*5GTesting: 5G SA 환경에서 NAS 구현 취약점 탐지를 위한 네트워크 상태 기반 테스팅 도구 개발

황영빈, 박철준, 손민철, 김용대

한국과학기술원 전기 및 전자공학부 (대학원생)

5GTesting: Framework for NAS Vulnerability Analysis of 5G SA Network with Stateful Testing

Yeongbin Hwang, CheolJun Park, Mincheol Son, Yongdae Kim

School of Electrical Engineering, KAIST (Graduate student)

요 약

2020년 T-Mobile에서 5G StandAlone (SA) 서비스가 처음 시작되었고 현재는 우리나라를 포함한 많은 나라에서 5G SA 서비스를 사용하고 있다. 하지만 테스트를 위한 오픈 소스 프로젝트의 부재로 인해 5G 네트워크 취약점 분석을 위한 연구가 충분히 진행되지 않았다. 본 논문에서는 5G SA 네트워크의 구현 취약점 탐지를 위해 다양한 네트워크 상태에서 테스팅 할 수 있는 도구인 5GTesting을 제시한다. 5GTesting은 기존 이동통신 네트워크에 존재하는 모든 공격 모델을 이용해 테스트를 진행할 수 있고, Registration 과정에 존재하는 다양한 상태에서의 테스트 역시 가능하다. 이를 통해, 상용 네트워크 장비에서 DoS 공격으로 이어질 수 있는 구현 취약점을 발견하였다.

I. 서론

현재 이동통신 네트워크에는 5G SA 서비스가 상용화되고 있고 국내 KT 통신사를 포함한 다양한 해외 통신사에서 5G SA 서비스를 제공하고 있다. 5G SA는 기존 LTE 코어를 사용한 채로 기지국만 5G 기지국을 사용하던 5G Non-StandAlone (NSA) 와는 다르게 코어 네트워크가 새롭게 바뀌며 독립적인 네트워크를 가지게 되었다.

새로운 코어 네트워크가 등장함에 따라 기존 LTE 네트워크에 존재했던 취약점뿐만 아니라 새로운 구성요소로 인해 다양한 위험에 노출될 수 있게 되었다. 하지만, 5G 네트워크 테스트를 위한 오픈 소스 프로젝트가 충분히 구현되지 않았다. 이로 인해, 5G 네트워크 취약점에 대한 분석이 거의 진행되지 않았고 표준 문서를 통한 취약점 분석만이 연구되었다[1]. 또한, LTE에서 진행한 네트워크 테스팅의 경우에는 REGISTERED 상태만 고려한 테스트를 진행하거나[2], Man-in-the-middle (MitM) 공격자만을 가정해 유효하지 않은 메시지를 테스트하였다[3]. 하지만 이러한 테스트의 경우 실제 네트워크가 겪는 다양한 상태와 공격 모델을 고려하지 못하게 된다.

본 논문에서는 이러한 문제점을 보완하고자 NAS 프로토콜을 대상으로 한 다양한 상태 기반 네트워크 테스팅 도구인 5GTesting을 개발하였다. 이 도구는 UE 시뮬레이터와 gNB 시뮬레이터를 이용해 동작하는 소프트웨어로 단말과 네트워크 사이에서 동작하는 메시지들을 조절해 다양한 네트워크 상태 및 공격 모델을 고려한 테스트를 지원한다. 이러한 도구를 통해 우리는 기존 LTE에 존재했던 공격뿐만 아니라 새롭게 등장한 5G에서의 메시지와 필드 등을 다양한 공격 모델을 적용해 테스트를 진행하였고, 이를 통해 실제 네트워크 장비에서 구현 취약점을 발견하였다.

본 논문에서는 5GTesting 디자인과 이를 통

* 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00428, 정형 및 비교 분석을 통한 자동화된 이동통신 프로토콜 보안성 진단 기술)

