Journal of KIIT. Vol. 15, No. 11, pp. 23-30, Nov. 30, 2017. pISSN 1598-8619, eISSN 2093-7571 23
http://dx.doi.org/10.14801/jkiit.2017.15.11.23

모바일 환경을 위한 프라이버시 보안 기술

김 희 열*

Security and Privacy Protection for Mobile Environments

Heeyoul Kim*

이 논문은 2015학년도 경기대학교 연구년 수혜로 연구되었음

요 약

최근에는 다양한 모바일 기기가 활발히 사용되고 있으며 사용자에게 새로운 경험을 제공하고 있다. 하지만 모바일 환경에서 사용자의 프라이버시 침해에 대한 우려가 높으며, 모바일 기기의 높은 휴대성과 지속적인 사용, 모바일 에코 시스템의 복잡성으로 인해 위험성이 더 커지고 있다. 모바일 시장을 더욱 확장하고 발전시키기 위해서는 프라이버시에 관한 우려를 해소해야 한다. 본 논문에서는 모바일 환경에서 프라이버시를 위협하는 주요 위험요소를 분석하고, 제안된 보안 정책과 보안 기술에 대한 분석을 토대로 프라이버시 보호 시스템을 제안한다. 이 시스템은 안드로이드 플랫폼을 기반으로 설계되었으며, 사용자는 유연하게 자신의 프라이버시 정책을 설정하고 집행할 수 있게 된다.

Abstract

Recently various mobile devices have been utilized actively and they provide new experiences to users. However, there are concerns regarding the invasion of users' privacy in mobile environments, and the risk is very high due to the high portability and the continuous usage of mobile devices and the complexity of mobile ecosystem. This kind of concerns should be resolved in order to expand and improve the mobile market. In this paper, major security threats against mobile privacy, previous security policies, and current mobile security techniques are analyzed. Moreover, we present a mobile privacy protection system which enables mobile users to configure their privacy policy flexibly and enforces the policy.

Keywords
privacy protection, mobile environments, security, android, security policy

* 경기대학교 컴퓨터과학과
- ORCID: http://orcid.org/0000-0001-6341-580X

· Received: Aug. 14, 2017, Revised: Oct. 11, 2017, Accepted: Oct. 14, 2017
· Corresponding Author: Heeyoul Kim
Dept. of Computer Science, Kyonggi University, 94-6 Iuidong, Yeongtonggu, Suwon, Gyeonggi, 443-760, Korea,
Tel.: +82-31-249-9675, Email: heeyoul.kim@kgu.ac.kr

Ⅰ. 서 론

불과 2000년대 초반까지만 해도 스마트폰과 태블릿이 출현하지 않았고 모바일 기기가 그리 많지 않았지만, 현재는 다양한 형태의 모바일 기기가 언제 어느 곳에서나 활발히 사용되고 있다. 그리고 모바일 기기를 위한 콘텐츠가 폭발적으로 증가해 왔고, 애플의 앱스토어나 구글 플레이에 수십만 개의 모바일 앱이 등록되어 배포되고 있다. 이러한 모바일 환경의 발달은 시장을 확장시켜왔고 사용자에게 새로운 경험을 제공해 왔으며, 모바일 기기는 사용자들 간에 상호 소통하는 방식과 일상생활에서의 활용 방식을 크게 변화시켰다.

하지만, 모바일 환경의 발전은 이와 동시에 사용자의 프라이버시를 위협하는 새로운 위험요소가 되고 있으며, 이는 기존 환경과 다른 차이점이 있다[1]. 우선 모바일 기기는 사용자가 개인적 용도로 많이 사용하며 항상 사용자가 소지하고 있다. 이로 인해 모바일 기기는 사용자의 방대한 개인정보를 수집할 수 있으며, 민감한 정보가 노출될 위험성이 높다. 또한, 복잡한 모바일 에코 시스템으로 인해 수집된 정보가 제조사, 플랫폼 개발사, 앱 개발자 등 다양한 주체들 간에 공유될 가능성이 높으며, 사용자가 자신의 프라이버시를 보호하기 위한 제한 조치의 대상을 파악하기 어려워지는 문제가 생긴다. 그리고 모바일 기기를 통해 사용자의 위치 정보와 과거 이동 경로, 사용 방식 등을 획득하면 사용자에 대한 프로파일링이 가능해지며, 이는 스토킹이나 신원 도용에 활용될 가능성이 높다.

이로 인해 모바일 프라이버시에 대한 관심이 높아지고 있으며, 사용자들은 모바일 환경에서 자신의 프라이버시를 침해할 가능성에 대해 우려하고 있다. 예를 들어, 한 조사에 따르면 사용자의 57%가 프라이버시 우려로 인해 사용중이던 모바일 앱을 삭제하거나 설치를 중지한 경험이 있다는 결과가 알려졌다[2]. 프라이버시에 관한 이런 우려를 해소해야 모바일 시장을 활성화할 수 있을 것으로 여겨진다.

본 논문에서는 모바일 환경에서 사용자의 프라이버시를 적절하게 보호하기 위한 연구 결과를 제공한다. 우선 모바일 환경에서 프라이버시를 위협하는 주요 위험요소를 분석하고, 프라이버시 강화를 위해 제안된 보안 정책과 보안 기술을 분석한다. 그리고 대표적 모바일 플랫폼인 안드로이드에서 프라이버시를 보호하는 시스템을 제안하며, 이 시스템을 통해 사용자는 유연하게 자신의 프라이버시 정책을 설정할 수 있고 모바일 앱을 통한 프라이버시 침해를 방지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 모바일 프라이버시의 주요 위험요소와 안드로이드 플랫폼에 적용된 보안 기술에 대한 분석을 제공한다. 3장에서는 프라이버시 보호를 위해 제안되어온 보안 정책들을 분석하고, 4장에서는 제안하는 프라이버시 보호 시스템의 설계와 구현 방식을 설명한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 모바일 프라이버시 관련 연구

2.1 모바일 프라이버시 위험요소 분석

모바일 에코 시스템은 기존의 PC 기반 에코 시스템보다 다양한 주체들이 참여하고 있으며, 이로 인해 모바일 환경에서의 프라이버시 관련 문제는 기존 PC 환경에서의 문제보다 훨씬 복잡한 형태를 가지게 된다. 또한 모바일 환경에서 수집되는 사용자의 정보도 훨씬 다양하고 정보의 질과 민감도도 매우 높으며, 이는 언제 어디서나 사용자에게 밀착되는 모바일 기기의 특성에 기반한다. 이로 인해 사용자의 프라이버시를 침해하는 위험 요소도 매우 다양해졌으며, 이들이 어디에서 발생했는지 분석하는 것 자체도 매우 어려워졌다.

모바일 에코 시스템을 구성하는 각 주체들의 위험요소는 다음과 같이 분석된다.

- 모바일 플랫폼 제공사

안드로이드, iOS와 같은 모바일 플랫폼은 애플리케이션의 설치, 동작 및 관리를 수행하며, 이를 위한 막강한 권한을 가지고 있다. 특히 모바일 플랫폼은 가이드라인과 요구사항을 통해 앱 개발자들에게 개발 방향을 유도할 수 있으며, 앱스토어와의 인터페이스 역할도 수행한다. 이러한 특성으로 인해 모바일 플랫폼은 사용자 프라이버시를 보호하는 데 있어 가장 중요한 역할을 수행해야 하며, 반대로 제

대로 역할을 수행하지 못할 경우 프라이버시에 큰 위험이 된다.

• 앱 개발자

일반적으로 앱 개발자들은 자신이 개발한 앱을 통해 다양한 사용자 정보를 수집하고 있으며, 앱의 정상적인 기능을 위해 정보가 수집하기도 하지만 때로는 광고나 마케팅을 통한 수익을 위해 불필요한 정보가 수집되기도 한다. 이처럼 모바일 앱은 사용자의 프라이버시를 침해하는 대표적인 1차적 수단이 되고 있으며, 이를 방지하기 위해 앱 개발자는 자신의 정보 수집 정책을 사용자에게 명확히 제공해야 할 의무가 있다.

• 모바일 기기 제조사

삼성전자 등의 모바일 기기 제조사는 모바일 플랫폼 제공사와는 별도로 자사를 위해 사용자 정보를 수집하고 있다. 특히 사용자의 USIM 정보, 사용되는 기기 정보 등이 초기에 기기에 기본적으로 탑재되는 앱을 통해 과도하게 수집되는 경향이 있다. 이러한 앱들은 사용자에 의한 삭제가 불가능하거나 어려운 부분이 있어 프라이버시 침해의 주요 요인이 되며, 또한 제조사에 의해 수집된 정보에 대한 사용 및 공유에 대해서도 불명확한 부분들이 있다.

