Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.3, Jun. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.3.565

5G NAS COUNT 취약점을 이용한 보안 위협 분석*

김 민 재,[1†] 박 종 근,[2] 신 지 수,[2] 문 대 성[3,4‡]
[1]㈜이스트소프트 (연구원), [2,3]한국전자통신연구원 (연구원, 실장),
[4]과학기술연합대학원대학교 (교수)

An Analysis of Security Vulnerabilities Using 5G NAS COUNT*

Min-Jae Kim,[1†] Jong-Geun Park,[2] Ji-Soo Shin,[2] Dae-Sung Moon[3,4‡]
[1]EstSoft (Researcher), [2,3]Electronics and Telecommunications Research Institute (Researcher, Department Manager),
[4]University of Science and Technology (Professor)

요 약

현재 이동 통신 시스템은 4G LTE 네트워크에서 5G 네트워크로 전환하는 과정에 있으며, 이동 통신 서비스의 보편화에 따라 식별자 및 위치 정보를 포함하는 개인 정보들이 이동통신 네트워크를 통해 전달되고 있다. 무선 이동통신망의 특성에 따라 무선 공유 채널의 사용이 불가피하고, 요구하는 대역폭과 속도를 만족시키기 위해서는 모든 네트워크 시스템 요소에 보안 기술을 적용할 수 없으므로 가능한 공격 형태를 예측하고 보안 위협을 분석하는 기술의 중요성이 더욱 커지고 있다. 특히, 보안 위협 분석을 위해 5G 네트워크의 경우 사용자 서비스를 불가능하게 만들기 위해 허위 기지국 또는 공격자 UE를 통한 다양한 공격 형태와 취약성 분석에 대한 연구들이 이루어지고 있다. 본 논문에서는 오픈 소스를 이용하여 5G 네트워크 테스트베드를 구축하고, 테스트베드를 이용하거나 3GPP 규격을 분석하여 NAS COUNT와 관련한 세 가지 보안 취약점들을 분석하였으며, 두 가지 취약성에 대해 유효성을 확인하였다.

ABSTRACT

Current mobile communication system is in the mid-process of conversion from 4G LTE to 5G network. According to the generalization of mobile communication services, personal information such as user's identifiers and location information is transmitted through a mobile communication network. The importance of security technology is growing according to the characteristics of wireless mobile communication networks, the use of wireless shared channels is inevitable, and security technology cannot be applied to all network system elements in order to satisfy the bandwidth and speed requirements. In particular, for security threat analysis, researches are being conducted on various attack types and vulnerability analysis through rogue base stations or attacker UE to make user services impossible in the case of 5G networks. In this paper, we established a 5G network testbed using open sources. And we analyzed three security vulnerabilities related to NAS COUNT and confirmed the validity of two vulnerabilities based on the testbed or analyzing the 3GPP standard.

Keywords: 5G Network, Vulnerability Analysis, NAS Count

Received(03. 16. 2022), Modified(05. 03. 2022), Accepted(05. 03. 2022)

* 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발].

† 주저자, opnkj67@gmail.com

‡ 교신저자, daesung@etri.re.kr(Corresponding author)

I. 서 론

이동 통신 기술은 각 세대를 거치면서 빠른 속도로 발전하고 있으며, 우리 나라의 경우 전국적으로 4G LTE(Long-Term Evolution) 네트워크가 보편화 되었으며 일부 지역에 대해 5G 네트워크 서비스를 제공하고 있다.

현재 5G 네트워크는 특성상 셀 커버리지 제약에도 불구하고 서비스 가용성을 보장하기 위해 일부분 4G LTE 네트워크망과 연계된 NSA(Non-Stand Alone)방식으로 서비스를 제공한다. 5G 네트워크는 4G LTE 네트워크에 비해 상호 운용 가능한 구조의 액세스 네트워크와 네트워크 가상화 및 프로그래밍, 분산 네트워크 아키텍처와 같은 부분들이 크게 변화하였다. 동시에, 4G LTE 네트워크에서 확인할 수 있는 보안 취약점 중 하나인 가입자 식별 번호의 노출 문제는 5G 네트워크로 발전하면서 3GPP(3rd Generation Partnership Project) 규격에서 암호화를 적용함으로써 해결되었으나, 여전히 다양한 보안 취약점들이 보고되고 있다. 예를 들어 5G 네트워크의 제어 평면 메시지 중 무결성 보호 또는 암호화 없이 전송되는 메시지를 이용해 NAS(Non Access Stratum) Count를 조작하여 정상적인 서비스를 불가하게 만드는 취약점들이 확인되었다[1-2]. 이는 5G 네트워크를 시뮬레이션[3-4]과 3GPP 규격을 기반으로 검증을 수행하였다.

5G 네트워크의 보안 취약점은 단말에 대한 서비스 거부 상태를 유발하거나 과금 유도, 배터리 고갈 문제를 야기할 수 있을 뿐만 아니라 위치 정보를 포함는 개인 정보 침해 문제를 발생시킬 수 있기 때문에 실제 5G 네트워크 프로토콜에서 보고된 취약점들에 대한 분석과 유효성을 확인하는 일은 필수적이다.

본 연구에서는 선행 연구[1-2]에서 제시된 5G 네트워크의 제어 평면 보안 취약점 중 NAS Count와 관련한 보안 취약점을 분석하고, 이를 이용한 공격이 유효한지 확인한다.

2장에서는 연구 배경과 NAS Count의 개념에 대해 설명하고, 3장에서는 각 NAS Count와 관련한 공격에 대해 설명한다. 4장에서는 취약성 분석을 위한 테스트베드 환경을 설명한다. 5장에서는 취약성 분석 결과와 결과에 대한 근거와 제약사항들을 정리한다.

II. 연구 배경

2.1 5G 네트워크 구조

5G 전체 구조는 〈Fig 1〉과 같이 5G 코어, RAN(Radio Access Network), 사용자 단말로 구성된다. RAN은 단말과의 무선 신호 구간을 담당해 단말이 무선 신호로 통신할 수 있게 하며 코어는 단말의 제어 신호와 데이터 신호를 관리한다. 코어와 단말이 제어 신호를 주고 받을 때는 이후 설명할 NAS 계층 신호를 사용한다.

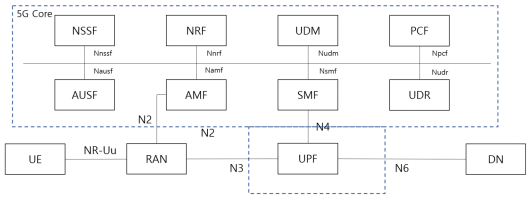


Fig. 1. 5G Network architecture

2.2 Non Access Stratum (NAS)

NAS는 단말과 5G 코어 네트워크 간 통신 계층으로, 단말과 세션의 관리를 NAS 계층의 제어 평면에서 담당한다[5]. NAS 계층에서 AMF(Access and Mobility Management Function)는 5G 네트워크 단말의 등록과 인증, 이동성을 관리하며, SMF(Session Management Function)에서 사용자 단말 (UE: User Equipment)의 IP 주소 할당 및 PDU(Protocol Data Unit) 세션 제어를 담당한다. 단말의 인터넷 사용과 관련된 DN(Data Network)과의 통신은 UPF(User Plane Function)이 담당한다.

NAS 연결에서 단말과 AMF는 Security Mode Command와 Security Mode Complete 메시지를 통해 NAS 메시지에서 사용할 무결성 및 암호화 알고리즘을 합의한다. 무결성 및 암호화 알고리즘인 NIA(NR Integrity Algorithm), NEA(NR Encryption Alogrithm)는 각각 〈Table 1〉, 〈Table 2〉와 같이 4가지 옵션이 존재한다. 3GPP TS 24.501[5]의 무결성 및 암호화 규칙에 따르면 암호화 알고리즘의 지정은 관리자에 의해 결정되지만, 무결성 알고리즘의 경우 응급상황 이외에는 Null 알고리즘을 사용하지 못하도록 강제된다. 단말

Table 1. 5G Integrity Algorithm type

Identifier	Algorithm
NIA0	Null
NIA1	Snow 3G
NIA2	AES
NIA3	ZUC

Table 2. 5G Encryption Algorithm type

Identifier	Algorithm
NEA0	Null
NEA1	Snow 3G
NEA2	AES
NEA3	ZUC

과 AMF간 무결성 및 암호화 알고리즘을 합의하기 이전에는 NAS 계층 메시지들이 무결성 및 암호화가 적용되지 않은 상태로 전달되기 때문에 스니핑과 재생 공격 등에 취약성을 가진다. 따라서, 5G NAS 계층에 대한 대부분의 공격은 무결성 및 암호화 알고리즘을 합의하는 Security Mode Procedure가 진행되기 전 단계에서 시도된다.

