情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

전기자동차 충전 인프라에서의 보안위협 및 보안요구사항 분석*

강 성 구,† 서 정 택‡
ETRI 부설연구소

An Analysis of the Security Threats and Security Requirements for Electric Vehicle Charging Infrastructure*

Seong-ku Kang,† Jung-taek Seo‡
The Attached Institute of ETRI

요 약

지구 온난화에 대한 대응 노력으로 스마트그리드가 주목받고 있으며, 국내의 경우 정부는 CO2 배출량의 20%를 차지하고 있는 수송 분야를 대체하기 위한 노력으로 전기자동차 및 충전 인프라 구축을 확대하고 있다. 하지만 전기자동차 충전 인프라는 지능화를 위해 IT기술을 접목하고 있어 기존 IT기술이 가지고 있던 보안위협들을 그대로 상속받을 수 있다. 이로 인해 발생할 수 있는 보안 사고를 미연에 방지할 수 있도록 보다 안전한 전기자동차 충전 인프라 구축이 요구된다. 이에 본 논문은 전기자동차 충전 인프라에 대한 논리적 아키텍처를 제시하고 이를 바탕으로 발생 가능한 보안위협들을 식별하였다. 또한, 이러한 보안위협들을 대응하기 위한 보안요구사항을 분석 및 제시하였다.

ABSTRACT

With response to the critical issue of global warming, Smart Grid system has been extensively investigated as next efficient power grid system. Domestically, Korean is trying to expand the usage of Electric Vehicles (EVs) and the charging infrastructure in order to replace the current transportation using fossil fuels holding 20% of overall CO2 emission. The EVs charging infrastructures are combined with IT technologies to build intelligent environments but have considerable number of cyber security issues because of its inherent nature of the technologies. This work not only provides logical architecture of EV charging infrastructures with security threats based on them but also analyses security requirements against security threats in order to overcome the adversarial activities to Smart Grid.

Keywords: EV Charging Infrastructure, Security Threats, Security Requirement

I. 서 론

최근 전 세계적으로 지구 온난화에 대한 우려를 나타내고 있으며 이에 대응하기 위한 온실가스 감축 노력을 강화하고 있다. 1997년 12월 일본 교토에서 열린 기후 변화협약 제3차 당사국 총회에서 '교토의정서'가 채택되었고, 2007년 12월 인도네시아 '발리로드맵'에서 제13차 기후 변화협약에서 환경문제가 이슈화되

접수일(2011년 11월 8일), 수정일(1차: 2012년 4월 24일, 2차: 2012년 7월 2일), 게재확정일(2012년 8월 20일)
* 본 연구는 2010년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (NO. 201010040046A)
† 주저자, ssabro@ensec.re.kr
‡ 교신저자, seojt@ensec.re.kr

면서 이에 따라 우리나라도 2013년부터 온실가스 의무 감축 대상국에 포함되었다. 이에 따라 우리나라는 스마트그리드(Smart Grid)에 주목하고 있다. 스마트그리드란 기존 전력망(Grid)에 ICT기술(Smart)을 접목하여 전력공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지효율을 최적화하는 차세대 전력망이다. 전력망이 스마트그리드로 진화되면, 양방향 실시간 정보교환을 통하여 합리적 에너지 소비를 유도할 수 있어 고품질의 에너지 및 다양한 부가서비스 제공이 가능하고 개방적 운영시스템의 특성으로 인해 신재생에너지발전, 전기자동차 등 청정 녹색기술의 접목·확장이 용이해진다. 특히 국내 스마트그리드 분야 중 전기자동차 영역의 경우 저탄소 녹색성장정책을 통해 CO2 배출량의 20%를 차지하고 있는 수송 분야를 대체할 전기자동차 개발과 원활한 보급을 위한 충전 인프라 구축 계획이 지난 2010년 12월 발표되었다. 따라서 전기자동차의 보급 확대와 전기자동차를 위한 충전 인프라 구축이 가속화 될 것으로 판단되고 있다[1].

하지만, 전기자동차 충전을 위한 인프라는 다양한 시스템 및 유·무선 통신 기술들을 조합하여 사용하므로 네트워크 구축, 서비스 개발, 시스템 운영 등에 있어 다양한 보안위협이 발생할 수 있으며, 이런 보안위협들이 발생할 경우 정상적인 충전 및 거래 불가, 사용자의 개인정보 침해 등 다양한 문제들이 야기될 수 있다. 따라서 보다 안전한 전기자동차 충전 인프라 구축을 위해서는 먼저 전기자동차 충전 인프라 환경을 분석하고, 이러한 환경에서 어떤 보안위협들이 존재하고 있는지에 대한 분석이 선행되어야 한다. 이어 식별된 보안위협에 대응하기 위한 보안요구사항을 확인하여 충전 인프라 구축 시 반영이 될 수 있도록 해야 한다.

본 논문에서는 전기자동차 충전 인프라 환경에서의 서비스분석을 통해 사용사례를 도출하고 도출된 사용사례 분석을 통해 충전 인프라 환경을 파악 및 참조할 수 있는 논리적 아키텍처를 제시한다. 또한, 제시한 논리적 아키텍처를 바탕으로 충전 인프라 환경이 가질 수 있는 보안위협을 식별한 뒤 이에 대응하기 위한 보안요구사항을 제시한다.

본 논문의 구성은 2장에서 전기자 충전 인프라 사용사례 분석을 통해 논리적 아키텍처를 제시한 뒤 3장에서는 제안된 논리적 아키텍처를 바탕으로 보안위협을 식별한다. 4장에서는 식별된 보안위협에 대응하기 위한 보안요구사항을 제시한 뒤 5장에서 결론을 맺는다.

