5G 이동통신 표준 네트워크 프로토콜 취약점 분석: 5G-AKA를 중심으로

고용호, 원태호, 유일선

국민대학교

{koyh0911, xoghdnjs12, isyou}@kookmin.ac.kr

Vulnerability Analysis of 5G Mobile Communication Standard Protocols: Based on 5G-AKA

Yongho Ko, Taeho Won, IlsunYou

Kookmin Univ.

요 약

5세대 이동통신 네트워크 5G는 4차 산업 혁명의 핵심으로 다양한 기술과 융합하여 미래 산업의 급속한 발전에 기여하고 있다. 이에 따라, 성공적인 미래 산업의 발전은 5G 이동통신의 견고한 보안에 달려있다는 것은 부인할 수 없는 사실이며, 이러한 목표 달성을 위해 표준기구 3GPP에서는 초기 인증단계에서의 안전한 인증 및 키 합의를 위해 5G-AKA 프로토콜을 제안하여 표준화하였다. 본 논문에서는 암호 프로토콜 표준 문서 ISO/IEC 29128-1:2023에서 제시하는 요구사항을 만족하는 정형화 검증 도구 ProVerif를 사용하여 5G-AKA를 모델링하고 정형화 검증 수행을 통해 취약점 분석을 진행하였다. 검증 결과를 토대로 5G 가입자의 식별자 SUPI에 대한 재전송 공격과 완전 순방향 비밀성에 대한 취약점 도출을 통해 5G 이동통신 네트워크 보안 기술 발전을 위한 방향을 제안하였다.

Ⅰ. 서 론

5세대 이동통신 네트워크(5G)는 단순한 개인의 휴대전화 중심의 서비스를 넘어 자율주행, 스마트 홈, 스마트 팩토리, 원격 의료, XR(eXtended Reality)과 같은 다양한 융합 서비스를 통해 우리의 삶을 크게 변화시켰다[1]. 이를 통해 5G의 보안 취약점은 우리 실생활에 큰 영향을 줄 수 있기 때문에 견고한 보안 프로토콜 설계가 요구되고 있다, 표준기구 3GPP(3rd Generation Partnership Project)에서는 안전한 5G 초기 인증을 위해 키 합의 프로토콜 5G-AKA(Authentication and Key Agreement)를 제안하고 표준화하였다[2].

본 논문에서는 암호 프로토콜 표준 문서 ISO/IEC 29128-1:2023[3]에서 제시하는 요구사항을 만족하는 정형화 검증 도구 ProVerif[4]를 통해 5G-AKA 프로토콜을 모델링하고 정형화 검증을 통해 취약점을 분석하여 5G 이동통신 네트워크 보안 기술이 나아가야 할 방향을 제안하고자 한다.

Ⅱ. 본론

2.1 프로토콜 구성

5G-AKA 프로토콜은 그림 1과 같이 등록 단계와 인증 단계로 설계되어 있다. 참여 개체로 USIM(Universal Subscriber Identity Module)과 ME(Mobile Equipment)로 구성되는 UE(User Equipment)와 무선을 통해 연결되는 네트워크인 SN(Serving Network)의 역할을 하는 SEAF (Security Anchor Function)와 UE가 등록되어 있으며 접속이 시도되는 네트워크 HN(Home Network)에 속하는 AUSF(Authentication Server Function)와 UDM/ARPF(Unified Data Management / Authentication credential Repository and Processing Function)로 구성되어 있다.

초기 단계에서 UE는 SUPI(Subscription Permanent Identifier)와 HN의 공개키 그리고 롱텀 키를 통해 계산되는 암호 값 SUCI(SUbscription Concealed Identifier)을 통해 SN에 전달하게된다. 이후, SN은 식별자를 추가하여 HN에 전달하며 통신 간 매개체 역할을 수행한다. HN에서는 SUCI를 복호화하고 SUPI를 획득하여 등록된 가입자인지 검증한다.

