Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.195

모바일 어플리케이션 개인정보 유출탐지 및 보안강화 연구

김 성 진,† 허 준 범‡
고려대학교

Mobile Application Privacy Leak Detection and Security Enhancement Research

Sungjin Kim,† Junbeom Hur‡
Korea University

요 약

구글 플레이 스토어와 애플 앱 스토어 등 모바일 앱 스토어는 금융, 쇼핑, 엔터테인먼트 등 다양한 카테고리로 영역을 확장하고 있으며, 등록되어 있는 어플리케이션(이하 앱)만 수백만 개에 이른다. 하지만 휴대성과 편리성을 제공하는 모바일 앱의 보안 취약점으로 인해서 최근 모바일 앱을 통한 개인정보 및 데이터 유출이 급격히 증가되고 있는 상황이다. 본 논문에서는 국내 최대 규모의 사용자가 사용하는 상용 모바일 앱을 카테고리별로 분류하고, 사용자가 각 카테고리 별 모바일 앱을 사용하는 경우 유출될 수 있는 개인정보를 분석한다. 분석 결과 해당 앱들을 통해서 실시간으로 개인정보가 유출될 수 있음을 증명하고, 모바일 앱 사용자의 개인정보 유출방지와 안전한 사용을 위한 보안강화 방안을 제안한다.

ABSTRACT

Mobile applications stores such as Google Play Store and Apple App Store, are widely used to distribute a variety of applications including finance, shopping, and entertainment. Recently, however, vulnerabilities of the mobile applications are likely to violate users' privacy such as personal information leakage. In this paper, we classify mobile applications that can be download from mobile stores, and analyze the personal information that could be leaked when users are using the mobile applications. As a result of analysis, we found that personal information are leaked in some widely used mobile applications in practice. On the basis of our experiment results, we propose some mitigations to enhance security of the mobile applications and prevent leakage of personal information.

Keywords: Mobile Application, Personal Information Leakage, Privacy, Security

I. 서 론

모바일 어플리케이션(이하 앱)이 출시된 이후 금융, 쇼핑, 여행, 엔터테인먼트 등 다양한 카테고리로 영역을 확장해가고 있다. 올해로 10주년을 맞은 구글 플레이 스토어와 애플 앱 스토어에 등록되어 있는 앱은 2018년 6, 7월 기준으로 각각 330만개[1], 245만개[2]를 돌파하고 있다. 편의성이 높은 모바일 앱은 비즈니스 뿐 아니라 일상생활 등 모든 분야에서 활용되고 있는 실정이다.

하지만 최근 산업별 오픈소스에 대한 보안리스크 발표[3]에 의하면, 심각한 보안 취약점을 포함하는

Received(12. 06. 2018), Modified(01. 15. 2019), Accepted(01. 17. 2019)
† 주저자, kinet18@korea.ac.kr
‡ 교신저자, jbhur@korea.ac.kr(Corresponding author)

어플리케이션 비율이 가장 높은 산업군은 인터넷 & 소프트웨어 기반 시설(67%) 이었으며, 인터넷 & 모바일 어플리케이션 산업(60%)이 뒤를 이었다. 휴대성과 편리성을 제공해주는 모바일 앱의 사용으로 인한 개인정보 유출로 프라이버시 침해, 금전적 손실, 명의도용 등 심각한 문제로 대두되고 있다.

이에 본 논문에서는 100만명 이상 사용하는 최대 규모의 상용 모바일 앱을 카테고리 별로 분류하여 선정하였다. 그리고 스마트폰 사용자가 모바일 앱을 사용하는 동안 제 3자가 데이터 패킷을 스니핑(sniffing)하여 실시간으로 사생활 개인정보 데이터 패킷이 유출됨을 증명하고자 한다. 즉, 모바일 앱 데이터 패킷 분석을 통해 개인정보 유출의 심각성을 살펴보고, 분석 결과를 바탕으로 가장 효과적인 보안강화 대응방안을 제안함으로써 개인정보 유출을 방지하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존의 모바일 앱 개인정보 유출 및 취약점 분석에 관한 관련 연구들에 대해 소개한다. Ⅲ장은 앱 분석 환경 및 개인정보 유출탐지 Risk별 분석을 수행하고, Ⅳ장은 앞선 Ⅲ장 문제에 관한 보안강화 방안에 대해서 논의하며, 마지막으로 Ⅴ장에서는 결론 및 향후 연구에 대해 기술한다.

Ⅱ. 관련 연구

기존 모바일 앱에 대한 취약점과 개인정보 유출에 대한 연구는 다양하게 진행되고 있다. 대부분의 연구는 모바일 앱의 소프트웨어 라이브러리 및 소스코드에 대한 취약점과 앱 사용으로 인한 스마트폰 정보에 대한 유출 관련 연구가 다수 발표되었다.

모바일 앱 소프트웨어 라이브러리 취약점의 주요 연구를 살펴보면, Android에서 30,000 개 무료 및 유료 앱을 수집하여 광범위하게 취약점 연구를 진행하였다[4]. 이 연구에서는 60 % 이상의 안드로이드 어플리케이션이 타사 라이브러리에 비롯됨을 기반으로 취약점을 분석하였다. 분석한 결과 무료앱의 70%, 유료앱 50%는 소프트웨어에서 취약점이 발생하였고, 비싸고 인기 있는 유료앱이 더 많은 취약점이 있다는 것을 발견하였다. 라이브러리 출처와 소프트웨어 업데이트 빈도는 취약점 특성에 영향을 주었다. 가장 큰 취약점 중 하나는 SSL/TLS의 미숙한 구현이 암호화 통신을 안전하지 못하게 하여 심각한 위험을 초래할 수 있다고 주장하였다. 또 다른 연구로는 안드로이드 모바일 앱에서 사용한 자바스크립트 소스코드 관련 취약점을 발견하였다[5]. JSDroid라는 자동 도구를 설계 및 구현하여 1000개의 안드로이드 앱에서 70%이상 자바스크립트 잠재적 취약점을 발견하였고, 실제 공격을 통한 결과 값을 발표하였다.

스마트폰 정보 유출에 관한 연구를 살펴보면, 모바일 앱 설치 및 사용 중에 제 3자가 중간자공격(MITM)을 통해 스마트폰에 등록된 정보가 유출되는 연구를 진행하였다[6]. 유출된 정보는 앱에 등록된 정보가 아닌 앱 사용으로 인해 스마트폰 정보(IMEI/IMSI, Location, Email, Username, Password, Contact, Mac Address, UDID/UUID, MCC/MNC)등 개인 고유 식별자 정보가 유출되었다. 이와 유사한 연구에서는 MobileAppScrutinator 플랫폼을 통하여 안드로이드와 iOS 상에서 140개의 무료 및 인기앱을 분석해본 결과, 개인 식별정보(WiFi, MAC address, AndoridID, IMEI)등 유출이 확인되었다[7].

국내 논문에서도 APK를 추출하여 정적·동적분석을 통한 모바일 앱의 취약점에 대한 연구[8][9]가 다수 발표 되었지만, 개인 사생활에 큰 문제가 될 수 있는 개인정보 데이터 유출은 확인하지 못했다.

하지만 본 논문에서는 기존연구를 토대로 소스코드 결함 및 완전하지 않은 암호화 구현으로 인한 개인정보 유출을 증명하였다. 기존 연구에서는 발견되지 않았지만, 유출시 큰 문제가 될 수 있는 개인 주소지, 방문한 프렌차이즈 가맹점 및 이용지역, 연락처에 등록된 모든 이름과 전화번호 목록 등의 유출로 제3자에게도 큰 피해를 유발할 수 있는 앱의 취약성을 살펴본다. 또한 모바일 앱의 안전한 사용을 위한 보안강화 방안을 제안함으로써 개인정보 유출을 막고자 한다.

Ⅲ. 모바일 앱 개인정보 유출분석

본 연구에서는 100만명 이상 이용하는 모바일 앱을 카테고리별로 총 4개 앱(스포츠, 포인트, 배달, 도서)을 분류하고, 제 3자에게 개인정보 데이터가 유출되는 Risk순으로 정리하였다. 4개의 모바일 앱 대상으로 개인정보 유출 유형과 특징을 분석하였고, 분석 대상은 Table 1과 같다.

Table 1. Target for mobile app analytics

APP Type	Platform	Installations
G application	Sports	1,000,000
H application	Point	5,000,000
M application	Delivery	1,000,000
K application	Book	1,000,000

3.1 앱 분석 환경

노트북의 무선 랜카드를 이용한 무선AP(Wi-Fi)를 생성해주고, 스마트폰은 노트북 무선AP를 연결하였다. 스마트폰 사용자가 모바일 앱을 사용하는 동안 노트북(제3자)을 통해 지나가는 무선 패킷을 스니핑(sniffing)하여 분석하였다.

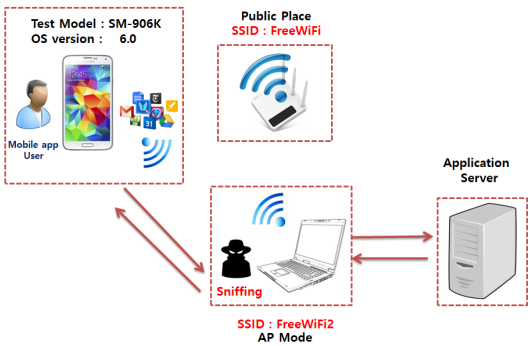

Fig. 1. Smartphone application data packet sniffing environment

3.2 High Risk 앱 분석

제3자에게 개인정보 데이터 패킷이 유출되는 High Risk 앱으로 G앱을 선정하였다. G앱은 국내에서 대표적인 스포츠 앱으로 이용자 수가 100만명 이상이고, 전국 매장에서 활용되어 많은 매니아층을 보유한 앱이다.

첫 번째로 G앱의 분석을 위해 아래 Fig. 2과 같이 스마트폰 상의 툴을 이용하여 IP를 확인하고, 앱 상에서 개인정보 프로필을 실행하였다. Fig. 3, 4와 같이 제3자(노트북)에서 단말기 모델명과 OS버전, 개인정보 프로필 정보(계정, 닉네임, 상태메시지)가 암호화 되지 않는 상태에서 유출됨을 알 수 있었고, 회원정보 수정을 위해 이용한 기능에서 패스워드가 노출됨을 탐지하였다. 이는 G앱 상에서 현금처럼 사용하는 마일리지 유출로 인해 금전적 손실이 이어질

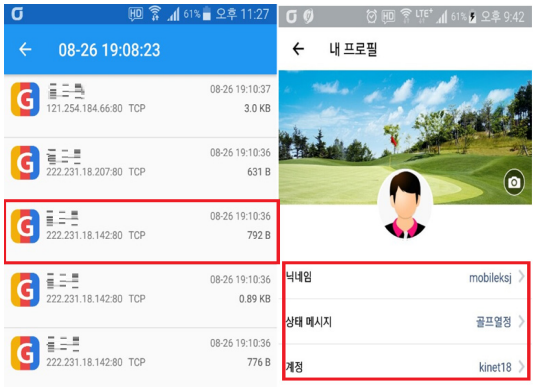

Fig. 2. G application IP verification and personal profile

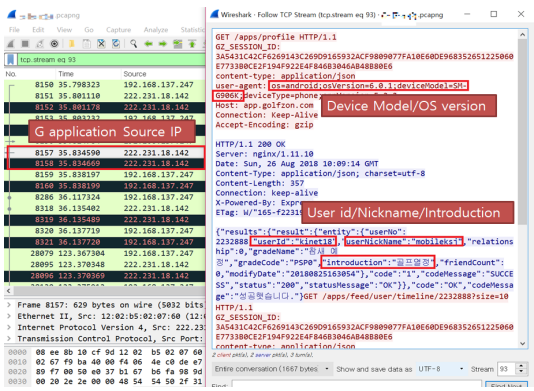

Fig. 3. G application personal information leak data packet(1)

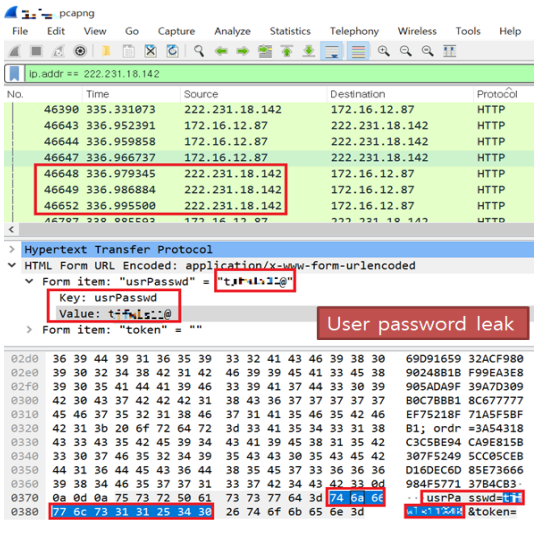

Fig. 4. G application personal information leak data packet(2)

