Journal of KIIT. Vol. 19, No. 10, pp. 79-85, Oct. 31, 2021. pISSN 1598-8619. eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.10.79

5G SNPN에서 위장 RRC 연결을 이용한 사용자 DoS 공격 분석

김기원*, 박경민**, 박태근***

Analysis of DoS Attack against Users with Spoofed RRC Connections in 5G SNPN

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

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).

요 약

5G 이동통신 네트워크에서 위장 RRC 연결(Spoofed RRC Connection)을 이용하여 피해자 UE(User Equipment)를 네트워크에서 은밀하게 연결 해제시키고 더 이상 피해자 UE가 네트워크에 연결을 하지 못하게 하는 공격이 있었다. 본 논문은 5G SNPN(Standalone Non-Public Network)에서 3GPP(3rd Generation Partnership Project) 표준 문서에 근거하여 위장 RRC 연결을 이용한 사용자 DoS 공격의 가능성을 분석하였다. 첫째, gNB에서 UE의 RRC 상태를 관리하는 것을 확인하였다. 둘째, 피해자 UE로 가장한 공격자가 피해자 UE와 연결되어 있는 gNB와 위장 RRC 연결이 가능한 것을 확인하였다. 셋째, UE의 AS 보안 컨텍스트의 생성과 삭제의 시점에 대해 분석하였다. 이를 통해 위조 RRC 연결을 이용한 DoS 공격은 가능하며 이 공격을 통해서 피해자 UE가 어떤 RRC 상태이더라도 RRC_IDLE 상태로 만들 수 있다.

Abstract

In the 5G mobile communication network, there has been an attack that uses a spoofed RRC connection to stealthily disconnect a victim UE(User Equipment) from the network and prevent the victim UE from connecting to the network anymore. In this paper, we analyzed the possibility of user DoS attack using spoofed RRC connection based on 3GPP(3rd Generation Partnership Project) standard document in 5G SNPN(Standalone Non-Public Network). First, it was confirmed that the gNB manages the RRC state of the UE. Second, it was confirmed that an attacker masquerading as a victim UE could establish a spoofed RRC connection with the gNB connected to the victim UE. Third, the timing of creation and deletion of the AS security context of the UE was analyzed. Through this, DoS attacks using a spoofed RRC connection can make the victim UE into the RRC_IDLE state no matter what RRC state it is in.

Keywords

5G standalone non-public network, 3GPP standard, RRC connection, DoS attack

* 목포해양대학교 해양컴퓨터공학과 교수
- ORCID: https://orcid.org/0000-0002-4445-5723
** 한국전자통신연구원 선임연구원
- ORCID: https://orcid.org/0000-0001-9049-3635
*** 단국대학교 컴퓨터공학과 교수 (교신저자)
- ORCID: https://orcid.org/0000-0001-7654-8652

· Received: Sep. 20, 2021, Revised: Oct. 13, 2021, Accepted: Oct. 16, 2021
· Corresponding Author: Tae-Keun Park
Dept. of Computer Engineering, Dankook University, Yongin, Korea
Tel.: +82-31-8005-3162, Email: tkpark@dankook.ac.kr

Ⅰ. 서 론

5G 이동통신 네트워크는 증가된 통신 용량, 향상된 서비스 품질(QoS), 매우 짧은 지연 시간, 매우 높은 데이터 전송 속도 제공이라는 특성을 가진다. 이러한 5G 이동통신 네트워크에서 고품질 이동통신 서비스의 안전한 응용을 지원하기 위해서는 가입자 개인 정보와 통신 기밀성 및 무결성을 보호하는 것 외에도 다양한 사이버 공격에 대해 안전해야 한다[1][2].

이동통신 네트워크에서의 안전한 응용을 위해서 4G와 5G에 대한 다양한 보안 연구가 진행되었다[2]-[7]. 5G 이동통신 네트워크 보안 연구 중에서, Hussain 등[7]은 5G의 NAS와 RRC 계층의 프로토콜에 대한 보안 검증을 위해, 정형적인 모델(Formal model) 구성하여 5GReasoner라는 프레임워크를 제안하였으며 이를 이용하여 5G 보안 설계 취약점을 도출하였다. 4G 이동통신 네트워크 보안 연구 중에서, Kim 등[6]은 실제 운영 중인 LTE 네트워크에서 RRC와 NAS 계층의 보안 검증을 위해 LTEFuzz라는 도구를 구현하였고, 이를 이용하여 LTE 보안 취약점들을 찾아냈다.

