스마트에너지 해킹으로 인한 사회기반시설 마비 시나리오

20161267 김동준

요 약

스마트에너지란 전기 및 정보통신 기술을 활용하여 지능화, 고도화함으로써 고품질의 에너지 서비스를 제공하고 에너지 이용효율을 극대화하는 전력망이다.
이렇게 정보통신기술(ICT)를 접목하여 에너지 인프라를 효율적으로 관리하는 '스마트에너지' 산업이 성장함에 따라 다양한 해킹 공격의 대상으로 노려지고 있다.
에너지 분야는 사이버공격 피해를 입어 시설이 마비되면 오프라인 생활권에 중대한 지장을 주거나 심각할 경우 인명 피해도 발생할 가능성도 있다.

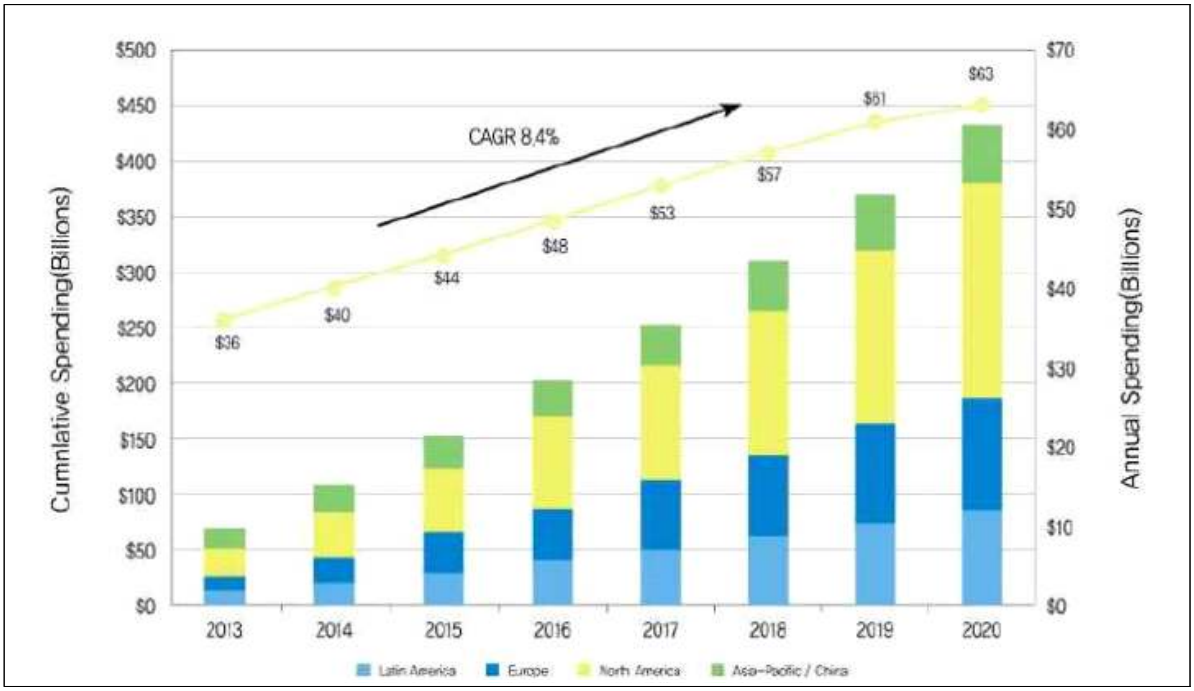
본 시나리오에서는 점차 성장하고 있는 스마트에너지를 주제로 다양한 해킹사례, 보안 위협을 시작으로 다양한 가상 해킹 시나리오를 작성해보고 그에 따른 보안대책들을 서술해보려고 한다.

1. 서론

1.1. 스마트에너지 시장의 전망 및 중요도

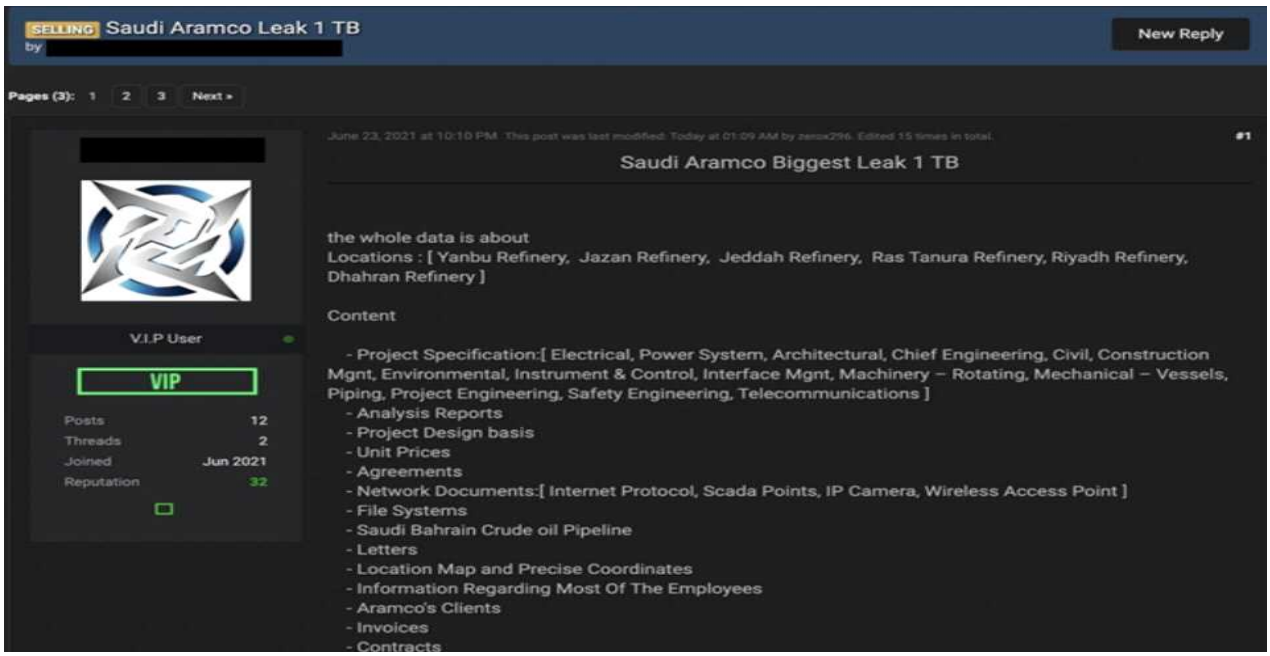
기후변화 문제로 전세계 주요국들이 탄소중립을 선언하면서 스마트에너지에 대한 관심이 고조되고 있다. 기후위기 상황에 맞서 에너지 절약의 중요성이 커지고 있는 상황에서 스마트에너지 분야의 활용과 성장은 에너지 이용효율을 최적화하여 탄소중립 목표달성에 기여할 수 있을 것으로 기대된다.