• 모바일 광고 네트워크

모바일 광고 네트워크는 일반적으로 모바일 앱과 연계되어 사용자의 개인정보를 수집한 후 이를 분석해서 적절한 광고를 제공한다. 이때 수집되는 정보는 사용자의 성향, 위치 정보 등 매우 다양하며, 대규모 사용자들의 정보가 중앙 서버에 수집되어 분석되기 때문에 정보의 악용 가능성이 더욱 높아진다. 또한 여러 모바일 기기를 사용하는 특정 사용자에 대해 연관성 분석을 통해 프라이버시를 침해하는 유형의 위험요소도 가지고 있다.

위에서 분석된 것처럼, 모바일 환경에서 사용자 정보를 수집하고 프라이버시를 침해하는 1차적인 요소는 모바일 앱이다. 그리고 이런 앱들을 관리하는 역할을 하는 모바일 플랫폼이 프라이버시를 보호할 수 있도록 강화되어야 함을 알 수 있다. 또한 위의 다양한 주체들의 위험요소를 줄이고 올바른 방향을 제시하기 위한 정책적인 접근도 필요하다.

2.2 안드로이드 플랫폼 보안 기술 분석

모바일 플랫폼은 설치된 모바일 앱이 정상적으로 동작함을 보장하고 악의적인 행동을 하지 못하도록 제어할 수 있어야 한다. 이를 위해서 모바일 플랫폼들은 다양한 보안 기술을 적용하고 있으며, 대표적인 모바일 플랫폼인 안드로이드에서는 다음의 방식을 사용하고 있다.

안드로이드에서는 설치된 모바일 앱이 정해진 시스템 자원만을 이용하고 지정된 동작만 하도록 제어하기 위해 권한(Permission) 기반의 보안 모델을 사용하고 있다[3]. 모바일 앱은 자신의 안드로이드 매니페스트(Android Manifest) 파일에 필요한 권한을 명시해야 하며, 사용자는 설치 과정에서 권한을 확인하고 승인한다. 이후 모바일 앱의 동작 중에 해당 권한이 필요한 작업이 요청되면 플랫폼은 미리 등록된 권한 목록을 확인한 뒤 작업을 허가한다.

하지만, 권한 기반 모델은 몇 가지 문제점을 가지고 있다. 첫째, 사용자는 앱에서 요구하는 권한들에 대해 선택적으로 승인할 방법이 없으며 전체를 승인하거나 설치를 포기해야 한다. 둘째, 승인된 권한이 어느 시점에 구체적으로 어떻게 사용되는지 확인할 수 없다. 셋째, 모바일 앱이 불필요하게 과도한 권한을 요청하는 것을 억제할 수단이 없다. 이러한 문제점들을 개선하기 위해 다양한 연구가 제안되어 왔으며[4]-[6], 안드로이드 4.3 버전에서는 설치된 앱이 가지는 각각의 권한을 세부적으로 제어할 수 있는 App Ops 기능이 제공되었다. 하지만 이 기능은 4.4.2 버전 이후에 제거되었으며, 구글이 앱을 통한 광고 수입의 저하를 우려해 제거했다는 비판을 받고 있다[7].

프라이버시 보호를 위해서는 앱의 권한 제어와 별개로 사용자가 수립한 보안 정책을 수행할 수 있는 수단이 필요하다. 안드로이드에서는 2.2 버전부터 그림 1과 같이 시스템 전반에 걸쳐 보안 정책을 설정하고 집행할 수 있게 하는 기기 관리 기능을 제공하고 있다.

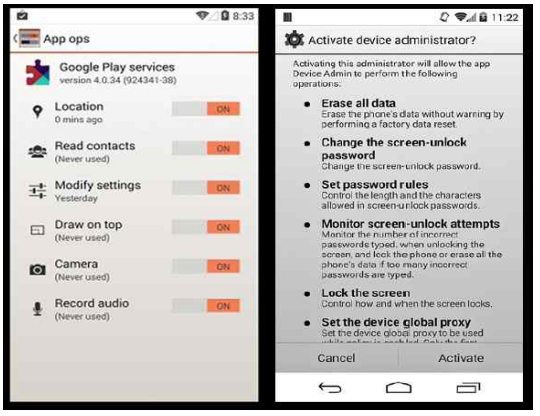

그림 1. 안드로이드 App Ops 기능 화면
Fig. 1. A screenshot of android App Ops

이 기능은 원래 기업용 모바일 기기를 위해 만들어진 것으로 기업 데이터에 대한 기기의 접근 등을 제어하기 위한 목적이지만, 개인 사용자의 프라이버시 보호를 위해서도 활용될 수 있다. 하지만 현재 설정할 수 있는 보안 정책은 매우 제한적이고, 주로 사용자의 패스워드 관리와 로그인 행위, 저장 공간 암호화 등에 관련된 정책만 제공하고 있다.