일반 대중에게 통신 서비스를 제공하는 일반적인 이동통신 네트워크와 달리 5G NPN(Non-Public Network)은 명확하게 정의된 사용자 조직 또는 그룹에 5G 무선 네트워크 서비스를 제공하는 용도로 정의된 이동통신 네트워크이다. 5G NPN은 캠퍼스나 공장과 같이 특정 조직에 의해 정의된 구내에 구축되며, 높은 서비스 품질, 높은 보안 요구 사항, 네트워크의 격리, 관리 및 운영에 대한 책임 등의 요구사항을 만족하도록 설계된다[8]. 5G-ACIA (Alliance for Connected Industries and Automation)는 산업 도메인에 5G 이동통신 네트워크의 적용을 위해 네 가지의 5G NPN 구축 모델을 제시하였다[8].

본 논문에서는 5G-ACIA가 제시한 네 가지 구축 모델 중 5G SNPN(Standalone NPN) 환경에 초점을 맞춘다.

Hussain 등[7]은 5GReasoner를 이용하여 5G 무선 네트워크에서 찾은 취약점을 활용하여, 특정 사용자를 네트워크에서 은밀하게 연결 해제하는 “Denial-of-Service with RRCSetupRequest” 공격을 제안하였다. 본 논문에서는 Hussain 등[7]이 제시한 “Denial-of-Service with RRCSetupRequest” 공격의 실현 가능성을 5G SNPN 환경에서 3GPP 표준 문서에 근거하여 분석한다.

Ⅱ. 관련 연구

본 장에서는 4G와 5G 환경에서 위장 RRC 연결을 이용한 사용자에 대한 DoS(Denial-of-Service) 공격에 대한 기존 연구들에 대하여 간략히 소개한다.

2.1 Blind DoS Attack

Kim 등[6]은 4G LTE에서 위장 RRC 연결(Spoofed RRC connection)을 이용하여 피해자 UE(User Equipment)가 4G 기지국인 eNB에 연결하지 못하게 하는 “Blind DoS Attack”을 제안하였다. 공격자는 피해자 UE의 서빙 eNB가 커버하는 영역 내에서 공격을 수행할 수 있고, 피해자 UE의 RRC 연결 절차를 스니핑하여 피해자 UE의 S-TMSI (S-Temporary Mobile Subscriber Identity)를 얻을 수 있다[9].

피해자 UE의 RRC 연결 상태가 RRC_IDLE 또는 RRC_CONNECTED인 경우 각각에 대해 해당 공격의 영향을 분석하면 다음과 같다.

첫째, 피해자 UE가 RRC_IDLE 상태에 있는 경우, UE가 페이징(Paging) 메시지를 수신하였거나 UE가 네트워크로 전송하고자 하는 트래픽을 가지고 있으면 UE는 RRC 연결 설정을 시도한다. 그런데 공격자가 피해자 UE로 가장하여 위장 RRC 연결을 이미 설정하였다면, 서빙 eNB는 피해자 UE의 RRC 상태를 RRC_CONNECTED로 저장하고 서빙 MME에게 이 변경 사항을 통지한 상태가 된다. 이러한 상태에서 MME는 피해자 UE에 대한 페이징 메시지 전송을 트리거하지 않는다. 결과적으로 피해자 UE는 자신의 트래픽 전송을 위하여 새로운 RRC 연결을 설정하려고 시도할 때까지 서빙 eNB와 연결 해제된 상태가 유지된다. 사용자 입장에서 보면, 음성 전화와 데이터의 수신이 불가능한 상태가 된다.

둘째, 피해자 UE가 RRC CONNECTED 상태에 있는 경우, 공격자가 피해자 UE로 가장하여 위장

RRC 연결을 설정하면 피해자 UE에게 어떠한 알림도 없이 피해자 UE의 기존 RRC 연결이 eNB에 의하여 해제된다. 이 경우 피해자 UE는 서빙 eNB와 계속 통신을 시도하려고 하더라도 무선 베어러가 이미 해제되었기 때문에 그 시도는 실패하게 된다. 만약 공격자가 위장 RRC 연결 설정을 지속한다면, 피해자는 계속 연결이 끊긴 상태에 머무르게 된다.

2.2 Denial-of-Service with RRCSetupRequest

Hussaine 등[7]은 5G에서 위장 RRC 연결을 이용하여 피해자 UE를 5G 네트워크에서 은밀하게 연결 해제하는 "Denial-of-Service with RRCSetupRequest" 공격을 제안하였다. 공격자는 피해자 UE의 TMSI를 알고 있고 피해자 UE로 가장할 수 있다고 가정한다[7].

일반적으로 RRCSetupRequest 메시지는 5G 기지국인 gNB와의 RRC 연결 설정을 위해 사용자 UE에 의해 전송된다. 이 메시지는 무결성 보호가 되지 않기 때문에 공격자가 이 메시지를 스푸핑하여 잠재적인 DoS 공격을 일으킬 수 있다.

공격 절차를 간략히 서술하면 다음과 같다. 먼저 피해자 UE를 사칭하는 공격자는 피해자가 이미 연결된 gNB에게 피해자의 TMSI가 포함된 위장 RRCSetupRequest 메시지를 전송한다. 그러면 네트워크는 묵시적으로 피해자 UE와의 연결을 해제하고 공격자와 연결을 맺으면서, 피해자 UE의 현재 AS 보안 컨텍스트(AS security context)를 삭제한다.

III. 5G SNPN에서 위장 RRC 연결을 이용한 특정 UE에 대한 DoS 공격의 타당성 분석

이 장에서는, 5G SNPN 환경에서, Hussaine 등[7]이 제안한 "Denial-of-Service with RRCSetupRequest" 공격의 실현 가능성을 3GPP 표준에 기반하여 분석한다.

3.1 5G 네트워크에서의 UE의 RRC 상태 관리 분석

3GPP 38.331[10]의 "4.2.1 UE states and state transitions including inter RAT"에 명시된 NR(New Radio)에서 UE의 상태 머신과 상태 천이는 그림 1과 같다.

또한 3GPP 23.502[11]의 "4.8.3 N2 Notification procedure"에 명시되어 있는 UE의 RRC 상태 천이 통보 절차는 그림 2와 같다. 그림 2의 NG-RAN은 5G 네트워크의 RAN(Radio Access Network)을 의미한다. 그림 2의 절차는, 대상 UE가 CM-CONNECTED 상태에 있을 때, 접속과 이동성 관리 기능의 AMF(Access and Mobility management Function)가 NG-RAN에 RRC 상태 정보를 보고하도록 요청하는 절차이다. 즉, NG-RAN에서 관리하고 있는 UE의 RRC 상태가 변경되면 이를 AMF에게 보고하는 것에 관련된 절차이다.

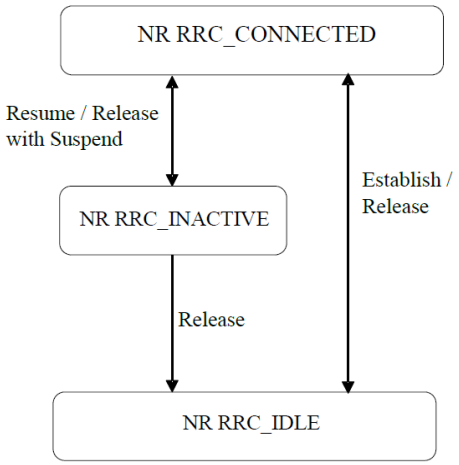

그림 1. NR에서 UE 상태 머신 및 상태 천이 [10]
Fig. 1. UE state machine and state transitions in NR [10]

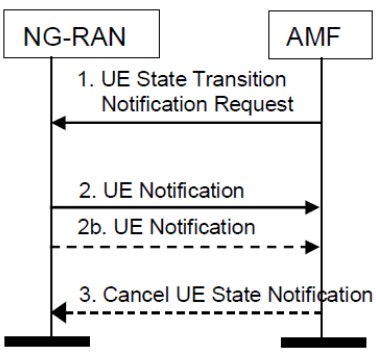

그림 2. RRC 상태 천이 통보 [11]
Fig. 2. RRC state transition notification [11]

그림 2의 단계 1에서 AMF는 NG-RAN에게 “UE State Transition Notification Request” 메시지를 보낼 때, 어떤 UE의 상태 변화를 보고해야 하는지를 지정한다. 그러면, 단계 2에서 NG-RAN이 AMF에게 UE 통지(Notification) 메시지를 전송하여 UE의 현재 RRC 상태를 보고한다. 또한, NG-RAN은 UE의 RRC 상태가 변할 때마다, UE의 RRC 상태를 단계 2b에서와 같이 AMF에게 보고한다. 그림 1과 그림 2로부터, UE와 5G 네트워크에 의하여 UE의 RRC 상태가 동일하게 관리되고 있음을 확인할 수 있다.

그렇다면, Hussaine 등[7]이 제안한 “Denial-of-Service with RRCSetupRequest” 공격에서 피해자 UE가 이미 연결된 기지국에게 피해자 UE를 사칭하는 공격자가 위장 RRCSetupRequest를 전송하였을 때, 피해자 UE의 RRC 상태를 관리하고 있는 NG-RAN이 피해자 UE의 RRC 상태에 관계없이 위장 RRCSetupRequest를 처리할 것인가에 대하여 확인할 필요가 있다. 이와 관련하여, 3GPP 표준 문서에 서술되어 있지는 않지만 다음과 같은 상황을 생각할 수 있다. 예를 들어, UE에서 전원이 갑자기 차단되었다가 다시 전원이 공급되어 UE가 재시작되었다고 가정하자. UE가 어떠한 메시지를 보내지도 못한 상태로 재시작되었기 때문에, NG-RAN에서 UE의 RRC 상태는 UE가 재시작하기 전의 상태로 유지되고 있지만, 재시작한 UE의 RRC 상태는 RRC_IDLE 상태가 된다. 이러한 상태 불일치 문제를 해결하기 위해서는, NG-RAN이 관리하고 있는 UE의 RRC 상태에 관계없이 UE의 RRCSetupRequest를 처리하여야 한다.

따라서 피해자 UE로 가장한 공격자가 RRC 연결 설정 절차를 수행할 경우, 공격자와 NG-RAN이 동일한 RRC 상태를 가지게 되고, 결과적으로, 피해자 UE의 RRC 상태와 NG-RAN의 RRC 상태가 달라질 수 있게 된다.

3.2 공격자의 위장 RRC 연결 분석

위장 RRC 연결을 이용한 피해자 UE에 대한 DoS 공격이 성공하려면, 먼저 피해자 UE로 가장한 공격자가 피해자 UE와 연결되어 있는 gNB와 위장 RRC 연결이 가능해야 한다.

3GPP TS 38.401 [12]의 “8 Overall procedures in gNB-CU/gNB-DU Architecture”의 “8.1 UE Initial Access”에 UE의 초기 액세스 절차가 서술되어 있다. 그림 3은 UE 초기 액세스 절차의 일부를 보여준다. 위장 RRC 연결이 설정되기 위해서는 그림 3의 UE 초기 액세스 절차에서 피해자 UE로 가장한 공격자가 “1. RRCSetupRequest” 단계부터 “5. RRCSetupComplete” 단계까지 정상적으로 수행 가능하여야 한다.

먼저, 공격자는 피해자 UE로 가장하여 위장된 RRCSetupRequest 메시지를 생성할 수 있어야 한다. RRCSetupRequest 메시지 포맷과 IE(Infomation Element) 확인을 위해서 3GPP TS 38.331 [10]를 보면, RRCSetupRequest 메시지의 Signalling Radio Bearer는 SRB0이고 Logical Channel은 CCCH (CommonControlChannel)이다. 또한, 공격자는 위장된 RRCSetupRequest 메시지를 생성하기 위해 필요한 피해자 UE의 TMSI를 알고 있다고 가정하고 있다 [7]. 따라서 UE의 초기 액세스 절차에서 피해자 UE로 가장한 공격자는 위장된 RRCSetupRequest 메시지를 전송하여 “1. RRCSetupRequest” 단계를 수행할 수 있다.

