한국정보과학회
KOREAN INSTITUTE OF INFORMATION SCIENTISTS AND ENGINEERS
http://www.kiise.or.kr

Korea Computer Congress 2021

한국정보과학회 KCC2021

2021. 6. 23.(수) ~ 25.(금)

ICC 제주 & 씨에스호텔 & 온라인

Unimagined Futures:
Healing and Recovery with K-SW

주요행사

6.23

[특별세션]
- Green AI를 위한 뉴로모픽 컴퓨팅 세션

[Top Conference 특별세션]

[워크샵]
- 디지털 헬스 플랫폼 워크샵
- 빅 데이터 기술의 산업 동향 워크샵
- 머신러닝을 활용한 네트워크 기술 워크샵
- 지능형 자율주행 최신기술 워크샵
- AI 기반 도시 교통 최적화 기술 교류 워크샵
- 자율성장 휴먼증강 인지컴퓨팅 기술 교류 워크샵

6.24

[기조강연]
- Gabriele Kotsis 회장(ACM)
- 박종현 부원장(ETRI)

[특별세션]
- 비대면 시대와 보안 세션
- IT 정책 세션

[특별콜로키움]
- SW · AI 교육 혁신

[워크샵]
- 휴먼증강을 위한 단일 감각 정보의 변환 및 대외 지각 검증 워크샵
- 차세대 AI 예타 후속방안 회의
- 지속가능한 디지털 경제 실현을 위한 기술 R&D 정책 워크샵
- 준지도학습 과제 3차년도 워크샵
- 암흑데이터극한활용연구센터 하계 워크샵
- 여성연구자들이 함께 할 K-SW 미래 워크샵

6.25

[특별세션]
- 추천시스템 최신 기술 동향 세션
- 신진연구자 세션

[특별콜로키움]
- 초우수 SW 육성

[워크샵]
- 제주대 SW융합 컨퍼런스
- 인공지능연구소 기술 융합, 자율주행서비스 전략 워크샵
- 현대자동차의 데이터와 AI기술 워크샵

후원

OKESTRO NAVER Jeju CVB LINE N-N SAMSUNG 삼성SDS SUNJESOFT HYUNDAI
kakao Microsoft DMOA DREAMMARK1 TmaxSoft Gridwiz SK하이닉스 쌍용정보통신
CUBRID 지능정보산업협회 올포랜드 INFRANICS SK broadband 주식회사 투 비 콤 LG히다찌

다중 메모리 소자 구조 방식을 활용한 IoT 의료장치의 내부 데이터 유출방지 메커니즘 디자인

안성규[1O], 정혜림[1], 박기웅[2†]
[1]서울시 광진구 능동로, 세종대학교 시스템보안 연구실
[2]서울시 광진구 능동로, 세종대학교 정보보호학과
yiimfn@gmail.com[1O], hyello13@gmail.com[1], woongbak@sejong.ac.kr[2]

Design of a system to prevent data leakage inside IoT-based medical devices using the volatile characteristics of memory devices

Ahn Sung-Kyu[O], Hye Lim Jeong, Ki-Woong Park
Department of Information Security, Sejong University, Seoul, South Korea

요 약

최근 디지털 분야와 의료분야의 융합적 발달로 다양한 형태의 디지털 의료장치 및 디지털 헬스케어 시스템이 출시되고 있다. 특히 IoT 분야와 의료분야의 융합으로써, IoT 기반의 임베디드 의료장치의 발달이 활발하게 지속되고 있으며, IoT 의료장치로 인해 질병이 있는 환자들의 삶의 질이 향상되었다. 이러한 IoT 임베디드 의료장치의 발전은 IoT 환경에서 발생 가능한 보안 위협들이 의료장치에서도 발생 가능하다는 단점을 야기할 수 있다. IoT 의료장치는 컴퓨팅 리소스 및 전력 자원 등의 문제로 인해 기존 IoT 시스템의 솔루션을 적용하기 어렵고, 의료장치 특성상 사용자에게 이식되거나 침습 형태로 사용될 수가 있어, 위협으로 인해 보안 위협 상황이 발생할 경우, 환자의 생명에 지장을 줄 수 있을 정도로 치명적인 영향을 끼칠 수 있다. 본 논문에서는 이러한 문제를 해결하기 위해 컴퓨팅 리소스와 전력 사용량이 기존의 솔루션보다 작은 IoT 기반의 의료장치를 위한 보안 시스템을 제시한다. 본 논문에서 제시하는 시스템은 임베디드 시스템에 이식성이 높은 메모리 관리 모듈을 사용하여 물리적으로 분할된 메모리 영역을 정보보호를 위한 영역으로 적용함으로써 개인정보 보호 또는 데이터 유출방지를 효율적으로 관리하는 방법을 사용한다. 또한, 본 논문에서 제시하는 시스템을 확장하여 다양한 임베디드 시스템에 적용하여 효율적이고 경제적인 보안 솔루션으로 발전할 것으로 예상한다.

