전기차 충전 인프라 보안 사고사례 및 취약점 분석

김태우[1], 송유래[2], 김득훈[3], 곽진[4]
[1]아주대학교 사이버보안학과 석사과정, 정보보호응용및보증연구실
[2]아주대학교 사이버보안학과 석박통합과정, 정보보호응용및보증연구실
[3]아주대학교 소프트웨어융합연구소 박사후연구원
[4]아주대학교 사이버보안학과 교수
twkim.isaa@gmail.com, clara701@ajou.ac.kr, dhkim.isaa@gmail.com, security@ajou.ac.kr

Security Incidents and Vulnerability Analysis of Electric Vehicle Charging Infrastructure

Tae-Woo Kim[1], Yu-Rae Song[2], Deuk-Hun Kim[3], Jin Kwak[4]
[1,2]ISAA Lab., Dept. of Cyber Security, Ajou University
[3]Inst. for Computing and Informatics Research, Ajou University
[4]Dept. of Cyber Security, Ajou University

요 약

전기차 충전 인프라는 기존 내연 기관의 충전 인프라와 달리 차량과 충전소 간의 실시간 네트워크 연결을 기반으로 구성된다. 이를 통해 사용자 편의성이 향상되었으나, 네트워크 연결을 악용한 해킹, 데이터 탈취, 시스템 조작 등으로 인해 보안 위협 또한 증가하고 있다. 실제로 전기차 충전 인프라를 대상으로 한 다양한 보안 사고가 보고되고 있으며, 이는 시스템의 안전성과 신뢰성 확보에 대한 문제로 제기되고 있다. 이러한 문제를 해결하기 위해 발생 빈도가 높은 주요 취약점을 중심으로 그 원인을 분석하고, 이를 통해 향후 보안 사고를 예방하고 피해를 최소화할 수 있는 대응 방안 도출이 필요하다. 이에 따라, 본 논문에서는 전기차 충전 인프라에서 발생한 보안 사고사례와 취약점의 발생 구조 및 원인을 분석하고자 한다.

1. 서론

전기차 시장은 지속적으로 성장하고 있으며, 전기차는 일상에서 점차 보편화되고 있다. 에너지 전문 시장조사 업체인 S사의 보고서에 따르면, 전기차 충전 인프라 시장은 2018년부터 2024년까지 연평균 32%의 성장률을 보이며, 2025년부터 2027년까지 연평균 약 20%의 성장세가 이어질 것으로 예측된다[1].

한편, V사의 보고서에 따르면 충전 인프라의 확산과 함께 보안 취약점 관련 보고 건수는 2019년 266건에서 2024년 413건으로, 보안 사고는 같은 기간 52건에서 150건으로 증가하였다. 랜섬웨어, 데이터 유출, 시스템 중단 등으로 인한 경제적 손실은 2021년 약 13억 8천만 달러에서 2023년 127억 달러로 약 10배 증가하였으며, 2024년 3분기까지의 피해 규모는 16억 3천만 달러로 집계되었다[2]. Hamdare 등은 사회 기반 시설의 전산 시스템 마비, 국가 전력망 손상, 충전 과정에서의 전압 및 속도 조작에 따른 폭발·화재 등 물리적 피해와 인명 피해 가능성까지 포함하여 다양한 위협 요소를 제시하였다[3]. 이와 같은 사례는 보안 취약점이 지속해서 발생하고 있으며 그에 따른 피해 규모 또한 증가 추세에 있음을 나타낸다. 따라서, 본 논문은 전기차 충전 인프라 대상의 잠재 보안 위협에 대응하고 피해를 최소화하기 위해 관련 사례와 유형별 취약점을 분석한다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서 전기차 충전 인프라의 유형별 취약점을 설명하고, 이어지는 3장에서 보안 사고사례와 발생할 수 있는 취약점을 분석한 뒤, 4장에서 결론을 맺는다.

2. 관련 연구

전기차 충전소는 충전기, 양방향 통신 모듈, 제어 모듈, 충전 관리 시스템 등으로 구성된다[4]. 이와 같은 구성 요소들은 인터넷 및 전력망과 연계되어

다양한 보안 위협에 노출된다. Ahalawat 등은 충전소의 보안 취약점과 공격 유형을 분석하였으며 이를 소프트웨어, 하드웨어, 물리적, 스마트 미터, 인적 요소의 다섯 가지 범주로 분류하였다[5]. 이 중 스마트 미터는 전력 사용량을 실시간으로 측정하고 데이터를 송·수신하는 장치로, 네트워크 기반의 통신 구조를 갖는다. <표 1>은 각 보안 취약점 유형을 세부 항목으로 구분하고, 이에 대한 설명을 정리한 것이다.

<표 1> 취약점 유형 및 세부 위협

취약점 유형	세부 취약점	설명
소프트웨어	인증 시스템 미흡	사용자의 고유 카드를 모방해 충전 서비스에 무단 접근
	서버 측 요청 위조	서버 파일 접근 또는 트래픽 우회를 통한 DoS(Denial of Service) 유발
	악성 코드 확산	악성 코드 주입을 통한 기기 감염
하드웨어	충전 커넥터 및 충전기 조작	프로토콜 보안 미적용 시 플러그 변조 가능
물리적 보안	무단 접근 및 하드웨어 조작	하드웨어 접근을 통한 악성 코드 주입 및 개인정보 유출
스마트 미터	스마트 미터 해킹	전력 사용 데이터 변조 및 개인정보 탈취
	전력망 연계 취약점	데이터 시스템 조작을 통한 전력망 교란 및 정전 유발
인적 요소	업데이트 누락	소프트웨어 업데이트 누락으로 알려진 취약점 악용
	소셜 엔지니어링	피싱 및 메시지를 통한 계정 탈취 시도

3. 전기차 충전소 보안 사고사례 및 위협 분석

<표 1>에서 정리한 취약점과 매칭하기 위해, 실제 보안사고 및 보안 업체의 해킹 시연 사례를 기반으로 발생할 수 있는 취약점들을 분석하였다.

3.1 전기차 충전카드 번호 도용 사례

2021년 국내에서 발생한 보안 사고사례 중, 비밀번호 인증 없이 단순히 회원 카드 번호만으로 결제가 이루어진 사례가 보고되었다[6]. 해당 시스템은 카드 번호가 고정된 패턴으로 생성되어 예측할 수 있었으며, 이를 사용자 인증 수단으로 신뢰하여 별도의 검증 절차 없이 결제를 처리하는 구조적 결함이 존재하였다.

이에 따라, 공격자는 임의로 조합한 카드 번호를 입력함으로써 인증 없이 타인의 결제 수단을 사용할 수 있었으며, 결과적으로 타인의 계정을 통한 무단 충전이 가능하였다. 본 사례는 클라이언트 입력값을 신뢰하는 설계 방식이 초래할 수 있는 구조적 취약점을 보여준다.

3.2 충전소 해킹 사례 I

2022년 러시아와 우크라이나 간 갈등 상황에서, 공격 대상의 불안 및 혼란을 조장하는 편향 메시지를 표시하고 충전 기능을 비활성화하는 보안 사고가 보고되었다[7]. 해당 사례에서 우크라이나 제조업체가 납품한 전기차 충전기에 사전 설치된 백도어는 원격 디스플레이 조작, 전원 시스템 비활성화 등 서비스 제공을 방해하였다.

이는 CVE-2017-17106에서 나타난 인증 우회 및 백도어 기반의 권한 획득 방식과 구조적 유사성을 보인다. 해당 취약점은 인증 절차 없이 HTTP(Hypertext Transfer Protocol) 요청만으로 관리자 권한을 얻을 수 있으며, 본 사례 또한 인증 절차 없이 시스템 제어가 가능하다는 점에서 동일한 공격 벡터를 공유한다. 이러한 유형의 공격은 정보 탈취, 악성 코드 주입 및 확산, 하드웨어 손상 등으로 이어진다.

3.3 충전소 해킹 사례 II

2023년 유럽 내 전기차 충전소 운영 시스템이 외부 네트워크로부터 원격 조작된 사례가 보고되었다. 공격자는 원격 제어 도구인 TeamViewer를 이용해 충전소 시스템에 접근하고, 전체 운영 환경의 제어권을 확보하였다[8,9].

인증 절차의 부재와 취약한 인증 구조가 원인이었으며, 공격자는 무단 접근 경로를 통해 네트워크에 침입해 소프트웨어 시스템을 통제하였다. 특히, 서버 측 요청 위조 기법을 활용해 충전소의 동작을 조작할 수 있는 상태로 전환하였다. 이 과정에서 제어 시스템은 인증 절차 없이 접근할 수 있었으며, 사용자 신원 확인 없이

외부 명령을 수용하도록 조작되었다. 공격자는 이 취약 경로를 악용해 시스템을 탈취한 후, 원격 제어 도구를 설치함으로써 전체 시스템에 대한 제어권을 확보하였다. 이를 통해 충전소는 관리자 권한으로 조작될 수 있으며, 전력 공급 중단이나 요금 조작 등의 피해로 이어질 수 있다.

3.4 전기차 큐싱 피해 사례

2023년 유럽 지역의 전기차 충전소를 대상으로 한 큐싱(QR코드 피싱) 피해 사례가 보고되었다[10]. 해당 결제 시스템의 QR코드 접근 시 사용자 인증 절차가 부재하였으며, 스마트 미터 시스템의 인증 구조상 취약점을 악용한 것으로 분석된다.

공격자는 공식 결제 시스템을 모방하여 설계한 악성 페이지로 유도하기 위해 충전소에 부착된 QR코드를 악용하였으며, 신용카드 정보와 개인정보를 탈취하였다. 또한, 무선 신호 방해 기술을 악용하여 사용자의 충전소 전용 애플리케이션 접속을 차단한 후, 조작된 환경에서 악성 QR코드 접속을 유도하였다. 이 과정에서 공격자가 스마트 미터의 취약점을 악용해 사용자 기기에 접근하였고 그 결과 민감 정보가 유출되었다.

3.5 전기차 충전소 해킹 시연

2024년 보안 전문가 Ken Munro는 미국 언론 매체를 통해 전기차 충전소에서 발견된 세 가지 보안 취약점에 관해 설명하였다[11].

먼저 충전 커넥터를 악용한 하드웨어 기반 취약점이다. 충전 커넥터는 배터리 충전뿐만 아니라 데이터 전송 기능도 수행하므로 이를 통해 악성 코드 삽입이나 내부 시스템 접근이 가능하다. 이 과정에서 합법적인 사용자로 위장하여 와이파이 비밀번호 등 민감 정보를 탈취하는 스푸핑(Spoofing) 기법으로 금융 정보가 유출될 수 있으며, 급속 충전 기능을 악용해 전력망에 과부하를 유발하여 대규모 정전 사태를 초래할 수 있다.

다음으로 클라우드 기반 에코시스템의 구조적 취약점이다. 인증 절차가 미흡할 경우, 공격자는 타인의 기기를 무단 제어할 수 있으며, 다수 장치가 연결된 구조적 특성상 업데이트 누락은 전체 시스템에 위협으로 작용한다.

마지막은 설계상 결함으로 인한 취약점이다. 일부 충전기는 외부에서 식별할 수 있는 일련번호를 통해 소프트웨어에 접근이 가능하며, 이를 통해 사용자 계정 탈취 및 충전 기능 차단이 이루어졌다. 또한 원격 연결을 통한 악성 코드 배포로 충전소 네트워크 장악, 전기차 배터리 과부하 유도, 차량 제어 등의 공격도 가능하다.

3.6 보안사고 사례별 분석된 취약점 매칭

<표 2>는 분석한 보안 사고사례와 도출된 취약점을 정리한 결과이다. 분석된 전기차 충전소 관련 보안 사고에서 소프트웨어 계층 취약점이 가장 빈번하게 악용되었으며, 그중 인증 절차의 미비가 주요 원인이었다. 이는 인증 구조의 부재 혹은 설계상의 결함이 실질적인 공격 벡터로 작용했음을 보여준다.

<표 2> 보안사고 사례별 분석된 취약점 매칭

조사된 취약점 유형	세부 취약점	취약점 관련 사례
소프트웨어	인증 시스템 미흡	3.1 / 3.3 / 3.4 / 3.5
	서버 측 요청 위조	3.2 / 3.3
	악성 코드 확산	3.2 / 3.5
하드웨어	충전 커넥터 및 충전기 조작	3.2 / 3.5
물리적 보안	무단 접근 및 하드웨어 조작	3.5
스마트 미터	스마트 미터 해킹	3.4
	전력망 연계 취약점	3.5
인적 요소	업데이트 누락	3.5
	소셜 엔지니어링	3.5

분석된 사례들은 보안 취약점 유형에 따라 분류 가능하며, 그 근거는 다음과 같다. 3.1절 사례는 인증 수단이 부재한 상태에서 사용자 입력값 검증 없이 결제가 처리되도록 설계되어, 인증 체계의 미구현 또는 무력화로 인한 취약점을 나타낸다. 3.2절 사례는 사전 설치된 백도어를 통해 인증 없이 원격 명령이 실행되며, 서버 측 요청 위조 구조를 포함해 악성 코드 확산의 위험을 보인다. 3.3절 사례는 원격 제어 도구가 인증 없이 작동하고 외부 명령을 제한 없이 수용해 구조적 인증 메커니즘이 실패한 사례다. 3.4절 사례는 QR코드 기반 접근 방식에서 사용자 식별이 생략되며, 스마트 미터 내 인증 논리의 취약성을 반영한다. 3.5절 사례는 물리적 조작, 인증 미비, 접근 통제 실패가 복합된

취약점으로, 충전 커넥터 및 하드웨어의 구조의 결함과 연계된다.

4. 결론

전기차 시장 확장과 함께 충전소 인프라도 확대되고 있으나, 새로운 소프트웨어와 하드웨어의 도입으로 다양한 보안 취약점이 드러나고 있어 이에 대한 대응 방안이 확보되어야 한다. 본 연구에서 분석한 보안 사고사례들에 따르면, 전체 취약점의 절반 이상이 소프트웨어와 하드웨어 계층에서 발생하고 있으며, 그중 네트워크 기반 공격이 상대적으로 높은 비중을 차지한다. 그리고 내연기관 차량과 달리 충전과 결제가 동시에 이루어지는 기술인 PnC(Plug and Charge)의 도입은 소프트웨어 기반 보안 위협을 심화시키는 요인으로 작용한다.

향후에는 인증 구조 취약점 대응 방안을 중심으로 연구를 진행할 계획이다.

사사문구

이 연구는 산업통상자원부와 한국산업기술기획평가원의 "자동차산업기술개발(R&D)사업"의 지원을 받아 수행된 연구결과임. (과제번호: RS-2024-00443436)

참고문헌

[1] SNE, "2024년 글로벌 충전 인프라 시장 성장률 32% 전망 (2022 - 2030)", SNE리서치, Aug. 2024. https://www.sneresearch.com/kr/insight/release_view/312.

[2] VicOne, "Automotive cybersecurity snapshot what you need to know", VicOne Auto Cybesecurity, Feb. 2025. https://documents.vicone.com/reports/automotive-cybersecurity-snapshot.pdf.

[3] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D. and Lloret, J., "Cybersecurity risk analysis of electric vehicles charging stations", Sensors, vol. 23, no. 15, pp. 1-23, Jul. 2023.

[4] 권영일, "ASTI market insight 35: 전기자동차 충전소", 한국과학기술정보연구원, Mar. 2022.

[5] Ahalawat, A., Adepu, S. and Gardiner, J., "Security threats in electric vehicle charging", In 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 399-404, Oct. 2022.

[6] 최경민, "분실한 적 없는데…전기차 충전카드 번호 도용당했다", 연합뉴스, Oct. 2021. https://www.yna.co.kr/view/AKR20211026094200505.

[7] Hopkins, B., "A Ukrainian company hacked Russian EV charging stations to protest the invasion", MotorBiscuit, May. 2022. https://www.motorbiscuit.com/a-ukrainian-company-hacked-russian-ev-charging-stations-to-protest-the-invasion.

[8] Michael, A., "Hacked electrify America charger exposes major cybersecurity risk", ScreenRant, Jan. 2023. https://screenrant.com/electrify-america-hacked-charger-cybersecurity-risk.

[9] Steven, L., "Electrify America charging stations vulnerable to hacking", InsideEVs, Jan. 2023. https://insideevs.com/news/642914/electrify-america-charging-station-bugs-easy-hacking.

[10] Muncaster, P., "Quishing attacks are targeting electric car owners", WeLiveSecurity, Oct. 2024. https://www.welivesecurity.com/en/scams/quishing-attacks-targeting-electric-car-owners-slam-on-brakes.

[11] Bragdon, A., "How EV charger hacking threatens personal data and the power grid", The Wall Street Journal, Mar. 2024. https://www.wsj.com/video/series/in-depth-features/how-ev-charger-hacking-threatens-personal-data-and-the-power-grid/FCA59258-C92E-4C51-AE92-B39FE6CFE704.