SCADA 시스템을 위한 보안기술 동향

송 경 영
울산과학대학교
전기전자공학부

Ⅰ. 서 론

산업제어시스템(Industrial Control System; ICS)이란 산업현장에서 이용하는 제어시스템으로, 센서의 측정값과 현장(field)에서의 운용 정보를 수집하고, 이 정보들을 처리/표시하고, 제어정보(control information)를 멀리 떨어진 장치(remote equipment)로 전달하는 역할을 하는 시스템을 말한다. 이러한 제어시스템의 예로 전력시스템, 석유공정시스템, 상하수도 시스템 등을 들 수 있다. 이러한 제어시스템은 스마트폰을 이용하여 가정의 조명을 점등하는 간단한 기능에서부터 원자력발전소에서 행해지는 다양한 설비의 운용과 같은 복잡한 기능을 수행하는 등 다양하다.

공압시스템 등 여전히 아날로그 방식으로 동작하는 제어시스템이 있지만, 최근에는 대규모 시스템 제어를 비롯한 대부분의 시스템의 제어는 컴퓨터를 기반으로 행해지고 있다. 최근에는 적대국, 테러리스트 집단 혹은 특별한 의도를 갖지 않고 단지 자신들의 보안 기술력을 과시하는 집단에 의해 행해지는 제어시스템에 대한 사이버 공격이 증가하는 추세이다. 이에 따라, 제어시스템 보안의 흐름은 '물리적 공격 방어'에서 '사이버 보안 강화'로 진화하고 있다.

SCADA 시스템은 산업 현장에서 이용하는 제어 시스템으로 지역적으로 분산되어 있는 시스템의 감시, 제어 및 데이터를 취득하는 정보통신 기반의 시스템을 의미한다.

제어시스템은 처리 영역에 따라 크게 분산제어시스템(Distributed Control Systems; DCS)와 원방감시제어 및 데이터취득(Supervisory Control And Data Acquisition; SCADA) 시스템으로 나눌 수 있다. DCS는 일반적으로 한 지역 혹은 작은 지역에서 운용하는 제어시스템

인데 반해, SCADA 시스템은 지역적으로 분산되어 있는 시스템의 감시제어와 데이터를 취득하는 시스템을 말한다. 시스템이 대형화되고 복잡해지면서 SCADA 시스템과 산업제어시스템은 용어적으로 큰 구분 없이 사용되고 있다. 이 후로 본고에서는 산업제어시스템과 SCADA 시스템을 구분하지 않는다.

본고는 다음과 같은 순서로 SCADA 시스템의 보안기술 동향을 설명하고자 한다. 2장에서는 SCADA 시스템의 구성 및 SCADA 시스템의 대표적인 예인 전력시스템의 통신 프로토콜의 표준화 에 대해 설명한다. 3장에서는 SCADA 시스템 관련 보안 사고를 소개하고, 보안위협 요소를 설명한 후, SCADA 시스템의 보안성 강화를 위해 최근 연구되고 있는 요소기술에 대해 설명한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. SCADA 시스템이란?

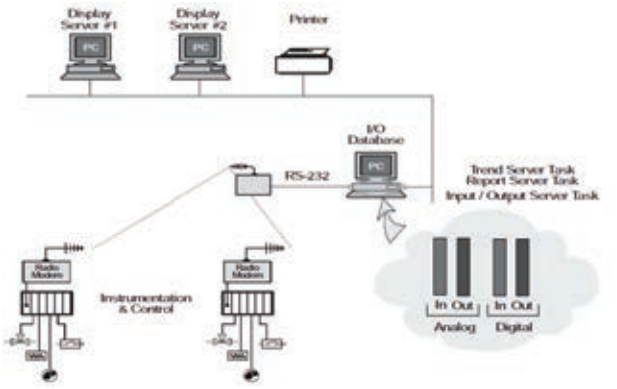
1. SCADA 시스템의 구성

초창기의 SCADA 시스템은 기기 및 장치의 외부에 표시되는 미터기 혹은 스트립 차트 레코더 등을 이용하여 데이터를 취득하였다. 다양한 제어 밸브를 운용하는 운영자는 이렇게 취득한 데이터를 바탕으로 감시 제어를 직접 수행하였다. 이러한 방식의 감시 제어 및 데이터 취득은 현재까지도 일부 공장에서 사용되고 있다.