1. 서 론

의료 및 헬스케어 관련 분야는 규모가 빠르게 성장하며 또 하나의 의료혁신으로 발전하고 있다. 과거의 의료혁신 경우, 의학계 내부, 약학, 생명공학 등 의학계와 인접한 분야의 발전으로 인해 진행되는 것에 반해, 최근 발생하고 있는 의료혁신은 발전된 디지털 기술을 활용하여 의료기술과 헬스케어의 활용분야를 넓히고 있다[1]. 의료의 패러다임이 디지털 의료 및 디지털 헬스케어 모델로 변화하면서, 의료분야에서의 가치는 질병 중심의 의료행위보다 환자 중심의 의료행위로 최우선으로 변화되었다[2]. 이로 인해, 디지털 의료장치 산업은 전통적인 하드웨어 및 첨단 기술 기반의 융복합 의료장치 개발뿐 아니라 의료용 소프트웨어 및 하드웨어의 발전을 가속화 하고 있다. 하지만 의료용 소프트웨어 및 하드웨어의 발전은 필연적으로 의료용기기를 대상으로 하는 디지털 위협을 내포하고 있다[3][4].

의료장치를 대상으로 하는 디지털 위협의 예로써, IoT 기술이 접목된 임베디드 기반의 의료장치를 대상으로 하는 공격이 있다. 최근 IoT 의료장치의 발달로 인해 임베디드 환경을 기반으로 하는 의료장치의 종류가 다양해졌고, 사용자는 이러한 임베디드 의료장치 및 헬스케어 장치를 통해 건강을 유지하고 삶의 질을 높일 수 있다. 하지만, 사용자와 밀접한 거리를 유지하며 사용되는 임베디드 기반의 의료장치의 경우, 사용자의 의료행위기록, 사용자 위치 정보, 사용자 신체 정보 등 사용자에 대한 개인정보나 사용자의 의료정보와 같은 민감정보를 저장하거나 활용할 수가 있다[5].

본 논문에서는 이러한 임베디드 기반의 의료장치에서 발생하는 데이터 유출의 위협을 해소하기 위해 임베디드 의료장치의 메모리를 물리적으로 분리하여 관리하고, 전원공급 관리 모듈을 제어함으로써, 분리된 메모리에 저장된 사용자의 개인정보 및 의료정보와 같은 민감정보 등 의료장치의 데이터 유출을 최소화하는 방법을 제시한다.

2. 관련 연구

사용자와 밀접한 환경의 임베디드 의료장치의 위협은 사용자에게 치명적인 위험요소로써 악용될 수 있다[6]. 이러한 임베디드 의료장치 환경에서 발생할 수 있는 위협을 해

† 교신저자

* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (No.2019-0-00426, IoT 기반 이식-침습형 고위험 의료장치를 위한 능동형 킬 스위치 및 바이오 마커 활용 방어 시스템 개발,30%)과 2020년도 한국연구재단 연구과제의 지원을 받아 수행된 연구임(NRF-2020R1A2C400273, IoT 침해사고 대응을 위한 지능형 분석 플랫폼 기술 연구, 70%)

소하기 위한 연구는 기존에도 지속 되어 왔다. 의료 목적을 위한 임베디드 기반의 의료장치는 그 특성에 따라 기기를 구성하고 있는 리소스 및 전력 자원 등에 민감하여 보안 솔루션과 의료 행위를 위한 모듈을 동시에 활용하기 어렵다. 따라서 기존의 연구들은 별도의 보안장치를 별도로 추가함으로써, 임베디드 의료장치의 리소스와 전력 자원 등에 영향을 최소화하는 아키텍쳐를 제시했다.