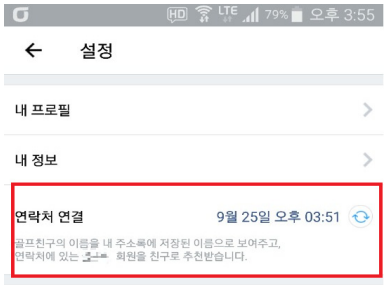

Fig. 5. G application personal information leak data packet(3)

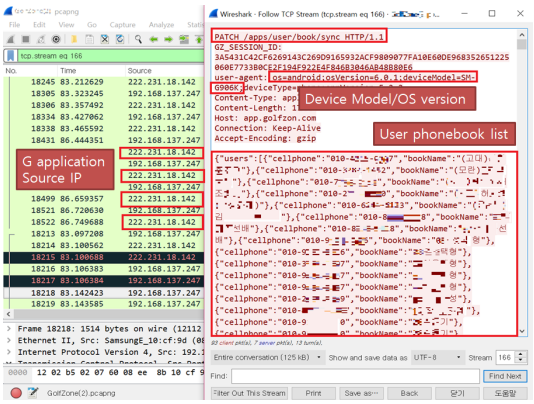

Fig. 6. G application personal information leak data packet(4)

수 있고, 스마트폰 사용자가 다른 앱에서 사용하는 아이디와 패스워드가 동일한 경우가 많기 때문에 패스워드 재사용 공격[10]에 취약하다.

두 번째로 G앱의 가장 큰 개인정보 유출의 문제점은 앱 상의 '연락처 연결' 기능이다. 스마트폰에 저장되어 있는 연락처 인원들과 G앱을 함께 이용할 수 있는 편리한 기능인데, 이 기능으로 인해 저장되어 있는 이름과 연락처가 모두 제3자(노트북)으로 유출됨을 Fig. 6과 같이 탐지하였다. 이는 제 3자에게 유출될 뿐 아니라, 사용자의 저장된 연락처가 G앱 서버로 모두 전송되는 큰 문제점을 가지고 있다.

3.3 Middle Risk 앱 분석

개인정보 데이터 패킷이 유출되는 Middle Risk 앱으로 대표적인 포인트앱과 배달앱이 있다. 이용자 수가 500만명 이상되는 H앱과 100만명 이상 이용하는 M앱을 선정하여 분석을 실시하였다.

3.3.1 H앱 개인정보 유출사례

H앱을 앞선 방식으로 분석해본 결과, Fig. 8에 나타나는 바 같이 단말기 모델명과 OS버전, 사용자 아이디가 유출됨을 탐지할 수 있었다. Fig. 9의 같은 경우, H앱 카드번호와 사용하는 지역과 매장명, 사용일자의 유출로 제3자에게 이동경로가 노출되어 사생활의 큰 문제로 이어질 수 있다.

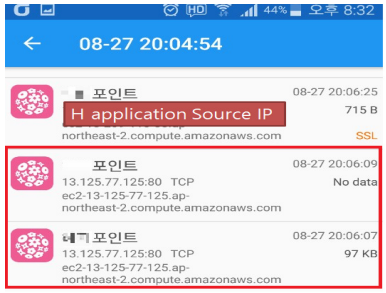

Fig. 7. H application source IP verification

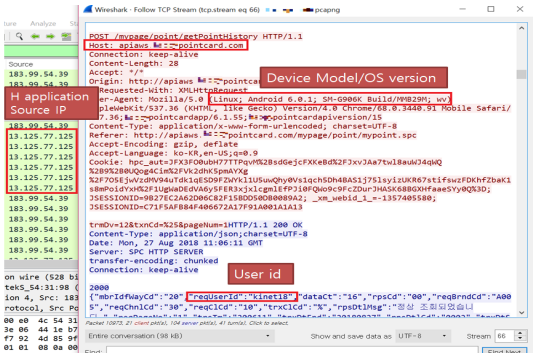

Fig. 8. H application personal information leak data packet(1)

Fig. 9. H application personal information leak data packet(2)

3.3.2 M앱 개인정보 유출사례

M앱을 분석해본 결과, Fig. 10을 살펴보면 단말기 모델명과 OS버전, M앱 상에 등록해놓은 배달집 주소가 유출됨을 알 수 있다. 앱 사용자의 거주지 개인정보 유출로 프라이버시 침해와 범죄에 악용될 수 있는 심각한 문제로 확인된다.

