제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

# 스마트폰 애플리케이션 콘텐츠 통합 관리 모델에 대한 연구

박대식*, 곽진*
*순천향대학교 정보보호학과
e-mail:dspark@sch.ac.kr, jkwak@sch.ac.kr

# A Study on Smartphone Application Contents Integrated Management Model

Dae-Sik Park*, Jin Kwak*
*Dept of Information Security Engineering, Soonchunhyang University

요 약

안전한 스마트폰 사용 환경을 위해 스마트폰 애플리케이션 콘텐츠의 검증 및 운영은 필수적이다. 기존 스마트폰 환경에서의 스마트폰 애플리케이션 콘텐츠 등록 및 관리는 애플리케이션 콘텐츠 등록 시에만 수행되어 지속적인 관리가 수행되지 않았기 때문에 사용자가 직접 관리해야하는 문제점이 있었다. 하지만 이러한 애플리케이션 콘텐츠 관리는 다양한 보안 취약점이 내포되어 있다. 따라서 본 논문에서는 기존 방식에서의 보안 취약점을 분석하고 이를 기반으로 스마트폰 애플리케이션 콘텐츠 통합 관리 모델을 제안한다.

## 1. 서론

최근 모바일 컴퓨팅 기술의 급속한 발전으로 다양한 모바일 기기들이 개발되고 있으며 다양한 기능을 탑재한 스마트폰이 주목받고 있다. 또한 WIPI(Wireless Internet Platform for Interoperability)탑재 의무화가 폐지됨에 따라 외산 스마트폰 도입이 확산되고 있으며 스마트폰의 경우 스마트폰의 애플리케이션 콘텐츠가 스마트폰 보급 및 시장 활성화에 많은 영향력을 미치고 있다. 또한 스마트폰 애플리케이션 콘텐츠 시장이 개방 및 활성화됨에 따라 다양한 운영체제를 탑재한 스마트폰이 출시되고 있어 스마트폰 시장 경쟁이 점차 치열해 질 것으로 예상된다[1].

스마트폰에는 애플리케이션 콘텐츠에 따라 다양한 기능들이 융합되어 있으며 사용자의 개인 정보 및 금융 정보들이 단말기 내에 저장된다. 따라서 이를 보호하기 위한 애플리케이션 콘텐츠 검증 및 관리가 필수적으로 요구되고 있지만 관리 대상이 스마트폰에 한정되어있어 사용자가 직접 애플리케이션 콘텐츠를 관리해야한다. 그러나 사용자가 직접 애플리케이션 콘텐츠를 관리하는 것은 한계가 있기 때문에 본 논문에서는 이러한 문제점을 해결하기 위해 기존 애플리케이션 콘텐츠 관리 방법들의 보안 취약점을 분석하고 이를 바탕으로 사전 검증 기법을 이용하여 효과적인 애플리케이션 콘텐츠 관리 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트폰의 개요와 기존 애플리케이션 콘텐츠 관리 및 보안 기술 동향과 취약점을 분석한다. 3장에서는 제안 모델의 구성 요소와 동작 방식을 설명하고 4장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 스마트폰 개요

스마트폰은 기존 휴대폰과 PDA의 장점을 결합시킨 제품으로 PC에서 제공하던 문서 작업 및 보관, 멀티미디어 애플리케이션 재생, 전자메일 전송, 웹 브라우저를 통한 인터넷 서비스 이용 등 부가기능을 결합한 제품으로써 최근에는 휴대전화를 통해 일반적인 유선 웹 사이트에 접근하는 개념으로 서비스 제공 업체의 무선 포탈이 제공하는 제한된 애플리케이션의 범위를 넘어 직접 URL 입력을 통해 유선 웹 포탈에 접속하는 풀 브라우징(Full Browsing)이 가능한 모바일 기기를 의미한다[2]. 또한 기존의 휴대폰에서 사용되는 애플리케이션은 제조업체에서 제공하는 애플리케이션 외에 사용자가 추가적으로 설치 및 사용하지 못하였지만 스마트폰 사용자는 이동 통신사의 3G망이나 WiFi 등과 같은 네트워크 접속 방식으로 애플리케이션 마켓에서 애플리케이션을 다운받아 사용할 수 있다[3,4].

### 2.2 관련 기술 동향 및 취약점 분석

현재 스마트폰 애플리케이션 콘텐츠 관리에 있어 애플의 앱스토어, 구글의 안드로이드 마켓이 크게 주도 하고 있다. 따라서 본 장에서는 애플과 구글의 애플리케이션 콘텐츠 관리 방식에 대해 분석한다.

