OTP를 이용한 디지털 도어락 모듈의 설계

고정현*, 고성민* ,김석준* ,김정호*
*한밭대학교 컴퓨터공학과
kjh5717727@naver.com,kkg555@naver.com,sjkim.skw.laa@gmail.com

Design of Door Lock Module using One Time Password Method

Joung-Hyun Ko*, Seong-Min Ko*,, Seok-Jun Kim* Jeong-Ho Kim*
*Dept. of Computer Engineering, Hanbat National University

요 약

사회에서 다양한 디지털 도어락 관련 범죄들이 꾸준히 늘어나면서 소비자들은 보안성이 강화된 도어락을 요구하고 있다. 이에 따라 도어락 시장도 보안성을 강화한 스마트 도어락을 개발하는 데 집중하고 있다. 본 연구에서는 사람이 보안을 위해 사용하는 OTP(One-Time-Password) 라는 검증된 암호시스템을 사용하여 비밀번호의 노출, 비밀번호의 분실의 위험이 없는 보안성과 편의성을 강화한 OTP 스마트 도어락 모듈을 구현하였다.

1. 연구의 필요성

2015년에서 2020년의 5년 간 주거침입의 통계는 주로 도어락을 통해 일어났다[1]. 주거침입을 하는 방법은 공동현관 벽에 적힌 비밀번호를 사용하는 방식, CCTV나 훔쳐보기를 이용하는 방식, 도어락에 묻은 지문을 이용하는 방식 등이 있다[1]. 이러한 도어락의 단점은 비밀번호가 고정적이고, 버튼을 사용해 개폐하는 방식이다.

본 연구에서는 주거침입의 방지를 위한 도어락을 해결하고자 OTP(One Time Password)를 사용하여 비밀번호를 유동적 변화를 주어 사용자가 계속 변경을 하지 않고, 기억하지 않아도 된다. 또한 도어락에 버튼을 이용하지 않고 사용자 스마트폰의 어플리케이션을 사용하여 개폐하는 시스템을 제안하고 구현하였다.

2. 관련 연구

2-1. One Time Password의 방법

OTP 방식은 시간 동기화(Time Synchronous), 이벤트 동기화(Event-Synchronous), 질의응답(Challenge-Response) 방식 등으로 나뉜다. 시간 동기화 방식으로 서버와 OTP토큰 간에 동기화된 시간을 기준으로 특정 시간 간격마다 변하는 OTP를 생성하는 방식이다. 이벤트 동기화 방식은 서버와 OTP 토큰이 동기화된 시간 대신 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 그리고 질의응답 방식은 서버가 제시하는 시도 값을 사용자가 알고리즘에 입력해 출력되는 값을 얻고 이를 응답 값으로 서버에 전송하여 자신을 인증하는 방식이다[2].

본 연구에서는 원거리 통신에서도 같은 시드값을 사용함으로써 디바이스와 도어락 간에 같은 값을 얻을 수 있다는 신뢰성을 보장받을 수 있기 때문에 시간 동기화 방식을 채택하여 설계하였다.

2-2. 디지털 도어락의 보안방식

디지털 도어락에 사용된 보안기술로는 네트워크 팩, 손바닥 터치기능, 허수기능 등이 있다[2].

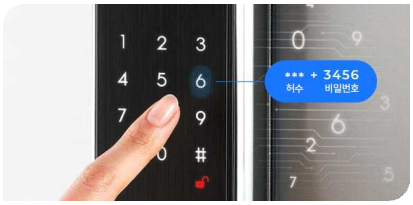
(그림1) 네트워크 팩 도어락

(그림 1)에 나타낸 네트워크 팩이란 홈 네트워크 보안 시스템이다. 기능으로서는 침입감지, 공동경비, 무감지모드, 비상연락, 정전발생알림 등이 있다.

네트워크 팩의 장점은 다양한 보안옵션을 제공하지만, 기존 도어락 외에 별도의 기능을 위한 모듈 등을 설치가 필요하다.

(그림2) 손바닥 터치 기능의 도어락

(그림 2)는 손바닥 터치 기능으로 지문을 확인하는 지능범들에 대비하여 방지하기 위한 도어락이다 이는 사용자가 번호를 입력하기 위해서는 손가락이 아닌 손바닥을 터치해야 문을 열수 있으며, 이로써 지문식별을 어렵게 하는 효과를 가질 수 있다.



(그림3) 허수기능 탑재 도어락

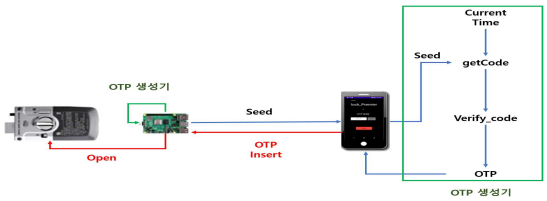
(그림 3)은 허수 기능은 사용자에게 노출될 가능성이 높은 일반 비밀번호를 보완하여 사전에 설정된 비밀번호 외의 허수를 추가 입력하게 함으로써 엿보기 범죄를 방지하는 기술이다. 그러나, 허수 기능은 사용자가 추가 번호를 설정하고 입력해야한다는 번거로움이 있으며, 일정한 패턴이 존재하기 때문에 결국 보안에 허점이 드러날 수 있다.

본 연구에서 설계한 OTP 도어락은 사람의 손이 닿지 않는 도어락이기 때문에 위에서 엿보기, 지문 노출에 관한 문제를 원천적으로 차단할 수 있다. 또한, 네트워크 기능을 지닌 하드웨어를 내장하고 있어 별도의 설치 없이 네트워크 기능을 통해 네트워크 팩 기능을 수행할 수 있다.

<표 1> OTP도어락과 기존제품간의 비교

	일반 도어락	디지털 도어락	블루투스 IoT 도어락	OTP 도어락
패스워드	고정형	고정형	고정형 / 미사용	OTP
입력방식	버튼 키패드	키패드	키패드 / 원격입력	원격입력
개폐방식	입력키 비교	입력키 비교	입력키 비교 / 원격 개폐	원격개폐
패스워드 노출성	상	상	중	하
지문 노출 유무	유	유	유	무
IoT 연계 유연성	무	무	유	유
가격	하	중	상	중

3. OTP 인증과정의 설계



(그림 4) OTP를 이용한 도어락의 개폐동작

본 연구에서 OTP 모듈을 구축하기 위해서 OTP 생성기의 알고리즘을 먼저 설계해야 한다. (그림 4)는 OTP를 활용한 도어락개폐의 동작을 나타내었다. 이 도어락에서 사용할 OTP는 시간동기화 방식으로 도어락을 제어하는 컨트롤러에서 OTP 생성에 필요한 시드(Seed)값을 먼저 생성한다. 생성된 시드 값은 Wifi 통신을 통해 사용자 디바이스로 전달된다[3]. 사용자 디바이스에서 받은 시드 값은 OTP Generator라고 하는 클래스 내부의 메서드가 실행되면서 OTP를 생성하게 된다. 먼저 getCode 메서드에서는 시드 값을 받아서 Base32로 코딩한 후, 현재 시간과 함께 코딩된 바이트를 넣어 verify_code를 반환한다. verify_code에서 OTP가 만들어지는데, 여기에서는 SHA256 해싱(hashing)기법을 적용하여 패스워드의 가용성과 기밀성을 확보한다[3][4]. 원하는 OTP 길이에 맞게 적절하게 자른(Truncate)후 생성된 일련의 int값이 결과적으로 반환되며, 이 결과 값이 OTP가 된다.

생성된 OTP는 사용자의 디바이스에 표시되며, 사용자는 이 OTP를 입력하여 전송버튼을 누른다. 이 설정한 OTP는 블루투스 통신을 통해 도어락 컨트롤러에 전달되며, 컨트롤러에서 같은 방식으로 생성된 OTP와 값을 비교하여 문을 개폐한다.

4. 하드웨어 설계

(그림 5) OTP 모듈이 연결된 도어락

(그림 5)는 OTP 개폐 시스템의 하드웨어를_나타내었다. 도어락에서 실시간으로 OTP를 생성하기 위한 수단으로 적합한 컨트롤러인 라즈베리파이를 이용하였다[5]. 본 연구에서 OTP 도어락에 사용되는 기본 기능인 OTP 개폐기능은 와이파이, 블루투스 통신, GPIO 제어를 사용한다.

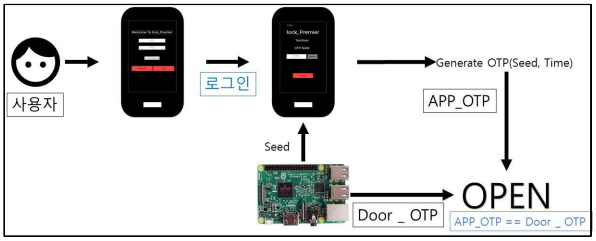
라즈베리파이에 내장된 JAVA 코드는 반복적으로 일정한 간격을 두고 시드 값을 생성한다. 이 시드 값은 와이파이를 통해 등록된 사용자 기기로 전송된다. 이와 동시에 전달된 시드 값으로 라즈베리파이, 사용자 디바이스에서는 동일한 OTP 생성기가 실행되며, 이로써 도어락과 사용자 디바이스에는 동기화된 동일한 OTP가 생성된다. 개폐장치는 가정에서 쓰이는 폼팩터를 그대로 사용하였다.

5. 소프트웨어 설계

5-1. 도어락 개폐 과정

(그림 6)은 도어락의 개폐과정을 나타내었다. 도어락과 와이파이연결이 성공할 경우 OTP를 생성하는 Seed 값을 생성하여 연결된 스마트폰에 보낸다. 스마트폰에선 받은 Seed 값과 시간 값으로 OTP값을 생성하며, Bluetooth를 통해 보낸다. 도어락은 스마트폰에서 보낸 OTP값과 도어락에서 생성한 OTP값을 비교하여 일치 시 문을 연다. 동시에 도어락에서 웹서버에 출입시간과 ID로 출입기록을 저장한다.

```
getSecretkey() --- Generate Seed
SendSeed() --- wifi Send
verify_code(seed, time) ---Generate OTP
if(RecevieOTP == GenerateOTP)
        OPEN DOOR
        SendLOG()
```



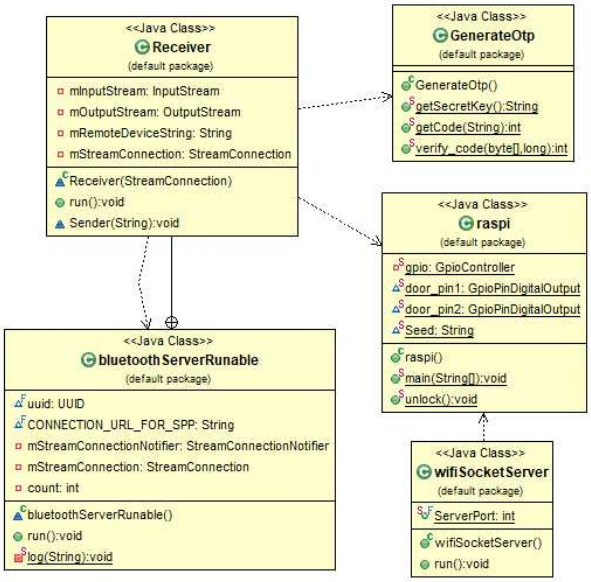
(그림 6) 도어락의 개폐과정

5-2 사용자 설정

사용자는 또한 마스터 사용자와 일반 사용자가 있다. 마스터 사용자는 처음 스마트폰과 연결한 사용자가 마스터가 된다. 그리고 일반 사용자를 추가해주는 기능이 있다. 마스터 사용자는 아이디와 비밀번호, 스마트폰 ID를 웹서버를 통해 등록 절차를 거친다. 그 후, 일반 사용자는 마스터가 준 아이디와 비밀번호를 사용하여 애플리케이션에 로그인할 수 있다.

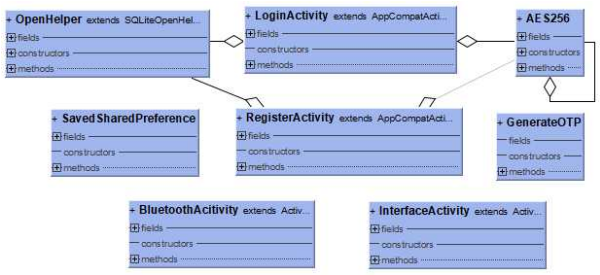
5-3. 설계

OTP의 생성과 원격통신은 JAVA(Open-jdk8)을 사용하였고, 애플리케이션은 Android 10을 사용하여 개발하였다[6].



(그림 7) DoorLock_RaspberryPi Class

Raspberry Pi에선 wifiSocketServer로 WifiSocket 서버를 생성하고 들어오는 사용자에게 Seed값을 준다. BluetoothServer로 블루투스 서버를 열고 사용자가 블루투스를 사용해 OTP를 보내면 Receiver로 받고 GenerateOTP를 사용해 도어락과 받은 OTP를 비교하여 도어락을 개폐를 결정한다[6][7].



(그림 8) 응용클래스

(그림 8)은 디지털 도어락의 연계한 SW응용 클래스를 나타내었다. Android에선 LoginActivity에서 로그인을 관리한다. 웹서버를 통해 ID와 패스워드

일치여부를 확인한다. 일치 시 OTP입력창(InterfaceActivity)으로 넘어간다. 만약 ID가 없을 경우 마스터 사용자가 Register로 넘어가 일반 사용자의 ID, PassWord, 스마트폰 ID를 웹서버에 등록한다. InterfaceActivity에선 먼저 wifit서버에 접속하여 Seed값을 받는다[7][8].

그 후, Seed값으로 GenerateOTP을 사용해 OTP 생성하고 OTP입력창에 띄운다. 버튼을 눌러 OTP를 보내면 BluetoothActivity를 호출하여 OTP를 전송한다. (그림6)에서 OTP는 Seed 값과 시간값을 합쳐 생성되며, 30초마다 OTP값이 재생성된다. 3 ~ 5번 이상 틀릴 경우 로그아웃을 시킨다. 만약 그러한 경우가 2연속 발생할 경우 웹서버에서 해당 ID를 삭제시킨다.

6. 기대효과

주거침입을 방지하기 위한 도어락이 위협을 받으며 2015년에서 2020년의 5년 간 주거침입 범죄율은 2배로 증가하였다. 이는 평범한 저장형 보안방식에 허점이 있음을 반증하는 결과라고 볼 수 있다. 또한 저장형이 아닌 블루투스를 이용한 원격 도어락은 높은 가격으로 책정되어 있다.

본 연구는 OTP 시스템을 적용한 도어락을 사용하면, 고정된 패스워드라는 불안정성을 해소할 수 있으며 단가를 낮추는 경제적인 설계가 가능하다.
기존 스마트 도어락보다 가용성과 기밀성을 확보한 OTP 도어락은 주거, 연구시설 등에서 널리 쓰이는 보안 제품이 될 수 있으며, 이는 사회적 치안의 질을 높이는데 기여를 할 수 있을 것이다.

7. 결 론

본 연구에서는 디지털 도어락의 보안성을 강화하기 위해 게임, 금융권 등 다양한 산업에서 개인 인증을 위해 사용하던 OTP 인증 방식을 적용하여 일정 간격으로 동적으로 생성되는 비밀번호를 사용하여 디지털 도어락에 설계하였다. 이는 기밀성, 가용성, 무결성을 포함한 안전성이 개선되어 비밀번호가 노출과 비밀번호의 망각이라는 두 가지 문제점을 해결할 수 있다. 추후 연구는 스마트폰의 생체인식기능과 OTP와 결합한 인증방식에 관한 연구를 진행할 계획이다.

참고문헌

[1] 주거침입범죄 통계 - 경찰청 범죄발생 및 검거현황(전국),http://kosis.kr/statHtml/statHtml.do.orgId=132&tblId=DT_13204_2011_211
[2] 서승현, 강우진, OTP 기술현황 및 국내 금융권 OTP도입사례. 정보보호학회지, 17(3), 18-25. 2007.
[3]네이버 D2 2차 인증 ,One Time Password의 방법 - https://d2.naver.com/helloworld/279640
[4] 히로시유키, 이재광,전태일,조재신역, 알기쉬운 정보보호개론, 인피닉스 북스, 2012.
[5] 김덕규, 최신 라즈베리파이 (Raspberry Pi)로 시작하는 사물인터넷 (IOT)의 모든 것 - 초보에서 고급까지 (상/하), 리얼오메가 컨설팅, 2016.
[6] 앨리엇 러스티 헤럴드, 강성용역 자바 네트워크 프로그래밍, 제4판, 오라일리 미디어, 2014.
[7] 박진솔, 권용민, 김준빈, 권민지, 장재민, 정우원. '원격 제어가 가능한 스마트 도어락', 한국컴퓨터정보학회 학술발표논문집, 28(2), 261-262, 2020.
[8] 이가연, 박용범, 이동수, 김진술, "라즈베리파이를 이용한 IoT 기반 스마트 도어락 개발",. 한국정보기술학회 종합학술발표논문집, 597-600, 2019.