https://doi.org/10.5392/JKCA.2022.22.09.064

OT제어망에서 다중 제어시스템 접근통제용 공개키 기반 운용자 인증 방안

Public Key-Based Operator Authentication Mechanism for Access Control of Multi-Control Systems in OT Control Network

김대휘, 조인준
배재대학교 사이버보안학과

Dae-Hwi Kim(ds5rid@naver.com), In-June Jo(injune@pcu.ac.kr)

요약

운용기술 중심의 OT제어망내의 다중 제어시스템들에 접근하는 방법은 각각의 제어시스템이 제공하는 운용자 인증기술을 사용한다. 그 예로 ID/PW 운용자 인증기술을 들 수 있다. 이 경우 OT제어망은 다중 제어시스템으로 구성되기 때문에 각각 제어시스템별로 운용자 인증기술이 적용되어야 한다. 따라서 운용자는 자신이 관리하는 제어시스템별로 인증정보를 관리해야 하는 불편을 감수해야한다. 이러한 문제 해결을 위해 비즈니스 중심의 IT망에서는 SSO기술을 사용한다. 하지만, 이를 OT제어망에 그대로 도입할 경우 OT제어망의 제한된 규모 및 신속한 운용자 인증 등의 특성이 반영되지 않아 현실적인 대안으로 볼 수 없다. 본 논문에서는 이러한 문제를 해결하고자 운용자인증기술로 공개키 기반 인증방안을 새롭게 제안하였다. 즉, OT제어망내의 모든 제어시스템들에 동일하게 적용되는 하나의 통합 공개키 인증서를 발행하고 이를 모든 제어시스템에 접근할 경우 활용함으로써 운용자의 인증정보관리의 단순화 및 제어시스템에 접근을 보다 효율적이고 안전하게 하였다.

■ 중심어 : | OT제어망 | 운영자 인증기술 | 공개키 | 다중 SCADA제어시스템 | 보안 |

Abstract

The method of accessing multiple control systems in the OT control network centered on operation technology uses the operator authentication technology of each control system. An example is ID/PW operator authentication technology. In this case, since the OT control network is composed of multiple control systems, operator authentication technology must be applied to each control system. Therefore, the operator must bear the inconvenience of having to manage authentication information for each control system he manages. To solve these problems, SSO technology is used in business-oriented IT networks. However, if this is introduced into the OT control network as it is, the characteristics of the limited size of the OT control network and rapid operator authentication are not reflected, so it cannot be seen as a realistic alternative. In this paper, a public key-based authentication mechanism was newly proposed as an operator authentication technology to solve this problem. In other words, an integrated public key certificate that applies equally to all control systems in the OT control network was issued and used to access all control systems, thereby simplifying the authentication information management and making access to the control system more efficient and secure.

■ keyword : | OT Control Network | Operator Authentication | Public key | Multi SCADA Control Systems | Security |

* 본 논문은 2022학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임
접수일자 : 2022년 07월 18일
심사완료일 : 2022년 08월 19일
수정일자 : 2022년 08월 08일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

일반 비즈니스 정보처리 중심의 IT(Information Technology)망과 스마트 공장 및 시설 등의 제어정보처리 중심의 OT(Operational Technology)제어망을 구성하는 범용/제어시스템들에 대해 사용자/운용자의 접근통제는 중요한 쟁점 사항이다. IT망에서 사용자 접근제어를 위해 사용자를 인증하는 기술로는 ID/PW, 인증서, 보안카드, OTP(One Time Password), 지문, 얼굴인식, 전화인증 등을 들 수 있다. 하지만, IOT(Internet Of Thing) 중심의 4차 산업혁명에서 새로운 쟁점으로 부각된 OT제어망에서 운용자 접근제어는 IT망에서 초기에 사용되었던 초보적인 ID/PW인증기술이 적용되는 실정이다. 이는 비즈니스 정보처리 영역으로부터 시작하여 진화된 것이기 때문에 현재 활용중인 인증기술들은 IT망 환경에 적응적이다. 즉, 이들 기술들이 제어정보 처리중심의 OT제어망 환경에서 여러 측면에서 부적절할 수 있다.

제어정보처리가 중심인 OT제어망 환경의 주요특성을 살펴보면 IT망 환경과 비교하여 보다 강화된 보안성과 가용성을 요구한다. 여기에서 강화된 보안성은 외부해커(블랙햇 해커)가 인터넷을 통해서 혹은 내부 운용자 해커(하드햇 해커)가 SCADA(Supervisory Control And Data Acquisition)제어시스템을 직접 해킹할 수 없도록 보안체제를 갖추어야 한다는 것이다. 이를 위해서 보다 강화된 물리적, 기술적, 관리적 보안체계가 요구된다. 다음으로 최고의 가용성은 앞에서 전제한 최고의 보안성 보장이란 전제하에서 어떤 상황에서든 365일 24시간 SCADA제어시스템이 가용할 수 있는 환경을 갖추어야 한다는 것이다[1].

이에 대한 보안대책으로 정부는 외부해커(블랙햇 해커)를 격리시키기 위해 외부 인터넷과 내부 업무망 및 OT제어망의 분리를 원칙으로 하고 있다[2]. 이는 각각의 망 분리를 통해서 외부인터넷으로부터 침입하는 수많은 블랙햇 해커들을 원천적으로 차단하여 내부 업무망 및 OT제어망의 안전성 확보를 최대의 정책적 목표로 한 것으로 판단된다[3][4].

이렇게 분리된 OT제어망은 내·외부 해커(블랙햇, 하드햇 해커)로부터 안전성 확보를 위해 여러 보안쟁점들이 존재한다. 여기에서 가장 기본적인 보안기술은 제어시스템에 접근 허용 유·무를 결정하는 운용자 인증기술이다. 하지만, 현재의 OT제어망 환경에서 운용자 인증기술은 비즈니스 정보처리가 중심인 IT망 환경에서 사용된 인증기술을 그대로 사용하고 있는 실정이다. 따라서 OT제어망 환경의 특성이 반영된 보다 강화된 인증기술이 필요하다.

결론적으로 본 논문에서는 OT제어망의 보안성 강화를 위한 하나의 방안으로 SCADA제어 시스템만의 특성을 반영한 공개키 기반 다중제어시스템용 통합 인증방안을 새롭게 제안하였다. 이를 통해서 폐쇠망으로 운용되는 OT제어망 운용자들이 단일의 제어시스템마다 인증정보를 관리해야하는 번거로운 부담을 제거함과 동시에 해커에 의한 해킹을 최소화할 수 있어 OT제어망의 특화된 새로운 인증기술로 자리매김이 가능할 것으로 사료된다.

