Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.453

해외 애플리케이션의 개인정보 무단 수집 실태 분석과 대응 방안에 대한 연구

김 세 환,[1†] 윤 형 준,[2] 정 다 현,[3] 장 승 훈,[4] 한 철 규[5‡]
[1]경일대학교 (학생), [2]경기과학기술대학교 (학생), [3]세종대학교 (학생),
[4]한국교원대학교 (학생), [5]LG CNS (총괄 PM)

Research on the Analysis and Response of Unauthorized Personal Information Collection in Foreign Applications

Se-Hwan Kim,[1†] Hyung-Jun Yun,[2] Da-Hyun Jung,[3]
Seung-Hoon Jang,[4] Cheol-Kyu Han[5‡]
[1]Kyungil University (Student),
[2]Gyeonggi University of Science and Technology (Student),
[3]Sejong University (Student), [4]Korea National University of Education (Student),
[5]LG CNS (Security Professional)

요 약

국내에서 서비스되고 있는 해외 애플리케이션의 수가 증가하고 있다. 이들 중 많은 국내 이용자의 수를 보유한 애플리케이션에서 이용자의 개인정보를 무단으로 수집하는 사례가 많이 발생하여 문제가 되고 있다. 애플리케이션을 통해 행해지는 개인정보 무단 수집은 이용자의 민감한 개인정보들이 악의적인 형태로 사용될 수 있어 위험성이 크다. 또한, 이는 사업자윤리에 위반되는 행위이고 건전한 IT 생태계 조성을 방해할 수 있다. 본 연구에서는 국내에서 서비스되고 있는 해외 애플리케이션의 이용자 개인정보 무단 수집 실태를 분석하고, 이에 대한 대응 방안을 도출하는 것을 목적으로 한다.

ABSTRACT

The number of foreign applications available in Korea is increasing. Among them, there are many cases where applications having a large number of domestic users collect users' personal information in an unauthorized manner, causing serious problems. Unauthorized collection of personal information conducted through such applications is highly dangerous, because sensitive personal information of users can be used in a malicious way. Further, this is violation of business ethics and may interrupt the creation of the sound information technology ecosystem. This research is purposed to analyze the current status of unauthorized collection of users' personal information by foreign applications available in Korea and to derive countermeasures thereof.

Keywords: Information Security, foreign Applications, Personal information, Business ethics

Received(03. 15. 2021), Modified(05. 31. 2021),
Accepted(05. 31. 2021)

† 주저자, he3717@gmail.com
‡ 교신저자, hck214@daum.net(Corresponding author)

I. 서 론

리서치회사인 한국갤럽조사연구소에 따르면 2020년 8월 기준 국내 스마트폰 이용률은 93.4%, 20대부터 50대까지의 이용률은 99%[1]로 전 국민이 스마트폰을 사용하고 있다고 해도 과언이 아니다.

이처럼 스마트폰은 인간의 삶과 분리할 수 없을 정도로 밀접하게 연관되어 있고 4차 산업혁명 시대에 IoT(Internet of things) 기기와 연동하며 더욱 발전할 것이다.

현재의 스마트폰은 금융, 의료와 같은 민감한 개인정보를 처리하는 업무를 포함하여 전화, 메시지, GPS(Global Positioning System) 등의 다양한 기능들을 활용할 수 있다.

이와 같은 스마트폰의 특성상 기기 안에 이용자의 고유식별정보, 바이오 정보를 포함한 다량의 개인정보가 저장되어 있을 수 있어 스마트폰 개인정보 유출은 막대한 피해로 이어질 수 있다[2].

하지만 일부 해외 애플리케이션들에서 필요 이상의 과다한 개인정보를 수집하거나[3], 심지어 이용자의 동의 없이 무단으로 수집한 사례가 발견되었다[4].

스마트폰 OS(Operating System)에서 제공하고 있는 스토어를 통해 해외의 다양한 애플리케이션 서비스들도 손쉽게 이용할 수 있어, 일부 해외 애플리케이션들의 개인정보 무단 수집 행위는 국내 스마트폰 이용자들에게도 피해를 미칠 수 있다.

문제는 현행법상 국내 기업의 경우 엄격한 개인정보 보호법, 정보통신망법에 맞춰 취급하고 있으나, 해외 기업의 경우 본사가 해외에 존재한다면 정보통신서비스 제공자로 볼 수 없는 경우가 많고 국내법에 적용되지 않는 경우도 존재한다는 것이다[5].

따라서 본 연구에서는 국내에서 서비스되고 있는 애플리케이션들의 개인정보 수집 실태 전반에 대한 분석을 통해 국내 애플리케이션과 해외 애플리케이션에서 수집하는 개인정보 간의 차이와 개인정보 수집 과정의 차이를 비교하고, 해외 애플리케이션의 무분별한 개인정보 수집이 이루어지는 원인과 개인정보 처리 과정을 분석하여 해외 애플리케이션의 무분별한 개인정보 수집을 개선할 방안을 도출하고자 한다.

