모바일 헬스케어와 정보보안

우성희

한국교통대학교

Mobile Healthcare and Security

SungHee Woo

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr

요 약

스마트폰의 사용은 모바일 인터넷 비즈니스 성장의 큰 영향을 주었다. 커머스와 광고, 결제와 게임, 영상콘텐츠, 미디어, 헬스케어와 최근의 소셜과 함께 일어나는 O2O 비즈니스까지 그리고 헬스케어 분야에서도 많은 성장을 보이고 있다. 미국의 경우 2015년 스마트폰 기기용 헬스케어 앱규제를 완화하고, 같은 해 중국은 웨어러블등 모바일 기기를 활용해 부족한 의료진과 병상문제 해결을 위한 5개년 로드맵을 마련하기도 하였다. 국내에서도 웨어러블 기기를 의료분야에 활용이 점차 증가하고 있다. 하지만 여기에 반드시 해결해야 할 선과제가 있다면 바로 보안문제이다. ICT 활용 증가로 금융, 의료등 비 ICT 분야에서도 보안사고가 해마다 증가하고 있다. 또한 금융사기, 불법 판촉, 보험 제약 회사 악용 등 2차 피해 발생 가능성이 높은 금융, 의료 분야에서 개인정보 유출 사고 등의 위험이 증가 추세이다. 따라서 본 연구에서는 모바일의 위협요소인 악성코드와 스마트폰의 5대 위험, 국내외 모바일 헬스케어 활용사례와 헬스케어를 위한 모바일 위협 대응 방안을 분석한다.

ABSTRACT

The use of smart phones has had a great impact on the mobile internet business. It shows a lot of growth in the healthcare sector not only commerce, advertising, billing, games, video content, media, amd O2O business. The United States has eased the regulations for healthcare apps smart phone devices in 2015, and China has established a five-year road map to solve shortage of doctors and hospital beds by utilizing mobile devices such as wearable in the same year. The application of wearable devices in the medical field is gradually increasing in Korea too, but there is a security problem as leading challenge. Security incidents in non-ICT sectors such as financial, medical, etc. have increased by using ICT each year. Personal information leakage is also increasing in field likely occurring the potential secondary damages such as financial fraud, illegal promotions, insurance and pharmaceutical companies abuse. In this study, we analyze malwares as the mobile threats, the five risks of mobile smart phone, mobile use cases and the mobile threat countermeasures for healthcare.

키워드

Mobile Healthcare, Wearable, O2O, ICT

Ⅰ. 서 론

스마트폰의 사용전과 후는 모바일 인터넷 비즈니스 성장의 큰 차이가 있다. 스마트폰을 사용한 서비스들의 예를보면 커머스와 광고, 결제와 게임, 영상콘텐츠, 미디어, 헬스케어와 최근의 소셜과 함께 일어나는 O2O 비즈니스까지 모든 분야에서 활발한 성장하고 있다. 특히 헬스케어 분야에 많은 성장을 보이며 웨어러블 기기를 활용한 헬스케어 사용자가 증가하고 글로벌 ICT 기업의 헬스케어 서비스간의 연동을 지원하는 플랫폼 개발, 개발자 참여유도 등을 통한 서비스가 확산되고 있다. 애플리케이션의 확산과 이용자 증가 및 개인건강 정보를 실제 진단과 치료에 활용하는 사례가 증가하고 있다. 미국의 경우 2015년 스마트폰 기기용 헬스케어 앱규제를 완화하고

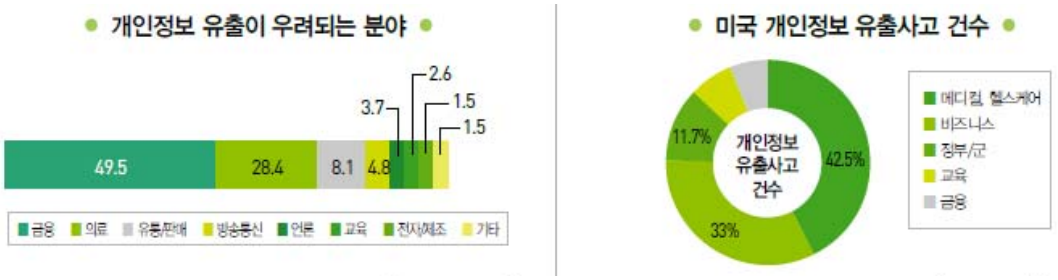

그림 1. 개인 정보 유출 분야와 건수

같은 해 중국 웨어러블 등 모바일 기기를 활용해 부족한 의료진과 병상문제 해결을 위한 5개년 로드맵을 마련하기도 하였다. 국내에서도 웨어러블 기기를 의료분야에 활용이 점차 증가하고 있다. 그러나 여기에 반드시 해결해야 할 선과제가 있다면 바로 보안문제이다. ICT 활용 증가로 금융, 의료 등 비 ICT 분야에서도 보안사고[5]가 해마다 증가하고 있다. 또한 금융사기, 불법 판촉, 보험 · 제약 회사 악용 등 2차 피해 발생 가능성이 높은 금융, 의료 분야에서 개인정보 유출 사고 등의 위험이 증가 추세이다. 특히 미국의 경우 개인정보 유출 사고[5]가 42.5%가 의료 부문에서 발생하고 있으며 국내외에서 금융 · 의료 부문의 보안사고로 사회적 비용 발생하고 있다. 미국의 경우 2위 건강보험회사인 앤섬에서 임직원 및 고객들의 개인정보 8천만 건 유출되었고 국내에서는 다국적 의료정보업체 대표가 25억 건의 의료정보를 미국에 유출하기도 하였다. 따라서 금융, 의료 기업의 보안강화를 위한 정보보호 강화 대책이 추진 중이다. 미국의 경우는 금융, 의료 분야를 주요 기반시설로 분류, 위험관리 절차에 사이버보안 프레임워크를 반영하도록 유도하였고 영국은 금융 등 핵심부문을 대상으로 정기적 훈련 및 사이버 복원력 테스트를 시행하였다. 국내에서는 사이버안전대진단을 통해 기업의 대응능력을 점검하고 정보보호관리체계, 정보보호준비등 인증 의무화를 추진하고 있다[6]. 따라서 본 연구에서는 모바일의 위협요소인 악성코드와 스마트폰의 5대 위험을 분석하고 국내외 모바일 헬스케어 활용사례와 헬스케어를 위한 모바일 위협 대응방안을 분석한다.

II. 모바일 위협 악성코드

빠르게 진화하는 스마트폰은 언제 어디서나 실시간으로 사람들과 소통하고 업무의 생산성을 높일 수 있지만 자신의 위치 정보, 성별, 직업 등 개인정보가 사용자동의라는 불가피한 선택사항에 의해 노출되고 있다. 스마트폰의 위협은 크게 분실, 악성코드 감염, 정보유출, 금전적 손실, 공격지 활용으로 나누어 볼 수 있으며, 표 1[2]의 스마트폰의 5대 위험과 같이 사용자의 피해가 가장 크며, 이에 대한 대책이 필요하다. 또한 스마트폰을 분실시 큰 손실을 피할수 없다. 예로, 뱅킹 서비스나 증권 서비스와 같은 금융 거래 앱을 이용하여 계좌이체, 증권거래까지 가능하며, 해당 정보들이 스마트폰에 그대로 보관될 경우 그 위협 수준이 높다할 수 있다.

표 1. 스마트 폰의 5대 위험

위협 요인	손실 내용
분실	.폰에 저장된 개인적 업무적 정보 유출 .재구매에 따른 추가 비용 발생
악성코드감염	.PC와의 Sync. Bluetooth 연결, Wi-Fi를 이용한 감염 .트로이 목마등을 이용한 단말기 탈취, 정보 유출, 공격지 활용
정보 유출	.통화기록, USIM Card 정보, GPS 이용한 위치정보 등 .외장형 메모리에 보관된 파일 .주소록, 이메일등 개인적인 리스트와 사진, 멀티미디어 화일
금전적 손실	.SMS, MMS등을 통한 불법적 유료 컨텐츠 과금 .모바일 뱅킹, 인터넷 뱅킹등을 이용한 금전적 탈취
공격지 활용	.사업자의 기지국에대한 DDos공격 .사용자의 PC에 대한 악성코드 다운로드 .기업 이메일 서버등을 목표로 하는 공격

최근에는 PC를 주요 대상으로 하는 랜섬웨어가 스마트폰 등 모바일로 확대되고 있다. 모바일 기기 이용 확산으로 개인정보 데이터가 스마트폰에 주로 저장됨에 따라 랜섬웨어의 공격대상이 PC에서 모바일로 전이 되었고 전 세계적으로 모바일 랜섬웨어가 2015년 3분기는 전년대비 6배 증가한 4만 건 발생, 북미, 유럽을 중심으로 모바일 랜섬웨어가 빠르게 확산중이다. 미국에서는 스마트폰에서 FBI를 사칭한 조직이 유포한 새로운 종류의 모바일 랜섬웨어 심플라커가 출현하였고 성인용 앱으로 위장한 랜섬웨어가 스마트폰 카메라로 사진을 촬영하고 이를 미끼로 금품을 요구하였다. 또한 미국・호주, 프랑스에서 아이폰 사용자들의 애플 계정 22만 5,000개가 해킹으로 유출되면서 일부 피해자들이 잠금을 풀어주는 대가로 돈을 요구하는 랜섬웨어에 감염되었다. 따라서 스마트폰이나 모바일 기기를 이용한 헬스케어 서비스를 위해서는 이러한 모바일 상에서의 보안 문제가 미리 해결되어야 할 것이다. 최근 발견된 모바일

기기를 위협하는 악성코드들을 살펴보면 다음 표 2[1][3][4][5]와 같다.

표 2. 모바일 기기 위협 악성코드

모바일 악성코드		특 징
RuMMS		.폰 사용자가 URL을 클릭하도록 유도하여 감염시킴, C&C서버에 사용자 정보 전송 .감염된 스마트폰에서 금융기관 및 은행의 SMS뱅킹 계좌 잔고를 SMS으로 확인 .은행 및 금융기관에서 감염된 스마트폰에 요청하는 이중인증(전화인증)을 차단하고, SMS 뱅킹 계좌로부터 10,000원 이하의 금액 탈취
Godless		.안드로이드 5.1(롤리팝) 또는 그 이전 버전의 기기를 대상 .앱 안에 숨어 있다가 취약점을 활용해 OS를 루트하고 기기 관리자 권한 획득, 비인가 앱을 사용자 몰래 설치 .최신 변종의 경우 구글 플레이와 같은 앱 스토어에서 보안 체크를 우회하고, 루팅 이후에는 삭제하기 힘듬
앱스토어를 통한 Rooting Malware		.Third-Party 앱 스토어를 통하여 확산 및 유포 .1,163개의 안드로이드 앱 패키지에 ANDROIDOS_LIBSKIN.A 라는 멀웨어가 포함되어 있음, .휴대전화에 대해 악의적인 Rooting과 최고 수준의 권한 획득
랜섬웨어	악성 자바스크립트를 이용	.사용자의 정보를 암호화한 경우는 아니고 기기내 다른 앱을 강제 종료하여 기기의 사용을 불가능하게 함 .비트 코인대신 iTunes 기프티 카드를 요구 .취약점을 이용하여 랜섬웨어를 배포하는 악성 광고와 악성 자바스크립트 .안드로이드에서도 쓰이는 리눅스 라이브러리를 악용한 취약점 이용 , 사용자의 허락없이 랜섬웨어 설치
	모바일 장치에서 직접 만듬	.해커는 AIDE가 제공하는 유연성과 신속성의 장점을 활용하여 랜섬웨어 제작 .초보 개발자의 경우 PC 환경에 간단한 코드(하드 코딩된 E-mail, 암호키 등) 수정을 통한 변종 생성이 가능 .고급 개발자는 PC와 같은 장비 없이 이동 중에 랜섬웨어 변종을 생성할 수 있다는 장점 이용

III. 국내외 모바일 헬스케어 활용

인구의 고령화, 생활수준 향상, 의료비 부담 증가에 따라 질병의 예방 및 일상생활 관리의 중요성에 대한 인식이 커지고 있다. 우리나라의 고령화 속도는 빠르게 진행되고 약물, 치료기술의 발달로 의료비가 상승하는 추세이다. 따라서 의료서비스는 치료중심구조에서 관리와 예방으로 전환되고 모바일 헬스케어는 이러한 변화를 주도할 서비스 부분으로 주목받고 있다. 특히 스마트폰, 스마트 워치등에 탑재된 모바일 앱과 스마트 밴드에 내장된 센서로 사용자의 건강정보 수집과 모니터링이 가능해져 개인 맞춤형 의료서비스가 확산될 것으로 기대된다. 이에 애플과 구글, 삼성전자등 글로벌 기업은 모바일 헬스케어 시장의 성장 가능성에 주목하고 자사의 플랫폼 영향력을 확대 개방하기 위해 협업을 확대하고 있다. 플랫폼 기업의 헬스케어 전략을 보면 다음 표 3과 같다.

