JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 9, pp. 81-88, September 2021
https://doi.org/10.9708/jksci.2021.26.09.081

Analysis of Deregistration Attacks in 5G Standalone Non-Public Network

Keewon Kim*, Kyungmin Park**, Tae-Keun Park***

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

[Abstract]

In this paper, we analyze the possibility of deregistration attack in 5G SNPN (Standalone Non-Public Network) based on 3GPP standard document. In the deregistraion attack, the attacker pretends to be a UE that is normally registered with AMF (Access and Mobility Management Function) and attempts to establish a spoofed RRC (Radio Resource Control) connection, causing AMF to deregister the existing UE. The existing deregistration attack attempts a spoofed RRC connection to the AMF in which the UE is registered. In addition, this paper analyzes whether deregistration attack is possible even when an attacker attempts to establish a spoofed RRC connection to a new AMF that is different from the registered AMF. When the 5G mobile communication network system is implemented by faithfully complying with the 3GPP standard, it is determined that a deregistration attack of a UE is impossible.

▸ **Key words**: 5G, Standalone Non-Public Network, 3GPP Standard, Deregistration Attack, Attack Analysis

[요 약]

본 논문에서는 5G SNPN (Standalone Non-Public Network)에서 등록 해제 공격(Deregistration Attack)의 가능 여부를 3GPP 표준 문서에 근거하여 분석한다. 등록 해제 공격에서 공격자는 AMF (Access and Mobility Management Function)에 정상적으로 등록되어 있는 UE로 가장하여 스푸핑된 RRC (Radio Resource Control) 연결을 설정을 시도하여 AMF가 기존의 UE의 등록을 해제하게 한다. 기존의 등록 해제 공격은 UE가 등록되어 있는 AMF에게 스푸핑된 RRC 연결을 시도하는데, 본 논문에서는 추가적으로, 사용자가 등록 되어 있는 AMF와는 다른 새로운 AMF에게 공격자가 스푸핑된 RRC 연결 설정을 시도하였을 때에도, 등록 해제 공격이 가능한지 분석한다. 분석 결과, 5G 이동통신 네트워크 시스템이 3GPP 표준을 충실히 준수하여 구현된 경우에는 UE의 등록 해제 공격은 불가능한 것으로 판단된다.

▸ **주제어**: 5G, Standalone Non-Public Network, 3GPP 표준, 등록 해제 공격, 공격 분석

• First Author: Keewon Kim, Corresponding Author: Tae-Keun Park
*Keewon Kim (kwkim@mmu.ac.kr), Dept. of Computer Engineering, Mokpo National Maritime University
**Kyungmin Park (kmpark@etri.re.kr), Information Security Research Division, ETRI
***Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
• Received: 2021. 08. 24, Revised: 2021. 09. 15, Accepted: 2021. 09. 16.

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

I. Introduction

다양한 네트워크 서비스의 향상된 성능, 휴대성, 탄력성 및 에너지 효율성에 대한 새로운 요구를 충족하기 위해서 이동통신 네트워크는 진화되고 있다. 5G 이동 네트워크는 기존의 기능을 더욱 개선하기 위해 새로운 네트워크 개념을 채택하여, 4차 산업혁명의 핵심 인프라 기술로서 자리매김하고 있다. 특히, 5G 이동통신 네트워크는 인공지능, IoT, 빅데이터와 같은 기술들과 융합하여 다양한 산업에서 통신 서비스를 제공할 것이다 [1-4].

다양한 융합 산업에서의 안전한 통신 서비스를 위해서 보안이 매우 중요하며, 4G 와 5G 이동통신 네트워크 보안을 위해 다양한 노력들이 있어 왔다. Kim 등 [5]은 작동중인 4G 이동 통신 네트워크에서 RRC (Radio Resource Control)와 NAS (Non-Access Stratum) 계층의 보안을 동적으로 테스트하기 위해 LTEFuzz라는 반자동 테스트 도구를 구현하였다. Hussain 등 [6]은 세 개의 4G LTE 제어 평면 프로토콜 (Control-Plane Protocols)을 테스트하기 위해 LTEInspector라는 프레임워크를 제안하였다. Basin 등 [7]은 5G 인증에 대해 정형적인 분석을 하였고, Cremers와 Dehnel-Wild [8]는 5G-AKA에 대해 정형적인 분석을 하였다. Hussain 등 [9]은 5G NAS 계층과 RRC 계층의 5G 프로토콜에 대해 정형적인 모델을 구성하였고, 정형적인 보안 검증을 위해 5GReasoner 프레임워크를 제안하고 그것을 이용하여 5G 이동통신 네트워크의 보안 설계 취약점을 발견하여 제시하였다.

5G NPN (Non-Public Network)은 캠퍼스나 공장과 같은 특정 지역의 범위 내에서 특정 사용자나 그룹에게 서비스를 제공하기 위해 도입되는 맞춤형 5G 이동통신 네트워크이다 [10,11]. 5G-ACIA (Alliance for Connected Industries and Automation)는 산업 도메인에 5G 이동통신 네트워크의 적용을 위해 네 가지 5G NPN 구축 모델을 제시하였다 [10]. 본 논문에서는 5G-ACIA가 제시한 네 가지 구축 모델 중 하나인 5G Standalone NPN의 환경에 초점을 맞추고 있다.

본 논문에서는 4G 이동통신 네트워크에서 Kim 등 [5]과 5G 이동통신 네트워크에서 Hussain 등 [9]이 제시한 UE (User Equipment)의 등록 해제 공격 (Deregistration Attack)이 실현 가능한지 분석한다. 또한 기존의 공격은 UE가 등록되어 있는 AMF (Access and Mobility Management Function)만 고려하였는데, 본 논문에서는 이에 추가로, 다른 AMF에게 등록 해제 공격이 가능 여부를 분석한다.

II. Related Works

본 장에서는 4G와 5G 이동통신 네트워크에서의 등록 해제 공격과 관련한 기존 연구들에 대해 간략히 소개한다.

1. Kim et al.'s "Remote de-registration attack"

Kim 등 [5]은 4G LTE에서 UE의 등록 해제 공격 "Remote de-registration attack"을 제안하였다. 이 공격은 LTE에서 MME (Mobility Management Entity)의 취약성을 악용한 공격으로, 공격자가 스푸핑된 RRC 연결 (Spoofed RRC Connection)을 악용하여 NAS 메시지를 보낼 때 발생하며, 운영중인 MME에서 알림 없이 불필요하게 피해자 UE의 등록을 취소한다.

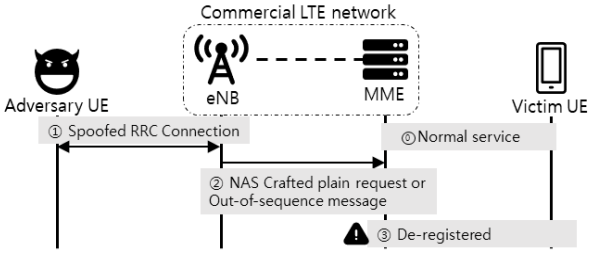

Fig. 1. Remote de-registration attack [5]

공격자는 피해자 UE가 등록된 MME에게 악성 NAS 메시지를 보낼 수 있고, 피해자의 S-TMSI (S-Temporary Mobile Subscriber Identity)를 알고 있다고 가정한다. "Remote de-registration attack"의 공격 절차는 Fig. 1과 같다. 공격 절차의 각 단계를 살펴보면, ① 공격자는 먼저 피해자의 S-TMSI를 사용하여 스푸핑된 RRC 연결을 설정한다. ② 공격자는 가공된 초기 일반 요청, 유효하지 않은 보안 메시지, 또는 재생된 메시지를 피해자 UE를 서비스하는 MME에게 전송한다. 이 경우 공격자가 스푸핑된 RRC 연결을 통해 메시지를 전송하면 서빙 eNB (Evolved Node B)는 S-TMSI를 확인하여 피해자를 서빙하는 MME에게 메시지를 전달한다. ③ 해당 MME는 공격자로부터 받은 메시지를 이용해 새로운 연결을 설정하다. 그러면 MME는 기존의 피해자 UE에게 어떠한 통지도 없이 피해자 UE의 등록을 해제한다.

Kim 등 [5]은 작동중인 LTE 네트워크에서 각기 다른 MME_1, MME_2, MME_3에 대해 그들이 제안한 등록 해제 공격을 시연했다. 시연한 내용 중에, ATTACH REQUEST를 악용한 공격은 MME_1과 MME_3에서 가능하였으며, MME_2에서는 불가능하였다. 반면 DETACH REQUEST를 악용한 공격은 MME_1, MME_2, MME_3 모두에서 가능하였다. Kim

등은 이 공격의 원인은 운영 중인 MME의 잘못된 구현이라고 하였고, 3GPP 표준을 엄격하게 따르고 주의하여 구현해야 한다고 주장했다.

2. Hussain et al.'s "Cutting off the Device"

4G LTE의 Fig. 1의 "Remote de-registration attack"과 유사하게, Hussain 등 [9]은 5G 이동통신 네트워크에서 UE의 등록 해제 공격인 "Cutting off the Device"를 제안하였다. 이 공격에서 공격자는 피해자 장치의 C-RNTI (Cell Radio Network Temporary Identifier) 또는 TMSI (Temporary Mobile Subscriber Identity)를 알고 있고 피해자 UE로 가장할 수 있다고 가정한다. 공격자의 목표는 네트워크에서 피해자 장치의 연결을 은밀하게 해제하는 것이다. Hussain 등 [9]이 제시한 공격과정에서 공격자는 피해자 장치로 가장하여 AMF에게 REGISTRATION REQUEST 또는 DEREGISTRATION REQUEST 메시지를 전송한다. 그러면, AMF가 네트워크에서 피해자 장치의 등록을 해제하고 피해자로 위장한 공격자와 연결하여, 피해자 장치와의 기존 연결을 묵시적으로 해제한다고 Hussain 등 [9]은 주장하였다.

III. Analysis of Existing the Deregistration Attack in 5G

앞장에서 살펴본 5G 이동통신 네트워크에서의 "Cutting off the Device" 공격 [9]에 대해 3GPP 표준을 기반으로 공격의 실현 가능 여부를 분석하고자 한다. 즉, 공격자가 피해자 UE로 가장하여 피해자 UE가 연결되어 있는 AMF에게 무결성이 유효하지 않은 NAS 메시지를 전송하였을 때 AMF의 메시지 처리 절차를 확인하며 실제로 피해자 UE와의 연결을 등록 해제하는지 확인하고자 한다.

5G 이동통신 네트워크의 AMF에서 NAS 시그널링 메시지의 무결성 검사에 관한 3GPP TS 24.501 [12]의 "4.4.4.3 Integrity checking of NAS signalling messages in the AMF"의 자세한 분석을 위해서, NAS 메시지의 안전한 교환 설정에 관련된 상황을 나누어서 분석하고자 한다. NAS 메시지의 안전한 교환이 설정되지 않은 경우, NAS Security Context가 설정되었지만 네트워크에서 사용이 불가능한 상태인 경우, NAS 메시지가 무결성 검사에 실패한 경우로 나누어서 분석한다.

1. A case that the secure exchange of NAS messages is not established

3GPP TS 24.501 [12]의 4.4.4.3절에 따르면, NAS 시그널링 연결을 위한 NAS 메시지의 안전한 교환 (Secure Exchange)이 설정되어 있지 않은 경우에, Table 1의 메시지들을 제외한 다른 NAS 메시지는 AMF에서 수신한 5GMM 엔티티가 처리하거나 5GSM 엔티티로 전달되면 안 된다고 되어 있다. 즉, NAS 메시지의 안전한 교환이 설정되어 있지 않은 경우에도 Table 1의 메시지들은 처리되어야 한다.

Table 1. 5G NAS signaling messages that need to be processed without a secure exchange of NAS messages

1	REGISTRATION REQUEST	5	SECURITY MODE REJECT
2	IDENTITY RESPONSE	6	DEREGISTRATION REQUEST
3	AUTHENTICATION RESPONSE	7	DEREGISTRATION ACCEPT
4	AUTHENTICATION FAILURE	-	

Hussain 등 [9]의 "Cutting off the Device" 공격에서 피해자 UE는 등록 절차가 완료된 경우에 해당하므로 NAS 메시지의 안전한 교환이 설정된 것으로 판단되어, 이 경우에 해당되지 않는다.

