정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

풍력발전단지 보안수준 강화를 위한 제언: CSRF 공격 예방을 중심으로

김 정 완*, 김 휘 강**

요 약

본 연구에서는 신재생에너지의 큰 비중을 차지하고 있는 풍력발전의 ICT 환경을 조사하고 최신해킹사례를 분석하여, 예상되는 보안위협을 도출하였다. 이 중 가장 영향도가 높은 보안위협요소로 CSRF(Cross-Site Request Forgery) 공격을 선정하고 공격을 방어할 수 있는 인증강화모델을 제안하였다. 우선, 풍력발전 관련한 국제표준화 동향 및 대형제작사 구현 실태를 살펴보고 CSRF 공격 예방을 위한 선행연구를 조사하였다. 선행연구의 이점을 접목하고 약점을 강화하여 재인증, CAPTCHA, OTP(One Time Password)와 같은 인증방식을 주요명령수행 구간에 임의로 표출시켜 인증시점의 불확실성(Entropy)을 높여 공격자가 쉽게 예측하지 못하도록 하였다. 명령수행과정의 일관성(고정성)이 매회 변화되므로 고정화된 형태의 CSRF 공격을 예방할 수 있다.

Ⅰ. 서 론

최근 기후환경 변화에 따라 세계적으로 신재생에너지 발전 수요가 급증하고 있다. 우리나라는 「재생에너지 3020 계획[1]」에 맞물려 신재생에너지 분야의 수요를 미리 예측, 전문 ICT솔루션을 개발하는 등 제어시스템 운용SW의 개발 및 활용이 늘어나고 있는 추세이다.

한수원 등 발전 6사는 정부정책에 발맞추어 신재생에너지 개발로의 전환으로 이동을 신속히 추진 중에 있다. 이에 필요한 ICT 플랫폼과 관련 솔루션의 수요를 분석·대응하여 MG-EMS(Micro-Grid Energy Management System) 등 관련솔루션 10여종이 개발되어 서남해 해상풍력사업 개발주체인 한국해상풍력(주)에서 사용되고 있다.

이에 본 연구에서는 대규모 경제발전이 가능한 신재생에너지 부문의 풍력발전·태양광의 ICT 환경을 조사하고 최신해킹사례를 분석하여, 예상되는 핵심 보안취약점을 도출하고 이에 대한 예방책을 제시하였다.

Ⅱ. 산업 환경 분석

2.1. 풍력관련 국제보안 표준화 동향

풍력발전을 포함한 Renewable Energy 관련 국제보안표준화 동향으로는 IEC-62433(공통, Oil and Gas 중심) 중 IEC 62443-3-3(Industrial communication networks), IEC 61850[2], NISTIR 7628(Guideline for Smart Grid Cyber Security) 등이 있다. IEC 61850에서 스마트그리드상의 통신규격에 대해 상세하게 기술된 것처럼 보안을 고려한 구현표준에 대해서도 제정이 필요하다. 유럽은 전통적인 표준기구로 DNV-GL 이 있다. 선박, 풍력발전 등 다양한 부문의 안전, 품질보증 및 위험관리 관련한 표준을 제정하고 있으나 보안관련해서는 깊이있게 다루고 있지 않다.

이 외 EU의 지원을 받아 진행된 대표적인 표준 프로젝트로 SEGRID(Security for smart Electricity GRIDs)가 있다[9]. SEGRID는 EU 전력계통(Grid) 보안을 위한 Project로 10개 기업 및 연구기관이 협업하여 1차 연구를 마치고 현재 2차 과제(2018~2025년)로 영역별 세부과제를 진행하고 있다. 제작사로는

* 고려대학교 정보보호대학원 (대학원생, ww0jeff@korea.ac.kr)
** 고려대학교 정보보호대학원 (교수, cenda@korea.ac.kr)

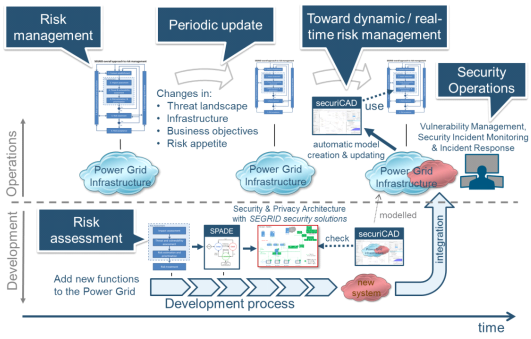
〔표 1〕 Cyber security 관련 가이드(DNV-GL)

가이드	최신 개정
Cyber security in the oil and gas industry based on IEC 62443	2017-09
Cyber security capabilities of control system components	2018-01
Cyber security resilience management for ships and mobile offshore units in opration	2016-09

ABB와 ZIV가 참여하고 있고. 연구 범위는 [그림 1]과 같다[10].