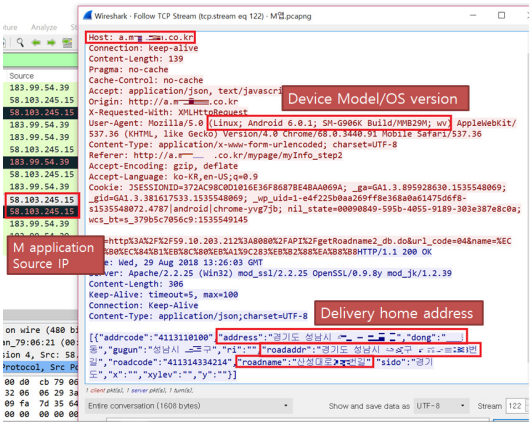

Fig. 10. M application personal information leak data packet

3.4 Low Risk 앱 분석

개인정보 데이터 패킷이 유출되는 Low Risk 앱으로 K앱을 선정하였다. 대표적인 도서앱으로 이용자 수가 100만명 이상이고, 전국 매장에서 이용되는 앱이다. Fig. 11을 살펴보면 단말기 모델명과 OS버전, 사용 아이디, K앱 상에서 클릭하는 도서리스트와 URL 정보가 실시간 유출되어 개인 프라이버시에 문제가 될 수 있다.

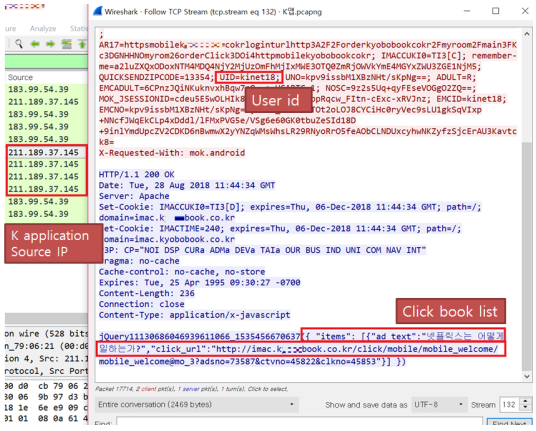

Fig. 11. K application personal information leak data packet

3.5 Risk별 모바일 앱 비교분석

Table 2은 제 3자에게 개인정보 데이터가 유출되었던 모바일 앱을 Risk별로 분류하여 아래와 같이 정리하였다.

Table 2. Mobile application analysis by risk

Risk Type	App Type	Leak Data
High	G application	Device Model, OS version, User id, password, Nickname, introduction, User phone book list
Middle	H application	Device Model, OS version, Point card number, Brand name location, Purchase date
	M application	Device Model, OS version, Delivery home address
Low	K application	Device Model, OS version, User id, Click book list

IV. 보안강화 방안

모바일 앱 사용으로 인한 개인 사생활 정보가 제3자에게 유출되는 심각성을 증명하였다. 본 논문에서는 모바일 앱의 안전한 사용과 개인 유출을 방지하기 위한 보안강화를 위한 3가지 방안을 제안한다.

4.1 SSL/TLS

4.1.1 소개

SSL/TLS는 웹사이트와 모바일 어플리케이션(이

하 앱)에서 가장 널리 사용되고 있는 보안 서비스로 미국 Netscape사가 웹 브라우저와 웹 서버 간의 암호화된 정보 송수신을 위해 개발한 프로토콜을 말한다. 서버와 클라이언트의 진위여부를 조사하여 사이버 공간에서의 정보전달을 안전하게 만드는 역할을 하는 통신규약이며, HTTP뿐 만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 계층의 모바일 앱에서도 적용이 가능하다는 장점을 지니고 있다. 최초 SSL(Secure Sockets Layer) 1.0 버전은 공개되지 않고, SSL 2.0은 1995년, SSL 3.0은 1996년에 발표되었다. 1999년 SSL 3.1에 해당되는 공식 표준인 TLS(Transport Layer Security) 1.0이 발표된다. 2006년에 TLS 1.1이 공개되고, 2008년 발표된 TLS.1.2는 RFC 5246 표준 규약으로 정의되고 있다. 그리고 총 4년에 걸쳐 28개의 초안들이 마련되고, 10년만인 2018년 8월 TLS 1.3 최종버전이 공식발표 되었다[11].

모바일 앱 개발자들이 암호화 프로토콜 적용을 기피하는 큰 이유는 앱의 실행속도 저하이다. 하지만 최근에 발표된 TLS 1.3 암호화 프로토콜은 이전버전보다 실행속도와 보안이 강화되었다[12].

