논문 20-45-11-10 The Journal of Korean Institute of Communications and Information Sciences '20-11 Vol.45 No.11
https://doi.org/10.7840/kics.2020.45.11.1868

위협 모델링을 이용한 스마트 도어락 위협 분석

심 신 우◆°, 임 선 영*, 류 한 얼*, 전 성 구*, 김 태 규*

Threat Analysis of the Smart Doorlock Systems Using Threat Modeling

Shinwoo Shim◆°, Sun-Young Im*, Han-Eul Ryu*, Sung-Goo Jun*, Taekyu Kim*

요 약

스마트폰의 확산과 스마트폰과 연동되는 스마트 도어락의 편의성으로 인해 스마트 도어락의 수요는 점차 늘어나고, 그에 따라 시중에 다양한 종류의 스마트 도어락이 보급되고 있다. 스마트 도어락은 사용자의 자산을 보호하는 가장 필수적이고 기초적인 물리적 보안 장치이기 때문에 스마트 도어락의 취약점은 사용자 자산의 안전성을 저해하는 큰 위협이 될 수 있다. 하지만, 스마트 도어락 제조 업체별 보안 수준은 상이하고, 스마트 도어락 보안성에 대한 기준이 미비하여, 스마트 도어락에 대한 보안성 연구가 필요하다. 본 연구에서는 데이터 흐름도(DFD, Data Flow Diagram)를 통해 스마트 도어락 시스템에서 필요한 데이터 저장소, 프로세스, 데이터, 외부 인자 등을 식별하여 스마트 도어락의 기능을 파악하고, 생성된 데이터 흐름도를 기반으로 스마트 도어락 시스템에 발생할 수 있는 위협들을 식별한다. 식별된 위협을 기반으로 공격 트리를 생성하여 공격자 입장에서의 공격 목적과 공격 방법을 파악하여 공격 시나리오를 작성하고, 도출한 시나리오에 대해 DREAD 분석 기법을 이용해 위험도를 분석하고, 최종적으로 위험에 대한 대처 방안을 수립하여 스마트 도어락 보안성 향상 방안에 대해 제시한다.

Key Words : Information Security, Threat Modeling, Risk Analysis, Risk Assessment, Risk Mitigation, Smart Doorlock

ABSTRACT

Smart doorlocks are prevailing because of the convenience of the smart doorlocks. The lack of security on smart doorlocks can lead to the significant loss of safety on user's asset because smart doorlocks are the basic and essential physical security equipments which protect user's asset. However, the technology on the securities of the manufacturing companies differ and the criterions on the smart doorlocks are lacking. Therefore the research on the security analysis on the smart doorlocks is needed. This paper analyzes the operation of the smart doorlock systems by DFD(Data Flow Diagram) and the possible threats are identified. By using the identified threats, attack tree is drawn and the attack scenarios are described by analyzing the intention and the actions of the adversaries. We analyzed the risk of the attacks and finally the countermeasures will be drawn by using DREAD analysis.

◆° First and Corresponding Author : LIG Nex1 Co., shimshinwoo@lignex1.com, 정회원
* LIG Nex1 Co., sunyoung.im@lignex1.com, 정회원; haneul.ryu@lignex1.com, 정회원; sunggoo.jun@lignex1.com; taekyu.kim@lignex1.com
논문번호 : 202007-163-B-RN, Received July 23, 2020; Revised August 31, 2020; Accepted August 31, 2020

Ⅰ. 서 론

스마트폰의 보급이 확산됨에 따라 스마트폰의 블루투스 통신 기능을 활용해 도어락을 열 수 있는 스마트 도어락 제품의 보급이 증가하고 있다. 기존의 디지털 도어락은 키패드에 비밀번호를 입력해야만 문이 열리는 방식이었지만 스마트 도어락은 스마트폰 버튼 하나만 누르거나, 스마트폰을 가지고 문에 가까이 가기만 하여도 잠금이 해제되는 편의성으로 인해 많은 업체에서 제품을 제조하고 출시하고 있다. 도어락은 사용자의 자산을 보호하는 가장 필수적이고 기초적인 물리적 보안 장치이므로, 그 특성상 높은 수준의 보안성을 보장해야 하지만 스마트 도어락 제조 업체마다 보안 기술 수준과 그 기준이 상이하다.

따라서, 스마트 도어락이 기본적으로 갖추어야 할 보안 기능을 분석하기 위해 스마트 도어락에 대해 발생할 수 있는 위협에 대해 연구하고, 그에 대한 대책을 세우는 작업이 필요하다. 따라서 본 논문에서는 휴대폰과 블루투스 통신을 하여 도어락 잠금을 해제할 수 있는 스마트 도어락에 대해서 위협 모델링(Threat Modeling)[1]을 수행하여 위협을 식별하고 식별된 위협을 기반으로 공격자의 의도와 공격 방법을 분석하여 공격 시나리오를 작성하고, 도출된 시나리오에 대해 위험도 분석과 대처 방안을 수립한다.

본 논문 2장에서는 스마트 도어락 관련 보안성 연구와 위협 모델링에 대한 관련 연구를 설명하고, 3장에서는 스마트 도어락에 대한 위협 모델링 분석 과정과 결과에 대해 기술하고, 4장에서는 차후 연구와 결론에 대해 기술한다.

Ⅱ. 관련 연구

스마트 홈이나 모바일 건강관리 시스템, 자동차 등 개인이 사용하는 IoT 시스템에 대한 보안 연구는 지속적으로 이루어지고 있다.

Nikolay Akatyev와 Joshua I. James는 스마트 홈과 스마트 오피스에 대한 IoT 시스템의 네트워크에 대한 사이버 위협에 대해 식별하고, IoT 네트워크에 대해 침해할 수 있는 사례에 대해 연구하여 IoT 네트워크 설계 및 조사 시 필요한 가이드를 제시하였다[2].

Andreas Jacobsson 외 2명은 스마트 홈 오토메이션 시스템에 대해 위협 분석을 수행하고 위협에 대해 분류 및 위험도 분석을 수행하였다. 이 연구에서는 보안성 기준에 대한 표준을 준수한 제품 디자인을 통해 스마트 홈에 대한 위험성을 경감시킬 수 있다는 의견을 제시하였다[3].

Olayemi Olawumi 외 3명은 스마트 홈과 모바일 건강 관리 시스템에 대한 보안 이슈에 대해 분석하여 발생할 수 있는 공격과 취약점에 대해 식별하고 위협에 대한 대책을 제시하기 위해 스마트 홈과 모바일 건강 관리 시스템을 결합한 환경을 제공하는 시스템인 Smart Environment for Assisted Living (SEAL) system에 대해 위협 모델링을 수행하였다[4].

Georg Macher 외 3명은 자동차 보안 분야에서 활용할 수 있는 위험 평가 기술에 대해 분석하고, 사이버 보안 위협에 대해 분류하고 해당 위협에 대해 대응할 수 있는 방책들을 식별하여 개발 시 적용할 수 있는 보안 분석 방법에 대해 연구하였다[5].

위협 모델링에 대한 연구는 여러 분야의 여러 제품군에 대해 이루어져 개인이 사용하는 웨어러블 디바이스에 대해서도 연구된 바 있으며[6] 개인이 사용하는 일반적인 스마트홈, 자동차 IoT 시스템에 대한 위협 및 취약점에 대한 연구는 지속적으로 이루어지고 있지만, 스마트 도어락 개별 제품의 기능과 특성에 중점을 둔 연구는 아직 이루어진 경우가 없기 때문에 스마트 도어락에 한정하여 발생할 수 있는 구체적인 위협 분석을 위한 위협 모델링 연구가 필요하다.

Ⅲ. 스마트 도어락에 대한 위협 모델링

스마트 도어락에 대한 위협 모델링은 데이터 흐름도 작성, STRIDE를 이용한 위협 식별, 공격 트리(Attack Tree) 및 공격 시나리오 작성, 위험도 분석 순으로 이루어진다. 다음의 각 절에서 각 항목에 대해 설명한다.

3.1 데이터 흐름도

시스템에 대한 위협을 식별하기 위해서는 해당 시스템이 어떻게 작동하는지에 대한 분석이 필요하다. 시스템 분석은 데이터 흐름도(Data Flow Diagram), 수영 표시선도(Swim Lane Diagram), 상태도(State Diagram) 등을 통해 수행할 수 있다.

본 연구에서는 데이터 흐름도를 통해 스마트 도어락에 대한 동작을 분석한다. 데이터 흐름도는 데이터 저장(Data Store), 프로세스(Process), 데이터 흐름(Data Flow), 외부 엔티티(External entity)로 구성되며, 이들 간의 관계가 나타나므로, 데이터 흐름도를 활용하면 공격자가 어떤 취약점을 통해 스마트 도어락을 공격할 수 있는지 분석할 수 있기 때문이다. 또한 데이터 흐름도는 데이터의 흐름에 따라 다이어그

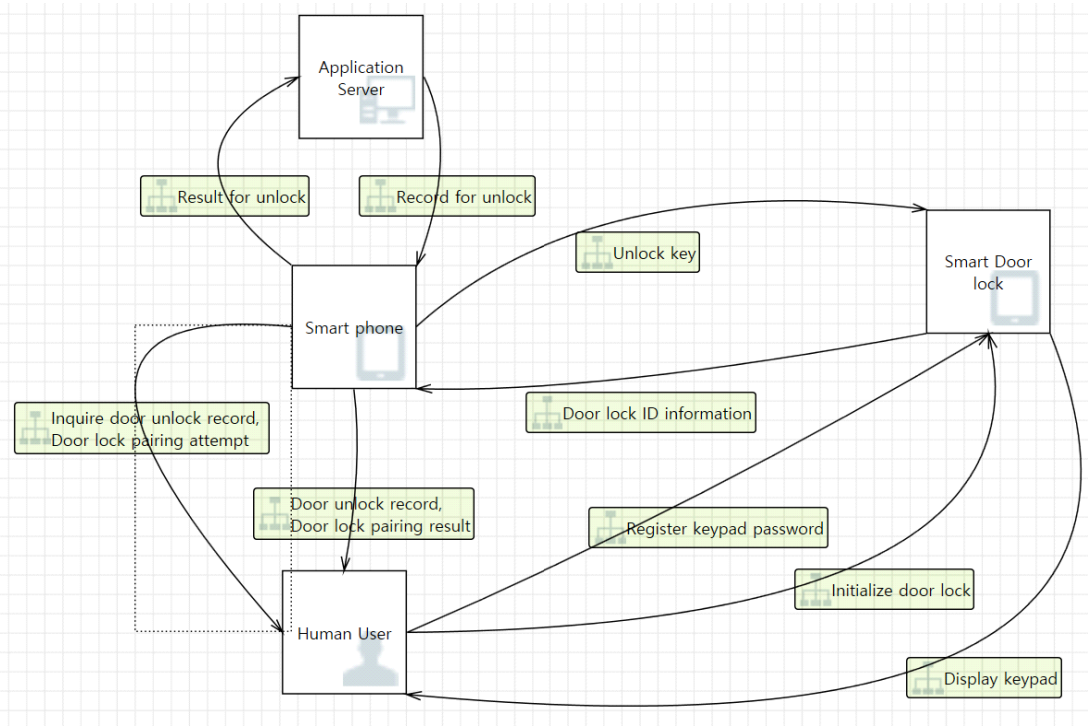


그림 1. 수준 0 데이터 흐름도
Fig. 1. Level 0 Data Flow Diagram

램을 그리기 때문에 공격이 어떻게 발생하는지 파악할 수 있어 위협 모델링을 수행할 때 주로 사용되는 다이어그램이다.[7] 데이터 흐름도의 작성은 Microsoft Threat Modeling Tool 2016[8] 프로그램을 사용하였다.

그림. 1 은 수준(Level) 0의 데이터 흐름도를 나타낸다. 수준 0에서는 직관적으로 생각하여 알 수 있는 객체와 데이터의 흐름을 통해 추상화 레벨이 높은 다이어그램을 작성한다. 스마트폰, 스마트 도어락, 어플리케이션 서버에서 각각의 프로세스들을 모두 수행한다고 가정하였으며, 이들 간의 데이터 플로우도 일반인이 상식적으로 생각하여 도출해낼 수 있는 수준의 내용으로 나타내었다.

스마트 도어락은 사용자의 스마트폰과 블루투스로 통신하여 잠금 해제가 가능하고, 기존의 디지털 도어락과 같이 키패드로 비밀번호를 입력해 잠금을 해제할 수 있다. 또한 사용자는 스마트폰의 앱을 통해 잠금 해제 이력을 확인할 수 있다. 잠금 해제 이력은 어플리케이션 서버에 저장되어, 가족 구성원끼리 출입 이력이 공유된다.

다음은 추상화 정도를 낮추어 수준(Level) 1 데이터 흐름도를 작성하였다(그림 2). 수준 1에서는 실제 제품 개발 시 필요한 데이터 저장소, 세부적으로 이루어지는 프로세스, 프로세스 간에 오가는 세부 데이터를 표시한다.

스마트 도어락 시스템을 구성하는 요소는 크게 세 부분으로 어플리케이션 서버, 스마트폰 앱, 그리고 도어락 본체로 나뉜다.

어플리케이션 서버에서는 출입이력 로그 데이터 저장소를 가지며, 스마트폰 앱과의 통신을 통해 출입이력 로그 데이터를 서로 송수신한다.

스마트폰 앱에서는 도어락과 블루투스 통신을 하여 도어락 잠금을 해제할 수 있다. 잠금 해제 키는 스마트폰 앱 내의 별도의 저장소에 저장되어 관리된다. 또한 어플리케이션 서버와는 출입이력을 송수신하고, 사용자 입력을 받아 사용자에게 출입 이력을 보여 주는 기능도 수행한다.

스마트 도어락 본체에서는 크게 블루투스 통신을 하여 잠금을 해제하는 기능, 키패드로부터 사용자 입력을 받아 잠금을 해제하는 기능을 가진다.

블루투스 잠금해제 키는 키 저장소에 저장되며, 스마트폰과 블루투스 통신을 하여 이 키를 등록하고, 나중에 잠금 해제 시 키를 비교한다. 키패드 비밀번호는 사용자로부터 키패드 비밀번호를 입력받아 키패드 비밀번호 키 저장소에 저장하고, 나중에 사용자로부터

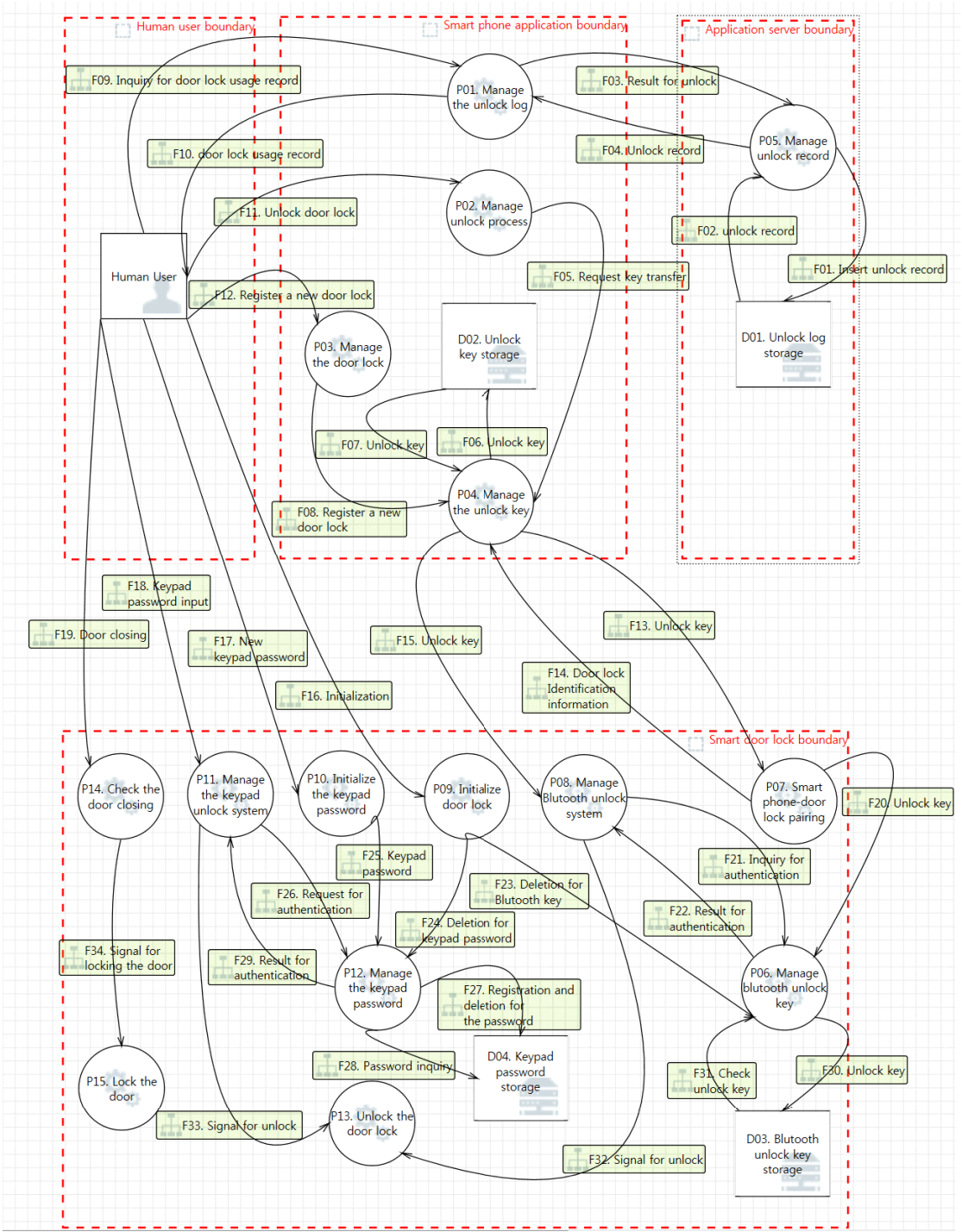


그림 2. 수준 1 데이터 흐름도
Fig. 2. Level 1 Data Flow Diagram

비밀번호를 입력받아 키를 비교하여 도어락 잠금 해제를 수행한다. 그림 2 에서 어플리케이션 서버, 스마트폰 앱, 스마트 도어락, 그리고 사용자 간의 데이터 플로우 및 필요한 데이터 저장소, 세부 프로세스를 식별하고, 그 사이의 관계에 대해 다이어그램으로 나타내었다.

3.2 STRIDE를 이용한 위협 식별

3.1에서 분석한 데이터 흐름도에 대해 각 흐름이나 프로세스, 데이터 저장소에서 발생할 수 있는 취약점을 분석하기 위해서 STRIDE[9] 분석을 수행하였다. STRIDE는 스푸핑(Spoofing), 탬퍼링(Tampering), 거부(Repudiation), 정보 유출(Information disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of Privilege)의 약자로 공격자의 입장에서 공격을 수행하는 목적과 수단을 분석하는 방법이다. 방어자 입장보다 공격자의 관점에서 보는 것이 좀 더 쉽게 취약점을 식별할 수 있기 때문이다.

표 1에서 STRIDE 분석을 통해 발생할 수 있는 위협을 나열하였으며, 여기서 위협유형(Threat Type)의 약자는 각각 다음과 같다.

◉ S : Spoofing(정당한 사용자로 가장함)

표 1. 스마트 도어락에 대한 STRIDE 분석
Table 1. STRIDE Analysis on Smart doorlocks

DFD ID	Threat ID	Threat Type	Description
F15	T01	S	Unlocking doorlock by sniffing communication between a smart phone and a doorlock to perform replay attack
F15	T02	S	Obtaining secret key by sniffing communication between a smart phone and a doorlock
F18 P11	T03	S	Attempting an on-line guessing attack on the keypad by guessing the doorlock password
F13	T04	D	Trying to disturb the Bluetooth connection between a smart phone and a doorlock by using a fake doorlock in advance,
F14	T05	D	Trying to disturb the Bluetooth connection between a smart phone and a doorlock by using a fake smart phone in advance
F13 F14 F15	T06	D	Trying to disturb the Bluetooth connection using an Android vulnerability (CVE-2016-3839)[10]
F13	T07	S	A Man in the Middle Attack when performing a pairing between a smart phone and a doorlock, the communication between the smart phone and the doorlock is intercepted
D01	T08	T	Inserting a fake access record into the application server DB
F04	T09	T	Sending fake unlock logs to a smart phone to manipulate access logs
F10 P01	T10	T	Sending fake unlock logs to the application server to manipulate access logs
F15 P08	T11	D	Exhausting the battery in a doorlock by continuously attempting a Bluetooth connection
P09	T12	S	Initializing the doorlock and set a new keypad password
P09	T13	S	Pairing a doorlock with the attacker's smart phone by initializing the doorlock
D03	T14	S	Attempting to off-line guessing attack by stealing the Bluetooth unlock key database and brute force attack against it
D03	T15	D	Deleting Bluetooth unlock key database
D04	T16	S	Attempting off-line guessing attack by stealing a keypad password key database and brute force attack against it
D04	T17	D	Deleting keypad password database
D02	T18	S	Off-line guessing attack by brute force attack by taking the unlock key storage of a smart phone
D02	T19	D	Deleting a smart phone's key database
F03	T20	I	Obtaining the person's information by sniffing the transmission data of the unlocking record
D01	T21	I	Obtaining access information by accessing the unlock history data
P08	T22	S	Unlocking the doorlock by bypassing Bluetooth key authentication
P11	T23	S	Unlocking doorlock by bypassing keypad password authentication

◉ T : Tampering(데이터 변조)
◉ R : Repudiation(수행한 행동이나 이력을 부인)
◉ I : Information disclosure(공개되지 않아야 할 정보 공개)
◉ D : Denial of Service(서비스 거부)
◉ E : Elevation of Privilege(권한 상승)

3.3 공격 트리 및 공격 시나리오

3.2에서 분석한 위협을 기반으로 공격 트리[11]를 작성하고 공격 시나리오를 도출하여 공격자의 입장에서 어떤 목적으로 어떤 절차와 방식을 통해 공격을 수행하는지 분석하였다. 공격 트리를 통해 공격자의 의도로부터 세부 행동까지 톱-다운(Top-Down) 방식으로 공격자의 행위를 분석할 수 있으므로 체계적으로 공격 시나리오를 만들 수 있다. 공격자의 의도에 따라 공격 트리를 4가지로 분류하였으며, 각각의 경우에 따라 공격 시나리오를 분석하였다. 그리고 위에서 분석한 각 위협들이 각 공격 트리에서 어느 부분에 해당하는지를 표시하였다. 공격자의 4가지 의도는 다음과 같다.

3.3.1 도어락 잠금 해제

첫 번째 공격 방식은 도어락을 잠금 해제하여 피해자의 집으로 침입하는 공격이다. 이는 공격자의 가장 궁극적인 공격 의도이며, 그 피해도 가장 크다고 볼 수 있다.

그림. 3 은 도어락 잠금 해제에 대한 공격 트리를 나타낸다. 도어락을 잠금 해제하는 방식은 블루투스 잠금 해제 장치를 공격하는 방법, 키패드 비밀번호를 공격하는 방법,도어락을 초기화하는 방법 3가지로 나뉜다.

블루투스 잠금 해제 장치를 공격하는 방법으로는 블루투스 통신 데이터를 스니핑한 뒤 해당 데이터를 재전송하여 도어락을 속이는 방법, 블루투스 통신 데이터를 스니핑하거나 키 데이터베이스를 해킹하여 블루투스 비밀 키를 획득하는 방법, 블루투스 키 인증을 우회하는 방법이 있다.

키패드 비밀번호를 공격하는 방법으로는 사용자가 비밀번호를 입력하는 행위를 엿보거나 키패드를 확인하여 지문이 많이 묻은 번호를 통해 비밀번호를 추측하여 키패드 비밀번호를 획득하는 방법, 키패드 비밀번호 인증을 우회하는 방법이 있다.

마지막으로 도어락을 초기화하여 공격자의 스마트폰과 도어락을 페어링하는 방법, 새로운 키패드 비밀번호를 등록하는 방법이 있다.

3.3.2 도어락 잠금 해제 방해

두 번째 공격 방식은 사용자의 도어락 잠금 해제를 방해하는 공격이다. 이는 공격자가 직접적으로 침입에 성공하진 못하지만 악의적인 의도를 가지고 사용자에게 피해를 입히는 공격 방식이다.

도어락 잠금 해제를 방해하는 방법은 크게 키 비교를 방해하는 방법, 도어락 배터리를 방전시켜 도어락이 동작을 멈추게 하는 방법이 있다.

도어락 잠금 해제를 방해하는 방법으로는 블루투스 통신을 방해하는 방법, 블루투스 키나 키패드 비밀번호를 삭제하는 방법이 있다.

그림 4 는 도어락 잠금 해제 방해에 대한 공격 트리를 나타낸다.

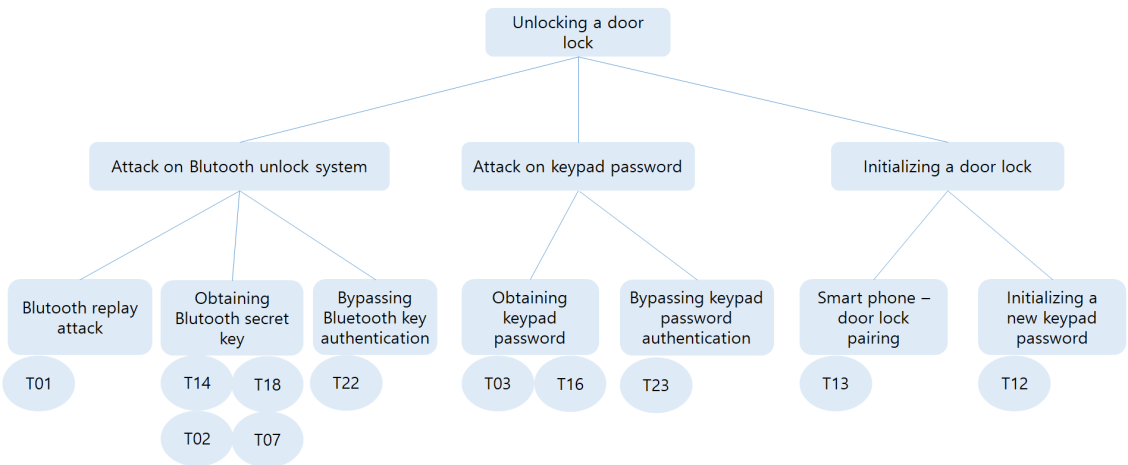


그림 3. 도어락 잠금 해제에 대한 공격 트리
Fig. 3. Attack Tree for Unlocking the doorlock

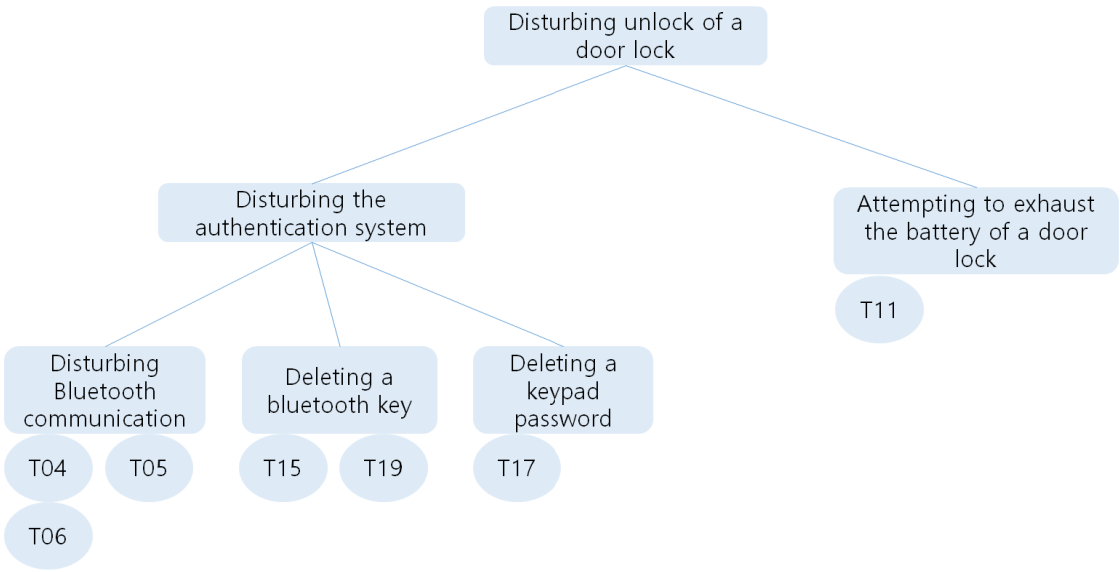


그림 4. 도어락 잠금 해제 방해에 대한 공격 트리
Fig. 4. Attack Tree for Disturbing unlock of a doorlock

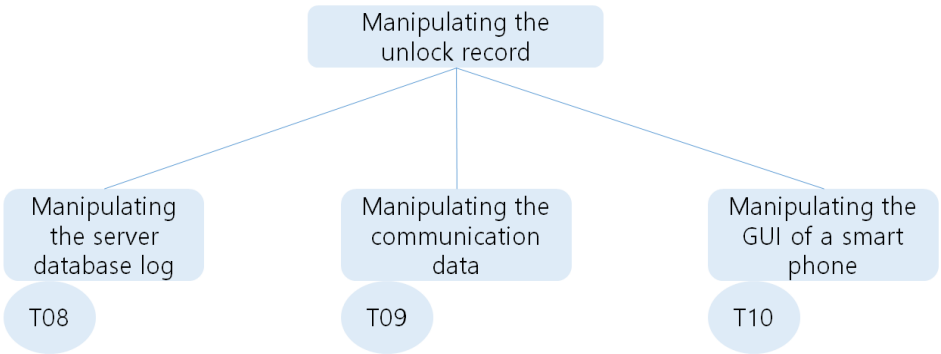


그림 5. 잠금해제 이력 조작에 대한 공격 트리
Fig. 5. Attack Tree for Manipulating the unlock record

3.3.3 잠금해제 이력 조작

세 번째 공격 방식은 잠금해제 이력을 조작하는 공격이다. 이 공격을 통해서는 침입자가 침입을 하고 나서 그 이력을 삭제하여 증거를 없애거나, 집에 들어가지 않은 가족 구성원이 집에 출입하였다는 이력을 추가하여, 다른 구성원이 안심하도록 만드는 의도로 공격이 가능하다. 잠금해제 이력 조작은 서버 출입이력 로그 데이터 조작, 통신 데이터 조작, 스마트폰 어플리케이션의 출입이력 조회 화면 조작을 통해 이루어진다.

그림 5 는 잠금 해제 이력 조작에 대한 공격 트리를 나타낸다.

3.3.4 잠금해제 이력 조회

네 번째 공격 방식은 잠금해제 이력 조회 권한이 없는 공격자가 타인의 잠금해제 이력을 조회하는 공격이다. 이 공격은 피해자에게 큰 피해를 입힐 수 없을 것으로 보이지만, 예를 들어, 어린이가 집에 혼자 있음을 확인한 뒤 어린이를 유인하여 집으로 침입하는 등의 공격으로 이루어져 피해자에게 심각한 피해를 입힐 수 있는 공격이다. 잠금해제 이력 조회는 송수신되는 잠금해제 이력 데이터를 스니핑하거나, 잠금해제 데이터베이스를 탈취하여 이루어질 수 있다.

그림 6 은 잠금 해제 이력 조회에 대한 공격 트리를 나타낸다.

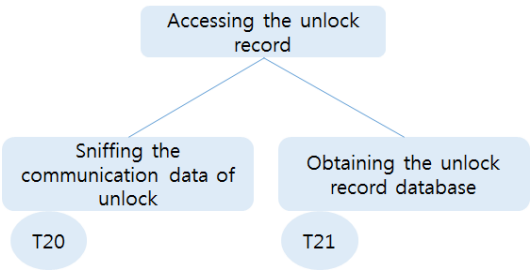


그림 6. 잠금해제 이력 조회에 대한 공격 트리
Fig. 6. Attack Tree for data disclosure of the log

3.4 위험도 및 대책 분석

위에서 도출한 시나리오에 대해 DREAD[12] 방법론을 이용해 위험도 분석을 수행하였다. DREAD는 Damage(피해의 정도), Reproducibility(재현 가능성), Exploitability(수행 가능성), Affected Users(영향 받는 피해자의 수), Discoverability (탐지 가능성)의 준말로 각 요소들의 위험도를 분석하여 위협의 영향이 어느 정도인지를 평가할 수 있다.

본 연구에서는 DREAD 각 요소에 대한 값을 1에서 5까지 측정하였으며, 이 값을 모두 더해 위험도를 정량적으로 산출하였다.

위험 대책으로는 위험 회피, 위험 전가, 위험 감소, 위험 수용 네가지 위험 대처 방식을 사용하며 위험도의 총합이 10점을 초과하면 위험 회피, 위험 전가, 위

표 2. DREAD 위험도 분석
Table 2. DREAD Risk Analysis

ID	Threat	D	R	E	A	D	Sum	Risk
A1	Unlocking a doorlock (Blutooth replay attack)	5	3	1	5	1	15	Reduction
A2	Unlocking a doorlock (Obtaining Blutooth secret key)	5	3	1	5	1	15	Reduction
A3	Unlocking a doorlock (bypassing Bluetooth key authentication)	5	3	1	5	1	15	Reduction
A4	Unlocking a doorlock (Obtaining a keypad password)	5	3	2	5	2	17	Reduction
A5	Unlocking a doorlock (bypassing keypad password authentication)	5	3	1	5	1	15	Reduction
A6	Unlocking a doorlock (Smart phone - doorlock pairing)	5	1	1	5	3	15	Reduction
A7	Unlocking a doorlock (Setting a new keypad password)	5	1	1	5	3	15	Reduction
A8	Disturbing unlock of a doorlock (Disturbing Bluetooth communication)	3	3	3	2	3	14	Reduction
A9	Disturbing unlock of a doorlock (Deleting a bluetooth key)	3	3	1	2	3	12	Reduction
A10	Disturbing unlock of a doorlock (Deleting a keypad password)	3	2	1	2	1	9	Retention
A11	Disturbing unlock of a doorlock (Attempting to exhaust the battery of a doorlock)	3	3	3	2	2	13	Reduction
A12	Manipulating the unlock record (Manipulating the server database log)	2	2	1	2	1	8	Retention
A13	Manipulating the unlock record (Manipulating the communication data)	2	3	1	2	2	10	Retention
A14	Manipulating the unlock record (Manipulating the GUI of a smart phone)	2	2	1	2	1	8	Retention
A15	Accessing the unlock record (Sniffing the communication data of unlock)	2	3	3	2	2	12	Reduction
A16	Accessing the unlock record (Obtaining the unlock record database)	2	2	1	2	1	8	Retention

험 감소를 수행하여 위험을 경감시키고, 10점 이하일 경우 위험을 수용하도록 하였다.

표 2는 DREAD 분석의 결과를 나타낸다. A1부터 A7까지는 공격자가 도어락 잠금 해제에 성공하여 침입에 성공하는 경우이고 DREAD 분석 결과의 점수도 15 이상이기 때문에 보안 모듈을 보완하여 위험을 감소시켜야 한다. 블루투스 통신 데이터를 암호화하여 통신하여 스니핑 공격이 불가능하게 하고, 키 교환 시 타임스탬프를 함께 보내 리플레이 공격이 불가하도록 조치한다. 또한 블루투스 키나 비밀번호 키 저장소를 공격자가 탈취하지 못하도록 하거나 탈취하여도 키를 알아낼 수 없게 하는 등의 기술적인 보완을 통해 위험을 감소시켜야 한다.

A8, A9, A11, A15는 도어락 잠금 해제에 성공하지는 못하지만, 사용자에게 상당한 위협이 될 수 있는 상황이고, DREAD 분석 결과의 점수도 10점 이상으로 위험을 감소시켜야 한다. 블루투스 통신 프로토콜이나, 구현 과정 상에서 발생할 수 있는 취약점을 보완하고, 잠금해제 이력 데이터를 암호화하여 송수신하여 스니핑이 불가하게 하는 등의 기술적인 보완을 통해 위험을 감소시킨다.

A10, A12, A13, A14, A16은 DREAD 분석 결과의 점수가 10점 이하로, 공격자가 얻을 수 있는 이득이 크지 않아 발생할 수 있는 확률이 낮고, 발생한다 하더라도 그 피해의 규모가 크지 않기 때문에 위험을 수용한다.

Ⅳ. 결 론

지금까지 블루투스 통신 기능을 가진 스마트 도어락에 대한 데이터 흐름도를 작성하고, 스마트 도어락 시스템에 대해 STRIDE 분석을 하여 발생할 수 있는 위협을 분석하고, 공격 트리를 그려 공격 시나리오를 작성한 다음, DREAD 방법론을 통한 위험도 분석을 수행하였다. 본 연구에서는 블루투스를 통한 잠금 해제 기능을 탑재하고, 사용자의 스마트폰을 통해 도어락 출입 이력을 조회할 수 있는, 기본적인 기능을 가진 스마트 도어락을 대상으로 위험도 분석을 수행하였다. 현재 시중에는 카메라가 탑재되어 방문자를 집주인의 스마트폰으로 보여 주거나, 와이파이로도 통신이 가능한 스마트 도어락도 출시되어 추후에는 이러한 보강된 기능을 가진 스마트 도어락에 대한 위험도 분석을 수행하여 발생할 수 있는 위협과 그에 대한 보완 방안을 찾는 연구도 이루어질 필요가 있다.

References

[1] Microsoft, *Threat Modeling,* Retrieved Jul. 22, 2020, from https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

[2] N. Akatyev and Joshua I. James, "Evidence identification in iot networks based on threat assessment," *Future Generation Comput. Syst.,* vol. 93, pp. 814-821, 2019.

[3] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Comput. Syst.,* vol. 56, pp. 719-733, 2016.

[4] O. Olawumi, A. Väänänen, K. Haataja, and P. Toivanen, "Security issues in smart homes and mobile health system: Threat analysis, possible countermeasures and lessons learned," *Int. J. Inf. Technol. and Secur.,* vol. 9, pp. 31-52, 2017.

[5] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "Threat and risk assessment methodologies in the automotive domain," *1st Workshop on Safety & Security Assurance for Critical Infrastructures Protection (S4CIP),* vol. 83, pp. 1288-1294, 2016.

[6] S. Kang, H. M. Kim, and H. K. Kim, "Trustworthy smart band: Security requirements analysis with threat modeling," *J. KIISC*, vol. 28, no. 6, pp. 1355-1369, 2018.

[7] L. Sion, K. Yskout, D. Van Landuyt, and W. Joosen, "Solution-aware data flow diagrams for security threat modeling," in *Proc. 33rd Annu. ACM Symp. Applied Computing (SAC '18),* NY, USA, 2018.

[8] Microsoft, *Microsoft Threat Modeling Tool 2016,* Retrieved Jul. 21, 2020, from https://www.microsoft.com/en-us/download/details.aspx?id=49168

[9] Microsoft, *STRIDE,* Retrieved Jul. 21, 2020, from https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

[10] MITRE, *Common Vulnerabilities and Exposures,* Retrieved Jul. 22, 2020, from https://cve.mitre.org

[11] B. Schneier, "Attack trees," *Dr. Dobb's J.,*

vol. 24, no. 12, pp. 21-29, 1999.
[12] M. Howard and D. LeBlanc, *Writing Secure Code,* 2nd Ed., Microsoft Press, pp. 93-95, 2002.

심 신 우 (Shinwoo Shim)

2007년 2월 : 포항공과대학교 컴퓨터공학 학사
2019년 2월 : 고려대학교 정보보호학 석사
2007년 1월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버 지휘통제, 임무영향평가, 사이버 위협 대응
[ORCID:0000-0003-0959-9200]

임 선 영 (Sun-Young Im)

2015년 2월 : 아주대학교 컴퓨터공학 학사
2017년 2월 : 아주대학교 컴퓨터공학 석사
2017년 1월~현재 : LIG넥스원 선임연구원

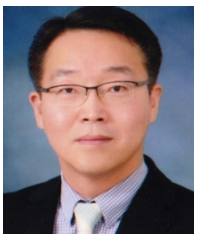
<관심분야> 사이버전, 사이버 위협 피해평가
[ORCID:0000-0003-4385-173X]

류 한 얼 (Han-Eul Ryu)

2009년 2월 : 한국항공대학교 컴퓨터공학 학사
2011년 2월 : 한국항공대학교 컴퓨터공학 석사
2011년 1월~현재 : LIG넥스원 선임연구원

<관심분야> 사이버 보안, 사이버 훈련체계, 시스템및 네트워크 가상화
[ORCID:0000-0003-2236-1766]

전 성 구 (Sung-Goo Jun)



1998년 2월 : 육군3사관학교 전산정보학 학사
2012년 2월 : 연세대학교 전산정보학 석사
2017년 2월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버전, 사이버 훈련체계, 사이버 지휘통제

김 태 규 (Taekyu Kim)

2000년 2월 : 중앙대학교 컴퓨터공학 학사
2006년 5월 : the University of Arizona 컴퓨터공학 석사
2008년 5월 : the University of Arizona 컴퓨터공학 박사
2010년 2월~현재 : LIG넥스원 수석연구원

<관심분야> Cybersecurity Killchain and TTP (Tactics, Techniques, and procedures), 임베디드 시스템 보안, System Modeling and Simulation