1.1 선행연구

기존 '모바일 어플리케이션 개인정보 유출탐지 및 보안강화 연구'[6]의 연구에서는 애플리케이션의 단말 식별 정보 유출을 다루고 있으나 연구 대상이 국내 애플리케이션에 국한되어 있으며 무단 수집이 아닌 유출에 대한 연구였다. 또한 '국내 모바일 앱 이용자 정보 수집 현황 및 법적 쟁점 - ADID를 중심으로 -'[7]의 연구에서는 안드로이드 애플리케이션을 대상으로 이용자의 광고 식별자(ADID) 현황을 실증적으로 분석하였으나 대안은 제시하지 못하였다. 본 논문에서는 해외 애플리케이션의 단말고유정보(MAC, IMEI) 무단 수집을 중점적으로 연구하여 해외 애플리케이션의 개인정보 무단 수집 현황을 증명하고 이해관계자별 대안을 제시하고자 한다.

1.2 연구 방법

본 연구에서는 해외 애플리케이션 개인정보 수집에 대한 현황을 조사하고 '정보통신망 취약점 분석·평가 방법론'[8]을 활용하여 해외 애플리케이션을 분석하였으며, 그에 대한 문제점 도출 및 대응 방안을 제시하였다. 특히 해외 애플리케이션 분석은 총 4단계(준비, 사전, 실시, 대응 방안)로 진행하였다. 준비 단계에서는 트래픽 분석 프로그램, 가상 모바일 기기, VPN과 같은 도구 조사를 하였다. 사전 단계에서는 과거 인도 정부에서 개인정보 무단 수집 이슈가 발생했던 중국 애플리케이션을 대상으로 제재를 가한 것을 참고하여, 분석을 진행할 애플리케이션을 선정하였다. 실시 단계에서는 선정된 애플리케이션들을 대상으로 실질적인 분석을 하였으며, 그 결과 해당 애플리케이션들에서 IMEI와 MAC 주소를 수집한다는 것을 확인할 수 있었다. 해당 결과를 토대로, 대응 방안 단계에서는 개인정보 무단 수집 실태에 대해 애플리케이션 이용자, 애플리케이션 제공자, 입법 및 집행기관 측면에서의 대응 방안을 각각 제시하였다.

II. 현황 조사

2020년 7월 기준 전 세계 월간 활성화 이용자 수가 8억 8000여만 명에 달하는 대형 애플리케이션인[9], 중국 ByteDance의 틱톡이 이용자의 정보를 무단으로 수집한다는 사실이 보도되어 이슈가 발생한 적이 있다. 틱톡은 국내에서도 다수의 이용자를 보유하고 있고 유튜브를 이어 가장 많이 사용하는 동영상 애플리케이션 2위를 차지하였다[10]. 다만 약 2019

년도부터 보안 측면에서 여러 문제가 제기되어 왔고, 특히, 2020년 8월 WSJ(The Wall Street Journal)에서 틱톡이 이용자의 MAC(Media Access Control) 주소와 같은 개인정보를 무단으로 수집한다는 기사를 보도하여 큰 이슈가 되었다[11]. 이러한 보안 이슈가 제기된 이후, 국내 이용자 수집에 대한 실증적인 분석을 확인할 수 없어 본 연구를 통해 이에 대해 확인하고자 한다.

III. 애플리케이션 분석

3.1 분석 환경 및 수행

틱톡에서 수집하는 개인정보를 확인하기 위하여 틱톡 애플리케이션을 가상 안드로이드 기기 환경에 설치 후 이를 실행하여 틱톡과 서버 사이에 통신하는 네트워크 패킷을 확인하였고, 실제로 패킷 내 개인정보를 수집하는지에 대한 여부를 확인하는 방식으로 연구가 진행되었다. 그리고 틱톡뿐만 아니라 현재 구글 플레이스토어를 통해 유통되고 있는 애플리케이션의 개인정보 수집 여부 또한 확인하기 위해 추가적인 애플리케이션 분석을 진행하였다.

구글 플레이스토어에서 유통되고 있는 틱톡 서비스는 TikTok Pte. Ltd에서 발행한 버전(이하 PTE)과 TikTok Inc에서 발행한 버전(이하 INC) 두 가지 버전이 존재한다. PTE와 INC 버전은 각각 동아시아 국가와 영어권 국가를 대상으로 서비스하고 있다. 본 논문에서는 국내 사용자들을 대상으로 수집하는 데이터를 확인하고, 국내 버전과 해외 버전 이용자에 대한 수집 정보의 차이를 알아보기 위해, PTE 버전과 INC 버전 두 유통사에서 배포한 APK(Android Application Package)를 모두 이용하였다.

네트워크 패킷 분석을 위해 HTTP(S) 요청과 응답을 모니터링하는 프록시 도구인 Mitmproxy를 활용하였고, 이는 비교적 가벼운 프로그램이며 웹을 통해 분석이 가능하다는 이점이 있어 분석 도구로 선정하게 되었다. 또한 국내 및 해외 이용자를 대상으로 수집하는 정보 간의 차이가 있는지에 대한 여부를 확인하기 위해 VPN(Virtual Private Network)을 이용하였고, 해외 사용자와의 환경을 유사하게 만들기 위해 애플리케이션들이 수집하는 정보인 언어, 시간, 지역, IP(Internet Protocol) 등을 분석이 진행되는 국가에 해당하는 나라로 설정한 이후 분석을 진행하였다.

Table 1. Analysis Environment

Emulator	Noxplayer 6.6.1.3
VPN	Express VPN 9.0.2.58
Virtual Device	Samsung Galaxy S7
	Samsung Galaxy S9+
SIM Card	None
Level	Root
OS	Android 5.1.1

3.2 분석 결과

2017년 10월부터 2020년 9월 사이에 출시된 25개 버전의 틱톡 애플리케이션을 분석 대상으로 선정하였으며, APK 아카이브 사이트인 Uptodown와 Apkmirror 두 곳에서 APK를 다운로드하여 분석을 진행할 수 있었다.

MAC 주소, IMEI(International Mobile Equipment Identify), HS(Hardware Serial number) 그리고 ADID(Android Device IDentification) 값의 수집 여부를 중심으로 틱톡이 수집하는 데이터를 확인한 결과는 Table 2.와 같고, 수집하는 항목이 동일할 경우 중복으로 인해 일부 버전을 제외하여 생략하였다.

그리하여 분석 결과, 틱톡은 25개의 버전 중 14개 버전에서 MAC 주소를, 9개 버전에서 IMEI를

Fig. 1. TikTok 7.6.5 version IMEI acquisition status

Fig. 2. TikTok 7.6.5 version MAC, HS, ADID acquisition status

수집하는 것으로 나타났다. 1.3.0 버전이 출시된 2017년 10월부터 7.6.5 버전이 출시된 2019년 8월까지 최소 23개월 동안 MAC 주소가 수집된 것이다.

Table 2. Timeline by TikTok PTE User Information Collection Version

	1.3.0	1.9.3	2.7.0		16.0.4	17.6.3
I	O	O	X		O	X
H	X	O	O	…	X	X
M	O	O	O		X	X
A	O	O	O		O	O

* I : IMEI
H : Hardware Serial Number
M : MAC Address
A : Android Device IDentification

Table 3. Timeline by INC User Information Collection Version

	8.7.0	9.9.5	16.0.4	17.6.3
I	O	O	O	X
H	O	O	X	X
M	O	O	X	X
A	O	O	O	O

* I : IMEI
H : Hardware Serial Number
M : MAC Address
A : Android Device IDentification

해외 이용자 대상의 온라인 식별자 수집에 대한 분석을 진행한 결과, 국내 이용자의 경우와 크게 차이가 나타나지 않았다. 다만 9.9.5 버전에서는 국내에서는 수집하지 않았지만 INC 이용자를 대상으로 MAC 주소를 수집하는 것으로 확인하였다.

Table 4.는 틱톡이 이용자를 대상으로 수집하는 정보들을 보내는 서버와 그 빈도에 대해 도식화한 것이다. 모든 수집은 기기에 설치한 애플리케이션을 최초로 실행한 직후 개인정보 처리방침에 동의하기 이전에 이루어졌다.

이러한 수집 행태가 틱톡뿐만 아니라 모바일 애플리케이션 시장의 전반적인 문제로 이어질 수 있어 구글 플레이 스토어에 유통되고 있는 애플리케이션들을 대상으로 추가적인 분석을 진행하였다. 해당 애플리케이션들은 2020년 6월 인도 정부가 사용을 금지한

Table 4. TikTok send and receive domains

Domain	User Information Collection List	Packet Occurrence Frequency
log.tiktokv.com	IMEI, ADID, mobile carrier code, device type, manufacturer, carrier nationality, country, time zone information, app language, etc.	Every minute
mon-va.tiktokv.com	MAC, IMEI, HS, ADID, mobile carrier code, device type, manufacturer, nationality of carrier, national time zone information, app language, SIM country, etc.	Immediately after execution
api.tiktokv.com	IMEI, ADID, mobile carrier code, device type, manufacturer, carrier nationality, national time zone information, app language, SIM country	Every 15 minutes

틱톡을 포함한 몇몇 애플리케이션들의 리스트를 분석 대상으로 선정하였다[12].