II. 연구배경

OT제어망의 특성을 반영하여 운용자 인증기술을 설계하고 구현을 위해서는 전체적인 네트워크 보안모델 측면에서 OT제어망을 조망해볼 필요가 있다.

현재까지 언급되고 있는 모델은 크게 3가지이다. 그 첫 번째는 “퍼듀(Purdue) 보안모델”이다. 이는 2004년 ISA99위원회에서 제시한 것으로 스마트공장 보안의 이론적 배경을 설명하기 위한 것이다[1]. 둘째, “ICS-CERT의 ICS 참조모델”이다. 이는 ISA/IEC 62443(ANSI/ISA-95)에서 정의한 모델로 산업제어시스템 네트워크 참조모델이다[2]. 마지막 세 번째는 국가보안기술연구소(NSR, National Security Research Institute)가 제시한 “ICS 운영환경”을 들 수 있다[그림 1].

이들 3가지 모델 모두에서 공통점은 [그림 1]에서 보듯이 OT제어망을 IT망과 망 분리를 원칙으로 하고 있다는 점이다. 이는 IT망으로부터 OT제어망을 고립시켜 외부로부터 공격을 시도하는 블랙햇 해커의 공격을 원천적으로 차단을 위한 구성으로 볼 수 있다.

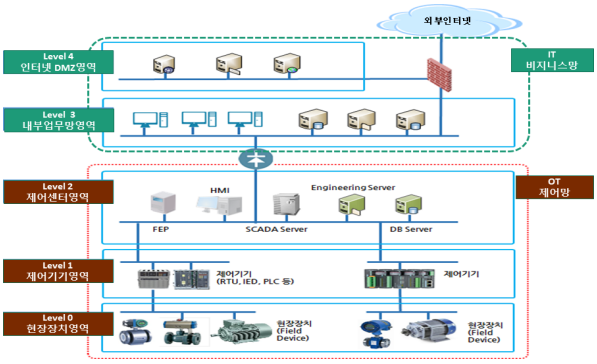

그림 1. NSR의 ICS 운영환경 모델

하지만, OT제어망의 특성과 IT망의 특성이 다름에도 불구하고 현재 OT제어망에서 채택된 보안기술들은 그동안 IT망에서 사용된 것을 그대로 사용하고 있는 것이 현실이다. 이러할 경우 OT제어망의 특성들이 충분히 반영되지 않아 기능, 비용, 복잡성 등에서 괴리 현상이 발생한다.

OT제어망이 기본적으로 갖추어야 할 보안기술은 유·무선 제어네트워크 접근제어, 제어네트워크 보안, 제어시스템보안, 제어시스템 로그관리 등을 들 수 있다. 이들 중에서 OT제어망에 특화된 운용자 인증기술을 참고문헌[6]에서 새롭게 제안하였다. 즉, OT제어망의 운용자들의 특성과 IT망 사용자의 특성을 서로 비교하여 OT제어망에 특화된 운용자 인증방안이다. 이 제안에서는 OT제어망 운용자의 특성을 4가지로 전제하고 제안한 방안이다. 첫째, 운용자를 특정할 수 있다. 둘째, 사용하는 단말장비를 특정할 수 있다. 셋째, 사용위치를 특정할 수 있다. 넷째, 보다 엄격한 운용자인증이 요구된다는 점을 반영한 것이다.

하지만, 참고문헌[6]에서 제안한 운용자 인증기술은 단일 제어시스템을 대상으로 적용이 가능한 기술이다. 따라서 전체적인 OT제어망에 다수의 제어시스템에 통합적으로 적용이 가능한 운용자 인증기술로 볼 수 없다. OT제어망에서 개별 제어시스템에 적용되는 운용자 인증기술 보다는 모든 제어시스템에 통합적으로 적용이 가능한 운용자 인증기술이 필요한 이유는 다음과 같다.

OT제어망은 고 보안성과 고 가용성을 전제로 한다[5]. 첫째, 이를 위해서는 제어시스템별 운용자 인증보다는 하나의 OT제어망의 제어시스템들에 대해 통일된 운용자인증이 합리적이라고 볼 수 있다. 둘째, 각각의 제어시스템 별로 운용자를 분산관리 보다는 특정 OT제어망에 소속된 모든 운용자를 중앙집중식 인증관리가 필요하다는 점을 들 수 있다. 셋째, 통일된 운용자 인증관련 로그를 유지하고 분석이 가능하게 함으로써 OT제어망에서 운용자인증관련 특이사항 발생 시 신속한 대처가 필요하다는 점을 들 수 있다. 넷째, 제어시스템 추가 및 철거 시 통합 운영자 인증기술이 운용자 추가 및 관리가 용이하다는 점을 들 수 있다.

결론적으로 상기에서 살펴본 특성들이 시사하는 바는 OT제어망에 특화되고 효율적인 운용자 인증기술을 필요로 한다는 점이다. 이러한 해결책 제안이 본 논문의 연구배경이다.

Ⅲ. OT제어망에 특화된 새로운 통합 운용자 인증방안

1. 제안 인증기술의 주요 내용

OT제어망에 소속된 제어시스템들에 대해 통합적으로 적용이 가능한 기술로 OT제어망 전용 공개키 기반 PKI(Public Key Infrastructure)기술을 들 수 있다[8]. 공개키 기반 PKI기술은 현재 우리사회에서 친숙하게 사용 중인 금융인증서, 공동인증서, PASS인증서 등과 같은 공인/공동인증서를 통한 사용자인증기술을 말한다[7]. 이는 정부가 위임한 신뢰할 수 있는 공인/공동인증서발행기관(CA, Certification Authority)을 통해서 발행한 공인/공동인증서로 공용성이 있는 특정 시스템에 대해 자신을 인증하는 기술이다. 이를 특정기관이나 폐쇄망내 시스템들의 사용자 인증용으로 사용하기에는 여러 문제점들이 상존한다. 첫째는 공용성이 있는 인증서를 조직 내에서만 영향이 한정된 특정업무에 사용한다는 모순을 들 수 있다. 둘째는 인증서 발행이 공인/공동인증서 발행기관을 통해서 이루어지고 관리된다는 점이다. 이는 조직 내의 각종 업무의 특성에 따라 신속하게 인증업무가 이루어져함을 간과한 것이다. 셋째, 공인/공용인증서를 종합관리 하는 PKI는 국가적 차원에서 공동으로 활용하고자 하는 업무에 활용할 목

적으로 만들어졌기 때문에 IETF(Internet Engineering Task Force)와 같은 국제표준을 철저히 준용하고 있다. 따라서 조직 내부에서만 사용할 목적으로 할 경우에는 불필요한 요소들이 많은 것이 사실이다. 넷째, 공인/공용인증서는 비즈니스 업무중심의 IT망 시스템들의 사용자인증에는 안정적인기술로 보인다. 하지만 OT제어망과 같이 제어정보처리 중심의 폐쇄망 환경에서는 그 적절성이 검증되지 않은 점을 들 수 있다.

본 논문에서는 상기와 같은 문제점들 때문에 적용이 어려운 공인/공동인증서 지원 PKI기술을 대체할 수 있는 OT제어망 전용 사설 PKI인증기술을 제안하였다. 제안한 인증기술은 폐쇄망으로 운영되는 OT제어망으로 한정되기 때문에 PKI기술에 대한 IETF표준을 엄격히 준용하기 보다는 OT제어망의 특성을 충분히 반영되도록 조정하여 제안하였다. 제안 기술의 핵심내용을 살펴보면 다음과 같다.

첫째, OT제어망을 구성하는 모든 제어시스템들에 동일하게 적용이 가능한 통합인증기술을 제안한 점이다. 현재는 각 제어시스템마다 각자의 ID/PW 운용자 인증기술을 사용하는 것이 일반적이다. 이 경우 각 시스템마다 운용자가 인증정보를 기억하여 인증절차를 거쳐야하는 번거로움이 따른다. 또한 패스워드의 안전성을 확보하기 위해서는 운용자가 직접 주기적인 패스워드 갱신 부담도 따른다. 따라서 OT제어망 전용인증서를 소유케 하여 모든 제어시스템에 적용함으로써 이러한 문제를 해결할 수 있다.

둘째, 특정 OT제어망 운용자가 특정 제어시스템에 접근통제 및 그 제어시스템 내 특정업무에 접근통제가 가능하도록 하였다. 즉, 현재 공인/공용인증서는 X.509 표준을 준용하여 활용되고 있다. 본 제안에서는 이 표준에서 불필요한 부분을 제거하고 특정제어시스템의 특정업무까지 접근통제가 가능하도록 수정하였다.

셋째, 한 기관의 OT제어망에 신뢰할 수 있는 인증서 발행기관인 CA를 하나 두도록 하였다. 이는 한 기관의 OT제어망을 전제로 한 것이기 때문에 다른 CA들과 상호인증 등의 필요성도 없고, 일관된 인증서 발행 및 인증서 검증 등이 용이하기 때문이다.

넷째, 고도의 보안성과 가용성을 지원하기 위해서는 운용자 인증로그 관리가 중요하다. 모든 인증관련 로그가 하나의 CA에서 관리 되도록 중앙 집중화하여 로그 분석의 효율성 및 응급 시 대처가 용이하도록 하였다.

다섯째, 비즈니스중심의 IT망에서 사용자 인증기술은 불특정한 사용자가 스스로 인증등록 절차를 거치도록 설계되어 있다. 이는 불특정한 모든 사용자가 대상이 되기 때문에 블랙리스트 기반의 복잡한 인증절차가 필요하다. 하지만 OT제어망에서는 정해진 소수의 운용자를 대상으로 하기 때문에 OT제어망 제어시스템 관리자가 총괄적으로 운용자를 특정하여 특정제어시스템 및 그 제어시스템 내의 특정업무에 대해 접근제어권한을 관리할 수 있다. 따라서, 소수의 운용자를 대상으로 한 화이트리스트 기반으로 인증기술 구현이 가능하다. 즉, 시스템 관리자에 의해 관리되는 운용자들 외에 모든 운용자는 인증대상에서 제외하는 기법을 사용한다. 이렇게 함으로써 운용자 인증절차를 단순화 하면서 저비용으로 운용이 가능하다.

본 논문에서는 이러한 4가지 핵심내용을 반영하여 화이트리스트 운영자 인증기술을 구현하였다. 즉, 저비용으로 인증의 효율을 제고하고, 원천적으로 블랙 및 하드 햇 해커를 차단하도록 하였다.

2. 제안 운용자인증 방안의 기본 동작

I장의 서론에서 현재 OT제어망에서 운용자 인증기술의 현안 문제점을 정리하였고, II장의 연구배경에서 OT제어망의 특성 때문에 비즈니스 중심의 IT망에서 사용자 인증기술이 OT제어망에 적합지 않다는 점을 요약하였다. 본 논문에서 제안하는 새로운 운용자 인증방안의 적용은 제어중심의 특정 OT제어망으로 제한하였다.

본 논문에서 제안한 운용자 인증기술은 레벨 2의 제어센터에 설치된 각종 센터장비에 접근하여 운영하는 소수의 특정된 운용자를 대상으로 적용되는 기술이다. 이는 운용자가 레벨 1 제어기기와 레벨 0의 현장장치 제어 행위는 제어센터의 각종 제어시스템들을 통해서 이루어진다는 점이다. 따라서 레벨 2에 위치하는 제어센터 장비에 대해서 보다 엄격한 운용자 통제가 이루어져야 한다.

제안한 인증방안의 기본동작은 [그림 2]와 같다. 여기에서 기본동작절차는 관리자가 OT제어망 통합운용자

정보를 반영하여 OT제어망내의 다중제어시스템용 인증서를 발행하여 OT망 운용자 인증서저장소 및 운용자가 각각 소유하고 있다는 전제하에서 설명을 하였다.

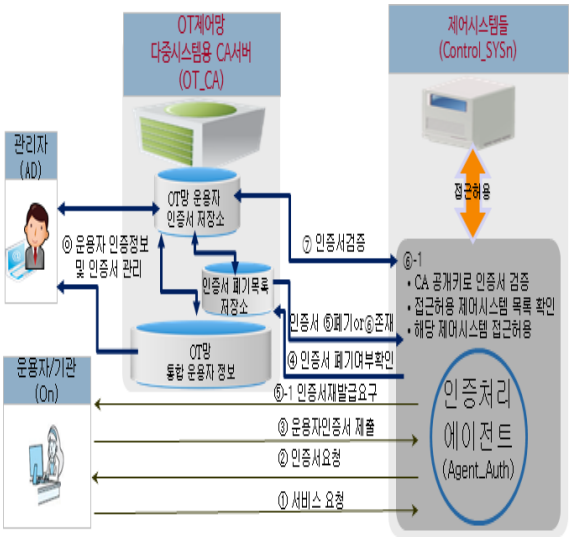

그림 2. OT제어망 인증기본 동작 제안

첫째, ①운용자가 운용하고 하는 제어시스템에 접근서비스를 요청한다. ②이를 제어시스템의 인증서에이전트가 수신하여 인증서를 요청한다. ③운용자는 자신이 소지한 인증서를 인증서 에이전트에게 제출한다. ④인증서를 수신한 인증서 에이전트는 OT제어망 다중시스템용 CA서버에게 인증서폐기목록에 수신된 운용자 인증서의 존재유무를 확인한다. ⑤ 폐기된 경우는 인증처리에이전트에게 폐기로 전달하고 이를 수신한 인증처리에이전트는 ⑤-1 운용자에게 인증서 재발행절차를 거치도록 안내한다. ⑥ 폐기되지 않은 경우는 ⑥-1처럼 인증서 검증절차를 거친다. 인증서를 검증하고 적격한 인증서이면 인증서에 기록된 제어시스템목록을 검사하여 존재하면 제어시스템에 접근이 허용된다.

3. OT제어망용 인증서형식 설계 및 생성방안

잘 알려진 바와 국제표준으로 정의된 공인/공동인증서는 [표 1]과 같은 X.509 인증서 형식을 준용한다.

이 형식의 특징은 특정기관으로 제한된 인증서가 아니라 월드와이드로 사용을 목적으로 만든 것이기 때문에 특정기관의 OT제어망으로 한정된 사설 인증서로는 적절치 않다.

표 1. X.509 인증서형식

항목명	필수/옵션	설명
Version	필수	버젼(V3)
SerialNumber	필수	고유일련번호
Signature Algorithm	필수	발행자 서명알고리즘
Issuer	필수	DN형식 발급자정보
Validity	필수	유효기간
Subject	필수	DN형식 소유자/기관 정보
SubjectPublicKeyInfo	필수	소유자 공개키
SubjectAltName	필수/옵션	DN형식이아닌 소유자/기관정보
PolicyMappings	옵션	다른 정책과 연결 정보
NameConstraints	옵션	
PolicyConstraints	옵션	인증서 경로 제약사항
IssuerAltName	옵션	DN형식이아닌 발행자/기관정보
AuthorityKeyIdentifier	옵션	발급자 키 이름
BasicConstraints	필수/옵션	이인증서가 다른 인증서를 발급 권한 유무
CRLDistributionPoints	옵션	CRL을 얻을 수 있는 장소
KeyUseage	옵션	공개키 용도(서명, 부인방지, 전자서명, 키 교환 등)
Certificate Signature	필수	상기항목을 발행자의 개인키로 서명한 결과

이러한 OT제어망이란 특수환경을 반영하여 제안한 인증서 형식은 [표 2]와 같다.

표 2. OT제어망용 인증서형식 제안

항목명	값	설명	범위별 명칭	
SerialNumber	N	고유일련번호	On 인증 정보	운용자(on)의 인증서 (On_Cert)
Signature Algorithm	(SHA_256, RSA)	발행자 서명알고리즘		
Issuer	OT_CA	발행자 정보		
Operator	On	소유자/기관 정보		
Subject Public Key	On_Pubkey	소유자/기관 공개키		
System List	SLn(Options)	접근허용 시스템 목록		
Subject Public Key Usage	(Auth, KEx)	공개키 용도(서명, 부인방지, 전자서명, 키 교환 등)		
Certificate Signature	OT_CA_sig_On	상기 On인증정보에 발행자의 개인키로 서명한 결과		

제안의 특징은 OT제어망 운용자는 불 특정인이 아니라는 점이다. 즉, 특정한 운용자만이 제어시스템에 접근하기 때문에 X.509인증서형식에서 불필요한 항목을 대폭제거하고 꼭 필요한 항목으로 최소화한 것이다.

[표 2]에서 운용자의 인증서(On_Cert)는 다음과 같이 표시할 수 있다.

On_Cert={N+(SHA256,RSA)+OT_CA+On+On_Pubkey+SLn(options)+(Auth, KEx)+OT_CA_sig_On)}

이들 중에서 중요한 항목 몇 가지를 설명하면 다음과 같다. 다섯번째 항목인 운용자 On의 공개키인 On_Pubkey는 운용자 On 자신이 생성한 키 쌍(공개키(On_Pubkey), 개인키(On_Prikey))중에서 전자를 말한다. 즉, 운용자 On은 자신이 생성한 공개키(On_Pubkey)를 OT제어망 인증서발행기관(OT_CA)의 공개키(OT_CA_Pubkey)로 암호화하여 OT_CA에게 보낸다. 이는 운용자 On의 인증서인 On_cert 발행을 OT_CA에게 요청하는 행위이다. 이를 요청받은 OT제어망 인증서발행기관(OT_CA)는 자신의 개인키(OT_CA_Prikey)로 복호화하여 운용자 On의 공개키인 On_Pubkey를 얻는다. 이를 토대로 OT_CA는 운용자 On의 인증서인 On_Cert 생성작업을 시작한다. 다음으로 인증서를 구성하는 서명알고리즘 (SHA256, RSA)의 의미는 이 인증서가 길이가 길기 때문에 RSA 서명알고리즘의 특성상 서명에는 많은 시간이 걸리기 때문에 인증서(On_Cert)를 SHA256으로 해쉬하여 256비트 해쉬코드를 얻기 위해 필요한 알고리즘들을 적시한 것이다. 다음으로 SLn(Options)은 운용자 On이 접근할 수 있는 제어시스템 목록들의 집합이다. 여기에서 옵션은 특정제어시스템에 접근할 수 있는 단말기 식별자나 운용자 접속허용 위치범위 등을 추가하여 보다 강화된 접근통제를 선택적으로 할 수 있도록 하였다. 다음으로 (Auth, KEx)는 이 인증서의 용도를 인증과 키 교환용으로 만 사용한다는 의미이다. 마지막으로 OT_CA_sig_On는 OT_CA가 SHA256알고리즘을 이용하여 운용자 “On의 인증정보”를 대상으로 256비트 해쉬값(H256_On_Cert)을 생성하고, 생성된 256비트(즉, H256_On_Cert)에 OT_CA자신의 개인키인 OT_CA_Prikey로 전자서명 한 값이다.

다음 설명들에서 사용되는 표기는 [표 3]과 같이 정의된 의미를 지닌다.

표 3. 표기법

부호	의미
OT_CA	OT제어망 다중시스템용 CA서버
Control_SYSn	특정 제어시스템 n
AD	관리자(Administrator)
On	특정 운용자(Operator) n
Agent_Auth	인증(Authentication)처리 에이전트
On_Pubkey	운용자 On의 공개키
On_Prikey	운용자 On의 개인키
OT_CA_Pubkey	OT_CA의 공개키
OT_CA_Prikey	OT_CA의 개인키
On_Cert	운용자 On의 인증서
(SHA256, RSA)	인증서 서명에 필요한 알고리즘들
(Auth, KEx)	인증서용도(서명, 키교환)
OT_CA_sig_On	OT_CA가 On_Cert에 전자서명값
H256_On_Cert	On_Cert의 SHA 256비트 해쉬값
RSAprikey(m)	RSA알고리즘으로 m을 전자서명
RSApubkey(m)	RSA알고리즘으로 m을 암호화
AESkey(m)	AES알고리즘으로 m을 암·복호
s_key	한 세션에서만 사용되는 세션키

4. OT제어망에 운용자 인증기능 설계

본 논문에서 새롭게 제안한 운용자 인증방안에서 핵심이 되는 운용자 등록절차, 인증절차, 인증정보 재구성 절차에 관해 세 가지 모듈 설계내용을 설명하면 다음과 같다.

(1) OT제어망 인증기관(OT-CA)에 운용자(On) 등록 및 공개키인증서/개인키 파일 발행절차

본 절에서는 운용자(On)을 최초로 OT제어망 인증서 발행기관에 등록하고, 자신의 인증서를 확보하는 절차에 대해 설명한다. 즉, 운용자(On)이 직접 OT제어망 총괄관리자(AD)를 통해서 OT제어망 인증기관(OT_CA)로부터 운용자(On)의 인증서(On_Cert)를 생성하여 OT_CA의 인증서저장소에 저장하고, 인증서파일과 개인키 파일을 생성하여 자신의 인증서에 이를 저장하는 절차에 대하여 설명한다. 이에 대한 자세한 절차는 [그림 3]과 같다. 보다 상세하게 단계별 절차를 살펴보면 다음과 같다.

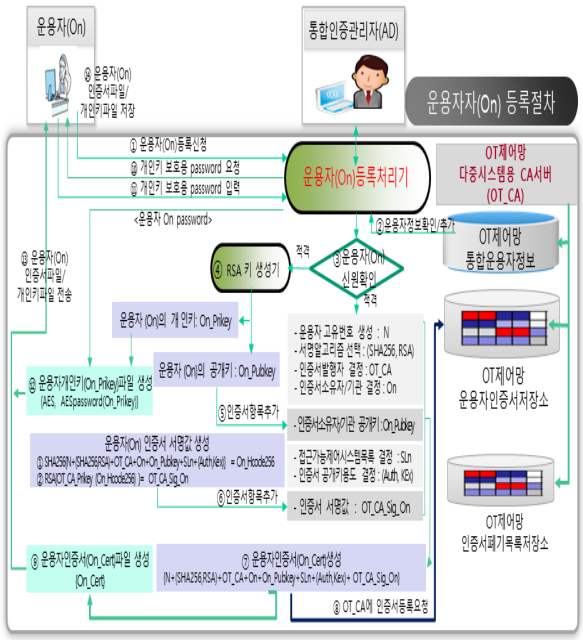

그림 3. 운용자(On) 등록 및 공개키 인증서/개인키 파일 발행절차

Step1) 운영시스템(SYSn)을 총괄시스템관리자(AD)가 운용자(On)을 등록하는 첫 번째 절차이다. 등록은 반듯이 운용자(On)이 총괄시스템관리자(AD)에게 요청을 통해서 이루어진다. 이는 인증서 발행기관(OT_CA)이 운용자(On)에게 발행한 인증서(On_Cert)간에 신뢰관계를 확보하기 위함이다. ①시작은 운용자(On)이 총괄시스템관리자(AD)에게 인증서 발행을 요청한다. 이를 수신한 ②③총괄시스템관리자(AD)는 운용자(On)을 확인한다. 그리고 사용할 공개키 알고리즘을 결정하고, 이에 적용할 ④공개키(On_Pubkey)와 이에 대응하는 개인키(On_Prikey)를 생성한다.

Step2) 다음으로 Step1)에서 생성된 ⑤공개키(On_Pubkey) 및 ⑥운용자(On)의 인증서 서명값을 생성한다. 그리고 ⑦운용자 인증서(On_Cert)를 생성하고 이를 ⑧OT_CA에 등록한다. 이와 더불어 ⑨[표 2]와 같은 형식의 공개키 인증서 파일을 생성한다. 이에 대한 상세한 절차는 3.3절에서 설명하였다.

Step3) 다음으로 Step1)에서 생성된 개인키(On_Prikey)를 안전하게 보전하기 위한 개인키 파일을 생성한다.

파일형식은 PKCS#8을 부분적으로 준용하여 다음과 같은 구문형식을 취한다.

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
  encryptionAlgorithm EncryptionAlgorithmIdentifier,
  encryptedData       EncryptedData}
```

여기에서 EncryptedData는 아래에 정의한 PrivateKeyInfo 내용을 기밀키로 암호화한 결과이다.

```
PrivateKeyInfo ::= SEQUENCE {
  privateKeyAlgorithm   PrivateKeyAlgorithmIdentifier,
  privateKey            PrivateKey}
```

요약하여 정리하면 운용자(On)의 개인키 파일은 두 부분으로 나누어 설명이 가능하다. 첫째, 개인키 정보를 암호화한 암호알고리즘 식별자 부분이다. 둘째는 개인키를 서명용 혹은 복호용으로 사용할 경우 이에 해당하는 공개키 알고리즘 식별자와 그리고 운용자(On)의 개인키(On_Prikey)를 운용자 On이 제시한 비밀키로 암호화한 부분이다.

따라서 ⑩운용자(On)등록처리기는 운용자의 개인키(On_Prikey)를 보호하기 위해 운용자(On)에게 개인키 보호용 패스워드를 요청하고 ⑪이를 받아 상기의 구문에서 처럼 개인키를 암호화한다. 마지막으로 이를 ⑫개인키 파일로 만들게 된다.

Step4) 시스템총괄관리자(AD)는 ⑬운용자(On)에게 Step2와 Step3)에 생성된 2개 파일을 운용자(On)에게 제공하고 ⑭이를 운용자(On)이 보관한다.

(2) 제어시스템(Control_SYSn)에 운용자(On) 인증 절차

본 절에서는 제어시스템(Control_SYSn)에 운용자 On이 (1)절의 절차에 따라 OT_CA에 등록되고, 운용자 On이 자신의 공개키인증서 파일과 개인키 파일을 소지하고 있다는 전제하에서 시작된다. 운용자 On이 특정 제어시스템 (Control_SYSn)에 인증을 요구할 경우 이루어지는 인증절차는 [그림 4]와 같다. 보다 상세하게 단계별 절차를 살펴보면 다음과 같다.

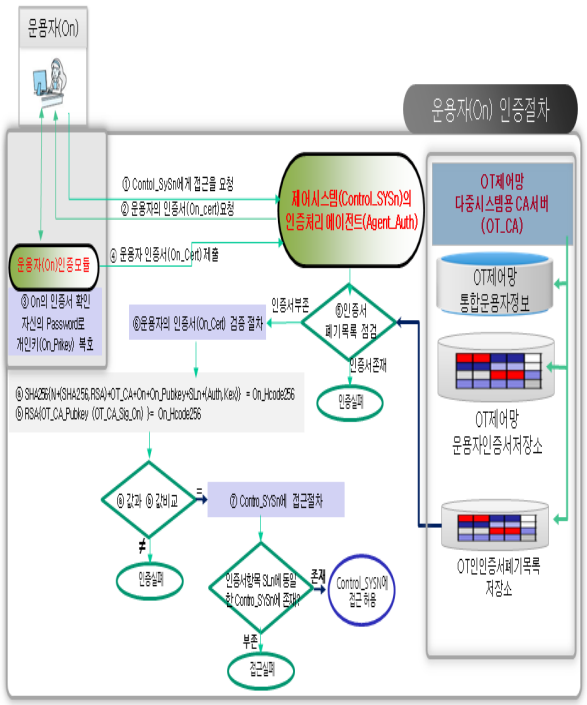

그림 4. 제어시스템(Control_SYSn)에 운용자(On) 인증절차

Step1) 운용자(On)가 특정 제어시스템(Control_SYSn)의 로그-인 화면을 클릭하여 ①제어시스템(Control_SYSn)에 로그-인 의사를 그 제어시스템에 미리 설치된 인증처리 에이전트(Agent_Auth)에게 보낸다.

Step2) 이를 수신한 그 제어시스템의 ②인증처리 에이전트(Agent_Auth)는 운용자 On에게 자신이 소유한 공개키인증서(On_Cert)를 요청한다.

Step3) 이를 요청 받은 ③운용자 On은 자신이 알고 있는 패스워드를 입력하여 ④자신이 소유한 공개키 인증서(On_Cert)를 접근하고자 하는 제어시스템(Control_SYSn)의 인증처리 에이전트(Agent_Auth)에게 보낸다.

Step4) 이를 수신한 제어시스템(Control_SYSn)의 인증처리 에이전트(Agent_Auth)는 ⑤ OT-CA에게 On_Cert가 인증서 폐기목록에 존재 유무를 검사한다. 존재하지 않으면 ⑥ 인증서검증절차인 Step5)를 시행하고 존재하면 폐기된 인증서임을 운용자 On에게 알리고 종료한다.

Step5) 운용자 On의 공개키인증서(On_Cert)를 OT_CA의 공개키를 사용하여 다음과 같이 서명 검증한다. 운용자의 인증서(On_Cert)는 다음과 같이 표시할 수 있다.

$$On\_Cert=\{N+(SHA256,RSA)+OT\_CA+On+On\_Pubkey+SLn(options)+(Auth,KEx)+OT\_CA\_sig\_On)\}$$

먼저 SHA256해쉬알고리즘을 사용하여 아래 ⓐ와 같이 'On인증서정보'의 해쉬값을 계산한다. 그리고 인증서 발행 시 OT_CA가 자신의 개인키로 ⓐ에서 계산된 'On인증정보' 해쉬값에 전자서명해서 그 결과를 OT_CA_sig_On으로 저장하고 있기 때문에 이를 아래 ⓑ와 같이 OT_CA의 공개키로 복호하여 해쉬값을 얻는다.

ⓐ $SHA256\{N, (SHA\_256, RSA), OT\_CA, On, On\_Pubkey, SLn, (Auth, KEx)\} = On\_Hcode256$

ⓑ $RSA_{OT\_CA\_Pubkey}(OT\_CA\_sig\_On) = On\_Hcode256$

이렇게 하여 얻어진 ⓐ과 ⓑ의 해쉬값을 비교하여 동일하면 OT_CA가 발행한 On의 공개키 인증서임이 검증된다.

Step6) 다음으로 ⑦On이 제어시스템(Control_SYSn)에 접근 허용유무를 결정하는 절차를 거친다. 이는 운용자 On의 인증서(On_Cert)를 구성하는 항목 중에 접근허용 가능 시스템목록(SLn(Options))에 현재 접근을 시도하는 제어시스템명이 존재하면 접근이 허용되고 존재하지 않으면 접근이 허용되지 않는다.

(3) 인증서 재발급 및 인증정보 재구성

본 절에서는 (2)절에서 운용자 On의 인증서가 OT_CA의 인증서 폐기목록에 등록된 경우 인증서 재발급 및 인정정보 재구성이 이루어진다. 인증서 폐기목록에 On의 인증서가 등록되는 경우는 2가지 경우이다. 첫째는 운용자(On)가 자신의 Password를 기억하지 못하거나 해킹 당했을 경우 폐기를 요청했을 경우이다. 둘째는 제어시스템 총괄관리자가 인증서를 강제로 폐기목록에 등록한 경우이다.

이에 대한 자세한 절차는 [그림 5]와 같다. 보다 상

세하게 단계별 절차를 살펴보면 다음과 같다.

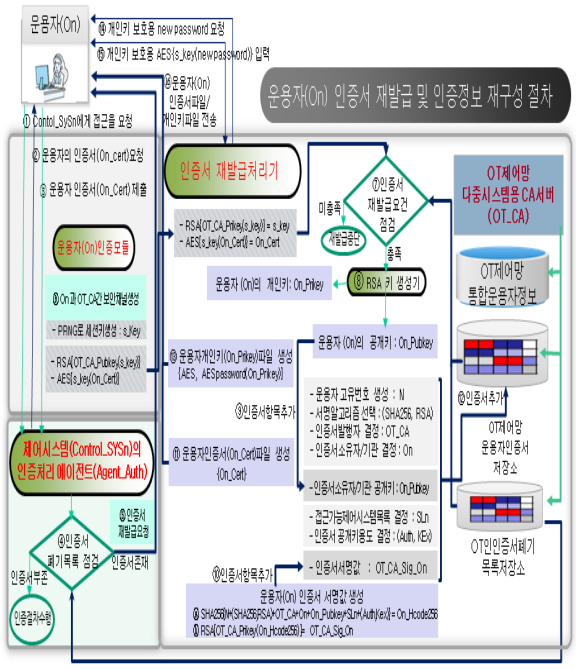

그림 5. 인증서 재발급 및 인증정보 재구성

Step1) 운용자 On이 제어시스템(Control_SYSn)에 접근하는 과정(①~③)에서 자신의 인증서(On_Cert)가 OT_CA에 의해 ④인증서 폐기목록에 등록되어 있음이 확인되면 ⑤제어시스템(Control_SYSn)의 인증처리 에이전트(Agent_Auth)는 운용자 On에게 인증서 재발급을 요청한다.

Step2) 이를 요청받은 운용자 On은 자신의 운용자(On)인증모듈을 통해서 ⑥운용자(On)과 제어망 인증기관(OT_CA)간에 보안채널을 생성한다. 그 절차는 다음과 같다.

