Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.6, Dec. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.6.893

갤럭시 워치를 중심으로 본 스마트워치 활용 기술유출의 위험성 및 대응방안에 대한 연구

전 승 제,[1†] 정 재 현,[1] 정 두 원[2‡]
[1,2]동국대학교 (대학원생, 교수)

A Study on the Risks of Technology Leakage Using Smartwatch and Its Countermeasures Focusing on Galaxy Watch

Seungjae Jeon,[1†] Jaehyun Chung,[1] Doowon Jeong[2‡]
[1,2]Dongguk University (Graduate student, Professor)

요 약

스마트폰이 범행 도구로 사용될 수 있다는 인식은 많은 기관에서 만연하지만, 기능적으로 스마트폰과 유사한 스마트워치의 범행 도구로의 잠재력은 간과되고 있다. 본 논문은 이러한 상황을 고려하여, 보안 규정과 기술 등에 의하여 스마트폰은 통제되고 있지만, 스마트워치는 통제되지 않는 상황에서, 내부자의 스마트워치를 통한 정보유출 가능성을 입증한다. 입증 과정에 의해 스마트워치에서 발생한 애플리케이션 사용 관련 정보, Wi-Fi 연결 관련 정보를 분석함으로써, 포렌식 가능한 정보와 한계를 파악한다. 마지막으로, 스마트워치 관련 잠재적 범죄에 대비하기 위한 예방 방법을 제안하고, 스마트워치의 범행 도구로의 사용 가능성에 대한 경각심을 재고한다.

ABSTRACT

Awareness that smartphones can be used as tools for criminal activity is prevalent in many organizations, but the functionally smartphone-like smartwatch's potential as a criminal tool is being overlooked. Considering this situation, this research verifies the possibility of information leakage through an insider's smartwatch in a situation where smartphones are controlled by security regulations and technologies, but smart watch are not. By analyzing information related application usage and Wi-Fi connection generated in the smartwatch during the verification process, forensic information and limitations are identified. Finally, this research proposes preventive methods to prepare for potential smartwatch-related crimes, and reconsiders awareness of the possibility of using smartwatches as criminal tools.

Keywords: Inforamtion Leakage, Smartwatch Forensics, Android Forensics, Mobile Device Management, Security Policy

I. 서 론

기술 및 경영상의 정보유출은 기업 생존에 치명적인 위협으로 작용하는 심각한 범죄이다. 국가정보원 산업기밀보호센터에 의하면 2017년부터 2022년까지 산업기술의 국외 유출 적발 건수는 총 117건이며, 이 중 국가 핵심기술 유출은 36건(약 30.7%)이었으며, 피해 규모는 26조 원으로 추정된다[1]. 이러한 상황을 극복하기 위하여, 경찰청은 2023년 2월부터 '경제안보 위해 범죄 특별단속'을 실시하였다. 특별단속 중간 결과 발표에 의하면 4개월 동안 총 35건의 정보유출 범죄를 수사하였으며, 이중 유출 주체가 내부인인 경우가 30건(약 85.7%), 외부인인 경우가 5건(약 14.3%)으로 확인되어, 정보유출의 주된 주체

Received(08. 18. 2023), Modified(11. 01. 2023), Accepted(11. 01. 2023)
† 주저자, jsj970515@dgu.ac.kr
‡ 교신저자, doowon@dgu.ac.kr(Corresponding author)

가 기업 내부인이라는 것을 확인할 수 있다[2]. 이러한 문제에 대응하기 위하여 정보유출 시나리오를 설계하고 시나리오에서 도출된 핵심 지표를 분석하는 연구가 이루어진 바가 있다[3]. 본 연구는 선행 연구의 방법론에 착안하여, 가장 대중화되었고 휴대하기 간편한 IoT(Internet of Things) 기기인 스마트워치를 내부정보 유출의 새로운 저장 및 통신 매체로 사용하는 시나리오를 제시한다.

우리나라의 스마트워치 사용률은 2020년 12.0%, 2021년 19.0%, 2022년 24.0%로 전 연령대의 사용률이 고르게 증가하고 있으며[4], 이러한 통계는 스마트워치가 국내에서도 충분히 대중화된 IoT 기기임을 입증한다. 기존 디지털 포렌식 연구의 초점은, 가해자 혹은 피해자가 우연히 스마트워치를 착용하고 있었던 범죄 상황에서 스마트워치 내 정보를 혐의 입증의 증거로 활용하기 위한 연구에 집중되어 있었다. 스마트워치가 운동 보조를 위해 생성한 데이터를 통해서는 사용자의 건강정보 및 GPS 정보를 식별할 수 있고, 스마트폰과의 동기화로 인해 사용자가 스마트폰에 저장한 일정이나 스마트폰으로 받은 알림을 스마트워치에서 확인할 수 있었기 때문이다.

본 연구는 이러한 기존 연구와 다른 관점에서 스마트워치가 그 자체로 기밀 정보유출의 도구로 사용될 때의 포렌식 조사 방안에 대한 연구를 수행하였다. 스마트워치에 비하여 고성능의 정보통신 도구인 스마트폰의 경우 범죄 수단으로 활용될 수 있다는 우려가 커, 이미 많은 기관에서 사용을 금지하거나 통신을 불가하게 하는 등의 규범적이고 기술적인 노력을 행하고 있다. 그러나 유사한 OS(Operating System)를 사용하는 스마트워치에 대한 사전 대응은 현재 부족한 상황이다. 이러한 보안 정책의 격차에 주목하여 본 연구는 스마트워치 전용으로 개발된 애플리케이션과 스마트폰 전용으로 개발된 애플리케이션을 스마트워치에 설치하고, FTP(File Transfer Protocol), SFTP(Secure File Transfer Protocol)를 통한 정보 전송과 소형카메라 연결을 통한 정보 촬영이 가능하다는 것을 입증하여 스마트워치를 이용한 범죄의 위험성을 규명한다. 이어서 입증 과정에서 발생한 데이터를 안드로이드 시스템 로그를 통해서 분석하는 포렌식 대응 방안을 제시한다.

이어지는 2장에서는 스마트워치 포렌식과 관련한 선행연구와 스마트워치 분석이 실제로 범죄자 검거에 이용된 사례를 살펴본다. 3장에서는 구글과 삼성이 제작한 최신 웨어러블 OS인 Wear OS Powered by SAMSUNG이 지닌 특성과 제원을 확인한다. Google과 삼성이 공동 제작한 Wear OS Powered by SAMSUNG에 주목한 까닭은 타 OS와 비교하여 애플리케이션 개발과 설치 측면에서 개발자와 사용자의 자유도가 높아 범죄에 활용하기 적합하다고 판단하였기 때문이다. 4장에서는 스마트워치를 이용한 범죄가 가능함을 입증하고 5장에서는 입증 과정에서 발생한 데이터를 ADB(Android Debug Bridge)를 통해 분석하는 방법을 소개한다. 6장에서는 5장에서 사용한 분석 방법의 한계와 스마트워치를 이용한 기술유출 범죄의 대응 방안을 논의한다.

II. 선행연구

Rughani와 Dahiya[5]는 Android Wear 운영체제의 스마트워치를 분석하였다. Android Wear 운영체제는 현재 최신 스마트워치에 탑재되고 있는 Wear OS 운영체제의 전신으로, 안드로이드 4.3 이상의 기기와 연결된다. 스마트폰과 연결 시 스마트폰의 구글 메일, 캘린더, 휴대전화 알림 등의 정보가 스마트워치로 업데이트되는데, 해당 논문에서는 스마트워치로 업데이트된 정보를 분석하기 위하여 dd 명령어를 사용하여 스마트워치의 이미지를 덤프하여 아티팩트를 분석하는 방법을 사용하였다. 분석 결과 연결된 기기 정보, 음성 명령 이력, 알림 내역, DropBox 아티팩트 등을 파악할 수 있었다.