II. 전기자동차 충전 인프라 논리적 아키텍처

전기자동차 충전 인프라는 전기자동차에 전력을 공급하기 위한 기반시설과 서비스로 다양한 시스템 및 통신 기술들이 조합되어 구성될 수 있다. 전기자동차 충전 인프라에 대해 보다 명확한 보안요구사항을 제시하기 위해 충전 인프라에 대해 충분한 이해가 필요하며 이를 돕기 위해 전기자동차 충전 인프라를 참조할 수 있는 모델이 필요하다. 이러한 참조 모델을 통해 인프라를 구성하는 객체들을 식별할 수 있으며 그 객체들 간의 관계와 객체들 사이에 교환되는 정보 종류 등을 알 수 있다. 국내 전기자동차 충전 인프라 모델은 현재 구체적으로 정의되지 못하고 있으므로, 본 장에서는 전기자동차 충전 인프라 서비스에 대한 사용사례를 분석한 뒤 이를 바탕으로 충전 인프라를 구성하는 객체(Actor, 행위자)를 식별하고 객체들 간의 정보흐름 확인 및 통신환경 등을 분석하여 전기자동차 충전 인프라 참조 모델을 제시한다.

2.1 전기자동차 충전 인프라관련 서비스 및 사용사례

국내 제주 스마트그리드 실증단지에는 세계적인 스마트그리드 실증단지를 조기에 구축하고 관련기술의 상용화 및 수출 산업화를 촉진하기 위해 제주도 구좌읍의 6천호 가구를 대상으로 5개 분야에 12개의 컨소시엄이 참여하고 있다. 5개 분야는 지능형 전력망(Smart Power Grid), 지능형 소비자(Smart Consumer), 지능형 운송(Smart Transportation), 지능형 신재생(Smart Renewable), 지능형 전력서비스(Smart Electricity Service) 이며, 이 중 지능형 운송 분야는 차세대 교통수단인 전기자동차의 운행을 위한 충전 인프라 시험구축 및 전기자동차 운행정보 중앙관제 시스템 구축 등의 신서비스 구축을 목적으로 실증이 진행 중이다[2].

제주 스마트그리드 실증단지 지능형 운송 분야에서 실증중인 충전 인프라에 대한 서비스 내용을 살펴보면 [표 1] 과 같이 정리할 수 있다[3,4,5,6].

국내의 경우 단순 전기자동차의 충전 서비스뿐만 아니라 전기자동차 렌터카 등과 같은 비즈니스 모델들을 구상하여 사용자에게 보다 다양한 서비스를 제공할 수 있도록 실증하고 있음을 알 수 있다.

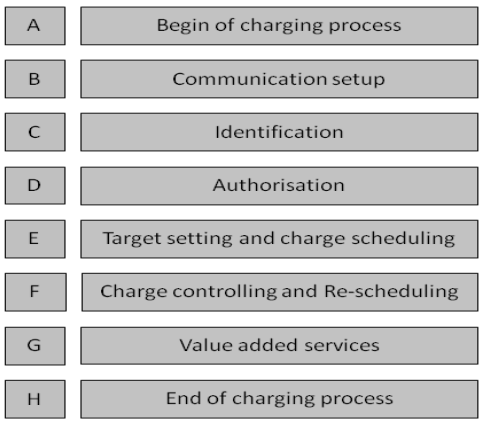
현재 국외의 경우 ISO/IEC를 중심으로 전기자동차 인프라에 대한 통신 인터페이스에 대해 표준화를 진행 중에 있다. ISO/IEC 15118은 전기자동차와

〔표 1〕 제주 스마트그리드 실증단지 지능형 운송 분야 서비스

서비스	설명
충전기 상태 모니터링 서비스	충전기 상태, 충전기 이력, 각 충전기별 전력 소비량을 운영센터에 전송
충전 관련 정보 제공 서비스	운영센터에서 충전소 및 충전기에 전력 단가 기준정보, 기상정보, 구좌읍 전력 사용량, CO2 배출량, 구좌읍계통고장정보들을 제공
충전 결제 서비스	전기자동차 충전 시 스마트카드를 사용하여 결제 관련 정보를 CDMA 망을 통해 T-money 발행사인 한국스마트카드社로 전송
충전소 및 전기자동차 홈페이지 서비스	충전소정보조회, 차량위치조회, 전기자동차정보, 충전이력조회, 차량운행조회 가능
전기 자동차 충전 서비스	전기 자동차 충전 서비스 제공
사용자 웹 포탈 및 원격 관리 서비스	인터넷 웹 포탈을 통해 일반 사용자에게 충전 서비스 사용량 조회 서비스를 제공할 예정
충전내역 정보 수집 서비스	충전소로부터 사용된 충전 내역(충전량, 충전대상 등) 수집

그리드 사이의 통신 링크 및 프로토콜을 포함한 인터페이스에 관한 표준을 다루는 문서로 파트1의 경우 전기자동차와 그리드 사이에서의 사용사례를 분석하고 있다. 본 논문에서 언급되는 사용사례는 〔그림 1〕 과 같이 충전의 시작, 통신설정, 사용자 식별, 인증, 충전방법 설정, 충전제어, 부가서비스, 충전종료 그룹으로 나누어 설명한다[7].

본 표준에서는 사용사례들을 개발 시 단순하면서 자동화된 지불이 가능하도록, 가격 또는 배터리 효용



〔그림 1〕 ISO/IEC 15118 파트1 사용사례 그룹

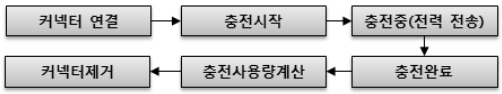
측면에서 최적화된 충전 서비스를 제공할 수 있도록, 다양한 서비스들이 개발되고 적용될 수 있도록 다양한 사례들을 고민하여 개발되고 있다.

위와 같은 내용을 종합할 때 전기자동차 충전 인프라와 관련한 서비스는 크게 충전을 위한 서비스, 충전 운영관리를 위한 서비스, 기타 부가서비스로 나누어 볼 수 있다. 충전 서비스는 충전 인프라의 가장 기본이 되는 서비스이며, 충전 서비스를 보다 안전하고, 효과적으로 관리하기 위해 충전운영관리 서비스가 존재한다. 더불어, 충전 서비스 외에 사업자의 차별성, 고객 유치 등을 고려한 기타 부가서비스가 존재할 수 있다. 이러한 서비스 별로 고려될 수 있는 사용사례는 〔표 2〕 와 같다.

⊙ UA1. 전기자동차 충전은 일반적으로 〔그림 2〕 와 같은 기본 절차를 가질 수 있다.

〔표 2〕 전기자동차 충전 인프라관련 서비스

서비스	사용사례	설명
A. 충전 서비스	UA1. 전기자동차 충전	전기자동차 배터리에 전기를 충전
	UA2. 전기자동차 충전 중 제어	전기자동차 배터리 충전 시 충전 전류 등을 제어
	UA3. 충전금액결제	전기자동차 배터리에 충전한 전력량에 대한 금액 결제
B. 충전 운영 관리 서비스	UB1. 충전모니터링	충전상태, 충전기 상태, 각 충전기별 전력 소비량을 공급자가 모니터링
	UB2. 전력계통 운영	실시간 전력 사용정보와 전력 단가 정보를 상위 기관(전력 제공자 등)과 정보 공유
	UB3. 사용자(회원)인증	전기자동차 충전 사용자에 대한 ID카드, 전기자동차 정보 등을 통한 인증
	UB4. 사용자(회원)관리	전기자동차 충전 사용자 등록, 수정, 해지 등에 대한 사용자 정보 관리
	UB5. 충전기관리 서비스	충전기 시스템점검, 충전기의 펌웨어 및 S/W 업데이트 등
C. 기타 부가 서비스	UC1. 전기자동차 부가서비스	충전소정보조회, 차량위치조회, 전기자동차정보, 차량운행조회 등 다양한 부가 서비스 제공
	UC2. 고객 부가서비스	고객 충전이력 조회, 고객 충전요금 부과 정보 조회 등의 서비스 제공



〔그림 2〕 전기자동차 충전 기본 절차

충전을 위해 사용자가 충전기의 커넥터를 전기자동차에 연결 시 전기자동차와 충전기 간에 통신을 위한 파라미터 교환을 통해 통신프로토콜 버전 등을 파악하여 두 객체 간 통신이 정상적으로 이루어 질 수 있도록 도울 수 있다. 또한, 사용자는 충전방식을 충전량이나 충전금액을 기준으로 선택할 수 있으며, 충전완료 시 충전금액 결제 등을 위해 사용된 전력 사용량을 계산할 필요가 있다.

⊙ UA2. 전기자동차 충전 중 제어는 전기자동차에게 전송되는 전력정보를 모니터링 하여 예기치 않은 상황 등이 발생될 경우 충전기에 제어명령을 보내 처리하게끔 유도하는 사용사례이다. 이러한 제어는 충전기 자체에서 판단하여 스스로 제어하거나, 중앙 제어 시스템을 두어 충전기를 제어할 수 있다.

⊙ UA3. 충전금액 결제는 전기자동차에 충전된 전력량과 충전 단가를 바탕으로 계산되며 현금, 신용카드, 체크카드, 사용자 가정 요금에 합산, 상품권, 선불카드, 스마트폰 결제, 은행계좌 결제 등을 사용하여 충전금액을 결제할 수 있다. 결제수단에 따라 사용자 인증이 불필요하거나 요구될 수 있다. 현금, 상품권, 선불카드의 경우에는 사용자 인증이 불필요하며, 신용카드를 포함한 나머지 방법들은 사용자 인증이 요구된다.

⊙ UB1. 충전모니터링은 충전상태, 충전기 시스템 자체의 건강(Health)상태, 충전기별 전력 소비량 등을 모니터링 하는 것으로, 특히 충전기가 충전기에 전력을 공급하고 있을 경우, 충전절차의 단계, 출력 전압 및 전류 상태, 차량배터리 상태 등을 모니터링 한다.

⊙ UB2. 전력계통운영은 상위 전력운영시스템과 양방향으로 전력운영정보를 교환하고 전력품질을 관리하는 사용사례로 운영자는 실시간 전력사용정보, 사용한 전력통계정보 등을 제공할 수 있으며, 상위 전력공급자는 실시간 전력단가 정보, 전력품질 등과 같은 정보를 제공할 수 있다.

⊙ UB3. 사용자(회원)인증은 충전 인프라 환경, 결제수단 등에 따라 요구될 수 있으며 다양한 인증 방식이 사용될 수 있다. 먼저 신용카드, ID, 스마트폰 등 전기자동차 사용자가 가지고 있는 수단을 통해 인증을 수행할 수 있으며 더 나아가서는 전기자동차 자체가 가지고 있는 정보를 바탕으로 사용자 인증을 수행할 수 있다.

⊙ UB4. 사용자(회원)관리는 운영자가 사용자를 등록 및 관리하고 필요 시 해지하는 등 사용자 정보를 관리하는 사용사례로 사용자별 요금제 관리, 부과된 요금 정보 확인 등을 수행할 수 있다.

⊙ UB5. 충전기관리서비스는 충전기 관리를 위해 시스템을 점검하고 필요 시 충전기의 펌웨어, O/S 등을 패치 및 업데이트하는 서비스이다.

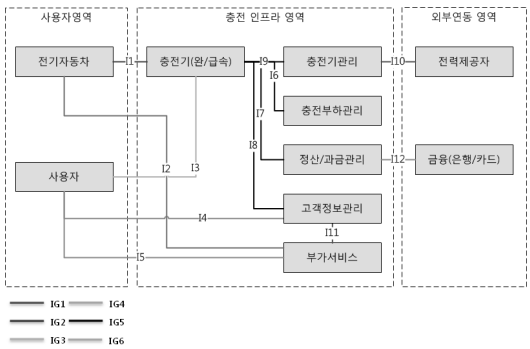
⊙ UC1. 전기자동차 부가서비스는 전기자동차에게 다양한 정보를 제공하는 서비스로 가까운 충전소 위치 정보, 주행한 거리 정보, 실시간 주변 교통정보 등 위치정보를 기반을 둔 서비스들을 제공할 수 있으며, 전기자동차 차량 상태를 원격으로 점검하도록 하거나 응급 호출 서비스를 제공하는 등 다양한 서비스들이 제공될 것으로 판단된다.

⊙ UC2. 고객 부가서비스는 공급자가 사용자에게 정보를 제공하는 사용사례로 사용자가 전기자동차 충전 내역을 확인하거나 부과된 요금 등을 확인하거나 사용할 수 있는 요금제, 결제방식 등을 선택하게 하는 등, 다양한 서비스들이 제공될 것으로 판단된다.