'Stydis et al' [7] 은 임베디드 기반의 의료장치에 추가적인 보안 모듈을 적용하는 Smart Implant Security Core(SISC) 환경을 제시하였다. 본 연구에서 제시하는 보안 모듈은 RF 신호에서 수집한 에너지로써 전력을 확보하고 외부에서 전송되는 신호를 자체적으로 처리한 뒤, 인증된 신호만 임베디드 의료장치로 전달하는 메커니즘을 수행한다. 이를 통해 임베디드 의료장치를 대상으로 하는 공격 중 신호를 연속적으로 보냄으로써 배터리 소모를 가속화하는 배터리 소모 공격을 방지할 수 있다. 본 연구는 임베디드 의료장치 환경에서 보안을 위해 Proxy 개념의 보안장치를 추가하는 기존 연구들과 달리 의료장치 내부에 모듈을 추가하여 모듈이나 기기가 외부로 노출됨으로써 발생하는 보안 위협을 최소화했다. 본 연구에서 제시하는 보안 모듈을 추가로 내장하는 방법은 보안 위협을 방지하기 위한 모듈이 외부에 있는 방식보다 안전할 수 있고, RF신호에서 에너지를 수집하여 운용함으로써, 임베디드 의료장치의 리소스나 전력 자원에 영향을 주지 않는다는 장점이 있다. 하지만 본 연구와 같이 보안 모듈을 추가하는 환경에서는 임베디드 의료장치에 대한 공격이 발생하였을 때, 내부에 저장된 의료데이터 및 개인정보의 유출을 차단하기 위해 내부적으로 설정된 정책에 의해 동작할 수밖에 없다는 단점이 있다. 이러한 문제를 해소하기 위해, 본 논문에서 제시하는 시스템은 추가적인 모듈의 추가를 최소화하고 물리적인 메모리의 휘발성 특징을 이용하여 데이터를 삭제함으로써 내부 데이터의 유출에 빠르게 대처할 수 있다는 차이점이 있다.

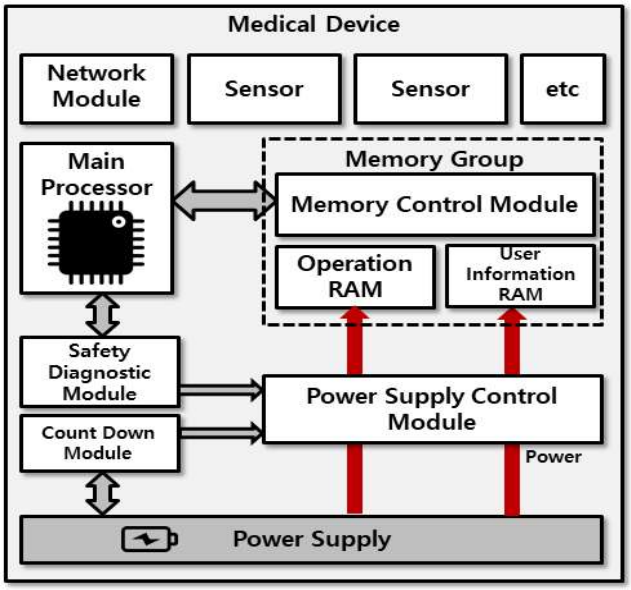

그림 1 메모리 분할을 통한 개인정보 보호 플랫폼

3. IoT 의료장치의 내부 데이터 유출방지 메커니즘

본 논문에서 제시하는 시스템은 임베디드 의료장치의 의료데이터 및 개인정보를 포함하는 시스템의 보안 효율성을 높이는 것을 목표로 한다. 본 시스템이 적용되는 의료환경의 위협요소들은 다음과 같이 정의할 수 있다.

1. 사용자가 사용하고 있는 의료장치에서 직접 데이터를 추출하거나 유출되는 경우.
2. 사용기한이 초과하여 폐기된 의료장치 및 센서 등의 고장 등으로 교체된 의료장치에서 사용자 정보를 추출하는 경우

3.1. 기본 디자인

본 논문에서 제시하는 전체 시스템의 구조는 [그림 1]과 같다. [그림 1]과 같이 물리적으로 분리된 다중 메모리의 환경을 기반으로 '일반 메모리 영역'과 '사용자 정보 메모리 영역'으로 구분한다. [그림 1]과 같이 사용자가 사용하는 의료장치의 펌웨어는 기기 자체의 전원 공급 관리 모듈을 제어할 수 있다. 펌웨어 기본 방어 메커니즘 또는 네트워크를 통해 중앙 제어 시스템에서 사용자 정보 삭제 요청이 발생하는 경우, 펌웨어는 전원 공급 관리 모듈을 제어함으로써, 사용자 정보 메모리의 전원을 일시적으로 차단할 수 있다. 전원이 차단됨으로써, 의료장치에서 활용되고 있던 사용자 정보와 관련된 연산 및 데이터들은 휘발됨으로써, 정보의 유출을 차단한다.

또한, 펌웨어 내부에 설정된 의료장치의 사용 기간이 초과하거나 의료장치를 구성하고 있는 물리적인 구성요소의 고장으로 인해 의료장치를 교체가 필요한 경우에도 사용자 정보 메모리를 초기화하여 의료장치 내의 펌웨어를 포함한 사용자의 정보 유출을 방지한다.

3.2. 위협 요소 해결 방안

본 절에서는 3장에서 정의한 2가지의 위협요소에 대해 본 논문에서 제시하는 시스템을 적용하여 해결하는 방안에 대해 제시한다.

3.2.1 물리적으로 분할된 메모리를 위한 데이터 분할 알고리즘

본 논문에서 제시하는 시스템은 물리적으로 분할된 2개 이상의 메모리 장치를 사용함으로써 데이터를 보호하는 메커니즘이다. 이러한 메모리 구성을 효율적으로 사용하기 위해, 2개 이상의 메모리를 1개의 메모리 영역처럼 사용할 수 있는 메모리 관리 모듈을 사용한다. 본 시스템은 [그림2]와 같이 임베디드 시스템의 펌웨어 환경에서 보안 메모리에 적용되는 추가적인 보안 함수를 사용한다. 임베디드 시스템 펌웨어 개발 단계에서 보안용 함수를 사용함으로써 메모리 관리 모듈을 통해 일반 운영 데이터와 민감정보를 분리하여 처리 및 저장할 수 있다. 보안 함수를 사용하여 사용자 정보 메모리 영역에 저장된 민감 데이터는 서명 과정을 통해 데이터 복사 및 이동을 관리한다. 만약, 보안 함수를 통해 생성된 민감 데

이터가 일반 메모리 영역으로 전달되는 경우, MPU(Memory Protection Unit)는 데이터를 삭제한 뒤 의료기기를 보안 위협 상황으로 처리한다. 본 시스템에 내장된 안전점검 모듈 또는 외부에서 발생하는 데이터 유출 위협 경고를 전달받는 경우, 전원공급 관리 모듈을 조작하여 유저 정보 메모리의 데이터를 강제적으로 삭제한다. 따라서, 공격자에 의해 펌웨어의 권한이 탈취당하더라도 메모리 내 정보 유출을 방지할 수 있다. 이후, 의료장치가 안전하다고 판단되는 경우, 다시 유저 정보 메모리에 전원을 인가하여 유저 정보 메모리를 활용한다. 만약 의료장치가 외부 위협에 지속해서 노출된 경우, 의료장치는 일반 메모리만을 사용하며, 의료장치의 안전이 보장되는 환경이 구성될 때까지 의료장치의 기본적인 동작만을 제한적으로 수행하며 지속해서 사용자와 관리 서버에 경고함으로써 안전한 환경 구성을 요청한다.

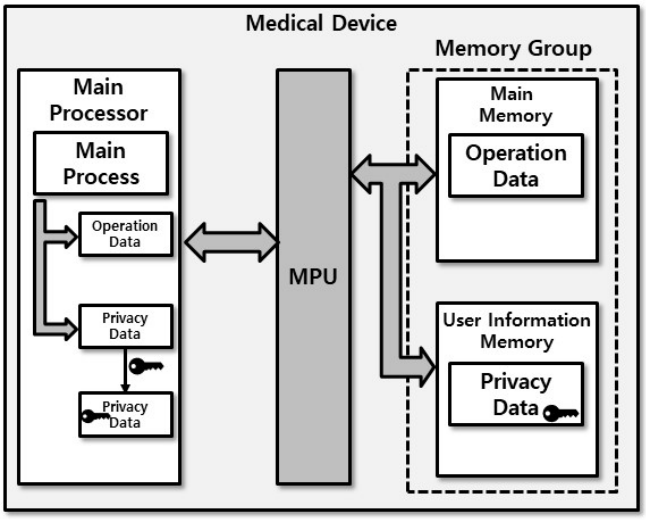

그림 2 데이터 타입에 따른 분할 메모리 구동 방식

3.2.2 제한된 사용시간 정책에 따른 의료장치 폐기 관리 메커니즘

임베디드 시스템 기반의 의료장치는 사용자의 안전을 위해 사용기한이 제한될 수가 있으며, 그 예로 사용자 신체에 부착하여 인슐린을 주입하는 인슐린 주입 펌프 등이 있다. 의료장치의 제한 기간을 초과하게 되는 경우, 사용자는 의료장치가 정상적으로 동작하더라도 해당 의료장치를 폐기하고 새로운 의료장치를 부착하는 형태로써 건강관리를 지속한다. 이러한 환경에서 공격자는 사용자가 폐기한 의료장치를 습득함으로써, 내부에 존재하는 사용자의 정보와 의료정보를 추출할 수 있는 위험이 있다.

이러한 위협을 해소하기 위해 본 시스템은 카운트 다운 모듈을 이용한다. 카운트 다운 모듈은 지속적으로 저장된 값이 감소하는 메커니즘을 활용한다. 사용자가 의료장치를 정상적으로 이용하고 있는 상황에서는 펌웨어는 카운트 다운 모듈에 지속적으로 신호를 전송하여 저장된 값이 감소하는 것을 제어하여 사용자는 의료장치를 지속적으로 사용할 수 있다. 만일 의료장치의 사용기한을 초과하여 사용하거나, 내부적인 고장으로 인해 사용자가 의료장치를 제거하는 경우, 펌웨어는 카운트 다운 모듈에 신호를 보내지 않으며, 카운트 다운 모듈은 저장된 값이 모두 감소할 때까지 동작한다. 카운트 다운 모듈 내 저장된 값이 모두 감소하여 0이 되면 카운트 다운 모듈은 전원 공급 관리 모듈을 제어하여 일반 메모리 및 유저 정보 메모리의 전원공급을 모두 차단함으로써, 내부에 저장된 코드 및 동작하고 있던 펌웨어들을 모두 삭제함으로써, 폐기되거나 고장난 의료장치에서 발생 가능한 데이터 유출을 방지한다.

3. 결론

디지털 분야와 의료분야의 융합을 통해 새로운 의료혁신으로 발전하였다. 이러한 의료혁신을 통해 IoT 의료장치 또는 디지털 헬스케어 등 다양한 형태의 디지털 의료행위 요소가 활용되고 있다. 하지만, 디지털 분야의 융합된 의료장치에는 디지털 분야의 위협요소까지 내포하게 되었다. 하지만 디지털 의료장치의 특성상, 기존의 임베디드 시스템에서 활용되고 있는 보안 솔루션을 그대로 적용하기에는 컴퓨팅 리소스 및 전력 부족 등의 문제가 있다. 따라서 본 논문에서는 이러한 문제를 해결하기 위해 하드웨어적으로 분리된 메모리 형태의 임베디드 시스템 의료장치 메커니즘을 제안하였다. 본 시스템을 의료장치뿐만 아니라, 일반 임베디드 시스템 등에 적용할 경우, 기존의 솔루션보다 자원 소모를 최소화하며 데이터 유출을 방지할 수 있을 것으로 예상한다. 추후 연구로써, 본 논문에서 제시한 시스템을 하드웨어 형태로 제작함으로써, 실제 임베디드 의료장치의 데이터 유출방지 효과 실험을 진행할 예정이다.

4. 참고문헌

1. Chacko, Anil, and Thaier Hayajneh. “Security and privacy issues with IoT in healthcare.“ EAI Endorsed Transactions on Pervasive Health and Technology 4.14, 2018
2. 최윤섭, “디지털 헬스케어:의료의미래”, 2020
3. Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. “Security and privacy issues in implantable medical devices: A comprehensive survey.“ Journal of biomedical informatics 55, 272-289, 2015
4. NAWIR, Mukrimah, et al. Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED). IEEE, p. 321-326, 2016
5. Zheng, Guanglou, et al. “Ideas and challenges for securing wireless implantable medical devices: A review.“ IEEE Sensors Journal 17.3, p562-576, 2016
6. A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbea’H and S. Alrabaee, “Security Vulnerabilities Detected in Medical Devices,“ 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), Dubai, United Arab Emirates, 2020.
7. Zheng, Guanglou, et al. “Ideas and challenges for securing wireless implantable medical devices: A review.“ IEEE Sensors Journal 17.3, 562-576, 2016