원격 의료지원 서비스 환경의 공격 기법과 대응 방안

허윤아, 홍근목, 이근호
백석대학교 정보통신학부
e-mail: yj77222@bu.ac.kr, mok0524@naver.com, root1004@bu.ac.kr

Attacks and Countermeasures of Telemedicine Support Services Environment

Yun-A Hur, Gun-Mok Hong, Keun-Ho Lee
Division of Information and Communication, Baekseok University

요 약

1. 서론


대응하기 위해 시스템을 공격하는 여러 기법과 그에 대한 대응 방안은 바이테이프에 저장한다. 저장된 바이테이프는 U-Healthcare기기의 점검하여 보안장비 및 보안소프트웨어로부터 수집 된 다양한 로그를 분석하고 보안사례로 기반 상시 모니터링을 통하여 보안사고 방지 및 첨예한 대응한다.

2. 관련연구
2.1 U-Healthcare
U-Healthcare는 언제 어디서나 이용할 수 있도록 정보통신기술을 기반으로 사용하는 보건의료서비스이다. 현재에 들어서면서 의학이 발달하고 생활수준이 높아져서 의료수급이 현저하게 줄었다. 또한 안전성은 감소하고 사용자는 범죄적거나 불법적 사용함으로서, 보안상의 문제를 부수적으로 겪고 있다. 이를 대응하기 위하여 2016년의 보안 인프라 비용은 20%이상이 되었다.

![그림 1] 노인 증가율
(1980년부터 2040년까지)

이렇게 고령화 사회가 진행되면서 의료 시장은 자연스럽게 커질 것이고 노인들은 좀 더 편하게 진료 받기를 원하게 될 것이다.

U-Healthcare시장은 크게 만성 질환자 대상의 치료 중
임 서비스 U-Medical, 고려자 대상의 U-Silver, 건강관리 서비스인 U-Wellness로 분류된다. 한국보건산업진흥원에 따르면 U-Healthcare 체계시장은 09년 기준 1,433억 규모로 매년 15%이상 성장추세를 보여왔으며, 범 야 할 평균성장률은 U-Silver(9.7%), U-Medical(15.0%), U-Wellness(17.9%)으로 나타났다. 특히 U-Wellness 시장은 법적 제약이 적어, 기존 제조업을 종사하는 제조활동 관심 속에 연계시킬 경우 급속한 성장 가능성을 보유하고 있었다[1].

2.2 벡터데이터

벡터데이터는 기존의 데이터 수집, 저장, 관리, 분석 역할을 넘어선 대형 데이터 세트를 의미하며 기존의 관계형 데이터와 비교하여 약, 속도, 다양성 및 복잡성에 있어서 그 차이를 볼 수 있다. 벡터데이터의 정의는 다양하지만, 기업적인 측면에서 벡터데이터 기업의 효과적인 전략 도출에 필요한 상세하고 높은 복잡도로 생성되는 다양한 종류의 정보 또는 비정형 데이터로 정의할 수 있다. 벡터데이터 특성에 따르면 양측성이 높은 기존 기술로는 처리하기 어려웠던 정형 및 비정형 데이터가 다양하고 광범위한 분야에 널리 사용되는 데이터를 신속하게 처리 가능하며 이를 기반으로 고급 분석과 예측 등을 통한 새로운 비즈니스 첨단이 가능하다는 점이다. 이렇게 복잡한 데이터는 성장 규모를 V(Volume)로 정의하고 대용량으로 방대한 부가값으로 비용 지불 가능하게 하고, 빠른 처리 속도를 (Velocity)는 고성능 분산저장처리 기술을 보급, 다양한 형태(=Variety)는 다양하게 분산화된 정보가 복잡히 통합되어 있는 특성을 가진다[2].

3. 보안위협


(그림 2) DDoS 공격 시나리오

그림 2를 보면 매우 주요한 컴퓨터 PC가 한꺼번에 서비스를 공격 하게 된다면 공격대상인 서버나 U-Healthcare 기기는 다운이 될 것이다. 애초에 PC는 10000대로 하고 한 컴퓨터 PC당 3개의 패킷을 보낸다 할 때 서비스는 공격될 은 패킷은 30000개가 되어 서비스가 다운이 된다. 서비스가 다운이 되면 위급 시 보내지는 패킷을 받을 수 없기 때문에 환자의 상태가 위험해진다. 이렇게 발생한 DDoS 공격 분석을 비디오데이터를 이용하여 보완 위협을 줄인다.

이처럼 총격 의료에서 보안을 강화하지 않으면 나타날 수 있는 위협과 비러스로 인한 진단오류 및 소상의 위험까지도 함께 날 수 있다. 그리고 RFID를 통해 과도한 개인정보 수집으로 프라이버시 침해 가능성 증가, 보안특성 의료정보에 대한 비밀성 위험, 의료정보에 대해 인가되지 않은 사람의 접근으로 개인정보가 노출되거나 조작될 수 있으며, 내부자에 의한 개인 의료정보 유출사고가 일어날 수 있다[3].

4. 대응방안

지급까지 발생한 DDoS 공격은 비디오데이터로 분석하여 한 자료 서비스의 위험성 보안에 대해 효율적으로 대응하기 위해 제안하고자 한다.

(그림 3) 비디오데이터를 통한 DDoS 방지

그림 3는 DDoS 공격 장치라고 가정한다. U-Healthcare 기기는 병원서비스에 가장 관심이 집중되어 있는 근데 비슷한 경우에서 PC를 개인의 것임을 인정하기 어렵다. 더 이에 기기 기판(최대 이용값)을 20%로 잡는다면 모든 패킷 80%는 차단하고 20%는 이용을 한다. 즉 병원서비스 5번 연결 중 4번은 서비스가 다운되었다고 본 것이고, 5번 연결에서 1번은 정상 통신이다.

또 다른 방법은 5초에 패킷이 3개 이상 들어올 시 공격 영수증을 인식하고 차단하는 방법도 있다.

전화망의 체력은 서비스를 보안하기 위해 보안에 위협한 공격 정보나 시나리오에 대한 대응 기술을 수립하여 로그 확인 사용 가능하다. 수록한 위협에 대응한 솔루션은 비디오데이터에 대해 핵심 원문에 비디오데이터, 관리 및 전문 서비스를 보호한다.
5. 결론


감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A2A05012348)

참고문헌