표 3. 플랫폼 기업의 헬스케어 전략

기업	개발 플랫폼	특 징
애플	.헬스 .헬스키트	.의료데이터 측정 및 병원까지 연계 .헬스는 이용자의 몸무게 혹은 체질량지수 추세를 그래프로 표현, 자가 입력된 다이어트, 운동등에 대한 데이터 관리 .헬스키트는 수집된 의료정보를 의료진과 병원에 원격으로 전달
구글	구글핏	.개인의 건강관리 활용에 초점 .의료 관련 모바일 앱에서 생성된 건강정보 수집 .의료기관 시스템과 연계를 통한 의료서비스 제공보다 개인의 피트니스 데이터 활용에 중점
삼성	.사미 .심밴드	.데이터를 분석하고 연구하는 헬스케어 플랫폼 지향. 사미는 각종기기에서 수집된 건강정보 데이터를 클라우드 서버에 저장, 상황인지, 맥락분석 과정을 거쳐 정체된 데이터를 사용자에게 다시 제공 .심밴드는 각종 건강정보를 측정할수 있도록 각종 센서가 하나의 모듈로 통합, 특정된 정보는 무선으로 사미에게 전달.

이외에도 디지털 헬스케어 전문매체 ‘모비헬스뉴스’의 보도에 따르면, 미국 국립보건원이 모바일 단말을 이용한 의료 정보 수집 방안을 검토 중이고 미국 국립보건원은 공식 블로그를 통해 스마트폰과 웨어러블 단말을 이용한 환자의 건강 정보와 생활 습관 등의 수집을 고려하고 있다. 국립보건원의 의료정보 수집 프로젝트는 ‘정밀의학 이니셔티브’의 일환으로 진행되고 있으며 환자의 특성을 고려한 맞춤형 치료 방식을 개발하는 것이 주목적이다. 또한 산학에서도 모바일 웨어러블 단말을 이용한 임상연구 가속화가 이루어지고 있다. 그 예로 글락소스미스클라인은 자사 임상실험 과정에 애플의 의료 데이터 수집 플랫폼 ‘리서치킷’을 포함시켜 가동하고 있다. 또한 학계에서는 이미 모바일 단말과 리서치킷을 이용한 대규모 임상 실험을 진행 중이며 어느 정도의 성과도 거두고 있는 상황이다. 마운트 시나이 아이칸 의과대학, 코넬 의과대학등이 공동 개발한 리서치킷 기반의 천식 연구용 앱 ’애스마 헬스’의 경우 출시 수개월 만에 이용자 7만 5,000명을 확보하였다. 모바일 기반의

의료 연구는 현재 대중화가 많이 진행된 스마트폰을 중심으로 전개되고 있지만, 웨어러블 단말 역시 빠른 확산이 예상되는 만큼 해당 플랫폼을 이용한 연구도 보다 활발해지고 있다.

Ⅳ. 헬스케어를 위한 모바일 위협 대응방안

모바일 헬스케어를 활성화하기 위해서는 많은 법적 규제나 정보보호 관리체계, 인증 의무화등이 추진되어야하고 가장 많이 사용하는 스마트 폰에 대한 위협요소를 파악하고 이것에 대한 대응방안을 마련하는 것이 우선일 것이다. 다음 표 4는 몇 가지 개념을 기준으로 기술한 대응방안이다[7].

표 4. 기준 지점별 대응방안

기준지점	대응 방안
운영체제	루트킷감지, 프로세스 관리, 파일권한, 메모리 보호, 런타임 환경에서 개발
어플리케이션	안티바이러스, 방화벽, 시각적 알림, 개발보안, 디버그 모드 제거, 디폴트 설정, 보안감사, 앱권한감지 및 경고, 원격삭제, 앱업데이트
리 소 스 모니터링	배터리, 메모리, 네트워크 트래픽 서비스
네트워크 감시	스팸필터링, 암호화, 데이터 통신 감시
사 용 자 보안의식	자각노력, 권한에 대한 신중, 보호조치, 데이터 흐름주시

운영체제측면에서 본다면 일차적으로 앱을 보호하기 위해서는 앱들의 리소스와 데이터를 관리하는 운영체제를 보호하는 것이 우선적이어야 한다. 스마폰의 경우 샌드박스 모델이다. 보안적인 개념을 운영체제에 도입한 것으로 앱으로 각자 구획화 시켜서 프로세스와 리소스를 분리시켜 관리하는 것이다. 따라서 앱간의 리소스나 프로세스를 공유할 수 없다. 표에서는 안도로이드에 도입된 메카니즘을 의미한다. 어플리케이션 측면에서 보면 운영체제 위에 어플리케이션계층이 존재하게 된다. 운영체제가 구동하기 위한 기본적인 기능을 수행하는 것에 초점을 둔다면 어플리케이션 계층에서는 다양한 목적을 가지고 보안을 위한 소프트웨어가 개별적으로 운영된다. 리소스 모니터링 측면에서 보면 선재적인 방어수단을 이용하여 우회하여 감염되는 경우가 발생할 수 있다. 항상 새로운 기법에 의한 공격이 발생하기 때문에 원천적으로 100%막는 것이 불가능하다. 감염된 멀웨어는 잠복기간을 거치거나 즉시 활동을 사작하게 되는데 이때 비정상적인 행위를 하게 된다. 사용자가 지속적으로 리소스를 감시하고 있다면 일정수준 멀웨어의 존재를 인지 할 수 있게 된다. 네트워크 감시 측면에서 보면 스마트 폰의 경우 PC보다 네트워크에 대하여 제한적인 경우가 많기 때문에 감시하기가 더 용이한 편이다. 전화 또는 메시지의 경우 이외에 규칙을 정해서 감시하는 것이 일반적이다. 사용자 보안의식의 제고측면에서 보면 멀웨어의 대부분 감염은 사용자의 부주위한 습성으로 발생된다. 쉬운 암호를 사용한다든지 관리자 권한을 요구하는 상황을 쉽게 허용하는 경우이다.

Ⅴ. 결 론

스마트폰은 어느 곳에서나 원하는 정보를 활용할 수 있게 하는 연결 매체로 하나의 장소에 고정되어 있지 않고, 항상 곁에서 켜져 있는 개인화 장치이다. 이것은 사용자 중심의 장치로 인간적, 지능적 감지기능을 통해 다양한 형태의 정보를 얻고 사용할 수 있는 특성으로 패러다임의 변화를 주도하고 있다. 따라서 스마트폰은 이용하는 많은 서비스들이 활발한 성장하고 있다. 특히 헬스케어 분야에 많은 성장을 보이며 웨어러블 기기를 활용한 헬스케어 사용자가 증가하고 글로벌 ICT 기업의 헬스케어 서비스간의 연동을 지원하는 플랫폼 개발, 개발자 참여유도등을 통한 서비스가 확산되고 있다. 그러나 이것에 비례하여 보안사고가 해마다 증가하고 있다. 금융사기, 불법 판촉, 보험 제약 회사 악용 등 2차 피해 발생 가능성이 높은 금융, 의료 분야에서 개인정보 유출 사고 등의 위험이 증가 추세이다. 따라서 모바일 에코시스템 전반적인 보안을 위해 단말제조사, 이동통신사, 마켓 운영자, 개발사 등 에코시스템의 모든 구성원의 협업 및 협조가 필요하며 제도적인 뒷받침도 있어야 할 것이다.

감사의 글

이 논문은 2016년 한국교통대학교 지원을 받아 수행한 연구임.

참고문헌

[1] “사용자 입력 없이 안드로이드 기기를 감염시키는 랜섬웨어 발견” KISA report 2016.5.
[2] 김홍선, 최은혁, “ 모바일 생태계의 보안 이슈 및 전망”, 스마트 폰 정보보호, TTA Journal No.132, 2010.11.
[3] “앱스토어를 통한 Rooting Malware 발견” KISA report 2016.5.
[4] “모바일 장치에서 직접 만드는 안드로이드 랜섬웨어 변종 발견”, KISA report 2016.3.
[5] “금융 · 의료등 전 산업에 적용되는 정보보호 관리체계”, 정보보호 10대 이슈 전망, 2016.
[6] “국내외 모바일 헬스케어 동향과 시사점”, ICT Spot Issue, 2015.8.
[7] http://ahope.net/blog/2015/09/02