모든 애플리케이션은 2020년 12월 5일 기준으로 구글 플레이스토어를 통해 배포되고 있는 최신 버전을 대상으로 분석하였고, 일부 애플리케이션들은 애플리케이션 내 결제 기능을 목적으로 MAC 주소와 IMEI 값과 같은 온라인 식별자를 정당하게 수집하였을 가능성이 존재한다. 기타 애플리케이션 분석 또한 틱톡 애플리케이션을 대상으로 분석한 것과 동일한 방식으로 진행되었다.

3.3 기타 애플리케이션 분석 결과

기타 애플리케이션으로는 CamScanner, CamCard, Super Clean, Meitu, 배틀그라운드, FaceU 애플리케이션을 선정하였다. 그중 FaceU 애플리케이션은 Bytedance PTE. Ltd에서 제작한 애플리케이션으로 틱톡과 동일한 회사에서 만든 애플리케이션인 것을 확인할 수 있었고, MAC 주소 수집 시 mac_address 인자를 통해 02:00:00:00:00:00과 같은 일반적인 MAC 주소라고 보기 어려운 값을 전송하고 있었다.

틱톡과 같은 회사에서 제작한 애플리케이션인 만큼 틱톡이 MAC 주소 무단 수집 이슈 논란이 제기되었을 비슷한 시기에 수집을 중단한 것으로 추측된다. 또한, 실제로 틱톡 또한 비슷한 시기인 9.9.5 버전부터 16.0.42 버전까지 FaceU 애플리케이션과 동일하게 mc 인자 값이 02:00:00:00:00:00으로 전송된 것을 확인하였다.

Table 5. Other App User Information Collection Status

	Cam Scan-ner	Cam Card	Su-per Cle-an	Mei-tu	Battle ground	Fa-ce U
I	O	O	O	O	O	O
H	X	X	X	X	X	X
M	X	X	X	O	O	X
A	X	X	O	X	X	O

* I : IMEI
H : Hardware Serial Number
M : MAC Address
A : Android Device IDentification

3.4 애플리케이션의 개인정보 관련 법규 위반 실태

방송통신위원회와 한국인터넷진흥원(이하 KISA)에서 제출받은 '스마트폰 애플리케이션 모니터링 및 개선현황' 분석 결과, 2017년 스마트폰 애플리케이션 12,008개 중 63%인 7,560개의 애플리케이션이 국내 개인정보 수집 관련 법규를 위반한 것으로 조사되었다. 이들 중 1.5%인 122개의 애플리케이션들만이 이에 대한 개선을 완료한 것으로 나타났다.

국내 법규를 위반한 애플리케이션들 중에는 설치 수가 최소 5억 건에서 10억 건 이상에 해당하는 인기 애플리케이션들도 포함되어 있는 것으로 나타났고, 하루 평균 국내 접속자 수가 천만 명에 이르는 페이스북의 경우, 위치정보법 제16조 제1항 위도, 경도 등 위치정보 전송 및 암호화 여부를 포함하여 제19조 제1항 제1호와 제2호의 이용약관 명시, 그리고 제2항 위치정보 제3자 제공 관련 내용의 이용약관 명시와 동의 여부에 대한 규정을 위반한 것으로 나타났다. 또한 정보통신망법 제22조 제1항 개인정보 수집이용 동의, 제22조의 2 제1항 접근권한에 대한 동의, 제27조의 2 제2항 5호와 7호 개인정보 처리방침 공개, 제28조 개인정보 보호조치 등 총 9가지 규정을 위반하고 있는 것으로 조사되었다[13].

2020년 11월 진행된 개인정보보호위원회 전체회의에서 발표된 바에 따르면, 페이스북의 개인정보보호 위반 사례는 다음과 같았다. 페이스북이 이용자의 개인정보를 제3자에게 제공하는 경우, 이용자 당사자의 동의를 받아야 하는 법적 의무를 준수하지 않고 이용자의 동의를 받지 않은 상태에서 다른 사업자에게 이용자의 개인정보를 제공한 사실이 확인되었다. 조사 결과, 2012년 5월부터 2018년 6월까지 약 6년간 이러한 위반 행위가 있었던 것으로 드러났고, 국내 페이스북 이용자 1,800만 명 중 최소 330만 명 이상의 개인정보가 다른 사업자에게 제공된 것으로 확인되었다. 또한, 페이스북은 이용자의 비밀번호를 암호화하는 등의 기술적 보안조치를 해야 하는 법적 의무를 준수하지 않고, 암호화 조치를 취하지 않은 상태에서 이용자의 비밀번호를 평문으로 저장한 것으로 밝혀졌다[14].

IV. 문제점 도출

4.1 개인정보로서의 IMEI, MAC

최근 모바일 기기의 수가 증가함과 동시에, 기기에 내장되어 있는 모바일 고유식별정보인 IMEI 값과 MAC 주소 또한 다수 생성되고 있다. 스마트폰에는 고유식별정보, 바이오 정보를 포함한 다량의 개인정보가 저장되어 있는 만큼, 모바일에 대한 보안 인식이 나날이 중요해지고 있다.