연구 로드맵 중 WP(Work Package)3은 현재 추진 중으로 Web Application Protection에 대한 탐지 및 교정 방법이 구체화될 전망이다. 이중 1차 결과물로 스마트그리드를 대상으로 한 Use cases 시나리오가 개발되었다[11]. 우리회사와 연구, 사업 범위가 상당부분 중첩되어 향후 연구결과를 참조할 필요가 있다.

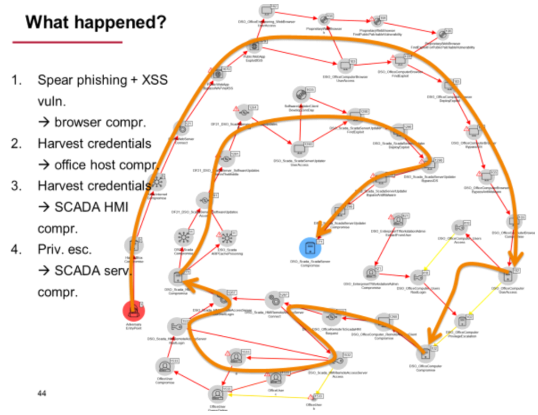
또한, 스마트그리드를 대상으로 한 다양한 공격, 정보유출 시나리오가 개발되어 있다. 아래 [그림 2]는 스피어피싱 메일로 XSS 취약점이 있는 웹기반시스템을 공격하여 브라우저를 점령하고, 브라우저에 저장된 주변 로그인 정보(Credentials)를 탈취, 이후 주변 Office



〔그림 1〕 EU SEGRID 연구 범위

〔표 2〕 보안가이드 연구 분과 및 관련 활동(EU SEGRID)

WP1	WP2	WP3	WP4
• Cost Assessment • Operational Security Capability Model	• SEGRID Risk Management Methodology (SRMM)	• SecuriCAD & UC2.2 model • Automated model generation • Vulnerability Detection and Correction with Web Application Protection (WAP) • Prevention of Injection Attacks in DBMS	• Security and Privacy Architecture DEsign (SPADE) • Trusted Platform • Resilient SCADA systems • IDS and authentication in mesh networks • Robustness and scalable (D)TLS • Resilient communication infrastructure • Key management for group software distribution • Privacy by design



〔그림 2〕 스피어피싱 메일+XSS 취약점을 통한 침투시나리오(EU SEGRID)

단말로 로그인 성공, 추가적으로 HMI 로그인 정보를 획득하고, 권한 상승(Privilege Escalation)하여 계속 주변 단말로 측면이동(Latteral Movement)하며 내부로 진입해 들어가는 시나리오를 담고 있다.

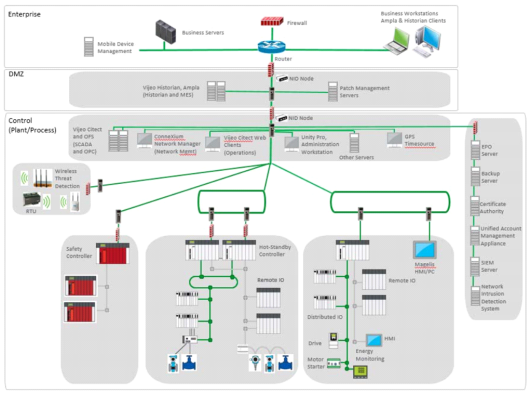
그러나 보안 아키텍처, 위험관리, 소프트웨어 부문에서의 세부적인 가이드는 2025년까지 개발 예정이다. 이 외에도 전세계 해상풍력 점유율 1위인 영국에서는 자체적으로 CPNI[1], CESG[2], EECSP 등을 통한 가이드를 제시하고 있다. 비영리 단체로는 ENCS(European Network for Cyber Security)등이 있다. CPNI 에서는 Cyber Assessment Framework 3.0(2019. 9.30) 등 실용적인 부분 가이드를 제공하고 있다[3].

