*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.27, NO.6, Dec. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.6.1441

# 위협모델링을 이용한 전기차 충전 인프라의 보안요구사항에 대한 연구*

차 예 슬†, 김 승 주‡
고려대학교 정보보호대학원

# A Study on Security Requirements of Electric Vehicle Charging Infrastructure Using Threat Modeling*

Ye-Seul Cha,† Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

전기차 충전 인프라에서는 충전 및 결제 데이터를 포함하여 다양한 데이터가 전송되기 때문에 안전한 전기차 충전 인프라를 구축하기 위해서는 이에 대한 보안 연구가 요구된다. 그렇지만 기존에 진행된 연구들은 전기차 충전을 위한 충전 인프라 보다는 전력 계통 인프라와 같은 스마트 그리드 관련 보안 연구가 주를 이루고 있다. 또한 충전 인프라 관련 연구는 아직 부족한 현실이며, 위협모델링과 같은 체계적인 방법론을 이용한 연구는 아직 진행되고 있지 않다. 따라서 안전한 전기차 충전 인프라의 구축을 위해 위협모델링을 적용하여 보안 위협을 식별하고 보안요구사항을 체계적으로 분석하는 것이 필요하다. 본 논문에서는 Data Flow Diagram, STRIDE, Attack Tree를 활용한 위협모델링을 이용하여 충전 인프라에서 발생 가능한 위협을 정확히 식별하고 객관적인 보안요구사항을 도출하여 전기차 충전 인프라를 분석한다.

ABSTRACT

In order to build a secure electric vehicle charging infrastructure, security research is required because various data including charging and payment data are transmitted in the electric vehicle charging infrastructure. However, previous researches have focused on smart grid related security research such as power system infrastructure rather than charging infrastructure for electric vehicle charging. In addition, research on charging infrastructure is still lacking, and research using a systematic methodology such as threat modeling is not yet under way. Therefore, it is necessary to apply threat modeling to identify security threats and systematically analyze security requirements to build a secure electric vehicle charging infrastructure. In this paper, we analyze the electric vehicle charging infrastructure by accurately identifying possible threats and deriving objective security requirements using threat modeling including Data Flow Diagram, STRIDE, and Attack Tree.

**Keywords:** Threat-Modeling, Electric Vehicle Charging Infrastructure, Threat Analysis

Received(11. 08. 2017), Modified(12. 15. 2017), Accepted(12. 15. 2017)

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-17-1001)

† 주저자, yscha@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

## I. 서 론

전 세계적으로 내연기관 차량은 감소하고 전기차는 증가하는 추세를 보이고 있다. 네덜란드와 노르웨이는 2025년부터, 영국과 프랑스는 2040년부터 디젤차 및 휘발류차의 판매를 금지하고, 독일은 2020년까지 100만대의 전기차를 보급할 예정이다. 중국 정부는 '중국제조 2025'이라는 정책의 일환으로 전기차와 하이브리드차를 포함하는 신에너지차 산업을 적극적으로 육성하고 있다. 이러한 국가적 정책과 맞물려 전기차 시대는 더욱 빨리 도래할 것으로 전망된다[1]. 이와 같은 전기차 시장의 성장에 따라 전기차를 충전하기 위한 전기차 충전기 및 충전 인프라 역시 그 수와 규모가 증가할 것으로 예측된다. 전기차 충전 인프라에서는 다양한 데이터가 전송되며 이러한 데이터를 안전하게 보호하기 위한 충전 인프라의 구축을 위해 보안 연구가 요구된다. 하지만 기존의 연구는 전력 계통 인프라와 같은 전력 설비에 초점을 둔 스마트 그리드 관련 보안 연구가 주를 이루고 있다. Oliver Kosut, Liyan Jia 외 2명은 [2]에서 전력 시스템 공격을 통해 미터기를 제어하고 미터기의 측정값을 변경하는 공격 방법을 소개하였으며, Wenye Wang, Zhuo Lu는 [3]에서 스마트 그리드에서의 네트워크 위협을 분류하고 평가하여 적용 가능한 네트워크 및 암호 대응책을 분석하였다. Todd Baumeister은 [4]에서 PCS 및 스마트 미터에 대한 보안 위협, 전력 시스템 상태 측정 관련 공격, 그리고 스마트 그리드 통신 프로토콜의 보안에 대해 연구하였다. 한편, 전기차 충전 인프라에 대한 기존 보안 연구들은 보안 분석을 위한 방법론적 접근이 부족한 현실이다. 따라서 본 논문에서는 위협모델링 기법을 사용하여 전기차 충전 인프라에 대한 위협을 체계적으로 식별 및 분석하고, 추적성과 완전성을 만족하는 보안요구사항을 도출한다.

본 논문은 다음과 같이 구성된다. 2장에서는 전기차 충전 인프라 구성에 대한 설명과 보안위협모델링과 관련된 연구, 기존의 충전 인프라 보안 관련 연구에 대해 소개한다. 3장에서는 위협모델링을 통해 전기차 충전 인프라의 보안 위협을 도출한다. 4장에서는 3장에서 도출한 위협과 대응되는 보안요구사항을 도출하고, 마지막으로 5장에서는 본 논문의 결론을 기술한다.

## II. 관련 연구

### 2.1 전기차 충전 인프라

전기차 충전 인프라는 넓은 범위로 전력 공급 설비, 충전기, 인터페이스, 충전인프라 정보시스템과 같은 구성 요소들을 포함한다. 여기서 전력공급설비란 전력량계, 분전반, 배선, 배선용 차단기 등을 포함한 전기설비로 전원을 공급하기 위한 설비이다. 충전기는 전기차를 충전하는데 사용하는 기기로 220v의 전원을 공급받는 완속 충전기와 380v의 전원을 공급받는 급속 충전기로 구분된다. 인터페이스는 전기자동차와 충전기를 연결해주는 장치이다. 그리고 충전인프라 정보시스템은 충전기를 관리 및 감독하고, 충전자료 DB화 및 각종 통계자료를 제작하고, 충전기 위치 정보 등을 운전자에게 제공하는 역할을 한다[5].

국내 환경부에서는 전기차 충전기와 정보시스템 간 통신에 필요한 표준화된 프로토콜을 제정하였다. 환경부 프로토콜은 충전기와 통신네트워크에 대해 상시 모니터링, 관리가 가능하도록 하며, 충전정보시스템과 충전기 간 통신의 기술적 보편성 및 호환성을 제공한다. 해당 통신 규약은 범용성, 신뢰성을 기본적으로 제공한다. 우선 전기자동차 충전기 제조사와 충전기 종류에 무관하게 수용 가능하도록 하여 범용성을 제공한다. 그리고 전기자동차 충전기의 장애가 발생하거나 데이터가 손실 될 경우에 대처하기 위한 안정적인 통신환경 구축을 위한 통신 규약을 구현하고 전기자동차 충전기 내 모듈간 상호 호환성을 확보하여 신뢰성을 제공한다.

