IMT-2000기반 컨텐츠 서비스를 위한 보안 프로토콜

이 덕 규[†] · 이 임 영[††]

요 약

IMT-2000은 인터넷 서비스와 멀티미디어 고속 데이터 정보 등 유선에서 제공하고 있는 서비스 대부분을 무선으로 공급하고자하는 사용자의 요구 충족을 위해 등장하였다. 그러나 글로벌 로밍시 신호 데이터 및 사용자 데이터가 타 사업자의 망을 거쳐 전송된다. 또한 고속의 데이터 통신이 제공됨에 따라 기밀성 보호에 필요한 데이터 통신 량이 증대될 것으로 판단된다. 최근 IMT-2000 사업은 2002년을 기점으로 상용 서비스가 진행될 예정이다. 이러한 시점에서 무선 컨텐츠는 그 특성상 데이터에 대한 제 3자로부터의 불법적인 행위에 대해 많이 노출되어져 있다. 따라서 이동 통신 환경에서의 보안과 인증 문제는 필수적인 사항이라 할 수 있다. 이를 위해 본 논문에서는 기존의 IMT-2000 인증 방식 분석을 통해 더욱 안전하고 효율적인 인증 방식을 제시함과 동시에 무선 컨텐츠 제공에 있어 필요한 보안 프로토콜을 설계하고자 한다.

A Secure Protocol for Contents Service in IMT-2000

Deok-Gyu Lee[†] · Im-Yeong Lee[††]

ABSTRACT

IMT-2000 appeared in order to satisfy the desires of the uses who wish to supply through wireless most of the services being provided through wire, such as Internet services and multimedia high-speed data information. However, during global roaming, the signal data and the user data get transmitted through the networks of other users. Also, it is judged that with the provision of high speed data communication the amount of data communication necessary for confidentiality protection will increase. It is planned that the recent IMT-2000 project will begin its commercial service in 2002. From this viewpoint, wireless contents, due to their special characteristics, are greatly exposed to illegal actions by third persons. As a result, it can be said that security and certification issues in the mobile telecommunication environment are indispensable matters. For this purpose, it is intended that in this thesis through an analysis of the existent IMT-2000 certification method, a more safe and efficient authentication method is presented and, at the same time, a security protocol necessary in the provision of wireless contents is designed.

키워드 : IMT-2000, 컨텐츠 제공(Offered Contents), 상호 인증(Mutual Authentication)

1. 서 론

이동 통신은 1세대와 2세대를 거치면서 비약적인 발전을 거듭하였으며 많은 사용자가 발생하였다. 그러나 1세대와 2세대 이동 통신 서비스는 기본적으로 음성위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선 인터넷 통신 서비스 수요자의 요구를 충족시키지는 못하고 있다. 향후 무선에서는 음성위주의 서비스가 아닌 데이터와 이동 멀티미디어 서비스와 같이 고도화된 서비스를 통하여 얻을 수 있을 것이다. 이러한 이동 통신 서비스는 시간과 장소의 제약을 받지 않고 음성 및 데이터 서비스를 제공하는 편리함을 가지고 있는 반면에 사용자가 이동성을 가지고 있고 전파를 통신 매개로 이용하는 특성으로 인하여 보안상의 취약점을 가지고 있다.[7]

제 3세대 이동 통신 시스템인 IMT-2000(International Mobile Telecommunication-2000)의 특징은 현재 유선 망에서 제공하고 있는 서비스의 대부분을 무선망에서도 사용할 수 있게 하면서 유선 망에서의 품질을 보장한다는 목표를 가지고 있다. 그렇지만 무선망은 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다.

본 논문에서는 기존의 표준에서 제시한 묵시적 양방향 인증을 제공하는 것과는 달리 강력한 인증을 제공하기 위해 IMT-2000에서 사용하는 새로운 양방향 인증 프로토콜을 설계하였다.

이와 동시에 이를 바탕으로 암호화키와 무결성키를 가지고 컨텐츠 제공에 있어서의 보안 프로토콜을 제시한다.

2. IMT-2000 개요와 보안 구성도

본 장에서는 인증을 위한 IMT-2000 개요와 보안 구성

† 준 회 원 : 순천향대학교 대학원 전산학과
†† 종신회원 : 순천향대학교 정보기술공학부 교수
논문접수 : 2002년 9월 19일, 심사완료 : 2003년 1월 6일

도를 살펴본다[1, 5].

IMT-2000의 전체적인 목적과 보안 관련 부분 - 네트워크, 도메인 등에 관해 살펴보도록 한다. 기술하는 부분은 IMT-2000 상에서 전체적인 이해와 문제 제기 부분에 있어 중요한 부분이 된다.

2.1 IMT-2000 개요

IMT-2000은 International Mobile Telecommunication-2000의 약어로서 범세계적 이동 통신이란 뜻이다. IMT-2000이란 용어가 통용되기 시작한 것은 지난 1996년부터이다. 이전에는 미래공중육상이동통신(FPLMTS : Future Public Land Mobile Telecommunication System)이란 용어가 사용되었다. FPLMTS는 지난 1978년 국제전기통신연합(ITU)이 향후 이동 통신의 단일 표준화를 연구과제로 삼으면서 프로젝트 코드로 정했던 것이다[2, 3].

그러나 FPLMTS는 발음하기가 어렵고 뜻도 이해하기가 쉽지 않아 새로운 용어의 필요성이 제기 되었다. ITU는 FPLMTS가 사용하려는 주파수 대역(2000 MHz대)과 도입 시기(2000년경)를 고려, IMT-2000 이라는 이름을 고안하고 FPLMTS와 병행해 사용토록 권고했다. 현재는 이해하기 쉬운 IMT-2000이 표준용어로 굳어진 상황이고, 서비스 방식에 따라 북미방식인 동기식(cdma2000)과 유럽방식인 비동기식(W-CDMA)으로 나뉜다.

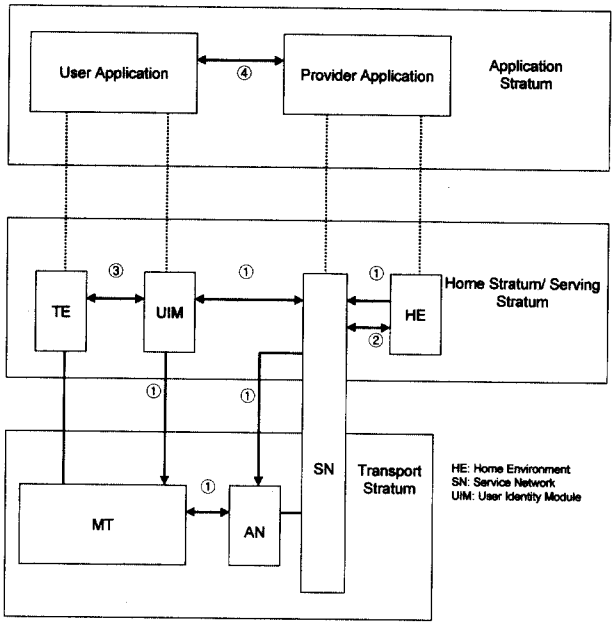
GSM(Global System for Mobile communication)이나 IS-95 CDMA(Code Division Multiple Access)시스템과 같은 2세대 이동통신 시스템과 비교하여 진보된 3세대 방식인 IMT-2000 시스템은 고속 멀티미디어 서비스 제공 및 글로벌 로밍을 특징으로 한다.

이러한 이동 통신의 환경의 변화는 정보보호에 대한 대책을 절실히 요구하고 있고, 또한 정보보호 기술도 새로운 환경 변화에 맞추어 발전해야 한다. 이에 부합하여 IMT-2000의 발전을 주도하고 있는 지역 그룹인 3GPP(3rd Generation Partnership Project)와 3GPP2(3rd Generation Partnership Project2)에서는 각각 자신들의 기술에 맞는 표준화 작업을 진행 중이다. 특히, 비동기 방식 표준을 제정하고 있는 3GPP는 ETSI(European Telecommunications Standards Institute), ARIB(Association of Radio Industries and Business), TTA(Telecommunication Technology Association), T1(T1 Committee), TTC(Telecommunication Technology Committee)로 구성되어 있고 여러 작업 그룹에서 활발한 활동을 보이고 있다. 보안 아키텍처, 인증 메커니즘, 암호 알고리즘 등과 같은 정보보호와 관련해서는 3GPP의 TSG SA WG3(Technical Specification Group Service and system Aspect Working Group 3)에서 담당하고 있다.

2.2 IMT-2000에서의 보안 요소

IMT-2000에서 보안을 제공하기 위한 구조를 (그림 1)에 나타내었다[1-5].

아래의 (그림 1)에서는 다섯 가지의 보안 관련 부분을 정의하였으며, 각각의 부분은 다음과 같다.



(그림 1) IMT-2000 보안 구성도

① 네트워크 엑세스 보안 : 3G(3rd Generation) 서비스에 대한 안전한 access 및 radio link 상에서 제3자의 attack 을 방지하는 기능을 제공한다.

② 네트워크 도메인 보안 : 네트워크의 유선구간에서 전송되는 정보의 보호 및 signaling 정보에 대한 보호를 제공한다.

③ 사용자 도메인 보안 : MS(Mobile Station)에 안전하게 access 하는 부분을 제공한다.

④ 어플리케이션 도메인 보안 : 사용자와 Service provider domain에서 안전하게 메시지가 전송되도록 하는 기능을 제공한다.

본 제안 방식에서는 4가지 부분 중에서 사용자 도메인 보안과 어플리케이션 도메인 보안 부분에서 이뤄진다. 두 부분 중에서 기본적으로 제공되어야할 네트워크 엑세스 보안, 사용자 도메인 보안에 대한 취약점을 살펴 본 후 이를 바탕으로 새로운 방식을 제안한다.

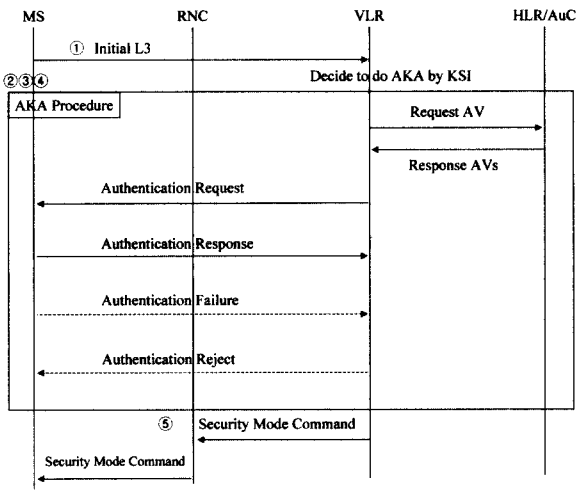
3. 3GPP 인증 매커니즘

3.1 인증 개요

3GPP에서의 가입자 인증은 USIM(Universal Subscriber

Identity Module)과 AuC(Authentication Center)가 같은 비밀키를 소유하고 있음을 증명함으로써 이루어진다. VLR (Visitor Location Register)은 서비스를 제공하기 전에 가입자를 인증하기 위해 HLR(Home Location Register)/AuC에 의해서 생성된 인증 벡터 AV(Authentication Vector)를 사용한다. 인증이 성공하면 VLR과 MS는 보안 모드에서 사용하는 암호화키(CK : Cipher Key)와 무결성키(IK : Integrity Key)를 공유한다. 그리고 VLR은 KSI(Key Set Identifier)의 값을 바탕으로 AKA(Authentication Key Agreement) 절차의 생략 유무를 결정한다[4-6].

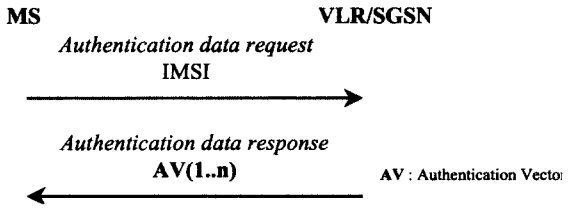
3GPP 인증 메커니즘에 대하여 간략히 전송되는 메시지를 위주로 나타낼 수 있다. 초기 전송되는 값(Initial L3)에 대하여 AKA 과정을 거쳐 마지막으로 Security Mode Command를 거치게 된다. 자세한 과정은 아래의 과정과 같다. ((그림 2) 참조)



(그림 2) 3GPP 인증 메커니즘

① 먼저 MS는 Initial L3 메시지를 MM(Mobility Management) 연결(connection) 과정에서 VLR로 전송한다.

② 실제로 AKA 과정이 일어나기 전에 MS와 RNC 사이에는 RRC(Radio Resource Control) 연결 설정이 일어난다. 이때 MS는 사용할 암호 알고리즘과 무결성 알고리즘 등을 RNC(Radio Network Controller)에 전송한다.



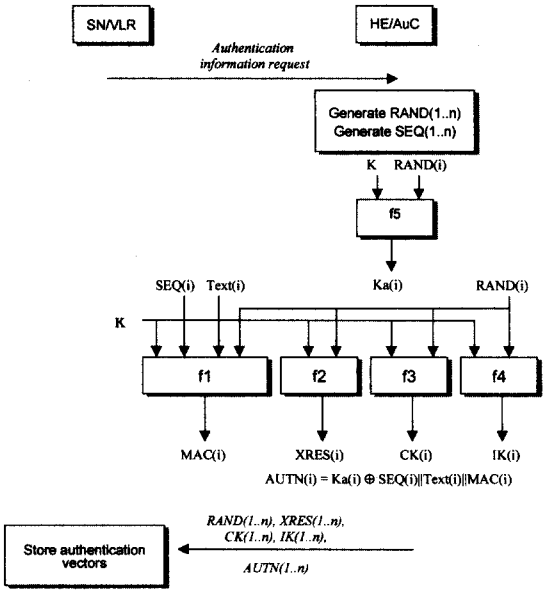
(그림 3) HE에서 SN으로의 인증 데이터 분배

③ Initial L3 메시지에는 사용자 ID, KSI, LAI를 포함하고 있어서 VLR은 KSI 값을 가지고 AKA의 수행여부를 판단한다. 이것과 관련해서 이전 가입자 방문망(VLRo)과 새로운 가입자 방문망(VLRn) 사이에는 ID (Identification) 확인 절차가 일어날 수도 있다.

④ AKA가 수행된다면 VLR은 HLR/AuC에게 인증 벡터 AV 생성을 요구한다.

: 인증 벡터 AV 생성과 분배의 과정은 다음과 같다.

- SN/VLR은 HE/AuC에게 인증 벡터 AV를 요구하는 authentication data request를 전송한다.
  - Authentication data request에는 IMUI 또는 EMUI가 포함된다.
  - EMUI가 포함될 경우는 복호화 과정이 필요하다.
- HE는 요구된 인증 벡터 AV에 대해 이미 생성한 경우는 DB를 통해 찾거나, SN의 요구에 따라 생성한다.
- 인증 벡터 AV를 위해 HE는 임의의 난수 RAND(i), 계속적으로 변경되는 SEQ(i)를 생성한다.
  - SEQ(i)의 생성은 다음과 같이 이루어 진다.
    - 2000년을 기준으로 현재가지 경과된 시간을 사용할 수 있다. 32비트가 사용될 경우 총 136년간 사용이 가능하다.
    - 각 개인이 유지하고 있는 SQN_{HE}는 이용하는 방법이 있다. SEQ를 $SQN_{HE}+1$처럼 SQN_{HE}를 증가 시키면서 사용하는 방법이다.
  - $XRES(i) = f2_K(PAR2 \parallel RAND(i))$,
    f2는 MAC 함수
  - Cipher key $CK(i) = f3_K(PAR3 \parallel RAND(i))$,
    f3은 키 생성 함수



(그림 4) 인증 벡터 AV의 분배(HE/AuC to SN/VLR)값

- Integrity key IK(i) = $f4_K$(PAR4 || RAND(i)), f4는 키 생성 함수
- Anonymity key AK(i) = $f5_K$(PAR5 || RAND(i)), f5는 키 생성 함수
- 인증 token AUTN(i) = SEQ(i) ⊕ AK(i) || Text(i) || $f1_K$(PAR1 || SEQ(i) || RAND(i) || Text(i)), f1은 메시지 인증 함수

• AK(i)는 sequence number를 감추기 위한 목적으로 사용된다. 이러한 sequence number의 보호는 replay attack에 대한 보호 작용을 하게 된다.

• PAR1, …, PAR5는 f1, …, f5가 동일허가나 유사한 함수인 경우에 서로 다른 고정된 초기 값을 갖게 된다

⑤ 인증이 성공하면 보안 모드(Security Mode) 단계로 들어간다.

3.2 인증과 Security 관련 절차

본 절에서는 각각의 인터페이스에서의 인증 절차에 관해서 좀더 구체적으로 살펴본다. 우선 VLR과 HLR/AuC 구간에서의 AKA에 대하여 살펴본 후, MS(Mobile Station)와 VLR 구간에서의 AKA, 이전 방문지로부터의 IMSI(International Mobile Subscriber Identity)와 인증 데이터 분배 마지막으로 보안모드 Setup 절차에 대하여 알아보도록 하겠다.

3.2.1 VLR과 HLR/AuC 구간에서의 AKA

만약 VLR이 사용자를 인증하는데 필요한 인증 벡터 AV (Authentication Vector)가 없다면 VLR은 HLR/AuC에 새로운 인증 벡터 AV를 요구하게 된다. 여기서 필요한 인증 벡터 AV는 MS의 인증과정에 필요한 사항으로 보안 모드에 들어가기 전에 인증과 키 동의 과정으로 거치기 때문이다. 따라서, VLR에 인증 벡터 AV가 없으면 인증 벡터 AV에 대한 요구로써 HLR/AuC에 요구 메시지를 전송하며 이에 응답으로 인증 벡터 AV를 전송 받는다. 전송하는 메시지는 node identity, node type과 IMSI를 포함하는 메시지를 보내고, HLR/AuC은 이에 응답해서 인증 벡터 AV를 생성한 다음 VLR에 전송한다.

3.2.2 MS와 VLR 구간에서의 AKA

이 구간에서의 AKA의 목적은 MS와 VLR이 인증을 하고, 새로운 암호화키(CK : Cipher Key), 무결성키(IK : Integrity Key)를 설정하는데 있다. 먼저, VLR이 RAND(Random Number), AUTN(Authentication Token), KSI를 포함하는 Authentication Request 메시지를 MS에 보내면 MS는 AUTN을 구성하는 요소중 하나인 MAC(Message Authentication Code)과 자신이 계산할 수 있는 XMAC(Expected Message Authentication Code)을 비교한다. 만약 두 개의 결과가 다르다면 MAC 실패에 대한 이유와 함께 Authentication Failure 메시지를 VLR에 전송하고, 같다면 MS는 USIM에 생성한 SQN_{MS}(Sequence Number)와 AUTN의 또 다른 한 요소인 SQN_{HE}과 비교한다. 그래서, SQN이 올바른 범위 내에 있는지를 판단하여 단말기의 네트워크에 대한 인증 성공 응답 메시지인 Authentication Response 메시지를 전송하거나, SQN 범위의 실패에 따른 Authentication Failure 메시지를 VLR에 전송한다. 만약 SQN이 올바른 범위 내에 있지 않으면, MS는 AUTS(Authentication Synchronization failure parameter)를 계산하고, 그것을 Authentication Failure와 함께 보낸다. 한편, MS가 네트워크를 인증하면 응답으로 RES(Response)를 계산하는데 이는 Authentication Response 메시지와 함께 VLR로 전송이 되어서 VLR이 가지고 있는 XRES(Expected Response)와 같은지를 비교할 수 있게 한다. 이 비교로 네트워크는 단말기에 대한 인증을 성공해서 인증 절차를 완료하거나, 인증 실패에 따른 Authentication Reject 메시지를 MS에 전송한다.

3.2.3 이전 방문망으로부터의 IMSI와 인증 데이터의 분배와 Identification 절차

이 절차는 동일한 SN(Service Network) 내에서 이전 방문망인 VLRo에서 새로운 방문망인 VLRn으로 인증 데이터를 제공할 때 발생한다. VLRn은 TMSI와 LAI를 포함하는 Initial L3 메시지를 MS로부터 받자마자 VLRo로 TMSI를 확인하기 위한 메시지를 전송한다. VLRo는 TMSI와 관련된 정보를 자신의 데이터베이스에서 찾아서 남아있는 암호화키, 무결성키 등을 VLRn에게 전송하거나, 혹은 TMSI 확인 실패 메시지를 전송한다. TMSI를 사용한 Identification 확인 절차가 실패할 경우, VLRn은 IMSI를 이용하여 MS와 Identification 확인을 하게된다.

3.2.4 보안 모드 setup 절차

MS와 HLR/AuC 사이에서 AKA가 성공적으로 완료되거나, KSI 확인으로 인한 AKA가 생략되면 보안 모드 협상 절차를 하게된다. 이 과정에서 사용할 암호 알고리즘을 선택하는 등 MS와 RNC 사이의 많은 협상 과정을 하게 되지만, 본 논문의 주제와는 약간 거리가 있으므로 상세히 다루지는 않는다. 하지만, 시스널링 메지지에 대한 무결성 체크를 하는 것은 필수적이다.

4. 3GPP 인증 매커니즘 취약성

본 장에서 3GPP의 IMT-2000 상에서 나타나는 취약점에 대하여 기술한다. Network Access Security Mechanism을 바탕으로 하여 임시신원의 증명, TMSI(Temporary Mobile Subscriber Identity) 재할당 절차, 임시신원 할당 부인, AKA

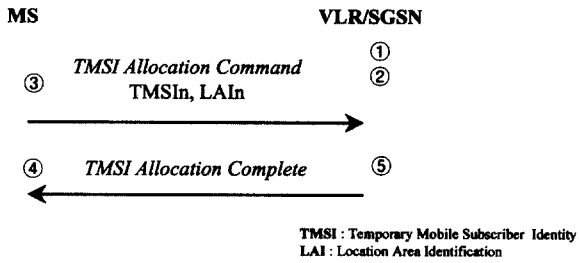
(Authentication and Key Agreement)에 관하여 살펴보도록 한다[13, 14].

4.1 임시 신원의 증명

일반적인 사항은 다음과 같다. Radio link 상에서 사용자의 식별은 임시 식별자를 사용하게 되며, 사용자의 등록 시에 해당 지역에서 이루어지고 그 지역에서만 유효한 값을 갖는다. 사용자의 등록 시에 사용자의 영구 식별자와 임시 식별자 사이의 관계가 현재 VLR(Visitor Location Register)에서 보관된다.

4.2 TMSI 재할당 절차

무선 구간에서 사용자의 식별을 위한 절차는 새로운 TMSI (Temporary Mobile Subscriber Identity)와 LAI(Location Area Identification)의 쌍으로 사용자에게 할당된다. 할당 절차는 초기 암호화 단계를 거친 후에 이루어진다. (그림 5)에서는 TMSI 할당 절차를 나타내고 있다.



(그림 5) TMSI 할당 절차

① 초기에 VLR이 시작한다.
② VLR은 IMSI(International Mobile Subscriber Identity)와 새로운 TMSIn을 DB에 저장한다.
③ MS에게 TMSIn과 LAI를 전송한다.
④ MS는 TMSIn을 수신하면 이전 TMSI를 삭제하고 VLR에 ack를 송신한다.
⑤ VLR은 ack를 수신하면 IMSI와 TMUIo에 대한 관계를 DB에서 삭제한다.

위 TMSI 할당 절차에 있어 다음과 같이 TMSIn값이 저장되어 MS의 ack를 받아야만 TMSIn을 DB에서 삭제하게 되므로 만약 MS의 ack를 전송받지 못하게 되면 DB는 그대로 남아 있게되어 VLR에 DB에 대한 공격이 이루어 질 수 있다.

또한 TMSI값과 IMSI값에 대한 관계가 DB에 저장되어 있으므로 TMSI를 이용하여 IMSI를 알아낼 수 있다.

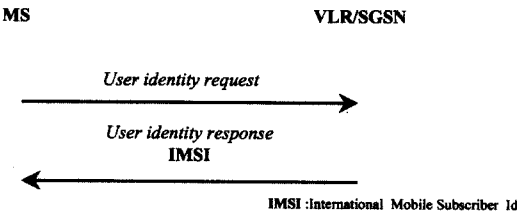
4.3 임시 신원 할당 부인

SN(Service Network)이 사용자로부터 임시 신원 할당의 성공을 승인 받지 않고, 네트워크는 예전의 임시 신원 TMSIo과 IMSI, 새로운 임시 신원 TMSIn과 IMSI 집합을 유지한다. 사용자로부터 비롯된 처리, 네트워크는 예전 임시 신원 TMSIo 또는 새로운 임시 신원 TMSIn 중에 하나로 자신의 신원을 사용자에게 확인한다. 사용자 확인은 2가지의 방법으로 이루어 질 수 있다.

첫 번째 방법으로 위치 이동에 따른 위치 갱신의 경우 사용자 인증은 TMSIo/LAIo 쌍을 사용하는 경우 VLRn 방문, IMSI는 DB로부터 규칙을 가지고 올 수 있다.

두 번째 방법은 영구적인 신원으로 증명하는 것인데 이 매커니즘은 영구적인 서명자 신원을 매개로 신호 통로에 사용자 증명을 허락한다.

(그림 6)에서는 임시 신원 할당 절차를 나타내고 있다.



(그림 6) 임시 신원 할당 절차

임시 신원 할당, 인증, 키 동의가 Global Authentication에 해당할 수 있다. 이러한 전체 적인 부분에 있어서 IMT-2000에서 Authentication 실제 적용시 예측되는 공격은 다음과 같다.

4.3.1 SN에서의 DataBase에 대한 공격

SN에는 TMSI와 IMSI를 매핑시켜줄 수 있는 DB가 존재하게 되는데 이 SN에 대한 사용자 위장 공격으로 SN에서 불법 사용자는 IMSI를 취득할 수 있다. 취득한 IMSI를 이용하여 여러 서비스에 접근이 용이하므로 전체 시스템에 악영향을 줄 우려가 있다. 또한 IMSI는 인증과 키 동의(AKA)과정 전에 비교하여 사용자를 확인하게 되는데 이를 통해 사용자의 Key에서 위험도 커지게 된다.

4.3.2 SN과 HE사이의 인증 데이터 요구시 가로채기 하여 도용

SN과 HE사이에서의 인증 데이터 요구시 인증 벡터 AV는 Quintet의 형태로 암호화가 되지 않은 채 전달된다. 이 과정에서 도청자의 인증 벡터 AV의 수집으로 인증 데이터의 도용이 이루어 질 수 있다. 인증 정보의 도용이 SN과 HE 상에서뿐만 아니라 전체적인 Handshake 상에서 이루어 질 수 있다. 따라서 Quintet의 보호는 필수적이라 할 수 있다. SQN(Sequence Number), RAND(Random Number), 암호화키(CK : Cipher Key), 무결성키(IK : Integrity Key) 등에 대한 노출로 인해 사용자 인증 정보에 대한 노출 우

려가 있다.

4.3.3 SN이 인증 벡터 AV를 이용할 경우

위장 기지국인 경우 SN은 HE로 받은 인증 벡터를 MS에게 넘겨주게 되고 계산되어진 SRES 값을 이용할 수 있다. 이 경우 위장 SN이 사용자 정보를 수집하여 임의의 K를 생산해 공격할 수 있다. 또한 악의적인 목적을 가지는 SN의 경우 인증 벡터 AV를 폐기하지 않고 인증 벡터 AV를 이용하여 사용자로 위장하여 서비스를 사용할 수 있다.

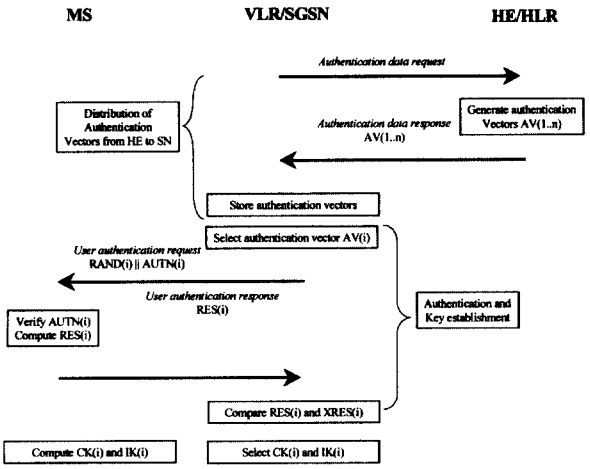
4.4 AKA(Authentication and Key Agreement)에 대한 취약점

4.4.1 일반 사항

사용자와 네트워크 사이의 비밀 정보인 비밀키 K의 값을 서로가 알고있음을 보여줌으로써 상호 인증을 하는 방식을 사용하고 있다. 비밀키 K의 값은 USIM(Universal Subscriber Identity Module)과 HE(Home Environment)에서 보관하고 있으며, 네트워크 인증을 위해 SEQ_{MS}와 SEQ_{HE}도 보관된다. (그림 7)에서는 인증 방식을 보여주고 있다.

인증 수행은 사용자의 HE내의 AuC(Authentication Center)와 사용자 MS내의 UIM에서 이루어진다. 인증의 수행 과정에 필요한 요구사항은 다음과 같다.

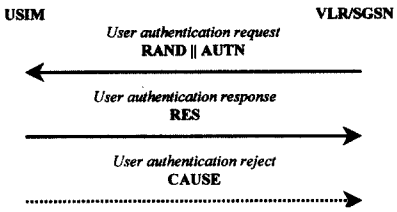
- HE/AuC에서 SN/VLR로의 인증 정보의 전달이 있다. 이 때 인증 정보가 안전하게 전달하기 위하여 SN/VLR은 HE가 신뢰한다고 가정한다. 또한 SN/VLR과 HE 사이에는 안전한 intra-system 링크가 존재한다고 가정한다. 사용자는 HE를 신뢰한다.
- SN/VLR과 MS 사이의 새로운 암호 키와 무결성키를 인증하고 설정하는 과정이 있다.
- 이전 방문한 VLR로부터 새로운 VLR로의 인증 데이터 전달이 있다. 이 때 SN/VLR 사이의 링크는 안전하다고 가정한다.



(그림 7) 인증 데이터의 흐름

4.4.2 인증과 키 동의

이 프로시져의 목적은 사용자의 인증과 VLR/SGSN과 USIM 사이에서 새로운 암호키와 무결성키 쌍을 확립하는 것이다. (그림 8)은 인증과 키 동의 프로시져에 관한 사항이다.



(그림 8) 인증과 키동의 프로시져

다음과 같이 인증과 키동의에 대해 간략히 소개하였다.

여기에서는 이것에 관한 3GPP 표준 문서 내의 취약성에 대하여 살펴보도록 하겠다.

4.4.2.1 SQN 동기화하는 과정에서의 도청 공격

이것은 SQN(Sequence Number)의 번호 생성은 3가지로 볼수 있는데 시간에 의존하여 만들어진 SQN, 시간에 의존하지 않은 SQN, 또한 MS Module을 이용한 SQN이 있는데 이중에서 MS와 시간에 의존하여 만들어진 SQN의 경우에는 SQN에 대한 예측이 가능하며 초기 설정시 SQN에 대한 도청으로 불법적인 사용이 가능하다.

4.4.2.2 인증 벡터 AV(SN과 MS 사이에서)재사용이 불가능

인증 벡터 AV는 AUTN이 n개가 생성되어 SN에 전달되게 됨으로 HE와 SN 사이에서의 도청으로 AUTN를 수집하여 key값 K를 결정할 수 있다. 또한 사용자로 위장하여 인증에 실패하여 SN에게 새로운 벡터 AV 값을 취득함으로써 수집을 통해 알아낼 수 있다.

4.4.2.3 SN과 HE 사이에서 인증 수행

표준 문서에서는 SN과 HE 사이의 인증 과정 없이 신뢰된 통신로라고 지칭되어있다. Quintet 혹은 인증 벡터 AV (Authentication Vector)에 대한 보호 없이 전송로 상에서 전송된다. 이러한 취약점으로 인해 SN과 HE 사이의 SN의 인증없이 데이터에 대한 전송은 위장 SN 공격에 당할 위험이 있으며 또한 사용자의 위치 추적이 가능해 질 수 있다.

5. 보안 요구 사항

다음은 기존 방식의 취약성을 바탕으로 제안방식에서 기본적으로 가져야 할 보안 요구 사항에 대하여 기술한 것이다.

5.1 네트워크 내의 안전한 데이터베이스

MS의 인증 인자와 HE의 인증 인자에 대하여 불법적인

데이터베이스 접근에 의한 사용자 프로파일을 획득하거나 조작하여 프라이버시를 위협하거나 불법복제에 사용될 수 있다. 이러한 이유로 MS의 인증 인자와 HE의 인증 인자의 보관을 위한 안전한 데이터베이스가 필요하다.

5.2 비밀키의 사전 공유

인증에 있어 MS와 HE가 비밀키 K에 대해 서로 알고 있다는 가정 하에 상호 인증을 하고 있다. MS와 HE는 비밀키를 사전에 공유해야 한다.

5.3 SN과 HE 사이의 신뢰확보

SN과 HE 사이의 신뢰성 확보는 매우 중요하다. SN의 불법적인 MS 정보 도용 및 데이터베이스에 대한 안전한 접근제어를 제공하지 않는다면 서비스를 제공할 수 없을 것이다.

5.4 SN과 HE 사이의 안전한 통신 채널 필요

SN과 HE 사이의 통신상에는 MS 인증에 대한 인증 인자와 HE에 대한 인증 인자가 있으므로 인증 인자에 대한 가로채기, 불법복제에 대하여 안전해야 한다.

6. 제안 방식

앞에서 살펴보았듯이 3GPP 표준안에서는 기본적으로 묵시적인 상호 인증을 제공하고 있다. 본 논문에서는 무선링크에서의 보안에 관련된 서비스를 제공하는 네트워크 도메인 보안과 어플리케이션 도메인 보안에 대해 인증 프로토콜과 보안 프로토콜을 설계한다. 특히 인증 절차에 있어 MS에서 HE로, HE에서 MS로의 인증이 가능하도록 하기 위하여, 두 가지 인증 방식을 통합하여 양방향 인증 프로토콜을 설계하였으며, 컨텐츠 제공을 위한 보안 프로토콜을 제안하였다. 무선링크에서의 보안에 관련된 서비스를 제공하는 네트워크 도메인 보안과 애플리케이션 도메인 보안에 대해 인증 프로토콜과 보안 프로토콜을 설계한다.

따라서 본 제안 방식은 기존의 묵시적 양방향 인증 방식의 취약점을 개선한 것으로서 보다 안전한 무선 컨텐츠 서비스를 제공할 수 있다.

6.1 구성 요소

본 방식에서 구성하는 요소에 대하여 설명한다. 사용자가 이용하는 USIM, ME와 서비스를 제공하는 SN/VLR, 사용자 인증과 인증 벡터 AV를 제공하는 HE/AuC로 구성된다. 다음은 각각의 구성 요소에 대해 특징 및 고려사항을 살펴보도록 한다.

6.1.1 MS

Mobile Station로서 ME와 USIM을 통칭하는 단어이다. HE 혹은 SN에서 공통으로 ME와 USIM에게 제공되는 인자는 MS로 표기되어 있으며, 사용도 MS가 사용하여 ME와 USIM에게 전달하는 것으로 표현되어 있다.

6.1.2 USIM

Universal Subscriber Identity Module로서 ME의 컨텐츠 제공과 인증을 위한 인자를 가지고 있다. USIM은 저장공간이 있으며, Random Number Generator(이하 RNG)를 포함한다. 이 RNG는 MS가 HE를 인증시에 필요로 하며, 작은 RNG로서 HE에 대한 인증을 취할 수 있다.

6.1.3 ME

Mobile Eqipement로써 암호화와 복호화를 수행할 수 있으며 연산능력을 가지고 있다. HE에 대한 인증 인자를 생성한다. Sequence Number는 ME가 생성할 수 있으나, HE에서 생성된 Sequence Number를 사용하며, Random Number는 USIM의 도움을 받는다. ME와 HE내의 f1~f5의 함수는 사전에 정의되어 있다.

6.1.4 SN/VLR

Service Network로서 MS와 HE의 중간에서 도움 역할을 하여 인증 과정을 수행한다. 자체 데이터베이스는 인증 인자를 보관한다. SN은 MS로부터 전달받은 인증 인자를 보관하였다가 HE의 인증이 완료되면 MS로부터 받은 인증 인자를 데이터베이스에서 삭제한다. 이와 반대로 HE로부터 받은 인증 인자에 대한 처리는 MS가 SN의 서비스를 벗어난 경우에 처리한다.

6.1.5 HE/AuC

Home Environment/Authentication Center로서 MS와 같이 비밀키 K를 공유한다. MS에 대한 인증 인자를 생성한다. 인증에 따른 암호화키, 무결성키 등 인증 인자를 생성하고 이를 SN과 MS에게 전송하며, 컨텐츠를 제공하는데 SN은 인증 인자 중에서 암호화키, 무결성키를 이용하여 제공하게 된다.

6.2 시스템 계수

다음은 본 논문에서 인증과 컨텐츠 보호에 필요한 시스템 계수에 대해 설명한다.

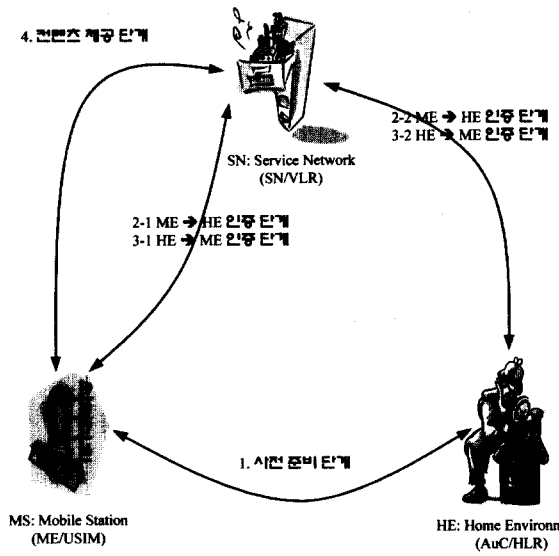
- * : (US : User, HE : Home Environment, SN : Service Network)
- RAND* : *가 생성한 Random Number
- Kh : Sequence Number를 보호하기 위해 사용되는 값
- Ka : 사용자가 생성한 Kh에 대한 비교 값
- AUTN* : *의 Authentication Token (US : User, HE : Home Environment)
- *RES : Authentication check value (URES : User Authentication check value, XRES :

Home Environment check value, HRES : Service Network Authentication check value)

- PAR : Parameter
- $F2_K$: HRES 생성 함수
- $F3_K$: 암호화키 생성 함수
- $F4_K$: 무결성키 생성 함수
- $F5_K$: Kh 생성 함수, Kh에 대한 Ka 검증
- CK : 암호화키(Cipher Key)
- IK : 무결성키(Integrity Key)
- SEQ : Sequence Number
- M : Contents File
- SCF : Service Contents File
- MID : Media ID
- ID : User Identity
- K_T : Temporary Key
- K_S : Storage Key
- H : Storage Key에 대한 해쉬 함수
- K* : Contente에 사용되는 키 값(무결성키(IK : Integrity Key), 암호화키(CK : Cipher Key))
- SEQ* : *가 생성하는 SEQ(US : User, HE : Home Environment)

6.3 전체 흐름도

다음은 본 방식에서의 전체 흐름도에 대하여 기술한다. 전체적인 흐름은 MS와 HE 사이에서의 상호 인증 단계와 MS와 SN에서의 컨텐츠 제공단계로 이뤄지게 된다.



(그림 9) 제안방식 전체 그림

6.4 사전 준비 단계

다음은 인증 절차와 컨텐츠 제공에 있어 사전에 준비하는 단계이다.

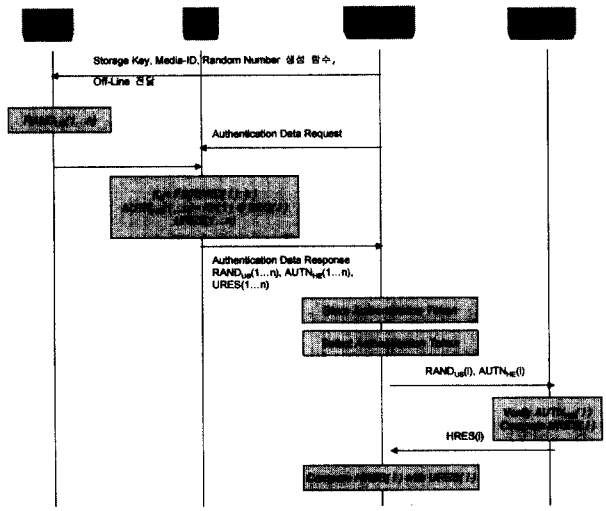
Step 1 : 비밀키 K에 대한 교환은 사전에 MS와 HE 사이에서 이루어져야 한다. 비밀키 K에 대해 사전에 공유되며 USIM와 HE에 보관되어진다.

Step 2 : USIM(Universal Subscribe Identity Module)는 Smart Card로 구성되어지며 Smart Card 내에 삽입될 항목은 SN에서 MS에게 Off-line으로 전달되어져야 한다.

Step 3 : 컨텐츠에 대해 Watermarking 기법이 행해져 불법적인 복제는 검출될 수 있어야 한다.

6.5 MS에서 HE로의 인증 단계

MS가 처음 SN의 service 환경으로 접속시의 인증 인자에 대한 요구 및 HE에 대한 인증 절차에 대해 설명한다.



(그림 12) MS에서 HE로의 인증 단계

Step 1 : SN으로부터 Storage Key, Random Number 생성 함수, Media-ID를 포함하여 Smart Card로 전달된다.

Step 2 : MS가 SN내에 위치하게 되면 SN은 HE 인증을 위한 인증 데이터를 요구한다.

Step 3 : HE에 대한 인증 데이터 요구에 대해 MS는 인증 인자를 생성한다.

- $RAND_{US}(1\cdots n)$
- $Kh(1\cdots n) = F5_K\{RAND_{US}(i) : K\}$
- $AUTN_{HE}(1\cdots n) = Kh(i) \oplus SEQ_{US}(i)$
- $URES(1\cdots n)$

Step 4 : ME은 USIM의 도움을 받아 인증인자를 생성하고 생성한 인증 인자를 SN에 전달한다.

- $RAND_{US}(1\cdots n)$
- $AUTN_{HE}(1\cdots n)$
- $URES(1\cdots n)$

Step 5 : SN은 ME로부터 받은 인증 인자를 자신의 DB에 저장한다.

Step 6 : SN은 n개의 인증 인자 중에서 하나의 인증 인자

를 선택하여 HE에게 전달한다.

- $RAND_{US}(i)$, $AUTN_{HE}(i)$

Step 7 : HE는 SN으로부터 전달받은 인증 인자로부터 HRES(i)를 계산한다.

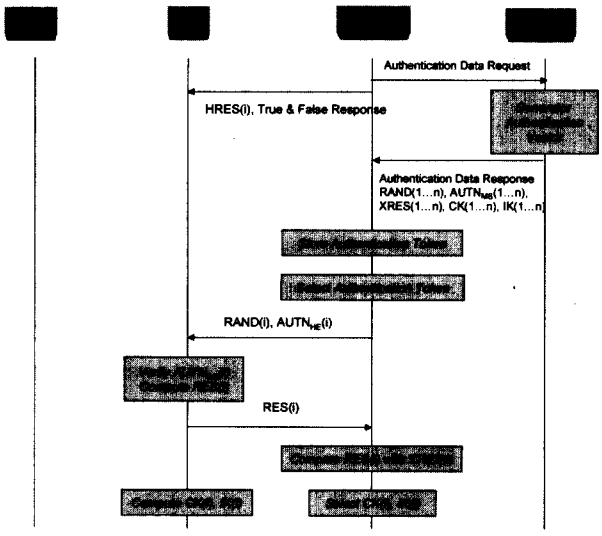
- $Kh(i) = F5_K\{RAND_{US}(i) : K\}$
- $AUTN_{HE}(i) = \{Kh(i) \oplus SEQ_{US}(i)\} \oplus Kh(i)$
- $HRES(i) = F2_K\{RAND_{US}(i) : K\}$

Step 8 : SN은 HE로부터 전달받은 HRES(i)와 URES(i)를 비교한다.

- Compare HRES(i) = URES(i)

6.6 HE에서 MS로의 인증 단계

이 단계에서는 상기 ME가 생성한 인증 인자에 대해 HE에서 인증이 완료되었을 경우 SN이 HE에게 인증 인자를 요구하고 응답 받은 인증 인자를 가지고 MS에 대한 인증 절차에 대한 설명을 한다. 인증 절차가 모두 완료되었을 경우 MS와 SN은 무결성키(IK : Integrity Key), 암호화키(CK : Cipher Key)를 생성한다.



(그림 11) HE에서 MS로의 인증 단계

Step 1 : SN은 MS의 인증을 위해 HE에게 인증 데이터를 요구한다.

Step 2 : SN은 전달받은 두 값을 비교한 값에 대해 동일하면 인증된 것으로 하고 MS에게 통보한다.

- Compare HRES(i) = URES(i)

Step 3 : HE는 SN의 인증 데이터 요구에 대한 MS 인증 인자를 생성한다.

- $Ka(i) = F5_K\{RAND_{HE}(i) : K\}$
- $MAC(i) = F1_K\{SEQ_{HE}(i) : Text(i) : RAND_{HE}(i) : K\}$
- $XRES(i) = F2_K\{RAND_{HE}(i) : K\}$
- $CK(i) = F3_K\{RAND_{HE}(i) : K\}$
- $IK(i) = F4_K\{RAND_{HE}(i) : K\}$
- $AUTN_{US} = [(Ka(i) \oplus SEQ_{HE}(i)) \| Text(i) \| IK(i)]$

Step 4 : HE는 생성한 인증 인자를 SN에게 전달한다.

- $RAND_{HE}(1\cdots n)$
- $XRES(1\cdots n)$
- $CK(1\cdots n)$
- $IK(1\cdots n)$
- $AUTN_{US}(1\cdots n)$

Step 5 : SN은 HE로부터 전송받은 인증 인자를 자신의 DB에 저장한다.

Step 6 : MS는 SN은 n개의 인증 토큰 중에서 하나의 인증 인자를 선택하여 MS에게 전달한다.

- $RAND_{HE}(i)$, $AUTN_{US}(i)$

Step 7 : MS는 SN으로부터 전달받은 인증 인자로부터 MS는 XRES(i)를 계산한다.

- $Ka(i) = F5_K\{RAND_{HE}(i) : K\}$
- $AUTN_{US}(i) = \{Ka(i) \oplus SEQ_{HE}(i)\} \oplus Ka(i)$
- $XMAC(i) = F1_K\{PAR1 : SEQ_{HE}(i) : RAND(i) : Text(i)\}$
- $XMAC(i) = MAC(i)$

Step 8 : MS는 RAND로부터 생성한 RES(i)를 SN에게 전송한다.

- $RES(i) = F2_K\{PAR2 : RAND(i)\}$

Step 9 : MS는 RES(i)를 전송한 뒤, IK(i)와 CK(i)를 계산한다.

- Generate IK(i), CK(i)

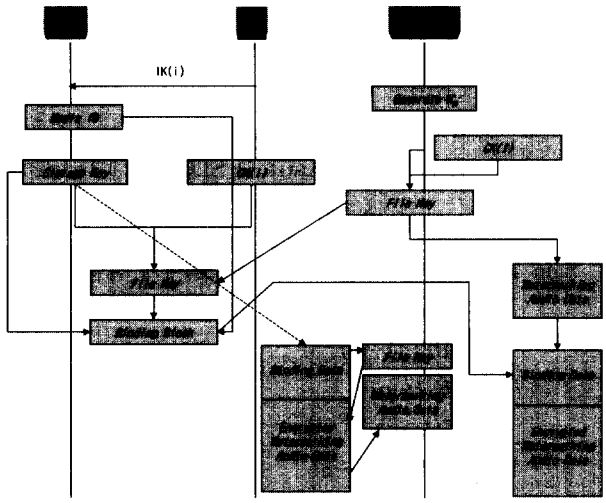
Step 10 : SN은 수신한 RES(i)를 XRES(i)와 동일한지 검사한다. 같으면 인증된 것으로 한다.

- Compare RES(i) = XRES(i)

Step 11 : SN은 HE가 보낸 $AUTN_{US}$의 IK(i)와 CK(i)를 선택한다.

6.7 MS와 SN에서의 컨텐츠 제공 단계

이 단계는 HE에서 MS로의 인증 단계로서 생성한 무결성키(IK), 암호화키(CK), Media-ID와 Storage Key를 가지고 컨텐츠를 보호함과 동시에 인증된 사용자에게 컨텐츠를 제공하는 과정이다.



(그림 12) MS와 SN에서의 컨텐츠 제공 단계

Step 1 : ME는 USIM에 IK(i)를 저장한다.

Step 2 : SN에서 컨텐츠에 대하여 암호화한다.

① 임의의 생성키 K_T로 하여 음악 파일 M을 암호화한다.

② SN에서는 생성된 File Key 암호정보를 MS에게 제공한다.

- $K_{CK}(K_{IK} \| K_T)$

Step 3 : MS는 암호화된 Binding Block SN에게 제공한다.

① 암호화된 File Key를 수신하여 File Key를 확인한다.

- $T = K_{CK}(K_{IK} \| K_T)$

② 이를 이용하여 Binding Block을 생성하여 SN에게 전송한다.

- Binding Block = $K_{CK}(H(K_S) \| K_T(K_S) \| MID_{US} \| H(T \| K_{IK}))$

Step 4 : SN에서는 MS에서 온 Binding Block에 대해 복호화하고 확인한 다음 암호화된 컨텐츠에 연접한다.

① Binding Block을 복호한다.

- K_{CK}(Binding Block)
  $= K_{CK}(K_{CK}(H(K_S) \| K_T(K_S) \| MID_{US} \| H(T \| K_{IK}))$
  $= H(KS) \| KT(KS) \| MIDUS \| H(T\|KIK)$
- Compare $H(K_S) = H(K_S)'$

② SCF(Service Contents File) 파일을 구성해 USIM를 사용하는 MS에게 전송한다.

- $SCF = (Binding\ Block \| K_T(M))$

Step 5 : MS에서 SN으로부터 전달된 컨텐츠를 사용한다.

① Binding Block 확인
Storage Key를 이용하여 File Key 복구하여 비교한다.

- $K_T(K'_T(K_S))$

② 확인된 File Key를 이용하여 컨텐츠를 이용한다.

7. 비교 분석

본 논문은 기존 표준 3GPP 제시된 인증 프로토콜의 묵시적 양방향 인증에 대하여 취약점을 개선하였다. 기존의 HE에서 MS로의 단방향 인증이 아닌 MS에서 HE로의 인증을 추가함으로써 양방향 인증을 실현하였다. MS에서 HE로의 인증과 HE에서 MS로의 인증을 실현하였는데 초기 3GPP에서 제공하는 방식에서는 단지 사전에 공유한 키 K에 대하여 MS를 인증하는 방식을 취하고 있다. 하지만 앞에서 문제 제기에서도 보았듯이 악의적인 공격자 혹은 악의적인 SN에 의해서 사용자 위장 공격이 가능해지므로 인해 문제점이 발생하게 된다. 이러한 문제점에 대해 본 방식에서는 MS에서 HE로의 인증 과정을 추가함으로써 이러한 문제점을 해결하였다. RES, URES, HRES, XRES를 이용함으로써 MS와 HE 간의 묵시적인 상호 인증을 강력한 상호 인증 체계를 구축함으로써 차후 글로벌 로밍시 문제시 될 수 있는 부분을 해결하였다고 사료된다.

또한 MS의 효율성을 고려하여 MS와 HE 사이의 함수 f1~f5를 이용하게 함으로써 양방향 인증에 따른 또 다른 인터페이스의 사용이 필요치 않게 되었다.

본 논문에서는 표준안을 크게 벗어나지 않는 범위에서 묵시적 양방향 인증이 아닌 명시적 인증 절차를 제공하였다. 함수 또한 표준에서 언급하고 있는 함수를 사용하게 하였다.

본 논문에서 제시하고 있는 컨텐츠 제공 서비스는 SN에서 MS로의 컨텐츠 전송을 나타내고 있다. 컨텐츠 제공 단계는 사전 인증 단계에서 제공된 암호화키(CK : Cipher Key)와 무결성키(IK : Integrity Key)를 이용하여 컨텐츠를 제공한다. 또한 암호화키와 무결성키뿐만 아니라 Media-ID와 K_T를 이용하여 컨텐츠를 암호화하여 제공한다. 이때 MS에서 SN에게 제공되는 Binding Block을 생성하여 제공하게 되는데 이것은 컨텐츠 사용자에게만 컨텐츠를 제공하여 컨텐츠의 불법사용을 막는데 있다. 무선으로 제공되는 컨텐츠는 보호되어야한다. 이에 따라 컨텐츠 자체에는 암호화를 취하지 않고 Binding Block을 이용하여 사용자에게 컨텐츠를 제공하기 때문에 컨텐츠 자체에 대한 암호화 없이 제공받은 사용자는 Binding Block으로부터 인가된 사용자임을 확인하고 컨텐츠를 사용하게 된다. SN에서는 컨텐츠 자체에 암호화를 하지 않고 Binding Block을 이용하기 때문에 MS

의 부담을 줄여 빠른 속도로 사용자가 컨텐츠를 접근할 수 있도록 하였다. 또한 유선의 컨텐츠 제공에서와 같이 라이센스 서버로의 접속없이 사용할 수 있으므로 사용자는 라이센스 서버와 같은 곳의 접속을 하지않고 컨텐츠를 획득할 수 있다.

8. 결 론

무선 이동 통신의 비약적인 발전을 통해 그 사용자가 기하급수적으로 증가하고 있다. 그러나 1세대와 2세대 이동 통신 서비스는 기본적으로 음성위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선 통신 서비스 수요자의 요구를 충족시키지는 못하고 있다.

제 3세대 이동 통신 시스템인 IMT-2000은 현재 유선 망에서 제공하고 있는 서비스의 대부분을 무선망에서도 사용할 수 있게 하면서 유선 망에서 품질을 보장한다는 목표를 가지고 있다. 그렇지만 무선망은 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다.

컨텐츠 제공에 있어 인가되지 않은 제 3자에게는 서비스가 원천적으로 이루어지지 않아야 하며 서비스는 반드시 인가된 사용자에게만 이루어져야 한다. 이러한 문제점을 해결하기 위해 본 논문에서는 기존의 일방향 인증성을 가지고 있는 문제점을 보완한 양방향 인증을 제공하고 이를 통해 컨텐츠 제공에 있어 보안 프로토콜을 제시하였다.

따라서 본 제안 방식은 기존의 묵시적 양방향 인증 방식의 취약점을 개선한 것으로서 더욱 더 안전한 무선 컨텐츠 서비스를 제공할 수 있다. 또한 제안된 방식은 컨텐츠를 제공함에 있어 MS의 효율성을 고려하여 제안하였다. 또한 제 3자로부터의 컨텐츠에 대한 불법적인 접근과 불법복제에 대해 검출할 수 있다. 앞으로 더욱 많은 연구를 통해 전자상거래 멀티미디어 컨텐츠 제공에 있어 충분한 활용이 가능하리라 판단된다.

참 고 문 헌

[1] 3GPP TS 33.102, "3rd Generation Partnership Project (3GPP) ; Technical Specification Group Services and System Aspects ; 3G Security security Architecture."

[2] 3GPP TS 22.022, "3rd Generation Partnership Project (3GPP) ; Technical Specification Group Services and System Aspects ; Personalisation of UMTS Mobile Equipment (ME) ; Mobile functionality specification."

[3] 3GPP TS 33.103, "3rd Generation Partnership Project (3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; integration Guidelines."

[4] 3GPP TS 33.105, "3rd Generation Partnership Project (3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Cryptographic Algorithm Requirements."

[5] 3GPP TS 33.120, "3rd Generation Partnership Project (3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Security Principles and Objectives."

[6] 3G TR 33.901, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Criteria for cryptographic algorithm design process."

[7] 3G TR 33.902, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Formal Analysis of the 3G Authentication Protocol."

[8] 3G TR 33.908, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms."

[9] ETSI SAGE, "Security Algorithm Group of Experts (SAGE) ; General Report Design, Specification adn Evaluation of The MILENAGE Algorithm Set : An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions."

[10] ESTI SAGE, "Specification of the MILENAGE Algorithm Set : an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$," Document 1 : Algorithm Specification.

[11] ESTI SAGE, "Specification of the MILENAGE Algorithm Set : an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$," Document 2 : Implementors' Test Data.

[12] ESTI SAGE, "Specification of the MILENAGE Algorithm Set : an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$," Document 3 : Design Conformance Test Data.

[13] ITU : ITU-R SECURITY PRINCIPLES FOR INTERNATIONAL MOBILE : TELECOMMUNICATIONS-2000 (IMT-2000) Recommandation ITU-R M.1078.

[14] ITU : EVALUATION OF SECURITY MECHANISMS FOR IMT-2000 : RECOMMENDATION ITU-R M.1223.

[15] "정보통신 표준화 백서", 정보통신부, 2000.

[16] 정원영, 정 욱, "IMT-2000 보안 위협 및 대책", 1999.

이 덕 규

e-mail : hbrhcdbr@catholic.or.kr

2001년 순천향대학교 컴퓨터공학과 졸업

2003년 순천향대학교 전산학과 석사과정

2003년~현재 순천향대학교 전산학과 박사과정

관심분야 : IMT-2000, PKI, DRM

이 임 영

e-mail : imylee@sch.or.kr

1981년 홍익대학교 전자공학과 졸업

1986년 오사카대학 통신공학전공 석사

1989년 오사카대학 통신공학전공 박사

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 정보기술공학부 부교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안