2. A case that NAS security context exists, but it is not available on the network

3GPP TS 24.501 [12]의 4.4.4.3절에 따르면, 현재 5G NAS security context가 존재하는 경우에, 이를 네트워크에서 사용 가능한 상태가 아니어서, 수신한 NAS 메시지의 MAC이 무결성 검사 (Integrity Check)에 실패하거나 검증될 수 없더라도, NAS 시그널링 연결을 위하여 NAS 메시지의 안전한 교환이 설정될 때까지, AMF의 수신 5GMM 엔티티는 Table 2의 NAS 메시지들을 처리해야 한다.

Table 2. 5G NAS signaling messages that need to be processed when NAS security context exists, but it is not available on the network

1	REGISTRATION REQUEST	6	DEREGISTRATION REQUEST
2	IDENTITY RESPONSE	7	DEREGISTRATION ACCEPT
3	AUTHENTICATION RESPONSE	8	SERVICE REQUEST
4	AUTHENTICATION FAILURE	9	CONTROL PLANE SERVICE REQUEST
5	SECURITY MODE REJECT	-	

이는 특정한 상황에서 네트워크에서 5G NAS security context를 더 이상 사용할 수 없을 때, UE는 메시지 보호를 위해 이를 사용해 전송할 수 있다. 이러한 메시지의

MAC이 무결성 검사에 실패하거나 확인할 수 없는 경우에도 AMF에 의해 처리된다.

이러한 경우는 현재 UE가 NAS security context를 설정한 최근 serving AMF를 벗어나 새로운 AMF로 이동한 경우로 볼 수 있다. Hussain 등 [9]의 “Cutting off the Device” 공격은 무결성이 유효하지 않은 NAS 메시지를 피해자 UE의 serving AMF에 전송하는 것이므로 이 상황에 해당되지 않는다.

3. A case that NAS messages fail integrity check

3GPP TS 24.501 [12]의 4.4.4.3절에 따르면, 만약 초기 등록 (Initial Registration)을 위한 REGISTRATION REQUEST 메시지가 무결성 검사에 실패하고 emergency service에 대한 등록 요청이 아닌 경우이면, AMF는 REGISTRATION REQUEST의 처리를 계속하기 전에 가입자를 먼저 인증해야 한다. 이상의 규격이 정확하게 구현되었다면, Hussain 등 [9]의 “Cutting off the Device” 공격에서 공격자는 피해자로 가장해서 REGISTRATION REQUEST를 보낼 수는 있지만, 인증 과정을 통과할 수는 없다.

3GPP TS 24.501 [12]의 4.4.4.3절에 따르면, 만약 DEREGISTRATION REQUEST 메시지가 무결성 검사에 실패하면, AMF는 다음과 같이 처리해야 한다.

- 만약 switch off로 인한 등록 해제 요청(Deregistration Request)이 아니고 AMF가 인증 절차를 시작할 수 있는 경우이면, AMF는 더 이상 등록 해제 요청을 처리하기 전에 가입자를 인증해야 한다.
- 만약 switch off로 인한 등록 해제 요청이거나 AMF가 다른 이유로 인증 절차를 시작하지 않은 경우이면, AMF는 등록 해제 요청을 무시하고 5GMM-REGISTERED 상태를 유지할 수 있다.

이상의 규격이 정확하게 구현되었다면, 공격자가 피해자를 가장하여 DEREGISTRATION REQUEST를 전송하더라도, 가입자의 인증이 필요하거나 AMF는 등록 해제 요청을 무시하고 5GMM-REGISTERED 상태를 유지하게 된다. 따라서 Hussain 등 [9]의 DEREGISTRATION REQUEST를 이용한 “Cutting off the Device” 공격은 성공할 수 없다.

또한, 3GPP TS 24.501 [12]의 4.4.4.3절의 마지막 부분에 보면, NAS 메시지의 안전한 교환이 설정되었지만 무결성이 보호되지 않는 NAS 신호 메시지가 수신되면 NAS는 이 메시지를 폐기해야 한다고 강조하고 있다. 만약 3GPP 표준을 엄격하게 준수하여 올바르게 AMF가 구현된다면 Hussain 등 [9]의 REGISTRATION REQUEST 또는 DEREGISTRATION REQUEST를 이용한 “Cutting off the Device” 공격은 가능하지 않다.

IV. Additional Vulnerability Analysis on Deregistration Attacks in 5G SNPN

이전의 분석에 따르면, 5G 이동통신 네트워크를 3GPP 표준에 따라 정확하게 구현하면, Hussain 등 [9]의 “Cutting off the Device” 공격은 성공하지 못할 것으로 판단된다. 본 장에서는 5GMM-REGISTERED 상태의 UE를 강제로 등록 해제시킬 수 있는 가능성에 대하여 추가적인 분석을 수행한다. Hussain 등 [9]의 공격에서는 피해자 UE가 등록되어 있는 AMF와 동일한 AMF에게 REGISTRATION REQUEST 또는 DEREGISTRATION REQUEST를 공격자가 전송한다. 하지만 피해자 UE가 등록되어 있는 AMF가 아닌 다른 AMF에게 이러한 메시지를 전송하였을 때 발생 가능한 취약점의 확인도 필요하다.

3GPP TS 24.501 [12]의 4.4.4.3절에서, 피해자 UE가 등록되어 있는 AMF가 아닌 다른 AMF에게 REGISTRATION REQUEST 또는 DEREGISTRATION REQUEST 메시지를 전송할 때, 다음과 같이 NAS 보안 컨텍스트를 사용할 수 없거나 메시지 무결성 검사가 실패하는 경우가 있다.

1) 5GMM-IDLE 모드에서 시스템간 변경 (Inter-System Change)으로 인해 등록 절차가 시작되고 UE에서 현재 5G NAS 보안 컨텍스트를 사용할 수 없는 경우. 즉, 보안이 활성화되기 전에 UE가 메시지를 전송하는 경우.
2) 특정한 상황에서 네트워크에서 더 이상 사용할 수 없는 5G NAS 보안 컨텍스트로 보호되는 UE에 의해 전송되는 경우.
3) Mobility와 Periodic registration update를 위한 REGISTRATION REQUEST 메시지가 무결성 검사에 실패하고 UE가 source MME에서 성공적으로 검증된 EPS NAS 메시지 컨테이너 IE를 제공하는 경우. 그렇지 않고 UE가 non-emergency PDU 세션만 설정된 경우.

위와 같이 피해자 UE가 등록되어 있는 AMF와 다른 AMF에게 공격자가 무결성이 잘못된 REGISTRATION REQUEST, DEREGISTRATION REQUEST, SERVICE REQUEST를 전송할 가능성이 있음을 확인하였다. 이를 이용하여 등록 해제 공격이 가능한지 분석하고자 한다.

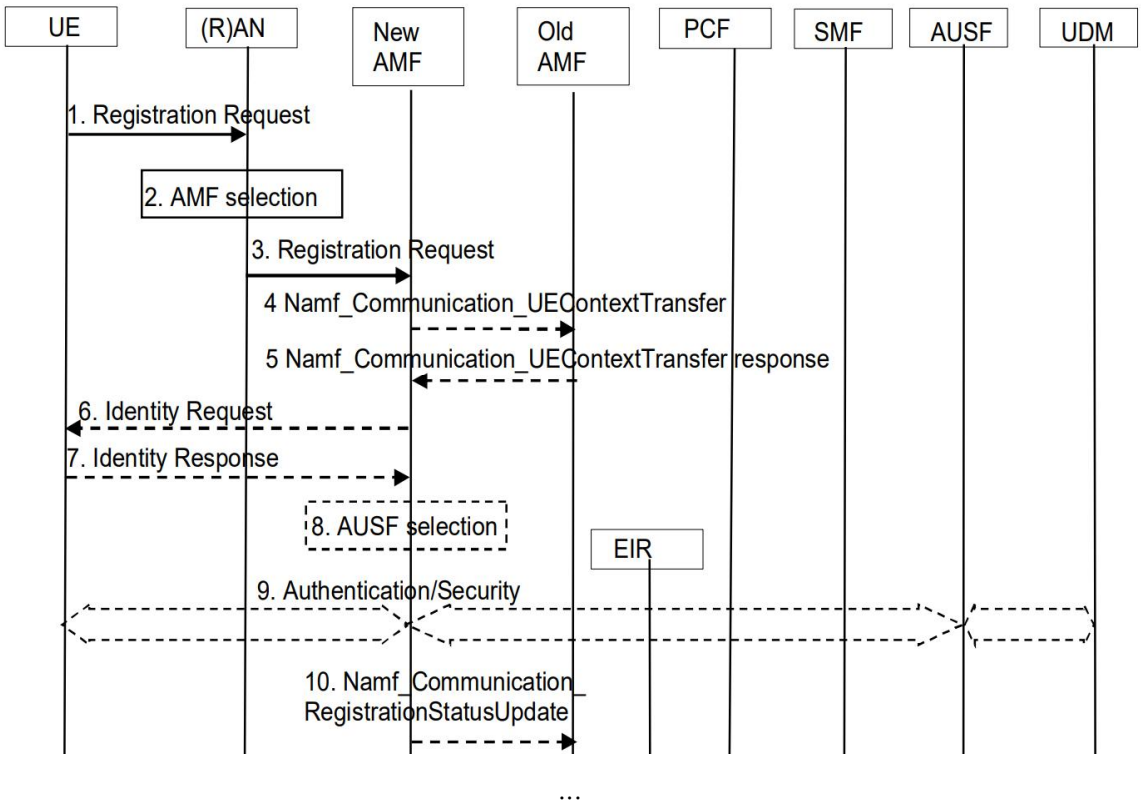

Fig. 2. Registration procedure [13]

1. Sending REGISTRATION REQUEST with invalid integrity to new AMF

공격자가 피해자 UE가 등록되어 있는 AMF와 다른 AMF에게 스푸핑된 RRC 연결 설정을 시도할 수 있다. 공격자가 피해자 UE로 위장하여 REGISTRATION REQUEST를 전송하고, AMF에서 무결성 검사에 실패할 경우에 AMF의 처리 과정의 확인이 필요하다. 이를 위해 3GPP TS 23.502 [13]의 "4.2.2 Registration Management procedures"에서 "4.2.2.2.2 General Registration"를 보면 UE의 등록 관리 절차가 서술되어 있다. 등록 절차의 일부는 Fig. 2와 같으며, 등록 절차의 시작부터 순차적으로 분석한다.

① 등록 절차의 "Step 1. Registration Request"에서 피해자 UE로 가장한 공격자가 피해자 UE가 등록된 AMF가 아닌 다른 새로운 AMF에서 무결성이 잘못된 REGISTRATION REQUEST를 전송하기 위해서 기지국에게 전송할 수 있다.

② "Step 2. AMF selection"과 "Step 3. Registration Request"가 수행된다.

③ 피해자 UE는 old AMF에 연결되어 있고 공격자는 피해자 UE로 가장하여 new AMF에서 REGISTRATION REQUEST를 전송한 경우이므로, "Step 4. Namf_Communication_UEContextTransfer"가 수행된다. 여기서, 공격자가 전송한 REGISTRATION REQUEST는 old AMF에서 무결성 검사가 실패하므로, "Step 9a"에 따라 new AMF는 성공적인 UE 인증을 수행한 경우에, UE 가 검증되었음을 표시(Indicate)하도록 되어 있다.

④ "Step 5. Response to Namf_Communication_UEContextTransfer"가 수행된다. 여기서, old AMF에서 공격자가 보낸 REGISTRATION REQUEST는 무결성 검사를 실패하므로, old AMF는 "무결성 검사 실패"를 표시(Indicate)한다.

⑤ "Step 8. AUSF selcetion" 수행 후에, "Step 9. Authentication/Security"가 수행된다. 앞의 "Step 4"와 "Step 5"에서 무결성 검사를 실패하였으므로, AMF는 공격자의 인증을 수행하게 된다. 피해자 UE로 위장한 공격자는 "Step 9a"의 단계에서 new AMF의 인증 요구에 응답하지 않거나 잘못된 응답을 할 수 있다.

⑥ "Step 10. Namf_Communication_RegistrationStatusUpdate"이 수행된다. 그러나, 피해자 UE로 가장한 공격자는 인증 과정을 통과할 수 없으므로, 결국 인증에 실패할 것이다.

이상의 과정을 보면 공격자가 피해자 UE가 등록되어 있는 AMF와 다른 AMF에게 스푸핑된 RRC 연결 설정을 시도하더라도, 피해자 UE가 old AMF에 정상적으로 등록되어 있는 상태로 유지될 것으로 판단된다.

2. Sending DEREGISTRATION REQUEST with invalid integrity to new AMF

공격자가 피해자 UE가 등록되어 있는 AMF와 다른 AMF에게 무결성이 잘못된 DEREGISTRATION REQUEST를 전송하고, AMF에서 무결성 검사에 실패한 경우에 네트워크의 처리 과정을 확인하고자 한다. 이를 위해 3GPP TS 23.502 [13]의 “4.2.2.3 Deregistration procedures”에서 “4.2.2.3.2 UE-initiated Deregistration”를 분석한다.

공격자가 피해자 UE로 가장하여 피해자 UE가 등록된 AMF가 아닌 다른 새로운 AMF에서 무결성이 잘못된 DEREGISTRATION REQUEST를 전송할 경우, 3GPP TS 23.502 [13]의 “4.2.2.3.2 UE-initiated Deregistration”의 절차가 시작된다. oldAMF와 newAMF를 구분하여 표시하지 않고 하나의 AMF 표시되어 있으므로, DEREGISTRATION REQUEST는 UE가 등록되어 있는 AMF에게 전송해야 처리가 되는 것으로 판단된다.

3GPP TS 24.501 [12]에 따르면, 만약 공격자가 보낸 DEREGISTRATION REQUEST 메시지가 AMF에서 무결성 검사에 실패하면, 추가적인 가입자의 인증이 필요하거나 AMF는 해당 DEREGISTRATION REQUEST를 무시하고 5GMM-REGISTERED 상태를 유지하게 된다. 따라서 공격자의 이러한 시도는 피해자 UE에게 아무 영향을 미치지 못할 것으로 판단된다.

3. Sending SERVICE REQUEST with invalid integrity to new AMF

공격자가 피해자 UE가 등록되어 있는 AMF와 다른 AMF에게 무결성이 잘못된 SERVICE REQUEST를 전송하고, AMF에서 무결성 검사에 실패할 경우에 네트워크의 처리 과정을 확인하고자 한다. 이를 위해서 3GPP TS 23.502 [13]의 “4.2.3 Service Request procedures”에서 “4.2.3.2 UE Triggered Service Request”를 분석한다.

“UE Triggered Service Request” 절차의 “Step 3. Authentication Security”에서 만약 SERVICE REQUEST가 무결성 보호로 전송되지 않았거나 무결성 보호 검증이 실패한 경우에, AMF는 3GPP TS 24.501 [12]에 명시된 대로 서비스 요청을 거부해야 한다. 3GPP TS 24.501 [12]의 “4.4.4.3 Integrity checking of NAS signalling messages in the AMF”에서 해당 부분을 찾아보면, SERVICE REQUEST 메시지가 무결성 검사에 실패하고 UE가 non-emergency PDU 세션만 설정된 경우, AMF는 5GMM cause # 9 “UE identity cannot be derived by the network”가 포함된 SERVICE REJECT 메시지를 전송하고 5GMM context와 5G NAS security context를 변경하지 않은 상태로 유지해야 한다. SERVICE REQUEST 메시지에 대한 응답으로 cause 번호는 # 9인 SERVICE REJECT를 보냈을 때 네트워크에서의 상태변화를 확인하기 위해서, 3GPP TS 24.501 [12]에 기술된 네트워크의 5GMM 주요 상태를 보면 5GMM-REGISTERED 상태에서 cause 번호 #9를 가진 SERVICE REJECT는 5GMM-DEREGISTERED 상태로 천이하지 못한다.

“UE Triggered Service Request” 절차에 따르면, UE는 등록되어 있는 AMF에게 SERVICE REQUEST를 보내야하는 것으로 판단되며, UE와 AMF 사이에 “Authentication Security” 절차가 있으므로, 공격자가 피해자 UE로 가정하여 공격한 경우에는 인증을 실패할 것이다. 그 다음 SERVICE REJECT를 UE에게 보내지만 네트워크 쪽에서 5GMM-DEREGISTERED 상태로 천이하지는 않는다. 따라서 공격자가 피해자 UE로 가장하여 무결성이 잘못된 SERVICE REQUEST를 전송하여도 피해자 UE에 악영향을 미치지 않을 것으로 판단된다.

V. Discussion

Hussain 등[9]은 3GPP 표준 문서에서 수작업으로 보안 요구 사항을 추출하고 형식적인 속성으로 변환하여 모델 검사기를 만들었다. 그리고 5G 제어-평면 프로토콜에서 필요한 속성에 대해 정형적으로 추론할 수 있는 5GReasoner 프레임워크를 제시했다. 그들은 5GReasoner를 이용하여, 공격자가 피해자 장치로 가장하여 AMF에게 REGISTRATION REQUEST 또는 DEREGISTRATION REQUEST 메시지를 전송하여 피해자 장치의 연결을 네트워크에서 은밀하게 해제하는 “Cutting off the Device” 공격을 발견하였다. 하지만 우리가 3GPP 표준 문서 [12, 13]를 기반으로 분석한 결과, 5G 이동통신 네트워크 시스템이 3GPP 표준을 충실히 준수하여 구현된 경우에는 등록 해제 공격은 불가능한 것으로 판단된다. 그 이유는 그들이 3GPP 표준 문서에서 보안 요구 사항을 추출하고 형식적인 속성으로 변환할 때, 3GPP 표준 문서의 내용이 완전하게 적용되지 않아 발생한 것으로 판단된다.

VI. Conclusions

본 논문은 5G Standalone NPN에서 UE의 등록 해제 공격의 가능 여부를 3GPP 표준 문서에 근거하여 분석하였다. 또한 사용자가 등록 되어 있는 AMF와는 다른 새로운 AMF에게 스푸핑된 RRC 연결 설정을 시도하였을 때 등록 해제 공격의 가능성도 분석하였다. 5G 이동통신 네트워크 시스템이 3GPP 표준을 충실히 준수하여 구현된 경우에는 UE의 등록 해제 공격은 불가능한 것으로 판단된다. Hussain 등 [9]은 보안 요구 사항을 추출하고 형식적인 속성으로 변환할 때, 3GPP 표준의 기술 규격 및 기술 요구 사항 문서의 내용이 완전하게 적용이 되지 않아서 그들의 공격이 성공 가능한 것으로 도출된 것으로 판단된다. 본 연구에서 분석한 결과물들은 5G Standalone NPN을 보안 안전하게 구현하는데 있어 중요한 역할을 수행할 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] M. Agiwal, A. Roy, and N. Saxena: “Next Generation 5G Wireless Networks: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, Vol. 18, No. 3, pp. 1617-1655, 3rd Quart., 2016, DOI: 10.1109/COMST.2016.2532458

[2] M. Wollschlaeger, T. Sauter and J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0,” IEEE Industrial Electronics Magazine, Vol. 11, No. 1, pp. 17-27, Mar. 2017, DOI: 10.110 9/MIE.2017.2649104.

[3] 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. 196-248, 1st Quart., 2020. DOI: 10.1109/COMST.2019.2933899

[4] 3GPP TS 22.261 v16.11.0: “Service Requirements for the 5G System; Stage 1,” March 2020.

[5] 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.

[6] 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.

[7] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A Formal Analysis of 5G Authentication,” In Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS ’18), pp. 1383-1396, Oct. 2018. DOI: 10.1145/3243734.3243846.

[8] C. Cremers and M. Dehnel-Wild, “Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion,” in Proc. 26th Annual Network and Distributed System Security Symposium, NDSS, pp. 24-27, Feb. 2019. DOI: 10.14722/ndss.2019.23394

[9] 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.

[10] 5G-ACIA White Paper: “5G Non-Public Networks for Industrial Scenarios,” July 2019.

[11] T.K. Park, J.G. Park, K. Kim: “Security Threats and Potential Security Requirements in 5G Non-Public Networks for Industrial Applications,” Journal of the Korea Society of Computer and Information, Vol. 25, No. 11, pp. 105-114, Nov. 2020. DOI: 10.9708/jksci.2020.25.11.105.

[12] 3GPP. TS 24.501 v16.7.0: “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3,” Dec. 2020.

[13] 3GPP. TS 23.502 v16.8.0: “Procedures for the 5G System (5GS); Stage 2,” Mar. 2021.

Authors

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.

Kyungmin Park received his B.S., M.S., and Ph.D. degree in Computer Engineering from Chungnam National University, Rep. of Korea, in 2010, 2013, and 2019. He joined the Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea, in 2017, where he is currently working as a senior researcher. Currently, he is interested in mobile network security.

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.