운용자 On은 PRNG(Pseudo Random Number Generator)를 통해서 세션키 s_key를 생성한다. 생성된 s_key를 ⓐ과 같이 OT_CA_Pubkey로 암호화 하여 OT_CA에게 보낸다.

ⓐ $RSAo_{T\_CA\_Pubkey}(s\_key) = Cs\_key$

ⓑ $RSAo_{T\_CA\_Prikey}(s\_key) = s\_key$

이를 수신한 OT_CA는 ⓑ와 같이 자신의 개인키로 복호화하여 세션키 s_key를 얻게 된다.

이렇게 양자간에 분배된세션키(s-key)로 AES 대칭암호알고리즘을 이용하여 보안채널을 만든다. 이후 운용자 On과 OT_CA간에 전달되는 모든 메시지는 세션키 S_key로 암호 및 복호된다.

다음으로 만들어진 보안채널을 통해 운용자 인증서(On_Cert)를 제어망인증기관(OT_CA)에 보내어 인증서 재발급 절차를 거치게 된다.

Step3) 운용자 On으로부터 수신된 On_Cert가 ⑦인증서 폐기 목록에 존재하는지 확인한다. 확인이 되면 새로운 인증서 재발급을 위해 On_Cert를 재구성한다. 이때, ⑧운용자 On에서 사용할 새로운 RSA 공개키와 개인키 쌍을 생성한다. 이중에서 ⑨새롭게 만들어진 공개키를 On_Cert에 반영한다. ⑩새롭게 구성된 On_Cert를 SHA256으로 256비트 해쉬코드 얻는다. 얻어진 256해쉬코드를 OT_CA_Prikey로 전자서명하여 On_Cert에 추가한다. 이렇게 만들어진 On-Cert와 전자서명 값으로 이루어진 On의 ⑪인증서 파일을 완성한다. 그리고 이를 ⑫OT제어망 운용자 인증서저장소에 저장한다.

Step4) 다음은 ⑬운용자 On이 가져야할 개인키 파일을 생성한다. 그 절차는 (1)절에서 설명한 것과 같다. 여기에서 하나의 특징은 개인키를 암호화하는 패스워드를 이 과정에서 변경이 가능하다는 점이다. 이 절차는 다음과 같다. 먼저 생성된 보안채널을 통해서 ⑭개인키 보호용 "New Password"를 운용자 On에게 요청한다. 이를 요청받은 운용자 On이 새로운 패스워드를 입력하면 이를 운용자(On)의 ⑮인증모듈이 AES{s_key(New Password)}와 같이 새로운 패스워드를 암호화하여 OT_CA의 인증서 재발급처리기에 보낸다. 이를 수신한 OT_CA의 인증서 재발급처리기는 AES암호알고리즘을 사용하여 "New Password"를 얻고 이를 사용하여 운용자 On의 개인키를 다음처럼 암호화하여 개인키 파일을 완성한다.

{AES, AESnewpassword(On_Prikey)}

Step5) 이렇게 Step3 ~4)에서 만들어진 2개의 파일을 s_key로 암호화하여 ⑯운용자 On에게 보내면 이를 수신한 On은 s_key로 복호화하여 자신의 기존의 인증

서 및 개인키 파일을 대체하는 것으로 갱신을 마친다.

Ⅳ. 기존 방안과 비교 및 검토

이 장에서는 본 논문에서 새롭게 제안한 OT제어망용 운용자 인증기술을 2가지측면에서 비교 검토하였다. 첫 번째는 현재 범용적으로 사용 중인 공인/공동인증서기술이다. 두 번째는 IT망에서 가장 범용적으로 사용하는 ID/PW 인증기술, 그리고 참고문헌[6]의 제어망 인증기술을 서로 비교하여 제안방안의 우수성을 도출하였다.

첫 번째는 현재 범용적으로 사용 중인 공인/공동인증기술과 비교내용을 [표 4]와 같이 정리하였다.

[표 4]에서 보듯이 공인/공동인증서는 불특정사용자를 대상으로 외부의 신뢰기관이 인증서를 그 목적에 맞게 발행하고 관리하기 때문에 폐쇄망으로 운영되는 OT 제어망환경에서 활용은 매우 복잡하다. 즉, 망 분리가 되어있는 OT제어망 환경에서 망간 자료전송 보안규정에 따라 인증서발급, 갱신, 폐기 등이 이루어져야 하기 때문에 즉시성을 요구하는 제어망에서는 적합하지 않는 것으로 판단된다.

표 4. 기존 공인/공동인증서기술과 제안인증기술 비교분석

비교요소 \ 인증방법		공인/공동인증서기술	OT제어망 전용인증서기술
특징 1	발행대상	불특정 사용자	특정 운용자
	인증인자	신뢰CA가 발행한 인증서확인	신뢰CA가 발행한 인증서확인 + 접근허용제어시스템 목록
특징 2	인증서발행	외부신뢰 CA	내부 OT제어망 전용 CA
	인증서갱신	유효기간 (비용발생)	관리자 및 운용자 요구(무비용)
	용도	단일시스템 인증/ 1개 인증서	다중시스템인증/1개 인증서
	인증서형식	X.509표준형식 (복잡)	OT제어망용 독자형식(단순)
특징 3	인증정보등록 주체	관리자 + 운용자	관리자 + 운용자
	적용기술	불랙리스트 인증기술	화이트리스트 인증기술
	인증정보 관리	외부CA에 종속관리	내부 제어망CA 독자관리
종합	제어망용으로 활용 편의성	복잡 (제어망은 폐쇠망으로 운영)	적합 (제어망내 모든시스템에 단일인증서활용)

두 번째는 현재 IT망에서 가장 범용적으로 사용하는 ID/PW 인증기술, 그리고 참고문헌[6]의 제어망용 인증기술과 비교한 내용을 [표 5]와 같이 정리하였다. 정리된 [표 5]를 통해서 비교검토 한 내용을 정리하면 다음과 같다.

첫째 큰 특징은 기존 인증기술의 인증인자는 패스워드, 단말장치주소정보, 위치정보를 사용한다는 점이다. 하지만 제안기술은 인증인자로 OT전용인증서를 사용한다는 점을 들 수 있다. OT전용인증서 내에 접근이 허용되는 시스템목록과 각 목록에 옵션을 통해서 단말기식별자, 운용자 위치정보범위 등을 지정할 수 있도록 하여 참고문헌[6]의 인증인자를 지원이 가능하도록 하였다. 이를 통해서 참고문헌[6]수준의 엄격한 인증이 가능하도록 하였다.

표 5. 기존 인증기술과 제안인증기술 비교분석

비교요소 \ 인증방법		IT망에서 ID/PW 인증기술	OT제어망에서 참고문헌[6] 인증기술	OT제어망에서 새롭게 제안한 인증기술
특징 1	인증인자	패스워드	자동생성 패스워드, MAC주소, GPS정보	OT전용인증서
	단말인증	불가	가능	옵션추가 가능
	위치인증	불가	가능	옵션추가 가능
특징 2	인증대상	단일시스템	단일시스템	다중시스템인증
	주기적 PW 갱신	필요	불필요 (자동 갱신)	불필요
	사용자 편의성	저 (시스템별ID/PW입력)	중 (시스템별 ID만 입력)	고 (다중시스템에 단일인증서)
특징 3	인증정보등록주체	사용자	관리자 + 운용자	관리자 + 운용자
	적용기술	블랙리스트 인증기술	화이트리스트 인증기술	화이트리스트 인증기술
	인증정보 관리	복잡 (사용자 중심)	복잡 (관리자 중심)	단순 (통합관리자 중심)
종합	보안수준	하 (Only PW)	상 (Pw, 단말주소, 접근위치)	상 (OT전용인증서)
	인증 편의성	하 (주기적 갱신)	상 (앱을 통한 세션단위로 자동갱신)	상 (모든시스템에 단일인증서활용)

둘째 특징은 기존의 인증기술은 단일시스템에 적용이 가능한 기술인 반면에 제안 인증기술은 하나의 인증서로 다중의 제어시스템에 적용이 가능한 인증기술이란 점이다. 즉, 기존의 인증기술이 각 시스템별로 인증정보를 분산관리 함으로써 발생되는 하는 인증정보 불

일치로 인한 혼란, 운용자가 각각의 제어시스템별 인증정보 관리로 발생하는 혼란, 문제발생시 운용자 이벤트 추적의 혼란 등은 고도의 보안성과 가용성을 보장해야 하는 OT제어망에서는 결정적인 단점이다. 하지만, 새롭게 제안한 인증기술은 하나의 인증서로 모든 제어시스템을 대상으로 중앙집중적으로 관리되기 때문에 이러한 혼란들의 최소화가 가능하다.

마지막 특징은 기존의 ID/PW인증기술은 불특정다수가 스스로 자신이 사용할 시스템에 등록하여 승인절차를 거쳐 사용시스템의 사용자가 되는 절차를 거친다. 즉, 블랙리스트기반으로 인증기술을 적용한 것이다. 하지만 참고문헌[6]은 관리자가 허용한 운용자만 접근이 허용되는 화이트리스기반의 인증기술을 적용한 것이다. 본 논문에 새롭게 제안한 인증기술도 참고문헌[6]과 같은 화이트리스트기반 인증기술이다.

[표 5]에서 본바와 같이 본 논문에서 새롭게 제안한 OT제어망용 인증기술이 기존의 인증기술보다 여러 비교요소들에서 우수성을 보이고 있다. 이는 OT제어망 보안에 적합하도록 공개키 기반의 단일인증서를 새롭게 제시하고 그 인증서 내에 접근이 가능한 제어시스템 목록을 정의하여 다중시스템용 인증이 가능하도록 하였기 때문이다.

Ⅴ. 결론

본 논문은 OT제어망에 적합한 운용자 인증기술 개선에 관한 내용이다. 본 논문에서 새롭게 제안한 인증기술이 ID/PW인증기술과 참고문헌[6]의 OT제어망 인증기술들에 내제된 여러 문제점들을 해결할 수 있음을 보였다. 이중에서도 고도의 보안과 가용성을 보장해야하는 OT제어망의 특성을 고려할 때, 각 제어시스템별로 분산 인증정보 관리는 커다란 문제점으로 인식되어 왔다. 본 제안에서 공개키기반 PKI기술을 수정하여 OT제어망에 적합한 운용자인증서를 설계하고, 특정 운용자에게 하나의 설계된 인증서를 발행하고, 이를 통해서 다중제어시스템들에 접근할 수 있도록 하였다. 이를 통해서 중앙집중식 인증정보관리가 가능하여 기존의 분산 인증정보관리에 따른 여러 문제점들을 해결할 수 있는 방안을 새롭게 제시한 점도 성과라 볼 수 있다. 반면에 제안기술이 OT제어망에 새로운 공개키 기반 PKI 구축이란 추가적인 부담은 피할 수 없다. 하지만 이러한 부담에도 불구하고 기존의 ID/PW인증기술, 참고문헌[6]이 지니는 다양한 문제점들을 근본적으로 해결하기 때문에 충분히 유의미한 새로운 인증기술이라고 볼 수 있다.

향후 연구로는 제안기술을 특정 제어망에 직접 구현하여 학술적 관점에서 인증기술의 면밀한 검증과 더불어 실무적 관점에서 구현의 용이성 및 활용의 편의성 등의 검증이 필요하다. 마지막으로 새롭게 제안한 본 인증기술이 제품화되어 OT제어망에서 다중제어시스템용 운용자 인증기술로 자리매김 되길 기대한다.

참 고 문 헌

[1] Pascal Ackerman, *Industrial Cybersecurity,* Packt Publishing Limited, 2017.

[2] 김일용, 임희택, 지대범, 박재표, “산업제어시스템 환경에서 효과적인 네트워크보안모델,” 한국산학기술학회논문지, 제19권, 제4호, pp.664-673, 2018.

[3] 행정안전부, 국가정보원, 한국정보사회진흥원, *국가기관 망분리 구축 가이드*, 2008.

[4] 이은배, 김기영, “망 분리기반의 정보보호에 대한 고찰,” 한국정보보호학회지, 제20권, 제1호, pp.39-46, 2010(2).

[5] 이현정, 조대일, 고갑승, “망분리환경에서 안전한 서비스 연계를 위한 단방향 망간자료전송 시스템 보안모델연구,” Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol.5, No.6, pp.539-547, 2015.

[6] 조인준, “SCADA제어망에서 강화된 운용자 인증 방안,” 한국콘텐츠학회논문지, 제19권, 제12호, pp.416-424, 2019.

[7] 윤병남, 반형식, “공공분야의 정보보호- 공공분야의 공인인증서비스-,” 한국통신학회 정보보와통신 논문지, 제19권, 제8호, pp.20-29, 2002.

[8] 백종현, 김민정, 이진주, “지능형 교통시스템 보안아키텍쳐 및 PKI 인증체계연구,” 한국정보과학회 논문지, 제35권, 제1호, pp.32-36, 2017,

저 자 소 개

김 대 휘(Dae-Hwi Kim) 정회원

- 1995년 2월 : 대구대학교 물리학과 학사
- 2012년 2월 : 아주대학교 ITS학과 석사
- 2007년 ~ 2015년 : ㈜경봉(현, 시티랩스) 대표이사
- 2016년 ~ 현재 : 한국정보기술(주) 대표이사

〈관심분야〉 : ITS망 보안, 컴퓨터네트워크보안, ITS설계 및 구축

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1991년 ~ 현재 : 정보처리기술사(정보시스템응용)
- 2006년 ~ 현재 : 정보시스템수석감리원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 정보시스템응용기술