이처럼 안드로이드 플랫폼은 프라이버시 보호를 위해 활용될 수 있는 몇 가지의 보안 기술을 제공하고 있지만, 여전히 해결해야할 문제점이 존재하고 기술의 적용 범위와 유연성에 많은 제약을 지닌다. 그래서 보다 유연하게 사용자의 프라이버시 보호를 위한 보안 정책을 설정하고 이를 강제할 수 있는 새로운 방식을 필요로 하고 있다.

III. 모바일 프라이버시 정책 분석

다양한 모바일 콘텐츠의 증가와 모바일 기기를 통한 업무의 효율성 증가로 인해 모바일 생태계는 폭발적으로 성장해 왔다. 하지만, 언제나 사용자와 함께하는 모바일 기기로 인해 사용자의 프라이버시를 침해하는 다양한 사고들이 발생했고, 여러 국가와 단체에서는 모바일 환경에서 프라이버시 강화를 위한 정책과 가이드라인을 설정해 배포하고 있다. 그 중 대표적인 정책들의 주요 내용은 다음과 같다.

• EFF의 모바일 사용자 프라이버시 권리(Mobile User Privacy Bill of Rights)[8]

EFF 단체에서는 사용자들의 권리를 존중하는 방식으로 모바일 앱을 개발해야 한다는 가이드라인을 발표했고, 다음의 내용을 포함하고 있다.

- 사용자는 앱이 어떤 개인정보를 수집하여 어떻게 사용하는지에 대한 통제권을 행사할 권리가 있다. 그리고 사용자가 동의를 철회하는 경우 개인정보 이용 역시 중단되어야 한다.
- 모바일에 특화된 민감 정보의 수집에 신중해야 하며, 서비스 제공에 필요한 최소 정보만을 수집해야 한다.
- 사용자는 앱이 어떤 정보에 접근하고, 얼마나 오래 보유하고, 누구와 공유되는지 알 권리가 있다.
- 앱은 정보가 제공된 맥락에서만 해당 정보를 이용하거나 공유해야 한다.
- 모바일 앱 개발자는 수집하고 저장하는 개인정보의 보호에 대한 책임이 있다.
- 모바일 산업의 모든 관계자는 그들이 생산하는 H/W, S/W에 대한 책임이 있으며, 사용자는 그들에 대해 책임 추적성을 요구할 권리를 갖는다.

• 프라이버시 온더고(Privacy on the Go)[9]

2012년 캘리포니아 법무부는 모바일 산업 관계자들의 프라이버시 보호를 위한 책임 사항을 발표했으며, 각 주체별 내용은 다음과 같다.

- 모바일 앱 개발자: 앱이 수집 가능한 개인식별정보를 검토하여 프라이버시 행태 의사 결정을 해야 한다. 앱의 기본 기능에 필요하지 않은 개인식별정보의 수집을 피하거나 제한해야 한다.
- 플랫폼 제공자: 이용자들이 앱을 다운로드하기 전에 충분히 검토할 수 있도록 플랫폼사가 앱의 개인정보 보호정책에 대한 접근성을 제공해야 한다.
- 모바일 광고 네트워크: 개인정보 보호정책을 수립하여 앱 개발자들에게 제공해야 하며, 기기 식별정보의 이용을 지양해야 한다.
- OS 개발자: 사용자가 앱에서 접근 가능한 데이터와 디바이스 기능을 제한할 수 있는 개인정보 설정 기능을 개발해야 한다.

• 모바일 앱 개발자: 보안과 함께 시작(Mobile App Developers: start with security)[10]

FTC에서는 모바일 앱 개발자에 초점을 맞춰 보

안성을 확보하고 프라이버시를 보호하기 위한 권고안을 제공했다.

- 모바일 앱의 복잡도, 성격, 서버와의 통신 여부 등 다양한 환경에 따라 적절한 보안 방식을 적용해야 하며, 환경에 대한 분석을 통해 적정한 데이터 보안을 추구해야 한다.
- 모바일 플랫폼의 SDK를 맹신하고 서두르면 보안 위협에 노출될 가능성이 있다. 그리고 사용자가 증가할수록 보안에 대한 필요성도 증가하며, 사용자는 취약 WIFI 접속 등 로우 테크 위협에 취약하다. 그러므로 모바일 앱 개발자는 개발을 시작하기 전 에코 시스템을 면밀히 검도해야 한다.
- 보안에 대한 책임자를 지정해야 하며, 수집/보관하는 데이터에 대한 면밀한 관리가 필요하다. 그리고 인증 정보를 안전하게 생성해야 하고 민감한 정보를 전송할 때는 SSL/TLS 등의 보안 프로토콜을 적용해야 한다.

