http://dx.doi.org/10.3745/KIPSTC.2012.19C.4.235

안드로이드 로컬 마켓 인증 방안

한 규 석[†] · 손 태 식[††]

요 약

급격하게 증가하고 있는 스마트폰의 애플리케이션 이용의 편의를 위한 마켓 기반의 배포 방식이 활성화되고 있으며, 안드로이드의 경우 개방성을 제공하여 다양한 형태의 애플리케이션 배포 방식이 존재하고 있다. 그러나 애플리케이션의 직접 설치를 허용하는 개방성은 안드로이드 애플리케이션의 불법적인 이용이라는 부작용을 낳고 있으며, 이에 대응하기 위해 온라인 인증과 같은 강력한 사용자 인증 방식을 이용하고 있다. 그러나 이러한 방식은 정당한 사용자에게도 경우에 따라 이용을 제한할 수 있다는 문제점을 갖고 있으며 특히 구글 외 로컬 마켓에서 사용자의 애플리케이션 이용을 저해하는 요인이 된다. 따라서 본 논문에서는 사용자가 로밍, 통신사 변경 등의 다양한 변동 상황에서 구매한 애플리케이션을 그대로 이용할 수 있는 인증 방안을 제시한다.

키워드 : 안드로이드, 인증, 로밍

Application Authentication via Various Distributors

Kyusuk Han[†] · Taeshik Shon[††]

ABSTRACT

Google Android provides market based application distribution to provide ease use of application services. While openness of Android allows various ways of application distribution, including installation of unsigned application. such openness also invokes critical threats such as the spread of malwares and the illegal distribution of applications. In order to prevent such threats, several distributors use on-line authentication techniques by using mobile subscriber's information. However such methods also have limits that even legal users cannot use their purchased application in situations. Therefore, in this paper, we discuss such problems and provide some ideas of authentication method that allow users to use their purchased application when users change their status.

Keywords : Android, Authentication, Roaming

1. 서 론

최근에 급격히 보급되고 있는 스마트폰은 앱스토어(Appstore)를 통해 사용자가 직접 다양한 애플리케이션을 선택하여 설치하고 사용하는 것을 용이하게 하며, 이는 과거 휴대 기기에서 가장 큰 문제가 되어 왔던 애플리케이션 구입 및 설치에 대한 번거로움을 해소하여 사용자들의 이용을 활성화하는데 도움을 주고 있다. 2008년 애플사에서 iPhone을 대상으로 하는 앱스토어(Appstore)를 제공한 이후 Google, Microsoft 등에서도 스마트폰을 대상으로 하는 다양한 앱스토어가 활발하게 운영되고 있다. Google에서 제공하는 안드로이드의 경우 Google이 직접 운영하는 안드로이드 마켓 (현 Google Play) 외에 각 국가 내 통신 사업자, 제조사 등이 제공하는 마켓이 공존하고 있으며, Table 1과 같이 다양한 형식의 애플리케이션 배포 방식이 존재하고 있다.

Google Play, Samsung Apps, 등의 글로벌 앱스토어의 경우 사용자가 스토어 이용을 위해 계정을 생성한 후 동일 계정 이용 시 휴대전화 및 가입 상태 변동의 경우에도 이용 가능하도록 하고 있으나 각 국가의 로컬 앱스토어와 비교하여 가입자의 환경에 적합한 발 빠른 현지화 등에 약점을 갖고 있다. 예를 들어 구글의 안드로이드 마켓의 경우 한국의 사용자에게 유료 애플리케이션 구매 시 최근까지 원화 대신 달러를 기준으로 가격을 책정하도록 하고 있으며, 한국에서 심의가 필요한 게임 등의 경우 심의를 받는 대신 게임 항목을 제거하여 최근에야 추가하는 방식으로 대응하는 등의 문제가 존재한다.

안드로이드의 경우 사용자의 입장에서 가입한 휴대전화 사업자가 제공하는 등의 로컬 마켓을 이용하는 비중이 크게

※ 본 연구는 2011년도 산학협동재단 학술연구비 지원에 의해서 수행된 결과임.
† 정 회 원 : University of Michigan, Visiting Scholar
†† 정 회 원 : 아주대학교 정보통신공학부 조교수(교신저자)
논문접수 : 2012년 5월 8일
수 정 일 : 1차 2012년 6월 28일
심사완료 : 2012년 7월 3일
* Corresponding Author : Taeshik Shon(tsshon@ajou.ac.kr)

증가하고 있으나, 안드로이드의 상대적으로 개방적인 정보를 바탕으로 여러 형태의 공격 [1]이 발생하며 현재의 사용자의 휴대전화의 가입 정보를 기반으로 하고 있는 애플리케이션 인증 방식은 해지, 혹은 해외 로밍과 같은 상태 변경 시 애플리케이션 이용이 제한되는 문제가 있다.

