재난안전통신망 앱스토어를 위한 AI 보안 방안 마련

정재은* · 안중현 · 백남균

부산외국어대학교

AI Security Plan for Public Safety Network App Store

Jae-eun Jung* · Jung-hyun Ahn · Nam-kyun Baik

Busan University of Foreign Studies

E-mail : wow520wow@bufs.ac.kr / endrk723@naver.com / namkyun@bufs.ac.kr

요 약

우리나라 재난안전통신망 제공 및 응용 서비스는 개발 추진, 초기 구축, 실증 및 초기 서비스 단계로 재난안전통신망 모바일 앱에 대한 보안 대응은 아직 미흡하다. 재난안전통신망(PS-LTE)에서 사용할 수 있는 단말은 개방형 안드로이드 기반 전용 단말로 다양한 모바일 악성코드에 사용될 수 있는 취약성이 잠재적으로 존재하기 때문에 미국의 FirstNet Certified 및 구글의 Google Play Protect와 비슷한 선제적 대응이 필요하다. 본 논문에서는 응용서비스 앱을 재난안전통신망 모바일 앱스토어에 등재하기 전, 악성 앱 및 정상 앱에 대해 데이터 셋을 구축하여 특징을 추출하고 가장 효과적인 AI 모델을 선정하여 정적 및 동적 분석을 수행하며, 분석 결과에 따라 악성 앱이 아닌 경우 앱 스토어에 등재하는 방안을 제안한다. 해당 방안으로 악성행위 앱 등재를 사전에 차단하는 서비스 제공이 필수가 되어 공인된 인증을 부여함으로써 재난안전통신망의 보안 사각지대를 최소화하고 인증된 앱을 재난안전 제공 및 응용 서비스 지원으로 재난상황에 대한 재난안전통신망의 안전성을 확보할 수 있다.

ABSTRACT

The provision and application of public safety network in Korea is still insufficient for security response to the mobile app of public safety network in the stages of development, initial construction, demonstration, and initial service. The available terminals on the Disaster Safety Network (PS-LTE) are open, Android-based, dedicated terminals that potentially have vulnerabilities that can be used for a variety of mobile malware, requiring preemptive responses similar to FirstNet Certified in U.S and Google's Google Play Protect. In this paper, before listing the application service app on the public safety network mobile app store, we construct a data set for malicious and normal apps, extract features, select the most effective AI model, perform static and dynamic analysis, and analyze Based on the result, if it is not a malicious app, it is suggested to list it in the App Store.

As it becomes essential to provide a service that blocks malicious behavior app listing in advance, it is essential to provide authorized authentication to minimize the security blind spot of the public safety network, and to provide certified apps for disaster safety and application service support. The safety of the public safety network can be secured.

키워드

public safety network, app store, android, data-set, AI model

Ⅰ. 서 론

재난안전통신망이란 태풍·홍수·지진 등의 자연재해는 물론 도심화재·건축물 붕괴·해상사고·환경오염사고 등 대규모 재난 발생 시, 소방, 경찰, 해경 등 재난 관련 기관이 4세대 무선통신기술로 소통하며 신속하게 현장대응을 할 수 있도록 구축된 통신망이다. 재난안전통신망이 도입됨으로써 여러

* speaker

재난관련 기관들이 단일 통신망으로 신속하고 효율적으로 소통하게 되었다. 각 사용 기관들의 업무와 연계되는 앱을 개발해 사용할 수 있도록 구성함으로써 재난이 발생하지 않는 평시에도 재난안전통신망을 활용한 일상 업무수행이 가능해졌고 별도의 통신망을 구축할 필요가 없어 기관 간 중복 투자를 방지하며, 국가차원의 효율적인 운영 및 유지보수가 가능해졌다[1].

재난안전통신망에서 사용하는 PS-LTE기술은 전국 규모의 광대역 공공안전 통신망을 구축하는 LTE기술이다. PS-LTE기술은 기존의 LTE기술에 D2D통신, 그룹통신을 제공하는 GCSE, MCPTT, 단독 기지국 모드 등 재난안전에 필수적인 기능을 추가한 것이다. 3GPP에서 공식적으로 본 기술을 LTE for Public Safety라고 부르고 있으나, 우리나라에서는 PS-LTE로 축약하여 부르고 있다. 국제 동향을 보면 미국은 국가 차원의 공공안전 광대역 통신망 구축과 운영을 위하여 2012년 상무부 통신정보관리청(NTIA) 내에 추진기구 FirstNet을 발족하였고, LTE기반 재난망 구축에 필요한 주파수 사용권을 FirstNet에 부여했다. 영국 내무부는 기존 TETRA 기반 재난망을 2017년부터 LTE 기반의 공공안전통신망으로 대체한다는 계획이다[2].

국내 재난안전통신망(PS-LTE)에서 사용할 수 있는 단말은 사용자의 업무유형에 따라 스마트폰형, 무전기형, 복합형 등 전용단말기를 사용한다. 전용단말은 안드로이드 기반으로 제작되어 사용이 어렵지 않고 다양한 앱을 통해 업무확장이 가능하지만, 재난상황정보 변조, 개인정보 유출, 랜섬웨어, 스파이 앱, 스미싱 등의 다양한 모바일 악성코드에 사용될 수 있는 취약성이 잠재적으로 존재하기 때문에 재난안전 관련 피해(재산 및 생명)를 예방하기 위해서는 재난안전통신망 및 공용 앱에 대한 보안 신뢰성을 확보하는 방안이 필요하다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 재난안전통신망 앱 보안과 관련된 국내외 사례들을 알아보고 Ⅲ장에서는 재난안전통신망 앱스토어를 위한 AI보안 방안 마련을 제안한다. Ⅳ장에서는 방안을 검증하고 마지막 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

재난안전통신망 앱 보안과 관련된 국내외 사례들을 알아본다.

2.1 재난안전통신망 앱 보안 관련 국외 사례

미국의 PS-LTE기반 재난안전통신망인 FirstNet에서는 앱 개발자 프로그램 전용 포털을 통해 통제적 절차 없이 개인, 그룹 또는 기업으로 가입 후 자유롭게 앱을 공유할 수 있으며, 최종적으로 개발된 앱을 앱 카탈로그에 공유하려면 먼저 보안, 관련성, 데이터 개인 정보보호 및 가용성에 대한 엄격한 테스트를 통과해야한다. 이에 대한 FirstNet 위원회는 잠재적인 개발 코드 취약성을 검증하여 FirstNet Certified를 부여한다[3].

2.2 민간상업망 앱 보안 관련 국외 사례

구글에서는 Google Play Store를 통해 다운받거나 APK파일을 직접 설치했을 때 설치된 앱들이 잠재적인 위험이 있는지 지속적으로 검사하여 악성 앱으로 의심되면 경고 메시지와 함께 제거하도록 안내해주는 Google Play Protect 기능이 있다. Google Play Protect의 기계학습에서는 전체 앱 DB를 분석하여 유해한 앱과 안전한 앱을 학습하고 정적분석을 통해 앱의 코드가 분석되고 기능이 추출되어 예상되는 정상 동작 및 잠재적인 악성 동작과 비교한다. 시그니처를 이용해 알려진 악성 앱 및 취약점 DB와 앱을 비교한다. 정적분석으로 볼 수 없는 대화형 동작을 식별하는 응용 프로그램을 실행하고 이를 통해 검토자는 서버 액세스 및 동적코드 다운로드가 필요한 공격을 식별할 수 있지만, Google Play Protect의 인증 앱 부여 기준은 공개하지 않았다[4].

2.3 민간상업망 앱 보안 관련 국내 사례

국내 이동통신 3사와 네이버의 통합 앱스토어인 원스토어는 보안솔루션을 통해 사용자 기기에 해를 끼치는 바이러스, 스파이웨어, 트로이목마, 애드웨어 등 악성코드가 탐지되는 경우 앱 등록을 허용하지 않는다.

Ⅲ. 제안 방안

재난안전통신망(PS-LTE)에서 사용하는 단말은 안드로이드 기반 전용 단말로 사용이 어렵지 않고 다양한 앱을 통해 업무확장이 가능하지만, 재난상황정보 변조, 개인정보 유출, 랜섬웨어, 스파이 앱, 스미싱 등의 다양한 모바일 악성코드에 사용될 수 있는 취약성이 잠재적으로 존재한다. 안드로이드 기반 취약성 및 악성코드는 재난안전통신망 응용서비스 중 재난안전통신망 모바일 앱스토어를 통한 유포가 가능하다. 서비스 초기단계인 재난안전통신망은 재난안전통신망 모바일 앱에 대한 보안 대응이 미흡하여 미국의 FirstNet Certified와 Google Play Protect와 같은 보안 대응이 필요하기 때문에 재난안전통신망 앱스토어를 위한 AI 보안 방안을 단계별로 설명하고자 한다.

3.1 구축 1단계 : 안드로이드 기반 전용 단말에 관련된 데이터 셋 구축

안드로이드 앱에 대한 악성코드 특성을 추출하여 딥러닝을 통해 악성 행위를 분석 및 판단 가능한 정적·동적 기능을 설계하고 구현하고자, 우선적으로 안드로이드 앱에 대한 악성 앱 그리고 정상 앱

에 대한 데이터 셋이 필요하다.
데이터 셋 구축 절차는 웹크롤링/앱스토어 수집/악성 앱 구입 및 검증으로 안드로이드 기반 악성 앱 데이터 셋을 구축하고 추가적으로 분석, 학습, 시험 및 검증을 위한 정상 앱도 같이 수집한다.

3.2 구축 2단계 : 데이터 셋 분석을 통한 특성 추출 및 AI 모델 구현

확보된 안드로이드 기반 악성 앱 데이터 셋(빅데이터)을 분석하여 정상 앱과 구분된 피쳐(특성)를 추출하고 가장 효과 및 효율적인 AI 모델을 구현하기 위해 데이터 셋은 학습, 검증 및 시험데이터로 구분되어지는 비율을 지정한다. 딥러닝 기반 탐지는 사용되는 특성과 알고리즘에 따라 성능이 크게 좌우되므로 가능한 다양한 딥러닝 기법을 활용하여 최적 및 최상의 모델을 시험 및 검증하여 선택한다.
이후 정적분석 및 동적분석 기능까지 구현한 AI 기반 모델 학습 후 검증 및 시험을 수행하여 안드로이드 기반 악성 앱 탐지 기능을 완성한다.

그림1. 구축 1, 2단계의 흐름도

3.3 구축 3단계 : 개발된 응용서비스 앱을 재난안전통신망 모바일 앱스토어에 등재

재난안전통신망에 사용될 모든 재난안전관련 앱은 오직 재난안전통신망 모바일 앱스토어를 통해서만 공유 가능하도록 절차를 규정한다. 재난안전 관련 앱 개발자는 공개하고자 하는 서비스 앱을 필요 제출물과 함께 앱스토어 인증위원회에 제출하고 인증위원회는 재난안전통신망 모바일 앱스토어에 등재하기 위해서 AI 기반 보안 방안을 수행하고 이에 대한 결과를 기반으로, 악성 앱이 아닌 경우에 대해서 안전 앱 인증서를 부여한다.

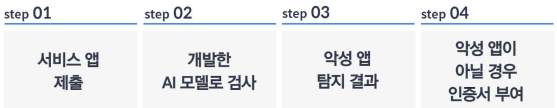

그림2. 구축 3단계의 흐름도

이후 인증된 안전 앱에 대한 앱 카탈로그 서비스를 제공하고 재난안전통신망 앱스토어 및 등재된 앱에 대하여 주기적인 업데이트 및 관리가 필요하다.

재난안전통신망에서 사용하는 단말과 앱을 유통하는 앱스토어는 안드로이드 기반으로 사용이 어렵지 않고 다양한 앱을 통해 업무확장이 가능하지만, 안드로이드 운영체제는 다양한 모바일 악성코드에 사용될 수 있는 잠재적인 취약성이 존재하기 때문에 응용서비스 앱을 재난안전통신망 모바일 앱스토어에 등재하기 전, 악성 앱 및 정상 앱에 대해 데이터 셋을 구축하여 특징을 추출하고 가장 효과적인 AI 모델을 선정하여 정적 및 동적 분석을 수행한다. 분석 결과에 따라 악성 앱이 아닌 경우 앱 스토어에 등재하며, 해당 방안을 통해 재난안전통신망의 보안 및 기술력을 향상시킬 수 있다.

Ⅳ. 결 론

본 연구에서는 재난안전통신망에서 앱을 유통하는 앱스토어와 전용 단말에서 앱이 동작되는 안드로이드 운영체제에 대한 잠재적 취약점을 사전 예방하고자 재난안전통신망 앱스토어를 위한 AI 보안 방안 마련을 제안하였다. 악성 앱 등재를 사전에 차단하는 서비스 제공이 필수가 되어 공인된 인증을 부여함으로써 재난안전통신망의 보안 사각지대를 최소화하고 인증된 앱을 재난안전 제공 및 응용 서비스 지원으로 재난상황에 대한 재난안전통신망의 안전성을 확보할 수 있다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0사업의 연구결과로 수행되었음.(IITP-2021-2020-0-01825)

References

[1] public safety network(PS-LTE) [Internet]. Available : https://www.mois.go.kr/frt/sub/a06/b11/policyBriefingView/screen.do
[2] PS-LTE [Internet]. Available : https://terms.naver.com/entry.naver?docId=2751859&cid=42346&categoryId=42346
[3] FirstNet Certified [Internet]. Available : https://developer.firstnet.com/firstnet/resources/submission
[4] Google Play Protect [Internet]. Available : https://developers.google.com/android/play-protect/client-protections