IV. 모바일 프라이버시 보호 시스템 제안

4.1 시스템 구조 설계

이 장에서는 모바일 기기 상에서 사용자가 자신의 프라이버시를 보호하기 위해 정책을 스스로 설정하고, 설정된 정책을 실시간으로 집행하는 시스템을 제안한다. 제안 시스템은, 비록 설치시에 이미 권한이 승인되었어도, 모바일 앱이 권한을 필요로 하는 기능을 요청했을 때 사용자가 설정한 정책에 위배되는지 지속적으로 검사하게 된다. 또한 제안 시스템은 모바일 앱의 행위를 지속적으로 모니터링해서 설정된 정책에 위반되는 행위를 할 때 사용자에게 경고를 하는 기능도 제공한다. 제안 시스템의 전반적인 구조는 그림 2와 같다.

모바일 앱은 설치 시에 특정 권한을 요청하고 사용자에게 승인받지만, 이 권한을 사용할 때 사용자의 정책과 일치하지 않는 경우가 자주 발생한다. 예를 들어, 한 앱이 사용자의 위치정보를 획득할 수 있는 권한을 가지고 동작중이라고 하더라도, 만약 사용자가 특정 시간대에 자신의 위치정보를 제공하지 않기로 정책을 설정했다면, 이 앱은 정책에 따라 위치정보를 얻을 수 없게 된다. 이처럼 유연하게 설정된 프라이버시 정책에 맞춰 모바일 앱의 요청에 대해 정책을 검사하고 승인/거부 결정을 내리는 시스템의 주요 흐름은 다음과 같다.

1. 사용자는 PAP를 통해 자신이 원하는 프라이버시 보호 정책을 설정한다. PAP는 정책을 저장소에 저장한다.
2. 모바일 앱이 특정 권한을 필요로 하는 기능을 요청하면, PEP는 이 요청을 가로채서 PDP에 전달한다.
3. PDP는 정책 저장소로부터 설정된 정책을 가져와서 앱의 요청이 정책을 위반하는지 판단한 후 그 결과 승인/거부를 PEP에게 전달한다.
4. PEP는 결과에 따라 앱이 요청한 기능을 제공하게 하거나 혹은 제공하지 않게 된다.

그리고 때로는 권한의 범위가 너무 커서 세밀하게 설정된 정책에 맞춰 검사하기 어렵거나 모바일 앱이 별도의 수단으로 정책에 위배되는 행위를 수행하는 경우도 가능하다. 예를 들어, 사용자는 A라는 특정 파일이 외부에 유출되는 것을 막는 정책을 설정했다고 하자. 모바일 앱의 권한이 각각의 파일 단위로 설정되지 않기 때문에 위의 검사 방식으로는 정책을 집행하기 어려운 부분이 있다. 제안 시스템에서는 이를 보완하기 위해 모바일 기기가 외부와 연결되는 접점에서의 활동을 실시간으로 모니터링하고 모바일 앱이 정책을 위배하는 행위를 수행할 경우 사용자에게 경고를 하는 모듈을 추가했으며, 다음의 방식으로 동작한다.

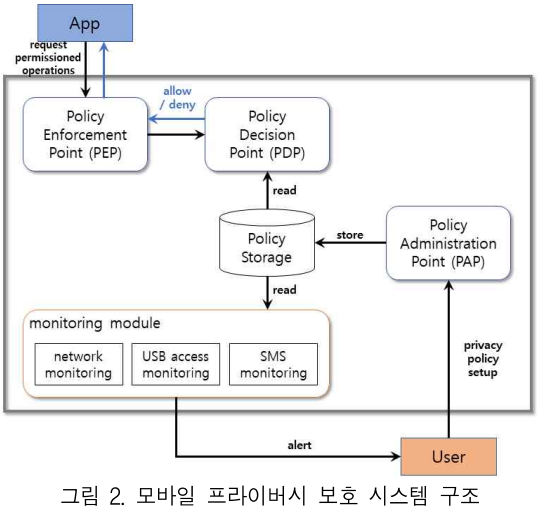

그림 2. 모바일 프라이버시 보호 시스템 구조
Fig. 2. Architecture of a mobile privacy protection system

1. 모니터링 모듈은 정책 저장소로부터 설정된 정책을 가져온다.
2. 사용자의 개인정보를 외부로 유출할 때 사용될 수 있는 통로인 네트워크, USB 포트를 통한 통신, 그리고 SMS/MMS 기반 통신 환경에서 전송되는 데이터를 실시간으로 검사한다.
3. 설정된 정책에 위배해서 전송되는 데이터가 발견되면, 이 모듈은 즉시 사용자에게 경고 메시지를 전송한다.

4.2 시스템 구현

앞서 4.1장에서 제안된 시스템 설계를 바탕으로 안드로이드 플랫폼에 시스템의 프로토타입을 구현했다. 각 구성요소 별로 자세한 구현 방식에 대한 설명은 다음과 같다.

• PEP와 PDP 구현

모바일 앱의 요청을 가로채서 정책을 집행하는 PEP와 정책에 맞춰 요청을 허가/거부를 결정하는 PDP를 구현하기 위해 그림 3과 같이 안드로이드 플랫폼의 코드를 수정했다. 기존의 안드로이드에서 모바일 앱의 요청에 대해 권한을 확인하는 과정은 PackageManagerService 내의 checkUidPermission() 메소드에서 수행된다. PEP의 구현을 위해 이 메소드를 수정했으며, 기존의 확인 과정에 추가적으로 PDP의 구현물인 PrivacyManager로 요청을 연결하고 그 결과에 따라 요청의 승인/거부 결과를 리턴한다.

또한 PDP의 역할을 수행하기 위해 별도의 PrivacyManager를 구현했으며, 이 클래스는 요청 권한의 종류, 앱의 UID등 모바일 앱의 요청 정보를 PEP로부터 전달받는다. 그리고 정책 저장소로부터 설정된 정책을 받아서 요청 정보와 정책에 대한 비교, 검사를 통해 요청의 승인/거부를 결정한다.

• PAP 구현

PAP는 사용자가 자신의 프라이버시 정책을 설정할 수 있도록 관리하고, 설정된 정책을 다른 개체들에게 전달하는 역할을 수행한다.

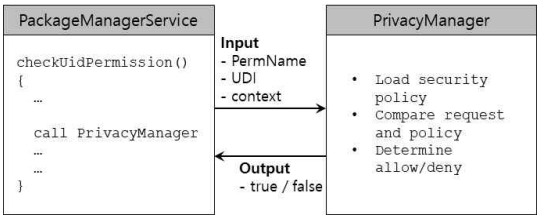

그림 3. 안드로이드 플랫폼 내의 PEP와 PDP 동작
Fig. 3. PEP and PDP operation in android platform

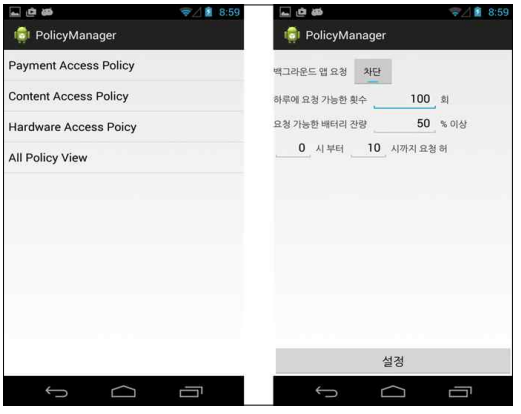

그림 4. PAP 역할의 안드로이드 앱
Fig. 4. Android app for the role of PAP

이를 위해 그림 4와 같이 모바일 앱의 형태로 PAP를 구현했으며, 사용자는 앱을 실행한 후 원하는 프라이버시 정책을 설정할 수 있게 된다. 그리고 정책은 JSON 형태로 표현되며, 설정된 정책은 정책 저장소에 저장되어 PEP와 PDP 등에게 공유된다.

• 모니터링 모듈 구현

프라이버시 정책에 위배되는 정보가 외부에 유출되는 것을 방지하기 위해 모니터링 모듈은 실시간으로 모바일 기기를 통한 네트워크 활동, USB 포트 기반 활동, SMS 기반 데이터 전송 활동을 감시해야 한다. 네트워크 활동 모니터링은 안드로이드용 libpcap을 이용해 전송 패킷을 가로챈 후 분석을 통해 이루어지며, 그림 5는 특정 사이트로의 파일 업로드를 감지한 로그를 보여준다. USB 활동 모니터링은 안드로이드용 usbmon을 활용했으며, USB 포트 접속 장치의 정보와 전송 데이터의 확인이 가능하다. 그리고 SMS 활동 모니터링의 경우, 수신되는 SMS 메시지의 확인을 위해서는 인텐트 후킹 방식[11]을 사용했으며, 발신되는 SMS 메시지의 확인을 위해서는 ContentObserver를 활용했다.