따라서 본 논문에서는 구글의 앱스토어 인증 방식과 로컬 앱스토어 인증 방식을 융합하여 사용자가 로밍 혹은 가입 상태 변경 시에 구매한 애플리케이션에 대한 인증을 통해 이용을 허용하는 방안을 제시한다.

표 1. 안드로이드 애플리케이션 유통 방식
Table 1. Distribution Methods of Android Application

유통 형태	예	특징
OS 제공자	Google Play	구글에 사용자 계정을 등록한 후 이용하도록 하고 있으며 기본적으로 계정 생성 시 위치한 국가의 스토어로 연결
기간 통신사	T스토어, Olleh Market, 등	프로그램 실행 시 USIM에 기록된 가입자 등록 번호를 통해 구매자 가입 인증 확인을 요구하고 있으며, 인증이 된 사용자에게 프로그램 실행을 허용
제조사	Samsung Apps	스마트폰 제조사인 삼성전자에서 자체 제공하며 삼성전자의 스마트폰에 최적화된 애플리케이션 위주로 제공
유통사	Amazon Appstore	미국의 Amazon에서 제공하며 Amazon 계정 이용자에게 제공. Amazon Kindle Fire에는 기본 탑재되어 있으며, 기타 안드로이드 기기에는 사용자가 직접 설치하여 사용
공개 유통	GetJar	Android, Blackberry, Java, Symbian 등의 모바일 OS의 공개 애플리케이션을 제공하고 있으며, 특별한 절차 없이 웹사이트를 통해 애플리케이션을 다운로드할 수 있다.
직접 설치	비인가 APK 직접 설치	안드로이드의 경우 비 인가된 apk 형식의 프로그램 설치

2. 안드로이드 애플리케이션 배포 방식의 문제점

위와 같은 현재 환경에서 안드로이드 애플리케이션 배포 방식의 문제점은 다음과 같다.

2.1 미등록 애플리케이션 신뢰 방안 제약

안드로이드에서 마켓을 통하지 않은 비 인가된 apk 형식의 파일을 통해 사용자의 임의의 애플리케이션 설치를 허용하는 개방성을 갖고 있다. 이에 대한 부작용으로 애플리케이션에 대한 악성 코드 유포 [6] 및 애플리케이션의 불법적인 배포가 iOS에 비해 매우 심각한 수준에 있으며 이에 대한 다양한 연구가 진행되고 있다[2,3,4,5]. 결과적으로 안드로이드 OS 애플리케이션의 불법 복제의 방지를 위해 온라인 인증과 같은 강력한 수준의 인증 방식을 요구하게 된다. 그러나 이는 다음과 같은 문제를 발생시킨다.

2.2 다양한 사용자 환경 따른 애플리케이션 인증 문제

사용자의 권한 인증을 위해 애플리케이션 실행 시 온라인 인증을 거치는 방법을 보편적으로 사용하고 있다. 한국의 경우, 다수의 안드로이드 애플리케이션이 이동통신망을 통해 USIM 등록 번호의 확인을 통해 사용자 인증을 하고 있으며, flight mode 등을 통해 오프라인 환경에서는 정당한 사용자인 경우에도 구매한 애플리케이션의 실행 자체를 제한하는 경우가 발생하는 문제가 발생한다.

2.3 안드로이드 마켓에서 스토어 간 등록된 동일한 애플리케이션 충돌 및 상호 인증 방안 부재 문제

소프트웨어의 버그 패치, 기능 추가와 같은 사후 지원은 매우 필수적이며, 전통적인 배포 방식은 제작사가 공급한 소프트웨어 패키지를 제작사가 직접 판매하거나 혹은 온라인 혹은 오프라인 마켓을 통해 유통하고, 제작사가 사후 지원을 담당하는 형태가 일반적이며, 사용자는 구입 경로와 무관하게 사후 지원을 받을 수 있으나, 앱스토어의 경우, 각 마켓에서 구입한 애플리케이션의 사후지원은 구매한 앱스토어를 경유하여 사후 지원을 받게 된다.

그러나 구입한 마켓에서 업데이트를 제공 받을 수 없는 경우 사후 지원은 불가능하며 기본적으로 제공되는 Google Play를 제외하고 통신사 이동 혹은 해외 이민 등을 통한 변경이 발생한 경우에는 재 구입하는 방법 외에는 지원이 불가능하다. 이는 사용자가 로컬 마켓을 통한 애플리케이션 구매를 망설이게 하는 요인이 될 수 있다.

