https://doi.org/10.33778/kcsa.2019.19.5.055

블록체인 기반의 SCADA 시스템 보안★

지승원*, 이원기*, 고태광*, 박소희*, 오구연*, 김종민**, 김동민***

요 약

본 논문은 갈수록 치밀해지고 정교해지는 위협으로부터 SCADA 망을 지키기 위한 보안 방안에 대해 연구하였다. 현재 SCADA 시스템 보안은 일반 IT 보안 시스템과 거의 유사한 방법이 사용되고 있다. 공통적으로 필요한 보안 기법들도 있겠지만, 일반 IT 시스템과는 다른 SCADA 시스템만을 위한 보안 기법이 필요한 실정이다. 따라서 본 논문은 현재 SCADA 시스템에 사용되는 보안 기법에 대해 알아보고, 현재 보안 기법을 사용하였을 시 생기는 문제점을 SCADA 시스템의 공격에 따른 피해 사례들을 통해 알아볼 예정이다. 마지막으로 현재 SCADA 시스템에 필요한 가용성과 무결성을 보장하기 위한 새로운 대응 방안으로 Blockchain 과 SCADA 시스템의 연계를 제안하였다.

Blockchain-based SCADA system security

Seungwon Ji*, Wongi Lee*, TaeGwang Ko*, Sohee Park*,

Gooyeon Oh* Jongmin Kim**, DongMin Kim***

ABSTRACT

This paper studied security measures to protect the SCADA network from the increasingly sophisticated threats. Currently, SCADA system security uses methods that are almost like regular IT security systems. While there may be some common security techniques, security techniques are needed only for SCADA systems that are different fr om typical IT systems. Therefore, this paper will explore the security techniques currently used in SCADA system s, and the problems that arise when the current security techniques are used will be identified through the damage cases resulting from attacks in SCADA systems. Finally, as a new solution to ensure the availability and integrity r equired for current SCADA systems, we proposed linking Blockchain and SCADA systems.

Keywords : SCADA, Blockchain, System security

접수일(2019년 12월 9일), 게재확정일(2019년 12월 27일)

★ 본 연구는 한국전력공사의 2018년 선정 기초연구개발 과제 연구비에 의해 지원되었음 (과제번호: R18XA06-43)

* 경기대학교 융합보안학과 학사과정

** 경기대학교/융합보안학과 교수

*** 동신대학교 에너지융합대학 전기공학부(교신저자)

1. 서 론

현재 SCADA 시스템 보안대책은 일반 it 시스템 보안에도 사용되는 일반적인 보안 관리 프로세스를 보안대책으로 사용하고 있다. 데이터는 암호화가 이루어졌고, 보안정책에 따라 인가된 서비스에 대한 접근은 허용하고, 인가되지 않은 서비스에 따른 트래픽은 차단함으로써 내부의 중요한 데이터와 정보를 보호하였다. 방화벽을 사용하여 다른 네트워크와 분리하고, 일반 업무계열 네트워크에서 SCADA 네트워크로의 침입을 완전히 차단하기 위해서 물리적으로 한 방향으로만 통신을 허가하는 한 방향 게이트웨이를 사용한다. 또 소프트웨어의 취약성을 보완하기 위해 하드웨어 패치나 주기적인 업데이트를 통해 공격을 예방하고 있다. 이렇게 일반 IT 시스템의 보안대책 기술을 어느 정도 응용하여 사용하고 있지만 일반 IT 시스템과 SCADA 시스템은 엄연히 다른 시스템이다. 따라서 보안대책에 있어서는 두 시스템의 차이를 고려할 필요가 있다. 일반 IT 시스템 같은 경우 정보 기밀성이나 무결성이 중시되는 경우가 많지만 SCADA 시스템에서는 출력 품질이나 사람의 안전이 관련 있는 부분이 존재해 가용성과 무결성이 더 중시된다[1]. 보호하는 자산도 일반 IT 시스템은 정보가 집중되는 서버를 중시하지만 SCADA 시스템에서는 감시 제어의 중앙장치와 감시제어를 하는 단말장치를 더 중요시한다. 이러한 분명한 차이점이 있기 때문에 SCADA 시스템과 일반 IT 시스템에는 같은 보안대책을 적용할 수는 없다.