2.2. 제작사 보안 구현

대부분의 표준기구에서는 네트워크 보안에 대해서는 기본 Architecture 를 제시하고 있다. 그러나 응용계층의 최신 공격기법에 대해서는 구체적인 대안을 제시하고 있지 않다. DNV-GL에서는 네트워크 구성 컨셉만을 제시하고 있다. [그림 3]은 Schneider-Electric에서 제시하는 네트워크 분리 개념도이다.

Schneider-Electric은 기업망(IT)과 제어망(OT

1) CPNI(Center for the Protection of National Infrastructure)는 기반시설 보호를 위한 영국의 중앙기관이다.
2) CESG(Communications Electronics Security Group)는 영국 GCHQ(Government Communications Headquarters) 산하의 조직이다.



〔그림 3〕 Network Segmentation and segregation

Operation Technology) 사이의 완충구간(DMZ)의 방화벽 정책관리 미흡, 장애등을 고려하여 방화벽을 물리적으로 분리하여 2개를 안정적으로 운영하고 있다. 실무에서 보안수준을 한 단계 높인 경우이다.

Ⅲ. 풍력발전단지를 대상으로 한 공격사례

본 절에서는 신재생에너지 부문 중 풍력발전단지를 대상으로 한 공격에 대해 조사하였다. 대표적으로 세 가지 사건으로 정리할 수 있다.

〔표 3〕 풍력발전을 대상으로 한 최신 취약점 발견 사례

발생 일시	사고 내용	원인 및 대책
2015년 3월	XZERES 풍력터빈 관리프로그램 통해 통제 - CSRF 취약점, 관리자 웹페이지를 통해 임의명령 수행 - 제품: XZERES 442SR Wind Turbine 용량: 10.4kw (지름 7.2M) - 취약점: CVE-2015-0985(CSRF), CVE-2015-3950(CSRF) - 영향: 비밀번호 변경, 터빈 Shutdown Credit: Maxim Rupp(Independent Researcher)	CSRF 취약점 존재 제작사 SW 패치로 해결
2017년 7월	BlackHat 2017에서 풍력발전 산업계에 존재하는 전반적인 취약점 공개 - 취약한 Legacy OS 사용 - 모든 프로세스가 root 계정으로 운영 - 원격관리 접근통제 미흡 - 제작사 Default Password Weakness - 인증, 암호화, 전자서명 미사용 - 풍력터빈 간 네트워크 구간 미분리 - 취약한 물리보안 Credit: Jason Staggs(University of Tulsa)	과도한 root 권한 제거 원격관리 접근통제 강화 Default Password 강화 터빈간 네트워크 분리 Security by Design 프로토콜 강화 - 인증, 암호화, 전자서명 물리보안 강화
2019년 3월 (공개 2019.10)	미국 sPower 서부 관제센터 Cyber Attack 에 의한 운영지장(미국 첫사례) - 미국 서부의 태양광, 풍력 단지 12곳을 관리하는 서부관제센터에 DoS 공격이 지속되어 5분간 통신두절 몇차례 발생. - 발전이나 송전이 중단되지는 않았으나 운영 상태를 Power Grid Operator인 sPower 사가 알지 못하게 되어 미 법령 기준에 의거 미에너지부(DOE)에 사이버사고 피해를 보고한 첫 사례	Cisco Firewall 보안패치를 적용하지 않은 채 1년 넘게 운영 Firmware Patch

3.1. 풍력터빈 관리프로그램 최초 취약점 발견

먼저, 2015년 3월, XZERES 442 SR 풍력터빈의 취약점 사례이다. XSS 취약점을 이용하여 웹인터페이스상에서 관리자 권한으로 터빈의 설정값을 변경하거나 중단시킬 수 있었으며, 관리자 비밀번호를 변경하는 등의 작업이 가능함이 밝혀졌다.

CSRF[4] 취약점은 XSS가 존재하는 웹사이트를 대상으로 공격자가 원하는 명령문을 스크립트로 작성해서(위조해서) 관리자에게 전송후, 관리자가 열람시 자동 실행되게끔 하는 공격방식이다. 홈페이지상의 모든 GET, POST 요청은 재연이 가능하기 때문에 관리자

〔그림 4〕 XZERES 442SR Wind Turbine 으로 구성된 단지, XZERES 모델

권한으로 임의명령 수행이 가능하여 웹기반의 취약점 중 SQL Injection 과 함께 가장 높은 위험도가 배정되어 있다. SEGRID에서 분석한 스마트그리드 공격 시나리오 중에도 XSS 취약점을 악용한 사례가 포함되어 있다.

