공공안전통신망 단말기 보안성 시험 방법에 관한 연구

김미경, 박선우, 이태호, 조영진, 박준우
한국정보통신기술협회
kimmi@tta.or.kr, swpark@tta.or.kr, lth1124@tta.or.kr, choyj@tta.or.kr, junusee@tta.or.kr

A Study on Security Test Method for Public-Safety Network Mobile Device

Kim Mi Kyoung, Park Sun Woo, Lee Tae Ho, Cho Young Jin, Park Jun Woo
Telecommunications Technology Association

요 약

정부는 재난발생 시 통합지휘 및 신속한 상황전파를 위해 공공안전통신망을 구축하여 운영하고 있다. 공공안전통신망은 주제어시스템, 기지국, 네트워크장비, 단말기 등으로 구성되어 있으며, 공공안전통신망 단말기는 소방, 경찰, 해경 등 재난관리 및 대응기관 담당자들에게 음성 및 영상 통화, 비상시 통화, 그룹 통화, 데이터통신, eMBMS, 단말 간 통화, 단말 위치 제공과 같은 특별한 기능을 제공한다. 이와 같이 주요정보통신기반시설에서 사용되는 단말기는 민감한 정보가 유출되지 않도록 보안성이 확보되어야 한다. 본 논문에서는 공공안전통신망 단말기에 대한 보안성 시험 방법을 제시하였다.

Ⅰ. 서 론

공공안전통신망에서 사용되는 단말기는 필수적으로 요구되는 네트워크 접속 및 단말 서비스 프로토콜(VoLTE/PSVT, 위치관리서비스, SMS, MMS, CBS, MCPTT)을 포함하고 있으며, FOTA(Firmware Over the Air), 백신 기능, 공공안전통신망에서 제공하는 기본(Pre-load) 앱 등과 같은 기본 기능을 제공한다[2]. 공공안전통신망 전용단말은 업무유형에 따라 스마트폰형, 무전기형, 복합형 등으로 구분되며 안드로이드 기반으로 제작되어 다양한 앱을 통한 업무 확장이 가능하다[3].

그림 1. 공공안전통신망 단말기 종류[1]

공격자는 단말기에 설치된 기본 앱의 취약점을 이용하여 단말기 내 주요 정보에 접근하거나 단말기 기능을 사용할 수 있으며, 안드로이드 OS 기반의 보안 취약점을 악용하여 중요 정보를 탈취할 수 있다. 또한, 물리적으로 안전한 위치에서 운영되는 다른 장비와 달리 단말기는 분실, 탈취 등을 통해 비인가된 사용자가 단말기로 수신되는 정보를 불법적으로 획득할 수 있는 취약점이 존재할 수 있다.

따라서 본 논문에서는 공공안전통신망의 보안성 확보 여부를 검증하기 위해, 단말기 및 사전설치 앱 특성에 따른 취약점을 기반으로 보안성 시험 방법을 제시한다.

Ⅱ. 본론

단말기 및 사전설치 앱은 안드로이드 기반 OS에서 점검해야 하는 기본적인 보안성과 단말 접근통제를 위한 MDM 연동 기능을 확인해야 한다.

안드로이드 OS는 대표적인 스마트폰 운영체제이며, 최대 장점인 개방성으로 인해 하드웨어와 응용시스템 제조사, 앱 개발자들이 쉽게 개발할 수 있는 환경을 제공하고 있다. 그러나 안드로이드 OS에 대한 쉬운 접근성은 공격자에게 공격의 기회로 악용될 수 있다.[4]

2021년 안드로이드는 574개의 취약점이 발견되었고, 이중 79%는 공격 복잡성이 낮아 악용하기 쉬운 결함이었으며, CVSS 점수가 7.2 이상인 치명적인 결함이 23%(135개)를 차지했다. 이로 인해 공격자가 공공안전통신망 단말기를 불법적으로 취득하였을 때 공격이 용이하며, 재난 관련 데이터에 접근이 쉬울 수 있다.

단말기를 취득한 후 안드로이드 스튜디오와 같은 도구를 이용하면 단말기 로그, 메모리 등 정보를 쉽게 확인할 수 있으며, 기본 앱의 소스코드 등을 분석할 수 있다.

단말기의 취약한 설정으로 인해 불법 권한을 획득하고, 단말기 로그 및 메모리에서 주요 정보가 평문으로 출력되거나, 기본 앱에 패스워드가 하드코딩 되어 있을 경우 해당 정보를 이용하여 공공안전통신망에 불법적으로 접근하는 데 악용될 수 있다. 이러한 취약점에 대응할 수 있도록 안드로이드 OS와 기본 앱에 대한 보안성 시험항목을 [표1]과 같이 정의하였다[5][6].

시험항목	세부 내용
단말기 로그에 중요정보 저장 취약성	단말기 로그에 패스워드나 설정정보 등을 저장하여 중요정보가 노출될 수 있는 취약성이 존재하는지 확인
android manifest 파일에 취약한 권한 설정 취약성	android manifest 파일에 취약한 설정을 허용하여 권한을 과도하게 부여하거나 다른 앱에서 불필요한 activity, service, receiver 등을 호출할 수 있는지 확인
불필요한 권한설정 취약성	단말기의 폴더나 파일에 불필요한 권한이 설정되어 일반 사용자가 접근하여 중요 데이터를 획득할 수 있는 취약성이 존재하는지 확인

메모리 주요 정보 노출 취약성	플랫폼 앱(기능 ID)에서 다른 앱 호출 시 비밀정보와 같은 중요정보를 전송하여 임의의 공격자가 중요정보를 획득할 수 있는 취약성이 존재하는지 확인
Java 소스코드에 패스워드 하드코딩 취약성	Java 소스코드에 패스워드와 같은 중요정보를 하드코딩 하여 패스워드가 노출될 수 있는 취약성이 존재하는지 확인
기능ID앱 전송 데이터 보호	기능ID앱 로그인 시 서버로 전송되는 데이터에서 사용자의 ID/PW 정보 및 단말기 고유정보가 평문으로 노출되는 취약성이 존재하는지 확인
펌웨어 업데이트 무결성 보장	단말기 사용자에 의해 FOTA 서버 주소 변조가 불가해야 하며, 단말기는 펌웨어 업데이트 과정에서 FOTA 서버로부터 전송받은 펌웨어의 무결성이 훼손된 경우 이를 탐지하는지 확인

[표 1] 펌웨어 및 앱 기반 공공안전통신망 단말기 보안성 시험항목

공격자는 단말기 카메라, 마이크, GPS 기능에 불법적으로 접근하여 재난관련 데이터를 탈취할 수 있으며, 무차별대입공격 등을 통해 단말기 비밀번호를 풀고 단말에 불법적으로 접근할 수 있다. 이러한 취약점에 대응할 수 있도록 단말기에 모바일 단말 보안관리(MDM)가 설치되어 있어야 하며, MDM에 대한 보안성 시험항목을 [표2]와 같이 정의하였다[5][6].

시험항목	세부 내용
USB 외부메모리 접근통제	USB 외부메모리에 대한 접근통제가 정상적으로 수행되는지 시험
USB 디버깅 접근통제	USB를 통한 통신경로 중 디버깅에 대한 접근통제가 정상적으로 수행되는지 시험
USB 테더링 접근통제	USB를 통한 통신경로 중 USB 테더링에 대한 접근통제가 정상적으로 수행되는지 시험
Wi-Fi 접근통제	Wi-Fi를 통한 통신경로에 대한 접근통제가 정상적으로 수행되는지 시험
Bluetooth 접근통제	Bluetooth를 통한 통신경로에 대한 접근통제가 정상적으로 수행되는지 시험
카메라 접근통제	단말기의 카메라에 대한 접근통제가 정상적으로 수행되는지 시험
마이크 접근통제	단말기의 마이크에 대한 접근통제가 정상적으로 수행되는지 시험
화면캡쳐 기능 접근통제	단말기의 화면캡쳐 기능에 대한 접근통제가 정상적으로 수행되는지 시험
브라우저 접근통제	단말기의 브라우저 기능에 대한 접근통제가 정상적으로 수행되는지 시험
GPS 접근통제	단말기의 GPS에 대한 접근통제가 정상적으로 수행되는지 시험
단말기 사용자 패스워드 조합규칙 검증	단말기 사용자 패스워드에 대하여 패스워드 조합규칙 준수 여부에 대한 검증이 정상적으로 수행되는지 시험
단말기 사용자의 연속 인증 실패 시 대응행동	단말기 사용자 인증 시도 시, 연속 인증실패 횟수가 임계치를 초과하는 경우 정의된 대응행동이 정상적으로 수행되는지 시험
단말기 사용자 비활동 시 화면잠금	단말기 사용자가 정의된 시간 동안 비활동 시, 정상적으로 화면 잠금 기능을 수행하는지 시험
공장초기화 기능 수행	관리자가 원격에서 공장초기화 명령을 전송하면 단말기의 사용자 데이터에 대한 원격삭제가 정상적으로 수행되는지 시험
안전모드를 이용한 보안정책 우회 취약성	사용자가 안전모드로 부팅하여 기존에 설정된 보안정책을 우회할 수 있는 취약성이 존재하는지 시험

[표 2] MDM 기반 공공안전통신망 단말기 보안성 시험항목

Ⅲ. 결론

본 논문에서는 공공안전통신망에서 사용되는 전용단말기에 대한 보안성 시험 방법을 제시하였다. 행정안전부는 공공안전통신망과 드론을 연계하여 현장수색 및 재난현장영상 실시간 송출, IoT 센서를 활용한 하천범람, 화재감시, IoT 센서가 탑재된 손목밴드, 헬멧 등 웨어러블 안전장비를 이용한 재난대응 능력을 강화할 수 있도록 다양한 기기 연계를 확대하고 있다.

본 논문에서 분석한 결과는 추후 공공안전통신망과 연계될 다양한 기기의 보안성 시험에 활용될 수 있으며, 한국정보통신기술협회는 기기별 특성에 따른 추가적인 보안 고려사항까지 검증할 수 있도록 공공안전통신망 보안성 TTA Verified 인증 서비스의 시험 분야를 확대할 예정이다.

참 고 문 헌

[1] 행정안전부. 재난안전통신망 단말기 기본 사용법 및 교육영상

[2] 재난안전통신망 단말기 기술규격(TTA.KO-06.0496), 2018.12

[3] 재난안전통신망 이용기관 단말기 구매 규격 작성 가이드(행정안전부), 2019.5

[4] 한국정보통신학회논문지, “재난안전망 앱 보안 체계 구축”, 2021.10.

[5] 한국정보통신기술협회, “재난안전통신망 보안성 TTA Verified 인증 기준”, TCS-0006/R02:2021, 2021.10.

[6] 한국정보통신기술협회, “철도통합무선망 보안성 TTA Verified 인증 기준”, TCS-0007/R02:2021, 2021.10.