따라서 본 논문에서는 몇 가지 국내외 피해 사례들을 통해 현재 SCADA 시스템 보안의 문제점을 확인해보고, 무결성이 보장되는 블록체인과 SCADA 시스템을 연계하는 새로운 대응 방안을 제시할 예정이다.

2. 피해 사례

첫 번째 사례는 2010년 7월 이란에서 발생하였다. SCADA 시스템인 원자력발전소 발전시설 시스템이 마비되는 공격이 발생했다[2]. 이 공격은 웜 바이러스로 2010년 6월에는 Stuxnet 컴퓨터 웜이 벨라루스 보안 업체, VirusBlokAda에 의해 발견되었다. 그 웜을 분석한 후에 전문가들은 그것이 SCADA 시스템을 목표로 한 최초의 사이버 무기라고 주장하였다. 특히, 그 웜이 이란에 있는 특정한 컴퓨터 시스템을 타겟으로 하는데 의도적으로 핵 기술의 산출로 쓰이고 있고, 호환적으로 PLC를 비밀스럽게 재프로그래밍 할 수 있다. 침투경로는 USB 저장장치를 통해 외부 인터넷과 차단된 시설 내부망에 침투하여 감염되었고, 이로 인해 독일 지멘스의 산업 자동화 시스템인 SCADA 시스템을 임의로 제어할 수 있게 되어 가동 중인 우라늄 원심분리기 1,000대(전체의 약 10%)를 작동 불능상태로 만들었다.

두 번째 사례는 일본의 자동차업체인 혼다에서 발생한 사건이다[3]. 2017년 6월 일본 사야마 공장에서 약 48시간 동안 생산이 중단됨으로써 1,000여 대 차량에 영향을 받았다. 혼다 오딧세이 미니밴과 혼다 어코드를 포함한 생산라인에서 엔진 생산과 조립에 지장을 받았다. 문제의 원인은 사야마 자동차 공장의 오래된 생산 라인의 컴퓨터 여러 대가 워너크라이 바이러스로 인하여 정지가 되었기 때문이다. 아시아, 북미, 유럽, 중국 등지의 혼다 공장 시스템 역시 일본의 사야마 공장과 비슷하게 워너크라이에 감염된 것으로 확인되었다. 혼다는 워너크라이 감염 사태를 인지한 뒤 즉시 복구 절차에 들어갔지만 2일 뒤 오전이 돼서야 생산을 재가동할 수 있었다. 사야마 공장에 설치된 낡은 컴퓨터 여러 대에 대한 대응 조치가 부족하여 발생한 것으로 나타났다.

위 두 사건은 공장 시스템에 침투해 가용성을 침해한 사건이라고 볼 수 있다. 다음에 나오는 사례는 국내 사례로 무결성이 침해된 사건이다.

2016년 4월 24일 오후, 여수지역 내 한 버스정류장의 안내 시스템에서 약 40 분간 음란 동영상이 재생됐다[4]. 음란 동영상이 재생되는 사고가 발생한 버스정보시스템(BIS) 단말기모니터는 해킹이 쉬운 KT 임대망을 사용 중이었다. 자가망보다 설치비가 훨씬 저렴한 임대망은 TV나 인터넷 등을 공용하는 회선이라 해킹에 더 쉽게 노출된다. 해커는 외부망에 노출된 인터넷주소(IP)를 이용해 상황실의 원격제어 기능도 무력화한 것으로 전해졌다. 이 사건은 원래 나와야 하는 안내 화면이 아닌 음란 동영상이 나오며 데이터의 정확성과 일관성을 유지하지 못한 무결성이 침해된 사건이라고 볼 수 있다.

