主題

차세대 이동통신 서비스를 위한 보안 기술

대구가톨릭대학교 컴퓨터정보통신공학부 교수 전 용 희

차 례

I. 서 론

이동 통신 시스템의 최종적인 목표는 광범위한 사용을 위하여 정보통신 서비스에 대한 유비쿼터스 접근을 제공하기 위한 것이다. 이 목적을 달성하기 위하여, 여러 가지 많은 기술적인 문제들이 극복되어야 하지만, 그 중에서도 특히 비인가된 사용자로부터 네트워크와 가입자 자원을 보호하는 것이 매우 중요한 과제 중의 하나이다. 이러한 보호는 네트워크에서 비밀성, 인증 및 접근 제어를 통하여 실현될 수 있다. 따라서 본 고에서는 이 문제에 대하여 기술하고자 한다[10].

보안은 공중 교환 전화망(PSTN: Public Switched Telephone Networks), 근거리 통신망(LAN: Local Area Networks)과 같은 유선통신 시스템에서 보다 무선 통신시스템에서 더욱 중요한 역할을 차지한다. 이와 같은 무선 통신시스템 환경을 위한 보안에는 크게 무선 사용으로 인한 무선 보안(Wireless Security)과 사용자의 이동성을 지원하기 위한 이동 보안(Mobile Security)으로 구분될 수 있다. 무선 보안에서는 무선 환경으로 인하여 나타날 수 있는 재밍(jamming) 현상, 데이터 삽입이나 수정, 중간자 공격 등과 같은 위협에 대처하기 위하여 주파수 호핑(hopping)과 같은 기법을 이용하여 대처하는 분야이고, 이동 보안은 이용자의 서비스 중 위치 변경에 따른 위협에 대처하기 위하여, 권한 검증 및 인증 등과 같은 기법을 이용하여 대처하는 영역이라 할 수 있다[1,3,5,6]. 따라서 무선 환경에서의 보안이 부분적으로 포함되겠지만, 본 고에서는 특히 3G(3rd generation)와 4G 시스템의 이동 통신 서비스를 위한 보안 기술에 대하여 초점을 맞추고자 한다[10-12, 16, 19].

4G 시스템의 중요한 측면은, 네트워크 레벨에서 이종의 액세스 네트워크 기술의 통합과 서비스 레벨에서 부가가치 서비스와 기반 네트워크

능력을 이용하는 애플리케이션의 통합이라고 말할 수 있다. 이렇게 함으로써 언제 어디서라도 항상 연결성을 허용할 수 있는 것이다. 4G 네트워크에서 보안, 특히 종단 사용자 인증 및 비밀성이 매우 중요하다[7]. 위에서 기술하였듯이, 4G 비전으로 이기종 액세스 네트워크 기술의 통합을 포함하기 때문에, 통합될 필요가 있는 바로 첫 번째 항목이 개별 네트워크를 위한 보안 메커니즘이다. 4G에서의 인증 메커니즘은 종단 사용자에게 투명하여야 하며, 그리하여 일상 비즈니스 상에서 방해받지 않아야 된다. 결론적으로, 여러 가지의 인증 기법이 적용될 때 끊임없는(seamless) 로밍이 어렵다. 그러므로 서비스와 네트워크 레벨에서 인증(보안) 기법의 통합과 합병이 필요하다. 이와 같은 통합 보안을 위하여 서비스 레벨과 네트워크 레벨에서 사용자 신분 확인사이의 일관성 있는 링크를 획득하고 유지하여야 하며, 이 확인(인증)을 확립하기 위하여 공통된 수단이 있어야 하며, 일단 가입자가 성공적으로 로그인 되면, 비밀성이 보장되어야 한다.

4세대 이동통신 개발을 위한 표준화 또는 기술 개발은 ITU-R의 WP8F(Working Party 8F), EU(European Union)의 WWRF(Wireless World Research Forum), 일본의 mITF(Mobile IT Forum), 중국의 FuTURE(Future Technologies for Universal Radio Environment), 우리나라의 NGMC(Next Generation Mobile Communication) 등에서 추진되고 있다[2,4].

2. 보안 위협 및 요구사항

2.1 비밀성 정의

사용자의 비밀성이 고려될 때, 다음과 같이 네 가지 수준의 비밀성이 정의될 수 있다[10, 21].

- 없음(None) : 비밀성이 없는 것이다. 이 경우 누구라도 호나 스캐너를 사용하여 데이터를 감청할 수 있다. 사용자에게 호의 불안전한 성질에 대하여 정보를 주는 비밀성 지시자(Privacy Indicator)가 수반되어야 한다. 이것의 예로는 호의 시작부에 "이 회선은 안전하지 않다"는 것과 같은 매 15-20 초마다 간단한 비프 톤을 사용할 수 있다. 이것이 시스템이 제공해야 할 최소 수준의 비밀성이다.
- WEP(Wired Equivalent Privacy) : 이것은 무선 네트워크에 의하여 제공되는 비밀성이 대응되는 유선과 같아야 한다는 것을 의미한다. 안전한 시스템을 제공하도록 해독하는데 일년 이상 소요되는 암호 시스템이 설계되어야 한다.
- 상업적 안전(Commercially Secure) : 이 수준은 주식 거래, 인수 합병, 거래 협상과 같은 독점 정보를 다루는 것이다. 이 정도의 보안은 암호 시스템을 해독하는데 적어도 10-25 년 걸리는 것을 요구한다.
- 군사/정부 안전(Military/Government Secure): 이 수준은 군사 활동이나 정부 통신을 위하여 사용될 수 있다. 이 수준의 요구사항은 적절한 정부 기관에 의하여 정의될 수 있다.

2.2 보안 위협

이동 통신 환경에서의 종단간 통신은 기존의 네트워크와는 다른 다양한 특성을 가지고 있다. 따라서 이동 통신 환경에서의 보안 위협은 일반적인 보안 위협들뿐만 아니라, 이동 통신의 무선 특성과 단말기의 소형화와 같은 특성도 포함된다. 보안 위협 요소들로는 도청(eavesdropping), 통신 재밍과 같은 서비스 거부(DoS: Denial of Service) 공격, 데이터 삽입 및 변조 같은 무결성에 대한 위협, 비인가된 접근, 송수신 부인

(repudiation), 분실된 장치 사용 등이 있다. 아래는 무선 시스템에서의 보안 문제점들을 보여준다[18]:

- 서비스에 대한 부정한 액세스
  - cloning
  - channel hijacking
  - subscription fraud
- 사용자 비밀성
  - air interface 공격
  - 네트워크 공격
- 가용성
  - 서비스 거부(DoS)
  - 용량 과부하(capacity overload)
  - 네트워크 보안

2.3 요구사항

1) 가입자 보안 요구사항

이동 통신 시스템 가입자를 위한 보안 요구사항으로 다음과 같은 것이 있다[10].