그러면 gNB-DU와 gNB-CU가 “2. INITIAL UL RRC MESSAGE TRANSFER”와 “3. DL RRC MESSAGE TRANSFER” 단계를 수행한 뒤, “4. RRCSetup” 단계에서 gNB-DU는 UE로 가장한 공격자에게 RRCSetup 메시지를 전송한다. 3GPP TS 38.331[10]에서 RRCSetup 메시지는 SRB1을 설정하기 위해서 사용된다고 명시되어 있고, RRCSetup 메시지의 Signalling Radio Bearer는 SRB0이고 Logical Channel은 CCCH라고 명시되어 있다.

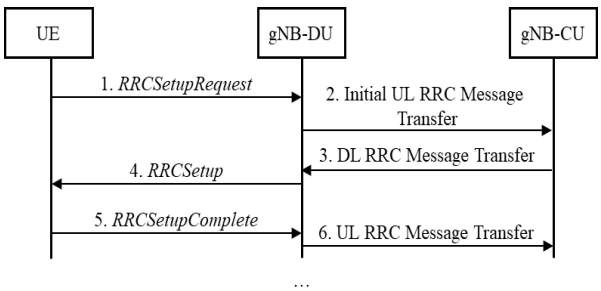

그림 3. UE 초기 액세스 절차의 일부 [12]
Fig. 3. Part of the UE initial access procedure [12]

RRCSetup 메시지를 수신한 공격자는 “5. RRCSetupComplete” 단계의 수행을 위해서, gNB-DU에게 RRCSetupComplete를 전송해야 한다. 3GPP TS 38.331[10]에 따르면, RRCSetupComplete 메시지의 Signalling Radio Bearer는 RRCSetup 메시지에서 설정한 SRB1이고 Logical Channel은 DCCH라고 명시되어 있다.

여기까지의 분석된 내용을 정리하면 다음과 같다. 피해자 UE로 가장한 공격자가, 그림 3에서, RRCSetupComplete 메시지를 보내는 단계까지 수행하는 것은 가능하다고 판단되며, RRCSetup 메시지로부터 SRB1을 위한 정보를 받음으로써, 피해자 UE에게 할당되었던 무선 자원을 NG-RAN이 해제하도록 만드는 것도 가능하다고 판단할 수 있다.

그러나 추가로 확인이 필요한 사항이 있다. 피해자 UE의 RRC 상태에 관계없이 공격자의 위장 RRC 연결 설정이 가능하다는 결론을 내리기 위해서는, 피해자 UE의 AS 보안 컨텍스트에 의하여 RRCSetupRequest, RRC Setup, RRCSetupComplete 메시지가 어느 수준까지 보호되는지 여부를 확인하여야 한다.

3GPP TS 38.331[10]에서 “Annex B (informative): RRC Information”의 “B.1 Protection of RRC messages”을 보면, RRCSetupRequest, RRCSetup, RRCSetupComplete, 메시지의 AS 보안 활성화(AS Security activation) 전/후에 전송 가능 여부와 메시지 보호 수준이 서술되어 있다.

이 내용에 따르면, RRCSetup은 “P”, “A-I”, “A-C”에 대하여 모두 “+”로 표시되어 있다. “P”가 “+”라는 것은 AS 보안 활성화 이전에 해당 메시지가 아무런 보호 없이 전송될 수 있다는 것을 의미한다. 그리고 “A-I”가 “+”라는 것은 AS 보안 활성화가 이루어진 다음에도 해당 메시지는 무결성 보호 없이 전송될 수 있음을 의미한다. 마지막으로 “A-C”가 “+”라는 것은 AS 보안 활성화가 이루어진 다음에도 해당 메시지는 암호화되지 않고 전송될 수 있음을 의미한다. 이상의 내용은, 앞서 언급한 바와 같이, 5G 네트워크에서 저장 중인 UE의 RRC 상태와 관련없이, UE가 요청한다면 5G 네트워크는 UE가 읽을 수 있는 상태로 RRCSetup 메시지를 보내주겠다는 뜻으로 해석할 수 있다.

