Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.6, Dec. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.6.1483

스마트워치 데이터 분석 및 위험도 평가*

이 영 주,† 양 원 석, 권 태 경‡
연세대학교 정보보호연구실

Data Analysis and Risk Assessment of Smartwatch*

Youngjoo Lee,† Wonseok Yang, Teakyoung Kwon‡
Information Security Lab, Yonsei University

요 약

스마트워치는 사용자가 착용하는 소형 스마트 기기로 연결성, 기능성 및 유용성을 위해 호스트 기기인 스마트폰과 페어링 과정을 필요로 한다. 페어링 과정 이후에는 사용자의 의식 없이도 스마트워치와 스마트폰 기기 간의 데이터 업데이트 및 백업 과정이 가능하며 스마트폰의 다양한 데이터가 복제되어 스마트워치로 넘어온다. 본 연구는 플랫폼별 스마트워치에 대해 스마트폰으로부터 복제되어 넘어오는 데이터를 사용 시점별로 추출 및 관찰하여 분석한다. 또한 스마트워치 사용자를 대상으로 실시한 보안관련 인식에 대한 설문조사를 바탕으로 데이터 추출 실험 결과에 따른 보안 및 개인 정보보호관점에서의 데이터별 위험도 평가를 수행하고 대응방안을 고찰한다.

ABSTRACT

Wearable devices need a host device to be paired with because of connectivity, functionality and ease personalization. There should be frequent update and backup processes between the paired devices even without user's consciousness. Due to pairing process, user-specific data are copied from smartphone and transferred to paired smartwatch. We focus on what happens in smartwatch because of pairing process. We perform an experiment study by observing and extracting data from smartwatch under real world usage phases. With a survey of user awareness on smartwatch regarding security and privacy, moreover, we suggest risk assessment on smartwatch in five levels, particularly considering pairing process based on security and privacy.

Keywords: Wearable Device, Data Extraction, Risk Assessment

I. 서 론

스마트폰은 연결성, 컴퓨팅 및 정보 저장의 용도로 사용자에게 편의성을 제공하며 오늘날 많은 사람들은 새로운 종류의 스마트 기기를 스마트폰과 연결하여 사용한다. 스마트 모바일 기기 확대 및 이에 따른 모바일 데이터 트래픽 증가는 IoT(Internet of Things) 환경의 발전과 더불어 가속화되고 있다.

다양한 IoT 기기 중에서 웨어러블 기기는 키보드와 같은 일반적인 사용자 인터페이스가 없는 착용형 소형 전자기기로 사용자와 밀접하게 작동한다. 이러한 스마트 기기는 내장된 센서를 통해 데이터를 수집하거나 기능성 및 유용성을 향상시키기 위해 스마트폰과 같은 호스트 장치와의 연결을 바탕으로 작동하여 편의성을 극대화한다. 특히, 스마트워치의 경우 개인의 다양한 정보를 스마트폰으로부터 가져와서 이를 이용하기 위해 호스트 장치인 스마트폰과의 연결이 필요하다. 이는 추후 스마트워치 사용 시, 사용자

Received(06. 30. 2017), Accepted(07. 20. 2017)
* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 육성지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00304)
† 주저자, yj.lee91@yonsei.ac.kr
‡ 교신저자, teakyoung@yonsei.ac.kr(Corresponding author)

의 의식 없이 스마트폰의 데이터가 넘어오는 것을 가능하게 한다. 따라서 사용자는 스마트워치를 사용하기 전에 스마트워치와 호스트 장치인 스마트폰 사이의 초기 연결 과정인 기기 간 페어링(device pairing)을 수행해야한다. 기기 간 페어링은 스마트워치와 스마트폰 간의 데이터 업데이트 및 백업 과정을 가능하게하며 사용을 위해서는 반드시 허용을 해야 한다. 사용자의 의식과 무관하게 SMS 알림 및 건강 기록 등의 데이터 전송에 관한 통신이 이뤄진다. 페어링을 통한 데이터 복제 현상으로 연결된 호스트 장치의 데이터를 복제하여 스마트워치로 그 데이터가 전송된다.

본 연구에서는 스마트워치가 호스트 장치인 스마트폰과 페어링함으로써 발생하는 데이터 복제 현상을 실험을 통해 연구한다. Android wear, watchOS 및 Tizen의 각 플랫폼에서 작동하는 다양한 스마트워치에서의 데이터 추출 실험을 수행하며 스마트워치에 대한 사용자 인식을 바탕으로 추출한 데이터에 대한 위험도를 평가한다.

II. 스마트워치에서의 데이터 추출 및 분석

2.1 실험 환경

스마트워치에서의 데이터 추출 실험을 위해, Android wear, WatchOS 및 Tizen의 세 가지 플랫폼에서 작동하는 다섯 가지 스마트워치를 Table 1.과 같이 해당 스마트폰과 페어링한다. 데이터 추출 및 데이터 분석을 위해 PC (MS Windows 10, Intel Core i7 4770k, 24GB RAM, 512GB SSD)를 사용한다.

Table 1. Experiment setup

Wearable Device	Host Device
Sony SmartWatch3 (Android Wear 1.3)	LG Nexus 5X (Android 7.0)
LG G Watch (Android Wear 1.4)	
Samsung Galaxy Gear (Tizen 2.2.1.1)	Samsung Galaxy S3 (Android 4.3)
Samsung Galaxy Gear2 Neo (Tizen 2.2.1.2)	
Apple Watch (watchOS 3.1)	Apple iPhone 6S Plus (iOS 10.1.1)

2.2 실험 설계 및 방법

스마트폰에서 데이터를 복제하여 스마트워치로 넘어가는 현상을 관찰하기 위해 전체 과정을 사용시간 순서에 따라 Fig.1.과 같이 4단계(t0, t1, t2, t3) 시점으로 나누어 실험을 수행한다. t0은 사용 이전으로 스마트워치가 출고된 상태이며 t1, t2, t3 세 가지 단계는 실제 사용하는 상태로 실제 본 연구에서 데이터를 관찰하는 단계이다. 각 단계별 데이터 복제 현상과 더불어 각 시점별 데이터 복제 현상을 알리는 경고 메시지가 있는지 확인한다.

t1은 사용자가 스마트워치와 스마트폰을 초기 페어링하는 과정이다. 페어링 직후 데이터 복제 현상을 관찰하기 위해서는 네트워크 인터페이스을 중지하고 스마트 폰에서 스마트 워치를 분리하여 PC에 연결한다. t2는 실제 스마트워치를 사용하면서 나타나는 데이터 복제 현상을 관찰하기 위한 것으로, 추가 어플리케이션을 설치하지 않고 내장된 기본 어플리케이션 사용을 사용하는 과정이다. t3은 t2에 이어서 추가적인 어플리케이션 설치하여 사용함에 따라 나타나는 데이터 복제 현상을 관찰하는 단계이다. 본 연구에서는 피트니스 어플리케이션인 Strava[13]와 Endomondo[14]를 설치한다.

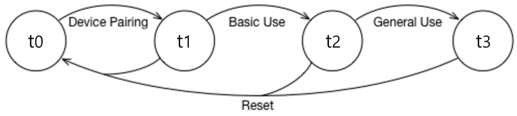


Fig. 1. Experiment phase

2.3 데이터 추출

Sony SmartWatch3, LG G Watch, 삼성 갤럭시 기어, 삼성 갤럭시 기어2 Neo 4개의 스마트워치에서 데이터 추출을 통해 데이터 복제현상을 분석하며 Apple Watch의 경우 데이터를 추출이 불가하여 실제 사용을 바탕으로 관찰 및 분석을 한다. 각 단계별 데이터 분석을 위해 각 단계 후에는 네트워크를 인터페이스를 비활성화 한다.

Android wear를 사용하는 스마트워치의 경우 루트 권한을 획득하여 ADB (Android Debug Bridge)를 통해 데이터 디렉터리 및 파티션을 PC로 가져온다. 그 후 커스텀 리커버리 이미지를 사용하여 루트 권한을 획득하고 커스텀 리커버리 모드로

부팅하여 데이터 액세스 및 USB 디버깅을 한다. Sony SmartWatch3의 경우 커스텀 리커버리 이미지를 플래시할 필요가 없어 부트 로더의 취약점을 이용하여 데이터를 추출하지만 LG G Watch의 경우에는 이러한 보안결함이 없었기 때문에 커스텀 리커버리 이미지를 플래시하고 데이터를 추출한다.

Tizen 기반 스마트워치의 경우, SDB(Smart Development Bridge)를 통해 스마트워치에서 PC로 데이터 디렉터리 및 파티션을 가져올 수 있다. 삼성 자체의 모바일 장치 플래싱 도구를 이용하여 수정 된 rootfs 파티션 이미지 파일을 스마트 워치로 플래싱하고 루트 모드에서 SDB를 활성화한 후 스마트워치 내 파일 시스템에 액세스하여 필요한 파일을 PC로 추출한다.

Apple Watch의 경우, 루트 권한 획득이 불가능하여 스마트워치를 사용한 후 단계별로 네트워크 인터페이스를 비활성화하여 스마트폰으로부터 데이터 복제 현상 관찰을 통해 분석한다.

2.4 실험 결과 및 분석

사용 시간의 순서에 따라 시점별로 데이터 복제 현상을 관찰한 결과는 Table 2.와 같은 양상을 보였다. 스마트워치로 넘어오는 데이터의 종류가 다양하며 사용 시간이 지남에 따라 복제되어 넘어오는 데이터의 양이 증가한다.

Android wear 기반의 Sony SmartWatch3은 초기 페어링 단계인 t1부터 스마트 폰에서 복제된 데이터가 넘어온다. 분석결과, 연락처 정보, SMS/MMS 메시지, 피트니스 데이터, 사진, WiFi SSID/비밀번호 및 호스트 기기 정보가 넘어왔으며 이 정보들은 넘어온다는 알림 없이 복제되어 넘어온다. WiFi SSID/비밀번호 정보의 경우, 스마트폰이 연결한 네트워크 정보로 스마트워치와 무관한 정보임에도 불구하고 넘어온다는 점에서 의미가 있다. e-mail, 메모 및 달력 정보는 t2 단계, 암호화된 잠금 패턴 및 위치정보는 t3 단계에서 복제된다. 특히, 암호화된 잠금 패턴은 쉽게 rainbow attack을 통해 쉽게 복호화가 가능했다[16]. 또한 위치 정보는 타 스마트워치와 달리 Sony SmartWatch3에서만 넘어온다.

Tizen의 경우, 삼성 갤럭시 기어와 갤럭시 기어2 Neo에서 데이터를 추출하였다. t1 단계에서는 연락처 정보, 사진 및 호스트 기기 정보가 복제되어 넘어왔으며 SMS/MMS 메시지, e-mail, 피트니스 데이터 달력 정보는 t2 단계에서 복제되었다. 이후, t3에서는 t2와 동일한 결과를 얻었으며 이는 Tizen 기반 스마트워치가 추가로 설치된 어플리케이션에 대한 데이터를 따로 저장하지 않기 때문에 나타난 결과이다.

타 플랫폼과 같이 Apple Watch 또한 초기 페어링 단계인 t1에서 연락처 정보와 SMS/MMS 메시지가 넘어오며 e-mail과 비밀번호 값은 단계 t2에서 넘어온다. 또한 t3단계에서 달력 정보가 넘어왔으나 그 외 사진 및 피트니스 데이터는 다른 스마트워치와 다르게 복제되는 현상을 관찰할 수 없었다.

Table 2. Experiment result of four phases (□: Not-Copied, ■: Copied, ▨: Unavailable)

Data \ Platforms	Android wear	Tizen	watchOS
Encrypted Lock Pattern	□□□■	□▨▨▨	□▨▨▨
Contact	□■■■	□■■■	□■■■
SMS/MMS/Messenger	□■■■	□□■■	□■■■
E-mail	□□■■	□□■■	□□■■
Memo	□□■■	□▨▨▨	□▨▨▨
WiFi SSID/Password	□■■■	□▨▨▨	□▨▨▨
Photo	□■■■	□■■■	□□□□
Fitness Data	□■■■	□□■■	□□□□
Location	□□□■	□▨▨▨	□▨▨▨
Calendar	□□■■	□□■■	□□□■
Host Device Info.	□▨▨▨	□■■■	□▨▨▨
Host Installed Apps	□■■■	□▨▨▨	□□■■

III. 위험도 평가 및 대응방안

앞서 실험 연구를 통해, 스마트워치 내 다양한 데이터가 스마트폰으로부터 복제되어 넘어온다는 것을 알아냈다. 본 연구는 이러한 사용자 별 데이터에 대해 실험결과와 더불어 사용자인식에 대한 설문조사를 실시하여 ISO/IEC 27005를 바탕으로 다음과 같이 위험도 평가를 수행한다.

3.1 스마트워치 보안에 대한 사용자 인식

실제 상용화된 기기에 대해 위험도를 평가를 한다는 점에서 그 기기를 사용하는 사용자의 인식은 위험도 평가에 영향을 미친다. 이를 위해 실제 스마트워치 사용자 205명을 대상으로 설문조사를 실시하였으며 스마트워치에 대한 보안인식을 조사하고 스마트폰으로부터 데이터가 복제되어 넘어오는 현상에 대한 인식을 조사하였다. 설문의 결과에 대해서는 위험도 평가에 반영할 필요가 있는 결과에 대해 보고한다.

설문 결과, 205명 중 74.1%인 152명이 스마트워치가 스마트폰보다 취약하다고 답하였다. 하지만 기기 내 개인정보 저장, 유출 및 위협에 대해 인지하고 있는지에 대해서는 스마트폰 보다 스마트워치에서의 인지정도가 낮다는 결과를 보였다. 따라서 스마트워치에 대한 보안인식이 낮다고 할 수 있으며 이를 위험도 평가에 반영한다.

또한, 73.2%가 스마트폰에서 스마트워치로의 데이터 복제 및 이동 현상을 알고 있음에도 불구하고 69.8%가 스마트폰과 스마트워치에 동일한 비밀번호를 설정하고 있거나 설정할 것이라고 답하였다. 이와 더불어 실험결과에서 Android wear의 암호화된 패턴락은 쉽게 복호화가 가능했다는 점에서 암호화된 비밀번호 값은 보안 및 개인정보보호 관점에서 매우 큰 위험이 있다고 판단된다[16]. 따라서 이를 위험도 평가에 반영한다.

3.2 데이터 분류

본 연구의 위험도 평가는 데이터 위협 및 유출을 Fig. 2.과 같이 보안 및 개인정보보호의 두 가지 관점에서 이를 각각을 3가지 수준으로 나누어 고려하여 각 수준의 조합에 따라 위협수준의 등급을 차등적으로 부여한다. 보안과 개인정보보호 수준이 모두 3인 최대 수준을 가장 높은 등급인 5등급으로 분류한다. 또한 둘 중 하나가 최대 수준인 3인 경우, 스마트워치에서의 보안의식이 낮다는 설문 결과에 따라 높은 위험이 있다고 판단하여 4등급을 부여한다.

본 연구에서는 스마트워치 내 데이터를 기기제어 정보, 교류 정보, 센서 수집정보 및 사용자 작성 정보의 네 가지 범주로 분류한다. Table 3.은 분류에 따른 데이터별 정의 및 각각의 데이터에 대한 보안 관점 및 개인정보보호 관점의 수준을 나타내며 이를 종합하여 위협수준에 따라 5단계로 부여한다. 다음은 5단계의 위협 수준에 대한 설명이다.

Table 3. Data categorization and impact score

Extracted Data	Description	Security level	Privacy Level	Impact Score
Control of Device				
Encrypted Lock Pattern	Exploit to unlock host smartphone	3	3	5
WiFi SSID/Password	Compromise secure wireless network	2	2	3
Host Device Info.	Contains phone number and name	1	2	2
Host Installed Apps	Represents owner's app preference	1	1	1
Communication				
Contact	Indicates user's human relationship	2	2	3
SMS/MMS/Messenger	Personally exchanged information	2	3	4
E-mail		2	3	4
Sensor Data				
Photo	Private photos and can be shared to others	2	2	3
Fitness Data	Contains owner's physical traits	2	2	3
Location	Provide owner's radius of action	2	3	4
User Written Data				
Memo	Indicates owner's action or intention	1	2	2
Calendar	Contains owner's schedule or plan	1	2	2

Security level \ Privacy level	1	2	3
1	1	2	4
2	2	3	4
3	4	4	5

Fig. 2. Impact score of security and privacy level

• very high(5): 암호란 타인과 공유하지 않는 것으로 잠금 패턴에 대한 유출을 매우 높은 위협을 초래하고 스마트워치의 암호화된 잠금패턴의 경우 쉽게 복호화 됨에 따라 가장 높은 수준을 부여한다. 또한 이는 상당수의 사용자가 잠금 패턴 및 비밀번호를 스마트워치와 스마트폰에 동일하게 설정한다는 설문결과를 반영한 결과이다.

• high(4): GPS 위치 정보, e-mail 및 SMS/MMS 메시지와 같은 사용자의 최신 정보를 나타내는 데이터로 이러한 정보를 바탕으로 사용자 행동을 예측 및 추적 할 수 있다.

• moderate(3): 사용자는 사진, 피트니스 데이터 및 연락처 정보를 숨기지 않고 타인과 공유하기도 한다. 이러한 데이터를 통해 사용자 행동을 추적하기는 어렵지만 공개될 시에 보안 및 개인정보보호 문제를 야기할 수 있다.

• low(2): 기기제어 정보와 관련된 정보는 개인정보보호 관점에서 3단계 중 2단계에 할당되지만 보안 위협은 거의 발생하지 않는다. 또한 사용자 작성 데이터는 개인정보보호 관점에만 영향을 받는다.

• very low(1): 기기에 설치된 어플리케이션 종류는 사용자를 식별하는 측면에서 의미가 없다고 볼 수 있다.

3.3 데이터별 위험도 점수

본 연구는 스마트워치 내 데이터에 대한 위험도 평가를 수행함에 있어서 기존 스마트폰의 위험도 평가 방법을 기반으로 한다. 이와 더불어 데이터 복제 현상에 관한 실험 연구에 따라 시점별 데이터 존재 가능성을 위험도 점수에 반영하여 계산한다.

데이터 복제현상이 빠를수록 위협 및 취약점이 증가함에 따라 세 가지 기기 사용 시점인 t1, t2, t3에 대해 높음, 보통, 낮음으로 서로 다른 등급을 부여한다. t1 단계에서 복제되어 넘어오는 데이터는 초기 페어링 과정부터 존재 가능성이 높으므로 '높음(3)' 로 간주한다. 이와 같이 t2와 t3에서의 데이터는 각각 '보통(2)'과 '낮음(1)'을 할당한다. 각 데이터에 대해 단계별 존재 가능성에 대한 수준을 위험 수준과 곱하여 다음의 식과 같이 계산한다.

$$Risk_{platform}(data) = Impact(data) * Likelihood_{phase}(data) \quad (1)$$

Fig.3.는 이를 각 플랫폼에 따라 종합적으로 계산한 결과이다. 스마트워치의 데이터에 대한 위험은 시간이 증가함에 따라 증가한다. Android wear 기반 스마트워치의 위험도 점수가 가장 높았으며 Apple Watch는 49점으로 가장 낮음을 도출하였다.

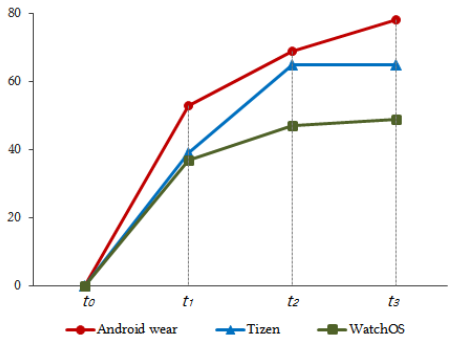


Fig. 3. Risk score distribution in phases

3.4 대응방안

데이터 복제 및 넘어감 현상에 대한 알림의 관해서는 Android Wear 기반 스마트워치의 경우에만 알림이 있었으며 Tizen 및 watchOS의 경우 알림이 없었다. 예상보다 많은 데이터가 복제됨에 따라 스마트워치에 대한 보안기준 확립과 사용자에게 이를 알리는 알림기능의 확대가 필요하다.

데이터별 분석결과, 최종시점에서의 데이터별 점수분포는 Fig.4.와 같은 결과를 보였으며 데이터별로 위험의 정도에 대한 차이가 분명함을 알 수 있다. 따라서 페어링이 종료되었거나 사용 후 일정시간이 지난 후에는 위험도가 높은 순서에 따라 데이터가 선별적으로 삭제될 수 있는 방안을 제안한다. 데이터가 선별적으로 삭제될 때에는 본 연구에서 도출한 데이터별 위험정도인 Fig.4.에 따라 점수가 높은 순서대로 데이터가 삭제되도록 한다. 그 후 사용자가 다

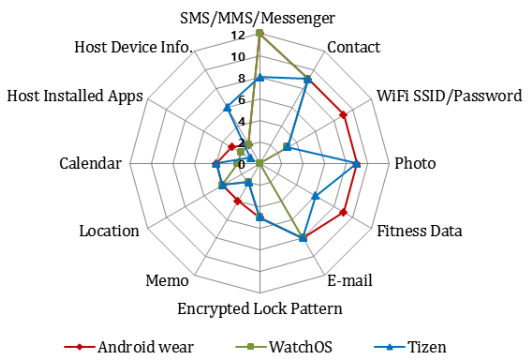


Fig. 4. Risk scores of data in each platform

시 스마트워치 사용을 시작하여 페어링되면 다시 빠르게 데이터가 복제되어 넘어오도록 한다.

IV. 관련연구

4.1 데이터 추출

2015년 Baggili 등은 사용 시나리오를 바탕으로 삼성 갤럭시 기어2 네오 및 LG G워치 스마트 워치에서 데이터를 추출하였다. 삼성 갤럭시 S4 액티브 스마트 폰과 페어링 하였으며 userdata 파티션을 덤프하여 덤프 된 사용자 데이터 파티션에서 검색된 정보를 분류했다[1]. 2016년 Do, Quang 등은 시나리오 및 위협 모델을 바탕으로 부트 로더 취약점을 이용하여 삼성 갤럭시 기어 Live 스마트 워치에서 다양한 개인 정보를 추출하였다[2]. 커스텀 부트 이미지를 통해 루트권한을 획득하였으며 ADB 인터페이스를 사용하여 데이터를 추출하였다.

본 논문은 Android Wear, watchOS 및 Tizen의 플랫폼에서 5개의 스마트워치를 실험 대상으로 하며 사용 시점을 4단계로 구분하여 데이터 복제 현상을 관찰했다는 점에서 이전 연구들을 확장했다고 볼 수 있다. 뿐만 아니라 이전 연구와는 달리 데이터 추출 실험 및 설문조사를 기반으로 데이터에 대한 위험 평가를 수행하였다.

4.2 위험도 평가(Risk assessment)

데이터 위험도 평가방법은 정보 보안 위험 관리 지침을 제공하는 국제 표준인 ISO/IEC 27005에 근거한다[5]. ISO/IEC 27005에 따르면 일반적인 위험도 평가의 절차는 다음과 같다. 먼저, 선택한 데이터 자원에 대한 정의를 한다. 그 다음, 정의된 자원의 데이터별 위협 정도 및 수준을 할당한다. 마지막으로 위협에 따른 영향 정도에 등급과 점수를 계산하고 통합된 위험도 평가 결과를 도출한다.

Hogben 등은 스마트 폰에 대한 위험도를 평가하기 위해 실제 위험도와 사용 시점별 잠재적인 위험도를 분석하여 점수를 부여했다[6]. 기기 대상별로 시나리오를 정의하였으며 이 연구는 타 연구에서의 위험도 평가를 위한 기초를 제공한다. Theoharidou 등은 안드로이드 플랫폼에서의 사례 연구를 통해 위험도 평가를 제안하였다[7]. 기기 사용 목적에 따른 데이터의 유형과 출처를 기반으로 데이터를 분류하여 데이터의 영향, 위협 허용 정도 및 발생 가능성을 종합하여 5가지 척도로 위험도를 평가한다[11].

본 연구는 과거에 수행된 적이 없는 스마트워치 내 데이터에 대한 위험도를 평가하며 스마트폰에서 넘어오는 데이터를 분석하므로 스마트폰에서의 위험도 평가 관련 연구를 기반으로 하였다. 단계별 데이터 복제 현상에 대해 서로 다른 가중치를 부여하여 스마트워치에서의 위험도 평가를 수행한다.

V. 결 론

본 논문은 스마트폰으로부터 스마트워치로 복제되어 넘어오는 데이터를 분석하고 스마트워치에 대한 보안 인식에 대한 설문을 바탕으로 위험도 평가를 수행한다. 데이터에 대한 플랫폼별 및 시점별 위험도를 평가한 결과, 데이터별 위험정도가 다르게 나타났으며 시간이 지남에 따라 위험도가 증가하며 Android wear 기반 스마트워치의 위험도 점수가 가장 높았다. 많은 데이터가 복제됨에 따라 이에 대한 대응방안으로 데이터의 위험도가 높은 순서대로 데이터가 선별적으로 삭제되는 방안을 제시한다.

References

[1] I. Baggili, J. Oduro, K. Anthony, F. Breitinger, and G. McGee. "Watch what you wear: preliminary forensic analysis of smart watches." IEEE 10th International Conference on Availability, Reliability and Security (ARES). pp. 303 - 311. 2015.

[2] Q. Do, B. Martini, and K.R. Choo. "Is the

data on your wearable device secure? An Android Wear smartwatch case study." Software: Practice and Experience. 2016.

[3] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. BenOved, and S. Moller. "On the need for different security methods on mobile phones." In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. ACM, pp. 465 - 473. 2011.

[4] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. "Measuring user con dence in smartphone security and privacy." In Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 2012

[5] I ISO and I Std. 2011. Iso 27005: Information technology - Security techniques - Information security risk management. 2011.

[6] G. Hogben and M. Dekker. "Smartphones: Information security risks, opportunities and recommendations for users." European Network and Information Security Agency. 2010.

[7] M. Theoharidou, A. Mylonas, and D. Gritzalis. "A risk assessment method for smartphones." In IFIP International Information Security Conference. Springer, pp. 443 - 456. 2012.

[8] S. Egelman, S. Jain, R. S. Portno, K. Liao, S. Consolvo, and D. Wagner. "Are you ready to lock?." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 750 - 761. 2014.

[9] M. Harbach, A. D. Luca, and S. Egelman. "The Anatomy of Smartphone Unlocking." In Proceedings of the 34th Annual ACM Conference on Human Factors in Computing Systems, CHI. 2016.

[10] M. Harbach, E. V. Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith. "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception." In Symposium on usable privacy and security (SOUPS). pp. 213 - 230. 2014.

[11] T. Lederm and N. L. Clarke. "Risk assessment for mobile devices." In International Conference on Trust, Privacy and Security in Digital Business. Springer, pp. 210 - 221. 2011

[12] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao. "Stealing PINs via Mobile Sensors: Actual Risk versus User Perception." International Journal of Information Security. 2016.

[13] Strava Inc. 2017. Strava https://www.strava.com/

[14] Under Armour Inc. 2017. Endomondo. https://www.endomondo.com/

[15] D. V. Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcs. "Modifying smartphone user locking behavior." In Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM, 10. 2013.

[16] M. Spreitzenbarth. Cracking the Pattern Lock on Android. https://forensics.spreitzenbarth.de/2012/02/28/cracking-the-pattern-lock-on-android/ 2012.

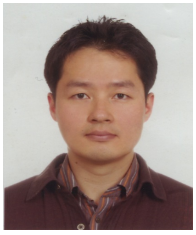
[17] S. Willassen. "Forensics and the GSM mobile telephone system." International Journal of Digital Evidence. 2003

[18] H. Xu, S. Gupta, M. B. Rosson, and J. M. Carroll. "Measuring mobile users' concerns for information privacy." International Conference on Information Systems (ICIS). 2012.

〈저자소개〉

이 영 주 (Youngju Lee) 학생회원
2016년 2월: 이화여자대학교 컴퓨터공학과 학사
2016년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 Usable Security, IoT Security 등

양 원 석 (Wonseok Yang) 학생회원
2015년 2월: 상명대학교 미디어소프트웨어학과 학사
2017년 2월: 연세대학교 정보대학원 석사
〈관심분야〉 Mobile Security, Usable Security 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년 Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 인증, Usable Security, 사물인터넷 보안, 소프트웨어 보안, 펌웨어 보안 등