3. 제안하는 기법

3.1 시스템 모델 및 시나리오

시스템 모델은 다음 Fig. 1과 같다. 일반적인 사용 시나리오는 다음과 같다. 사용자가 최초로 연결된 스토어 M_1 을 통해 등록 요청 (3.2)을 하게 된다. 등록 이후에 변동이 없는 이상 사용자가 등록된 스토어를 통해 애플리케이션 구매를 하게 된다. M1은 구매 인증 시스템 (Purchase Authentication System, PAS)에 사용자 정보를 저장한다. 만약 사용자의 등록 상태 변동이 발생하는 경우 사용자는 새로 연결된 마켓에 사용자의 등록 상태의 변경을 요청하게

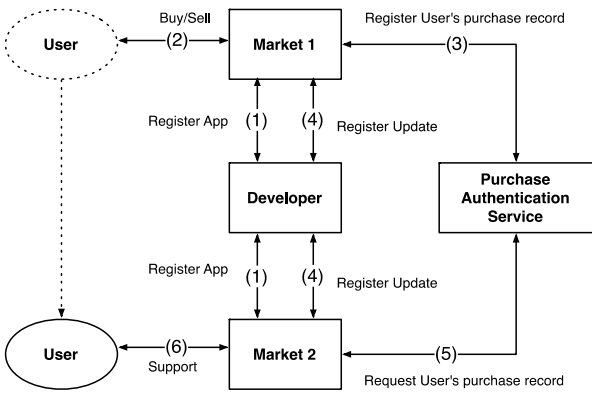

그림 1. 애플리케이션 마켓 인증 시스템 모델
Fig. 1. Authentication System Model of Application Market

된다 (3.3). 발생할 수 있는 사용자 등록 상태 변경의 경우는 다음과 같이 발생할 수 있다: 일시적인 로밍; 동일 통신사 해지 및 재가입; 통신사 이동, 해지 및 타 통신 수단을 통한 이용; Offline 모드 이용. 이 경우 사용자는 새로 연결된 마켓인 (M_2)를 통해 기존에 등록 및 구매한 애플리케이션의 사용 혹은 지원에 대한 인증 요청을 하게 되며, 이 후 M_2는 PAS와 통신 (혹은 M_2과 직접 통신)을 통해 사용자의 구매 정보를 확인한 후 사용자에게 애플리케이션 이용 허가 혹은 지원 응답을 하게 된다.

3.2 사용자 정보 등

사용자가 애플리케이션 구매 확인을 위한 사용자정보 $UINFO$ 는 구매 시 마켓에 제공되며 이 정보는 PAS에도 제공된다. $UINFO$의 항목은 Table 2의 내용을 포함한다.

표 2. UINFO 포함 사용자 정보 요소
Table 2. User Information Attribute in UINFO

요소	설명
UAddr	이용자가 가입 시 등록하며 전화 가입 정보와 별도로 이용할 수 있다. 실제로 여러 형태로 가입자 확인을 위해 e-mail을 통한 인증을 한다.
UIMSI	이용자가 등록 시 기록된 휴대전화 가입자의 고유 번호로 이용한다. 동일 통신사에 가입하는 경우 본 정보 확인을 통해 인증을 한다. (Optional)
UPN	DEVICE INFO, 변경 기기 확인을 위해 이용한다. (Optional)
CN	Country Code, 국가 별 허용하는 애플리케이션, 혹은 미디어 정보를 관리하기 위해 이용한다. (Optional)
CR	Carrier Code, 통신사 간 제휴 관계를 확인하기 위해 이용한다. (Optional)
TS	Timestamp, 일정 시간 동안의 Offline 인증을 위해 이용한다. (Optional)

사용자는 마켓에 등록 시 다음 Fig. 2와 같은 절차를 수행하며 여기서 전달되는 u, v는 다음과 같이 Market 1 (M_1)에 의해 생성되며 K_{M_1}은 M1과 PAS 간에 공유되는 비밀 키이다. Enc와 MAC은 각각 암호화 및 Message Authentication Code 생성 함수를 의미한다.

$$u = enc_{K_{M_1}}(UINFO),\ v = MAC_{K_{M_1}}(u)$$

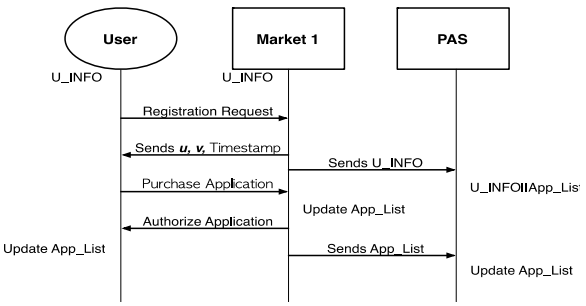

그림 2. 사용자의 마켓 등록 과정
Fig. 2. User Market Registration Process

사용자는 u, v와 함께 $UAddr$, TS, 그리고 사용자의 애플리케이션 구매 기록인 APP를 보관한다. APP은 구매 시마다 갱신되며, 사용자 외에 현재 이용 중인 마켓, 그리고 PAS 에 저장된다.

3.3 사용자의 타 마켓을 통한 인증 확인

3.3.1 UAddr 확인

M_1을 이용한 적이 있는 사용자 (U)의 정보를 확인하기 위해 M_2는 U와 보안 채널을 설정하게 된다. 본 과정에서는 사용자의 e-mail을 통한 보안 채널을 설정하는 것으로 가정하며, 실제로 안드로이드 기반의 스마트폰의 경우 모든 사용자가 최소한 한 개 이상의 e-mail (Google에서 제공하는 Gmail) 계정을 보유하고 있으므로 가능한 시나리오로 예상된다. 다만, 사용자의 부주의에 의한 e-mail 도용 등의 문제는 본 논문에서는 논외로 한다.

3.3.2 UINFO 및 Application 구매 확인

A. 사용자가 일시적인 로밍 중 인증을 요구하는 경우

사용자가 인증이 필요한 애플리케이션에 대해서 u, v, 타임스탬프 TS와 $UINFO$ 중 필요한 경우 CN, CR 등의 정보를 전달한다. 여기서는 CN, CR만 보낸다고 가정하며, 이 경우 사용자는 아래와 같이 V_u를 생성한다.

$$V_u = MAC_{K_U}(u||v||TS||CN||CR||APP)$$

K_U는 사용자와 PAS 간의 공유하고 있는 비밀 키이다.

사용자는 아래와 같이 M_2에게 전달한다. 사용자와 M_2 간의 보안 채널이 생성되었다고 가정하며 프로토콜 상의 암호화는 생략한다.

$$U \rightarrow M_2 : u, v, TS, CN, CR, APP, V_u$$

M_2는 전달받은 정보를 PAS에게 전달하여 사용자의 인증을 요청한다. 마켓과 PAS 간에는 이미 보안 채널이 구성되어 있다고 가정한다. PAS는 사용자의 $UAddr$을 통해 V_u를 검증한 후 CN와 CR를 통해 사용자가 기존에 연결되어있던 M_1에 대한 정보를 확인한 후, K_{M_1}을 이용하여 v를 검사한 후 u를 복호화하여 $UINFO$를 확인한다.

PAS는 사용자의 애플리케이션 리스트 APP와 $UINFO$에 대한 정보를 M_2에게 전달하며, M_2는 이를 통해 사용자를 인증하여 서비스 인증을 허용한다. 일시적인 로밍의 경우 M_1은 M_2에게 인증 확인만 하며 기존 정보를 갱신하지 않는다.

B. 사용자가 동일한 마켓을 바로 재이용하는 경우

M_1의 경우 사용자의 정보가 기존과 동일한 경우, 타임스탬프 TS만 갱신하여 사용자에게 전달한다.

$$U \rightarrow M_1 : u, v, TS, APP, V_u^*$$

여기서 V_u^*는 $V_u^* = MAC_{K_U}(u||v||TS^*||APP)$이다.

M_1은 이미 K_{M_1}에 대해 알고 있으므로, PAS를 경유하여 V_u^*의 검증 여부만 확인한다.

C. 사용자가 이용 마켓을 완전히 변경하는 경우

대부분의 과정은 A와 같으나 기존의 $UINFO$는 M_2에 의해 $UINFO^*$로 새로 갱신되며 갱신되는 내용은 다음 예와 같다. 국가의 변경 시 새로운 CN^*, CR^*, TS^*, $UPIN^*$ 등이 갱신되며, 사용자의 e-mail 등은 고정되어 있는 경우 $UAddr$의 항목은 그대로 유지하게 된다. 만약 사용자가 기존의 기기를 이용하는 경우 UPN을 동일하게 유지할 수 있으며, 만약 e-mail 등의 통신사와 독립된 정보의 변경의 경우 $UAddr$이 변경될 수 있다.

이 과정에서 U는 M_2에게 기존에 보관하고 있던 $UINFO$ 및 APP을 전달하며 M_2는 $UINFO$를 PAS에서 확인 후 u, v를 갱신한 u^*, v^*를 생성하여 사용자에게 반환한다. 이후 사용자는 $UINFO^*$와 u^*, v^*를 보관한다. 여기서 u^*, v^*는 다음과 같이 생성된다.

$$u^* = enc_{K_{M_2}}(UINFO^*),\ v^* = MAC_{K_{M_2}}(u^*)$$

4. 제안 방안 분석

제안된 방식은 사용자의 로밍 중 사용, 동일 마켓의 재이용 시 이용, 그리고 타 마켓으로 변경 시 이용에 대한 방식을 고려하고 있다.

본 논문에서 제안한 사용자 인증 방법으로 이용한 사용자 정보 중 사용자의 e-mail 정보는 사용자 확인을 위해 사용되는 일반적인 방식이며, 구글의 Play store, 애플의 앱스토어 등에서도 사용되고 있다.

제안한 모델에서 포함된 Purchase Authentication Service는 각 마켓이 로밍 사용자에 대한 인증을 위해 정보를 상호 공유하는 신뢰할 수 있는 개체로서, 이를 통해 각 사용자는 이미 구매한 애플리케이션의 인증 및 사후 지원을 다음과 같이 용이하게 할 수 있다.

마켓에서 애플리케이션의 고유한 ID를 공유하고 있으며, 사용자의 구매 목록 APP을 보관함으로써, 사용자가 이미 해지한 상황이라도 PAS에 저장된 APP을 통해 차후에 어떤 서비스를 이용하는 경우에도 PAS를 통해 구매한 애플리케이션에 대한 온라인 인증이 가능하며 사후 지원을 받을 수 있는 증빙자료로 사용하게 된다.

또한, 추가적으로 각 마켓에서 애플리케이션의 상호 인증에 대한 적절한 서비스 과금을 부과하여, 사용자의 애플리케이션 재 구입에 대한 우려를 감소하면서, 추가적인 수입을 얻을 수 있으며, 로컬 마켓의 애플리케이션 구매를 촉진할 수 있는 이점이 있다.

5. 결 론

본 논문에서는 안드로이드 기반의 마켓 간에 애플리케이션의 상호 인증의 필요성 및 방안에 대해 제시하고 있으며, 향후 실질적인 이용을 위한 설계 및 실험, 그리고 상세한 안전성 분석 등을 통한 효용성에 대한 검토가 진행될 예정이다.

참 고 문 헌

[1] M. Backes, S. Gerling, and P. von Styp-Rekowsky, “A Novel Attack against Android Phones,” arXiv.org, Vol.cs.CR. 21-Jun.-2011.

[2] Pietro Albano, A. Castiglione, G. Cattaneo, and A. De Santis, “A Novel Anti-forensics Technique for the Android OS.,” BWCCA, pp.380 - 385, 2011.

[3] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, “A Study of Android Application Security,” USENIX Security Symposium 2011, 2011.

[4] W. Zhou, Y. Zhou, X. Jiang, and P. Ning, “Detecting repackaged smartphone applications in third-party android marketplaces.,” CODASPY, pp.317 - 326, 2012.

[5] F. Di Cerbo, A. Girardello, F. Michahelles, and S. Voronkova, “Detection of Malicious Applications on Android OS.,” ICWF, pp.138 - 149, 2010.

[6] http://nakedsecurity.sophos.com/2012/04/12/android-malware-angry-birds-space-game/

한 규 석

e-mail : kyusuk@umich.edu

2001년 2월 홍익대학교 기계공학과(학사)

2004년 8월 한국정보통신대학교 공학부(석사)

2010년 8월 한국과학기술원 정보통신학과(박사)

2010년 12월~2011년 9월 한국과학기술원 박사후연수연구원

2011년 10월~현 재 University of Michigan, Visiting Scholar

관심분야 : Wireless/Mobile Network Security, WSN, Security Policy, Automotive Network

손 태 식

e-mail : tsshon@ajou.ac.kr

2000년 2월 아주대학교 정보 및 컴퓨터공학부

2002년 2월 아주대학교 컴퓨터(공학석사)

2005년 8월 고려대학교 정보보호대학원(박사)

2004년 2월~2005년 2월 University of Minnesota, Research Scholar

2005년 8월~2011년 2월 삼성전자 DMC연구소 책임연구원

2011년 2월~현 재 아주대학교 정보통신공학부 조교수

관심분야 : Wireless/Mobile Network Security, WSN/WPAN, Anomaly Detection/Machine Learning