JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 9, pp. 113-120, September 2022
https://doi.org/10.9708/jksci.2022.27.09.113

Analysis of the IP Spoofing Attack Exploiting Null Security Algorithms in 5G Networks

Tae-Keun Park*, Jong-Geun Park**, Keewon Kim***

*Professor, Dept. of Computer Engineering, Dankook University, Yongin, Korea
**Principal Researcher, Information Security Research Division, ETRI, Daejeon, Korea
***Professor, Dept. of Computer Engineering, Mokpo National Maritime University, Mokpo, Korea

[Abstract]

In this paper, we analyze the feasibility of the IP spoofing attack exploiting null security algorithms in 5G networks based on 3GPP standard specifications. According to 3GPP standard specifications, the initial Registration Request message is not protected by encryption and integrity. The IP spoofing attack exploits the vulnerability that allows a malicious gNB (next generation Node B) to modify the contents of the initial Registration Request message of a victim UE (User Equipment) before forwarding it to AMF (Access and Mobility Management Function). If the attack succeeds, the victim UE is disconnected from the 5G network and a malicious UE gets Internet services, while the 5G operator will charge the victim UE. In this paper, we analyze the feasibility of the IP spoofing attack by analyzing whether each signaling message composing the attack conforms to the 3GPP Rel-17 standard specifications. As a result of the analysis, it is determined that the IP spoofing attack is not feasible in the 5G system implemented according to the 3GPP Rel-17 standard specifications.

▸ **Key words**: 5G, Null Security Algorithm, 3GPP Standard, IP Spoofing Attack, Attack Analysis

[요 약]

본 논문에서는 5G 네트워크에서 Null 보안 알고리즘 (Null Security Algorithm)을 악용한 IP 스푸핑 공격 (IP Spoofing Attack)의 실현 가능성을 3GPP 표준 규격에 근거하여 분석한다. 3GPP 표준 규격에 따르면, 초기 Registration Request 메시지는 암호화 및 무결성 보호를 받지 못한다. IP 스푸핑 공격은 피해자 UE (User Equipment)의 초기 Registration Request 메시지의 내용을 악의적인 gNB (next generation Node B)가 수정한 뒤 AMF (Access and Mobility Management Function)에게 전송할 수 있다는 취약점을 활용하는 공격이다. 공격이 성공하면, 피해자 UE는 5G 네트워크에서 연결이 끊어지고 악의적인 UE가 인터넷 서비스를 사용하지만 5G 사업자는 피해자 UE에게 요금을 청구한다. 본 논문에서는 IP 스푸핑 공격을 구성하는 각각의 시그널링 메시지가 3GPP Rel-17 표준 규격에서 허용되는 것인지 여부를 분석함으로써 IP 스푸핑 공격의 실현 가능성을 분석한다. 분석 결과, 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 IP 스푸핑 공격은 실현 불가능한 공격으로 판단된다.

▸ **주제어**: 5G, Null 보안 알고리즘, 3GPP 표준, IP 스푸핑 공격, 공격 분석

• First Author: Tae-Keun Park, Corresponding Author: Keewon Kim
*Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
**Jong-Geun Park (queue@etri.re.kr), Information Security Research Division, ETRI
***Keewon Kim (kwkim@mmu.ac.kr), Dept. of Computer Engineering, Mokpo National Maritime University
• Received: 2022. 08. 17, Revised: 2022. 09. 06, Accepted: 2022. 09. 15.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

디지털 셀룰러 네트워크에서의 다섯 번째 기술 표준인 5G (Fifth-Generation)는 이전 세대에서 발견된 한계들을 극복할 뿐만 아니라 이전 세대에 비해 증가한 사용 사례들의 요구사항을 충족시키기 위하여 새로운 아키텍처와 기술들을 채택하고 있다 [1-5]. 그러나 보안 측면에서 5G의 새로운 보안 정책들이 공식적으로 검증 완료되지 않았다는 것과 4G LTE (Long Term Evolution)로부터 상속되는 보안 문제 (예: 일부 초기 시그널링 메시지들이 무결성 보호되지 않는 취약점)들이 5G에 여전히 포함되어 있다는 것이 문제점으로 지적되고 있다 [6].

4G LTE에서의 보안 취약점 발견 연구로 LTEFuzz [7]와 LTEInspector [8]가 있다. LTEFuzz [7]에서는 4G LTE NAS (Non-Access Stratum) 계층과 RRC (Radio Resource Control) 계층에서의 보안 문제를 동적으로 테스트하기 위하여 반자동 테스트 도구인 LTEFuzz를 개발하였다. LTEInspector [8]에서는 4G LTE 제어 평면 프로토콜 (Control-Plane Protocol)에 대한 보안 테스트를 수행하기 위하여 LTEInspector 프레임워크를 제안하였다.

5G에서의 보안 취약점을 찾고 그 취약점을 활용하는 공격을 식별할 목적으로 진행된 연구로는 5GReasoner [6]와 Null 보안 알고리즘에 대한 5G 보안 분석 [9]이 있다.

5GReasoner [6]에서는 5G RRC 계층과 NAS 계층에 대한 정형적인 보안 검증을 수행할 수 있는 5GReasoner 프레임워크를 개발한 뒤, 5GReasoner 프레임워크를 활용하여 5G에서의 보안 설계 취약점과 취약점을 활용하는 공격을 식별하고자 하였다. 이와 관련하여, 최근 연구 [10-12]에서 5GReasoner [6]가 제시한 세 가지 공격 각각에 대하여 3GPP 표준 규격에 따라 구현된 5G 시스템에서의 실현 가능성에 대하여 분석하였는데, 그 결과, 분석된 공격의 일부 혹은 전체가 실현 불가능한 것임이 밝혀졌다. 이러한 결과는 5GReasoner [6]에서 형식적인 속성들을 3GPP 표준 문서로부터 추출할 때 표준 규격의 세부적인 사항들을 정확하게 반영하지 못하였기 때문에 발생한 것으로 추정된다 [10].

Null 보안 알고리즘에 대한 5G 보안 분석 [9]은 모델 검증 원칙 (Principle of Model Checking)에 기반한 시스템적 접근 방법을 적용하여 Null 보안 알고리즘 관련 취약점이 5G에 미치는 영향에 대하여 분석하였다. 5G에서 Null 보안 알고리즘이란 암호화와 무결성 보호를 제공하지 않는 알고리즘을 의미하며, NEA0과 NIA0이 이에 속한다 [9]. NEA0은 암호화에 사용되는 Null 보안 알고리즘을 의미하고, NIA0은 무결성 보호에 사용되는 Null 보안 알고리즘을 의미한다. 이러한 Null 보안 알고리즘에 대한 5G 보안 분석 결과물 중 하나로 [9]는 5G에서의 IP 스푸핑 공격 (IP Spoofing Attack)을 제시하였다.

본 논문에서는 Null 보안 알고리즘에 대한 5G 보안 분석 [9]에서 제시한 IP 스푸핑 공격이 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 실현 가능한 공격인지에 대하여 분석한다. 본 논문의 구성은 다음과 같다. 제 2장에서 IP 스푸핑 공격 [9]에 대하여 소개한 뒤, 제 3장에서 IP 스푸핑 공격을 구성하는 각각의 시그널링 메시지가 3GPP Rel-17 표준 규격에서 허용되는 것인지 여부를 분석함으로써 IP 스푸핑 공격의 실현 가능성을 판단한다. 마지막으로 제 4장에서 결론을 기술한다.

II. IP Spoofing Attack

본 장에서는 Null 보안 알고리즘에 대한 5G 보안 분석 [9]이 제시한 IP 스푸핑 공격에 대하여 소개한다. IP 스푸핑 공격 [9]에서 공격자는 악의적인 gNB (Malicious next generation Node B)와 악의적인 UE (Malicious User Equipment)를 설정할 수 있으며, 강력한 신호를 송출함으로써 피해자 UE (Victim UE)를 악의적인 gNB로 끌어들일 수 있다고 가정한다. 또한, SUPI (Subscription Permanent Identifier) 및 암호화 키와 같은 피해자 UE에 대한 어떠한 정보도 공격자가 사전에 가지고 있지 않다고 가정한다.

Fig. 1의 IP 스푸핑 공격 절차 [9]에서, 피해자 UE는 코어 네트워크 (Core Network)에 등록하고 IP 주소를 할당받기 위하여, Attach 절차를 시작한다. Attach 절차는 4G LTE에서 사용되는 용어이지만, Null 보안 알고리즘에 대한 5G 보안 분석 [9]에서 IP 스푸핑 공격을 서술할 때 사용하였기 때문에, 본 장에서는 Fig. 1에 표기된 용어를 사용하여 IP 스푸핑 공격 절차를 소개한다. 그러나 다음 장에서 3GPP Rel-17 표준 규격에 기반하여 IP 스푸핑 공격 [9]의 실현 가능성을 분석할 때에는 3GPP Rel-17의 5G 용어를 사용한다.

Fig. 1에서 Attach 절차는 피해자 UE가 코어 네트워크에 Attach Request 메시지 (Fig. 1의 시그널링 메시지 1)를 전송하면서 시작된다. 초기 Attach Request 메시지는 암호화 보호 및 무결성 보호를 받지 못하므로, 악의적인 gNB는, 첫째, 이 메시지에 포함된 UE의 보안 능력 (Security Capabilities) 매개변수를 조작하고, 둘째, UE

가 지원하는 보안 알고리즘을 Null 보안 알고리즘 (즉, NIA0, NEA0)으로 변경하거나 또는 Null 보안 알고리즘의 우선순위를 가장 높게 설정할 수 있다.

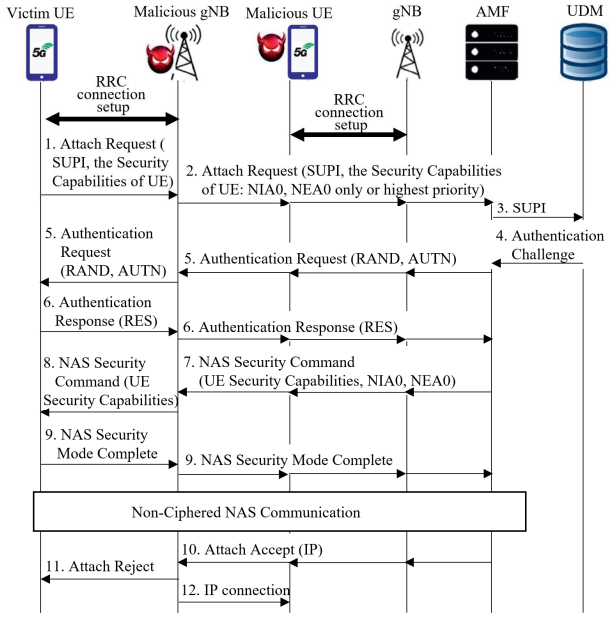

Fig. 1. IP Spoofing Attack

이상과 같이 악의적인 gNB에 의해 조작된 Attach Request 메시지 (Fig. 1의 시그널링 메시지 2)를 AMF (Access and Mobility Management Function)가 수신하면, AMF는 인증 (Authentication) 절차를 시작한다. 피해자 UE와 코어 네트워크 사이의 인증 절차가 성공적으로 완료되면, 코어 네트워크의 AMF는 Null 보안 알고리즘인 NIA0과 NEA0을 보안 알고리즘으로 선택한 뒤, 그러한 선택 결과를 포함한 NAS Security Mode Command 메시지 (Fig. 1의 시그널링 메시지 7)를 피해자 UE에게 전송한다. 이후의 통신에는 암호화 키가 필요하지 않기 때문에, 공격자는 암호화 및 무결성 보호 없이 평문 형식으로 코어 네트워크와 시그널링 메시지를 교환할 수 있다.

코어 네트워크의 AMF가 Attach Accept 메시지 (Fig. 1의 시그널링 메시지 10)내에 피해자 UE에게 할당한 IP 주소를 포함시켜 전송하면, 악의적인 gNB는 피해자 UE에게 Attach Reject 메시지 (Fig. 1의 시그널링 메시지 11)를 전송함과 동시에, 악의적인 UE에게 피해자 UE의 IP 주소 사용을 지시 (Fig. 1의 시그널링 메시지 12)한다. 피해자 UE는 악의적인 gNB로부터 Attach Reject 메시지를 수신하면, 피해자 UE가 재시작되거나 SIM 카드가 재설치될 때까지 코어 네트워크와 연결을 맺지 못할 수 있다. IP 스푸핑 공격의 결과, 인터넷 서비스는 악의적인 UE가 사용하지만 네트워크 서비스 사용 요금은 피해자 UE에게 부과된다.

III. Analysis of the IP Spoofing Attack

본 장에서는 Null 보안 알고리즘에 대한 5G 보안 분석 [9]이 제시한 IP 스푸핑 공격이 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 실현 가능한 공격인지에 대하여 분석한다. 분석할 IP 스푸핑 공격 절차는 Fig. 1의 절차와 동일하지만, 앞서 서술한 바와 같이, 본 장에서는 3GPP Rel-17의 5G 용어를 사용하여 공격 실현 가능성을 분석한다. Table 1과 같이 IP 스푸핑 공격의 시그널링 절차를 네 개의 부분으로 나눈 뒤, 각각에 대하여 Table 1에 명시된 의문을 중심으로 분석을 수행한다. Table 1의 네 개의 부분에서 괄호 안의 숫자는 각 부분에서 분석할 Fig. 1의 시그널링 메시지 번호를 의미한다.

Table 1. Four Parts to Analyze

Four Parts	Questions
Sending Registration Request (1~2)	Can the malicious gNB modify the Registration Request?
Authentication Procedure (3~6)	Can the authentication procedure be successful?
NAS Security Mode Command / Control (7~9)	Do the victim UE and AMF agree to use NEA0 and NIA0?
Registration Accept / Reject (10~12)	Does the victim UE accept the Registration Reject sent by the malicious gNB?

1. Analysis of Sending Registration Request

본 분석은 Fig. 1의 시그널링 메시지 1부터 2까지에 대한 것이다. Fig. 1의 시그널링 메시지 1과 2인 Attach Request 메시지는 3GPP Rel-17 표준 규격의 Registration Request 메시지에 해당한다 [13].

악의적인 gNB가 피해자 UE를 강력한 신호로 끌어들이면, 피해자 UE는 악의적인 gNB와 RRC Connection Setup 절차를 시작한다 [14]. RRC Connection Setup 절차의 마지막 단계는 피해자 UE로부터 악의적인 gNB에게로 RRCSetupComplete 메시지가 전송되는 것인데, 이 RRCSetupComplete 메시지의 dedicatedNAS-Message 필드에 NAS의 Registration Request 메시지가 포함되어 전송된다 [13-14].

Fig. 1에는 Attach Request가 SUPI를 포함하는 것으로 되어 있으나, 3GPP TS 23.502 [15]에 따르면, UE가 NAS 보안 컨텍스트 (Security Context)를 가지고 있지 않은 경우에 Registration Request 메시지에는 SUPI가 아니라 SUCI (Subscription Concealed Identifier) 또는 5G-GUTI (Global Unique Temporary Identifier)가 포

함되어야 하는데, 초기 등록의 경우에는 SUPI를 보호하기 위하여 암호화된 SUCI가 포함되어야 한다.

이상에서 서술한 바와 같이, Fig. 1의 시그널링 메시지 1과 2는 용어 측면에서 수정이 필요하다. 하지만, 피해자 UE의 초기 Registration Request 메시지는 암호화 및 무결성 보호를 받지 못하므로 초기 Registration Request 메시지의 내용을 악의적인 gNB가 수정한 뒤 AMF에게 전송할 수 있다는 취약점이 3GPP Rel-17 표준 규격에 존재함을 3GPP TS 24.501 [13]의 4.4.4.3에서 확인할 수 있다.

정리하면, 초기 Registration Request 메시지의 경우, 악의적인 gNB는 피해자 UE가 지원하는 보안 알고리즘을 Null 보안 알고리즘 (즉, NIA0, NEA0)으로 변경하거나 또는 Null 보안 알고리즘의 우선순위를 가장 높게 설정하는 형태로 Registration Request 메시지를 변경한 뒤 AMF에게 전송할 수 있다.

2. Analysis of Authentication Procedure

본 분석은 Fig. 1의 시그널링 메시지 3부터 6까지에 대한 것이다. 5G에서의 전반적인 보안 구조와 절차를 서술하고 있는 3GPP TS 33.501 [16]에 따르면, 시그널링 메시지 3은 Nausf_UEAuthentication_Authenticate Request 메시지와 Nudm_UEAuthentication_Get Request 메시지가 합쳐져서 표현된 것이고, 시그널링 메시지 4는 Nudm_UEAuthentication_Get Response 메시지와 Nausf_UEAuthentication_Authenticate Response 메시지가 합쳐져서 표현된 것으로 볼 수 있다. 다만 시그널링 메시지 3과 4는 IP 스푸핑 공격과 관련하여 구체적인 설명을 필요로 하는 부분이 아니기 때문에 Fig. 1에서 간략하게 표현된 것으로 보인다. 시그널링 메시지 5와 6은 각각 NAS Authentication Request와 Response 메시지 [13]에 해당한다.

정리하면, Fig.1의 시그널링 메시지 3에서 6까지에 해당하는 인증 절차는 3GPP Rel-17 표준 규격에 따라 구현된 시스템에서 문제없이 진행될 수 있다.

3. Analysis of NAS Security Mode Command / Complete

본 분석은 Fig. 1의 시그널링 메시지 7부터 9까지에 대한 것이다. Fig. 1의 시그널링 메시지 7인 NAS Security Mode Command 메시지는 UE의 보안 능력 (Security Capability)과 함께 선택된 보안 알고리즘으로 NIA0과 NEA0을 포함하고 있다. 이와 관련하여, AMF가 NIA0과 NEA0을 보안 알고리즘으로 선택한 UE에 대하여 Security Mode Command 메시지를 전송하는지 여부에 대하여 3GPP Rel-17 표준 규격을 확인할 필요가 있다.

3GPP TS 24.501 [13]의 5.4.2.2는 네트워크에서 시작하는 NAS Security Mode Control 절차에 대하여 서술하고 있다. 초기 등록에서 보안 알고리즘으로 NIA0과 NEA0이 선택된 경우에 대하여 기술된 내용을 살펴보면, UE에 대한 유효한 5G NAS 보안 컨텍스트 (Security Context)가 존재하지 않으면서 긴급 서비스를 위하여 초기 등록하는 경우에만 AMF가 NIA0과 NEA0을 포함하는 NAS Security Mode Command 메시지를 UE에게 전송할 수 있다고 명시되어 있다. 따라서, 이와 관련하여, UE에 대한 유효한 5G NAS 보안 컨텍스트가 언제 생성되는지와 어떠한 경우에 유효한 NAS 보안 컨텍스트가 존재하지 않는지에 대하여 확인할 필요가 있다.

3GPP TS 24.501 [13]의 4.4.2는 5G NAS 보안 컨텍스트에 대한 처리 방법을 기술하고 있다. 그 내용에 따르면, 5G NAS 보안 컨텍스트는 Primary Authentication and Key Agreement 절차의 결과로 생성된다. Fig. 1의 절차에서 시그널링 메시지 7인 NAS Security Mode Command 메시지가 전송되기 전에, 앞서 살펴본 바와 같이, 시그널링 메시지 3에서 6까지에 해당하는 인증 절차가 성공적으로 완료되었기 때문에, 이 시점에 AMF와 UE 사이의 Key Agreement가 성공적으로 완료되었는지에 대하여 확인할 필요가 있다.

3GPP TS 33.501 [16]의 6.2는 계층적인 키 생성에 대하여 기술하고 있다. Fig. 2는 3GPP TS 33.501 [16]의 Figure 6.2.1-1과 동일한 내용을 보여준다. 3GPP TS 33.501 [16]의 6.2에 따르면, UE와 네트워크가 K_{AMF}까지의 키들을 생성하면, Primary Authentication and Key Agreement 절차에서 Key Agreement가 완료되었다고 판단한다. 그렇다면, UE와 네트워크가 언제 K_{AMF}를 생성하고, K_{AMF}와 5G NAS 보안 컨텍스트를 어떻게 연결시키는지에 대하여 확인할 필요가 있다.

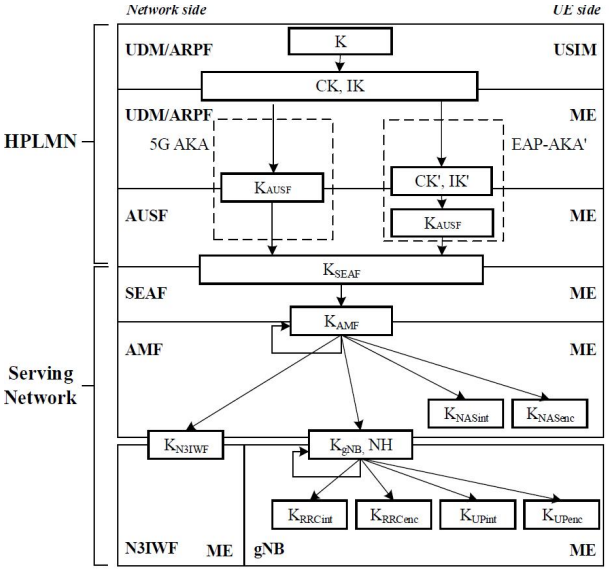

Fig. 2. Key Hierarchy Generation in 5GS [16]

3GPP TS 24.501 [13]의 5.4.1.3.1은 5G AKA-based Primary Authentication and Key Agreement에 대하여 기술하고 있다. 그 내용에 따르면, 5G 인증이 성공적으로 완료된 경우, Partial Native 5G NAS 보안 컨텍스트가 생성되며, 이것을 AMF가 사용하기 위하여 AMF는 Security Mode Control 절차를 시작한다. 또한 3GPP TS 24.501 [13]의 5.4.1.3.1에 따르면, Fig. 1의 시그널링 메시지 5인 NAS Authentication Request 메시지는 ngKSI를 포함하고 있으며, 이 ngKSI는 UE와 AMF가, 인증이 성공하였을 때 생성되는, Partial Native 5G NAS 보안 컨텍스트와 K_{AMF}를 식별하기 위하여 사용된다. UE에서의 K_{AMF}와 5G NAS 보안 컨텍스트 처리에 대한 내용은 3GPP TS 24.501 [13]의 5.4.1.3.2에 기술되어 있다. 그 내용에 따르면, 5G Authentication Challenge가 성공하였을 때, UE는 새로 계산하여 생성한 K_{AMF}를 새로운 5G NAS 보안 컨텍스트에 저장한다.

이상의 내용으로부터, Fig. 1의 시그널링 메시지 6까지 성공적으로 진행되었다면 UE와 AMF는 유효한 5G NAS 보안 컨텍스트를 가진다라고 정리할 수 있다. 그러나 Fig. 1의 시그널링 메시지 7인 NIA0과 NEA0을 포함하는 Security Mode Command 메시지가 전송되기 위해서는 UE에 대한 유효한 5G NAS 보안 컨텍스트가 존재하지 않아야 한다.

따라서, 본 분석의 앞부분으로 돌아가서, AMF가 NIA0과 NEA0을 보안 알고리즘으로 선택한 UE에 대하여 Security Mode Command 메시지를 전송하는지 여부에 대하여 판단해 본다면, AMF는 그렇게 하지 않을 것이라는 결론을 얻을 수 있다. 왜냐하면, UE의 인증이 성공적으로 완료된 시점에 유효한 5G NAS 보안 컨텍스트가 생성되고, 그렇다면, 3GPP TS 24.501 [13]의 5.4.2.2에 기술된 "UE에 대한 유효한 5G NAS 보안 컨텍스트가 존재하지 않으면서 긴급 서비스를 위하여 초기 등록하는 경우"라는 조건이 거짓이 되기 때문이다.

지금까지의 분석 내용을 정리하면, Fig.1의 시그널링 메시지 7을 포함하는 NAS Security Mode Control 절차는 3GPP Rel-17 표준 규격에 따라 구현된 시스템에서 동작할 수 없다. 따라서, 본 논문에서 분석하고자 하는 Null 보안 알고리즘에 대한 5G 보안 분석 [9]에서 제시한 IP 스푸핑 공격은 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 실현 불가능한 공격이라고 결론을 낼 수 있다.

그러나, LTEFuzz [7]에서 밝혀진 바와 같이 3GPP 규격을 정확하게 반영하지 못한 상용 시스템도 존재할 수 있기 때문에, Fig. 1의 시그널링 메시지 7을 전송하는 그러한 상용 시스템이 존재한다고 가정하고 IP 스푸핑 공격에 대한 분석을 계속 진행하면 다음과 같다.

Fig.1의 시그널링 메시지 8인 NAS Security Mode Command 메시지는 시그널링 메시지 7과 다른 메시지처럼 표현되어 있으나, Null 보안 알고리즘에 대한 5G 보안 분석 [9]에는 시그널링 메시지 8에 대한 구체적인 설명이 존재하지 않는다. 따라서 시그널링 메시지 8에 포함된 UE의 보안 능력 (Security Capabilities)과 선택된 5G 보안 알고리즘이 어떤 것인지에 대하여 분석할 필요가 있다.

첫째, 시그널링 메시지 8에 포함된 UE의 보안 능력 (Security Capabilities)에 대하여 분석하면 다음과 같다. 3GPP TS 24.501 [13]의 5.4.2.3은 NAS Security Mode Command 메시지를 수신한 UE의 동작에 대하여 기술하고 있다. 그 내용에 따르면, 악의적인 gNB는 반드시 피해자 UE가 Fig. 1의 시그널링 메시지 1에 포함시켰던 UE의 보안 능력 (Security Capabilities)과 동일한 내용을 시그널링 메시지 8인 NAS Security Mode Command 메시지에 포함시켜야 한다. 왜냐하면, UE의 보안 능력 (Security Capabilities) 내용이 변경된 NAS Security Mode Command 메시지를 피해자 UE가 Accept하는 것을 3GPP Rel-17 표준 규격 [13]이 허용하지 않기 때문이다.

둘째, 시그널링 메시지 8의 선택된 5G 보안 알고리즘에 대하여 분석하면 다음과 같다. Fig. 1의 시그널링 메시지 7에는 NIA0과 NEA0이 포함된 것으로 표시되어 있으나, Fig. 1의 시그널링 메시지 8에는 NIA0과 NEA0이 포함되어 있지 않다. 이에 대하여, 악의적인 gNB가 시그널링 메시지 8을 생성할 때 NIA0과 NEA0이 아닌 다른 보안 알고리즘을 선택하였다고 추정할 수도 있다. 하지만, Fig. 1에

서 시그널링 메시지 9인 NAS Security Mode Complete 메시지의 송수신이 끝나고 나면, 피해자 UE로부터 AMF까지 “Non-Ciphered NAS Communication”이라고 표시되어 있으므로, 시그널링 메시지 8의 선택된 5G 보안 알고리즘은 NIA0과 NEA0이어야 한다. 또한, 이하의 분석에서 다시 언급하겠지만, Fig. 1의 시그널링 메시지 11이 악의적인 gNB로부터 피해자 UE로 무결성 보호 (Integrity Protection) 없이 전송되기 위해서는 시그널링 메시지 8의 선택된 5G 보안 알고리즘은 NIA0과 NEA0이어야 한다. 이에 대하여, 3GPP TS 24.501 [13]의 5.4.2.3에 따르면, UE는 응급이거나 W-AGF (Wireline Access Gateway Function)와 관련된 경우에만 NIA0과 NEA0이 포함된 NAS Security Mode Command 메시지를 Accept한다. 따라서, 일반적인 초기 등록 절차를 수행 중인 피해자 UE는 NIA0과 NEA0이 포함된 NAS Security Mode Command 메시지를 Accept하지 않을 것이다.

정리하면, 3GPP 규격을 정확하게 반영하지 못하고 Fig. 1의 시그널링 메시지 7을 전송하는 시스템이 존재한다고 하더라도, 3GPP Rel-17 표준 규격에 따라 구현된 UE는 Fig. 1의 시그널링 메시지 8을 Accept하지 않는다. 따라서, Fig.1의 시그널링 메시지 7에서 9까지에 해당하는 NAS Security Mode Control 절차는 3GPP Rel-17 표준 규격에 따라 구현된 시스템과 UE에서 진행될 수 없다.

4. Analysis of Registration Accept / Reject

3GPP Rel-17 표준 규격에 따라 구현되지 않은 AMF와 UE가 존재하고, 그 결과, Fig. 1의 시그널링 메시지 8까지 절차가 성공적으로 진행되었다면, Fig. 1의 시그널링 메시지 9인 NAS Security Mode Complete 메시지가 피해자 UE로부터 AMF에게까지 전달될 수 있다. 만일 그렇다면 악의적인 gNB는 NAS 메시지를 원하는대로 수정할 수 있다. 즉, Fig. 1에 표시된 바와 같이, 피해자 UE와 AMF 사이의 통신은 “Non-Ciphered NAS Communication” 상태가 된다.

Fig. 1의 시그널링 메시지 10인 Attach Accept 메시지는 3GPP Rel-17 표준 규격의 Registration Accept 메시지에 해당한다. Fig. 1의 시그널링 메시지 10을 3GPP Rel-17 표준 규격에 맞게 상세히 표현하면 Fig. 3과 같다. AMF로부터 Registration Accept 메시지를 수신한 gNB는 악의적인 UE와 5G-NR RRC Security 절차를 수행한다. 앞서 Fig. 1의 시그널링 메시지 7을 전송한 AMF가 Null 보안 알고리즘인 NIA0과 NEA0을 보안 알고리즘으로 선택한 것이 가능하다고 가정한 상태로 분석을 진행하고 있으므로, Fig. 3에서 AS 보안 컨텍스트를 설정할 때에도 NIA0과 NEA0이 보안 알고리즘으로 사용될 것이다.

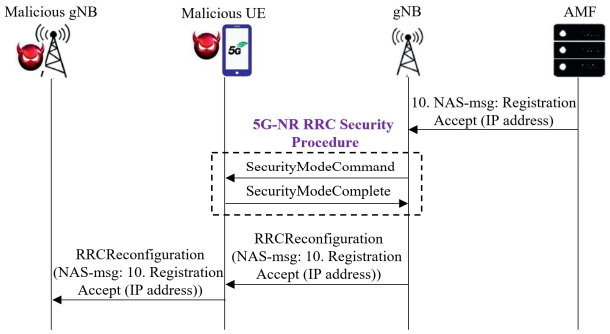

Fig. 3. Registration Accept

Fig. 1의 시그널링 메시지 10인 Attach Reject 메시지는 3GPP Rel-17 표준 규격의 Registration Reject 메시지에 해당한다. 이것 또한, 우리가 Fig. 1의 시그널링 메시지 8을 UE가 Accept한다고 가정한 상태로 분석을 진행하고 있으므로, 악의적인 gNB는 피해자 UE에게 Registration Reject 메시지를 전송할 수 있다. 3GPP TS 24.501 [13]의 4.4.4.2는 UE에서의 NAS 시그널링 메시지의 무결성 검사에 대하여 기술하고 있는데, 그 내용에 따르면, Registration Reject 메시지에 대하여 Secure Exchange가 설정되기 전에만 무결성 보호 없이 전송될 수 있도록 되어 있다. 하지만, 앞서 서술한 바와 같이, 피해자 UE와 AMF 사이의 통신이 “Non-Ciphered NAS Communication”이라고 가정한 상태로 분석하고 있으므로, 이러한 상태에서 악의적인 gNB는, Fig.1과 같이, 피해자 UE에게 Registration Reject 메시지를 전송할 수 있다.

3GPP TS 24.501 [13]의 5.5.1.2.5는 네트워크에 의하여 Accept되지 못한 초기 등록에 대하여 기술하고 있다. 그 내용에 따르면, Registration Reject 사유가 #3, #6, #7일 때, USIM을 제거할 때까지 UE는 5G 서비스를 사용할 수 없다. 이러한 내용을 근거로 Null 보안 알고리즘에 대한 5G 보안 분석 [9]에서는 IP 스푸핑 공격을 당한 피해자 UE는 USIM 카드를 재시동하거나 재설치할 때까지 코어 네트워크와 연결을 맺을 수 없다라고 주장한 것으로 판단된다. 다만, Registration Reject 사유 #3은 인증에 실패한 경우에 해당하므로, Fig. 1의 시그널링 메시지 11에서는 사용될 수 없다.

5. Summary of Analysis

Null 보안 알고리즘에 대한 5G 보안 분석 [9]의 IP 스푸핑 공격을 분석한 결과를 요약해서 정리하면 다음과 같다.

3GPP Rel-17 표준 규격에 따라 구현된 AMF와 UE는 Fig. 1의 시그널링 메시지 7과 8을 허용하지 않기 때문에, IP 스푸핑 공격 [9]은 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 실현 불가능한 공격이 된다. 다만, LTEFuzz [7]의 예와 같이, 3GPP Rel-17 표준 규격을 정확하게 구현하지 못한 경우에는 IP 스푸핑 공격을 허용할 수도 있으므로, 상용 시스템을 구현할 때 표준 규격을 반드시 준수할 필요가 있다.

IV. Conclusions

본 논문에서는 5G 네트워크에서 Null 보안 알고리즘을 악용한 IP 스푸핑 공격의 실현 가능성을 3GPP Rel-17 표준 문서에 근거하여 분석하였다. 먼저 Registration Request 메시지를 전송하는 절차를 분석한 뒤, 인증 절차에 대하여 분석하였다. 그 다음, NAS Security Mode Control 절차를 분석하고, 마지막으로 Registration Accept / Reject 메시지를 전송하는 절차에 대하여 분석하였다. 분석 결과, 인증 절차까지는 3GPP Rel-17 표준 규격에 따라 구현된 시스템에서 문제없이 진행될 수 있음을 확인하였다. 그러나 3GPP Rel-17 표준 규격에 따라 구현된 AMF와 UE는 IP 스푸핑 공격 절차에서의 시그널링 메시지 7과 8을 허용하지 않기 때문에, IP 스푸핑 공격은 3GPP Rel-17 표준 규격에 따라 구현된 5G 시스템에서 실현 불가능한 공격으로 판단된다. 본 연구의 분석 결과는 3GPP Rel-17 표준 규격에 따라 5G 시스템을 구현하는데 있어 유용하게 활용될 수 있을 것으로 기대한다.

ACKNOWLEDGEMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability).

REFERENCES

[1] A. Gupta and R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,” IEEE Access, Vol. 3, pp.1206-1232, July 2015. DOI: 10.1109/ACCESS.2015.2461602

[2] J. Navarro-Ortiz, P. Romero-Dias, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, “A Survey on 5G Usage Scenarios and Traffic Models,” IEEE Communications Surveys & Tutorials, Vol. 22, Issue 2, pp.905-929, 2nd Quart., June 2020. DOI: 10.1109/COMST.2020.2971781

[3] O. O. Erunkulu, A. M. Zungeru, C. K. Lebekwe, M. Mosalaosi, and J. M. Chuma, “5G Mobile Communication Applications: A Survey and Comparison of Use Cases,” IEEE Access, Vol. 9, pp.97251-97295, July 2021. DOI: 10.1109/ACCESS.2021.3093213

[4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage: ‘‘A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions,’’ IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, pp. 196-278, 1st Quart., March 2020. DOI: 10.1109/COMST.2019.2933899

[5] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, “5G Security Challenges and Solutions: A Review by OSI Layers,” IEEE Access, Vol. 9, pp.116294-116314, Aug. 2021. DOI: 10.1109/ACCESS.2021.3105396

[6] S.R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, E. Bertino: “5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol,” in Proc. 2019 ACM SIGSAC Conference on Computer and Communications Security, pp.669-684, Nov. 2019. doi: 10.1145/3319535.3354263.

[7] H. Kim, J. Lee, E. Lee, Y. Kim: “Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane,” in Proc. IEEE Symposium on Security and Privacy (SP), pp. 1153-1168, May 2019. DOI: 10.1109/SP.2019.00038.

[8] S.R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,” in Proc. 25th Annual Network and Distributed System Security Symposium, NDSS, pp. 18-21, Feb. 2018. DOI: 10.14722/NDSS.2018.23313.

[9] R. Zhang, W. Zhou, and H. Hu, “Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication,” Hindawi Security and Communication Networks, Vol. 2021, Article ID 4498324, Oct. 2021. DOI: 10.1155/2021/4498324

[10] K. Kim, K. Park, and T.K. Park, “Analysis of Deregistration Attacks in 5G Standalone Non-Public Network,” Journal of the Korea Society of Computer and Information, Vol. 26, No. 9, pp. 81-88, Sep. 2021. DOI: 10.9708/jksci.2021.26.09.081.

[11] K. Kim, K. Park, and T.K. Park, “Analysis of DoS Attack against Users with Spoofed RRC Connections in 5G SNPN,” Journal of KIIT, Vol. 19, No. 10, pp. 79-85, Oct. 31, 2021. DOI: 10.14801/

jkiit.2021.19.10.79.

[12] K. Kim, J.G. Park, and T.K. Park, “Analysis of Incarceration Attacks with RRCReject and RRCRelease in 5G Standalone Non-Public Network,” Journal of the Korea Society of Computer and Information, Vol. 26 No. 10, pp. 93-100, October 2021. DOI: 10.9708/jksci.2021.26.10.093.

[13] 3GPP. TS 24.501 v17.6.1: “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3; (Rel-17),” March. 2022.

[14] 3GPP. TS 38.331 v17.0.0: “NR; Radio Resource Control (RRC) Protocol Sepcification (Rel-17),” March. 2022.

[15] 3GPP. TS 23.502 v17.4.0: “Procedures for the 5G System (5GS); Stage 2; (Rel-17),” March. 2022.

[16] 3GPP. TS 33.501 v17.5.0: “Security architecture and procedures for 5G system (Rel-17),” March. 2022.

Authors

Tae-Keun Park received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea in 1991, 1993, and 2004, respectively. He joined POSTECH PIRL in 1993 and moved to SK Telecom in 1996. From 2000 to 2001 and from 2001 to 2002, he worked for 3Com Korea and Ericsson Korea, respectively. In 2004, he joined in the department of Multimedia Engineering, Dankook University, Korea. He is currently on the faculty of the department of Computer Engineering at Dankook University. His research interests include network security, IoT, wireless/mobile communications, and distributed services.

Jong-Geun Park received his BS and MS degree in industrial engineering from SungKyunKwan University, Rep. of Korea, in 1997 and 1999, respectively, and received his PhD degree in computer engineering from Chungnam National University, Rep. of Korea, in 2013. From 1999 to 2001, he was a researcher at ADD, Daejeon, Rep. of Korea. Then, he joined ETRI, Daejeon, Rep. of Korea, in 2001, where he is currently working as a principal researcher. Currently, he is interested in mobile network security, SDN/NFV, and Cloud security.

Keewon Kim received his M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Korea, in 2001 and 2006, respectively. He is currently an assistant professor in the department of Computer Engineering, Mokpo National Maritime University. He is interested in information security, security protocol, VLSI, and big data analysis.