정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

서비스 융합 네트워크를 위한 5G의 보안 전략: EAP 인증 프레임워크

윤 건*, 박 훈 용*, 유 일 선*

요 약

보안은 5G 이동통신 네트워크의 성공적인 정착을 위한 필요충분조건이다. 5G 보안의 중요한 표준으로 3GPP (3rd Generation Partnership Project)의 보안 담당 워킹그룹인 SA3는 3GPP 5G 보안구조를 제시하였다. 특히, 3GPP 5G 보안구조는 Extensible Authentication Protocol (EAP) 인증 프레임워크를 채택함으로써 이기종의 다양한 인증 기법과 자격증명을 용이하게 포용할 수 있는 유연성을 갖추었다. 서비스 융합 네트워크를 지향하는 5G의 비전을 고려할 때, EAP 인증 프레임워크는 보안측면에 있어서 매우 중요한 전략이라고 볼 수 있다. 따라서, 본 논문에서는 3GPP 5G 보안구조를 위한 EAP 인증 프레임워크를 고찰한다. 이를 위해, 1차 인증을 위한 EAP 기반의 인증 프로토콜 EAP-AKA'을 면밀히 검토하면서 1차 인증에서의 EAP 인증 프레임워크 적용방안을 분석한다. 아울러, 2차 인증을 위한 EAP 인증 프레임워크의 적용과 네트워크 슬라이싱 (Network Slicing)과의 연동을 살펴본다.

Ⅰ. 서 론

2019년 4월3일 23시, 국내 이동통신3사에 의해 세계 첫 5G 상용화 서비스[1]가 시작되면서 본격적인 5G 시대가 도래하였다. 5G 이동통신 네트워크는 20Gbps급의 초고속, 1km^2 면적당 100만개 이상 기기에 대한 초연결, 1ms내의 초저지연의 요구사항을 만족하며, 최초의 서비스 융합 이동통신 네트워크로서 폭넓은 응용 스펙트럼과 상상이상의 혁신을 우리 생활에 가져다 줄 것으로 기대된다.

한편, 이러한 혁신을 가능하게 하는 5G 이동통신 기술의 진화는 새롭고 다양한 보안위협과 공격을 수반할 것으로 예상된다. 따라서, 보안은 5G 기술의 성공적인 정착을 위해 가장 중요한 요소로 간주된다.

5G 보안을 위한 첫 걸음으로 이동통신 네트워크의 보안을 담당하는 워킹그룹인 3GPP (3rd Generation Partnership Project)의 SA3에서는 관련 표준을 진행하면서 3GPP 5G 보안 구조를 제안하였다 [1][2]. 3GPP 5G 보안 구조는 다음과 같은 중요한 특징을 갖는다.

- 새로운 인증 프레임워크: 3GPP 5G 보안 구조의 인증절차는 현재 정보통신 환경에서 널리 사용되는 Extensible Authentication Protocol (EAP)[3]을 지원하는 인증프레임워크로서 설계되었다. 이처럼, 3GPP 5G의 보안구조는 EAP를 전격적으로 채택함으로써 SIM 카드기반의 공유 비밀키 이외에 다양한 자격증명 (credential) 및 인증기법을 지원하는 유연성을 갖추게 되었고, 이는 폭넓은 응용 서비스와의 융합을 보다 용이하게 하였다.
- 프라이버시 강화: 5G 보안구조는 공개키 암호화 기법을 적용하여 단말장치의 식별자를 암호화한 형태로 전송되도록 함으로써 프라이버시를 강화하였다.
- 서비스 기반의 구조 및 상호연동 보안: 5G 네트워크는 네트워크 가상화 기술을 기반으로 네트워크구조에 있어서 패러다임의 전환을 이끌었다. 특히, 서비스 기반의 구조 (SBA: Service Based Architecture)를 도입함으로써 하나의 네트워크 객체가 포함하는 여러 기능 하나하나를 개별 서비스로 전환하고, 각 서비스 (NF: Network Function로 불림)의 인터페이스를 Service-based Interfaces (SBI)로 오픈함으로써 다른 네트워크 객체와의 상호연동을 체계화 하였다.

* 순천향대학교 정보보호학과 모바일인터넷보안 연구실 (theldbsrjs@gmail.com, hoon4569@gmail.com, ilsunu@gmail.com)

1) “한국, 5G 서비스 세계 최초 상용화,” 한국경제, 2019년 4월4일, https://www.hankyung.com/it/article/2019040484531

2) https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

5G 보안구조의 핵심 NF들은 NF 사이의 상호연동을 보호하기 위해 IPSec이외에 Transport layer security (TLS)[4]와 OAuth 2.0[5]을 지원한다. 또한, 도메인이 다른 NF들의 상호연동을 지원하기 위해 보안 프록시 역할을 하는 Security Edge Protection Proxy (SEPP)가 제안되었다. SEPP는 소속 도메인 네트워크의 경계에 위치하고, 다른 도메인의 SEPP들과 연동함으로써 도메인을 넘어서는 NF간 상호작용을 보호한다.

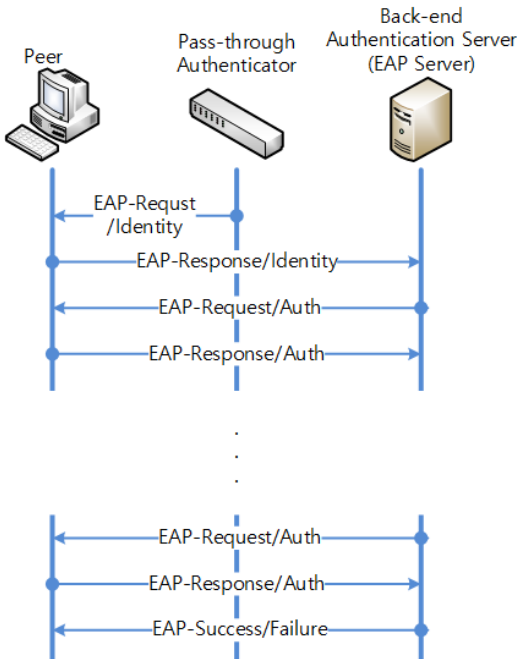
5G는 최초의 서비스 융합 이동통신 네트워크로 네트워크 영역내에 응용 서비스를 위한 엣지 클라우드를 도입하고, 네트워크 가상화 기술을 바탕으로 네트워크 슬라이싱 (Network Slicing)을 제공함으로써 각 응용 서비스에 특화된 맞춤형 네트워크를 효과적으로 지원할 수 있다. 이러한 서비스 융합 네트워크를 성공적으로 구현하기 위해 앞서 언급된 것처럼 3GPP 5G 보안구조는 EAP 기반의 인증프레임워크를 채택하여 다양한 인증 기법과 관련 자격증명을 지원할 수 있는 유연성을 갖추었다. 예를 들어, 5G 기반의 스마트팩토리 응용 서비스를 지원하기 위해 스마트팩토리의 보안요구사항을 고려하여 3GPP 5G 보안구조의 기본 인증기법인 5G AKA[1] 혹은 EAP-AKA' [1, 6]이 아닌 EAP-TLS[8]를 채택할 수 있다. 즉, 스마트팩토리 시스템내 단말장치는 EAP-TLS를 통해 5G 네트워크와 상호인증 및 키 교환을 수행할 수 있다.

따라서, EAP 인증 프레임워크는 서비스 융합 네트워크를 위한 5G 핵심전략으로 중요하다. 이에 본 논문에서는 3GPP 5G 보안구조를 위한 EAP 인증 프레임워크를 검토 및 고찰한다.

본 논문의 구성은 다음과 같다. 2장에서 EAP 인증 프레임워크를 검토하고, 3장에서 EAP 기반의 1차 인증 (Primary Authentication) 기법인 EAP-AKA'과 인증 이후 NAS (Non Access Stratum) 및 AS (Access Stratum) 보안설정 과정을 면밀히 살펴본다. 4장에서는 이동단말과 응용서비스 사이의 보안을 위한 2차 인증 (Secondary Authentication)을 EAP 관점에서 계사하고, 5장에서 본 논문의 결론을 제시한다.

Ⅱ. EAP 인증 프레임워크

인증 및 보안 관리 처리를 통합함에 있어 여러 액세스 기술과 인증 프로토콜을 지원하는 프레임워크는 필수적 요소이다. 인증 프레임워크를 통해 보안 관리의 복잡성은 줄이고, 서로 다른 액세스 접근을 유용하게 할 수 있다. 이는 보안 컨텍스트를 다른 액세스 기술에 적용할 때 대기 시간을 줄이는 이점을 갖는다. EAP는 이러한 요구 사항을 만족하는 인증 프레임워크 기술 중 하나이다[3]. EAP의 장점 중 하나인 확장성은 EAP-AKA, EAP-TLS 등 다양한 인증 기법들을 지원한다. 이처럼 타사 서비스로 인증 범위를 쉽게 확장하는 프레임워크에는 EAP가 적합하다. 5G 또한 다양한 응용서비스에 특화된 보안을 제공하기 위한 핵심 인증 프레임워크로 EAP를 채택하였다. 이를 실현하기 위해서 5G에서는 1차 인증을 위해 4G의 EPS-AKA를 계승하는 5G AKA 이외에 EAP 기반의 EAP-AKA'을 지원한다. 2차 인증(Secondary Authentication)을 위해서는 EAP 기반 인증 기법의 사용을 권고한다. 결론적으로 EAP의 채택은 5G가 이동통신망 외 스마트 홈, 스마트 팩토리와 같은 다양한 응용 서비스의 인증을 지원할 수 있을 것으로 예상된다.



〔그림 1〕 EAP 인증 프레임워크

EAP 인증 프레임워크는 [그림 1]과 같이 3개의 객체 즉, 피어, 인증자, 백-엔드 인증서버로 구성되고, 백-엔드 인증서버를 기반으로 피어와 인증자가 (상호)인증 및 키교환을 하도록 지원한다. 이 때, 피어는 인증자에게 응답하는 역할을 수행하고, 인증자는 인증을 시작한다. 백-엔드 서버는 인증자에게 인증 서버를 제공한다. EAP 프로토콜은 EAP Request/Response 메시지를 중심으로 다음과 같이 수행된다:

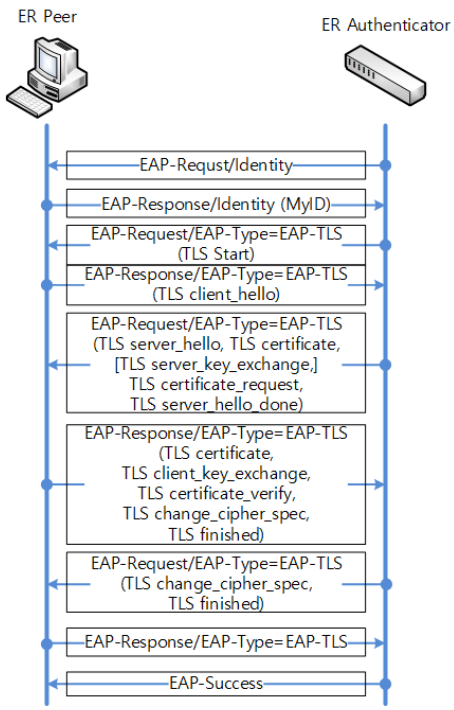
(1) 인증자가 EAP-Request/Identity를 통해 ID를 요청하는 것으로 EAP의 인증 절차가 시작된다.
(2) 피어는 인증자가 요청한 ID값을 전송하고 백-엔드 인증 서버에 접속을 요청한다.
(3) 이후 가능한 후보 중에서 선택된 인증 기법(예 : EAP-TLS)에 따라 EAP 인증 절차를 수행한다.
(4) 백-엔드 서버는 인증 절차가 종료되면, 결과가 성공적으로 마무리될 경우 Success 메시지를 송출, 실패로 마무리될 경우 Failure 메시지를 송출한다.

EAP 인증 프레임워크에 대한 이해를 넓히기 위해 대표적인 인증 기법인 EAP-TLS와 EAP 초기 인증(Initial Full Authentication) 후 후속 인증을 최적화 하는 ERP를 소개함으로써 본 장을 마무리한다.

2.1. EAP-TLS

EAP-TLS(Transport Layer Security)는 EAP 프레임워크에서 TLS를 기반으로 하는 프로토콜이다[8]. [그림 2]는 EAP-TLS의 절차를 나타낸다.

(1) 프로토콜은 인증자가 피어에게 EAP-Request/Identity 메시지를 전송함과 동시에 시작된다.
(2) 피어는 사용자 아이디가 포함된 EAP-Response/Identity 메시지로 응답한다.
(3) EAP 서버는 피어의 아이디를 받으면 EAP-Type=EAP-TLS이고 Start 비트가 세팅된 EAP-Request 메시지로 응답한다.
(4) 피어는 EAP-Type=EAP-TLS인 EAP-Response 메시지를 전송함으로써 본격적으로 EAP-TLS 프로토콜을 시작한다. 이 때, 메시지의 데이터 필드는 TLS client_hello 핸드셰이크 메시지가 포함된 하나 이상의 TLS 레코드 레이어 포맷의 TLS 레코드로 캡슐화 된다.



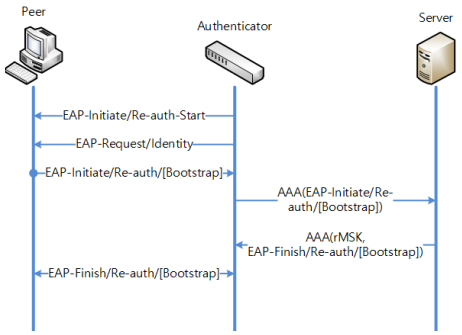
〔그림 2〕 EAP-TLS 프로토콜

(5) 인증자는 EAP-Request(EAP-Type=EAP-TLS) 메시지를 전송함으로써, TLS 인증 프로토콜의 다음 단계를 수행한다. 이 메시지의 데이터 필드는 하나 이상의 TLS 레코드로 캡슐화되고, TLS server_hello 핸드셰이크 메시지를 포함한다. 이후, 피어와 인증자는 EAP-Request/Response 메시지를 바탕으로 TLS 프로토콜의 잔여 절차를 수행한다. 여기서 성공적으로 인증이 되면 서버에서 EAP-Success 패킷을 보내며 인증이 완료된다[4].

2.2. ERP

ERP(EAP Re-authentication Protocol)는 피어와 인증자 사이의 수행된 초기 EAP 인증의 보안 문맥(Security Context)을 기반으로 향후 발생하는 후속 인증을 최적화하기 위해 제안된 프로토콜이다[9].

[그림 3]은 ERP 프로토콜을 도식화하였다. ERP는 피어와 서버로 하여금 이전의 EAP 초기 인증으로부터 얻은 보안 문맥(즉, 마스터 세션키 등)을 소유하고 있는지 상호 검증하도록 하고, 이를 바탕으로 피어와 인증자



〔그림 3〕 ERP 프로토콜

사이의 보안 연결을 수립하도록 한다. 특히 ERP는 피어와 서버사이의 단일 라운드-트립 메시지 교환을 통해 효율적으로 인증을 수행하는 장점을 갖는다. ERP의 수행은 다음과 같다:

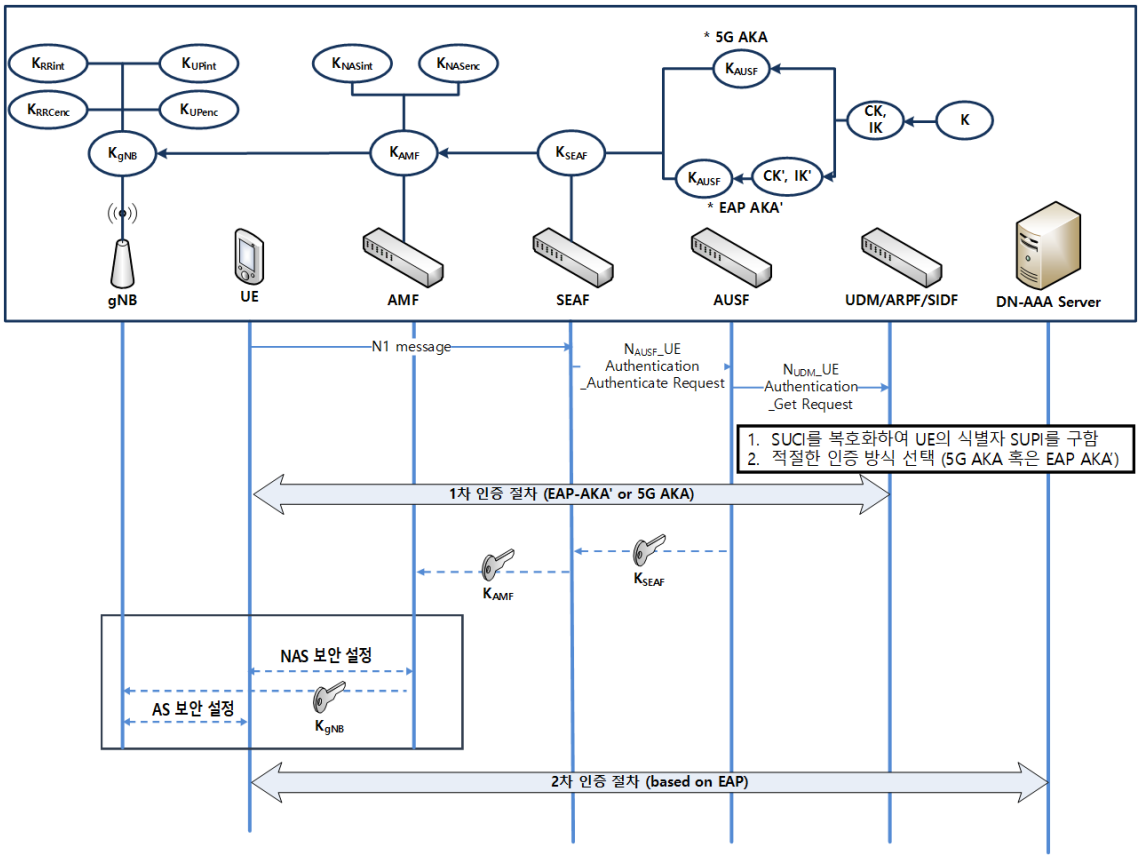
(1) EAP-Initiate/Re-auth-Start 메시지를 전송한다. 이 메시지는 피어에게 인증자가 ERP를 지원한다고 알려준다.
(2) 이후 설정된 시간 동안 잠시 기다린 후 응답이 없으면 피어에게 EAP-Request/Identity 메시지를 전송한다.
(3) 피어는 EAP-Initiate/Re-auth 메시지를 전송하여 ERP 교환을 시작할 수 있다. 피어는 이 메시지에 서버의 도메인을 식별하기 위한 keyName-NAI와 메시지의 무결성을 보호하기 위한 rIK, 그리고 재전송 공격을 막기 위한 시퀀스 넘버를 포함하여 보낸다.
(4) 인증자는 keyName-NAI를 참조하여 수신 메시지를 적절한 서버에게 전달한다. 서버는 수신받은 keyName-NAI를 무결성 키인 rIk를 찾는데 사용한다.
(5) 서버는 rIk의 소유 증명과 메시지의 적시성을 검증한 후에 새로운 마스터 세션키 rMSK를 생성한다. 서버는 피어의 메시지에 응답하기 위해 EAP-Finish/Re-auth 메시지를 전송한다. 여기서, 메시지 무결성 보호키 rIK로 보호되며 서버는 rMSK를 이 메시지와 함께 인증자로 전송한다.
(6) 피어는 시퀀스 넘버와 메시지의 무결성을 검증한다. 그 후 EAP-Finish/Re-auth 메시지의 시퀀스 넘버를 사용하여 rMSK를 계산한다. 이 시점부터 보안 연결이 수립된다.

Ⅲ. 5G의 1차 인증 및 NAS/AS 보안설정

5G의 인증은 이동통신망에 대한 1차 인증과 응용 서비스에 대한 2차 인증으로 분류된다. 본 장에서는 1차 인증을 다룬다. 1차 인증의 주 목적은 UE(User Equipment)와 5G 코어 네트워크(5G Core Network) 사이의 상호인증 이다[1]. 5G 네트워크의 기능과 역할은 [표 1]과 같다. 5G 인증 절차를 도식화한 [그림 4]와 같이 5G 네트워크를 구성하는 엔티티 중 SEAF, AUSF, ARPF가 인증 절차에 참여한다. 그리고 1차 인

〔표 1〕 5G 네트워크 엔티티의 기능 및 역할

엔티티	기능 및 역할
UE (User Equipment)	- 이동 단말 장치
gNB (Next Gen Node Base Station)	- Access Network의 최전방에 존재하는 5G 기지국
AN (Access Network)	- 이동단말의 5G 이동통신 망 접속을 지원하는 무선 네트워크
UPF(User Plane Function)	- UE가 접속된 Serving Network에서 사용자 영역 데이터 처리 담당
SMF (Session Management Function)	- 세션 설정 수정 및 해제 관리 - UE의 IP 주소 할당 및 관리 - 로밍 기능
PCF (Policy Control Function)	- 네트워크 제어를 위해 프레임워크 지원
SEAF (Security Anchor Function)	- UE와 5G 네트워크 사이의 보안 앵커로서 UE가 소속된 Serving Network에 존재하고, 1차 인증 후 UE와 네트워크 사이의 보안설정을 수행함
AUSF (Authentication Server Function)	- 5G의 홈 네트워크에 존재하고, ARPF와의 유기적인 연동을 통해 1차 인증과정에서 UE와의 상호인증 및 키교환을 주도함
ARPF (Authentication Credential Repository and Processing Function)	- UE의 인증정보를 가지고 있으며 인증 서버역할을 수행



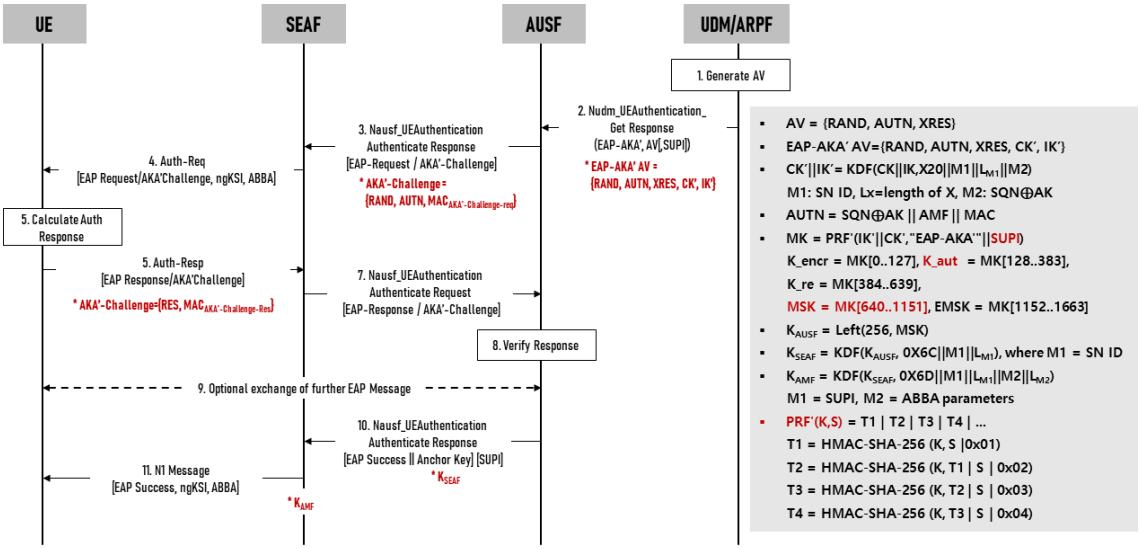
〔그림 4〕 5G 인증 절차

증 절차를 통해 서빙 네트워크 SEAF에 제공되는 앵커 키인 K_{SEAF}를 최종적으로 파생한다. [그림 4]의 절차대로 UE는 SEAF에 접속하여 메시지를 전송함으로써, 인증을 시작한다. UE의 인증 요청은 SEAF에 의해 AUSF에게 전달되고 최종적으로 UDM/ARPF/SIDF에 도달한다. 이 때 UE의 암호화 된 식별자 SUCI가 수신되면 SIDF는 이를 복호화하여 SUPI를 생성하고, UE를 식별한다. 최종적으로 UDM/ARPF는 UE의 SUPI를 참조하여 1차 인증을 위한 인증 기법을 선택한다. 5G의 1차 인증을 위해 채택된 프로토콜은 EAP 기반의 EAP-AKA'과 EPS-AKA를 계승한 5G AKA가 있다. 인증 기법이 선택되면 UE와 AUSF는 ARPF를 의존하여 상호 인증 및 키교환을 수행한다. 1차 인증의 결과로 앵커키 K_{SEAF}가 생성되고 이는 AUSF로부터 SEAF로 전달된다. 이후 K_{SEAF}에서 파생된 세션키들을 통해 NAS/AS 보안 설정이 차례대로 수행된다. 위 과정은 3.1, 3.2절을 통해 상세히 설명된다.

3.1. EAP-AKA'

EAP-AKA'은 EAP-AKA의 개정된 새로운 EAP 기법이다[6][7]. EAP-AKA'은 기존 AKA 알고리즘(그림 6 참조)의 CK 및 IK, AK 그리고 순차번호(Sequence Number)를 서빙 네트워크 아이디에 바인딩함으로써, CK'와 IK'를 생성하고 이를 바탕으로 마스터 키블럭을 생성하여 K_{AUSF}를 비롯한 여러 세션키를 생성한다[10]. 또한, 해시 함수는 SAH-256으로 강화하였다[11]. [그림 5]는 EAP-AKA'의 절차를 나타낸다.

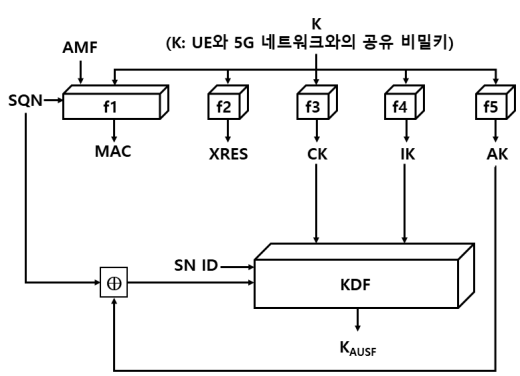
(1) UDM/ARPF는 UE와의 공유 비밀키와 AKA 알고리즘을 통해 인증 벡터 AV를 생성한다. 이후 CK 및 IK, AK 그리고 SQN(순차번호)을 SN ID(서빙 네트워크 아이디)에 바인딩함으로써 CK'와 IK'를 계산하고 EAP-AKA' AV={RAND, AUTN, XRES, CK', IK'}를 작성한다.



〔그림 5〕 EAP-AKA′ 절차

(2) UDM/ARPF는 (1)에서 작성한 인증 벡터 EAP-AKA' AV를 AUSF에 전송한다. 이때, 이전 메시지에서 SUCI가 포함되었다면 SUPI를 함께 전송한다.

(3) AUSF는 EAP-AKA' AV의 CK' 및 IK'와 UE의 SUPI를 통해 마스터 키블럭 MK를 생성하고 이로부터 마스터 세션키 MSK를 추출한 후 KAUSF를 계산한다. 또한 같은 방식으로 MK로부터 메시지 인증키 K_aut를 추출하고 이를 활용하여 AKA'-Challenge={RAND,AUTN,MAGAKA'-Challenge-Req}를 위한 메시지 인증 코드 $MAG_{AKA'\text{-}Challenge\text{-}Req}$를 계산한다. 이후 AKA'-Challenge는 AUSF에 의해 SEAF로 전달된다. 아울러 AUSF는 KAUSF를 SN ID와 바인딩하여 앵커키 K_{SEAF}를 생성하고 (10)번 단계에서 SEAF에게 전달하기 전까지 보관한다.



〔그림 6〕 AKA 알고리즘

(4) SEAF는 수신 메시지 3에 보안 문맥 식별자 ngKSI와 매개변수 ABBA를 포함하여 메시지 4를 작성한 후 UE에게 전송한다.

(5) 메시지 4의 수신 후 UE는 EAP AKA' AV에 포함된 인증토큰 AUTN에서 SQN의 적시성을 검증함과 동시에 MAC값을 통해 5G 코어망을 인증한다. 아울러 UDM/ARPF와 동일한 방식으로 CK'와 IK'를 생성하고 이를 바탕으로 K_{AUSF}와 앵커키 K_{SEAF} 그리고 메시지 인증키 K_aut를 파생한다. 특히 K_aut를 사용하여 메시지 인증 코드 $MAG_{AKA\text{-}Challenge\text{-}Req}$값을 검증함으로써 AKA'-Challenge의 무결성을 확인함과 동시에 AUSF가 성공적으로 마스터 키블럭을 생성했다는 믿음을 확보한다.

(6) EAK-AKA' AV의 검증이 성공적이면, UE는 RES값을 생성 후, RES값과 메시지 인증 코드 $MAC_{AKA'\text{-}Challenge\text{-}Res}$(K_aut로 계산됨)로 구성된 AKA'-Challenge를 작성하고 이를 포함하는 메시지 6을 SEAF에게 전달한다.

(7) SEAF는 메시지 6을 메시지 7의 형태로 변환시켜 AUSF에 전송한다.

(8) 메시지 7의 수신 후, AUSF는 K_aut를 사용하여 $MAC_{AKA'\text{-}Challenge\text{-}Res}$를 검증하고, XRES값과 RES값

을 비교함으로써 UE를 인증한다. 이후 AUSF는 메시지 10을 통해 K_{SEAF}와 SUPI를 전달한다.

(9) SEAF는 K_{SEAF}로부터 K_{AMF}를 생성한 후, AMF에게 전달하여 이후 UE와 AMF 사이에 NAS 보안 설정이 진행되도록 지원한다. 또한 AMF는 K_{AMF}로부터 K_{gNB}를 파생하여 gNB(UE가 현재 접속되어 있는 액세스 네트워크에 존재하는)에게 전달함으로써 gNB와 UE가 AS 보안 설정을 할 수 있도록 지원한다.

(10) 마지막으로 UE는 인증 성공을 암시하는 EAP Success메시지를 ngKSI와 ABBA 값들과 함께 UE에게 전달함으로써 EAP-AKA'을 종료한다.

3.2. NAS/AS 보안 설정

EAP AKA'이 성공적으로 종료되면 UE는 AMF와의 무선 구간(NAS)과 gNB와의 유선 구간(AS)을 보호하기 위한 보안 설정을 수행한다.

3.2.1. NAS 보안 설정

NAS 보안 설정은 무선 구간에서의 UE와 AMF 간 시그널링 메시지를 안전하게 전달하는 것을 목표로 한다.

(1) AMF는 UE security capability에 포함된 보안 알고리즘(즉, UE가 지원 가능한) 중 NAS 시그널링 메시지 보호를 위한 무결성 및 암호화 알고리즘을 선택한다. 또한 K_{AMF}로부터 무결성키인 K_{NASint}와 암호화키 K_{NASenc}를 파생하고 이 중 K_{NASint}를 앞서 선택한 무결성 알고리즘을 적용하여 NAS 메시지 인증 코드(NAS-MAC)를 생성한 후 NAS Security Mode Command 메시지를 UE에게 전송한다.

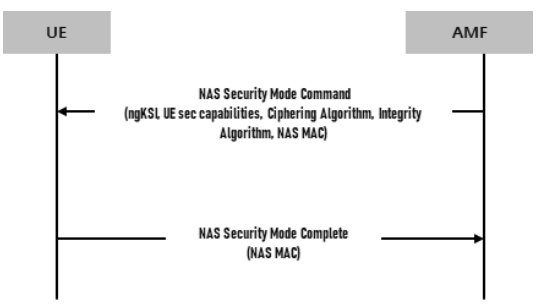
(2) UE는 AMF로부터 메시지을 수신 한 뒤, 메시지에 포함된 보안 알고리즘과 K_{AMF}로부터 K_{NASint}와 K_{NASenc}를 계산한다. 또한 무결성 알고리즘과 K_{NASint}를 통해 메시지에 무결성을 검증한다. K_{NASenc}를 적용하여 암호화 한 후, K_{NASint}를 적용해 메시지 인증 코드를 생성한다. 이 후 암호화 된 메시지에 NAS-MAC을 포함한 뒤 AMF에 전달한다. AMF가 NAS Security Mode Complete 메시지를 수신하고, 두 가지의 키를 사용함으로써 무결성 검증 및 복호화를 수행하면 보안 설정을 마친다.

3.2.2. AS 보안 설정

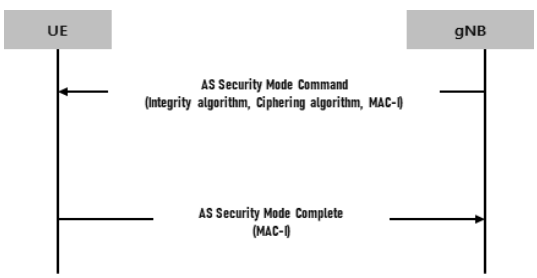
NAS 보안 설정을 마치면, UE와 gNB 간 AS 보안 설정 절차가 진행된다. 이는 RRC(Radio Resource Control) 시그널링 메시지와 패킷을 안전하게 전달하기 위한 과정이다. AS 보안 설정에 이용되는 키는 K_{gNB}로부터 파생되며 무결성키 K_{RRCint}와 암호화키 K_{RRCenc}로 구성된다.

(1) gNB는 AS 보안 알고리즘(K_{gNB}와 함께 AMF로부터 전달된)을 적용하여 K_{gNB}로부터 RRC 시그널링 메시지에 적용될 무결성 키 K_{RRCint}와 암호화 키 K_{RRCenc}를 파생한다. 그리고 AS Security Mode Command 메시지에 K_{RRCint}를 적용하여 MAC-I(Message Authentication Code for Integrity)를 생성하고 메시지와 함께 UE에게 전송한다.

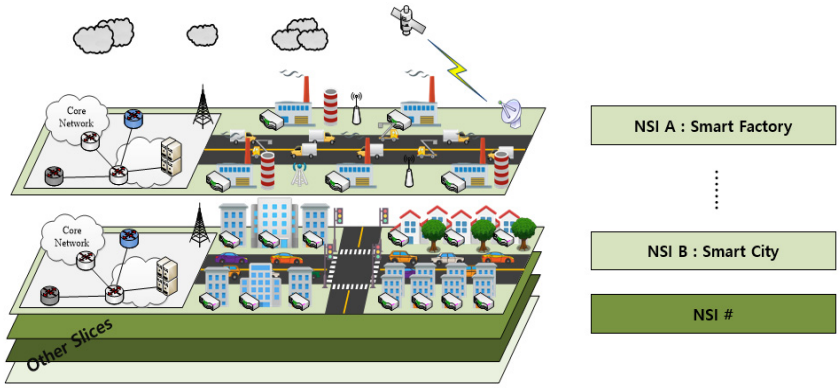
(2) UE는 gNB로부터 메시지를 수신 후 보안 알고리즘과 K_{gNB}를 적용하여 두 개의 키를 생성한 후 메시지 인증 코드 MAC-I를 검증한다. 이후 gNB는 AS



〔그림 7〕 NAS 보안 설정



〔그림 8〕 AS 보안 설정



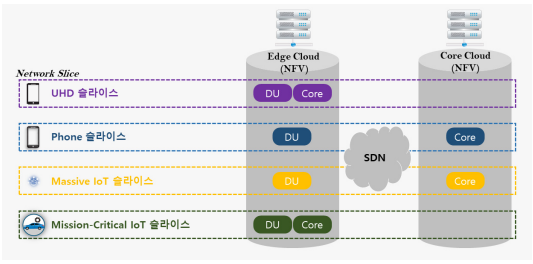
〔그림 9〕 5G 네트워크 슬라이싱의 예시

Security Complete 메시지를 gNB에게 전달함으로써 AS 보안 설정을 종료한다. 이 때 AS Security Complete 메시지는 무결성 키 K_{RRCint}를 통해 작성된 메시지 인증 코드 MAC-I에 의해 보호된다.

Ⅳ. 네트워크 슬라이싱 및 2차 인증

4.1. 네트워크 슬라이싱

네트워크 슬라이싱은 5G의 최첨단 기술로, 하나의 네트워크에서 논리적으로 분리된 다수의 가상 네트워크를 만들어 서로 다른 요구사항을 갖는 다양한 서비스들에 대해 특화된 네트워크를 제공한다[12]. 이는 네트워크의 자원과 기능을 개별 서비스에 맞춰 하나의 독립적인 슬라이싱을 제공하는 것으로 맞춤형(Customization), 자원의 분리(Isolation) 그리고 독립적 관리(Independent Management and Orchestration)의 특징을 갖는다. 따라서 사용자, 서비스, 비즈니스 모델 등의 기준에 따라 네트워크 기능들을 선택하여 유연한 서비스를 제공할 수 있다. [그림 9]는 동일한 인프라에서 동시에 운영되는 여러 네트워크 슬라이스의 예를 보여준다.



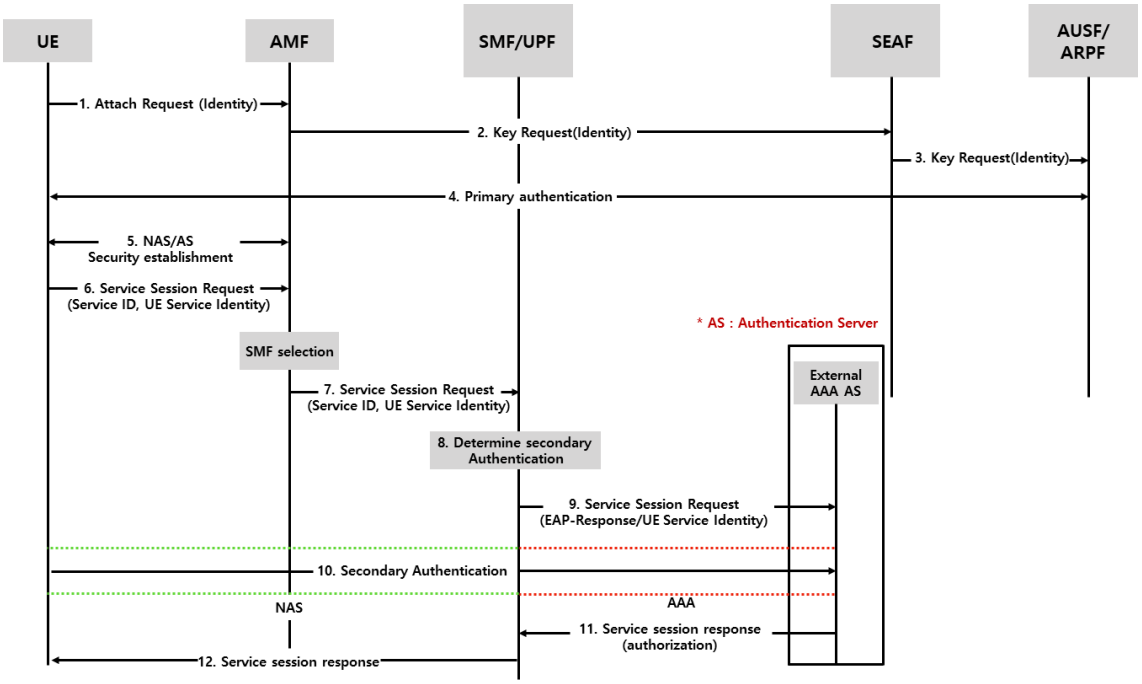
〔그림 10〕 네트워크 슬라이싱 개요〔14〕

NFV(Network Function Virtualisation) 기술은 5G 네트워크 슬라이싱을 구현하기 위한 핵심기술로서[12][13], 네트워크 슬라이스의 인스턴스화 및 운영을 지원하고, 슬라이스의 자원을 필요한 서비스 품질과 성능 수준에 맞춰 자동화 하는 기반이 된다. NFV 기술을 이용한 네트워크 슬라이스는 [그림 10]과 같이 나타낼 수 있다[14].

각 클라우드에는 응용 서비스(NF)를 탑재하고 이를 SDN(Software Defined Networking) 기술로 연결하여 네트워크 슬라이스를 구현 할 수 있다[12]. 네트워크 슬라이스는 처리 능력, 스토리지 및 대역폭 측면에서 전용 리소스 및 공유 리소스로 구성되며 다른 네트워크 슬라이스와 격리된다. 따라서 각 슬라이스 마다 특화된 보안이 고려되어야 한다[15]. 이를 위해 3GPP 5G 보안 구조는 1차 인증과 더불어 응용 서비스에 특화된 2차 인증을 지원한다. 즉, 네트워크 슬라이스는 융합된 응용 서비스에 특화된 보안을 지원하기 위해 2차 인증을 활용 할 수 있다[16]. 다음 4.2절은 2차 인증에 대해 상세히 기술한다.

4.2. 2차 인증 (Secondary Authentication)

2차 인증은 각 네트워크 슬라이스 별로 특화된 보안 요구사항 따라 설계 및 구축된다. 3GPP 5G보안구조에서 제시된 2차 인증은 응용 서비스 공급자가 지정한 외



〔그림 11〕 2차 인증 및 권한 부여

부의 Authentication Authorization and Accounting (AAA) 인증서버와 EAP 인증 프레임워크를 기반으로 수행된다. 여기서 SMF는 UE와 AAA 인증서버 사이에서 인증자 역할 (Authenticator)을 수행하며 2차 인증을 주도한다. [그림 11]은 외부 AAA 인증서버를 활용한 EAP 기반의 2차 인증을 나타낸다.

(1)-(5) UE는 1차 인증 및 NAS/AS 보안설정을 완료한다.

(6) UE는 AMF에게 서비스 세션 요청 메시지를 전달한다. 이때, 요청 메시지는 응용 서비스 아이디와 UE의 서비스 아이디를 포함하며 UE와 AMF 사이에 설정된 NAS 보안에 의해 보호된다.

(7) AMF는 UE가 명시한 서비스 아이디를 기준으로 적합한 SMF를 결정하고 UE로부터 수신한 서비스 세션 요청을 SMF에 전달한다.

(8) SMF는 UE의 가입 프로파일에 기초하여 2차 인증 여부를 결정한다.

(9) 2차 인증이 결정되면 SMF는 외부 AAA 인증서버에 인증 요청 메시지를 보내 EAP 인증을 시작한다. 이때 요청메시지는 EAP-Response 유형으로 UE의 서비스 아이디를 포함한다.

(10) 수신된 UE의 서비스 아이디에 기초하여, AAA 인증서버는 EAP 인증 프로토콜을 결정한다. 이후, 인증서버와 UE는 인증자 역할을 수행하는 SMF의 지원하에 앞서 결정된 EAP 인증 프로토콜을 수행한다.

(11) EAP 인증에 성공하면 외부 AAA 인증서버는 EAP 성공 메시지를 포함하는 서비스 세션 응답 메시지를 SMF에게 전송한다.

(12) SMF는 UE에게 서비스 세션 응답 메시지를 전송함으로써 세션 생성을 완료한다.

Ⅵ. 결 론

본 논문에서는 서비스 융합 네트워크를 위한 5G의 중요한 보안 전략인 EAP 인증 프레임워크를 고찰하는데 목적을 두었다. 이를 위해 EAP 구조를 살펴본 후, 5G의 1차인증 및 2차인증에서 EAP 인증 프레임워크의 역할을 분석하였다. 1차 인증의 EAP-AKA'은 그 자체로서 5G AKA의 중요한 대안이 될 수 있고, 아울러 모든 단말장치가 EAP 인증 프레임워크를 장착하도록 유도하였다. 이는 향후 1차 인증을 위해EAP-AKA'외에

다른 EAP 인증기법이 적용될 길을 열어 놓음으로써 다양한 이기종의 인증기법을 요구하는 응용 서비스를 포용할 수 있도록 하였다. 한편, 응용 서비스에 특화된 2차 인증은 이동단말이 EAP를 기반으로 외부 인증서버와 상호인증 및 키교환을 할 수 있도록 설계되었기 때문에 응용 서비스에 특화된 EAP 기반의 다양한 인증기술을 용이하게 지원할 수 있다. 향후 연구로 보안 및 효율성 측면에서 5G AKA와 EAP-AKA'의 비교 연구가 필요하고, 5G 5대 핵심서비스 등과 같이 주요 응용 서비스를 위한 기존 EAP 인증 프로토콜의 적용 분석 및 신규 프로토콜 개발이 요구된다.

참 고 문 헌

[1] 3GPP, “Security architecture and procedures for 5G system (Release 16),” 3GPP TS 33.501, Sep 2019

[2] N. B. Henda, M. Wifvesson and C. Jost, “An overview of the 3GPP 5G security standard,” ERICSSON BLOG, July 2019 https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

[3] B. Aboba, L. Blunk and J. Vollbrecht, “Extensible Authentication Protocol (EAP),” IETF RFC 3748, June 2004

[4] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,“ IETF RFC 5246, August 2008

[5] D. Hardt, “The OAuth 2.0 Authorization Framework,” IETF RFC 6749, October 2012

[6] J. Arkko, V. Lehtovirta and P. Eronen, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'),” IETF RFC 5448, May 2009

[7] J. Arkko and H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),” IETF RFC 4187, January 2006

[8] D. Simon, B. Aboba and R. Hurst, “The EAP-TLS Authentication Protocol,” IETF RFC 5216, March 2008

[9] Z. Cao, B. He and Y. Shi, “EAP Extensions for the EAP Re-authentication Protocol (ERP),” IETF RFC 6696, July 2012

[10] 3GPP, “Security aspects of non-3GPP accesses,” 3GPP TS 33.402, June 2018

[11] National Institute of Standards and Technology, “Secure Hash Standard (SHS)”, FIPS.180-2, August 2002

[12] Ahmed EI hakim, “5G Network Slicing Reference Model, White Paper”, Research Gate, March 2019.

[13] Bruno Chatras, Steve Tsang Kwong U and Nicolas Bihannic, “NFV enabling network slicing for 5G”, Proc. of the 20th Innovations in Clouds Internet and Networks (ICIN'17), Paris, France, pp. 219-225, March 2017.

[14] NetManias, https://www.netmanias.com/ko/post/blog/8292/5g-data-center-iot-network-slicing-sdn-nfv/5g-and-e2e-network-slicing, November 2015.

[15] Xin Li, M. Samaka, H. A. Chan, D. Bh, L. Gupta, C. Guo and R. Jain, “Network Slicing for 5G: Challenges and Opportunities,” IEEE Internet Computing, Volume 21, Issue 5, pp. 20-27, August 2017.

[16] [3GPP TR 33.899-130] 3GPP “Study on the security aspects of the next generation system,” Aug, 2017. October 2012

〈저 자 소 개〉

윤 건 (Keon Yun)

학생회원

2019년 2월 : 순천향대학교 정보보호학과 졸업

2019년 2월~현재 : 순천향 대학교 정보보호 석사 과정 중

<관심분야> 정보보호, 모바일 인터넷 보안, 5G

박 훈 용 (Hoon Yong Park)
학생회원
2019년 2월 : 순천향대학교 정보보호학과 졸업
2019년 2월~현재 : 순천향 대학교 정보보호 석사 과정 중
<관심분야> 정보보호, 정형화 검증, 모바일 인터넷 보안

유 일 선 (Ilsun You)
종신회원
2002년 2월 : 단국대학교 전산통계학과 박사 졸업
2005년 3월 : 한국성서대학교 정보과학부 전임강사
2008년 3월 : 한국성서대학교 정보과학부 조교수
2012년 3월 : 한국성서대학교 정보과학부 부교수
2015년 9월~현재 : 순천향대학교 정보보호학과 부교수
<관심분야> 인증 및 접근통제, 이동통신보안, 인터넷 보안, 정형화 보안 검증