체내 이식형 의료기기의 보안성 향상을 위한 3-Tier 보안 메커니즘 설계★

안승현* · 박창섭** · 박주호***

요 약

의료기술 및 IT 기술의 급격한 발전으로 인해 체내 이식형 의료기기와 같은 융합 의료기술에 대한 관심이 날로 증가하고 있다. 하지만, 체내 이식형 의료기기와 같은 새로운 형태의 의료서비스는 무선통신을 통해서 제공되고 있기 때문에 무선통신에서 발생가능한 개인정보 위협을 포함한 다양한 보안 취약점에 관한 문제 역시 중요 이슈로 떠오르고 있다. 특히, 이러한 의료서비스에서의 보안상 취약점은 환자에게 치명적인 위협으로 다가갈 수 있기 때문에 더욱 안전한 방식의 보안성 제공이 요구된다. 본 논문에서는 현재 제공되고 있는 체내 이식형 의료기기를 이용한 의료서비스에서 발생할 수 있는 보안상 취약점들을 지적하고 이에 대응하기 위한 보안 메커니즘을 제안한다.

Design of 3-Tier Security Mechanism for Improving Security of the Implantable Medical Devices

Seung-Hyun Ahn* · Chang-Seop Park** · Joo-Ho Park***

Abstract

As both medical and IT technologies advance, convergent medical technologies such as implantable medical devices are receiving a lot of attentions from the research and medical appliance market. On the other hand, such a new medical service is facing several new security threats including patient privacy breach since the service is based on the wireless communication. Especially, the new security threat could induce the patient's life threatening accident, so that more secure measures should be provided. In this paper, a variety of security threats associated with the implantable medical devices are pinpointed and a new security mechanism against such threats is proposed.

Key words : 의료기기 보안, 체내 이식형 의료기기, 인증 메커니즘, 부인방지, 인증서버

접수일(2014년 5월 8일), 수정일(1차: 2014년 5월 24일), 게재확정일(2014년 5월 26일)

★ 본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(NRF-2012R1A1A2000677)"

★ 본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원(NRF-2011-0023118)과 미래창조과학부의 방송통신정책연구센터운영지원사업의 연구결과로 수행되었음 (KCA-2013-003)

* 단국대학교 일반대학원 전자계산학과

** 단국대학교 컴퓨터과학과(교신저자)

*** 단국대학교 일반대학원 소프트웨어보안전공

Ⅰ. 서 론

의료기술에 대한 관심과 안전한 의료 서비스 제공에 대한 연구는 빠르게 진행되고 있으며, 이에 따라 치료 서비스를 제공하기 위한 의료기기의 발전도 지속적으로 성장하고 있다. 최근에는 기존 의료기기들과 IT 기술을 접목시킨 체내 이식형 의료기기(Implantable Medical Devices, IMD)에 대한 관심이 크게 증가되면서, 관련 연구가 활발해지고 있다. 심장박동기, 인슐린 펌프 등의 체내 이식형 의료기기의 사용이 증가 되고 있는 추세이며, 이식형 의료기기 시장의 규모 또한 눈에 띄게 성장해 가고 있다 [1]. 또한, 기존 치료 방식의 경우 환자가 직접 병원이나 치료기관에 방문하여 진단을 받고 치료를 받아야 하는 방식 이었으나, 체내 이식형 의료기기의 경우 특정 장소에 제한받지 않고 원격으로 환자의 상태를 진단하고 치료 서비스를 제공 할 수 있게 되었으며, 환자에게 접근성을 높이고 편리성을 증가 시킬 수 있는 수준으로 발전해 가고 있다 [2,3]. IEEE 802 워킹그룹에서는 사람의 인체 센싱 정보 수집을 위해 부착되어 있거나 이식되어 있는 저 전력 무선 센서 노드 표준으로 802.15.6 WBAN (Wireless Body Area Network)을 제시하였고 관련 연구도 지속되고 있다 [4].

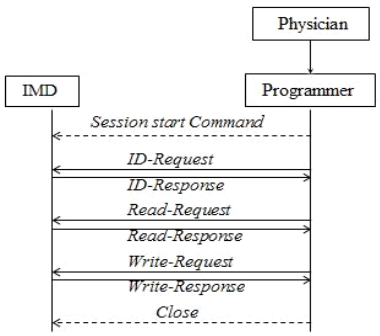
IMD는 환자의 체내에 이식되기 때문에 이를 제어하고 환자에게 치료 서비스를 제공하기 위해서는 의료 인력 (Physician)과 상호작용을 하는 외부단말기인 “Programmer”가 필요하다. Programmer는 IMD에서 수집된 생체정보에 대한 조회 및 치료설정 데이터 전송을 위해 사용된다. 그러나 현재 상용화 되어 사용되는 IMD와 Programmer에는 보안 메커니즘이 전혀 내장되어 있지 않기 때문에 안전한 통신채널이 보장될 수가 없고, 특히 IMD는 환자의 신체에 직접 이식되어 사용되는 만큼 취약점을 악용한 공격에 노출될 경우 환자에게 치명적인 위험을 야기 할 수 있다 [5]. 이러한 문제점들을 부분적으로 완화시킬 수 있는 학술적 연구들이 지난 수년간 진행되어 왔다. IMD와 Programmer 사이에 패스워드 및 대칭키/공개키를 기반으로 한 인증기법들이 제안되었고[6,7,8], 응급상황 시에 응급의료진이 사용할 수 있는 IMD-Programmer 간의 사전 비밀정보를 안전하게 저장하기 위한 기법들 역시 제안되었다 [9,10]. 본 논문에서는 안전한 통신 채널 보장을 위하여 IMD와 Programmer 사이에서 공유되는 정보관리 방식을 기존의 IMD-Programmer 만 존재하는 2-Tier 모델을 확장하여 HAS(Hospital Authentication Server) 기반의 3-Tier 모델을 제시하고 관련 보안 메커니즘을 제안한다.

