한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

u-헬스케어 보안 위협 및 향후 대책

강영진*, 이훈재°
*°동서대학교 정보통신공학과
e-mail: rkddudwls55@gmail.com*, hjlee@dongseo.ac.kr°

A survey of security threats on u-healthcare

Young-Jin Kang*, Hoon-Jae Lee*°
*°Dept. of Information and Communication Engineering, Dongseo University

● 요 약 ●

최근 u-헬스케어 서비스는 바이오센서 및 스마트 의료 기기의 발달과 의료 데이터의 교환 및 처리를 위한 표준 기술 등이 뒷받침 되면서 서비스의 실체화가 가속화되고 있는 추세이다. u-헬스케어는 유·무선 네트워크와 밀접한 연관을 맺고 있으며, 이러한 유·무선 네트워크의 사용은 기존의 서비스에서 발생 가능한 보안상의 취약점 및 공격이 u-헬스케어 환경에서도 유사하게 나타나며, 개인 의료정보를 주로 다루는 만큼 그 위험성은 더욱 심각하다 사료된다. 이에 본 논문에서는 u-헬스케어의 보안 위협 및 그에 따른 향후 대책방안에 대하여 논하고자 한다.

키워드: u-헬스케어 보안위협, u-헬스케어 표준 기술, TCP/IP 기반의 취약점

I. 서론

u-헬스케어의 목적은 유·무선 네트워킹과 전자 의료기기를 통해 언제, 어디서나 이용 가능한 건강관리 및 의료서비스 지원과 환자의 질병에 대한 원격관리와 일반인의 건강유지 및 향상이다. 또한, 최근 바이오센서 및 스마트 의료 기기의 발달과 의료 데이터의 교환 및 처리를 위한 표준 기술 등이 뒷받침 되면서 서비스의 실체화가 가속되고 있는 추세이다. 그러나 u-헬스케어는 TCP/IP 기반의 인터넷 프로토콜이 의료 장비에 필수적으로 지원되며 네트워크 보호 솔루션이 그대로 사용되어 개인 의료 정보보호에 대한 우려의 목소리가 점차 커지고 있다. 아래의 (그림 1)은 u-헬스케어 환경에서 발생 가능한 보안위협 및 취약점을 나타낸다.

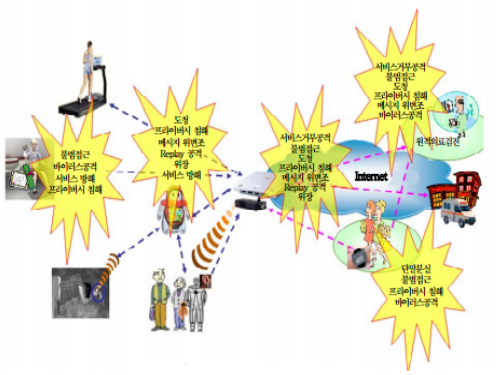

그림 1. u-헬스케어 환경의 보안 위협
Fig 1. Security threat in u-health care environment

본 문에서는 이러한 보안 위협 및 취약점들에 대해 자세히 설명하고 그에 대한 향후 대책을 논하고자 한다.

II. 관련 연구

u-헬스케어는 유무선 네트워크의 TCP/IP 기반의 인터넷 프로토콜이 의료장비에 필수적으로 지원되면서, 기존의 서비스에서 발생 가능한 보안상의 취약점 및 공격이 u-헬스케어 환경에서도 유사하게 나타난다. 이러한 TCP/IP의 취약점에 기반한 대표적인 공격 유형에 대해 설명하고자 한다.

1. u-헬스케어 보안위협

1.1 공격 유형

- IP스푸핑

IP스푸핑은 신뢰관계에 있는 두 시스템 사이에서 허가 받지 않은 자기 자신의 IP 주소를 신뢰관계에 있는 호스트의 IP주소로 바꾸어 속이는 것으로 IP 주소로 인증하는 서비스를 무력화 할 수 있으며, 공격자가 마치 신뢰성 있는 자가 송신한 것처럼 패킷의 소스 IP를 변조하여 접속을 시도하는 침입 형태를 말한다.

- Man-in-the-Middle Attack

이 공격 기법은 데이터 스트림의 불법 수정이나 거짓 데이터 스트림의 생성을 수반하며, 서버와 사용자간에 상호인증이 이루어지지 않으면 공격이 가능하다. 즉, 공격자는 송신자 측과는 수신자로 위장하며, 수신자 측과는 송신자로 위장하여 통신하고 이 공격은

신분 위장(Masquerade), 재전송(replay), 서비스 거부 공격(denial of service attack)등의 적극적 형태의 공격이 가능 하다.

- 재전송 공격(replay attack)

프로토콜 상에서 유효 메시지를 골라 복사한 후 나중에 재전송 함으로써 정당한 사용자로 가장하는 공격이다.

- Dos 공격(Denial of service attack)

시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다.

III. u-헬스케어의 보안기술

1.1 유·무선 네트워크 보안 기술

유·무선 네트워크 보안 기술에는 전자서명, 암호화, 사용자 인증, Rogue Ap 관리, 유·무선 통합 인증, 데이터 위변조 방지 기술 등이 핵심 기술이며, 간단히 설명 하고자 한다.

- 전자서명
  - 서명자가 자신이 서명한 사실을 부인할 수 없음
  - 서명한 사용자에 대해 제3자가 확인 가능
- 암호화
  - 서명된 메시지 내용에 무결성 보증
- 사용자 인증
  - 임의의 정보에 접근할 수 있는 주체의 능력이나 자격을 검증,
  - 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방지
- Rogue AP 관리
  - 악의적으로 설치된 Rogue AP 탐지
- 유·무선 통합 인증
  - 각종 유·무선망에서 인증, 보안 인터넷 로밍 보안 등을 통합적으로 관리할 수 있는 기술
- 데이터 위·변조 방지
  - 데이터의 정확성은 위·변조를 막아내는가가 중요
  - 데이터 사용을 제한하는 사전 관리 방법
  - 나중에 위·변조 여부를 검증하는 사후 관리 방법

1.2 개인/의료 정보에 의한 프라이버시 보호기술

개인정보보호 방법으로는 P3P라는 개인정보 자기통제권 기술과 익명화 방식 기술을 들 수 있다. 먼저 P3P는 웹사이트 접속 시 프라이버시를 보호하기 위해 국제 웹 표준화 기구인 W3C 권고안으로 2002년 승인되었으며, 이 기술은 사용자가 요구하는 정보보호 요구 수준에 부합하는 경우에만 해당 정보를 제공함으로써 사용자 스스로 본인의 정보를 관리하고 제공할 수 있도록 한다. 또한 익명화 방식은 개인 정보를 전송하고자 하는 대상자만이 해석할 수 있도록 암호화하는 방법 및 정보 활용 시 개인 정보를 통해 개인을 식별하지 못하도록 하는 방식이다.

1.3 전자의무기록의 안전한 교환 및 공유 기술

IHE-XDS에서는 의료 데이터의 공유를 동의한 의료 도메인 간에 데이터 교환 상호호환성을 보장 하고 데이터의 안전한 접근 및 활용을 보장하기 위한 기술 내용을 포함하고 있다. 이에 따른 보안 모델 기술 요소로는 Risk Assessment, Accountability, Policy Enforcement 이다. 아래 (표 1) 에서 각 기술들에 관해 간단히 설명 하고 있다.

표 1. 보안 모델 기술 요소
Table 1. Technical elements for the security model

항목	설명
Risk Assessment	데이터에 대한 기밀성, 무결성, 가용성 보장을 기본으로 하며 환자의 안전이 개인 프라이버시보다 우선하도록 한다.
Accountability	정보 요청자를 식별, 접근 제어를 수행하고 관련된 이벤트에 반드시 로그를 남겨 보안 감사를 수행해야 한다.
Policy Enforcement	상호 식별이나 인증, 접근 제어 정책, 보안 감사 레벨 등의 보안 정책에 대한 설정과 시행의 동의가 이루어져야 한다.

u-헬스케어 환경에서 IHE-XDS를 이용한 정보 공유 방법은 (그림 2)과 같다.

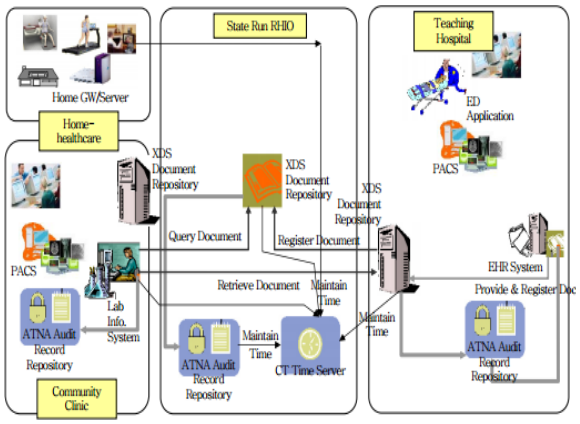

그림 2. u-헬스케어 환경에서의 IHE-XDS
Fig 2. IHE-XDS on u-health care environment

IHE-XDS를 이용한 정보 공유 방법은 클리닉 센터 및 중대형 병원 내의 XDS document repository 간에 건강 정보 요청 및 접근이 수행될 경우, 각 repository는 IHE-XDS 모델에서 지원하는 DSIG, CT, ATNA 등을 이용하여 건강 정보 요청자의 식별, 접근 제어, 교환 데이터의 기밀성과 무결성 보장, 발생하는 정보 이벤트에 대한 보안 감사 등을 지원함으로써 안전한 건강 정보 공유를 보장할 수 있다.

1.4 멀티 도메인 간 인증 및 ID 관리 기술

IHE-XUA는 멀티 도메인 간 사용자 인증을 지원하기 위한 통합 프로 파일로서 도메인 간 교환되는 트랜잭션에 대해 책임을 부여하기 위해 피 요청기관이 접근 결정과 보안 감시를 수행하는데 사용 가능한 방법으로 요청자를 식별 가능해야 한다. 뿐만 아니라, 국제표준인 SAML 2.0을 기반으로 Federation-ID를 지원함으로써 협력 관계를 맺은 관련 서비스를 지원가능하다.

표 2. u-헬스케어의 Federation-ID 기술 효과
Table 2. The Federation-ID effect of technology on u-health care environment

장 점	구체적 예
보 안	-사용자 인증 -다중 접근 제어 레벨 설정 가능
HIPAA 호환	-인증 레벨 설정 지원 -데이터 접근에 대한 상세 보안 감 사 지원
운영 효과 개선	-싱글 사인 온-중복 ID 관리 방지 -애플리케이션에 따른 구별된 UserID 관리 -새로운 구성원 추가 및 확장성 용이
비용 절감	-ID 관리자를 위한 운영관리자 지원 -개발 시간 감소 -표준 준수 개발-상이한 인터페이스에 대한 중복 개발 낭비 방지
상호 호환성	-기존 시스템 간 통합 지원 -새로운 시스템 구축 및 통합 용이

u-헬스케어 시스템에 Federation-ID 기술 도입을 할 경우, (표 2) 와 같은 효용성을 얻을 수 있다.

1.5 헬스케어 시스템 위험 평가 및 보안 관리 기술

u-헬스케어 시스템의 오류 및 결함, 사용 부주의 등으로 인한 의료 사고 등으로부터 환자의 건강 및 생명에 대한 악영향을 최소화하기 위하여 u-헬스s케어 시스템에 대한 안정성 평가 및 위험관리 기술이 요구 되며 의료 시스템으로 인한 환자 위협의 치명성 및 영향 받는 환자 규모 등을 기준으로 위협도를 분류한 후, 각 위협의 발생 가능한 빈도수를 반영하여 시스템의 위험등급을 A부터 E까지 분류하는 체계를 띄고 있다.

IV. 취약점 분석 및 대응방안

1.1 TCP/IP기반의 취약점

TCP/IP 프로토콜은 OSI7 계층의 기능을 필요한 부분 5계층으로 계층화화여 사용한다. 계층 1, 2의 경우 보통 LAN 구성 프로토콜을 사용하고 상위 계층들인 IP, TCP, APP계층은 캡슐화가 된다. 이 캡슐화의 특성으로 인해 TCP/IP 취약성을 이용한 공격이 이용된다. 그 첫 번째로 네트워크 스캐닝공격이 있고 두 번째로 LAN 환경의 이더넷 특성에 기인한 패킷 모니터링(Sniffing), 마지막으로 TCP/IP 인증과 관련된 IP, ARP, DNS Spoofing 공격과 서비스 거부 공격(Dos/DDos)공격이 있다. 이러한 취약점을 통한 공격기법에 대한 대응방안을 살펴보고자 한다.

- 네트워크 스캐닝 공격
  - 스캐닝 도구를 사용한 자가진단
  - 불필요한 ICMP 메시지 차단
  - 프록시 기반 방화벽 및 패킷 필터링 도구 사용

- 패킷 모니터링(Sniffing)

스위치에 브로드캐스트 도메인, MAC 주소 수동 설정 등을 함으로 패킷을 가로채는 시도는 줄일 수 있으나 원천 봉쇄는 불가능하다. 따라서 패킷을 가로채더라도 그것의 내용을 가지고 어떠한 행동조차 할 수 없도록 암호화 기법을 이용하는 것이 일반적이고 중요한 방어 기법이라 할 수 있다.

- TCP/IP 인증 공격

먼저 Spoofing 공격에 대응하려면 Gateway의 IP와 MAC주소를 정적으로 고정시킴으로써 잘못된 ARP Reply 정보가 오더라도 이를 ARP Table에 반영하지 못하도록 한다. 그리고 송수신 되는 서버의 경우 SSL방식 등을 이용하여 웹 트래픽을 암호화할 필요가 있다.

아래의 (그림 3)은 시스코사의 헬스케어 네트워크 보안 구성의 예를 나타낸다.

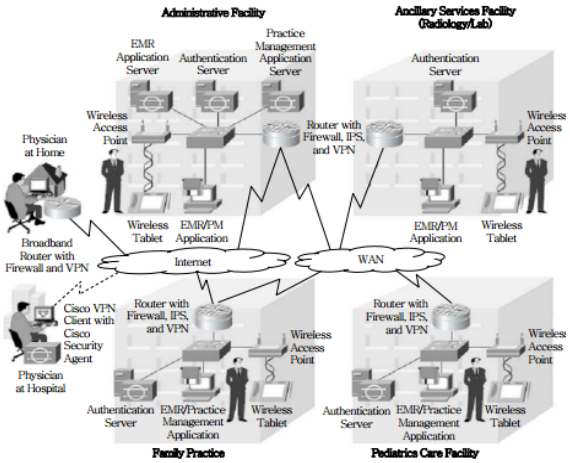

그림 3. 시스코의 헬스케어 네트워크 보안 구성 예
Fig 3. Example of Cisco healthcare network security configuration

(그림 3)은 네트워크 장비 내장용 바이러스 백신, 침입탐지, VPN 장비 및 보안 관리, 사용자 인증을 위한 AAA장비, PoC 장비와 의료 단말용 태블릿 PC 또는 PDA에 적용하기 위한 무선 보안 구간 인증 및 암호 툴 등을 사용하여 TCP/IP 기반의 취약점을 보완 할 수 있다.

V. 결론

본 논문은 현재 u-헬스케어의 개인 프라이버시 보호문제와 TCP/IP 기반의 취약점과 보안 기술들을 살펴보았다. u-헬스케어의 최대 장점은 언제, 어디서나 이용 가능한 건강관리 및 의료서비스 지원과 환자의 질병에 대한 원격 관리와 일반인의 건강유지 및 향상에 목적을 두고 있으나, 최근 u-헬스케어의 개인 프라이버시 문제와 TCP/IP 기반의 취약점들이 문제가 되고 있다. u-헬스케어에서는 정확한 진료를 받기 위해서는 자신의 생체정보를 포함한 개인 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보를 충분히 제공해야 하기 때문에 보안상의 문제로 인한 정보 유출시 그 피해는 금전적인 문제와 더불어 개인의 생명까지 위협할 수 있다. 앞서 거론한 사례들을 통해 기술상의 취약점으로 인한 유출보다 내부자의 의도적인 정보 유출행위 및 관련 지식 부재로 인한 정보 유출 사례가 더욱 많음을 알 수 있다. 이를 미루어 볼 때, 기술적인 보안 취약점을 해결하기 위한 기술 보완과 더불어 내부자에 의한 의도적인 유출 또는 관련 지식 부재로 인한 정보 유출을 막기 위하여 정기적인 교육 및 법적 제도 마련이 시급하다 사료된다.

참고문헌

[1] jeSong, and shKim, and maJung, and kiJung, “Seculity issue and techinal trend in u-health care,” A trend analysis of telecommunication, Vol 22, No1, pp.123-127, February 2007.

[2] shKim, and jeSong, and maJung, and kiJung, “Medical informationization and trand of standardization on security technology,” A trend analysis of telecommunication, Vol 21, No6, pp 198-199, December 2006.

[3] hsOh, “Trend on technology and standardization for u-health care,” Journal of TTA NO. 112, pp 103-105, August 2007.