> SCADA 시스템의 현장 데이터 수집 전송을 위한 원격단말(RTU), 데이터를 수집해 처리하는 주단말(MTU), 그리고 인터페이스 및 네트워크로 구분된다.

산업이 급속도로 발전하면서 공장은 대형화되고 자동화되고 있다. 이러한 공장이나 공정의 대형화는 수 많은 센서가 존재를 의미하고, 관련 데이터 취득 과정이나 감시 제어 과정이 복잡해짐을 의미한다. 또한 전력시스템과 같이 현장과 제어실의 거리 이격이 큰 경우도 많다. 이에 따라 SCADA 시스템의 개념도 근본적인 변화를 격게 되었다.

하나의 SCADA 시스템은 현장의 데이터를 수집하고, 그 데이터를 통신시스템을 통해 주단말장치(Master Terminal Unit; MTU)로 전송하는 다수의 원격단말장치(Remote Terminal Unit; RTU), HMI, network 등으로



〈그림 1〉 SCADA 시스템 개념도

구성되며, 〈그림 1〉은 SCADA 시스템의 개념도를 나타낸 것이다.

- MTU는 RTU로부터의 데이터를 수집 및 저장하고 RTU로의 송신을 관리하며, 운영자와의 인터페이스를 통해 현장 감시 및 제어 기능을 제공하며, 각종 경보 및 사건 기록 등을 수행한다.
- HMI(Human-Machine Interface)는 운영자를 위한 콘솔로 경보, 제어 화면, 상태 화면, 상태 화면 리포트 등을 위한 GUI 환경을 통해 데이터 표시, 제어, 연산 등의 기능을 제공한다. 〈그림 1〉에서의 Display server 등은 이 기능을 수행하는 예로 볼 수 있다.
- RTU는 원격지의 IED(Inteligent Electronic Device) 관리를 담당하며, 하위 장비(PLC(Programmable Logic Controller), DCS, IED 등)로부터 수집된 자료를 각 시설의 상태 정보를 취합하여 MTU로 전송한다.
- SCADA 시스템의 데이터 취득 및 감시제어는 다양한 네트워크를 통해 이뤄진다. 종래에는 RS232나 RS485 등의 시리얼 통신이 주가 되었지만 최근에는 Ethernet을 활용한 통신 뿐 아니라 Bluetooth와 ZigBee와 같은 다양한 통신망을 이용하고 있다.

2. SCADA 시스템을 위한 프로토콜

SCADA 시스템을 위한 통신 프로토콜은 매우 다양하다. 최근에는 전력제어시스템을 위한 프로토콜의 표준화

가 활발하게 진행되고 있다. 그 중 대표적인 전력제어시스템용 프로토콜을 소개한다.

2.1. Modbus 프로토콜

Modbus는 1979년에 Modicon사(현재, Schneider Electric)가 구축한 OSI 제7 계층인 응용 계층(Application Layer) 메시지 프로토콜로서 다른 형태의 버스와 네트워크로 연결된 디바이스 간의 클라이언트/서버 통신을 지원한다. 또한 Modbus 프로토콜은 PLC와의 통신을 위해 만든 프로토콜로서 PLC가 동시에 인지할 수 있는 데이터 형태의 수가 제한되어 있다.

Modbus 프로토콜을 이용하여 통신하는 모든 디바이스들은 하나의 통신 링크에서 유일한 주소를 부여받는다. 이 프로토콜은 북미와 유럽에 700백만 이상의 노드에 설치되어 있지만, 데이터 값의 Time Stamp가 없고, 방해 이벤트가 생겼을 때 알려주는 방식이 없어 디바이스 간의 공통적인 데이터 포맷이 없는 단점을 가지고 있다. 최근에는 기존의 시리얼 통신과 함께 이더넷 통신을 지원하는 새로운 프로토콜인 Modbus-TCP가 추가되었다.

SCADA를 위한 통신 프로토콜들에는, Modbus, IEC 60870, DNP3 가 있으며, 이더넷 통신 및 TCP/IP 프로토콜을 지원할 수 있다. 현재 제어 시스템에 대한 보안 침해 사고가 지속적으로 증가되고 있으며, 국가간 외교 전쟁으로 비화될 가능성이 있다.

2.2. IEC 60870

IEC 60870-5는 1990~1995년에 국제전기기술위원회(IEC: International Electro-technical Commission) TC(Technical Committee) 57이 전력시스템을 위한 제어, 보호 및 그와 관련된 통신을 위해 제정한 표준을 말한다. IEC 60870-5는 유럽, 중동 및 아시아 지역에서 주로 채택된 프로토콜로 지금까지 현장에 설치된 대부분의 RTU들은 IEC60870 프로토콜을 필수적으로 지원하고 있다.

2.3. DNP3 프로토콜

DNP3(Distributed Network Protocol)는 IEC 60870-5의 표준화이전, SCADA 관련 제조사들이 상호 운용성이 필요하여, 1993년에 Westronic사(현재, GE Harris)가 부분적으로 완성한 표준이며, 이후 미국전기전자통신학회 (IEEE)가 DNP3를 IEEE Std. 1815로 채택하였다.

DNP3 표준화 이전의 프로토콜은, 타 제조사 간 호환이 되지 않고, 단방향 통신이었으므로, 다양한 장비가 접목되고 양방향 제어가 필수적인 SCADA 제어 시스템에는 적합하지 않았다. IEC60870과 달리 DNP3는 북미와 남미, 남아프리카, 호주 지역에서 수 처리와 오일, 가스 설비 제어용으로 주로 채택되며 산업현장의 RTU들은 D이러한 DNP3는 기기제어와 감시에 기반하여 설계된 프로토콜(Protocol)로 보안성을 가지고 있지 않아 해킹에 취약성을 갖고 있다.

최근에는 실행 비용 및 엔지니어링 작업의 감소를 통한 비용 절감을 목표로 IEC 60870과 DNP3 표준을 통폐합한 IEC 61850이 제정되었다.

Ⅲ. SCADA 시스템 보안

1. 보안 사고 사례

해외의 제어시스템에 대한 보안 침해 통계 자료를 보면 2002년~2008년까지 누적된 보안 침해 사례는 보고된 것만 38,000여 건에 이르며, 2009년 이후로 지속적으로 보안 침해 사고가 증가하고 있다. 2009년 4월 CNN의 보도에 의하면 미국 전력망에서 적성국가에서 설치한 것으로 보이는 악성코드가 발견되었으며, 이 코드는 전기공급을 차단할 수 있는 것으로 알려졌다. 2010년 이후부터는 석유, 가스, 전자통신 및 금융시스템에서도 악성코드가 발견되는 등 주요 산업제어시스템에 대한 해킹시도가 광범위하게 퍼져나가고 있는 상황이다.

미국의 제어시스템 영역별 보안 침해 비율을 살펴보면 전체의 41%는 에너지 분야이며, 15%가 수도, 10%가 상용제어시스템으로 나타났다.

대표적인 보안 침해 사례는 스턱스넷(Stuxnet)을 들 수 있다. 이란 원전 시설의 파괴로 약1,000여개의 원심분리기가 스턱스넷(Stuxnet)에 의해 고장이 남으로써 이란