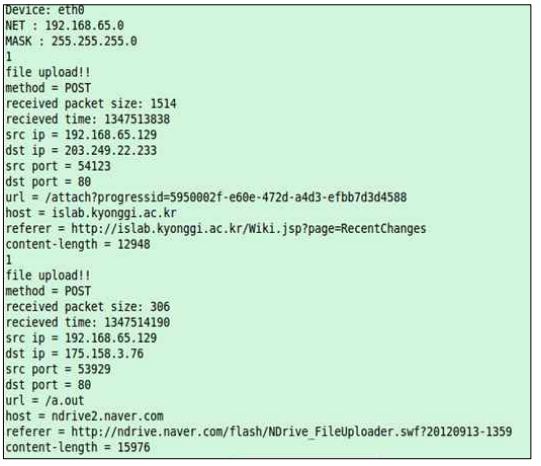

그림 5. 파일 업로드 감지 로그 예
Fig. 5. An example log of detecting file upload

4.3 시스템 비교 분석

모바일 프라이버시에 대한 사용자의 관심이 매우 높아지고 있으며, 이를 반영해서 프라이버시 보호를 위한 다양한 앱들이 출시되어 사용되고 있다. 그 중 국내에서 사용중인 대표적인 앱들에 대한 분석은 다음과 같다.

- V3 모바일 시큐리티[12]

설치된 앱들의 분석을 통해 악성코드를 검사하고 바이러스를 치료하는 백신 기능을 제공한다. 그리고 설치된 앱들이 사용 중인 권한 정보를 제공하며, 특정 앱이 실행될 때 사용자의 잠금해제를 요청하도록 하는 앱 잠금 기능을 제공한다. 또한 갤러리 내의 특정 사진/동영상에 대한 숨김 기능을 제공한다.

- 지란지교 마이프라이버시[13]

통화 내역, 문자 메시지, 사진, 검색 기록 등 주로 사용자가 생성한 컨텐츠에 대해 초점을 맞추고 있으며, 이러한 컨텐츠가 다른 앱들에게 공유되어 프라이버시가 침해되는 것을 방지하고 있다. 이를 위해 기존 안드로이드의 갤러리 및 저장소와는 별도로 내부적인 저장소를 기반으로 컨텐츠를 관리하는 것으로 분석된다.

- 알약 안드로이드[14]

모바일 기기 내의 바이러스와 악성코드에 대한 검사를 수행하며 클라우드 서버 기반의 실시간 탐지를 제공한다. 또한 지능적 스미싱 메시지에 대한 차단을 통해 개인정보를 보호하며, 배터리 및 임시 파일 관리 기능도 제공한다.

위 제품들은 모바일 앱의 형태로 제작/설치되며, 안드로이드에서 앱은 시스템의 관점에서 매우 제한적인 권한만을 허가받기 때문에 다음과 같은 한계를 가진다. 첫째, 사용자의 주소록, 통화기록, 갤러리 등 다른 앱들과 공유되는 저장소에 대한 접근제어를 위의 앱들이 수행할 수 없다. 즉, 공유 저장소에 있는 민감한 개인정보를 권한을 부여받은 다른 앱이 가져가는 것을 막을 수 없으며, 이를 우회하기 위해 별도로 자신이 관리하는 저장소를 따로 관리하고 있으며 정상적인 공유에 대한 불편함 등을 초래한다. 둘째, 다른 앱들에 대한 수동적인 감시는 가능하지만 능동적으로 다른 앱들을 제어할 수는 없다. 즉, 다른 앱의 악성코드 및 바이러스 검사와 앱에게 부여된 권한 정보 수집, 앱의 실행 관련 모니터링은 가능하지만, 프라이버시를 침해하려 하는 다른 앱의 시도를 차단하고 적극적으로 실행을 중지시킬 수는 없다. 이는 안드로이드 플랫폼의 설계 방식에 기인한 것으로, 다른 앱의 실행에 대한 제어는 플랫폼 수준에서 가능하며 앱 수준에서는 제공하지 않고 있다.

