한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

u-Healthcare 환경에서 안전한 의료정보공유에 대한 연구

장선주°, 김규석*
°*성균관대학교 전자전기컴퓨터공학과
e-mail:wkd486@hotmail.com°, tuffever@naver.com*

A Study on the Implementation of User Medical Information Sharing System in u-Healthcare Enviornment

Seon-Ju Jang°, Kyu-Seok Kim*
°*Dept. of Electronic and Computer Engineering, Sungkyunkwan University

● 요 약 ●

본 연구에서는 의료정보공유가 활발하게 이루어지게 될 u-Healthcare환경에서 발생할 수 있는 보안 취약점에 대하여 알아보고 안전하게 의료정보를 공유하기 위한 보안요구사항을 제안한다.

키워드: 유헬스케어(u-Healthcare), 취약점(Vulnerability), 보안 요구사항(Security Requirements)

I. 서 론

u-Healthcare는 ubiquitous Health의 약자로, 정보기술과 보건의료를 결합하여 언제 어디서나 환자의 질병에 대한 예방·진단·치료·사후관리 등 보건의료 서비스를 제공하는 것을 의미하는 것으로 이동성(mobility)과 내재성(embeddedness)의 특징을 가지고 있다. u-Healthcare 환경을 위한 의료정보화는 환자 원무기록의 디지털화, 영상정보 저장으로 파일화, 병원업무전산화 등 병원정보화가 실현되고 있으며 의료관련 법·제도 분야도 진화하여, 2002년 의료법 개정을 통해 원격의료 및 전자의무기록 관련 규정을 도입한 바 있다. 이렇듯 활발하게 이루어지고 있는 의료정보공유 환경에서 주고받는 공동 활용 대상 의료정보에 대하여 알아보고 통신 중에 발생할 수 있는 보안 취약점과 필요한 보안요구 사항을 살펴본다.

II. 본 론

1. 공동 활용 대상 의료정보

의료정보공유를 위해 이용되는 의료정보는 공동 활용대상 진료정보 우선순위 선정기준인 활용가치도, 정보의 중요도, 정보화 수준, 정보전달의 용이성에 의해 그림 1과 같이 5가지 순위로 분류할 수 있다.[1]

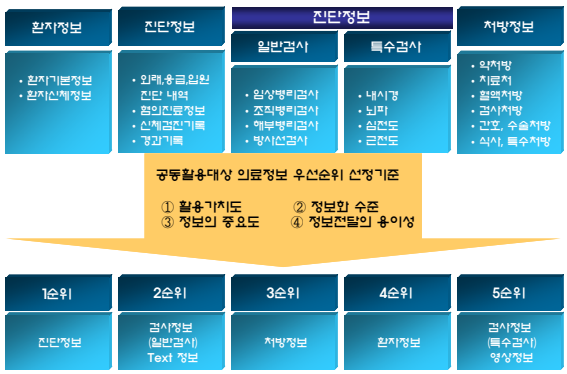

그림 1. 공동 활용 대상 의료정보
Figure 1. Common User Shared Medical Information

2. 보안취약점

u-Healthcare 환경에서 존재하는 보안취약점은 Dos 공격, 바이러스, 웜 해킹 공격, 도청 위변조 공격 등이 있다. 그 밖에 유·무선 인프라에서 가능한 여러 불법 접근, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기 마비, 방해전파, 화재와 같은 인재 또는 악의적인 행위를 통한 공격 등이 존재한다.

2.1 DoS 공격

서비스를 지원하는 서버를 악의적으로 공격해 서버의 자원을 부족하게 하여 사용자의 의료정보가 정상적으로 제공되지 못하게 만드는 Dos 공격에 노출 될 수 있다. 이 공격기법은 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스

이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격을 통하여 서비스의 기능을 일시적 또는 무기한으로 방해 또는 중단을 초래한다.

2.2 바이러스/웹 해킹 공격

서비스에 대하여 허가받지 않은 사용자가 불법적인 침투을 시도하는 불법적인 접근과 무선통신용 AP 또는 공유기의 무선망에 접근 및 불법 침투하는 무선 해킹이 있다. 장비에서 발생할 수 있는 해킹은 의료장비에 백도어 또는 원격터미널 클라이언트 등으로 권한을 획득하여 공격하는 방법이 있고 의료 지원용 홈페이지를 해킹하여 환장의 정보를 수집하는 웹 해킹이 있다. 그 밖에 DB에 접근하여 내부 중요정보를 획득하는 개인 및 의료정보 DB 해킹과 웹 서버 권한을 획득 한 후, 연동된 내부 망으로 2차 침투 시도를 하는 의료망 침투 등의 해킹 공격이 발생할 수 있으며 바이러스를 이용하여 사용자의료정보를 획득하는 공격이 있다.[2]

2.3 도청/위변조 공격

장비의 취약점을 이용하여 화상시스템에 직접 침투 또는 화상 전송되는 데이터를 도청 및 위.변조하는 화상시스템 해킹과 불법적인 접근 시도 후, 전송되는 데이터를 도청 및 위.변조하는 공격이 있다.[3]

3. 보안요구사항

의료정보공유 및 의료정보전송은 보안되어야할 중요한 데이터로써 필수적으로 갖추어야할 보안 요구사항은 다음과 같다.

3.1 사용자 인증

서버에 접근하는 사용자에 대해 정당한 사용자만 서비스를 이용할 수 있도록 해야 한다. 접근하는 개체가 정당한 개체인지를 판단하는 인증이 제공되어야 한다.

3.2 익명성

의료정보를 제공받는 사용자가 누군지 알 수 없도록 하여 어떤 행위를 한 사람이 누구인지 드러나지 않도록 함으로써 보다 객관적인 서비스 제공과 사용자의 민감한 개인정보를 보호 할 수 있다.

3.3 기밀성

사용자의 개인의료 정보는 민감한 사용자 정보로써 사용자 본인이 아닌 제 3자가 알게 되면 그 정보를 사용하여 악의적인 행동을 취할 수 있다. 따라서 사용자 의료정보는 기밀성이 제공되어야 한다.

3.4 무결성

컴퓨터 바이러스 등의 악성 코드로 인한 의료 정보의 파괴나 시스템 소프트웨어 버그나 하드웨어 고장으로 인한 의료정보의 변질은 잘못된 진단으로 인한 생명의 위협으로도 연결된 가능성이 있기 때문에 사용자와 서버, 서버와 병원, 병원과 병원 간의 데이터 전송에 있어서 데이터가 변경되지 않고 혹 변경된다 하더라도 그 사실을 알아야한다. 그리고 어떠한 개체도 송신자가 생성한 메시지에 대해 수정을 할 수 없도록 해야 한다. 따라서 모든 통신 데이터에 대해 무결성이 제공되어야 한다.

Ⅲ. 결 론

지금까지 u-Healthcare 환경에서의 보안 취약점 및 보안 요구사항에 대하여 알아보았다.

다가오는 u-Healthcare 시대에 부합되는 서비스를 제공하기 위해서 폭 넓은 의료정보공유의 활성화와 사용자가 보다 편리하게 이용할 수 있도록 인터페이스 환경을 조성하기 위한 노력이 필요하다. 그 중에서도 의료서비스 정보는 신체 및 정신적 건강상태를 담고 있으므로 정보의 분류에서도 민감도 높은 정보로 분류되고 있으며 완벽하도록 철저히 정보보안이 이루어져야할 데이터이다. 본 논문을 통하여 사용자 의료정보보호의 중요성에 대하여 깨닫고 해당 분야에 대한 연구가 활발하게 이루어져서 보다 안전한 의료서비스를 제공할 수 있는 환경을 만들어야한다.

참고문헌

[1] Korea Internet Security Agency, *"Information Security on regional communitiy meidcal paradigm and it's changes"*, 2006

[2] Lee Bong Guen, Jung Yun Su, Lee Sang Ho *"Design of Personal Information Security Model in U-Healthcare Service Environment"*, 2011.

[3] J. E. Song, S. H. Kim, M. A. Chung, K. I. Chung, *"Security Issues and Its Technology Trends in u-Healthcare"*, Electronics and Telecommunications Trend Analysis Vol. 22, No. 1, pp. 70-86, Feb. 2007.