- 종단 사용자 비밀성: 호 설정 정보(송신 번호, 송신 카드 번호, 요청 서비스 형태 등), 통화 내용에 대한 도청 보호, 데이터의 비밀성, 사용자 위치 비밀성, 호 패턴의 비밀성, 사용자 신원의 비밀성, 재정 거래의 비밀성.
- 로밍 지원: 로밍으로 인한 이동 사용자 인증
- 데이터 무결성 보호: 수신된 데이터의 변경 여부를 탐지하기 위한 수단이 네트워크 및 핸드 셋에 제공되어야 한다.
- 장비 혹은 서비스 절도 방지: 분실된 터미널의 재사용이 불가능하도록 암호 시스템 설계. 이동 전화 복제(cloning) 기술에 의한 서비스 절도 방지
- 최소 전력, 대역폭 및 암호 계산: 이동 통신 채널은 전력, 대역폭 및 핸드 셋의 전지 수명이 제한되기 때문에, 암호 시스템은 다음 요구사항을 고려해야 한다:
  - 알고리즘은 제한된 계산 복잡성을 가져야 한다.
  - 암호 시스템의 출력은 제한된 크기를 가지고, 시스템에 많은 오버 헤드를 주지 않아야 한다.
  - 이동 사용자와 네트워크 사이의 거래 수는 대역폭과 전력을 보존하기 위하여 가능한 한 최소가 되어야 한다.
- 암호 시스템의 갱신이 용이하도록 키 길이와 알고리즘의 융통성
- 기타 법적 요구사항

2) 인프라 보안 요구사항

이동 통신 인프라 보안은 네트워크 인프라의 물리적 보안, 인프라에 대한 접근 제어, 인프라의 가용성, 네트워크 관리 신호 보안과 같은 문제가 있는데, 이와 같은 인프라 보안에서의 과제는 다음과 같다[17]:

- 개방성: 증가된 시스템 개방성이 인프라 보안에 대한 더 높은 보안 요구사항을 둔다.
- 융통성 및 다중 기능성: 이기종 접근 기술위에 중단 없는 이동성을 가지고 음성, 데이터 및 멀티미디어 통신을 지원해야 한다.
- 표준 기술의 사용: IP 기반 보안 위협에 대한 기술이 개발되어야 한다.
- 중요 서비스: 점점 더 중요한 서비스가 이동 통신 시스템을 통하여 생성되고 제공되기 때문에, 이에 대한 대책이 필요하다.

이러한 목표를 기반으로, 차세대 이동 통신 시스템의 인프라 보안에 대한 주요한 요구사항은 다음과 같다.

- 모든 통신 네트워크의 요소가 여러 가지의 보안 공격에 저항적이도록 강화되어야 한다.
- 중요 인프라 요소가 식별되고 잘 보호되어

야 하며, 잉여(redundant) 요소의 필요성이 주의 깊게 평가되어야 한다.

- 토폴로지, 플랫폼 형태, 용량 등 네트워크의 내부 구조와 사용 형태, 계정 정보 등과 같은 고객 데이터에 대한 정보는 권한이 부여된 집단과 실제로 필요한 정도로만 이용 가능하여야 한다.
- 보안 공격을 탐지, 감시, 보고하기 위하여 침입탐지시스템(IDS: Intrusion Detection System)이 설치되어야 한다.
- 보안 공격에 대한 신속한 대응과 보안 침해의 자동 복구가 비즈니스 연속성의 확률을 증가시키고 공격의 영향을 완화시키기 위하여 제공되어야 한다.
- 네트워크는 관리가 용이하고 실제적이고 실현가능한 보안 정책이 개발되어야 한다.
- 다른 관리 도메인 네트워크의 신속한 결합은 인증, 무결성, 기밀성, 가용성 및 항-재생 공격 등과 같은 외부 공격자에 대하여 안전해야 한다.
- 인프라 보안과 생성될 신규 서비스 간의 상호 의존성이 최소화되어야 한다.
- 네트워크 관리 신호를 위한 인증성, 기밀성, 무결성, 항-재생 보호가 제공되어야 한다.
- 관리 도메인 사이의 상호 운용성이 포함된 도메인의 보안을 침해하지 않아야 한다.

3. 관련 기술

3.1 인증

인증 혹은 접근 제어는 네트워크 자산을 보호하기 위하여 필요하고 보안(혹은 비밀성)은 가입자 자산을 보호하기 위하여 요구된다. 무선 환경에서, 인증과 비밀성은 일반적으로 서로 관련이 된다. 왜냐하면, 사용자 데이터의 추가 암호를 위한 세션 키의 유도가 인증단계에서 행해지기 때문이다.

개인 통신 시스템에서 비밀성과 인증을 제공하기 위하여 두 가지의 단계가 있다[8,10].

- 인증 및 키 협약(AKA: Authentication and Key Agreement): 네트워크가 이동 사용자의 신원을 검증하고 추가적인 암호화를 위하여 세션 키가 통상적으로 유도되는 과정이다.
- 비밀성을 위한 암호화: 이전 단계에서 유도된 세션 키가 비밀성 제공을 위한 사용자 트래픽 암호화를 하기 위하여 사용되는 과정이다.

인증 및 키 협약은 일반적으로 세 가지-부분 보안 모델을 사용하여 기술될 수 있다.

1. Provisioning 과정 : 개인 핸드셋을 소유하고 있는 가입자가 네트워크로 하여금 자신을 합법적인 사용자로 인정하게 하는 방법이다.

2. 로밍 지원 과정 : 가입자가 등록된 홈 네트워크가 아닌 지역 네트워크에 대하여 신원을 검증하기 위한 과정이다.

3. 네트워크 접근 수락 및 키 설정 과정 : 비밀키 시스템에서는 단순한 수하-응답(challenge-response) 메커니즘이며, 공개키 시스템에서는 인증서의 교환이 필요하다.

3.1.1 비밀키 시스템

본 절에서는 2세대 시스템인 유럽의 GSM(Global System for Mobile Communications)과 북미 USDC의 비밀키 시스템에 대한 AKA 기법에 대하여 기술한다[10].

1) Provisioning

GSM에서, provisioning은 SIM(Subscriber Identity Module) 카드의 사용을 통하여 이루어

진다. 이 SIM 카드는 사용자가 서비스 제공자로부터 서비스를 구입할 때 발행된다. SIM 카드는 구입된 서비스에 대한 정보와 각 SIM에 유일한 "Ki"라고 하는 128비트 번호를 또한 포함한다. Ki가 네트워크로 하여금 사용자를 인증하도록 한다.

2세대 북미 USDC 시스템에서, provisioning은 서비스 구입 시 가입자에게 발행되는 "A-키"의 사용에 의하여 이루어진다. 이 A-키는 가입자에게 비밀스럽게 발행되는 64비트 값이다. 사용자는 키패드를 사용하여 자신의 핸드셋에 이 보안 파라미터를 입력해야 한다. 키의 정확한 입력은 핸드셋 내부에 있는 보안 소프트웨어에 의하여 검증된다. 서비스 제공자 또한 가입자 홈네트워크에 A키의 복사본을 저장하고 있다. 사용자의 A키로부터 "공유 비밀 데이터(SSD: Shared Secret Data)" 라고 하는 보안 변수가 유도된다. 이것은 사용자의 홈네트워크와 방문 네트워크 사이에서 공유하기 위한 것이다. A키도 GSM의 Ki와 마찬가지로 홈네트워크를 떠나지 않는다.

2) 로밍 접근 지원

2세대 시스템인 USDC와 GSM 모두 HLR(Home Location Register)과 VLR(Visitor Location Register)을 가지고 있다. HLR은 가입자의 계정 번호와 비밀키와 같은 빌링 정보를 저장하고 있다. 서빙 네트워크(SN: Serving Network)에 존재하는 VLR은 위치 데이터베이스이며 서빙 네트워크 상으로 그 지역에 로밍되는 사용자에 대한 정보를 저장한다. 사용자는 자신의 홈네트워크(HN)에서 SN으로 로밍하고, VLR에 사용자 핸드셋 등록을 하여 VLR에 의하여 인증이 수행된다. GSM에서는 HLR이 VLR에게 호 별로 수하 값, 기대되는 응답, 암호 키 정보를 전송한다. USDC에서는 SSD 값이 HLR로부터 VLR로 전송된다.

3) 인증 및 세션 키 설정

AKA 프로세스의 마지막 단계는 실제 인증 프로토콜이 따라오며 추가적인 암호화를 위한 암호키의 생성이다. GSM 시스템에서는, 임의의 수하/응답 쌍(challenge-response pairs)을 생성하거나 선택함으로써 인증을 시작하며, 인증을 위하여 모바일 단말에게 수하를 보낸다. USDC는 수하-응답 쌍을 생성하기 위하여 SSD 보안 변수 안의 정보를 이용한다. 여기서는, 32 비트 전역 수하(global challenge)가 빈번한 간격으로 생성되고 시스템 정보 채널상으로 서비스 지역을 통하여 방송된다. 서비스에 대한 접근을 필요로 하는 핸드셋은 현재 전역 수하와 SSD를 사용하는 알고리즘을 이용하여 18 비트 인증 응답을 계산한다. 이 인증 응답이 등록 및 호 설정 정보와 접합되어 검증을 위하여 홈네트워크로 보내진다. 만약 핸드셋이 인증된 것으로 발견되고 SN에 의하여 현재 서비스된다면, SSD가 SN에게 전송될 것이다. SN에서의 호 설정동안, SN에서 지역적으로 저장된 SSD 정보가 수하-응답 쌍과 추가적인 암호화를 위한 암호키를 생성하기 위하여 사용된다.

홈과 서빙 네트워크의 판단에 따라서 언제라도 인증이 수행될 수 있으며 사용자 신원은 공중 인터페이스(air interface)로 평문 형태로 전송되지 않는다.

3.1.2 공개키 시스템

3세대 PCS 표준을 위한 보안 및 인증 프로토콜은 대부분 기존의 2세대 GSM/USDC 표준의 결합으로 되어 있다. 기존 네트워크에서의 비밀키 메커니즘 이외에, 몇 개의 3 세대 제안은 추가적인 장점이 있는 공개 키 기법을 도입하고 있다. 3세대 PCS 시스템을 위하여 제안된 가능한 공개키 메커니즘은 대략 아래와 같다[8, 21].

1. 사용자가 서비스 요구를 위하여 전화기를 구입할 때 provisioning이 시작된다.
2. 그런 후 사용자는 그 신용장과 핸드셋에 대한 식별 정보를 가지고 신뢰된 인증기관(CA)을 접근한다.
3. CA는 정보의 정확성을 검증하고 자신의 개인키를 사용하여 정보의 코드된 버전에 디지털 서명을 한다. 이 서명은 CA가 아닌 어떤 다른 개체에 의하여도 위조될 수 없다. 이 서명이 사용자를 위한 '인증서'를 형성한다.
4. 어떤 PCS 네트워크도 CA의 공개키를 이용하여 인증서의 신빙성을 증명할 수 있다.
5. 인증서가 특별한 핸드셋을 제공하기 위하여 일단 발행되면, 지역 보안 신용장(local security credentials)이 등록 시에 서빙 네트워크와 확립된다.

3.1.3 IEEE 802.1X 인증 스킴

IEEE 802.1X 표준에서는 근거리 통신망(LAN) 하부구조의 물리적 액세스 특성을 사용하는 포트-기반 네트워크 접근 통제 메커니즘을 정의하고 있다. 점대점 연결을 확립하기 위한 액세스를 허락하는데 있어서, 장치의 LAN 포트를 위하여 802.1X에 의하여 인증이 제공된다. 802.1X의 경우, 인증자가 제공하는 서비스를 이용하기 위하여 인증받기를 원하는 파티를 탄원자(supplicant)라 한다. 인증 기능을 수행하는 엔티티를 인증 서버라 하며, 탄원자와 통신하기 위하여 RADIUS(Remote Authentication Dial-In User Service) 프로토콜을 사용할 수 있다. 802.1X 기반 인증은 Extensible Authentication Protocol (EAP)를 사용하기 위하여 설계되었다[13]. 가장 두드러진 EAP 방법으로 다음과 같이 세 가지가 있다:

- EAP-TLS(Transport Layer Security)[14]: 탄원자와 인증 서버 사이의 상호 인증이 X.509 기반 인증서를 교환함으로써 이루어진다. 양측이 다른 종단점의 인증을 성공적으로 검증하였다면, 세션을 암호화하기 위한 세션키가 유도된다. 이 방법의 장점은 고도의 보안에 있으며, 잠재적인 단점은 모든 탄원자에게 인증서를 분배해야 하는 것이다.
- EAP-TTLS(Tunneled TLS): 이 방법 역시 단방향 인증을 허용한다. 결과적으로, 인증 서버가 단지 인증서를 사용하고 소유하는 것이 요구되고, 탄원자는 인증 과정동안 터널된 사용자명 패스워드 결합을 통하여 인증될 수 있다.
- EAP-SIM(Subscriber Identity Module): 최근에 정의된 인증 방법으로[13], GSM 보안 메커니즘과 매우 관련 있다. 인증을 하고 세션 키를 생성하기 위하여, 탄원자 혹은 클라이언트에게 GSM SIM이 분배되어 있다고 가정한다. EAP 서버는 AAA(Authentication , Authorization and Accounting) 서버 상에 구현된 것으로 가정하며, GSM 네트워크와 인터페이스를 가져야 한다. SIM을 가지고 있는 사용자를 인증하기 위하여 비밀키와 인증 알고리즘이 SIM 상에 저장된다.

실제 단말의 예로, GSM 네트워크에서 사용자는 인증된 터미널의 소유와 그것을 활성화하기 위한 PIN 코드에 의하여 간접적으로 인증이 된다. 각 이동 단말은 공장에서 나올 때 IMEI (International Mobile Equipment Identity)라고 하는 고정된 식별 코드가 할당이 된다. Ireland Dublin에 위치한 CEIR(Central Equipment Identity Register)에서는 화이트리스트(white list)와 블랙리스트(black list) 데이터베이스를 유지하며 갱신한다. 블랙리스트에 등재된 단말은 네트워크 상의 접속이 차단된다[9].

3.2 데이터 암호화

802.11 표준 위원회에서는 기밀성, 인증 및 접근 통제, 계층관리를 제공하기 위하여 WEP (Wired Equivalent Privacy)를 채택하였다. 그러나 암호화 키가 쉽게 복구될 수 있는 위험성으로, 안전한 암호화 스킴으로 고려되지 않고 있다. 이 문제를 극복하기 위하여 IEEE 802.11i 그룹에서는 개선된 보안 애플리케이션에 대하여 작업을 수행하고 있다. 이것은 다음과 같이 두 단계로 분할 될 수 있다:

1) TKIP(Temporal Key Integrity Protocol)과 함께 WPA(Wireless Protection Access):

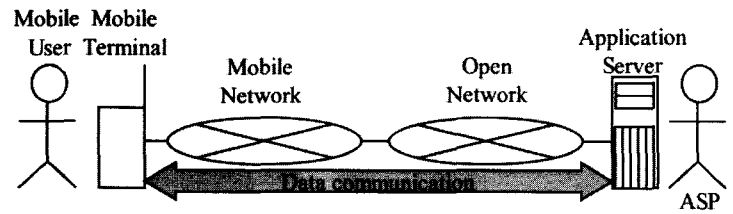
TKIP와 802.1X 인증을 포함한다. EAP와 결합하여 사용되는 802.1X가 인증을 통하여 증진된 보안을 제공한다.

2) Counter mode with CBC-MAC Protocol (CCMP) AES(Advanced Encryption Standard):

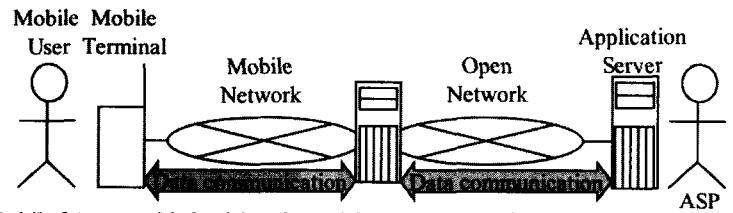
이 기능은 하드웨어로 구축될 필요가 있으며, 암호화를 위하여 하드웨어 가속기가 필요하다. 캡슐화 기법에서, TKIP는 WEP의 결점을 일시적으로 해결하려고 한다. 사실상, CCMP가 802.11 시스템의 보안 문제에 대한 장기간 솔루션이 될 것이다. 새로운 인증 및 암호화 기법이외에, 최근의 802.11i 드래프트는 동적인 암호화 키 및 키 관리를 위한 특징을 포함하고 있다. 키 관리 및 인증을 위하여, 802.11i는 IEEE 802.1X에 의존한다[7, 20].

4. 최근 표준화 기술 동향

본 절에서는 ITU-T를 중심으로 모바일 보안에 대한 최근 기술 동향에 대하여 살펴본다. 지난 3월에 개최된 ITU-T SG17 회의에서는 한국과 일본이 공동으로 제안한 표준안이 승인되었다. 두 가지 종류의 표준은 각각 X.1121과 X.1122로써, X.1121은 모바일 종점간 데이터통신을 위한 프레임워크를 제시하고 있다. 본 절에서는 이 두 가지의 표준에 대하여 소개하고자 한다[15].



Model1: General model of mobile end-to-end data communication between mobile user and ASP



Model2: Gateway model of mobile end-to-end data communication between mobile user and ASP

그림 1. 모바일 사용자와 ASP 간의 두 가지 데이터 통신 형태[15]

4.1 ITU-T X.1121

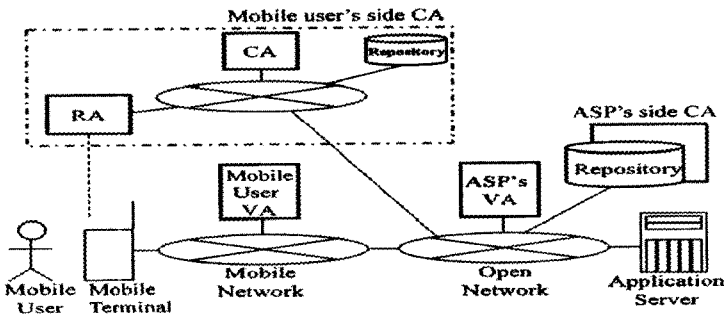
그림 1은 모바일 사용자와 응용 서비스 제공자(ASP: Application Service Provider) 간의 통신을 위한 두 가지의 모델을 보여준다. 모델 1은 게이트웨이 시스템을 사용하지 않고 직접 연결하는 일반적인 통신 모델이고, 모델 2는 게이트웨이를 사용한 모델이다.