〈표 1〉 제어시스템 위협 형태

구 분	설 명
공격자 (Attacker)	실력 과시 및 스릴을 위해 네트워크 침입을 시도할 수 있다. 현재 공격 스크립트 및 프로토콜을 인터넷을 통해 쉽게 구할 수 있기 때문에 전문적인 지식 없어도 쉽게 공격을 수행할 수 있다.
봇-넷 (Bot-network)	공격을 조직화하고 피싱, 스팸, 악성코드를 유포하여 해커가 마음대로 제어할 수 있는 좀비 PC들의 네트워크이다.
피셔 (Phishers)	금전적 이익을 목적으로 스팸, 스파이웨어/멀웨어를 이용하여 계정 탈취 및 정보 취득을 시도한다.
스팸 전파자 (Spammers)	상품 판매, 피싱 수행, 스파이웨어/멀웨어 유포, DoS 공격 수행을 위해 수신인이 원하지 않는 잘못된 정보 및 정보를 숨긴 이메일을 퍼뜨린다.
내부자 (Insiders)	– 불만을 품은 내부 직원은 사이버 범죄의 주요근원이다. – 내부자는 목표 시스템에 제한 없이 접근을 할 수 있기 때문에 풍부한 지식 없이도 정보를 획득하거나 시스템 침해를 야기할 수 있다. – 내부 위협은 내부 직원뿐 아니라 아웃소싱 벤더 및 비즈니스 파트너 등도 포함되며, 불완전한 정책, 절차, 테스팅은 제어시스템에 영향을 줄 수 있다. – 제어시스템의 침해사고는 내부자의 실수로 인해서도 높은 확률로 발생한다.
테러리스트 (Terrorists)	국가안보를 위협하기 위해 제어시스템을 파괴하거나 불능상태로 만든다. 이것은 다수의 사상자를 유발하고, 국가 경제에 타격을 주고, 국가 신뢰도에 영향을 미친다.
산업스파이 (Industrial spies)	기업 기밀에 대한 지적자산 및 노하우 취득을 목적으로 한다.

핵 프로그램에 상당한 타격을 가할 수 있는 것으로 보고되었다.

SCADA 시스템에 대한 공격은 국가간의 외교 전쟁으로 비화될 수 있다. 2012~2013년 사이 중국군 61398부대가 미국의 수도, 전기, 가스 제어에 필요한 주요 정보를 탈취한 것으로 알려졌다.

우리나라에서는 2014년 12월 한국수력원자력의 정보유출 사고를 계기로 SCADA 시스템 등 폐쇄망 보안에 대한 기관 · 기업들의 관심이 높아지고 있다.

2. 보안 위협 형태 및 취약성

전력 제어시스템에 대한 보안 위협은 적국, 테러리스트, 산업스파이, 불만을 가진 직원, 악의적인 침입자 등에 의한 악의적인 위협과 시스템 복잡성, 사람에 의한 실수 및 사고, 장치 고장과 자연재해와 같은 자연적인 위협 등 다양한 위협 인자에 의해 발생할 수 있다. 악의적인 위협 및 자연적 위협으로부터 제어시스템을 보호하기 위해서는 심층 방어(defense-in-depth) 전략을 수립할 필요가 있다. 전력 제어시스템에 공격을 수행할 가능성이 있는 악의적인 위협의 유형은 〈표 1〉과 같다.

전력 제어시스템이 가지는 취약성은 아래와 같이 세 가지 분류의 취약성으로 구분해 볼 수 있다.

2.1. 정책 및 절차

제어시스템 보안에 관한 정책 및 구현 절차(Guide)가 불완전/부적절하거나 없는 경우에서 오는 취약성이다. 보안 정책 및 절차, 관리 지원은 보안의 기초이기 때문에 보안 정책은 패스워드 정책 또는 제어시스템에 연결 모뎀 등에 대한 보안 요구사항을 권고함으로써 취약성을 완화시킬 수 있다.

2.2. 플랫폼

하드웨어, 운영체제(OS), 제어시스템 애플리케이션을 포함하는 플랫폼의 결함, 잘못된 구성 또는 부실한 유지보수에서 오는 취약성이다. 이러한 취약성은 OS 및 애플리케이션 패치, 물리적 접근통제와 보안 소프트웨어(예, 백신)와 같은 다양한 보안 통제를 통해 완화될 수 있다.

2.3. 네트워크

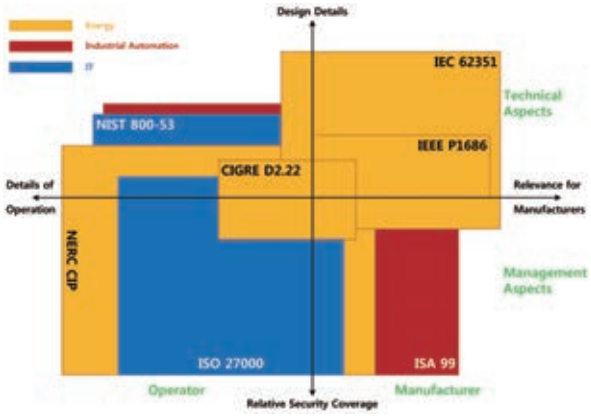
제어시스템의 네트워크의 결함, 잘못된 구성 또는 부실한 관리와 다른 네트워크와의 연결성으로 인하여 발생하는 취약점이다. 이러한 취약성은 심층 네트워크 설계, 통신 암호화, 네트워크 트래픽 제한, 네트워크 컴포넌트에 대한 물리적인 접근통제와 같은 보안 통제를 통해 제거 또는 완화될 수 있다.

3. SCADA 시스템을 위한 보안 표준

국가 중요기반 시설을 보호한다는 측면에서 전력 제어시스템 보안기술 개발의 필요성을 인식한 IEC, IEEE, P2030, SGIP(Smart Grid Interoperability Panel)등 국제 표준화기구는 보안 요구사항과 아키텍처를 정의하고 NIST 및 DHS는 전력 제어시스템 및 네트워크 간 상

〈표 2〉 전력제어시스템을 위한 보안 관련 표준

구 분	설 명
Security Profile for Advanced Metering Infrastructure	AMI(Advanced Metering Infrastructure)를 포함하는 지능형 전력망 제어 시스템에 대한 end-to-end 보안 요구사항
IEC 62351 Parts 1~11	전력 제어시스템의 운영에서 정보보안[8]
IEEE 1686-2007	IEDs, PLCs, RTUs 등의 제어장치에 대한 보안 권고사항
NERC CIP 002~009	대규모 전력 설비에 대한 사이버보안 강화 권고사항
NIST SP 800-53	연방 정보시스템 보안강화를 위한 종합적인 보안통제사항
NIST SP 800-82	안전한 산업 제어시스템 구축을 위한 보안 가이드라인



〈그림 2〉 전력제어시스템 표준의 영역별 활동

호운용성과 사이버 보안성 확보를 위해 표준 가이드 및 시험 · 인증 체계 개발을 지속적으로 진행하고 있다. 현재 IEC TC 57에서 정의하고 있는 전력 제어시스템을 위한 통신 프로토콜 표준은 IEC 60870-5 Series, IEC 60870-6 Series, IEC 61850 Series, IEC 61970 Series, IEC 61968 Series 등이 제정되었고 전력 제어시스템 및 네트워크 간 상호운용성과 사이버 보안성 확보를 위한 대표적인 표준 프레임워크가 NIST SP 1108 "NIST Framework and Roadmap for Smart Grid Interoperability Standard"가 적용되고 있으며, 현재는 버전 v3.0이 발표되었다. 〈표 2〉는 지능형 전력망 구축 시 사이버 보안성 확보를 위해 적용할 수 있는 표준을 정리하였으며, 〈그림 2〉는 표준의 영역별 활동을 에너지, 산업용, IT 관점으로 분류하여 운영측면, 설계측면, 관리적 측면으로 명시하였다. 또한, 지능형 전력망에서 IED 및 AMI에도 암호 · 인증 및 키 관리 기술의 개발 필요성을 인식하고 스마트그리드 보안 가이드라인 문서 "NIST IR 7628"을 통해 스마트그리드 시스템 및 네트워크를 위한 보안 가이드라인을 통해 스마트그리드 환경에 적합한 암호 · 인증 및 키 관리 요구사항을 언급하여 IEEE P1711에서는 지능형 전력망 환경에서 데이터 기밀성과 무결성을 함께 제공하는 블록 암호 모드인 PE(Position Embedding) 모드를 표준화하였다. 그리고 현재 EPRI, 록히드 마틴社, 캐나다 Ryerson대학, Honeywell International社는 지능형 전력망에서 기기 보안 인증과 검증 기법(Device Security Authentication), 권한 및 자원의 접근제어 기술(Access control of Resource and Authorization), 분산 역할기반 접근제어(Distribute RBAC) 기법, 역할기반 권한관리(RBAC) 시스템 개발을 위해 지속적으로 연구 중에 있다.

IEC, IEEE, P2030, SGIP 등 국제 표준화 기구에서는 전력 제어시스템을 위한 보안 요구사항과 보안 아키텍처를 정의하고 NIST 및 DHS는 전력 제어시스템 및 네트워크 간 상호운용성과 사이버 보안성 확보를 위해 표준 가이드 및 시험 · 인증 체계 개발을 지속적으로 진행하고 있다.

4. 보안성 강화를 위한 요소 기술

4.1. RBAC

RBAC은 컴퓨터 시스템 보안에서 권한이 있는 사용자들에게 시스템 접근을 통제하는 한 방법으로 1992년 Ferradiolo와 Kuhn에 의해 제안되었고, 2000 NIST RBAC 모델이 제안되었고, 2004년에 ANSI/INCITS 표준으로 제정되었다. IEC 62351-8은 전력시스템의 접근제어를 다루고 있다. RBAC을 위해 정의된 주요 규칙은 다음과 같다.

- 역할 할당(Role Assignment)
- 역할 권한 부여(Role Autorization)
- 권한 부여(Permission Authorization)

4.2. 부인방지

부인방지란 통신 참여자 중 하나가 참여 사실을 부인하는 것에 대한 보안 서비스를 말한다. 부인방지의 목적은 사건이나 행위에 대한 증명을 제공하는 것이다. 증명이 제공되기 위해서는 통신 당사자의 식별과 데이터의 무결성이 확인되어야 한다. 부인방지는 다음과 같은 4단계로 구성된다.

1) 1단계: 증거생성
2) 2단계: 증거전송, 저장과 검색
3) 3단계: 증거확인
4) 4단계: 논쟁해결

증거는 분쟁을 해결하는 데 사용되는 정보로 부인할 가능성이 있는 통신 당사자가 생성한다. 증거는 증거의 사용자 또는 제3 신뢰 기관(Trusted Third Party; TTP)이 보관할 수 있다. 증거는 메시지 내용, 시간, 날짜, 부인할 가능성이 있는 통신 당사자의 식별 정보를 포함해야 한다.

발신자와 수신자가 직접 통신할 때 제공되는 부인방지로는 발신 부인방지와 수신 부인방지가 있다. 발신 부인방지는 메시지 발신자가 수신자에게 증거를 제공하는 것으로, 수신자는 발신자가 메시지 발신 사실을 부인할 때 증거를 이용해 발신자의 부인 사실을 증명할 수 있다. 수신 부인방지는 메시지 수신자가 발신자에게 증거를 제공하는 것이다. 발신자는 수신자가 메시지 수신 사실을 부인할 때 증거를 이용해 수신자의 부인 사실을 증명할 수 있다.

4.3. 일회용 암호

로그인 할 때마다 그 세션에서만 사용 가능한 일회성 패스워드를 생성하여 사용자에 대한 로그인 정보 유출을 최소화하기 위한 방식이다. 변형 패스워드 방식은 단방향 해시함수를 도입하여 위 패스워드 방식의 문제점을 해결하고 있다. 즉 사용자의 식별 정보 ID와 패스워드를 해시함수를 이용하여 해시 한 후 전송함으로서, 제 3자에 의한 도청(Eavesdropping)을 방지하고 동시에 전송 시 노출에 대한 예방을 하고 있다. 또한 패스워드 재전송(Replay)을 방지하기 위해 랜덤값 R을 사용하고, 서버 인증 정보 공격을 막기 위해 해시된 정 보를 그대로 저장함으로서 안전성을 획득하고 있다. 현재 변형된 패스워드를 제공하는 솔루션은 OTP(One Time Password)가 있다.

4.4. 안전한 부팅

SCADA 시스템의 운영자는 제어 장비가 잘 식별된(well-identified) 정품 소프트웨어 상에서 동작하는 것을 확인해야 한다. 이를 위해서는 장치에 멀웨어나 비정상적 소프트웨어의 주입을 방지하는 방법을 고려해야 한다. 이는 안전한 부팅(secure boot)를 통해 가능하다.