애플리케이션에서 수집되고 있는 MAC 주소와 IMEI의 경우, 국내에서도 개인정보로 판단될 가능성이 존재하는 정보이다. MAC 주소는 바꿀 수 없는 고유한 하드웨어 기기 번호이기 때문에 다른 정보들과 결합될 경우 사용자를 특정할 여지가 있다. 이와 같은 이유로 유럽의 개인정보 보호법인 GDPR(General Data Protection Regulation)의 경우, 온라인 식별자를 개인정보에 포함하기도 한다. 국내에서도 KISA에서 발행한 "개인정보 영향평가 수행안내서"에 기재된 개인정보영향도 등급표 작성 예시에서 MAC 주소가 개인정보로 분류되어 있다. IMEI는 단말기에 부여된 고유한 일련번호로, 국내에서 개인정보로 판단된 판례가 있다. 이는 2011년 증권정보 애플리케이션 '증권통'에서 IMEI와 USIM(Universal Subscriber Identity Module) 일련번호 등을 수집하여 개인정보 무단 수집으로 유죄 판결을 받은 사례이다[15].

개인정보 보호법 제 16조에 따르면 개인정보처리자는 최소한의 개인정보만을 수집하여야 하며, 최소한의 정보 외의 수집에는 동의하지 않을 수 있다는 사실을 정보주체에게 고지해야 한다. 그러나 틱톡은 애플리케이션 실행 직후 개인정보로 판단될 여지가 있는 MAC 주소와 IMEI를 틱톡의 서버로 전송했고, 해당 정보들이 애플리케이션 운영을 위해 필수적이었는지도 확실하지 않다.

틱톡과 인도 정부에서 사용을 금지한 애플리케이션들에서도 온라인 식별자인 MAC 주소나 안드로이드 고유식별정보인 IMEI 값을 수집하고 있는 것이 확인되었다. 이러한 정보 수집은 개인정보 보호법 제 16조를 위반했을 가능성이 있다.

호주 정보보안 의회 합동위원회 의장인 앤드류 해스티 하원의원은 틱톡이 베이징 당국과 개인정보를 공유할 수 있는 것에 우려를 표하였고, 이는 잠재적인 국가 안보 위협이 될 수 있다고 언급하였다[16]. 이처럼 IMEI와 MAC 주소와 다른 개인정보를 추가적으로 결합할 시 개인을 특정할 수 있는 소지가 있을 뿐만 아니라, 더 나아가 국가적인 문제로 이어질 가능성이 존재한다[17].

다만 이러한 개인정보 수집 이슈가 발생한 것은 틱톡이 최초 사례인 것은 아니다.

본 연구에서 분석을 진행한 모바일 애플리케이션들을 제외한, 현재 구글 플레이스토어를 통해 유통되고 있는 다른 애플리케이션 중에서도 이용자의 IMEI와 MAC 주소를 수집할 가능성이 존재한다.

4.2 IMEI, MAC 수집의 문제점

기기의 IMEI 값을 알아낼 시, 모바일 기기를 복제할 수 있는 위험성이 존재할 수 있다. 기존 휴대전화와 복제된 휴대전화가 동시에 켜져 있을 경우, 통신사 측에서 두 휴대전화를 비활성화시킬 가능성이 있고, 이로 인해 기존에 사용하고 있는 사용자의 네트워크가 연결되지 않아 정상적으로 서비스를 이용할 수 없는 문제가 야기될 수 있다.

또한 복제된 휴대전화를 통해 신분 도용이 가능할 것이라고 예상된다. 예를 들어, 공격자가 악의적인 목적을 지니고 사전에 만들어 둔 피싱 사이트를 SMS 내에 포함시켜 기존 사용자의 지인에게 발송할 수 있는 위험이 존재할 수 있다. 또한 기존 휴대전화를 통해 수신할 수 있는 SMS 문자 등이 복제된 휴대전화에서 수신될 수 있으며, 최근 은행에서는 SMS 내 이중 인증 코드를 송수신하여 사용자를 식별하는 방식을 채택하는 경우도 있는 만큼, IMEI 복제 문제의 위험도는 상당히 높을 것으로 예상된다.

실제로 IMEI를 통해 휴대전화를 복제하여 범죄에 악용한 사례들이 존재한다. 과거 기초생활 보장 수급자 등을 대상으로 고가의 스마트폰을 개통시키는 것을 유도한 이후, 휴대전화 복제 프로그램을 이용해 약 1,184대의 휴대전화를 복제한 사례가 있었다. 해당 사례에서는 IMEI를 통해 휴대전화 복제를 진행하였고, 이 과정에서 'IMEI Changer'라는 프로그램이 사용된 것으로 밝혀졌다[18].

뿐만 아니라, 미국의 사이버 보안 정보 공유 기관인 SC 미디어는 Bitdefender社 연구 보고서에 따르면, 중국과 일본의 안드로이드 사용자를 대상으로 스크린샷을 찍고, 전화 통화를 엿듣는 등의 기능을 가진 악성코드가 발견되었고, 피해자를 선별하는 과정에서 안드로이드 고유의 기기값인 IMEI를 기반했

다고 전했다[19]. 이처럼 IMEI 값을 악용한 범죄가 늘어나는 만큼 개인 및 기업 측에서 IMEI 값이 유출되지 않도록 보안을 강화해야 할 필요가 있다.

MAC 주소는 48bit로 구성되어 있는 네트워크 카드 하드웨어에 존재하는 고유한 물리적 주소이며 대부분의 네트워크 장비당 하나의 번호를 지니고 있다. 고유한 특징으로 인해 다른 추가적인 정보와 결합할 시 개인을 특정할 수 있는 소지가 있다. 정보보안 전문 언론사인 보안뉴스에서는 과거 아시아나 항공 홈페이지가 핵티비즘으로 추정되는 공격으로 인한 피해를 입었고, 일각에서는 MAC 주소를 변경시키는 스푸핑 공격 가능성이 제기되었다고 전했다[20]. 이처럼, 다수의 서비스를 운영하고 있는 기업이 이러한 공격을 통해 고객의 개인정보가 유출되거나, 이용자가 서비스를 정상적으로 이용하는 것이 불가능해지는 것 등과 같은 막대한 피해를 입을 수 있다. 다만, 기업의 관점이 아닌 개인의 측면에서도 MAC 주소와 같은 고유 식별 번호에 대한 관리에 유의해야 할 필요가 있다. 최근 카페와 같은 편의 시설뿐만 아니라 공공장소에서도 Wi-Fi 설치가 확대되면서 인터넷을 어디에서나 이용할 수 있게 되었다. 공격자는 개방되어 있는 공유기를 대상으로 악의적인 목적을 지니고 ARP(Address Resolution Protocol) Spoofing과 같은 공격을 진행할 수 있는 가능성이 있다. 공격자는 다수의 인원이 사용하고 있는 Wi-Fi에 접근하여 자신이 공유기인 것처럼 사칭할 수 있고 일반 사용자들은 이를 눈치채기 쉽지 않으며, Wi-Fi를 이용하고 있는 동안 이용자들이 접근하고 있는 데이터, 사이트 정보, 개인정보 등을 공격자는 무단으로 탈취할 수 있는 위험이 존재한다.

V. 대응 방안

도출된 해외 애플리케이션의 문제점을 해결하기 위해 수행 관점에서 애플리케이션 제공자, 애플리케이션 이용자, 입법 및 집행기관으로 구분하였으며 각각에 대해 대응 방안을 제시하고자 한다.

5.1 애플리케이션 제공자 측면

애플리케이션 공급사에서 애플리케이션의 개인정보처리방침을 공개하는 절차를 운영하는 방식의 개선이 이루어질 수 있다. 예를 들어, 애플리케이션을 공급하는 단계에서 애플리케이션이 수집하는 개인정보를 목적과 속성에 따라 구분하여 다운로드 페이지에 기재한 후, 이용자가 애플리케이션을 내려받기 이전에 이를 쉽게 확인하게 할 수 있다. 애플의 애플리케이션 스토어의 경우, 실제로 2020년 12월부터 자사 애플리케이션 스토어에 애플리케이션을 등록하려는 개발사가 애플리케이션이 수집하는 개인정보처리방침에 대한 정보를 함께 제출하도록 하는 방식으로 이와 같은 서비스를 제공하고 있다. 이는 개인정보처리방침의 내용을 더욱더 접근하기 쉬운 곳에 노출시키는 것뿐만 아니라, 이용자가 개인정보 수집 목적과 종류 등의 정보를 더 명확하게 알고 애플리케이션을 내려받을 것인지에 대해 선택할 수 있도록 한다. 또한 이때 애플리케이션 공급사가 개인정보처리방침의 내용이 적절한지에 대해 검수하여 애플리케이션의 등록을 허용 및 거부하는 방법으로 공급하는 애플리케이션을 관리할 수 있다.

5.2 애플리케이션 이용자 측면

5.2.1 최신 버전의 시스템 이용

애플리케이션 이용자는 자신의 개인정보를 보호할 수 있도록 기능을 업데이트하여 시스템을 최신화해야 한다. OS는 MAC 주소, IMEI와 같이 일반적으로 서비스 제공을 위해 필수적이지 않은 개인정보를 애플리케이션 차원에서 수집을 시도할 때 접근할 수 없도록 한다. 안드로이드 OS의 경우 Android 10부터 MAC 주소, IMEI와 같이 애플리케이션 이용자가 재설정할 수 없는 식별자를 읽는 함수의 사용을 제한하여 특별 권한을 가지지 않은 애플리케이션이 해당 함수를 사용할 수 없도록 조치하였으므로 애플리케이션 이용자는 OS 버전을 업데이트하여 개인정보 무단 유출을 방지하도록 한다.

5.2.2 모니터링 및 알람 기능 이용

애플리케이션 이용자는 애플리케이션이 이용자 데이터에 접근할 권한을 요청할 때 이를 이용자가 인지하고, 선별적으로 동의하여야 한다. OS에서는 애플리케이션의 활동을 모니터링하여 애플리케이션이 특정한 권한을 요청하거나 사용할 때, 애플리케이션 이용자에게 팝업 또는 특정한 표시 등으로 해당 사실을 알릴 수 있다. 이를 통해 불필요하거나 과도한 접근이 발생할 경우 애플리케이션 이용자가 이를 인지하

고 알람 기능을 즉각적으로 활성화할 수 있다.

5.3 입법 및 집행기관 측면

입법 및 집행기관은 정보주체의 동의를 받지 않고 개인정보를 제 3자에게 제공하는 등의 위반 행위에 대해서 과징금을 부과하고, 위반행위 주체인 기업 및 사업자를 수사기관에 고발하는 법안을 입법할 수 있다. 그리고 개인정보 암호화 조치 위반 및 이용내용 통지 위반, 거짓 자료 제출 등의 위반 행위에 대해서도 과징금을 부과하는 법안도 고려할 수 있다. 법규에 명시된 과징금에 대해서는, 최대 금액을 상향 조정하여 이러한 위반행위가 재발하는 것을 방지하는 등의 개정안도 제시될 수 있다.

또한, 모바일 서비스 환경에 따른 개인정보 침해 논란이 증가하자, 미국 국회에서는 2014년 위치사생활 보호법을 통과하여 시행하고 있다[21]. 이처럼, 국내에서 서비스되는 해외 애플리케이션에서 개인정보 무단 수집 문제가 발생할 경우, 이를 제재하기 위한 모바일 개인정보 관련 법안의 입법을 고려할 수 있다.

VI. 결 론

국내에서 서비스되는 해외 애플리케이션의 사용이 빠르게 늘어나고 있지만, 이러한 서비스에 대한 보안 측면의 우려도 그만큼 증가하고 있다. 특히, 국내에서 서비스되는 해외 애플리케이션에서 국내 개인정보 수집 관련 법규를 위반하여 이용자의 정보를 무단으로 수집하는 등의 사례가 늘어나고 있다.

이러한 문제는 법적인 대응이 확실하게 이루어지지 않았던 것은 물론 기술적 보안 문제에 대해 선제적인 실증 분석이 이루어지지 않았기 때문에 본 논문에서는 해당 부분에 대한 분석을 진행하였고, 결과적으로 개인정보가 무단으로 수집되는 문제가 존재한다는 것을 밝혀내었다. 또한, 국내 기업에 의해 서비스되는 애플리케이션과는 달리 법적 제재가 정상적으로 이루어지지 않는 해외 애플리케이션에 대해, 이들의 위반 행위를 처벌할 수 있는 법적 근거가 부족한 것을 확인하였다.

본 연구에서는 앱 분석 대상이 안드로이드 애플리케이션에 국한되어 iOS 애플리케이션에 대한 분석은 진행되지 않았고, 전체적으로 분석 환경이 모바일에 집중되었다. 또한, 미국의 위치사생활 보호법의 사례를 제시하였으나, 실행 효과에 대해서는 확인하지 못하였다. 추후 연구에서는 기술적으로 분석 환경을 iOS 및 웹 서비스와 같은 다양한 환경으로 확대하고, 법적으로는 국내외 위치정보 관련 법을 추가적으로 분석하여 지속적인 연구를 수행하고자 한다.

References

[1] Gallup, "2012-2020 Smartphone Usage Rate & Brand," https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1134, May. 2021.

[2] IT Chosun, "[If Smartphones are pierced, they will all be pierced] ① There's me on my phone that I don't even know," http://it.chosun.com/site/data/html_dir/2020/01/20/2020012003210.html, May. 2021.

[3] Penetrum, "Penetrum Security Analysis of Tiktok version 10.0.8-15.2.3," Available: https://penetrum.com/tiktok/Penetrum_TikTok_Security_Analysis_whitepaper.pdf, May. 2021.

[4] THE WALL STREET JOURNAL, "TikTok Tracked User Data Using Tactic Banned by Google," https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-1159 7176738, May. 2021.

[5] Maeil Economic Daily, "Alleged leakage of personal information and unauthorized use of global IT that kept domestic laws," https://www.mk.co.kr/news/economy/view/2018/12/802153, May. 2021.

[6] Sung-jin Kim and Jun-beom Hur, "Mobile Application Privacy Leak Detection and Security Enhancement Research," Journal of the Korea Institute of Information Security & Cryptology, 29(1), pp. 195-203, Feb. 2019.

[7] Hak-soo Ko et al, "Collection of User Data through Mobile Devices in South Korea using ADID: Current Status and Legal Implications," Korean Legal Center, the

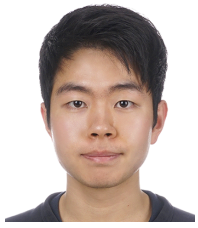
Justice, (180), pp. 442-486, Oct. 2020.
[8] Cheol-won Lee et al, "Information and Communication Network Vulnerability Analysis," Journal of the Korea Institute of Information Security & Cryptology, 19(5), pp. 16-23, Oct. 2003.
[9] Forbes, "TikTok: Why The Enormous Success?," https://www.forbes.com/sites/tomtaulli/2020/01/31/tiktok-why-the-enormous-success/?sh=3e20886565d1, May. 2021.
[10] Yonhapnews, "The app that Koreans use the most is YouTube...20% more usage than last year," https://www.yna.co.kr/view/AKR20201103041600017, May. 2021.
[11] THE WALL STREET JOURNAL, "TikTok Tracked User Data Using Tactic Banned by Google," https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738, May. 2021.
[12] The Indian EXPRESS, "AliExpress to TikTok to PUBG Mobile: Check out full list of Chinese apps banned in India so far," https://indianexpress.com/article/technology/tech-news-technology/aliexpress-to-tiktok-to-pubg-mobile-full-list-of-all-chinese-apps-banned-in-india-so-far-7064134/, May. 2021.
[13] IT Chosun, "60% of smartphone apps such as Facebook and Line violate laws such as location information law," http://it.chosun.com/site/data/html_dir/2017/10/13/2017101385040.html, May. 2021.
[14] Korea Policy Briefing, "Corrective measures were taken against violations of laws related to personal information protection," https://www.korea.kr/news/policyNewsView.do?newsId=156423138, May. 2021.
[15] Boannews, "Court found Itomato guilty of collecting personal information without permission," https://www.boannews.com/media/view.asp?idx=24992, May. 2021.
[16] ABC news, "TikTok ban 'not necessary' but Prime Minister Scott Morrison urges caution over app's China connection," https://www.abc.net.au/news/2020-08-05/prime-minister-scott-morrison-says-government-wont-ban-tiktok/12526246, May. 2021.
[17] ABC news, "It's time to talk about TikTok and what it's doing with our kids' data," https://www.abc.net.au/news/2020-02-19/should-we-trust-chinese-owned-tiktok-personal-data/11962086, May. 2021.
[18] JoongAng Ilbo, "The opening of 1184 cloned phones under the name of basic living beneficiaries is 1.7 billion won," https://news.joins.com/article/20936278, May. 2021.
[19] SC media, "Italian RAT targets Android devices in China by IMEI codes," https://www.scmagazine.com/home/security-news/italian-rat-targets-android-devices-in-china-by-imei-codes/, May. 2021.
[20] Boannews, "[UPDATE] What caused Asiana Airlines 'homepage hacking? DNS attack or ARP spoofing?," https://citation.sawoo.com/qna/item/48, May. 2021.
[21] Davis Wright Tremaine LLP, "Updated Location Privacy Protection Act Introduced," https://www.dwt.com/blogs/privacy-security-law-blog/2014/04/updated-location-privacy-protection-act-introduced, May. 2021.

〈저자소개〉

김 세 환 (Se-hwan Kim) 학생회원
2016년 3월~현재 : 경일대학교 사이버보안학과 학사과정
〈관심분야〉 정보보안, 개인정보보호, 보안컨설팅, 금융보안

윤 형 준 (Hyung-jun Yun) 정회원
2021년 2월: 경기과학기술대학교 전자통신공학과 졸업
〈관심분야〉 정보보호, 개인정보보호, 보안컨설팅, 사이버안보, 정보보호정책

정 다 현 (Da-hyun Jung) 학생회원
2019년 3월~현재: 세종대학교 정보보호학과 학사과정
〈관심분야〉 정보보호, 인공지능, 사이버보안



장 승 훈 (Seung-hoon Jang) 학생회원
2015년 3월~현재: 한국교원대학교 컴퓨터교육과 학사과정
〈관심분야〉 정보보호, 디지털 윤리, 사이버보안, 인공지능

한 철 규 (Cheol-kyu Han) 정회원
1992년 2월: 한양대 산업공학과 졸업
2014년 2월: 서울과학기술대학교 NID융합대학원 정보통신미디어공학 석사
2019년 3월~현재: 중앙대학교 융합보안학과 박사 수료
2000년 1월~현재: LG CNS 사이버시큐리티팀 총괄 PM
〈관심분야〉 보안컨설팅, 융합보안, 보안SI, 정보보안 교육, 인공지능