IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

권혁동*, 임지환*, 우재민*, 안규황*, 김도영*, 서화정*

*한성대학교 IT융합공학부

hdgwon@naver.com, jhim000@naver.com, vlxksla123@naver.com, tigerk9212@gmail.com, kyl123451@naver.com, hwajeong@hansung.ac.kr

Hyeokdong Kwan*, Ji-Hwan Lim*, Jae-Min Woo*,

Kyuhwang An*, Do-Young Kim*, Hwa-Jeong Seo*

*Division of IT engineering, Hansung University.

요 약

스마트폰을 중심으로 많은 사물인터넷 (Internet of Things, IoT) 기기들이 무선으로 연결되는데 있어서 빼놓을 수 없는 기술이 바로 블루투스이다. 또한, IoT 디바이스와 사용자 간에 블루투스 통신은 주로 Bluetooth Low Energy (BLE)를 통해서 이루어지는데, 블루투스 통신기술이 점차 발전함에 따라 기존 BLE의 보안 취약점은 더욱 두드러질 것이다. 현재까지 블루투스 접근성에 대한 연구는 꾸준히 이뤄지고 있지만, 블루투스 통신에서 데이터 보호에 대한 연구는 많이 부족하다. 따라서 본 논문에서는 IoT와 사용자 간 BLE 통신에서 데이터를 주고받을 때, 평문이 아닌 형태보존암호 (Format Preserving Encryption, FEA)를 통한 암호문을 주고받으며 통신하기 위한 효과적 방법에 대해 제안하고, Arduino에서 직접 테스트하여 성능을 측정한다.

I. 서론

블루투스 (Bluetooth)는 휴대기기를 서로 연결해 정보를 교환하는 단거리 무선통신 기술로서, 최신 IoT 기술에서는 여러 분야에 걸쳐 블루투스가 다양한 용도로 사용되는 추세이다. IoT의 Bluetooth 통신으로는 BLE를 사용하여 통신한다. BLE란 기존의 Bluetooth Classic보다 훨씬 적은 전력을 사용하여 Classic과 비슷한 수준의 무선 통신을 할 수 있다는 점이다. 이로 인해 다양한 IoT 디바이스들이 개발될 수 있는 원동력이 되었다. 현재 BLE를 사용한 IoT 통신은 비콘, 다중 IoT 센서 연결 또는 IoT와 사용자 간에 직접 통신 등에 사용되고 있다.

2016년에 Bluetooth SIG (Special Interest Group)는 6년 만에 블루투스 5.0을 선보여 기존 Bluetooth 4.0보다 통신 거리 4배, 통신속도 2배, Pairing 문제 해결 등 기존보다 진보된 무선통신 기술을 내놓았다 [1]. 하지만 이에 단점으로 기존의 블루투스 보안상 취약점이 많아 다양한 블루투스 공격 형태가 존재한다는 것이다. 블루투스 접근 상 문제도 Wi-Fi 보안의 WPA2 보안보다 취약하다. 또한, 아직 BLE 통신에서는 무결성, 가용성 이외에 통신하는 데이터를 보호하는 기밀성 연구의 진행이 매우 저조하여, 기술의 발전에 비교하면 데이터의 보안성이 매우 취약한 상태이다. 따라서 본 논문에서는 BLE 통신에서 IoT 센서와 사용자가 통신할 때, 데이터 보안을 위주로 정보의 기밀성 강화에 대한 방법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장 본론에서 BLE 연구 동향 및 제안방법에 대해 설명한다. 그리고 3장에서 IoT 환경에서 제안 기법에 대한 성능 평가를 수행하고, 마지막 4장에서 본 논문의 결론을 맺도록 한다.

I. 본론

2.1 관련 연구 동향

최근 IoT와 스마트 디바이스 간의 통신에 대한

보안이 중요하게 떠오르고 있다. 또한, 블루투스 무선통신상에서 연결 부분에 대한 보안 기술 관련 취약점이 발견되고 있다 [2]. 그리고 블루투스 기반 비콘은 현재 여러 IT산업에서 활발히 적용됨에 따라 관련 보안 방법들이 제안되고 있지만, 아직 활용 분야별 세부적인 해커의 공격에 대한 대응 방안과 보안 모듈 개발에 대해서는 추가적인 연구가 필요한 상황이다 [3]. 그림. 1은 원격 의료 서비스에 대한 공격으로 사용자가 애플리케이션으로 로그인 시 아이디, 비밀번호를 포함한 중요 정보가 공격자에게 평문으로 전송되는 취약점을 악용해, 사용자의 개인정보뿐만 아니라 정보를 바탕으로 병원의 의료정보에 대해서도 가로챌 수 있는 문제점을 보여준다. 사용자의 의료정보는 개인정보 중에서도 개인의 생명과 즉결된 정보이다. 이와 같은 위험성을 제거하고 사물인터넷 제품과 모바일 앱의 연동이 활성화되기 위해 2017년 11월 말부터 과학기술정보통신부와 한국인터넷진흥원에서 사물인터넷 보안 인증서비스를 시행했다.

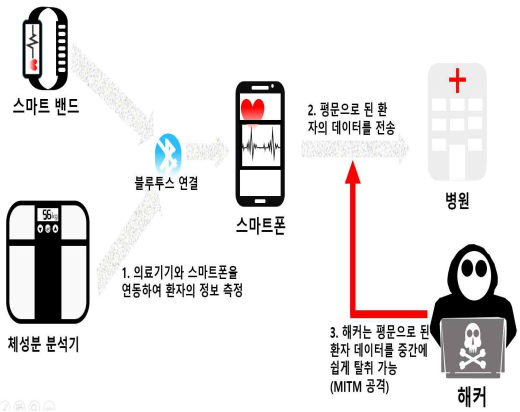
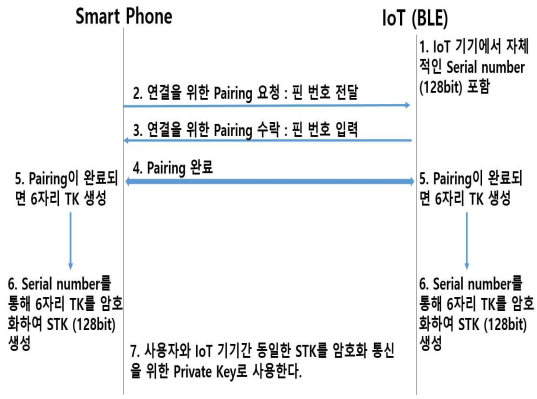


Fig. 1 Infringible scenario through hacking of hospital information system [4]

2.2 형태보존암호화를 통한 BLE 암호화 통신

본 절에서는 BLE 통신에서 IoT와 사용자 간에 안전한 통신을 할 수 있도록, 그림. 2를 통해 사용자와 IoT기기 간 Private Key 생성하는 방식을 소개하고, 그림. 3에서 생성한 Private Key를 활용하여 사용자와 IoT 기기 간 암호문 통신을 설명한다.

그림. 2의 방식은 IoT 기기에서 초기 설정된 Serial Number (128bit)를 갖고 있다(1). (2,3,4) 과정을 통하여 사용자와 IoT 기기 간 Pairing이 완료되면, 양 측에 동일한 6자리의 TK가 생성된다(5). 양 측에서 Serial Number를 Private Key로 사용하여 TK를 암호화하여 STK (128bit)를 생성한다(6). 최종적으로 사용자와 IoT 기기 간 동일한 STK를 암호화 통신을 위한 Private Key로 사용한다.



그

Fig. 2 Generation method of private key used for data encryption

림. 3은 통신할 데이터를 암호화하기 위해서 그림. 2에서 생성한 Private Key를 FEA의 TBC.KeyScheduling, TBC.TweakSchduling함수로 Round Key (RK), Round Tweak (RT)를 생성한다(1). 최종적으로 (2, 3, 4) 과정은 사용자가 데이터를 보낼 때 암호화하여 보내고 IoT에서 복호화하는 모습이고, (5, 6, 7) 과정은 IoT에서 사용자에게 암호화하여 데이터를 보내고, 사용자는 복호화하여 데이터 원본을 받는 모습이다.

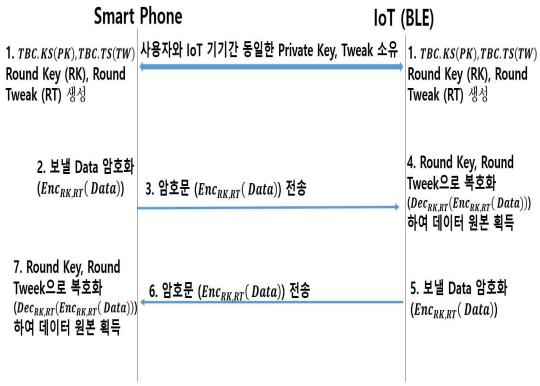


Fig. 3 Encrypted data communication between user and IoT device

II. 성능평가

본 장에서는 Arduino Mega에서 구현한 128bit의 키 길이를 갖고, 제 2형 TBC로 구현

한 FEA의 성능을 평가하고자 한다. 구현 및 테스트 환경은 표. 1과 같다. 구현은 형태보존암호 TTA 표준[5]을 참조하여 구현하였고, [6]의 Look Up Table (LUT) 사용 방식을 참조하여 FEA의 SBL과 DL 함수를 최적화하였다. 표. 2는 테스트 케이스 1000개에 대한 4byte 평문 암·복호화 속도를 비교한 표이다. Arduino에서 LUT (2KB)를 사용한 결과 최적화 전보다 8배 속도가 향상된다.

Table. 1 Test Environment for Arduino and Program

Processor	ATmega2560 (8 bit AVR)
Flash Memory	256KB
SRAM	8KB
EEPROM	4KB
Implementation Environment	Arduino IDE
FEA	Functions for TBC operation type 2
	Implementaion based on TTA-Standard (AVR-GCC)

Table. 2 FEA performance improvement in 4byte encryption and decryption before and after using LUT in 1,000 test cases

Method	**FEA**	**FEA (LUT)**
Timing	46s	5.75s

III. 결론

본 논문에서는 사물인터넷 BLE 무선통신 환경에서 무결성, 가용성 측면보다 연구 진행이 저조한 데이터 기밀성 측면에서 형태보존암호를 활용하여 이를 효과적으로 보완하는 방식을 제안하였다. 기존의 블록 암호는 데이터를 암호화하면 크기가 늘어나지만, 형태보존암호를 사용하면 평문과 암호문의 크기와 길이가 일치하기 때문에 데이터베이스 활용도 또한 매우 효과적이고, 한 번에 적은 양의 데이터를 보내는 BLE 통신에서 암호화하여도 데이터의 크기가 늘어나지 않는다는 매우 큰 장점이 있다. 또한, 8bit-AVR Arduino Mega에서 형태보존암호를 AVR-GCC로 직접 구현하여 성능 평가하였다. 향후 16, 32bit 프로세서 환경에서 추가로 형태보존암호 최적화 구현을 완료하고, 서비스를 구현하고자 한다.

Acknowledgement

이 성과는 부분적으로 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5075742). 본 연구는 부분적으로 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT 연구센터 육성지원사업의 연구결과로 수행되었음(2014-1-00743).

[참고문헌]

[1] Bluetooth. Bluetooth Core Specification Version 5.0 [Internet]. Available: https://goo.gl/4KXUc5.

[2] G. W. Kwon, S. H. Cho, “A Study on the vulnerability of Bluetooth Low Energy Security”, in *Proceeding of the 2016 Winter Conference of the Korean Institute of Communications and Information Sciences*, vol. 59, pp. 183-184.

[3] M. J. Kim, “An Analysis on the Number of Advertisements for Device Discovery in the Bluetooth Low Energy Network,” *Journal of the Institute of Electronics and Information Engineers*, vol. 53, no. 8, pp. 1151-1160, Aug, 2016.

[4] J. H. Jeon, "Study on the Security Threats Factors of A Bluetooth Low Energy," *Journal of the Korea Convergence Security Association*, vol. 17, no. 4, pp. 3-9, Oct, 2017.

[5] Telecommunications Technology Association. TTAK.KO- 12.0275. Format-Preserving Encryption Algorithm FEA [Internet]. Available: https://goo.gl/gqg53E.

[6] J. H. Lim, G. W. Na, J. M. Woo, and H. J. Seo, "Ransomware Prevention and Steganography Security Enhancement Technology Using Format Preserving Encryption," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22, no. 5, pp. 805-811, May, 2018.