모델 1은 모바일 사용자, 모바일 단말기, 모바일 네트워크, 개방 네트워크, 애플리케이션 서버 및 ASP로 구성되어 있음을 보여준다.

ITU-T의 X.1121에서 다루고 있는 주요 내용은 다음과 같다[5].

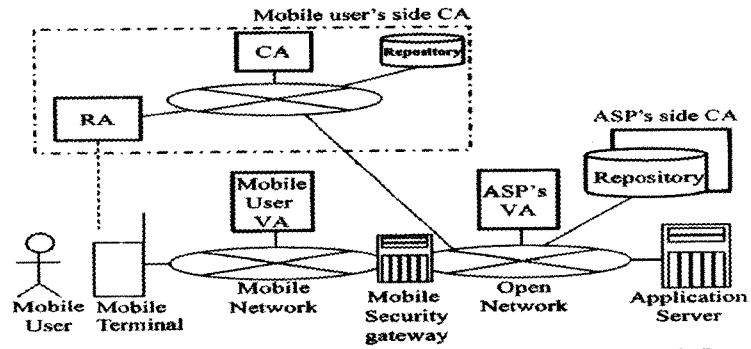
- 모바일 환경에서 종단간 통신을 위한 모델 정의
- 모방일 환경에서 종단간 데이터 통신에서의 특성 분석
- 모바일 환경에서의 위협 요소 정리
- 모바일 환경에서의 종단간 데이터 통신을 위한 보안 요구사항 정의 및 보안 기술
- 각 요구사항들을 고려한 보안 기능 정의

모바일 환경에서 발생 가능한 위협으로, 일반적인 통신망에서 발생하고 있는 보안 위협인 도청, 삽입, 변조, 삭제, 서비스 중단, 송수신 부인, 불법적인 접근과 무선 통신망에서 주로 발생하는 도청, 단말기 분실 및 도난, 입력 에러, 예고 없는 서비스 중단 등과 같은 보안 위협으로 구분되



Model1: General model of secure mobile systems based on PKI

그림 2. PKI 기반의 안전한 모바일 시스템을 위한 일반 모델[15]



Model2: Gateway model of secure mobile systems based on PKI

그림 3. PKI 기반의 안전한 모바일 시스템을 위한 게이트웨이 모델[15]

어 기술하고 있다. X.1121에서는 사용자 관점에서 요구되는 보안 서비스인 신분정보 관리, 기밀성 서비스, 무결성 서비스, 인증 서비스, 접근 제어 서비스 등의 서비스가 정의되었고, 애플리케이션 서비스 관점에서 요구되는 기밀성, 무결성, 인증, 액세스 제어, 가용성 등의 보안 서비스가 정의되었다.

X.1121은 향후 추가적인 모바일 표준을 개발하기 위한 기준 문서로 활용될 수 있을 것으로 기대된다.

4.2 ITU-T X.1122

이 문서는 PKI 기반의 안전한 모바일 시스템 구현을 위한 가이드라인 표준이다. 그림 2와 3은 PKI 기반의 안전한 모바일 시스템을 위한 일반 모델(그림 2)과 게이트웨이 모델(그림 3)을 보여준다.

이 문서에서는 키 생성 절차, 인증서 발급, 인증서 활성화, 단말기 획득 등의 절차를 발생 순서에 따라서 정의하는 다양한 서비스 운영 모델을 정의하고 있다. 이 문서에서는 다음과 같은 절차들을 규정하고 있다.

- 인증서 활용, 취소 및 갱신
- 인증서를 활용한 안전한 통신 채널 구축
- 세션 레벨 보안 기능을 위한 사용자 인증 및 응용 서비스 인증, 암호와 무결성 서비스 제공
- 애플리케이션 레벨 보안을 위한 서명과 암호 기능 제공
- 단말기 제조 회사의 인증서 발급
- 사용자의 단말기 인증서 발급
- 인증서 유효성 확인 및 취소

또한 두 가지 레벨을 가지는 보안 서비스에 대한 보안 요구사항을 정의하고 있다:

- 채널 레벨 보안 서비스: 사용자와 서버 인증, 무결성 서비스 등
- 애플리케이션 레벨 보안 서비스: 인증, 무결성, 디지털 서명 등

5. 사례 연구

5.1 3GPP 보안

3GPP(Third-Generation Partnership Project)는 진화된 GSM 코어 네트워크와 그것이 지원하는 무선 액세스 기술을 기반으로 하는 3세대 이동 통신 시스템이다. 이 절에서는 3G-UMTS 표준에 의하여 기술된 보안 특징의 개관에 대하여 기술한다.

5.1.1 보안 원칙

전반적인 3G 보안 구조는 세 가지의 기본 원칙을 기반으로 설계되었다[10].

- 3G 보안 구조는 2세대 시스템의 보안 특징 위에서 구축된다. 2세대 시스템의 어떤 견고한 특징은 유지된다.
- 3G 보안은 2세대 시스템의 보안을 개선한다. 2G 시스템의 몇 가지의 보안 허점과 단점이 3G 시스템에서 다루어지고 고쳐진다.
- 3G 보안은 새로운 특징을 제공하고 3G에 의한 신규 서비스를 안전하게 제공한다.

2G 시스템을 위한 보안 약점은 다음과 같다.

- 거짓 BTS(Base Station Transceiver)를 이용한 능동적인 공격이 가능하다. 이것은 모바일 시스템이 연결 설정동안 BTS의 신빙성(authenticity)을 조사하지 않기 때문에 발생한다. 단순히 자신에게 부과된 수하(challenge)에 응답한다.
- 암호키와 인증 데이터가 네트워크 사이와

내부에서 평문으로 전송된다.

- 대부분의 경우, 암호화는 무선 인터페이스에게만 적용된다. 코어 네트워크에 충분히 확장되지 않아 마이크로웨이브와 광 링크사이의 신호 전송에 평문을 사용한다.
- 2G 시스템에는 데이터 무결성이 없다.
- 2G 시스템은 갱신을 위한 융통성이 별로 없이 구축되었다.
- 서비스 네트워크가 로밍 가입자 인증을 위하여 제공된 인증 파라미터를 어떻게 사용하는지에 대한 지식과 제어가 홈 네트워크에 없다.