2.2. 전기자동차 충전 인프라 논리적 아키텍처

위에서 언급한 사용사례로부터 분석된 전기자동차 충전 인프라에 대한 논리적 아키텍처는 〔그림 3〕 과 같다.

위와 같은 논리적 아키텍처를 제시하기 위해 먼저 사용사례로부터 객체들을 식별하였으며 식별된 객체 간의 관계를 파악하여 인터페이스를 확인하는 순서로 분석을 진행하였다.



〔그림 3〕 전기자동차 충전 인프라 논리적 아키텍처

〔표 3〕 사용사례로부터 식별된 객체 설명

객체	설명
전기자동차	PHEV(Plug-in Hybrid Electric Vehicle)를 포함하여 배터리와 전기모터의 동력을 이용하는 자동차
사용자	전기자동차 사용자 및 충전 인프라 서비스 사용자
충전기	전기자동차 배터리를 충전하기 위한 장치로 A.C(교류) 또는 D.C(직류) 형태의 충전기로 나눌 수 있음
충전부하관리	충전기의 부하 및 전기품질 관리와 급전지시와 같은 제어기능을 수행, 충전상태를 모니터링 할 수 있는 시스템으로 충전 시 전기자동차의 상태정보, 충전진행사항, 충전부하정보 등을 모니터링
충전기관리	충전운영을 위한 시스템으로 충전기에서 사용된 전력량을 수집하고 전력공급 상위시스템과 실시간으로 정보를 교환하는 시스템. 또한, 충전기관리를 위한 충전기상태정보를 확인하고 시스템 업데이트 등을 관리
정산/과금관리	충전 과금 및 결제를 외부 금융사(은행, 카드 등)와 연계하여 수행 및 관리
고객정보관리	고객의 개인정보 관리를 관리하고 사용자 인증 처리, 충전 이력 등의 정보를 관리
부가서비스	전기자동차 및 사용자에게 부가적인 정보를 제공해 주는 시스템으로 충전소 위치정보, 주행거리, 교통관련 정보(실시간 도로상황 등), 충전통계관련정보, 전기자동차정보(이력, 이동경로 등), 기타(뉴스, 날씨, 지역정보 등등)를 제공
전력제공자	충전 서비스 제공자에게 전력을 제공
금융(은행/카드)	사용자에게 부과된 과금을 실제로 처리

〔표 4〕 전기자동차 충전 인프라 논리적 인터페이스 식별

식별 번호	행위자 A	행위자 B	교환정보	인터페이스 네트워크 특성
I1	전기자동차	충전기	UA1. 커넥터 연결 및 해지 신호, 통신 파라미터정보, 충전 방법(금액, 충전량 등) 결정 정보, 충전상태 정보 UA2. 충전 제어 명령 및 응답 UA3. 결제수단에 필요한 전기자동차정보(전기자동차 ID 등) UB1. 충전 상태 정보 UB3. 전기자동차 식별정보 및 인증정보	CAN(Controller Area Network), PLC(Power Line Communications), ZigBee 통신방식이 고려되고 있으며, 저수준 통신 및 IP통신 모두 고려되고 있음
I2	전기자동차	부가서비스	UC1. 충전소 위치정보, 주행거리 정보 등등	무선통신(공용망)이용
I3	사용자	충전기	UA3. 결제수단에 필요한 사용자 정보(카드번호 등) UB3. 사용자 식별정보 및 인증정보	충전기 HMI를 이용
I4	사용자	고객정보관리	UB4. 사용자 식별 및 인증정보, 사용자(전기자동차) 관련 정보,	사용자 PC, 단말기기 등을 사용하여 IP기반의 유/무선통신(공용망)이용
I5	사용자	부가서비스	UC2. 충전 이력정보, 부과된 요금정보 등등	사용자 PC, 단말기기 등을 사용하여 IP기반의 유/무선통신(공용망)이용
I6	충전기	충전부하관리	UA2. 충전 제어 명령 및 응답 UB1. 충전기 시스템 정보, 전력 부하정보 등	IP기반의 유/무선통신(공용망, 사설망) 이용
I7	충전기	정산/과금관리	UA3. 사용자 정보, 전기자동차 정보, 충전량(전력사용량)정보, 결제관련 정보	IP기반의 유/무선통신(공용망, 사설망) 이용
I8	충전기	고객정보관리	UA3. 사용자 정보, 전기자동차 정보 UB3. 전기자동차, 사용자 식별정보 및 인증정보	IP기반의 유/무선통신(공용망, 사설망) 이용
I9	충전기	충전기관리	UB5. 충전기 상태 정보, 충전기 업데이트 정보	IP기반의 유/무선통신(공용망, 사설망) 이용
I10	충전기 관리	전력제공자	UB1. 전력부하정보 UB2. 전력품질 정보, 실시간 전력사용량, 실시간 전력 단가 정보	IP기반의 유선통신(사설망) 이용
I11	부가서비스	정산/과금관리	UA3. 충전량(전력사용량)정보, 결제관련 정보	IP기반의 유선통신(사설망) 이용
I12	정산/ 과금관리	금융 (은행/카드)	UA3. 결제관련 정보	IP기반의 유/무선통신(공용망, 사설망) 이용

먼저 사용사례로부터 식별한 객체들과 이에 대한 설명은 〔표 3〕 과 같다. 식별된 객체들은 물리적으로 독립되어 운영되는 객체를 식별하기보다 기능적인 측면에서 논리적인 객체로 파악하여 구분 및 명명하였다.

논리적 인터페이스는 각 객체들 사이에서 발생되는 모든 정보교환 인터페이스를 의미한다. 따라서 각 인터페이스에 대한 관련 객체, 관련 객체 간에 교환되는 정보를 〔표 4〕 와 같이 사용사례별로 분석할 수 있었으며 총 12개의 인터페이스로 정리할 수 있었다.

전기자동차와 부가서비스, 사용자와 부가서비스, 사용자와 고객정보관리 인터페이스는 일반 유·무선 환경의 인터넷망과 같은 공용망을 사용할 가능성이 높으며 그 외의 인터페이스의 경우 대부분 전용선 등을 통해 폐쇄적인 사설망으로 구성될 가능성이 높다. 하지만 충전기와 충전부하관리, 정산/과금관리, 고객정보관리, 충전기관리에 해당하는 인터페이스는 충전기의 위치가 물리적으로 원격지에 위치하거나, 충전서비스를 제공하는 사업모델에 따라 유·무선통신의 공용망을 사용하여 충전인프라를 구성할 수 있다. 전기자동차와 충전기는 임베디드 시스템 또는 일반PC급의 성능을 가질 것으로 판단되며 기타 시스템들은 서버 급에 해당되는 성능을 가질 것으로 판단된다. 운영환경의 경우 전기자동차와 충전기는 물리적으로 외부, 공개된 장소에서 설치 및 운영될 것이며, 기타 시스템들은 상대적으로 제한된 구역에서 운영될 것으로 판단된다.

〔표 5〕 인터페이스 특성 별 구분 및 그룹화

구분	인터페이스 특성	인터페이스 식별번호
IG1	저수준 통신 및 IP통신 모두 고려, CAN, PLC, ZigBee등 이용 가능	I1
IG2	IP기반 통신 고려, 무선통신(공용망)이용	I2
IG3	충전기 HMI를 이용	I3
IG4	IP기반 통신 고려, 유·무선(공용망)을 이용	I4, I5
IG5	IP기반 통신 고려, 유·무선(공용망, 사설망)을 이용	I6, I7, I8, I9, I12
IG6	IP기반 통신 고려, 유선(사설망)을 이용	I10, I11

인터페이스 특성에 따라 위에서 식별한 인터페이스들을 〔표 5〕 와 같이 구분 및 그룹화 할 수 있다.

III. 전기자동차 충전 인프라 보안위협

Ⅱ장에서 제시한 전기자동차 충전 인프라 아키텍처를 바탕으로 각 인터페이스에서 발생될 수 있는 보안위협을 식별하고 각 인터페이스별 해당될 수 있는 위협 및 취약점을 식별한다.

충전 인프라 환경에서의 위협원은 내·외부 모두 존재할 수 있으며, 위협원들은 악의적·비악의적인 의도

〔표 6〕 인터페이스에서 발생될 수 있는 보안위협

위협 항목	설명	발생구간
T1. 우회	시스템의 인증 메커니즘을 우회하는 공격	시스템
T2. 유출	데이터의 기밀성을 무력화 시키는 행위	
T3. 악성코드	시스템 또는 네트워크에 위해를 가할 목적으로 개발된 악의적인 소프트웨어를 배포하는 행위	
T4. 위장	인가된 사용자/자산으로 가장하여 위장하는 행위	
T5. 위/변조	데이터의 무결성을 무력화 시키는 행위	
T6. 무작위 대입	보안 속성(키, 패스워드 등)에 대한 대입 가능한 모든 값을 시험	
T7. 권한상승	허가되지 않은 권한 사용	
T8. 템퍼링	승인되지 않은 방식으로 시스템 데이터, 비즈니스 정보 및 환경설정 정보를 수정	
T9. 부인	시스템 자신이 수행(요청 등)한 일을 부인하는 행위	
T10. 서비스 거부	시스템 및 네트워크 자원에 과부하를 주어 서비스 요청을 처리하지 못하게 하는 행위	시스템/ 네트워크
T11. 하이잭(Hijack)	기존에 인증된 통신 연결을 도용하여 사용하는 행위	네트워크
T12. 중간자 공격	두 접속자 사이에 감지되지 않도록 위치해 메시지 읽기, 삽입 및 변조를 임으로 가하	
T13. 재전송 공격	수집된 통신 데이터를 이용하여 불법적인 재전송 행위	
T14. 도청	승인되지 않은 통신망 분석 행위	
T15. 물리적 공격	물리적인 위해나 파괴를 하는 행위	기타
T16. 사회공학	기밀정보 또는 특정 접근 권한을 얻기 위해 해당 주체에 접근하여 정보 수집	

〔표 7〕 인터페이스 그룹별 발생 가능한 보안위협

구분	인터페이스 특성	발생 가능한 보안위협
IG1	저수준 통신 및 IP통신 모두 고려, 임베디드 시스템↔임베디드 시스템	T1~T9, T10, T11~T14, T15
IG2	IP기반 통신 고려, 무선통신(공용망)이용, 임베디드 시스템↔서버급 시스템	T1~T9, T10, T15
IG3	충전기 HMI를 이용, 사람↔임베디드 시스템	T1~T9, T10, T15, T16
IG4	IP기반 통신 고려, 유·무선(공용망)을 이용, 사람↔서버급 시스템	T1~T9, T10, T11~T14, T15, T16
IG5	IP기반 통신 고려, 유·무선(공용망, 사설망)을 이용, 임베디드 시스템↔서버급 시스템	T1~T9, T10, T11~T14
IG6	IP기반 통신 고려, 유선(사설망)을 이용, 서버급 시스템↔서버급 시스템	T1~T9, T10

를 가질 수 있다. 이러한 위협원들로부터 인터페이스 상에 발생될 수 있는 잠재적 보안위협은 〔표 6〕 과 같다[14].

이러한 잠재적 보안위협들이 실제 각 인터페이스별 적용될 수 있는 내용을 살펴보면 〔표 7〕 과 같이 적용할 수 있다.

충전인프라에 존재하는 시스템들의 경우 기존 정보시스템과 큰 차이가 존재하지 않으므로 위에서 식별한 시스템에서 발생될 수 있는 잠재적 보안위협들은 대부분의 인터페이스 그룹에 적용이 가능하다. IG1 인터페이스는 커넥터를 통해 물리적으로 CAN과 PLC의 1:1 통신을 보장할 수 있지만, 이런 통신매체를 이용하여 차량 내부네트워크와 직접적으로 연결될 경우 차량 내부 네트워크에 연결된 악의적인 기기 등에 의해 도청, 재전송 공격, 서비스 거부 공격 등의 보안위협에 노출될 수 있다[14]. IG2와 같이 보안기술이 이미 적용된 3G 또는 4G와 같은 이동통신을 사용하는 인터페이스나 IG6과 같은 유선 사설망을 사용하는 인터페이스들은 네트워크상에 발생될 수 있는 보안위협들이 실제 발생되기 어려울 것으로 판단되며 IG4, IG5와 같이 유선 공용망을 사용하는 경우 네트워크와 관련된 보안위협들이 발생될 수 있다. 전기자동차와 충

〔표 8〕 인터페이스에서 발생될 수 있는 보안취약점

분류	보안위협	설명
S/W 취약점	V1. API 오용	API에 대한 부정확한 사용으로 인한 취약점
	V2. 소프트웨어 코드 품질	미 검증된 소프트웨어 사용, 버퍼 오버플로, Off-By-One Overwrite, 라이브러리 스트링 포맷 취약성, 정수 오버플로
	V3. 취약한 API 사용	취약성을 가지고 API를 사용
	V4. 에러처리	의도하지 않거나 예측 불가한 동작을 일으킬 수 있는 부적절한 에러처리
	V5. 유효하지 않은 입력	포맷 및 내용이 유효하지 않은 입력에 대한 처리
	V6. 프로토콜	취약점을 가진 프로토콜 사용 및 입증되지 않은 프로토콜의 사용
접근 제어	V7. 부실한 접근제어	임무의 적절한 분리나 범위 제한을 위한 접근제어 방법의 부적절성
	V8. 접근제어의 불필요한 사용	일반 동작에도 불필요하게 높은 권한을 요구하는 소프트웨어
암호/ 인증	V9. 민감한 데이터에 대한 미 보호	전송, 저장 및 처리 데이터에 대한 부적절한 보호
	V10. 암호의 부적절한 사용	키의 유도 방식의 취약, 키 스트림 및 초기 벡터의 부적절한 재사용, 안전하지 않은 암호 모드(e.g. AES ECB) 사용, 안전하지 않은 무결성 알고리즘 사용, 불충분한 키 길이, 안전하지 않은 초기 벡터(IV) 사용
	V11. 난수발생기 결함	난수 생성은 암호프로토콜의 무결성과 기밀성을 보장하는데 사용되며 구현 결함은 시스템 취약성을 가져옴
	V12. 부적절한 암호키 분배	시스템 내 고정된 공통키 사용 등
	V13. 부적절한 인증	인증 메커니즘의 취약점
기기 및 시스템운영	V14. 불필요한 서비스	시스템에 대한 불필요한 서비스
	V15. 세션 관리	부적절한 세션 식별자 사용으로 재연 공격을 발생시킴
	V16. 기본 설정 사용	보안이 고려되지 않은 기본 보안설정 사용
	V17. 로그 및 감사	부적절한 이벤트 기록, 저장, 및 처리

전기는 물리적으로 사람의 접근이 가능하므로 T15. 물리적 공격이 가능하며 HMI를 통한 사용자간 통신의 경우 HMI의 취약점을 통해 위에서 언급한 보안위협들이 발생할 수 있다. 실제 HMI를 사용하는 은행 ATM기기의 경우 초소형 카메라 사용, 이중덮개 번호판, 스키밍 장비 등을 사용하여 사용자의 핀(PIN) 번호를 탈취하는 등의 공격사례가 있으며, 충전기 HMI 또한 이와 유사한 형태로 공격이 수행될 수 있다[8].

전기자동차, 충전기를 포함한 행위자들은 기존 IT 시스템들과 마찬가지로 시스템 자체 설계상의 오류 등 공격자에 의해 오용될 수 있는 다양한 보안취약점들을 가질 수 있다. 이러한 보안취약점들은 S/W취약점, 접근제어에 관한 취약점, 암호·인증에 관한 취약점, 기기 및 시스템 운영상의 취약점, 물리적 취약점이 있을 수 있으며 정리하면 〔표 8〕 과 같이 처리할 수 있다[15].

IV. 전기자동차 충전 인프라 보안요구사항 분석

4.1. 인터페이스별 보안요구사항 분석

인터페이스의 보안위협에 대응하기 위해 필요한 보안서비스로는 기밀성, 무결성, 가용성, 부인방지, 인증 및 허가 서비스가 요구된다. 각 인터페이스 및 인터페이스에서 교환되는 정보별 요구되는 보안요구사항을 제시하기 전에 인터페이스에서 발생 가능한 보안위협과 보안서비스를 매핑하면 〔표 9〕 와 같다.

보안요구사항에 대한 보안강도 설정을 위해 먼저 인터페이스별 교환되는 정보 내용의 중요성을 '상',

〔표 9〕 인터페이스에서 발생할 수 있는 보안위협과 보안서비스 매핑

위협 항목	필요한 보안서비스
T1. 우회	인증/허가, 가용성
T2. 유출	기밀성
T3. 악성코드	무결성
T4. 위장	인증/허가
T5. 위/변조	기밀성, 무결성
T6. 무작위 대입	인증/허가
T7. 권한상승	인증/허가
T8. 템퍼링	무결성
T9. 부인	부인방지
T10. 서비스 거부	기밀성
T11. 하이잭(Hijack)	인증/허가
T12. 중간자 공격	기밀성, 무결성
T13. 재전송 공격	인증/허가
T14. 도청	기밀성
T15. 물리적 공격	-
T16. 사회공학	-

