u-헬스케어시스템의 정보보안 체계 확보를 위한 5단계 보안위험도 평가모델 설계

노시춘*

요 약

모든 u-헬스케어 시스템은 보안 취약점을 가지고 있다. 이 취약점은 로컬(local) 또는 네트워크(network) 상에서 잠재적인 위험이 된다. 의료정보 기술의 Smart 환경, Ad-hoc networking, 무선통신 환경은, u-헬스케어 보안 취약성을 증가시키는 주요 요인이다. u-헬스케어 의료정보시스템 도메인은 사용자단말 구간, 공중통신망 인프라구간 ,네트워킹구간, 인트라넷구간으로 구분된다. 의료정보시스템 도메인별을 구분하여 취약점을 평가하는 이유는 도메인별로 취약점에 대한 대처방법이 다르기 때문이다. u-헬스케어시스템 5단계의 보안위험도 평가체계는 도메인별 보안취약성 진단체계를 설계하여 보안대책을 강구하기 위해 필요하다. 제안하는 모델을 사용할 경우 현재까지 막연하게 진행 되어온 USN 기반 의료정보네트워크 보안취약성 진단대책을 좀 더 체계적으로 수행할 수 있는 모형을 제공한다.

A Study on Five Levels of Security Risk Assessment Model Design for Ensuring the u-Healthcare Information System

Si Choon Noh*

ABSTRACT

All u-Health system has security vulnerabilities. This vulnerability locally(local) or network(network) is on the potential risk. Smart environment of health information technology, Ad-hoc networking, wireless communication environments, u-health are major factor to increase the security vulnerability. u-health care information systems user terminal domain interval, interval public network infrastructure, networking section, the intranet are divided into sections. Health information systems by separating domain specific reason to assess vulnerability vulnerability countermeasure for each domain are different. u-Healthcare System 5 layers of security risk assessment system for domain-specific security vulnerability diagnosis system designed to take the security measures are needed. If you use this proposed model that has been conducted so far vaguely USN-based health information network security vulnerabilities diagnostic measures can be done more systematically provide a model.

keywords : Security Risk Assessment, Model Design, 5 Layers, u-Healthcare System, USN

접수일(2013년 8월 31일), 수정일(1차: 2013년 9월 11일), 게재확정일(2013년 9월 12일)

* 남서울대학교 컴퓨터학과

1. 서 론

u-헬스케어 서비스에서 사용되는 센서네트워크는 네트워크시스템 중 다수의 센서 노드로 구성되는 네트워크를 말하며 각각의 센서 노드는 주변 환경을 센싱하여 정보를 수집한다. 센서 네트워크 기술은 인간 생활환경 모니터링, 야생 동물 관찰, 군사 감시 등 용도로 개발 되었으나 최근 의료부분에 활발하게 적용되고 있다. 환자가 이동하면서 환자상태를 모니터링 할 수 있고 원격 모니터링이 가능하여 지속적이고 꾸준한 데이터를 수집 할 수 있다. u-헬스케어 의료정보는 무선인프라 환경에서 전송 되므로서 이 환경에서는 관련자 모두 접근이 가능하며 내부인에 의한 의료정보 조작이나 노출, 개인의료정보가 불순한 의도로 수정이나 조작 가능성이 커진다. 시스템의 보안 성공여부는 시스템이 가지고 있는 취약점 위험도나 공격의 강도, 대응수단의 효율성에 따라 결정된다. 본 논문에서는 USN 기반 u-헬스케어 시스템 환경의 의료정보보안 문제점을 해결하고 보다 강력한 방어를 수행하기 위해 취약점 평가체계를 제안한다. 본 연구의 목적은 무선 네트워크 기반의 u-헬스케어 시스템의 트래픽 처리경로를 기준으로 보안취약성 진단체계를 제시하여 의료정보 보안대책을 1차적으로 강구하고자 하는 것 이다. 논문 기술순서는 5단계 취약점 평가관리 필요성, 5단계 보안위험도 평가체계 설계, 결론이다.

2. 5단계 취약점 평가관리 필요성

u-헬스케어 의료정보시스템상에 취약성이 존재하지 않으면 위협 발생 시 손실이 없게 된다. 따라서 취약성은 자산과 위협 연관관계를 갖는다. 자산과 위협 간 어느정도 관계가 있는지, 즉 특정 위협이 발생할 때 특정자산에 자산의 가치와 관련 하여 어느정도 피해가 발생 할지를 취약성, 노출 정도(Exposure) 또는 효과 값으로 나타낸다. 취약점 자체로서는 직접적 위험을 초래하지 않지만 위험을 발생시킬 환경을 제공하게 되는데 일반적으로 대응방법이 증가할수록 취약점은 감소 하지만 대응 역시 완벽할 수 없으므로 잠재적 취약점은 항상 지니고 있다. u-헬스케어 시스템은 매우 다원화된 정보 시스템의 구조로 변화되고 있다. 접속접 다양화, 다원화는 보안위협 가능성을 증대시킨다. u-헬스케어시스템의 어떤 특정구간과 자원만을 대상으로하는 보안 대책으로는 복잡한 구조의 보안취약점 해결이 어렵다. u-헬스케어 의료정보 시스템 보안 취약성 평가틀은 1. u-헬스케어 의료정보시스템 연동기능 파악, 2.트래픽 도메인 구조의 진단, 3. 도메인별 취약점 진단체계 설계, 4. 위험도 평가체계 설계, 5. 실제 평가 작업 등 5개단계로 이루어 질 필요가 있다[1][2].

3. 5단계 보안위험도 평가체계설계

본 연구의 전체적인 틀은 u-헬스케어 의료정보 시스템 무선 트래픽 연동구간을 파악하고 이를 대상으로 취약점 진단체계를 설계하는 방법이다. 본 연구에서 제안하는 5단계 평가체계 구성은 유헬스 무선 트래픽 연동구간 파악, 트래픽 도메인 진단, 도메인별 취약점 진단체계 설계, 위험도 평가 체계 설계, 위험도 평가작업이다. 도메인별 취약점 진단체계 설계는 설정된 u-헬스케어 의료정보 시스템상에서 트래픽 도메인을 기준으로 기술적 보안 취약성을 점검하기 위해 취약점 진단체계를 설계하는 과정이다. 위험도 평가체계 설계는 취약점 진단체계 구성 다음단계, 도메인별 취약점을 정량적으로 평가 설계하는 작업이다[5][6].

<표 1> 5단계 평가체계 구성

단 계	수 행 사 항
유헬스 무선 트래픽 연동구간 파악	생체인식 및 센싱 RFID 시스템 전송 무선랜(802.11b)전송
트래픽 도메인 진단	센싱 트래픽도메인 사용자 PC 구역 원격 통신망 구역
도메인별 취약점 진단체계 설계	설정된 u-health 의료정보시스템 도메인을 기준으로 기술적 보안 취약성 진단체계 설계
위험도 평가체계 설계	취약점 진단체계구성 다음 단계, 도메인별 취약점을 정량적 평가 설계
위험도 평가작업	위협, 취약성, 자산가치,위험도 평가

3.1 제1단계 : 트래픽 연동구간 파악

3.1.1 생체인식 및 센싱

생체인식 및 센싱 시스템은 센서부, 수집된 생체 신호의 분석부, 지속적인 건강상태 모니터링 및 데이터 축적부, 응용서비스를 위한 정보 교환 인터페이스 및 사설 방화벽 등으로 구성된다. 환자 댁내에서 피부암 등 피부상태를 상시 체크할 수 있는 smart mirror, 상처의 병원체 감염 유무를 상시 감시하는 smart bandage, 복용약에 대한 정보와 복용 유무를 알려주는 smart drug 등 서비스가 개발되었다. 생활공간 속에서 다양한 의료센서 및 기기를 통해 수집된 생체정보와 환경정보를 기반으로 중앙의 원격 의료서비스 시스템을 통해 언제 어디서나 의료 피드백을 받을 수 있다. 채집되는 환자 정보는 생체 ID 정보, 생체 상태 정보, 생체분석 결과 정보, 시스템 관리정보, 관리 기능상 생성된 인식/상태 정보, Context-aware정보, Location, ID 등 이다[8][9].

3.1.2 RFID 시스템 전송

RFID기술은 칩의 저장 능력과 인식능력이 향상되면서 유비쿼터스 환경에서 필수적인 기술로 실생활에 가장 먼저 접목시킬 기술로 주목받고 있다. RFID는 판독 및 해독 기능을 하는 RF 판독기와 정보를 제공하는 RF 태그로 구성된 무선통신 시스템이다. RFID는 사람, 자동차, 화물 등에 개체를 식별하는 정보를 부가하는 시스템으로 그 부가 정보를 무선통신 매체를 이용하여 비접촉으로 해독하여 기존 오프라인으로 이루어지는 다양한 애플리케이션을 자동화 할 수 있는 시스템이다. 그러나 RFID 기술은 물리적인 공격, 위조, 스푸핑, 도청, 트래픽 분석, 서비스 거부 공격 등에 대한 취약점을 가지고 있다. 이 취약점 들은 개인이나 조직의 심각한 보안과 프라이버시 문제를 야기할 수 있다[10].

3.1.3 무선랜(802.11b)전송

무선랜 구간에서는 일반적으로 2.4 GHz ISM 대역의 무선랜(802.11b)을 사용한다. 전송거리는 300 moutdoor, 30 mindoor 정도며 11Mbps의 최대 속도를 제공하는 DSSS 방식 무선랜 표준을 사용한다. SSID(SSID는 무선랜을 통해 전송되는 패킷의 각 헤더에 붙여지는 32 바이트 고유 식별자로 무선장치가 BSS(basicserviceset)에 접속할 때 마치 암호처럼 사용된다. SSID는 한 무선랜을 다른 무선랜으로 구분해주므로, 특정 무선랜에 접속하려는 모든 AP나 무선장치는 반드시 동일한 SSID를 사용한다.

3.2 제2단계 : 트래픽 도메인 진단

u-헬스케어 의료정보시스템상 트래픽 도메인은 의료정보시스템을 통과하는 트래픽 구간의 구분 영역이다. 네트워크 구조상 에서 패킷은 소통경로를 따라 정보가 유통되며 이 경로에서 보안기능 수행이 필요하고 타 도메인과 차별화가 가능하다. 따라서 구분된 영역 기준에 따라 보안 적용을 차별화하여 적용할 필요성이 제기된다. 이러한 이유로 보안 도메인 영역설정이 필요해진다.

3.2.1 트래픽 도메인 기준

본 논문에서 사용하는 u-헬스케어 의료정보 시스템 트래픽 구간별 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 적용 시 타 영역의 보안기능으로 기능 중복이 발생치 않는 영역에 따라 도메인을 설정하는 기준은 다음<표 2>와 같다. 보안도메인 설정은 더 세부적 단계로도 적용될 수 있지만 그렇게 될 경우 보안기능 중복이 발생하고 무엇보다 Performance 지연과 필요이상의 네트워크 구조 복잡을 초래하게 된다.

<표 2> u-헬스케어 보안 도메인 설정기준

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

3.2.2 센싱 트래픽도메인 구간

센서구간은 특정 상황이나 환경에 대한 센싱이 가능한 센서(Sensor Node)와 수집된 정보를 처리하는 프로세서, 데이터 송수신 장치(Sink Node)로 구성된다.

- 보디센싱 구간 : 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 정보기술에서는 지문, 눈의 망막 및 홍채, 음성, 얼굴 표정, 손 측정 등 인증 목적으로 사람의 신체특성을 측정, 분석하는 기술이다.
- 환경센싱 구간 : 집안, 공장, 사무실등 인간 생활 공간 상의 가전 ,전자 기구에 장착된 센서이다. 센서 사이는 무선 또는 유선 네트워크를 연결하며 환경을 스스로 인지하고 판단하기 위한 센서와 프로세서로 구성한다. RFID에서 센서는 다양한 종류의 태그가 그 역할을 한다. 프로세서는 RFID 태그안에 포함되는 칩을 의미하며 원활한 커뮤니케이션을 위해서 RFID에 안테나를 부착하고 RFID 태그를 읽을 수 있는 리더기를 사용 할 수 있다.

3.2.3 사용자 PC 구역

이 구간에서 이용자가 정보를 열람하고 입력하며 입력정보를 전송하는 단순기능이 주류이다. 그러나 PC를 대상으로하는 많은 해킹 기법이 등장하고 해킹을 자동화 형태로 발전시킨 웜이 증가하며 PC에 저장된 개인정보를 자동으로 유출 시키는 바이러스로 인해 서버 시스템에 버금가는 위협이 등장한다. 일반적으로 u-헬스케어 의료정보시스템은 사용자 구역을 무선랜(802.11b) 전송구간으로 분류한다. 이 구간에서는 일반적으로 2.4 GHz ISM대역 무선랜(802.11b)이 사용된다. SSID(SSID는 무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32 바이트 길이 고유 식별자로서, 무선장치들이 BSS(basicserviceset)에 접속될 때 마치 암호처럼 사용된다.

3.2.4 원격 통신망 구역

u-헬스케어 의료정보시스템 네트워킹 도메인에서 제3구역으로 설정되는 구간은 원격 통신망 구역으로서 원격 무선통신 구간을 설정할 수 있다. 선박, 항공기, 자동차 등의 이동체와 고정국과의 상호 무선통신. 무선국이 이동하는 장소에 따라 육상 이동무선, 해상 이동무선, 항공 이동무선 등으로 분류된다. 원거리 통신인 경우 장파, 중파, 단파가 사용된다. 통신 범위가 좁은 경우는 초단파(VHF)대나 극초단파(UHF)대가 사용되며, 60MHz, 150MHz, 400 MHz, 800 MHz대가 주로 이용된다. 원격 무선통신 환경에서 ECG는 벨트 착용자의 cellphone 이나 PocketPC(GPS 포함)를 통해 중앙센터의 Cardiac Data Management System으로 데이터를 보낸다.

3.2.5 의료정보호스트 구간

u-헬스케어 의료정보시스템 호스트 구간에는 환자 진료기록 원장, 치료기록, 의료 개인정보 등 중요정보가 집중되고 다수 직원 접근으로 정보 유출 문제가 가장 심각한 부분이다. 호스트 구간에서는 분석, 필터링, 로깅구간으로서 데이터가 모아져 base로 전송되므로 다양한 환자상태 정보를 판독하고 분석된다. 모니터링 결과 다양한 화면을 통해 환자에게 필요한 정보 제공, 약물 복용시간, 응급조치, 건강관리 방법, 병원 후송 지시를 피드백 한다. 웹브라우저와 웹서버 간 전송데이타는 128bits 이상 키값으로 암호화되어 전송되므로 공개된 네트워크라 해도 1차적 위협은 서버 시스템에 대한 것이다.

3.3 제3단계 : 도메인별 취약점 진단체계

u-헬스케어 의료정보시스템 도메인은 사용자 단말 구간, 공중통신망인프라구간, 네트워킹구간, 인트라넷 구간으로 구분된다. 사용자 단말 구간은 진단, 진료 서비스가 수행되는 구간이며 일반 고객이 정보시스템을 이용하는 사용자 영역이기도 하다. 이 구간에서는 사용자가 원격 통신을 이용하여 건강 검진 행위를 센싱하여 그 결과를 통신망을 통해 의료정보시스템으로 전송하게 된다. 센싱구간은 여러 형태가 있지만 일반적으로 센서기능, 전송기능, 원격 모니터링, 처방 및

진료 등 4개과정을 거친다. 공중통신망 인프라구간은 공공 통신망의 백본망과 교환기 시스템, 인터넷 시스템으로 구성되는 영역이다.

<표 3> u-health 보안 도메인 설정

도메인	구간	구간범위	통신방법
센싱구간	센싱	센서노드,프로세서, 싱크노드	Bluetooth,태그 = 마이크로 칩 + RF 및 안테나
		PDA-access-point-게이트웨이	무선자원 송수신 역할
인트라넷 구간	서버구간	호스트 컴퓨터	응용프로그램 (ERP,SCM)LAN통신
	데이타베이스구간	각종 데이터를 저장 역할	정보를 저장하고 프로토콜데이터교환
사용자PC 구간	유선랜 구간	내부유선통신PC-host LAN통신	프로토콜데이터교환
	무선랜 구간	인트라넷내부 무선LAN통신	프로토콜데이터교환
공중통신망 인프라구간	전용선통신	단말기-교환기-단말기	유선통신
	무선통신	단말기-교환기-단말기	무선통신
	인터넷통신	단말기-교환기-단말기	유선통신

설정된 도메인을 기준으로 기술적 보안 취약성을 점검하기 위해 취약점 진단체계를 설계한다. 진단 체계는 기술적 보안 전체영역 중 정보시스템 자산에 대한 내외부로부터의 보안침해 위협 가능성을 점검, 평가하는 과정을 설계하는 것이다. 이는 정보시스템 자산이 위험에 노출될 수 있는 가능성과 수준을 점검, 평가한다. 정보 시스템에 가해지는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 현행 보안대응 체계를 진단, 평가하며 조사된 정보 시스템 자산에 가해지는 위협과 내부적인 취약성 및 이를 대처하는 대응체계를 연계 분석하여 위험수준을 평가한다.

<표 4> 취약점 점검 체계

구간	1구역	2구역	3구역	4구역	4구역
구성 자원	.센서	.내부용 단말기	.공중망 네트워크 .통신장비	.웹서버 .응용서버	.db서버 .계정계서버
측정 체크리스트	경량암호및 인증기술, 량키 관리 , 프라이버시 보호기술.부채널공격방지	.사용자인증능 .데이터관리 해킹시도	.도청,감청 .전송정보 노출	.전송정보 노출 .보안카드 변호노출 .피싱 .파밍 .패스워드 관리 .암호화, 복호화	.내부통제 제도 .데이터관리
측정 방법	모의침투 .취약점점검 .기술보안체계점검	.모의침투 .취약점점검 .기술보안체계점검	모의침투 .취약점점검 .기술보안체계점검	.모의침투 .취약점점검 .기술보안체계점검	.모의침투 .취약점점검 .기술보안체계점검

3.4 제4단계 : 위험도 평가체계 설계

u-헬스케어 의료정보시스템 취약점 진단체계를 설계하여 기술적 취약점 진단체계를 구성한 다음 단계에서 도메인별 취약점을 정량적으로 평가해야 한다. 취약점 평가는 위협요인이 자산에 손실이나 부정적 결과를 확대시킬 수 있는 약점을 산정하며 보통 0에서 1 까지 척도로 측정결과를 계량화 한다. 위협에 적절한 통제가 존재하지 않는다면 취약성 값은 1이다. 취약점 점검분야는 기술구조를 기준으로 네트워크, 서버, 운영 체제, 데이터, 프로그램, 통신 프로토콜, 단말 시스템으로 구분된다. 점검 대상자원은 네트워크, 운영 체제, 데이터베이스. 서버시스템, 클라이언트로 구분된다.

3.5 제5단계 : 위험도 평가작업

u-헬스케어 의료정보시스템의 기술적 보안 취약점 측정체계 설계의 방향에 의거하여 취약점 점검은 취약점 점검도구를 이용하거나 수동으로 점검 항목에 대한 기술적 취약점을 탐지한다. 위협은 정보시스템 자산에 대한 내외부로부터의 보안 침해 위협이며, 취약성은 운용 중인 정보시스템 자산이 위험에 노출될

수 있는 가능성이다. 보안 체계는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 대응체계이다. 수동 점검은 점검대상 시스템을 대상으로 체크리스트 점검을 실시한다.

<표 5> 측정TOOL활용 자동점검 항목

	항목	세부항목	취약	안전	취약율
1.네트워크	네트워크 스위치	패스워드 인증			
		SNMP 기능			
		HTTP 기능			
		명령 실행 제어			
		트래픽 제어			
		소 계			
	네트워크 라우터	패스워드 인증			
		라우팅			
		트래픽 제어			
		Logging			
		Time			
		소 계			
2.운영체제	운영시스템	사용자 계정과 패스워드			
		시스템 Trust 관계			
		부적절한 권한 설정			
		네트워크 접근 제어			
		Patch Check			
		소 계			
3.데이터베이스	데이터베이스 시스템	DBA 사용자 관리			
		사용자별 Resouce/ Product 권한			
		Privilege 및 Role			
		접근 통제			
		Backup 및 Recovery			
		소 계			
4.애플리케이션	웹애플리케이션	Hidden Manipulation 입력 값			
		XSS 취약점			
		파일 업로드 취약점			
		IIS WebDAV 설정 취약점			
		소 계			
5.클라이언트	단말기	웹 브라우저 취약점			
		도움말 취약점			
		아웃룩 익스프레스 취약점			
		백신 프로그램			
		업데이트 정보			
		소 계			

위협은 정보시스템 자산에 대한 내외부로부터의 보안 침해위협이며 취약성은 운용중인 정보시스템 자산이 위험에 노출될 수 있는 가능성이다. 보안체계는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 대응체계이다. 위험도 산출은 다음공식을 사용한다.

1) 위협 = 위협영향*위협발생빈도 (T)
2) 취약성 = 자산이 가지고 있는 정보보호항목 약점의 수치 (V)
3) 자산가치= 자산가치 (A)
4) 위험도 = 위협, 취약성, 자산가치 승산에 의한 예상손실 수치
(ALE : Annual Loss Exposure) =T*V*A

<표 6> 위험도 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																				

<표 7> 위협 영향평가

등 급	지수	위협영향 수준
VL	1-20	의료정보자산에 경미한 영향
L	21-40	의료정보자산에 경미한 피해 발생
M	41-60	의료정보시스템에 일정수준 피해
H	61-80	정보시스템 중단 상황, 복구에 수 의료시간 소요
VH	81-100	의료정보시스템의 영구적 중단 상황, 복구에 장기간 소요

4. 결 론

u-헬스케어 의료정보시스템은 정보통신기술과 보건의료를 연결하여 언제어디서나 “예방, 진단, 치료 사후관리” 보건의료 서비스를 제공하는 서비스이다.

원격의료로 대표되는 u-헬스케어는 의료정보 이동성이 증가하고 이동량도 증가하면서 의료정보에 대한 외부로부터 공격 가능성이 증가하며 RFID를 이용한 과도한 개인정보 수집으로 인한 프라이버시 침해 가능성이 높아진다. u-헬스 케어 의료정보시스템 보안 취약성은 의료정보가 무선전송되므로 이 환경에서 통합의료정보 데이터베이스에 관련자들이 모두 접근가능하다. 내부인에 의한 의료정보 조작이나 노출, 개인의료정보가 경제적 가치를 갖게 될 경우 불순한 의도로 수정이나 조작 가능성이 커진다. 본 논문에서는 u-헬스케어 의료정보 시스템 보안 문제를 해결하고 보다 강력한 방어를 수행하기 위하여 취약점을 진단하는 5단계의 보안위험도 평가체계를 제안했다. u-헬스케어 의료정보시스템 보안 대책 성공 여부는 시스템이 가지고 있는 취약점 위험도나 공격의 강도, 대응수단의 효율성에 따라 결정된다. 본 논문으로 제안된 방법론은 향후 의료정보시스템 개발업무에 참고 될 수 있기를 기대한다.

참고문헌

[1] Sichoon,Noh,Dong Chun Lee,"Assurance Method of High Availability in Information Security Infrastructure System", SCIE LNCS 3794,2005.12

[2] Sichoon,Noh,"Building of an Integrated Multilevel Virus Protection Infrastructure", IEEE Computer Society,2005.12.

[3] Sichoon,Noh,"A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrne System", DCS, 2006.02

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

[5] 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.

[6] 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

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

[8] Healthwear:Medical Technology Becomes Wearable - 2004 IEEE

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

[저자소개]

노 시 춘 (Si Choon Noh)

1987년2월 : 고려대학교 경영정보학 석사
2005년2월 : 경기대학교 정보보호기술 박사
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~ 현재 :남서울대학교 컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr