Journal of Korea Multimedia Society Vol. 13, No. 11, November 2010(pp. 1677-1686)

사전 검증 기법을 활용한 스마트폰용 애플리케이션 콘텐츠 관리 기법

박대식†, 곽 진††

요 약

안전한 스마트폰 사용 환경을 위해 애플리케이션 콘텐츠의 검증 및 운영은 필수적이다. 기존 스마트폰 환경에서의 애플리케이션 콘텐츠 검증은 애플리케이션 마켓 업체에서만 수행되었으며 해당 애플리케이션은 사용자가 직접 관리해야했다. 하지만 이러한 애플리케이션 콘텐츠 검증 및 관리에는 다양한 보안 취약점이 발생할 수 있다. 따라서 본 논문에서는 기존 방식에서의 보안 취약점을 분석하고 이를 기반으로 사전 검증 방식을 활용한 스마트폰용 애플리케이션 콘텐츠 관리 기법을 제안한다.

Pre-qualification based Application Contents Management Method for Smartphone

Dae-Sik Park†, Jin Kwak††

ABSTRACT

Application contents verifications and operations are essential for using a secure smart phone environment. In the existing smartphone environment, application verification was performed only in the application company and users has direct management application. However these application verification and management practices have been caused by a variety of security vulnerabilities. Therefore, we will analyze the security vulnerabilities in the existing methods and then we propose an application contents management of smart phone using pre-qualification method.

Key words: Smart Phone(스마트폰), Application Contents Management(애플리케이션 콘텐츠 관리), Pre-qualification(사전 검증)

1. 서 론

최근 모바일 컴퓨팅 기술의 급속한 발전으로 다양한 스마트폰들이 개발되고 있다. 스마트폰은 기존의 전화나 SMS 뿐 아니라 일정 및 연락처 관리, 모바일 결제, 사진 및 게임, 인터넷 기능 등 다양한 기능들을 제공한다. 특히 Wi-Fi 무선 네트워크와 3G망을 통한 데이터 전송이 가능하기 때문에 유비쿼터스 환경에서 유용한 도구가 될 것으로 예상된다.

또한 최근 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

※ 교신저자(Corresponding Author) : 곽진, 주소 : 충청남도 아산시 신창면 읍내리 646 순천향대학교 공과대학 정보보호학과(336-745), 전화 : 070)7516-6293, FAX : 041)530-4728, E-mail : jkwak@sch.ac.kr
접수일 : 2010년 7월 14일, 수정일 : 2010년 9월 16일
완료일 : 2010년 10월 8일
† 준회원, 순천향대학교 정보보호학과 석사과정
(E-mail : dspark@sch.ac.kr)
†† 종신회원, 순천향대학교 정보보호학과 학과장

출시되고 있어 모바일 스마트폰 시장 경쟁이 점차 치열해 질 것으로 예상된다[1].

스마트폰에는 애플리케이션 콘텐츠에 따라 다양한 기능들이 융합되어 있으며 사용자의 개인 정보 및 금융정보들이 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 제안하는 기법의 구성 요소와 동작 방식을 설명하고 4장에서 제안 기법과 기존 애플리케이션 콘텐츠 검증 및 관리 기법을 비교 분석하고 평가하며 5장에서 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, e-mail 전송, 웹 브라우저를 통한 인터넷 서비스 이용 등 부가기능을 결합한 제품으로써 최근에는 휴대전화를 통해 일반적인 유선 웹 사이트에 접근하는 개념으로 이동통신사의 무선 포탈이 제공하는 제한된 애플리케이션의 범위를 넘어 직접 URL 입력을 통해 유선 웹 포탈에 접속하는 풀 브라우징(Full Browsing)이 가능한 모바일 기기를 의미한다[2,3].

또한 기존의 휴대폰에서 사용되는 애플리케이션은 제조업체에서 제공하는 애플리케이션 외에 사용자가 추가적으로 설치 및 사용하지 못하였지만 스마트폰은 사용자가 직접 애플리케이션을 설치하고 사용할 수 있다.

그림 1은 스마트폰에서 애플리케이션 설치와 관련된 산업 구조를 보여주고 있다. 그림 1에서 볼 수 있듯이 스마트폰 사용자는 이동 통신사의 3G망이나 WiFi 등과 같은 네트워크 접속 방식으로 애플리케이션 마켓에서 애플리케이션을 다운받아 사용할 수 있다[4,5].

2.2 관련 기술 동향 및 취약점 분석

스마트폰의 애플리케이션 콘텐츠 관리 및 보안 기술은 크게 개발자 전자서명 기법, 시그니처(Signature) 기반 탐지 기법, 휴리스틱(Heuristic) 기반 탐지 기법으로 나눌 수 있다.

ㅁ 개발자 전자서명 기법

개발자 전자서명 기법은 애플리케이션 마켓에 업로드 할 개발된 애플리케이션에 개발자의 전자서명을 요구하여 전자 서명된 애플리케이션만 마켓에 등록하는 방식으로써 현재 스마트폰 애플리케이션 개방화를 주도하고 있는 구글의 안드로이드 마켓에서 시행하고 있으며 안드로이드 마켓의 애플리케이션 등록 절차는 그림 2와 같다.

하지만 안드로이드 마켓에서는 애플리케이션 등록에 따라 요구되는 개발자 서명을 신뢰도가 보장되지 않은 개발자 자체 서명도 허용함으로써 개발자 인증의 신뢰도가 부족하며 애플리케이션 등록 시 애플리케이션 보안성 및 정당성 검증 과정이 없기 때문에 악의적인 애플리케이션 등록이 용이하다. 실제로 2010년 1월 안드로이드 마켓에 은행 프로그램을 가장하여 이용자의 은행 패스워드를 훔쳐가는 악성코

그림 1. 스마트폰 산업 구조

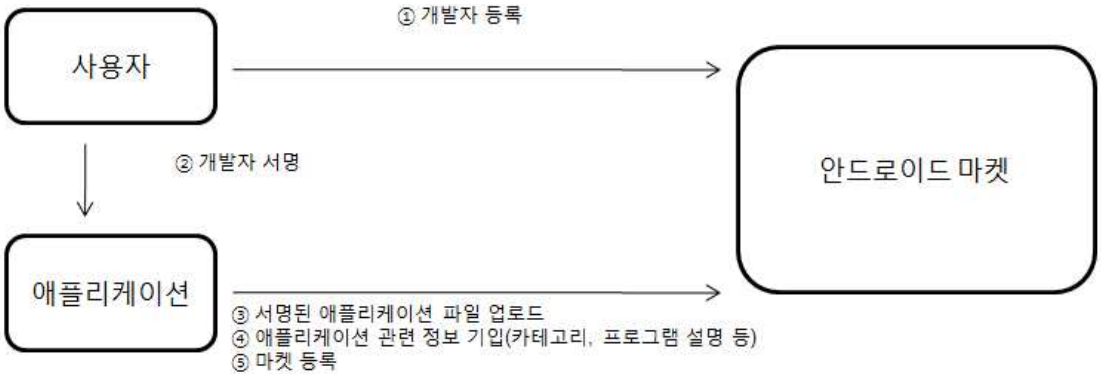

그림 2. 안드로이드 마켓 애플리케이션 등록절차

드가 삽입된 애플리케이션 판매 사례가 발생하는 등 애플리케이션 콘텐츠 검증에 대한 보안 취약점이 존재한다[4,6].

ㅁ 시그니처 기반 탐지 기법

시그니처 기반 탐지 기법은 악성코드의 시그니처를 수집 및 분석하여 데이터베이스화 한 후, 해당 애플리케이션 코드를 시그니처 데이터베이스와 비교하여 악성코드 삽입 여부를 판단하는 기법이다. 이러한 시그니처 기반 탐지 기법은 악성코드로 분류된 애플리케이션의 특정 및 고유 부분을 검사함으로써 오탐지(False Positive)나 미탐지(False Negative)를 최소화하여 정확한 진단이 가능하다는 장점과 애플리케이션 검사 시에 애플리케이션 코드의 특징적인 부분들만 비교함으로써 효율적으로 애플리케이션 코드를 진단할 수 있는 장점이 있다. 그러나 시그니처 기반 탐지 기법의 경우 시그니처 데이터베이스에 저장된 악성코드 시그니처와 악성코드가 포함된 애플리케이션 코드가 정확하게 일치되지 않는 경우 이를 탐지를 할 수 없으며 스마트폰의 경우 신종 및 변종 악성코드에 대한 실시간 시그니처 데이터베이스 업데이트를 수행하기 어렵기 때문에 다양한 보안 취약점이 발생할 수 있다[5].

ㅁ 휴리스틱 기반 탐지 기법

휴리스틱 기반 탐지 기법은 시스템의 룰과 패턴을 사용하여 알려지지 않은 악성코드를 탐지하기 위해 사용하는 기법으로써 정의된 비정상적인 기준들의 휴리스틱 룰셋과 디바이스에서 발생하는 모든 행위들을 실시간으로 분석하여 비정상적인 행위 발생 시 사용자에게 해당 정보를 통보한다. 하지만 휴대매체인 스마트폰의 경우, 모든 작업들에 대한 탐지가 이뤄질 경우 급격한 스마트폰 배터리 소모 문제와 오탐지 문제가 발생할 수 있다.

3. 제안하는 사전 검증 기법

앞서 2장에서 분석한 바와 같이 기존의 스마트폰 애플리케이션 콘텐츠 관리 기술들은 다양한 문제점들을 내포하고 있다. 따라서 본 장에서는 앞서 분석

표 1. 관련 기술의 관리 기술 및 보안 취약점

비교 항목 / 각 방식	관리 방식	보안 취약점
개발자 전자 서명 방식	‣ 애플리케이션 마켓 등록 시, 전자 서명된 애플리케이션만 마켓에 등록하는 방식	‣ 개발자의 자체 서명 허용에 따른 개발자 인증에 취약
시그니처 기반 탐지 기법	‣ 악성코드의 시그니처를 데이터베이스화하고 데이터베이스를 기반으로 악성코드 탐지	‣ 신종 및 변종 악성코드 탐지 불가 ‣ 실시간 시그니처 데이터베이스 업데이트가 어려움
휴리스틱 기반 탐지 기법	‣ 악성코드 실행에 따른 시스템의 룰과 패턴을 분석하여 악성코드 탐지	‣ 모든 행동 패턴 분석에 따른 시스템 자원 소모 ‣ 정상적인 행위에 대한 오탐지 발생 가능성 존재

한 문제점들을 해결할 수 있는 사전 검증 기법을 이용한 스마트폰 애플리케이션 콘텐츠 관리 기법을 제안한다.

3.1 시스템 개요

본 논문에서 제안하는 애플리케이션 콘텐츠 관리 기법의 전체적인 흐름은 그림 3과 같으며 각 단계는 애플리케이션 이용까지 총 7단계로 구성되어 있다. 각 단계별 절차는 다음과 같다.

step 1 : 사용자는 자신의 스마트폰 기기를 이동통신사에 등록한다.

step 2 : 이동통신사는 사용자와 스마트폰의 정보를 바탕으로 클라우드 서버에 해당 사용자의 모바일 컴퓨팅 환경을 구축한다.

step 3 : 사용자는 스마트폰 애플리케이션 마켓에서 애플리케이션을 구입한다.

step 4 : 애플리케이션 마켓에서는 사용자 등록정보를 바탕으로 사용자가 구입한 애플리케이션을 사용자가 이용하는 이동통신사에 전송한다.

step 5 : 이동통신사는 애플리케이션 마켓에서 전송받은 애플리케이션을 검증하기 위해 자체적으로 구성한 가상화된 테스트 서버에서 애플리케이션 콘텐츠 검증을 실시한다.

step 6 : 가상화된 테스트 서버에서 애플리케이션 콘텐츠 검증이 완료되면 클라우드 서버의 해당 사용자의 모바일 컴퓨팅 환경에 애플리케이션을 설치한다.

step 7 : 애플리케이션 설치가 완료되면 사용자가 애플리케이션 사용 요청 시, 이동통신사에서는 사용자에게 서비스를 제공한다.

3.2 구성 요소

본 논문에서 제안하는 스마트폰 애플리케이션 콘텐츠 관리 기법은 클라우드 컴퓨팅 환경에서 스마트폰 애플리케이션 관리를 용이하게 하며 애플리케이션에 대한 오류 검증 및 안전성 검증을 제공한다. 제안하는 스마트폰 애플리케이션 콘텐츠 관리 기법의 구성요소는 다음과 같다.

- 클라우드 테스트 서버(Cloud Test Server)
- 데이터베이스 서버(Data Base Server)
- 클라우드 데이터 서버(Cloud Data Server)
- 보안 알고리즘(Security Algorithm)

클라우드 테스트 서버는 사용자가 설치하고자 하는 스마트폰 애플리케이션에 대한 오류 및 안전성 검증을 수행하여 애플리케이션에 대한 직접적인 검증을 수행한다. 데이터베이스 서버는 다양한 데이터베이스를 통해 애플리케이션을 검증하고 검증된 애

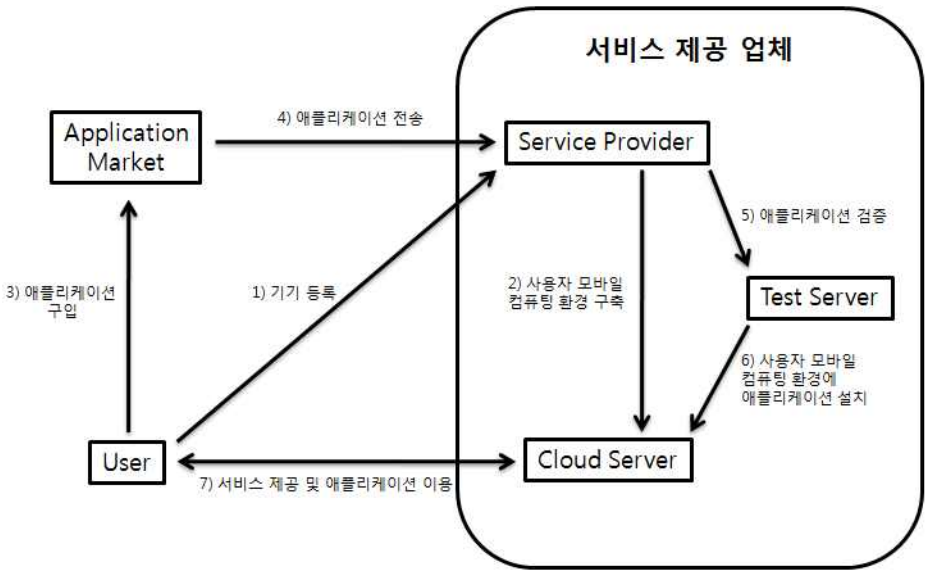

그림 3. 제안 기법의 개념도

플리케이션을 목록화하여 보관하는데 사용된다. 클라우드 데이터 서버는 테스트 서버에서 검증된 애플리케이션을 사용자가 사용할 수 있도록 사용자에 적합한 환경을 구축하여 애플리케이션을 설치하며 사용자의 개인 정보를 저장한다. 보안 알고리즘은 사용자의 개인 정보를 안전하게 보관하기 위해 사용되는 다양한 알고리즘들을 의미한다.

3.2.1 클라우드 테스트 서버

클라우드 테스트 서버는 제안 기법에서 중요한 구성요소로써 사용자가 설치하고자 하는 스마트폰 애플리케이션을 검증한다. 클라우드 테스트 서버에는 애플리케이션을 테스트할 가상화 환경이 구축되어 있으며 구축된 가상화 환경에서 애플리케이션 검증을 진행한다. 클라우드 테스트 서버는 크게 오류 탐지 모듈, 보안 모듈, 장비 모듈로 구성되어 있다.

오류 탐지 모듈을 통해 애플리케이션에 대한 오류를 탐지하고 오류가 발견되지 않은 애플리케이션을 보안 모듈로 전송한다. 보안 모듈은 다양한 데이터베이스를 이용하여 애플리케이션 콘텐츠를 검증하고 장비 모듈에 전송한다. 장비 모듈은 스마트폰의 비 이상적인 기능사용에 대한 검증을 실시한다. 클라우드 테스트 서버를 구성하는 요소는 표 2와 같다[7].

3.2.2 데이터베이스 서버

데이터베이스 서버는 애플리케이션 콘텐츠 검증에 필요한 데이터베이스를 제공한다. OS 정책 데이터베이스는 스마트폰의 OS의 정책에 따라 애플리케이션이 개발되었는지 확인하는데 이용된다. 화이트리스트 데이터베이스는 신규 애플리케이션에 대한 평판 정보들을 실시간으로 분석 및 저장하고 블랙리스트 데이터베이스는 악성코드 및 바이러스와 같은 공격기법들의 정보를 저장하여 보안성 검증에 이용된다. 장비 기능 데이터베이스는 스마트폰 기능에 대한 정보들이 저장되어 장비 모듈에서 애플리케이션을 검증할 때 이용된다. 신뢰리스트 데이터베이스에는 검증된 애플리케이션의 정보가 저장되어 동일한 애플리케이션 콘텐츠 검증을 간소화하여 애플리케이션 콘텐츠 검증에 따른 시스템 오버헤드를 최소화한다.

3.2.3 클라우드 데이터 서버

클라우드 데이터 서버는 사용자 정보를 바탕으로 사용자의 가상화 환경을 구축하여 검증된 애플리케이션을 사용자가 이용할 수 있도록 서비스를 제공한다. 사용자 애플리케이션에는 테스트 서버를 통해 검증된 애플리케이션이 설치된다. 서비스 모듈은 사용자에게 애플리케이션을 이용할 수 있게 서비스를 제공하며 실시간 분석기에서는 애플리케이션에 대한 지속적인 악성코드 및 바이러스 탐지를 제공한다. 사용자 정보 스토리지는 사용자의 연락처, 사진 등의 사용자 개인 정보를 저장한다. 이를 통해 사용자의 스마트폰은 클라우드 데이터 서버에 접속하는 단말기의 기능만을 지닌다.

3.2.4 보안 알고리즘

보안 알고리즘은 클라우드 데이터 서버에 저장된 사용자 개인 정보 유출을 막기 위해 사용되는 암호화 알고리즘을 말한다. 보안 알고리즘은 지속적으로 강력한 알고리즘으로 업데이트하여 효과적으로 사용자 개인 정보를 관리한다.

3.3 동작 방식

본 논문에서 제안하는 애플리케이션 콘텐츠 관리 기법은 그림 4와 같으며 동작 방식은 크게 3가지 단계로 나눌 수 있다.

각 단계는 1) 모바일 환경 구축 단계, 2) 애플리케이션 콘텐츠 검증 단계, 3) 애플리케이션 운영 및 서비스 단계로써 각 단계별 동작 방식은 다음과 같다.

표 2. 클라우드 테스트 서버 구성 요소

구성 요소	기 능
오류 탐지 모듈 (Error Detection Module)	애플리케이션 마켓에서 전송받은 애플리케이션의 오류 및 무결성 검증
보안 모듈 (Security Module)	애플리케이션 코드를 분석하여 코드 내에 적재되어 있는 악성코드 및 바이러스 탐지
장비 모듈 (Device Module)	애플리케이션의 기능에 따라 스마트폰의 비 이상적인 기능사용 탐지

(1) 모바일 환경 구축 단계

모바일 환경 구축 단계에서는 그림 4의 ①에 해당되는 단계로써 사용자와 서비스 제공업체간 등록 및 모바일 환경 구축이 진행되는 단계이다. 사용자는 서비스 제공업체와 서비스 계약을 체결한다. 서비스 제공업체는 사용자의 스마트폰의 정보를 기반으로 자사의 클라우드 데이터 서버에 사용자의 가상화 운영체제를 구성하고 애플리케이션 마켓의 정보를 실시간으로 동기화하여 사용자에게 보여준다.

(2) 애플리케이션 콘텐츠 검증 단계

애플리케이션 콘텐츠 검증 단계는 그림 4의 ②, ③, ④, ⑤에 해당되는 단계로써 단계별 수행되는 과정은 다음과 같다.

② 애플리케이션 선택 단계 : 사용자는 서비스 제공업체에서 실시간으로 동기화한 애플리케이션 마켓의 정보를 바탕으로 애플리케이션 선택한다.

③ 애플리케이션 확보 단계 : 애플리케이션 마켓은 사용자가 선택한 애플리케이션을 사용자의 서비스 제공업체의 클라우드 테스트 서버에 전송한다.

④, ⑤ 애플리케이션 콘텐츠 검증 단계 : 전송받은 애플리케이션을 검증하기 위한 단계이며 애플리케이션 콘텐츠 검증 단계에서는 해당 애플리케이션의 검증을 위해 2가지 모듈을 통해 애플리케이션을 검증한다.

1) 오류 탐지 모듈 : 서비스 제공업체가 최초 애플리케이션 마켓에서 애플리케이션을 전송받고 검증을 수행하는 단계로 애플리케이션의 무결성과 가용성을 검증하는 모듈이다. 애플리케이션 마켓에 저장된 정보와 전송받은 애플리케이션을 비교분석함으로써 애플리케이션 위·변조에 대한 검증을 수행하며 가상화된 테스트 환경을 구축하여 애플리케이션 실행 시 발생할 수 있는 오류들을 검증한다. 그림 5는 오류 탐지 과정을 흐름을 보여준다.

2) 보안 및 디바이스 모듈 : 오류가 발생되지 않은 애플리케이션에 대해 악성코드 및 바이러스 감염 유·무를 검증하는 모듈로 가상화된 테스트 환경에서 데이터베이스 서버에 구축되어 있는 데이터베이스를 바탕으로 실시간 평판 기반 탐지 및 행위 기반 탐지를 통해 애플리케이션을 검증하는 단계이다. 또한 검증된 애플리케이션은 버전, 개발일, 개발자 등의 애플리케이션 정보를 데이터베이

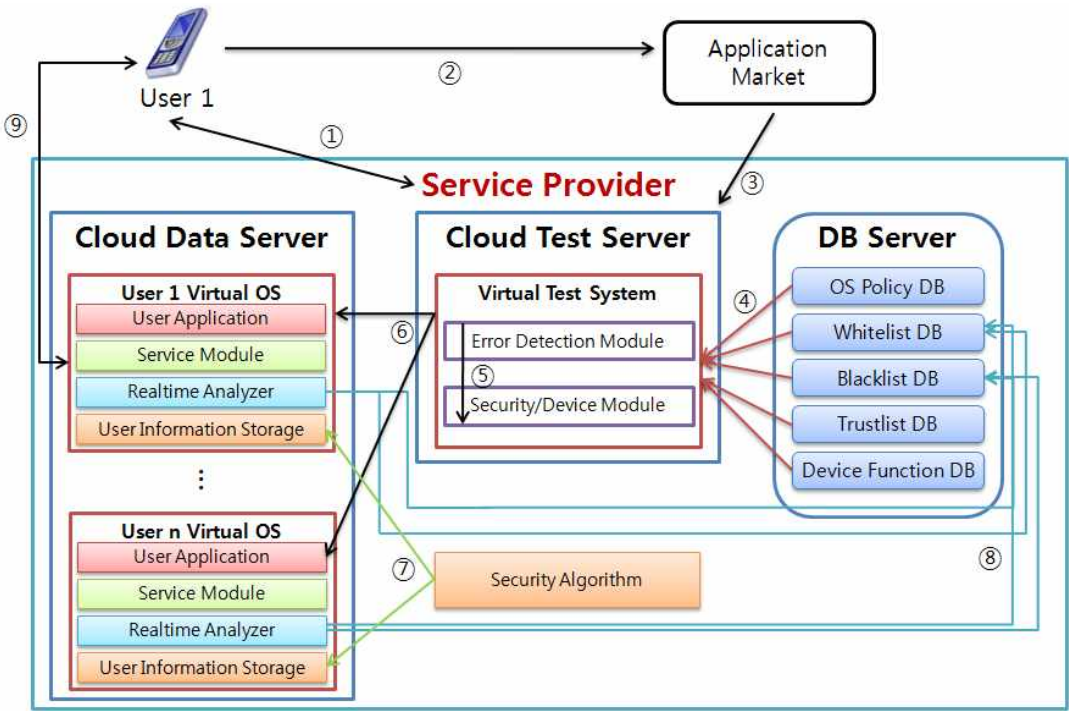

그림 4. 제안된 애플리케이션 콘텐츠 관리 기법 구성도

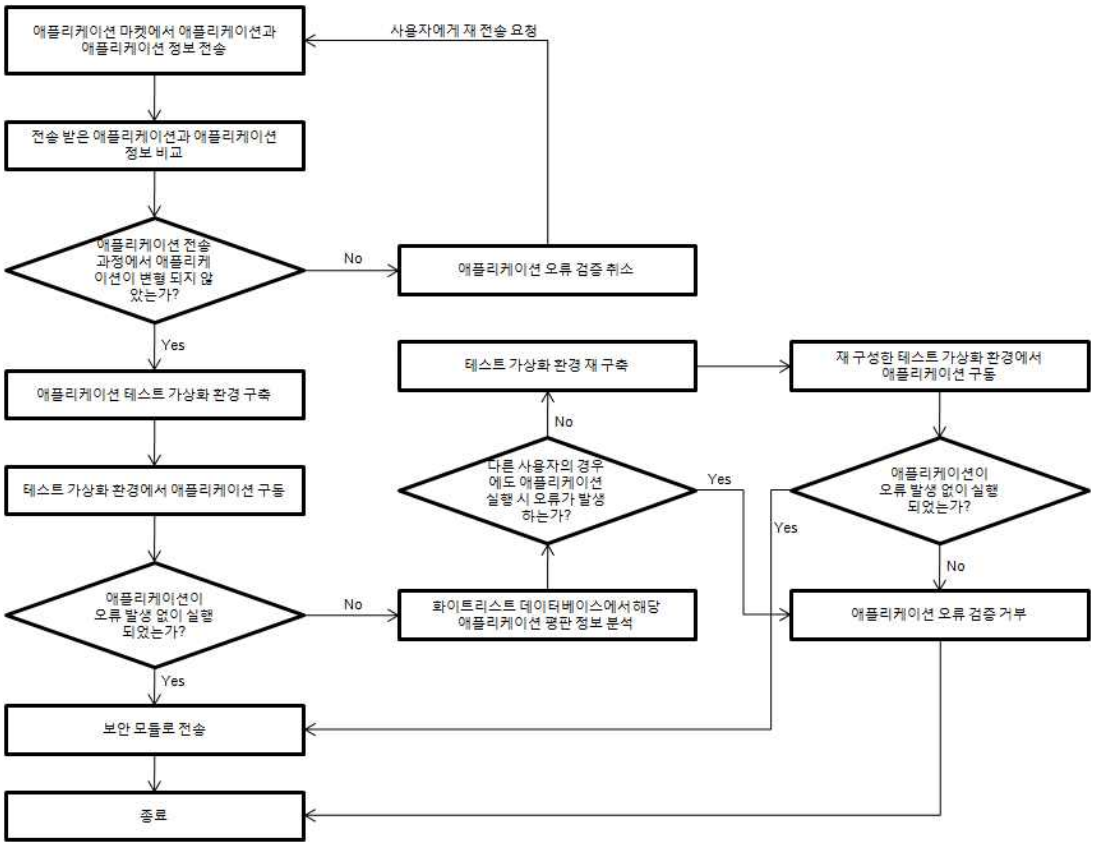

그림 5. 애플리케이션 오류 탐지 과정의 흐름도

스화하여 저장하고 차후, 동일한 애플리케이션의 재검증을 생략하여 불필요한 시스템 자원 사용을 최소화한다. 그림 6은 보안 검증 과정의 흐름을 나타낸다.

(3) 애플리케이션 운영 및 서비스 단계

애플리케이션 운영 및 서비스 단계는 그림 4의 ⑥, ⑦, ⑧, ⑨에 해당되는 단계로써 검증된 애플리케이션을 클라우드 데이터 서버에 지정된 사용자 컴퓨팅 환경에 설치하고 사용자에게 서비스를 제공하는 단계이다.

⑥, ⑦, ⑧ 애플리케이션 운영 단계 : 클라우드 테스트 서버에서 검증이 완료된 애플리케이션을 클라우드 데이터 서버 내의 사용자의 가상화 OS에 구축된 사용자 애플리케이션 환경에 설치한다. 설치된 애플리케이션은 실시간 분석기를 통해 지속적으로 분석이이루어지며 분석 결과는 실시간으로 데이터베이스에 저장된다. 이를 통해 앞서 2장에서 분석한 행위기반 탐지 기법의 문제점인 배터리 소모 문제와 스마트폰 단말기의 불필요한 시스템 자원 사용 문제를 해결한다. 또한 모든 애플리케이션과 개인 정보를 서비스 제공업체에서 관리함에 따라 악성코드 및 바이러스 발견 시, 신속하게 애플리케이션을 관리할 수 있으며 스마트폰 분실에 따른 개인 정보 유출을 최소화할 수 있다.

⑨ 서비스 단계 : 사용자의 서비스 이용 요청 시, 가상화 OS를 통해 지정된 사용자에게 서비스를 제공한다.

4. 비교분석

본 장에서는 제안 기법과 기존 애플리케이션 콘텐츠 검증 및 관리 기법을 비교 분석하여 평가한다.

표 3은 제안한 기법과 기존 검증 및 관리 기법을 비교 분석한 것이다. 구글사의 개발자 전자서명 기법은 앞서 2장에서 언급한 바와 같이 애플리케이션 보

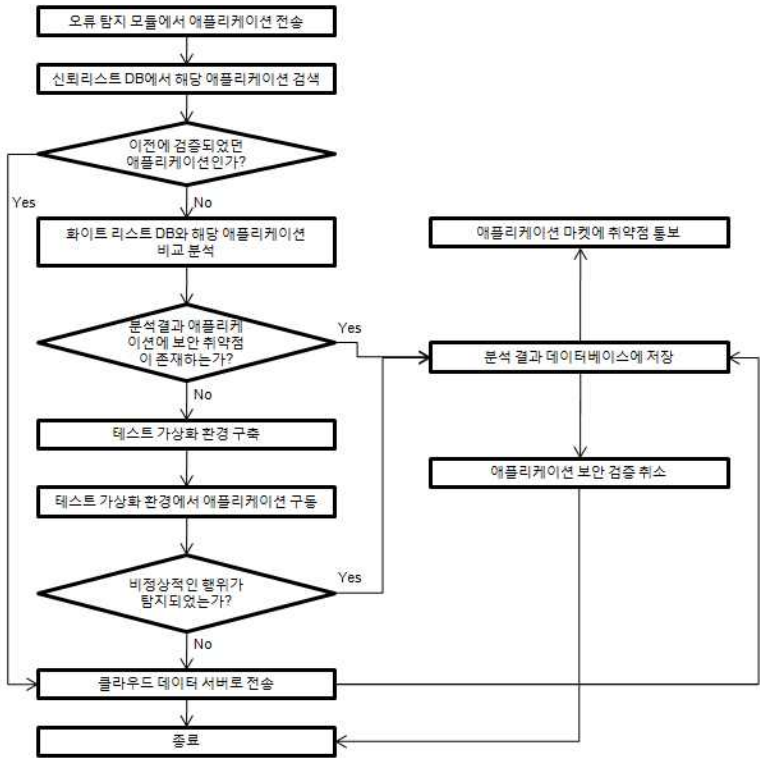

그림 6. 애플리케이션 보안 검증 과정의 흐름도

안성 및 정당성 검증 과정이 없기 때문에 악성코드가 삽입된 애플리케이션을 검증할 수 있는 방안이 미비함에 따라 악성코드가 삽입된 애플리케이션이 유포되는 등 문제점이 발생하였다. 하지만 제안 기법에서는 애플리케이션을 설치하기 전에 서비스 제공업체의 클라우드 테스트 서버에서 애플리케이션에 대한 오류 검증 및 보안 검증이 수행되어 애플리케이션의 보안성을 확보할 수 있다.

애플리케이션 설치 시, 애플리케이션 무결성 검증에 있어 시그니처 기반 탐지 기법 및 휴리스틱 기반 탐지 기법은 애플리케이션 구동에 따른 코드 및 행동 패턴들을 검출하는데 사용되는 데이터베이스 통해 작업을 수행한다. 하지만 해당 데이터베이스는 애플리케이션에 대한 기본정보를 저장하고 있지 않기 때문에 애플리케이션에 대한 무결성을 검증할 수 없다. 그러나 본 제안 기법은 애플리케이션 마켓에 등록된 애플리케이션과 마켓으로부터 전송받은 애플리케이션을 코드사이닝 기술을 적용하여 비교・분석하고 무결성을 제공한다.

개발자 전자서명 기법은 애플리케이션 등록, 검증 및 설치와 관련된 환경만을 관리하고 애플리케이션이 사용자의 스마트폰에 설치된 이후에는 직접적인 관리를 하지 않기 때문에 실시간 애플리케이션 콘텐츠 관리의 문제점이 발생한다. 또한 시그니처 기반 탐지 기법 및 휴리스틱 기반 탐지 기법에서 실시간으로 애플리케이션 콘텐츠 관리를 수행하기 위해서는 악성코드에 대한 데이터베이스를 실시간으로 관리 및 업데이트를 수행이 요구된다. 하지만 시그니처 기반 탐지 기법 및 휴리스틱 기반 탐지 기법의 경우 사용자 스마트폰 내에 백신 애플리케이션을 설치하고 실시간으로 데이터베이스 업데이트를 수행하여 사용자가 직접 애플리케이션에 대한 업데이트를 수행해야하기 때문에 애플리케이션에 대한 실시간 관리에는 한계가 있다. 또한 시그니처 기반 탐지 기법 및 휴리스틱 기반 탐지 기법은 사용자의 개인정보 보호에 있어서 데이터베이스를 기반으로 악성코드를 검출한다. 하지만 앞서 언급한 바와 같이 사용자가 직접 애플리케이션에 대한 업데이트를 수행해야

표 3. 제안 기법과 기존 애플리케이션 콘텐츠 검증 및 관리 기법 비교 분석

비교 항목 / 각 방식	애플리케이션 보안성 검증	애플리케이션 설치 시, 무결성 제공	실시간 애플리케이션 콘텐츠 관리	사용자 개인정보 보호
개발자 전자 서명 기법	X	O	X	X
시그니처 기반 탐지 기법	O	X	△	△
휴리스틱 기반 탐지 기법	O	X	△	△
제안 기법	O	O	O	O

(O : 가능, △ : 부분적 가능, X : 불가능)

하기 때문에 실시간 관리의 어려움이 따른다[8].

제안 기법에서는 사용자의 애플리케이션이 클라우드 서버 내의 사용자 가상화 환경에 설치되며 구동 및 관리되기 때문에 실시간으로 업데이트된 데이터베이스를 적용하여 애플리케이션을 분석하고 문제점이 발생하였을 경우, 신속한 대응 조치가 가능하다. 또한 제안 기법은 클라우드 서버 내의 사용자 가상화 환경에서 사용자의 개인정보를 저장하고 실시간으로 데이터베이스를 기반으로 악성코드를 검출하기 때문에 개인정보 유출을 방지할 수 있다.

5. 결 론

안정적인 스마트폰 애플리케이션 콘텐츠 관리를 위해 본 논문에서는 클라우드 시스템을 도입하여 사전 검증 방식을 활용한 스마트폰용 애플리케이션 콘텐츠 관리 기법을 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 제공업체에서 스마트폰 애플리케이션에 대한 검증을 수행하고 애플리케이션을 클라우드 서버의 사용자 가상화 환경에 설치 및 관리함으로써 통합적인 애플리케이션 콘텐츠 관리와 스마트폰 자원 사용의 오버헤드를 최소화한 스마트폰 애플리케이션 콘텐츠 관리 기법을 제안하였다.

향후 계획으로는 본 논문에서 제안한 사전 검증 방식을 활용한 스마트폰용 애플리케이션 콘텐츠 관리 기법을 바탕으로 스마트폰 애플리케이션 사용에 따른 사용자 접근 제어 모델과 프로토콜을 개발하고자 한다.

참 고 문 헌

[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] 김성개, “사용자 환경과 스마트폰 특성 요인이 인지된 유용성과 사용용이성 및 수용의도에 미치는 영향에 관한 연구,” 홍익대학교 광고홍보대학원 석사학위 논문, 2009. 6.

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

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

[6] Kadra Alvaro, “Android Security : Investigating Google's Mobile OS,” http://whitearray.com/2010/06/android-security, 2010.

[7] 이광근, “무결점 소프트웨어 검증 기술,” 정보과학회지, 제24권 제12호, pp. 17-20, 2006. 3.

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

박 대 식

2010년 순천향대학교 정보보호학과 학사
2010년~현재 순천향대학교 정보보호학과 석사과정
관심분야 : 정보보호, 평가 및 인증, 스마트폰, 클라우드 컴퓨팅 등

곽 진

성균관대학교 학사, 석사, 박사(2000, 2003, 2006)
2006~2006 일본 큐슈대학교 방문연구원
2006~2006 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009 정보통신연구진흥원 집필위원
2007~현재 정보통신산업진흥원 기술평가위원
2008~현재 디지털아이디관리포럼 운영위원
2009~현재 한국정보통신기술협회 JTC/SC27 분과 기술위원
2009~현재 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원
2009~현재 순천향대학교 정보보호학과 학과장
2009~2009 순천향대학교 공과대학 교학부장
2010~현재 순천향BIT 창업보육센터 소장
2010~현재 사)국제정보능력평가원 쇼핑몰 플래너 자격검정 출제 및 채점위원
2010~현재 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원
2010~현재 교육과학기술부 국가기술 수준 평가 전문위원
2010~현재 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원
2010~현재 지식경제부 지식경제기술혁신평가단 평가위원
관심분야 : 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등