Odom et al.[6]은 Tizen OS를 사용하는 삼성의 Galaxy Gear S3와 Watch OS를 사용하는 애플의 Apple Watch Series 3를 분석하였다. 호스트 기기인 스마트폰과 연결되어 사용하는 블루투스 연결 방식과 독립적으로 사용하는 Stand-Alone 방식을 비교하여 스마트워치 내부에 남는 연락처, 일정, 알람, 리마인더, 노트, 비밀번호, 이메일, 멀티미디어, 전화 기록, SMS(Short Message Service), MMS(Messengers Multimedia Message), IM(Instant Messenger), 음성 명령, 건강 기록 등을 확인하였다. 분석한 결과를 통해 GearGadget이라는 Galaxy Gear S3 분석 도구를 제작하였다.

Kim et al.[7]은 삼성의 Galaxy Gear S3와 애플의 Apple Watch 5, Garmin Vivosport를 분석하였고, 포렌식 모델을 제안한다. 논리적 추출을 목적으로 PC와의 연결을 통한 포렌식 방법, 물리적

추출을 위하여 PCB(Printed Circuit Board) Service Port, PCB Debugging Port, Chip Off 등의 방식을 통한 포렌식 방법을 사용하여, 제조사별로 기기에서 추출 및 분석할 수 있었던 정보들을 정리하였다. 특히 기기 정보와 건강 관리 정보 분석에 초점을 맞추었다.

앞선 선행연구들은 사용자의 손목이라는, 사용자와 가장 가깝게 위치하는 스마트 기기인 스마트워치에 저장되는 정보를 분석하고 이를 통해 범죄 혐의를 입증하는 방법을 제시하였다. 실제로 국제적으로 스마트워치에 저장된 정보가 살인 혐의 입증에 사용된 사례가 발생하고 있다. 2021년 그리스에서 발생한 신부 살해 사건의 경우, 피해자의 배우자는 피해자가 강도에 의해 강도살인 당한 것이라고 증언하였으나, 피해자의 스마트워치 분석 결과 남편의 증언 시각 이후에도 피해자의 심박이 유지되고 있었다는 사실이 드러나, 배우자의 위증이 입증되었다[8]. 2022년 영국의 경우 경찰관의 스마트워치에 측정된 급격한 심장박동 증가에 대한 정보가 경찰관이 범죄자를 식별한 시기를 입증하는 증거로 활용되었다[9].

이러한 사례들은 선행연구의 기여를 입증하며, 스마트워치가 스마트폰과 같이 포렌식적으로 유의미한 정보를 가진 기기라는 것을 분명히 한다. 그러나 선행연구들의 주요 분석 대상이었던 구글의 Android Wear는 현재 Wear OS로 대체되었으며, 갤럭시 기어 S3의 운영체제인 Tizen OS는 삼성이 Galaxy Watch 4와 5의 운영체제를 Wear OS Powered by SAMSUNG으로 채택하면서 시장점유율이 급감하게 되었다. 애플의 애플 워치의 경우 7세대부터 PC 연결 포트가 삭제되면서 스마트워치와 PC의 유선 연결을 통한 논리적 분석이 불가능하게 되었다.

이에 본 연구는 최신 웨어러블 운영체제인 Wear OS Powered by SAMSUNG을 중심으로 분석을 진행하였으며, 기존 연구에서는 범죄 상황에서 가·피해자가 우연히 스마트워치를 착용했을 경우를 주로 가정하였으나, 본 연구에서는 스마트워치가 범행 도구로 직접 활용되는 시나리오를 제시하고 분석하여, 범행 도구로써 스마트워치의 잠재적인 위험성을 강조한다.

III. Wear OS 특징과 제원

Wear OS Powered by SAMSUNG은 삼성과 Google이 협업하여 제작한 스마트워치 OS로 2021년 출시한 Galaxy Watch 4, Galaxy Watch 4 Classic, 2022년에 출시한 Galaxy Watch 5, Galaxy Watch 5 Pro의 운영체제다. One UI Watch를 적용하여 이전 Galaxy Watch 3와 유사한 인터페이스를 가지며, Tizen OS와 Wear OS의 장점을 결합하여 제작되었기 때문에 Wear OS Powered by SAMSUNG은 ADB를 사용할 수 있다.

Table 1은 연구에 사용한 Wear OS Powered by SAMSUNG 운영체제를 사용하는 스마트워치를 대상으로 소프트웨어 정보와 ABI(Applicaion Binary Interface) 버전을 정리한 것이다. 안드로이드 스마트폰에는 “안드로이드 버전”으로 나타나 있는 부분이 스마트워치에서는 “시스템 버전”으로 표기되어 있어 스마트워치의 시스템이 곧 안드로이드를 나타내는 것인지에 대한 확인이 필요하였다. 이를 ‘getprop ro.build.version.release’ ADB 명령어를 통해 스마트워치의 “시스템 버전”이 “안드로이드 버전”을 나타냄을 확인하였고, Wear OS Powered by SAMSUNG을 사용하는 스마트워치는 현재 Android 11 기반으로 동작한다는 것을 확인하였다. 이와 더불어 ‘getprop ro.product.cpu.abi’ ADB 명령어를 통해 각각의 스마트워치들이 모두 armeabi-v7a를 사용하는 것을 확인할 수 있었다. 이는 Galaxy Watch 4, 5 시리즈가 ARMv7 기반 32비트 아키텍처를 사용한다는 것을 의미한다.

Table 1. Device information used in the study

Product Name	Model Number	System Version (Android Version)	Wear OS Version	CPU ABI
Galaxy Watch 5 Pro	SM-R920	11	3.5	armeabi-v7a
Galaxy Watch 5	SM-R915	11	3.5	armeabi-v7a
Galaxy Watch 4	SM-R860	11	3.5	armeabi-v7a

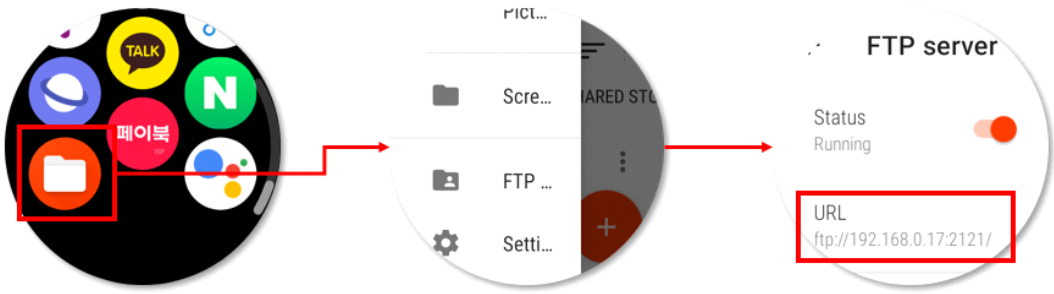

Fig. 1. A file explorer application for smart watch that supports FTP

IV. 범행 도구로의 스마트워치

스마트폰의 경우, 범죄 악용 가능성이 일찍이 예견되면서, 기업들은 보안 스티커 부착과 같은 가벼운 수준의 보안 절차에서 반입 금지와 같은 원천 예방 수준의 보안 절차를 두었고, MDM(Mobile Device Management)과 같은 기술적 방법을 통해 기업 내 보안을 유지하고 있다. 그러나, 이러한 스마트폰에 비해 스마트워치는 악용 가능성이 상대적으로 저평가되고 있어, 스마트워치와 관련된 보안 규정은 스마트폰에 비교하여 견고하지 않은 상태이다. 이러한 상황을 반영하여 본 장에서는 스마트폰에 대한 보안 규정으로 인해 스마트폰을 정보유출의 도구로 사용할 수 없지만, 스마트워치에 대한 보안 규정은 없어, 스마트폰의 역할을 스마트워치로 대체한 내부자 범행이 가능하다는 것을 설명한다.

4.1 스마트워치 전용 상용 애플리케이션을 이용한 정보유출

일반적으로 Wear OS Powered by SAMSUNG 스마트워치에는 구글플레이에서 Watch 항목을 선택하여, 스마트워치 전용으로 제작된 애플리케이션을 설치한다. 일정 관리, 건강 관리와 같이 스마트워치의 일반적인 용도를 위하여 제작된 애플리케이션이 대다수이지만 스마트워치 내부 저장소 탐색기 애플리케이션 중 FTP 기능을 제공하는 애플리케이션을 확인하였다. File Explorer FTP Server(com.corproxy.files)는 구글플레이에서 찾을 수 있는 스마트워치 전용 상용 애플리케이션으로 스마트워치 내 파일 탐색기 기능을 제공한다. 문제는 해당 애플리케이션은 FTP 서버 기능을 제공하는데, 이 기능은 외부 단자가 없어 PC와의 유선 연결이 불가능한 스마트워치를 Wi-Fi 망을 통해 PC와 무선 연결하여 파일 송수신을 가능하게 한다는 것이다. Fig. 1은 File Explorer FTP Server를 사용하여 스마트워치 내 FTP 서버를 활성화하는 모습을 보여준다. FileZilla, XFTP 7과 같은 PC 응용프로그램을 사용해서 스마트워치의 FTP 서버에 연결할 수 있으며, 혹은 탐색기 주소 표시줄에 FTP 서버 주소와 포트 번호를 입력하는 것으로도 PC와 스마트워치를 연결할 수 있다.

이러한 File Explorer FTP Server와 같은 스마트워치 전용 상용 애플리케이션의 경우 구글플레이를 통해 설치할 수 있다. 이는 사용자가 ADB를 PC에 설치하지 않아도 스마트폰에 애플리케이션을 설치하는 익숙한 방법으로 스마트워치에 FTP 기능을 제공하는 애플리케이션을 설치할 수 있다는 것을 의미한다. 따라서 상용 애플리케이션을 이용한 정보유출은 ADB를 경험한 적이 없는 안드로이드 비전문가도 간편하게 정보유출 수단을 스마트워치에 설치하고 PC 내 정보를 스마트워치로 이동시킬 수 있다는 점에서 위협적이다.

4.2 스마트폰 전용 애플리케이션 설치를 통한 정보유출

File Explorer FTP Server를 통한 파일 탈취는 상용 애플리케이션을 사용한다는 점에서 누구나 쉽게 접근 가능하다는 장점이 있지만, 결정적으로 FTP 프로토콜을 사용하기 때문에, 암호화 통신을 사용할 수 없어 파일 이동이 식별될 수 있다는 단점을 갖는다. 이와 더불어 스마트워치 애플리케이션 시장은 현재 건강 관리와 일정 관리 애플리케이션에 주된 초점이 맞추어져 있기에, 정보유출에 사용할 수

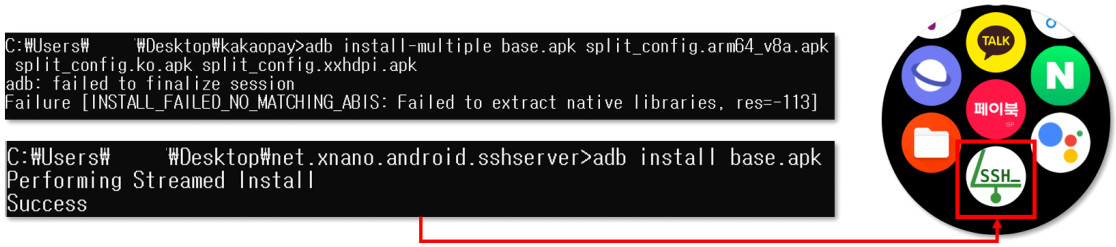

Fig. 2. Results of attempting to install 64-bit and 32-bit applications using the adb install command

있는 애플리케이션을 찾기 어렵다는 단점도 존재한다. 무엇보다, 구글플레이를 통한 애플리케이션 설치 시, 설치 기록이 계정에 남게 되어 증거 인멸의 어려움이 따른다는 한계점도 있다.

그러나 이러한 한계는 스마트워치 애플리케이션을 벗어났을 때 제거된다. 앞서 Wear OS Powered by SAMSUNG은 Android 11 기반이라는 것을 확인하였다. 이는 곧, ADB를 사용할 수 있다는 것을 의미하며, 애플리케이션 설치를 위해 구글플레이에 의존하지 않고, 'ADB Install' 명령어를 통해 APK 파일을 설치할 수 있다는 것을 나타낸다. 본 연구에서는 스마트워치 전용으로 개발되지 않은 APK 파일도 'ADB Install' 명령어를 통해 스마트워치에 설치할 수 있는지 확인하였다.

Fig. 2는 스마트폰용으로 제작된 64비트 애플리케이션 카카오페이(com.kakaopay.app)의 APK 파일과 32비트 애플리케이션인 SSH Server(net.xnano.android.sshserver)의 APK 파일을 Galaxy Watch 5를 대상으로 'ADB Install' 명령어를 사용한 결과이다. Galaxy Watch 4, 5 시리즈가 모두 ARMv7 기반 32비트 아키텍처를 사용하기 때문에, 64비트 APK 파일은 abi 매칭 오류가 발생하여 설치되지 않았지만, 32비트 APK 파일은 스마트워치로 문제없이 설치되는 것을 확인할 수 있었다

하지만 스마트폰용 APK 파일을 스마트워치에 설치했을 때, 스마트폰 화면에서는 발생하지 않았던 문제점들이 스마트워치 화면에서는 발생한다. 스마트워치에 비해 화면 크기가 크고 직사각형인 스마트폰의 화면을 가정하고 애플리케이션이 제작되었기 때문에, Fig. 3의 좌측 화면과 같이 스마트워치에 설치된 스마트폰용 애플리케이션은 버튼과 같은 화면 구성요소들이 중첩되어 보인다. 스마트폰용 애플리케이션은 대게 직사각형을 상정하고 제작되는 반면, 삼성 스마트워치는 원형 화면을 갖는다. 따라서 스마트폰 전용으로 개발된 애플리케이션이 스마트워치에 설치되었을 때 Fig. 3 중앙의 스마트워치 화면과 같이 애플리케이션의 직사각형 화면의 꼭짓점에 있는 구성요소들이 Fig. 3 우측의 화면과 달리 스마트워치의 화면을 벗어나, 보이지 않는 경우가 있다. 그러나 이러한 문제점들로 인하여 스마트워치에서 스마트폰용 애플리케이션을 사용할 수 없는 것은 아니다.

Fig. 2에서 스마트워치에 설치한 SSH Server(net.xnano.android.sshserver)는 안드로이드 스마트폰에서 SSH(Secure Shell) 서버를 열어 SFTP 프로토콜을 사용할 수 있도록 기능하는, 스마트폰을 상정하고 개발된 애플리케이션이다. Fig. 4의 좌측 사진은 이러한 SSH Server가 스마트워치에서 실행되는 것을 보여준다. 비록 화면 구성요소들이 중첩되는 문제점이 발생하지만, 이는 해당 애플리케이션의 설정을 조작함으로써 극복할 수 있다. 이후 PC의 명령 프롬프트에서 SFTP 명령어를 입력하면 SSH Server 애플리케이션을 통해 스마트워치 내부에 활성화한 SSH server를 PC와 연결할 수 있다. Fig. 4의 우측 명령 프롬프트 화면은 'sftp -P [SSH 서버 포트 번호] [사용자 이름]@[스마트워치 IP]' 명령을 실행하여 PC에서 스마트워치의 SSH 셸에 접근하고 'put' 명령을 사용하여 PC에서 스마트워치로 데이터를 쉽게 전송해 정보를 유출할 수 있다는 것을 보여준다.

Fig. 3. Problems on the smart watch screen

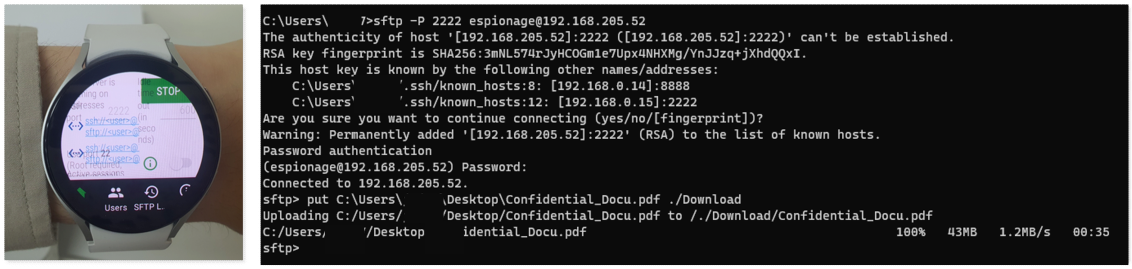

Fig. 4. SSH connection and file transfer between smart watch and PC

4.3 소형카메라 통제 기기로의 스마트워치

Galaxy Watch 4, 5에는 카메라가 탑재되어 있지 않다. 그러나 스마트워치에 스마트폰용 소형카메라 애플리케이션을 설치하면, 스마트워치의 Wi-Fi 기능을 이용하여 소형카메라와 스마트워치를 연결할 수 있다. Lookcam(com.view.ppcs)은 이러한 가정을 입증할 수 있는 스마트폰용 소형카메라 연결 애플리케이션이다. 최근 소형카메라는 Wi-Fi를 발신하여 통제 기기와 무선 연결한다. Fig. 5는 사무실 내 티슈 곽으로 위장하여 은밀하게 반입된 소형카메라와 스마트워치와의 연결을 통해 정보를 유출하는 시나리오를 보여준다. 특정 기업들의 경우 직원들의 퇴근 시 반출 물품에 대해서만 보안 검사를 진행하고 출근 시 반입 물품에 대해서는 보안 검사를 진행하지 않는 경우가 있다. 이러한 보안 절차를 이용하여 유출자는 소형카메라를 반입시킨 후, 소형카메라에서 발신하는 Wi-Fi를 스마트워치와 연결하여, 소형카메라를 원격 통제할 수 있다. 따라서 유출자는 스마트폰이 없는 상황에서도 주기적으로 소형카메라와 스마트워치를 연결하여 영상을 스트리밍하거나 다운로드하여 정보를 수신할 수 있다. 이러한 방식으로 충분한 정보를 촬영했다면, 유출자는 기업 내부에서 소형카메라를 분해, 폐기하여 퇴근 시 진행하는 반출 물품 검사에서도 걸리지 않고 정보를 스마트워치에 담아 외부로 유출할 수 있다.

이렇게 파악한 스마트워치를 통한 정보유출 방법은 스마트워치와 관련된 보안 절차가 개선되어야 한

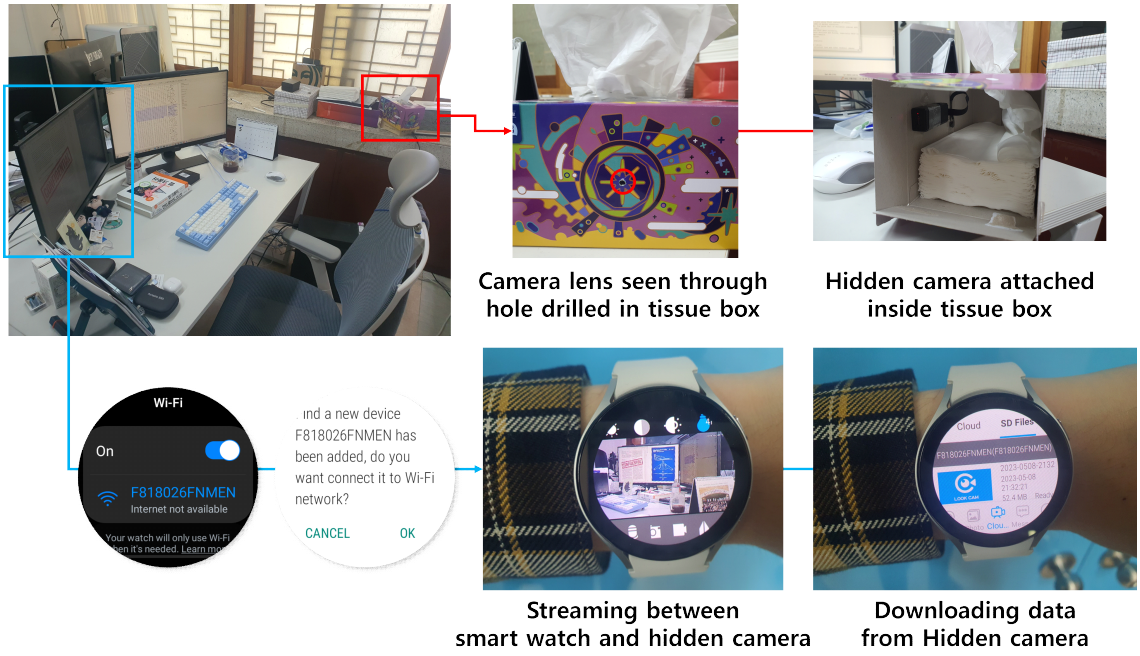

Fig. 5. Environment when connecting a hidden camera to a smart watch

다는 점을 강조한다. 또한, 스마트워치의 반입을 허용한다면, 오용 방지를 위하여 스마트워치 내 애플리케이션의 설치 및 사용을 규제하고 모니터링할 수 있어야 한다는 것을 나타낸다.

V. 포렌식 방법

5.1 스마트워치 포렌식과 스마트폰 포렌식의 차이점

Wear OS Powered by SAMSUNG 운영체제를 사용하는 Galaxy Watch 4, 5는 안드로이드 스마트폰과 비교했을 때 2가지 차이점으로 인해 기존 모바일 포렌식 연구 및 조사 방법을 사용하기 어렵다. 첫 번째는 USB 단자의 부재이다. 최신 스마트워치는 충전 시 무선 충전을 주로 이용하기 때문에, USB 단자가 생략되어있는 경우가 많다. 따라서, USB 단자를 이용해 PC와 유선 연결한 후 MD-NEXT와 같은 모바일 데이터 획득 도구를 통해 기기 내 데이터를 이미징하고 분석 도구를 통해 분석하는 기존의 스마트폰 포렌식의 방법을 사용할 수 없다. 이와 더불어 USB 단자의 부재는 접근 가능한 경로에서도 차이점을 만든다. 안드로이드 11 이후로 /storage/emulated/0/Android/data 경로는 기기의 기본 탐색기로는 접근할 수 없고, PC와 유선 연결 시에만 접근할 수 있도록 변경이 이루어졌다. 따라서 무선연결만이 가능한, 앞서 안드로이드 11 기반임을 밝혔던, Wear OS Powered by SAMSUNG 운영체제를 사용하는 스마트워치의 경우 Fig. 6과 같이 해당 경로에 대한 접근이 불가능하여 분석 가능한 경로에서 안드로이드 스마트폰과 차이를 갖는다.

이어서 두 번째 차이점은 공개된 펌웨어의 부재이다. /data/data 경로의 애플리케이션 패키지 데이터는 안드로이드 스마트폰 포렌식에서의 주요 분석 대상이다. 해당 경로에 접근하기 위해선 SU(Super User) 권한이 필요하다. 안드로이드 스마트폰 수사 시에는 Full File System 이미징을 통해 SU 권한 없이도, 포렌식 프로그램을 통해 해당 경로의 데이터를 확인하는 방법을 사용할 수 있지만, 앞서 설명한 바와 같이 스마트워치의 경우 해당 방법을 사용할 수 없다. 한편, 연구 시에는 안드로이드 기기를 미리 루팅한 상태에서 실험을 진행하고 ADB Shell에서 SU 권한을 통해 /data/data 경로의 데이터에 접근하는데, Wear OS Powered by SAMSUNG 운영체제를 사용하는 Galaxy Watch 4, 5는 펌웨어가 공개되어 있지 않아 현재 루팅이 어렵다. 따라서, 안드로이드 스마트폰과 달리 /data/data 경로에 접근할 수 없는 상황이기에 애플리케이션 패키지 데이터를 분석할 수 없다는 차이점으로 이어진다.

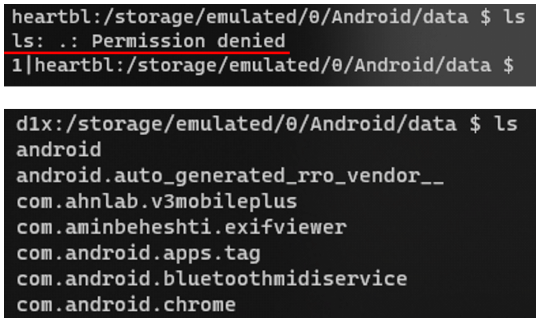

Fig. 6. Galaxy Watch 5(top) / Galaxy Note 10 (bottom)

이러한 차이점을 반영하여 스마트워치를 분석하는 방법은 ADB를 이용한 안드로이드 라이브 포렌식 방법이다. 앞서 스마트폰용 APK 파일을 스마트워치에 설치했던 것과 같이 ADB의 무선 디버깅 기능을 이용하면 수사관의 PC와 분석 대상인 스마트워치를 연결할 수 있다. 비록 SU 권한을 획득할 수는 없지만, 허용하는 권한 내에서 안드로이드 스마트워치에 존재하는 파일들을 PC로 옮기는 것이 가능하다. 무엇보다 dumpsys 로그와 같이 개발자들을 위하여 제공되는, ADB의 각종 로그를 활용한 사용자 행위 분석이 가능하다.

5.2 dumpsys 명령어를 통한 안드로이드 로그 분석

5.2.1 dumpsys usagestats

많은 선행연구에서 안드로이드 로그인 dumpsys를 포렌식 방법으로 사용할 수 있음을 설명한다[10, 11, 12]. 이는 Galaxy Watch 4, 5에도 적용할 수 있다. 안드로이드 11기기는 /data/system_ce/usagestats/0 경로에 usagestats를 저장하며 해당 아티팩트 분석 시 사용자의 앱 사용 기록을 확인할 수 있다[13, 14]. 선행 연구는 스마트폰의 해당 경로에 저장된 usagestats 파일을 추출하고 분석하는 방식으로 연구를 진행하였다. 하지만 /data/system_ce/usagestats/0 경로에 접근

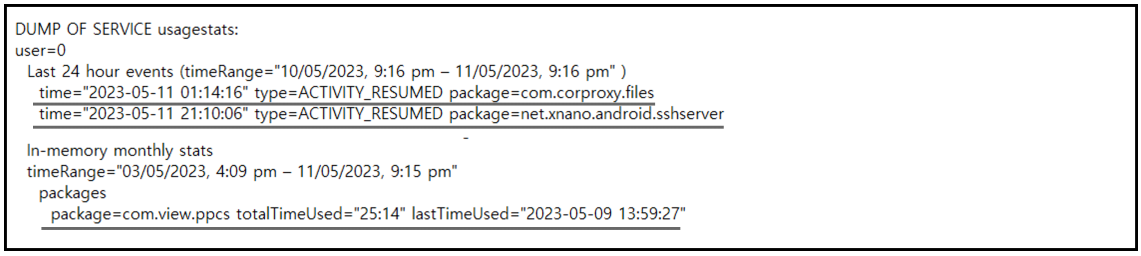

Fig. 7. dumpsys usagestats

하여 usagestats 파일을 추출하기 위해서는 SU 권한이 필요하다. 따라서 스마트워치에 바로 적용할 수는 없지만, 이는 무선 디버깅으로 연결한 ADB에서 dumpsys usagestats 명령어를 사용하는 것으로 대체할 수 있다.

Fig. 7은 dumpsys usagestats 명령어를 사용하여 얻은 usagestats 로그의 일부를 나타낸다. usagestats 로그는 "Last 24 hour events", "In-memory weekly stats", "In-memory monthly stats", "In-memory yearly stats" 항목으로 명령어 실행 시간 기준 24시간, 한 주, 한 달, 일 년의 데이터를 저장한다. 명령어 실행 시각 24시간 전까지 로그에서는 몇 시 몇 초에 어떤 앱의 액티비티가 스마트워치의 화면에 활성화되고 비가시화되었는지, 어떤 앱의 notification이 발생하였는지를 FOREGROUND_SERVICE_START, ACTIVITY_RESUMED, NOTIFICATION_INTERRUPTION 등의 이벤트 정보를 통해 알 수 있다[15]. 1주일, 1달, 1년 동안의 앱 동작 정보 역시 확인할 수 있으나, 24시간 usagestats와는 다르게 시, 분, 초 단위의 정보를 확인할 수는 없고, 가장 마지막에 사용된 일자와 시각, 사용된 횟수 등의 정보를 확인할 수 있다.

5.2.2 dumpsys netstats

dumpsys netstats 명령어를 통해선 스마트워치가 접속한 Wi-Fi 망 정보를 알 수 있다. Fig. 8은 명령어를 통해 출력된 로그의 일부를 보여준다. 'networkId' 항목은 연결된 Wi-Fi 망의 SSID (Service Set Identifier)를, 'st' 항목은 연결된 시각을, 'rb'와 'rp'는 수신한 데이터의 크기와 패킷 수를, 'tb'와 'tp'는 송신한 데이터의 크기와 패킷 수를 나타낸다. 이 때 주의할 점은 'st' 항목의 경우 1시간 단위로 기록된다는 것이다. 따라서 예를 들면, 특정 Wi-Fi망에 2023년 5월 10일 20시 40분에서 50분까지, 단 10분만 연결되었어도, 'st'값은 1683716400(2023년 5월 10일 20시)으로 표시된다.

5.2.3 dumpsys network_stack

Fig. 9 및 Fig. 10은 dumpsys network_stack

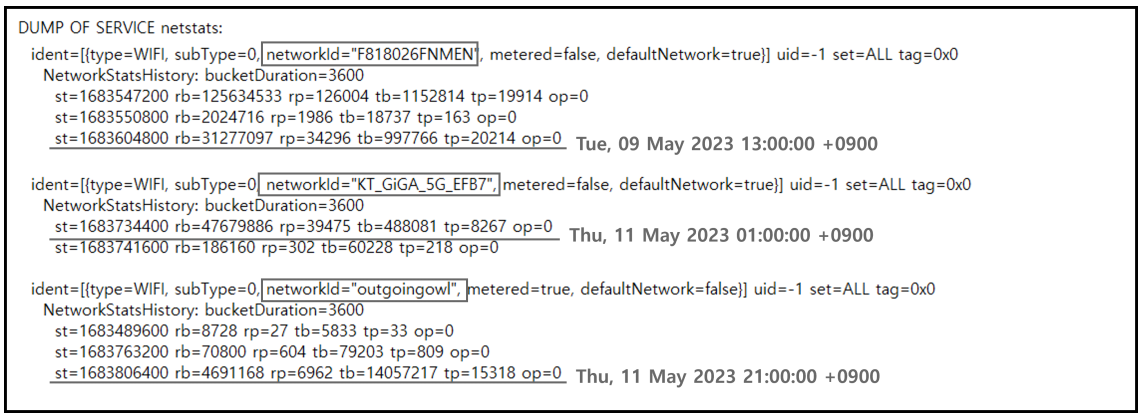

Fig. 8. dumpsys netstats

Fig. 9. dumpsys network_stack 1

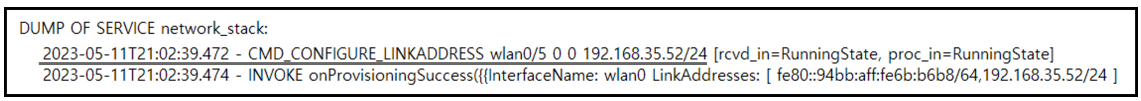

Fig. 10. dumpsys network_stack 2

명령어로 출력된 로그를 나타낸다. 해당 로그에서는 네트워크 인터페이스, 네트워크 토폴로지 및 네트워크 스택에 대한 정보를 제공하고 DHCP(Dynamic Host Configuration Protocol) 프로토콜을 통해 Wi-Fi 망과 연결된 정보를 확인할 수 있어 시간별로 기록된 스마트워치의 사설 IP 주소를 확인할 수 있다. 그러나 스마트워치 재부팅 시 기존 기록이 사라지고 새롭게 기록되어 재부팅 이전 기록을 확인할 수 없다는 한계를 갖는다.

5.3 케이스 스터디

앞서 4장에서 제시하고 실증한 FTP, SFTP 프로토콜, 소형카메라 연결을 통한 정보유출 시나리오를 ADB 명령어를 통해 확보한 dumpsys usagestats, netstats, network_stack 정보를 종합하여 사용자 행위를 분석한다.

5.3.1 스마트워치, PC 간 FTP 이용 정보유출

먼저, Fig. 7에 있는 usagestats 로그를 확인하였을 때, 2023년 5월 11일 01시 14분 16초 경, 스마트워치 사용자가 File Explorer FTP Server(com.corproxy.files)를 실행한 것을 확인할 수 있다. 이후, Fig. 8의 netstats 로그에서는, File Explorer FTP Server가 활성화된 시각에 스마트워치가 SSID가 KT_GiGA_5G_EFB7인 Wi-fi 망에 연결되었고, 약 47MB 상당의 데이터가 스마트워치로 전송되었다는 것을 확인할 수 있었다.

다음으로 Fig. 9의 network_stack 1 로그에서는 KT_GiGA_5G_EFB7에 연결되었을 때, 스마트워치가 부여받은 사설 IP가 172.30.1.76이라는 것을 보여준다. 이렇게 ADB를 통해 스마트워치에서 추출한 로그 정보는, PC에서 얻은 정보와 결합하였을 때, 사용자가 스마트워치와 PC 간 FTP 연결을 시도하였다는 것을 알 수 있다. 예를 들어, 만약 사용자가 전형적인 FTP, SFTP 연결 PC 응용프로그램인 FileZilla를 사용하여 무선연결하였을 경우, %UserProfile%\AppData\Roaming\FileZilla 경로의 filezilla.xml, recentservers,xml 파일로부터 연결된 사설 IP 정보를 교차 검증할 수 있으며, FTP 사용자 명, 비밀번호 등의 정보를 추가적으로 확보할 수 있다.

5.3.2 스마트워치, PC 간 SFTP 이용 정보유출

Fig. 7의 usagestats 로그에 의하면, 2023년 5월 11일 21시 10분 06초경 사용자가 SSH Server(net.xnano.android.sshserver) 애플리케이션을 활성화하였다는 것을 확인할 수 있다. 이어서 Fig. 8의 netstats 로그를 확인하였을 때, 해당 시각 스마트워치와 연결된 Wi-Fi 망의 SSID가 “outgoingowl”이라는 것을 알 수 있다. 이와 더불어 Fig. 10의 network_stack 2 로그는 스마트워치가 outgoingowl Wi-Fi로부터 할당받은 사설 IP가 192.168.35.52라는 것을 보여준다. SFTP 연결

역시 FTP 연결과 유사하게, PC 포렌식을 통해 얻은 정보와 결합하면, 사용자의 스마트워치, PC 간 연결 행위를 더욱 구체적으로 입증할 수 있다. 예를 들어 만약 사용자가 PC의 터미널을 통해 sftp.exe 사용했을 경우, 수사관은 스마트워치 로그 데이터를 통해 확보한 SSID와 사설 IP 정보를 Windows PC의 %UserProfile%\.ssh\known_hosts 파일에서 확인하여 교차 검증할 수 있다.

5.3.3 스마트워치, 소형카메라 연결을 통한 정보유출

Fig. 7의 usagestats 로그를 통해 사용자는 2023년 5월 9일 13시 59분경 Lookcam (com.view.ppcs) 애플리케이션을 활성화하였다는 것을 알 수 있다. Fig. 8의 netstats에 의하면, 해당 앱이 활성화된 시간 동안 연결되었던 Wi-Fi 망의 SSID는 F818026FNMEN이었다는 것을 식별할 수 있으며, 총 31MB에 해당하는 데이터를 전송받았다는 것을 알 수 있다. 이와 더불어 st=1683547200을 통해 2023년 5월 8일 21시에도 연결되어 약 125MB에 상당하는 데이터를 전송받은 것을 확인할 수 있다. usagestats에서 5월 8일 21시경에 소형카메라 통제 애플리케이션의 활성화 로그를 확인할 수 없었던 까닭은 5.2.1. dumpsys usagestats에서 설명하였던 바와 같이, Lookcam(com.view.ppcs) 애플리케이션을 사용한 지 24시간이 지나, 가장 마지막에 사용된 시간 정보만이 usagestats 로그에 남았기 때문이다.

VI. 토 의

6.1 한계

비록 dumpsys 명령어를 통한 안드로이드 로그 분석을 통해 스마트워치에 기록되는 ADB 로그 정보로 사용자 행위를 입증할 수 있음을 이야기하였지만, 이러한 방법엔 분명한 한계가 존재한다. 먼저 ADB 로그의 경우 유지 기간이 짧다는 것이 포렌식 분석에서 큰 제약으로 작용한다. usagstats 로그에서 확인할 수 있다시피, 사용자의 범행 후 24시간이 경과하면, 애플리케이션이 가장 마지막에 사용된 시각과 총 사용 횟수만을 알 수 있다는 한계가 있었다. 이러한 한계점은 범행이 수차례에 걸쳐 이루어졌을 경우, 각각의 범행의 정확한 시기를 알기 어렵다는 문제로 이어진다. 이와 더불어 network_stack 로그의 경우, 스마트워치가 재부팅되었을 경우 사라진다는 휘발성을 갖고 있다. 이러한 단점은, 스마트워치 기기 자체가 적은 배터리 용량을 갖고 있어 방전되기 쉽다는 점과 결합하여 더 큰 문제점으로 작용한다.

모호함은 ADB 로그 분석이 갖는 또 하나의 한계점이다. netstats 로그의 경우 한 시간 단위로 연결된 Wi-Fi 망의 SSID와 송수신한 데이터 크기를 저장한다. 이러한 로깅 방식은 수사의 관점에서 문제로 작용한다. 만약 스마트워치가 Fig. 11과 같이 1시간 안에 여러 Wi-Fi 망과 연결되었을 경우, 해당 Wi-Fi 망에 연결된 정확한 시간을 알기 어려우며, network_stack 로그와 결합했을 때 알 수 있었던 사설 IP를 정확히 어떤 SSID를 가진 Wi-Fi 망이 부여한 것인지 알기 어려워지기 때문이다.

이와 더불어 ADB 로그를 통해 스마트워치와 PC가 연결된 적이 있다는 것을 충분히 입증할 수 있으나, 사용자가 범행 후 스마트워치로 송신한 데이터를 삭제하였을 경우, 정확히 어떤 데이터를 PC에서 스마트워치로 송신하였는지 알기 어렵다는 문제점이 존재한다.

```
ident=[{type=WIFI, subType=0, networkId="C3DF", metered=false, defaultNetwork=false}] uid=-1 set=ALL tag=0x0
  NetworkStatsHistory: bucketDuration=3600
    st=1683547200 rb=47610236 rp=37996 tb=335982 tp=7753 op=0
    st=1683550800 rb=6844 rp=44 tb=8535 tp=47 op=0
    st=1683590400 rb=16134 rp=59 tb=19909 tp=77 op=0

ident=[{type=WIFI, subType=0, networkId="F818026FNMEN", metered=false, defaultNetwork=false}] uid=-1 set=ALL tag=0x0
  NetworkStatsHistory: bucketDuration=3600
    st=1683547200 rb=80 rp=2 tb=136 tp=2 op=0
    st=1683604800 rb=80 rp=2 tb=120 tp=2 op=0
```

Fig. 11. Two networkId with the same st value

6.2 예방 방안

기술 및 경영정보는 유출되었을 경우, 유출된 정보를 추적하고 차단하는 것이 어렵다. 따라서 원천적인 예방이 중요하다. 먼저 회사 기술 보호 규정에 스마트워치 사용에 대한 업데이트가 필요하다. 규모가 큰 기업의 경우 자체적으로 보안스티커와 MDM을 활용하여 모바일 기기에 의한 유출 취약점을 방어하고, 회사 내 Wi-Fi 차단 솔루션, 화이트리스트 방식 네트워크 접근통제 솔루션을 이용하여 기술적으로 기술 및 경영정보 유출 범죄를 방어하고 있다. 그러나 스마트워치의 보급률과 유출 도구로서의 성능에 비하여 스마트워치 관련 보안 규제는 부족하다. 스마트워치 비인가 구역과 상황을 규정해야 하며, 사내 보안팀이 있다면 이를 정기적으로 감사하여야 한다.

기술 보호 규정 재정 및 업데이트는 보안 측면에서 당연히 유지해야 하는 것이기 때문에 형식적인 해결방안으로 여겨질 수 있으나, 해외 기업 통계와 우리나라 정부 통계 보고서를 확인하였을 때 이는 형식적이지 않고 반드시 필요한 방안이라는 것을 알 수 있다. INFOWATCH의 보고서에 의하면 국제적으로 기술 및 경영정보 유출 유형의 64.5%를 내부자에 의한 유출이 차지한다[16]. 우리나라 중소벤처기업부의 2022 중소기업 기술보호 수준 실태조사 보고서에 의하면 우리나라의 기술 침해 유형의 68.4%는 내부직원에 의한 유출로 발생하였으며, 21.1%는 제3자(외주업체, 외주용역, 협력업체 등)에 의하여 발생하였다는 것을 확인할 수 있다[17]. 동 보고서에 의하면 우리나라의 중소기업 중 기술 보호 규정이 없는 기업이 45.0%를 차지하며 중견 기업의 경우 14.2%인 상황이다. 따라서 스마트워치를 포함한 기술 보호 규정 재정 및 업데이트는 기업 내 직원들에게 유출 관련 경각심을 고취하여 특히 중소 및 중견 기업에서의 기술 및 경영 정보유출 범죄 예방에 도움이 될 수 있다.

상대적으로 기술적인 보안 조치가 우수한 대기업의 경우 스마트워치용 MDM을 제작하는 것을 예방 방안으로 제시할 수 있다. 앞선 case study에서 분석했던 사례들은 공통적으로 Wi-Fi 망을 이용한 방법이었고, 스마트워치에 통상 설치되지 않는 스마트폰용 애플리케이션을 설치하는 방법 또한 사용하는 것을 확인하였다.

Fig. 12의 AndroidManifest.xml 파일의 〈uses-feature android:name="android.hardware.type.watch"〉 항목은 스마트워치용으로 제작된 애플리케이션에서 찾을 수 있는 정보이다. 따라서 스마트워치에 설치된 애플리케이션 중의 AndroidManifest.xml 파일에서 해당 항목이 없는 것은 스마트폰용 애플리케이션이 스마트워치에 설치된 경우일 가능성이 존재한다. 이러한 특성들을 이용하여 회사 내 진입 시 스마트워치의 Wi-Fi를 제한하는 기능, 스마트워치용으로 개발되지 않은 애플리케이션의 설치를 차단하는 기능, 스마트워치 내 마이크 권한을 회수하는 기능 등을 포함하는 MDM이 제작된다면 스마트워치를 이용한 기술 및 경영정보 유출 범죄에 선제적으로 대응할 수 있다.

Fig. 12. AndroidManifest.xml of applications for smart watch

VII. 결 론

대중에 점점 보편화되면서, 스마트워치는 사용자의 손목 위에서 동작하는 초소형 컴퓨터로 기능한다. 본 연구는 이러한 스마트워치의 특징을 이용하면, 특히 안드로이드 기반의 Wear OS 운영체제의 개발자 편의성을 이용하면 스마트워치를 통한 범죄를 저지를

수 있다는 우려에서 작성되었다. 이를 입증하기 위하여 Wear OS Powered by SAMSUNG 운영체제를 사용하는 Galaxy Watch 4, 5 시리즈를 통한 실험을 진행하였고, 현재 유통되고 있는 스마트워치 전용 애플리케이션, 스마트폰 전용 애플리케이션을 ADB 명령어를 통해 스마트워치에 설치하는 것으로, FTP, SFTP, 소형카메라 등을 이용하여 정보유출이 가능하다는 것을 제시하였다.

이후 ADB dumpsys 명령어를 통해 얻은 시스템 로그를 분석함으로써 스마트워치 활용 범죄의 조사 방안을 제시하였다. dumpsys usagestats 명령어는 명령어 실행 시각을 기준으로 24시간, 일주일, 한 달, 일 년 단위로 애플리케이션의 동작 관련 로그를 출력한다. 24시간 동안의 로그의 경우 각 애플리케이션이 여러 번 동작하여도 각 동작 시각이 언제인지 각각 파악할 수 있었지만, 24시간이 경과되었을 경우 제일 마지막에 실행된 시간과 총 실행 횟수만을 확인할 수 있었다. dumpsys netstats 명령어를 통해서는 스마트워치가 유지한 네트워크 관련 정보를 확인할 수 있었으며, 연결되었던 Wi-Fi 망의 연결 시각을 1시간 단위로 파악할 수 있었고 SSID와 송수신한 데이터의 크기를 파악할 수 있었다. dumpsys network_stack 명령어는 DHCP 통신 정보를 제공하여 스마트워치가 연결되었던 Wi-Fi 망으로부터 할당받은 사설 IP를 확인할 수 있었다.

한편 이렇게 제시한 3가지 로그를 통해서 스마트워치의 앱 사용에 대한 정보와 네트워크 통신 관련 정보를 확인할 수 있었으나, 이러한 ADB dumpsys 명령어를 통해 얻은 로그는 유지되는 시간이 짧고, 시간 정보가 1시간 단위로 기록되는 경우 또한 존재해, 짧은 수명과 모호함이라는 한계 또한 존재하였다. 이와 더불어 스마트폰과 달리 스마트워치에는 존재하지 않는 USB 단자와 스마트워치 펌웨어의 비공개로 인하여, 현재 스마트폰에 적용 가능한 포렌식 방법을 스마트워치에는 바로 적용할 수 없다는 문제점을 확인하였다.

비록 현재 정보유출 범죄에서 스마트워치를 범죄 수단으로 사용하는 경우는 많지 않지만, 스마트워치 기기의 성능 발전 속도와 안드로이드 특유의 애플리케이션 개발의 용이성을 고려한다면, 스마트워치는 기술유출 범죄의 수단으로 충분히 사용될 수 있을 것으로 추측된다. 현재 스마트워치는 보안 정책의 범위를 벗어나는 경우가 많다. 여전히 많은 기관에서 접근통제 시 스마트워치를 통제하지 않고 있으며, 기밀유출 범죄 발생 시 이메일, 클라우드, 모바일 저장매체 등이 수사 대상이 되지만 스마트워치를 고려하는 상황은 많지 않다. 따라서 현재 성능에 비해 저평가된 스마트워치의 보안 위협을 고려하여 선제적으로 보안 정책에 반영하려는 시도가 필요하다. 이와 더불어 명확한 혐의 입증을 위하여 스마트워치의 Full File System 분석을 위한 취약점 연구가 필요하며, 스마트워치의 데이터 확보가 용이하도록 모바일 데이터 획득 도구의 무선연결, 무선 디버깅 기능이 가능하도록 추가적인 개발이 필요하다.

References

[1] The Hankyoreh, "Estimated 26 trillion won in damages from technology leakage... Supreme Prosecutor's Office 'Principle of arresting participants'", https://www.hani.co.kr/arti/society/society_general/1089452.html, Apr. 2023.

[2] National Office of Investigation, "Interim results of 'Special Crimes Crackdown for Economic Security' were announced", https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20230612072734633, Jun. 2023.

[3] Hyunchul Park, Jinsang Park and Jungduk Kim, "A Study on Development of Internal Information Leak Symptom Detection Model by Using Internal Information Leak Scenario & Data Analytics", *Journal of The Korea Institute of information Security & Cryptology*, 30(5), pp. 957-966, Oct. 2020.

[4] Korean Gallup, "2012-2022 Smartphone Usage & Brand, Smartwatch, Wireless Earphone Survey", https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1405, Jul. 2022.

[5] Parag H Rughani and M Dahiya, "Analysis of android smart watch artifacts", International Journal of

Scientific & Engineering Research, vol. 6, no. 8, pp. 920-930, Aug. 2015

〔6〕 Nicole R Odom, Jesse M Lindmar, John Hirt and Josh Brunty, "Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices", Journal of forensic sciences, vol. 64, no. 6, pp.1673-1686, Jun. 2019.

〔7〕 Minju Kim, Yeonghun Shin, Wooyeon Jo and Taeshik Shon, "Security analysis of smart watch and band devices", Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence, pp. 655-658, Dec. 2021.

〔8〕 BBC, "Greece killing: Husband confesses to caroline crouch death", https://www.bbc.com/news/world-europe-57523469, Jun. 2021.

〔9〕 The Telegraph, "Julia james murder trial: Smartwatch captured pcso 'running for her life as she fled killer'", https://www.telegraph.co.uk/news/2022/05/09/julia-james-pcso-murder-trial-news-live-callum-wheeler-court/, May. 2022.

〔10〕 Lukas Bortnik and Arturs Lavrenovas, "Android dumpsys analysis to indicate driver distraction", Proceedings of the 2020 International Conference on Digital Forensics and Cyber Crime, pp. 139-163, Feb, 2021.

〔11〕 Fujia Cheng and Chengxiang Tan, "Sedalvik: A kernel-level android behavior forensic method", Proceedings of the 2018 International Conference on Security, Pattern Analysis, and Cyvernetics(SPAC), pp.499-503, Dec. 2018.

〔12〕 Chuck Easttom, "A methodology for smart tv forensics", Proceedings of the 2021 International Conference on Cyber Warfare and Security, pp.65, Feb. 2021.

〔13〕 Kang Yeji, Kim Donghyun, Lee Sunkyoung, Park Jungheum and Lee Sangjin, "Analysis on android usagestats for digital investigation", Journal of Digital Forensics, 15(4), pp.1-12, Dec. 2021.

〔14〕 Hongkyun Kwon, Sangjin Lee, Doowon Jeong, "User profiling via application usage pattern on digital devices for digital forensics", Expert Systems with Applications, 168, pp.114488, Apr, 2021.

〔15〕 Android Deveplopers, "Usage Events. Event", https://developer.android.com/reference/android/app/usage/UsageEvents.Event, Aug. 2023.

〔16〕 InfoWatch Analytics Center, "Study on Global Data Leaks in H1 2018", https://infowatch.com/report2018, Aug, 2020.

〔17〕 Republic of Korea Ministry of SMEs and Startups, "2022 sme technology protection level survey", https://www.ultari.go.kr/portal/piy/publishView.do, Jul. 2022.

〈저자소개〉

전 승 제 (Seungjae Jeon) 학생회원
2023년 2월: 동국대학교 경찰사법대학 경찰행정학부 졸업
2023년 3월~현재: 동국대학교 일반대학원 경찰행정학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호, 스마트폰 포렌식 등

정 재 현 (Jaehyun Chung) 학생회원
2023년 2월: 동국대학교 경찰사법대학 경찰행정학부 졸업
2023년 3월~현재: 동국대학교 일반대학원 경찰행정학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호, 가상현실, 사이버보안 등

정 두 원 (Doowon Jeong) 정회원
2019년 2월: 고려대학교 정보보호대학원 공학박사
2020년 9월~현재: 동국대학교 경찰사법대학 조교수
2022년 1월~현재: 동국대학교 융합안전학술원 사이버안전연구센터 센터장
〈관심분야〉 디지털 포렌식, 정보보호 등