2.3 NAS COUNT

NAS Count는 NAS 계층의 단말과 AMF 간 통신에서 NAS 계층에 메시지 재전송 방지와 인증 과정에서 사용되는 키 발급에 입력 값으로 사용된다. 따라서, NAS Count를 악의적인 목적으로 사용할 경우 정상적인 서비스를 불가능하게 만들 수 있다.

〈Fig. 2〉는 3GPP TS 33.501[6]의 키 발급 계층도이다. NAS Count는 NAS 키 발급 과정에 입력값으로 사용되며, 특히 K_{gNB} 발급 과정에서 상향 Count를 입력값으로 사용한다.

NAS Count는 코어 방향으로 상향 메시지에 대한 UL(Uplink) Count와 하향 메시지에 대한 DL(Downlink) Count를 정의하였으며, 단말과 AMF는 자신의 UL COUNT와 DL COUNT를 각각 저장한다. NAS Count는 〈Fig. 3〉과 같이 총 길이 24bit로 16bit의 OC(Overflow Count)와 8bit의 SQN(Seqeunce Number)로 구성된다.

NAS Count는 단말과 AMF가 NAS 메시지를

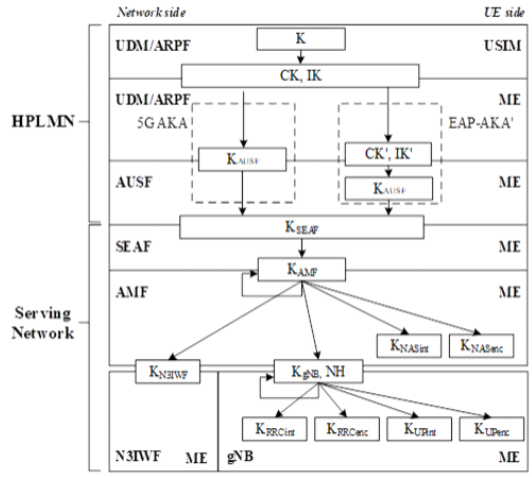


Fig. 2. Key generation hierarchy in 5G

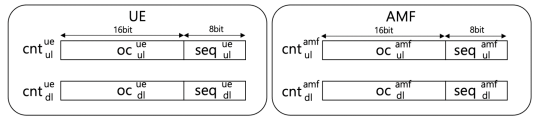


Fig. 3. NAS Count structure

주고 받을 때 SQN 값을 1씩 증가시키고 SQN 값이 임계점(256)에 도달하면 OC 값을 1 증가시켜 전송한다. NAS 계층보다 아래 계층인 PDCP(Packet Data Convergence Protocol) 계층 등에서 발생한 메시지 폐기와 같은 이유로 정상적인 통신 상황에서 단말과 AMF 간 NAS Count 값의 비동기화가 일어날 수 있으므로, NAS 메시지를 수신하면 단말과 AMF는 수신한 NAS 메시지의 Count 값을 참조하여 자신의 UL Count와 DL Count를 업데이트한다. 새롭게 키를 발급할 때 NAS Count 비동기화가 일어나면 취약점으로 작용할 수 있으며, NAS Count 비동기화로 인한 취약점은 키 발급 상황에서 단말과 AMF의 NAS Count 초기화를 통해 단말과 AMF의 NAS Count 비동기화를 유도해 발생할 수 있다.

III. NAS COUNT 취약점

본 장에서는 선행 연구[1-2]에서 언급한 보안 취약점 중 NAS Count를 이용한 취약점에 대해 설명한다.

3.1 NAS 카운터 초기화 공격

NAS 카운터 초기화 공격은 단말과 AMF 간 NAS Count 값의 비동기화에 의해 서로 다른 K_{gNB}를 생성하도록 유도하여 피해 단말이 정상적인 통신이 불가능하게 만드는 공격이다. 공격자는 허위 기지국을 구성하고 피해 단말과 AMF 사이에 중간자로 위치한다. 공격자는 가장 먼저 피해 단말과 AMF의 initial connection에 사용되는 Security Mode Command와 Security Mode Complete (NAS COUNT : 0)을 캡쳐한다. 이후 공격자는 AMF 서버에서 K_{gNB}를 재발급하도록 한다.

〈Fig. 4〉는 NAS 카운터 초기화 공격 시나리오의 절차이다. 3GPP TS 33.501[6]에 따르면, NAS key를 재발급할 때 NAS 무결성, 암호화 알고리즘 교환 절차인 Security Mode Procedure를 진행하여 단말과 AMF간 재발급한 NAS key를 동기화한다. NAS 카운터 초기화 공격에서 AMF는 5G 네트워크 표준 절차에 따라 재발급한 K_{gNB}를 동기화하기 위해 피해 단말에게 Security Mode Command를 전송한다. 공격자는 AMF가 전송한 Security Mode Command 메시지를 폐기하고 이전에 캡쳐한 DL Count 값이 0인 Security Mode Command 메시지를 피해 단말에게 전송한다. 공격자는 피해 단말의 응답 메시지인 Security Mode Complete 메시지 또한 폐기한 뒤 이전에 캡쳐한 UL Count 값이 0인 Security Mode Complete 메시지를 AMF로 전송한다. 따라서 피해 단말의 DL Count와 AMF의 UL Count가 0으로 업데이트된다. 이후 각각 저장하고 있는 UL Count를 이용해 새로운 K_{gNB}를 발급할 때 사용하는 UL Count 값이 피해 단말은 0으로 reset 되지 않기 때문에 피해 단말과 AMF 간 K_{gNB}의 비동기화가 발생하고, 피해 단말이 서비스 거부 상태에 빠지게 된다.

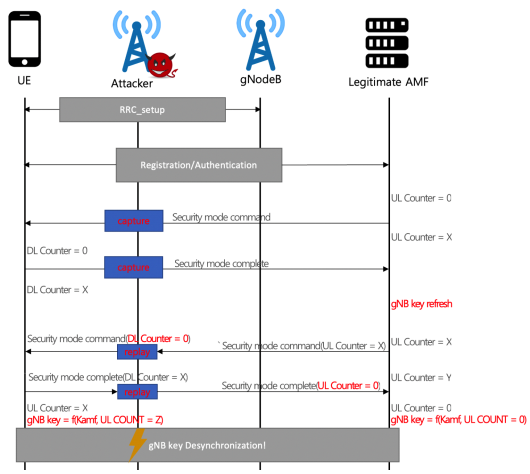


Fig. 4. NAS Counter Reset attack

3.2 상향 NAS 카운터 비동기화 공격

상향 NAS 카운터 비동기화 공격은 단말과 AMF 간 NAS Count 값의 비동기화를 유발하여 단말이 정상적인 서비스를 받지 못하도록 하는 공격으로, 〈Fig. 5〉는 상향 NAS 카운터 비동기화 공격의 전체 절차를 나타낸다.

5G 네트워크의 Security Mode Procedure에서 사용자 단말은 AMF가 전송한 Security Mode Command 메시지에 유효하지 않은 MAC 값이 포함될 경우 Security Mode Reject 메시지로 응답하고 자신의 UL Count 값을 1 증가시킨다.

상향 NAS 카운터 비동기화 공격에서 공격자는 단말이 Security Mode Reject 메시지를 몇 번 보냈는지 체크하지 않는 점을 이용한다. 공격자는 허위 기지국을 이용하여 다수의 임의 MAC 값을 생성하고 이를 Security Mode Command 메시지에 포함하여 피해 단말에게 반복적으로 전송한다. 피해 단말은 수신한 Security Mode Command 메시지에 대해 MAC 값 검증에 실패하기 때문에 Security Mode Reject 메시지로 응답하면서 UL Count를 1 증가시킨다. 공격자는 위 공격을 단말의 UL Count 값이 256이 될 때까지 반복한다. 단말은 UL Count 값이 256에 도달하면 UL Overflow

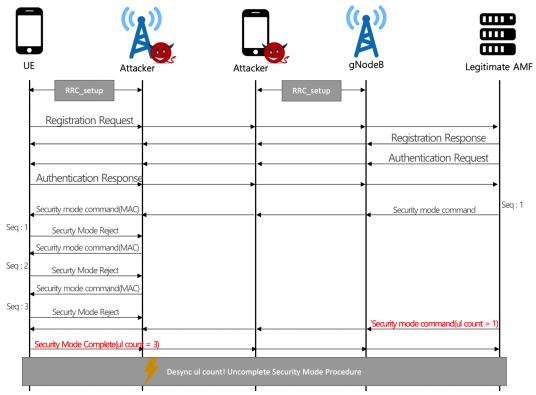


Fig. 5. Uplink desynchronization attack

Count를 1 증가시킨다. AMF는 Security Mode Reject 메시지를 수신하지 못했으므로 initial connection 때의 UL Count 값을 유지한다. 따라서, 단말과 AMF 간 UL Count 비동기화가 발생하고 단말은 AMF가 보낸 메시지의 MAC 검증을 올바르게 할 수 있지만 AMF는 단말이 보낸 메시지에 대해 MAC 검증에 실패하고 메시지를 폐기하기 때문에 단말이 서비스 거부 상태에 빠지게 된다. 이후 AMF가 UL Count의 재동기화를 위해 Security Mode Command를 전송하더라도 피해 단말의 응답인 Security Mode Complete 메시지의 MAC 검증에 문제가 발생하므로 피해 단말의 서비스 거부 상태는 지속될 수 있다.

3.3 NAS 시퀀스 값 노출 공격

NAS 계층에서 Security Mode Procedure가 정상적으로 끝나면 송수신 메시지에 대한 무결성을 확인할 수 있고 암호화가 적용된 상태로 통신이 이루어지지만, NAS 시퀀스 값 노출 공격 공격은 MAC 값과 시퀀스 값이 평문으로 전송되는 취약성을 이용한다. 공격자가 피해 단말과 AMF 사이의 NAS 메시지를 캡쳐할 수 있으면 현재 시퀀스 값을 확인할 수 있으므로 공격자는 피해 단말의 시퀀스 값에 대한 스니핑을 통해 피해 단말의 서비스 사용량에 대한 모니터링이 가능하다.

IV. 5G 취약성 분석 테스트베드

5G 네트워크의 취약점 분석을 실제 상용망을 기반으로 수행하거나 물리적인 테스트베드를 구축하는 데에는 많은 한계점이 존재한다. 따라서 본 연구에서는 공개 소프트웨어를 이용해 5G 네트워크 테스트베드를 구축하였다. 5G 취약성 분석 테스트베드는 3GPP 표준 규격을 따라야 하며 SA 모드의 5G 네트워크를 지원하는 것이 중요하다.

우리는 공개 소프트웨어의 개발 진척도 및 안정성을 고려하여 5G 코어 네트워크로 Open5GS[8-9]를, 5G RAN으로 UERANSIM[10]을 이용하였다. Open5GS는 현재 AMF, SMF, UPF와 함께 PCF(Policy Control Function), AUSF(Authentication Server Function), UDM(Unified Data Management) 등의 요소들도 함께 구현되어있는 상태이다. 또한 Open5GS는 3GPP Release 16의 5G 코어 네트워크 표준을 따르고 있으며 단말 접속 및 인증 등 코어 네트워크의 기능을 비교적 충실하게 제공한다.

5G RAN 역할로써 UERANSIM은 기지국과 단말이 시뮬레이팅 형태로 동작하며 3GPP의 5G 네트워크 표준을 따라 5G 신호의 생성 및 관리를 수행한다. UERANSIM은 PHY/MAC 계층의 개발이 이루어지기 이전 상태이기 때문에 5G 신호의 송/수신은 유선으로 에뮬레이션된다.

우리는 본 테스트베드를 구축하기 위해 Open5GS v2.3.2와 UERANSIM v3.2.2를 사용하였으며 취약점 검증에 필요한 공격을 위해 일부 코드를 수정하거나 공격 도구들을 추가적으로 구현했다.

〈Fig. 6〉은 5G 취약성 분석 테스트베드의 구조를 나타낸다. 우리는 이를 활용하여 UE와 AMF 사이와 UE와 gNodeB 사이 및 gNodeB와 AMF 사이의 패킷을 모니터링해 각 공격을 분석하고 제약사항과 유효성을 확인하였다. 각 공격에 대해 3GPP 표준 기반으로 공격의 유효성을 함께 살펴보기 위해 3GPP 표준 중 NAS 계층과 관련된 표준인 TS 24.501[5], Security와 관련된 표준인 TS 33.501[6] 그리고 RRC 계층과 관련된 표준인 TS 38.331[7] 문서의 분석도 활용하였다.

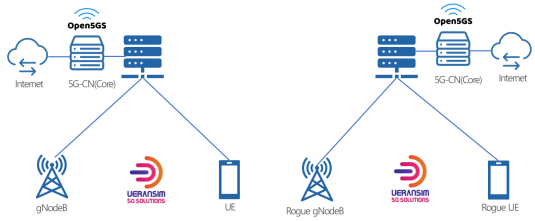


Fig. 6. 5G vulnerability analysis testbed

V. 5G 취약성 공격 실험 결과

이 장에서는 5G NAS 카운터와 관련한 보안 위협에 대해 분석하고 테스트베드와 3GPP 규격 상 실험한 결과를 설명한다.

5.1 NAS 카운터 초기화 공격

5.1.1 취약점의 유효성 판단 기준

NAS 카운터 초기화 공격에 대한 유효성 판단 기준은 NAS 카운터 중 상향 카운터가 key gNB의 발급에 관여하기 때문에 카운터가 틀어질 경우 AMF와 단말이 서로 다른 key gNB가 발급하게 된다. 따라서, key gNB의 refresh 유도로 인한 Security Mode Procedure 가 종료된 후 단말과 AMF의 key gNB가 서로 다른 값으로 발급되었는지 확인하여 판단할 수 있다.

5.1.2 취약성 분석 결과

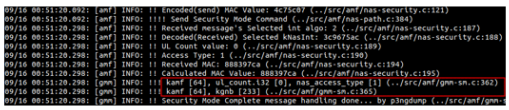
NAS 카운터 초기화 공격 수행을 위해 오픈소스를 이용해 구성한 테스트베드 상에서 key gNB에 발급에 대한 로그 출력 부분과 일정 범위까지 NAS 카운터를 증가시키기 위한 부분 및 key gNB refresh에 대한 공격에 대해 코드를 수정하였다.

NAS 카운터 초기화 공격에 대한 취약점 실행 결과 〈Fig. 7〉과 같이 피해 단말과 AMF의 key gNB가 서로 다른 값이 발급되는 것을 확인할 수 있다. 정상적인 key gNB 값은 AMF와 피해 단말 모두 “233” 이었으나, 공격 이후 피해 단말의 key gNB 값이 “146” 으로 바뀌어 AMF와 피해 단말 사이의 key gNB 동기화가 틀어지는 것을 확인하였다. 따라서 NAS 카운터 초기화 공격에 대한 취약성은 유효하다.

NAS 카운터 초기화 공격이 실제 5G 프로토콜 상에서도 유효한 것을 확인하였으나 공격이 발생할 수 있는 가능성은 매우 낮다. 만약, NAS 카운터 초기화 공격이 성공하기 위해서는 공격자가 아래와 같은 두 가지 조건을 충족해야 한다.

- 허위 기지국 구성 및 피해 단말과 AMF가 통신 전 피해 단말의 허위 기지국 연결 유도로 중간자 공격 선행
- 정상 AMF 서버 장악 후 key gNB refresh 유발

<AMF's Key gNB>



<UE's Key gNB>

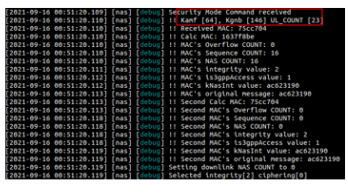


Fig. 7. NAS Counter reset result

위 조건 중 AMF 서버를 장악한 후 key gNB refresh 유발 과정은 AMF가 운용되는 서버의 보안 취약점을 추가로 이용해야 한다. 이는 상용 5G 망을 대상으로 한다면 통신사업자가 관리하는 AMF 서버에 대한 장악이 선행되어야 한다는 것이다. 따라서, NAS 카운터 초기화 공격은 유효할 수 있으나 실제 발생할 가능성은 매우 낮다.

5.2 상향 NAS 카운터 비동기화 공격

5.2.1 취약점의 유효성 판단 기준

상향 NAS 카운터 비동기화 공격에 대한 유효성 판단은 공격자가 허위 기지국을 통해 피해 단말에게 임의의 MAC 값을 포함한 Security Mode Command 메시지를 지속적으로 전송했을 때 피해 단말이 UL Count를 증가시키고 단말과 AMF 간 UL Count의 비동기화가 발생하여 단말이 서비스 거부 상태가 될 수 있는가로 판단할 수 있다.

5.2.2 취약성 분석 결과

상향 NAS 카운터 비동기화 공격의 유효성은 3GPP 규격으로 판별할 수 있으며, 결과적으로 유효하지 않은 공격이며 그 이유는 다음과 같다. 만약 공격에 의해 피해 단말이 UL Count를 증가시키더라도 Overflow Count가 증가하지 않는다면 피해 단말은 서비스 불능 상태가 되는 것이 아니며, 수신한 SQN으로 자신의 SQN을 업데이트하고 정상적인 서비스를 이어나가는 것으로 확인하였다.

