In-body OTP : 이식형 의료 장치의 고유성 확보를 위한 체내형 One Time Password 생성 방법

안성규*,정혜림*,박기웅†

세종대학교 시스템 보안 연구실*, 세종대학교 정보보호학과†

In-Body OTP : One Time Password generation method for the ensure the uniqueness of the implantable medical device

Sung-Kyu Ahn*,Hyelim Jeong*, Ki-Woong Park†

* System Security Laboratory, Sejong University

† Department of Computer and Information Security, Sejong University

요 약

4차 산업혁명을 거치며 의학분야와 ICT 분야의 융합이 이루어지면서 다양한 형태의 의료방법이 탄생했다. 체내 이식형 의료 장치 분야는 ICT 분야와 융합되면서 임베디드 분야의 IoT 기반 기술로 발전하였다. 이러한 발전은 한편으로 해킹의 위험성을 초래할 수 있다. 이러한 문제를 해결하기 위해, 본 논문에서는 체내 이식형 의료 장치의 고유성 및 인증과정을 수행하기 위한 "In-Body OTP"기술을 제시한다. 이 기술을 통해 이식형 의료장치는 각각의 고유성을 가짐으로써 인증기술 등에 사용되어 이식형 의료 장치의 보안성 및 안전성을 확보할 수 있다.

I. 서론

4차 산업혁명 이후 의학분야와 ICT 분야의 융합이 급속도로 이루어지며, 의학과 IT가 접목된 제품이 제작되어 환자의 생명을 지키고 유지하는것에 큰 도움이 되고 있다. 일례로는 원격 로봇팔 수술, 환자 정보에 따라 의약품 자동 분배기, 인공지능을 사용한 암 진단 시스템, 체내에 이식·침습되어 사용하는 이식·침습형 의료장치(또는, 이식·침습형 의료장치, Implantable Mediacal Device)가 있다[1]. 이러한 기술은 임베디드 개념의 IoT기반의 기술로써 발전하면서 환자의 삶의 질을 높이고 고통을 줄여주는 긍정적인 역할을 수행하지만, 악의적인 목적으로 사용 될 가능성이 있다[2][3]. 특히, 이식형 의료장치는 환자의 신체 내부에 이식되어 사용됨으로 인해, 환자의 생명에 가장 가까운 의료기기로써 보안 측면 위험으로 인해 생명에 직접적인 영향을 끼칠 수 있는 부정적인 위험요소로써 사용될 수 있다. 하지만 이식형 의료 장치는 본래의 의료적 목표를 달성하기 위한 최소한의 컴퓨팅 파워 및 배터리 등으로 구성되어 있다. 이러한 자원 문제로 인해 기기에 직접 부가적인 보안 장치를 추가하기 위해서는 기존의 컴퓨팅 파워보다 높은 성능의 컴퓨팅 파워가 필요하며, 이는 곧 높은 전력 소모를 의미한다. 결국, 환자는 배터리 교체를 위해 몸속에 있는 기기를 꺼내야 하는 의료적 행위를 반복적으로 진행해야 하는 부정적인 결과를 초래한다[4].

이러한 문제를 해결하기 위해 본 논문에서는 이식형 의료기기에 보안 장치의 추가를 최소화하면서 보안성을 확보할 수 있는 '이식형 의료장치를 위한 체내 OTP 시스템'에 대한 개념인 'In body OTP"를 제시한다.

본 논문은 2장에서 본 논문에서 제시하는 '이식형 의료 장치를 위한 체네 OTP 시스템'의 개념을 제시한다. 마지막으로 3장에서 결론을 제시한다.

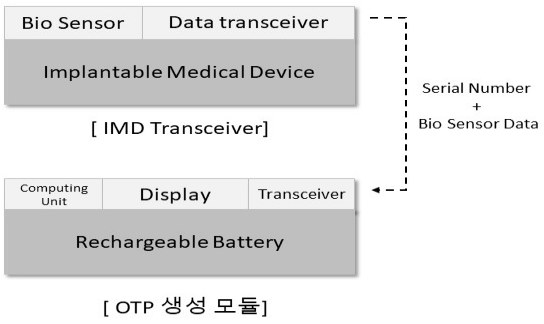
II. In body-OTP

본 장에서는 본 논문에서 제시하는 이식형 의료 장치를 위한 보안 기술과 관련된 연구와 체내 통신 기술 관련 연구에 대해 제시한다.

기본적으로 이식형 의료 장치를 인증하기 위한 시스템에는 In body-OTP가 환자에게 이식되는 과정에서 이식형 의료 장치의 고유번호와 환자의 일반적인 바이오 정보 (심장박동, 뇌파 등)을 획득하고 디지털화하여 저장된다.

1.1 In body-OTP 구조

In body-OTP의 구성은 크게 [그림1]과 같이 송수신기능이 부착된 IMD Transceiver와 송수신기가 장착된 OTP 생성 모듈로 구성되어 있다.

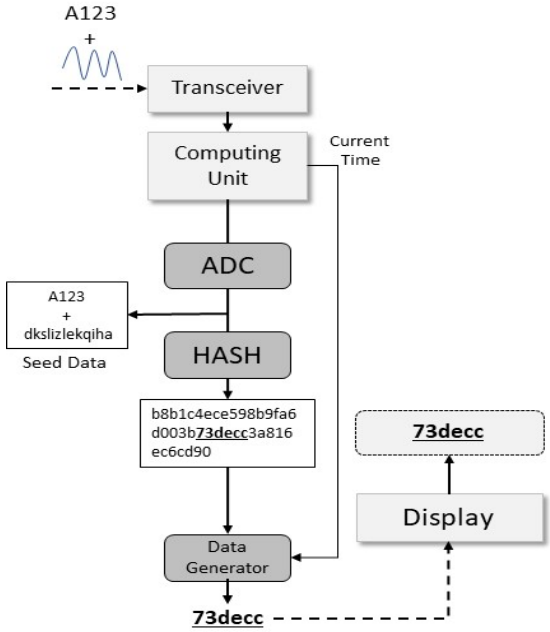


[그림 1] In body-OTP 구조도

IMD Transceiver는 이식형 의료 장치의 기본적인 의료 행위를 포함한 기기와 데이터 송수신 기능을 수행하는 Data transceiver 모듈이 추가로 구성되어 있다. OTP 생성 모듈은 배터리 및 MCU, 송수신 모듈, 컴퓨팅 모듈 및 디스플레이로 구성되어 있다.

1.2 In body-OTP 구현

IMD Transceiver는 기본적으로 이식형 의료 장치와 같은 기능을 수행한다. 만약 이식형 의료 장치의 인증이 필요한 시점이 되었을 때, [그림 2]와 같이 이용자는 OTP 생성 모듈의 수신 기능을 사용하여 체내 통신[5][6]을 통해 IMD Transceiver로부터 기기의 고유번호와 현재 측정되고 있는 신체 데이터를 수신한다. OTP 생성기는 수신한 기기의 고유번호와 디지털화된 바이오 데이터를 결합하여 OTP를 생성하기 위한 Seed 데이터값을 생성한 뒤, 해시 연산을 수행하여 최종값을 도출하고, 현재 시각을 기준값으로 하여 해시 데이터의 특정 부분을 추출한 뒤 디스플레이 모듈로 전달한다[7]. 디스플레이 모듈은 해당 값을 디스플레이에 출력하여 사용자가 확인할 수 있도록 한다. 디스플레이 출력의 최소 시간은 10초이며, 10초가 지난 뒤에는 다른 바이오 데이터를 이용하여 OTP를 생성한다.



[그림 2] OTP 데이터 생성과정

사용자의 OTP를 입력받은 시스템은 기존에 보유하고 있던 기기 고유번호와 바이오 데이터에 해시 연산을 반복해 가면서 해당 시간 단위에 해당하는 값을 도출하게 된다.

III. 결론

의학 분야와 ICT 분야의 접목으로 인해 많은 IoT 기반의 의료기기가 생성되고 있지만, 이러한 의료기기는 질병 치료 및 환자의 생명 유지 등과 같은 의료 목적으로 사용됨으로써, 기존의 ICT 기술을 동일하게 접목하기 어려운 실정이다[8]. 특히 이식형 의료 장치 분야의 경우, 환자의 질병을 모니터링 하고 특정 상황에 맞는

동작을 위해 최적화된 기기를 사용함으로 인해, 의료기기를 대상으로 하는 보안 기술을 적용하기 어렵다. 본 논문은 이런 문제점을 해결하기 위해 In body-OTP를 제시하였으며, 이 기술은 별도의 무선네트워크가 아닌 신체 네트워크를 통해 데이터를 송수신하고, 시간과 환자의 생체정보를 기준으로 인증데이터를 생성함으로써, 인증데이터가 무선환경에서 유출되거나 가로채기 당하는 문제점을 해결할 수 있다. 추후 연구로써는 본 논문에서 제시한 In body-OTP를 활용하여 이식형 의료 장치 인증 플랫폼 모듈을 구성하는 연구를 진행할 예정이다.

[참고문헌]

[1] 식품의약품안전평가원 “2018년 신개발 의료기기 전망 분석 보고서”, 2018.03.

[2] Tabasum, Aliya, et al. "Cybersecurity Issues in Implanted Medical Devices." 2018 International Conference on Computer and Applications (ICCA). IEEE, 2018.

[3] Papp, Dorottya, Zhendong Ma, and Levente Buttyan. "Embedded systems security: Threats, vulnerabilities, and attack taxonomy." 2015 13th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2015.

[4] Yaqoob, Tahreem, Haider Abbas, and Mohammed Atiquzzaman. "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices - A Review." IEEE Communications Surveys & Tutorials (2019).

[5] Li, Maoyuan, et al. "The modeling and simulation of the galvanic coupling intra-body communication via handshake channel." Sensors 17.4 (2017): 863.

[6] Sana Ullah, Henry Higgins, 곽경섭. (2008). 내장형 및 부착형 인체센서네트워크의 연구 동향 및 이슈. 한국통신학회지(정보와통신), 25(2), 18-25.

[7] M'Raihi, David, et al. "Totp: Time-based one-time password algorithm." Internet Request for Comments (2011).

[8] Belkhouja, Taha, et al. "Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack." 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018.