u-헬스 환경에서 개인건강관리를 위한 보안 위협 및 요구사항에 관한 연구

Study on Security Threat and Requirement for Personal Health Management in u-Health Environment

김순석*, 박홍진**

Soon-Seok Kim*, Hong-Jin Park**

요 약

개인건강관리를 위해 PHD(Personal Health Device)로부터 제공되는 개인 생체정보는 사생활 보호 측면에서 볼 때 개인의 생체와 관련한 매우 민감한 정보이며 환자를 가정할 때, 이것이 제 3자에게 노출되는 경우는 더욱 심각하다. 그러나 이번에 ISO에서 제정된 표준 프로토콜[1]의 경우, 개체 상호간에 생체 정보 교환을 위한 전송 부분만을 고려한 규격일 뿐 보안에 대한 요소는 전혀 고려되고 있지 않은 실정이다. 따라서 본 논문에서는 u-헬스 환경에서 개인건강관리를 위한 각종 보안 위협과 보안 요구사항에 대해 새롭게 제안하고자 한다.

Abstract

The personal bio-information supplied from the PHD(Personal Health Device) for personal health management is very sensitive in relation to a personal living body in an aspect of privacy protection. On the assumption that the information is about a patient, it is more serious problem if it is revealed to a third party. However, the established ISO (International Organizations for Standardization) standard protocol[1] in October 2009 has just considered a transmission part for mutual exchange of bio-information between individuals, but has never actually considered security elements. Accordingly, this paper is to show all sorts of security threats according to personal health management in the u-health environment and security requirements newly.

Key words : personal health management, security threats, security requirements

I. 서 론

u-헬스[2]란 흔히 정보통신 기술과 보건 의료를 연결하여 언제 어디서나 “예방, 진단, 치료, 사후관리”의 보건의료 서비스를 제공하는 것 또는 유무선 네트워크를 기반으로 언제 어디서든 인간의 건강한 삶을 보장해 주기 위한 시스템을 말한다. 이러한 u-헬스는 최신 기술이라기보다는 약 10여 년 전부터 e-헬스라는 이름으로 유럽과 미국 등에 이미 알려진 기술이다.

특히 최근 들어 의료의 중심이 진료 중심에서 예방중심, 그리고 질병관리에서 건강관리로 바뀌어 감

* 한라대학교 컴퓨터공학과(Department of Computer Science, Hal-La University)
** 상지대학교 컴퓨터정보공학부(School of Computer, Information and Communication., Sang-Ji University)
· 제1저자 (First Author) : 김순석
· 투고일자 : 2010년 5월 17일
· 심사(수정)일자 : 2010년 5월 18일 (수정일자 : 2010년 6월 28일)
· 게재일자 : 2010년 8월 30일

에 따라 기존의 HIS(Hospital Information System), OCS(Order Communication System), PACS(Picture Archiving Communication System)에서 센서를 통한 건강정보를 바탕으로 의료 및 건강관리를 제공하는 u-헬스케어로 진행됨에 따라 그 중요성이 날로 커지고 있다[3,4]. 또한 현재 선진국을 중심으로 국민들의 의료 서비스 제공에 소요되는 비용을 절감하고 보건의료의 선진화를 위해 보건의료 정보화에 많은 투자와 연구가 진행 중에 있다.

현재 u-헬스 서비스는 원격의료가 대표적인 사례이며 이를 구현하기 위해서는 가정에 있는 u-헬스 디바이스와 전송을 위한 핸드폰 또는 공유기간 통신, 공유기로부터 u-헬스 서비스센터와의 통신, 필요에 따라서는 u-헬스 서비스센터와 병원간의 통신이 필수적이다.

한편 이러한 각 개체간의 통신에 있어 전달되는 정보는 개인의 생체정보 또는 병력정보인 만큼 이들 정보에 대한 안전한 교환이 반드시 전제되어야 한다. 특히 전송과정에서 악의 있는 제삼자로부터의 개인건강 정보의 오남용과 위변조, 해킹 등으로 인한 사생활 침해 문제는 반드시 해결되어야 하는 선결과제이다.

의료분야와 관련한 그 동안의 보안 기술은 주로 병원 내 또는 병원 간에 이루어지는 의료정보의 흐름에 관심이 많았던 것이 사실이다. 표준화에 있어서도 주로 병원 내 의료정보 소프트웨어의 보안 기술이 그 주류를 이루고 있다. 일례가 바로 전자의무기록(EMR, Electronic Medical Record)에 대한 보안이며 이 분야 또한 현재 국내외에서 활발히 연구가 진행 중에 있다.

그러나 앞서 언급한 바와 같이 최근 의료의 중심이 진료를 통한 치료에서 웰빙, 웰니스의 영향에 따른 예방이나 건강관리로 이동하면서 의료 장비에 있어서도 일반가정 내에서 혈압, 혈당, 체중계와 같이 사용자가 간단히 검사를 할 수 있는 진단, 검사 장비들이 연이어 출시되고 있다. 이를 있다병원 내 현장진료형 의료장비인 PoC(Point of Care)와 대변된 가정용 헬스 장비 PHD(Personal Health Device)라 부르며 PHD 장비가 바로 본 논문에서 말하는 u-헬스 디바이스라 할 수 있다.

지난 2009년 10월 IEEE와 ISO에서는 각종 u-헬스 디바이스들과 디바이스들로부터 각각의 생체정보를 수집하는 이른바 데이터 매니저(DM, Data Manager) 간의 상호 호환성을 확보하고 관련 서비스를 활성화하기 위해 최적화된 교환 프로토콜 표준(ISO/IEEE 11073-20601)[1]을 발표한 바 있다. 현재 이 표준은 국제 표준으로서 u-헬스 디바이스와 관련한 통신을 다룬 국내외 첫 문건이기도 하다.

그러나 이 표준은 상호간 통신 프로토콜과 프레임워크에 대해서만 다루고 있을 뿐 앞서 말한 각종 보안 침해에도 불구하고 현재까지 보안에 대한 요소는 전혀 고려되고 있지 않다.

따라서 본 논문에서는 ISO/IEEE 11073-20601표준을 기반으로 반드시 추가되어야 할 보안 위협과 요구사항들을 제시하고 이를 해결하기 위한 보안 서비스와 보안을 고려한 u-헬스 디바이스를 위한 보안 아키텍처를 제안하고자 한다.

본 논문의 2장에서는 u-헬스 분야와 관련하여 최근에 발표된 표준 문건들을 살펴보고 3장에서는 u-헬스 보안에 필요한 보안 위협과 필수 요구사항들에 대해 새롭게 제안한 후, 4장을 끝으로 결론을 맺고자 한다.

Ⅱ. DVB-H 시스템

2-1 ISO/IEEE 11073-20601 표준[1]

본 표준은 u-헬스 디바이스들과 이들로부터 측정된 생체정보들을 수집하는 데이터 매니저로 구성되어 이들 상호간 정보의 표준 포맷과 상호 교환을 정의한 문서로 이들에 대한 용어는 그림 1과 같다.

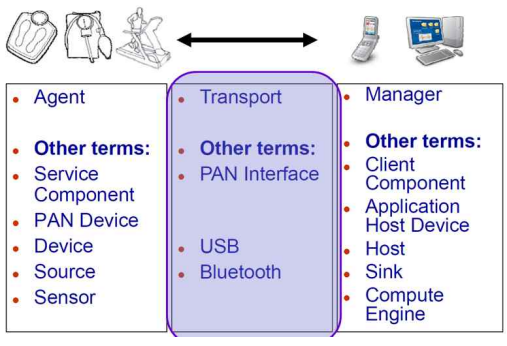

그림 1. ISO/IEEE 11073-20601 표준 용어 정의[1]
Fig. 1. ISO/IEEE 11073-20601 Standard Terms Definition[1]

그림 1에서 에이전트(혈압 측정기, 체중계, 혈당계 등으로 이후 간단히 PHD 장비로 표기한다.)는 개인들에 관한 생체 정보를 수집한 후 수집, 표시 및 추후 전송을 목적으로 관리자(게이트웨이, 핸드폰, 건강 기기 또는 개인용 컴퓨터 등을 말하여 이후 간단히 DM으로 표기한다.)에게 전송한다. 아울러 DM은 추가적인 분석 목적으로 데이터를 원격 지원 의 u-헬스 서비스 센터로 전송하기도 하며 질병 관리, 헬스 및 피트니스 또는 독립적인 연령 측정 기기 등과 같은 다양한 영역들로부터도 정보를 활용할 수 있다. PHD와 DM 사이에서의 통신 경로는 논리적인 점-대-점 연결로 가정한다. 일반적으로 PHD는 필요 시 특정 지점에 있는 단일 DM과 통신한다. DM은 별도의 점-대-점 연결을 사용하여 다수의 PHD들과 동시에 통신할 수 있다.

본 표준은 한마디로 PHD와 DM 간의 생체정보에 대한 상호 교환을 정의한 프로토콜이라 할 수 있다. 즉, 이 프로토콜은 어플리케이션 계층 서비스와 PHD와 DM 사이에서의 데이터 교환 프로토콜의 정의라는 2개의 측면으로 구성된다. 데이터 교환 프로토콜은 명령어, PHD 구성 정보, 데이터 포맷 및 전체 프로토콜로 정의된다. 또한 세부적으로는 그림 2와 같이 3 개의 시스템 모델로 나뉘며 각 모델의 역할은 다음과 같다. 이 3개의 모델들은 데이터를 표시하고, 데이터 접근 및 명령 방법론을 정의하며 데이터를 PHD로부터 DM으로 전달하기 위하여 함께 동작한다.

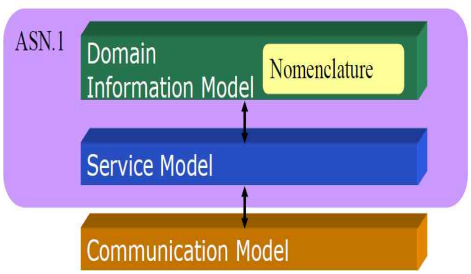

그림 2. ISO/IEEE 11073-20601 모델링[1]
Fig. 2 ISO/IEEE 11073-20601 Modelling[1]

■ DIM(Domain Information Model) : u-헬스 디바이스인 PHD와 생체 데이터 포맷(ASN.1)에 대해 기술한 것으로 PHD로부터 측정된 개인 생체 정보를 일련의 객체들로 특성화한다. 각각의 객체는 한 개 또는 다수의 속성들을 가지고 있는데 이 속성들은 행동을 제어하고 PHD의 상태에 기초하여 보고하는 요소들뿐만 아니라 DM에게 전달되는 특정 데이터를 기술하고 있다.

■ Service Model : PHD와 데이터의 상호작용에 대해 기술한 것으로 DIM으로부터 데이터를 교환하기 위하여 PHD와 DM 사이에서 전송된 데이터 접근 프리미티브(Get, Set, Action 및 event report 등과 같은 명령어들)를 제공한다.

■ Communication Model : 연결 상태 머신과 통신 특성에 대해 기술한 것으로 단일 관리자에게 점-대-점 연결 기능을 전송하는 한 개 또는 다수 PHD들의 위치를 지원한다. 각 점-대-점 연결의 경우, 동적인 액션은 연결 상태 관리자에 의해 정의되는데, 이때 연결 상태 머신이 상태를 정의하고 PHD를 설정하며, 연결, 연관성 및 운용과 관련된 상태를 포함한다. 아울러 통신 모델은 측정 데이터 전송을 위한 다양한 운용 절차를 포함한 각각의 상태들에 대한 입력, 출력 및 에러 상태를 상세하게 정의한다.

그 외 프로토콜에 대한 자세한 사항들은 표준 문건 [1]을 참조하기 바란다.

2-2 HL7(Health Layer 7) 표준[5]

본 표준은 의료정보를 다루는 소프트웨어 전반에 있어 어플리케이션 레벨에서 다루는 전송정보에 대한 상호교환에 대해 정의하고 있다. 특히 u-헬스와 관련하여서는 앞서 2.1절에서 언급한 DM과 병원 (또는 u-헬스 서비스센터)간의 상호 통신 규약을 포함한다.

한편 HL7표준은 지난 2007년 버전 2.6이 발표되었으며 2009년 현재 3.0 후보 버전이 발표된 상태이다.

보안과 관련하여서는 버전 2.6의 경우 사용자 인증 부분과 전자서명만이 반영이 되었으나 버전 3.0에서는 거의 보안 분야의 전 메커니즘에 대해 적용이 고려되고 있는 실정이다[6].

u-헬스 보안과 관련하여 현재 PHD 장비들로부터 이들 생체 정보들을 수집하는 DM간의 통신 프로토콜과 관련 데이터 포맷은 ISO/IEEE 11073표준이 적

용되고 있으며 DM으로부터 병원이나 u-헬스서비스 센터간의 통신은 HL7 표준이 적용되고 있다. 본 논문에서는 적용 범위를 현재 보안이 고려되고 있는 HL7분야가 아닌 u-헬스와 관련한 디바이스와 DM간의 보안 위협 및 요구사항에 대해서만 다루고자 한다.

III. u-헬스 보안 위협 및 요구사항

3-1 보안 위협

u-헬스 환경에서의 보안 위협은 일반적인 홈 네트워크 환경과 유사하다. 그러나 앞서 서론에서 언급한 바와 같이 u-헬스 환경은 무엇보다 환자나 혹은 이용자 개인의 병력정보나 건강과 관련된 생체 정보인 만큼 개인의 사생활 침해 즉, 프라이버시 보호가 가장 우선시 되어야 한다. 만일 그 대상이 환자일 경우 특히, 과거에 결혼 전 임신을 통해 출산을 한 사실이라든가 에이즈와 같은 병력 정보는 개인 프라이버시 보호 차원에서 반드시 보호되어야 한다. 또한 환자의 질병과 관련된 건강관리나 그밖에 u-헬스 응용에 있어 질병에 따른 생체정보를 이용하여 환자를 상담 또는 치료할 경우, 생체정보에 대해 의사나 간호사 이외 인가되지 않은 제 3자로부터 접근이 원천적으로 차단되어야 한다.

따라서 일반적인 홈 네트워크 환경의 위협 요소에 부가되어 사생활 침해와 인가되지 않은 접근의 두 요소가 무엇보다 중요하다.

지난 2006년 한국정보통신기술협회인 TTA에서는 홈 네트워크를 위한 보안 위협과 보안 요구사항에 관한 표준[7]을 제정한 바 있다. [7]에서는 보안 위협에 대해 크게 일반적인 보안 위협과 모바일 지향 보안 위협 2가지로 분류하여 기술하고 있다.

일반적인 보안 위협에 대해서는 도청/노출/가로채기, 방해/통신방해, 데이터의 삽입과 수정, 인가되지 않는 접근, 그리고 부인 5가지로 분류하고 있으며, 모바일 지향 보안 위협은 도청/노출/가로채기, 방해/통신/전파방해, 어깨너머로 보기, 원격 터미널 손실, 원격 터미널 강탈, 애기치 않는 통신 중단, 오독, 그리고 입력오류 8가지로 분류하고 있다.

그러나 홈 네트워크 환경과 달리 u-헬스 환경은 홈 서버나 응용 서버, 원격 터미널이 요구되지 않고 가벼우며 홈 네트워크와의 관계 면에서 볼 때 홈 디바이스와 보안 홈 게이트웨이가 u-헬스 환경에서 PHD와 DM과 기능적으로 유사한 것으로 생각해 볼 수 있다.

한편 u-헬스 환경은 PHD와 DM간의 관계 면에서 볼 때 혈당센서(PHD)가 장착된 휴대폰(DM)과 같이 일체형의 경우도 있고 혈압계(PHD)와 노트북(DM)과 같이 분리형의 유무선환경일 수도 있다.

본 논문에서는 보안의 대상을 PHD와 DM간의 개체를 포함한 생체 정보와 전송부분을 고려하고 u-헬스 환경의 특성을 반영하여 보안 위협요소를 일체형과 분리형으로 나누어 아래와 같이 정의하였다.

먼저 분리형의 경우 다음과 같이 모두 7가지로 분류할 수 있다.

■ 사생활 침해 : 통신 선로를 통해 데이터가 전송시 불법적인 개체로부터 사용자의 ID나 위치정보가 노출되어 발생하는 공격

■ 인가되지 않은 접근 : 통신 선로를 통해 인가되지 않은 불법적인 개체가 실제 사용자로 가장하여 PHD 디바이스에 접속하거나 혹은 디바이스를 통해 DM에 접속할 때 발생하는 공격, 따라서 이 공격은 개체가 인가되지 않은 접근 권한을 얻기를 시도할 때 식별되거나 인증되어야 한다.

■ 데이터의 삽입과 수정 : PHD 디바이스와 DM 사이에 전달되는 개인 생체 정보에 대해 인가되지 않은 개체(사람, 프로그램, 혹은 컴퓨터)에 의한 삽입, 변경, 삭제로 발생하는 공격, 이 공격은 무결성의 공격으로 공격자가 연결을 하이재킹하거나 악의있는 데이터를 보내려는 목적으로 현 연결에서 데이터를 추가할 때 발생한다.

표 1. 보안 위협과 개체와의 관계
Table 1. The relationship between security threats and objects

보안 위협 \ 종류		개체 혹은 개체와의 관계			타입	
		PHD	DM	PHD와 DM간의 관계	일체형	분리형
사생활 침해	저장데이터	0	0		0	0
	통신데이터			0	0	0
비인가된 접근	저장데이터	0	0		0	0
	통신데이터			0	0	0
데이터의 삽입과 수정	저장데이터	0	0		0	0
	통신데이터			0	0	0
디바이스 센서의 손실 및 도난			0		0	0
노출/도청	저장데이터	0	0			0
	통신데이터			0		0
가로채기	저장데이터	0	0			0
	통신데이터			0		0
통신방해				0		0
애기치않은 통신 중단				0		0

■ 디바이스 센서의 손실 및 도난 : PHD 디바이스가 물리적으로 손실 또는 강탈되어 인가되지 않은 접근으로부터 개인 생체 정보가 삭제되거나 혹은 디바이스 내에 저장된 정보까지 손실되는 공격

■ 노출/도청/가로채기 : 네트워크상에서 익명 공격자에 의해 전송되는 개인 생체정보가 노출되거나 혹은 능동적으로 가로챔, 그리고 도청에 의해 읽혀지는 공격

■ 통신 방해 : 고의적 혹은 비고의적으로 통신 선로의 송 수신측에 전원 과공급 또는 파괴의 문제로 인해 통신 선로를 사용할 수 없게 하는 공격

■ 애기치 않은 통신 중단 : 불안정한 통신 또는 전원 공급의 제한으로 인해 전송 중인 개인 생체 정보가 삭제될 수 있음

한편 일체형의 경우 두 개체간에 전송부분이 없기 때문에 전송과 관계된 노출/도청/가로채기, 통신 방해, 애기치 않은 통신 중단을 제외한 위 4가지가 보안 위협 요소에 해당한다.

아래 표 1은 각 개체 혹은 관계에 따른 보안 위협과의 관계에 대해 기술한 것이다.

3-2 보안 요구사항

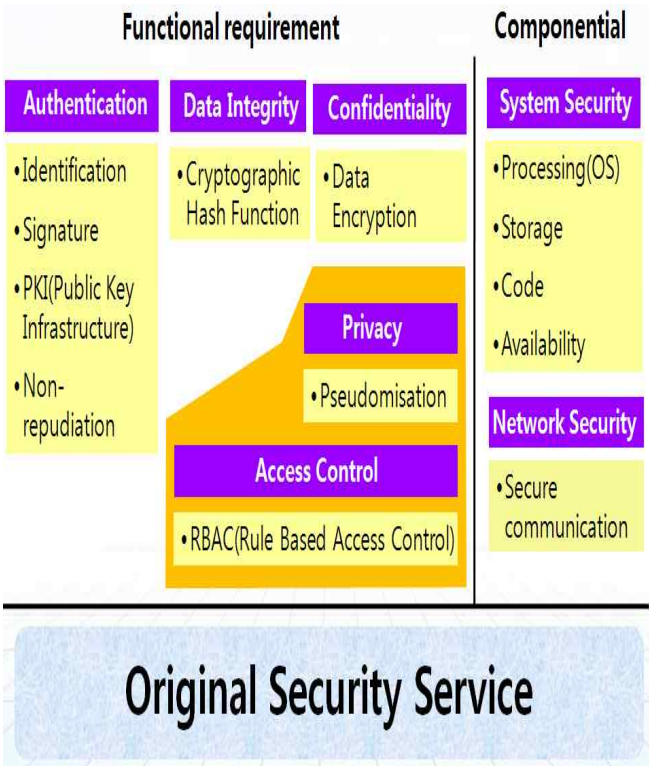

그림 3. u-헬스를 위한 보안 요구사항 및 서비스
Fig. 3 Security requirement and service for u-Health security

u-헬스 보안 요구사항의 핵심은 앞서 서론에서 언급한 대로 개인 병력정보의 사생활 침해를 보호할 수 있는 서비스를 제공하는 데 있다. 그러나 단순한 사생활 보호만으로는 앞서 3.1절에서 언급한 대로 개인 건강 정보의 오남용이라든가 위변조, 해킹 등의 위협으로부터 피해가기 어렵다.

표 2 보안 요구사항 및 보안 위협과의 관계
Table 2. The relationship between security requirements and security threats

보안 요구사항 / 보안 위협		인증		무결성		기밀성		프라이버시		접근제어		가용성		통신 흐름 보안
		실체	메시지	통신 데이터	저장 데이터	통신 데이터	저장 데이터	통신 데이터	저장 데이터	통신 데이터	저장 데이터	통신 데이터	저장 데이터	
사생활 침해	저장데이터	0	0						0					
	통신데이터							0						
비인가된 접근	저장데이터	0	0				0				0			
	통신데이터					0				0				
데이터의 삽입과 수정	저장데이터	0			0						0			
	통신데이터		0	0						0				
디바이스 센서의 손실 및 도난		0					0		0		0			
노출/도청	저장데이터	0	0				0		0		0			
	통신데이터					0		0						
가로채기	저장데이터	0	0								0		0	
	통신데이터											0		0
통신방해		0	0								0	0	0	0
애기치않은 통신 중단												0		

따라서 보안에 대한 요소는 단순한 사생활 침해를 넘어서 네트워크를 포함한 u-헬스 시스템 전반에 대해 다루어져야 한다.

이를 위해 본 논문에서는 안전한 u-헬스 서비스를 위해 필요한 기능적인 요구사항과 구성요소 관점에서 요구되는 보안 서비스에 대해 그림 3과 같이 분류하였다.

먼저 기능적인 요구사항에 대해서는 인증, 데이터 무결성, 기밀성, 프라이버시, 그리고 접근제어 5가지로 분류하였으며 각각에 대한 내용은 다음과 같다.

■ 인증 : 개체간(u-헬스 디바이스 사용자와 DM)의 신원을 확인할 수 있어야 한다. 인증은 두 가지로 개체인증과 메시지인증이 있는데 개체인증은 각 개체에 대한 신원의 유효성을 말하고 메시지인증은 메시지가 주장하는 개체로부터 온 것인지를 확인하는 것을 말한다. 즉, 메시지인증은 통신에 참여하는 두 개체가 주장하는 신원의 유효성을 검증하고 개체가 이전 통신에 대한 가장이나 인가되지 않은 재생을 시도하지 않았음을 보증한다.

■ 데이터 무결성 : 데이터 전송시 개체간에 주고받는 개인 생체 정보에 대해 결함이 없어야 한다. 즉, 인가되지 않은 변조, 삭제, 생성, 응답에 의해 보호되어야 한다.

■ 기밀성 : 데이터 전송시 개체간에 주고 받는 개인 생체 정보에 대해 당사자들 외에는 아무도 몰라야 한다. 즉, 인가되지 않은 노출로부터 생체정보를 보호하고 인가되지 않은 개체에 의해서는 읽혀질 수 없음을 보증한다.

■ 프라이버시 : 개인 병력정보 등을 포함한 개인 생체정보에 대해 본인 이외의 타인에게 그 신원이 노출되지 않아야 한다. 즉 사용자의 아이디, 지리적 위치 등이 비인가된 개체들로부터 보호되어야 한다.

■ 접근제어, 인가 : 접근이 인가된 자 만이 개인 생체정보에 대해 접근을 허용해야 한다. 즉, 네트워크 요소, 저장된 정보, 정보 흐름, 서비스, 응용으로의 접근이 인가된 사용자나 디바이스에게만 허용됨을 보증한다. 인가에는 3 종류가 있는데 접근제어리스트를 이용한 인가, 인증 서버를 이용한 인가, 권한 인증서, 그리고 인증서와 ID 인증서 속성을 이용한 인가가 있다.

구성요소관점에서는 크게 시스템 보안과 네트워크 보안 둘로 나눠 분류하였으며, 시스템과 관련하여서는 운영체제, 저장장치, 코드, 가용성에 대한 보안을 네트워크와 관련하여서는 통신 흐름에 대한 보안으로 분류하였다.

운영체제라 함은 PHD 장비나 DM 내에 장착된 임베디드 운영체제를 말하는 것으로 운영체제 내부 커널에 대한 보안을 말한다. 저장장치는 PHD와 DM 내부의 물리적 저장장치에 대한 보안을 말하며, 코드는 각 개체 디바이스 내부 또는 전송간에 처리되거나 주고받는 응용 바이너리 코드에 대한 보안을 말한다. 또한 가용성이라 함은 각 개체 디바이스가 네트워크에 충격을 받은 경우에도 네트워크 요소, 저장된 정보, 정보 흐름, 서비스와 응용으로의 인가된 접근이 거부되지 않음을 보증하는 것을 말한다.

네트워크와 관련한 통신 흐름에 대한 보안은 인가된 종단간 즉, PHD와 DM 뿐만 아니라 DM으로부터 u-헬스 서비스 센터나 병원 내 각종 정보시스템에 이르기까지 흐름이 우회되거나 가로챔이 없이 안전한 정보 흐름이 보증되는 것을 말한다.

한편 위 5가지의 요구사항과 기능적인 측면에서 가용성 및 통신흐름 보안에 대한 2가지를 추가하여 보안 요구사항과 보안 위협간의 관계를 살펴보면 표 2와 같다.

IV. 결 론

본 논문에서는 u-헬스 환경에서 특히 혈압계나 혈당계와 같은 개인 건강 의료 디바이스인 PHD와 이들 디바이스들로부터 개인 생체 정보를 수집하여 u-헬스 서비스센터로 정보를 전송하는 역할을 담당하는 데이터 매니저인 DM간에 생겨날 수 있는 각종 보안 위협과 요구사항, 서비스에 대해 제안하였다.

향후 연구로는 제안된 보안 위협들과 요구사항을 기반으로 기 표준과 호환성 있는 보안 프레임워크를 구현하여 각종 위협 요소들에 대해 실제로 검증해 보고자 한다.

감사의 글

이 논문은 2008년도 상지대학교 교수 연구년제 지원에 의한 것임

참 고 문 헌

[1] ISO/IEEE 11073-20601 : Health informatics - Point-of-care medical device communication - Part 20601: Application profile - Optimized exchange protocol, International Standard Organization, http://www.iso.org, 2009.

[2] B. Blobel and J. Zvarova, eHealth : Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge, *Methods of Information Medicine*, pp. 121-122, 2010.

[3] R. Haux, Strategic Information Management in Hospitals: An Introduction to Hospital Information Systems (Paperback), Health Informatics Series, Springer-Verlag New York Inc., 2010.

[4] H. K. Huang, PACS and Imaging Informatics: Basic Principles and Applications, 2 Edition, John Wiley & Sons, Inc., 2010.

[5] HL7 Ver 3.0 Nominative edition, Helath Level 7 International, http://www.hl7.org, 2009.

[6] A. E. F. Zuniga, K. T. Win, and W. Susilo, Biometrics for Electronic Health Records, Journal of Medical Systems, Published Online, http://www.springerlink.com /content/4727307m51027076/, June 2009.
[7] TTAI.KO-12.0035 : 홈 네트워크를 위한 보안 기술 프레임워크, *한국정보통신기술협회*, http://www.tta.or.kr, 2006.

김 순 석(金純錫)

1997년 2월 진주산업대학교 컴퓨터공학과(공학사)
1999년 2월 중앙대학교 컴퓨터공학과(공학석사)
2003년 2월 중앙대학교 컴퓨터공학과(공학박사)
2003년 3월～현재 한라대학교 컴퓨터공학과 조교수
관심분야 : 정보보호, 암호응용, 생체보안

박 홍 진(朴洪珍)

1993년 2월 원광대학교 컴퓨터공학과 (공학사)
1995년 8월 중앙대학교 컴퓨터공학과 (공학석사)
2001년 8월 중앙대학교 컴퓨터공학과 (공학박사)
2001년 9월～현재 상지대학교 컴퓨터정보공학부 부교수
관심분야 : 분산 시스템, 센서 네트워크, 모바일시스템