미국은 노후 전력망 현대화 및 신재생에너지 활용을 위해, 유럽은 신재생에너지 보급 확대와 회원국 간 전력거래 활성화를 위해 스마트에너지 사업을 추진하고 있다.
일본은 원전사고 이후 신재생에너지 보급, 중국은 송전계통 강화 측면에서 스마트에너지 사업을 확대해나가고 있다.
우리나라 스마트에너지 시장규모는 연평균 25%씩 성장하여 2022년 약 3.3조원 규모의 시장을 형성할 것으로 전망되며, 2030년까지 세계 최초의 국가 단위 스마트에너지 구축을 계획하고 있다.



위 그림처럼 GTM Research는 2020년 스마트 에너지 시장의 누적가치가 4,500억 달러를 넘어서고 연평균성장률(CAGR)은 8.4%에 달할 것으로 전망된바 있다.
중국은 24% 이상의 점유율로 세계 최대의 스마트 그리드 시장이 될 것으로 예상되며 그 뒤를 북미(23.9%), 아시아 태평양(21.2%), 유럽(20.6%) 순으로 따를 것으로 전망했다.

1.2. 스마트에너지(스마트그리드)관련 해킹 사례



세계 최대 규모의 정유 회사인 사우디 아람코의 1TB의 데이터 해킹 피해

ZeroX 해커그룹이 세계 최대 규모의 공공 석유 및 가스 회사인 Saudi Aramco에 제

로데이 취약점을 악용하여 1TB의 데이터를 탈취했다고 주장했다.
탈취한 정보에는 해당 기업의 직원 개인정보, 내부 분석 보고서 및 네트워크 정보 등이 포함되어 있으며, 해커들은 유출된 데이터 삭제 비용으로 5000만달러(약 580억원)의 암호화폐를 요구했다고 한다.

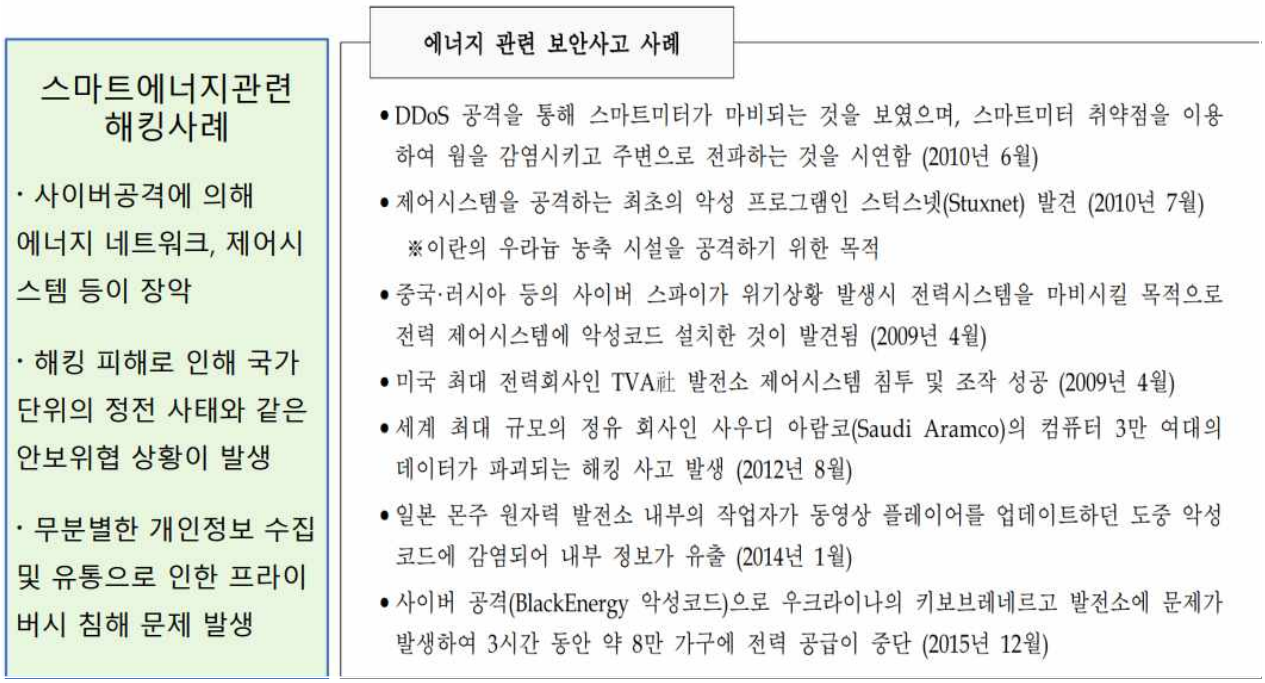
[제로데이: 보안상의 취약점이 발견된 후, 패치가 배포되기까지의 몇일을 기다리지 않고 그날 즉각적으로 공격이 이루어진다는 의미]

사우디 아람코가 해킹 공격을 받은 것은 이 사건이 처음이 아니며, 사우디 아람코는 지난 2012년에도 해킹 공격을 받아 정제 시설 가동이 중단된 바 있다.
당시 샤문이라 불리는 강력한 전파 속도와 파괴력을 가진 악성코드 공격으로 사우디 아람코 본사에 있는 컴퓨터 중 약 3만여 대의 컴퓨터 내 저장된 데이터 일부분 또는 전체 데이터가 삭제되기도 했다.

스마트미터의 취약점을 이용해 웜을 감염 후 주변으로 전파되는 것을 시연

스마트미터의 취약점을 이용해 24시간 동안 22,000개의 스마트미터 중 15,000~20,000개의 스마트미터가 웜에 감염되는 것을 시뮬레이션 하였다.
웜에 감염된 스마트미터는 단전 및 요금 조작이 가능하다.

