# 스마트워치 저성능 하드웨어에서 발생 가능한 보안위협 도출

박민서[1], 정인수[2], 김득훈[3], 곽진[4]
[1]아주대학교 사이버보안학과, 정보보호응용및보증연구실 학부생
[2]아주대학교 사이버보안학과, 정보보호응용및보증연구실 석박통합과정
[3]아주대학교 소프트웨어융합연구소 박사후연구원
[4]아주대학교 사이버보안학과 교수
winp82@ajou.ac.kr, jis0727@ajou.ac.kr, kimdh1206@ajou.ac.kr, security@ajou.ac.kr

# Potential Security Threat Derivation based on Low-Performance Hardware of Smartwatch

Min-Seo Park[1], In-Su Jung[2], Deuk-Hun Kim[3], Jin Kwak[4]
[1,2]ISAA Lab., Dept. of Cyber Security, Ajou University
[3]Inst. for Computing and Informatics Research, Ajou University
[4]Dept. of Cyber Security, Ajou University

요 약

최근 스마트워치는 통화, 문자, 간편 결제, 기타 장치 제어 등 스마트폰의 소형화 및 경량화 형태로 연구되어 여러 서비스를 제공하고 있다. 스마트워치는 스마트폰 대비 작은 물리적 크기로 인해 적용 가능한 하드웨어의 성능이 상대적으로 낮으며, 이로 인해 낮은 수준의 보안 기능을 제공한다. 이는 스마트워치 대상 보안위협으로 이어질 수 있으며, 이에 대응하기 위한 보안위협 분석 및 도출 연구가 필요한 실정이다. 따라서, 본 논문에서는 스마트워치의 하드웨어 적용 한계점으로 인한 스마트워치와 스마트폰의 성능 차이를 분석하고, 이로 인해 발생 가능한 보안위협을 도출한다.

## 1. 서론

스마트워치는 통화나 문자 등 기본적인 알림을 제공하는 것에서 확장되어 간편 결제, 헬스케어 등 다양한 서비스를 제공한다. 하지만 접근성, 편의성을 제공하기 위한 소형화 및 경량화로 스마트워치의 물리적 크기가 제한된다. 이에 따라, 스마트폰 대비 낮은 성능의 하드웨어가 탑재되고 보안 기능 또한 스마트폰 대비 낮은 수준을 제공한다. 이는 스마트워치 대상 사용자 데이터 및 권한 탈취와 같은 보안위협으로 이어질 수 있으며[1], 이에 대응하기 위해 하드웨어 차이 기반 스마트워치 대상 보안위협 도출 연구가 필요한 실정이다. 따라서, 본 논문에서는 스마트워치의 하드웨어 적용 한계로 인한 스마트폰과 성능 차이를 분석하고, 이로 인해 발생 가능한 보안위협을 도출한다.

본 논문은 2장에서 스마트워치와 스마트폰의 하드웨어 성능을 분석한다. 3장에서는 스마트워치와 스마트폰의 하드웨어 성능 차이로 인해 발생 가능한 보안위협을 도출하고, 4장에서 결론을 맺는다.

## 2. 스마트워치와 스마트폰의 하드웨어 성능

스마트워치의 하드웨어 한계점 분석을 위해 스마트워치[2,3,4]와 스마트폰[5,6]의 성능을 분석한다.

<표 1> 스마트워치 하드웨어 성능

| 구성요소 | 'A'사 | 'S'사 | 'H'사 |
|---|---|---|---|
| CPU | 듀얼 코어 | 듀얼 코어 | 알 수 없음 |
| RAM | 1GB | 2GB | 32MB |
| 인증 기능 | PIN, 패턴 | PIN, 패턴 | PIN |
| 배터리 | 303mAh | 425mAh | 451mAh |

<표 2> 스마트폰 하드웨어 성능

| 구성요소 | 'A'사 | 'S'사 | 'H'사 |
|---|---|---|---|
| CPU | 6코어 | 8코어 | 스마트폰 없음 |
| RAM | 6GB | 12GB | |
| 인증 기능 | 생체 인식, PIN, 패턴 | 생체 인식, PIN, 패턴 | |
| 배터리 | 3,877mAh~4,912mAh | 3,900mAh~5,000mAh | |

## 3. 스마트워치 저성능 하드웨어 상의 보안 성능 분석 및 발생 가능한 보안위협 도출

스마트워치는 경량화 및 소형화로 인해 CPU, RAM, 배터리 등 하드웨어 성능이 스마트폰 대비 낮은 성능을 가진다. 특히 'H'사의 저가형 스마트워치는 CPU 성능을 알 수 없지만 'A'사와 'S'사에 비해 낮은 성능으로 예상되고, RAM에서도 낮은 성능의 하드웨어가 탑재된다. 이로 인해, 스마트폰에서 사용되는 암호화

기법 적용 및 활용에 한계가 존재한다. 또한, 스마트폰은 Bluetooth Classic과 BLE(Bluetooth Low Energy)를 사용하는 반면, 스마트워치는 하드웨어 성능의 한계점을 해결하기 위해 BLE만 사용한다. 뿐만 아니라, 스마트폰에서 사용자 인증을 위해 사용하는 지문 인식, 안면 인식 같은 생체인식 센서가 탑재되지 않았다.

### 3.1 암호화의 부재

스마트워치는 스마트폰 대비 저성능 하드웨어를 지원함에 따라 스마트폰에서 사용하던 높은 강도의 암호화를 적용하는데 한계가 존재한다. 이로 인해, 일부 기기는 암호화 통신을 수행하지 않는다[7]. 이를 악용하여 공격자는 스니퍼 도구와 스마트워치의 MAC 주소를 이용하여 스마트워치와 스마트폰 간의 통신 및 스마트워치와 클라우드 간의 통신을 스니핑 할 수 있다. 이때, 통신 트래픽이 암호화 되어있지 않아 공격자는 통신 트래픽의 내용을 확인할 수 있다. 이를 통해, 스마트워치에서 전송되는 사용자의 개인정보, 헬스케어 및 결제 정보 등 민감 데이터를 탈취할 수 있다.

### 3.2 낮은 보안 수준의 경량 통신 기법

스마트워치는 스마트폰 대비 적은 배터리 용량 문제를 해결하기 위해 기존 블루투스보다 전력 소모량이 적은 BLE를 사용한다. 그러나, BLE를 사용하는 스마트워치의 일부 기기에서 한 번 페어링이 이루어졌던 스마트폰과 재연결 시 추가적인 기기 인증을 진행하지 않는 취약점이 존재한다. 공격자는 이를 악용하기 위해 페어링이 완료된 스마트워치와 스마트폰의 연결을 재밍 기법 등을 통한 전파 방해 기술로 강제 종료시킨다. 또한, 공격자는 이전에 스마트워치와 페어링이 이루어졌던 스마트폰으로 가장한다. 이로 인해, 스마트워치는 공격자를 재연결 대상으로 인식하고 추가적인 기기 인증 없이 페어링 하게 된다. 이를 통해, 공격자는 스마트워치의 권한을 탈취할 수 있다.

### 3.3 낮은 보안 수준의 사용자 인증

스마트워치는 생체인식 센서 도입의 한계로 사용자 인증에 PIN, 패턴을 사용한다. 이는 생체인식 대비 낮은 보안 수준을 지원하고, 이를 대상으로 하는 보안위협이 발생할 수 있다. 예를 들어, 공격자는 피싱을 통해 스마트워치에 악성 코드를 설치하여 스마트워치의 모션 센서 권한을 획득하고, 이를 통해 수집한 모션 데이터를 분석하여 PIN 및 패턴을 탈취할 수 있다. 공격자는 물리적으로 스마트워치를 획득하였을 때 탈취한 PIN 및 패턴을 악용하여 사용자의 데이터에 접근할 수 있으며, 스마트카와 같은 IoT 장치를 제어하여 2차 사고를 발생시킬 수 있다. 또한, 스마트워치를 활용하여 온·오프라인 간편 결제 시 탈취한 PIN이나 패턴을 통해 부정 결제에 악용할 수 있다.

## 4. 결론

본 논문에서는 스마트워치와 스마트폰에 탑재된 하드웨어 성능 차이를 분석하고, 이로 인해 발생 가능한 보안위협을 도출하였다. 추후 분석 내용을 기반으로 스마트워치에 발생 가능한 보안위협 대응 방안을 도출할 예정이다.

## 사사문구

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2011391)

## 참고문헌

[1] Araron James Webb, “Cyber Security of Smart Watches : A Review of the Vulnerabilities with Recommendations Presented to Protect the Wearables”, International Journal of Network Security & Its Applications, Vol. 14, No. 3, pp.39-56, Jun. 2023.

[2] Apple, “Apple Watch Series 8 - 제품사양”, 2023. [Online]. Available: https://support.apple.com/kb/SP878?viewlocale=ko_KR&locale=ko_KR

[3] Samsung, “갤럭시 워치6 클래식 43mm(블루투스)”, 2023. [Online]. Available: https://www.samsung.com/sec/watches/galaxywatch6-11-r950/SM-R950NZKAKOO/

[4] Honor, “HONER Watch 4”, 2023. [Online]. Available: https://www.hihonor.com/global/wearables/honor-watch-4/spec/

[5] Apple, “iPhone 15 Pro”, 2023. [Online]. Available: https://www.apple.com/kr/iphone-15-pro/specs/

[6] Samsung, “갤럭시 S23 Ultra”, 2023. [Online]. Available: https://www.samsung.com/sec/smartphones/galaxy-s23-ultra-s918/SM-S918NZGEKOO/

[7] Jaime Fuster, Sonia Solera-Cotanilla, Jaime Perez, Mario Vega-Barbas, Rafael Palacios, Manuel Alvarez-Campana and Gregorio Lopez, “Analysis of security and privacy issues in wearables for minors.”, Wireless Networks, pp. 1-17, Mar. 2023.