도 일반 네트워크 환경에서 많이 사용되는 세션 기반의 전송 방식보다는 각 개별 메시지에 보안 정보가 들어있도록 하여 개별 메시지 별로 보안에 대한 범위를 가지는 메시지 기반의 방식을 이용하여 구현하는 것이 적절하다.

Ⅴ. 결 론

지금까지 산업제어시스템의 보안을 위해 개발된 IEC62351-8의 RBAC 모델을 소개하고, 관련 연구 논문들을 살펴보았다. RBAC은 접근 제어 기술에서 발전된 형태이지만, 이를 기반으로 효율적인 관리, 정책 구성, 정책 간 충돌 등에 대해 세부적으로 더욱 보완 및 발전되어 왔다. 산업제어시스템을 위한 접근 제어 방법으로 RBAC을 적용할 경우에는 적용하고자 하는 업무 및 시스템에 대한 정책적인 접근과 연구가 필요하며, 시스템의 환경 및 하위 호환성, 각 장비의 암호화 및 프로세싱에 대한 처리 능력 등 상호간의 상충관계를 고려하여 적용할 필요가 있다.

참 고 문 헌

[1] IEC: 62351-8 Ed. 1.0 Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control (Draft) (2011)

[2] MOYER, Matthew J.; ABAMAD, Mustaque. Generalized role-based access control. In: Distributed Computing Systems, 2001. 21st International Conference on. IEEE, 2001. p. 391-398.

[3] BERTINO, Elisa; BONATTI, Piero Andrea; FERRARI, Elena. TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security (TISSEC), 2001, 4.3: 191-233.

[4] BONATTI, Piero; GALDI, Clemente; TORRES, Davide. ERBAC: event-driven RBAC. In: Proceedings of the 18th ACM symposium on Access control models and technologies. ACM, 2013. p. 125-136.

[5] SHAFIQ, Basit, et al. A framework for verification and optimal reconfiguration of event-driven role based access control policies. In: Proceedings of the 17th ACM symposium on Access Control Models and Technologies. ACM, 2012. p. 197-208.

[6] AL-KAHTANI, Mohammad, et al. A model for attribute-based user-role assignment. In: Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002. p. 353-362.

[7] AL-KAHTANI, Mohammad A.; SANDHU, Ravi. Induced role hierarchies with attribute-based RBAC. In: Proceedings of the eighth ACM symposium on Access control models and technologies. ACM, 2003. p. 142-148.

[8] SANDHU, Ravi; FERRAIOLO, David; KUHN, Richard. The NIST model for role-based access control: towards a unified standard. In: ACM workshop on Role-based access control. 2000.

[9] SCHREIVER, Jacob. Role Based Access Control and Authentication for SCADA Field Devices Using a Dual Bloom Filter and Challenge-response. 2012. PhD Thesis. University of Louisville.

[10] ZHU, Yujia, et al. Role-based cryptosystem: a new cryptographic RBAC system based on role-key hierarchy. Information Forensics and Security, IEEE Transactions on, 2013, 8.12: 2138-2153.

[11] IEEE: std 1815-2012 IEEE Standard for Electric Power systems communications – Distributed Network Protocol(DNP3), IEEE, 2012

박 경 원

- 2004년 2월 한국산업기술대학교 전자공학 학사
- 2014년 9월~현재 동국대학교 정보통신공학 석박사통합과정
- 2014년 9월~현재 동국대학교 부호 및 암호 연구실 연구원
- 2004년 2월~2009년 4월 Network S/W Engineer
- 2009년 5월~현재 포텍 마이크로 시스템, Technical Support & Field Application Engineer

〈관심분야〉
Network, Embedded System, Cryptography, Smart Grid, RBAC

임 대 운

- 1994년 8월 KAIST 전기및전자공학과 학사
- 1997년 2월 KAIST 전기및전자공학과 석사
- 2002년 8월 서울대학교 전기컴퓨터공학부 박사
- 1995년 9월~2002년 8월 LS산전 중앙연구소 선임연구원
- 2006년 9월~현재 동국대학교 정보통신공학과 부교수

〈관심분야〉
암호학, 제어시스템보안