첫 번째, 보안강화를 살펴보면 Handshake 과정부터 암호화를 수행하여 연결과정에서 노출될 수 있는 중요 정보를 보호한다. 또한 사용되고 있는 알고리즘 중 심각한 취약점이 발견된 MD5, SHA-1, DES, RC4, 3DES, AES-CBC 및 RSA 등을 제거하고 지원 Cipher Suites를 축소하여 보안을 강화하였다.

두 번째, 암호화 연결 속도향상을 살펴보면 TLS 1.2 버전은 Handshake를 완료하기 위해 두 번의 왕복이 필요했지만, TLS 1.3버전에서는 단일 왕복으로 대기시간이 단축되어 수백 밀리 초를 절약한다. 또한, Zero-Round-Trip(0-RTT) 기능을 통해 동일서버에 연결된 경우 Handshake의 연결속도가 한층 높아졌다.

4.1.2 최신버전 TLS 모바일 앱 적용

모바일 앱의 보안강화에 가장 효과적인 방안은 앞서 소개했던, 최신버전 TLS(Transport Layer Security) 암호화 프로토콜 적용이다. 하지만, 하위버전 SSL/TLS 적용은 이전에 많은 연구를 통해 취약점[13]이 발견되었다. 2018년 8월 기준으로 2016년도 DROWN 공격과 2014년 POODLE 공격에 치명적이었던 SSL 3.0 이하버전 사용을 전체의 10%가 Fig. 12과 같이 지원하고 있는 상황이다[14]. 따라서 보안 강화를 위해 낮은버전의 SSL 프로토콜 지원을 중단해야 한다. 또한 모바일 앱 개발 시, HSTS(HTTP Strict Transport Security) 적용[15]을 의무화하여 모든 앱의 인터넷 통신에서 암호화된 HTTPS(HTTP over SSL/TLS) 연결을 사용하도록 강제해야 한다. 구글과 애플 등 글로벌 기업들도 최신 암호화 프로토콜 설정을 의무화하며 암호화 트래픽 확산을 추진하고 있다.

앞서 소개하였던 TLS 1.3 버전이 모바일 앱에 적용된 사례를 살펴보면, Handshake 연결과정이 간소화 된 것을 Fig. 13와 같이 확인 할 수 있다.

최근 페이스북은 TLS 1.3 암호화 프로토콜 도입을 위해 피즈(Fizz)라는 라이브러리를 개발하여 적용하였다. 피즈란, C++14로 작성된 라이브러리로 수백만 건의 Handshake를 처리하고 암호화 알고리즘 및 메모리 및 CPU 사용량을 줄여 성능을 최적화 하였다. 페이스북 모바일 앱에는 앞서 살펴보았던, Zero-Round-Trip(0-RTT) 기능이 적용되어

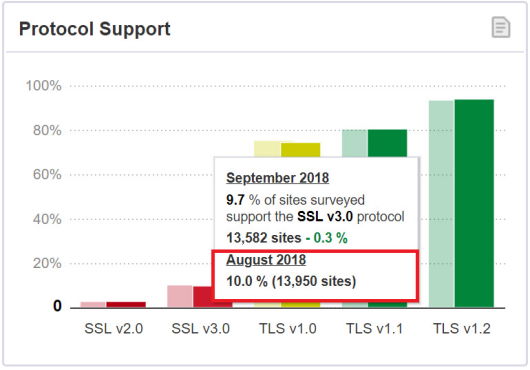

Fig. 12. SSL/TLS protocol support status

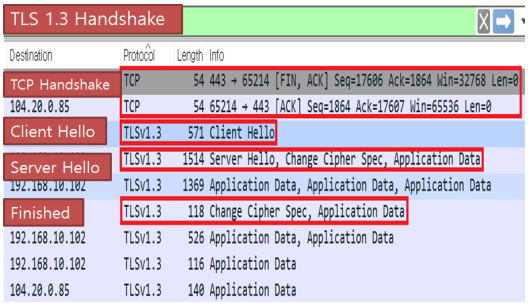

Fig. 13. TLS 1.3 connecting process

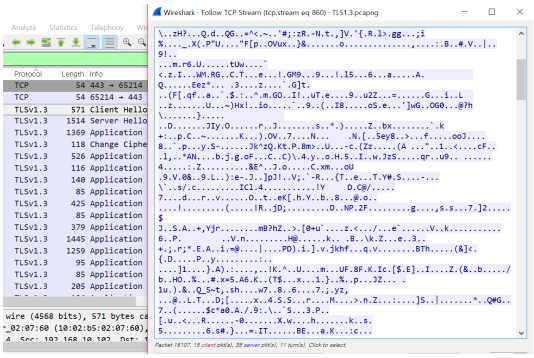

Fig. 14. Applying mobile application TLS 1.3

지연 속도를 낮추어 시스템 효율을 높였을 뿐 아니라 앱 사용자의 환경이 개선되었다. 페이스북은 피즈를 통해 TLS 1.3을 도입했을 때, TLS 1.2때보다 약 10% 높아진 처리량을 보여주며 성능을 지속적으로 개선하고 있다[16].