[스마트미터:기존의 원격검침용 전자식 전력량계와는 다르게 양방향 통신이 가능하며 고객에게는 전력품질과 전력사용량에 대한 정보를 제공하고, 나아가 가정용 전자제품에 대한 직접 제어도 할 수 있는 차세대 전력량계를 의미함]



스마트에너지관련 공격 사례

사이버공격에 의해 에너지 네트워크, 제어시스템 등이 장악되거나 해킹 피해로 인해 국가 단위의 정전 사태와 같은 안보위협 상황이 발생된다.
그뿐만 아니라 무분별한 개인정보 수집 및 유통으로 인한 프라이버시 침해 문제 발생 등 다양한 에너지 보안사고 사례등이 있다.

2. 적용분야 및 관련기술

2.1. 첨단계량인프라(AMI) 보안위협

스마트미터, DCU, ESI, CED(IHD, 스마트폰) 등을 이용하여 첨단계량인프라를 구축하기 위해 에너지 공급자(Third Party Provider)가 전력사용량을 원격검침하고 관련 정보를 소비자에게 알려주는 서비스 제공하는 과정에서 발생 가능한 보안위협

[1] 비인가 기기 접근

•외부로부터 연결된 네트워크를 통해 스마트미터, DCU, AMI Headend에 인가되지 않은 접근을 시도

[2] 교환 메시지 유출 및 변조

•AMI Headend와 MDMS 간 교환되는 메시지에 대해 유출 및 변조 시도

•TPP 와 MDMS 간 교환되는 메시지에 대해 위·변조 시도

[3] 분산서비스 거부공격(DDoS)

•AMI 주요 구성 요소에 대한 DDoS 공격을 시 도하여 정상적인 통신을 방해

•ESI 와 TTP 간 인 터페이스를 통한 DDoS 공격을 시 도하여 정상적인 통신방해

[4]물리적 접근 공격
•물리적으로 스마트미터, DCU 등에 접근하여 적절하지 못한 템퍼링 공격 보호 기술을 악용하여 중요 정 보 추출, 악성코드 삽입, 계측된 계량 정보 조작 및 상위 컨트롤 시스템 공격 시도

※탬퍼링 공격 : 디바이스의 하드웨어적 파괴 또는 분해를 통하여 해당 디바이스의 불법 개조 또는 보안 정보를 추출하여 공격

2.2. 에너지저장장치(ESS) 보안위협
공급자가 전력사용량을 원격검침하고 관련 정보를 소비자에게 알려주는 서비스 제공, 배전관리시스템(DMS)에 의한 변전소 정보 원격 취득 및 제어 등을 수행하는 과정에서 발생 가능한 보안위협

[1]교환 메시지 유출 및 변조
•ESS와 DSC(Distribution Substation Controller) 간, PMS와 Distribution SCADA 간 통신연계 구간에서 교환되는 메시지에 대해 불법적으로 유출 및 변조 시도
[2] 불법 제어명령 전송
•ESS로 인가되지 않은 제어명령(On/Off, Open/Close 등 개폐명령)로 전송 시도
[3] 불법적인 침입 시도
•ESS와 DSC(Distribution Substation Controller)/Distribution SCADA 간 통신연계 구간을 통해 ESS에 대 한 불법적인 침입을 시도

2.3. 전기차(EV) 충전시스템 보안위협
EV 전력사용량을 원격검침하고 관련 정보를 소비자에게 알려주는 서비스 제공 등을 수행하는 과정에서 발생 가능한 보안 위협

[1] 교환 메시지 변조 및 유출
•전기차의 통신모듈과 충전스테이션의 통신모듈 간 인터페이스를 통해 교환되는 메시지에 대해 불법 적으로 변조 시도 •HAN/BAN 네트워크를 통해 교환 메시지에 대해 불법적으로 유출 및 변조 시도
[2] 비인가 통신 데이터 유입
•외부로부터 연결된 네트워크를 통해 BAN 또는 HAN에 인가되지 않은 통신 데이터 유입 시도
[3] 메시지 부인
•전기차 충전에 대한 사실부인하거나 계량정보가 전송된 후에 그 사실을 증명하지 못하도록 사실 부인

2.4. 셀프주유기 및 셀프충전기 보안위협

주유 요금, 가스충전 요금을 결제하는 과정에서 민감한 정보(신용카드 정보 등)를 취급하는 셀프주유기 및 셀프충 전기의 POS 시스템에서 발생 가능한 보안위협

[1] 중요정보 불법 접근

• 메모리 해킹, 탭핑, 스키밍, 악성코드 등의 공격 기법을 사용하여 셀프주유기·충전기의 중요정보(민감한 신용카드 정보, 신용카드 번호)를 유출 시도

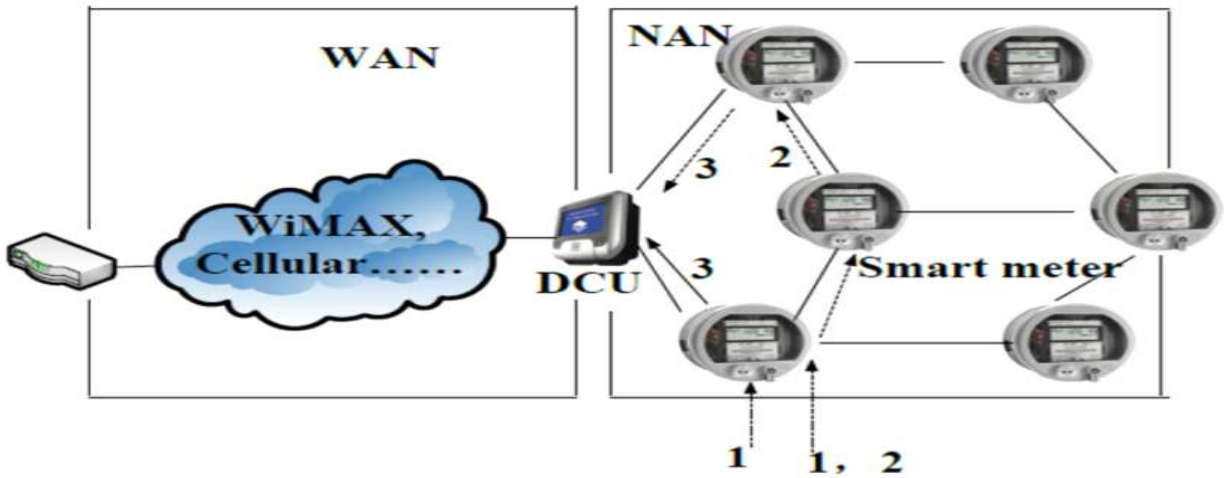
-메모리 해킹: 이용자가 입력한 데이터 등이 메모리상에 평문으로 처리되는 구간을 포착하여 민감한 신용카드 정보, 신용카드 번호, 암호키를 추출해내는 공격기법

-스키밍: 카드리더기 등에 부착되어 민감한 신용카드 정보 등을 빼내어 정보를 전자적으로 복제하는 공격기법

-탭핑: 카드리더기와 신용카드 단말기 사이의 케이블을 도청하여 민감한 신용카드 정보 등을 절취하고 복제하는 공격기법

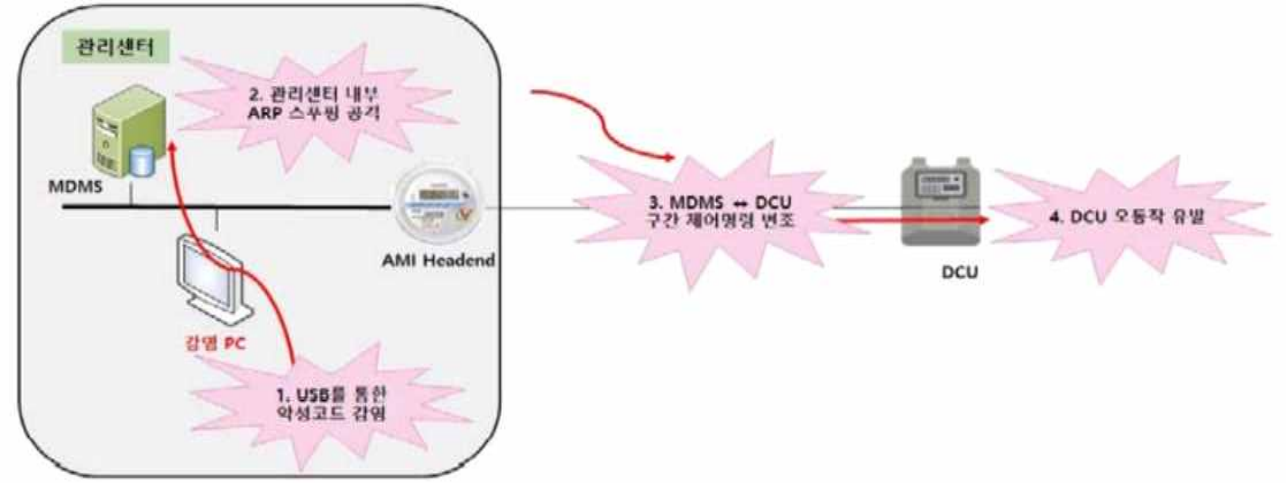
3. 시나리오

3.1. DCU에 대한 DDOS 공격 시나리오 [AMI]



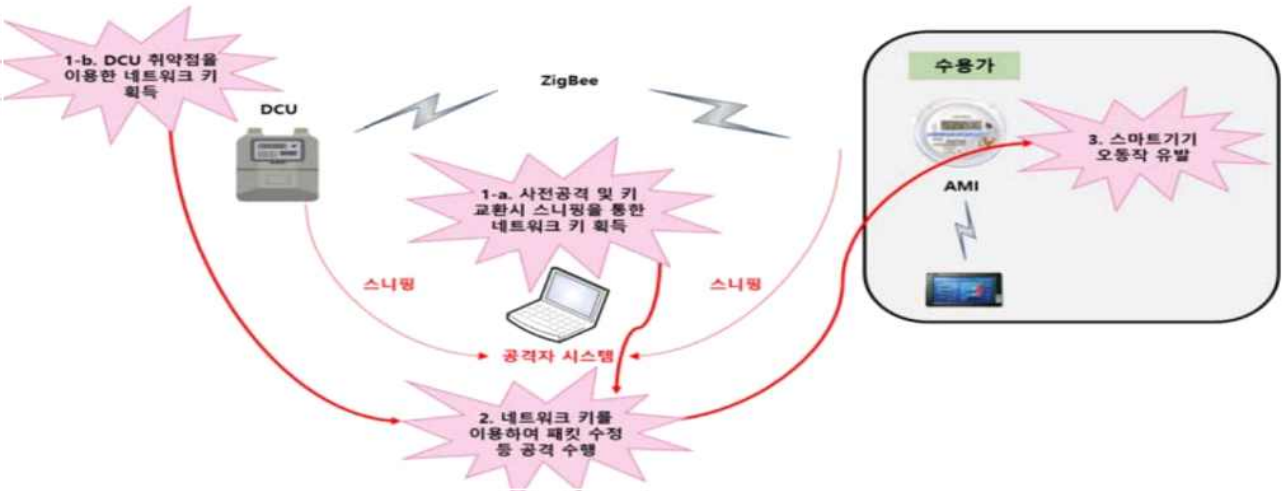
1. 네트워크 취약점을 악용하여 스마트미터 물리적 조작 또는 악성 소프트웨어 설치(그림 1번)
2. 침투된 스마트미터에서 DDOS 공격 개시(그림 2번)
3. DCU로 다량의 악의적인 네트워크 패킷이 전송됨(그림 3번)

3.2. 악성코드를 이용한 MDMS 시스템 공격 시나리오 [AMI]



