독립형 5G 특화망에서 양자내성암호를 이용한 UDR 데이터 보호

손세일, 나지민, 박연규, 이상윤
한국방송통신전파진흥원 디지털융합본부
seiilson@kca.kr, na4308@kca.kr, ygpark@kca.kr, sylee76@kca.kr

Protecting UDR data with Post Quantum Cryptography in standalone Private 5G

Son Sei Il, Na Ji Min, Park Yeon Gyu, Lee Sang Yun
Korea Communications Agency

요 약

3GPP 5G 표준에서 보안은 이전 세대보다 강화된 무선 링크의 개인 정보 보호를 제공하기 위해 IMSI와 같은 영구 식별자 대신 임시 식별자 사용, 식별자를 암호화할 수 있는 사양을 제시한다. 5G 표준에서 UDR(Unified Data Repository)에 저장되는 데이터의 보안은 다루지 않고 있다. 이는 5G 특화망 모바일 코어 시스템의 구현 및 운영 방식에 따라 보안 위협이 증대될 수 있기 때문에 양자내성암호(PQC)를 이용한 UDR 데이터 보호 방안을 소개한다.

Ⅰ. 서 론

3GPP의 5G 보안 표준은 이전 세대보다 강화된 무선 링크 상에서 개인정보보호를 위한 사양을 제시한다. 5G 특화망은 제조, 물류 등 산업 현장에서 설비, 로봇 등과 연결되기 때문에 개인정보 보호 보다 데이터 보호가 중요하다. 양자내성암호를 이용하여 5G특화망 시스템과 산업 데이터를 안전하게 보호하는 방안을 소개한다.

Ⅱ. 본론

5G 특화망을 도입할 때 기존 유무선망에 5G 특화망을 구성하는 모바일 코어, 액세스망, 단말이 추가된다. 모바일 코어는 서비스 모델에 따라 내부 또는 외부에 위치한다. 독립형 서비스 모델에서 모바일 코어는 내부망에 위치하며, 코어 공유형 서비스 모델에서는 외부 클라우드를 통해 서비스가 제공된다. 5G 보안 표준은 무선 링크에서 개인정보 보호를 위해 사용자 신원 기밀성, 사용자 위치 기밀성, 사용자 추적 불가능성 등의 사양을 제시하지만[1], UDR에 저장되는 가입 자격 증명(subscription credentials) 등과 같은 데이터의 보안은 구현 메커니즘으로 보고 다루지 않는다[2]. UDR에는 단말기 정보, 가입자 정과 등의 가입 데이터, 정책 데이터, 애플리케이션 데이터 등이 저장되며된다. 3GPP 표준에서는 UDR의 보안 방안이 제시되어 있지 않기 때문에 5G특화망 모바일 코어 시스템의 구현 및 운영 방식에 따라 중요 정보가 보안 위협에 노출될 수 있다.

<그림 1>과 같이 독립형 5G 특화망에서 망을 세분화하여 기존의 유무선망과 5G특화망을 분리하고, 장기간 저장할 데이터는 양자내성암호(PQC)를 이용하면 보다 안전한 5G 특화망을 구축할 수 있다. 양자내성암호의 보안 강도를 유지하기 위해서는 양자난수 발생기가 함께 도입되어야 한다. 5G 특화망을 위한 보안 표준은 별도의 인증 서버를 통한 인증이 가능하며 이 경우 인증 서버의 데이터 저장시 양자내성암호를 적용해야 한다.

제로 트러스터 보안을 위해 내부 사용자들도 횡적 이동이 필요한 경우는 추가적인 인증절차가 이루어질 수 있도록 관리해야 한다. 사용자 인증은 멀티팩터인증(MFA)를 기본으로 하며, 최소 권한 원칙을 적용하여 특정 작업을 완료할 수 있을 만큼의 접근 권한만 부여해야 한다. 외부에서 5G 특화망을 관리하는 경우 최소 활동만 허가하고 망들 간의 횡적 접근을 금지해야 한다. 망 관리의 가시성 확보하고 중첩된 보안 정책을 확인할 수 있도록 해야 한다.

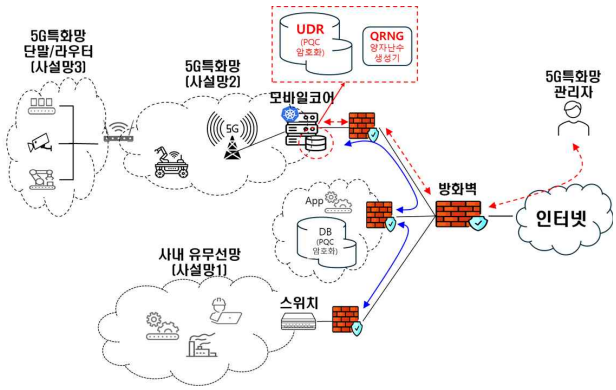

그림 1. 독립형 5G 특화망에서 PQC를 이용한 UDR 데이터 보호 예시

Ⅲ. 결론

본 논문에서는 독립형 5G 특화망 모바일 코어 시스템 내 정보 저장소인 UDR에 양자내성암호를 적용하여 보안을 강화하는 방안을 소개했다. 향후 5G 특화망의 구현 방식에 따른 양자내성암호 적용 방안에 대해 연구할 계획이다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2024-00398312 양자보안 기반 5G 특화망 기기 식별 기술 및 시험검증 기술개발)

참 고 문 헌

[1] 3GPP TS 33.102, 3G security; Security architecture (Rel.18.0.0), 2024.4.

[2] 3GPP TS 33.501, Security architecture and procedures for 5G system (Rel.18.0.0), 2022.12.