ISSN 1229-800X The Transactions of the Korean Institute of Electrical Engineers Vol. 66P, No. 2, pp. 76~81, 2017
http://doi.org/10.5370/KIEEP.2017.66.2.076

스마트홈 서비스 환경에서의 보안 위험 분석을 위한 위협 모델링 적용 방안

Application of Threat Modeling for Security Risk Analysis in Smart Home Service Environment

이 윤 환† · 박 상 건*
(Yun-Hwan Lee · Sang-Gun Park)

Abstract - In this paper, the risk analysis of smart home services was implemented by applying threat modeling. Identified possible threats for safe deployment of smart home services and identified threats through the STRIDE model. Through the creation of the Attack Tree, the attackable risk was analyzed and the risk was measured by applying the DREAD model. The derived results can be used to protect assets and mitigate risk by preventing security vulnerabilities from compromising and identifying threats from adversely affecting services. In addition, the modeled result of the derived threat can be utilized as a basis for performing the security check of the smart home service.

Key Words : Threat modeling, Smart home service, Smart grid, Security assesment, Risk analysis

1. 서 론

스마트그리드(Smart Grid)는 기존의 전력망에 정보통신기술(ICT)을 접목하여 공급자와 소비자가 양방향으로 실시간 전력정보를 교환하여 에너지 효율을 최적화하는 차세대 전력망 기술이다. 스마트그리드 기술을 활용하면 고품질의 에너지 및 다양한 부가서비스를 제공할 수 있으며, 에너지 기술의 접목·확장이 용이하여 산업간 융·복합을 통한 신규 비즈니스 창출이 가능해진다. 스마트그리드가 구축되면 전력인프라 관리측면에서 전력시설을 원격으로 제어하고 감시하는 기능이 활용 될 수 있다. 실시간으로 고장지점을 찾아내고 복구할 수 있는 시스템이 구축되면 전력공급에 대한 높은 가용성과 신뢰성 확보가 가능해진다. 또한, 발전·송전· 배전·소비자에 이르는 계층적 구조의 전력망에서 발전되어 다양한 주체들이 소비자 및 공급자의 역할을 하는 지능형 전력 네트워크 환경이 구축 될 수 있다[1].

스마트그리드 서비스 환경은 전력과 ICT 기술 기반의 이종 산업이 융합되어진 형태로 전력망 정보 이외에 사용자의 정보가 추가된 광대역·복합망 구조를 가지고 있다. 스마트그리드 내에서는 전력의 사용정보 외에 개인의 수요 정보나 지역별 분산 에너지 자원의 발전량, 개인의 검침 정보 등 다양한 전력 및 개인정보들이 생산· 전송되게 된다. 예를 들어, 소비자 영역에서 사용된 전력정보가 운영시스템으로 전송되거나, 운영시스템에서 소비자 영역으로 부하제어 또는 수요반응 신호를 송신하는 등 기존에는 분리되었던 일반 소비자 영역의 네트워크가 운영시스템의 네트워크에 연계되는 사례가 발생할 수 있다. 이러한 스마트그리드의 기술적인 특성으로 인해 전력망이 개방형 양방향 통신망과 융합된 스마트그리드는 인터넷과 마찬가지로 사이버공격, 악성 코드 등에 의한 보안 위협에 취약할 수 있다[2, 3].

최근의 스마트그리드 서비스 환경은 무선 통신 기술의 발달과 사물인터넷 기기 활용의 증가로 인해 보안 위협이 증가되고 있는 추세이다. 실제 적용 가능한 보안기술 및 보안대책에 대한 연구가 활발히 이루어지고 있는데, 다양한 서비스 영역 중 스마트홈 서비스 분야는 가장 높은 성장세와 점유율을 가지고 있어, 이에 따라 보안 위협도 증가하고 있다. 스마트홈의 보안 위협은 사생활 침해뿐 아니라 사람의 생명까지도 위협할 수 있기 때문에 스마트홈의 안전성에 대한 중요성이 어느 때보다 부각되고 있다.

스마트그리드 구현을 위한 필수 요소인 AMI(Advanced Metering Infrastructure)는 양방향 통신 기반의 스마트미터와 기타 전기사용 정보 전달 및 제어장치로 구성되어 있다. 스마트미터, HEMS(Home Energy Management System)와 가전기기 등이 연결됨에 따라 악의를 가진 제3자가 보안이 취약한 가전기기를 통해 사이버공격을 감행할 경우, 계량기를 원격 조정하여 정전을 일으키거나 계량시스템을 공격하여 스마트그리드내 스마트홈 서비스의 보안 위협을 초래 할 수 있다. 이러한 범용장비의 활용을 통한 상호연결성의 증가는 스마트그리드로의 접근을 용이하게 하지만 물리적으로 산재해 있는 장비의 관리가 쉽지 않기 때문에 관리적인 측면에서 사각지대가 생겨날 문제점을 내포하고 있다[4-6].

이에 본 논문에서는 위협 모델링 기법을 적용하여 스마트홈 서비스 환경에서의 위험 분석 방안에 대하여 제안하였다. 스마트홈 서비스 환경의 보안 위험 분석을 위해 스마트미터를

† Corresponding Author : Coon Tec, Korea
E-mail : yunan2@naver.com
* Division of Smart Electrical and Electronic Engineering, SILLA University, Korea
접수일자 : 2017년 4월 28일
수정일자 : 2017년 5월 23일
최종완료 : 2017년 5월 25일

포함한 소비자 영역의 네트워크인 스마트홈에 대한 보안 위협 요소들을 파악하였으며, 위협 모델링을 적용함으로써 스마트홈 서비스의 보안성을 강화할 수 방안에 대하여 분석하였다. 이를 통해 보안 위협 모델을 제시함으로써 안전한 스마트홈 서비스 환경을 구축 할 수 있는 방안에 대하여 제안하고자 한다.

2. 위협 모델링 방안에 대한 고찰

위험이란 주어진 위협이 자산의 취약점을 악용하여 해당 자산에 피해를 입힐 수 있는 가능성을 의미한다. 위험의 유형과 규모를 확인하기 위해서는 위험과 관련된 모든 요소들이 어떠한 영향을 미칠 수 있는 지를 분석해야 한다. 위험 분석은 위험을 계량화하여 규모를 측정하는 체계화된 절차로서 자산의 취약성을 식별하고 존재하는 위협을 분석하여 발생가능성 및 위협이 영향을 미치는 손실수준을 예측하여 위험의 내용과 수준을 결정하는 과정이라고 볼 수 있다. 위협 모델링은 분석대상의 잠재적인 위협을 분석하는 접근방법으로, 정보 자산에 영향을 줄 수 있는 위협 및 취약점을 파악하여 이를 극복할 수 있는 대안을 상세하게 검토하는 구조화된 접근 방법이다. 위협 모델링은 다양한 표준이 존재하며 운영 중인 시스템 환경에 맞는 방법론을 선택하여 적용하게 된다. 체계적으로 정리된 위협 모델링은 자산에 대한 보안 관리 체계를 명확하게 수립할 수 있으며, 서비스 운영 및 관리에 따라 위험을 경감시켜 침해사고 발생 시 효율적인 대응 방안을 마련 할 수 있다[7, 8].

초기의 위협 모델링은 주로 개발 초기나 일회성으로 수행되었지만, 시스템의 규모가 커짐에 따라 요구하는 사항이 빈번하게 변경되어 많은 비용이 발생되어 이를 해결하기 위한 다양한 연구가 수행되었다. 다양한 방법론 중에서 Microsoft 사의 위협모델링 방안이 직관적이며 다양한 이해 당사자들에게 적용되기 쉽다고 알려져 있다. 따라서 본 논문에서는 위험 분석을 위해 Microsoft사의 위협 모델링 방안을 활용한다[9-11].

2.1 위협 모델링 수행 절차

본 논문에서 언급되는 위협 모델링은 Microsoft에서 응용하고 있는 프로세스로, 해당 시스템이 가진 잠재적인 위협을 파악할 수 있고, 위협 모델링의 결과를 기반으로 시스템 점검 및 안전성 검사를 수행하기 위한 기반근거가 될 수 있다. 다음은 위협 모델링 수행을 위한 세부 수행 절차를 나타낸다.

위협 모델링은 안전한 애플리케이션 개발과 올바른 통제수단의 결정 및 위협에 대한 효과적인 대응방안을 수립하는 필수적인 프로세스이다. 세부적인 절차는 모두 5단계로 구성된다.

표 1 위협 모델링 수행절차
Table 1 Procedure of Threat Modeling

Step	수행내용
1	자산 식별(Identify Asset)
2	애플리케이션 분해(Decompose Application)
3	위협 식별(Identify Threat)
4	위협 구조 분석(Threat Analysis)
5	위협 측정(Rating the Threat)

2.1.1 자산 식별 단계

위협 모델링을 수행하는 첫 번째 단계로 해당 시스템이 가진 자산을 식별하고, 자산의 특징 및 자산이 가진 위협 요소들을 명시하고 위협 모델링을 수행할 대상을 명확히 하는 단계이다. 자산이란 시스템 내의 가치를 가지고 있는 모든 것으로 보호할 대상을 의미하게 되며, 시스템의 주요 이해관계자, 시스템 아키텍처를 구성하는 데 활용 될 수 있다. 이 단계의 목적은 수행 범위를 작성하고 자산의 분석에 초점을 맞추는 것이다. 분석 대상의 범위 내에서 자산을 식별하여 자산 목록을 목적에 맞게 다음과 같이 명시화 할 수 있다.

표 2 자산 식별 목록
Table 2 Identify Asset List

목록	내용
자산이 되는 이유 (Reasoning)	자산이 주요 이해 관계자들에게 가치를 갖는 이유 분석
외부 종속성 (External Dependency)	자산이 의존하는 외부시스템이나 이해 관계자에 대해 분석
보안 가정 (Security Assumptions)	자산 환경에 대한 보안 상태 분석
관련 자산 (Contain Asset)	다른 자산이 해당 자산에 영향을 미칠 수 있는지 여부 분석

2.1.2 애플리케이션 분해 단계

위협 모델링을 수행하는 두 번째 단계로 수집된 모든 정보를 통해 애플리케이션에 대한 데이터들의 흐름을 파악하여 정확하게 모델링하는 단계이다. 간단한 다이어그램과 테이블을 사용하여 애플리케이션에 대한 위협 요소를 파악할 수 있다. 다음은 데이터 흐름 다이어그램 작성에 필요한 주요 구성 요소를 나타낸다.

표 3 데이터 흐름 다이어그램의 구성 요소
Table 3 Element of Data Flow Diagram

구성 요소	표시 방식	내용
외부 객체		입력 지점을 통해 연동되는 애플리케이션
프로세스		애플리케이션 내의 데이터 처리
데이터 저장소		데이터가 저장된 위치
데이터 흐름		애플리케이션 내의 데이터 이동
신뢰 경계		애플리케이션의 경계 및 영역 구분

애플리케이션에 대한 분해를 위해서는 데이터 흐름 다이어그램(Data Flow Diagram) 작성이 필수적으로 작성되어야 한다. DFD는 네트워크나 설계된 시스템에 데이터 흐름을

추상적으로 표현하기 위해 일반적으로 사용된다.DFD는 외부 객체(External Entity), 프로세스(Process), 데이터 저장소(Data Store), 데이터 흐름(Data Flow), 신뢰 경계(Trust Boundary)로 구성되어 있다. DFD는 계층 구조이기 때문에 애플리케이션을 상위시스템과 하위시스템으로 분해하는데 사용된다. 애플리케이션의 아키텍처를 문서화하여 서비스 기능, 물리적 구성 등을 나타냄으로써 애플리케이션의 모든 진입점과 보안 프로필(입력 유효성 검사, 인증, 허가, 구성 관리 및 취약점)을 파악 할 수 있다.

2.1.3 위협 식별 단계

위협 모델링을 수행하는 세 번째 단계로 위협을 분류하고 공격자의 입장에서 자산들을 어떻게 공격할 수 있는지를 파악하는 단계이다. STRIDE 모델을 적용하면 공격 목적 분류 및 위협을 식별하는데 유용하게 활용이 가능하다. STRIDE 모델은 신분 위장(Spoofing Identify), 데이터 변조(Tampering with Data), 부인(Repudiation), 정보 노출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of Privilege)의 여섯 가지로 위협을 분류하여 적용할 수 있다. 이 모델은 Microsoft사에서 분석 대상의 위협을 식별하기 위해 제안한 방법으로 기밀성, 무결성, 가용성, 인증, 부인 방지, 권한 부여의 총 6가지의 목표에 대응하는 위반 속성을 분류 한다. 다음은 STRIDE 모델의 위협목록에 대한 설명을 나타낸다.