### 2.2 보안위협모델링 관련 연구

#### 2.2.1 보안위협모델링

보안위협모델링에 대한 연구는 1990년대부터 진행되었으며 1999년 Microsoft사의 Jason Garms 등은 내부 문서인 "The threats to out product"에서 자체적으로 사용하는 보안위협모델링의 방법을 정리하여 STRIDE 방법론을 소개하였다[6]. 또한 Michael Howard, James A. Whittaker은 2005년 [7]에서 잠재적인 공격에 대비하여 제품의 위협 환경을 이해하기 위한 방안으로 위협모델링을 이용하는 것에 대해 각 분석 과정별로 구체적으로 소

개하였다. Adam Shostack은 [8]에서 소프트웨어 및 시스템을 개발할 때 발생할 수 있는 잠재적인 위협을 분석하고 해결하기 위해 사용가능한 위협모델링 기법을 소개하고 있으며 위협모델링을 수행하는 구체적인 방법과 기대 효과 등에 대해 설명하였다.

#### 2.2.2 보안위협모델링 활용 연구

IoT 및 CPS가 등장하며 연결에 따른 데이터의 흐름과 노출 위협이 증가함에 따라 보안위협모델링을 활용한 연구가 다양한 시스템 및 제품을 대상으로 진행되고 있다.

Paul Wang, Amjad Ali 외 1명은 [9]에서 스마트 시티 인프라의 보안 문제를 기술 및 비즈니스 운영 관점에서 살펴보고 위협을 분석하고 스마트 도시 시스템의 데이터 보안을 향상시키는 방법을 제안하였다. Data Flow Diagram을 사용하여 시스템의 구조를 파악하였으며 위협을 평가하기 위해 HiSPO algorithm을 활용하였다.

Markus Tasch, Rahamatullah Khondoker 외 2명은 [10]에서 SDN의 보안 응용 프로그램인 OpenFlow-Random Host Mutation과 Resonance을 STRIDE를 사용하여 분석하고 SDN 보안 응용 프로그램을 설계할 때 고려해야 할 일반적인 제안을 도출하였다. 분석 시 Data Flow Digram을 이용하여 시스템을 나타내었고 STRIDE를 통해 위협을 분석하였다. 특히 OCTAVE, Trike와 같은 STRIDE와 유사한 위협 모델링 프레임워크를 소개하며 해당 논문에서는 그 중 STRIDE 분석을 사용한 이유에 대해 구체적으로 소개하고 있다.

Inger Anne Tøndel, Martin Gilje Jaatun 외 1명은 [11]에서 AMI 시스템의 취약점을 분석하기 위해 하나의 실제 AMI 구성에 대한 위협모델링을 수행하였다. Data Flow Diagram을 이용하여 시스템의 데이터 흐름을 파악하고 STRIDE 분석을 사용하여 위협을 식별한 후 식별된 위협을 인터페이스 별로 분류하였다. 그 후 자산과 공격 목표를 고려하여 Attack Tree를 작성하였다.

Anthony Hadding는 [12]에서 위협모델링을 이용하여 임베디드 시스템을 분석하였다. 시스템을 분해하기 위해 Data Flow Diagram을 이용하였고 위협 분석을 위해 Attack Tree를 사용하였다. 그리고 추가적으로 SDL Threat Modeling Tool과 Trike Threat Modeling Tool을 사용하여 분석을 진행하였다.

Goncalo Martins, Sajal Bhatia 외 4명은 [13]에서 CPS(Cyber Physical System)에 대한 위협모델링을 수행하였다. 특히 실제 사례 연구를 위해 무선 철도 온도 모니터링 시스템을 이용하여 제안된 접근법을 검증하였다. 그리고 NIST (National Institute of Standard and Technology) 표준을 사용하여 시스템에서 식별된 위협의 완화 방법을 제안하였다.

Tong Xin, Ban Xiaofang은 [14]에서 온라인 뱅킹의 보안 위협을 효과적으로 평가하기 위해 STRIDE 위협 모델과 위협 트리 분석을 결합한 시스템 위협 분석 방법을 사용하였다. 핵심이 되는 비즈니스 데이터를 분석하여 STRIDE 위협 모델을 구축한 후, 보안위협에 대한 Attack Tree를 계층별로 분해함으로써 온라인 뱅킹 시스템에 대한 상세한 위협 분석을 제공하였다.

### 2.3 전기차 충전 인프라 보안 관련 연구

전기차 충전 인프라의 보안과 관련하여 기존에 몇몇 연구가 진행되었다. Hina Chaudhry, Theodore Bohn은 2012년 [15]에서 플러그인 전기 자동차가 충전 및 통신을 하는 과정에서 발생 가능한 보안 문제들에 대하여 연구를 진행하였다. 전기 자동차를 개인이 집에서 충전하는 시나리오에 대해 각 충전 단계를 행위 주체 별로 정리하였다. 그 후 데이터, 통신 네트워크, 인프라, 펌웨어 및 소프트웨어라는 총 4가지 범위에서 발생 가능한 주요 보안 문제 및 잠재적인 영향력을 분석하고 보안 문제들에 대한 대응책으로써 몇몇 솔루션을 제안하였다. 해당 논문은 충전 과정에서 각 주체별로 행위를 정리하고, 이를 기반으로 보안 문제와 솔루션을 제공하였다는 특징이 있다.

Mustafa A. Mustafa,Ning Zhang 외 2명은 [16]에서 스마트 그리드 환경에서의 전기차 충전 서비스에 대한 포괄적인 보안 분석 연구를 진행하였다. 가정, 직장 및 공공장소와 같이 장소 별로 3가지 전기차 충전 시나리오를 설명하고 해당 유스 케이스 시나리오를 기반으로 애플리케이션 엔티티와 엔티티 간의 상호 작용으로 구성된 스마트 전기차 충전을 위한 일반 모델을 제시하였다. 그리고 해당 모델과 교환되는 메시지를 기반으로 보안 문제 및 엔티티에 부과된

잠재적인 보안위협을 분석하고 보안 및 개인 정보 요구 사항을 제시하였다. 해당 논문은 충전 시나리오를 기반으로 일반화된 전기차 충전 모델을 제시하고, 이 모델을 기반으로 보안위협과 보안요구사항을 분석하였다는 특징이 있다.

강성구, 서정택은 [17]에서 안전한 전기차 충전 인프라 구축을 위해 보안위협 및 보안요구사항 분석에 대한 연구를 진행하였다. 해당 논문에서는 전기자동차 충전 인프라 관련 서비스를 충전 서비스, 충전 운영관리 서비스, 기타 부가서비스로 구분하였다. 그리고 각 서비스별 사용사례를 정리하고 객체 및 객체별 관계를 분석하여 논리적 아키텍처를 제시하였다. 그 후 충전 인프라에서 발생 가능한 보안위협들을 식별하고, 보안위협에 대응하는 보안요구사항을 제시하였다. 해당 논문은 사용 사례를 바탕으로 논리적 아키텍처를 제시하고, 아키텍처를 기반으로 보안위협과 보안요구사항을 분석하였다는 특징이 있다.

## III. 전기차 충전 인프라 보안위협모델링

보안위협모델링을 시행할 경우 우선 대상의 범위를 파악하고 대상의 기능 및 데이터 흐름을 파악한 후 보안위협을 식별해야 한다. 본 장에서는 Data Flow Diagram을 이용하여 분석 범위와 구성 요소를 식별한다. 또한 분석 대상에서 발생 가능한 공격들의 리스트인 Attack Library를 수집한다. 그리고 이를 바탕으로 MS사의 STRIDE를 이용하여 위협을 식별한 후 식별한 위협을 바탕으로 Attack Tree를 작성한다.