또한 모바일 앱에 최신버전 TLS 암호화 프로토콜이 적용 되었을 경우, Fig. 14와 같이 서버와 클라이언트 간의 암호화 통신이 이루어지기 때문에 제3자가 패킷을 스니핑 하여도 개인정보 데이터를 확인할 수 없다.

4.2 제도적 문제 및 개선방향

현재 시행되고 있는 방송통신위원회 「개인정보 기술적·관리적 보호조치 기준」에 의하면 "제6조(개인정보의 암호화) 1번 웹 서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화 하여 송/수신하는 기능을 갖추어야 한다."로 고시되어 있다[17]. 하지만 앞서 살펴본 것 같이 하위버전 SSL/TLS 적용은 많은 취약점을 가지고 있기 때문에, SSL 인증서 설치 문구를 최신버전 TLS(Transport Layer Security)으로 개정되어야 한다.

4.3 모바일 앱 사용자 유의사항

개인정보 유출방지와 보안강화를 위한 여러 가지 방안들이 제안되었지만, 스마트폰 모바일 앱 사용자도 아래와 같은 3가지 유의사항을 지켜야 한다.

첫째, 스마트폰 사용자는 단말기의 최신 안드로이드 OS버전 업데이트가 필요하다. 낮은 안드로이드 버전의 사용자는 악성코드 감염 및 해킹에 취약[18]하기 때문에 보안패치가 포함되는 안드로이드 OS버전 업데이트는 의무적이다.

둘째, 스마트폰 사용 시 공공장소 무료와이파이 사용에는 각별한 주의가 필요하며, 제공자가 불분명한 무선 공유기는 사용을 금지해야 한다. 앞서 모바일 앱 분석에서 살펴보았듯이 공유기는 전파를 전송매체로 사용하기 때문에 패킷이 다른 통신기기에도 수신 될 수 있다. 또한 해킹 당한 공유기를 이용할 경우 단말기의 사용자 데이터가 제 3자에게 노출 될 수밖에 없다[19]. 따라서 공공장소에서는 데이터 네트워크(LTE 및 3G) 사용을 권장하는 바이다.

셋째, 백신 앱을 설치하고 의심 가는 URL은 클릭하지 말아야 한다. Table 2와 같이 모바일 앱의 대부분은 제 3자에게 단말기 모델명과 OS버전이 유출된다. 매월 OS버전별로 취약점 버그리포트[20]가 실시간으로 업데이트 되기 때문에 해당 취약점에 맞는 악성코드를 심을 수 있다. 따라서 의심 가는 URL을 주의하여 해킹의 위협을 줄여야 한다.

V. 결론 및 향후 연구

본 연구는 국내 최대 규모의 사용자가 사용하는 상용 모바일 앱을 카테고리 별로 분류하였고, 사용자가 앱을 사용하는 동안 유출될 수 있는 사생활 개인정보를 Risk별로 분류하여 비교 분석하였다.

연구 결과, 모바일 앱 사용만으로 제 3자에게 개인 프라이버시 정보와 연락처에 등록된 모든 정보가 유출됨을 확인하였다. 이는 보이스피싱, 프라이버시 침해, 금전적 손실, 범죄의 표적이 될 수도 있는 잠재적인 문제를 가지고 있다.

본 연구를 통하여 모바일 앱 사용자의 개인정보 유출방지와 안전한 사용을 위한 3가지 보안강화 방안을 제안하였다. 앞서 살펴본 바와 같이 모바일 앱에는 최신 암호화 프로토콜 적용이 의무화되어야 하지만 법적 근거가 명확하지 않음을 볼 수 있었다.

따라서 향후 연구를 지속하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「개인정보 기술적·관리적 보호조치 기준」의 상세한 추가조항과 전반적인 개선방안을 제안한다. 또한 모바일 앱 보안강화를 위한 체계적인 기술적·정책적인 방안 수립에 대한 연구를 진행할 계획이다.