5.1.2 보안 구조

3G 보안 사양서는 5대 보안 특성 그룹을 정의하고 있다.

1. 네트워크 접근 보안
- 3G 서비스에 대한 안전한 접근을 사용자에게 제공한다.
- 무선 액세스 링크 상의 공격에 대하여 보호한다.

2. 네트워크 도메인 보안
- 공급자 도메인 내의 노드들이 신호 데이터를 안전하게 교환하도록 한다.
- 유선 네트워크 상의 공격에 대하여 보호를 한다.

3. 사용자 도메인 보안
- 사용자에게 모바일 스테이션에 대한 안전한 접근을 제공한다.

4. 애플리케이션 도메인 보안
- 사용자와 제공자 도메인 내의 애플리케이션들이 안전하게 메시지들을 교환하도록 해준다.

5. 보안의 가시성(visibility)과 배열성(configurability)
- 사용자로 하여금 보안 특징이 운용 중인지 아닌지에 대하여 알게 한다.
- 사용자로 하여금 서비스의 사용과 제공이 보안 특징에 의존해야 하는지에 대하여 알게 한다.

그림 4는 완전한 3G 보안 구조의 개관을 제공한다.

그림 4에서 번호는 3G에 의하여 제공되는 보안 특징과 직접 연관된다.

(1) 네트워크 접근 보안

정의에 의하면, 이 특징은 사용자 신원 기밀

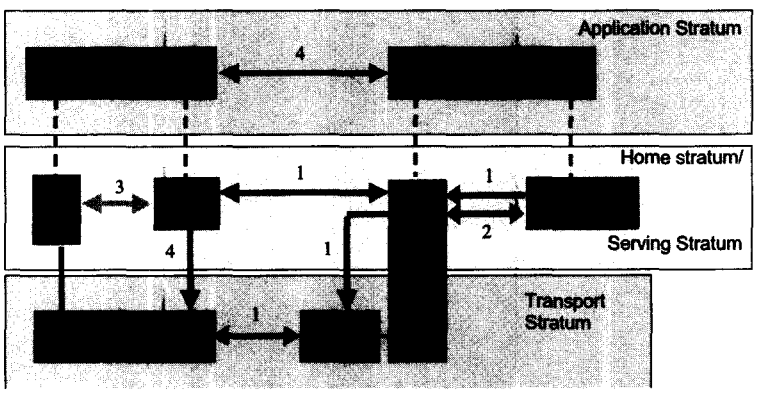


그림 4. 3GPP-UMTS 보안 구조

성, 사용자의 인증, 네트워크 액세스 링크 상의 데이터 기밀성, 데이터 무결성 및 모바일 장비 식별을 제공한다. 각각에 대한 주요한 내용은 다음과 같다.

- 사용자-신원 기밀성
  - 사용자 신원 기밀성
  - 사용자 위치 기밀성
  - 사용자 비추적성
- 사용자의 인증: 비밀키를 사용한 사용자와 네트워크의 상호 인증
- 사용자 데이터 기밀성
  - 암호 알고리즘 협약
  - 비밀 암호 키 설정
  - 사용자 데이터의 기밀성
  - 신호 데이터의 기밀성
- 데이터 무결성
  - 무결성 알고리즘 협약
  - 무결성 키 설정
  - 신호 데이터의 데이터 무결성
  - 신호 데이터의 데이터 근원지 인증
- 모바일 장비 식별: 국제 모바일 장비 식별자(IMEI: International Mobile Equipment Identifier)를 이용한 식별

(2) 네트워크 도메인 보안

이 특징에 의하여 제공되는 기능성은 다른 네트워크 요소에 속하는 네트워크 요소들 사이에 민감한 신호 정보가 교환되어야 할 경우에 매우 중요하다. 이 특징은 아래와 같이 3-계층 구조를 이용하여 구현된다.

- 엔티티(네트워크 요소) 인증
  - 인증 메커니즘 협약
  - 네트워크 요소 인증
  - 신호 데이터의 데이터 근원지 인증
- 데이터 기밀성
  - 암호 알고리즘 협약
  - 암호 키 분배
  - 교환된 데이터의 기밀성
- 데이터 무결성
  - 무결성 알고리즘 협약
  - 무결성 키 협약
  - 신호 데이터의 데이터 무결성
- 거짓 정보 수집 시스템

(3) 사용자 도메인 보안

- USIM(User Services Identity Module)에 대한 사용자 인증
  - USIM에 안전하게 저장된 비밀(PIN)에 의하여 인증이 이루어진다.
- 터미널에 대한 사용자 인증
  - USIM과 터미널에 안전하게 저장된 비밀에 의하여 인증이 이루어진다.

(4) 애플리케이션 보안

USIM 상의 애플리케이션에 대하여 3G 네트워크 위로 전송되는 메시지를 안전하게 하기 위하여 네트워크 운영자나 애플리케이션 제공자에 의하여 선택된 보안 수준을 제공한다. 메시지 보안을 제공하기 위한 특징은 다음과 같다:

- 애플리케이션 엔티티 인증
- 애플리케이션 데이터의 데이터 근원지 인증
- 애플리케이션 데이터의 데이터 무결성
- 애플리케이션 데이터의 재생 탐지
- 애플리케이션 데이터의 순서 무결성
- 수령 증명(Proof of receipt)

(5) 보안 가시성과 배열성

이상적으로, 모든 보안 특징들은 사용자에게 투명하여야 한다. 그러나 어떤 경우에 사용자의 관심사에 따라서 보안 특징의 운용에 대한 가시성이 크게 제공되어야 한다. 가능한 특징들의 예로는 액세스 망 암호화, 네트워크 암호화 및 보

안 수준을 나타내는 것들이 있다. 3G 모바일 시스템에서는, 사용자와 사용자의 HE(Home Environment)가 사용자 혹은 서비스의 제공이 운용 중인 보안 특징에 의존해야 하는가를 구성(configure)할 수 있다. 이 특징을 배열성(configurability)이라고 하는데, 3GPP에 의하여 제안된 몇 가지의 특징들은 다음과 같다.

- 사용자-USIM 인증 실행/비실행
- 입력 비 암호 호(call)의 수락/거절
- 비 암호 호의 설정 혹은 비설정
- 암호 알고리즘의 수락/거절

5.2 3G CDMA 보안

3세대인 CDMA 2000(IMT-2000) 기술은 128 비트 비밀성과 인증키의 사용을 포함하여 더 많은 보안 프로토콜이 추가되었다[22]. CDMA 2000 네트워크를 위하여 SHA-1(Secure Hash Algorithm-1)과 같은 새로운 알고리즘이 해싱과 무결성을 위하여 사용되며, Rijndael Advanced Encryption Standard(AES) 알고리즘이 메시지 암호화를 위하여 사용된다. AKA 프로토콜이 CDMA 2000 Release C 다음에 모두 사용된다. AKA 프로토콜은 WCDMA-MAP(Mobile Applications Part) 네트워크에서 또한 사용되며, 암호화와 메시지 무결성을 위하여 Kasumi 알고리즘이 사용된다. 언급할 가치가 있는 몇 가지의 운용 목적에서 보안관련 사항은 다음과 같다:

- 필요한 사용자 인증, 유일한 사용자 식별, 유일한 사용자 번호 및 유일한 장비 식별 기법의 제공
- 사기(fraud)가 가능한 어떤 서비스를 제한하여 사기 기회를 최소화한다.
- 분실된 이동 스테이션 목록을 유지하고 그들의 사용에 대한 트래픽 감시를 통하여 분실된 이동 스테이션의 오용에 대하여 사용자를 보호한다.
- 비상(emergency) 호와 함께 유용한 정보를 가능한 제공하여 비상 서비스를 지원한다. 이 정보로는 사용자 신원, 위치 정보 및 지역 당국에 필요한 다른 정보가 있다.

5.3 4G 보안

5.3.1 참조 구조

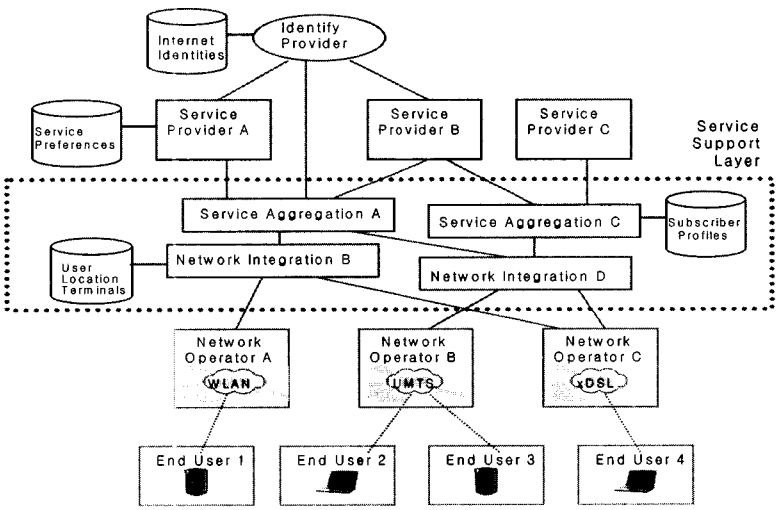


그림 5. 4G 서비스를 위한 보안 참조 구조

본 절에서는 WWRF #7에서 제시된 4G 서비스를 위한 보안 구조에 대하여 기술한다. 그림 5는 4G 서비스를 위한 보안 참조 구조를 보여준다.

종단 사용자에게 유비쿼터스 서비스를 제공하기 위하여 서비스 집합(service aggregation)이 필요하며, 네트워크 통합(network integration)으로 종단 사용자가 연결된 네트워크에 관계없이 보안 서비스를 지원 받도록 해준다. 이와 같이 서비스 지원 계층은 다음과 같은 주요기능을 제공한다.

- 가입 상황(subscription context)
- 서비스 집합
- 네트워크 통합
- 연합(federation)
- 기능성 분배 허용

5.3.2 신원 관계성

사용자 신분은 인증을 통하여 확립된다. 이 절차에서 제공된 신용장(credential)이 유효한 사용자나 가입자의 목록과 대조된다. 인증 절차에서 각 서비스 제공자, 액세스 네트워크에 대하여 개별 신원 인증 절차를 가질 수 있는데, 이것은 분명히 4G 환경에서는 너무 복잡하여 다루고 관리할 수 없게 된다. 따라서 개별 신원 확인 절차 대신, 통합된 신원확인 모델이 다른 도메인 사이의 사용자 신원을 관리하는 더욱 편리한 방법이다. 이를 위하여 WG2-WWRF#7에서는 그림 5에서와 같이 서비스 지원 계층을 둔다. 그림 6에서는 개별(separate) 신원 관계성과 통합(integrated) 신원 관계성을 보여준다.

개별 신원 관계성 모델은 현재 널리 설치되어 있는데, 사용자는 각 서비스 제공자, 액세스 네트워크, 다른 파티와 법적인 관계를 가진다. 4G 환경에서 이것은 너무 복잡하여 다루고 관리할 수 없는 것이 명백하다. 반면에, 통합된 신원 관계성 모델은 다른 도메인간의 사용자 신원을 관리하는데 더욱 편리한 방법이다. 여기서는 서비스 지원 계층이 중요한 부분을 차지한다.

통합 인증의 장점은 다음과 같다[19]:

신용장 분배를 위한 설치비용이 한번만 발생한다.

- 관리가 단순하다.
- 종단 사용자에게 사용이 편리하다.
- 네트워크 액세스와 사용한 서비스에 대하여 통합된 빌링이 가능하다.

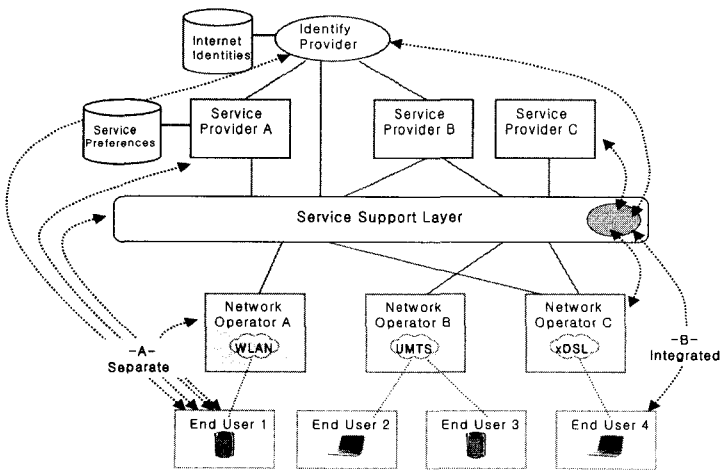


그림 6. 신원(identity) 관계성

통합된 인증을 성취할 수 있는 방법은 다음과 같다[19]:

- 신원인증의 단일 소스-터미널 측: 네트워크와 서비스 레벨에서 사용자 인증은 작은 휴대용 디지털 장치의 소유를 기반으로 한다. 이것은 다른 터미널들과 쉽게 교환될 수 있으며, 사용자 신용장과 사용자에 따른 수정 가능한 데이터를 위한 저장 용량을 가지고 있다. 이 장치의 사용이 종단 사용자를 거슬리게 하여서는 안 되고 터미널에 넣을 때는 패스워드가 요구된다. 물론 이 기술은 표준화되어야 한다. 사용자 신용장으로부터 서비스 제공자를 유도하는 것이 가능해야 한다.
- 통합된 인증 및 식별-후단 요구사항: 서비스 지원 계층을 운영하는 각 서비스 제공자는 인증 요구를 다루기 위하여 단일 인증 서버를 가져야 한다. 이 서버는 네트워크 액세스 요구와 서비스 레벨 액세스 요구를 위하여 사용된다. 또한 이 서버는 RADIUS, LDAP 등과 같은 다중 프로토콜, 직접적인 데이터베이스 접근도 지원해야 한다. 서버는 터미널과 상호 인증을 지원해야 한다. 복수의 서비스 제공자를 위한 연합된 인증을 구현하기 위하여 전달 인증 프록시도 필요하다.

6. 맺음말

이동통신 시스템의 진화는 1세대의 아날로그 휴대전화로부터 시작하여 3세대 이동통신 시스템인 CDMA2000 이후의 4G 시스템이 연구 개발되고 있다. 이동통신 환경이 다양한 기자재를 서로 접속하여 언제, 어디서나 정보를 교환할 수 있는 유비쿼터스 통신으로 변하고 있기 때문에, 보안 문제는 더욱 심각해지고 중요하다고 할 수 있다.

그러나 국내에서 이동통신의 보안 문제, 특히 차세대 이동통신 서비스를 위한 보안 이슈를 다루는 발표된 문헌이 별로 없는 실정이다. 이에 따라 본 고에서는 국내외 참고 문헌을 통하여 이동통신 서비스를 위한 비밀성, 인증, 접근 통제를 중심으로 3G와 4G 이동통신 시스템의 보안 기술에 대하여 살펴보고 표준화 활동에 대하여도 기술하였다.

ITU-T SG 17 회의에서 한국과 일본이 공동으로 제출한 모바일 보안 표준이 승인을 받는 등 국내 전문가의 보안 표준화 활동이 매우 활발히 이루어지고 있다. 이와 같이 국내 기술의 국제 정보보호 표준화 제정을 통한 경쟁력 확보를 위하여 보다 적극적인 관심이 요구된다고 하겠다.

참 고 문 헌

[1] 박정현, 임선배, 이경준, "이동통신 보호를 위한 인증 방식 분석", 전자통신동향분석, 제13권 제4호, 1998년 8월.

[2] 오돈성, "이동통신 서비스 연구 동향", 주간 기술동향, 통권 1142호, 2004. 4월.

[3] 원유재, 이동통신 환경의 보안 기술, ppt 자료, 2001년 4월 18일.

[4] 전자통신동향분석 19권 3호(통권 87호), 차세대 이동통신 특집 논문, 2004.6.15. 한국전자통신연구원.

[5] 최성곤, "Mobile Security", TTA 저널 제 92호, pp.92-96, 2004.

[6] 하정락, 김성희, 김대식, "4세대 이동통신의 비전", 전자통신동향분석, 제 18권 제5호, 2003년 10월.

[7] Jeroen van Bemmel, Harold Teunissen, Gerald Hoekstra, "Security Aspects of 4G Services", WWRF(Wireless World Research

Forum).

[8] Dan Brown, "Techniques for Privacy and Authentication in Personal Communication Systems", IEEE Personal Communications, August 1995, pp6-10.

[9] CEIR back in the spotlight? http://www.gsmworld.com/using/security/index.shtml

[10] Vijaya Chandran Ramasami, "Security, authentication and access control for mobile communications", EECS Dept, Univ. of Kansas.

[11] Tomas B. Contreras, Rene A. Cumplido-Parra, "Security Architecture in UMTS Third Generation Cellular Networks", INAOE Tech. Report No. CCC-04-002, Feb. 2004, Mexico.

[12] Kaj J. Grahn, G. Pulkkis, Jean-S. Guillard, "Security of Mobile and Wireless Networks", Informing Science pp587-600, June 2002.

[13] IETF RFC2284, PPP Extensible Authentication Protocol(EAP), March 1998.

[14] IETF RFC2716, PPP EAP TLS Authentication Protocol, Oct. 1999.

[15] ITU-T SG 17 Meeting, Proposal for a security technology framework in end-to-end mobile communications, March 2004, Geneva Switzerland.

[16] Astrid Lubinski, "Security Adaptation Components for Mobile Communication".

[17] A. Prasad, H. Wang, P. Schoo, "Infrastructure Security for Future Mobile Communications System", Proc. of WPMC 2003, Yokosuka, Japan, Oct. 2003.

[18] Frank Quick, Security in CDMA2000 Wireless Systems, Nov. 2002, Qualcomm Inc.

[19] Harold Teunissen, Jeroen van Bemmel, Gerald Hoekstra, Security Aspects for 4 G Services, WG2 WWRF #9, July, 2003, Zurich.

[20] Wi-Fi Alliance Announces First Products Certified for Wi-Fi Protected Access, Security, http://www.wifi.org

[21] Joseph E. Wilkes, "Privacy and Authentication Needs of PCS", IEEE Personal Communications, August 1995, pp11-15.

[22] Christopher Winger, Mullaguru Naidu, CDMA 1XRTT Security Overview, Aug. 2002, Qualcomm.

전 용 희

1971. 3~1978.2 고려대학교 전기공학과

1985. 8~1987.8 미국 플로리다 공대 대학원 컴퓨터공학과

1987.8~1992.12 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사

1978. 1~1978.11 삼성중공업(주)

1978.11~1985.7 한국전력기술(주)

1989.1~1989.6 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989.7~1992.9 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA

1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원

1994.3~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수

2000.1~현재 한국통신학회 학회지 편집위원

2001.3~2003.2 대구가톨릭대학교 공과대학장 역임

2004.2~현재 한국전자통신연구원 정보보호연구단 초빙연구원

<관심분야> 네트워크 보안, 통신망 자원관리 및 성능분석, QoS 보장 기술