5G 인증 및 키합의 프로토콜(5G-AKA)의 보안취약점과 PUF 기반의 보안성 향상 방안

정 진 우*, 이 수 진**

요 약

5G 네트워크는 초고속, 초연결, 초저지연이라는 요구를 구현하기 위해 다양한 ICT 기술들을 접목한 차세대 융합 네트워크로서, 이전 세대 이동통신 네트워크의 보안취약점을 해결하기 위해 다양한 노력들이 시도되었다. 그러나 현재까지 발표된 표준화 규격들에는 USIM 탈취 및 복제, 메시지 재전송 공격, 경쟁조건 공격 등의 보안취약점이 여전히 존재한다. 이러한 문제를 해결하기 위해, 본 논문에서는 물리적 복제방지 기능인 PUF 기술을 적용한 새로운 5G 인증 및 키합의 프로토콜을 제시한다. 제시된 PUF 기반의 인증 및 키합의 프로토콜은 특정 입력값에 대해 장치별로 고유하게 생성되는 응답값과 해시함수를 이용하여 현재까지 식별된 보안취약점을 개선한다. 이러한 접근 방법은 보안성이 중요하게 요구되는 영역에서 5G 네트워크를 활용할 경우, 저렴한 PUF 회로의 추가를 통해 강력한 화이트리스트 정책을 구현할 수 있게 해 준다. 또한 기존 프로토콜에 추가적인 암호 알고리즘을 적용하지 않기 때문에 연산 비용 증가나 인증 파라미터 저장 공간 증가의 부담도 상대적으로 적다.

The Security Vulnerabilities of 5G-AKA and PUF-based Security Improvement

Jung Jin Woo*, Lee Soo Jin**

ABSTRACT

The 5G network is a next-generation converged network that combines various ICT technologies to realize the need for high speed, hyper connection and ultra low delay, and various efforts have been made to address the security vulnerabilities of the previous generation mobile networks. However, the standards released so far still have potential security vulnerabilities, such as USIM deception and replication attack, message re-transmission attack, and race-condition attack. In order to solve these security problems, this paper proposes a new 5G-AKA protocol with PUF technology, which is a physical unclonable function. The proposed PUF-based 5G-AKA improves the security vulnerabilities identified so far using the device-specific response for a specific challenge and hash function. This approach enables a strong white-list policy through the addition of inexpensive PUF circuits when utilizing 5G networks in areas where security is critical. In addition, since additional cryptographic algorithms are not applied to existing protocols, there is relatively little burden on increasing computational costs or increasing authentication parameter storage.

Key words : 5G, Security, Authentication, Key Agreement, Physical Unclonable Function

접수일(2018년 11월 1일), 수정일(1차: 2018년 12월 19일), 게재확정일(2018년 12월 30일)

* 육군 지상작전사령부 연합사단협조단 (주저자)

** 국방대학교 국방과학학과 (교신저자)

1. 서 론

4차 산업혁명 시대는 최신 정보통신기술들이 융합된 다양한 서비스를 통해 일상의 전반에서 혁신적인 초연결 사회를 추구한다. 이를 구현하기 위한 핵심 인프라로 초고속, 초연결, 초저지연 특성을 가지는 차세대 융합 네트워크는 필수적이다.

이러한 시대적 요구에 맞춰 국제 표준화를 담당하는 ITU(International Telecommunication Union)에서는 5세대 이동통신인 IMT-2020(5G)의 개념을 정립하고 요구사항을 정의하였으며[1], 2020년 표준안 승인을 통한 상용화를 목표로 여러 나라 및 국제단체들은 기술 개발에 박차를 가하고 있다. 대표적인 이동통신 분야 국제 표준화 단체인 3GPP(3rd Generation Partnership Project)에서는 2016년부터 5G NR(New Radio) 표준화 작업을 2단계로 진행해 왔으며, 1단계 규격인 Release 15가 2018년 6월에 발표되었다[2].

제안된 규격에서는 ITU의 5G 기술 요구사항을 충족시킬 수 있도록 가변적 채널 대역폭, 네트워크 슬라이싱, 소프트웨어 기반의 네트워크 구조(SDN), Dynamic TDD, Massive MIMO 등 다양한 기술들이 제시되었고[3], 표준화 및 상용화가 완료되면 4G LTE(Long Term Evolution) 네트워크를 빠르게 대체할 것으로 전망하고 있다.

5G 네트워크에서는 기술의 진보와 함께 보안적인 측면도 더욱 강조되어 현재의 이동통신 기술 보안 규격들을 보완하기 위한 새로운 구조들이 설계되었다. 5G 네트워크에 연결된 수많은 장치와 사용자를 상호 인증하면서 보안 채널을 구축하는데 핵심적인 역할을 수행할 인증 및 키합의 프로토콜도 이전보다 보안수준이 향상된 5G-AKA로 진화하였다. 그러나 현재까지 발표된 것을 분석해보면 여전히 해결되지 않은 보안취약점이 존재한다. 이전 4G LTE나 IoT 네트워크에 대해서도 보안성 향상의 핵심인 인증 및 키 교환에 관한 활발한 연구가 진행되었듯이[4], 5G 네트워크에서도 기존의 인증 및 키합의 프로토콜이 가진 보안취약점은 반드시 해결되어야 한다.

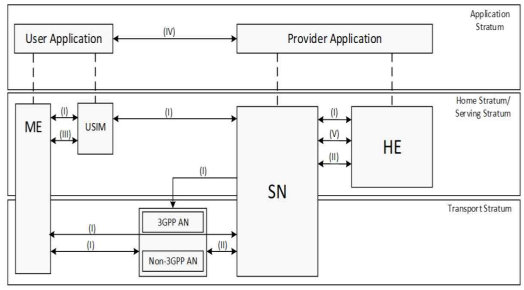
이러한 문제를 해결하기 위해 본 논문에서는 PUF(Physical Unclonable Function) 기술을 응용한 강화된 5G-AKA 프로토콜을 제시한다. 제시한 프로토콜은 기존 5G-AKA 틀을 그대로 유지하면서 PUF를 통한 Challenge-Response를 추가함으로써, 예상되는 보안 취약점들을 해결한다.

본 논문의 구성은 다음과 같다. 2장에서는 5G 네트워크의 보안 구조와 인증 및 키합의 프로토콜에 대해 살펴본다. 3장에서는 5G 인증 및 키합의 프로토콜을 분석하고 보안취약점을 도출한다. 4장에서는 도출된 보안취약점을 해결할 수 있는 PUF 기술 기반의 보안성이 향상된 인증 및 키합의 프로토콜을 제시하고, 제시된 접근방법에 대한 분석결과를 기술한다. 마지막으로 5장에서 향후 연구방향을 제시하고 결론을 맺는다.

2. 5G Security

2.1 Security Architecture

5G는 다양한 응용 서비스, 네트워크, 인터페이스를 정의하고, 코어 네트워크와 외부 네트워크 간의 데이터 전송을 보장하여야 한다. 따라서 5G 보안 구조 역시 이러한 기능들을 지원하기 위해 (그림 1)에서와 같이 UE(User Equipment), AN(Access Network), SN(Serving Network), HE(Home Environment), Application 등 5G 네트워크 구성요소 전반에 걸쳐 안전하면서도 유연하게 설계되어 있다[5].



(그림 1) Overview of the security architecture[4]

- Network Access Security(Ⅰ) : UE가 네트워크를 통해 서비스를 안전하게 인증하고, 접속할 수 있도록 하는 보안 속성 집합.
- Network Domain Security(Ⅱ) : 네트워크 노드가 신호 데이터 및 사용자 평면 데이터를 안전하게 교환할 수 있게 해주는 보안 속성 집합.

- User Domain Security(Ⅲ) : 사용자의 모바일 장치에 대한 접속을 보호하는 보안 속성 집합.

- Application Domain Security(Ⅳ) : 사용자와 공급자의 어플리케이션이 메시지를 안전하게 교환할 수 있게 해주는 보안 속성 집합.

- SBA(Service-Based Architecture) Domain Security(Ⅴ) : 서비스 기반 구조의 네트워크 기능이 서빙 네트워크 및 다른 네트워크 내에서 안전하게 통신할 수 있도록 하는 보안 속성 집합.

본 논문에서는 위와 같은 5G 보안 구조 중에서 첫 째 항목인 Network Access Security를 다루며, 세부적으로는 인증 및 키합의 프로토콜을 다룬다.

2.2 인증 및 키합의 프로토콜(5G-AKA)

5G-AKA는 4G LTE의 EPS-AKA를 기초하여[6] 보안 수준을 보다 향상시킨 AKA의 새로운 버전이다.

2.2.1 참여 개체

(1) UE : USIM(Universal Subscriber Identity Module)과 ME(Mobile Equipment)로 구성된다. UE는 인증 및 키합의 절차를 거쳐 Home Network(UE가 등록되어 있고 접속할 네트워크, 이하 HN)에 접속이 되는데, 이를 위해 USIM에 는 영구적인 가입자 ID 역할을 하는 SUPI (Subscription Permanent Identifier), HN의 공개키(pkHN), HN과 공유 비밀키로 활용하는 K(Long-term key)를 비롯한 모든 필수 정보가 포함되어 있다. AKA 절차에서 생성되는 키들의 seed 역할을 수행하는 'K'는 절대로 USIM 외부로 유출되지 않으며, SUPI는 HN 공급자의 결정에 의해 공개키로 암호화되어 SUCI(SUbscription Concealed Identifier)로 변환될 수 있다.

(2) SEAF(Security Anchor Function) : Serving Network(UE가 무선을 통해 연결되는 네트워크, 이하 SN) 내 존재하는 물리적 보호 시스템이다. UE와 HN 간 매개체 역할을 수행한다.

(3) AUSF(Authentication Server Function) : HN에 의한 사용자 장치 인증을 위하여 SEAF와 상호작용하는 HN 내의 시스템이다.

(4) UDM/ARPF(Unified Data Management / Authentication credential Repository and Processing Function) : HN의 보안 환경 내에 존재하는 개체이다. 이는 UE 인증을 위한 비밀키 K, HN의 개인키 skHN 등 인증 자격들을 입력으로 한 암호화 알고리즘을 수행하여 출력값을 생성한다.

(5) SIDF(Subscription Identifier De-concealing Function) : UDM/ARPF 내에서, HN의 개인키 skHN을 통해 SUCI를 SUPI로 복호화 한다.

2.2.2 동작 절차

5G-AKA 프로토콜의 동작 절차는 (그림 2)와 같고 [5][6][7][8], 의미에 대한 설명은 다음과 같다.

(1) UE는 'SUPI'를 HN의 공개키로 암호화 한 'SUCI'를 전달한다. 5G-AKA에서 사용하는 알고리즘은 타원 곡선 암호로 설계된 ECIES(Elliptic Curve Integrated Encryption Scheme)이다.

(2) SN name은 서비스 코드인 '5G'와 'SN id'를 바인딩한 값이다.

(3) AUSF는 메시지를 수신하면 알고 있는 SN 리스트와 비교하여, 정상 SN 여부를 판단한다.

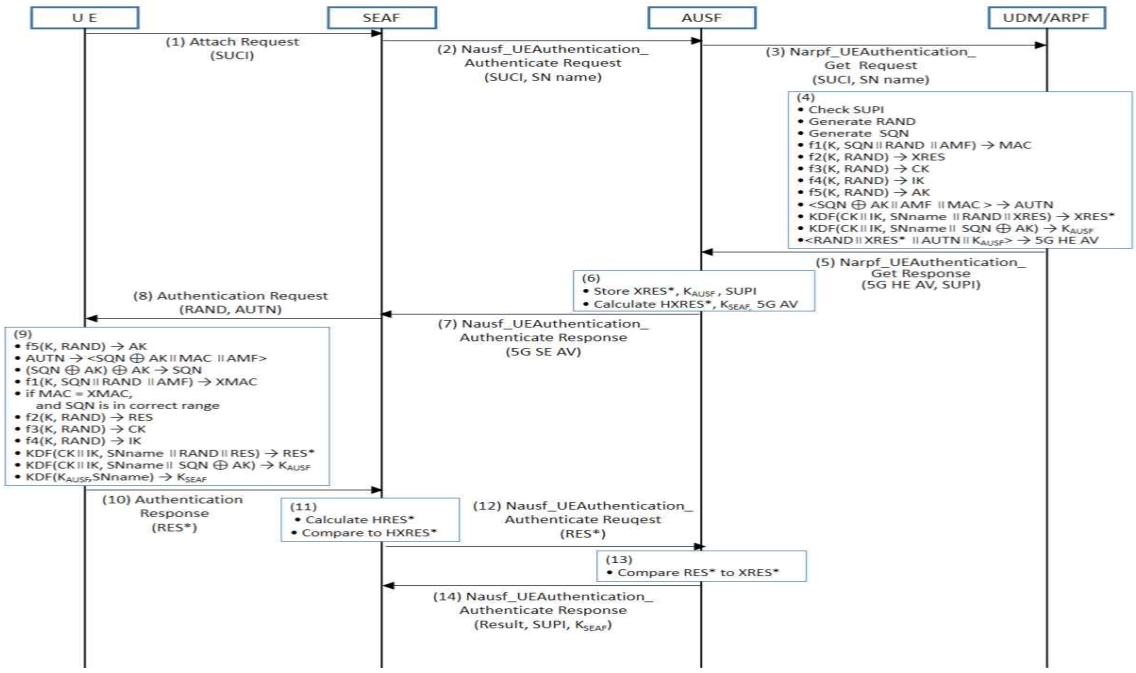
(4) UDM/ARPF는 메시지를 수신하면 'SIDF'를 호출하여 'SUCI'를 복호화하고 'SUPI'를 얻는다. SUPI를 통해 정상적으로 HN에 등록된 가입자인지를 확인하고, '5G HE AV(Authentication Vector)'를 생성한다.

'RAND'는 임의로 생성된 128비트 값이며, 'SQN'은 순차번호로서 최초 인증 단계에서만 생성되고, 인증 절차가 수행될 때마다 누적 증가한다.

그리고 'CK'는 암호화 키, 'IK'는 무결성 키, 'AK'는 익명성 키를 의미한다. f1~f5 함수는 모두 128비트 알고리즘이며, 키는 'K'를 사용한다. f1과 f2는 메시지 인증 기능을 수행하므로 NIA(Integrity Algorithm for 5G) 3종류 중 선택하여 사용하고, f3~f5 함수는 키 생성 기능을 수행하므로 NEA(Encryption Algorithm for 5G) 3종류 중 선택하여 사용한다. KDF(Key Derivation Function)로는 'HMAC-SHA256'을 활용한다. 'AUTN'은 최종 UE에게 전달되어 활용되는 인증 파라미터들로 구성되며, 'K_{AUSF}'는 최상위 레벨키이다.

(5) 'SUPI'를 '5G HE AV'와 함께 전달한다.

(6) AUSF는 차후 단계 수행을 위해 필요한 값은 보관하고, SEAF에게 전달할 값은 생성하여 '5G AV'를 구성한다.



(그림 2) 5G-AKA 동작 절차

(7) AUSF는 중요 키 'K_{SEAF}'를 제거하고 '5G SE (Serving Environment) AV'를 구성한다.

(8) SEAF는 차후 단계 수행을 위해 필요한 값은 보관하고, UE에게 필요한 값은 전달한다.

(9) UE의 USIM은 'RAND'와 'AUTN' 만으로 UDM/ARPF에서 사용한 동일한 알고리즘을 활용하여 자체적으로 인증 파라미터들을 생성한다. 절차 수행 중, UE에서 산출한 'MAC'과 'XMAC' 일치 여부와 산출한 'SQN'이 허용된 증가치 내에 있는지를 확인하는데, MAC과 XMAC이 다르면 "Cause = MAC Failure" 메시지를, SQN이 비정상이라면 "Cause = Synchronization Failure"를 SEAF에게 전달하여 인증 과정에 오류가 있음을 알린다. 최종 생성한 'RES^*'는 SEAF에게 전달하고 생성된 'K_{AUSF}'와 'K_{SEAF}'는 UE와 HN 간 공유된 상위 레벨 키로서 UE에 보관한다.

(10) 'RES^*'는 UE 인증을 위해 전달된다.

(11)(12) 'RES^*'로부터 '$HRES^*$' 값을 산출하고, '$HRES^*$' = '$HXRES^*$'이라면, SEAF는 UE로부터 전달받은 'RES^*'를 AUSF로 전달한다.

(13) AUSF는 RES^*=$XRES^*$이면, 최종적으로 UE를 인증하고, 사용할 키를 확정한다.

(14) AUSF는 UE의 최종 인증 결과와 함께, 초기 AKA 절차 이후 SEAF에서 사용할 K_{SEAF}, SUPI를 SEAF로 전달한다.

3. 5G-AKA 보안 취약점

3.1 USIM 복제 및 탈취를 이용한 공격

LTE의 EPS-AKA에서 IMSI (International Mobile Subscriber Identity)가 평문으로 무선 전송되는 보안 취약점을 해결하고자, 5G-AKA에서는 LTE의 IMSI와 같은 역할을 하는 SUPI를 암호화한 SUCI를 무선 전송한다. 새롭게 시도된 5G 인증 매커니즘은 메시지 도청으로 가입자 식별 정보를 알아내는 공격에 강하다. 하지만, USIM 내에는 K, SUPI, HN 공개키를 비롯한 AKA 절차에 필요한 모든 필수 정보가 포함되어 있기 때문에 USIM 자체가 탈취되거나 복제된 상황에서 5G-AKA는 무용지물이 되며, 공격자를 정상적인 가입자로 인식하여 네트워크 접속을 허용한다. 공격자가 HN 접속에 성공한 이후에는 손쉽게 다른 공격들을 수행할 수 있으며, 정상적인 사용자의 접속

을 악의적으로 차단할 수도 있다.

3.2 Race-Condition 공격

공격 대상자(A)가 5G 네트워크에 접속하기 위해서 5G-AKA 세션을 시작할 때 UE가 SEAF로 전달하는 메시지를 공격자(B)가 도청하게 되면 UE의 SUCI를 도청할 수 있다. 이 때 공격자(B)는 해당 5G 네트워크의 정상 USIM을 악의적인 목적으로 구매하여 등록한 사용자라고 간주한다. 이후 B는 지역 SN과 5G-AKA 세션을 시작하며 동시에 엿들었던 A의 SUCI를 재생하여 세션을 함께 시작한다. 이렇게 세션이 병렬로 실행될 경우 UDM/ARPF에서는 경쟁 조건이 발생하고, 각각의 세션에 대한 잘못된 응답(결과 Key)을 연관 짓기 쉬워진다. A를 위한 5G HE AV와 K_{AUSF}가 K_B(B의 Long-term Key)에 의해 파생되는 경우가 생기는 것이다. 이런 상황이 발생하고 나면 B는 A의 앵커 키를 파생시킬 수 있어, A로 가장하여 5G 네트워크에 연결이 가능해진다[9]. 이를 통해 B가 사용한 서비스 요금이 A에게 잘못 청구되거나, 악의적 사용자로 인해 정상 사용자의 네트워크 접속이 차단되는 상황이 발생 가능하다.

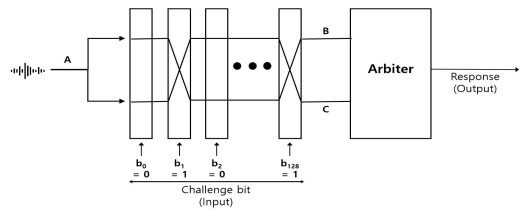
이러한 공격은 경쟁조건에 의해 세션을 잘못 바인딩하면서 이루어지는 취약점을 이용한 공격이므로 가입 식별자인 SUPI가 SUCI로 보호되는지 여부와 관계없이 수행 가능하다.

3.3 중간자에 의한 메세지 연결성 공격

공격 대상자(A)가 SEAF로 보내는 등록 요청 메시지를 공격자(B)가 도청을 통해 확보하였다면, 다음번 A의 재등록 요청이 있을 때 확보하고 있던 메세지와 비교하여 A가 해당 지역 SN 주변에 있음을 확인할 수 있다. 그리고 인증 및 키합의 절차 상 SEAF가 A에게 보내는 'Authentication Request' 메시지를 얻을 수 있다. 공격자가 확보한 메시지를 관찰 구역 내 모든 UE에게 재전송하게 되면, 메시지를 수신한 UE들은 두 종류의 에러 메시지를 보내게 된다. A는 SEAF로부터 이미 수신했던 메시지를 다시 받았기 때문에 SQN이 비정상이므로 'Synchronization Failure' 메시지를 전송한다. 반면 A가 아닌 다른 일반 사용자들의 경우, 메시지에 대한 MAC이 불일치하므로 'MAC Failure' 메시지를 보내게 된다. 따라서 B는 'Synchronization Failure'를 확인함으로써 A의 위치를 예측할 수 있음은 물론, UE와 HN 간 잘못된 SQN 업데이트를 유발하여 정상적인 인증 매커니즘에 영향을 미친다[10]. 그리고 일반 사용자들이 보낸 'Mac Failure'를 수신한 HN에서는 일반 사용자들에게 'Identity Request' 메시지를 보낸다. 이후 UE들은 자신의 SUCI를 포함한 'Identity Response' 메시지를 보내는데, 이 메시지를 탈취하면 메시지를 보낸 모든 UE들의 SUCI를 수집할 수 있어, 앞서 이뤄졌던 공격들을 반복해서 다시 수행할 수 있다. 이를 통해 특정 사용자의 위치가 노출될 수 있으며, 정상적인 AKA 절차에 오류가 발생한다.

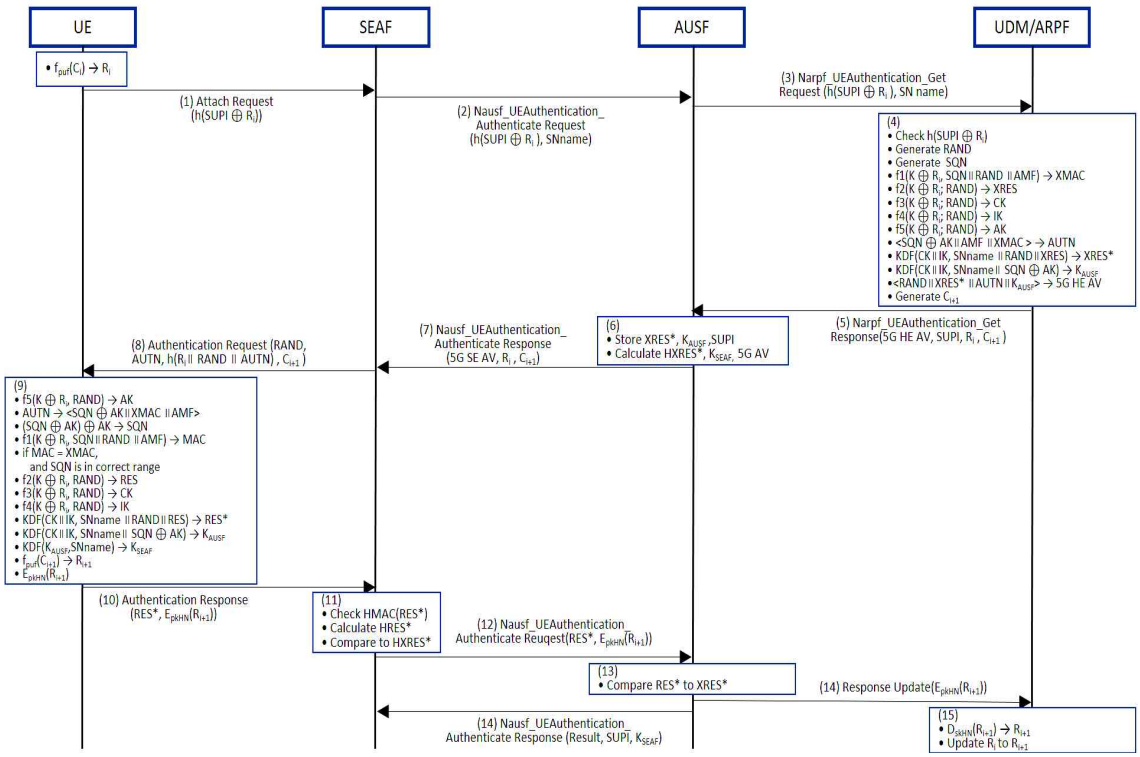
4. PUF 기술을 활용한 5G-AKA

PUF는 동일한 공정을 통해 제조된 장치라 하더라도 사람의 생체정보처럼 각자만의 고유한 특성들을 가질 수 있음에 착안하여 개발된 기술로서, 장치 제조 공정에서 생기는 편차로 발생하는 소자 및 회로 특성 등의 물리적 미세구조를 활용한다[11]. 특정 장치 내에 IC(Integrated Circuit)의 형태로 활용되는 PUF는 동일한 입력에 대해 동일한 응답을 유지한다는 강인함, 새로운 입력에 대한 응답을 예측하기 어렵다는 예측 불가능성, 그리고 복제불가능성의 특성을 가진다[12]. 그리고 입력과 출력의 쌍인 CRP(Challenge Response Pair)는 독특성과 다양성을 만족하여야 한다[13].



(그림 3) Arbiter PUF 구조 및 동작

구현 방법에 따라 크게 Mismatch-based PUF와 Physical-based PUF로 구분하며, 세부적으로 다수의 기술이 제안된 바 있다[14]. 본 논문에서는 제한된 자원을 가진 플랫폼에 적합하고 구현이 간단하여, 다양



(그림 4) PUF 기반 5G 인증 및 키합의(AKA) 절차

한 분야에서 활용성이 큰 Arbiter PUF를 적용 대상으로 선정하였다. 이는 (그림 3)에서 보는 바와 같이 2개의 MUX로 구현되는 스위칭 박스와 latch로 구현되는 Arbiter로 구성되어 있다[15]. 공정상 동일한 거리를 가지는 상단과 하단, 두 경로에 동일한 신호(A)를 보내 어떤 신호(B or C)가 먼저 Arbiter에 도착하는지에 따라서 비트 출력이 결정된다.

이러한 PUF 기술을 활용하여 앞서 제시된 보안취약점을 개선할 수 있도록 설계된 새로운 5G-AKA는 (그림 4)에서 보는 바와 같다.

최초 UE를 인증 센터인 UDM/ARPF에 등록 시, UE와 UDM/ARPF 간에는 공통적으로 사용할 해시함수 h(f), 사용자 고유 식별자인 SUPI 및 Long-term key인 K, 그리고 UE의 PUF에서 생성한 최초 Challenge인 'C_0'에 대한 Response 'R_0'를 공유하여 보관한다.

(1) UE는 초기 인증 시도 메시지 생성 시, 'SUCI'를 생성하는 기존 방식 대신 PUF에 최초 Challenge인 'C_0'를 입력하여 출력된 'R_0'를 활용하며, 이를 'SUPI'와 XOR하여 Hash로 보호한다.

· $f_{PUF}(C_0) \rightarrow R_0$

(h(SUPI⊕R_0)) 포함된 메시지 전송

(2)(3) SEAF는 'h(SUPI⊕R_0)'에 'SNname'을 바인딩 하여 UDM/ARPF에게 전송한다.

(4) UDM/ARPF는 UE를 최초 등록 시 저장해 놓은 'R_0'을 통해 'h(SUPI⊕R_0)'를 자체 연산하여 정상적으로 등록된 사용자임을 최초 확인한다. 그리고 PUF 기반 5G-AKA 알고리즘을 수행한다. 기존 알고리즘에서 달라지는 점은 키 값을 'K' 대신 'K⊕R_0'을 사용하는 점이다. 그리고 모든 알고리즘 수행 후, 다음 인증 절차 시 사용할 'R_1'을 얻기 위한 'C_1'을 생성한다.

(5) UDM/ARPF는 AUSF에게 '5G HE AV', 'SUPI', 그리고 'R_0', 'C_1'을 메시지로 전달한다.

(6) 기존 5G-AKA 절차와 동일하다.

(7) AUSF는 '5G SE AV'와 함께, UDM /ARPF로부터 받은 'R_0', 'C_1'을 전달한다.

(8) SEAF는 'RAND'와 'AUTN'에 더해, UE가 'R_1'을 유도할 수 있도록 'C_1'을 함께 전달한다. 메시지 도청을 통한 재생 공격을 방지하기 위해 'R_0'를 활용하여 생성한 HMAC을 함께 전달한다.

(9) UE는 HMAC을 통해 메시지에 대한 무결성을 검증하고, USIM은 UDM/ARPF에서 사용한 동일한 알고리즘을 활용하여 'RES*'를 생성한다. 그리고 다음 번 인증 절차에서 사용할 PUF의 Response 생성을 위해, 전달받은 'C_1'으로 'R_1'을 생성한다. 그리고 이를 기존 5G-AKA에서 제공하는 ECIES 공개키 알고리즘으로 암호화한다.

(10) UE는 'RES*'와 '$E_{pkHN}(R_1)$'을 전달한다.

(11)(12) 'HRES*'='HXRES*'이면, 전달받은 'RES*'와 '$E_{pkHN}(R_1)$'을 AUSF에게 전달한다.

(13) 'RES*' 확인을 통해 UE를 최종 인증한다.

(14) 'Result', 'K_{SEAF}', 'SUPI'는 SEAF로 전달하고, UDM/ARPF로 '$E_{pkHN}(R_1)$'을 전달한다.

(15) SIDF를 호출하여 '$E_{pkHN}(R_1)$'를 복호화 시키고, 'R_1'을 추출한다. 이렇게 추출된 R_1은 R_0를 대체하여 다음 번 인증 시에 사용된다.

- $D_{skHN}(E_{pkHN}(R_1)) \rightarrow R_1$
- Update $R_0 \rightarrow R_1$

이상에서 설명한 PUF 기술 기반의 5G-AKA는 기존 프로토콜에 비해 다양한 강점을 가진다.

첫째, UE에 복제 불가능한 하드웨어 보안 기술인 PUF를 접목하여, Challenge-Response를 인증 및 키합의 절차 전 단계에서 활용함으로써 USIM 복제나 탈취에 의한 공격 가능성을 원천적으로 배제할 수 있다. 공격자는 공격하고자 하는 UE의 USIM을 복제하거나 탈취하여 공격자의 장치에 장착할 수는 있겠지만, PUF에 의해 생성되는 값은 만들어 낼 수 없다. 따라서 UDM/ARPF와의 정상적인 인증 및 키합의 절차 수행은 불가능하다. 또한 가입자 고유 식별자 역할을 하는 SUPI나 SUCI가 노출되어 재생되더라도 PUF에 의해 생성되는 Response를 통해 정상 UE의 식별이 가능하기 때문에, 경쟁조건 공격도 해결할 수 있다.

둘째, 항상 동일한 인증 식별정보를 사용하는 기존 5G-AKA 프로토콜과 달리 PUF를 통해 인증 절차가 수행될 때마다 사용되는 C_i와 R_i가 업데이트되기 때문에, 무선 네트워크상에서 전송되는 메시지를 도청한 후 재전송 공격을 수행하는 것이 불가능해진다. 그리고 도청을 통해 획득한 메시지를 재사용해서 인증을 시도하는 공격자를 식별하고 네트워크에서 배제하는 것도 가능하다.

셋째, 'Authentication Request' 메시지가 평문으로 전송됨에 따라 메시지 연결성 공격에 취약했던 부분을 Response를 활용한 HMAC 적용을 통해 보완하였다. 공격자가 무선 메시지를 탈취하더라도 해당 시점에 적용된 Response와 Hash를 모르면 같은 메세지를 재전송할 수 없어, 결과적으로는 UE의 정보 노출이나 위치 노출을 방지한다.

넷째, SUPI를 타원곡선 공개키 알고리즘을 통해 SUCI로 암호화하고 다시 복호화하는 기존 5G-AKA 과정을 SUPI에 해당 시점의 PUF Response 값을 XOR하고 해시함수를 적용하는 것으로 바꿈으로써 연산 효율성이 향상된다.

마지막으로, 기존 PUF 기반 인증 기법들은 CRP 테이블을 미리 생성하여 저장하는 방식을 취했던 반면, 제시된 프로토콜은 CRP 테이블의 저장 없이도 Challenge-Reponse의 지속적 업데이트를 제공함으로써 UDM/ARPF의 저장 공간 낭비를 방지할 수 있다. CRP 테이블 사전 저장 기법을 활용하여 UE 하나당 128비트 PUF 기반의 CRP 테이블 100,000개 쌍을 미리 저장해둔다고 가정할 때 1.5Mbyte 정도의 HSS/AuC의 저장 공간이 요구되지만, 본 논문에서 제시하는 기법은 이러한 저장 공간이 요구되지 않으므로 이를 절약할 수 있다. 이러한 측면은 5G 네트워크 환경 특성 상 HSS/AuC에 등록되는 UE의 숫자가 많으면 많아질수록 더욱 큰 효과를 가져온다.

5. 결론

본 논문에서는 5G 네트워크의 인증 및 키합의 프로토콜에서 발생 가능한 보안취약점을 개선하기 위해 PUF 기술 기반의 보안성이 강화된 새로운 인증 및 키합의 프로토콜을 제시하였다.

제시된 프로토콜은 기존 5G-AKA에 Arbiter PUF를 추가하고, 이를 통해 생성되는 Challenge와 Response 및 그에 대한 해시함수를 인증 과정에 추가적으로 적용하였다. 또한 CRP 테이블의 사전 생성을 통한

저장 과정 없이도 PUF의 C_i와 R_i 값이 계속 갱신되도록 설계하였으며, HMAC을 이용하여 무선 메시지에 대한 무결성 검증을 실시한다. 이러한 과정을 통해 개선된 5G-AKA 프로토콜은 기존 프로토콜에서 문제시되었던 USIM 복제 및 탈취에 의한 불법적인 네트워크 접속, 무선 구간 메시지 탈취 및 연결성을 이용한 중간자 공격, 경쟁조건 공격에 의한 정상 사용자의 접속 차단 등의 발생 가능한 보안 취약점을 손쉽게 해결할 수 있다.

제시된 프로토콜은 기존 프로토콜에서 사용했던 인증 변수들에 변경 및 위조가 불가능한 정보를 추가적으로 사용하기 때문에 저장 공간 사용량은 다소 증가한다. 그러나 1$ 정도의 간단한 PUF 회로 추가를 통해, 기존 5G-AKA 절차와 기술적인 연동을 유지하면서 기존 프로토콜에서 발생 가능했던 보안취약점을 모두 해결할 수 있는 상당히 효율적인 접근방법이다.

향후에는 초기 인증단계에만 국한되어 있는 본 연구를 확장하여 이후 단계에서 발생 가능한 보안취약점을 분석하고, 이를 보완할 수 있는 추가적인 대책도 마련되어야 할 것이다.

참고문헌

[1] 박성준, “5G 이동통신 기술동향,” 주간기술동향, 제 1844호, pp. 2-11, 2018.
[2] “Release 15,”http://www.3gpp.org/release-15
[3] 김득원, “4차 산업혁명시대의 핵심 인프라, 5G”, KISDI Premium Report, 17-06, pp. 1-16, 2017.
[4] 유우영, “IoT 보안에 대한 국내외 연구 동향 분석,” 융합보안논문지, 제 18권, 제 1호, pp. 62-67.
[5] 3GPP , “TS 33.501, Security architecture and procedures for 5G system,” V15.2.0, 2018.
[6] 3GPP, “TS 33.401, 3GPP System Architecture Evolution Security architecture,” V15.5.0, 2018.
[7] 3GPP “TS 24.501, Non Access Stratum(NAS) protocol for 5G System,” V15.1.0, 2018.
[8] 3GPP, “TS 23.501, System Architecture for the 5G System” V15.3.0, 2018.
[9] Martin Dehnel-Wild, ″Security vulnerability in 5G-AKA draft,″ University of Oxford, 2018.
[10] David Basin, “A Formal Analysis of 5G Authentication,” arXiv:1806. 10360, 2018.
[11] 이동건, 이연철, 김경훈, 박종규, 최용제, 김호원, “안전하고 신뢰성 있는 PUF 구현을 위한 가이드라인,” 정보보호학회논문지, 제 24권, 제 1호, pp. 241-259, 2014.
[12] 변진욱, “PUF 기반 RFID 인증 프로토콜의 효율적 설계에 관한 연구,” 정보보호학회논문지, 제 24권, 제 5호, pp. 987-999, 2014.
[13] 김승열, 이제훈, “신뢰성 향상을 위한 듀얼 안티퓨즈 OTP 메모리 채택 D-PUF 회로,” 융합보안논문지, 제 15권, 제 3호, pp. 100-105, 2015.
[14] 백종학, 신광조, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” 전자공학회지, 제 43권, 제 7호, pp. 59-67, 2016.
[15] Daihyun Lim, “Extracting Secret Keys from Integrated Circuits,” IEEE Transactions on VLSI Systems. vol. 13, no. 10, pp. 1200-1205, 2015.

〔저자소개〕

정 진 우 (Jinwoo Jung)
2006년 3월 육군사관학교 학사
2016년 3월 국방대학교 석사
2019년 1월 ~ 현재
육군 지상작전사령부 연합사단협조단

email : jwjung7@gmail.com

이 수 진 (Soojin Lee)
1992년 3월 육군사관학교 학사
1996년 2월 연세대학교 석사
2006년 2월 한국과학기술원 박사
2006년 3월 ~ 현재
국방대학교 국방과학학과 교수

email : cyberkma@gmail.com