제작사에서 수동 패치파일을 제공(2015년 6월)하였으나 2016년에도 여전히 또다른 XSS 취약점이 발견되었다(CVE-2016-2287).

3.2. 풍력터빈 PLC, PAC 취약점 발견

BlackHat 2017에서는 풍력터빈에 사용되는 다양한 PAC(Programmable Automation Controllers) 들에서 공통적으로 발견되는 취약점이 발표되었다[7].

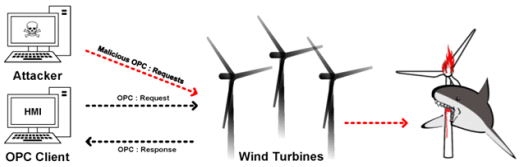
위 PAC의 취약점을 이용해서 풍력터빈에 서비스거부공격 뿐 아니라, 임의 OPC 요청을 보내 응답을 받을 수 있고, 명령을 수행할 수 있는 취약점이 밝혀졌다.

아래는 취약한 기능을 통해 읽을 수 있는 값들이다.

Turbine Speed, Blade 상태, Rotor 피치 각도, Rotor RPM, 나셀 방향, 온도측정, 컨트롤러 운영 상태 등.

특히 심각한 것은 풍력터빈의 상태를 On, Off, Idle, Emergency shutdown(강제 중단으로 터빈에 무리를 준다. Hard Stop이라고도 한다)

〔그림 5〕 풍력터빈에 사용된 취약한 PAC들



〔그림 6〕 악의적인 명령어를 전송하여 터빈 조작

3.3. 미국 전력망 사이버공격 피해(최초사례)

세 번째 사례는 보안패치가 미흡하여 발생된 사고로, 사이버공격에 의한 전력망 운영회사(Power Grid Operator)의 통신두절 첫 사례로 등재되었다[8]. 2018년 3월 5일 미국 서부지역의 12개 풍력 및 태양광 발전단지를 연계해 운영하는 sPower 의 서부관제센터가 출처미상의 공격자로부터 서비스거부(DoS, Denial of Service) 공격을 받아 11시간동안 간헐적으로 통신두절 피해를 본 사건이다. 사고 원인은 관제센터 경계방화벽으로 운영중인 Cisco사 방화벽 제품의 Firmware 패치를 1년이 넘도록 설치하지 않고 운영하다가 발생되었다. 미국의 연방에너지관리법(Public Law 93-275)에 보면 전력계통이나 통신계통에 Cyber Attack 이 감지되고 운영에 잠재적인 영향을 미칠 것으로 추정될 때는 6시간 이내 미에너지부(DOE)로 신고하도록 되어 있다[5].

이 외에도 인터넷에 공개된 ICS Device 들이 많다. 대부분 웹 관리자용 접속포트(HTTP)이거나 FTP, SSH인 경우가 많다. 이 들 중 CSRF 취약점이 존재하는 관리 프로그램이 있다면 원격에서 점령될 가능성이 있어 보안책이 필요하다.

Ⅳ. 연구과제 도출

4.1. 요구 조건

지금까지 풍력발전단지를 대상으로 한 공격과 취약점, 파급효과에 대해 살펴보았다. 앞서 살펴보았듯이 웹 기반의 관리S/W를 운영하는 관리자가 CSRF 공격에 노출 될 경우, 동 SW에서 설정할 수 있는 다양한 기능을 공격자가 임의로 조정할 수 있다. 이러한 공격을 예방하기 위해서는 어떻게 해야 할까? 웹기반으로 이루어지는 모든 통신내용은 공격자가 모든 기능을 수행해봄으로써 어떤 순서와 호출이 되는지 분석할 수 있기 때문에 이러한 CSRF와 같은 공격을 저지할 방법이 필요하게 된다. [표 4]는 OWASP에서 강력히 권고하는 CSRF 방어대책[6]으로 본 논문의 보안모델에 적용 가능한 요소기술이라 할 수 있다.3)

3) OWASP에서는 위 기능 외에도 여러 가지 기능을 제시하고 있으나 실용적이고 강력한 예방책은 위 3가지로 함축된다.

4.2. 추가 인증요소

[표 4]의 추가인증 요소 중 재인증과 OTP(One Time Token)는 최근 널리 적용되고 있는 인증 방식으로 주로 금융기관 인터넷 뱅킹, 개인정보의 비밀번호 변경 등 중요 행위를 수행하기 전 사용자에게 인증을 요구하는 방식으로 활용되고 있다. CAPTCHA는 HIP(Human Interaction Proof) 기술의 일종으로, 정당한 사용자가 실제 액션을 수행하고 있는지 확인하기 위해 개발된 인증방식이다. 전자상거래 결제, 중요시스템 로그인 시 추가 인증 용도로 사용되고 있다.

〔표 4〕 CSRF 예방대책(OWASP)

구분	설명	영향
Re-Authentication (재인증)	웹 응용프로그램의 중요한 기능 사용 전에 재인증을 요구한다. (쉽게 유추할 수 없는 Password 사용)	중간
CAPTCHA	웹 응용프로그램의 중요한 기능 사용 전에 CAPTCHA 인증을 수행하도록 한다. 사람만이 이 인증 테스트를 통과할 수 있다.	높음
Onetime Token	웹 응용프로그램의 중요한 기능 사용 전에 One-Time Token 의 값을 입력하도록 유도한다. 인가된 사용자만이 이 인증 과정을 통과할 수 있다.	매우 높음

4.3. 연구 방향(CSRF 분석 및 해결방안 모색)

신재생에너지를 포함한 스마트그리드 환경에서의 기반시설 제어프로그램의 보안을 강화하는 기술이므로 오퍼레이터의 상호작용에 다소 불편함을 야기하더라도 숙련된 해커의 공격을 저지하기 위해 추가인증 요소기술을 반영할 것을 고려하였다.

4.4. 선행 연구

대표적인 방법으로 웹서버 내 존재하는 모든 웹페이지의 정상적인 순서에 따른 호출패턴에서 벗어날 경우 탐지하는 기술이 있다[12]. 다음으로 클라이언트와 웹서버 양단에서만 알수 있는 비밀정보를 공유하며 시도-응답방식으로 확인하는 방법이 있다[13]. 세션ID, 페이지 식별번호(웹서버에서 랜덤생성), 사용자 비밀번호 해시값을 연접하여 SHA1 함수로 다이제스트값을 취한 후 서버에 전송하여 인가된 사용자 인증임을 증명한다. 이 작동방식은 가능성은 적지만, 공격자가 사용자의 비밀번호를 알고, 클라이언트측의 소스코드를 분석하여 작동메커니즘을 알게 될 경우 CSRF 공격에 취약해지게 된다. 보다 강화된 대책이 필요하다.

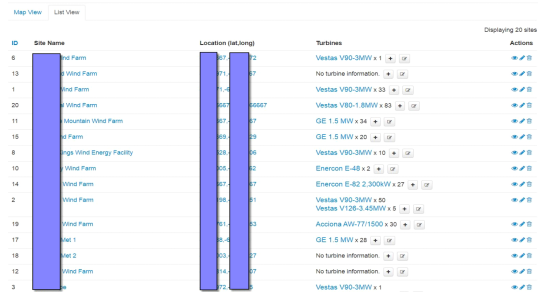
Ⅴ. CSRF 방어모델 설계

본 연구의 주목적은 무작위 추가인증적용을 통해 공격자의 자동화된 CSRF 공격을 방어하는 것이다. 여기에 더해 고도로 은닉된 해커가 내부에 침입해있다는 가정 하에, 별도의 보안에이전트 설치 없이 효과적으로 내부위협을 탐지하는 방안을 제안하고자 한다.

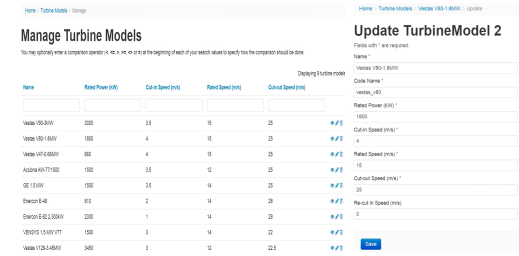
5.1. CSRF 공격 예방 및 탐지

실제 다수의 풍력발전단지를 운영하는 통합 웹관리 프로그램이 Shodan 서비스에 노출된 곳을 예시로 CSRF 방어대책을 설계해보고자 한다. 실제 예시로 발전단지를 선택하고, 특정 터빈을 골라 운영 환경값을 변경하는 과정을 살펴볼 수 있다[그림-7,8,9].

이때 관리자가 마우스를 클릭하는 절차가 다음과 같



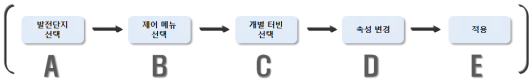
〔그림 7〕 풍력발전단지 선택(예시)



〔그림 8〕 풍력발전단지 내 터빈 List(예시)

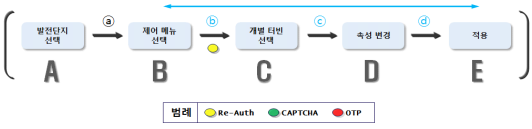
〔그림 9〕 터빈 설정 변경(예시)

이 A→B→C→D→E 일때, 공격자가 해당 웹기반의 클릭행위시 전송되는 메소드와 파라미터값들을 분석하여, 재연공격(Replay Attack)을 수행할 수 있다. 공격자가 A→B→C→D→E 순서대로 웹서버에 전송되는 데이터를 순서대로 재생하면 결국, 관리자가 한 행위를 그대로 실행하게 되는 것이다.



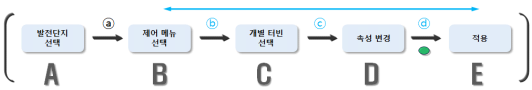
〔그림 10〕 풍력발전단지 일반 제어활동(예시)

이렇게 공격자가 임의로 구성하여 전송되는 일련의 웹명령어가 순서대로 실행되지 않도록 방어대책을 강구하여야 한다. 관리자가 마우스를 클릭하는 절차가 다음과 같이 A→B→C→D→E 일때, B 와 E 구간의 3 지점(ⓑ, ⓒ, ⓓ)에서 무작위로 재인증이나 CAPTCHA 인증을 표출시키는 것이다. [그림 11]은 예시로 ⓑ구간에서 재인증을 표출시킨 예이다. 공격자가 관리자 비밀번호를 알지 못할 경우 B 까지만 명령어가 전송되어 실행되고 그 이후의 C, D, E 과정은 실행되지 않는다.



〔그림 11〕 풍력발전단지 일반 제어활동, 무작위 추가인증 반영(위치:ⓑ, 방식:재인증)

이번엔 다른 예시로, 다른 위치(d)에 CAPTCHA 인증을 추가한 예이다. 마찬가지로, 공격자가 B, C, D, E 명령을 순차적으로 구성하여 전송할 경우, 관리자가 이 스크립트를 실행시키더라도, D까지만 정상적으로 실행되고, E 바로 직전에 CAPTCHA인증, 즉 일그러진 문자를 맞추거나, 사물의 종류를 마우스를 클릭하여 선택해야 하는 CAPTCHA 인증을 통과할 수 없기 때문에, 일련의 공격은 이 지점에서 중단되게 된다.



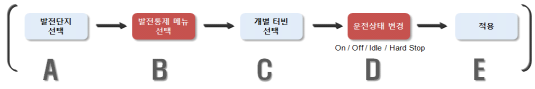
〔그림 12〕 풍력발전단지 일반 제어활동, 무작위 추가인증 반영(위치:ⓓ, 방식:CAPTCHA)

〔표 5〕 운영자 행위에 따른 추가인증 적용방법

No	행위구분	표출위치선정	표출되는 추가인증 방식	인증횟수	비고
❶	일반제어	무작위	Re-authentication or CAPTCHA	1~2	
❷	특별제어	무작위	Re-authentication and CAPTCHA	2	
			(Re-authentication or CAPTCHA) and OTP	2	비상정지 등

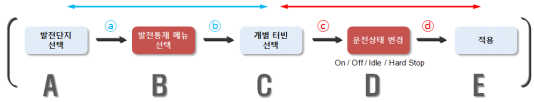
본 모델에서의 주안점은 첫째, 일반 제어명령을 실행할 때(❶)는 중간 구간에서 재인증이나 CAPTCHA 인증 둘 중에 1개 또는 2개를 무작위로 표출시키는 것이고, Mission Critical 한 특별제어 명령을 수행할 때(❷)는 재인증이나 CAPTCHA를 무작위로 1개 표출하고, 나머지 잔여 장소에서 무작위로 OTP를 표출시키는 것이다.

다음은 특별제어 명령을 수행하는 예시로 개별 터빈을 Off(Smooth shutdown)시키거나 비상 중단(Hard stop)하는 등의 절차이다.



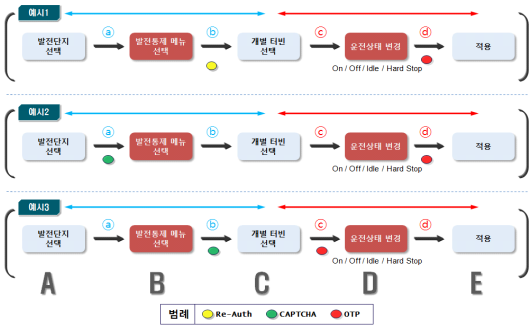
〔그림 13〕 풍력발전단지 특별제어명령 실행(예시)

이때는 중요한 명령을 선택하는 구간(A~C), 선택한 명령의 속성을 지정하고 적용하는 구간(C~E)에서 추가인증 방식을 표출시키면 적정하다. 또한, 보안 강도는 높지만 사용자의 불편지수가 높은 OTP를 뒤쪽 구간에 배치하는 것이 효과적이다.



〔그림 14〕 특별제어명령 실행시 추가인증 적용구간

OTP 적용이 어려울 경우는 SMS 인증방식으로 대체하여도 무방하다. 다만 OTP, SMS가 운영자의 행위에 효율성을 감소시킬 수 있으므로, 첫 번째 방식(❶)



〔그림 15〕 특별제어명령 실행시 추가인증 적용 예시

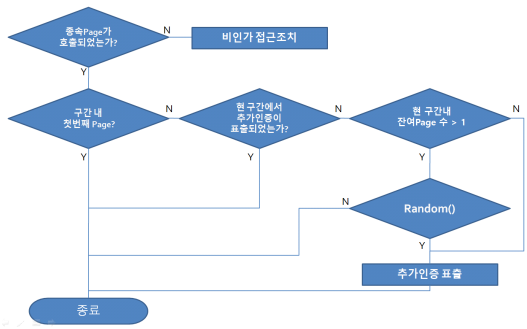
만을 사용하는 것도 유의미하다.

5.2. 추가인증 표출 방식(알고리즘)

지금까지 설명한 추가인증 방식 표출 알고리즘은 [그림 16]과 같다. 웹서버 내 특정 페이지가 호출되었을 경우, 정상적인 종속페이지를 거쳐 호출 된 것이라면, 첫 번째 페이지가 아니고, 잔여 페이지가 존재할 경우 임의 인증방식을 선택하여 표출시키는 방법이다. 이 알고리즘을 구현하기 위해서는 웹서버에 별도의 테이블을 만들어, 일반/제어명령 구간에 대한 정의, 모든 페이지의 종속관계 저장, 현 구간에서의 인증방식 표출이력을 저장하여 운영에 참고할 수 있도록 하여야 한다. 본 연구에서는 개념설계를 목표로 하였다.

5.3. 설계 모델의 강도

공격자가 무작위 추가인증방식 ❶의 방법을 깨기 위해서는 [그림 11]의 경우 재인증이 위치하는 ⓑ, ⓒ, ⓓ를 공격 시도하면서 동시에 운영자 비밀번호를 알고



〔그림 16〕 추가인증방식 표출 알고리즘

있어야 한다. 초기 XSS 취약점에 기반하여 공격할 때는 운영자 비밀번호를 알지 못하므로 간단한 스크립트로 수십 개의 비밀번호만 대입하는 수준에서 그치게 된다. 통상 비밀번호가 5회 이상 틀릴 경우 계정이 일정기간 잠기도록 운영하는 클리핑 레벨(Clipping Level)을 적용하므로 공격은 성공하기 어렵다. 쉽게 유추 가능한 비밀번호를 사용하지 않는 한 스크립트에 의한 CSRF 공격으로는 명령 수행을 끝까지 완수할 수 없게 된다

마찬가지로, CAPTCHA를 적용할 경우에도 ⓑ, ⓒ, ⓓ 위치에 CAPTCHA 인증이 표출되는지 여부를 스크립트로 감지하고 CAPTCHA를 해독하는 스크립트가 구동되어야 하나 브라우저상에서 컴퓨팅 파워가 약해 계산에 오랜 시간이 소요되며 브라우저 프로세스의 CPU 점유율이 높아지고 Hang(멈춤)이 걸려 운영자의 눈에 쉽게 띄게 된다. 최근 머신러닝 등 AI를 활용한 CAPTCHA 크랙이 활성화 되고 있으나 시간제한을 10초 이내로 제한하면 차단효과가 높다.

공격자가 사전에 정보를 알 수 없는 재인증과 CAPTCHA 인증방식을 무작위로 표출시키기 때문에 순서상의 위치를 파악해야 하는 어려움까지 추가되어 공격방어효과가 높다. 이는 OWASP에서 강력하게 권고하는 3가지 인증 선택 방식[표 4]에 무작위성을 가미한 형태이다.

Ⅵ. 결 론

본 연구에서는 풍력발전단지를 대상으로 한 사이버 공격 사례를 살펴보았으며. CSRF 공격을 효과적으로 대응하기 위한 대응방안을 설계하였다. 본 연구에서는 인증모델에 대한 설계만을 다루었다.

고도로 숙련된 해커가 산업제어영역에 침투하여 관리SW의 기능을 사용하고자 할 때 무작위로 표출되는 재인증(Re-authentication), CAPTCHA, OTP 기술이 접목된다면 자동화된 스크립트의 공격으로는 정상적인 공격을 수행할 수 없게 된다. 웹 기반의 CSRF 공격 뿐만 아니라 일반 실행파일 형태의 관리프로그램에서도 위 기능을 적용하여 예방할 수 있을 것으로 기대한다.

참 고 문 헌

[1] 산업통상자원부, “재생에너지 3020 이행계획(안) 발표(보도자료)”, Dec 2017.

[2] 임성정, “전력유틸리티 자동화 표준, IEC 61850의 표준개발 현황“, *Journal of the Electric World,* Aug, 2015

[3] CPNI, "The Cyber Assessment Frame work 3.0", Sep, 2019

[4] MITRE, Common Weakness Enumerati on 352(CSRF, Cross Site Request For- gery)

[5] DOE, “미연방에너지관리법(Public Law 93-275)", 1973～1974

[6] OWASP, "Cross Site Request Forgery Prevention Cheet Sheet", Mar, 2018

[7] Jason Staggs, "Adventures in Attacking Wind Farm Control Networks", Blakhat, Jul 2017

[8] CyberScoop, "Utah renewables company was hit by rare cyberattack in March", Oct, 2019

[9] SEGRID(Security for Smart Electricity GRIDs)

[10] SEGRID, "D6.7 Final report on disse- mination and standardisation activit- ies", Jan, 2018

[11] SEGRID, "D6.8 Elaborate use case scenario", Jan, 2018

[12] 최재영, "웹사이트 구조와 사용패턴 분석을 통한 CSRF 공격 탐지", 융합보안논문지 제11권 제6호, 2011년 12월

[13] 박진현, “서버와 사용자간 비밀 값을 이용한 보안성이 강화된 CSRF 방어”, 한국통신학회논문지 제39권 제3호, 2014년 3월

〈저 자 소 개〉

김 정 완 (Jeong Wan Kim)

정회원

2007년 2월: 세종사이버대학교 정보보호시스템공학과 졸업

2018년 8월~현재: 고려대학교 정보보호대학원 석사 과정

2010년 3월~2011.11월: 방송통신사이버안전센터 운영 총괄

2011년 12월~현재: 한국남동발전 정보보호팀, 신재생사업처 근무

<관심분야> 침해사고대응, 제어시스템보안, 위협헌팅

김 휘 강 (Huy Kang Kim)

종신회원

1998년 2월: KAIST 산업경영학과 학사

2000년 2월: KAIST 산업공학과 석사

2009년 2월: KAIST 산업및시스템공학과 박사

2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director

2010년 3월～현재: 고려대학교 정보호호대학원 교수

<관심분야> 온라인게임 보안, 네트워크 보안, 네트워크 포렌직, 침입탐지시스템, 봇넷탐지