HN에서 SUPI에 대한 검증이 완료되면 인증 단계를 시작하게 된다. HN에서는 5G-KDF(Key derivation function)을 통해 인증 벡터를 생성한 뒤 회신하며 Challenge를 시작한다. SN은 인증 벡터값을 UE에 포워딩하게 되고 인증 매개변수를 전달받은 UE는 이를 계산하며 MAC(Message Authentication Code) 값과 SQN(Sequence Number)를 검증하고 이를 완료하면 Response를 수행한다. SN과 HN은 이 메시지를 검증하며 UE를 검증하고 HN이 완료 메시지와 함께 UE의 SUPI와 앵커키를 SN에게 응답하며 5G-AKA 프로토콜이 성공적으로 완료된다.

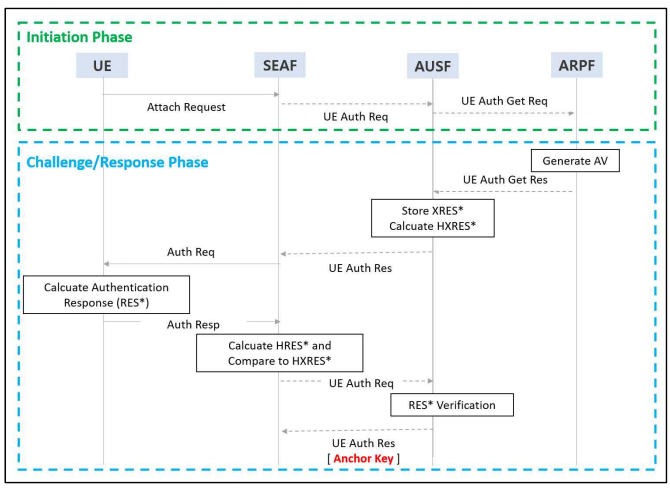

그림 1. 5G-AKA Protocol Procedure

2.2 정형화 검증기법을 통한 취약점 분석

본 연구에서는 정형화 검증 도구 ProVerif을 통해 5G-AKA를 모델링한 뒤 정형화 검증 수행을 통해 취약점을 도출하였다. ISO/IEC 29128-1:2023에서는 무제한 병렬 세션 검증 수행을 위한 속성인 Unbounded 지원 유무 요구사항에 따라 Unbounded(강력한 검증)/Bounded(일반 검증) 검증으로 분류되며 ProVerif은 Unbounded 속성을 지원하며 강력한 검증을 수행할 수 있다.

ProVerif은 모델링을 위해 Declartion, Process Macro, Main Process로 세 단계로 나누어져 있다.

Declaration 단계는 모델링을 위해 타입, 변수, 상수, 통신 채널, 생성자 및 소멸자를 사용자 정의에 맞게 선언할 수 있으며 이러한 확정성을 통해 암호화 프리미티브 모델링에 용이하다. 본 단계에서는 5G-AKA에서 사용되는 암호기법과 타입을 선언하였으며 UE와 SN 간 통신은 공격자가 언제든지 침해할 수 있도록 공개채널로 설정하였으며 SN과 HN 간의 통신은 시큐어 채널로 모델링하였다.

Process Macro 단계에서는 하위 프로세스의 동작을 선언하며 각 엔티티의 동작은 개별적으로 선언함으로써 모듈화 기반 모델링에 용이하다. 본 단계에서는 UE, SN 그리고 HN의 동작을 모델링하였다.

Main Process 단계에서는 그림 2와 같이 프로세스를 실행하는 역할을 한다. 암호 기법과 주요 정보를 채널을 통해 공유할 수 있으며 하위 프로세스를 호출한다 여기서 Unbounded 속성을 통한 강력한 검증을 수행하였으며 Phase 기능을 통한 완전 순방향 비밀성의 검증을 수행하였다.

```
process
    new prHN: secKey; let puHN = pk(prHN) in out(usch, puHN);
    new SUPI: bitstring; new K: key;
    new SQN: seq;

    insert ueDB(SUPI, K, SQN);
    (!UE(SUPI, K, SQN, puHN))|
    (!SN(SNname))|
    (!HN(SUPI, prHN))|
    phase 1; out(usch, (prHN, K))
```

그림 2. Proverif Main Process

ProVerif에서는 Event 기능을 통해 도달 가능성, 대응의 보안속성으로 검증을 수행한다. 본 연구에서는 Attcker 기능을 통해 기밀성을 검증하였으며 Inj-event을 사용하여 프로토콜 메시지 간 인증 및 적시성을 검증하였다.

의도적으로 참여자 간 생성되어있는 공개 채널에 파생된 매개변수를 암호키로 사용하여 암호계산되는 평문 값을 브로드 캐스팅하고 해당 평문 값에 대한 기밀성 검증을 통해 공격자에 의해 기밀성이 침해되었는가를 검증하였다. 5G-AKA 프로토콜의 주요한 값인 SUPI, K_{ausf} 그리고 앵커키 K_{seaf}를 대상으로 검증하였으며 ProVerif의 경우 디버깅 기능을 제공하지 않기 때문에 각 엔티티 간 마지막에 의도적 평문 유출을 통한 기밀성 검증으로 프로세스가 정상적으로 종료되었는지에 대한 코드를 추가하였다. 또한, ProVerif에서 제공하는 보안성 검증 기능인 Event의 경우 적시성 검증 유무에 따라 Event(재전송 공격 허용)/Inj-event(재전송 공격 불허용)의 기능으로 나뉜다. 본 연구에서는 강력한 보안성 검증을 위해 Inj-event 기능을 사용하여 엔티티 간 1:1 통신이 적시성의 보안요구사항을 만족하는가를 검증하였다.

모델링을 마치고 정상적으로 프로세스가 동작하여 완료된다면 그림 3과 같은 결과를 반환한다. 본 결과를 통해 SUCI에 대한 재사용 공격 가능성 및 롱텀키 K 유출에 의한 순방향 비밀성 침해의 취약점 결과를 도출하였다.

그림 3. ProVeirf Verification Summary

Ⅲ. 결론

본 논문에서는 5G 표준 이동통신 네트워크의 인증 및 키합의 과정에서 발생가능한 보안 취약점을 도출하고 개선하기 위해 정형화 검증도구 ProVerif를 이용하여 검증을 수행하였다.

검증 결과를 통해 초기인증 단계에서 SUCI에 대한 재전송 공격이 가능함을 보였으며, 롱텀 키 K가 유출되었을 경우에 따른 완전 순방향 비밀성 침해에 의한 공격을 보이며 통신 간 기밀성 침해 가능성을 보였다. 5G 이동통신 네트워크 표준 프로토콜의 경우 프로토콜 간 호환을 위해 초기인증 단계에서의 개선은 이루어 지지 않는 실정이므로 이에 대한 개선이 미진한 상황이다. 하지만 향후 6세대 이동통신 네트워크 시대에서도 5G 네트워크가 사용될 것을 고려한다면 SUCI에 대한 취약점들에 대한 개선은 필수적이다. 또한, 하트블리드 버그 사태[6]를 통해 완전 순방향 비밀성에 대한 교훈을 얻었음에도 불구하고 아직까지 표준 프로토콜인 5G-AKA에서는 이에 대한 대응이 부족한 실정이다.

이에 따라, 향후연구로 초기인증 단계에서 재전송 공격을 대응할 수 있으며 완전 순방향 비밀성을 보장할 수 있도록 5G-AKA 프로토콜을 개선하고 설계된 프로토콜을 정형화 검증 기법을 통해 보안성을 검증하는 연구를 진행하고자 한다.

ACKNOWLEDGMENT

본 과제(결과물)은 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업(차세대통신)의 연구 결과입니다.

Following are results of a study on the "Convergence and Open Sharing System(NCCOSS)" Project, supported by the Ministry of Education and National Research Foundation of Korea.

참 고 문 헌

[1] 이지혜, 정제민, 이종식, “모바일 ICT 융합서비스”, 한국통신학회, pp. 3-11. 2017년 11월.

[2] 3GPP, “Security architecture and procedures for 5G System” 3GPP TS 33.501v18.3.0, Sep. 2023

[3] ISO/IEC 29128:2011: Information technology - Security techniques - Verification of cryptographic protocols, International Organization for Standardization, Geneva, Switzerland, Dec. 2011.

[4] B. Blanchet, “Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif,” In International School on Foundations of Security Analysis and Design (FOSAD 2012/2013), pp. 54-87, 2014.

[5] Daemen, J., and Rijmen, V. “AES Proposal: Rijndael, Version2.,” Submission to NIST, March 1999.

[6] 보안뉴스, “암호화 통신 늘어나고, 부하 분산 장치 중요해지고”, 2017. Available: https://www.boannews.com/media/view.asp?idx=53108&kind=4 [Online: accessed on May. 8 ,2024]