References

[1] Number of available applications in the Google Play Store from December 2009 to June 2018, https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[2] Number of available apps in the Apple App Store from 2008 to 2018 (in 1,000s), https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/

[3] Synopsys, "2018 Open Source Security and Risk Analysis Report," Network Security, June. 2018.

[4] T. Watanabe, M. Akiyama, F. Kanei, E. Shioji, Y. Takata, B. Sun, Y. Ishii, T. Shibahara, T. Yagi, and T. Mori, "Understanding the Origins of Mobile App Vulnerabilities: A Large-scale Measurement Study of Free and Paid Apps," In Proceedings of IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), pp. 14-24, July. 2017.

[5] Wei Song, Qingqing Huang, and Jeff Huang, "Understanding JavaScript Vulnerabilities in Large Real-World Android Applications," IEEE Transactions on Dependable and Secure Computing, pp. 1-1, June. 2018.

[6] Timothy A. Chadza, Francisco J. Aparicio-Navarro, Konstantinos G. Kyriakopoulos, Jonathon A. Chambers, "A Look Into the Information Your Smartphone Leaks," 2017 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6, May. 2017.

[7] Jagdish Prasad Achara, Vincent Roca, Claude Castelluccia, and Aurélien Francillon, "Mobileappscrutinator: A simple yet efficient dynamic analysis approach for detecting privacy leaks across mobile OSs," The 32nd Annual Computer Security Applications Conference (ACSAC), 2016.

[8] Sanho-ho Park, Hyeonjin Kim, Taekyoung Kwon, "OnSecurity of Android Smartphone Apps Employing Cryptography", Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 6, Dec. 2013.

[9] Ko Seung Won, Joung Sang Gon, "Implementation example of mobile application analysis and verification solution", Korea Institute of Information Security and Cryptology, Vol. 23, No. 2, pp. 21-28, April. 2013.

[10] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," in ACM SOUPS 2006: Proc. 2nd Symp. on Usable Privacy and Security, pp. 44 - 55, July. 2016.

[11] RFC 8446, "The Transport Layer Security(TLS) Protocol Version 1.3," August. 2018, https://datatracker.ietf.org/doc/rfc8446

[12] K. Bhargavan, B. Blanchet, and N. Kobeissi, "Verified models and reference implementations for the tls 1.3 standard candidate," In IEEE Symposium on Security and Privacy (S&P), May. 2017.

[13] C. Meyer and J. Schwenk, "Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses," IACR Cryptology ePrint Archive, 2013.

[14] Qulays SSL Labs, "SSL Pulse Protocol Support," August. 2018, https://www.ssllabs.com/ssl-pulse

[15] M. Kranch and J. Bonneau. Upgrading HTTPS in midair: HSTS and key pinning in practice. In NDSS

'15: The 2015 Network and Distributed System Security Symposium, February. 2015.
〔16〕 C++14 implementation of the TLS-1.3 standard GitHub, https://github.com/facebookincubator/fizz
〔17〕 Korea Laws, www.law.go.kr/
〔18〕 H. Shewale, S. Patil, V. Deshmukh, and P. Singh, "Analysis of androidvulnerabilities and modern exploitation techniques." ICTACT Journal on Communication Technology, vol. 5, no. 1, 2014.
〔19〕 Reddy, S. Vinjosh, et al. "Wireless hacking-a WiFi hack by cracking WEP," 2010 2nd International Conference on, vol. 1, pp. 189-193, 2010.
〔20〕 Android Secrurity Bullentins - Android Open Source Project, Oct. 2018, https://source. android.com/security/bulletin

〈저자소개〉

김 성 진 (Sungjin Kim) 정회원
2015년 2월: 한국산업기술대학교 전자공학과 졸업
2016년 9월~현재: 고려대학교 컴퓨터정보통신대학원 소프트웨어보안학과 석사과정
〈관심분야〉 개인정보보호, 네트워크 보안

허 준 범 (Junbeom Hur) 종신회원
2001년 2월: 고려대학교 컴퓨터공학 졸업
2005년 8월: 한국과학기술원 전산학 석사
2009년 8월: 한국과학기술원 전산학 박사
2009년 9월~2011년 8월: University of Illinois at Urbana-Champaign 박사후 연구원
2011년 9월~2015년 2월: 중앙대학교 컴퓨터공학부 조교수
2015년 2월~현재: 고려대학교 컴퓨터학과 부교수
〈관심분야〉 클라우드 보안, 빅데이터 보안, 네트워크 보안, 응용 암호학