〔표 10〕 인터페이스 및 사용사례별 보안요구사항

식별번호	교환정보	중요도	기밀성	무결성	가용성	부인방지	인증/허가
I1	UA1. 커넥터 연결 및 해지 신호, 통신파라미터정보, 충전 방법(금액, 충전량 등) 결정 정보, 충전상태 정보	중	하	중	중	X	상
	UA2. 충전 제어 명령 및 응답	상	중	상	상	O	
	UA3. 결제수단에 필요한 전기자동차 정보(전기자동차 ID 등)	상	상	상	중	O	
	UB1. 충전상태 정보	중	하	중	중	X	
	UB3. 전기자동차 식별정보 및 인증정보	상	상	상	중	X	
I2	UC1. 충전소 위치정보, 주행거리 정보 등등	하	하	하	하	X	하
I3	UA3. 결제수단에 필요한 사용자 정보(카드번호 등)	상	상	상	중	O	상
	UB3. 사용자 식별정보 및 인증정보	상	상	상	중	X	
I4	UB4. 사용자 식별 및 인증정보, 사용자(전기자동차) 관련정보,	상	상	상	중	X	상
I5	UC2. 충전이력정보, 부과된 요금정보 등등	중	중	중	중	O	중
I6	UA2. 충전 제어 명령 및 응답	상	중	상	상	O	상
	UB1. 충전기 시스템정보, 전력부하 정보 등	상	중	중	상	X	
I7	UA3. 사용자 정보, 전기자동차 정보, 충전량(전력사용량)정보, 결제관련 정보	상	상	상	중	O	상
I8	UA3. 사용자 정보, 전기자동차 정보	상	상	상	중	X	상
	UB3. 전기자동차, 사용자 식별정보 및 인증정보	상	상	상	중	X	
I9	UB5. 충전기 상태 정보, 충전기 업데이트 정보	중	하	중	중	O	중
I10	UB1. 전력부하 정보	상	중	중	상	X	상
	UB2. 전력품질 정보, 실시간 전력사용량, 실시간 전력 단가 정보	상	중	중	상	X	상
I11	UA3. 충전량(전력사용량)정보, 결제관련 정보	상	상	상	중	O	중
I12	UA3. 결제관련 정보	상	상	상	중	O	중

'중', '하'로 판단하였다. 교환되는 정보가 개인정보 또는 충전금액 결제와 관련된 정보, 충전 제어와 관련된 정보일 경우 다른 정보에 비해 보다 더 중요하다고 판단되어 '상'으로 판단하였으며 그 외 정보들은 '중'으로 판단하였다. 이 중 충전소 위치정보와 같이 사용자에게 편의를 위한 부가서비스정보는 충전서비스와 상대적으로 직접적인 관계가 없으므로 '하'로 그 중요성을 나타였다. 위에서 매핑한 보안서비스 내용과 정보의 중요성을 기준으로 판단한 보안요구사항은 〔표 10〕과 같다.

기밀성은 인가된 사용자만이 데이터 공유, 의도적 또는 비의도적인 데이터 유출 발생 방지, 사용자의 개인정보에 대한 기밀을 유지가 요구됨을 의미하며, 무결성은 데이터가 변질되지 않았음에 대한 신뢰가 요구됨을 의미한다. 가용성은 데이터, 응용 및 시스템 서비스를 필요로 하는 사용자 및 운영자에게 제공 가능하도록 유지를 의미하며, 부인방지는 데이터를 생성, 변경 및 전송한 사용자가 자신이 생성한 데이터 내용과 전송여부를 부인하는 것에 대한 방지를 의미한다. 인증 및 허가는 기기, 시스템 및 사용자 접근을 위한 상호 인증이 요구됨을 의미한다.

보안요구사항 중 기밀성, 무결성, 가용성은 교환되는 정보의 중요도에 따라 '상', '중', '하'로 판단하였다. 중요도가 '상'인 정보 중 개인정보 및 결제와 관련된 정보일 경우 기밀성은 '상', 무결성은 '상', 가용성은 '중'으로 판단하였으며, 제어와 관련된 정보의 경우 기밀성은 '중', 무결성은 '상', 가용성은 '상'으로 판단하였다. 중요도가 '중'인 정보의 경우 기밀성은 '하', 무결성은 '중', 가용성은 '중'으로 판단하였으며, 이 중 개인정보와 간접적으로 연관된 UC.2 충전이력정보 등은 기밀성을 '중'으로 판단하였다. 중요도가 '하'인 정보의 경우 기밀성은 '하', 무결성은 '하', 가용성은 '하'로 판단하였다. 또한, 부인방지는 교환되는 정보의 특성이 제어와 관련된 정보, 결제와 관련된 정보일 경우 부인에 대한 방지 기능이 요구될 것으로 판단된다. 인증 및 허가는 인터페이스와 관련된 두 행위자간에 일어나는 행위이기 때문에 교화되는 정보별이 아닌 각 인터페이스에 대해 '상', '중', '하'를 표시하였으며, 교환되는 정보의 중요성에 따라 인증 및 허가 서비스의 중요성을 판단하였다.

4.2. 보안취약점에 대한 대책

위에서 언급한 바와 같이 시스템 상에서 발생 가능한 보안취약점들은 S/W취약점, 접근제어에 관한 취약점, 암호·인증에 관한 취약점, 기기 및 시스템 운영상의 취약점들이 존재하며 시스템이 외부에 노출되어 위협원들이 쉽게 접근 가능하여 발생될 수 있는 물리적 취약점들이 존재할 수 있다. 식별된 보안취약점들에 대응하기 위한 보안요구사항은 〔표 11〕과 같다.

〔표 11〕 보안취약점에 따른 보안대책

보안취약점	보안대책	설명
S/W 취약점	보안성검토	운영 시스템에 대해 보안성이 검증된 제품(H/W, S/W)의 사용
	위험평가	지속적인 위험평가를 통한 취약점 발견 및 대응(보안 패치 등) 필요
	입력 값 검증	입력되는 데이터 또는 값에 대해 검증할 수 있는 메커니즘 사용
	안전한 프로토콜	검증된(표준화, 권고되는) 프로토콜을 사용
	시스템 무결성 보호	악성코드, 불법적인 변경으로부터 시스템, 소프트웨어 등을 보호하기 위한 시스템 무결성 보장 필요
접근제어	접근제어	시스템에 대해 인가된 사용자, 시스템, 기기, 설비 등에게만 접근을 허용하며, 허가된 권한에 한해서만 작업을 할 수 있도록 제어
	인적보안	구성원들에게 역할 및 책임을 부여하고 이에 맡는 적절한 권한 부여가 요구됨
암호/인증	식별 및 인증	안전하고 정상적인 사용자 식별 및 인증
	안전한 암호알고리즘 사용	검증된 암호알고리즘 및 암호모듈 사용
	정보 무결성 보호	시스템에 저장 및 송수신 되는 데이터에 대한 무결성 보장 필요
	안전한 키 관리	검증된 키 관리 메커니즘을 사용
기기 및 시스템운영	보안감사	적절한 보안감사 설정을 통한 침입대응 및 사고조사에 대한 대비 필요
	운영의 연속성	충전 서비스 운영이 사이버 사고에 의해 중지되지 않도록 보안 필요
	침입대응	침입에 대한 탐지와 이에 대한 적절한 사고대응 필요
	저장매체의 보호	정보가 저장된 디스크, 보조기억매체 등에 대한 보호 필요
물리적취약점	물리적 환경보안	시설, 장소, 시스템 등을 침해로부터 보호

해당 보안요구사항들이 현실적으로 적용되기 위해 먼저 전반적인 보안정책 설정이 요구되며, 이러한 보안정책을 기반으로 각 보안요구사항에 대해 보다 구체적인 내용을 담아 문서화를 할 필요가 있다. 또한, 이러한 보안요구사항이 적절히 수행되고 있는지에 대한 감사 및 평가가 요구되며 전기자동차 충전 인프라를 운영하는 관리자 및 직원에 대한 지속적인 훈련 및 시험을 통해 보안의식 고취 등이 요구된다.

V. 결 론

현재 전기자동차 충전 서비스는 기존 주유소와 같이 전문적으로 전기 충전을 제공하는 충전소뿐만 아니라 일반주택, 아파트, 직장, 공공기관, 공영주차장, 대형 쇼핑몰, 호텔 등과 같이 다양한 환경에서 충전 서비스가 제공될 수 있을 것으로 판단된다.

국내의 경우 전기자동차와 이를 위한 충전 인프라는 정부정책을 바탕으로 빠르게 발전되고 구축될 것으로 전망되고 있으며, 이러한 충전 인프라의 지능화와 효과적인 서비스 창출을 위해 다양한 ICT기술이 활용될 것으로 판단된다. 하지만, 기존 ICT환경이 가지고 있는 보안취약점들이 충전 인프라 환경에 그대로 상속되어 다양한 보안위협들이 발생 될 수 있다.

따라서 본 논문에서는 보다 안전한 전기자동차 충전 인프라 구축을 위해 다양한 형태로 구축될 충전 인프라에 대해 보안요구사항 개발에 있어 참조할 수 있는 논리적 아키텍처를 제시하였으며, 제시된 논리적 아키텍처를 바탕으로 발생될 수 있는 보안위협 및 보안취약점을 식별하였다. 이어 식별된 보안위협에 대응하기 위한 보안요구사항을 각 인터페이스에서 교환되는 정보의 중요성을 기준으로 기밀성, 무결성, 가용성, 부안방지, 인증 및 허가에 대해 구분하여 제시하였으며, 시스템에서 발생될 수 있는 보안취약점에 대한 보안대책을 정리하여 제시하였다.

하지만, 전기자동차 충전 인프라의 경우 아직 시험 및 구축 단계 이므로 본 논문에서 식별하지 못한 보안위협 및 보안요구사항이 존재할 수 있다. 따라서 앞으로 지속적인 보안위협 식별 및 이에 대한 보안요구사항 개발이 지속적으로 수행되어야 할 것으로 판단되며, 제시된 보안요구사항을 반영하기 위해 전기자동차 충전 인프라 특성을 고려한 구체적인 상호인증기술, 암호화 통신 기술 등에 대한 연구가 필요할 것으로 판단되며, 본 기술의 상호 운용성을 확보하기 위해 표준화가 필요할 것으로 판단된다.

참고문헌

〔1〕 손홍관, "전기자동차 충전인프라와 스마트그리드," 대한전기학회, 전기의세계 59(4), pp 47-53, 2010년 4월

〔2〕 제주스마트그리드실증단지, "제주스마트그리드 실증단지," http://smartgrid.jeju.go.kr/contents/index.php?mid=0202

〔3〕 이현기, "전기자동차 충전인프라 개발현황과 전망," 전력전자학회 전력전자학회지, 15(6), pp 73-76, 2010년 12월

〔4〕 양승권, "전력망 연계 전기자동차 충전인프라 운영 시스템 개발 및 운용 전략," 대한전기학회, 대한전기학회 학술대회 논문집, pp 1120-1121, 2010년 7월

〔5〕 한승호, "전기자동차 보급과 충전인프라 구축", 대한전기협회, 전기저널 402, pp 28-31, 2010년 6월

〔6〕 손홍관, "전기자동차 충전인프라 구축현황," 대한전기협회, 전기저널 397, pp 20-26, 2010년 1월

〔7〕 ISO/IEC 15118-1, "Road vehicles- Vehicle to grid communication interface-Part 1:General information and use-case definition"

〔8〕 장성협, "신용카드가 복제돼 사용되고 있다!...어떻게?," 보안뉴스, 2010년 6월

〔9〕 NIST, "Guidelines for Smart Grid Cyber Security," NISTIR 7628, Aug. 2010

〔10〕 NIST, "Recommended Security Controls for Federal Information Systems," NIST Special Publication 800-53, Aug. 2009

〔11〕 UCAlug, NIST Cyber Security Coordination Task Group, "Security Profile for AMI," Jun. 2010

〔12〕 UCAlug, "AMI System Security Requirements," Dec. 2008

〔13〕 OPENmeter, Requirements of AMI, Jan. 2009

〔14〕 Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, "Experimental Security Analysis of a Modern Automobile," IEEE Symposium on Security and Privacy, Oakland, CA, May. 2010.

〔15〕 Itron White Paper Advanced Metering Infrastructure, "Risk Analysis for Advanced Metering," http://metering.com/i/100934WP-01_Risk%20Analysis_For_Advanced_Metering%5B1%5D.pdf

〈著者紹介〉

사 진

강 성 구 (Seong-ku Kang) 정회원
2008년 2월: 충남대학교 컴퓨터공학과 졸업
2011년 2월: 충남대학교 컴퓨터공학과 석사
2010년 2월~2011년 2월: 한국인터넷진흥원 주임연구원
2011년 3월~현재: 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 스마트그리드 보안, 정보보호, 디지털 포렌식, 네트워크 보안

사 진

서 정 택 (Jung-taek Seo) 종신회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월 ~현재: 한국전자통신연구원 부설연구소 선임연구원/실장
〈관심분야〉 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응