USN기반 u-Healthcare 시스템 트래픽도메인 환경에서의 보안위험도 평가체계 설계방안

노시춘*

요 약

의료정보 기술의 Smart 환경, Ad-hoc networking, 무선통신 환경은, u-Healthcare 요소기술과 함께 정보보안 취약성을 증가시키는 주요 요인이다. 트래픽 도메인이란 u-Healthcare 의료정보시스템을 통과하는 트래픽 구간의 구분 영역으로서 보안기술의 적용이 가능하도록 네트워크 영역을 구분하는 개념이다. 그 구분의 기준은 보안기술의 적용이 필요한 영역. 트래픽 경로와 트래픽 성격이 타 도메인과 차별화 가능한 영역. 보안기술 적용시 타 영역의 보안기능으로 기능 중복이 발생치 않는 영역이다. u-Healthcare 의료정보시스템 도메인은 사용자단말구간, 공중통신망 인프라구간 ,네트워킹구간, 인트라넷구간으로 도출된다. 의료정보시스템을 도메인별로 구분하여 취약점을 평가하는 이유는 도메인별로 취약점에 대한 대처방법이 다르게 도출되기 때문이다. 본 연구는 의료정보시스템 도메인을 도출하고 도메인별 보안취약성 진단체계를 설계하여 USN 기반 u-Healthcare 시스템에서의 보안대책을 강구하기 위해서 이다. 본 연구에서 제안하는 모델을 사용할 경우 현재까지 막연하게 진행 되어온 USN 기반 의료정보네트워크 보안취약성 진단대책 수립 방법을 좀 더 효과적으로 수행 할 수 있을 것 으로 기대한다.

A Building Method of Security Vulnerability Measurement Framework under u-Healthcare System Traffic Domain Environment Based on USN

SiChoon Noh*

Abstract

Smart environment of health information technology, u-Healthcare architecture, ad-hoc networking and wireless communications environment are major factors that increase vulnerability of u-healthcare information systems. Traffic domain is the concept of network route that identifies the u-Healthcare information systems area as the traffic passing and security technologies application. The criterion of division is an area requiring the application of security technology. u-Healthcare information system domains are derived from the intranet section, the public switched network infrastructure, and networking sectors. Domains of health information systems are separated by domain vulnerability reason. In this study, domain-specific security vulnerability assessment system based on the USN in u-Healthcare system is derived. The model used in this study suggests how to establish more effective measurement USN-based health information network security vulnerability which has been vague until now.

keywords : Domains of health information systems,Network security,Measurement methodology

접수일(2011년 05월 28일), 수정일(1차: 2011년 06월 16일), 게재확정일(2011년 06월 20일)

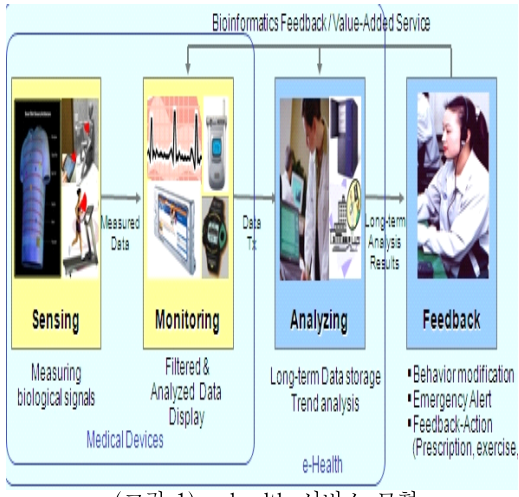
* 남서울대학교 컴퓨터학과

1. 서 론

유비쿼터스 기술을 기반으로 병원이 아닌 환자의 집, 사무실 또는 이동 중에도 의료서비스를 받을 수 있는 u-Healthcare 서비스는 모바일 의료서비스의 진화 모델이다. u-Healthcare 서비스에서 사용되는 센서네트워크는 네트워크시스템 중 다수의 센서 노드로 이루어진 네트워크를 말하며 각각의 센서 노드는 주변 환경을 센싱하여 정보를 수집한다. 센서 네트워크 기술은 인간의 생활환경 모니터링, 야생동물 관찰, 군사용 감시 등 용도로 개발되었으나 최근에는 의료부분에 활발하게 적용되고 있다. 환자가 병원에 오기 전에 혹은 병원 내에서 환자가 이동하면서도 환자 상태를 모니터링 할 수 있고 집에서 모니터링이 가능하여 지속적이고 꾸준한 데이터를 수집할 수 있다. Lifeguard System, Vital Pointing System, Caregiver's Assistance는 원격의료 기술로서 모두 인간생활에 필요한 기술이자 환자의 진료와 치료에 도움을 주는 u-헬스케어 서비스 센서네트워크 모델이다. u-헬스케어 서비스는 무선 어플리케이션으로서 Bluetooth나 802.11을 기반으로 하는 아날로그 Wireless Medical Telemetry Service (WMTS) bands를 사용한다. 본 연구는 무선네트워크 기반의 u-Healthcare 시스템의 트래픽 처리경로를 기준으로 보안취약성 진단체계를 제시하여 의료정보 보안대책을 1차적으로 연구하고자 한다. 본 연구의 진행 순서는 u-Healthcare 서비스모델 진단, u-Healthcare 모델 WSN(Wireless Sensor Network) 트랙픽 도메인 진단, u-Healthcare 모델 트래픽 처리기술 진단, u-Healthcare 모델 WSN 취약점 진단체계 설계,도메인별 취약점 평가 순서이다[1][3].

2. u-Healthcare 서비스 모델

u-Healthcare 서비스는 공간적, 시간적 제약을 없애고 환자가 생활 공간 속에서 다양한 의료센서 및 기기를 통해 수집된 생체 정보와 환경정보를 기반으로 중앙의 원격 의료 서비스 시스템을 통해 언제 어디서나 의료피드백을 받을 수 있는 서비스를 총칭한다. u-헬스케어 서비스는 스마트 의료 센서부, 수집된 각종 생체 신호의 분석부, 지속적인 건강상태 모니터링 및 데이터 축적부, 응용 서비스를 위한 정보교환 인터페이스 및 사설 방화벽 등으로 구성된다. 이와같은 프레임워크를 기반으로 원격으로 환자상태를 상시 체크할 수 있는 smart mirror, 상처의 병원체 감염유무를 상시 감시·보고하는 smart bandage, 복용 약에 대한 정보와 복용 유무를 알려주는 smart drug등의 서비스가 개발되었다. u-healthcare 서비스는 전자의무기록시스템(EMR)은 물론 처방전달시스템(OCS), 의료영상전달시스템(PACS),임상병리시스템(LIS), 일반관리시스템(ERP), 그룹웨어, 홈페이지 등과 연계시켜 진료 및 경영의 효율을 향상시켜 의료진뿐 아니라 환자와 병원 관계자의 편의성을 추구한다. u-health 서비스 모델로 Lifeguard System, Caregiver's Assistant,Vital Positioning System등을 들수 있다[4].



(그림 1) u-health 서비스 모형

출처 : 연세대학교 채영문, u-Health의 활성화 방향

3.u-Healthcare트랙픽도메인설정

3.1 트래픽 도메인 분류기준

u-Healthcare 의료정보 트래픽도메인 이란 유헬스 의료정보시스템을 통과하는 트래픽 구간의 구분 영역

이다. 네트워크 구조상에서 패킷은 소통 경로를 따라 정보가 유통되며 이 경로에서 보안 기능 수행이 필요하고 타도메인과 차별화가 가능하다. 따라서 구분된 영역 기준에 따라 보안 적용을 차별화하여 적용할 필요성이 제기 된다. 본 논문에서 구현하고자 하는 기능은 보안정책 적용 대상인 네트워크 그룹을 도메인이라는 개념으로 구분하는 일이 먼저 필요하다. 본 논문에서 사용하는 의료정보시스템 트래픽구간별 도메인 분류는 다음의 기준에 따라 설정한다. 보안기술 적용이 가능하도록 네트워크 영역을 구분한다. 구분기준은 보안기술의 적용이 필요한 영역. 트래픽 경로와 트래픽 성격이 타도메인과 차별화가 가능한 영역. 보안기술 적용시 타 영역의 보안기능으로 기능중복이 발생치 않는 영역에 따라 도메인을 설정하는 기준은 다음과 같다[6].

<표 1> u-Healthcare 보안 도메인 설정기준

유형	내 용
A	보안기술 적용 가능 영역
B	보안 기술의 적용이 필요한 영역
C	경로성격이 타도메인과 차별화 가능
D	보안 기술적용시 기능중복이 미 발생

3.2 트래픽도메인 구간 설정

3.2.1 센싱 구간(제1구역)

u-Healthcare 의료정보시스템 네트워킹 도메인 첫 번째 구간은 센서 구간이다. 센서는 수동형과 능동형으로 나누어지며, RFID는 무선으로 정보를 주고받을 수 있는 초소형 태그로 바코드를 대체할 기술이다. 센싱구간은 특정 상황이나 환경에 대한 센싱이 가능한 센서(Sensor Node)와 수집된 정보를 처리하는 프로세서, 그리고 데이터를 송수신하는 장치 (Sink Node)로 구성된다. 센서 네트워크 소프트웨어는 UC 버클리와 같은 TinyOS, microthreading, 데이터베이스, 스토리지 관리(TinyDB), 네트워크 프로토콜(802.15.4, ZigBee), 보안 (TinySec)이 사용된다. 유비쿼터스 센서 네트워크는 필요한 장소와 사물에 전자태그(RFID Tag)설치로 시작된다. RFID태그는 사물의 인식정보(identification information)와 주변의 온도, 습도, 오염정보, 균열정보 등의 환경정보를 탐지(sensor)하고 수집된 정보를 실시간으로 네트워크에 연결하여 새로운 정보들로 가공 및 관리한다[4][7].

○ 보디(body)센싱 구간

u-Healthcare 의료정보시스템 센서구간은 보디(body)센서와 환경센서로 나눈다. 보디(body)센서는 환자의 몸에 부착되는 센서 장치로 인체 활동을 감지하는 다수의 작고 가벼운 장치 센서가 부착된다. 사람의 신체적, 행동적 특징을 자동화된 장치로 추출하고 분석하여 정확하게 개인의 신원을 확인하는 기술. 넓은 뜻으로는 생물 데이터를 측정, 분석하는 기술을 의미하나 정보 기술에서는 지문, 눈의 망막 및 홍채, 음성, 얼굴 표정, 손 측정 등 인증 목적으로 사람의 신체 특성을 측정, 분석하는 기술이다 .외부의 정보나 환경(예: 온도)을 인지하기 위한 기술. 사람으로 말하자면 감각에 해당하는 기능을 수행하는 기술로 대상물의 상태를 파악하고 전기신호로 전달하는 것이 일반적이다[9].

○ 환경센싱 구간

u-Healthcare 의료정보시스템 환경센서는 집안, 공장, 사무실등 인간생활 공간상의 가전 ,전자 기구에 장착된 센서이다. 센서들 사이는 무선 또는 유선 네트워크를 구성하여 연결 하며 환경을 스스로 인지하고 판단하기 위한 센서와 프로세서이다. RFID에서 센서는 다양한 종류의 태그가 그 역할을 한다. 프로세서는 RFID 태그 안에 포함되는 칩을 의미하며 원활한 커뮤니케이션을 위해서는 RFID에 안테나를 부착하고 RFID 태그를 읽을 수 있는 리더기를 사용할 수 있다. 센서 네트워크는 센서 노드의 크기가 작아 전력 소모 및 컴퓨팅 능력, 메모리 등에 제한이 가해지며, 무선을 통해 센싱된 값을 전달하는 특징을 가지므로 노드 포획, 도청, 서비스 거부 공격, 라우팅 경로 공격 등 다양한 공격에 노출될 수 있는 특징을 가진다[8].

3.2.2 사용자PC 구역(제2구역)

u-Healthcare 의료정보시스템 네트워킹 도메인에서 두 번째로 설정되는 구간은 웹브라우저가 작동하

는 PC 구간이다. 이 구간 에서는 이용자가 정보를 열람하고 입력하며 입력정보를 전송하는 단순기능이 주류이다. 그러나 PC를 대상으로 하는 많은 해킹기법이 등장하고 해킹을 자동화 형태로 발전시킨 웜이 증가하며 PC에 저장된 개인정보를 자동으로 유출시키는 바이러스로 인해 서버시스템에 버금가는 위협이 등장하는 영역이다. 특히 클라이언트 보안위협은 윈도우, 인터넷익스플로러, ActiveX컨트롤 환경에서 기인한다.

○ 사용자PC 구역 : 유선랜 구간

랜의 범위는 통상 1~ 10㎞의 규모로 하고 있으나 게이트웨이를 통해 외부의 네트워크와도 접속할 수 있다. 의료진이 직접 입력하는 환자관련 개인정보가 있으며 또한 공인인증서 등의 저장정보가 있다. 이러한 정보를 획득하기 위하여 사용되는 Tools로는 Backdoor 프로그램과 Key Stroke 프로그램 등이 있다. 이 구간에서는 웹 브라우저 메뉴를 이용한 콘텐트 유출, 웹 브라우저 기본 메뉴기능 이용 웹 콘텐트 유출(저장,다른 이름으로 저장,인쇄,내보내기,소스보기) 등이 취약점 이다. 또한 화면 및 이미지 변환 유출, Screen Capture Program, 화면 프린트 스크린 기능을 이용하여 이미지 변환후 유출 (Snagit, HyperSnap) 등이 있다. 키보드, 마우스를 이용한 유출, 키보드 단축 키, 마우스 우측버튼 등 이용, 웹 콘텐트 유출(Ctrl+C, Ctrl+P, Drag & Drop),웹 브라우저 캐싱 데이터 이용 유출이 위험성 으로 지적된다[10].

○ 사용자PC 구역 : 무선랜(802.11b)구간

u-Healthcare 의료정보시스템 네트워킹 도메인에서의 사용자 PC 구역을 무선랜(802.11b)전송 구간으로 구분한다. 이 구간에서는 일반적으로 2.4GHz ISM 대역의 무선랜(802.11b)이 사용된다. 전송거리는 300moutdoor, 30mindoor 정도이며 11Mbps의 최대속도를 제공하는 DSSS 방식의 무선랜 표준을 사용한다. SSID(SSID는 무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여 지는 32바이트 길이의 고유 식별자로서, 무선장치들이 BSS(basicserviceset)에 접속 할 때 마치 암호처럼 사용한다. SSID는 하나의 무선랜을 다른 무선랜으로부터 구분해 주므로, 특정 무선랜에 접속 하려는 모든 AP나 무선장치들은 반드시 동일한 SSID를 사용한다. SSID는 패킷상에 부가된 평범한 텍스트 데이터 이므로 충분히 스니프 당할 가능성이 있기 때문에 네트워크에 대해 어떠한 보증도 하지 않는다[10].

3.2.3 원격 통신망 구역(제3구역)

u-Healthcare 의료정보시스템 네트워킹 도메인에서 제3구역으로 설정되는 구간은 원격 통신망 구역으로서 인터넷통신 구간과 원격 무선통신으로 구분 할 수 있다. 인터넷 통신 구간에서는 오픈 프로토콜인 TCP/IP 통신 프로토콜을 사용하므로 Line Tapping, 중계기관, 업무담당자 등에 의하여 송·수신되는 정보의 노출이 이루어질 수 있다. 이 구간에는 환자의 진료기록 원장 등 주요정보는 저장되지 않지만 내부 직원에 의한 인터넷 접속의 정보유출 취약점은 유의해야 한다. u-Healthcare 의료정보시스템 네트워킹 도메인에서 제3구역으로 설정되는 구간은 원격 통신망 구역으로서 원격 무선 통신구간을 설정할 수 있다. 선박, 항공기, 자동차 등의 이동체와 고정국과의 상호 무선통신. 무선국이 이동하는 장소에 따라 육상이동무선, 해상 이동무선, 항공 이동무선 등으로 분류된다. 원거리 통신인 경우는 장파, 중파, 단파가 사용된다. 통신 범위가 좁은 경우는 초단파(VHF)대나 극초단파(UHF)대가 사용되며, 60MHz, 150MHz, 400MHz, 800MHz대가 주로 이용된다[11].

3.2.4 의료정보호스트 구간(제4구역)

의료정보 호스트 구간에는 환자진료기록 원장, 치료기록, 의료 개인정보 등 중요정보가 집중되고 다수 직원 접근으로 정보유출 문제가 가장 심각한 부분이다. 네트워크 보안을 강화해도 서버영역은 별개의 보호장치가 요구된다. 웹 서비스를 제공하기 위하여 웹 서버를 구축할 때, 관리자는 웹 서비스가 공격에 노출되지 않도록 서버 프로그램의 설정에 주의를 기울여야 하며, 서버가 설치된 호스트의 보안성을 강화하여야 한다. 호스트 구간에서는 분석,필터링, 로깅 구간으로서 데이터가 모아져 base station으로 전송되므로 다양한 환자상태 정보를 판독 하고 분석한다.

모니터링 결과 다양한 화면을 통해 환자에게 필요한 정보제공. 약물복용 시간, 응급조치, 건강관리방법, 병원후송 지시를 피드백 한다.

4. 도메인별 취약점 진단체계

4.1 기본 프레임워크

u-Healthcare 의료정보시스템 도메인은 사용자 단말구간, 공중통신망인프라구간 ,네트워킹구간, 인트라넷구간으로 구분된다. 사용자단말 구간은 의료인력에 의해 진단, 진료 서비스가 수행되는구간이며 일반 고객이 정보시스템을 이용하는 사용자 영역이기도 하다. 이 구간에서는 사용자가 원격통신을 이용하여 건강검진 행위를 센싱 하여 그 결과를 통신망을 통해 의료정보 시스템으로 전송하게 된다. 센싱구간은 여러 가지 형태가 있지만 일반적으로 센서기능, 전송기능, 원격모니터링, 처방 및 진료 등 4개 과정을 거친다.

<표 2> u-Healthcare 보안 도메인 설정

구간범위		통신방법
센서노드,프로세서,싱크노드		Bluetooth,태그 =마이크로 칩 + R 및안테나
PDA-access-point-게이트웨이		무선자원 송수신 역할
서버구간	호스트 컴퓨터	응용프로그램(ERP,SCM)LAN통신
데이타베이스구간	각종 데이터를 저장역할	정보를 저장하고 프로토콜데이터교환
유선랜 구간	내부유선통신 PC-host LAN통신	프로토콜데이터교환
무선랜 구간	인트라넷내부 무선LAN통신	프로토콜데이터교환
전용선통신	단말기-교환기-단말기	유선통신
무선통신	단말기-교환기-단말기	무선통신
인터넷통신	단말기-교환기-단말기	유선통신

4.2 기술적 보안 취약점 점검방법

u-Healthcare 시스템상에서 취약점점검 분야는 기술구조를 기준으로 네트워크, 서버, 운영체제, 데이터, 프로그램,통신프로토콜,단말시스템시스템으로 구분된다. 취약점 점검방법은 수동점검과 자동점검 으로 구성된다. 점검은 네트워크, 운영체제, 데이터베이스,서버시스템, 클라이언트,.기타로 구분된다. 기술적 보안 취약점 측정체계 설계의 방향에 의거하여 취약점 점검은 취약점 점검도구를 이용 하거나 수동으로 점검항목에 대한 기술적 취약점을 탐지한다. 수동점검은 점검대상 시스템을 대상으로 체크리스트 점검을 실시한다 [10].

1) 네트워크구조 진단
- 시스템구간 네트워크도메인 분리수준
- 시스템구간 보안차단 기능수준
- 시스템구간 침입탐지 기능수준
- 네트워크도메인 분리수준

2) 공인인증서구조/암호화통신 보안측정
- 상호인증 기능의 안전성 여부
- 키 값의 송수신시 비밀성 여부
- 키 교환프로토콜 안전성 여부

3) 시스템분야 보안 측정
- 128bits 키 값 암호화 전송 여부
- 인터넷통신 도청, 감청 가능성
- 전송데이터 변조 가능성

4) 클라이언트 보안측정
- 윈도우 보안 설정 여부
- 운영체제 방화벽
- 인터넷익스플로러 보안 설정 여부
- Active-x 보안 설정 설정 여부
- 패스워드 안전성 설정 여부
- 보안업데이트 준수여부
- 매크로보안 설정 여부
- 보안패치 준수여부

5) 센싱보안 측정
- 경량 암호 및 인증 기술 사용여부
- 경량 키 관리 기술 사용여부
- 프라이버시보호 기술 사용여부
- 부 채널 공격방지 기술 사용여부

6) 개인정보 침해 (Private domain)환경 측정
- 내부인에 의한 의료정보 조작 노출 가능성
- 컴퓨터바이러스로 진단오류, 위협 가능성
- 생체/ID정보, 생체상태 정보, 생체분석 정보 유출 가능성

<표 3> 점검 양식/ 측정TOOL활용/ 자동점검

구분	항목	세부항목	점검 결과
• 네트워크, • 운영체제, • 데이터베이스 • 애플리케이션 • 클라이언트	• 네트워크스위치 • 네트워크라우터 • 운영체제 • 데이터베이스,• 애플리케이션,• 클라이언트	• 패스워드 인증등 네트워크 취약성 • 시스템 Trust 관계 등 영체제취약성 • 사용자별 리소스 사용 권한등 데이터베이스 취약성 • Hidden Manipulation 입력값등 웹애플리케이션 취약성 • 웹 브라우저 취약점등 클라이언트 취약성	• 취약서버수 • 안전서버수 • 취약율(%)

4.3 취약점 점검 도구

u-Healthcare 의료정보시스템 취약점 진단 도구는 취약점 스캐너 또는 보안 스캐너로 불리며 컴퓨터 시스템 상에 존재하는 취약점을 진단하고 발견하여 해결방안 및 적절한 패치 정보를 제공하여 시스템을 안전한 상태로 유지할 수 있도록 하는 보안도구이다. 네트워크 스캐너는 외부의 해커가 공격 가능한 모든 취약점을 진단하는데 네트워크 취약점 진단 시스템이 설치된 원격 시스템에서 특정 네트워크에 연결된 시스템이나 네트워크의 취약점을 알아내는 것이 목적이므로 특정 시스템이 내부적으로 가지고 있는 취약점을 모두 파악하는 것에는 한계가 있다. 시스템 취약점 점검도구는 패스워드의 취약점을 비롯한 내부 취약점, 설정오류, 파일 퍼미션 오류 등을 점검하고 중요파일 서버, 이메일 서버, 웹 서버, 디렉토리 서버, 원거리 접근 서버, 데이터베이스 서버, 다른 어플리케이션 서비스 실행서버 등 보호를 목표로 한다.

5. 도메인별 위험도 평가체계 설계

5.1 평가체계 개관

u-Healthcare 시스템 취약점 진단체계를 설계하여 도메인별 취약점을 정량적으로 평가해야 한다. 도메인별 취약점을 평가하는 이유는 평가를 통해서 취약점에 대한 대처방법이 다르게 도출되기 때문이다. 취약점 평가는 위협요인이 자산에 손실을 야기 시키거나 부정적 결과를 확대시킬 수 있는 약점을 산정하며 보통 0에서 1까지 척도로 측정결과를 계량화 한다. 자산과 위협간 어느정도 관계가 있는지, 즉 특정 위협이 발생할때 특정자산에 자산의 가치와 관련하여 어느정도 피해가 발생할지를 취약성, 노출정도(Exposure) 또는 효과(Effectiveness factor) 라는 값으로 나타낸다. 평가기준은 평가항목 설정과 평가항목별 등급설정 및 평가과정이다. 평가항목별 등급 설정시 일반적으로 3개등급을 설정하거나 좀더 자세한 등급을 설정할 필요가 있을 경우 5개등급 으로 설정한다.

5.2 평가 모형

위협은 정보시스템 자산에 대한 내외부로부터의 보안 침해위협이며 취약성은 운용중인 정보시스템 자산이 위험에 노출될 수 있는 가능성이다. 보안체계는 정보보호침해 위험을 회피 또는 감소 시킬 수 있는 기술적 분야의 대응체계 이다. 위험도 산정 방향은 1) 현재운용중인 정보시스템 자산이 진단당시의 환경에서 위협, 취약성진단 결과 어느정도의 위험수준을 보여주고 있는가를 산정한다. 2) 위협평가, 취약성평가, 보안체계 평가결과를 연계하여 산출한다. 위험도 산출은 다음공식을 사용한다.1) 위협 = 위협영향*위협발생빈도 (T), 2) 취약성 = 자산이 가지고 있는 정보보호항목 약점의 수치 (V), 3) 자산가치= 자산가치 (A),위험도 = 위협, 취약성, 자산가치 승산에 의한 연간예상손실 수치(ALE : Annual Loss Exposure) =T*V*A

<표 4> 위험도 산정 조사표

위협	VL					L					M					H				
취약성	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH
VL																				
L																				
M																				
H																				
VH																				

5.3 종합 위험도 수준 산출

u-Healthcare 시스템 기술적 보안 취약성 점검은 기술적보안 전체영역 중 정보시스템 자산에 대한 내외부로부터의 보안 침해 위협 가능성을 점검, 평가하는 과정이며 운용중인 정보시스템 자산이 위험에 노출될 수 있는 가능성과 수준을 점검, 평가하는 것 이다. 이를 위해 정보시스템에 가해지는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 현행 보안대응 체계를 진단, 평가하며 조사된 정보시스템 자산에 가해지는 위협과 내부적인 취약성 및 이를 대처하는 대응체계를 연계 분석하여 현재의 위험수준을 종합적으로 평가하는 방법론이다. 모든 평가결과는 다음과 같이 위협영향 평가와 위험도 산출결과에 의한 위험도 수준 으로 나타난다.

<표 5> 위협영향 평가

등 급	지수	위협영향 수준
VL	1-20	정보자산에 경미한 영향
L	21-40	정보자산에 경미한 피해 발생
M	41-60	정보시스템에 일정수준 피해
H	61-80	정보시스템 중단 상황, 복구에 수시간 소요
VH	81-100	정보시스템의 영구적 중단 상황, 복구에 장기간 소요

<표 6> 도메인 위험도 종합 수준

구분	VL	L	M	H	VH
위험도	1-25	26-50	51-75	76-100	101-125

6. 결 론

모든 u-Healthcare 시스템이 보안 취약점을 가지고 있지만 이것이 시스템을 사용할 수 없을 정도의 심각한 결함을 의미하지는 않는다 하더라도 이러한 취약점은 로컬(local) 또는 네트워크(network) 상에서의 침입에 큰 손상을 입을 잠재적인 위험이 된다. u-Health시스템의 보안 성공 여부는 시스템이 가지고 있는 취약점의 위험도나 공격의 강도, 대응 수단의 효율성에 따라 결정된다. 취약점 자체로서는 직접적인 위험을 초래하지 않지만 위험을 발생시킬 환경을 제공하게 되는데 일반적으로 대응방법이 늘어날수록 취약점은 감소하지만 대응 자체 역시 완벽할 수 없으므로 잠재적인 취약점은 항상 지니고 있다.

u-Healthcare 시스템의 위험평가 결과에 따라 시스템 접근권한 관리 및 발생가능한 사고 대응등에 관련한 보안관리 기술을 활발히 개발하여 u-Healthcare 시스템 환경에서 사용자의 Wellness와Healthcare의 Needs를 충족시켜주는 역할을 지속하여야 한다.

참고문헌

[1] K.F. Akyildiz et al., “wirelesssensornetworks :asurvey”,Computernetworks,Vol.38,pp.393-422, March2002.

[2] Sensor Networks for Medical Care, Victor Shnayder, Bor-rong Chen, Konrad Lorincz, Thaddeus R. F. Fulford-Jones, and Matt Welsh. HarvardUniversity TechnicalReport TR-08-05,April2005.

[3] Sensor Networks for Emergency Response: Challenges and Opportunities, Konrad Lorincz, David Malan, Thaddeus R. F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoff Mainland, Steve Moulton, and Matt Welsh. In IEEE Pervasive Computing, SpecialIssueonPervasiveComputingforFirstResponse,Oct-Dec2004.

[4] A Portable, Low-Power, Wireless Two-Lead

EKG System, Thaddeus R. F. Fulford-Jones, Gu-Yeon Wei, and Matt Welsh. In Proceedings of the 26th IEEE EMBS Annual International Conference, SanFrancisco, September2004

[5] CodeBlue: An Ad Hoc Sensor Network Infrast ructure for Emergency Medical Care, David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. International Workshop on Wearable and Implantable Body Sensor Networ ks, April 2004.

[6] Biomedical telemedicine - CSCI E-170 January 11, 2005

[7] Healthwear:Medical Technology Becomes Wear able - 2004 IEEE

[8] Vital Positioning System Product Page, Medical Intelligence website, Retrieved December 28, 2004.

[9] Lifeguard User Guide, Stanford Lifeguard Website, Retrieved December 23, 2004

[10] Lifeguard Overview, Stanford Lifeguard Webs ite, Retrieved December 23,2004 URL: http://lifeguard.stanford.edu/lifeguard_flyer.pdf

[11] Perrig, A., Stankovic, J., and Wagner, D. 2004. Security in wireless sensor networks. Commun. ACM 47, 6 (Jun. 2004), 53-57.

[저 자 소 개]

노 시 춘 (SiChoon Noh)

1987년 2월 고려대학교
경영정보학(석사)
2005년 2월 경기대학교
정보보호기술(박사)
2002년 11월 KT 시스템보안부장
2004년 12월 KT 충청전산국장
2005년3월 ~현 재 : 남서울대학교
컴퓨터학과 교수
2011년2월 ~현 재 : 남서울대학교
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr