Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.919

5G 기지국에 대한 보안성평가기준 연구

홍 바 울,[1†] 김 예 준,[1] 조 광 수,[1] 김 승 주[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

A Study on Security Requirements for 5G Base Station

Paul Hong,[1†] Yejun Kim,[1] Kwangsoo Cho,[1] Seungjoo Kim[2‡]
[1,2]ICSP(Institute of Cyber Security & Privacy), School of Cybersecurity,
Korea University (Graduate student, Professor)

요 약

5G 네트워크는 차세대 통신기술로서 4G 네트워크 대비 빠른 속도, 짧은 통신 지연, 높은 연결성을 기반으로 대량의 트래픽 처리가 가능하다. 이에 따라 4차 산업혁명의 핵심 기술로 대두되어 그 중요성이 증가하고 있다. 이러한 5G 네트워크 환경에서 기지국은 그 특성상 높은 밀도로 도심 전역에 설치되어 있으며, 사용자 단말과 연결되어 서비스를 제공한다. 따라서 악의적인 공격자에 의한 피해가 기지국에 발생하는 경우, 사용자 및 사회 전반에 큰 피해를 줄 것으로 예상된다. 2016년 뉴욕타임즈 기사에 따르면 중국의 특정 서버로 사용자 데이터를 전송하는 백도어로 추정되는 소프트웨어가 미국 내 안드로이드 기기, 자동차와 같은 스마트 기기에 포함되어 있다고 보도되었다. 이후 통신 장비에 백도어 설치에 대한 이슈가 지속적으로 제기되었으며, 5G 기지국과 같은 통신장비에 대한 안전성 확보의 필요성이 대두되었다. 따라서 본 논문에서는 5G 기지국을 대상으로 체계적인 방법론인 위협모델링을 사용하여 도출한 보안기능요구사항과 백도어 이슈에 대응할 수 있는 수준의 보안보증요구사항을 제안한다. 본 논문에서 제안하는 보안요구사항은 5G 기지국에 대한 보안성평가기준으로서 안전한 네트워크 환경을 구성하기 위한 기지국 설계 및 개발에 사용될 수 있다.

ABSTRACT

As a next-generation communication technology, 5G networks are capable of handling large amounts of traffic based on higher speeds, shorter communication delays, and higher connectivity compared to 4G networks. In this 5G network environment, base stations are installed all over the city at high density due to their characteristics, and are connected to user terminals to provide services. Therefore, if the base station is damaged by a malicious attacker, it is expected to cause great damage to users and society as a whole. So the need for secure communication equipment such as 5G base stations has emerged. Therefore, in this paper, we propose the security functional requirements derived using threat modeling, a systematic methodology for 5G base stations, and the security assurance requirements at the level that can cope with the backdoor issues. The security requirements proposed in this paper can be used for base station design and development to construct a secure network environment as a security evaluation standard for 5G base stations.

Keywords: 5G, Base Station, Security Requirements, Threat Modeling

Received(06. 15. 2021), Modified(09. 27. 2021), Accepted(09. 27. 2021)

† 주저자, visitator00@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

5G 네트워크는 국제 전기 통신 연합 ITU (International Telecommunication Union)의 전파 통신국 ITU-R(ITU Radio communication Sector)에 의해 제정된 차세대 이동 통신 기술이다[1]. 5G 네트워크는 4차 산업혁명을 위한 핵심 기술로 꼽히며 초고속, 초저지연, 초연결성을 주요 속성으로 가진다[2]. 5G 네트워크 서비스는 2019년 4월 세계 최초로 한국에서 시작되었으며 뒤이어 미국, 유럽, 중국, 일본, 유럽과 같은 다양한 나라에서도 5G 네트워크 서비스가 시작되었다. 해당 서비스의 시장규모는 2020년 대비 2023년에 약 9.4배 증가한 3,565억 달러로 2026년에는 2023년 대비 약 3.3배 증가한 11,588억 달러까지 증가할 것으로 예상된다[3]. 이러한 5G 네트워크 서비스의 구성요소 중 기지국은 사용자 단말기(UE, User Equipment)와 직접 연결되어 5G 네트워크 서비스를 제공하는 핵심요소이다[4]. 5G 네트워크 기지국(gNodeB)은 4G 기지국(eNodeB)과 비교하여 대용량 정보처리가 가능하지만, 상대적으로 파장의 길이가 짧고 높은 주파수 대역을 갖는 단파를 사용함에 따라 장애물에 약하고 도달거리가 짧다는 특징을 가진다. 따라서 5G 네트워크는 4G 네트워크에 비해 많은 수의 기지국이 높은 밀집도로 설치되어야 한다. 이러한 5G 네트워크 기지국은 국내 기준으로 2019년 4월 약 3.5만개, 2021년 3월 약 14.2만개로 설치된 수량이 증가하였다. 5G 네트워크 기지국은 높은 밀집도로 설치되고, 5G 네트워크 특성상 기존 4G에 비해 다양한 분야에 대해 UE와 연결되어 서비스를 제공하는 만큼 기지국에 대한 공격이 발생하는 경우 사용자 및 서비스 전체에 대한 피해가 클 것으로 예상된다. 2016년 뉴욕타임즈 기사에 따르면 중국의 특정 서버로 사용자 데이터를 전송하는 백도어로 추정되는 소프트웨어가 미국 내 안드로이드 기기, 자동차 및 기타 스마트 기기에 포함되어 있다고 보도되었다. 이에 따라 각종 통신 장비에 백도어가 설치되어 있을 것이라는 논란이 발생되었다. 이렇듯 5G 네트워크 기지국과 같은 통신 장비는 백도어에 대한 보안 이슈를 가지고 있으며, 이를 대응 할 수 있도록 통신 장비의 보안성을 평가할 수 있는 기준 및 방법이 개발되어야 할 필요성이 있다.

따라서 본 논문은 안전한 5G 네트워크 환경 구축을 위해 5G 네트워크 기지국(gNodeB)에 대한 보안성평가기준 수립을 목적으로 한다. 이를 위해 본 논문에서는 위협모델링을 사용하여 보안기능요구사항을 도출하고, 통신장비에 대한 공격 가능성 수준을 고려한 보증요구사항을 선정한다. 위협모델링을 사용한 상세한 연구 방법은 본 논문 3장에 기술하고 있으며 연구 내용의 표 및 그림 전체는 다음 링크[1)]를 통해 확인가능하다. 본 논문에서는 통신 장비에 대한 보안 이슈를 대응 할 수 있는 5G 기지국에 대한 보안기능 요구사항을 체계적으로 도출하였으며, 도출된 보안기능 요구사항을 통해 보다 안전한 기지국에 대한 설계가 가능하다는 점에 그 기여도가 있다.

논문은 총 5장으로 구성된다. 2장에서는 본 논문에 대한 관련 연구를 소개한다. 3장에서는 위협모델링을 통한 보안성평가기준 연구 내용을 소개한다. 4장에서는 도출한 보안성평가기준에 대한 보안기능 요구사항 및 보증요구사항을 소개한다. 5장에서는 본 논문에 대한 결론 및 향후 연구를 제안한다.

II. 관련 연구

본 장에서는 분석대상인 5G 기지국 및 네트워크와 관련한 최근 연구 동향을 기술한다. 5G 기지국은 5G 네트워크의 구성요소 중 사용자 단말기와 연결되어 서비스를 제공한다. 4G 기지국과 비교하여 대용량 정보처리가 가능하지만, 기지국이 사용하는 고주파 특성상 장애물에 약하고 도달거리가 짧다는 특징을 가진다. 따라서 5G 기지국은 기기 특성상 많은 수가 설치되어야 하고 UE와 연결되어 서비스를 제공하는 만큼 기지국에 대한 공격이 발생하는 경우 사용자 및 서비스 전체에 피해가 크다. 다양한 연구에서는 5G 기지국 및 네트워크에 발생 가능한 공격을 분석하고 있다. 본 논문에서는 이러한 관련 연구 동향을 체계적으로 수집·분류하기 위하여 4단계에 걸쳐 관련 연구 조사를 수행하였다. 다음 Fig.1은 관련연구 조사 단계의 요약을 보여준다.

관련연구 조사의 각 단계별 상세 수행 내용은 다음과 같다.

1) 키워드를 통한 관련 문헌 수집: 5G, Security Requirement, Base Station, Threat Modeling의 키워드를 조합하여 문헌을 수

1) https://drive.google.com/file/d/1SsdCwtwRxmmDDYC5nH6gm_ba6Kt28TrI/view?usp=sharing

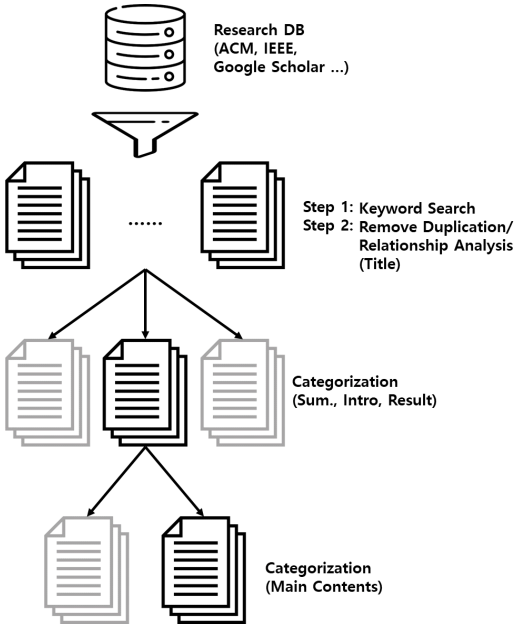


Fig. 1. Related Work Categorization Step

집하였다. 문헌 조사에 활용된 데이터베이스는 IEEE, ACM, Elsevier, Springer를 사용하였다.

2) 중복 수집된 문헌 제거 및 논문 제목을 통한 분류: 1단계에서 수집된 문헌은 동일한 논문이 검색된 결과가 존재할 수 있기 때문에 이를 제거하는 과정이 필요하다. 이후 본 논문의 연구 방향과 관련이 적은 문헌을 우선적으로 식별하여 관련성이 적은 내용은 배제된다.

3) 논문 요약, 서론, 결론 분석을 통한 분류: 2단계 과정에서의 분류 결과는 요약과 결론 내용을 기반으로 본 논문의 주제와의 연관성 분석이 수행된다. 해당 분석된 내용을 기반으로 본 논문의 연구 방향과 관련성이 적은 문헌은 배제된다.

4) 논문 본론 분석을 통한 분류: 3단계까지의 관련연구 분류 수행 결과 도출된 논문들의 본론을 본격적으로 분석한다. 본 단계를 통해 분석된 논문 분류를 최종적으로 본 연구 수행에 필요한 관련연구로 식별한다.

문헌 검색은 IEEE, ACM, Elsevier, Springer 등의 데이터베이스를 사용하였으며, 5G, Security Requirement, Threat Modeling, Base Station의 키워드를 조합하여 수행되었다. 문헌 작성 시기에 대한 범위는 5G 네트워크관련 첫

Table 1. Paper search criteria

Category	Condition
Databases	IEEE, ACM, Elsevier, Springer, etc
Search keyword	“5G”, “Security Requirement”, “5G” +“Security Requirement”, “5G“ + “Security Requirement” + “Base Station”, “5G” + “Threat Modeling“.
Publication period	4 Years (2018 ~ 2021)
Review period	2020. 02. ~ 2021. 04.

번째 표준인 3GPP Release-15가 발표된 2018년도부터 2021년까지 발간된 문서를 중심적으로 수집되었다. 2018년 이전에도 5G 네트워크 보안에 관한 연구가 수행되었으나 이때는 표준이 제정되지 않아 명확한 5G 네트워크에 대한 체계가 수립되지 않은 상태에서 수행된 연구이다. 이에 2018년 이전에 수행된 연구보단 2018년 이후에 수행된 연구에 초점을 맞추어 수집 및 분석을 수행하였다. 다음 Table 1은 관련연구 분석 1단계에서 수행된 문헌 검색 기준을 나타낸다. 각 단계별 수행결과 1단계에서는 총 612건의 문서가 수집되었으며, 2단계는 454건, 3단계는 109건, 마지막 4단계는 16건의 관련 연구가 분석 및 분류되었다. 분석된 결과는 아래 2.1, 2.2절에서 기술한다.

2.1 4단계 문서 분석에 따른 연구 동향

5G 네트워크 표준이 발표되기 이전인 2017년도에는 주로 5G 네트워크에 발생 가능한 일반적인 공격에 대한 연구가 주를 이루었다. 대표적으로 2017년 D Fang 등은 5G 네트워크의 구성요소 중 무선 네트워크 시스템 보안에 관한 연구를 수행하였다. 연구결과 D Fang 등은 5G 네트워크 기지국에 존재하는 통신 데이터에 대한 도청 및 트래픽 분석 공격, 기지국에 대한 DDoS(Distributed Denial of Service) 공격, 재밍 공격, 중간자 공격과 같은 잠재적인 공격을 분석하고 이에 대한 대응방안으로 유연한 인증을 제공하는 5G 네트워크 무선 아키텍처를 제안하였다[5].

이후 2018년도에 3GPP의 표준이 발표되었으며, 이에 따라 4G네트워크 대비 새로 추가된 기능 및 관

련 보안요구사항에 대한 연구가 진행되었다. 2018년 G Arfaoui 등은 5G 네트워크로 변경됨에 따라 추가적인 보안요구사항의 필요성에 대해 언급하였다[6]. 추가 보안요구사항을 도출하기 위해 5G 네트워크의 보안 모델링을 위한 도구, 보안 설계 원칙, 보안통제항목등을 분석하였다. 또한 I Ahmad 등은 5G 네트워크의 핵심 구성 요소인 클라우드, SDN, NFV에 대한 보안 문제를 제시하였다[7]. 이외의 연구들에서도 마찬가지로 5G 네트워크로의 변화에 따라 요구되는 일반적인 보안요구사항과 포괄적인 개요를 언급하고 있다[8-10].

2019년도에는 5G 네트워크 상에서 발생 가능한 위협분석과, 공격 시나리오, 보안 솔루션에 대한 연구가 진행되었다. 2019년 RP Jover 등은 기존 사용하던 프로토콜과 새로운 프로토콜을 비교 분석하여 5G 네트워크에서 발생 가능한 잠재적인 공격 시나리오를 분석하였다[11]. I Ahmad 등은 5G 네트워크 환경과 새로운 기술이 도입됨에 따라 발생하는 보안 위협을 분석하고 이에 대한 완화 기법을 제안하였다[12]. 이외에도 다양한 연구에서 발생 가능한 위협과 이를 완화할 수 있는 방안을 제안하였다[13-15].

2020년도에는 5G 네트워크에 대한 최신 기술을 분석하고 발생가능한 위협에 대응하기 위한 연구가 수행되었다. 2020년 D Fang 등은 5G 네트워크의 새로운 사용 사례에 초점을 맞추어 위협을 분석하였다[16]. 해당 논문의 저자는 먼저 새로운 기술의 등장에 따라 추가된 서비스들을 식별하였다. 이후 식별된 서비스에 따라 발생 가능한 사용 사례를 바탕으로 보안/개인정보 위협을 분석하고 이에 대한 해결방안을 제시하였다. 위에서 소개한 연구 이외에도 5G 네트워크 보안을 위한 자동 공격 탐지 프레임워크 제안, 5G 네트워크에 맞춤화 된 최신 기술 분석에 대한 연구도 진행되었다[17-18]. 그러나 기존의 연구들은 5G 네트워크에 대한 단편적인 공격 또는 취약점에 대한 해결방안만을 제시하고 있다. 즉, 안전한 5G 네트워크 환경 구축을 위해 구성요소별 상세한 보안요구사항에 대한 연구는 부족하다. 따라서 본 논문에서는 5G 네트워크 구성요소 중 기지국을 대상으로 보안성을 강화하기 위한 공통평가기준 기반의 상세 보안요구사항 도출에 대한 연구를 수행한다.

2.2 5G 표준 동향

5G 네트워크에 대한 국제 표준인 IMT-2020 (International Mobile Telecommunications-2020)은 ITU와 국제 표준화 단체인 3GPP의 협력 아래 제정되었다. ITU의 산하기관인 ITU-R은 5G 네트워크에 대한 핵심 목표를 제시하였으며, 이후 3GPP는 장기간에 걸쳐 ITU-R이 제시한 목표를 보완하고 ITU에게 해당 목표를 달성하기 위한 요구사항들을 제안하였다. ITU는 최종적으로 제안된 요구사항들을 승인하고 5G 네트워크 표준을 제정하였으며 2021년 Release-16이 상용화될 예정이다.

5G 네트워크와 관련된 내용은 3GPP 표준 중 2018년 6월에 발표된 Release-15부터 포함되며, Release-15이전 Release-14까지의 표준은 LTE 네트워크와 관련된 내용에 해당된다. Release-15는 5G Phase 1이라고 불리며, LTE 네트워크에서의 코어 네트워크 구조, EPC(Evolved Packet Core)에 대한 개선사항과 4G 네트워크와 5G 네트워크를 함께 사용하는 NSA 모드, 5G 네트워크만 사용하는 SA 모드에 대한 내용이 포함되어있다[19]. 이후 2020년 6월에 개발된 Release-16는 Release-15의 완성도를 높여 개발되었으며, 5G Phase 2 라고 불린다. Release-16에는 V2X (Vehicle-To-Everything) 애플리케이션 계층 서비스, 5G 위성 접근, 5G 근거리 통신망 지원, LAN(Local Area Network) 연동 등의 다양한 기술이 추가되었다. 또한 기존 표준에서 제안된 기술인 다수의 안테나를 배치하여 속도를 증가시키는 MIMO(Multiple Input Multiple Output), 고신뢰 저지연 통신인 uRLLC에 대한 개선사항이 제시되었다. Release-16 개발이 완료됨에 따라 3GPP는 해당 표준을 보완하는 Release-17 개발 작업에 착수하였다. 해당 작업은 Phase 3라고 불리며 하나의 물리적 네트워크를 논리적으로 분리하는 Network Slicing, LTE 네트워크와 5G 네트워크를 모두 지원하는 RAN(Radio Access Network) Slicing, LTE 네트워크와 5G 네트워크의 스펙트럼을 공유하는 기술인 DSS(Dynamic Spectrum Sharing)등 다양한 기술이 추가될 예정이다[20].

5G 네트워크 표준인 Release-15는 총 18개의 Series, 1136건의 문서로 구성되어 있으며 이중 보안과 관련한 문서는 총 4개로 Release-15의 33 Series에 해당한다. 그 중에서도 5G 네트워크의 기지국에 대한 보안은 "Rel15-33-401 System Architecture Evolution(SAE); Security architecture"과 "Rel15-33-501 Security

architecture and procedures for 5G system" 표준 문서에서 다루어진다[21,22]. 해당 표준 문서들은 사용자 데이터 및 신호에 대한 기밀성과 무결성, 설정 및 구성, 개방형 인터페이스, 키 관리, User Plane Data & Control Plane Data 처리, 보안 환경에 대한 항목을 중심으로 요구사항이 명시되어 있다. 그러나 해당 요구사항은 실제 보안기능 구현에 필요한 상세한 수준의 보안 요구사항을 명시하고 있지 않다는 한계가 존재한다. 또한 3GPP는 Release-16의 "Rel16-33-511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class"에서 Release-15의 33-501에서 언급하고 있는 보안 아키텍처를 실제로 적용하기 위한 보안 요구사항을 명시하고 있다[23]. 하지만 Rel16-33-511에서 제시된 요구사항은 실제 구현에 필요한 요구사항을 나태내고 있지만, 구현 수준에 대한 보증요구사항을 다루고 있지 않아 실제 설계 및 구현에 사용되기에 부족하다. 따라서 본 논문에서는 실제 보안기능 구현에 필요한 상세한 보안 요구사항을 도출하여 5G 기지국에 대한 보안성 평가 기준을 제시하고자 한다.

III. 5G 기지국 위협모델링

기지국은 LTE, 5G등의 무선 통신 서비스를 위해 코어 네트워크와 단말기를 연결하는 유·무선 통신 장비이다. 5G 네트워크에서 기지국은 연결 방식에 따라 상용화된 NSA(Non-Stand Alone)모드와 상용 예정인 SA(Stand Alone)모드가 존재한다[24]. NSA 모드는 기존 LTE 네트워크 기지국과 5G 네트워크 기지국을 둘 다 활용하여 통신하는 방식이며, SA 모드는 5G 네트워크 기지국만 활용하여 통신하는 방식이다. NSA는 LTE 네트워크 기지국과 5G 네트워크 기지국 둘 다 사용하기 때문에 5G 네트워크 서비스를 사용자에게 빠르게 제공해 줄 수 있으나, 5G 네트워크만을 위한 새로운 기술을 사용하는데 제한적이라는 단점이 있다. 다음 Fig.2는 NSA환경과 SA 환경에서의 기지국 형태를 나타낸다. 본 연구에서는 현재 서비스되고 있는 NSA 환경과 SA 환경을 모두 고려한 기지국을 대상으로 보안 요구사항을 도출한다.

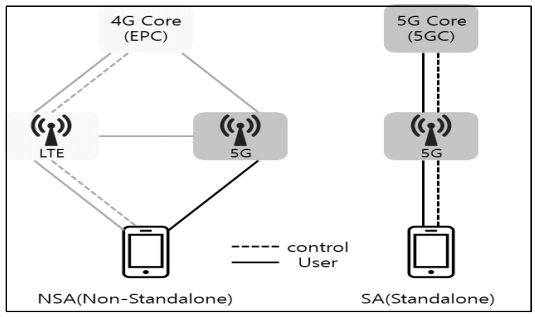


Fig. 2. 5G Base Station Environment

3.1 보안기능요구사항

위협모델링은 보안기능요구사항을 도출하는데 있어서 효과적인 방법이다[25,26]. 본 논문에서는 MS사의 STRIDE를 사용하여 위협모델링을 수행하였다[27]. STRIDE는 데이터 흐름도의 각 구성요소에 존재할 수 있는 위협을 식별하여 소프트웨어 시스템의 결함을 발견하는데 사용되는 대표적인 위협모델링 기법이다. 해당 기법은 실제 위협과 관련성이 떨어지는 위협인 false positive한 결과를 비교적 적게 도출하며, 5G 네트워크와 유사한 시스템 분석에 성공적으로 적용되는 연구 결과가 있다. 따라서 본 논문에서는 잘못된 위협 식별을 줄이고 분석대상 시스템에 적용이 가능한 STRIDE를 사용한다.

본 연구에서 사용한 위협모델링 접근 방식은 Fig.3과 같다. 5G 네트워크 기지국 환경 분석을 통해 DFD를 그린다. 이후 DFD 요소에 대해 STRIDE Model을 적용하여 위협을 식별한다. 식별된 위협을 기반으로 Attack Tree를 구성한다. 해당 식별된 공격에 대하여 잔류 위협과 함께 이를 대응 할 수 있는 대응방안을 도출한다. 해당 대응방안에 따라 점검할 수 있는 점검항목(check list)를 도출한다. 해당 내용에 따라 CC에서 표시하는 SFR 형태로 표현한다.

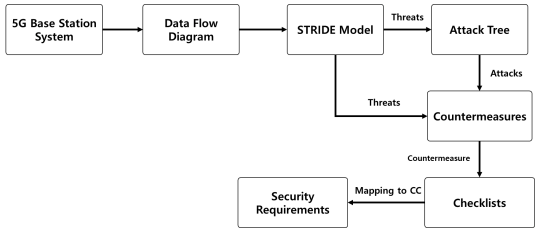


Fig. 3. Our Threat Modeling Approach using STRIDE

3.1.1 데이터 흐름도(DFD)

데이터 흐름도는 분석대상 시스템을 데이터 흐름에 따라 추상화 및 도식화한 것으로 시스템 구조 및 공격 지점을 파악할 수 있도록 도와준다[28]. 이러한 데이터 흐름도는 외부객체(external entity), 프로세스(process), 데이터 저장소(data store), 데이터 흐름(data flow), 신뢰 영역(trust boundary)의 5가지로 구성된다.

데이터 흐름도는 분석대상을 추상화한 모델로서 건전성(soundness)이 중요하다. 건전성은 추상화된 모델과 실제 분석대상의 시스템 사이에 간극이 무시 가능한 수준으로 최소화되어야 하는 성질을 의미하며 건전성이 보장된 모델은 분석대상을 올바르게 추상화했다고 판단된다. 따라서 데이터 흐름도는 추상화에 따른 분석대상과 모델 사이에 간극이 발생하지 않도록 가급적 함수 수준까지 표현될 필요가 있다. 함수 수준까지 표현하기 위해서 데이터 흐름도는 Context Level(Level 0)을 시작으로 Level 1, Level 2 순으로 상세화된다. Context Level은 분석대상 시스템 전체를 하나의 프로세스로 표현하고 해당 시스템과 상호작용을 수행하는 외부 개체를 식별하는 단계이며, Level 1, Level 2는 순서대로 프로세스를 시스템 내 구성 서브시스템, 모듈, 세부기능 수준까지 상세하게 표현하는 단계이다[29-32]. 데이터 흐름도는 세부기능 수준까지 상세화하기 위해서 소스코드 수준의 자료 또는 설계와 관련한 상세한 자료가 있어야 한다. 그러나 본 논문에서는 공개된 자료를 기반으로 분석을 수행하였고, 분석 가능한 소스코드 수준의 자료가 주어지지 않았기에 Level 1 수준의 데이터 흐름도까지 작성하였다.

5G 네트워크 기지국의 보안기능을 나타내는 프로세스는 ▲키 관리, ▲모니터링, ▲로깅, ▲인증, ▲암호화/복호화, ▲무결성 검사, ▲보안기능 인터페이스,▲스케쥴링, ▲세션 관리가 존재한다. 또한, 5G 네트워크 기지국의 비 보안기능을 나타내는 프로세스는 ▲라우팅, ▲품질 관리가 존재된다. 다음 Fig.4는 프로세스들을 애플리케이션 내 구성 모듈 단위로 분리한 Level 1 데이터 흐름도를 나타낸다.

3.1.2 공격라이브러리

시스템에 대한 데이터 흐름도를 작성한 이후에는 해당 시스템과 관련된 현재까지 알려진 취약점을 모두 수집해야한다. 이때 활용되는 공격라이브러리는 CVE(Common Vulnerabilities and Exposures), CWE(Common Weakness Enumeration) 및 각종 논문에서 발표된 취약점 관련

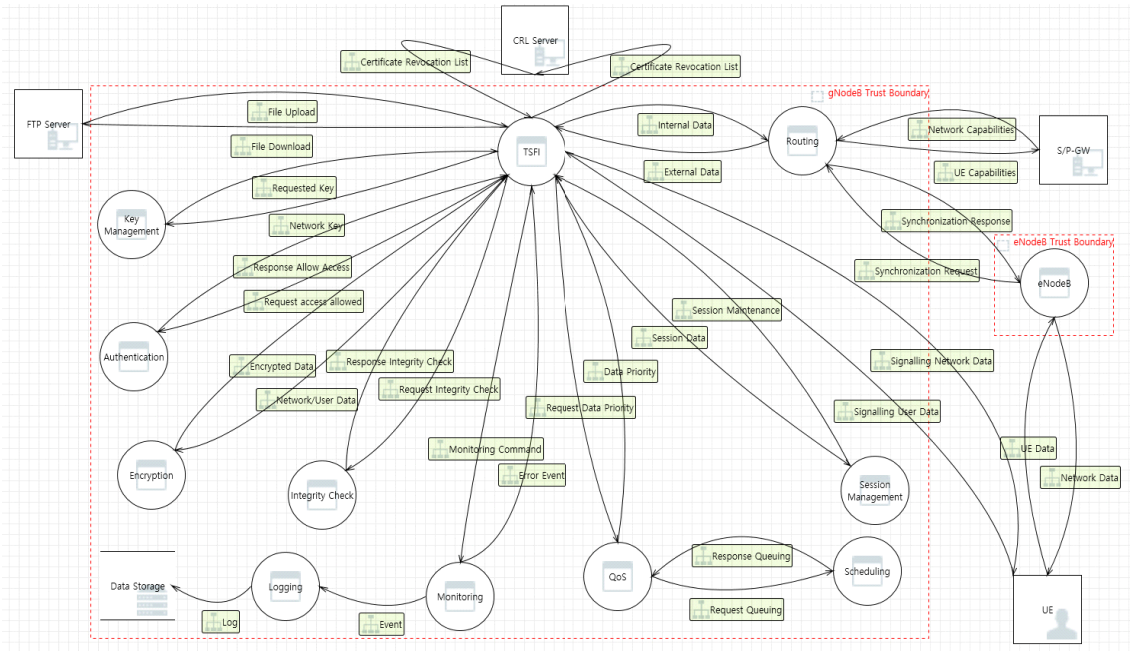


Fig. 4. 5G Base station DFD

Table 2. Attack Library for 5G Base station

Num	Category	Name	Author	Ref
1	conference	Battery Firmware Hacking	Charlie Miller	[33]
2	conference	Exploiting TrustZone on Android	Di Shen	[34]
3	conference	LTE Network Automation under Threat	Shaik, Altaf, and Ravishankar Borgaonkar	[35]
4	CVE	CVE-2015-0006	-	[36]
5	CVE	CVE-2015-5367	-	
6	CVE	CVE-2015-5368	-	
…	…	…	…	
39	CVE	CVE-2020-9495	-	
40	CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	-	[37]
…	…	…	…	
45	CWE	CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data	-	
46	paper	Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing	Mina Labib, Vuk Marojevic, Jeffrey H. Reed	[38]
…	…	…	…	[39-67]
78	paper	When Firmware Modifications Attack: A Case Study of Embedded Exploitation	Ang Cui, Michael Costello, Salvatore J. Stolfo	[68]
79	technical report	Downgrade Attack on TrustZone	Yue Chen1, Yulong Zhang, Zhi Wang, Tao Wei	[69]
80	technical report	Guide to LTE Security	NIST SP 800-187	[70]

최신 정보들을 수집해 데이터베이스화 해놓은 것을 의미한다. 공격라이브러리는 분석대상 시스템과 밀접한 취약점 및 공격 기법이 많이 수집될수록 발생 가능한 위협을 구체적으로 식별할 수 있도록 도와준다. 또한 공격라이브러리는 사람의 전문성에 따라 다른 결과가 도출되는 것이 아닌 일관된 결과를 도출할 수 있도록 도와준다. 공격라이브러리 수집은 새로운 위협이 발생하거나 발견되는 경우 위협모델링 전 과정에 걸쳐서 지속적으로 수행되어야 한다.본 논문에서는 컨퍼런스, CVE, CWE, 논문, 기술문서를 대상으로 취약점을 수집하여 공격라이브러리를 구축하였다. 구축된 공격라이브러리는 컨퍼런스 3건, CVE 36건, CWE 6건, 논문 33건, 기술문서 2건으로 총 80건의 취약점 정보들로 구성된다. 다음 Table 2.는 수집된 공격라이브러리를 나타낸다.

3.1.3 STRIDE

STRIDE는 위협모델링에서 사용되는 위협 분석 기법으로 데이터 흐름도의 각 구성요소에 존재할 수 있는 위협을 6가지의 범주로 식별 및 분류하여 분석할 수 있다. LINDDUN, Trike 등과 같이 다양한 위협 분석 기법 중에서 STRIDE는 소프트웨어 시스템의 보안 결함을 발견하기 위해 가장 대표적으로 사용되는 기법이다. STRIDE를 사용하여 위협모델링을 수행하는 경우는 실제 위협과 관련성이 떨어지는 위협(false positive)을 비교적 적게 도출하며, 5G 네트워크와 같은 시스템 분석에 성공적으로 적용되는 연구 결과가 있다[71-73]. 따라서 본 논문에서는 잘못된 위협 식별을 줄이고 분석대상 시스템에 성공적으로 적용된 선례가 존재하는 STRIDE를 사용한다. STRIDE는 소프트웨어에서 발생할 수 있는 6가지 보안 위협인 위장(spoofing), 변조

(tampering), 부인(repudiation), 정보 유출(information disclosure), 서비스 거부(denial of service), 권한 상승(elevation of privilege)으로 구성되며 각 위협은 6가지 보안속성인 인증(authentication), 무결성(integrity), 부인방지(non-repudiation), 기밀성(confidentiality), 가용성(availability), 인가(authorization)와 매핑된다.

STRIDE 위협 분석 기법은 상세하게 "STRIDE per Element"와 "STRIDE per Interaction"으로 구분된다. "STRIDE per Element"는 시스템의 각 구성요소의 위협을 식별하는 접근 방식이고 "STRIDE per Interaction"은 두 구성요소 간 발생하는 상호작용 관점에서 위협을 식별하는 접근 방식이다[74]. "STRIDE per Element"는 "STRIDE per Interaction"과 비교하여 각 시스템 전체 구성요소의 동작을 비교하기 때문에 더욱 복잡하다. 그러나 "STRIDE per Element"는 모델에서 식별한 위협이 실제 위협에 해당하는 True Positive 결과를 더 많이 도출한다[75, 76]. 따라

Table 3. STRIDE between DFD elements and Attack Library

Eleme-nts	Id	Name	Threat	Attack Library	Num
Entity	E1	UE	S	44, 60, 62, 64	T1
					T2
					T3
					T4
			R	68	T5
			D	50	T6
Entity	E2	S/P-GW	S	59	T7
			S	27	T8
			S	28	T9
			R	-	T10
Entity	E3	CRL Server	S	4	T11
			R	36	T12
Entity	E4	FTP Server	S	27	T13
			S	28	T14
			R	36	T15
Process	P1	4G Base station	S	3, 35	T16
			S	27	T17
			S	46, 60, 73	T18
			S	75	T19
			S	28	T20
			T	57, 61	T21
			T	25, 32, 56	T22
			T	3	T23
			R	68	T24
			I	26	T25
			I	78	T26
			I	51, 67, 69	T27
			I	61, 65	T28
			I	71, 76	T29
			I	40	T30
			I	42	T31
…					

Eleme-nts	Id	Name	Threat	Attack Library	Num
Process	P8	Key management	R	-	T119
			I	42, 60	T120
			D	43, 80	T121
			D	9, 17, 49	T122
			D	-	T123
			E	2, 79	T124
…					
Data store	D1	Data store	T	25	T152
			R	41	T153
			I	51	T154
			I	41	T155
			D	43	T156
			D	37, 74	T157
			D	-	T158
Data flow	DF1	User data	T	25, 28, 60	T159
			R		T160
			I	60, 71, 80	T161
			I	42	T162
			I	11	T163
			D	33, 34	T164
			D	43, 80	T165
			D	9, 22, 37	T166
			D	54, 71, 77	T167
			D	18, 63	T168
Data flow	DF2	Network data	T	28, 25	T169
			R	-	T170
…					
Data flow	DF12	File download	T	25	T231
			T	28	T232
			R	-	T233
			I	42, 60	T234
			D	43	T235

서 본 논문에서는 “STRIDE per Element”를 사용하여 구성요소의 위협을 식별하였다. Table 3은 식별한 위협을 나타낸다.

3.1.4 공격트리

공격트리는 시스템의 잠재적인 공격 벡터들을 활용하여 공격시나리오를 도출하기 위해 사용되는 기법이다[77]. 최상위 노드는 공격의 최종 목표를 나타내며 하위 노드는 AND, OR 관계를 통해서 상위 노드의 공격 목표를 달성하기 위해 필요한 단계별 세부 목표들을 나타낸다. 공격라이브러리에 수집된 보안 위협은 공격트리의 최하위 노드에 배치되어 실제 공격에서 어떻게 활용될 수 있는지 도식화를 통해 알 수 있다. 본 논문에서는 5G 네트워크 기지국에서 발생될 수 있는 공격 목표를 최상위 노드로 구성하여 공격트리를 구성하였다.

이에 본 논문에서 제시하는 5G 네트워크 기지국에 대한 공격트리의 최상위 노드는 시스템 데이터 삭제, 네트워크 서비스 거부, 시스템 파괴, 기지국 위장, 시스템 제어, 내부 시스템 변조에 총 6가지 공격 목표로 구성된다. 또한 위에서 설명한 바와 같이

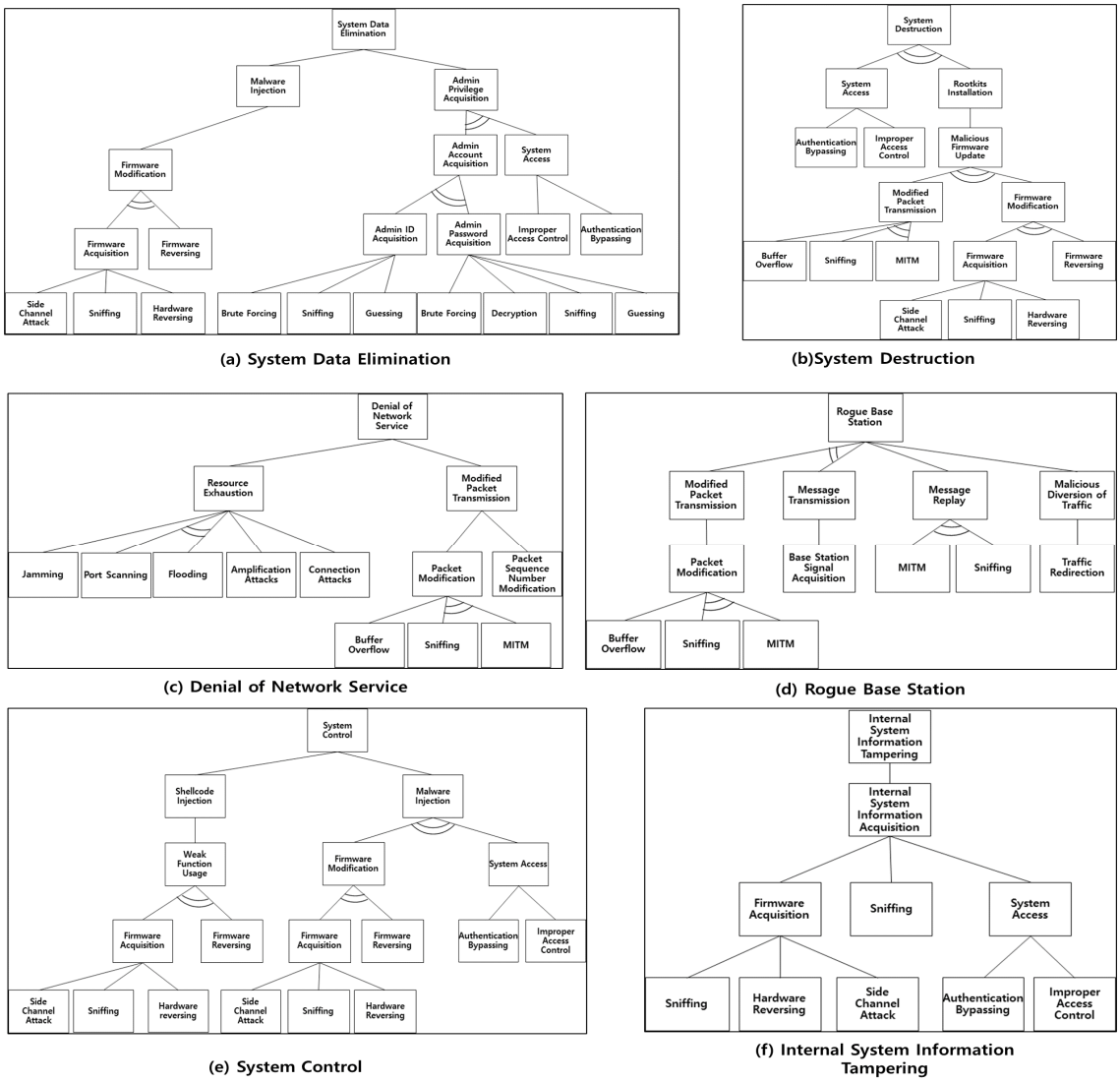


Fig. 5. Attack Tree for 5G base station

본 논문의 공격 트리는 6가지의 각 공격 목표를 달성하기 위해 허위 기지국 생성, 포맷 스트링 공격 등의 하위 노드로 구성된다. Fig.5.는 5G 네트워크 기지국에 대한 공격 트리를 나타낸다.

3.1.5 점검항목

점검항목은 위협모델링을 통해 식별한 위협과 공격시나리오를 완화할 수 있도록 점검해야 하는 내용을 도출한 것이다. 점검항목 작성 시에는 공격트리를 통해 도출된 공격시나리오에 대한 대응방법을 우선적으로 하되, STRIDE를 통해 식별된 잠재적 취약점까지 모두 고려되어야 한다. 따라서 본 논문에서는 공격트리에 포함되지 않은 STRIDE 위협을 상이한 항목간의 분류를 통해 총 12가지의 잠재적 잔존 위협을 도출했고 해당 항목에 대한 대응책과 점검항목, SFR(Security Functional Requirements) 매핑을 수행하였다. Table 4.는 위협과 공격트리에 대한 대응 방안과 해당하는 점검항목을 나타낸다.

3.1.6 보안기능요구사항 매핑

본 논문에서 공격트리를 통해 도출한 최하위 공격목표는 총 19가지로 도출된 최하위 공격 목표(공격트리의 리프 노드)를 완화하기 위한 보안기능요구사항을 도출해야한다. 먼저 각 공격에 대한 대응책을 도출하고 다음으로 해당 대응책이 실제로 구현되었는지 점검할 수 있는 점검항목을 도출하였다. 최종적으로는 도출된 점검항목과 공통평가기준 SFR을 매핑하는 것으로 5G 네트워크 기지국에 대한 보안기능요구사항을 도출하였다. 또한 우리는 공격 및 위협이 자산에 영향을 미치는 보안속성에 따라 기밀성(confidentiality), 무결성(integrity), 가용성(availability), 인가(authorization), 인증(authentication), 부인방지(non-repudiation)의 6가지 항목의 분류로 나타내었다. 다음 Table 4

Table 4. Mapping among Attack/Threat, Counter measures, CheckLists, and SFRs

Attack/Threat	C	I	A	Ar	Au	Nr	Countermeasure	CheckList	SFR
Flooding			O				Network Resource Management	Checking the error handling when receiving excessive communication data	FMT_MTD.2
									FDP_IFC.2
									FDP_IFF.1
									FPT_FLS.1
									FTA_SSL.3
								Check whether a mechanism to forcibly reduce the traffic exceeding the bandwidth is applied	FRU_FLT.2
Amplification Attack			O				Network Resource Management	Checking the error handling when receiving excessive communication data	FMT_MTD.2
									FDP_IFC.2
									FDP_IFF.1
									FPT_FLS.1
									FTA_SSL.3
								Check whether a mechanism to forcibly reduce the traffic exceeding the bandwidth is applied	FRU_FLT.2
…									
Signal Spoofing					O		Authentication	Checking for access to unauthorized signals	FIA_UAU.2
									FIA_UID.2
									FTA_TSE.1
									FMT_MSA.1

Attack/Threat	C	I	A	Ar	Au	Nr	Countermeasure	CheckList	SFR
Jamming			O				Physical Security Policy Compliance	Check whether the installed place is safe according to the physical security policy	FPT_PHP.3
Connection Attacks			O				Session Management	End unused sessions and check the number of concurrently connected sessions	FTA_SSL.3
									FTA_MCS.2
Traffic Redirection		O			O		Destination of Request Traffic Check	Check if the destination of response traffic for incoming traffic exists	FCO_NRR.1
									FCO_NRO.1
Port scanning	O						Unnecessary port removal, well-known port usage check	Check if unused and known ports are open	FDP_ACC.1
									FTP_ITC.1

는 공격트리에서 확인 가능한 공격 및 STRIDE의 잔존 위협과 관련된 보안속성, 그에 대한 대응책 및 점검항목, SFR 매핑을 나타낸다.

3.2 보증요구사항

보증요구사항은 개발된 IT 제품의 보안목적 만족 여부, 각 개발 단계 간 건전성(soundness) 만족여부 등과 같이 IT 제품이 견고하게 개발되었음을 보증하기 위한 요구사항이다. 보증요구사항은 EAL 등급에 따라서 만족하여야 하는 컴포넌트가 정해진다. ST의 EAL 등급은 일반적으로 해당 ST가 준수하고 있는 PP를 따르지만, 필요한 경우 제조사가 원하는 컴포넌트를 추가로 달성할 수 있다. 평가자는 PP와 ST에 서술된 EAL 등급을 기반으로 제조사의 제출물을 평가한다.

본 논문에서는 보증수준을 선정하기 위해서 기존에 CC 인증을 받은 제품 중 기지국과 유사한 제품군의 ST를 모두 수집하였다. 이후, 수집된 ST를 분석하여 제품들이 어느 정도의 보증수준을 달성하는지 조사하였다. 조사 결과 기존에 CC 인증을 획득한 유사장비의 최고 보증수준은 EAL4 등급에서 ALC.FLR.1을 추가한 EAL4+ 등급이었다. 이에 우리는 기지국에 대한 최소 보증수준을 유사장비가 획득한 최고 보증수준인 EAL4+로 선정하였으며, 통신장비 특성상 은닉채널(covert channel)에 대한 분석 수행이 필요하여 AVA_VAN.4와 ADV_IMP.2 컴포넌트를 추가로 달성하도록 선정하였다. 이때 추가된 컴포넌트 중 ADV_IMP.2는 ALC_CMC.5, ALC_DVS.2를 종속관계로 포함하고 있으므로 해당 컴포넌트들 또한 추가 보증요구사항으로 포함하였다.

3.2.1 Vulnerability analysis(AVA_VAN.4)

CC에서는 사용자가 강제적으로 허용되지 않은 신호 채널을 이용하여 TOE 내부에 접근할 수 있는 은닉 채널도 다루고 있다. 이러한 은닉 채널은 특성상 내부 데이터가 외부로 노출될 가능성을 가지고 있으며 공격자는 은닉 채널을 통해 백도어와 통신하여 시스템 정보를 수집할 수도 있다[78, 79]. 따라서 은닉 채널은 취약점 분석 시 반드시 고려되어야 하며 제거되어야 한다. EAL5 수준에서 다루고 있는 취약성 평가 보증 컴포넌트인 AVA_VAN.4에서 은닉 채널에 대한 분석을 다루기 때문에 우리는 해당 컴포넌트를 추가 달성하도록 요구조건으로 선정하였다[80]. AVA_VAN은 취약성 분석 패밀리로 해당 패밀리에 속한 컴포넌트의 숫자가 높을수록 TOE가 더욱 강력한 공격을 견딜 수 있음을 의미한다. AVA_VAN 패밀리에 속한 컴포넌트는 EAL 등급 및 공격 성공 가능성(attack potential) 점수와 직접적인 연관이 있다. 다음 Table 5는 AVA_VAN 컴포넌트에 따른 EAL 등급 및 공격 성공 가능성 점수를 나타낸다.

우리는 백도어 공격을 견디기 위해 해당 공격에 대한 공격 성공 가능성 점수를 계산하고 이를 견딜 수 있는 EAL 등급을 산정하였다. 다음 Table 6은 CC의 공격 성공 가능성 점수 계산 기준을 나타낸

Table 5. EAL and Attack Potential score according to AVA_VAN component

Component	EAL	Attack Potential
AVA_VAN.3	EAL 4	14 - 19
AVA_VAN.4	EAL 5	20 - 24
AVA_VAN.5	EAL 6, 7	25 이상

다. CC의 공격 성공 가능성 점수 계산 기준은 ▲공격자의 공격에 필요한 시간, ▲공격 기회, ▲공격자의 공격 기법에 대한 전문성, ▲공격에 필요한 장비의 전문성, ▲공격자의 TOE에 대한 지식의 총 5가지 항목으로 구성된다. 이에 우리는 공격자가 공격 성공을 위하여 최소 3개월 이상의 시간이 필요할 것으로 판단하였으며, 기지국의 특성상 공격자가 원하는 경우 언제든 휴대기기를 통해 접근할 수 있기 때문에 제한 없이 접근 가능한 것으로 판단하였다. 또한 우리는 공격자가 시스템 해킹에 대한 지식이 있으며, 기지국에 대한 공격 기법을 숙지하고 있다고 가정하여 공격자의 전문성을 숙련자 수준으로 선정하였다. 공격에 필요한 장비의 전문성은 기지국의 특성을 고려하여 공격자는 전문적인 장비를 이용하여 공격을 수행하는 것으로 선정하였다. 마지막으로 기지국의 경우 공개된 표준을 기반으로 구현되며 상세한 설계및 구현 내용은 외부에 공개되지 않기 때문에 공격자는 기지국에 대해 공개된 정보만 수집할 수 있다고 판단하였다. 최종적으로 우리는 백도어에 대한 공격 성공 가능성을 20점으로 산출하였으며 해당 공격 성공 가능성을 견디기 위해 필요한 취약성 분석 수준은 AVA_VAN.4에 해당한다. 앞의 두 가지 이유에 따라 최종적으로 5G 기지국은 AVA_VAN.4를 추가 달성해야 하는 컴포넌트로 선정하였다.

3.2.2 Impementation representation (ADV_IMP.2)

ADV_IMP는 TSF 구현물에 대해 평가자가 분석할 수 있는 형태로 제공할 것을 요구하는 패밀리다. 평가자가 제공받은 제출물은 실제 개발 인력이 사용한 소스코드와 같은 형태여야 한다. ADV_IMP 패밀리에 따라 제공받은 제출물은 구현과 설계의 일치성 입증, 취약성 분석과 같은 평가 수행에 필요한 근거 자료로도 사용된다.

우리가 제안한 취약성 분석 컴포넌트인 AVA_VAN.4는 종속관계로 ADV_IMP.1을 필요로 하고 있다. 하지만, ADV_IMP.1을 통해 평가자는 전체 구현물 중 일부분인 TSF에 대해서만 검증하기 때문에 ADV_IMP.1에 의해 검증되지 않은 부분에 설치된 백도어를 발견할 수 없다. 이에 따라 우리는 구현물 전체를 검증하여 백도어가 설치될 수 있는 모든 부분에 대해 검사할 수 있도록 ADV_IMP.2를 추가 달성해야하는 컴포넌트로 선정하였다.

3.2.3 Flaw remediation(ALC_FLR.1)

ALC_FLR은 개발자가 발견된 보안 결함을 추적 및 교정하고 이에 대한 정보를 사용자에게 제공할

Table 6. CC's attack probability score calculation criteria

Factor	Value	Factor	Value	Factor	Value
Elapsed Time		Window of Opportunity		Expertise	
〈= One day	0	Unnecessary/ unlimited access	0	Layman	0
〈= One week	1	Easy	1	Proficient	3
〈= Two weeks	2	Moderate	4	Expert	6
〈= One months	4	Difficult	10	Multiple experts	8
〈= Two months	7	Equipment		Knowledge of TOE	
〈= Three months	10				
〈= Four months	13	Standard	0	Public	0
〈= Five months	15	Specialised	4	Restricted	3
〈= Six months	17	Bespoke	7	Sensitive	7
〉 Six months	19	Multiple bespoke	9	Critical	11

것을 요구하는 패밀리다. 해당 패밀리를 통해 평가자는 제품의 배포 이후 사용자 또는 개발자에 의해 식별된 보안 결함을 개발자가 추적하고 적절한 조치를 취할 수 있도록 하는 절차와 매뉴얼이 수립되어 있는지 여부를 평가한다. 기지국의 경우 제품이 배포된 이후 폐기되기 전까지 서비스를 지속적으로 제공해야 한다. 이러한 기지국의 특성으로 인해 개발자는 배포 이전단계에서 발견하지 못한 제로데이(zero-day) 취약점들을 지속적으로 관리 및 대응해야 한다. 이러한 유지보수 단계는 제조사가 필수적으로 수행해야 하므로 우리는 ALC_FLR.1을 추가 달성해야 하는 컴포넌트로 선정하였다.

IV. 5G 기지국 보안성평가기준

본 장에서는 앞서 수행한 위협모델링 과정을 통해 도출된 보안요구사항을 바탕으로 공통평가기준의 보안기능요구사항과 보증요구사항의 형태로 5G 네트워크 기지국에 대한 보안성 평가기준을 제안한다.

4.1 보안기능요구사항

본 논문에서 최종적으로 도출한 5G 네트워크 기지국에 대한 보안기능 요구사항은 Table 7.과 같다. 도출된 보안기능 요구사항은 11개의 보안기능 클래스로 구성되며 보안감사(FAU, Security Audit) 클래스에서는 5개, 통신(FCO, Communication)

Table 7. Security Functional Requirements for 5G base station

Functional class	Security functional compontents	
Security audit	FAU_GEN.1	Audit data generation
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit receive
Communication	FCO_NRO.1	Selective proof of origin
	FCO_NRR.1	Selective proof of receipt
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Class FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITT.1	Basic internal transfer protection
	FDP_ITT.3	Integrity monitoring
	FDP_ITC.1	Import of user data without security attributes
	FDP_SDI.2	Stored data integrity monitoring and action
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UID.2	User identification before any action

Functional class	Security functional compontents	
Security management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_MTD.3	Secure TSF data
	FMT_SMR.1	Security roles
	FMT_SMF.1	Specification of Management Functions
Privacy	FPR_PSE.1	Pseudonymity
	FPR_UNO.1	Unobservability
Protection of the TSF	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_PHP.3	Resistance to physical attack
	FPT_RPL.1	Replay detection
	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Resource utilisation	FRU_FLT.2	Limited fault tolerance
TOE access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel

클래스에서는 2개, 암호 지원(FCS, Cryptographic Support) 클래스에서는 4개, 사용자 데이터 보호(FDP, User Data Protection) 클래스에서는 10개, 식별 및 인증(FIA, Identification & Authentication) 클래스에서는 5개, 보안 관리(FMT, Security Management) 클래스에서는 7개, 프라이버시(FPR, Privacy) 클래스에서는 2개, TSF 보호(FPT, Protection of the TSF) 클래스에서는 6개, 자원 활용(FRU, Resource Utilisation) 클래스에서는 1개, TOE 접근(FTA, TOE Access) 클래스에서는 3개, 안전한 경로/채널(FTP, Trusted Path/Channel) 클래스에서는 1개의 컴포넌트로 총 46개의 컴포넌트가 이에 해당된다.

4.2 보증요구사항

본 논문에서 제안하는 보증요구사항은 Table 8.과 같다. 해당 보증요구사항은 기지국과 유사한 네트워크 장비들의 ST에서 명시하고 있는 EAL 등급을 분석하여 이중 가장 높은 수준인 EAL 4+로 선정되었다. 공격자는 은닉 채널을 통해 백도어와 통신하여 시스템 정보를 수집할 수도 있음을 고려하여 ▲ADV_IMP.2, ▲ALC_CMC.5, ▲ALC_DVS.2, ▲ALC_FLR.1, ▲AVA_VAN.4 컴포넌트를 추가하여 최종적으로 도출하였다.

V. 결론 및 향후 연구

5G 네트워크는 4차 산업혁명을 위한 핵심 기술로 그 중요성은 점차 증가할 것으로 전망된다. 5G 네트워크 구조에서 기지국은 UE와 연결되어 서비스를 제공하는 기능을 수행한다. 따라서 기지국에 대한 공격이 발생하는 경우 사용자 및 서비스 전체에 대한 피해가 클 것으로 예상되며, 높은 보안보증수준을 필요로 한다. 본 논문에서는 안전한 5G 네트워크 환경을 위하여 기지국에 대한 보안기능요구사항과 보증요구사항을 제시하였다. 제시된 보안기능요구사항은 위협 분석 방법론인 위협모델링을 사용하여 체계적으로 도출되었으며, 보증요구사항은 백도어 이슈에 대응할 수 있도록 유사한 제품군의 보증수준을 분석하여 안전한 기지국에 필요한 적정 수준을 제시하였다. 제시된 요구사항은 5G 기지국을 설계 및 개발하고자 하

Table 8. Security Assurance Requirements for 5G base station

EAL4+ Security Assurance Compontents		Descriptions
Security Target Evaluation	ASE_CCL.1	Systematic security threat identification and security objective identification
	ASE_ECD.1	
	ASE_INT.1	
	ASE_OBJ.2	
	ASE_REQ.2	Derivation of security function requirements
	ASE_SPD.1	
	ASE_TSS.1	
Development	ADV_ARC.1	High/low level design and implementation
	ADV_FSP.4	
	ADV_IMP.2	
	ADV_TDS.3	
Guidance Documents	AGD_OPE.1	Describe safe installation and operation plans
	AGD_PRE.1	
Life-Cycle Support	ALC_CMC.5	Life cycle
	ALC_CMS.4	
	ALC_DEL.1	Configuration management
	ALC_DVS.2	
	ALC_TAT.1	
	ALC_LCD.1	
	ALC_FLR.1	Security flaw remediation
Tests	ATE_COV.2	High/Low level and interface test
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
Vulnerability Assessment	AVA_VAN.4	vulnerability analysis

는 단체에서 보다 안전한 네트워크 환경을 구성하기 위해 사용될 수 있다. 우리는 해당 연구를 통해 5G 네트워크 기지국 PP를 최초로 제안하였으며, 제안한 PP는 향후 5G 네트워크 기지국에 대한 보안성평가 기준으로 활용 될 수 있을 것으로 기대한다. 하지만 본 논문에서는 분석 범위를 5G 기지국으로 한정하여 보안성평가기준을 도출하였기 때문에 전체 5G 시스템을 평가할 수 있는 보안성평가기준이 없다는 한계점이 존재한다. 따라서 향후 연구로 5G 네트워크 전체 시스템을 평가하기 위해 시스템 구성요소를 통합한 전체 시스템을 평가할 수 있는 합성평가에 대한 연구가 필요하다.

References

〔1〕 ITU. "FG IMT-2020" (2015) 〔Online〕. Available: https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx, May 2020.

〔2〕 Lee Dong-myeon. "The basis of the 4th industrial revolution, intelligent hyper-connected network" TTA Journal ,2017

〔3〕 Park Seon-hoo. "The future of 5G mobile communication (5G) - Is it good news for small and medium-sized telecommunication equipment

companies?" IBK Economic Research Institute, 2018
〔4〕 Lee, Young-dae, et al. "Method and terminal for performing handover in mobile communications system of point-to-multipoint service." U.S. Patent Application No. 12/113,816.
〔5〕 Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu. "Security for 5G mobile wireless networks." IEEE Access. vol. 6, pp. 4850-4874, 2017.
〔6〕 Arfaoui, Ghada, et al. "A security architecture for 5G networks." IEEE Access, vol. 6, pp. 22466-22479, 2018.
〔7〕 Ahmad, Ijaz, et al. "Overview of 5G security challenges and solutions." IEEE Communications Standards Magazine, vol. 2, pp. 36-43, 2018.
〔8〕 Ferrag, Mohamed Amine, et al. "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes." Journal of Network and Computer Applications, vol. 101, pp. 55-82, 2018.
〔9〕 Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu. "Security requirement and standards for 4G and 5G wireless systems." GetMobile: Mobile Computing and Communications 22.1, pp. 15-20, 2018.
〔10〕 Sattar, Danish, et al. "Threat Modeling in LTE Small Cell Networks." IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2018.
〔11〕 Jover, Roger Piqueras, and Vuk Marojevic. "Security and protocol exploit analysis of the 5G specifications." IEEE Access, vol. 7, pp. 24956-24963, 2019.
〔12〕 Ahmad, Ijaz, et al. "Security for 5G and beyond." IEEE Communications Surveys & Tutorials. vol. 21, pp. 3682-3722, 2019.
〔13〕 Soldani, David. "5G and the Future of Security in ICT." IEEE International Telecommunication Networks and Applications Conference (ITNAC), 2019.
〔14〕 Cao, Jin, et al. "A survey on security aspects for 3GPP 5G networks." IEEE communications surveys & tutorials. vol. 22, pp. 170-195, 2019.
〔15〕 Tian, Zhihong, et al. "Automated attack and defense framework for 5G security on physical and logical layers." arXiv preprint arXiv: 1902.04009, 2019.
〔16〕 Fang, Dongfeng, and Yi Qian. "5G wireless security and privacy: Architecture and flexible mechanisms." IEEE Vehicular Technology Magazine, vol. 15, pp. 58-64, 2020.
〔17〕 Sun, Yanbin, et al. "Automated Attack and Defense Framework toward 5G Security." IEEE Network. vol. 34, pp. 247-253, 2020.
〔18〕 Dutta, Ashutosh, and Eman Hammad. "5G Security Challenges and Opportunities: A System Approach." IEEE 5G World Forum (5GWF). 2020.
〔19〕 3GPP. "Release 15" 〔Online〕. Available: https://www.3gpp.org/release-15
〔20〕 3GPP. "Release 17" 〔Online〕. Available: https://www.3gpp.org/release-17
〔21〕 ETSI. "System Architecture Evolution (SAE); Security architecture" 〔Online〕. Available: https://www.etsi.org/deliver/etsi_ts/133400_133499/ 133401/15.04.00_60/ts_133401v150400p.pdf
〔22〕 ETSI. "Security architecture and procedures for 5G system" 〔Online〕. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf, Jun, 2020
〔23〕 3GPP, "Security Assurance Specification

(SCAS) for the next generation Node B (gNodeB) network product class" [Online], Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3444

[24] GSMA. "5G Implementation Guidelines: NSA Option 3" [Online]. Available: https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/

[25] Ma Zhendong, Christoph Schmittner. "Threat modeling for automotive security analysis" Advanced Science and Technology Letters. vol. 139, pp.333-339, 2016.

[26] Montana State University. "Threat Modeling" [Online]. Available: https://www.cs.montana.edu/courses/csci476/topics/threat_modeling.pdf

[27] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.

[28] Caroline Mockel, Ali E. Abdallah. "Threat modeling approaches and tools for securing architectural designs of an e-banking application" IEEE International Conference on Information Assurance and Security. 2010.

[29] University of Missouri - St. Louis. "Data Flow Diagrams Examples" [Online] Available: http://www.umsl.edu/~sauterv/analysis/ dfd/dfd_intro.html

[30] Lucidchart. "What is a Data FDlow Diagram" [Online] Available: https://www.lucidchart.com/pages/data-flow-diagram

[31] Marwan Abi-Antoun, Daniel Wang, Peter Torr. "Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security" [Online] Available: http://reports-archive.adm.cs.cmu.edu/ anon/isri2006/CMU-ISRI-06-124.pdf, 2006

[32] Smartdraw. "Data Flow Diagram" [Online] Available: https://www.smartdraw.com/data-flow-diagram

[33] Miller, Charlie. "Battery firmware hacking." Black Hat USA (2011): 3-4.

[34] Shen, Di. "Exploiting TrustZone on android." Black Hat USA (2015).

[35] Shaik. Altaf, and Ravishankar Borgaonkar. "LTE Network Automation under Threat." (2018)

[36] MITRE. "CVE-2015-0006" [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0006

[37] MITRE. "CWE-200: Exposure of Sensitive Information to an Unauthorized Actor" [Online]. Available:

[38] Labib, Mina, Vuk Marojevic, and Jeffrey H. Reed. "Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing." IEEE Conference on Standards for Communications and Networking (CSCN), 2015.

[39] Behrad, Shanay, et al. "A new scalable authentication and access control mechanism for 5G-based IoT." Future Generation Computer Systems. vol. 108, pp. 46-61, 2020.

[40] Long, James, and John Roth. "A Novel Denial of Service Vulnerability in Long Term Evolution Cellular Networks.", 2019.

[41] Park, Yongsuk, and Taejoon Park. "A survey of security threats on 4G networks." IEEE Globecom workshops, 2007.

[42] Hu, Xinxin, et al. "A systematic analysis method for 5G non-access stratum signalling security." IEEE Access, vol. 7, pp. 125424-125441, 2019.

[43] Fievisohn, Lauren M. Wagoner. "A taxonomy of firmware extraction

methodologies." The University of Tulsa, 2014.
〔44〕 Gupta, Akhil, Rakesh Kumar Jha, and Sanjeev Jain. "Attack modeling and intrusion detection system for 5G wireless communication network." International Journal of Communication Systems. vol. 30, 2017.
〔45〕 Thomas, Sam Lloyd. "Backdoor detection systems for embedded devices." University of Birmingham, 2018.
〔46〕 Jover, Roger Piqueras, Joshua Lackey, and Arvind Raghavan. "Enhancing the security of LTE networks against jamming attacks." EURASIP Journal on Information Security, 2014.
〔47〕 Wang, Jiang, et al. "Firmware-assisted memory acquisition and analysis tools for digital forensics." IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011.
〔48〕 Basnight, Zachry H. Firmware counterfeiting and modification attacks on programmable logic controllers. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT, 2013.
〔49〕 Basnight, Zachry, et al. "Firmware modification attacks on programmable logic controllers." International Journal of Critical Infrastructure Protection. vol. 6, pp. 76-84, 2013.
〔50〕 Huang, Junying, et al. "Instruction Vulnerability Test and Code Optimization Against DVFS Attack." IEEE International Test Conference in Asia (ITC-Asia). 2019.
〔51〕 Dehnel-Wild, Martin, and Cas Cremers. "Security vulnerability in 5G-AKA draft." Department of Computer Science, University of Oxford, Tech. Rep (2018): 14-37.
〔52〕 Kim, Hongil, et al. "Touching the untouchables: Dynamic security analysis of the LTE control plane." IEEE Symposium on Security and Privacy (SP). 2019.
〔53〕 Bikos, Anastasios N., and Nicolas Sklavos. "LTE/SAE security issues on 4G wireless networks." IEEE Security & Privacy. vol. 11, pp. 55-62, 2012.
〔54〕 Fei, Teng, and Wenye Wang. "LTE is vulnerable: implementing identity spoofing and denial-of-service attacks in LTE networks." IEEE Global Communications Conference (GLOBECOM). 2019.
〔55〕 Chandavarkar, B. R. "Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE." IEEE International Conference on Contemporary Computing (IC3). 2015.
〔56〕 Tu, Guan-Hua, et al. "New security threats caused by IMS-based SMS service in 4G LTE networks." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.
〔57〕 Shaik, Altaf, et al. "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities." Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. 2019.
〔58〕 Schulz, Matthias, Daniel Wegemer, and Matthias Hollick. "Nexmon: Build your own WiFi testbeds with low-level MAC and PHY-access using firmware patches on off-the-shelf mobile devices." Proceedings of the 11th

Workshop on Wireless Network Testbeds, Experimental evaluation & CHaracterization. 2017.
〔59〕 Palmarini, Francesco. "Reverse Engineering Of Embedded Architectures." BS thesis. Università Ca'Foscari Venezia, 2015.
〔60〕 Saxena, Neetesh, and Narendra S. Chaudhari. "Prevention of SMS against Repudiation Attack over the GSM Network." Journal of Information Assurance & Security, pp. 155-166, 2013.
〔61〕 Chipounov, Vitaly, and George Candea. "Reverse engineering of binary device drivers with RevNIC." Proceedings of the 5th European conference on Computer systems. 2010.
〔62〕 Gupta, Shubham, Balu L. Parne, and Narendra S. Chaudhari. "Security vulnerabilities in handover authentication mechanism of 5G network." IEEE International Conference on Secure Cyber Computing and Communication (ICSCCC). 2018.
〔63〕 Lee, Gyuhong, et al. "This is your president speaking: spoofing alerts in 4G LTE networks." Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. 2019.
〔64〕 Luo, Shibo, et al. "Toward vulnerability assessment for 5G mobile communication networks." IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity). 2015.
〔65〕 Li, Xiaona, et al. "Vulnerability analysis and verification for LTE initial synchronization mechanism." IEEE Sarnoff Symposium. 2015.
〔66〕 Hofer, Mark, John McEachen, and Murali Tummala. "Vulnerability analysis of LTE location services." IEEE Hawaii International Conference on System Sciences. 2014.
〔67〕 Lichtman, Marc, et al. "Vulnerability of LTE to hostile interference." IEEE Global Conference on Signal and Information Processing. 2013.
〔68〕 Cui, Ang, Michael Costello, and Salvatore Stolfo. "When firmware modifications attack: A case study of embedded exploitation." Presented at the 20th Annual Network & Distributed System Security Symposium, 2013.
〔69〕 Chen, Yue, et al. "Downgrade attack on TrustZone." arXiv preprint arXiv:1707.05082, 2017.
〔70〕 Cichonski, Jeffrey, Joshua Franklin, and Michael Bartock. "Guide to LTE security." National Institute of Standards and Technology, No. NIST Special Publication (SP) 800-187 (Draft). 2016.
〔71〕 R.Scandariato, K.Wuyts, W.Joosen. "A descriptive study of Microsoft's threat modeling technique" Requirement Engineering. 2013.
〔72〕 N.Mead. "The Hybrid Threat Modeling Method", Carnegie Mellon University, Pittsburgh CMU/SEI-2018-TN-002, 2018.
〔73〕 Shevchenko, Nataliya, et al. "Threat modeling: a summary of available methods." Carnegie Mellon University Software Engineering Institute Pittsburgh United States 2018.
〔74〕 CyberArmyID. "Threat Modeling Using STRIDE" 〔Online〕 Available: https://owasp.org/www-pdf-archive//Threat_Modeling_Using_STRIDE_v1.1.pdf, 2017
〔75〕 khan, Rafiullah, et al. "STRIDE-based threat modeling for cyber-physical

systems." IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). 2017.

〔76〕 FFRI, Inc. "STRIDE Variants and Security Requirements-based Threat Analysis" 〔Online〕 Available: https://www.ffri.jp/assets/files/monthly_research/MR201610_STRIDE_Variants_and_Security_Requirements-based_Threat_Analysis_ENG.pdf, 2016

〔77〕 Saini, Vineet, Qiang Duan, Vamsi Paruchuri. "Threat modeling using attack trees" Journal of Computing Sciences in Colleges, pp. 124-131, 2008.

〔78〕 Salaün, M. "Practical overview of a Xen covert channel." Journal of Computer Virology and Hacking Techniques, pp. 317–328, 2010.

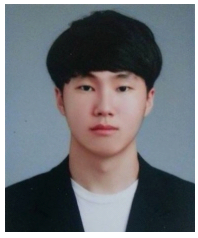
〔79〕 Tamer S. Fatayer, Sherif Khattab and Fatma A. Omara. "OverCovert: Using Stack-Overflow Software Vulnerability to Create a Covert Channel." IFIP International Conference on New Technologies, Mobility and Security, pp. 1-5, 2011.

〔80〕 David Martin. "AVA updates in v3.0" International Common Criteria Conference, 2005.

〈저자소개〉

홍 바 울 (Paul Hong) 학생회원
2010년 3월~2015년 2월: 홍익대학교 학사
2015년 3월~2017년 2월: 고려대학교 정보보호대학원 석사
2017년 2월~2020년 3월: 한국전자인증 개발팀
2020년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안공학, 위협모델링, 시큐어코딩, 소프트웨어 개발

김 예 준 (Yejun Kim) 학생회원
2019년 2월: 순천향대학교 정보보호학과 학사
2019년 3월~현재: 고려대학교 정보보호대학원 석박사통합과정
〈관심분야〉 보안공학, 리버스 엔지니어링, 위협모델링



조 광 수(Kwangsoo Cho) 정회원
2019년 2월: 호서대학교 컴퓨터공학과 학사
2019년 3월~2021년 8월: 고려대학교 정보보호대학원 석사
2021년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안공학, RMF A&A, 시큐어코딩, 소프트웨어 개발

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보보호학회 이사
2011년~현재: 고려대학교 정보보호대학원 정교수
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고려대학교 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2019년~현재: 중소벤처기업부 규제특례 심의위원
2020년: 합동참모본부 정책자문위원회 자문위원
2020년~현재: 해군발전자문위원회 자문위원
2020년~현재: 서울특별시 스마트도시위원회 위원
2021년~현재: 사이버작전사령부 자문위원
〈관심분야〉 보안공학 및 보안내재화 방법론, 자동차 및 무인이동체 보안성 평가 인증, RMF A&A, 암호학 및 블록체인