http://dx.doi.org/10.14400/JDC.2014.12.5.249

함수 기반의 체내 삽입장치용 보안 인증프로토콜 검증

배우식*제1저자, 한군희**
아주자동차대학*, 백석대학교 정보통신학부**

Verification of a Function-based Security Authentication Protocol for Implantable Medical Devices

WooSik Bae*1st Author, KunHee Han**
Dept. of AIS Center, Ajou Motor College*
Dept. of Information Communication Engineering, Baekseok University**

요 약 최근 USN 기술의 발전으로 의료기술 분야에서 서비스를 받을 수 있는 체내 삽입장치 통신기술이 많은 발전을 하고 있다. 체내 삽입장치(Implantable Medical Device)는 환자와 장비사이에 무선으로 전송되는 구간이 있어서 외부 공격자의 해킹으로 인한 환자의 개인 의료정보 유출사고로 프라이버시 침해 발생이 우려되고 있다. 또한 환자의 의료 정보를 조작할 경우 심각한 의료 문제가 발생할 수 있다. 본 논문에서는 체내 삽입장치에 RFID/USN 기술을 이용할 때 공격자의 공격에 안전한 인증프로토콜을 제안한다. 해시함수 기반으로 연산하며 세션키와 난수를 도입하여 재 암호화를 방지하고 스푸핑공격, 정보노출 및 도청공격에 안전하며 이를 증명하기 위해 정형검증 도구인 Casper/FDR 도구를 이용하여 보안성을 검증 실험하였으며 안전함이 확인되었다.

주제어 : 인증프로토콜, RFID 보안, Casper, RFID 인증, 모델검증

Abstract Recent advancement of USN technology has lent itself to the evolving communication technology for implantable devices in the field of medical service. The wireless transmission section for communication between implantable medical devices and patients is a cause of concern over invasion of privacy, resulting from external attackers' hacking and thus leakage of private medical information. In addition, any attempt to manipulate patients' medical information could end up in serious medical issues. The present study proposes an authentication protocol safe against intruders' attacks when RFID/USN technology is applied to implantable medical devices. Being safe against spoofing, information exposure and eavesdropping attacks, the proposed protocol is based on hash-function operation and adopts session keys and random numbers to prevent re-encryption. This paper verifies the security of the proposed protocol using the formal verification tool, Casper/FDR.

Key Words : Authentication protocol, RFID security, Casper, RFID authentication, Model Checking

Received 7 March 2013, Revised 16 April 2014
Accepted 20 May 2014
Corresponding Author: KunHee Han(Baekseok University)
Email: hankh@bu.ac.kr

ISSN: 1738-1916

1. 서론

최근 USN 기술발전과 함께 센서 및 측정장치가 소형화되어 많은 산업분야에 응용되고 있으며 의료기기 분야에도 개발이 활성화 되고 있다[1]. 이제는 언제 어디서나 의료서비스를 지원 받을 수 있으며 의료 서비스를 받기 어려운 섬, 산간 오지의 환자에게도 체내정보 데이터를 수시로 파악할 수 있다[2]. 따라서 최근 이러한 보안 문제를 해결하기 위해서 많은 연구자들이 의료용 체내삽입장치의 보안통신을 위해서 활발한 연구를 하고 있다[3][4]. 환자 신체에 부착된 체내삽입장치에서 발생되는 생체 의료정보의 안전성을 높이기 위해 의료 장비에게 키 분배 방식의 프로토콜을 통해 사전에 암호키를 분배하는 방식이 연구되고 있다[5][6]. 또한 기존의 프로토콜 연구는 수학적인 정리 증명으로 대부분 연구가 되어 타 연구자에 의해 취약성이 발견되는 프로토콜이 제안되고 있는 실정이다[7][8]. 본 논문에서는 정형검증 분야에서 많이 사용하는 Casper/FDR[9][10] 도구를 사용하여 제안한 프로토콜을 검증실험 하였으며 보안적으로 안전한 프로토콜임이 증명되었다. 본 논문의 구성은 다음과 같다 , 2장에서는 관련 연구로 u-헬스케어 서비스와 CASPER/FDR에 대하여 알아본다. 3장에서는 인증프로토콜을 제안하고, Casper/FDR을 이용하여 실험 검증하며 4장에서 실험 결과의 안전성을 확인하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 u-헬스케어

최근 유비쿼터스 기술의 등장으로 환자가 병원에 직접 가지 않고 환자의 집, 사무실 또는 이동중에도 의료서비스를 받을 수 있는 u-헬스케어 서비스의 기술연구가 다양하게 진행되고 있다. 즉 최근 이슈가 되고 있던 모바일 의료 서비스 보다 앞선 모델로써 환자가 생활공간 속에서 다양한 의료 센서 및 기기를 통해 수집된 생체정보를 기반으로 의료서비스 시스템을 통해 의료 결과를 받을 수 있는 서비스를 말한다. 일반적으로 고 위험군의 임산부, 만성 질환자, 심장 질환자 등을 대상으로 일상생활 속에서 환자를 지속적으로 모니터링하고 이를 통해 질병을 판단 및 예측으로 응급상황 발생 시 서비스를 제공할 수 있다. 이 외에도 u-헬스케어 정보에 대한 다양한 서비스가 존재함에 따라 시스템 권한이나 효율성, 보안문제 등이 중요시 되고 있다. 이는 환자의 생명 및 안전에 매우 민감한 부분으로써 보안 및 안정성 평가는 매우 중요한 부분이다.[11]

2.2 CASPER/FDR

Casper는 CSP(Communication Sequential Process)방식으로 프로토콜을 명세하기 쉽게 개발 되어진 컴파일러이다. Casper(a Compile for the Analysis of Security Protocols)[7]은 기존의 CSP[12] 언어를 이용한 정형명세 과정에서 오류가 생겨 설계 및 분석을 어렵게 진행하는 단점이 있었다. 이를 개선하기 위해 보안프로토콜의 동작을 간략히 설계할 수 있도록 개발된 프로그램이 Casper이다.

명세 방법은 (Defines the agents, variables, and functions in the protocol), (Represents each agent as a process), (Shows all the messages exchanged between the agents), (Specifies the security properties to be checked), (Defines the real variables, in the actual system to be checked), (Defines all the functions used in the protocol), (Lists the agents participating in the actual system with their parameters instantiated), (Specifies the intruder's knowledge and capabilities) 등을 명세한 후 프로그램을 실행 시키면 CSP 문서로 변환시켜 준다. 이렇게 변환된 CSP 문서를 FDR(Failure Divergence Refinements)[9] 프로그램을 이용하여 보안성과 인증속성 같은 보안속성을 만족하는지 검증하며 FDR 에서는 safety 검증, deadlock 검증, livelock 검증을 확인하며 보안상 취약점이 발견 되면 어떤 공격 시나리오가 가능한지 보여주어 취약점 분석이 쉽도록 되어있다.

2.3 Kim-Ryoo의 RFID 인증 프로토콜

Kim-Ryoo 인증 프로토콜[13]의 동작은 리더가 태그를 인증하기 위해 난수 R1(R_1)을 생성하여 Query와 함께 태그에게 전송한다. 리더를 인증하기 위해 난수 R2(R_2)를 생성한 후 태그는 R1, R2(R_1, R_2)를 이용하여 $h(R_1 \oplus R_2) = S_t$ 를 계산하고 R_2와 함께 리더에 무선으

로 전송하게 된다. 리더는 수신한 $h(ID \oplus S_t) \| R_2$에 R_1을 연접하여 데이터베이스에게 전송한다. 수신한 $h(ID \oplus S_t)$와 비교하여 일치하면 리더가 데이터베이스에 인증된다. 데이터베이스는 R_2를 이용하여 S_{db}를 계산한 후, 리더가 데이터베이스를 인증하기 위한 $h(ID \oplus S_{db})$ 메시지를 리더에게 전송한다. 리더는 수신한 $h(ID \oplus S_{db})$를 태그에게 전송한다. 태그는 $h(ID \oplus S_{db})$데이터를 수신하면 자신이 저장하고 있는 R_2와 자신의 ID를 이용하여 $h(ID \oplus S_{db})$를 계산한다. 수신된 $h(ID \oplus S_{db})$ 값과 계산된 $h(ID \oplus S_{db})$ 값이 일치하면 데이터베이스가 인증되는 방법으로써 스텝별 동작은 다음과 같다.

Step 1. 리더 -> 태그: Query, R_1

Step 2. 태그 → 리더: $h(ID \oplus S_t) \| R_2$

Step 3. 리더 → 백-엔드 DB: $h(ID \oplus S_t) \| R_2 \| R_1$

Step 4. DB → 리더: R1과 R2를 이용하여 S′를 계산

- $h(ID \oplus St) \neq h(ID \oplus S_t)'$ 이면, Error 메시지를 전송
- $h(ID \oplus St)$ = 계산된 $h(ID \oplus S_t)$ 이면, $h(ID \oplus S_{db})$ 메시지 전송

Step 5. 리더 → 태그: $h(ID \| R_2)$

Step 6. 태그: 태그는 $h(ID \| S_{db}) = h(ID \| S_{db})'$ 이면, 리더 인증

본 프로토콜은 효율성 부분에서 태그에서의 연산이 해시연산 4회, XOR 연산 3회 등 타 프로토콜에 비해 상대적으로 복잡하고 많은 계산을 실행하여 시스템에 많은 부하를 준다. 또한 보안상 문제점이 발견되는데 태그가 리더에게 전송한 난수 R_2와 리더가 태그에게 전송한 $h(ID \oplus S_{db})$를 공격자가 도청할 경우 공격자에 의해 스푸핑공격 등에 취약한 단점이 있다.

2.4 Ahn-Bu외 2명의 프로토콜

Ahn-Bu 프로토콜은[14]는 최근 제안된 프로토콜에 비하여 비교적 복잡한 연산을 수행한다. 전체적으로 보면 태그에서 해시연산 3회, 난수생성 1회, 쓰기연산을 한다. 리더에서는 난수 1회, DB에서 해시연산이 2n+2회의 연산이 필요하고 태그에서의 해시 연산이

$$S_T = h(0 \| ID \| N_T \| N_R)$$

로 상당히 복잡하게 이루어진다. 타 인증 프로토콜에 비해 많은 데이터의 전송과 연산이 이루어지며

$$S_T = h(1 \| ID \| N_T \| N_R), \ S_T = h(2 \| ID \| N_T \| N_R)$$

값을 계산하여 저장하기 때문에 공격자가 해시연산을 하기 전에 0, 1, 2를 알아낼 경우 태그로 위장하여 도청공격 이 가능하다. DB에서 최종처리 된

$$ID_{\neq w} = h(2 \| ID \| N_T \| N_R)$$

값도 공격자가 알아내기 쉽기 때문에 리더로 가장한 각종 공격자의 공격위험성이 있는 문제가 있다.

3. 제안 프로토콜

체내 삽입 USN 장치는 무선 통신방식을 이용하여 정보를 송수신 한다. 따라서 무선통신 구간에 다양한 보안위협이 있으며 공격자의 공격 등 보안위협으로부터 안전한 통신환경을 제공하고자 본 논문에서는 변수 값을 이용하고 해시함수를 기반으로 설계하였다. 세션간 전송되는 데이터는 매 세션 암호화 및 해시에 의해 계산되며 전송값은 항상 바뀌어 세션별 전송되는 데이터가 다르다. 공격자가 도청한 정보를 가지고 다른 용도로 이용하거나 재생공격을 할 수 없으며 스푸핑공격, 재전송 공격, 위치추적, 도청공격 및 트래픽 분석 등에 안전하다. 제안 프로토콜에 사용할 기호의 정의는 <Table 1>과 같다.

〈Table 1〉 Symbols and definition

Symbols	Definition
Tag	Tag Agent
Reader	Reader Agent
S	Server
H	Hash Function
x,k	Nonce
a1, a2	Session Key
enc1, enc2, enc3	Variable

3.1 Casper 명세

[Fig. 1]은 본 논문에서 제안하는 프로토콜의 Casper 명세코드이다. 그리고 보안프로토콜에서 중요하게 사용되는 변수유형 선언, 동작절차의 영역을 나열하였다. 변수들과 함수타입은 #Free variables에 정의된다. InverseKeys = (k,k), (a1,a1), (a2,a2), (x,x), (Tag,Tag), (Reader,Reader)는 각 함수별 서로의 역의 키들을 반환

한다는 뜻이다. #Protocol description에는 프로토콜에서 전송되는 메시지들에 대한 순차적 정의이다. 정수 0. 1. 2 등은 전달되는 메시지의 단계를 나타낸다. 각 단계별 매번 바뀌는 값으로 암호화 하여 전송하며 무선 구간에 공격자에게 노출되어도 해독할 수 없어 안전한 방식이다.

```
#Free variables

Tag, Reader : Agent
S : Server
x,k : Nonce
H : HashFunction
a1, a2 : SessionKey
InverseKeys = (k,k), (a1,a1), (a2,a2), (x,x),
(Tag,Tag), (Reader,Reader)

#Protocol description

0.    -> Reader : Tag
1. Tag -> Reader : {x}{a1}%enc1,H(Reader)
2. Reader -> S : {enc1%{x}{a1},H(Reader),a2,k}{a2}
3.          S          ->          Reader          :
{Tag,x,{k}{a1}%enc2}{a2},H(S,Tag),H(Reader)
4. Reader -> Tag : enc2%{k}{a1},H(S),{x}{k}
5. Tag -> Reader : H(Tag),{x}{a1}{a2}%enc3
```

[Fig. 1] Casper specification in the protocol

3.2 동작설명

단계별 자세한 동작 및 설명은 다음과 같다.

Step 1 : Tag → Reader

Agent Tag는 Reader으로부터 Query를 수신한 후 Tag에서 난수 x 값, Session Key 를 생성하고 변수 %Emc에 각 값을 연접(concatenation)하고 Reader 값을 해시 연산하여 Reader에게 전송한다. 이때 생성 값은 고유한 값으로 다른 Agent에서는 생성할 수 없는 값이다.

Step 2 : Reader → S

Tag 에서 전송한 {x}{a1}%enc1,H(Reader) 값을 수신하며 Reader이 계산한 {enc1%{x}{a1},H(Reader),a2,k} {a2} 값을 서버로 전송한다.

Step 3 : S → Reader

Reader에게서 전송된 {enc1%{x}{a1},H(Reader),a2,k} {a2}값을 이용하여 데이터베이스서버에서 계산되어 지는 값은 고정 길이의 데이터를 해시하는 방식으로 다음과 같다. 최초 해시 함수는

$$h_a(\overline{x}) = h \int ((\sum_{i=0}^{k} x_i . a^i) \bmod p)$$

형식으로 계산되어 Reader 에게 전송된다.

Step 4 : Reader → Tag

Reader은 서버에서 수신한 {Tag,x,{k}{a1}%enc2}{a2}, H(S,Tag),H(Reader)값을 인증하고 enc2%{k}{a1}, H(S){x}{k}값을 생성하는데 이번 세션에서도 전송되는 x, k값이 바뀌어 전송하게 된다.

Step 5 :Tag → Reader

마지막으로 Tag는 Reader에게 enc2%{k}{a1},{x}{k} 값을 전송 받은 후 확인되면 자신의 H(Tag),{x}{a1}{a2} %enc3로 연산 암호화하여 Reader에게 전송함으로 Tag 에서의 인증 세션을 완료한다. 이후 통신구간의 Agent구간은 상호인증 되었으므로 안정적인 통신을 진행한다.

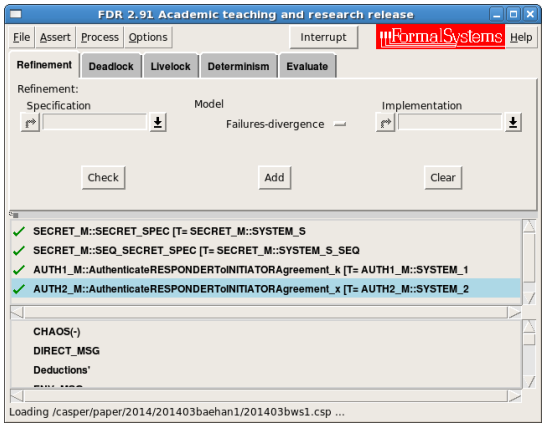
4. 실험결과

제안한 인증프로토콜의 실험을 위하여 다음과 같은 환경에서 프로그램을 설치하고 실험을 진행하였다. Casper 2.0 버전을 실행하기 위해 리눅스 커널 버전 2.6 32Bit 환경에서 Hugs 2006 버전 및 자바 1.6.0-openjdk 버전을 이용하였다. 또한 FDR 2.91 Academic teaching and research release 버전을 설치하여 CSP 언어의 보안성을 확인하였다. 실험에 사용한 환경은 [Table 2]와 같이 요약된다.

〈Table 2〉 Trial environment

Platform	Specification
CPU	Intel(R) Core(TM)2 Duo CPU E7300 2.66GHz
RAM	3GB DDR3 RDIMM, 1333MHz, ECC
HDD	1.5TB SATA(7200RPM)
VIDEO CARD	ATI Radeon HD 3450 512Mb Internal DAC(400Mhz)
OS	RedHat Linux 6.0 32 BIT
Kernel	Linux 2.6.32-71.el6.x86_64
Compiler Program	Casper version 2.0
Model Checking Program	FDR 2.91 Academic teaching and research release

제안한 프로토콜을 FDR의 모델검증 도구를 이용하여 설계한 체내 삽입장치 프로토콜의 안전성(safety), 교착상태(deadlock), 라이브락(livelock) 등의 동작을 검증하였다. [그림. 2]는 설계한 소스파일을 로딩 하여 기본적인 오류 없이 실행 완료된 상태이다. 제안한 프로토콜을 FDR 도구를 이용하여 보안프로토콜을 검증한 결과 그림과 같이 모든 보안속성에 대하여 만족함이 확인되었다.



[Fig. 2] Security verification results of the protocol

[그림. 2]에는 4가지 검증결과가 제시되며 각 결과의 표현은 다음과 같이 분석된다.

1) SECRET_M::SECRET_SPEC[T=SECRET_M::SYSTEM_S

프로토콜의 보안성 확보로 메시지 앞의 체크표시는 프로토콜이 공격자에게 노출되지 않았고 보안상 안전한지를 표현한다. 검증한 Agent간 통신과 해시와 세션키의 보안성이 안전한지 확인하였으며 각종 공격에 문제가 있는지 확인하였다.

2) SECRET_M::SEQ_SECRET_SPEC[T=SECRET_M:: SYSTEM - S_SEQ

이 항목은 프로토콜이 시스템에서 정상적인 프로세스로 동작하는지를 확인한 결과이며 제안한 프로토콜은 안전한 프로세스로 동작함을 확인하였다.

3)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_1

4)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_2

3), 4)는 k를 통해서 Responder와 Initiator가 서로 보안상 문제없이 인증할 수 있는지 검증하는 부분으로 제안한 프로토콜은 서로 안전하게 인증함이 확인되었다. 따라서 검증결과로 세션간 안전성이 충족되었으며 스텝별로 온전히 마무리가 되어 교착상태에 빠지지 않았다. 아울러 무한반복으로 시스템에 문제를 일으키지 않고 검증을 종료하였다.

5. 결론

최근 의료 분야에서 USN 기술발전으로 체내 삽입장치 시스템에 많은 연구가 이루어지고 있다. 사용범위도 의료분야 이외에 기상, 환경, 국방 등 그 범위가 다양하며 산업현장에서 광범위하게 도입되고 있다. 그러나 개인의 의료정보를 처리하는 의료분야 체내삽입장치 기술의 운용 특성상 시스템의 운용 및 제어에 외부의 공격자가 개입 된다면 심각한 타격을 입을 수 있다. 따라서 공격자의 보안문제를 해결하기 위해서 하드웨어적 업그레이드, 각종 암호화, 암호프로토콜 등으로 보안적 안전성을 확보하는 다양한 방법의 연구가 활발히 진행 중이다. 본 논문에서는 해시함수에 에이전트 및 서버 값을 이용하고 세션키와 난수를 삽입함으로 매 세션에서 다른 값이 전송되도록 설계하였다.

본 논문에서는 프로토콜을 설계하여 Casper 언어로 명세한 후 제안 프로토콜이 FDR Tool의 보안속성을 만족하는지 검증을 실시하였다. 검증결과 safety 검증, Deadlock검증, livelock 검증 등 FDR에서 제공하는 모든 보안적인 측면에서 만족함을 보였다. 본 실험의 결과로 향후 다음과 같은 기대효과가 있을 것으로 판단된다. 첫째, 무선 프로토콜 분야에서 정형검증을 함으로 프로토콜 검증에 사람의 실수를 줄이고 효과적인 검증이 확인되었다. 둘째, 무선 전송분야에서 취약한 부분을 보강하여 신속한 시스템의 개발에 도움이 될 것이라 확신한다. 향후 계산량은 줄이고 강력한 함수를 이용하여 무선 통신 및 의료분야에서 효율적이고 안전하게 사용할 수 있는 추가연구를 진행할 예정이다.

REFERENCES

[1] M. H. Yang, H. Y. Hu, Protocol for ownership transfer across authorities: with the ability to assign transfer targety. Security Comm. Networks Vol. 5, 164 - 177, 2012.

[2] D. W. Kim, J. W. Han, and K. I. Chung, Trend of Home Device Authentication/

Authorization Technology. Weekly IT BRIEF, No. 1329, pp. 1-11, 2008.

[3] Yu-Yi Chen, Jun-Chao Lu, Jinn-Ke Jan, A Secure EHR System Based on Hybrid Clouds. J Med Syst, Vol. 6, pp. 3375-3384, 2012.

[4] M. M. Morshed, A. A. H. Yu, An Efficient and Secure Authentication Protocol for RFID Systems. Proceedings of the 17th International Conference on Automation & Computing (ICAC'11), University of Huddersfield, Huddersfield, UK, 10 September, pp. 51-56, 2011.

[5] He, D. B., Chen, J. H., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. J. Med. Syst. doi: 10.1007/s10916-011-9658-5, 2011.

[6] Wei, J.,Hu, X.,Liu, W., AnImproved Authentication Scheme for Telecare Medicine Information Systems., J. Med. Syst. doi: 10.1007/s10916-012-9835-1, 2012.

[7] B. Alomair, L. Lazos, and R. Poovendran, Securing Low-Cost RFID Systems: An Unconditionally Secure Approach. J. Computer Security, Vol. 19, No. 2, pp. 229-256, 2011.

[8] B. Alomair and R. Poovendran, Privacy Versus Scalability in Radio Frequency Identification Systems. Computer Comm., Vol. 33, No. 18, pp. 2155-2163, 2010.

[9] G. Lowe. Casper: A compiler for the analysis of security protocols. User Manual and Tutorial. Version 1.12 2009.

[10] Oxford University Computing Laboratory. FDR2 User Manual, 19th October 2010.

[11] J.E. Song et al., Security Issues and Its Technology Trends in u-Healthcare. ETRI, Electronics and Telecommunications Trends, Vol.22, No.1, 2007.

[12] C.A.R Hoare. Communicating Sequential Processes. Prentice-Hall. 1985.

[13] B. H. Kim, I. T. Ryoo, RFID Mutual Authentication Protocol Against Reflection Attack, THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY, Vol. 32, No 3, pp. 348-354, 2007.

[14] H. S. Ahn, K. D. B, E. J. Yoon, I. G. Nam, RFID Mutual Authentication Protocol Providing Stronger Security. The KIPS Transactions : Part C Vol. 16.C, No. 3, pp. 325-334, 2009.

배 우 식(Bae, Woo Sik)

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2012년 2월 : 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템
- E-Mail : bws@motor.ac.kr

한 군 희(Han, Kun Hee)

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 정보보호
- E-Mail : hankh@bu.ac.kr