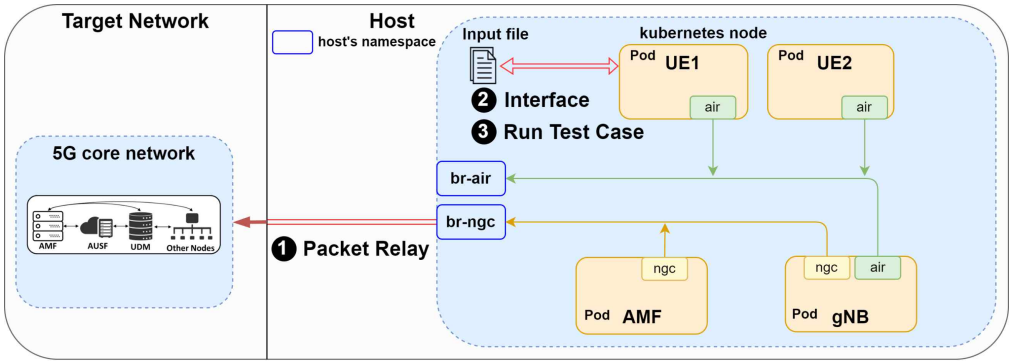

그림 1 5GTesting 디자인 구조

해 진행할 수 있는 테스트 시나리오를 보여준다. 또한, 5GTesting의 실제 동작 과정을 살펴보며 상용에서 발견된 취약점과 이를 이용한 공격을 소개한다.

II. 배경

2.1 5G 코어 네트워크

5G 코어 네트워크는 서비스 기반 구조로 구축되어 네트워크의 기능별로 구성요소가 나뉘어 있다. 그 중, Access Mobility Function (AMF)는 사용자의 등록 및 이동성 관리를 진행하는 구성요소로 UE가 보내는 NAS 메시지를 처리하게 된다. 본 논문에서는 NAS 프로토콜을 대상으로 하므로 AMF 테스트를 진행한다.

2.2 네트워크 공격 모델

네트워크를 대상으로 하는 대표적인 공격 모델은 Fake UE, MitM이 있다. Fake UE는 네트워크에 정상 유저인 것처럼 메시지를 보내는 공격자이고, MitM은 유저와 네트워크 사이에서 메시지를 드롭/변경 등이 가능한 공격자이다. 모든 공격자는 다른 사용자의 키를 가지고 있지 않아 잘못된 MAC 값을 가진 메시지를 만들거나 Plain 메시지만을 생성할 수 있다.

III. 디자인

5GTesting은 Open5GCore[4]를 기반으로 하여 테스트를 위한 모듈을 추가한 형태로 UE, gNB 시뮬레이터를 이용해 네트워크와 통신하며 다양한 테스트를 진행할 수 있다.

3.1 구조

Open5GCore는 UE, gNB를 포함한 5G 코어 네트워크를 구현한 최초의 프로젝트로, SA 네트워크를 위한 3GPP Release 15 및 16 기능이 구현되어있어 연구 개발에 적합한 형태이다. 하지만 내부 구성요소가 컨테이너로 실행되도록 구성돼있어 다른 네트워크를 테스트하기 위한 목적에는 적합하지 않습니다.

이 연구에서는 다양한 상태 기반으로 테스트하기 위해 몇 가지 모듈을 추가 구현하였고 모듈이 포함된 전체적인 구조는 **그림 1**과 같다. 첫 번째는 패킷 릴레이 모듈이다. 기존 프로그램은 UE, gNB 컨테이너가 br-ngc라는 가상 네트워크 브릿지를 통해 내부 5G 코어 네트워크와 통신하게 된다. 이것을 이용해, 우리는 네트워크 브릿지에서 메시지를 가로채 타겟 네트워크로 전달하는 방식으로 모듈을 구현하였다. 두 번째는 JSON 입력 파일을 프로그램에서 실행할 수 있도록 변환하는 인터페이스 모듈이다. UE 컨테이너에서 JSON 파일을 입력받아 프로그램 안에서 사용할 수 있는 구조로 변환시켜 저장한다. 이때 저장되는 값에는 네트워크 상태, 테스트 타입, 메시지 필드 등이 있다. 마지막은 테스트 실행 모듈이다. 저장된 입력값을 통해 네트워크와 통신하며 원하는 상태로 이동시킨다. 그 후 테스트 타입, 필드를 보고 메시지를 조절하여 테스트를 진행한다.

3.2 테스트 타입

우리는 기존 연구들에서 진행된 네트워크 대상 테스트 종류를 INJECT, MODIFY, REPLAY, DROP 4가지로 분류하였고 각각의 기능을 구현하였다.

INJECT: Fake UE 공격 모델을 이용한 경우로 특정 사용자의 아이디를 아는 공격자가 사용자 아이디를 포함한 메시지를 보내 사용자를 흉내내도록 하는 테스트이다. 이 테스트는 아이디 스푸핑에 해당하며 네트워크가 세션 및 아이디를 제대로 관리하지 않는다면 기존 사용자의

그림 2 JSON 입력 파일

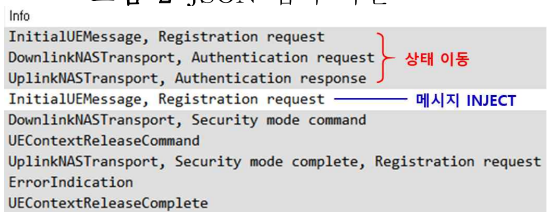

그림 3 공격 패킷 로그

연결이 끊어지는 DoS를 유도할 수 있다.

MODIFY: MitM 공격 모델을 이용해 진행되는 테스트로 사용자와 네트워크 사이에 전달되는 메시지들을 변조하는 테스트이다. 암호화 알고리즘을 바꿔 암호화를 없도록 설정하는 등 다운그레이드 공격을 확인할 수 있다.

REPLAY: MitM 공격 모델을 이용해 사용자와 네트워크 사이에서 교환되는 메시지를 캡처한 후에 정상 사용자인 것처럼 메시지를 보내는 경우이다. 네트워크에서 공격자를 정상 사용자로 인식한다면 공격자한테 정상 사용자의 트래픽이 전달되는 사용자 도용 (Impersonation) 공격을 일으킬 수 있다.

DROP: MitM 공격 모델을 이용해 사용자와 네트워크 사이에 교환되는 메시지를 드롭하는 테스트이다. 이 경우, 연결을 시도하는 메시지들을 지속해서 드롭하면 T3502와 같은 타이머가 유도돼 연결 시도 과정이 오랫동안 진행되지 않을 수 있다.

3.3 동작 예시

그림 2는 INJECT 테스트 타입을 실행하기 위한 JSON 입력 파일이다. 해당 파일을 입력하면 UE 시뮬레이터는 네트워크와 통신하며 *Authentication Response* 메시지를 보낸 상태로 이동하게 되고, 그 이후 테스트 타입을 결정하는 구간에서 INJECT라고 결정되어 새로운 UE 시뮬레이터를 실행해 *Registration Request* 메시지에 기존 UE의 아이디를 넣어 보내는 아이디 스푸핑 공격을 시도하게 된다. **그림 3**은 **그림 2** 시나리오를 실행했을 때 캡처한 패킷 로그로 *Authentication Response* 타이밍에 맞춰 새로운 UE가 *Registration Request* 메시지를 보낸 것을 확인할 수 있다.

		5GTesting	LTEFuzz [2]	Automata [3]	Bookworm [6]
테스트 타입	DROP	O	X	X	X
	REPLAY	O	O	X	X
	MODIFY	O	O	O	X
	INJECT	O	O	X	O
다양한 상태 지원		O	X	O	O
SDR 장비 유무		X	O	O	O

표 1 기존 테스팅 도구와의 차이점

3.4 기존 테스팅 도구과의 차이점

표 1은 기존 네트워크 취약점 연구에서 사용한 테스팅 도구들과 비교한 표이다.

이 도구는 크게 세 가지 장점을 제공한다. 첫 번째로, 메시지를 네트워크로 보내기 위한 Software Defined Radio (SDR) 장비가 필요하지 않다. 이전 연구에서는 네트워크에 메시지를 보내기 위해서는 srsRAN[5]과 같은 오픈 소스와 SDR 장비를 통해 라디오 신호를 전송해야 한다. 하지만, 5GTesting은 UE, gNB 연결을 시뮬레이터로 구현해 코어 네트워크에 바로 연결하므로 추가적인 장비가 필요하지 않다. 두 번째로, 네트워크 상태를 쉽게 변경할 수 있다. JSON 입력 파일을 통해 UE가 네트워크와 교환되는 메시지를 조절할 수 있어 원하는 상태로 쉽게 이동할 수 있다. 이를 통해, 다양한 상태에서 테스트도 진행할 수 있다. 세 번째로, 다양한 공격 모델에 대해서 테스트해볼 수 있다. 우리가 테스트하고 싶은 공격 타입을 JSON 파일을 통해 입력받을 수 있고 이를 통해 메시지 드롭/수정/재전송을 포함해 새로운 UE를 통한 아이디 스푸핑 또한 가능하다.

IV. 취약점 및 공격 시나리오

5GTesting을 통해 상용 네트워크 장비를 테스

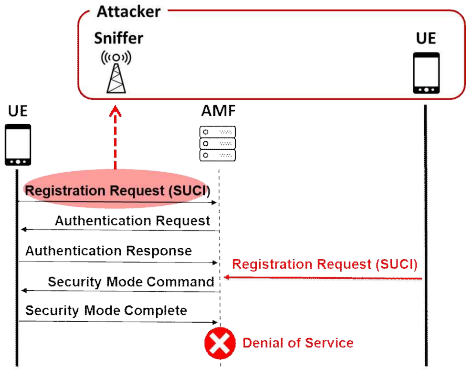

그림 4 공격 시나리오

트해 몇 가지 구현 취약점을 발견하였다. 그 중 INJECT 타입 시나리오에서 발견한 취약점과 이를 이용한 공격 시나리오는 다음과 같다.

4.1 취약점

UE가 네트워크와 암호화 통신을 위해서는 인증 과정을 통해 Security Context를 생성해야 한다. 하지만, **그림 3**의 상황처럼 네트워크가 정상 사용자의 Security Context가 생성되기 전에 같은 아이디를 가진 메시지를 받게 되면, 네트워크는 어떤 연결이 정상 사용자인지 알 수 없게 된다. 이로 인해, 네트워크에서 아이디 스푸핑을 시도한 사용자가 아닌 정상 사용자의 Context를 삭제하는 경우가 발생하였다.

4.2 공격 시나리오

위 취약점을 이용한 공격은 **그림 4**와 같은 과정으로 이루어진다. 공격자는 피해자와 같은 기지국 범위 내에 존재하며, Sniffer를 통해 정상 기지국과 피해 단말 사이의 무선 구간 통신을 들을 수 있고 fake UE를 통해 무선 신호를 전송할 수 있는 능력이 있다. 이 상황에서 피해자 UE가 망에 붙기 위해 *Registration Request* 메시지를 보낸다면, 공격자는 Sniffer를 통해 메시지 안에 있는 아이디 값을 얻을 수 있다. 이 후 *Authentication Response*에 맞춰 피해자 아이디를 넣은 *Registration Request* 메시지를 보내면 기존 피해자의 Context가 삭제되며 연결이 끊어지게 된다.

4.3 추가적인 공격 시나리오

위 공격은 피해자 UE가 접속을 시도할 때마다 공격을 진행해야 하는 단점이 존재한다. 하지만, UE에 존재하는 타이머인 T3502를 이용하면 더 의미 있는 공격을 시도할 수 있다. 피해자 UE가 *Registration* 과정이 실패하게 된다면, UE에 있는 *attempt counter* 값이 1 증가하게 된다. *attempt counter* 값이 5가 되면, UE에서는 T3502 타이머가 실행돼 12분간 접속을 시도하지 않게 된다[7]. 즉, 위에서 제시했던 공격을 5번 반복하게 된다면, 피해 사용자는 12분간 서비스를 이용하지 못하는 DoS 공격을 당하게 된다.

V. 결론

본 연구에서는 5G SA 네트워크에서의 구현 취약점을 찾기 위한 테스팅 도구를 구현하였고 이를 통해 상용 네트워크에 대한 테스트를 진행해 구현 취약점을 발견하였다.

향후 연구로는, 오픈 소스 5G 구현이 확장된다면, RRC 메시지까지 테스트 범위를 확장해 코어 네트워크뿐만 아니라 기지국에서 발생할 수 있는 구현 취약점에 대해서도 분석을 진행하고자 한다.

[참고문헌]

[1] Hussain, Syed Rafiul, et al. "5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol." Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019.

[2] Kim, Hongil, et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.

[3] Chlosta, Merlin, David Rupprecht, and Thorsten Holz. "On the challenges of automata reconstruction in LTE networks." Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2021.

[4] "Open5GCore" [Online]. Available: https://www.open5gcore.org/

[5] "srsRAN" [Online]. Available: https://github.com/srsran/srsRAN

[6] Chen, Yi, et al. "Bookworm game: Automatic discovery of LTE vulnerabilities through documentation analysis." 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021.

[7] 3GPP. TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)"