情 報 保 護 學 會 誌
第23卷 第2號, 2013. 4

모바일 어플리케이션 분석 및 검증 솔루션 구현 사례

고 승 원*, 정 상 곤**

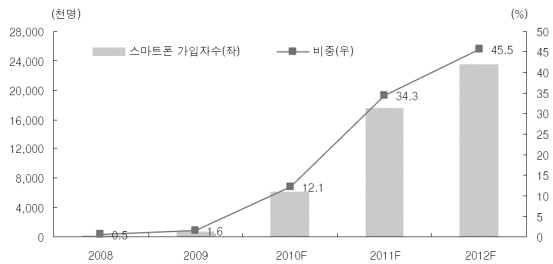
요 약

스마트폰의 급증 현상은 모바일 생태계의 패러다임을 변화시켰으며 다양한 SW 컨텐츠의 양산과 더불어 그 활용 영역의 확대를 가져왔다. 이에 따라 필연적으로 모바일 악성코드도 증가되고 있으며 개인정보 또는 회사 기밀정보의 무단 유출이라는 사회적 이슈도 대두되게 되었다. 이러한 문제를 해결하기 위해서는 모바일 어플리케이션에 대한 검증이 필요하고, 검증하는 방법에는 크게 정적분석 방법과 동적분석 방법이 있으며 분석 방법에 대한 자세한 내용은 선배 전문가들의 앞선 연구 사례와 논문에 몇 차례 소개된 바 있다.

이에 본 고에서는 정적분석 및 동적분석 방법을 응용하여 (주)안랩에서 실제로 운용 중인 모바일 어플리케이션의 분석 및 검증 솔루션(AMSD) 구현사례를 소개하고자 한다. 여기에는 기 알려진 정적분석 방법과 동적분석 방법에 대한 간략한 서술이 포함되어 있으며 시스템 아키텍처 정보와 실제 오픈 마켓을 대상으로 운용하면서 얻어진 앱 분석 사례 및 개선 방향도 담고 있다. 이를 통해 모바일 오픈 마켓 운영 시의 안전성과 신뢰성 확보 및 건전한 모바일 생태계 유지를 도모하는 데 조금이나마 도움이 되었으면 하는 바램이다.

Ⅰ. 서 론

모바일 시장은 2009년을 기점으로 스마트폰 시장이 폭발적인 성장세를 보이고 있으며 Apple社 AppStore로 대표되는 OMP(Open Market Price)의 등장으로 기존 모바일 생태계의 패러다임도 변화되었다. 이는 전통적으로 제조사와 이통사 중심이던 모바일 시장의 수익 모델이 새로운 부가가치를 창출하는 무선 데이터 통신과 SW 컨텐츠 유통 분야로 다각화되는 계기가 되었다.



〔그림 1〕 국내 모바일 시장 현황
출처 : KTOA(한국통신사연합회) 보도자료, 2012년

게다가 Google社 Android와 같은 개방형 모바일 플랫폼이 등장하면서 모바일 플랫폼의 무게 중심이 기존 피처폰 중심의 폐쇄형 플랫폼 환경에서 스마트폰 중심의 개방형 플랫폼 환경으로 더욱 더 급속히 이동 하게 되었으며, 근래에는 오히려 신규 피처폰의 출시를 접하기 힘든 상황이 되었다.

이렇듯 스마트 디바이스 수요 급증에 따라 소프트웨어 컨텐츠 유통이 늘어나고 그 활용 영역도 확대되면서 무선 인터넷과 웹 서비스를 활용하는 무선 통신량도 더불어 폭발적으로 증가하고 있고 스마트워킹으로 표현되는 모바일오피스의 필요성도 대두되었다.

이는 기존 PC 환경 중심의 클라우드 연계 서비스로의 확장과 모바일 금융, U-헬스와 같은 생활 서비스 인프라 전반으로의 영역 확대를 필연적으로 동반한다.

그러나 이러한 모바일 인프라와 활용 영역의 확대는 부작용 또한 필연적으로 동반하게 됨으로써 모바일 환경에서의 보안 이슈도 함께 대두되고 있다.

일단 모바일 마켓은 일련의 등록 절차만 거치면 누구나 업로드 가능한 특성을 지니고 있기 때문에 악성코드

* ㈜안랩 연구소 융합제품개발실 (swko@ahnlab.com)
** ㈜안랩 연구소 융합제품개발실 (sanggon.jung@ahnlab.com)

〔그림 2〕 모바일 서비스 인프라

유포 경로로 활용되기가 쉽다. 또한 모바일 기기의 활용 영역이 확대됨에 따라 PC를 대체하는 가장 Personal한 기기가 되었으며 이에 따라 기기 내 정보의 가치와 중요성도 상대적으로 부각되게 되었다.

특히 모바일 기기가 PC에 비해 더 위험한 점은 손쉽고 직접적인 과금 결제 수단을 내재하고 있기 때문이다. 사용자도 모르는 사이에 과금이 이루어진다거나 스미싱(SMS+Fishing)과 같은 공격에 의해 금전적인 손실을 보게 되는 피해 사례를 근래에는 빈번하게 접할 수 있는 상황에 직면해 있다.

그러나 현재 모바일 마켓의 신뢰도 높은 애플리케이션 검증 시스템은 전무한 상황이며 안드로이드와 같은 개방형 플랫폼 환경을 위한 경쟁력 있는 국내 모바일 보안 솔루션 또한 한 손으로 꼽을 수 있을 정도로 부족하다.

이처럼 개방형 모바일 플랫폼과 통신 환경을 이용한 외부의 악의적인 해킹 시도로부터 모바일 기기의 안전을 지켜주는 장치가 미흡하기 때문에 일부 무료 어플 설치 시에 무단 과금 및 개인정보 유출 사고가 발생하고 모바일 금융 거래 시에는 거래 정보를 도용하거나 계좌 정보를 유출시키는 사고가 발생되고 있다. 또한 사용자에게 적법한 내용을 고지한 후 동의를 구하지 않은 채로 위치 정보 또는 개인 정보를 무단 수집하거나 소셜 네트워크 애플리케이션을 이용한 트래픽 점유 및 피싱, 파밍 사고마저 빈번히 발생하고 있는 형편이다.

이러한 보안 위험성을 방치할 경우에는 개방화된 모바일 서비스를 막고 어플리케이션의 원활한 공급과 유통을 힘들게 하여 결과적으로는 모바일 마켓과 컨텐츠 및 서비스의 전체적인 성장을 저해하기 때문에 신규 플랫폼과 오픈 마켓을 보호하기 위한 보안 연구가 지속적으로 이루어져야 하고 악의적인 공격으로부터 모바일 생태계를 방어할 장치 마련이 필요하다.

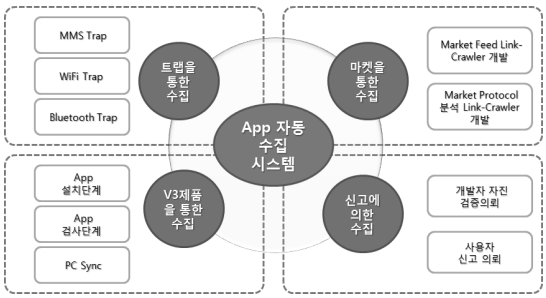
이에 본 고에서는 ㈜안랩에서 구축하여 운용중인 모바일 앱 분석 및 검증 인프라 구축 사례에 대한 기술을 소개하고 개략적으로 살펴봄으로서 향후 모바일 환경에서의 악성 코드 사전 탐지와 방어 솔루션 구축에 도움이 되고자 한다.

Ⅱ. AMSD 소개

자사에서 개발한 모바일 앱 분석 및 검증 인프라는 지식경제부 산업기술평가원에서 수행한 WBS 보안과제의 산출물로서 AMSD(AhnLab Mobile Smart Defense)라 일컬어진다. AMSD는 앱 마켓 연동, 크로울러 자동 수집 등 다양한 경로를 통해서 모바일 애플리케이션을 수집하고 이를 정적 또는 동적으로 분석하여 악성 코드들의 유통과 확산을 방지하기 위한 모바일 악성코드 탐지 및 방어 솔루션이자 서비스 인프라 그 자체이다.

2.1. AMSD의 특징

AMSD 솔루션의 주된 특징은 다음과 같이 요약된다.

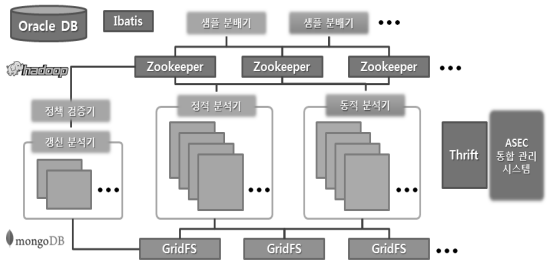


〔그림 3〕 AMSD의 다양한 수집 채널

- 능동적이고 적극적인 다 채널의 샘플 수집을 통한 사전 분석과 위험 감지
- 정적 코드 분석 기술과 진보된 동적 행위 분석 기술의 조합 및 인력에 의존하지 않는 자동화 시스템 구축
- 동적 행위 분석 기술과 자동화 분석 시스템을 통

해 사후 대처 방식에서 사전 예측 방식으로 보안 패러다임 진화 추구

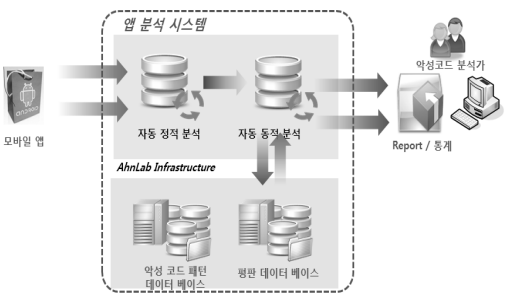
- 급증하는 모바일 App에 대한 안정적인 분석 처리와 확장성을 추구하기 위한 Cloud 기술 기반의 아키텍처 구성



〔그림 4〕 AMSD의 분산 처리 구조

2.2. AMSD의 분석 기법

AMSD의 분석 기법은 본래 의학 분야에서 이루어지고 있는 종합 검진 방법에 착안하여 고안되었다.



〔그림 5〕 AMSD의 분석 기법

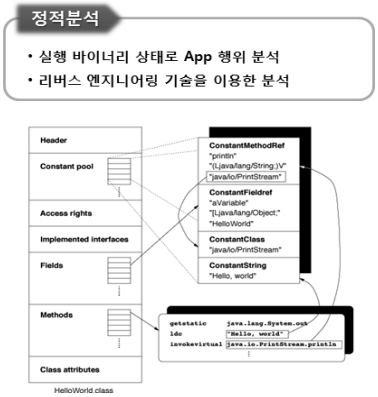
즉 의사들이 환자의 진찰을 위해 한 가지가 아닌 각종 검사를 병행하여 그 결과를 다각도로 보고 증세를 종합적으로 진단하듯이, 분석 솔루션에서도 바이너리 상태의 모바일 앱을 대상으로 특성이 다른 복수 개의 분석 방법을 통해 앱의 성향과 행동 특성을 심층 분석하여 그 위험 요소를 자동화된 프로세스를 통해 파악하고, 도출된 결과에 대해서 필요할 경우에는 악성코드 분석가들이 최종적으로 악성여부를 진단하도록 설계되어 있다.

여기에 추가적으로 악성코드 패턴 데이터베이스와 평판 데이터베이스를 연계시켜 분석 과정에서 분석가가 참고할 수 있게 함으로서 보다 더 세밀하고 정확한 판단이 가능하도록 지원한다.

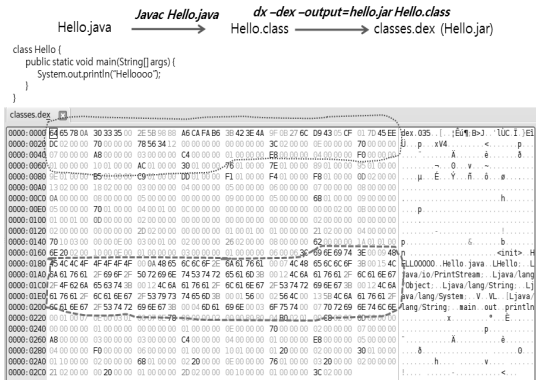
Ⅲ. AMSD 정적 분석 시스템

3.1. 모바일 어플리케이션의 정적 분석 기법

정적 분석 기법이란 모바일 어플리케이션에 대한 시그니처나 파일 구성 정보 등 대상 플랫폼 고유의 정적인 특성을 추출하거나 복호화 및 역공학 기술을 이용하여 소스 레벨의 내부 정보를 파악함으로써 앱의 행위나 위험성을 역으로 분석해 나가는 방법을 말한다.



〔그림 6〕 정적 분석 방법의 개념

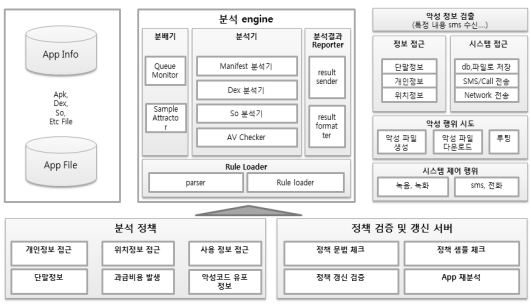


〔그림 7〕 Reverse engineering을 적용한 정적 분석 예

정적 분석 기법에 대한 자세한 설명은 선행 연구와 논문 등에서 이미 여러 차례 언급된 적이 있으므로 본고에서는 생략하도록 한다.

3.2. AMSD의 정적 분석 시스템

정적 분석 기법을 적용한 시스템은 분석 속도가 빠를 뿐만 아니라 진단 정책을 변경할 때 외에는 사람이 개입할 필요가 없어 자동화 실현에 용이하다. 자사 AMSD 솔루션에도 자동화된 정적 분석 시스템을 마련함으로써 최근 모바일 앱 수가 급속도로 늘어나고 있는 상황에서 어플리케이션 검증 또는 악성코드 분석가의 부담을 줄이고 효율적인 분석 프로세스를 마련하는데 기여하고 있다.



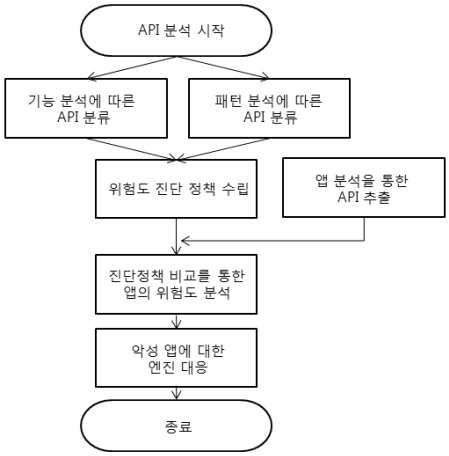
〔그림 8〕 AMSD 정적 분석 시스템의 개요

그리고 자사의 정적 분석 시스템에는 기존에 알려진 정적 분석 기법에 더하여 API 위험도 기반의 분석 방법이라는 차별화된 분석 정책을 채택하고 있다.

API 위험도 기반의 분석 방법이란 다음과 같다.

안드로이드 플랫폼 내의 API 들을 해당 행위 또는 위험 요소별로 분석 및 분류하고 이에 따라 단일 API, API 조합 등으로 나눠 각각에 위험도 가중치를 부여함으로써 위험도 진단 정책을 작성한다. 이후, 앱을 역공학으로 분석하여 앱 내의 안드로이드 플랫폼 API를 추출하고 상기 진단 정책을 통해 앱을 분석함으로써 앱의 기능적 성향과 위험도를 분석하고 진단, 예측할 수 있는 방법이다.

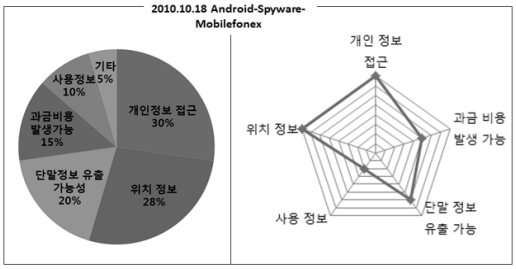
이와 같은 API 위험도 기반 분석 방법을 이용하면 앱 분석을 자동화하는 시스템을 구축하여 분석가에 의존하지 않고도 안드로이드 앱의 성향과 위험도를 보다 객관적이고 빠르게 분석해 낼 수 있을 뿐만 아니라 전체 API의 분포를 분석해 냄으로써 위험 요소별 API 분포도와 위험도라는 정량적 수치를 가지고 모바일 디바이스 사용자에게 향후 예측되는 위험 요소 및 리스크(Risk)에 대한 가이드를 제공할 수 있다.



〔그림 9〕 API 위험도 정책에 기반한 앱 분석 절차

또한 위험도가 일정 수준 이상이 되는 앱만 분석가에게 상세 분석을 의뢰함으로써 악성코드 분석가의 업무 부담을 획기적으로 줄일 수 있다.

아래 [그림10]은 안드로이드 샘플 앱[2010.10.18 Android-Spyware-Mobilefonex]에 대한 API별 성향을 위험도 진단 기법을 통해 비교 분석하여 나타낸 그래프로써 앱에 대한 특성 및 위험도를 한눈에 보기 쉽게 파악할 수 있다.



〔그림 10〕 AMSD 정적 분석 시스템의 분석 결과 예

3.3. AMSD 정적 분석 시스템의 개선방향 및 과제

현재 AMSD 솔루션은 안드로이드 플랫폼 뿐만 아니라 삼성의 바다 플랫폼, 삼성/인텔의 합작 프로젝트인 타이젠(Tizen) 플랫폼에도 적용되고 있으며 점차 웹 플랫폼까지 그 영역을 계속 확장해나가고 있고, 기능적으

로도 method call graph 분석, javascript 분석 엔진 등으로 고도화되고 있다.

그러나 정적 분석 방법에도 어느 정도 한계가 있어서 정적 분석 기법만으로 모든 경우의 위험성을 분석해낼 수는 없다. 예를 들어, 코드는 존재하지만 사용하지 않는 경우에는 실제 호출 및 실행 여부를 정확히 구분하기가 어렵다. 물론 call graph 등을 생성하여 함수간의 연관 관계를 기반으로 유추해나갈 수는 있으나 이 방법 또한 엔트리 포인트의 필연적인 시작 여부를 증명할 수는 없기 때문에 완벽한 대안이 되지는 못한다.

실제로 오픈 마켓을 대상으로 정적 분석 시스템만을 적용한 검증 서비스를 마켓에 도입하여 운영하는 기간 동안 등록 불가 판정을 받은 앱의 개발자가 '앱 실행 시에는 해당 기능을 실제로 호출하지 않는다'는 이유를 들어 불복 의사를 밝혀오는 경우가 간혹 있었다.

Ⅳ. AMSD의 동적 분석 기법

4.1. 모바일 어플리케이션의 동적 분석 기법

앞서 밝힌 바 있듯이 모바일 플랫폼 기반의 어플리케이션을 분석하는 데 있어서 정확성을 높이고 정적 분석이 미치지 못하는 부분을 보완하기 위해서는 동적 분석 방법을 병행하여 사용해야 한다.

동적 분석이라 함은, 리버스 엔지니어링을 통해 추출된 소스 코드 및 리소스 파일들로부터 정적인 특성 정보를 유추해 내는 정적 분석과는 대비되는 개념으로서, 어플리케이션을 가상 환경에서 직접 실행시켜서 해당 앱이 수행하는 동작과 행위 및 그에 연관되어 주고 받는 정보들을 동적으로 직접 탐지해내는 방법을 말한다.

정적 분석 방법에서는 의심스러운 혐의는 지니고 있으나 실제로 수행하는 지의 여부를 확인하기가 어려운 경우가 많은데 비해, 동적 분석 방법에서는 실제 수행 여부를 실시간으로 감지할 수 있고 이 때 주고 받는 정보도 캡처하여 분석할 수 있게 됨으로써 앱의 악성 행위를 직접적으로 증명하는데 활용될 수 있다는 장점이 있다.

사실, 동적 분석 방법은 앱을 실행할 수 있는 구동 환경만 구성할 수 있다면 개발 여건이 충분하기 때문에 에뮬레이터 같은 가상환경 뿐만 아니라 실제 모바일 기기 상에서도 분석이 이루어질 수 있다. 하지만 이들 두 가지 환경 사이에는 서로 장단점이 있기 때문에 목적과 상황에 따라 적절한 선택이 필요한데 이중 에뮬레이터 기반의 동적 분석 방법은 단말 특성에 종속되지 않는 표준화된 환경을 제공하며, 신규 플랫폼 대응에도 용이하다는 상대적인 장점이 있기 때문에 AMSD 솔루션에서는 실 단말 환경이 아닌 에뮬레이터를 채택하여 구현하였다.

대부분의 모바일 플랫폼들은 자사 플랫폼 기반의 앱을 개발하는 데 있어서 개발 편의성을 높이고 최적화된 개발 환경을 조성해주기 위해 SDK(Software Development Kit)를 제공하고 있으며, 이 SDK에는 고가의 단말 장비가 없이도 앱을 저작하고 시험할 수 있도록 가상 단말 환경을 제공해주는 에뮬레이터가 탑재되어 있다. 이는 Android, Tizen 등의 개방형 플랫폼도 예외가 아니어서 가상화를 지원하는 개발 환경이라면 큰 무리 없이 에뮬레이터를 동적 분석 기법에 활용할 수 있다.

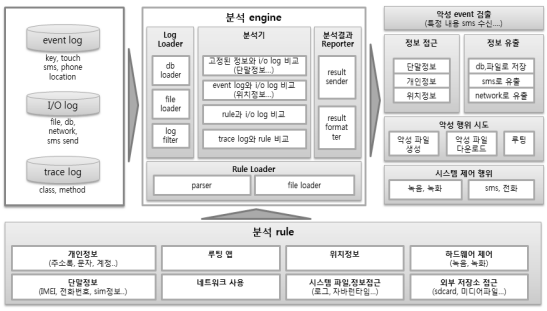
〔그림 11〕 AMSD 동적 분석 방법의 개념

이러한 에뮬레이터에 앱을 설치하여 구동을 시키게 되면 실제 단말 장치에서 사람이 사용하는 것과 거의 유사한 환경에서 앱을 테스트 할 수 있으며, 앱 실행 중에 실제로 수행하는 행위들을 감지하여 검증을 할 수 있게 되는 것이다.

4.2. AMSD의 동적 분석 시스템

본 고에서 소개하고 있는 AMSD 솔루션에서는 분석 대상인 모바일 앱을 플랫폼 SDK에서 제공하는 에뮬레이터 상에 설치하여 기동시키고, 앱이 가진 기능들을 실

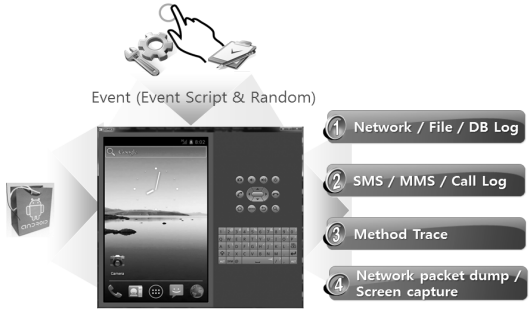
제적으로 수행하게 함으로써 정적 분석과는 달리 앱이 실제 구동되면서 일어나는 위험스러운 동작이나 실시간으로 변화되는 상황을 직접적으로 분석할 수 있는 동적 분석 시스템을 도입하여 운용하고 있다.



〔그림 12〕 AMSD 동적 분석 시스템의 개요

물론 앱을 구동시키는 것만으로 행위 모니터링을 할 수 있는 것은 아니다. 모니터링할 행위 유형을 먼저 정하고 그 행위와 관련되어 있는 프레임워크나 커널 모듈 내에 모니터링을 위한 코드를 삽입함으로써 분석에 필요한 로그와 덤프 데이터를 생성해낼 수 있다. 생성된 원시 데이터로부터 유용한 정보를 추출하기 위해서 동적 분석에 적합한 진단 정책과 고유의 파서가 필요한 것 또한 당연지사일 것이다.

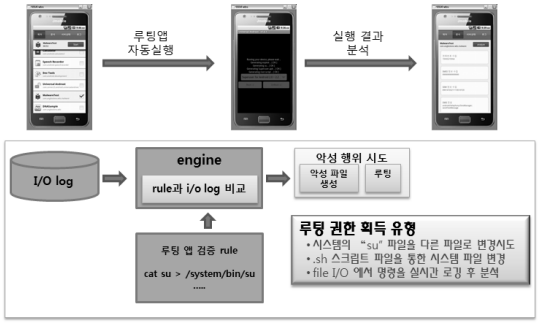
에뮬레이터 기반의 분석 방법에는 운용 면에 있어서도 두 가지의 다른 방법이 있는데, 부분적인 사람의 개입으로 정확도를 확보함과 동시에 높은 자동화 효율을 추구하는 방법과 불특정 이벤트를 자동으로 생성시켜 모든 과정을 자동화함으로써 신뢰도는 조금 낮아지더라도 완전한 자동화를 이끌어내는 방법이 있다.



〔그림 13〕 AMSD 동적 분석 시스템의 동작

사람이 개입한다 하더라도 단지 앱이 보유한 기능을 해당 앱의 GUI를 이용해 수행해보는 정도에 국한되며 에뮬레이터 구동 후 앱의 설치 및 실행, 앱의 행위에 수반되는 입출력 정보의 확보와 분석을 통한 근거 자료의 확보 등 그 외의 모든 과정은 자동으로 진행되게 된다. 이 방법에서는 앱 기능 실행 단계에서의 적절한 사람의 개입으로 인해 정확도를 최고 수준으로 확보하는 동시에 자동화 효과까지도 추구할 수 있다.

이와는 다르게 이벤트 자동 생성 방법을 통한 동적 분석 방법에서는 분석 대상 앱이 에뮬레이터에 설치되어 실행이 되었을 때, 플랫폼에서 생성 가능한 이벤트를 난수 방식으로 발생시켜서 해당 앱에 전송한다. 그리고 분석 대상 앱이 전송된 이벤트를 수행하면서 나타나는 주요 행위를 검증하게 된다. 이벤트를 난수 방식으로 생성시켜 테스트를 하게 되면 사람이 직접 앱을 사용하며 테스트를 수행할 때에 비해서 정확성 측면에서는 다소 미치지 못하는 단점이 있으나 충분한 시간을 두고 반복 수행함으로써 소기의 목표를 달성할 수 있으며 사람의 개입이 없어도 앱의 행위 분석이 가능해지기 때문에 궁극적인 자동화 실현이나 운영비용 감소 측면에서는 더욱 더 효과적이라 할 수 있다.

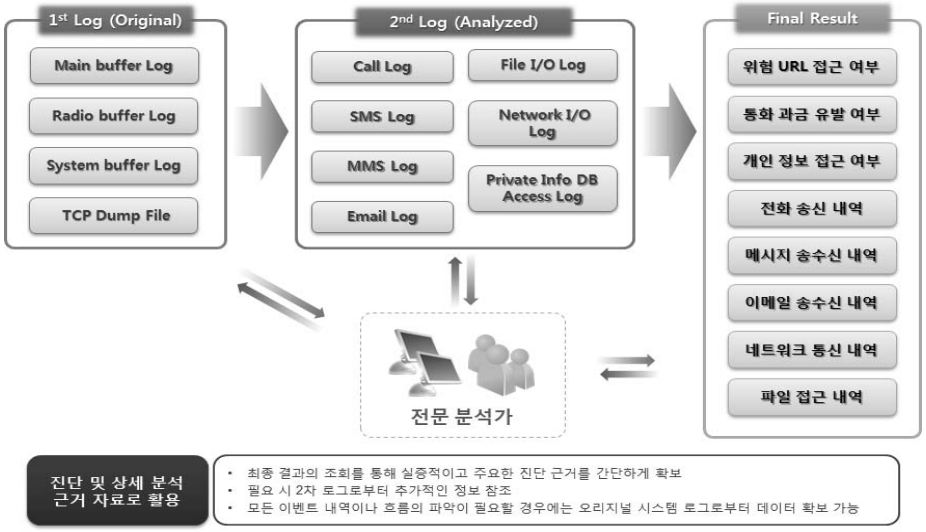


〔그림 14〕 동적 분석 시스템을 이용한 루팅 앱의 검증 예

4.3. AMSD 동적 분석 시스템의 효용성

현재 널리 사용되고 있는 모바일 앱의 분석 방법에서는 특정 피처나 소스 코드 상에 기재된 내용 만을 대상으로 분석하기 때문에 의심스러운 혐의를 추정해낼 수는 있으나 실제로 해당 코드가 실행되는지 여부는 확인할 수 없기 때문에 간혹 판단 오류가 생길 수 있는

데 비해, 동적 분석 방법에서는 실제 수행 여부를 실시간으로 감지할 수 있고 이 때 주고 받는 정보를 확인



〔그림 15〕 AMSD 동적 분석 시스템의 기능 및 활용

하여 그 근거로 삼는 동시에 해당 정보를 분석하여 대상앱의 위험성 여부를 판단 할 수 있게 됨으로써 저작자와의 논쟁을 줄이고 앱의 행위를 실증적으로 증명할 수 있다는 장점이 있다.

또한 에뮬레이터 기반의 가상 환경에서 테스트함으로써 단말기 특성이나 사양에 종속되지 않고 표준 사양의 환경에서 테스트가 가능해지고, 플랫폼이 업그레이드 되더라도 제조사에서 단말에 적용하는 시점까지 기다릴 필요 없이 SDK만 업그레이드함으로써 곧바로 테스트가 가능하다. 모바일 플랫폼은 신규 버전의 출시가 상대적으로 매우 잦기 때문에 이러한 분석 방법은 대응하기에 매우 효율적이라고 볼 수 있다.

AMSD 솔루션에서는 동적 분석 방법을 도입하여 병행 운용하게 되면서 정적 분석 방법만을 활용하여 앱 분석 자동화 시스템을 구축할 때 보다 분석 기능이 훨씬 더 정교해지면서 결과적으로는 사람이 개입되어야 하는 부분이 더욱 줄어들었기 때문에 보다 효율적이고 정확한 앱 분석 및 검증 시스템을 구축할 수 있게 되었다.

Ⅴ. 결 론

본 고에서는 모바일 기기의 활용 영역 확대에 따른 모바일 악성코드의 위험성을 상기시키고 이를 해소하고자 정적분석 및 동적분석 방법을 응용하여 (주)안랩에서 실제로 운용 중인 모바일 어플리케이션의 분석 및 검증 솔루션(AMSD) 인프라의 구축 사례를 소개하였다.

기 알려진 정적분석 방법과 동적분석 방법을 시스템에 구현하여 운영하면서 각 방법에 대한 장단점과 이를 보완해 나가기 위한 개선 방향을 밝혔으나 짧은 글안에 요지와 세부 구현 사항을 모두 서술하기엔 저자의 요약 전달 능력이 부족함을 한 번 더 느끼게 되었다. 비록 본 고의 내용이 기대에 못 미친다 할지라도 모바일 오픈 마켓 운영을 위한 안전성과 신뢰성 확보 및 이를 통한 건전한 모바일 생태계 유지를 도모하는 데 있어 향후 방향성을 잡아나가는데 조금이라도 도움이 되었으면 하는 바램을 가지면서 부족한 글을 마무리하고자 한다.

참고문헌

[1] 김세일, 고승원, 이동훈, “Risk-based Application Analysis for Android Malware Detection”, Journal of Pervasive Technology, 1(1), pp. 9-14, 2011.

[2] 심원태, 김종명, 류재철, 노봉남, “안드로이드 앱 악성행위 탐지를 위한 분석 기법 연구”, 정보보호*학회 논문지*, 21(1), pp. 213-219, 2011.

〈著者紹介〉

고 승 원 (Ko, Seung Won)
비회원

1999년 2월 : 중앙대학교 컴퓨터공학과 졸업
2001년 2월 : 중앙대학교 컴퓨터공학과 석사
1999년~2002년 : 국내최초 실험실 벤처 ㈜비전넷의 창업 멤버로 근무
2004년~2006년 : ㈜삼성전자 무선사업부 근무
2010년 4월~현재 : ㈜안랩(舊 ㈜안철수연구소) 융합제품개발실 책임연구원으로 재직 중
<관심분야> 모바일 플랫폼, 모바일 보안, 클라우드 기반의 데이터 동기화, 개인정보 보호

정 상 곤 (Joung, Sang Gon)
비회원

1997년 2월 : 동국대학교 전자공학과 졸업
1999년 2월 : 동국대학교 전자공학과 석사
1999년~2001년 : ㈜장미디어 인터렉티브 보안기술연구소 근무
2005년~2012년 : ㈜ 소프트포럼 보안연구소 부장 근무
2012년 4월~현재 : ㈜안랩(舊 ㈜안철수연구소) 융합제품개발실 책임연구원으로 재직 중
<관심분야> 모바일 플랫폼, 모바일 보안, 클라우드기반의 데이터 동기화, 개인정보 보호