이에 반하여, RRCSetupRequest와 RRCSetupComplete는 “P”만 “+”로 표시되어 있고 “A-I”와 “A-C”는 모두 “NA”로 표시되어 있다. 이상의 내용은 AS 보안 활성화가 되지 않은 UE만이 RRCSetupRequest와 RRCSetupComplete 메시지를 아무런 보호 없이 전송할 수 있다는 뜻으로 해석할 수 있다.

다음 절에서는, 피해자 UE의 RRC 상태에 관계없이 공격자의 위장 RRC 연결 설정이 가능한지에 대한 최종 결론을 내리기 위하여, UE와 5G 네트워크에서의 AS 보안 활성화에 대하여 추가 분석한다.

3.3 AS 보안 활성화 분석

3GPP 38.331[10]의 “5.3.3.4 Reception of the RRCSetup by the UE”을 보면, RRCSetup을 수신한 UE는 지금까지 사용하던 현재 AS(Current AS) 보안 컨텍스트 를 폐기(Discard)한다고 서술되어 있다. 이후 “Security Mode Command” 절차를 통해 새로운 AS 보안 컨텍스트를 생성하기 때문으로 판단된다. 이상의 내용으로부터, RRCSetup 메시지가 전송되는 시점에 NG-RAN에서도 UE의 현재 AS 보안 컨텍스트가 폐기되는 것으로 유추할 수 있다.

RRC_CONNECTED와 RRC_INACTIVE의 상태 사이의 천이 과정에서, AS 보안 컨텍스트의 관리를 확인하기 위해, 3GPP 33.501[13]의 “6.8.2 Security handling at RRC state transitions”을 살펴보면, UE의 AS 보안 컨텍스트는 RRC_CONNECTED와 RRC_INACTIVE 상태에서 유지된다고 서술되어 있다. 또한, 해당 문서에서는 UE가 RRC_INACTIVE 상태에서 RRC_CONNECTED 상태로 천이할 때, 저장되어 있던 UE의 AS 보안 컨텍스트를 재활성화한다(Reactivate)고 서술되어 있다.

이상의 내용들을 정리하면 다음과 같다. UE가 NG-RAN과 RRC 연결을 설정하고 AS 보안 컨텍스트를 생성하고 나면, AS 보안 활성화가 되어 있는 RRC_CONNECTED 상태가 된다. UE가 RRC_CONNECTED 상태에서 RRC_INACTIVE 상태로 바뀌더라도 AS 보안 컨텍스트는 유지된다. 하지만, UE의 RRCSetupRequest 메시지에 대한 응답으로

NG-RAN이 RRCSetup을 보내고 UE가 이를 수신하게 되면, UE와 RG-RAN 모두에서 UE의 현재 AS Security Context는 폐기된 상태가 된다.

따라서, 피해자 UE로 가장한 공격자가 피해자 UE의 RRC 상태에 관계없이 위장 RRC 연결을 설정하는, Hussain 등[7]이 제안한 “Denial-of-Service with RRCSetupRequest” 공격은 실현 가능한 공격이라고 판단할 수 있다.

Ⅳ. 결 론

본 논문에서는 5G SNPN에서 위장 RRC 연결을 이용한 DoS 공격의 가능 여부를 3GPP 표준에 기반으로 분석하였다. 분석 결과는 가능한 것으로 판단되며 근거로는, 첫째, 5G SNPN에서 UE의 RRC 상태를 gNB도 관리하고 있으며, 공격자가 이를 악용하여 UE의 RRC 상태와 gNB의 RRC 상태를 서로 상이하게 만들 수 있다. 둘째, 피해자 UE로 가장한 공격자가 위장 RRCSetupRequest 생성이 가능하며, RRCSetup을 gNB로부터 수신한 후, RRCSetupComplete 메시지를 보내는 것 까지 가능하다. 셋째, RRC 연결과 관련하여 AS 보안 컨텍스트의 생성과 삭제 시점을 볼 때 이 공격이 가능하다. 3GPP 표준 규격에 따라 정확하게 구현된 시스템에서, 위장 RRC 연결을 이용한 DoS 공격은 RRC 상태가 RRC_IDLE, RRC_INACTIVE, 또는 RRC_CONNECTED인 피해자 UE의 RRC 상태를 RRC_IDLE로 만들 수 있다.

또한 피해자 UE의 RRC 상태가 RRC_CONNECTED인 경우, 위장 RRC 연결의 반복적인 시도를 통해 피해자 UE가 계속 서비스를 받지 못하도록 할 수 있다. 본 연구에서 분석한 내용은 위장 RRC 연결을 이용한 DoS 공격 대응 방안 연구에 기여할 것으로 기대한다.

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, Feb. 2016. https://doi.org/10.1109/COMST.2016.2532458.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtovand, and M. Ylianttila, "Security for 5G and beyond", IEEE Communications Surveys & Tutorials, Vol. 21, No. 4, pp. 3682-3722, May 2019. https://doi.org/10.1109/COMST.2019.2916180.

[3] S. 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, San Diego, CA, USA, pp. 18-21, Feb. 2018. http://dx.doi.org/10.14722/ndss.2018.23313.

[4] 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), Toronto, Canada, pp. 1383-1396, Oct. 2018. https://doi.org/10.1145/3243734.3243846.

[5] 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, San Diego, CA, USA, pp. 24-27, Feb. 2019.

[6] H. Kim, J. Lee, E. Lee, and 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. https://doi.ieeecomputersociety.org/10.1109/SP.2019.00038.

[7] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and 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, London, United Kingdom, pp.669-684, Nov. 2019.

[8] 5G-ACIA White Paper, "5G non-public networks for industrial scenarios", Jul. 2019.

[9] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, "Breaking LTE on layer two", in IEEE Symposium on Security & Privacy (SP), pp. 1121-1136, May 2019. https://doi.org/10.1109/SP.2019.00006.
[10] 3GPP TS 38.331 v16.3.1, "Radio Resource Control (RRC) protocol specification", Jan. 2021.
[11] 3GPP TS 23.502 v16.8.0: "Procedures for 5GS", Mar. 2021.
[12] 3GPP TS 38.401 v16.5.0, "NG-RAN; Architecture description", Apr. 2021.
[13] 3GPP TS 33.501 v16.6.0, "Security architecture and procedures for 5G system", Apr. 2021.

저자소개

김 기 원 (Keewon Kim)

2001년 2월 : 경북대학교 컴퓨터공학과(공학석사)
2006년 8월 : 경북대학교 컴퓨터공학과(공학박사)
2012년 12월 ~ 2021년 8월 : 단국대학교 컴퓨터공학과 교수
2021년 9월 ~ 현재 : 목포해양대학교 컴퓨터공학과 교수
관심분야 : 정보보안, 보안 프로토콜, 모바일 보안, 암호 하드웨어

박 경 민 (Kyungmin Park)

2010년 2월 : 충남대학교 컴퓨터공학과(공학사)
2013년 2월 : 충남대학교 컴퓨터공학과(공학석사)
2019년 2월 : 충남대학교 컴퓨터공학과(공학박사)
2017년 2월 ~ 현재 : 한국전자통신연구원
관심분야 : 모바일 네트워크 보안

박 태 근 (Tae-Keun Park)

1991년 : 포항공과대학교 컴퓨터공학과(공학사)
1993년 : 포항공과대학교 컴퓨터공학과(공학석사)
2004년 : 포항공과대학교 컴퓨터공학과(공학박사)
1996년 ~ 2000년 : SK Telecom 중앙연구원 선임연구원
2000년 ~ 2001년 : 3Com Korea 과장
2001년 ~ 2002년 : Ericsson Korea 차장
2004년 ~ 현재 : 단국대학교 컴퓨터공학과 교수
관심분야 : 네트워크 보안, IoT, 무선/모바일 통신, 분산서비스