표 4 STRIDE 모델의 위협 목록
Table 4 Threat List of STRIDE Model

위협목록	내용	위반속성
신분 위장 (Spoofing Identify)	불법적인 접근 및 다른 사람의 인증정보 사용	인증
데이터 변조 (Tampering with Data)	악의적인 목적으로 데이터를 변경·수정	무결성
부인 (Repudiation)	아무것도 하지 않았고 책임이 없다고 주장	부인방지
정보 노출 (Information Disclosure))	권한이 없는 사람에게 정보 제공	기밀성
서비스 거부 (Denial of Service)	서비스를 일시적으로 중단시켜 정상 접근 거부	가용성
권한 상승 (Elevation of Privilege)	권한이 없는 자에게 권한 부여	인가

STRIDE를 위협 모델링에 활용하는 경우 분석대상에 대한 위협을 체계적으로 식별할 수 있다. 일반적으로 위협을 식별하는 경우 분석하는 사람의 역량에 따라 도출되는 결과가 다르게 나타날 수 있으므로 이를 최소화하고 분석대상의 전 범위를 빠짐없이 분석하기 위해 STRIDE 모델을 적용하여 위협을 식별한다. 이를 통해 위협 분류를 통해 해당하는 케이스와 함께 위협 분류 집합 정보를 제공하며, 이를 통해 구조적·반복적인 위협이 체계적으로 애플리케이션에서 식별이 가능해진다.

2.1.4 위협 구조 분석 단계

위협 모델링을 수행하는 네 번째 단계로 프로세스를 분해하여 효과적으로 모든 시스템의 구성 요소를 파악하고 잠재적 위협 요소를 파악할 수 있는 단계이다. 위협 트리(Attack Tree) 작성을 통해 애플리케이션의 구성요소를 열거하여 가능한 위협을 파악하고, 이 위협이 어떻게 구현 될 수 있는지 분석 할 수 있다. 위협 트리는 다양한 공격에 의거하여 시스템 보안의 특징을 규정짓는 체계적인 방법이며, 공격에 사용되는 가능한 모든 접근 수단을 분석 할 수 있게 한다. 위협 트리 작성을 위해서는 해당 시스템의 위험 분석과 관련된 자료를 해당 부분에 대한 위협, 실제 공격 여부 등의 초점에 맞춰 최대한 수집하여야 한다. 이를 통해 공격자가 위협을 실현하는 방법이 무언인지 고려해 볼 수 있다.

위협 트리를 구성하는 요소로는 노드(Node), 간선(Edge), 커넥터(Connector)가 있다. 각 노드는 공격을 나타내며 루트 노드(Root Node)는 공격자의 최종 목표를 나타낸다. 개별 공격 목표인 각각의 노드는 하위 공격 목표인 중간 노드(Sub Node)로 분해될 수 있다. 각각의 노드들은 다시 여러 가지 방법 중 선택이 가능한 OR 노드와 필수적으로 수행해야 하는 AND 노드로 구성된다. OR로 조합된 노드들은 연결되어 있는 중간 노드들 중에서 최소 하나 이상이 공격 이벤트를 발생하고 루트 노드로 전이되면 공격의 목적을 달성한 것으로 판단한다. AND로 조합된 노드들은 연결되어 있는 모든 중간 노드가 공격 이벤트를 발생하고 루트 노드로 전이되어야 공격이 성공한 것으로 판단한다. 위협 트리가 설계되면 공격 달성을 위한 가능한 모든 경우의 수를 나열하고 직접적인 방법이 도출될 때까지 세부 노드를 만들어 나간다. 이 과정에서 중간 노드들은 공격 방법에 대한 가중치를 할당받고 각각의 노드들이 가치를 계산하여 보안 대책을 수립할 수 있다.

2.1.5 위협 측정 단계

위협 모델링을 수행하는 다섯 번째 단계로 확인된 위협에 대하여 위험의 정도를 측정하는 단계이다. Microsoft사의 DREAD모델을 적용하면 위협의 정도를 측정하는데 유용하게 활용이 가능하다. 다음은 DREAD 모델의 위협목록에 대한 설명을 나타낸다.

DREAD모델은 피해 수준(Damage Potential), 재현 가능성(Reproducibility), 악용 가능성(Exploitability), 사용자 영향도

표 5 DREAD 모델의 위협 목록
Table 5 Threat List of DREAD Model

위협목록	내용
피해 수준 (Damage Potential)	피해가 얼마나 클 것인가?
재현 가능성 (Reproducibility)	공격이 성공할 확률이 얼마인가?
악용 가능성 (Exploitability)	공격을 위해 얼마나 많은 노력과 기술이 필요한가?
사용자 영향도 (Affected Users)	위협이 악용되어 공격 되었을 때 얼마나 많은 사람이 영향을 받는가?
발견 가능성 (Discoverability)	취약점을 발견하기 쉬운가?

(Affected Users), 발견 가능성(Discoverability)의 다섯 가지 항목의 위험 기준을 적용하여 위협에 대한 우선순위를 결정한다. DREAD모델을 활용하여 각각의 항목에 대하여 시스템에 어떠한 영향을 미칠 수 있는지를 파악할 수 있으며, 가장 위험한 위협이 무엇인지 결정하여 검토할 작업 순서를 정할 수 있다. DREAD 모델은 대상을 모델링하여 위험도를 단순화하고 위험의 정도를 계량하게 된다. DREAD 모델의 각 항목은 1~10점으로 평가하며, 각 항목에 대한 개별 평가 후 이를 합산하여 항목의 평균값으로 위험의 수준을 측정하게 된다. 1은 낮은 심각성·발생확률, 10은 높은 심각성·발생확률을 나타낸다.

DREAD 모델은 대상을 모델링하고 단순화하고 위험의 정도를 계량함에 있어 정성적인 방식으로 측정하므로, 평가자의 전문적인 역량수준과 주관적인 견해에 의해 결과가 영향을 받을 수 있다. 이러한 문제점을 보완하기 위해 관련 분야에 대한 정략적인 기준이 설정되어야 한다.

3. 스마트홈 서비스 위협 모델링 적용 사례연구

스마트홈 서비스는 집안에서 사용하는 가전기기에 네트워크를 연결하여 기기를 원격으로 제어할 수 있도록 하는 서비스를 제공한다. 저전력 소형 기기들이 소규모 네트워크를 내에서 사업자가 제공하는 서비스를 유기적으로 동작하게 한다. 스마트홈 서비스에서는 플러그, 열림 감지, 가스 차단 등을 주요 서비스로 제공하고 있으며, 이를 위해 서비스의 모바일 애플리케이션, 서버, 각종 센서 및 기기 등이 활용되고 있다. 2장에서 언급한 위협 모델링 방안은 Microsoft사에서 응용하고 있는 프로세스로, 해당 시스템이 가진 잠재적인 위협을 파악할 수 있고 설계상에 있어 보안 요구사항을 명확히 할 수 있다.

본 논문에서는 위협 모델링 방안을 적용하여 스마트홈의 전체적인 위험 분석을 수행하였다. 스마트홈 서비스 환경에서는 다양한 정보가 생성·전송되며 이들 중에서 보호할 정보를 확인하고 정보의 특성이나 기존에 해당 정보로부터 알려진 위협을 파악하여야 한다. 특히 개인정보의 경우 다양한 위협에 노출될 수 있으므로 간단하고 직관적인 모델링이 필요하다. 위협 모델링을 수행하기 위해 Microsoft사의 Threat Modeling Tool을 이용하였다.

3.1 위협 모델링 적용 결과

스마트홈 서비스에서는 개인정보를 수집하는 다양한 엔티티(Entity)들이 존재한다. 개인정보를 수집할 때 개인정보 수집, 사용, 공유에 대해 명확한 목적이 존재하기 때문에 데이터 액세스를 모니터링 해야 한다.

우선 스마트홈의 자산을 식별해야 하는데 스마트홈을 서비스의 주요 자산은 HEMS(Home Energy Management System), 스마트 미터(Smart Meter), 스마트 가전기기(Smart Appliance), AP(Access Point), 라우터(Router) 등이 고려될 수 있다. 스마트홈을 이루고 있는 자산 중 자산이 되는 이유(Reasoning), 외부 종속성(External Dependency), 보안 가정(Security Assumptions),관련 자산(Contain Asset)을 고려하여 자산 목록을 다음과 같이 도출 할 수 있다.

표 6 스마트홈의 자산 식별
Table 6 Identify Asset of Smart Home

자산	내용
자산이 되는 이유	• HEMS의 스마트 가전기기 제어 • 스마트미터를 통한 에너지 사용량 계량 • 전력망과 서버를 통한 통신 수행
외부 종속성	• 사용자가 애플리케이션을 통해 서버와 통신을 수행하고 상태 정보 등을 제공 • 스마트 기기를 통해 서버에 접근
보안 가정	• 통신의 안정적 구성 및 유지·관리 필요 • 적절한 인증을 통한 데이터의 신뢰성 확보 필요
관련 자산	• 미터 데이터 관리 시스템 • 홈 디바이스 • 데이터 저장 서버

다음은 애플리케이션 분해를 위해 데이터 흐름 다이어그램(Data Flow Diagram)을 작성한다. DFD 작성을 통한 데이터

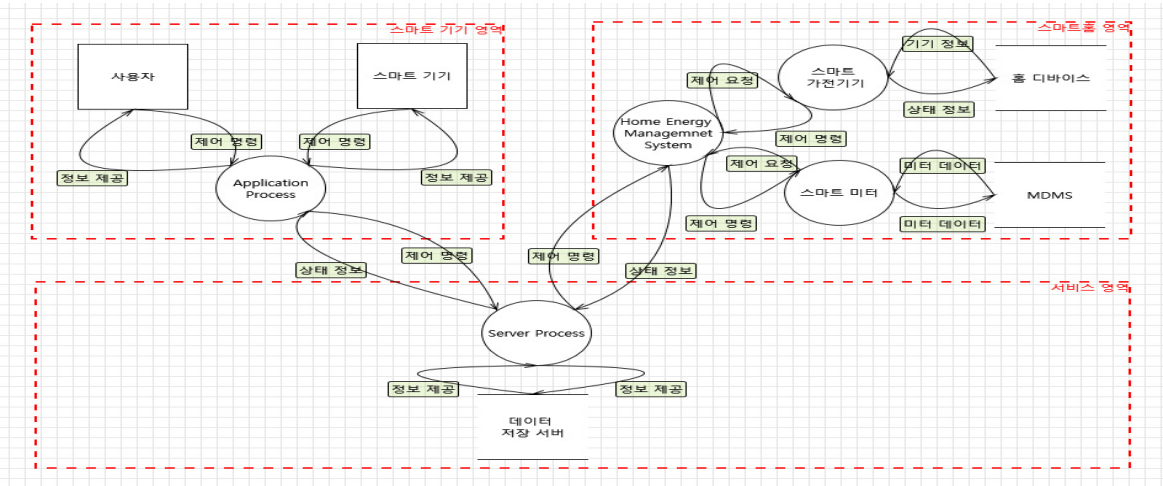

그림 1 스마트홈의 데이터 흐름 다이어그램
Fig. 1 Data Flow Diagram of Smart Home

흐름을 분석하여 보안 요구 사항, 가능한 위협을 정의할 수 있다. 총 3가지 신뢰 경계 영역으로 구성될 수 있는데, 사용자와 스마트기기가 원격으로 명령을 지시할 수 있는 스마트기기 영역, 스마트미터와 스마트 가전기기 등이 존재하는 스마트홈 영역, 서비스 영역으로 분류된다. 그림 1은 스마트홈의 데이터 흐름 다이어그램을 나타낸다.

DFD의 구조 및 구성요소들을 분석해 보면, 스마트 기기 영역에서의 사용자는 최초 로그인을 수행 할 경우 사용자의 아이디와 패스워드를 입력하며, 제어하고자 하는 가전기기를 스마트 기기를 이용하여 애플리케이션에 제어명령을 내린다. 스마트 홈 영역에서는 가정 내의 스마트 가전기기나 스마트미터 등의 정보를 통합하여 관리를 수행한다. 서비스 영역에서는 서비스를 제공하는 측면의 서버로 사용자들의 개인정보, 등록된 가전기기 등의 정보가 등록되어 있어 기기 제어와 관련된 서비스를 제공하게 된다.

앞서 도출한 DFD를 바탕으로 위협 식별을 위해 각 영역에서 발생 가능한 위협을 STRIDE 모델을 적용하여 분석을 수행한다. DFD 구성 요소에 따라 STRIDE 모델을 적용하여 실현 가능한 위협을 다음과 같이 식별하였다.

표 7 STRIDE 모델을 적용한 위험 식별 결과
Table 7 Identify Threat Results Applying the STRIDE Model

영역	요소	위협 목록	내용
스마트 기기	사용자	신분위장	위장 인증으로 로그인 시도
		부인	인증된 로그인 정보 악용
		서비스거부	사용자 서비스 거부
	스마트 기기	데이터변조	스마트 기기 데이터 수정
		정보노출	저장된 개인 정보 노출
스마트 홈	HEMS	데이터변조	저장된 정보 수정 및 변경
		부인	관리 시스템 불능
		정보노출	서비스 정보 노출
	스마트 미터	신분위장	위장 인증으로 로그인
		데이터변조	계량 데이터 수정
		부인	에너지 사용 부인
		정보노출	저장된 개인 정보 유출
서비스	서버	신분위장	위장 신분으로 공격 수행
		서비스거부	서버 공격 수행
		데이터변조	SQL 인젝션 공격 수행

위협 트리를 작성을 통하여 공격의 수단을 그림 2와 같이 단계적으로 분석하였다. 루트 노드를 분석상인 스마트홈 서비스에 대한 공격으로 설정하였으며, 루트 노드에 대한 공격을 수행하기 해서는 전체 서비스의 구성요소인 애플리케이션 공격, 홈 디바이스 공격, 서비스 서버 공격으로 하위 노드를 구성하였다. 위협 트리의 최하위 노드에는 STRIDE 모델과 관련한 위협들을 통해 공격 목표를 도출하였으며, 이를 통해 스마트홈에 대한 위험을 분석하였다.

위협 트리 분석을 통해 공격 유형을 파악하였으며, 확인된 위협에 대한 위험도를 측정하기 위해 DREAD 모델을 적용하여 위험 분석을 수행하였다. 항목별로 위험 등급을 구분하여 수치화 하였으며, 등급이 높을수록 위험이 높을 것

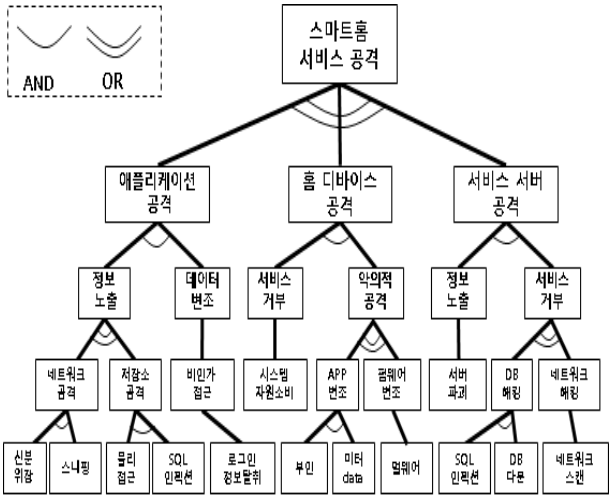

그림 2 스마트홈의 위협 트리
Fig. 2 Attack Tree of Smart Home

을 의미한다. 다음은 식별된 위협에 DREAD 모델을 적용한 위험 측정 결과를 나타낸다.

표 8 DREAD 모델을 적용한 위험 측정 결과
Table 8 Rating the Threat Results Applying the DREAD Model

위협 목록	D	R	E	A	D	합계	평균
홈 네트워크에 비인가 접근	5	5	5	5	5	25	5
스마트기기에 접근 권한 부여	8	5	5	5	5	28	5.6
저장된 개인 정보 수집	10	5	5	5	5	30	6
서비스 로그인 정보 변경	5	6	5	5	9	30	6
위장 신분으로 서버 공격	**10**	**5**	**5**	**8**	**8**	**36**	**7.2**

각 항목별로 피해수준 항목은 공격에 의해 발생 할 수 있는 피해가 클수록 등급이 높으며, 재현가능성 항목은 공격기회가 주어지는 시간적 범위가 클수록 등급이 높다고 볼 수 있다. 악용 가능성 항목은 공격 기법의 구현 난이도를 판단하여 구현이 쉬울수록 위험이 높으며, 사용자 영향도 항목은 하나의 공격 행위로 인해 영향을 받는 이용자의 수가 많을수록 위험이 높다. 발견 가능성 항목은 위협 취약점과 이를 이용한 구체적인 공격 방법을 찾아내는 것이 쉬울수록 등급이 높게 된다. 위험 측정 결과를 보면 홈 네트워크에 비인가 접근의 위협이 가장 위험도가 낮고, 위장 신분으로 서버 공격을 수행하는 위협이 가장 위험도가 높게 측정되었다. 이는 서버에 스마트홈 서비스에서 수집되는 정보들을 저장하고 있기 때문으로 판단되며, 전력사용 정보, 전력사용패턴, 가전기기 사용정보를 통해 개인행동 및 활동패턴을 파악할 수 있는 정보의 유출이 가능하다고 분석된다.

스마트홈 서비스의 안전한 사용을 위해 대응방안을 수립하기 위해서는 존재하는 보안위협이 파악되어야 한다. 스마트홈 서비스에 특화된 위협모델링을 수행함으로써 발생 가능한 취약점이 파악되었으며, 위험도를 고려하여 위협의 우선순위가 결정되었다. 도출된 결과를 바탕으로 취약점을 파악하여 사전에 위협 요소가 실현되는 것을 방지함으로써 스마트홈 서비스의 자산을 보호할 수 있으며 보안 점검 모델을 제시

하여 안전한 스마트 홈서비스 환경을 구축할 수 있는 방안을 마련할 수 있게 되었다.

4. 결 론

본 논문에서는 위협 모델링을 적용하여 스마트홈 서비스의 위험 분석을 수행하였다. 스마트홈 서비스의 안전한 구현을 위해 발생 가능한 위협을 분석하였다. STRIDE 모델을 통해 위협을 식별하였고, 위협 트리를 통해 공격 가능한 위험을 분석하였으며, DREAD 모델을 적용하여 위험도를 측정하였다. 도출된 결과를 통해 보안 취약점이 보완되고 식별된 위협 요소가 서비스에 악영향을 끼치는 것을 방지함으로써 자산을 보호하여 위험을 경감시킬 수 있다. 사용자에게 편의성을 제공하는 스마트홈 서비스 관련 시장이 빠르게 증가하고 있는 추세이며, 이에 따라 발생 가능한 보안 사고의 피해 규모는 상당히 클 것이라고 예상된다. 하지만, 스마트홈 서비스에 대한 위협에 대응하기 위한 체계적인 기준 등이 미비한 상태이다. 이에 도출된 위협 모델링 결과를 통해 스마트홈 서비스에 대한 보안 점검을 수행할 수 있는 기반근거로 활용할 수 있을 거라 판단된다.

향후에는, 스마트홈 서비스 환경에 활용이 가능한 위험 완화 기술에 대한 연구가 필요하다고 판단된다. 이를 위해 다양한 이론적인 검토와 실증을 통해 사용자의 관점에서 안정성과 편의성이 고려된 위험 완화 방안이 수립되어야 할 것이다.

References

[1] MKE, “Smart Grid Road Map”, 2010.

[2] “Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks”, PIER Program INTERIM PROJECT REPORT, 2012.

[3] P. Hong, S. Lee, M. Park, and S. Kim, "Threat-Based Security Analysis for the Domestic Smart Home Appliance," *KIPS Transactions on Computer and Communication Systems*, vol. 6, no. 3, pp. 143-158, 2017.

[4] Kim Kyoung Gon, Kim Soo Hoon, “Using Threat Modeling for Risk Analysis of SmartHome”, Proceedings of the Korean Institute of Communication Sciences Conference, 2015.

[5] Beckers, K., Faßbender, S., Heisel, M., & Suppan, S. “A Threat Analysis Methodology for Smart Home Scenarios”, Technical Report, 2016.

[6] Mikkelsen, Søren Aagaard, Jacobsen, Rune Hylsberg. “Securing the Home Energy Management Platform”, 2016.

[7] Rao, K. Ram Mohan, and Durgesh Pant. "A threat risk modeling framework for Geospatial Weather Information System (GWIS): a DREAD based study." international Journal of Advanced Computer Science and Applications, 2010.

[8] Suppan, Santiago. "A Threat Analysis Methodology for Smart Home Scenarios." Smart Grid Security: Second International Workshop, Revised Selected Papers. vol. 8448. Springer, 2014.

[9] Microsoft, “Threat Modeling Web Applications”, Available: https://msdn.microsoft.com/en-us/library/hh917316.aspx.

[10] Microsoft, “Threat Modeling Tool 2016 Getting Started Guide”, 2016.

[11] OWASP, “Threat Risk Modeling”, Available: https://www.owasp.org/index.php/Threat_Risk_Modeling.

저 자 소 개

이 윤 환 (李 允 煥)

2010년 고려대 일반대학원 전자전기공학과 졸업(석사), 2014년 동대학원 졸업(박사). 2014년~2016년 한국스마트그리드사업단 신사업추진실 대리, 2016년~쿤텍(주) 기술연구소 선임연구원

E-mail : yunan2@naver.com

박 상 건 (朴 相 建)

2009년~2014년 나고야(名古屋) 대학교 전기컴퓨터공학부 졸업(박사), 2003년~2007년 삼성SDI 중앙연구소 AM개발팀 전임연구원, 2007년~2016년 식품의약품안전처 식품의약품안전평가원 공업연구사, 2016년 3월~신라대학교 전기전자공학부 조교수

E-mail : sgpark@silla.ac.kr