3GPP TS 33.501[6]의 6.7.2의 NOTE 3 내용에 따르면, 만약 단말이 Security Mode Reject 메시지를 보냄으로써 UL Count의 Overflow Count가 1 증가하는 Wrap Around가 이루어질 경우 단말은 Security Mode Reject 메시지를 보내지 않고 AMF와 NAS 연결을 Release 하도록

정의되어있다. 따라서, 공격을 통한 UL Count의 Overflow Count 증가로 비동기화가 발생하기 전에 단말과 AMF는 NAS 연결을 Release한다.

또한, 해당 공격을 이용하여 피해 단말의 UL Count를 증가시키려면 다음과 같은 제약이 따른다. TS 24.501[5]의 5.4.2.7의 내용에 따르면, Security Mode Procedure는 T3560 타이머(6초)와 함께 진행된다. 만약 타이머가 만료될 때까지 절차가 완료되지 않으면 AMF는 단말에게 다시 Security Mode Command 메시지를 전송한다. 타이머 4회 만료 후 5회 재전송 시 AMF는 Security Mode Command 메시지를 전송하는 것이 아니며, 등록 절차를 다시 시작한다. 즉, 해당 공격에서 UL Count를 증가시키기 위해서는 타이머 4회 만료 시간인 24초 안에 256개의 Security Mode Command를 전송시켜야 하는데, 이는 짧은 시간 제약에 다수의 메시지 전송이기 때문에 메시지의 정상적인 송신을 보장할 수 없으며 UL Count의 증가도 보장할 수 없다.

5.3 NAS 시퀀스 값 노출 공격

5.3.1 취약점의 유효성 판단 기준

NAS 시퀀스 값 노출 공격이 유효한가에 대한 판단은 첫째, 단말과 AMF 간 송수신하는 NAS 메시지를 캡쳐하였을 때 시퀀스 값이 평문으로 전송되는지, 둘째, 스니핑된 시퀀스 값을 통해 피해 단말의 서비스 사용 모니터링이 가능한지를 확인하여 판단할 수 있다.

5.3.2 취약성 분석 결과

단말과 AMF 사이 NAS 계층 메시지에 대한 스니핑을 위해 NAS 계층 인터페이스에 대한 패킷 캡쳐를 수행하였다. 단말과 AMF 간 NAS 계층 메시지를 캡쳐해 pcap 파일로 저장 후 분석한 결과 〈Fig. 8〉과 같이 무결성 및 암호화 알고리즘 합의 이후에도 MAC 값과 시퀀스 값은 평문으로 전송되는 것을 확인할 수 있다. 또한, 만약 공격자가 지속적인 스니핑을 통해 시퀀스 값의 증가량을 확인하면 피해 단말의 서비스 사용량에 대한 모니터링이 가능하기 때문에 NAS 시퀀스 값 노출 공격에 대한 취약성은 유효하다.

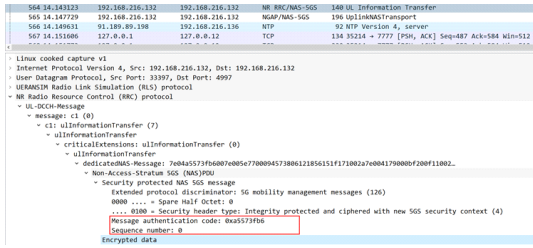


Fig. 8. Plain sequence number after security context established

NAS 시퀀스 값 노출 공격은 공격에 성공하더라도 피해가 크지 않다. 이는 공격자가 단말의 시퀀스 값을 스니핑한다고 해도 정상 서비스를 방해하거나 불가능하게 만들 수 없기 때문이다. 또한, 공격자가 지속적인 스니핑을 하더라도 피해 단말의 서비스 사용량을 모니터링 할 뿐 구체적인 서비스는 알 수 없다.

VI. 결 론

5G 규격에서는 5G의 기초적인 규격과 함께 4G LTE에서 발생했던 보안 취약점을 기반으로 하는 대응 방안이 추가되었지만 허위 기지국 또는 공격자 UE를 통한 또 다른 유형의 공격은 여전히 유효한 상태이다. 우리는 3GPP 규격을 따르는 공개 5G 소프트웨어를 이용하여 5G 테스트베드를 구축하고, 공격 도구를 추가적으로 구현하여 공격을 재현하였으며, 테스트베드와 3GPP 규격을 기반으로 5G 프로토콜 상에서 보안 취약점과 공격의 유효성을 분석하였다.

NAS 카운터 초기화 공격의 경우 NAS 카운터 초기화 이후 단말과 AMF가 각기 발급하는 key gNB가 서로 다른 것으로 나타나 유효함을 확인하였다. NAS 시퀀스 값 노출 공격은 단말과 AMF 간 NAS 계층 메시지 캡쳐를 진행해 NAS 시퀀스 값이 평문으로 나타나는 것을 확인해 유효함을 확인하였다. 마지막으로 상향 NAS 카운터 비동기화 공격의 경우 단말과 AMF의 UL Count의 비동기화 상태를 만들었지만 단말이 서비스 거부 상태에 빠지지 않는 것으로 확인하여 유효하지 않음을 확인하였다.

본 연구의 결과는 5G 네트워크 보안 취약점에 대해 3GPP 표준 규격을 침해하지 않으면서 공격에 대응하는 연구의 기초 자료로 활용할 수 있다.

References

[1] X. Hu, C. Liu, S. Liu, W. You, Y. Li and Y. Zhao, "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security," in IEEE Access, vol. 7, pp. 125424-125441, 2019, doi: 10.1109/ACCESS.2019.2937997.

[2] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 2019. 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, pp. 669–684. DOI:https://doi.org/10.1145/3319535.3354263.

[3] nuXmv. https://nuxmv.fbk.eu/. Accessed May 25, 2022.

[4] S. Meier, B. Schmidt, C. Cremers and D. Basin, "The TAMARIN prover for the symbolic analysis of security protocols", Proc. Int. Conf. Comput. Aided Verification, pp. 696-701, 2013.

[5] [n.d.]. Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3, Specification 3GPP TS 24.501 version 16.8.0 Release 16. 3GPP. 3GPP Mobile Competence Centre, c/o ETSI, 650, route des Lucioles, 06921 Sophia Antipolis Cedex, France. 696. 2021.

[6] [n.d.]. Security architecture and procedures for 5G system, Specification 3GPP TS 33.501 version 16.8.0 Release 16. 3GPP. 3GPP Mobile Competence Centre, c/o ETSI, 650, route des Lucioles, 06921 Sophia Antipolis Cedex, France. 248. 2021.

[7] [n.d.]. NR; Radio Resource Control(RRC) protocol specification, Specification 3GPP TS 38.331 version 16.4.0 Release 16. 3GPP. 3GPP Mobile Competence Centre, c/o ETSI, 650, route des Lucioles, 06921 Sophia Antipolis Cedex, France. 930. 2021.

[8] Open5GS. https://open5gs.org/. Accessed May 25, 2022.

[9] Open5GS. https://github.com/open5gs. Accessed May 25, 2022.

[10] UERANSIM. https://github.com/aligungr/UERANSIM. Accessed May 25, 2022.

〈저 자 소 개〉

김 민 재 (Min-Jae Kim) 정회원
2020년 2월: 순천향대학교 정보보호학과 학사
2022년 2월: 과학기술연합대학원대학교 정보보호공학 석사
2022년 2월~현재: 이스트소프트 연구원
〈관심분야〉 정보보호, 악성코드, 네트워크 보안, 5G 보안

박 종 근 (Jong-Geun Park) 정회원
1997년 2월: 성균관대학교 산업공학과 학사
1999년 2월: 성균관대학교 산업공학과 석사
2013년 2월: 충남대학교 컴퓨터공학과 박사
1999년 3월~2001년 4월: 국방과학연구소 연구원
2001년 5월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 이동통신보안, SDN/NFV, 클라우드보안

신 지 수 (Ji-Soo Shin) 정회원
2003년 2월: 숭실대학교 컴퓨터공학부 학사
2005년 2월: 숭실대학교 컴퓨터공학과 석사
2009년 8월: 숭실대학교 컴퓨터공학과 박사
2009년 8월~2010년 7월: 젠솔소프트 연구원
2010년 7월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 라우팅, 클라우드, SDN, 네트워크 보안

문 대 성 (Dae-Sung Moon) 정회원
2007년 2월: 고려대학교 전산학과 박사
2000년 12월~현재: 한국전자통신연구원 정보보호연구본부 실장
2009년 3월~현재: 과학기술연합대학원대학교 정보보호공학 전공주임교수
〈관심분야〉 정보보호, 네트워크보안, 인공지능보안, 영상보안