### 3.1 보안위협모델링 범위 및 구성요소 식별

#### 3.1.1 가정 사항 설정

본 연구에서는 전기차 충전 인프라의 구성 요소 중 데이터가 전송되는 충전기와 충전인프라 정보시스템 간의 구간을 집중적으로 분석하며 추가적으로 결제가 이루어지는 결제 시스템과의 구간을 포함하였다. 이와 같이 분석되는 구간은 Fig. 1.과 같은 형태를 가지고 있다. 분석 대상은 환경부 산하 한국환경공단의 전기차 충전 인프라로 설정하였으며, 분석 가정 사항으로는 충전기 운영 및 관리, 결제와 관련된 서비스를 주요 분석 대상으로 하였다.

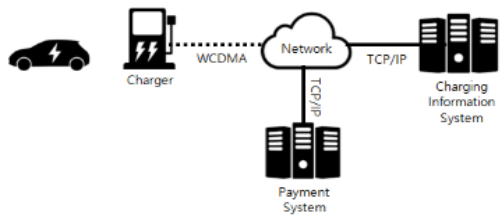


Fig. 1. Electric Vehicle Charging Infrastructure Analysis Section

#### 3.1.2 DFD(Data Flow Diagram) 작성

전기차 충전 인프라의 분석 범위와 구성 요소를 식별하기 위해 DFD를 이용하였다. DFD를 이용하면 분석 대상의 구성요소와 데이터 흐름을 추상적으로 파악할 수 있다. DFD를 작성 시 총 5가지 요소를 활용하는데, 각 요소는 다음 Table 1.과 같다.

DFD는 분석 대상을 포괄적인 형태로부터 구체화하는 정도에 따라 레벨을 구분하여 작성 가능하다. Level 0는 가장 포괄적인 형태로 분석 대상을 나타내며 Level 1, Level 2와 같이 데이터를 분할함에 따라 레벨의 숫자가 증가한다. DFD 작성을 위해 Microsoft사에서 공개 소프트웨어로 배포한 Microsoft Threat Modeling Tool 2016을 사용

Table 1. Five Elements of DFD

| Element | Symbol | Description |
|---|---|---|
| External Entity |  | People or code outside your control |
| Process |  | Any running code |
| Data Store |  | Things that store data |
| Data Flow |  | Communication between processes, or between process and data stores |
| Trust Boundary |  | Anyplace where various principles come together |

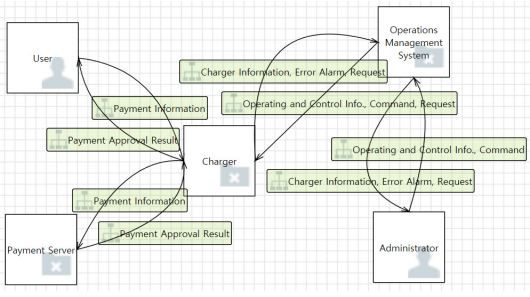


Fig. 2. Level 0 DFD

하였다[18]. Fig. 2.는 Level 0 DFD로써 전기차 충전 인프라를 하나의 프로세스로 보고 포괄적으로 그린 것이다.

Fig. 3.은 Level 1 DFD로써 Level 0 DFD를 분할하여 보다 상세하게 구성 요소 및 데이터 프로세스를 기술하고 있으며, Fig. 4.는 Level 2 DFD로 해당 DFD를 통해 2개의 External Entity와 15개의 Process, 그리고 6개의 Data Store와 36개의 Data Flow를 도출하였다. Table 2.에서는 Level 2 DFD의 각 Element에 대해 설명한다.

### 3.2 Attack Library 수집

Attack Library는 분석 대상에서 발생 가능한

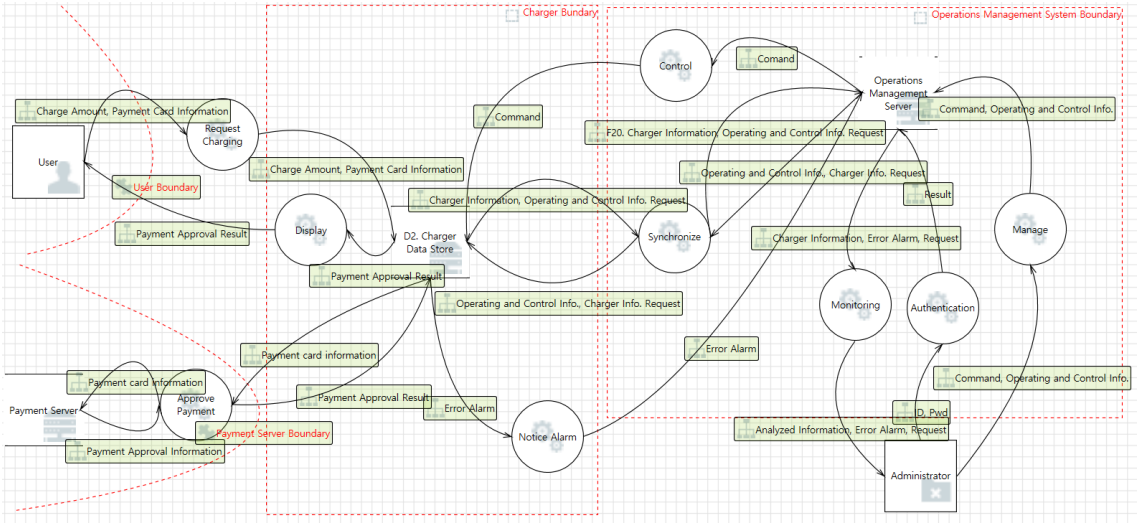


Fig. 3. Level 1 DFD

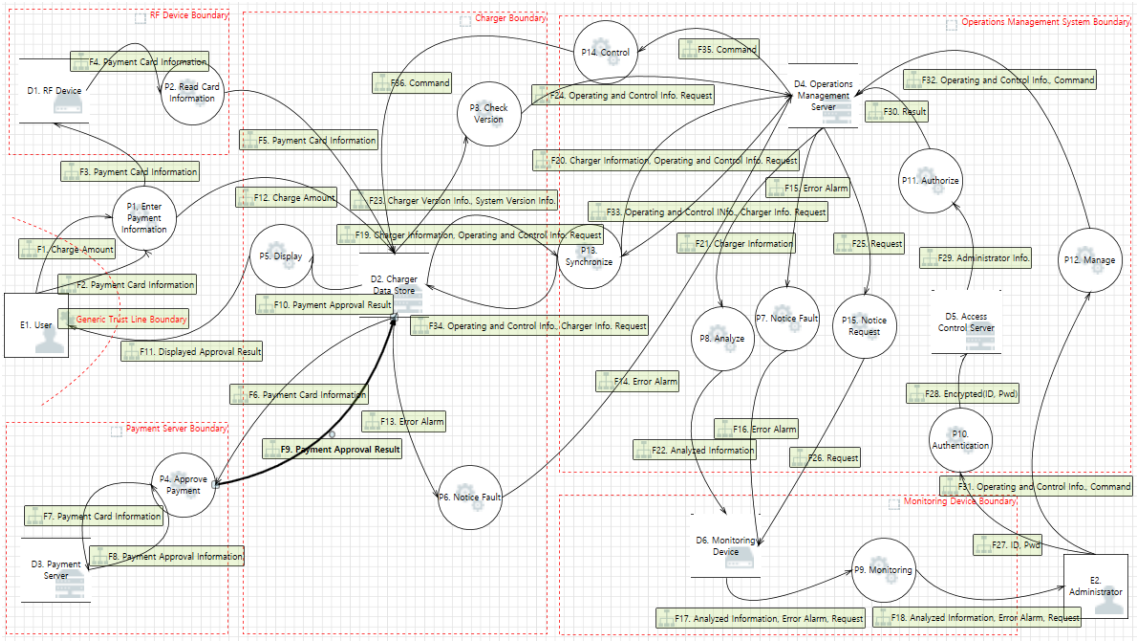


Fig. 4. Level 2 DFD

Table 2. Level 2 DFD Element Description

| Element Type | No | Name | Description |
|---|---|---|---|
| Entity | E1 | User | User who can charge the EV |
| Entity | E2 | Administrator | Administrator who can manage charger |
| Process | P1 | Enter Payment Information | A process that tags payment card and chooses charge amount for payment |
| Process | P2 | Read Card Information | A process that reads and sends payment card information to charge data store. |
| Process | P3 | Check Version | A process that checks the version info. of charger and system |
| Process | P4 | Approve Payment | A process that approves payment |
| Process | P5 | Display | A process that displays payment approval result |
| Process | P6<br>P7 | Notice Fault | A process that notices error alarm to administrator |
| Process | P8 | Analyze | A process that analyzes charger information |
| Process | P9 | Monitoring | A process that shows processed information to administrator |
| Process | P10 | Authenticate | A process that authenticates administrator |
| Process | P11 | Authorize | A process that authorizes administrator and grants access |
| Process | P12 | Manage | A process that manages charger by updating operating and control information and sending command |
| Process | P13 | Synchronize | A process that synchronizes data such as charger information, operating and control system |
| Process | P14 | Control | A process that sends control signal to control charger |
| Process | P15 | Notice Request | A process that notices request from charger |
| Data Store | D1 | RF Device | A data store for information such as payment card information |
| Data Store | D2 | Charger Data Store | A data store for information such as charger information, operating and control information, and etc |
| Data Store | D3 | Payment Server | A data store for payment card information |
| Data Store | D4 | Operations Management Server | A data store for information such as charger information, operating and control information, and etc |
| Data Store | D5 | Access Control Server | A data store for administrator info. |
| Data Store | D6 | Monitoring Device | A data store for analyzed charger information, error alarm, and request |
| Flow | F1 | Charge Amount | Amount of charge the user wants to charge |
| Flow | F2<br>F3<br>F4<br>F5<br>F6<br>F7 | Payment Card Information | Information on payment cards needed to make a payment |
| Flow | F8 | Payment Approval Information | Information indicating whether the payment has been approved |
| Flow | F9<br>F10 | Payment Approval Result | Information about payment authorization result |
| Flow | F11 | Displayed Approval Result | Payment approval result information shown to users |
| Flow | F12 | Charge Amount | Amount of charge the user wants to charge |
| Flow | F13<br>F14<br>F15<br>F16 | Error Alarm | Alarm notifying occurrence of fault event |
| Flow | F17<br>F18 | Analyzed Information, Error Alarm, Request | Information that analyzed charge information, Alarm notifying occurrence of fault event, Request for operating and control info. |
| Flow | F19<br>F20 | Charger Information, Operating and Control Info. Request | Charger information such as charger status, charger mode, charger power usage, charger log, charge progress status, Request for operating and control info. |
| Flow | F21 | Charger Information | Charger information such as charger status, charger mode, charger power usage, charger log, charge progress status |
| Flow | F22 | Analyzed Information | Information that analyzed charge information |
| Flow | F23 | Charger Version Info., System Version Info. | Version information of charger, Version information of operations management system |
| Flow | F24 | Operating and Control Info. Request | Request for operating and control info. |

| Element Type | No | Name | Description |
|---|---|---|---|
| Flow | F25<br>F26 | Request | Request for operating and control info. |
| Flow | F27 | ID, Pwd | Administrator Id and password to approve administrator |
| Flow | F28 | Encrypted(ID, Pwd) | Encrypted administrator Id and password to approve administrator |
| Flow | F29 | Administrator Info. | Stored administrator Id and password to approve administrator |
| Flow | F30 | Result | Administrator certification result |
| Flow | F31<br>F32 | Operating and Control Info., Command | Operating and control information for the charger, such as version information, unit price information, and program, Charger control command to change charger mode |
| Flow | F33<br>F34 | Operating and Control Info., Charger Info. Request | Operating and control information for the charger, such as version information, unit price information, and program, Request for charger info. |
| Flow | F35<br>F36 | Command | Charger control command to change charger mode |

공격들의 리스트로 본 논문에서는 Attack Library 작성을 위해 전기차 충전 인프라, RF System, Embedded System, Smart Grid와 관련된 신뢰할 수 있는 기관 혹은 저자의 기술 보고서, 논문, 표준, 컨퍼런스 발표, 공신력 있는 약점, 취약점 데이터베이스를 수집하였다. Table 3.에서는 전기차 충전 인프라의 Attack Library를 보여준다.

### 3.3 STRIDE를 이용한 분석

STRIDE는 Microsoft사에서 개발한 보안위협모델링 방법으로 인증, 무결성, 부인 방지, 기밀성, 가용성, 권한 부여와 같은 보안 속성을 고려하여 DFD의 각 요소에 존재하는 위협을 식별한다. STRIDE는 Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege와 같은 위협 용어의 영어 약자를 사용한다. STRIDE를 활용하면 위협 분석 시 분석자의 역량에 따른 영향을 최소화 할 수 있으며, 분석 대상의 전 범위에 대해 누락 없이 분석이 가능하다.

DFD의 각 요소별로 STRIDE에 적용 가능한 항목

Table 3. Attack Library

| Category | Title | Author | Type | Ref |
|---|---|---|---|---|
| Paper | RFID and its vulnerability to faults | Michael Hutter | Hardware | [19] |
| Paper | RFID Security Threats and Basic Solutions | A. Khattab | Hardware/Network | [20] |
| Paper | When Firmware Modifications Attack: A Case Study of Embedded Exploitation | Ang Cui | Firmware | [21] |
| Paper | Embedded Systems Security_Threats, Vulnerabilities, and Attack Taxonomy | Dorottya Papp | System/Network | [22] |
| Paper | Security Concerns of a Plug-In Vehicle | Hina Chaudhry | All | [15] |
| Paper | Smart Electric Vehicle Charging: Security Analysis | Mustafa A. Mustafa | All | [16] |
| Paper | An Analysis of the Security Threats and Security Requirements for Electric Vehicle Charging Infrastructure | S. G. Kang | All | [17] |
| Paper | Cyber security in the Smart Grid: Survey and challenges | Wenye Wang | Network | [3] |
| Paper | Malicious Data Attacks on the Smart Grid | Oliver Kosut | Hardware/Network | [2] |
| Paper | Security & Vulnerability in Electric Power Systems | David Watts | System/Network | [23] |
| Paper | Research for Vulnerability Detection of Embedded System Firmware | Jin-bingHou | Firmware | [24] |
| Report | A study of open port as security vulnerability in common user computer | Kuruvilla Mathew | Network | [25] |
| White paper | RFID Security and Privacy White Paper | Smart Border Alliance | Hardware/Network | [26] |
| Book | Security in RFID and Sensor Networks(Attacking RFID Systems) | Pedro Peris-Lopez | Network | [27] |
| Report | Technical Trends of DDoS Attacks and Defense in Cellular Network | S. W. Yi | Network | [28] |
| Conference | New Attacks against RFID-Systems | Lukas Grunwald | Network | [29] |
| Conference | TCP Injection attacks in the wild | Gabi Nakibly | Network | [30] |
| Conference | Vulnerabilities in Not-So-Embedded Systems | Brendan O'Connor | System/Hardware | [31] |

| Category | Title | Author | Type | Ref |
|---|---|---|---|---|
| Report | Hacking Embedded Devices | Phorkus | All | [32] |
| Report | Exploiting Embedded Devices | SANS Institute | All | [33] |
| Report | EV Charging Systems Security Requirements | ElaadNL | All | [34] |
| Report | The Infosec Risks of Charging Electric Cars | Ofer Shezaf | All | [35] |
| Report | Cyber-security of PEVs | Nihan Karali | All | [36] |
| Report | Smart Grid Cyber Security Potential Threats Vulnerabilities and Risks | Isaac Ghansah | All | [37] |
| CVE | CVE-2015-6839 | | Network | [38] |
| CVE | CVE-2016-4484 | | System | [38] |
| CVE | CVE-2013-2094 | | System | [38] |

에 차이가 있으며 Table 4.에서는 요소 별 적용 가능한 STRIDE 항목을 나타낸다.

해당 표에서는 STRIDE에 적용 가능한 DFD 요소에 따라 'X' 표시를 해두었다. 예를 들어 External Entity에서는 Spoofing, Repudiation, Denial of Service의 위협이 가능한 경우이다. DFD 요소 별 STRIDE 적용 항목은 STRIDE가 실현 불가능 할 경우 제외될 수 있지만 항목이 늘어날 수는 없다. 예외적으로 Data Store의 경우 로그가 남는 경우 Repudiation이 가능하기 때문에 상황에 따라 해당 항목을 적용할 수 있어 표에서 '?'로 표기한다.

Table 5.에서는 STRIDE를 이용하여 전기차 충전 인프라 Level 2 DFD에서의 위협을 식별한 결과를 보여준다. STRIDE를 이용하여 위협을 식별한 결과 총 142개의 보안위협이 식별되었다.

Table 4. DFD Elements per STRIDE

| | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| **External Entity** | x | | x | | x | |
| **Process** | x | x | x | x | x | x |
| **Data Store** | | x | ? | x | x | |
| **Data Flow** | | x | | x | x | |

Table 5. STRIDE

| Element Type | No | Name | STRIDE | Description | Threat No. |
|---|---|---|---|---|---|
| Entity | E1 | User | S | Attacker can spoof user and receive the displayed approval result | T1 |
| Entity | E1 | User | S | Attacker can spoof user and enter charge amount | T2 |
| Entity | E1 | User | S | Attacker can spoof user and enter payment card information | T3 |
| Entity | E1 | User | R | User repudiates that he/she did not receive displayed approval result | T4 |
| Entity | E2 | Administrator | S | Attacker can spoof administrator and do the authenticate process | T5 |
| Entity | E2 | Administrator | S | Attacker can spoof administrator and do the manage process | T6 |
| Entity | E2 | Administrator | S | Attacker can spoof administrator and receive analyzed information, error alarm, and request | T7 |
| Entity | E2 | Administrator | R | Administrator repudiate that he/she did not receive analyzed information, error alarm, and request | T8 |
| Process | P1 | Enter Payment Information | S | Attacker pretends to have normal charge amount and tries to access to charger | T9 |
| Process | P1 | Enter Payment Information | S | Attacker pretends to have normal payment card information and tries to access to RF device | T10 |
| Process | P1 | Enter Payment Information | R | Enter payment information process repudiates that it did not receive charge amount | T11 |
| Process | P1 | Enter Payment Information | R | Enter payment information process repudiates that it did not receive payment card information | T12 |
| Process | P1 | Enter Payment Information | I | Attacker learns payment card information | T13 |
| Process | P1 | Enter Payment Information | I | Attacker learns charge amount | T14 |
| Process | P1 | Enter Payment Information | D | Process cannot enter charge amount to charger | T15 |
| Process | P1 | Enter Payment Information | D | Process cannot enter payment card information to RF devide | T16 |
| Process | P1 | Enter Payment Information | E | Attacker passes data to change the flow of program execution | T17 |
| Process | P1 | Enter Payment Information | E | Elevation of privilege using remote code execution to enter payment card information | T18 |
| Process | P1 | Enter Payment Information | E | Attacker passes data to change the flow of program execution | T19 |
| Process | P1 | Enter Payment Information | E | Elevation of privilege using remote code execution to enter charge amount | T20 |
| Process | P2 | Read Card Information | S | Attacker pretends to have normal payment card information and tries to access to charger | T21 |
| Process | P2 | Read Card Information | T | Read card information process can be tampered by spoofed data storage | T22 |

| Element Type | No | Name | STRIDE | Description | Threat No. |
|---|---|---|---|---|---|
| Process | P2 | Read Card Information | D | Excessive resource consumption for the read card information process | T23 |
| Process | P3 | Check Version | T | Check version process can be tampered by spoofed data storage | T24 |
| Process | P3 | Check Version | D | Excessive resource consumption for the check version process | T25 |
| Process | P4 | Approve Payment | S | Attacker pretends to have normal payment approval result and tries to access to charger | T26 |
| Process | P4 | Approve Payment | T | Approve payment process can be tampered by spoofed data storage | T27 |
| Process | P4 | Approve Payment | R | Approve payment process repudiates that it did not receive payment card information | T28 |
| Process | P4 | Approve Payment | D | Excessive resource consumption for the approve payment process | T29 |
| Process | P4 | Approve Payment | D | Process cannot send payment approval result to charger | T30 |
| Process | P4 | Approve Payment | E | Attacker passes data to change the flow of program execution | T31 |
| Process | P4 | Approve Payment | E | Elevation of privilege using remote code execution to receive payment card information | T32 |
| Process | P4 | Approve Payment | E | Elevation of privilege using remote code execution to approve payment | T33 |
| Process | P5 | Display | T | Display process can be tampered by spoofed data storage | T34 |
| Process | P6 | Notice fault | S | Attacker pretends to have normal error alarm and tries to access to operations management server | T35 |
| Process | P6 | Notice fault | T | Notice fault process can be tampered by spoofed data storage | T36 |
| Process | P6 | Notice fault | D | Excessive resource consumption for the notice fault process | T37 |
| Process | P7 | Notice fault | S | Attacker pretends to have normal error alarm and tries to access to monitoring device | T38 |
| Process | P7 | Notice fault | T | Notice fault process can be tampered by spoofed data storage | T39 |
| Process | P7 | Notice fault | D | Excessive resource consumption for the notice fault process | T40 |
| Process | P8 | Analyze | S | Attacker pretends to have normal analyzed information and tries to access to monitoring device | T41 |
| Process | P8 | Analyze | T | Analyze process can be tampered by spoofed data storage | T42 |
| Process | P8 | Analyze | D | Excessive resource consumption for the analyze process | T43 |
| Process | P9 | Monitoring | T | Monitoring information process can be tampered by spoofed data storage | T44 |
| Middle omission | | | | | |
| Flow | F22 | Analyzed Information | T | Analyzed information (from / sent from)may be tampered | T122 |
| Flow | F22 | Analyzed Information | I | Analyzed information (from/ sent from)may be sniffed by an attacker | T123 |
| Flow | F22 | Analyzed Information | D | Interrupt analyzed information data flow so that it cannot be sent to the destination | T124 |
| Flow | F24 | Operating and Control Info. Request | T | Operating and Control Info. Request may be tampered | T125 |
| Flow | F24 | Operating and Control Info. Request | I | Operating and Control Info. Request may be sniffed by an attacker | T126 |
| Flow | F24 | Operating and Control Info. Request | D | Interrupt Operating and Control Info. Request data flow so that it cannot be sent to the destination | T127 |
| Flow | F26 | Request | T | Request sent from operations management server may be tampered | T128 |
| Flow | F26 | Request | I | Request sent from operations management server may be sniffed by an attacker | T129 |
| Flow | F26 | Request | D | Interrupt request data flow so that it cannot be sent to the destination | T130 |
| Flow | F27 | ID, Pwd | T | ID, Pwd sent from administrator may be tampered | T131 |
| Flow | F27 | ID, Pwd | I | ID, Pwd sent from administrator may be sniffed by an attacker | T132 |
| Flow | F27 | ID, Pwd | D | Interrupt ID, Pwd data flow so that it cannot be sent to the destination | T133 |
| Flow | F31 | Operating and Control Info., Command | T | Operating and Control Info., command may be tampered | T134 |
| Flow | F31 | Operating and Control Info., Command | I | Operating and Control Info., command may be sniffed by an attacker | T135 |
| Flow | F31 | Operating and Control Info., Command | D | Interrupt Operating and Control Info., command data flow so that it cannot be sent to the destination | T136 |
| Flow | F34 | Operating and Control Info., Charger Info., Request | T | Operating and Control Info., Charger Info. Request may be tampered | T137 |
| Flow | F34 | Operating and Control Info., Charger Info., Request | I | Operating and Control Info., Charger Info. Request may be sniffed by an attacker | T138 |
| Flow | F34 | Operating and Control Info., Charger Info., Request | D | Interrupt Operating and Control Info., Charger Info. Request data flow so that it cannot be sent to the destination | T139 |
| Flow | F36 | Command | T | Command sent from operations management server may be tampered | T140 |
| Flow | F36 | Command | I | Command sent from operations management server may be sniffed by an attacker | T141 |
| Flow | F36 | Command | D | Interrupt command data flow so that it cannot be sent to the destination | T142 |

### 3.4 Attack Tree 작성

공격자가 공격 목표를 달성하는 방법과 STRIDE를 통해 식별한 위협과의 연관성을 파악하고 체계화하기 위해 Attack Tree를 작성한다. Attack Tree의 루트 노드는 전기차 충전 인프라에 대한 공격으로 설정하였다. 하위 노드는 충전 인프라의 구성요소인 Charger, Server, RF Device, Monitoring Device로 구성하였다. 최하위 노드에는 STRIDE를 통해 도출한 위협사항들이 연결되며, Figure. 5.에서는 DFD를 바탕으로 작성한 Attack Tree를 보여주고 있다.

## IV. 전기차 충전 인프라 보안요구사항 도출

3장에서 정리한 DFD, Attack Library, STRIDE, Attack Tree를 바탕으로 보안요구사항 도출을 위한 체크리스트를 작성하였다. Attack Tree에서 도출한 공격 목표인 Charger, Server, RF Device, Monitoring Device를 체크리스트의 Bound로 설정하였으며, 각 Attack Tree의 최하위 노드에 정리된 공격 별로 체크리스트를 도출하였

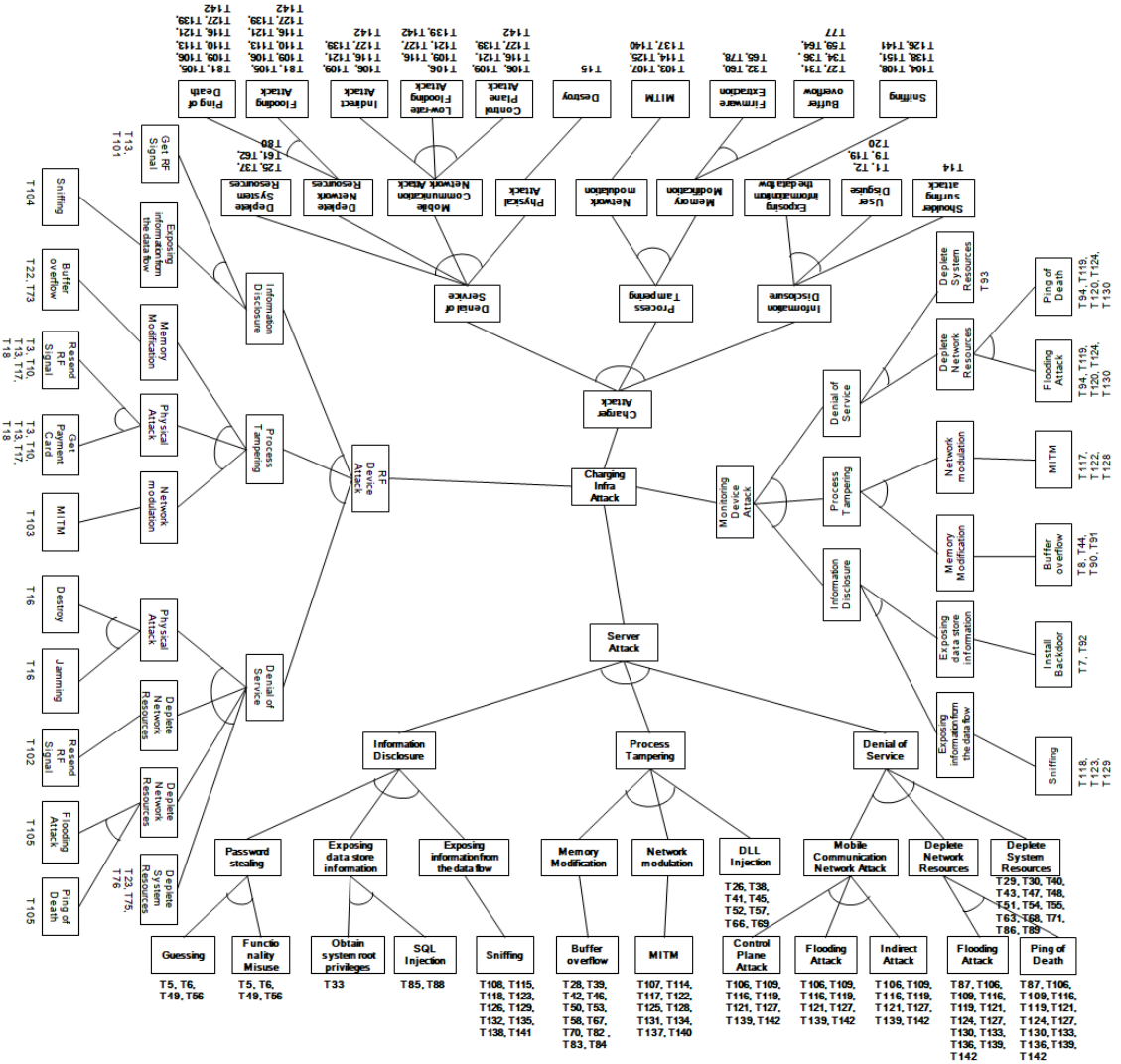


Fig. 5. Attack Tree

Table 6. Check List

| Bound | Attack | Detail | No. |
|---|---|---|---|
| Charger | Buffer overflow | Do not grant execute permission on the pages allocated in the data area | C1 |
| | | Randomize memory address space placement(ASLR) | C2 |
| | Firmware Extraction | Make sure directories and files have access control settings | C3 |
| | MITM | Encrypt sensitive information | C4 |
| | | Enable SSL communication | C5 |
| | | Determine if data manipulation is possible with MITM attacks | C6 |
| | Physical Attack(Destroy) | Check for possible damage to physical access | C7 |
| Server | Guessing | Limit number of login attempts | C8 |
| | | Validate Input Data | C9 |
| | | Set password complexity | C10 |
| | | Set maximum password age | C11 |
| | Functionality Misuse | Restrict use of default ID / PW | C12 |
| | | Uses a secure Pw generation mechanism | C13 |
| | | Change Password periodically | C14 |
| | Obtain system root privileges | Make sure no account has an easy password | C15 |
| | | Change SSH security settings to allow access only from authorized users and allowed IPs | C16 |
| | | Change the port number arbitrarily to avoid random scans for SSH | C17 |
| | | Use iptables firewall to allow access only from allowed IPs, but deny other connections | C18 |
| | SQL Injection | Validate strings used in database query statements | C19 |
| | | Validate user input values and parameters sent to the server | C20 |
| | | Confirm error information exposure on error page | C21 |
| | Buffer overflow | Do not grant execute permission on the pages allocated in the data area | C22 |
| | | Randomize memory address space placement(ASLR) | C23 |
| | | Searches for files with SetUID specified and removes the authority portion of unnecessary binaries | C24 |
| | MITM | Encrypt sensitive information | C25 |
| | | Determine if data manipulation is possible with MITM attacks | C26 |
| RF Device | Buffer overflow | Do not grant execute permission on the pages allocated in the data area | C27 |
| | | Randomize memory address space placement(ASLR) | C28 |
| | MITM | Encrypt sensitive information | C29 |
| | | Enable SSL communication | C30 |
| | | Determine if data manipulation is possible with MITM attacks | C31 |
| | Physical Attack(Destroy) | Check for possible damage to physical access | C32 |
| Monitoring Device | Install Backdoor | Identify active processes and open ports | C33 |
| | | Use virus and backdoor detection tools | C34 |
| | | Analyze logs on a regular basis | C35 |
| | | Eliminate unnecessary services such as Telnet | C36 |
| | Buffer overflow | Do not grant execute permission on the pages allocated in the data area | C37 |
| | | Randomize memory address space placement(ASLR) | C38 |
| | | Searches for files with SetUID specified and removes the authority portion of unnecessary binaries | C39 |
| | MITM | Encrypt sensitive information | C40 |
| | | Enable SSL communication | C41 |
| | | Determine if data manipulation is possible with MITM attacks | C42 |
| EVSE • Server • RF Device • Monitoring Device Communication | Sniffing | Inspect open ports | C43 |
| | | Restrict unnecessary port usage | C44 |
| | | Enable SSL communication | C45 |
| | | Using the tool to detect sniffer (ARPwatch / Sentinel tool) | C46 |
| | | Verify that sensitive information is encrypted and sent | C47 |
| | Mobile Communication Network Attack | Check whether GTP traffic is analyzed for GN section | C48 |
| | | Check for abnormal traffic detection | C49 |
| | | Use of dedicated GUI for system control, monitoring, and detection / blocking logs | C50 |
| | Flooding Attack | Blocks the flow of UDP / ICMP traffic above the threshold by setting the Packet Per Second (PPS) value lower than the incoming value | C51 |
| | | Blocking by phasing the PPS threshold for SYN requests per firewall IP | C52 |
| | | Drop the first SYN to check whether the re-request packet arrives (check whether it is spoofing) | C53 |
| | | Confirm error handling when excessive communication history is transmitted | C54 |
| | Ping of Death | Check sum of Fragment Offset value of packet | C55 |
| | | Confirm error handling when excessive communication history is transmitted | C56 |
| | Deplete System Resources | Check if firewall is built | C57 |
| | Resend RF Signal | Limit acquisition of information through RF signals | C58 |
| | | Enable RF signal encryption | C59 |

다. 도출해낸 총 46개의 최하의 노드 공격 중에서 사회공학기법이 적용된 공격이나 추상적이고 적용이 불가한 공격들은 체크리스트에서 제외하였다.

Table 6.은 도출된 체크리스트를 보여주며 총 59개의 점검 항목이 도출되었다. 도출한 체크리스트 항목들은 위협모델링 기법을 적용하여 분석대상 범위를 체계적으로 분석하여 도출하였기 때문에 전기차 충전 인프라의 분석 범위 전체를 다룰 수 있다. 또한 해당 체크리스트가 Attack Tree 분석을 통해 도출한 공격을 모두 포함하고 있다는 것을 보여주기 위해 점검 항목 별로 대응하는 공격 항목을 작성하였다.

## V. 결 론

기존 전기차 충전 인프라의 보안과 관련한 몇몇 연구들은 전기차 충전 시나리오를 작성하여 일반화된 모델 혹은 논리적 아키텍처를 제시하고, 해당 내용을 기반으로 보안위협과 보안요구사항을 도출하였다. 그렇지만 위협모델링과 같은 체계적인 방법론을 적용하여 충전 인프라에서 발생 가능한 보안위협을 분석하고 보안요구사항을 도출한 연구는 거의 이루어지지 않았다.

본 논문에서는 보안위협모델링을 적용하여 분석 범위의 완전성 및 내용의 추적성을 만족하도록 분석을 수행하였다. 분석 대상을 국내 환경부 산하 한국환경공단의 전기차 충전 인프라로 선정하고 정확한 분석을 위해 한국환경공단의 전기자동차 충전기 통신 규약 문서 및 특허 문서를 참고하여 Data Flow Diagram을 작성하였다. Attack Library는 신뢰할 수 있는 기관 혹은 저자의 기술보고서, 논문, 표준, 취약점 데이터베이스를 참고하여 작성하였다. 그리고 Microsoft사에서 공개 소프트웨어로 제공하는 Microsoft Threat Modeling Tool 2016을 이용하여 STRIDE 분석을 수행하고 보안위협을 식별하였으며 위와 같은 내용을 근간으로 Attack Tree 및 체크리스트를 도출하였다. 해당 체크리스트는 Attack Library 활용에 따라 현존하는 공격사항들을 포함하고 있기에 전기차 충전 인프라 분석 범위 전체에 대한 분석에 사용이 가능하다.

추후 전기차 충전 인프라를 구축하는 인프라 사업자들은 인프라 구축 시 본 논문에서의 보안요구사항과 체크리스트를 참고할 수 있을 것이다. 하지만 본 논문에서는 분석의 범위를 일부 제한하였기에 모든 Use-case와 충전 인프라 관련 서비스에 대해 다루지 못하고 있다. 따라서 추후 분석의 범위를 넓혀서 보안위협 및 보안요구사항을 도출해야하는 향후 과제가 남아있다.

## References


[1] Kyunghyang Opinion, "In the era of internal combustion engine," http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201709201405001&code=990100#csidx818d94bbcfed09083b6ff17698090df

[2] Oliver Kosut, Liyan Jia, Robert J. Thomas, and Lang Tong, "Malicious data attacks on the smart grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645-658, Dec. 2011

[3] Wenye Wang and Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp. 1344-1371, Apr. 2013

[4] Todd Baumeister, "Literature review on smart grid cyber security," Collaborative Software Development Laboratory at the University of Hawaii, Dec. 2010

[5] Korea Environment Corporation, EV Charging Information System, http://www.ev.or.kr/web/link/?pMENUMST_ID=21460

[6] Adam Shostack, "Experiences Threat Modeling at Microsoft," Microsoft, 2008

[7] P, Torr, "Demystifying the threat modeling process," IEEE Security & Privacy, vol. 3, no. 5, pp. 66-70, Oct. 2005

[8] Adam Shostack, Threat Modeling: Designing for Security, John Wiley & Sons, Feb. 2014

[9] Paul Wang, Amjad Ali, and William Kelly, "Data security and threat modeling for smart city infrastructure," 2015 International Conference on

Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE, 2015
〔10〕 Markus Tasch, Rahamatullah Khondoker, Ronald Marx, and Kpatcha Bayarou, "Security analysis of security applications for software defined networks," Proceedings of the AINTEC 2014 on Asian Internet Engineering Conference, ACM, 2014
〔11〕 Tøndel, Inger Anne, Martin Gilje Jaatun, and Maria Bartnes Line, "Threat modeling of AMI," International Workshop on Critical Information Infrastructures Security. Springer, Berlin, Heidelberg, 2012
〔12〕 Anthony Hadding and Dr. J. Zalewski, "Threat Modeling in Embedded Systems," Florida Gulf Coast University, 2012
〔13〕 Goncalo Martins, Sajal Bhatia, Xenofon Koutsoukos, Keith Stouffer, Cheeyee Tang, and Richard Candell, "Towards a systematic threat modeling approach for cyber-physical systems," Resilience Week (RWS), IEEE, 2015
〔14〕 Tong Xin and Ban Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model," International Journal of Security and Its Applications, vol. 8, no. 2, pp. 271-282, 2014
〔15〕 Hina Chaudhry and Theodore Bohn, "Security concerns of a plug-in vehicle," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), IEEE, 2012
〔16〕 Mustafa, Mustafa A., Ning Zhang, Georgios Kalogridis, and Zhong Fan, "Smart electric vehicle charging: Security analysis," Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, IEEE, 2013
〔17〕 Seong-ku Kang and Jung-taek Seo, "An Analysis of the Security Threats and Security Requirements for Electric Vehicle Charging Infrastructure," Journal of The Korea Institute of Information Security and Cryptology, 22(5), pp. 1027-1037, Oct. 2012
〔18〕 Microsoft, Microsoft Threat Modeling Tool 2016, https://www.microsoft.com/en-us/download/details.aspx?id=49168
〔19〕 Michael Hutter, Jorn-Marc Schmidt, and Thomas Plos, "RFID and its vulnerability to faults," Lecture Notes in Computer Science 5154, pp. 363-379, 2008
〔20〕 Ahmed Khattab, Zahra Jeddi, Esmaeil Amini, and Magdy Bayoumi, "RFID Security Threats and Basic Solutions," RFID Security, Springer International Publishing, pp. 27-41, 2017
〔21〕 Ang Cui, Michael Costello, and Salvatore J. Stolfo, "When Firmware Modifications Attaack: A Case Study of Embedded Exploitation," NDSS. 2013
〔22〕 Dorottya Papp, Zhendong Ma, and Levente Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," 2015 13th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2015
〔23〕 David Watts, "Security and vulnerability in electric power systems," 35th North American power symposium, vol. 2, pp. 559-566, Oct. 2003
〔24〕 Jin-bing Hou, Tong Li, and Cheng Chang, "Research for Vulnerability Detection of Embedded System Firmware," Procedia Computer Science 107, pp. 814-818, 2017
〔25〕 Mathew, Kuruvilla, Mujahid Tabassum, and Marlene Valerie Lu Ai Siok, "A study of open ports as security vulnerabilities in common user computers," 2014 International Confe-

rence on Computational Science and Technology (ICCST), IEEE, 2014
〔26〕 Smart Border Alliance, "RFID Security and Privacy White Paper," https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf
〔27〕 Yan Zhang and Paris Kitsos, Security in RFID and Sensor Networks, CRC Press, Apr. 2009
〔28〕 S.W. Yi, J.H. Kim, and D.I. Seo, "Technical Trends of DDos Attacks and Defense in Cellular Network," ETRI Electronics and telecommunications trend, 26(6), Dec. 2011
〔29〕 Lukas Grunwald, "New attacks against RFID-systems," BlackHat USA, USA, 2006
〔30〕 Gabi Nakibly, "TCP Injection attacks in the wild," BlackHat USA, USA, 2016
〔31〕 Brendan O'Connor, "Vulnerabilities in Not-So-Embedded Systems," BlackHat USA, USA, 2006
〔32〕 Mark Carey(PHORKUS), "Hacking Embedded Devices," DefCon 21, 2013
〔33〕 SANS Institute, "Exploiting Embedded Devices," https://www.sans.org/reading-room/whitepapers/testing/exploiting-embedded-devices-34022
〔34〕 Elaadnl, "EV Charging Systems Security Requirements," https://www.encs.eu/wp-content/uploads/2017/06/Security_Requirements_Charge_Points_v1.0_april2016.pdf
〔35〕 Ofer Shezaf, "Who can hack an plug," https://conference.hitb.org/hitbsecconf2013ams/materials/D2T2%20-%20Ofer%20Shezaf%20-%20The%20Infosec%20Risks%20of%20Charging%20Electric%20Cars.pdf
〔36〕 International Energy Agency, "Vehicle-Grid Integration Cyber-security of PEVs," https://www.iea.org/media/topics/transport/VehicletoGridCybersecurityBrief.pdf
〔37〕 Isaac Ghansah, "Smart grid cyber security potential threats, vulnerabilities and risks," California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047, 2009
〔38〕 Common Vulnerabilities and Exposures, https://cve.mitre.org/index.html

## 〈저자소개〉

차 예 슬 (Ye-Seul Cha) 학생회원
2013년 2월: 이화여자대학교 심리학과 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 IoT 보안, 정보보증, 개인정보 보호

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊 한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년 :국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년 :방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 12월~현재: 카카오 자문위원
2016년 1월~현재: 한국정보화진흥원 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable security