AI 기반 재난안전통신망 프로텍트 구현

배세진 · 안중현 · 이정수 · 박정수 · 백남균*

부산외국어대학교

Implementation of AI-based Disaster Safety Communication Network protect

Se-jin Bae · Jung-hyun Ahn · Jung-soo Rhee · Jung-soo Park · Nam-kyun Baik*

Busan University of Foreign Studies

E-mail : qotpqo@naver.com / endrk723@naver.com / rhee@bufs.ac.kr / jungsoop@bufs.ac.kr / namkyun@bufs.ac.kr

요 약

2021년 4월, 재난안전통신망 서비스가 개시되었으나 서비스 초기로 보안기능이 취약한 상태이다. 현재 Android 기반 APP의 보안방법은 구글 프로텍트(Google Protect)의 기술을 사용하여 악성코드를 탐지하는 것이다. 악성코드는 종류가 다양하고 많기 때문에 직접 탐지하기 어려우므로, AI와 구글 프로텍트의 기술을 합한 악성코드탐지 기술을 재난안전통신망에 적용함으로써 'AI 기반 재난안전통신망 프로텍트'를 구현하는 방법에 대해 연구한다.

ABSTRACT

April 2021, Disaster Safety Communication Network services have been launched, but security functions are weak at the beginning of the service. The current security method for Android-based APP is using Google Protect's technology to detect malware. Malware is difficult to detect directly because there are various types, so by applying malware detection technology that combines AI and Google Protect technology to Disaster Safety Communication Networks, research on how to implement 'AI-based Disaster Satety Communication Network Protect'.

키워드

AI, APK, Android, 재난안전통신망(Disaster Safety Communication Network), 구글 프로텍트(Google Protect)

Ⅰ. 서 론

재난안전통신망이란 소방, 경찰, 해경 등 재난관리 및 대응기관 담당자들이 일상 업무와 재난발생 시 활용하기 위해 전용으로 사용하는 무선망이다. 2021년 4월, 재난안전통신망 서비스가 개시되었으나 서비스 초기로 단말기 내 보안이 매우 취약한 상태이다. 취약점을 보완하기 위해서 구글 프로텍트와 같은 기술이 필요하다. 구글 프로텍트란 2017년 구글 I/O에서 공개한 일종의 안드로이드용 모바일 백신이다. 구글 플레이 스토어에서는 앱을 내려받을 때 앱의 안전성을 미리 검사하며, 이미 설치되어 있는 앱도 유해한 동작이 있는지 확인한다.

재난안전통신망은 인명과 관계되므로 신속하고 정확해야한다. 따라서 AI와 구글 프로텍트의 기술을 합한 악성코드 탐지 기술을 재난안전통신망에 적용함으로써 'AI 기반 재난안전통신망 프로텍트'를 구현하여 단말기 내 악성 앱을 탐지 및 통제하여 주요정보의 외부 유출을 사전에 예방하고 악성코드를 조기 식별하여 단말 내에 사용자 정보 유출을 예방하는 서비스 활용의 기회가 제공되는 환경을 만드는 것이 연구의 목표이다.

Ⅱ. 본 론

긴급재난 발생 시 특정 기관들은 재난안전통신망을 통해 현 상황 정보와 재난에 대한 조치를 실

* corresponding author

시간으로 공유한다. 하지만 최근에 서비스가 개시된 만큼 단말기 내 보안 시스템이 취약한 상태인데, 재난안전통신망은 인명과 관계되므로 신속하고 정확해야한다. 따라서 인공지능과 구글 프로텍트의 기술을 이용한 안드로이드 APK 악성코드 탐지가 필요하다.

본 논문에서는 재난안전통신망에 구글 프로텍트 개념을 적용한 '재난안전통신망 프로텍트'를 구현하는 방법에 대해 논하고자 한다.

2.1 세부 추진계획 및 방법

가. Raw Data Set(안드로이드 악성코드 앱 및 목록) 수집 및 분석

1) Google Play Store, Web, Black Market 등 다양한 경로를 통하여 앱을 확보하고, 앱의 특성을 분석(Feature Vector)하여 정상 앱과 구분하여 DB화 한다.

2) 안드로이드 어플리케이션 설치 파일인 APK 파일의 집합을 실제 안드로이드 운영체제에서 설치 및 실행이 가능한 데이터이다.

3) 각 개별 데이터는 안드로이드 악성코드라고 판단이 된 악성코드 데이터셋과 일반 앱 데이터셋으로 구분된다.

4) Feature Vector를 구축하여 모바일 앱을 구성하는 모든 요소(안드로이드 버전, 매니페스트 파일, System call, API, 레지스트리, 환경변수 등)에서 악성코드 식별에 필요한 모든 가능한 특징들을 조사하여 구분된 필드를 추출한다.

5) 사용자 접근통제시스템에 모바일 앱(Android) 통제 기능 영역에 악성 APK 차단 모듈을 개발한다.

표 1. 제공되는 안드로이드 악성코드 앱

구분	악성코드 앱(개)	출처
play store(deleted)	1,787	악성코드 앱
play store(benign)	20,095	정상 앱
virusshare	20,813	https://virusshare.com
AMD (Android Malware Dataset)	24,554	Argus cyber security lab (university of south florida)
VirusTotal	10,908	https://www.virustotal.com
합 계	78,157	

나. Raw Data의 특성을 분석하여 AI 모델링을 통해 분석된 결과데이터를 기반으로 대다수의 정상적인 앱과 다른 양상을 보이는 비정상적인 앱을 실시간 탐지 후 차단

다. AI 모델을 통하여 도출된 취약성 정도 DB는 앱의 악성코드 감염 여부 결과로, 타 AI 알고리즘을 활용한 악성코드 감염여부 모델의 정확성에 대한 검증에 활용 가능

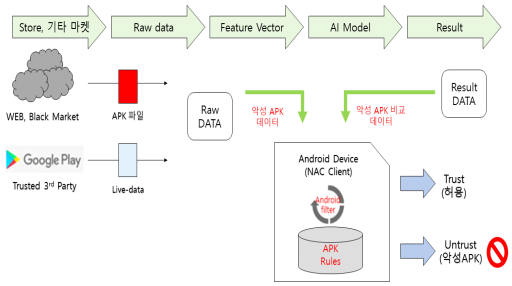

그림 1. 데이터 가공을 통한 악성APK 분석 FLOW

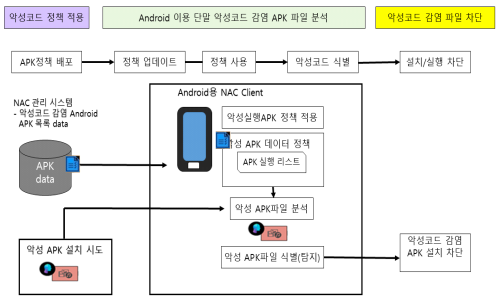

그림 2. 악성 APK 탐지 정책 적용 및 차단 개념도

라. 위의 프로젝트를 재난안전통신망에 적용

1) 프로텍트 역할을 하여 새로운 앱 추가 시 앱을 분석하여 이상이 없으면 설치한다.

III. 결 론

본 연구는 재난안전통신망 단말기 내의 악성코드를 탐지하는 기법을 연구함으로써 안드로이드 기반 태블릿, 휴대용 단말기에 앱 설치 시 악성 앱 보안 위협을 선제적으로 예방하여 단말 내에 중요 데이터를 보호하고, 악성 앱에 대한 AI 모델링을 통해 악의적 행위로 분류된 악성 APK 결과를 활용하여 현재 많이 취약한 재난안전통신망에 악성코드 탐지 서비스를 실행 시, 보다 안전하고 원활한 소통이 가능할 것으로 기대한다.