가정용 디지털 도어락 장치의 보안성 강화에 관한 연구

조영준
한국폴리텍대학 분당융합기술교육원 임베디드시스템과
e-mail: samcho2017@kopo.ac.kr

A Study On Robustness Security of Digital Door Lock Device for Home

Young-Joon, Cho
Dept. of embeded system, Bundang Convergence Technology Campus of Korea Polytechnic

요 약

본 논문에서는 최근 BLE(Bluetooth Low Energy) 기술이 적용된 가정용 보안장치인 도어락의 보안성 강화를 위한 간단한 아이디어를 제안한다. 가정용 도어락은 숫자로 입력하는 비밀번호와 13.56MHz의 RF 카드 입력 방식을 병행하여 사용하고 있는데, 최근에 BLE 기술이 적용이 되어 개인이 휴대하고 있는 스마트폰의 앱을 통해 간단하게 도어락의 잠금장치를 해제할 수 있다. 하지만, 스니핑(Sniffing)을 통해 앱과 BLE 모듈간의 트래픽을 도청하여 잠금장치를 해제할 수 있는 기술로 인해 가정용 보안장치가 무용지물이 되고 있다. 국내에서 제조. 판매되고 있는 제품의 경우 70%이사의 제품이 이러한 문제가 있는 것으로 파악되고 있고, 이는 보안에 대한 이해의 부족으로 판단된다. 즉, 단수하게 BLE 모듈의 하드웨어 주소 등을 기억하여 단순한 통신 규약을 사용하고 있기 때문이다. 이에 본 논문에서는 금육기관에서 사용하고 있는 OTP (One Time Password) 방식을 적용하여 가변식별번호의 생성을 통한 가정용 보안장치의 보안성 강화에 대한 방향을 제안 한다.

1. 서론

국내에서의 아파트 등의 현관문에 사용하고 있는 잠금장치는 전통적인 기계식 방식의 도어락과 디지털 방식의 도어락으로 구분될 수 있다. 최근에는 IoT 기술이 접목된 디지털 도어락의 보급이 증가하고 있으며, 이는 다른 나라와 구분이 될 정도로 보급률이 높게 나타나고 있다. 디지털 도어락은 비밀번호 입력 방식과 RF 카드를 사용하는 방식이 주를 이루고 있으며, 최근에는 BLE 기술이 적용되어 IoT 기술의 기반의 디지털 도어락의 보급이 늘고 있다. BLE 방식의 디지털 도어락의 장점은 별도의 키를 휴대하고 있지 않아도 되지만, 최근에는 해킹에 대한 이슈로 사회적인 문제가 되고 있다. 국내 디지털 도어락 생산 업체의 5군대 중에 3군대의 제품이 보안이 취약하여 간단한 해킹 앱으로 잠금장치가 해제되는 문제가 언론을 통해서도 제기되기 되기도 했다. 업체의 보안에 대한 이해의 부족으로 간단한 스니핑(sniffing) 기술을 통해 통신 트래픽을 해킹하여 전송하기 때문에 쉽게 잠금장치를 해제할 수 있다. 단순히 등록된 BLE 장치에 간단한 프로토콜을 사용하여 도어락의 잠금장치를 해제하기 때문에 트래픽 해킹만으로도 쉽게 가정용 보안장치를 해킹할 수 있다.

이에 본 논문에서는 이러한 문제를 해결하고자 금융권에서 사용하고 있는 OTP(One Time Password) 방식을 적용하여 가변식별번호의 생성을 통해 가정용 보안장치의 보안성을 강화할 수 있는 방법은 제안하고자 한다. 도어락에서 생성된 보안키를 스마트폰의 앱을 통해 전달하고 생성된 보안키의 사용여부를 기억하여 이전에 사용되었던 보안키인지를 판단하는 방식을 통해 스니핑을 통한 해킹으로 잠금장치를 해제하는 것을 방지하도록 한다.

본 논문에서 사용한 BLE 모듈은 저전력의 Nordic사의 nRF52832 IC가 사용된 국내 제조사의 BLE 모듈을 사용하였고, 안드로이드 앱을 통해 BLE 모듈과의 통신을 구현하였다. 기본적인 암호 알고리즘은 AES-128을 사용하였으며, 명령어를 해독할 수 있는 키값은 앱을 통해 전달 받는 방식을 사용하였다. BLE 모듈은 도어락의 잠금장치를 해제할 때마다 새로운 인증키를 생성하여 앱에 전달이 되고, 차후 도어락을 해제할 경우에 이 인증키를 이용하여 도어락을 해제할 수 있는 기회를 얻을 수 있다. 또한, 인증키를 사용 여부에 대한 별도의 필드를 통해 재사용되는 인증키를 예방할 수 있어 기존 방식에 비해 보안성이 강화되는 결과를 얻을 수 있었다.