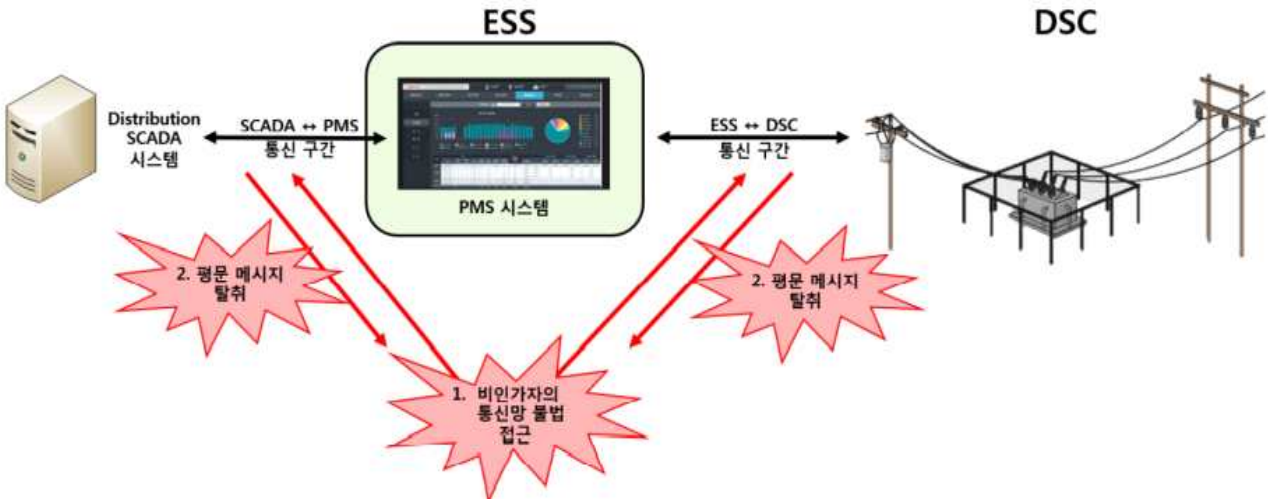
1. USB를 이용하여 공격코드(ARP 스푸핑 공격)를 관리자의 PC에 설치
2. MDMS 시스템은 감염PC를 AMI Headend로 인식하고, AMI Headend는 감염PC를 MDMS 시스템으로 인식
3. MDMS 시스템 및 DCU간 전송되는 모든 패킷은 감염 PC로 전송됨
4. 감염PC는 MDMS 시스템과 DCU사이에서 제어명령어 변조 공격을 통하여 DCU와 스마트미터에 대한 불법적인 제어 가능

3.3. 무선 통신 프로토콜에 대한 공격 시나리오 [AMI]



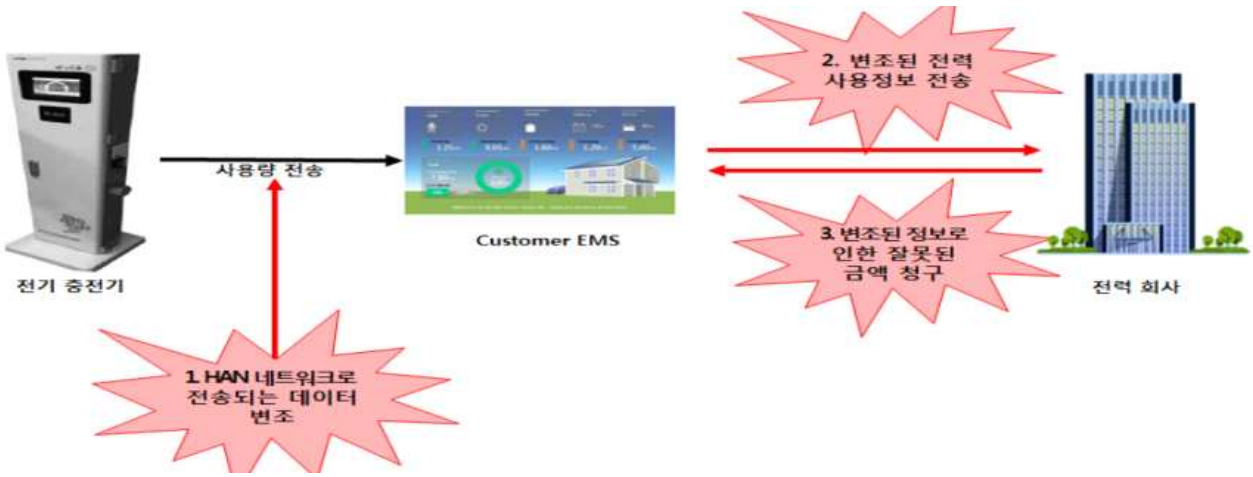
1.탬퍼링 방지가 구현되지 않은 DCU 장비에 직접 접근하여 ZigBee 프로토콜에서 사용하는 네트워크 키 획득 (DCU에 대해 사전공격을 수행하여 ZigBee 네트워크 키 획득)
2. 네트워크 키와 수집된 패킷 정보를 이용하여 스마트 미터조작 및 가전 제어 메시지 조작
3. 조작된 메시지를 이용하여 스마트미터 및 가전제품 조작

3.4. 통신연계 구간 접근을 통한 메시지 유출 시나리오 [ESS]



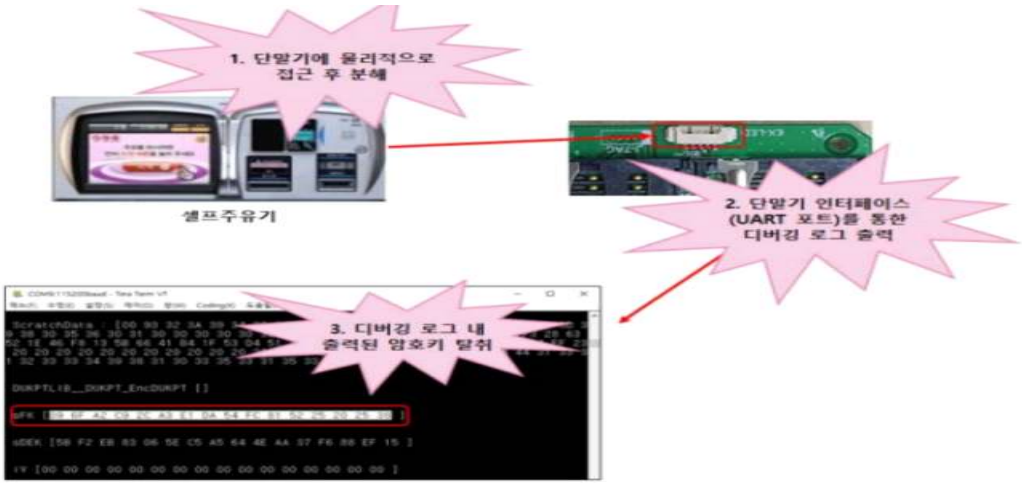
1. 비인가자의 불법적인 통신연계 구간으로 접근
2. 통신연계 구간을 통해 교환되는 평문 메시지 탈취하여 악용가능

3.5. 전기차 충전설비와 EMS간 통신에서 전력사용량 조작 시나리오 [EV충전기]



1. 충전설비와 Customer EMS간 통신 데이터(전력 사용량)를 변조
2. Customer EMS는 충전기로부터 변조된 데이터를 전달받아 전력회사로 전송
3. 전력 회사에서 변조된 전력 사용량에 따라 금액을 청구하게 되어 금전적 손실 발생

3.6. 셀프주유기 인터페이스를 통한 디버깅 로그 분석을 통한 암호 유출 시나리오 [셀프 주유기, 충전기]



1. 단말기에 물리적으로 접근하여 분해 후 내부 인터페이스 확인
2. 단말기 내부 인터페이스(UART 포트)를 통한 디버깅 로그 출력
3. 디버깅 로그 내 출력되는 암호키 정보 탈취

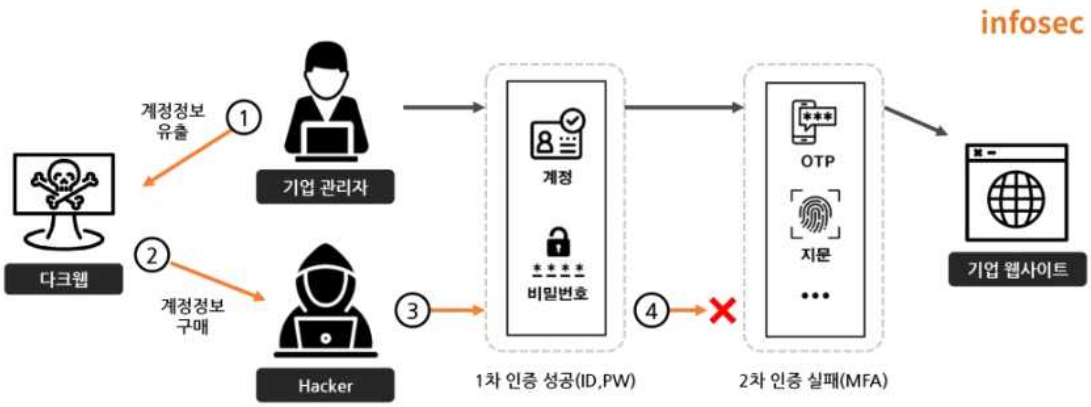
4. 대응책

4.1. AMI, ESS, EV충전기 보안대책

[1] 기기 인증(Device Authentication)

•외부 인터페이스를 통해 스마트미터, DCU, AMI Headend의 네트워크 비인가 접근을 차단하기 위한 기기 인증 기능 필요

-MFA[멀티팩터인증]



로그인 기능에서 MFA(멀티팩터인증)를 AMI, ESS, EV에 대한 해킹위협의 대응책으로 사용할 수 있다.

아이디와 비밀번호 입력 후 다른 인증요소를 사용한 2차 인증이 추가로 요구되기 때문에 정보가 해커나 다크웹에 유출되더라도 비인가자가 도용한 정보로 접근하지 못하게 방어할 수 있다.

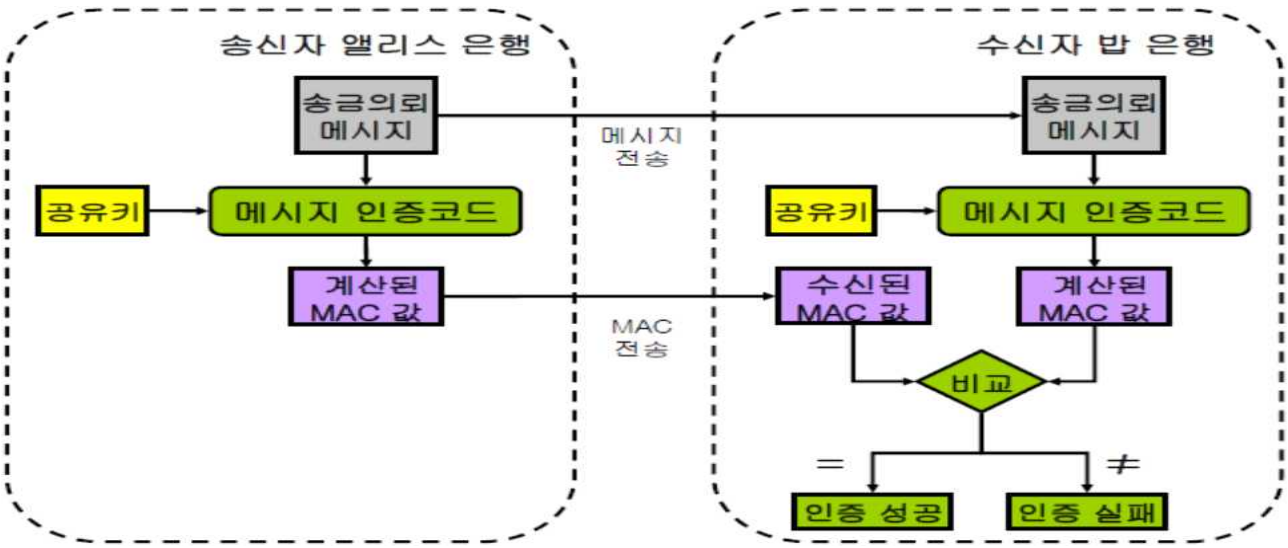
이 방법은 위에서 설명한 해커들이 제로데이 취약점을 이용하여 사우디 아람코의 해킹 피해를 준것에서의 대응책으로도 쓰일수 있을 것이다.

[2] 네트워크 접근제어(Network Access Control)

•스마트미터와 DCU(Data Collection Unit)에 유입되는 통신 데이터들에 대해서 MAC (Message Authentication Code) 검증을 통해 비인가 통신 데이터를 차단하는 네트워크 접근제어 기능 구현

메시지인증코드(MAC, Message Authentication Code)

데이터가 통신 중 변조되지 않았다는 무결성 검증이 필요할 때, 메시지인증코드 (MAC, Message Authentication Code)를 사용한다.



메시지 인증 코드를 이용한 인증 순서

① 송신자 앨리스와 수신자 밥은 사전에 키를 공유해 둔다.

② 송신자 앨리스는 송금 의뢰 메시지를 기초로 하여 공유키를 사용해서 MAC 값을 계산한다.

③ 송신자 앨리스는 수신자 밥에게 송금 의뢰 메시지와 MAC 값을 보낸다.

④ 수신자 밥은 수신한 송금 의뢰 메시지를 기초로 하여 공유키를 사용해서 MAC 값을 계산한다.

⑤ 수신자 밥은 앨리스로부터 수신한 MAC 값과 계산으로 얻어진 MAC 값을 비교한다.

⑥ 수신자 밥은 2개의 MAC 값이 동일하면 송금 의뢰가 틀림없이 앨리스로부터 온 것이라고 판단한다.(인증 성공)

동일하지 않다면 앨리스로부터 온 것이 아니라고 판단한다.(인증 실패)

[3] 부인방지(Non-Repudiation)

•전력사용량, 과금과 관련한 중요 정보를 교환하는 경우 해당 메시지 송신 사실에 대한 부인방지 기능을 구현

-부인 방지(Non-Repudiation)는 어느 개체가 수행한 행위를 부정(거짓말)하는 것을 방지하는 속성이다.

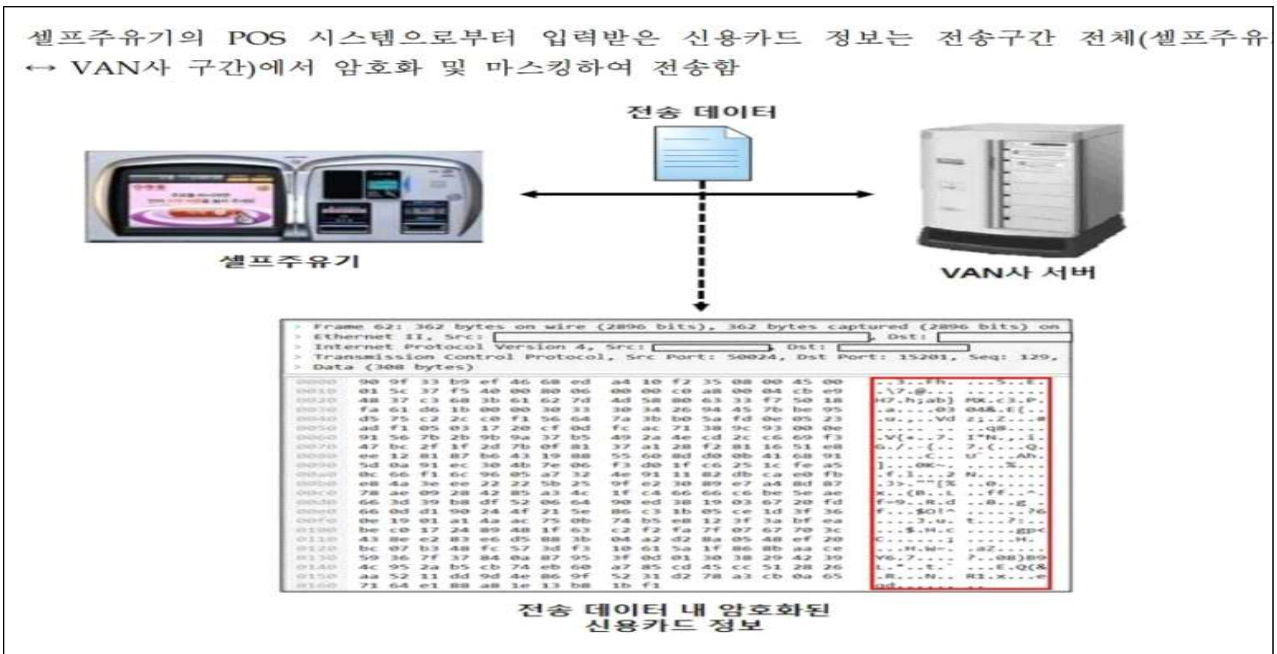
부인 방지를 보장한다는 것의 의미는 간단히 이야기하면 특정 값의 생성은 특정 개체만이 할 수 있다는 것이다.

즉, 특정 값을 "밥(Bob)"이 가지고 있어도, 그 값을 "앨리스(Alice)"만이 생성할 수 있다면, 자연스럽게 "송신 부인 방지"를 보장한다.

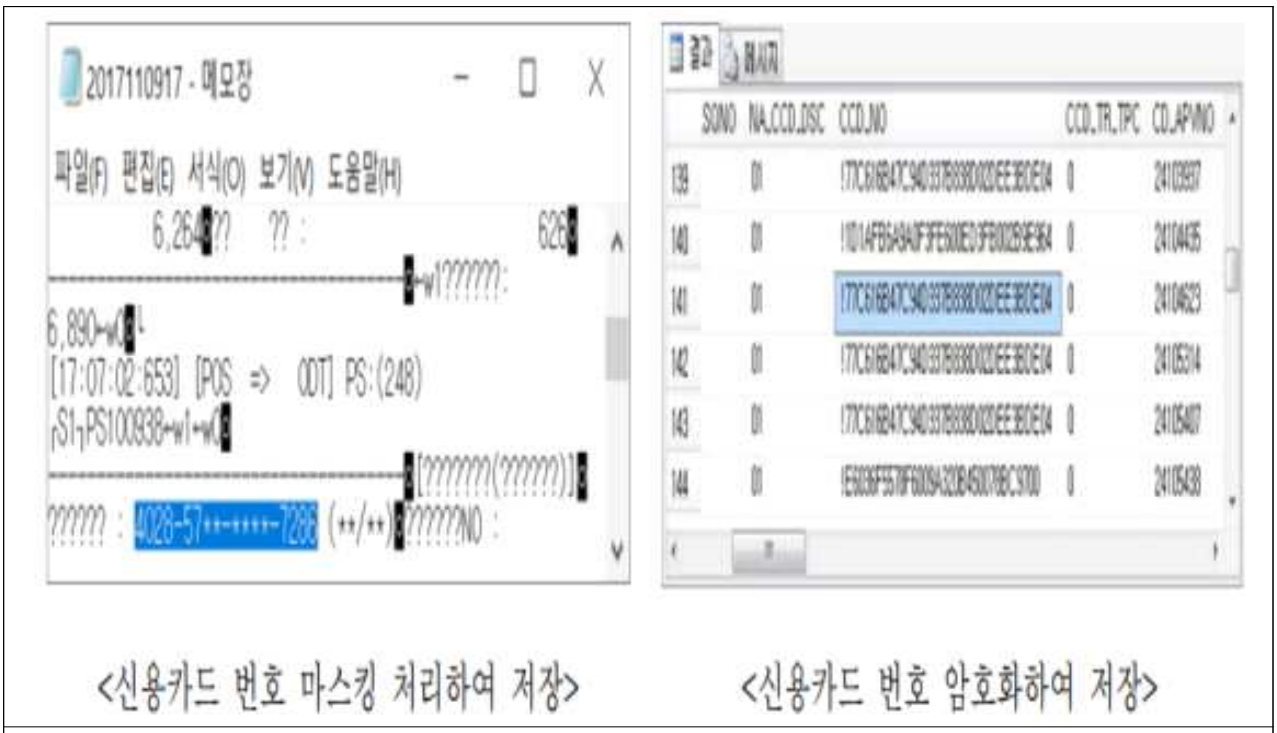
즉 앨리스가 이 값을 (실제로 송신했지만) 송신한 적이 없다고 부인할 수 없는 것이다.

4.2 셀프 주유기충전기 보안대책

[1] 신용카드 정보 보호



민감한 신용카드 정보 전송구간의 기밀성 보장

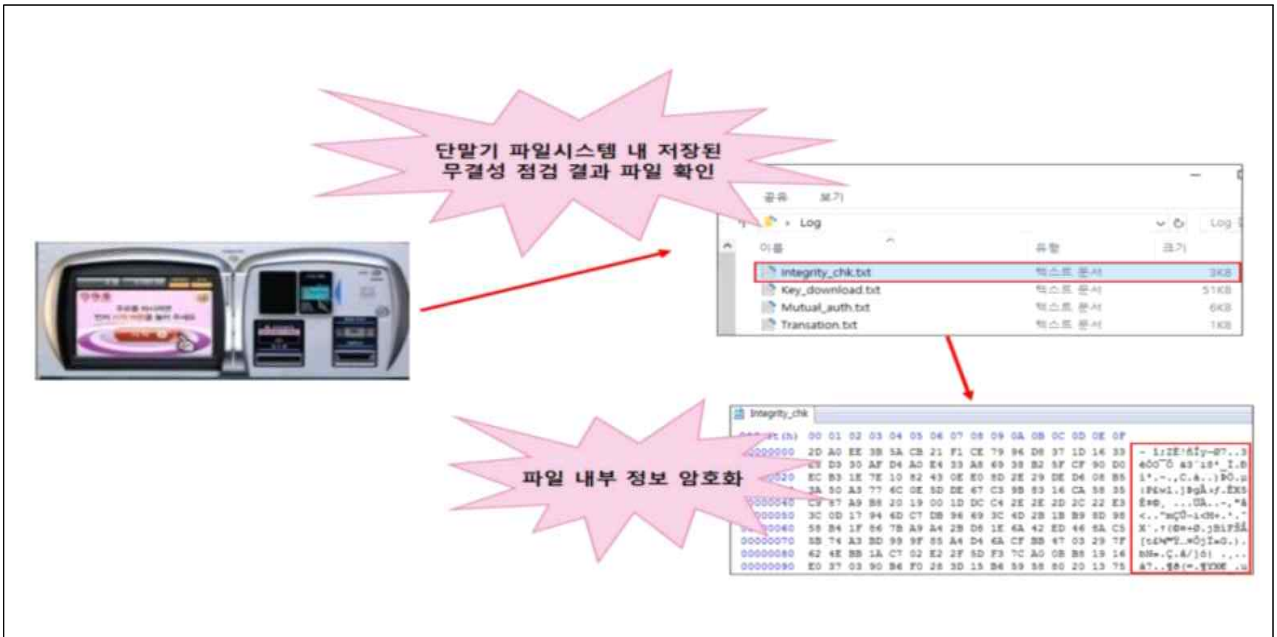


신용카드 번호 저장 시 보호 방안

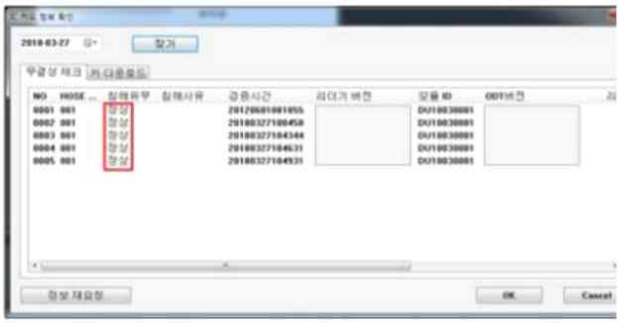
[2] 자체보호

• 셀프주유기충전기에서 POS단말기의 정상적인 동작을 위해 카드리더기 작동 시, 주기적으로 보안기능, 실행코드 및 보안기능관련 저장데이터 변경여부를 탐지하기위해 무결성 점검을 수행한다.

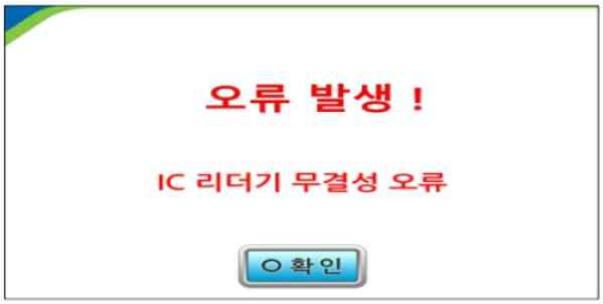
•무결성 검증 실패하면 동작을 중단하고 관리자에게 통보한다.

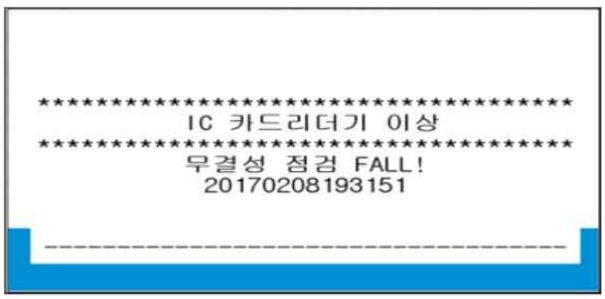


보안기능 관련 저장데이터(무결성 점검 결과)를 암호화



셀프충전기에서 무결성 점검 수행 및 무결성 점검결과 조회 화면





셀프충전기에서 무결성 점검 실패시 화면

5. 참고자료

[1] 한국IR협의회 스마트그리드 에너지 효율을 극대화하는 차세대 전력인프라 시스템 pp. 12, 2021.02

[2] https://news.mt.co.kr/mtview.php?no=2021072210203281049

[3] 한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 Smart Grid 해외 공격사례 및 한국 Smart Grid에 대한 예상 공격분석과 보안대책 (2011. 06)

[4] 스마트그리드 사이버 보안 동향 koreascience.kr 서정택 이철원(ETRI 부설연구소)

[5] 스마트에너지 사이버보안 가이드 KISA한국인터넷진흥원 (2019.12)

[6] https://m.blog.naver.com/wnrjsxo/221719726759