안전한 부팅을 지원하는 해결책으로 TPM, TrustZone, UEFI, Authentik 등이 있다. 신뢰 플랫폼 모듈(Trusted Platform Module)은 TCG Group에서 제안한 것으로 컴퓨팅 환경에서 암호화 키를 저장할 수 있는 보안 암호 처리자를 자세히 기록한 규격의 이름을 말한며, 최근에는 TPM 보안 장치 등을 통칭하여 TPM이라고 한다.

SCADA 시스템 보안을 위해서는 사용자 접근 제어를 위한 RBAC, 데이터 무결성 및 부인방지 알고리즘, 로그인 정보 유출 방지를 위한 일회용 암호, 안전한 시스템 환경 확보를 위한 Secure 부팅, 침입 방지 및 탐지 시스템, 소프트웨어 안전성 검사를 위한 화이트 박스 검사 등이 있다.

4.5. 침입 탐지

침입 탐지(Intrusion Detection)는 일반적으로 악의적인 해커의 공격을 통해 시스템에 대한 원치 않는 조작을 탐지하는 기법이다. 침입 탐지는 모든 종류의 악의적인 네트워크 트래픽 및 컴퓨터 사용을 탐지하기 위해 필요하다. 이것은 취약한 서비스에 대한 네트워크 공격과 애플리케이션에서의 데이터 처리 공격(data driven attack), 그리고 권한 상승(privilege escalation) 및 침입자 로그인 / 침입자에 의한 주요 파일 접근 / 악성 소프트웨어(컴퓨터 바이러스, 트로이 목마, 웜)와 같은 호스트 기반 공격을 포함한다. 다음은 다양한 침입 탐지 기법을 나열한 것이다.

– 네트워크 기반 침입 탐지
– 호스트 기반 침입 탐지

– 서명 기반 침입 탐지
– 변칙 기반 침입 탐지

4.6. 화이트박스 검사

화이트박스 검사(White-Box Test) 기법은 소프트웨어 내부 소스 코드를 테스트하는 기법이다. 화이트박스 테스트를 하면 내부 소스코드의 동작을 개발자가 추적 할 수 있기 때문에, 동작의 유효성 뿐 만 아니라 실행되는 과정을 분석하여 코드가 어떤 경로로 실행되며, 불필요한 코드 혹은 테스트 되지 못한 부분을 확인할 수 있다. 화이트박스 테스트를 하는 부분은 대개 코드의 실행 경로를 확인해야 하므로 커버리지 분석도구를 많이 활용하며, 타 검사 기법에 비해 많은 시간과 분석을 필요로 하지만 오류가 발생 되는 결함의 위치 등을 파악할 수 있다.

Ⅵ. 결 론

지금까지 SCADA 시스템에 대한 보안 위협과 이를 해결하기 위한 다양한 보안기술의 동향에 대해 살펴보았다. 클라우드 컴퓨팅, 양자컴퓨팅 등 정보통신의 발전으로 인해 제어시스템의 연결성은 더욱 확대될 것은 명확하며, 현존하는 제어시스템에 대한 보안기술 또한 지속적인 발전이 요구된다.

참 고 문 헌

[1] Robert Radvanovsky and Jacob Brodsky, “Handbook of SCADA/Control Systems Security”, CRC Press, 2013.
[2] David Bailey and Edwin Wright, “Practical SCADA for Industry,” Elsevier, 2003.
[3] IEC, IEC/TS 62351-1:2007(E), 2007.
[4] IEEE Power and Energy Society, IEEE Std. 1815:2012, 2012.
[5] ICS CERT. https://ics-cert.us-cert.gov/
[6] David Kushner, “The Real Story of Stuxnet,” 2013.02.26. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

송 경 영

• 2004년 2월 고려대학교 전기전자전파공학부 공학사/수학과 이학사
• 2010년 8월 서울대학교 전기컴퓨터공학부 공학박사
• 2005년 3월~2010년 8월 서울대학교 뉴미디어통신공동연구소 연구원
• 2010년 8월~2012년 2월 LG전자 차세대무선통신연구소 선임연구원
• 2012년 3월~현재 울산과학대학교 전기전자공학부 조교수

〈관심분야〉
스마트그리드, MIMO, 오류정정부호, 생체신호처리