벤처혁신연구 제2권 제1호(통권3호) http:www.kavi.or.kr
Journal of Venture Innovation, Vol.2. No.1, June. 2019, pp.13-21

LTE 환경에서 초기 식별자를 보호하기 위한 MILENAGE 알고리즘 기반의 상호인증

유재회(숭실대학교 박사과정)[1] 김형욱(한국전자인증)[2] 정용훈(바스랩)[3]

국 문 요 약

4세대 이동통신 기술인 LTE환경에서 사용자 단말기와 사용자를 확인하는 초기 식별자를 평문으로 전달하는 취약점으로 인한 사용자 정보가 노출되는 피해가 발생하고 있다. 본 논문에서는 고유 식별정보의 노출 문제점에 대한 해결책으로 시도응답을 이용한 일회용 패스워드와 AES기반의 Milenage 키 생성 알고리즘을 활용하여 안전한 초기 식별 통신을 위한 상호인증 프로토콜을 제안한다. Milenage 키 생성 알고리즘은 기존 프로토콜에서도 사용되고 있는 키 생성 알고리즘으로써 암호화 키, 무결성 키, 메시지 인증코드를 생성하는 알고리즘이다.
LTE 네트워크에서 표준으로 사용되고 있는 LTE Security 프로토콜은 EPS-AKA를 기반으로 사용자 단말기와 사용자를 식별할 수 있는 초기 식별자를 상호인증시 노출되는 취약점이 나타나는 한계점으로 인해 UE 추적 가능성과 IMSI 노출로 인한 사용자 개인정보 노출 취약점을 보완하여 노출의 문제점을 최소화 한다.

■ 중심어: AES-based Milenage key, MILENAGE Algorithm, LTE Security, private information

Ⅰ. 서 론

LTE는 3세대 이동통신의 진화기술인 Long-Term Evolution의 약자로 4세대 이동통신 기술이다. LTE는 고속 전송, 기존의 주파수 대역에서의 유연한 적용, 비트당 비용 절감, 낮은 전송 지연을 목표로 하고 있다. LTE 표준 현황은 2004년부터 시작하여 국제 표준은 Release 12까지 진행 중에 있으며 현재 국내 적용중인 표준은 Release 9을 적용하고 있다. 국제 표준이 R12까지 진행함에도 불구하고 2010년 표준인 R9에서 명시한 LTE 네트워크 취약점들에 대한 구체적인 방안 없이 대응책만을 제시하고 있다. 현재까지도 취약점을 해결하지 못한 채 R12에 대한 작업이 진행 중에 있다. LTE 표준에서는 현재 표준에 나타나있는 취약점에 대해 구체적으로 기술되어 있다. 첫 번째로 사용자가 UE(User Equipment)를 가지고 LTE 망에 접속하기 위해서는 사용자 단말기 가까이 있는 eNB를 탐색한다. LTE 네트워크와 통신하기 위해 사용자 단말기는 초기 탐색절차를 거쳐 가까운 eNB와 접속 동기화를 시작하게 된다. 이때 사용자 단말기에서는 RNTI(Radio Network Temporary Identifier)를 생성하며, 생성된 RNTI는 eNB에서 특정 사용자 단말기에 대한 고유한 CRNTI를 할당한다. 할당

1)저자: 숭실대학교 컴퓨터학과 박사과정, hwe100@ssu.ac.kr
2)교신저자: 숭실대학교 컴퓨터학과 공학박사, do3196@naver.com
3)공동저자: 숭실대학교 컴퓨터학과 공학박사, jung7773@naver.com
· 투고일: 2019-04-18 · 수정일: 2019-05-09 · 게재확정일: 2019-06-20

된 CRNTI는 셀내에서 사용자 단말기를 유일하게 식별하기 위해 사용된다. 생성되고 CRNTI는 다른 지역의 eNB로 접속하기 전까지 생성된 CRNTI를 오랫동안 유지하고 있기 때문에 사용자 단말기에 대한 추적을 할 수 있는 취약점이 존재한다고 기술되어 있다. 두 번째로 사용자 단말기가 LTE 네트워크망에 처음 접속할 때 정당한 사용자 단말기와 네트워크를 상호인증하기 위해 인증센터까지 IMSI (International Mobile Subscriber Identifier)를 평문으로 전송하게 되어 사용자 단말기를 유일하게 식별할 수 있는 IMSI가 노출되는 취약점이 존재하고 있다.

LTE 네트워크에서 초기식별 통신구간의 취약점은 현재 표준에 정의되고 있는 LTE Security에서 초기식별을 할 때 평문으로 노출되고 있는 위협에 대한 보안이 적용되지 않고 있기 때문이다. 본 논문은 위에서 언급한 기존 초기 네트워크 탐색 과정에서 RNTI 노출로부터 사용자 단말기에 대한 추적 위협성과 사용자 식별자 노출 취약점을 해결하기 위해 LTE AKA에서 쓰이는 Milenage 알고리즘을 사용한 초기 식별자를 보호하기 위한 암호화 및 상호인증 프로토콜을 제안한다.

Ⅱ. 관련 연구

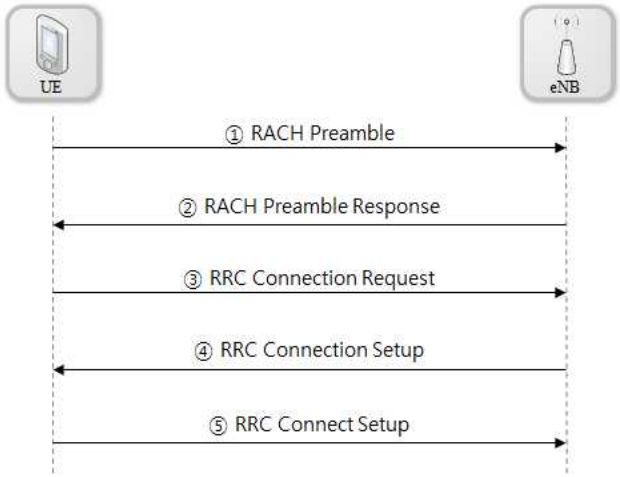
2.1 LTE

LTE는 Long-Term Evolution의 약자로 3GPP(3rd Generation Partnership Project)표준화 단체에서 2004년 11월부터 표준화를 진행했다. 현재 작업 중에 있는 LTE 국제 표준 버전 Release12 작업을 진행하고 있는 4세대 이동통신기술이다. LTE는 핵심기술인 OFDM과 MIMO를 이용하여 HSDPA보다 12배 이상 빠른 속도로 통신할 수 있다.

현재 국내에서 적용되고 있는 LTE 국제 표준 버전은 Release 9을 기반으로 적용되어 있다. Release 9에서는 20MHz 대역에서 100Mbps의 다운링크 최고속도, 50Mbps의 업링크 최고속도를 제공하며, MIMO(Multiple Input Multiple Output), 패킷 스케줄링, DRX(Discontinuous Reception)등의 핵심 기술에 대한 표준화가 진행되었다. 이렇게 규격화 작업이 완료된 LTE는 현재 상용화에 성공하였고 이보다 빠른 LTE-Advanced를 상용화시키기 위해 이에 대한 규격화 작업이 진행되고 있다. LTE-Advance는 국제 표준 Release 10, 11이다.

2.2 네트워크 탐색 프로토콜

LTE는 L사용자 단말기가 LTE 네트워크에 접속하기 위해 첫 번째로 사용자 단말기 근처에 위치해 있는 eNB와 접속해야한다. 이러한 과정을 접속 동기화라고하며 eNB에서 단말기들을 셀 내에서 유일하게 식별하기 위해 수행된다. 접속 동기화에서는 사용자 단말기와 eNB의 특정 셀에서 고유 식별자들이 평문상태로 통신하게 되며 특정한 이벤트가 발생하지 않으면 고유 식별자는 변경되지 않는 점이 있다. [그림 1]는 가까운 eNB와 접속동기화를 하기위한 절차를 간략하게 나타낸 것이다.



[그림 1] 접속 동기화 Protocol

첫째, 단말기가 자신의 근처에 위치해 있는 eNB와 통신하기 위해서는 사용자 단말기에서 자신의 정보를 담은 6bit 길이의 RA-RNTI를 RACH Preamble 메시지에 담아 가까운 eNB에게 전송한다.

둘째, RACH Preamble 메시지를 전달받은 eNB는 해당 메시지의 RA-RNTI값을 이용하여 T-CRNTI(Temp CRNTI)값으로 사용한다. T-CRNTI를 RACH Preamble Response 메시지에 담아 해당 단말기에 전송한다.

셋째, RACH Preamble Response 메시지를 받은 단말기에서는 UE Identity를 RRC Connection Request 메세지에 포함하여 전송한다. UE Identity는 40bit의 S-TMSI(SAE Temporary Mobile Subscriber Identifier), 32bit의 M-TMSI(MME Mobile Subscriber Identity)와 8bit의 MMEC(Mobile Management Entity Code)로 이루어져있다.

넷째, RRC Connection Request 메시지를 받은 eNB에서는 T-CRNTI를 CRNTI로 설정하며 단말기와 연결설정을 동기화하기 위해 정보를 담아 RRC Connection Setup 메시지를 전송한다.

다섯째, RRC Connection Setup 메시지를 받은 단말기는 해당 eNB로부터 메시지를 정확하게 전달받고 연결설정을 마쳤다는 메시지로 RRC Connect Setup 메시지를 전송한다.

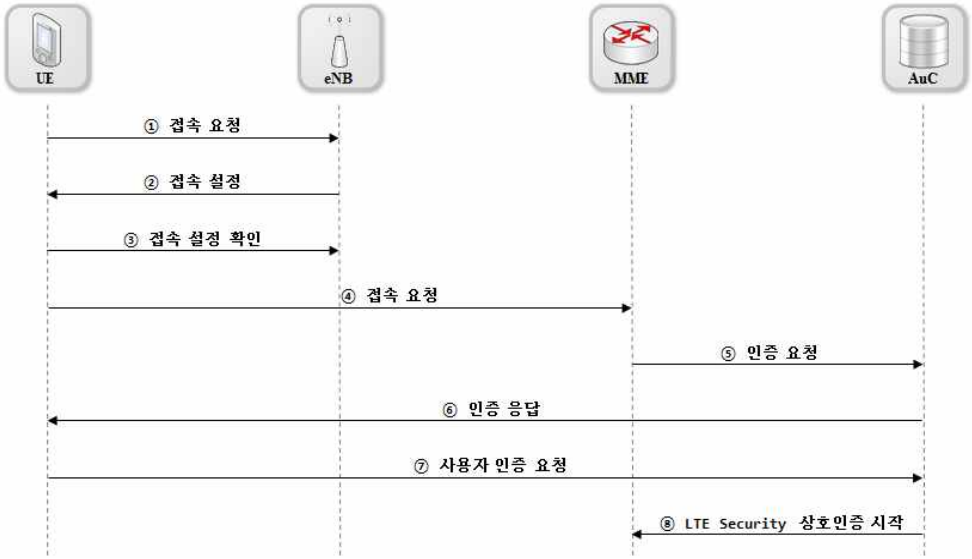
위와 같은 접속동기화 과정을 거치게 되면 특정 eNB의 해당 셀에 접속해 있는 단말기에게 고유 식별자를 지정하게 된다. eNB에서 단말기를 식별하고 난 후 LTE Security 프로토콜을 수행하게 된다.

Ⅲ. MILENAGE 알고리즘 기반 상호인증 프로토콜

3.1 제안하는 상호인증 프로토콜

기존 EPS-AKA기반의 LTE Security 프로토콜은 초기 식별통신에서 사용자 및 단말기를 식별하는 고유 식별값 노출에 대한 한계점을 보완하고자 본 논문에서는 LTE 네트워크 탐색프로토콜과 LTE Security 상호인증 프로토콜을 수행하기 전인 초기 식별통신 프로토콜에 Milenage 알고리즘을 적용하여 암호화된 고유 식별 값을 전송하는 안전한 초기식별 상호인증을 수행하는 프로토콜을 설계하였다. 제안하는 시스템 전체 구성은 (그림 2)과 같다. LTE 네트워크 탐색 프로토콜에서 RNTI 외의 암호화에 사용할 임의난수를 시도응답기반의 상호인증을 수행하며 서로 받은 임의난수를 Milenage 알고리즘으로 연산한다. 연산된 결과는 암호화 키를 사용해 사용자 단말기를 유일하게 식별할 수 있는 RNTI 값을 암호화하여 UE 추적 가능성을 방지한다.

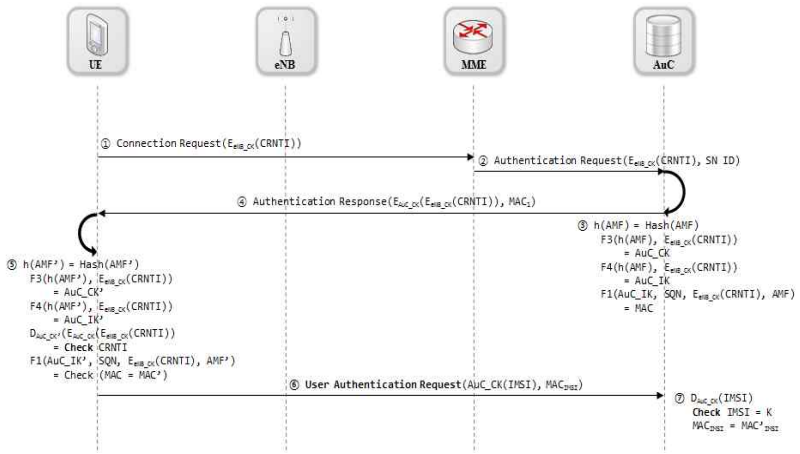
LTE Security 프로토콜의 상호인증 프로토콜에서 사용자를 식별할 수 있는 IMSI와 TMSI 값을 사전 공유된 키와 앞서 암호화된 RNTI값을 Milenage 알고리즘에 대입하여 임시 비밀키를 생성한다. 생성된 임시 비밀키를 이용하여 사용자 식별값(IMSI)을 암호화한다. 인증센터에서는 사용자 단말기로부터 전송 받은 메시지로 임시 비밀키를 생성하여 사용자 식별자를 얻은 후 해당 사용자 단말기와 사전 공유된 키를 이용해 새로운 상호인증 키를 생성함으로써 안전한 상호인증 프로토콜을 제공한다.



[그림 2] Authentication Protocol

3.2 상세 프로토콜

초기식별 암호화 프로토콜은 UE와 AuC간의 상호인증을 수행하는 프로토콜로써 UE와 AuC간의 사전 공유된 키와 암호화된 RNTI값을 활용하여 Milenage 알고리즘으로 임시 키를 생성하고, 상호인증 수행 후 IMSI값을 임시 키로 암호화하여 전송한다. AuC에서 IMSI를 확인해 사전 공유된 K값을 Milenage 알고리즘을 이용하여 암호키를 생성하는 프로토콜이다. 초기식별 암호화 프로토콜의 상세 절차는 다음 [그림 3]와 같다.



[그림 3] RNTI Protocol

- STEP 1 (UE→MME) : eNB와 접속동기화를 마친 UE는 AuC로부터 사용자 인증을 받기 위해 Connection Request(Msg)를 전송한다.
- STEP 2 (MME→AuC) : UE에게 받은 메시지에 자신의 네트워크아이디인 SN_ID를 첨부하여 AuC에게 인증요청
- STEP 3 (AuC) : MME로부터 인증요청을 받은 AuC는 자신이 갖고 있던 AMF(Authentication Management Field) Default값을 해쉬한다. MME로부터 받은 Msg와 해쉬 연산된 AMF를 Milenage알고리즘 F3과 F4 함수에 적용하여 암호화키와 무결성키를 생성한다.
- STEP 4 (AuC→UE) : AuC는 전달받은 Msg = EeNB_CK(CRNTI) 과 AuC가 알고 있는 AMF 값과 함께 암호화한다. EAuC_CK(Msg)에 대한 무결성을 검증하기 위해 MACA를 생성하고 UE에게 Authentication Response 메시지를 갖는다(??).
- STEP 5 (UE) : UE는 자신이 알고 있는 AMF Default값을 해쉬 연산한다. 해쉬된 AMF값과 자신이 갖고 있는 EeNB_CK(CRNTI)를 F3(h(AMF), Msg) = AuC_CK과 F4(h(AMF), Msg) = AuC_IK과 같은 과정을 통하여 암호화키 AuC_CK'와 무결성 키 AuC_IK'를 생성한다. AuC로부터 받은 EAuC_CK(Msg)을 DAuC_CK'(EAuC_CK(Msg))과 같은 과정으로 복호화를 한다. 복호화하여 자신의 CRNTI와 같음을 확인하고 최종적으로 F1(AuC_IK', SQN, Msg, AMF') = MACA'를 통해 메시지를 검증함으로써 AuC를 인증한다.
- STEP 6 (UE→AuC) : UE는 AuC를 인증함으로써 IMSI를 암호화하여 암호화된 IMSI의 검증을 위한 MAC을 생성한다. UE는 User Authentication Request를 AuC에게 전달한다.
- STEP 7 (AuC) : 무결성 검증을 위해 DAuC_CK(EAuC_CK'(IMSI)) = IMSI을 통하여 무결성 검증을 한다. MAC이 일치하게 되면 AuC는 자신이 가지고 있던 AuC_CK를 가지고 복호화 과정을 갖는다. 복호화된 값을 통해 IMSI를 도출하게 되면 해당 IMSI에 맞는 K값을 탐색하여 추출한다.

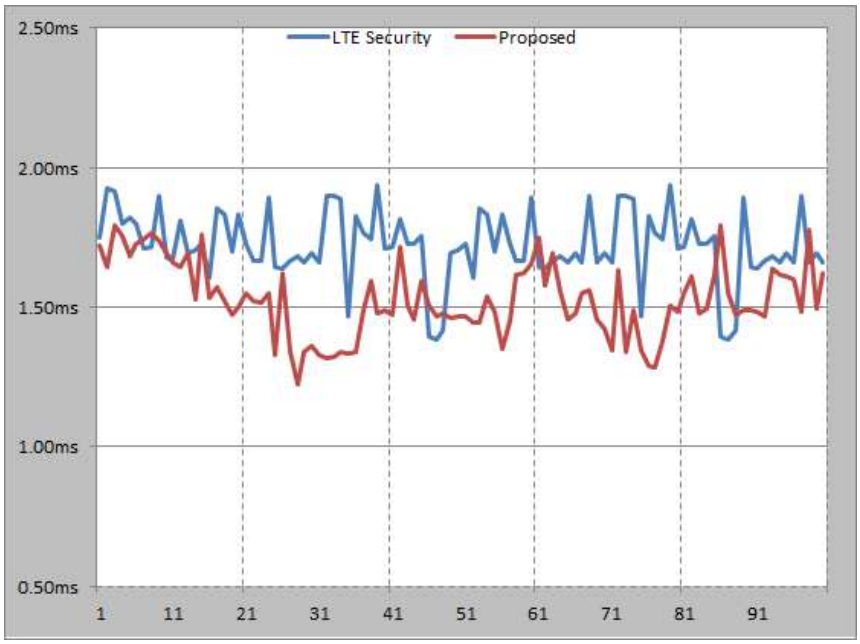
3.3 적합성 분석

제안 시스템의 적합성을 사용된 알고리즘의 횟수와 Algorithm Latency로 제안 시스템의 적합성을 분석하였다. 다음 <표1>은 기존 LTE Security 프로토콜과 제안 프로토콜의 적합성을 위하여 통신상에서 각각의 프로토콜에서 사용된 연산과 알고리즘의 수행 횟수를 비교분석한 기술한 내용이다.

<표1> LTE Security Protocol Operation Count

연산	LTE Security	제안프로토콜
Milenage F1(메시지 인증 코드 생성함수)	2회	2회
Milenage F2(네트워크 인증 코드 생성함수)	2회	2회
Milenage F3(비밀키 생성함수)	2회	4회
Milenage F4(무결성키 생성함수)	2회	4회
Milenage F5(익명키 생성함수)	2회	2회
HMAC-SHA256(해쉬함수)	11회	4회
AES-128 Algorithm(암/복호화 함수)	-	7회

[그림 4] 기존 LTE Security와 제안 프로토콜의 UE-eNB간 RRC 보안 계층과 사용자 단말기와 인증센터 간 상호인증 프로토콜을 100회 수행하여 나타낸 Latency 분석 그래프이다.



[그림 4] UE-AYC Authentication Protocol Latency

[그림 4] 는 기존 LTE Security 프로토콜의 RRC 보안 계층에서 Latency와 제안 프로토콜의 RNTI 암호화 프로토콜 Latency를 비교한 그래프이다. 아래 [Table. 1]과 같이 각 프로토콜의 연산 횟수는 다음과 같다. 제안 프로토콜이 최대 0.58ms 빠르다는 것을 보였고 기존 프로토콜보다 평균 0.19ms 빠른 것을 보였다.

Ⅳ. 결 론

본 연구에서는 본 논문은 LTE 네트워크에서 표준으로 사용되고 있는 LTE Security 프로토콜은 EPS-AKA를 기반으로 사용자 단말기와 사용자를 식별할 수 있는 초기 식별자를 상호인증시 노출되는 취약점이 나타나는 한계점으로 인해 UE 추적 가능성과 IMSI 노출로 인한 사용자 개인정보 노출 취약점을 보완하고자 Milenage 알고리즘 기반의 초기 식별자를 안전하게 암호화하여 LTE Security를 보완하는 상호인증 프로토콜을 제안하였다. UE가 LTE 네트워크에 접속하기 위해 eNB에게 접속요청을 보내게 되면 eNB는 셀내에 유일하게 UE를 식별할 수 있는 CRNTI을 전송하게 된다. CRNTI는 셀내에서 유일하기 때문에 CRNTI를 악의적인 사용자가 알게 된다면 해당 CRNTI를 부여받은 단말기 사용자를 추적할 수 있게 된다. 또한 어떤 공격도 없이 CRNTI가 전달이 잘되었다 하더라도 UE에서 LTE 네트워크 인증서버에 사용자 인증을 받기 위해 IMSI를 평문으로 전송하기 때문에 이중노출에 대한 취약점이 있다. 따라서 본 논문에서는 UE나 사용자 식별값을 알 수 없도록 암호화를 수행하는 상호인증 프로토콜을 설계하였다.

본 논문에서는 제안 프로토콜의 적합성을 분석하기 위해 프로토콜에 사용되는 연산 횟수와 Latency를 기존 LTE Security 프로토콜과 비교분석한 결과 UE-eNB간의 RRC 보안 프로토콜은 LTE 통신에 적합하다는 결과를 얻었다. 반면에 암호화 절차가 많은 UE-AuC간 상호인증 프로토콜에서는 기존 LTE Security보다 오래 걸릴 수 있지만 LTE-Advanced 요구사항인 Latency 50ms내에 수행되기 때문에 LTE 통신 요구사항도 충족시

켰다. 본 논문에서 제안한 프로토콜은 단일 통신으로 식별값 노출 취약점을 해결하였지만 UE-AuC간 상호인증 프로토콜에서 기존 프로토콜보다 높은 지연시간을 보였다. 따라서 향후에는 UE-AuC간 상호인증 프로토콜에 Latency를 낮춰 보다 빠르고 기밀성이 보장된 프로토콜에 대한 연구가 지속적으로 되어야한다.

REFERENCE

한국인터넷진흥원(2014), *LTE 및 4G 이동통신망 구조 분석 및 보안 위협 연구*, KISA-WP-2012-0037, 106-118.

한국인터넷진흥원(2011), *펨토셀 및 GRX 보안 취약점에 대한 연구*, KISA-WP-2011-0033, 49-58.

AlZain, M. A., E. Pardede, B. Soh, and A. T. James(2012), "Cloud computing security : From single to multi-clouds," *45th Hawaii International Conference on System Sciences. IEEE*, 5490-5499.

Boneh, D(1998), "The decision diffie-hellman problem," *International Algorithmic Number Theory Symposium.* Springer Berlin Heidelberg, 1423, 48-63.

Casalicchio, E., and M. Palmirani(2015), "A cloud service broker with legal-rule compliance checking and quality assurance capabilities," *Procedia Computer Science*, 68, 136-150.

Choi, C. H.(2014), "CPND ecosystem ICCT (Information, Communication, Contents Technology)." *Journal of Digital Convergence*. 12(3). 7-16.

Halpin, H.(2014), “The W3C web cryptography API: Motivation and overview,” *W3C, WWW'14 Companion*, 7(14), 62-79.

Han, J. H.(2015), "Effects of perceived usefulness and ease reliance on payment services and loyalty mall," *Journal of Digital Convergence,* 13(12), 75-87.

Han, C. K., H. K. Choi, J. W. Baek, and H. W. Lee(2015), “Evaluation of authentication signaling loads in 3GPP LTE/SAE networks,” 21-30.

ISO/IEC 13157-2:2010, Information Technology - Telecommunications and Information Exchange between Systems - NFC Security - Part 2: NFC-SEC Cryptography Standard using ECDH and AES

Kim, E. H.(2011), "Cloud service brokerage," *Internet & Security Issue*, 27-32,

Lee, J. K., J. G. Son, H. M. Kim, and H. K. Oh(2013), "An authentication scheme for providing to user service transparency in multicloud environment," *Journal of The Korea Institute of Information Security & Cryptology*, 23(6), 1131-1141.

Lee, S. H.(2015), “Actual cases and analysis of IT convergence for green IT,” *Journal of the Korea Convergence Society*, 6(6), 147-152.

TTA(2010), *IMT-2000 3GPP-LTE RAN/3GPP SAE 내에서 보안 결정에 관한 가능성 연구*, TTAT.3G-33.821, 41-48.

Won, S. H., and H. S. Yang(2015), "Research and policy direction for the success of ICT-based company fusion," *Journal of Digital Convergence,* 13(4), 39-50.

A Design of MILENAGE Algorithm-based Mutual Authentication Protocol for The Protection of Initial Identifier in LTE

Yoo, Jae-hoe[1)]
Kim, Hyung-uk[2)]
Jung, Yong-hoon[3)]

Abstract

In LTE environment ,which is 4th generation mobile communication systems, there is concern about private information exposure by transmitting initial identifier in plain text.

This paper suggest mutual authentication protocol, which uses one-time password utilizing challenge-response and AES-based Milenage key generation algorithm, as solution for safe initial identification communication, preventing unique identification information leaking. Milenage key generation algorithm has been used in LTE Security protocol for generating Cipher key, Integrity key, Message Authentication Code. Performance analysis evaluates the suitability of LTE Security protocol and LTE network by comparing LTE Security protocol with proposed protocol about algorithm operation count and Latency.Thus, this paper figures out initial identification communication's weak points of currently used LTE security protocol and complements in accordance with traditional protocol. So, it can be applied for traditional LTE communication on account of providing additional confidentiality to initial identifier.

Keywords: *AES-based Milenage key, MILENAGE Algorithm, LTE Security, private information*

1) Author,Department of Computer Science and Engineering, Soongsil University, hwe100@ssu.ac.kr
2) Corresponding author, Korea Electronic Certification Authroity, do3196@naver.com
3) Co-author, BaaS Lab, jung7773@naver.com

저 자 소 개

■유 재 회(Yoo, Jae-hoe)
■숭실대학교 컴퓨터학과 박사과정
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI

교 신 저 자 소 개

■김 형 욱(Kim, Hyung-uk)
■한국전자인증, 수석연구원
■숭실대학교 컴퓨터학과 공학박사
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI

공 동 저 자 소 개

■정 용 훈(Jung, Yong-hoon)
■바스랩, 연구소장
■숭실대학교 컴퓨터학과 공학박사
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI