JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 10: 1375~1380, Oct. 2021

재난안전망 앱 보안 체계 구축

백남균*

Establishment of a public safety network app security system

Nam-Kyun Baik*

*Assistant professor, Department of Information Security, Busan University of Foreign Studies, Busan, 46234 Korea

요 약

우리나라는 재난안전통신망 개통 초기로 응용서비스 앱에 대한 보안 대응은 아직은 미흡한 실정이기에, 이에 대한 선제적 보안 대응이 반드시 필요하다.

본 연구에서는 재난안전통신망에서 앱을 유통하는 앱 스토어와 전용 단말에서 앱이 동작되는 안드로이드 운영체제에 대한 잠재적 취약점을 사전 예방하고자 '재난안전망 앱 보안 체계 구축'을 제안하였다. 응용서비스 앱이 재난안전통신망 모바일 앱스토어에 등재하고자 하기 위해서는, 우선 악성 및 정상 앱에 대한 데이터 셋을 구축하여 피쳐를 추출하고 가장 효과적인 AI 모델을 선정하여 정적 및 동적 분석을 수행한다. 분석 결과에 따라 악성 앱이 아닌 경우에 대해서 '안전 앱 인증서'를 인증하여 공인 앱에 대한 신뢰성을 확보한다.

궁극적으로 재난안전통신망 앱의 보안 사각지대를 최소화하고 인증된 앱의 재난안전 응용 서비스 지원으로 재난상황에 대한 통신망의 안전성을 확보할 수 있다.

ABSTRACT

Korea's security response to application service app is still insufficient due to the initial opening of the public safety network. Therefore, preemptive security measures are essential.

In this study, we proposed to establish a 'public safety network app security system' to prevent potential vulnerabilities to the app store that distributes app in public safety network and android operating system that operate app on dedicated terminal devices. In order for an application service app to be listed on the public safety network mobile app store, a dataset of malicious and normal app is first established to extract characteristics and select the most effective AI model to perform static and dynamic analysis. According to the analysis results, 'Safety App Certificate' is certified for non-malicious app to secure reliability for listed apps.

Ultimately, it minimizes the security blind spots of public safety network app. In addition, the safety of the network can be secured by supporting public safety application service of certified apps.

키워드 : 재난안전통신망, 앱 스토어, 안드로이드, 데이터 셋, AI 모델

Keywords : Public safety network, App store, Android, Data-set, AI model

Received 8 August 2021, **Revised** 6 September 2021, **Accepted** 11 September 2021

*** Corresponding Author** Nam-Kyun Baik(E-mail:namkyun@bufs.ac.kr, Tel:+82-51-509-6136)
Assistant professor, Department of Information Security, Busan University of Foreign Studies, Busan, 46234 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.10.1375 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

사회 전반적으로 개인, 사회 및 환경에 안전을 위협하는 요소들이 늘어나고 있다. 자연 재해와 각종 크고 작은 인재들로 인하여 국민 안전에 대한 불안감이 증폭하고 자연재해와 인재와의 복합 등으로 새로운 유형의 대규모 재난발생 위험이 지속적으로 증가 되고 있다. 이러한 재난발생 위험을 예방 및 대응하기 위해서는 여러 가지 방안이 있지만 가장 효과적인 방안 중 하나는 빠른 대처로 피해를 최소화하는 것으로 바로 재난안전통신망 구축을 말할 수 있다.

우리나라는 ’14년 4월 재난안전통신망 추진을 본격화 하였으며 같은 해 7월에 기술 방식으로 ‘PS-LTE (Public Safety - Long Term Evolution)’을 확정하였다. ’16년 평창올림픽에서 시범사업을 완료 하였으며 1단계 구축(대전, 세종, 충남 충북, 강원), 2단계 구축(부산, 광주, 대구, 울산, 경남, 경북, 전남, 전북, 제주), 3단계 구축(서울, 인천, 경기) 및 4단계(대한민국 전역, ’21년 3월) 운영으로 단계별 구축 사업을 마무리 하였다[1][2][3]. 따라서 경찰, 소방, 지자체 등 재난관련 기관이 공동으로 사용할 수 있는 PS-LTE 기술방식의 전국 단일 재난안전통신망을 구축으로 통합적 재난대응체계 및 신속·정확한 상황전달 등 지원이 가능하다.

이러한 재난안전통신망은 재난 상황에 정상적인 기능 유지를 담보하기 위하여 평상시에도 예방적 방안을 통한 ‘재난안전통신망 자체에 대한 보안 안전성 확보’가 필요하다. 즉, 재난안전통신망도 인터넷과 같은 동일 개념으로 악의적 또는 악용된 사용자에 의한 사이버 침해 공격이 가능하며 특히 재난안전통신망에서 사용할 수 있는 단말은 개방형 안드로이드 기반 전용 단말로 재난상황 정보 변조, 개인정보 유출, 랜섬웨어, 스파이 앱, 스미싱 등의 다양한 모바일 악성코드에 사용될 수 있는 취약성이 잠재적으로 존재할 수 밖에 없다. 만약 재난안전통신망에 기존 네트워크 공격이 활용되어 해킹(루팅)된 전용 단말에서 악성 앱이 수행되면 루트 권한으로 모바일 모든 기능을 제어할 수 있으므로 저장된 중요 데이터 탈취를 포함하여 정상 앱을 악성 앱으로 임의 교체하거나 모바일 기기 설정을 임의 변경하는 등으로 이로 인한 재난안전 관련 큰 피해(재산 및 생명)가 발생 가능하다.

우리나라는 재난안전통신망 개통 초기로, 관련된 응용 서비스는 개발 추진, 초기 구축, 실증 및 초기 서비스 단계로 재난안전통신망 모바일 앱에 대한 보안 대응은 아직은 미흡한 실정으로 이에 대한 선제적 보안 대응이 반드시 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 재난안전통신망 보안 취약점에 대하여 설명한다. 3장에서 국외의 관련된 재난안전통신망 앱 관련 구축 사례를 알아보고 4장에서는 제안하는 재난안전통신망 앱 보안 체계를 설명한다. 마지막 5장은 결론으로 마무리하고자 한다.

Ⅱ. 재난안전통신망 보안 취약점

재난 상황에 효율적으로 대응하고 사용자 편의를 위한 대표적인 재난안전통신망 응용 서비스로는 ‘웹 포털 / 앱 스토어 서비스’가 있다. 통신망 공통 사용에 대한 환경(플랫폼)과 재난 관련 정보와 정책, 다양한 통계 정보 및 기타 제공 서비스를 제공하고 플랫폼과 인프라를 기반으로 각종 서비스를 개발하여 관련 사용자가 이용할 수 있도록 만든 온라인 공간을 제공한다. 이를 기반으로 통신망 운영자 및 사용자는 다양한 형태의 앱을 개발하고 직접 단말기에 설치하여 활용할 수 있는 창구의 역할도 하고 있다.

재난안전통신망에서 사용할 수 있는 전용 단말은 안드로이드 기반으로 스마트폰형, 무전기형, 복합형 단말 종류로 구성되며 향후 태블릿, 거치형 등 다양한 종류의 단말이 개발되어 활용될 수 있다. 시장조사기관 스탯카운터에 따르면 2019년 5월부터 2020년 5월까지 1년 동안 전 세계 스마트폰 가운데 무려 72.6%에 이르는 스마트폰이 안드로이드 운영체제를 쓰는 것으로 확인되며 이런 대중화된 모바일 운영체제라는 점과 개방형 환경이라는 특징이 전용단말의 운영체제로 선정된 이유인 듯하다[4][5].

재난안전통신망에서 앱을 유통하는 앱 스토어와 단말에서 앱이 동작되는 안드로이드 운영체제는 잠재적으로 보안에 취약한 문제점들을 가지고 있다. 앱 스토어는 수많은 앱을 공유하여 설치 및 활용할 수 있지만, 앱 개발자들 가운데 일부는 악의적인 앱을 만들어 재난관련 데이터와 개인정보를 탈취하는 데 악용될 수 있고 안드로이드 운영체제는 다양한 앱 기반 응용과 사용자 콘텐츠와의 원활한 연계성과 개방형 플랫폼의 특성으로 여러 가지 보안과 관련한 알려진 취약성이 있다. 일반적

으로 악성 앱은 앱 스토어를 통해 전파되고 안드로이드 운영체제의 취약성을 이용하여 단말기기에 저장된 재난안전 구축 정보, 환경 정보, 기타 개인정보 등의 탈취 및 변조 등으로 피해를 발생시키는 악성 행위들을 포함한다. 그리고 해커와 같은 공격자들은 국가, 공공 또는 기관의 내부 네트워크에 침투하기 위한 수단으로 재난안전 관련된 관계자들이 소지하는 모바일 단말에 악성코드를 심는 기법을 집중하며 이는 공용 앱을 통한 방법이 가장 쉽고 대부분을 차지할 것이다.

또한 지금은 취약하지 않으나 추후 환경(API, System call, 데이터베이스 등의 변화 및 업데이트 등)에 의해 취약할 수 있는 '알려지지 않은 취약성을 가진 앱'도 공용 사용자로 위장한 악의적인 사용자(해커)로 인하여 단말 내 정보가 유·노출되어 악용될 수 있으니, 이러한 제로데이 악성 앱을 효율적으로 탐지하는 방안이 필요한 실정이다.

따라서, 새롭게 구축·운영되는 재난안전통신망은 재난 상황뿐만 아니라 평상시에도 보안 사각지대가 최소화된 예방적인 활용방안을 통하여 '재난안전통신망 보안 안전성 확보'가 필요하고 국민생활안전 측정척도의 핵심인 재난재해 예방관리 및 안전사고 등의 개선을 위해 보다 현실적인 대안을 모색함이 필요하다.

Ⅲ. 관련 연구

우리나라는 재난안전통신망 개통 초기로 제공 및 응용 서비스는 개발 추진, 초기 구축, 실증 및 초기 서비스 단계로 재난안전통신망 모바일 앱에 대한 보안 대응은 아직은 미흡한 실정이다. 따라서 앞서 있는 국외 재난안전망 앱 보안에 대한 사례를 통하여, 향후 우리나라에 적용 가능한 방안을 마련하는 기초가 되고자 관련 연구들을 알아본다.

3.1. 공공안전망 앱 보안 관련 연구

미국은 9.11 테러를 비롯해 몇 번의 매우 큰 비상사태가 있었으며 이러한 재난 상황 등에서 겪은 인명 및 재산 피해의 주요 원인이 비상사태에 대응하는 여러 주파수 간의 상호 운용성의 부족을 하나의 이유로 파악하였다. 따라서 재난상황 발생 시 효율적인 대응 및 조치를 위해 안전하고 신속한 국가차원의 광대역 재난전송망 필요성 부각에 따라, 미국 상무부 산하 국가통신정보관리청(NTIA)의 독립기관인 FirstNet(First Responder Network Authority)을 설립하였다. FirstNet은 소방서, 병원 등과 같은 긴급 구조 기관을 위한 네트워크를 구축하여 미국 전역에서 일어나는 재난의 초기 대응 기관을 위한 전국적으로 상호 운용이 가능한 전용 PS-LTE 기반 네트워크를 제공하며 이것이 미국의 재난안전통신망이다[6][7][8].

공공안전통신망인 FirstNet에서 제공하는 앱 개발자 프로그램 전용 포털을 통해, 개발자는 통제적 절차 없이 개인, 그룹 또는 기업으로 가입 후 자유롭게 앱(API, 데이터, 프로그래밍 툴, 소프트웨어 개발 키트 및 공공안전 가이드라인)을 공유할 수 있으며 최종적으로 개발된 앱을 '앱 카탈로그(공공 안전 커뮤니티의 서비스 및 지원을 위한 사전 평가 및 승인된 모바일 앱 및 라이브러리 목록)'에 공유하려면 먼저 보안, 관련성, 데이터 개인정보 보호 및 가용성에 대한 엄격한 테스트를 통과해야 하며 이에 대해 FirstNet 위원회(Authority)는 잠재적인 개발 코드 취약성을 검증하여 '인증(FirstNet Certified)'을 부여한다.

3.2. 민간상업망 앱 보안 관련 연구

Google은 안드로이드 앱의 등록과 배포, 설치와 실행까지 전 과정에서 위협으로 의심되는 앱의 유통과 실행을 차단할 수 있는 보호를 위해 'Google Play 프로텍트 인증'을 개발하여 유해 앱으로부터 단말기기를 보호한다. 먼저 Google Play 스토어에서 앱을 다운로드하기 전에 기기에 다른 소스에서 받은 잠재적으로 위험한 앱(멀웨어)이 있는지 확인합니다. 잠재적으로 위험한 앱이 감지되면 경고 메시지를 표시하며, 알려진 위험 앱은 기기에서 삭제하고, 중요한 정보를 숨기거나 왜곡함으로써 Google의 원치 않는 소프트웨어 정책을 위반하는 앱이 감지되면 경고 메시지를 표시한다. 또한 개인정보에 액세스할 사용자 권한을 부여받을 수 있어 Google의 개발자 정책을 위반하는 앱에 대해 개인정보 보호 경고를 전송한다. Google Play 프로텍트는 사용자가 설치하는 앱을 주기적으로기기도 검사하여 잠재적으로 위험한 앱이 감지되면 알림을 전송 및 앱을 제거하며 앱이 제거되지 않으면 제거할 때까지 앱을 사용 중지한다[9][10].

Ⅳ. 제안하는 재난안전통신망 앱 보안 체계

4차 산업혁명에 의한 초연결 기반 지능화 혁명으로 산업뿐만 아니라 국가 및 사회 각 영역에서 실용적 기술이 융・복합 되면서 재난안전 분야에도 혁신적이고 다양한 공공안전 서비스 구현이 가능하며 이를 위한 대국민 서비스 구현의 방법으로 앱을 우선 생각할 수 있다. 하지만 재난안전통신망에서 앱을 유통하는 앱 스토어와 단말에서 앱이 동작되는 안드로이드 운영체제는 잠재적으로 보안에 취약한 문제점들을 가지고 있다. 이에 대한 우선적 문제점 해결이 필요하지만 앞장에서 서술한 바와 같이 우리나라 재난안전통신망은 개통 초기로 아직은 정보보안에 대한 많은 고려 및 침해 예방·대응 준비가 되어 있지 않아 향후 다양한 관점의 보안 설계 및 구현이 필요하다. 이에 본 연구에서는 다음과 같은 '재난안전통신망 앱 보안 체계'를 제안하고 단계별로 설명하고자 한다.

4.1. 구축 1 단계 : 안드로이드 기반 전용 단말에 관련된 데이터 셋 구축

안드로이드 기반 앱의 수 많은 악성코드들을 기존의 패턴(시그네쳐) 매칭으로 의심파일의 악성 여부를 판단하기에는 너무나 많은 시간과 인적 리소스가 투입되고 탐지 정확도 또한 높지 않다. 따라서 이에 대한 대응방안으로 AI를 적용하여 신속하고 더 효율적으로 이상행위를 탐지할 수 있는 방안을 활용할 수 있다. 이를 위해 안드로이드 앱에 대한 악성코드 피쳐를 추출하여 딥러닝을 통해 악성 행위를 분석 및 판단 가능한 정적·동적 기능을 설계하고 구현하고자, 우선적으로 안드로이드 앱에 대한 악성 앱 그리고 정상 앱에 대한 데이터 셋이 필요하다. 재난안전통신망 안드로이드 기반 전용 단말에 관련된 데이터 셋 구축 절차는, 웹크로링, 앱스토어 수집, 악성 앱 구입 및 검증으로 악성 앱 데이터 셋을 구축하고 추가적으로 분석, 학습, 시험 및 검증을 위한 정상 앱도 같이 수집한다.

4.2. 구축 2 단계 : 데이터 셋 분석을 통한 피쳐 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 모델(공개된 모든 알고리즘 모델 적용 가능) 또는 앙상블(병합) 모델을 구현하기 위해 데이터 셋은 학습, 검증 및 시험데이터로 구분되어지는 비율을 지정한다. 딥러닝 기반 탐지는 사용되는 피쳐와 알고리즘에 따라 성능이 크게 좌우되므로 가능한 다양한 딥러닝 기법을 활용하여 최적 및 최상의 모델을 시험 및 검증하여 선택한다.

이후 정적분석(악성코드 바이너리를 디컴파일하여 소스코드를 분석)을 기본으로 다양한 동적분석(에뮬레이터나 실제 폰에서 루팅 또는 디버거를 이용하여 분석) 기능까지 구현한 AI 기반 모델 학습 후 검증 및 시험을 수행하여 완성된 안드로이드 기반 악성 앱 탐지 기능을 완성한다. 그림 1은 구축 1과 2단계의 절차 흐름을 나타낸다.

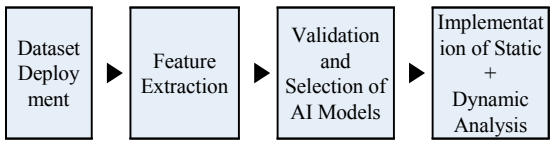

Fig. 1 Deployment 1 and 2 Phase Flow Diagram

4.3. 구축 3 단계 : 개발된 응용서비스 앱을 '재난안전통신망 모바일 앱스토어' 등재

재난안전통신망에 사용될 모든 재난안전관련 응용서비스 앱은 오직 '재난안전통신망 모바일 앱스토어(다양한 형태의 앱을 직접 전용 단말에 설치하여 활용할 수 있는 창구)' 등재를 통해서만 공유 가능하도록 절차를 규정하여 앱스토어에 등재되지 않은 앱을 사용할 경우 발생할 수 있는 위험을 사전에 제거한다.

개발자 인증(소속기관, 사용자 등의 확인) 후, 앱의 '안전 앱 인증서(안전 앱을 식별할 수 있는 해쉬 값 삽입, 非안전 앱과의 호환 금지 등의 기능 구현 등)' 취득을 위한 모든 과정을 관리할 수 있는 '앱스토어 인증위원회(가칭)'를 구성한다. 인증위원회는 응용 서비스 앱이 재난안전통신망 모바일 앱스토어에 등재하고자 하기 위해, 구축 1 및 2 단계를 통해 검증받은 결과를 기반으로, 악성 앱이 아닌 경우에 대해서 '안전 앱 인증서'를 부여하여 공인 앱에 대한 신뢰성을 확보한다. 이를 위해 재난안전통신망 응용서비스 관련 앱 개발자는 공개하고자 하는 안드로이드 기반 앱을 필요 제출물(추후 목록 정의 필요)과 함께 '앱스토어 인증위원회'에 제출한다. 추가적으로 인증위원회는 관련 안전앱에 대한 목적, 기

능성 및 사용방법 등을 서술하여 재난안전 앱 사용의 편리성 증대하기 위해, 미국 FirstNet과 같이 재난안전통신망 분야에 특화된 안전 앱 카탈로그 서비스를 제공한다[9][10].

앱 등재 후, 인증위원회는 다음과 같이 안드로이드 기반 전용 단말에 설치된 앱들에 대한 주기적인 관리를 수행한다.

- 향후 발생한 안드로이드 기반 취약점들에 대한 안전 앱 패치
- 非안전앱 설치 유무 및 설치된 非안전앱(다른 경로로 설치된 앱 또는 인증서 없는 앱) 제거
- 정보 유출, 공격지 활용 가능, 랜섬웨어 설치 등의 주기적 탐지
- 주기적인 단말 內 설치된 앱들을 스캔하여 기타 악성코드 및 악성 행위 탐지
- 탐지 시, 관리자 또는 소유자에게 경고 및 관련 정보를 전송하고 대응 전까지 해당 앱서비스 중단
- 탐지된 非안전앱, 악성코드 및 악성 행위는 AI 기반 보안 가드로 전송하여 대응방안 업데이트

그림 2는 구축 3단계의 절차 흐름을 나타낸다.

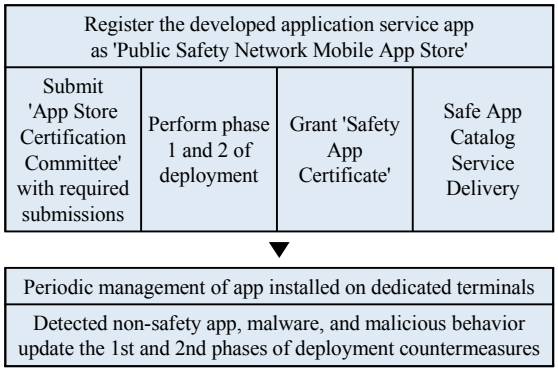

Fig. 2 Deployment 3 Phase Flow Diagram

4.4. 재난안전통신망 앱 보안체계 구축 개념

본 연구에서는 재난안전통신망에서 앱을 유통하는 앱 스토어와 단말에서 앱이 동작되는 안드로이드 운영체제에 대한 잠재적 보안 취약점에 대한 선제적 대응으로, AI 기반 재난안전통신망 보안 체계 구축을 제안하여 재난상황에 보안성을 유지하고자 하며 전체적인 개념 설명은 그림 3과 같이 요약되며 다음과 같다.

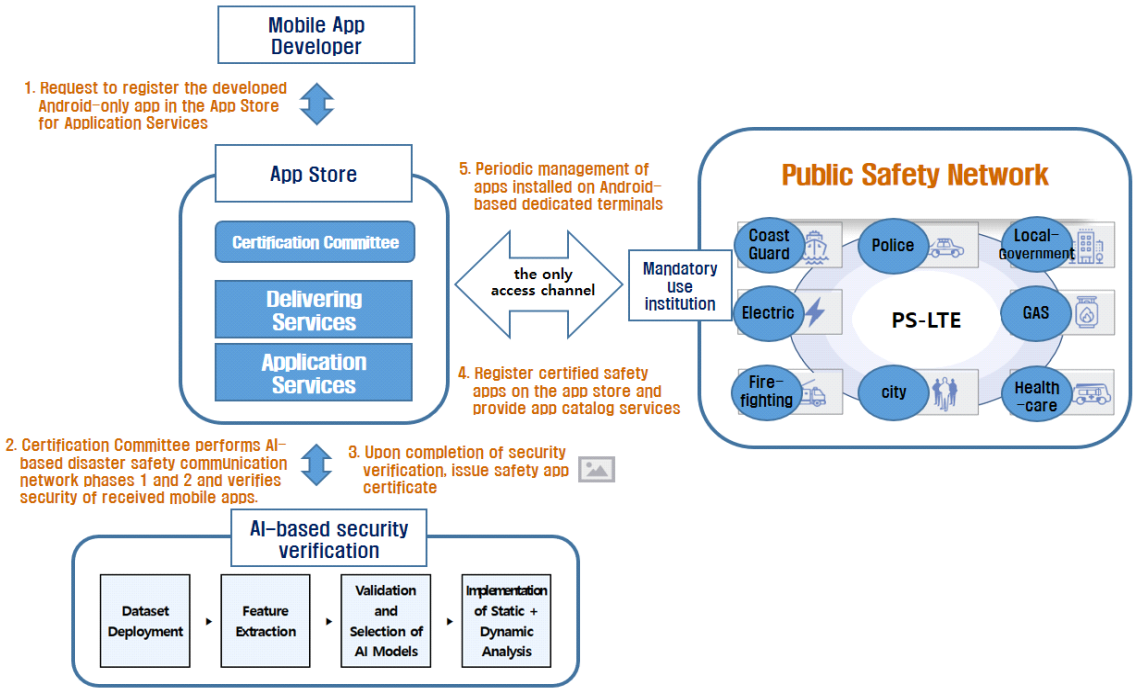

Fig. 3 Conceptual diagram of establishing a pubic safety network app security system

- 개발된 안드로이드 전용 앱을 모바일 앱스토어에 등재 요청(제출물)
- 인증위원회는 접수된 모바일 앱을 AI 기반 재난안전통신망 단계 1, 2 수행 및 보안성 검증
- 보안성 검증 완료 시, 안전 앱 인증서 발행
- 인증된 안전 앱을 앱스토어에 등재하고 앱카탈로그 서비스 제공
- 안드로이드 기반 전용단말에 설치된 앱들에 대한 주기적 관리

V. 결 론

본 연구에서는 재난안전통신망에서 앱을 유통하는 앱 스토어와 전용 단말에서 앱이 동작되는 안드로이드 운영체제에 대한 잠재적 취약점을 사전 예방하고자 '재난안전망 앱 보안 체계 구축'을 제안하였다. 제안된 체계는 재난안전통신망의 보안 사각지대를 최소화하고 인증된 앱의 재난안전 제공 및 응용 서비스 지원으로 재난상황에 대한 재난안전통신망의 안전성을 확보한다. 즉, 데이터 셋 구축 및 AI 모델의 정적 분석 및 동적 분석은 지금도 진화하고 있는 지능화된 모바일 앱 침해사고에 충분히 대응 가능하고 '재난안전통신망 모바일 앱스토어'에 등재되는 모든 앱에 '안전 앱 인증서' 부여로 재난안전통신망 관련된 모든 개발 앱에 대한 보안성 담보 및 기술력 향상을 도모한다. 궁극적으로 재난안전통신망 서비스에 대한 악용 모바일 앱의 완전 제거를 통해, 경제적 피해 예방 및 더 나아가 인명 구조의 재난안전의 본연의 의미 달성에 일조할 수 있다.

ACKNOWLEDGEMENT

This work was supported by a research grant of the Busan University of Foreign Studies in 2021

References

[1] Notification No. 2021-21 of the Ministry of the Interior and Safety, Regulations on the Operation and Use of Public Safety Network, 2021.

[2] Understanding the Public Safety Network [Internet]. Available: https://www.youtube.com/watch?v=S-om7tOS_sg, 2021.

[3] National Science and Technology Council, 3rd Comprehensive Plan for Technology Development of Disaster and Safety Management (Proposal), 2018.

[4] Statcounter-Mobile OS [Internet]. Available: https://gs.statcounter.com.

[5] KISA Report, Security that has supported Android to Android [Internet]. Available: https://www.kisa.or.kr/public/library/IS_List.jsp, KISA, 2020.

[6] American Disaster Network [Internet]. Available: https://www.firstnet.gov.

[7] LTE Overview [Internet]. Available: https://www.firstnet.gov, 2014.

[8] KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE, FirstNet's 2015 National Public Safety Broadband Annual Report, Information and Communication Policy Trends, vol. 28 no. 5, 2015.

[9] Guide for Google Play Protect [Internet]. Available: https://play.google.com/store/apps/details?id=com.protect.guide.

[10] Protect your device from harmful apps with Google Play Protect [Internet]. Available: https://support.google.com/googleplay/answer/2812853?hl=ko.

백남균(Nam-Kyun Baik)

'98.2. 숭실대학교 전자공학과 공학사
'01.2. 숭실대학교 전자공학과 공학석사
'11.2. 숭실대학교 전자공학과 공학박사
'00~'17. 한국인터넷진흥원 수석연구원
'19.3.~현재. 부산외국어대학교 정보보호학과
※ 관심분야 : 스마트융합보안, 정보보안컨설팅