□ 애플의 앱스토어

애플의 앱스토어에서는 애플리케이션 콘텐츠 등록 시,

자사의 애플리케이션 콘텐츠 검증자가 등록 신청된 애플리케이션을 직접 검증하는 방식을 사용하고 있다.

이는 자사의 내부 애플리케이션 콘텐츠 허용 규칙을 적용하여 등록 신청된 애플리케이션 콘텐츠를 직접 검증함으로써 보안 및 비 이상적인 애플리케이션을 원천 차단할 수 있는 방식으로 높은 보안성을 가지고 있다. 그러나 애플의 애플리케이션 콘텐츠를 사용하는 스마트폰 기기의 경우 탈옥(Jailbreak)라는 불법적인 스마트폰 기기 변경을 통해 애플에서 허용하지 않은 다양한 애플리케이션 콘텐츠가 사용될 수 있다. 이러한 방식으로 인해 스마트폰 기기에 불법적인 애플리케이션 콘텐츠가 설치됨에 따라 다양한 보안 문제점이 발생할 수 있으며 이를 방지하기 위해 애플리케이션 콘텐츠 설치 및 실행에 대한 대응 방안이 필요하다.

□ 구글의 안드로이드 마켓

구글의 안드로이드 마켓에서는 개방형 정책의 일환으로써 애플리케이션 콘텐츠 검증에 있어 애플의 앱스토어에 비해 상당히 간략화된 방식을 사용하고 있다.

이는 애플리케이션 콘텐츠의 보안성을 고려하지 않고 작동성만 고려하기 때문에 애플리케이션 콘텐츠는 다양한 보안상의 취약점을 내포하고 있다. 또한 스마트폰 기기에 애플리케이션 설치에 대한 제한 정책이 존재하지 않기 때문에 불법적인 애플리케이션 콘텐츠 설치에 대한 적절한 조치가 수행되지 않아 다양한 보안 위협에 노출되어 있다.

## 3. 제안 방식

앞서 2장에서 분석한 바와 같이 기존의 스마트폰 애플리케이션 콘텐츠 관리 기술들은 다양한 문제점들을 내포하고 있다. 따라서 본 장에서는 앞서 분석한 문제점들을 해결할 수 있는 스마트폰 애플리케이션 통합 관리 모델을 제안한다.

### 3.1 구성 요소

본 논문에서 제안하는 스마트폰 애플리케이션 통합 관리 모델은 애플리케이션 콘텐츠 개발, 검증, 등록 운영을 수행한다. 이를 통해 애플리케이션 콘텐츠는 등록 될 때부터 실행되고 삭제될 때까지 지속적으로 관리되어 보안성이 증가한다. 제안하는 스마트폰 애플리케이션 통합 관리 모델의 구성요소는 다음과 같다.

- SDK 서버
- 애플리케이션 운영 서버
- 데이터베이스 서버

#### 3.1.1 SDK 서버

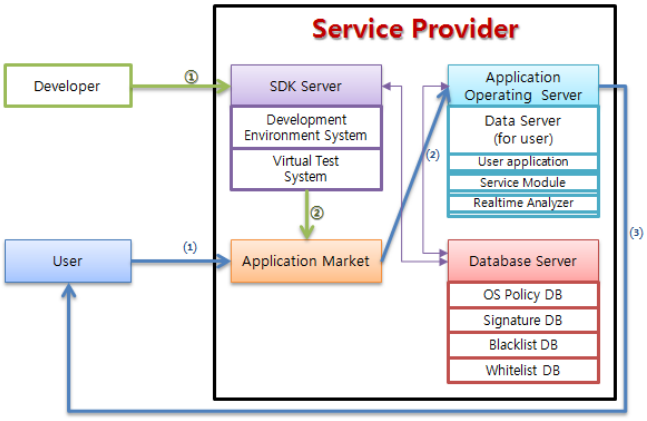
SDK 서버에서는 서비스 제공자가 애플리케이션 콘텐츠 개발자를 위해 클라우드 컴퓨팅 기술을 적용하여 구축한 가상화 환경으로써 개발자 별 SDK를 제공하는 서버이다. 이를 통해 개발자를 애플리케이션 콘텐츠를 개발하며 해당 애플리케이션 콘텐츠는 가상화된 운영환경에서 직접 시험 운영되어 보안성 검증이 수행된다.

#### 3.1.2 애플리케이션 운영 서버

사용자 정보를 바탕으로 사용자의 가상화 환경을 구축하여 사용자가 원하는 애플리케이션 콘텐츠를 이용할 수 있도록 서비스를 제공하는 서버이다. 애플리케이션 운영 서버에 사용자가 스마트폰 기기를 이용하는데 필요한 모든 기능을 제공함으로써 사용자의 스마트폰 기기는 애플리케이션 운영 서버에 접속하는 단말기의 기능만을 지닌다.

#### 3.1.3 데이터베이스 서버

데이터베이스 서버에서는 애플리케이션 콘텐츠 검증에 필요한 데이터베이스를 제공한다. 데이터베이스 서버 내에는 서비스 제공자가 제공하는 운영 환경 및 보안 정책들이 데이터베이스화되어 있으며 이를 통해 애플리케이션 콘텐츠 검증에 필요한 정보를 제공한다.




(그림 1) 스마트폰 애플리케이션 통합 관리 모델 구성도

### 3.2 동작 방식

(그림 1)은 스마트폰 애플리케이션 통합 관리 모델의 구성도를 나타내며 개발자 환경, 사용자 환경으로 크게 2가지로 구분할 수 있다. 개발자 환경의 경우 개발자가 애플리케이션 콘텐츠를 개발함에 따른 순서를 나타내며 사용자 환경은 사용자가 애플리케이션 콘텐츠를 사용함에 따른 순서를 나타낸다.

#### 3.2.1 개발자 환경

서비스 제공업체에서 운영하는 애플리케이션 콘텐츠 마켓에 등록하기 위해서 개발자는 애플리케이션을 개발하기 위해 서비스 제공업체에서 제공하는 SDK 서버에 접속하여 애플리케이션을 개발한다.

SDK 서버에서는 개발자가 개발하는 애플리케이션의 코

드들을 데이터베이스 서버에 저장된 다양한 시그니처 데이터베이스 등과 비교하여 실시간으로 보안성 검증을 수행한다.

이를 통해 서비스 제공업체의 애플리케이션 콘텐츠 검증자는 사전에 자동으로 애플리케이션 콘텐츠에 대한 기본적인 보안성 검증을 수행되었기 때문에 애플리케이션 콘텐츠 코드 부분을 검증하지 않고 애플리케이션 콘텐츠 운영 및 시험에 집중할 수 있어 효율성이 향상될 수 있다.

3.2.2 사용자 환경

사용자가 자신의 원하는 애플리케이션 콘텐츠를 애플리케이션 마켓에서 선택하면 서비스 제공업체에서는 해당 애플리케이션 콘텐츠를 사용자 가상화 환경에 설치하여 사용자에게 서비스를 제공한다. 검증된 애플리케이션 콘텐츠만 사용자 가상화 환경에 설치되기 때문에 보안성이 보장된다. 또한 사용자의 스마트폰 기기는 애플리케이션 운영 서버에 접속하는 단말기의 기능만을 지니기 때문에 탈옥(Jailbreak)과 같은 방식을 사용할 수 없다.

## 4. 결론

안정적인 스마트폰 애플리케이션 콘텐츠 관리를 위해 본 논문에서는 스마트폰 애플리케이션 콘텐츠 통합 관리 모델을 제안하였다. 기존의 스마트폰 애플리케이션 콘텐츠에 대한 검증은 애플리케이션 마켓에서만 수행되었고 사용자는 애플리케이션 마켓에서 애플리케이션을 구입하여 스마트폰 단말 내에 설치하고 사용하였다. 하지만 악성코드가 삽입된 애플리케이션으로 인한 스마트폰 내에 저장되어있는 개인 정보 및 금융 정보가 유출되는 등 많은 문제점이 발생함에 따라 본 논문에서는 서비스 제공 업체에서 스마트폰 애플리케이션에 대한 검증을 수행하고 애플리케이션을 사용자 가상화 환경에 설치 및 관리하는 통합적인 애플리케이션 콘텐츠 관리 모델을 제안하였다.

## 참고문헌

[1] Gartner Report, “Gartner Identifies the Top 10 Srategic Technologies for 2009,” Gartner, 2009. 10.

[2] Collin Mulliner, Giovanni Vigna, David Dagon, and Wenke Lee, “Using Labeling to Prevent Cross-Service Attacks Against Smart Phones,” DIMVA 2006, Springer-Verlag, Lecture Notes in Computer Science 4064, pp. 91-108, 2006.

[3] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술,” 한국정보보호학회지, 제19권 제5호, pp. 21-28, 2009. 10.

[4] 배근태, 김기영, “모바일 단말 보안 운영체제 기술 동향,” 전자통신동향분석, 제23권 제4호, pp. 39-47, 2008. 8.

[5] 김대원, 김익균, 오진태, 장종수, 조현숙, “신종 사이버 공격 탐지 및 차단을 위한 인프라 구축 프로젝트,” 주간기술동향, 통권 1373호, pp.13-23, 2008. 11.