웨어러블 기기로써의 스마트워치 보안 취약성 및 대응방안

A Study on the Security Vulnerabilities of Smart Watch as a Wearable Device

저자 (Authors)
유요셉, 이종원, 김기천
Yoo Joseph, Lee Jong Won, Keecheon Kim

출처 (Source)
한국통신학회 학술대회논문집 , 2016.6, 119-120(2 pages)
Proceedings of Symposium of the Korean Institute of communications and Information Sciences , 2016.6, 119-120(2 pages)

발행처 (Publisher)
한국통신학회
Korea Institute Of Communication Sciences

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06740031

APA Style
유요셉, 이종원, 김기천 (2016). 웨어러블 기기로써의 스마트워치 보안 취약성 및 대응방안. 한국통신학회 학술대회논문집, 119-120

웨어러블 기기로써의 스마트워치 보안 취약성 및 대응방안

유요셉, 이종원, 김기천*
건국대학교 컴퓨터공학부

josephyoo94@gmail.com, 123leej@naver.com, kckim@konkuk.ac.kr*

A Study on the Security Vulnerabilities of Smart Watch as a Wearable Device

Yoo Joseph, Lee Jong Won, Keecheon Kim*
Konkuk Univ.

요 약

스마트폰의 폭발적인 수요 증가로 인하여 다양한 웨어러블 디바이스들의 수요도 함께 증가하고 있다. 웨어러블 디바이스는 아직까지 발전이 이루어지고 있는 분야임에 따라 보안상의 이슈가 다양하게 존재하고 있으며, 제조사들 각각의 방식으로 구현되는 과정에서 보안 기능이 결여되는 경우가 대다수이다. 웨어러블 디바이스의 보안상 기능 결여로 인해 스마트폰과 연동한 통신 과정에서 데이터의 침해나 오작동으로 보안상의 위험이 발생할 소지가 다분히 높아지는 추세이다. 본 논문에서는 웨어러블 디바이스의 큰 부분을 차지하고 있는 스마트워치를 실례로 들어 스마트워치를 다방면으로 공격 해보고 다양한 보안 위험성이 존재함을 보여주고 이를 방지하기 위한 대응방안을 제안하고자 한다.

Ⅰ. 서 론

스마트폰의 증가와 함께 연동하여 사용이 가능한 웨어러블 디바이스들의 증가도 함께 이루어지고 있으며 대표적인 디바이스로 스마트워치가 부각되고 있다. 시장정보 회사인 Tractica에서는 2020 년경에 1 억대에 가까운 스마트워치 판매량을 보일 것으로 전망하고 있다. [1]

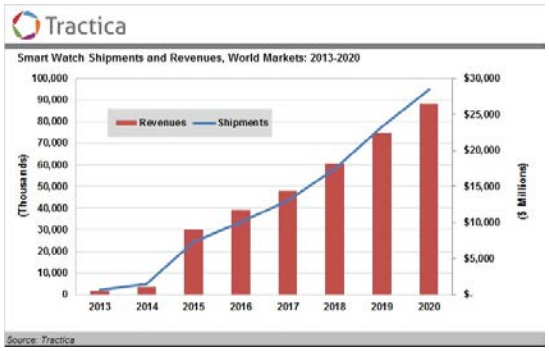

그림 1 스마트워치 시장규모 예상[1]

스마트워치의 수요는 증가하고 있지만 보안 기능 구현은 미비한 실정이다. 2015 년 HP사의 연구보고서에 따르면 스마트워치의 보안 상태는 스마트워치 관리기능, 네트워크 통신 기능, 모바일 인터페이스, 클라우드 인터페이스 등의 측면에서 취약한 부분이 존재하고 개인 정보 유출에도 매우 취약함을 지적하고 있다. [2]

보안 기능이 취약한 스마트워치의 증가로 보안 공격의 위험성이 증가하여 스마트워치와 스마트폰 사이의 통신 시 발생하는 데이터를 가로채거나 변조하여 큰 피해를 발생시킬 수 있는 위험성에 노출되게 된다. 스마트워치 시장이 아직 성장하는 분야인 만큼 보안적 위험성을 인지하고 대응방안도 충분히 고려되어야 한다.

Ⅱ. 관련연구

스마트워치는 스마트폰과 정보를 주고받기 위해 Bluetooth와 무선 LAN 환경에서 동작하게 된다. 스마트워치는 기본적으로 스마트폰과 Bluetooth 환경에서 연동하고 Bluetooth 기능을 해제 하거나 Bluetooth 신호 범위를 벗어나는 경우 같은 AP(Access Point)를 통해 무선 LAN으로 연동하게 된다. 스마트워치에서 사용되는 Bluetooth와 무선 LAN의 보안 기법은 다음과 같다.

1. Bluetooth 보안

Bluetooth 보안 기법에는 키 관리와 기기 인증 두 가지 방식이 존재하며, 키 관리의 경우 개인 식별번호와 개인 링크키, 인증키, 유닛키, 조합키, 마스터키, 초기화키, 개인용 인증키, 암호화키의 다양한 키를 사용하여 안전한 데이터 전송을 보장한다. 중요한 요소로서 기기간의 인증을 위해 사용되는 링크 키이다. 기기 인증의 경우에는 통신할 양쪽 기기가 같은 식별 비밀 키(대칭 키)를 가지고 있는지 확인하고 같은 경우에 연결을 유지시킨다. [3]

2. 무선 LAN 보안

무선 LAN 보안에서도 인증과 암호화를 원칙으로 한다. Wi-Fi WPA/WPA2 가 무선 LAN 국제 표준인 IEEE 802.1X/802.11i의 보안표준 규격으로 제정되어있다. 무선 LAN은 공유키나 PSK(Pre-shared Keys), 802.1X EAP인증, WEP(Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol), CCMP(Counter mode with CBC-MAC Protocol) 방식의 암호화 기술을 사용한다. 현재에는 보안이 취약한 WEP보다 보안성이 우수한 WPA의 TKIP, CCMP기술이나 높은 수준의 보안성을 제공하는 WPA2 의 AES를 사용하는 CCMP 기술을 사용하여 무선LAN 인증 및 암호화를 수행한다. [4]

Ⅲ. 스마트워치 보안 취약성 검증

인슐린 펌프, 심박조율기 등의 의료용 웨어러블 기기를 해킹하여 인슐린을 과다하게 투여하도록 조작하거나 심박조율기를 멈추게 하는 등의 오작동을 유도하는 웨어러블 디바이스 해킹 사례가 존재하며, 이는 의료용 웨어러블 디바이스가 보안에 매우 취약함을 나타내고 있다. [5]

* 교신저자

현재 상용화 되어 있는 스마트워치에서도 보안 취약성으로 인해 스마트폰과 통신중에 정보가 탈취되는 등의 큰 문제를 발생시키게 된다.

스마트폰의 앱을 통해 수신된 메시지를 연동된 스마트워치에서 확인하는 경우 스마트폰이 잠금 상태인 경우에는 스마트워치에서 메시지의 내용 확인이 불가하나, 스마트폰이 잠금 상태인 경우에도 스마트워치에서 메시지 내용을 확인 가능하도록 설정하면 이후에 도착한 메시지뿐만 아니라 이전의 메시지 내용도 확인이 가능하며, 이는 스마트폰과 연동된 스마트워치에서 스마트폰에 저장된 정보를 손쉽게 확인이 가능하다는 것을 보여준다.

그림 2 잠금시 수신한 데이터도 보여주는 스마트워치

스마트폰과 연동된 스마트워치에서 MITM(Man In The Middle) 공격, 스마트워치에 대한 서비스 거부 공격이 가능함을 실험을 통하여 보안 취약성을 검증하고자 한다.

1. 실험 환경

무선 LAN 기능을 지원하는 스마트워치인 삼성 Gear S2, 스마트폰과 동일한 AP에 연결하고 패킷을 수신하기 위한 iptime-n150ua 무선 LAN 카드를 이용하였다. 패킷은 Backtrack5 에서 제공하는 airmon-ng 툴을 사용하여 monitor 모드의 인터넷 인터페이스를 구축하여 802.11 프로토콜의 데이터를 캡쳐하였으며 서비스 거부 공격이 가능함을 실험하기 위해 Backtrack5 에서 제공하는 smurf 툴을 사용하여 실험을 진행하였다.

2. 실험 방법

스마트워치와 스마트폰이 주고받는 패킷을 와이어 샤크를 통해 수집하여 취약점과 공격이 유효함을 확인하기 위한 실험을 진행한다. 스마트워치의 보안 취약성을 예상하고 공격 시나리오를 구상하여 다음과 같은 실험을 진행함으로써 공격 시나리오 작용 여부를 확인하고 스마트워치의 보안 취약성을 검증한다.

① Sniffing과 이를 통한 MITM 공격

MITM(Man in The Middle) 공격이란 네트워크를 조작하여 통신 내용을 가로채거나 조작하는 공격으로 스마트폰과 스마트워치가 주고받는 신호를 가로채어 정보를 취득할 수 있는지 확인한다.

② DoS(Denial of Service)의 일종인 Smurf 공격

Smurf 공격은 ICMP(Internet Control Message Protocol)을 동일 네트워크에 존재하는 호스트 집단에 호스트 대상으로 하는 공격 패킷을 전송하여 응답을 받는 호스트 대상이 과다하게 발생한 패킷으로 정상적인 서비스를 할 수 없게하는 공격으로 스마트워치에 해당 공격 수행으로 정상적인 서비스가 불가능함을 확인한다.

3. 실험 결과

1) Sniffing과 이를 통한 MITM 공격

무선 LAN 환경에서 스마트폰과 스마트워치가 주고받는 전송된 데이터를 확인하기 위해 단순히 알림만 발생시키는 스마트폰 앱을 만들어 실험을 진행하였다. 알림 발생 후 802.11 프로토콜을 사용하는 패킷들을 캡쳐했다. 감지된 패킷의 종류들은 크게 QoS Data와 ACK, Request-to-send와 Clear-to-send의 흐름이 나타났다. 이를 통해 스마트폰과 스마트워치가 주고받는 데이터의 스니핑은 매우 간단히 이뤄짐을 알 수 있으며, 이를 악용해 MITM 공격이 가능함을 확인할 수 있었다.

2) DoS(Denial of Service)의 일종인 Smurf 공격

Backtrack의 Smurf 툴을 이용하여 스마트워치가 접속해 있는 AP를 통해 Smurf 공격을 시도해 보았다. 공격 당시 스마트워치로 수신되는 패킷수가 급증하였고 스마트워치는 계속 AP와의 접속이 끊기며 반복적으로 AP접속 시도를 하는 결과를 확인할 수 있었다.

Ⅳ. 결론

웨어러블 디바이스 중 가장 보편적으로 보급이 된 스마트워치를 타겟으로 다양한 시나리오를 통해 가능한 위험성을 분석해보았다. 실험 검증을 위해 스마트워치와 스마트폰이 주고받는 패킷을 수집, 분석하였으며 스마트워치에 과도한 패킷을 전송해 부하를 발생시키고 무선 LAN 접속 기능이 무력화됨을 확인하였다. 본 연구를 통해 스마트워치는 실생활과의 밀접한 정도에 비해 그 보안 기능이 충분하지 않아 인터넷에 유통되는 간단한 툴만으로도 쉽게 공격을 할 수 있다는 사실을 확인할 수 있었다.

웨어러블 디바이스는 우리 생활에서 큰 비중을 차지하고 있지만 실생활에서 가까이 사용되는 만큼 제공하는 보안성은 절대 충분하지 않은 현실이다.

이에 웨어러블 기기의 보안상 향상을 위해서는 비정상적인 패킷에 대한 무시와 불필요한 브로드캐스트 port의 해제, 그리고 검증된 강력한 암호화를 기반으로 한 통신의 사용을 제안한다.

ACKNOWLEDGMENT

이 논문은 2015 년도 정부(미래창조과학부)의 재원으로 정보통신 기술진흥센터의 지원(No.B0511-15-0001, 글로벌 딜리버리 클라우드 플랫폼의 대규모 OTT 서비스 적용을 위한 방송· 통신 사업자 공동의 시범 사업)으로 수행된 연구임

참 고 문 헌

[1] Tractica, Smart Watch Shipments Will More than Quadruple in 2015, Reaching 24.4 Million Units Worldwide, (https://www.tractica.com/newsroom/press-releases/smart-watch-shipments-will-more-than-quadruple-in-2015-reaching-24-4-million-units-worldwide)

[2] HP, HP Study Reveals Smartwatches Vulnerable to Attack, (http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386)

[3] 최유미,추현승. “Bluetooth 단거리 무선 네트워크 상에서 보안과 인증 매커니즘”. 한국인터넷정보학회 학술발표대회 논문집 5(1), p.365-368. 2004.5.

[4] 디지털데일리, [WiFi특집] 7. 무선랜의 취약점? 무선랜 보안을 말한다 (http://www.ddaily.co.kr/news/article.html?no=31479)

[5] 조선일보, 의료기기가 해킹 당한다면?... 3 가지 시나리오 (http://review.chosun.com/m/article.html?contid=2013080601265#)