본 논문의 2장에서는 기존 2-Tier 구조에서 발생 가능한 취약점을 지적하고, 2-Tier IMD-Programmer 구조에서의 주요 보안요구사항에 대해 서술한다. 3장에서는 2장에서 소개되는 기존 2-Tier 구조에서의 취약점 보완을 위해 본 논문에서 제안하는 새로운 형태의 3-Tier 기반의 메커니즘과 작동방식에 대하여 소개한다. 4장에서는 기존 구조와 본 논문에서 제안하는 HAS를 포함하는 3-Tier 구조와의 차이점 분석을 통하여 어떠한 방식으로 취약점 보완이 이루어지는지에 대하여 보이며, 마지막으로 5장에서는 향후 연구방향에 대해 서술한다.

2. 상용 2-Tier 모델과 보안요구사항

2.1. 상용 IMD-Programmer 2-Tier모델

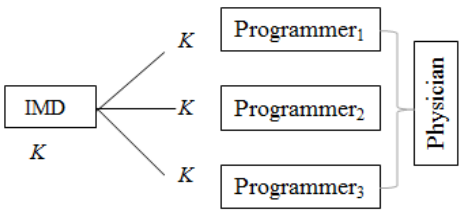
본 논문에서 제안하는 3-Tier 구조와의 차이점을 이해하기 위해, 현재 상용화되어 사용되고 있는 기존 2-Tier IMD-Programmer 구조의 작동 방식 [11]을 (그림 1)에서 간략히 설명한다. Programmer는 *Session-Start* 명령으로 IMD를 기동 시킨 이후에 IMD의 식별자를 요청 (*ID-Request* / *ID-Response*) 하고, 이를 기반으로 Programmer는 IMD에 저장된 환자의 생체정보나 현재 상태정보를 진단의 목적으로 요구/획득 (*Read-Request* / *Read-Response*) 할 수 있다. 또한, 진단된 내용을 기반으로 기존 치료 설정을 변경하기 위해 IMD에게 치료 설정 데이터를 전송 (*Write-Request*) 하여 치료가 이루어진 결과를 확인 (*Write-Response*) 할 수도 있다. 진단 및 치료세션이 모두 완료된 이후에는 *Session-Close* 명령을 통해 세션을 종료 한다.



(그림 1) 기존 2-Tier 구조 메커니즘

2.2. IMD 보안요구사항과 기존연구

IMD를 이용한 치료의 안전성을 높이기 위해서는 첫째 상호인증을 통한 IMD에의 접근제어가 필요하다. 악의적인 목적으로 Programmer를 이용할 경우, 현재 진행 중인 세션이 환자에게 필요한 치료 과정인지 아닌지에 대한 구분도 할 수 없게 된다. 따라서 이를 악용하여 환자의 IMD에 불필요한 치료행위를 유발하여 환자의 생명에 치명적인 위협을 가할 수 있다. 예를 들면, 심박동 조절기의 경우에 환자에게 심박동을 비정상적으로 조절하도록 IMD에게 치료세션을 진행하여 일정 범위로 유지 되어야 할 환자의 심박동이 기준치보다 크게 빨라지거나 크게 느려지는 상황을 유발하여 환자가 사망에 이르게 할 수도 있으며, 인슐린 펌프의 경우에도 인슐린의 과다 분비를 일으켜 환자에게 큰 위협을 초래할 수 있다 [12,13]. 둘째, IMD는 환자의 체내에 이식되어 있기 때문에, 외부 기기인 Programmer와 통신하기 위해서는 무선 통신을 사용해야만 한다. 따라서 환자의 프라이버시 보호 및 치료 데이터의 무결성이 외부 공격자로부터 보장되기 위해서는 안전한 무선채널 설정을 통해 기밀성과 무결성이 보장되어야 한다. 위 2가지 기본적인 보안요구사항을 만족시키기 위해서는 궁극적으로 Programmer와 IMD 간의 비밀 공유키가 설정되어야 하는데 이와 관련된 기존연구는 단순 패스워드 공유 또는 대칭키 및 공개키 공유가 되어 있다는 가정을 하고 있고[6,7,8], 세션키의 개념은 도입하고 있지 않다. 특히, 2-Tier 모델에서는 (그림 2)에서처럼 다수의 Programmer가 존재할 경우에는 특정 IMD와의 비밀 공유키 K가 사전에 다수의 Programmer에 설정이 되어 있어야 한다. 이는 특정 Programmer가 유출/도난 시에는 다수의 IMD에 대한 접근제어가 통제될 수 없다는 취약점을 가지게 된다.



(그림 2) 기존 IMD-Programmer 키 공유 구조

3. 3-Tier 모델기반의 IMD 보안 메커니즘 설계

기존 2-Tier 모델의 단점을 보완하기 위해서 본 논문에서는 (그림 3)과 같이 Hospital Authen- tication Server (HAS)를 이용한 새로운 보안 메커니즘이 적용된 3-Tier 모델을 제안한다. 3-Tier 모델에서는 의료진이 관리하는 다수의 Programmer에는 IMD와의 공유키가 저장되지 않는다. Programmer는 단지 IMD와의 데이터 교환을 위한 dummy 터미널의 역할을 하며 단지 무선구간을 보호하기 위한 암호화 모듈만이 존재한다.

3.1 기본적인 가정과 초기화 과정

앞으로 설명될 본 논문에서 사용되는 기호의 의미는 다음의 <표 1>을 따른다.

<표 1> 표기법 해설표

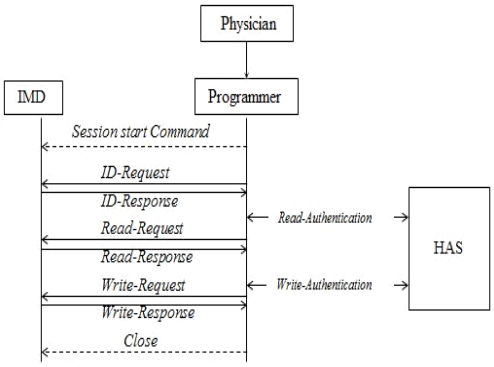
표기법	해설
dID	IMD의 기기 식별 번호
pID	의료 인력의 식별 번호
SN_j	j번째 세션 번호
$Data_j$	j번째 세션에서 IMD로부터 수집된 환자정보
$Conf_j$	j번째 세션에서 치료를 위한 의료 인력의 변경 정보
$MAC(K)$	대칭키 K를 이용한 필드들의 메시지 인증 값
$[m]K$	대칭키 K를 이용한 파라미터 m의 암호화
$kdf(.)$	키 도출 함수
$h(.)$	일 방향 해시 함수
K_{dID}	IMD와 HAS사이에 사전 공유된 롱텀키
PK_{pID}, SK_{pID}	의료 인력의 서명을 위한 공개키와 개인키
K_{pID}	의료 인력과 HAS사이에 사전 공유된 롱텀키
Kr_j, Kw_j	j번째 세션을 위한 READ 키와 WRITE 키
K_j	j번째 세션에서의 K_{pID}로부터 도출되는 세션키
$Sig(SK_{pID})$	의료 인력의 개인키를 이용한 필드들에 대한 서명 값

IMD가 환자에게 이식되기 이전에 dID, SN_0, K_{dID} 및 환자 성명, 생년월일 등의 $PatientInfo$를 내장하여 초기화 시킨다. 이때, SN_0는 초기 환자세션번호 (patient session number)를 의미한다. IMD와 HAS는 롱텀키 (long-term key) K_{dID}를 사전 공유하고, Programmer와 HAS는 상호간의 공개키를 미리 소지하고 있음을 가정한다. 의료 인력 (Physician) 개개인은 각자의 식별자 pID와 서명용 개인키 SK_{pID} 그리고 자신과 HAS가 사전에 공유하고 있는 롱텀키 K_{pID}가 내장된 스마트카드를 Programmer에 삽입하여 전용 Programmer로 사용하게 되며 또한 HAS를 통해 IMD와 전용 Programmer 사이에 사용될 세션키를 전달받음으로써 치료세션을 진행하게 된다. 의료 인력이 IMD에 접근하기 위해서는 우선적으로 HAS와의 인증과정을 거친 이후에 접근제어 키 (access key)를 전달받게 된다. 2가지 유형의 접근제어 키가 있다. 첫째는

READ 키로써 IMD에서 환자정보를 획득하기 위해서 사용되며, 둘째는 WRITE 키로써 치료설정 명령어를 IMD에 전달하기 위해 사용된다.

3.2 제안 메커니즘

새로운 환자세션 (patient session)을 개시하기 위해서 의료 인력은 개인별로 소지하고 있는 스마트카드를 사용하고자 하는 Programmer에 삽입 하여 전용 (personalized) Programmer로 전환시킨다.



(그림 3) HAS가 포함된 3-Tier 구조

① RFID 세션

Programmer → IMD : *ID-Request*
Programmer ← IMD : *ID-Response* (SN_j, *dID*)

의료 인력의 전용 Programmer는 환자의 IMD에게 *ID-Request*를 전송한다. 명령어를 전달받은 IMD는 *ID-Response*를 통해 Programmer에게 IMD에서 생성한 SN_j와 *dID*를 응답하게 되는데, 전달받은 *dID*를 통해 Programmer는 환자가 IMD를 사용하고 있음을 파악할 수 있을 뿐 아니라, 환자의 IMD와 진행할 세션에서 사용할 SN_j를 얻어낼 수 있게 된다. 특별히, 이 구간에서는 중요한 정보가 전달되지 않을 뿐만 아니라, 다소 빈번하게 이루어 질 수 있는 구간이기 때문에 해당 세션은 RFID 통신을 이용하여 진행하게 함으로써, IMD 배터리 소모량을 크게 줄일 수 있다 [14].

② Read-Authentication 세션

환자의 IMD 사용 유무 확인과 *dID*를 제공받은 Programmer는 IMD를 통해 환자의 상태정보를 수신하기 위해서는 HAS와 Read-Authentication 세션을 진행하게 된다. 먼저, Programmer는 현재 환자세션에 사용될 세션키 K_j = $kdf(K_{pID}, SN_j, dID, pID)$를 생성한다. HAS 역시 동일한 세션키를 도출할 수 있다.

Programmer → HAS : *Read-Auth-Request*
(SN_j, *dID*, *pID*, $MAC(K_j)$)
Programmer ← HAS : *Read-Auth-Response*
(SN_j, $[Kr_j]K_j$, $MAC(K_j)$)

본 세션을 통해서 전용 Programmer는 IMD와의 READ 세션에 사용될 접근제어 키인 READ 키 Kr_j = $Kdf(dID, pID, SN_j, K_{dID})$를 획득하게 된다. 특히, 이 과정에는 Programmer와 HAS 간의 상호인증이 수반된다. Kr_j 생성에는 K_{dID}가 포함되는데, 이는 전달된 *dID*에 해당하는 IMD와 HAS만이 사전 공유한 롱텀키 로써, Programmer가 보내온 값에 해당 파라미터가 포함되어 있다면, IMD는 현재 통신을 원하는 Programmer가 HAS의 인증을 거친 정당한 기기임을 확인할 수 있게 된다.

③ READ 세션

Programmer → IMD : *Read-Request*
(SN_j, *pID*, $MAC(Kr_j)$)
Programmer ← IMD : *Read-Response*
(SN_j, $[Data_j]Kr_j$, $Auth_j$, $MAC(Kr_j)$)

Programmer는 HAS로 부터 전달받은 READ 키 Kr_j를 이용하여 IMD와 READ 세션을 진행한다. *Read-Request* 명령어를 통해 IMD에게 SN_j와 의료 인력의 *pID*가 전달된다. IMD에는 Kr_j 생성에 사용되는 *dID*와 K_{dID}가 있기 때문에, Programmer로부터 전달되는 *pID*와 SN_j에 대한 MAC 값 검증을 통해서 Programmer가 전송한 *Read-Request* 명령어의 무결성 검증과 Programmer에 대한 인증을 수행할 수 있게 된다. IMD는 Programmer가 요청한 $Data_j$를 탑재한 *Read-Response* 명령어를 전송한다. 특히, 환자상태 데이터가 지금 세션에 참여중인 IMD에게서 수집, 전송 된 것임을 확인해주기 위한 $Auth_j$ = $h(K_{dID}, SN_j, Data_j)$와 함께 전송된다. $Auth_j$ 생성에는 K_{dID}가 포함되기 때문에 Programmer는 생성할 수 없는 값이며, 따라서 현재 세션에 참여하는 IMD 역시 정당한 기기인지를 확인해 주는 역할을 한다.

④ Write-Authentication 세션

Programmer → HAS : *Write-Auth-Request*
(SN_j, *dID*, *pID*, Z_j, $Auth_j$, Sig_j, $MAC(K_j)$)

Programmer ← HAS : *Write-Auth-Response*
(SN_j, $[Kw_j]K_j$, $MAC(K_j)$)

Read-Response 명령어를 통해 환자의 상태정보를 제공받은 Programmer는 환자에 대한 적절한 치료행위를 위한 치료설정 데이터 $Conf_j$를 생성한다. Write-Authentication 세션을 통해 Programmer는 HAS에게 IMD로부터 받은 데이터와 함께, $Conf_j$가 포함된 Z_j 그리고 현재 치료세션을 의료 인력 본인이 진행했음을 증명하기 위해 개인키로 서명한 값 Sig_j 역시 전송하게 된다.

Z_j = $[PatientData_j, Conf_j]K_j$
Sig_j = $Sig(SK_{pID})$ is obtained from W_j
W_j = $[SN_j, dID, pID, Data_j, Auth_j, Conf_j, Sig(SK_{pID})]$.

HAS는 전달된 서명 값을 검증하여 의료 인력 개인 식별을 진행함으로써, 향후 부인방지를 위해 사용된다. 또한, $Auth_j$를 검증하여 현재 세션에서 올바른 IMD와의 통신이 진행 중이란 것을 확인하게 된다. 특히, 본 논문에서 제안하는 메커니즘에서 중요한 기능 중 하나인 부인방지를 위한 값 W_j이 현재 세션에서 생성되어 HAS에 저장된다. HAS에 저장된 값은 이후 WRITE 세션에서 Programmer가 IMD에게 전송할 치료설정 데이터와 기기 인증에 소요되었던 파라미터 그리고 의료 인력의 서명이 포함되기 때문에, 의료 인력의 사후 의료사고 분쟁조정을 위한 자료로 사용될 수 있다. HAS는 Programmer에게 WRITE 키 Kw_j = $kdf(K_{dID}, SN_j, dID, pID, Data_j, h(Conf_j))$를 전송해주는데, 여기에는 Programmer가 생성한 $Conf_j$와 함께 IMD와 HAS만이 알고 있는 롱텀키(K_{dID})가 포함되어 Programmer는 임의적으로 WRITE 키를 생성해 다른 목적으로 IMD를 제어할 수 없게 된다.

⑤ WRITE 세션

Programmer → IMD : *Write-Request*
(SN_j, pID, $[Conf_j]Kw_j$, $h(Conf_j)$, $MAC(Kw_j)$)
Programmer ← IMD : *Write-Response*
(SN_j, $Status_j$, $MAC(Kw_j)$)

Programmer는 IMD를 이용해 환자에게 치료행위를 진행하고자 *Write-Request* 명령어를 전송한다. HAS로부터 전송받은 WRITE 키 Kw_j를 이용하여 $Conf_j$값을 암호화하여 전송하며, 무결성 검증을 위하여 MAC도 함께 보내준다. IMD는 Programmer로부터 전송된 *Write-Request* 명령어를 받고, 포함된 값들의 검증을 진행한다. 우선적으로, Kw_j = $kdf(K_{dID}, SN_j, dID, pID, Data_j, h(Conf_j))$를 도출해 낸다. 이 계산에는 롱텀키가 필요하기 때문에 HAS와 사전 공유된 롱텀키를 소유하지 않은, 또는 READ 세션을 진행하지 않은 정당치 못한 IMD라면 키 값 도출을 할 수 없게 된다. IMD 역시 Kw_j 값을 도출한 이후에는 Programmer로부터 전송된 값을 검증할 수 있게 된다. 이 검증이 정상적으로 통과 된다면, 의료 인력이 전송한 치료설정 데이터인 $Conf_j$를 적용하여 환자에 대한 치료정보를 변경하게 된다.

⑥ Close 세션

모든 치료행위 단계가 진행되고 난 이후에 IMD는 의료 인력 에게 변경된 현재 IMD의 상태정보를 전송하고, 세션이 성공적으로 진행되었음을 알려주게 되면 Programmer에 의해 최종적으로 현재 세션이 종료된다.

4. 분 석

4.1 기존 구조에서의 중요 취약점

기존 사용되던 2-Tier 구조에서의 중요 취약점으로는 IMD-Programmer 간에 일 방향 인증만이 제공되며 Programmer 사용자 (의료 인력)에 대한 개별인증 기능은 제공되지 않을 뿐만 아니라, Programmer를 이용한 세션 진행에 대한 어떤 기록도 남지 않는다. IMD-Programmer만이 존재하는 2-Tier 구조에서는 두 기기 사이에 사전에 비밀 공유키를 공유해야 하고, 이는 비밀키를 공유한 장치 간에만 통신이 가능한 기기 간 종속성 문제가 생겨나게 된다. 이는 응급상황과 같은 위급상황에서 기기간의 의존성으로 인해 환자가 신속히 치료를 받을 수 없는 상황이 발생할 수 있게 된다. Programmer를 사용한 의료 인력에 대한 개별인증이 이뤄지지 않고, Programmer를 이용한 치료행위 기록이 남겨지지 않기 때문에 의료행위로 인한 환자의 피해나 의료분쟁에 적절히 대처할 수가 없게 된다.

4.2 HAS가 포함된 새로운 메커니즘의 중요 이점

2-Tier 구조에서의 문제점 해결을 위한 본 논문에

서 제안하는 HAS가 포함된 3-Tier구조를 사용함에 있어서 중요 이점들은 다음과 같다.

4.2.1 기기 간 종속성 제거

HAS가 포함됨으로 인해서 IMD-Programmer는 더 이상 동일한 비밀키를 사전 공유할 필요가 없다. HAS는 IMD와 Programmer 각각과 다른 비밀정보를 공유, 관리하며 이를 통해서 각 기기간의 세션을 제어하기 때문에 동일한 비밀정보를 사전 공유한 기기 간에만 통신이 가능한 기기 간 종속성 문제가 해결된다. 특히 위급상황에서 발생 가능한 종속성에 의한 문제점 해결에 도움이 된다.

4.2.2 상호 인증 기능

HAS가 의료 인력 개별 식별자를 저장하고 있기 때문에, 의료 인력 개인 스마트카드를 사용가능해지고, 이로 인해 개별 인증이 가능해 진다. 각각의 IMD와 Programmer는 HAS와 사전 공유된 비밀정보 K_{dID}, K_j를 지니고 있기 때문에 HAS를 통해 세션이 진행된다면, 해당 세션은 HAS를 통한 상호인증을 보장받게 된다. 즉, IMD와 HAS간에 사전 공유된 롱텀키 K_{dID}를 통해서 의료 인력이 IMD로 부터 데이터를 획득하고 치료행위를 진행하기 위해서는 HAS가 생성하는 세션키 (READ / WRITE 키) Kr_j, Kw_j를 부여받아야 하는데, Kr_j, Kw_j는 다음의 계산식을 따르게 된다.

$$Kr_j = kdf(dID,\ pID,\ SN_j,\ K_{dID}) \quad (1)$$

$$Kw_j = kdf(K_{dID},\ SN_j,\ dID,\ pID,\ Data_j,\ h(Conf_j)) \quad (2)$$

K_{dID}는 IMD와 HAS간에 사전 공유된 값이기 때문에 정당하게 HAS를 통해 인증되지 않은 Programmer는 세션키 획득이 불가능하기 때문에 IMD에 접근할 수 없게 된다. 또한, IMD 역시 각 IMD별로 HAS와는 각기 다른 K_{dID}를 사전 공유하게 되므로 인해, HAS를 통해 현재 세션에서 인증된 IMD가 아니라면, K_{dID}가 사용되는 (1), (2)에 대한 검증을 진행 할 수 없기 때문에 Programmer와의 세션을 진행할 수 없게 된다.

4.2.3 부인 방지 기능

HAS를 이용한 로그기록의 저장 기능 또한 보안성 향상에 큰 역할을 한다. 이미 언급한 바와 같이, HAS를 통한 치료세션 진행과정에서 의료 인력이 생성한 치료설정 데이터에는 의료 인력의 개별서명이 포함된 데이터인 W_j 가 저장/관리된다. W_j 에는 현재 세션을 진행하는 의료 인력의 pID와 Sig_j가 포함되는데, 의료 인력의 서명 값은,

$$Sig_j = Sig(SK_{pID}) \text{ is obtained from } W_j \quad (3)$$

위 계산을 따라 도출된다. 저장되어지는 W_j의 관리를 통해 의료 인력의 서명 값을 확인 가능하기 때문에, 치료행위의 사후 문제에 대한 부인방지 기능을 제공할 수 있게 된다. 더불어 의료 사고 분쟁 해결에 중요자료로 사용 가능하며 이는, 체내이식형 의료기기를 이용한 의료서비스 신뢰성 향상에 큰 도움이 될 수 있다.

4.3 제안 메커니즘 안전성 분석

본 절에서는 제안된 보안 메커니즘에 대한 위조 및 재생공격 그리고 환자상태 정보의 위조공격 가능성에 대한 분석을 진행한다.

4.3.1 명령어에 대한 위조 및 재생공격

IMD와 개별 Programmer 사이에서의 모든 명령어에는 현재 세션에서 일종의 세션키 역할을 하는 Kr_j와 Kw_j가 암호화에 사용됨으로 인해서 안전하게 보호된다. (1), (2)의 도출 과정을 보면, IMD와 HAS사이에서만 사전 공유된 K_{dID}가 키 도출에 포함되어 지기 때문에, 이를 알 수 없는 외부 공격자에 의한 명령어 위조공격으로부터 안전하게 보호될 수 있다. 또한, IMD와 의료 인력의 식별 번호인 dID 와 pID, 현재 세션 번호인 SN_j는 (1)과 (2)의 도출에 포함됨을 볼 수 있는데, 이는 해당 세션에서의 현재성을 위한 파라미터로써, 재생공격을 방지하기 위해 사용된다.

4.3.2 환자 상태정보에 대한 위조공격

IMD로부터 수집, 저장되어 의료 인력에게 전달되어지는 환자의 상태정보 $Data_j$와 이를 기반으로 하는 치료데이터 $Conf_j$는 환자의 개인정보보호를 위해 대칭적으로 보호된다. 이를 위해서, $Data_j$, $Conf_j$ 값들의 암호화를 진행하는데 사용되는 세션키 K_j는 의료 인력의 롱텀키인 K_{pID}를 사용하여 다음 계산식을 따라 도출된다.

$$K_j = kdf(K_{pID},\ SN_j,\ dID,\ pID) \quad (4)$$

K_j는 HAS와 Programmer 사이에서 안전한 명령어 교환을 위해 사용된다. 따라서 개별 Programmer와 HAS사이에 사전 공유되어진 K_{pID}를 알지 못하게 된다면 현재 세션에서 사용되는 (4)의 값을 도출 해낼 수 없기 때문에 환자의 상태정보가 포함된 명령어는 위조 공격에 대해 안전하게 보호될 수 있다.

4.4 보안 모델 비교 분석

이번 장에서는 기존 두 가지 형태의 2-Tier 모델과 본 논문에서 제안하는 HAS가 포함된 3-Tier 모델사이의 보안성 비교 분석을 진행한다.

<표 2> 제안하는 3-Tier 모델과 2-Tier 모델 분석표

보안 모델	2-Tier [6]	2-Tier [7]	3-Tier(HAS)
인증 방식	패스워드	시도-응답 방식의 비밀정보 공유	시도-응답 기반의 비밀정보 공유
인증 형태	일방향 인증	일방향 인증	상호인증
세션키 생성방식	사용 안함	사용 안함	HAS에서 생성
키 관리 방식	해당 없음	MK를 통해 도출되는 특별키 사용	LK를 통해 도출되는 RK, WK 사용
다수 Programmer 지원	해당 없음	안전하지 않음	안전한 지원
환자 정보 보호	해당 없음	해당 없음	$Auth_j$ 를 통해 안전
치료 정보 보호	해당 없음	해당 없음	$Auth_j$, Sig_j를 이용해 가능

<표 2>에서 보이는 바와 같이, [6] 모델은 패스워드 기반의 인증방식을 취하고, [7]모델과 본 논문에서 제안하는 HAS를 포함한 3-Tier 모델은 공유된 비밀정보를 기반으로 하는 시도-응답 인증방식을 사용한다. [6] 모델의 경우, 저장된 패스워드 외에는 세션 보호를 위한 다른 정보들이 사용되지 않기에 세션키 사용방식이 도입되어 있지 않다. 따라서 현재 세션에서 송, 수신되는 환자정보나 치료정보에 대한 보호가 이루어 질 수 없을 뿐만 아니라, 사실상 모든 데이터에 대해서 안전성을 보장할 수 없는 모델이다.

[7] 모델의 경우에, 본 논문에서 제안하는 HAS가 포함된 3-Tier모델과 마찬가지로 시도-응답 기반의 인증 방식을 사용한다. 다만, IMD-Programmer 두 기기만이 존재하는 구조이기 때문에 상호인증 기능을 제공할 수 없다. HAS를 포함하는 3-Tier 모델은 HAS가 각각의 IMD와 Programmer들과의 사전 공유된 비밀정보를 기반으로 기기들의 인증을 대신 진행함으로써, IMD와 Programmer에게 상호인증을 제공할 수 있다. HAS가 각각 IMD와 Programmer 기기들과 비밀정보를 공유하고 있음으로 인해서 다수의 Programmer와의 통신도 지원할 수 있게 된다. [7]과 HAS를 포함하는 3-Tier 모델의 키 관리 방식에서도 안전성에서 크게 차이가 나는데 [7]의 경우, 저장된 Master-Key를 통해서 세션키가 도출되는 방식인데다, 모든 Programmer가 공통된 키를 소지하게 되기 때문에, 상호인증이 이뤄지지 않은 채 사용된다면 하나의 기기가 공격에 노출되었을 경우에 모든 기기들의 세션이 공격에 노출되는 위험성이 따르게 된다. 하지만 제안하는 HAS가 포함된 모델의 경우, 기기별로 다른 롱텀키를 소유하고 있으며, HAS에서 해당 롱텀키를 기반으로 생성하는 세션키가 사용된다. 이에, 공격자에 의한 세션키 도출이 불가능하기 때문에 각 기기별로 세션에 대한 개별 보호가 이루진다. 결국 다수의 Programmer와의 통신도 안전하게 제공 가능하다.

IMD를 사용하는 환자 입장에서 민감한 부분인, 환자의 프라이버시 보호를 위한 환자정보와 치료정보에 대한 안전성 역시 [7]의 경우에는 키 관리가 안전하게 이루어지지 않기 때문에, 해당 데이터들에 대한 위조나 재생공격에 대해서 안전성이 보장될 수 없는 구조이다. 이 경우에, 비밀정보가 Programmer안에 저장되는 [6, 7] 모델의 경우에, Programmer가 한 대라도 탈취되는 상황이 발생될 경우, 해당 Programmer와 공통된 키를 가진 다른 Programmer들이 진행하는 모든 통신들은 공격자에게 모두 노출되어 버리는 보안상 큰 위험이 발생한다. 반면에, 제안하는 HAS를 포함하는 3-Tier모델의 경우, 키 관리가 안전하게 이루어지게 되므로, 위험에 노출되지 않는다. 또한, HAS를 통해서 비밀정보를 기기 내부에 저장하지 않고, 의료 인력이 개별로 지닌 스마트카드를 통해 세션을 진행할 수 있기 때문에, 해당 스마트카드에 저장되어 있는 의료 인력의 서명 값을 통해 치료정보가 보호되어질 수 있다. 따라서 세션에서 송, 수신되는 환자와 관련된 정보는 어느 모델보다 안전하게 관리되고 보호된다.

5. 결론 및 향후 연구방향

본 논문에서는 기존 IMD-Programmer만이 존재하는 2-Tier 구조에서의 취약점 분석과 해당 위협점을 해결하기 위한 보안성 향상이 가능한 새로운 메커니즘을 제안하였다. 체내 이식형 의료기기의 연구방향은 기존 구조의 한계점을 명확하게 인지하여 다른 형태로의 변환을 꾀하고 있음을 볼 수 있다. HAS가 포함된 새로운 형태의 3-Tier 구조는 IMD가 하드웨어 제약으로 인해서 수행하지 못하는 기능을 HAS가 대신 수행하고 전제적인 통신 세션을 제어하도록 의도함으

로써, 상호인증이나 부인방지와 같이 무선통신 기반의 의료기기 보안요구사항을 제공할 수 있도록 하였다. HAS는 IMD를 대신하여 무거운 작업을 수행하기 때문에 하드웨어 자원이 풍부해야함은 물론이고, 안전한 저장소 역할을 해내야만 한다. 이를 위해서는 HAS에 대한 직접적인 외부공격에 대한 대비책으로써 매우 안전한 보안 시스템이 필요하다. 이를 위한 하나의 방안으로써, HAS 내에 저장되어지는 로그 기록들에 대한 시스템 로그파일들의 보안기법에 대해서 연구를 계획하고 있으며, HAS에서 관리하는 비밀정보가 노출된다면 전체적인 보안 메커니즘은 무용지물이 되어버리기 때문에 HAS 내부의 데이터베이스에 대한 보안시스템 구축이 필수적이고, 이를 위한 연구를 진행할 계획이다.

참고문헌

[1] U. Lakshmanadoss, A. Shah and J. P. Daubert, “Telemonitoring of the Pacemakers,” Modern Pacemakers - Present and Future, Prof. Mithilesh R Das (Ed.), InTech, pp. 129-146, Feb. 2011.

[2] Medtronic-Carelink ® Network, http://world.medtroniccarelink.net/, Accessed on June 2013.

[3] Biotronik-Home Monitoring ® Service Center, http://www.biotronik.com/, Accessed on June 2013.

[4] IEEE, “Part 15.6: Wireless Body Area Networks”, 29 February 2012.

[5] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and Privacy for Implantable Medical Devices,” IEEE Pervasive Computing, vol. 7, no. 1, pp. 30-39, Jan. 2008.

[6] R. A. Balczewski and K. Lent, “Security System for Implantable Medical Devices,” U.S. Patent 6,880,085, Apr. 12, 2005.

[7] J. A. von Arx, A. T. Koshiol, and J. E. Bange, “Secure Long-Range Telemetry for Implantable Medical Device,” U.S. Patent 7,155,290, Dec. 26, 2006.

[8] K. B. Rasmussen, C. Castelluccia, T. Heydt-Benjamin, and S. Capkun, “Proximity-based Access Control for Implantable Medical Devices,” in Proc. of the 16th ACM conference on Computer and Communications Security, pp. 410-419, Chicago, Illinois, U.S.A., Nov. 9-13, 2009.

[9] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno and W. H. Maisel, “Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices,” In Proc. of the SIGCHI Conference on Human Factors in Computing Systems, pp. 917-926, Atlanta, GA. U.S.A., Apr. 10-15, 2010.

[10] S. Schechter, “Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices,” in Proc. of the first USENIX Workshop on Health Security and Privacy, pp. 1-2, Washington D.C., U.S.A., Aug. 11-13, 2010.

[11] S. Barold, R. Stroobandt and A. Sinnaeve, "Cardiac Pacemakers Step by Step," An Illustratied Guide, Blackwell Futra, 2004.

[12] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,” in Proc. of the IEEE Symposium on Security and Privacy, pp. 129 - 142, Oakland, CA. U.S.A., May 18-22, 2008.

[13] C. Li, A. Raghunathan and N. K. Jha, “Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System,” In Proc. of the IEEE International Conference on e-Health Networking, Applications, and Services, pp. 150-156, Columbia, MO., U.S.A., June 13-15, 2011.

[14]K. Malasri and L. Wang, “Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges,” IEEE Communications Magazine, vol. 47, no. 7, pp. 74-80, July 2009.

[저 자 소 개]

안 승 현 (Seung-Hyun Ahn)

2013년 8월 단국대학교 컴퓨터과학과 학사
2013년 9월 ~현재 단국대학교 전자계산학과석사

email : corokuru@nate.com

박 주 호 (Joo-Ho Park)

2013년 2월 단국대학교 컴퓨터과학과 학사
2013년 3월~ 현재 단국대학교 소프트웨어보안전공 석사재학

email : wnghsla2000@naver.com

박 창 섭 (Chang-Sub Park)

1983년 2월 연세대학교 경제학과 학사
1987년 2월 Lehigh University 컴퓨터과학과 석사
1990년 2월 Lehigh University 컴퓨터과학과 박사
1990년 3월～현재: 단국대학교 컴퓨터과학과 교수

email : csp0@dankook.ac.kr