제안된 시스템은 위 제품들과 다른 접근방식을 사용하며, 위에서 언급된 한계들을 해결하고 있다. 즉, 제안 시스템은 앱의 형태로 설치되는 것이 아니라 기존 플랫폼을 개선하는 형태이며, 모든 앱들의 권한 요청 및 허가 부분에 개입해서 능동적으로 접근을 제어할 수 있다. 그래서 악성 앱의 공유 저장소에 대한 접근도 방지할 수 있으며, 프라이버시를 침해하려는 악성 앱의 시도를 차단하고 중지시킬 수 있다. 또한, 제안 시스템은 사용자가 유연하게 자신의 프라이버시 정책을 설정할 수 있으며, 이는 제공하는 기능 내에서 제한적으로 사용자가 정책을 선택하는 기존 제품들에 비해 높은 확장성을 가진다. 이처럼 제안 시스템은 기존 제안 방식들에 비해 사용자에게 유연성과 확장성을 제공하면서 동시에 강력한 프라이버시 보호 기능을 제공하는 장점을 가지고 있다.

V. 결론 및 향후 연구 방향

본 논문에서는 모바일 환경에서 사용자의 프라이버시를 강화하기 위한 연구를 제공했다. 프라이버시의 주요 위험요소와 제안된 보안 정책에 대한 분석을 수행했고, 기존의 보안 기술에 더해 프라이버시를 강화할 수 있는 시스템을 제안했다. 사용자는 유연하게 자신의 프라이버시를 보호하기 위한 정책을 설정할 수 있으며, 제안 시스템은 설정된 정책의 집행을 통해 모바일 앱의 프라이버시 유출 위험을 제어한다. 그리고 민감한 개인 정보가 외부에 유출되지 않도록 모니터링하는 기능도 함께 제공한다.

향후에는 제안된 시스템을 iOS등의 다른 모바일 플랫폼에 적용하는 연구를 진행할 계획이다. 또한 제안 시스템의 보안 정책 집행과 모니터링 기술을 활용해서 기업 내의 중요 정보에 대한 유출을 방지하는 기업용 모바일 보안 시스템을 개발하는 연구도 진행할 계획이다.

References

[1] Liu, Bin, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, S. A. Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal, "Follow my recommendations: A personalized privacy assistant for mobile app permissions", In Symposium on Usable Privacy and Security, pp. 27-41, Jun. 2016.

[2] "Apple knocks out android in mobile security", http://mashable.com/2012/11/13/apple-android-security/#PfPD181iu8qd. [Accessed: Sep. 11, 2017]

[3] "Android System Permissions", https://developer.android.com/guide/topics/permissions/index.html. [Accessed: Sep. 11, 2017]

[4] Liu Bin, Lin Jialiu, and Sadeh Norman, "Reconciling mobile app privacy and usability on smartphones", Proceedings of the 23rd international conference of World Wide Web, pp. 201-212, Apr. 2014.

[5] Nauman Mohammad, Khan Sohail, and Zhang Xinwen, "Extending Android Permission Model and Enforcement with User-defined Runtime Constraints", Proceeding of the 5th ACM Symposium on Information, pp. 238-332, Apr. 2010.

[6] T. Vidas, N. Christin, and L. Cranor, "Curbing Android Permission Creep", W2SP, 2011.

[7] "App Ops- what you need to know", http://www.androidauthority.com/app-ops-need-know-324850/. [Accessed Sep. 11, 2017]

[8] Parker Higgins, "Mobile User Privacy Bill of Rights", Electronic Frontier Foundation, Mar. 2012.

[9] Kamala D. Harris, "Privacy on the go: recommendations for the mobile ecosystem", California Department of Justice, Jan. 2013.

[10] Federal Trade Commission, "Mobile App Developers: Start with Security", 2015.

[11] Dong-Min Kim, Seung-Je Park, Won-Bo Shim, and Heeyoul Kim, "Analysis of Security Vulnerabilities in Implicit Intent Routing Mechanism of Android Platform", Journal of KIIT, Vol. 9, No. 8, pp. 93-99, Aug. 2011.

[12] "V3 mobile security", http://www.ahnlab.com/kr/ site/product/productView.do?prodSeq=19. [Accessed: Sep. 11, 2017]

[13] "My privacy", https://www.myprivacy.co.kr/#myprivacy. [Accessed: Sep. 11, 2017]

[14] "Alyak android 1.9", https://www.estsecurity.com/product/alyac_android. [Accessed: Sep. 11, 2017]

저자소개

김 희 열 (Heeyoul Kim)

2000년 2월 : 한국과학기술원 전산학과(공학사)
2002년 2월 : 한국과학기술원 전산학과(공학석사)
2007년 2월 : 한국과학기술원 전산학과(공학박사)
2009년 3월 ~ 현재 : 경기대학교 컴퓨터과학과 부교수
관심분야 : 정보보호, 암호학, 보안 프로토콜