TETRA 시스템에서 단말기 접속 제어를 위한 인증 프로토콜에 관한 연구

박용석 안재환 정창호 안정철

국가보안기술연구소

parkys@etri.re.kr

A Study on the Authentication Protocol to control radio access in TETRA System

Park Yong Seok Ahn Jae Hwan Jung Chang Ho Ahn Jeong Chul

National Security Research Institute

요 약

TETRA 시스템에서는 Challenge-response 프로토콜에 의해 단말기와 인증 센터 간에 사전에 공유된 인증키가 일치하는지를 확인하는 인증 서비스를 제공함으로써 인가된 단말기만 망에 접속하도록 하고 있다. 그러나 TETRA 표준 인증 프로토콜은 단말기 식별자인 ISSI(Individual Short Subscriber Identity)가 복제된 단말기의 망 접속은 차단할 수 있지만 ISSI와 인증키가 모두 복제된 경우 복제단말기의 불법 사용을 막을 수 없는 취약점이 존재한다. 본 논문에서는 TETRA 표준인 ETSI 규격에서 정의하고 있는 인증 프로토콜을 간략히 설명하고 인증 과정에서 사용되는 인증키의 생성/분배/주입 모델을 설명한 후 인증키가 인증 센터로 전달되는 과정에서 노출되었을 경우 발생할 수 있는 복제단말기의 위협을 분석한다. 마지막으로 ISSI와 인증키가 복제된 단말기의 망 접속을 차단할 수 있는 새로운 인증 프로토콜을 제안한다.

1. 서 론

주파수 공용통신 시스템(TRS)은 한정된 무선주파수를 다수의 이동 가입자가 공유하여 통신을 행할 수 있게 하는 일련의 시스템을 말하며 이동단말기, 기지국, 이동중계국 및 시스템 관리 설비 등으로 구성된다. 국내에서는 국가 긴급재난 발생 시 일원화된 종합지휘 무선통신 체계를 확보하기 위해 유럽형 디지털 TRS 개방형 표준인 TETRA(TErrestrial Trunked RAdio) 방식으로 국가통합지휘 무선통신망 구축 사업을 추진 중에 있다[1].

TETRA는 유럽 전기통신 표준위원회(European Telecommunications Standards Institute : ETSI)가 개인 이동 무선 통신(Professional Mobile Radio : PMR)과 공공 접속 이동 통신(Public Access Mobile Radio : PAMR)을 위해 지원하는 세계 유일의 무선 디지털 개방 표준으로서 업무용 이동 무선 통신을 위해 경쟁력이 높은 개방 시장을 형성하고 있으며 세계 각국의 공공안전 및 재난통신망으로 널리 사용되고 있다. 주로 군이나 경찰을 비롯한 재난관리책임기관 사용자들의 지휘/통제 시스템으로 활용되므로 정보보호에 대한 요구 사항이 높기 때문에 TETRA에서는 정보보호 서비스를 위해 별도의 표준을 정의하고 있다[2-4].

TETRA 표준 보안기능은 보안 수준에 따라 인증(Authentication), 무선구간 암호화(Air Interface Encryption : AIE), 종단간 암호화(End-To-End Encryption : E2EE)로 구성된다.

- 인증 : 적법한 단말기만이 망에 접속하도록 하기위한 보안서비스
- 무선구간 암호화 : 단말기와 기지국사이의 무선 링크상의 모든 신호(Signalling), 식별자(Identity) 및 데이터(음성 및 데이터)의 암호화를 통해 기밀성을 제공한다.
- 종단간 암호화 : 단말과 단말사이에서 시스템을 통해 전송되는 정보를 암호화함으로써 종단간 기밀성을 제공한다.

TETRA 표준 인증 프로토콜은 단말기 위치 등록 단계에서 단말기가 위치 업데이트 요구 메시지를 망으로 전송함으로써 시작된다. Challenge-response 프로토콜에 의해 단말기와 인증 센터간에 사전에 공유된 인증키가 일치하는지를 확인함으로써 적법한 단말기인지를 검증한다. 그러나 TETRA 표준 인증 프로토콜은 단말기 식별자인 ISSI(Individual Short Subscriber Identity)가 복제된 단말기의 망 접속은 차단할 수 있지만, ISSI와 인증키가 모두 복제된 경우 복제단말기의 불법 사용을 막을 수 없는 취약점이 존재한다. 즉, 인증키의 불법 복제 위협은 고려하지 않고 있다. 본 논문에서는 TETRA 표준 인증 프로토콜을 설명하고 인증 과정에서 사용되는 인증키의 생성/분배/주입 모델을 설명한 후, 인증키가 인증 센터로 전달되는 과정에서 노출되었을 경우 발생할 수 있는 복제단말기의 위협을 분석한다. 마지막으로 인증키