세 가지 국내외 사례를 통해 현재 SCADA 시스템은 가용성과 무결성 측면에서 매우 취약하다는 것을 확인할 수 있었다.

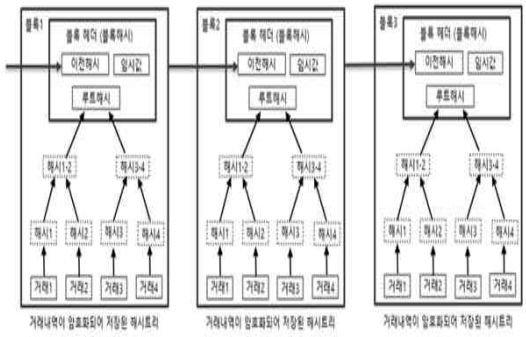
3. 새로운 대응 방안 제시

3.1 블록체인

흔히 블록체인기술은 모든 사용자가 블록체인 사본을 각자 가지고 있고, 블록체인 네트워크에 연결된 컴퓨터의 과반수가 넘는 사용자가 동의한 거래내역만 진짜로 인정하고 영구적으로 보관할 블록으로 묶는다. 서로 블록체인에 연결되어 모든 거래 내역이 중앙에 통제 받는 컴퓨터가 없이도 거짓이 발생되지 않는다[5]. 이와 같이 개인 간 공유 플랫폼을 형성해 민주적인 서비스를 제공하는 것으로, 지금의 SCADA 시스템과 같이 중앙 집중형에서 벗어날 수 있다.

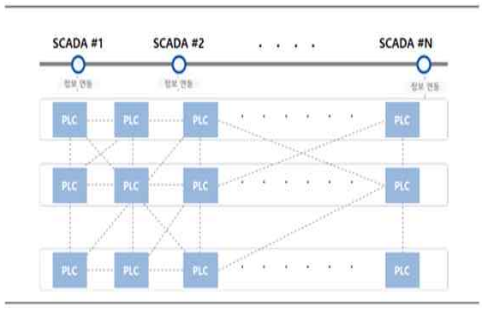
3.2 제공가치

블록체인의 제공가치로는 4가지를 들 수 있다[6]. 첫 번째, 공유성은 블록체인의 가장 근본적인 제공 가치로 모든 노드(블록체인 참여자) 사이에 공유함으로써 발생하는 가치이다. 두 번째, 투명성과 무결성은 노드 간에 정보 공유로 인해 참여자 간에 투명성의 가치가 생기고, 이러한 정보를 모든 참여자가 감시하기에 정보의 무결성 가치도 생겨난다. 세 번째, 정보의 투명성과 무결성은 정보에 신뢰성을 가지게 하고 마지막 효율성은 신뢰성을 보증할 제3자의 개입이 감소한다. 이는 탈 중앙화로 인한 복잡성 감소로 인해 효율성 향상이 생길 수 있음을 뜻하는데, 서비스 처리속도 향상 및 중개 수수료 감소를 예로 들 수 있다.



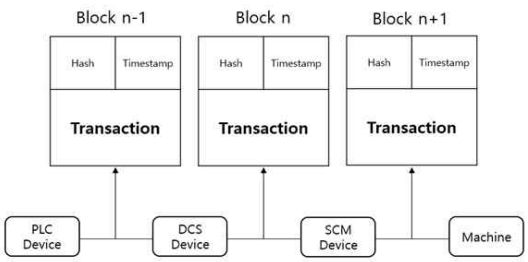
[그림 1] 블록체인의 진행과정 [7]

이러한 제공가치를 이용해 보안성을 활용한 SCADA 시스템의 적용방안을 제안하려고 한다. 발전소 자체는 폐쇄망을 사용하기 때문에 외부와 연동해 제공하는 '비 허가용 블록체인'(Permissionless Blockchain)보다는 '허가형 블록체인'(Permissioned Blockchain)이 더 적합하다. 각각의 사용 노드에만 권한을 부여해 내부 망으로 운영되게끔 할 수 있다. 또한 각각의 독립적인 SCADA를 다수의 SCADA로 나눠서 블록체인으로 엮고 PLC 또한 블록체인으로 서로 연동해 블록체인을 형성하여 SCADA와 PLC 간의 연결고리를 만들어 서로 정보를 교환할 수 있게 해야 한다. 아래 [그림 2]는 kisa에서 제안하는 블록체인을 활용한 SCADA 시스템의 보안 방법이다. kisa는 [그림 2]를 통해 SCACA 시스템과 블록체인의 연계 가능성을 제시하였지만, 이 제안은 무결성에 대한 보증이 구체적이지 못하고, 가용성의 침해가 우려된다.



[그림 2] kisa의 SCADA 보안 방법[6]

따라서 [그림 3]은 kisa가 제안한 SCADA 시스템과 블록체인의 연계를 구체화 하기 위해서 노드 간의 블록체인 연결을 그림으로 표현한 것이다. 각각 블록은 각 장치 노드에 의해 전송되는 데이터의 집합이며, 관련 정보와 기록은 블록체인

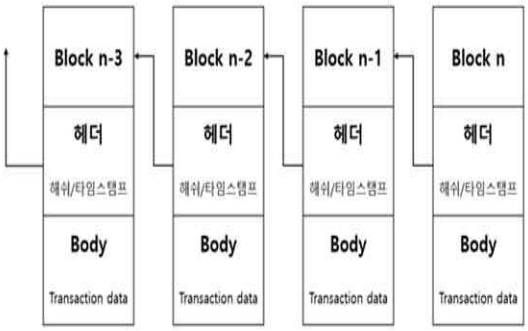


[그림 3] 노드 간 블록체인의 연결 [8]

을 형성하기 위한 기본 단위를 포함하고 있다. 블록체인의 추적성을 확보하기 위해, 각 블록은 고유한 태그로 타임 스탬프를 가진다. 블록의 두 가지 구성으로 Front block으로 연결된 블록 헤더와 무결성을 제공하는 블록체인이 있다. 각 블록에는 각 단 노드에 업데이트 된 데이터 정보를 기록한다.

또한 아래 [그림 4]를 보면 알 수 있듯이, 각각의 노드와 연결된 블록체인은 전 블록체인의 블록 값을 해시화하여 만들기 때문에 언제든지 해시함수만 알고 있으면 위▪변조 여부를 확인할 수 있다. 또한 헤더와 바디에 포함되어 있는 정보가 모두 유기적으로 연결되어 있어서 무결성을 얻는다

.



[그림 4] 블록체인과 헤더의 연결 [8]

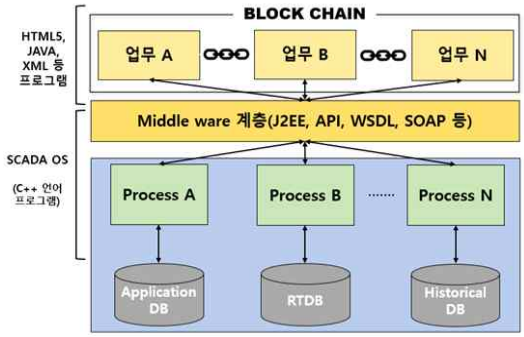
3.3 보안효과

블록체인 적용으로 향상되는 보안 효과는 아래와 같다[6].

- 정보무결성 : SCADA 와 PLC 의 정보를 블록체인 방식으로 기록하기 때문에 발전소에서 기록한 정보의 무결성을 강화할 수 있다.
- 프로세스 무결성 : 작업 프로세스의 메모리 값을 파일로 만들어 해당 해시 값을 블록체인으로 공유하면 작업 프로세스 메모리 변조를 막을 수 있는데, 이는 스턱스넷과 같은 프로세스 변조 공격에 대응할 수 있게 한다.
- SCADA 가용성 : 특정 SCADA 가 Dos 공격을 당해도 다른 SCADA 가 피해를 본 SCADA 를 대신할 수 있다.
- 인증 : 블록체인 연계 방식은 인증 정보의 무결성을 강화할 수 있기 때문에 비 인가된 사용자를 인가된 사용자로 위조, 변조하는 것을 막을 수 있다.
- 부인방지 : SCADA 와 PLC 에서 동작하는 활동은 블록체인으로 기록되기 때문에 SCADA 의 제어 명령 PLC 가 제대로 동작하는지 확인할 수 있다.
- 접근제어 : 접근제어 관련 정보 무결성을 블록체인으로 보증하기 때문에 정보 훼손으로 인한 접근제어 악용 공격을 막을 수 있다.

3.4 적용방안

과거에는 공장에서의 장치 조작과 공공망에서의 변화를 위해 물리적 접근이 요구되었으나 지금은 장치들이 인터넷에 연결되고 IoT 가 활용되면서 새로운 위험에 노출되어 있다. IT 와 운영기술, 보안기술이 융합됨에 따라 'security by design'이 기술 선택의 중요한 결정요인이 되고 있다. SCADA 로의 공격은 블록체인의 무결성 방지를 통해서 정보 변조 및 공격에 예방할 수 있지만 지금 실질적으로 가동 중인 SCADA 망에 적용을 했을 때 가용성에 대한 문제가 있다. 발전소 및 여러 SCADA 망이 일시적으로 정지가 될 경우에 입는 피해가 많기 때문에 가용성을 침해하지 않고 적용시키는 방법이 필요하다.



[그림 5] 블록체인을 활용한 SCADA 보안 방안

위의 [그림 5]는 블록체인을 활용한 SCADA 시스템의 보안 방안을 그림으로 나타낸 것이다. 기존의 SCADA 망 같은 경우는 별도의 Middleware 없이 Application(업무)자체가 직접 DB를 접근하며 유지보수가 어려우며, 장애 발생 시에는 중단되어 가용성 침해가 발생한다. 가용성 침해를 막기 위해서 지능형 SCADA 구조 도입을 생각해 보았다. 지능형 SCADA 시스템 구조는 Application와 Process를 엄격히 구분하고 중간에 이를 연결하는 Middleware 계층을 두어서 Application과 process를 따로 운영할 수 있다. Application에 서로 연결된 블록체인의 경우 산업망의 쓰임새에 따라서 알고리즘 자체는 다르게 구성될 것이다. 업무의 변화에 따라서 각각의 블록체인에서는 스마트계약(Smart Contracts)으로 이행 및 검증의 과정이 진행되며, 네트워크 상에서 자동화 되고, 외부의 Dos 공격에 대비하기 위해 최소한의 처리과정만 거치며 진행되게 설계된 스택 기반의 실행언어로 개발이 될 것이다. 반복되는 작업 속에 WorkingCycle은 블록체인의 스마트 계약 시스템으로 연결되어 서비스와 아래 middleware 플랫폼을 연결하는 IoS(Internet of Services) 단계에서 사용될 것이다. Middleware 계층은 사이버물리공간(CPS, Cyber Physical Spaces)으로 사이버 상에서 공장을 가상으로 가동하여 가동률 등을 확인하고 문제점이 발생하면 보완할 수 있다. 기존 공장이 생산방식을 변경하려면 기존에 있던 라인을 새롭게 깔아야 하며, 많은 돈과 시간이 투입된다. 하지만 CPS를 통해 몇 개의 머신, 라인 등만 교체해준다면 제품 생산이나, AI를 통해 신속하고 완벽한 의사결정에서도 도움을 받을 수 있다. 다르게 생각한다면 문제점이 발견되어 시스템적으로 수정할 방법이 필요하다면 미리 CPS상에서 수정하면 IoS에 반영이 되고 이에 문제없이 진행될 것이다.

4. 결론

SCADA 시스템은 전력, 가스, 석유, 상·하수도, 철도와 같은 국가의 주요 기반시설을 관리 및 제어 하거나 기업의 산업망을 위해 사용하고 있다. 이전의 SCADA 시스템은 폐쇄망으로 운영되었지만, 개방형 시스템으로 전환되어가며 보안상 취약점들은 계속 생겨나고 있다. 만약 SCADA 시스템에 공격이 들어오거나 침해를 받는 경우 국가 안보, 경제 및 국민 생활 안정에 엄청난 피해를 줄 것이다. 이에 따른 국가 주요 기반 시설의 핵심이자 이윤 추구를 위한 산업망의 핵심인 SCADA 시스템의 보안이 강화가 필요하다.

본 논문에서는 기존의 대응방안과 국내외 피해사례들을 통해 현재 SCADA 시스템의 보안상 문제점에 대해 알아보았다. 또 새로운 대응 방안으로 블록체인과 SCADA 시스템을 연계한 방안을

제시하였다. 블록체인은 세대를 거듭하며 발전하고 있으며 쓰임새 또한 전자화폐 뿐만 아니라 다양한 활용분야들이 생겨나고 있다. SCADA 시스템 보안을 위해 블록체인을 활용한 무결성 유지효과와 지능형 SCADA 시스템을 활용한 가용성의 침해 방지, 이 두 가지를 연계한다면 보다 안전하고 신뢰성 있는 SCADA 시스템의 서비스를 제공할 수 있을 것으로 예상된다.

참고문헌

[1] 김영진, 이정현, 임종인, 「SCADA 시스템의 안전성 확보방안에 관한 연구」, 「정보보호학회논문지」 19(6), 한국정보보호학회, 2009.12, 145-152(8 pages)

[2] 김지훈, 이성원, 윤종희 「무선통신기반 SCADA 시스템 공격기법과 위협사례 및 연구 동향분석」. 한국통신학회지, 2017.04

[3]https://www.boannews.com/media/view.asp?idx=55408&page=5&kind=1

[4]https://www.huffingtonpost.kr/entry/story_kr_9775226

[5] 문승혁, 「4차 산업혁명에서의 블록체인의 역할과 기회」, 국제문화기술진흥원, 2019.8

[6] 유성민, 「발전소 위협 현황과 블록체인 연계 모델 가능성」, KISA Report vol.11, 2018

[7]http://wiki.hash.kr/index.php/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8

[8]Mingyang Mao and Hong Xiao(2018). Blockchain-based Technology for Industrial Control System CyperSecurity. Advances in Intelligent Systems Research, volume 147, 903-907.

〔저자소개〕

지 승 원 (Seung-Won Ji)

경기대학교 융합보안학과 학부생

email : bigsan224@gmail.com

고 태 광 (Tae-Gwang Ko)

경기대학교 융합보안학과 학부생

email : ktk9058@naver.com

이 원 기 (Won-Gi Lee)

경기대학교 융합보안학과 학부생

email : lwg0907@naver.com

박 소 희 (So-Hee Park)

경기대학교 융합보안학과 학부생

email : wowoml@naver.com

오 구 연 (Goo-Yeon Oh)

경기대학교 융합보안학과 학부생

email : rntmf419@gmail.com

김 동 민 (DongMin Kim)
2011년 한양대학교 대학원 전기공학과 졸업(공박)
2011년~2012년 한양대학교 BK21 사업단 박사 후 연구원
2012년~현재 동신대학교 에너지융합대학 전기공학전공 부교수.

email : dmkim@dsu.ac.kr

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : dyuo1004@gmail.com