情 報 保 護 學 會 誌
第 14 券 第 3 號, 2004. 6

안전한 위치기반 서비스 제공을 위한 인증 및 보안 적용 방안

박 남 제*, 송 유 진**, 문 기 영*

요 약

위치기반 서비스(LBS : Location Based Services)란 휴대폰, PDA, 노트북 PC 등 휴대용 단말기를 기반으로 사람이나 사물의 위치를 정확하게 파악하고, 그 위치와 관련된 부가 정보 서비스 및 이를 위한 시스템을 통칭한다. 최근의 이동 통신 기술의 발달과 휴대폰, PDA 등과 같은 모바일 단말의 급속한 확산으로 인하여 위치기반 서비스는 유무선 인터넷의 응용 및 위치 정보를 사용한 부가 가치 창출에 있어 핵심적인 역할을 할 것으로 예상되고 있다. 이러한 위치기반 서비스를 위해서는 단말의 위치 정보들을 저장 및 관리하고 위치 정보를 이용하여 다양한 응용 서비스를 지원하는 위치기반 서비스에서 보안서비스의 역할이 매우 중요하다. 이를 위해 위치 정보의 획득, 위치 정보의 저장 및 관리, 인증 및 정보 보호 등의 사용자 관리, 대용량 위치 정보 데이터베이스의 관리 등의 기능에서 안전한 보안 서비스를 제공하여야 한다. 본 고에서는 위치기반 서비스를 구성하는 플랫폼과 서비스 시스템간의 인증 및 보안 기술 적용 방안을 제시한다.

Ⅰ. 서 론

최근 이동 통신 기술의 발달과 모바일 단말의 급속한 확산으로 인하여 위치 추적이 가능한 단말기를 휴대한 사용자의 현재 및 과거 위치 정보를 활용한 유무선 인터넷 서비스인 위치기반 서비스(LBS, Location Based Services)의 중요성이 한 층 대두 되고 있다. 위치기반 서비스는 위치 확인 기술(Location Detection Technology)을 이용해 이용자의 위치를 파악하고 이와 관련된 애플리케이션 등을 부가한 서비스를 말하는 것으로 다방면에 걸친 이용이 가능해 유무선 인터넷의 응용 및 위치정보를 사용한 부가 가치 창출에 있어 핵심적인 역할을 할 것으로 예상되고 있다.

최근의 개인정보 노출로 문제시되고 있는 온라인 사이트의 회원정보 수집 관행에 비추어 볼 때 위치정보 서비스의 특성상 현 위치에 대한 개인정보 노출의 우려는 높을 수밖에 없다. 온라인 사이트를 통해 노출되는 회원정보에는 이름, 주민등록번호, 주소 등의 정보로서 주민등록번호 등의 개인정보가 도용을 통해 다른 용도로 쓰일 우려가 있다. 더욱이 고객의 위치 정보, 이를 통한 이동 궤적의 파악 등은 그 자체가 이미 직접적인 사생활 침해 요소로 작용할 수 있다. 이 때문에 오히려 위치기반 서비스의 프라이버시 침해에 대한 우려가 더욱 심각하다.

공공 부문에서의 위치기반 서비스 활용 예로서 119 등 신고 전화를 통해 사고 상황이 전해질 경우 발신자의 위치가 자동 추적되거나, 얼마 전 대구 지하철 참사와 같은 사고가 발생했을 때 사고자의 위치를 추적하는 경우이다. 이러한 사례는 1999년 미국의 FCC (Federal Communications Commission)가 무선 응급구난 서비스(E-911) 규칙을 제정했던 것에서 찾을 수 있다[4]. 이 규칙은 미국 내의 망 사업자들이 2001년 10월까지 이동전화 사용자가 응급 호출(911)을 하였을 때 67%는 100m 이내의 위치 오차로, 95%는 300m 이내의 위치 오차로 응급 호출자의 위치정보 제공을 의무화하고 있다. 그러나 지난 2003년 3월, KTF의 위치기반 서비스인 '수호천사' 서비스의 해킹 사례를 통해 알 수 있듯이 고객의 동의 여부를 떠나 개

* 한국전자통신연구원 전자정부보안연구팀 ({namjepark,kymoon}@etri.re.kr)
** 동국대학교 전자상거래대학원 교수 (song@mail.dongguk.ac.kr)

개인의 위치 정보가 해킹 등의 부정한 방법으로 유출될 가능성이 높기 때문이다.

이와 같이 사용자에 대한 위치정보의 개인 프라이버시, 위치정보의 위·변조 문제, 위치정보의 기밀성, 위치정보 서비스 사용자의 인증문제, 위치기반 서비스 플랫폼 서버내의 위치정보 데이터에 불법적인 접근 등 많은 문제가 발생할 수 있다. 또한, 위치정보 수집에 대한 동의의 범위 문제가 있다. 개인 고객의 위치정보 값을 취득하지 않은 상태에서는 위치기반 서비스 자체가 의미가 없으므로 위치기반 서비스를 사용한다는 의미는 개인의 위치정보 수집에 대한 동의의 의미로 해석될 소지가 있다. 따라서 위치기반 서비스를 사용함에 있어 위치정보 수집에 대한 동의는 필수 불가결하다. 예를 들어, 자신이 위치한 주변의 식당, 백화점 등을 검색하기 위한 POI(Point of Interest, 관심지역 정보) 서비스 용도로 위치기반 서비스를 사용하고자 하는 고객의 경우 자신의 위치 정보를 이용해 주변 지역 광고 메시지가 전송되는 것은 원하지 않을 가능성이 있다. 이때, 고객의 위치정보 수집에 대한 동의를 구할 때 각종 서비스의 종류에 따라 동의 여부를 별도로 물어야 하는지에 대한 논란 역시 남아 있다. 또한 새로운 서비스가 선보일 때마다 매번 위치정보 수집에 대한 동의를 구한다는 것은 고객의 입장에서도, 또한 업체의 입장에서도 불편하고 어려운 사항이다.

이러한 문제들은 개인 신상정보 노출 및 범죄 등에 악용될 수 있기 때문에 인증 및 보안 분야에서 국내 및 국제적인 LBS 보안 연구의 필요성은 매우 절실하다. 본 연구는 정보의 유출을 차단하고 안전하게 위치기반 서비스를 제공하기 위한 위치기반 서비스 플랫폼과 서비스 시스템 간 인증 및 보안 서비스를 분석하고 적용 방안을 제시한다.

II. LBS 개요 및 동향

2.1 위치기반 서비스 개요

2.1.1 위치기반 서비스 정의

LBS는 Location-Based Service의 약어로서 위치기반 서비스로 통칭되며 이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스라고 일반적으로 정의된다. 즉, LBS란 이동 통신 기지국과 GPS(Global Positioning System)을 통해 개인이나 차량의 위치 정보를 파악하고 이를 기반으로 각종 첨단 서비스를 제공하는 시스템이다[1].

3GPP(The 3rd Generation Partnership Project)는 LBS를 위치기반 서비스 제공이 가능한 네트워크를 이용한 표준화된 서비스로 정의하고 있으며, OGC (Open GIS Consortium)는 위치정보의 접속, 제공 또는 위치정보에 의해 작용하는 모든 응용소프트웨어 서비스라고 정의하고 있다[2]. 또한 FCC는 이동식 사용자가 그들의 지리학적 위치, 소재 또는 알려진 존재에 대해 서비스를 받도록 하는 것이라고 정의하고 있다[4,5].

2.1.2 위치기반 서비스 활용

LBS는 위치정보에 기반한 다양한 응용서비스를 제공하는 것이다. 여기에는 비상구조 지원, 위치정보 서비스, 교통혼잡 및 네비게이션(Navigation) 정보, 위치 밀착형 과금 등이 포함된다. 이외에도 ITS (Intelligent Transport Systems) 연계분야, 장애인을 위한 보조수단, 위치정보를 기반으로 한 L-Commerce, 휴대 전화기를 그대로 사용하는 Cell ID 기반의 친구 찾기 등 그 적용분야는 무한하다. 다음 〔표 1〕은 위치기반 서비스 활용 분야의 예이다.

〔표 1〕 위치기반 서비스 활용 분야

활용분야	기대효과
어린이나 치매 노인의 위치추적	미아방지, 사고예방
애완동물 위치 추적	분실, 사고 예방
차량 네비게이션	차량의 이동 경로 파악
외근직원의 위치 파악	외근직원의 효과적 관리
현재 위치의 주변정보 제공	극장, 주유소, 식당, 백화점 등 주변 정보를 제공함으로써 고부가 서비스 제공
경찰/보안/군용차량 관리	범죄예방
택배/화물의 위치정보 제공	유류/교통비/통신비 절감

현재의 무선 통신망을 통한 가입자 위치 정보 수집 기술은 이미 개발된 GPS 등 위치측위 기술과 무선 통신망의 결합으로 보다 정밀한 위치 정보 수집이 가능하게 되어, 더욱 다양한 응용 서비스 제공이 가능하게 되었다. 위치정보가 이동통신망과 연결되면서 대중적이고 일반적인 서비스 제공이 가능하게 된 것이다. 향후 네

트워크에서 제공되는 응용 서비스 구조는 독립적이고 수직적인 구조의 유무선 통신망 구조에서 유무선 통합을 위한 수평적 구조로 바뀌고 있다. 또한, 모든 네트워크 개체들이 평등한 All IP망 기반으로 서비스를 제공하는 개방형 통합망 형태로 발전할 것이다. 그리고 A-GPS (Assistance-GPS)와 같은 위치측위 시스템의 발전과 Ubiquitous, Pervasive형태로의 컴퓨팅 환경의 패러다임 변화를 통해 MT(Mobile Terminal)는 독립적으로 정보제공의 주체가 되어 LBS SP (Service Provider)에게 자신의 위치정보를 전달하는 형태로 발전할 것이다. 이러한 발전과 함께 고려해야 할 사항은 위치기반 서비스의 구성 요소들에게 종래의 유무선 네트워크 수준 이상의 안전성, 신뢰성이 제공되어야 한다는 것이다.

2.2 위치기반 서비스 표준화 동향

위치기반 서비스는 현재 MLP(Mobile Location Protocol) 기반으로 LBS 플랫폼과 응용서비스 제공자 간 통신할 때 XML 기반의 보안 표준을 기반으로 최근 논의가 시작되었다. 국제기구에서의 관련 표준화 동향은 다음과 같다.

2.2.1 LIF (Location Interoperability Forum)

2000년 9월 모토롤라, 노키아, 에릭슨 등이 주축이 되어 설립된 포럼으로 LBS 솔루션의 상호호환성 및 테스팅을 통해 모든 모바일 환경에서 사용 가능한 표준을 추진 중이며, 특히 MLP 3.0은 사실상의 표준으로 사용된다. 주요 LIF 기술 규격은 다음과 같다.

- TS 101 : Mobile Location Protocol Specification
- TD 201 : The Challenge with Interoperability in Location Services
- TS 202 : Location Services Interoperability Test Specification in GSM
- Privacy Recommendations (LIF TR 102) 표준화 진행 중 : 미공개 상태
- Privacy under location roaming and local content : 향후 표준화 추진 예정

2.2.2 IETF Geopriv Working Group

IETF Geopriv(Geographic Location Privacy) 워킹그룹의 LBS Privacy와 관련된 주요 표준화 Internet Drafts는 다음과 같다.

- Threat Analysis of the Geopriv Protocol (2002년 10월) : LBS 프로토콜상에서의 여러 가지 공격 유형을 분석하고 대응 방안과 요구되는 보안 특성을 정의
- Geopriv Requirements (2003년 3월) : LBS에서 개인 위치 정보의 보호를 위한 권한, 보안, 프라이버시 요구사항 정의

2.2.3 OGC (Open GIS Consortium)

개방형 지리정보 서비스를 목적으로, 지리 정보를 위치기반 서비스로 확장하기 위한 개념적 모델 제시 및 세부 서비스의 기능과 인터페이스를 정의한다.

2.2.4 ISO/TC211

지리정보와 관련된 기술 규격을 제정하는 표준기구로 주로 ITS(Intelligent Transport System)와 관련된 표준을 제정한다.

2.2.5 3GPP/3GPP2

차세대 이동통신 네트워크에서의 위치정보 제공을 위한 통신망 참조 모델과 프로토콜 표준 규격을 발표하고 있다.

2.2.6 국내 LBS 표준화 포럼

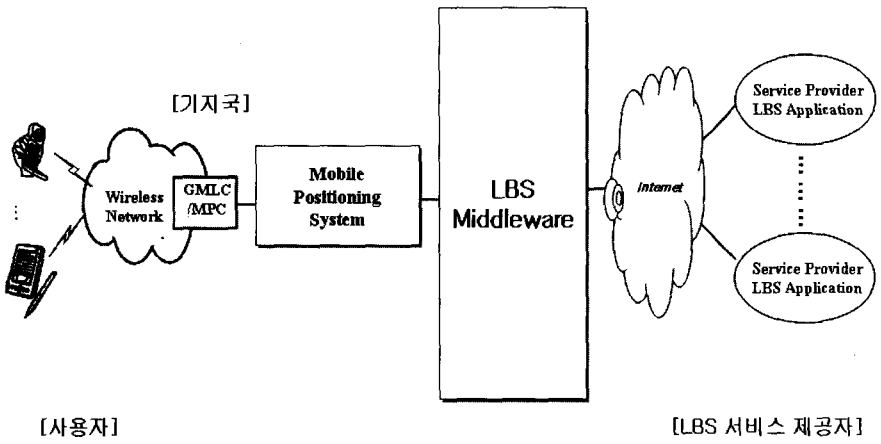
국내에서는 주로 LBS표준화포럼이 4개의 Working Group과 1개의 Special Interest Group 구성을 통하여 LBS 관련 표준화를 추진하고 있다.

Ⅲ. LBS 보안 기술

3.1 위치기반 서비스의 보안상 문제점

위치기반 서비스의 활성화를 위해서는 서비스의 순기능도 중요하지만 역기능의 방지를 통한 사용자의 프라이버시 및 인증의 확보가 중요하다. 위치기반 서비스의 역기능에는 사용자 개개인의 위치가 24시간 실시간으로 노출된다는 것이다. 그리고 네트워크 해킹 문제가 이미 심각한 사회적 문제로 대두되고 있는 현재 개인의 위치정보가 인터넷상에 유포되는 것은 사용자 프라이버시 문제를 심각하게 손상시킬 수 있는 문제이다. 또한, 위치정보를 악용할 경우 개인의 사생활 노출로 인한 프라이버시 침해는 물론 범죄에 악용될 우려도 있다.

이와 같이 LBS 시스템의 Mobile Terminal과 Service Provider간의 위치정보 송수신 인증과 부인방지를 위한 신뢰관계(Trust Relationship)를 보장



〔그림 1〕 위치기반 서비스 네트워크

하고, 개인정보 및 프라이버시를 보호할 수 있는 위치기반 서비스 구조 및 프로토콜이 요구된다. 또한 위치기반 서비스에는 관련 서비스 이용 시, 제 3자에 의해서 또는 불법으로 위치기반 서비스의 위치정보가 노출될 수 있다. 따라서 해당 위치정보를 보호하기 위해 현재 위치정보 보호법이 제정되어 있는 상황이며 인증 및 보안 서비스 제공이 중요하게 대두된다. 위치정보 서비스를 이용하게 되면 사용자에 대한 위치정보의 Privacy, 위치정보의 위·변조 문제, 위치정보의 기밀성, 위치정보서비스 사용자의 인증문제, LBS 플랫폼 서버로의 불법접근 등 많은 문제가 발생할 수 있다. 이러한 문제들은 개인 신상정보 노출 및 범죄 등에 악용될 수 있기 때문에 인증 및 보안 분야는 상당히 중요하다. 따라서 위치정보의 기밀성(Confidentiality), 위치서비스에 대한 인증(Authentication), 위치정보의 무결성(Integrity), LBS플랫폼 서버로의 접근제어(Access Control)에 관한 부분이 필요하다.

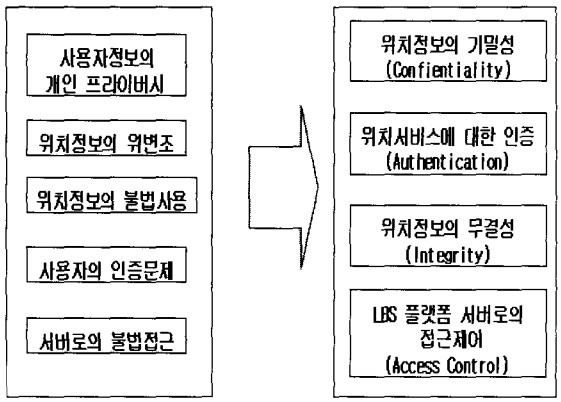
서비스 업체가 제공하는 위치정보의 노출, 변조, 불법접근 등이 이루어지게 되면 위치정보 서비스의 질 저하와 함께, 기업의 자산(Database) 침해 등이 우려됨에 따라 관련 서비스의 안정적인 측면에서 LBS 플랫폼과 위치기반 서비스 제공 시스템자간의 보안/인증 측면이 필요하게 된다. 기업적인 면에서 해킹 및 불법노출에 의해 개인정보가 유출된다면, 기업과 가입자 모두 막대한 피해를 보기 때문에 기업적 측면에서도 보안부분이 상당히 중요하다.

3.2 LBS 인증 및 보안 요구사항

XML은 데이터에 대한 의미적 접근과 확장성을 제공하는 표준으로서 언어적 미들웨어의 역할을 수행하는 반면, 중요 정보에 대한 표현이 구조적으로 드러나게 되어 있어, XML 문서상에 나타나는 많은 정보들이 외부에 무방비 상태로 노출되는 것이 사실이다.

현재 LBS 플랫폼의 보안/인증 요구사항이 명확하게 제시되지 않은 상태로서 LBS 플랫폼의 구체적인 보안/인증 요구사항을 정립하고 〔그림 2〕를 기반으로 보안/인증 체계를 정의한다.

LBS 플랫폼은 이동통신망에서 처리된 인증 결과를 처리할 수 있어야 하며, LBS 플랫폼과 이동통신망의 인증결과가 다른 경우에는 이동통신망의 인증결과를 기준으로 처리한다.



〔그림 2〕 위치기반 서비스 보안 요구사항 개념도

보안 서비스 요구사항인 기밀성, 무결성, 인증, 부인방지 등의 보안 서비스 해당별 위협 요소에 대한 안전

한 위치정보 서비스를 위해 제공되어야 할 보안 서비스를 분석하면 다음 〔표 2〕와 같다.

위치정보 문서는 XML을 기반으로 동작하므로 IETF와 W3C의 XML Signature, XML Encryption 및 OASIS의 SOAP Sec, SAML, XACML 그리고 SSO 등의 표준을 참고하여 다음과 같은 관점에서 LBS 플랫폼의 보안/인증 요구사항을 정립한다.

LBS 보안 플랫폼은 위치정보의 기밀성, 무결성 및 사용자의 인증을 위한 보안 요구사항을 정의하며 아래의 요구사항을 만족해야 한다.

〔표 2〕 LBS 위협요소별 적용 보안 기술

보안서비스	위협요소	적용 보안 기술
기밀성	메시지 도청	XML Encryption, SSL/TLS, S/MIME 등
무결성	메시지 변조	XML Signature, SHA-1, SSL/TLS, IPSec 등
인증	메시지 위조	ID/PWD, TLS, Kerberos, IPSec, PKI, XKMS 등
부인방지	메시지 송신 및 수신 부인	XML Signature, XKMS 등
접근제어	불법적 서비스 및 정보이용	XACML, PMI, SAML 등

1) 위치정보의 기밀성 - XML 암호화 등

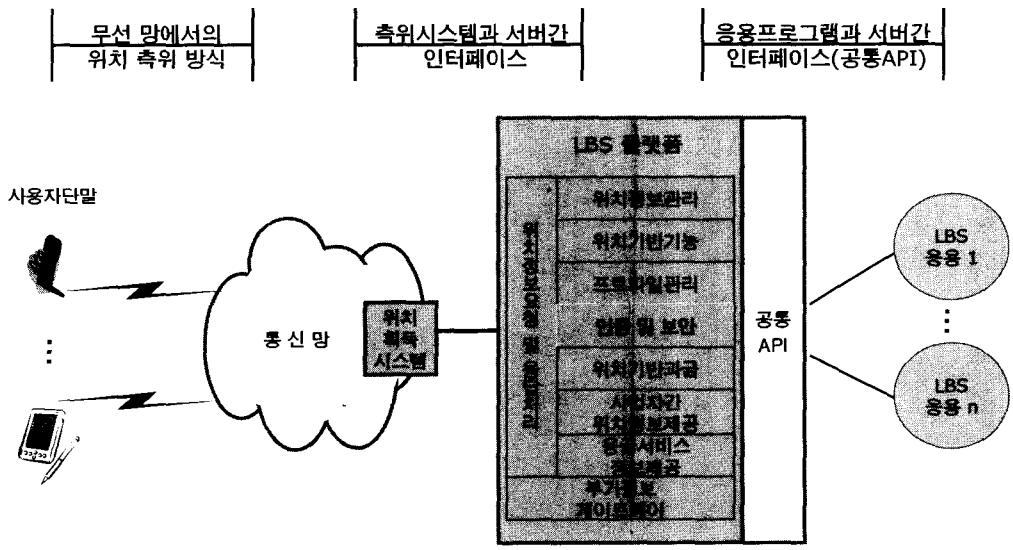
- XML을 포함한 다양한 LBS 정보에 대한 암호문을 XML 형태로 생성하고 복호화하여 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달할 수 있는 보안 요구사항
- 위치정보의 전달 과정에 있어 데이터의 보호가 필요한 경우 해당 위치 정보를 암호화 하거나 전달되는 모든 위치 정보를 암호화 할 수 있어야 한다.
- 요청된 어떠한 위치측정도 신뢰성 있고 안전한 방법으로 서비스 요청자에게 제공되어야 한다.

2) 위치정보의 무결성 - XML 전자서명 등

- XML을 포함한 LBS 정보에 대한 전자서명을 XML 형태로 생성하고 검증하기 위한 XML 전자서명 요구사항
- 위치정보 전달과정에서 데이터의 무결성이 보장되어야 한다. 즉 위치정보에 대한 위조나 변조가 가능해서는 안 된다.

3) 위치서비스에 대한 인증 - SAML, XKMS 등

- XML 기반의 인증 및 승인 정보를 안전하게 교환하기 위한 프레임워크에 대한 요구사항
- LBS 플랫폼은 인증 받지 않은 서비스 사용자에 대한 접근을 제어하여야 한다. 즉 위치정보는 인증된 사용자에게 안전해야 한다.
- 위치정보의 전달과정에서 인증정보를 포함할 수 있어야 한다.



〔그림 3〕 위치기반 서비스 플랫폼 논리 참조 모델

4) LBS 플랫폼 서버로의 접근제어 - XACML 등

- 접근 제어 리스트(Access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공하고 각각의 사용자 별 LBS 정보의 접근 정책을 수립하고 적용하기 위한 요구사항
- 국가가 정한 법에 따라 모든 위치정보의 요청과 응답을 감시하거나 차단할 수 있어야 한다. 이때 보안의 위반에 대한 해석을 용이하게 하기 위해서 위치정보의 요청/응답에 대한 감시 기록이 유지되어야 한다.

Ⅳ. LBS를 위한 인증 및 보안 적용 방안

위치기반 서비스를 위한 보안기술은 현재 MLP (Mobile Location Protocol) 기반으로 LBS 플랫폼과 응용서비스 제공자 간 통신할 때 XML 보안기술에 의한 안전성 측면에서 검토되고 있다. [그림 3]의 위치기반 서비스 플랫폼 논리참조 모델에서와 같이 LBS 응용서비스를 사용자에게 안전하게 제공하기 위해 플랫폼 내에 인증 및 보안 기능을 수행하는 인터페이스 모듈이 필요하다.

4.1 MLP 상의 보안 구조 정의

LBS 서버와 단말기 간 LBS 데이터 교환을 위한 프로토콜은 LIF에서 제정한 MLP 프로토콜을 기반으로 동작하며 이러한 MLP상의 인증 및 보안 요소 적용을 다음과 같은 관점에서 구성한다.

MLP는 위치기반 클라이언트로부터 위치기반 서버에게 위치정보를 보다 쉽게 처리하여 위치기반 응용 프로그램 개발을 보다 수월하게 하는데 기반이 되는 프로토콜이다.

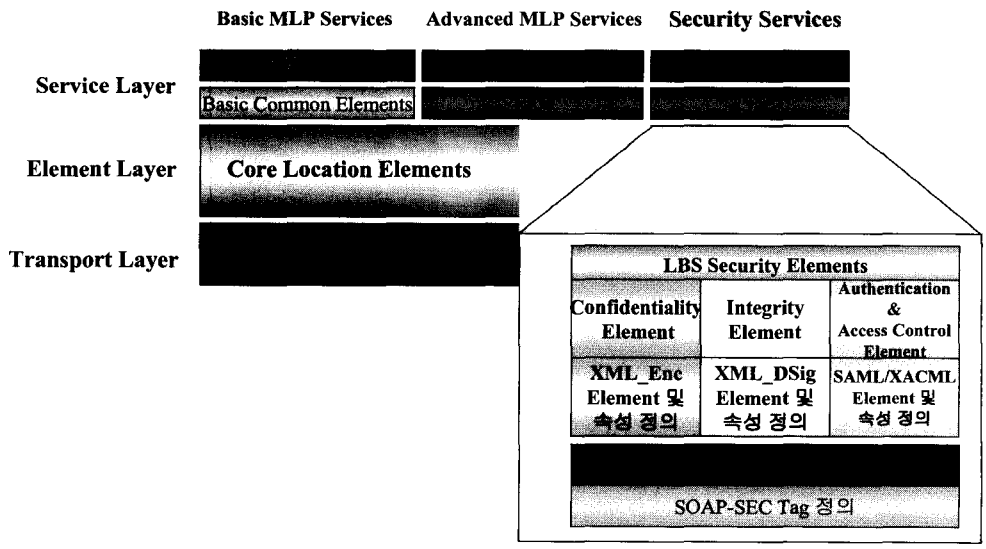
위치정보업체 및 위치기반 서비스 제공자간 위치정보 보안 구조의 세부 내용은 아래 [그림 4]와 같이 Confidentiality element, Integrity element, Authentication & Access Control element를 정의하고 이러한 element를 SOAP-SEC 기반의 전송 계층상에서 LBS 보안 인증 표준 참조 시스템으로 구성된다.

이러한 구조상에서 LBS 보안 서비스는 XML 기반의 Request & Response 모델에 따라 LBS 플랫폼과 서비스 제공자 간에서 위치정보가 안전하게 전달된다.

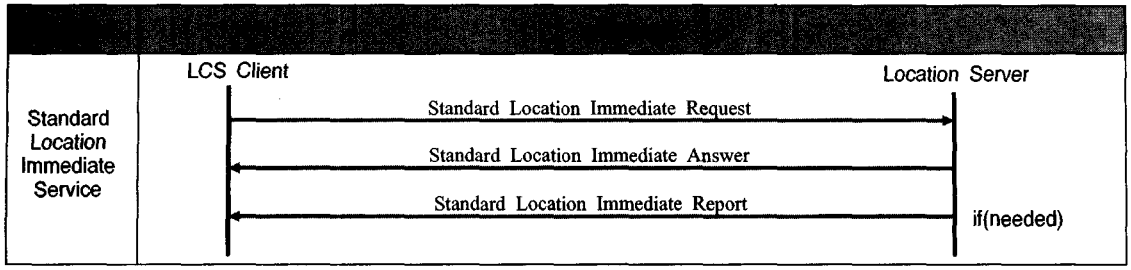
4.2 LBS 서비스 계층 정의

MLP상의 서비스 계층에서 제공되는 위치기반 서비스에 대해 살펴보면, MLP 서비스 프로토콜은 5가지 서비스로 구분되며 메시지의 전달은 요청, 응답, 보고의 3 종류로 정의된다.

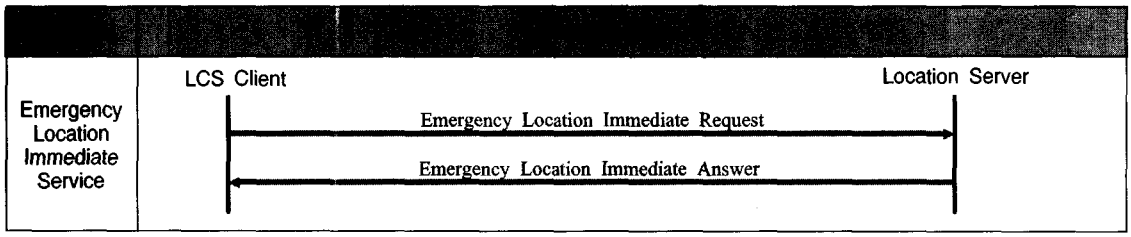
① 요청(Request) : 위치기반 서비스 클라이언트로부터 위치기반 서버로 전송되는 위치정보에 관련된 정보를 요구하는 메시지를 말한다.
② 응답(Answer) : 위치기반 서비스 클라이언트로



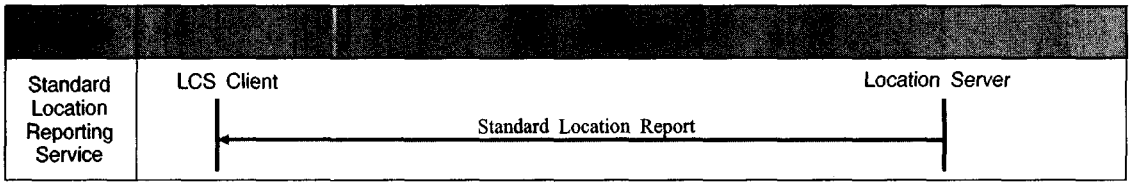
[그림 4] MLP 기반 보안 및 인증 서비스 구조도



〔그림 5〕 현재 위치 즉시 서비스 메시지 흐름



〔그림 6〕 응급 위치 즉시 서비스 메시지 흐름



〔그림 7〕 위치 보고 서비스 메시지 흐름

부터 요청에 대한 결과를 전달하는 위치기반 서버로부터 위치기반 서비스 클라이언트로 전송되는 메시지를 말한다.

③ 보고(Report) : 위치기반 서비스 클라이언트로부터의 요청 또는 위치기반 서버의 필요에 따라 위치기반 서버로부터 위치기반 서비스 클라이언트로 전달되는 메시지로 보고의 형태는 주기적 또는 불특정 시점이 될 수 있다.

4.2.1 현재 즉시 서비스

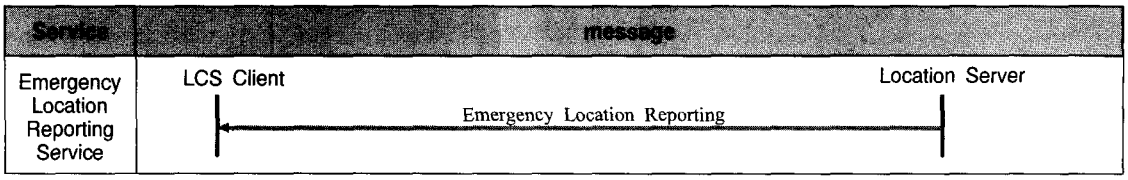
위치기반 서비스를 클라이언트가 하나 또는 그 이상의 모바일 가입자의 위치를 알기 위하여 위치기반 서비스 서버에 가입자 단말의 위치를 요청하고, 위치기반 서비스 서버가 즉시(정해진 범위에서 지연 가능) 가입자 단말의 위치를 위치기반 서비스 클라이언트에게 돌려주는 형태의 서비스이다. 〔그림 5〕에서는 현재 위치 즉시 서비스(Standard Location Immediate Service)의 메시지 흐름을 나타낸다.

4.2.2 응급 위치 즉시 서비스

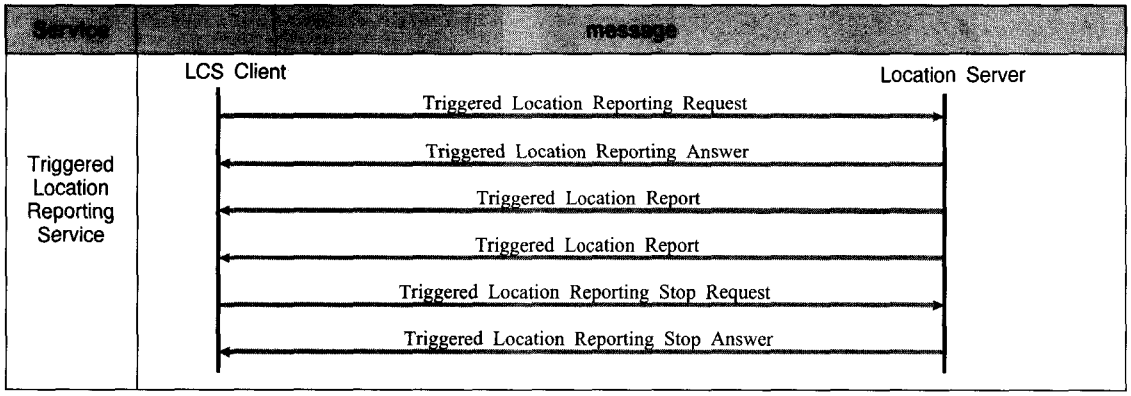
응급 구조 기관에 긴급 전화를 하거나 기타 응급 서비스를 요청한 모바일 가입자의 위치를 획득하는데 사용한다. 긴급한 상황을 전제로 하는 서비스이기 때문에, 보고 메시지를 보내는 경우는 제외한다. 또한 긴급한 상황을 전제로 이루어지는 서비스이기 때문에 QoS (Quality of Service)와 관련한 조건은 제외시키고, 우선 순위 또한 최우선적으로 처리해야 한다. 〔그림 6〕에서는 응급 위치 즉시 서비스(Emergency Location Immediate Service)의 메시지 흐름을 나타낸다.

4.2.3 위치 보고 서비스

이동 가입자가 위치기반 서비스 클라이언트에게 이동 단말의 위치를 알려주고 싶을 때 사용하는 서비스로 위치 정보를 받을 클라이언트는 위치기반 서비스 서버에 사전 정의하거나, 이동 단말이 위치기반 서버에 요청할 때 포함해야 한다. 〔그림 7〕에서는 현재 위치 보고 서비스(Standard Location Reporting Service)



〔그림 8〕 응급 위치 보고 서비스 메시지 흐름



〔그림 9〕 조건 위치 보고 서비스 메시지 흐름

의 메시지 흐름을 나타낸다.

4.2.4 응급 위치 보고 서비스

사용자가 긴급 구조 전화를 걸 때, 또는 끊을 때, 망에서 이를 자동으로 인식하여 사용자의 위치를 갖도록 한다. 사용자의 위치를 통보 받을 응급 위치기반 서비스 클라이언트는 위치기반 서비스 서버에 등록되어야 한다. 클라이언트에 전달되는 지리정보의 유형이나 주소도 서버에 정의 되어 있어야 한다. 〔그림 8〕에서는 응급 위치 보고 서비스(Emergency Location Reporting Service : ELRS)의 메시지 흐름을 나타낸다.

4.2.5 조건 위치 보고 서비스

LBS 클라이언트가 설정하는 조건에 반응하여 이동 단말의 위치 정보를 LBS 클라이언트에게 알리는 서비스이다. 위치정보는 기 정의된 이동 단말로부터의 이벤트가 발생하거나 정의된 시간 주기가 초과하는 경우 조건에 맞는 보고 서비스가 작동된다. 설정 가능한 조건은 일정 시간 동안 일정 시간 간격과 지정 위치의 진입 또는 이탈 정보이다. 〔그림 9〕에서는 조건 위치 보고 서비스(Triggered Location Reporting Service : TLRS)의 메시지 흐름을 나타낸다.

4.3 LBS 보안 요소(Element) 정의

LBS 서비스 계층에 제공되어야 하는 보안 기능을 LBS 보안 요소로서 정의한다. element 계층에서는 크게 가입자 식별 요소 정의, 기능적 요소 정의, 위치 요소 정의, 형상 요소 정의, 위치 정확도 요소 정의, 네트워크 요소 정의, 문맥 요소 정의 7가지로 정의 되어 있다. 이러한 7가지 요소 정의 DTD(Data Type Definition)에서 보안이 필요한 속성 파라메터를 bold체로 표시한다.

4.3.1 가입자 식별 요소 정의

가입자 식별 요소 중 보안이 필요한 요소로는 이동통신 가입자의 식별정보를 표현하는 msid, 개개의 가입자 단말기에 정의되어 있는 접근코드인 codeword, 위치기반 서비스 클라이언트가 가입자 단말기와 맺고 있는 세션에 대한 정보인 session이며, XML Encryption Tag element로 데이터를 암호화해야 할 필요가 있다.

4.3.2 기능적 요소 정의

기능 요소 중 보안이 필요한 요소로는 Report에 대한 응답을 보내기 위해 필요한 주소 정보를 나타내는 url이 해당되며, url은 아이디와 비밀번호를 포함할 수

```
<!-- MLP_ID -->

<!ELEMENT          msid       (#PCDATA)>
<!ATTLIST msid
          type (MSISDN | IMSI | IMEI | MIN | MDN | EME_MSID | ASID | OPE_ID | IPV4 | IPV6 | SESSID)
               "MSISDN"       enc (ASC | CRP)      "ASC">
<!ELEMENT          msid_range          (start_msid, stop_msid)>
<!ELEMENT          msids      (((msid, codeword?, session?) | (msid_range, codeword*))+)>
<!ELEMENT          codeword   (#PCDATA)>
<!ELEMENT          esrd       (#PCDATA)>
<!ATTLIST esrd
          type (NA)  "NA">
<!ELEMENT          esrk       (#PCDATA)>
<!ATTLIST esrk
          type (NA)  "NA">
<!ELEMENT          session    (#PCDATA)>
<!ATTLIST session
          type (APN | DIAL)     #REQUIRED>
<!ELEMENT          start_msid (msid)>
<!ELEMENT          stop_msid (msid)>
```

〔그림 10〕 가입자 식별 요소 정의 DTD

```
<!-- MLP_FUNC -->
<!ELEMENT          eme_event(eme_pos+)>
<!ATTLIST eme_event
          eme_trigger (EME_ORG | EME_REL)        #REQUIRED>
<!ELEMENT          tlrr_event  ( ms_action)>
<!ELEMENT          ms_action EMPTY>
<!ATTLIST ms_action
          type (MS_AVAIL)      #REQUIRED>
<!ELEMENT          interval    (#PCDATA)>
<!ELEMENT          loc_type    EMPTY>
<!ATTLIST loc_type
          type (CURRENT | LAST |CURRENT_OR_LAST | INITIAL)          "CURRENT">
<!ELEMENT          prio        EMPTY>
<!ATTLIST prio
          type (NORMAL | HIGH)          "NORMAL">
<!ELEMENT          pushaddr  (url, id?, pwd?)>
<!ELEMENT          req_id      (#PCDATA)>
<!ELEMENT          start_time  (#PCDATA)>
<!ATTLIST start_time
          utc_off CDATA        "0000">
<!ELEMENT          stop_time  (#PCDATA)>
<!ATTLIST stop_time
          utc_off CDATA        "0000">
<!ELEMENT          url         (#PCDATA)>
<!ELEMENT          time_remaining       (#PCDATA)>
```

〔그림 11〕 기능적 요소 정의 DTD

있는 pushaddr 항목의 일부분이다. 따라서 XML Encryption Tag element로 데이터를 암호화해야 할 필요가 있다.

4.3.3 위치 요소 정의

위치 요소 중 보안이 필요한 요소로는 위치정보 요청 시 이에 따른 서비스가 수행되었을 때의 시간을 나타내는 time이며, XML Encrytion Tag element로 데이터를 암호화해야 할 필요가 있다.

4.3.4 형상 요소 정의

형상 요소 중 보안이 필요한 요소로는 X, Y, Z 요소

```
<!-- MLP_LOC -->
<!ELEMENT          pos          (msid, (pd | poserr), gsm_net_param?)>
<!ELEMENT          eme_pos      (msid, (pd | poserr), esrd?, esrk?)>
<!ELEMENT          trl_pos      (msid, (pd | poserr))>
<!ATTLIST trl_pos
          trl_trigger (PERIODIC | MS_AVAIL)          #REQUIRED>
<!ELEMENT          pd           (time, shape, (alt, alt_acc?)?, speed?, direction?, lev_conf?)>
<!ELEMENT          poserr       (result, add_info?, time)>
<!ELEMENT          add_info     (#PCDATA)>
<!ELEMENT          result       (#PCDATA)>
<!ATTLIST result
          resid CDATA          #REQUIRED>
<!ELEMENT          time         (#PCDATA)>
<!ATTLIST time
          utc_off CDATA        "0000">
<!ELEMENT          alt          (#PCDATA)>
<!ELEMENT          alt_acc      (#PCDATA)>
<!ELEMENT          direction    (#PCDATA)>
<!ELEMENT          speed        (#PCDATA)>
<!ELEMENT          lev_conf     (#PCDATA)>
<!ELEMENT          geo_info     (CoordinateReferenceSystem)>
<!ELEMENT          CoordinateReferenceSystem     (Identifier)>
<!ELEMENT          Identifier   (code, codeSpace, edition)>
<!ELEMENT          code         (#PCDATA)>
<!ELEMENT          codeSpace          (#PCDATA)>
<!ELEMENT          edition      (#PCDATA)>
```

〔그림 12〕 위치 요소 정의 DTD

```
<!-- MLP_QOP -->

<!ELEMENT eqop     (resp_req?, resp_timer?, (ll_acc | hor_acc)?, alt_acc?,
    max_loc_age?)>
<!ELEMENT qop      ((ll_acc | hor_acc)?, alt_acc?)>
<!ELEMENT ll_acc   (#PCDATA)>
<!ELEMENT hor_acc  (#PCDATA)>
<!ELEMENT max_loc_age        (#PCDATA)>
<!ELEMENT resp_req EMPTY>
<!ATTLIST  resp_req
          type (NO_DELAY | LOW_DELAY | DELAY_TOL)        "DELAY_TOL">
<!ELEMENT          resp_timer (#PCDATA)>
```

〔그림 13〕 위치 정확도 요소 정의 DTD

이며, 이는 위치 정보의 기본 단위인 좌표 값이기 때문에 XML Encryption Tag element로 데이터를 암호화해야 할 필요가 있다.

4.3.5 위치 정확도 요소 정의

위치 정확도에 따른 요소들은 이미 보안이 처리된 위치 정보에 따른 정확도를 표현하기 때문에 별다른 보안이 필요한 요소는 없다. 향후 LBS 서비스 품질을 향상시키기에 필요한 속성 파라메터에 적용될 수 있는 보안 요소를 검토할 필요가 있다.

4.3.6 네트워크 요소 정의

네트워크에 따른 요소들은 CDMA(Code Division Multiple Access), GSM(Group Special Mobile), CDMA-2000, WCDMA(Wideband CDMA) 네트워크 요소를 정의한 곳으로 MLP의 Transport Layer에서 전송 계층에 따른 보안 처리를 하고 네트워크 기반 구조에 의존하는 보안 기능이 별도로 검토되어야 할 것이다.

```
<!-- MLP_GSM_NET -->

<!ELEMENT        NET_PARAM        (cgi?, neid?, nmr?, ta?)>
<!ELEMENT        cgi              (mcc, nmc, lac, cellid)>
<!ELEMENT        neid             (vmscid | vlrid | (vmscid, vlrid))>
<!ELEMENT        vmscid           (cc?, ndc?, vmscno)>
<!ELEMENT        vlrid            (cc?, ndc?, vlrno)>
<!ELEMENT        nmr              (#PCDATA)>
<!ELEMENT        mcc              (#PCDATA)>
<!ELEMENT        mnc              (#PCDATA)>
<!ELEMENT        ndc              (#PCDATA)>
<!ELEMENT        cc               (#PCDATA)>
<!ELEMENT        vmscno           (#PCDATA)>
<!ELEMENT        vlrno            (#PCDATA)>
<!ELEMENT        lac              (#PCDATA)>
<!ELEMENT        cellid           (#PCDATA)>
<!ELEMENT        ta               (#PCDATA)>
```

〔그림 14〕 네트워크 요소 정의 DTD

```
<!-- MLP_CTXT -->

<!ELEMENT        client       (id, pwd?, serviceid?, requestmode?)>
<!ELEMENT        sessionid    (#PCDATA)>
<!ELEMENT        id           (#PCDATA)>
<!ELEMENT        requestor    (id, serviceid?)>
<!ELEMENT        pwd          (#PCDATA)>
<!ELEMENT        serviceid    (#PCDATA)>
<!ELEMENT        requestmode          EMPTY>
<!ATTLIST requestmode
        type (ACTIVE | PASSIVE)       "PASSIVE">
<!ELEMENT        subclient    (id, pwd?, serviceid?)>
<!ATTLIST subclient
        last_client (YES | NO)"NO">
```

〔그림 15〕 문맥 요소 정의 DTD

4.3.7 문맥 요소 정의

문맥 요소 중 보안이 필요한 요소로는 프라이버시 구조를 제공하기 위한 요소에서 사용할 수 있는 식별자로, 위치 정보 서비스의 사용을 위한 id, pwd를 대체할 수 있는 sessionid, 위치 서비스를 수행하는 등록된 사용자의 비밀번호인 pwd, 네트워크에 접근하는 서비스나 애플리케이션을 구별하기 위한 식별자인 serviceid이며, sessionid와 pwd는 XML Encryption Tag element로 데이터를 암호화해야 할 필요가 있다. 또한 serviceid는 서비스 접근에 따른 보안을 취해야 하기 때문에 PKI(Public Key Infrastructure) 인터페이스로 처리되는 인증을 기반으로 보안을 해야 할 필요가 있다.

V. 결 론

최근 이동 통신 기술의 발달과 모바일 단말의 급속한 확산으로 인하여 위치 추적인 가능한 단말기를 휴대한 사용자의 현재 및 과거 위치 정보를 활용한 유무선 인터넷 서비스인 위치기반 서비스의 중요성이 한 층 대두되고 있다. 그러나 사용자에 대한 위치정보의 Privacy, 위치정보의 위·변조 문제, 위치정보의 기밀성, 위치정보서비스 사용자의 인증문제, LBS 플랫폼 서버로의 불법접근 등 많은 문제가 발생할 수 있다. 이러한 문제들은 개인 신상정보 노출 및 범죄 등에 악용될 수 있기 때문에 인증 및 보안 분야는 상당히 중요하다.

본 고는 정보의 유출을 차단하고 안전하게 위치기반

서비스를 제공하기 위한 LBS 플랫폼과 서비스 시스템 간 인증 및 보안 적용 방안을 수립하고 제시하는 것이 목적이었다. 이러한 목적을 달성하기 위해 LBS 보안 요구사항을 검토 분석 하였다. 그리고 안전한 위치기반 서비스를 제공하기 위한 기술 및 표준 동향을 분석하였다. 또한 LBS를 위한 MLP상에 인증 및 보안 기술 적용 방안을 도출하기 위해 KLP(Korea Location Protocol)의 기반이 되는 MLP 보안 구조를 정의함으로써, LBS 보안 요구사항을 기반으로 MLP 보안 요소를 도출하였다.

참 고 문 헌

[1] Location Interoperability Forum (LIF), http://www.locationforum.org

[2] 3GPP, "3GPP TS 23.271 V5.2.0 Functional stage 2 description of LCS (Release 5)", 2002, 3.

[3] 3GPP2, 3GPP2 N.S0030, TIA/EIA/J-STD-036-A, "Enhanced Wireless 9-1-1 Phase 2", April, 2002.

[4] FCC, FACT SHEET, FCC Wireless 911 Requirements, 2001.

[5] FCC, FACT SHEET, E911 Phase II Decisions, 2001.

[6] OASIS Web Services Security TC, http://www.oasis-open.org/committees/wss/

[7] Web Service Security Specification, http://www.verisign.com/wss/wss.pdf

[8] Simple Object Access Protocol(SOAP), http://www.w3.org/TR/2002/WD-soap12-part1-20020626

[9] XML Encryption, http://www.w3.org/Encryption/2001

[10] XML-Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[11] XML Access Control Markup Language, http://www.oasis-open.org/committees/xacml/index.shtml.

[12] XML Key Management Specification (XKMS),http://www.w3.org/TR/2001/NOTE-xkms-20010330/

[13] Getting Started With XML Security, http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html

〈著 者 紹 介〉

박 남 제 (Nam-Je Park)
정회원

2000년 : 동국대학교 정보산업학과 졸업
2003년 : 성균관대학교 정보보호학과 석사
2003년~현재 : 한국전자통신연구원 정보보호연구단 전자정부보안연구팀
관심분야 : 웹서비스 보안, 전자거래 보안, 그리드 보안, 무선인터넷 보안, 전자지불 등

송 유 진 (You-Jin Song)
정회원

1982년 : 한국항공대학교 전자공학과 졸업
1987년 : 경북대학교 대학원 정보시스템 전공 (석사)
1995년 : 일본 Tokyo Institute of Technology (박사)
1988년~1996년 : 한국전자통신연구원 선임연구원
1996년~현재 : 동국대학교 정보산업학과/전자상거래대학원 교수
1998년~현재 : 한국정보보호학회 이사, ISO/IEC JTC1/SC27-Korea 전문위원
관심분야 : 암호 및 인증이론, 웹서비스 보안, LBS 보안, 무선인터넷 보안, 전자화폐/전자지불 등

문 기 영 (Ki-Young Moon)
정회원

1986년 : 경북대학교 전자공학과 졸업
1989년 : 경북대학교 대학원 전자공학과 석사
1992년~1994년 : (주)대우정보시스템 기술연구소 대리
1994년 3월~현재 : 한국전자통신연구원 정보보호연구단 전자정부보안연구팀 팀장
관심분야 : 웹서비스 보안, 전자거래 보안, 분산시스템, 트랜잭션 등