http://dx.doi.org/10.3745/KIPSTC.2012.19C.1.029

모바일 네트워크에서 인터넷 응용을 위한 향상된 ID관리 프로토콜

박 인 신[†] · 정 종 필[††]

요 약

최근 급속도로 보급되고 있는 스마트폰과 SNS(Social Network Service)로 인한 인터넷 응용프로그램 활용의 증가는 3G 네트워크 이상의 네트워크 대역폭을 빠르게 잠식해가고 있으며 이로 인한 속도 저하와 서비스 질 저하로 인한 기간통신사들의 시설투자비 증가 요구가 강하게 대두되고 있다. 아울러 모바일 네트워크 사용자의 폭증에 따르는 모바일 서비스 제공자와 모바일 네트워크상의 ID관리문제를 촉발하고 있다. 본 논문은 3G 네트워크에서 모바일 인터넷 응용 서비스상의 사용자 ID관리와 보안문제를 해결하기 위한 프로토콜로 제안된 IDM3G[1]를 기반으로 보다 향상된 인증관리 프로토콜을 제안한다. 제안하는 I²DM 프로토콜은 기존의 IDM3G 프로토콜이 MO를 통한 상호 인증을 수행하면서 발생시키는 부하를 모바일 인터넷 응용 서비스 제공자에게 일정 부분의 역할을 분산시킴으로써 모바일 및 서비스 제공자의 ID관리와 함께 네트워크 부하와 정보처리를 위한 프로세스 부하 그리고 송수신되는 패킷의 수를 보다 효율화한다. 향후 더욱 그 수요가 폭증할 것으로 예상되는 3G 이후의 모바일 네트워크에 대한 수요를 대비하여 보다 최적화된 프로토콜을 제안한다.

키워드 : 정보통신, 모바일네트워크, 정보보안, 정보보호응용시스템

I²DM : An Improved Identity Management Protocol for Internet Applications in Mobile Networks

In-Shin Park[†] · Jong-Pil Jeong[††]

ABSTRACT

Due to rapid spread of smart phones and SNS(Social Network Service), using of Internet applications has increased and taking up bandwidth more than 3G network's capacity recently. This caused reduction of speed and service quality, and occurred strong needs that backbone network company to increasing investment costs. Also a great rise of mobile network users causing identity management problems on mobile service provider through mobile network. This paper proposes advanced IDM3G[1] - to solve user ID management and security problems on mobile internet application services over 3G network and more - authentication management protocol. I²DM protocol breakup loads which made by existing IDM3G protocol's mutual authentication via mobile operator, via sending some parts to internet application service provider, enhancing mobile and ID management of service provider and network load and process load from information handling and numbers of transmitting packets, to suggest more optimized protocol against further demanding of 3G mobile network.

Keywords : Information Communication, Mobile Network, Infomation Security, Information Protection Applied System

1. 서 론

최근 스마트폰의 변화 흐름과 모바일의 즉시성에 기반한 Facebook, Twitter와 같은 SP(Service Provider)들이 유행하면서 모바일 인터넷 응용 서비스 가입자 수가 크게 증가하고 있으며 앞으로 이의 수요는 더욱 크게 증가할 것으로 전망된다. 모바일 인터넷 응용 서비스 사용자 증가로 인해 대부분의 통신사들은 트래픽 부하 문제에 직면하고 있으며 이는 과도한 네트워크 유지비용에 따르는 투자대비 매출액간 불균형에 직면하였으며 이에 사업자 측면에서의 적절한 대응 전략이 요구된다. 이와 같은 네트워크 부하에 대한 이동통신사들의 전략은 MO(Mobile Operator)의 가용성을 확보하는데서 비롯되며 보다 적극적인 가용성 확보를 위해서 모바일 네트워크의 대역폭과 오퍼레이터의 정보처리를 가급적 최소화하지 않으면 안된다. 2009년 Ovum은 전세계 모바일 인터넷 가입자 수가 연평균 약 50%씩 성장하여 2010년에는

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0027030).
† 준 회 원 : 성균관대학교 정보보호학과 석사과정
†† 정 회 원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2011년 9월 9일
수 정 일 : 1차 2011년 11월 18일
심사완료 : 2011년 12월 2일

20억명으로 약 1,024% 증가할 것으로 예측한 바 있다. 2010년 7월12일 에릭슨코리아는 모바일 브로드밴드 가입자가 2015년까지 34억명을 초과할 것으로 보고 있으며, 한국에서는 이미 3000만명을 넘어선 것으로 보고 있다. 이 같은 추세는 2010년 'Facebook'(회원 약 5억8천만 명), 'Twitter'(회원 약 1억5천만 명)뿐 아니라 한국의 SNS(Social Network Service)인 '미투데이', '요즘', '토씨' 등 모바일 포털들의 회원 가입자도 약 2천5백만 명으로 전년 대비 57%나 증가한 것으로 나타나고 있다. 더욱이 현재 모바일 응용 서비스 유통 방식에 있어 모바일 응용 서비스 마켓 플레이스보다 모바일 웹사이트가 2배 이상 많은 이용량을 나타내며 실질적인 스마트폰 콘텐츠의 유통 채널이 되고 있어 향후 모바일 인터넷 응용 서비스와 그 가입자는 폭발적으로 증가할 것으로 보고 있어 3G 시스템 기반의 모바일 네트워크에 대한 효율적 ID관리의 필요성이 요구되고 있다.

모바일 시장에서 3G 시스템들은 새롭고 개선된 서비스를 제공할 통로로서 진정한 초고속 데이터 통신을 지원하고 있다[1]. UMTS(Universal Mobile Telecommunications System)와 CDMA2000(Code Division Multiple Access) 두 개의 지배적인 표준은 향상된 성능과 보안, 그리고 경제적이면서도 광범위한 멀티미디어 서비스의 지원을 목표로 설계되었으며 이러한 표준은 WLAN(Wireless Local Area Network)와 3G(3rd Generation)모바일 시스템의 통합 개발을 유도해왔는데[2] 이는 모바일 시스템의 높은 이동성과 넓은 영역의 커버리지 그리고 WLAN의 빠른 속도 기술을 상호 보완하기 위하여 개발된 것[3]으로 폭증하는 모바일 응용 서비스 가입자의 시대에 적절한 ID관리 메커니즘을 제공하고 있다. 모바일 인터넷 응용 서비스에 있어서 ID관리는 서비스의 성공에 있어 매우 중요한 요소[4] 중 하나로 서비스 제공자의 ID관리에 있어 사용자 친화적인 메커니즘을 도입하여 리소스를 효율적으로 관리할 필요가 있으며 이러한 이슈들은 마이크로소프트의 .NET Passport 프로토콜은 물론 오아시스의 SAML, XML 기반의 사용자 인증 데이터 교환 표준 개발을 이끌어 냈다. 이러한 표준에 대한 요구사항들은 사용자에 대한 투명성이나 다중ID 지원 뿐만 아니라 사용자의 익명성 유지와 사생활 보호는 물론하고 상호 운용성, 효율적인 신뢰관리, 강력하고 정교한 인증 및 권한 부여의 개념을 포함하고 있다[5].

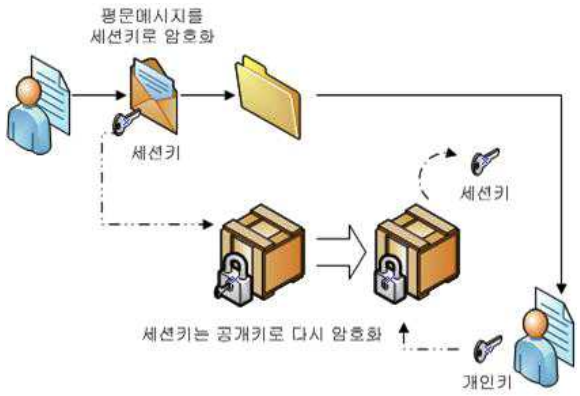
본 논문에서 제안하는 I²DM은 기존의 IDM3G와 같이 인터넷에서 서비스 제공자와 MO간의 개별적 통신이 아닌 상호 인증을 통한 SSO(Single Sign-On)와 같은 기능을 수행하기를 바라는 모바일 사용자들의 니즈(Needs)를 충족시키면서도[6] 기존의 IDM3G[7]에서 발생할 수 있는 MO의 성능 저하와 유지비용을 최소화시키는데 주력했다. 이는 서비스 제공자와 MO간의 쌍방향 인증을 통한 신뢰기반 구축으로 이루어졌으며 PKI(Public Key Infrastructure)에 기반한 PGP(Pretty Good Privacy)[8]의 원리를 도입함으로써 상호 신뢰기반의 통신은 물론이고 서비스 제공자에 대한 ID관리 가능성도 제시하고 있다. 이러한 기반 아래 I²DM은 서비스 제공자와 MO간의 모바일 ID 인증 단계(모바일 사용자 인증을 위한 패킷 수를 단축)를 단축함으로써 모바일 네트워크 대역폭과 모바일 오퍼레이팅 장비의 가용성을 향상시킬 수 있다.

본 논문은 I²DM을 구성할 PGP 응용 프로토콜과 IDM3G 표준 프로토콜과 관련된 각 표준들의 구성요소들에 대한 간략한 소개를, I²DM을 소개하는 프로토콜 설명, 그리고 그것에 대한 보안분석, 성능평가 및 구현복잡성 등으로 구성되어 있다.

2. 관련 연구

2.1 PGP 표준 프로토콜

인터넷에서 가장 광범위하게 사용되고 있는 전자우편 보안 시스템의 하나로 필 짐머만(Phil Zimmermann)이 독자 개발하여 프로그램을 공개한 것으로 전자 우편 내용의 기밀성, 메시지 인증, 사용자 인증, 송신 부인 방지 기능을 제공하고 있다. PGP(Pritty Good Privacy)는 메시지 비밀성 유지를 위하여 RSA와 IDEA 등의 암호화 알고리즘이 사용되며 메시지의 무결성과 사용자 인증을 위한 디지털 서명이 공개키 인증 방식(PKI)에 기반하고 있기 때문에 사용자 키 관리에 유리하다.



(그림 1) PGP 메시지 암호화 개요

(그림 1)과 같이 PGP는 전송하고자 하는 컨택스트를 로컬에서 생성한 세션키로 암호화 한 후 미리 상대방과 공유한(Key-Pairing) 공개키로 암호화하여 전송함으로써 사용자 인증과 메시지 보안을 획득하는 구조이다. 이 때 공개키는 송수신자간 상호 인증하는 것이 아니라 제3의 인증기관인 CA(Certificate Authority)를 이용하는 디지털 서명 방식을 채택할 경우 더 강력한 송수신자간 신뢰관계를 구축하는 것이 가능하며 공개 PGP 그룹(http://gnupg.org)[9]에서는 300,000개의 등록된 공개키를 가지고 있는 LDAP/HTTP 공개키 서버를 유지하며 이 서버는 전세계의 다른 사이트에 미러링되어 있다. 이와 같은 과정을 통해 제3자 인증과 공개키 관리(즉, 모바일 서비스 제공자의 ID)의 편의를 제공할 수 있다.

2.2 UMTS-AKA

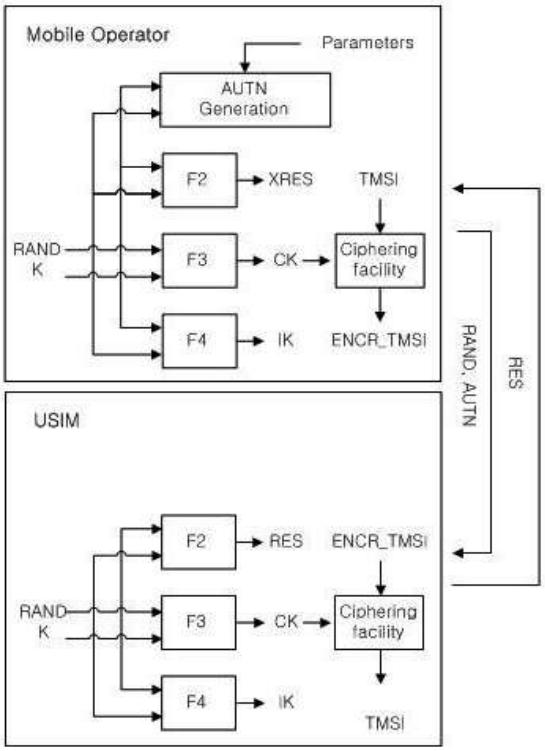
UMTS-AKA(Authentication and Key Agreement)는 3G 이동 통신 기술 중 하나로 셀룰러폰, 무선전화, 무선가입자망, 무선랜 등 무선 네트워크상의 안전한 통신을 위하여 설계된 프로토콜로 3GPP(3rd Generation Partnership Project)[10]에서 정의한 UMTS의 네트워크 접근 인증 메커니즘이다. UMTS-AKA는 통신 개체간에 상호 패스워드를 공유하지 않으면서도 한 개체가 다른 개체로 인증을 받기위한 의도로 설계된 Challenge/Response 프로토콜을 기본 개념으로 하고 있다. 이러한 UMTS-AKA의 인증과 키 인증 메커니즘은 3G 보안을 위한 3GPP 표준으로 사용자 ID관리, 기밀성, 무결성을 보장한다[11].

UMTS-AKA 메커니즘은 128비트 암호키를 기반으로 MO와 USIM 사이에 암호 알고리즘과 암호키를 사전에 공유한다. <표 1>은 이와 같은 UMTS-AKA의 인증요소를 나타낸다.

〈표 1〉 UMTS-AKA의 인증요소

인증요소	설 명
RAND	Random Number(Challenge)
K	Pre-shared 128bit secret key between MO and USIM
CK	Cipher Key
IK	Integrity Key
AUTN	Authentication Token
RES	Response
XRES	Expected Response
IMSI	International Mobile Subscriber Identity
TMSI	Temporary Mobile Subscriber Identity Privacy

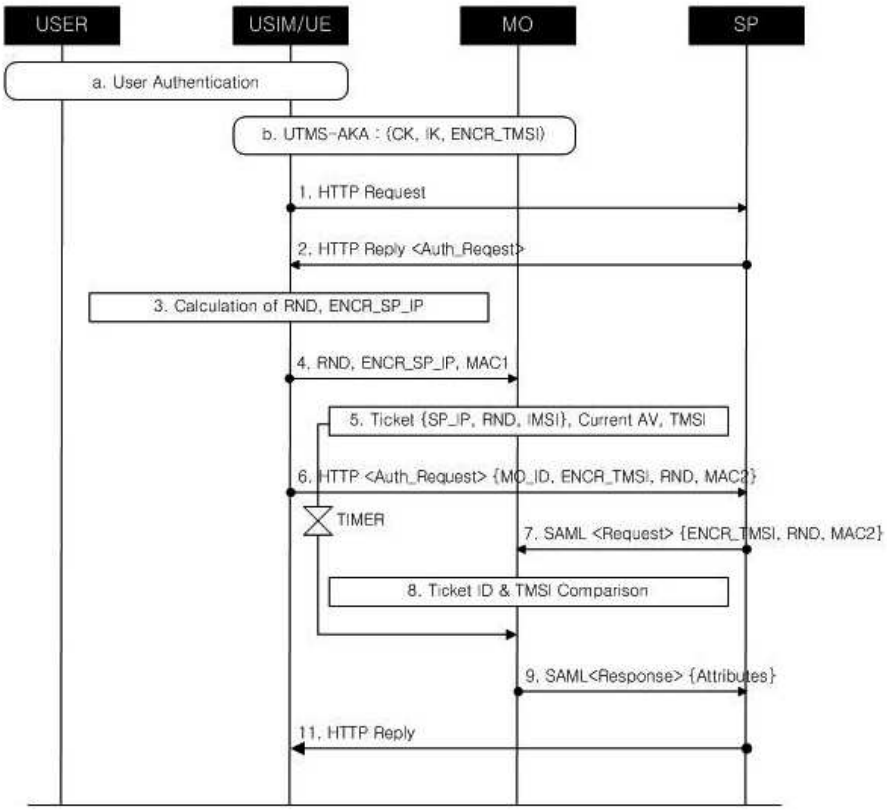
(그림 2)는 UMTS-AKA의 기본 구성 요소들을 단순화한 버전이다. (그림 2)에서 MO는 몇 개의 파라미터들과 RAND와 K에 의해 파생된 값(AUTN)과 시퀀스 값을 포함한 랜덤한 숫자를 USIM에 전달하고, USIM은 MO에 대하여 AUTN을 확인하여 인증하는데, USIM은 MO로부터 받은 RAND, K를 F2에 적용하여 RES를 계산하고 이를 MO로 전달함으로써(계산된 XRES와 비교) USIM의 인증을 구현한다. UMTS-AKA는 정교한 ID관리 메커니즘을 포함할 뿐 아니라 사용자 ID와 위치에 대한 불추적성도 포함하고 있다. 이러한 프라이버시는 IMSI(그룹 키 사용)의 암호화를 통해 달성된다. UMTS-AKA는 또한 사용자 정보(IMSI)를 보호하기 위해 TMSI를 사용하며 이러한 TMSI는 모바일 네트워크(Serving Network)에서의 첫 사용자 인증 이후 재인증의 목적으로 예측 불가능하게 할당된다. MO가 로컬로 보내는 임시 ID(TMSI, 위치 정보 - LAI와 동반될 수 있음)는 암호화되어 전송되는데(ENCR_TMSI) 128비트 Cipher Key(CK)를 사용하며, IMSI와 TMSI가 바인딩될 때 보내진다. 무결성 보호는 메시지 인증 코드(MAC)의 계산에 사용



(그림 2) UMTS-AKA의 기본 구성요소

되는 128비트 무결성 키(IK)의 배치로 실행된다. CK와 IK는 USIM과 MO에 의해 계산되는데, 미리 공유된 K와 RAND를 키 생성 함수에 적용함으로써 계산한다(F3과 F4). CK, IK, AUTN, RAND와 XRES는 UMTS-AKA 인증 요소의 그룹을 구성하고 있으며, 이들을 인증 벡터라고 한다. CK, IK와 TMSI는 I²DM에 의해 활용되는 요소들이다.

3G/WLAN 상호작용에서 UMTS에서의 ID관리는 사용자와 MO간의 상호 인증에 영향을 미친다[12]. I²DM에서는 이 두 독립적인 개체간의 관계를 활용하여 모바일 인터넷에서의 사용자와 서비스 제공자간의 ID관리를 실행한다. 이러한 프로토콜은 Liberty Alliance의 사양을 고려하여 구현됨으로써 ID관리를 위하여 개발한 공개표준으로 OASIS의 확장된 SAML 표준으로 구현되었다. SAML은 보안 정보를 교환하기 위한 XML 기반의 프레임워크로 각각의 주체는 보안 도메인 안의 ID를 포함한 독립적인 개체이다. 이와 같은 과정은 특정 리소스에 접근이 허가되었는지에 관한 인증 결정, 인증행위에 대한 정보를 처리할 수 있다[13]. Liberty Alliance는 집단적 정체성의 제휴 관리, 도메인 간 인증 및 세션 관리를 위한 솔루션을 제공하는 프로토콜의 집합을 정의하는데[14], Liberty Architecture의 주체 즉 ID 제공자와 서비스 제공자를 포함하고 있다[15]. 주체는 ID 제공자로부터 받은 ID를 가지고 있는 독립적인 개체이고 서비스 제공자는 서비스를 주체에게 제공하는 독립적인 개체이다. 주체가 ID제공자에게 인증받으면, ID 제공자는 인증을 제공할 수 있다. 서비스 제공자가 이 요청을 신뢰하는 것으로써 ID는 인증된다.



(그림 3) IDM3G 프로토콜 개요

2.3 IDM3G 프로토콜

IDM3G는 2004년 3G 모바일 네트워크상의 인터넷 이용시에 UMTS-AKA 프로토콜을 근간으로 서비스 제공자와 사용자간의 상호 인증과 허가에 중점을 두며 사용자 ID의 중복 제공을 피하기 위한 SSO 측면을 중점 구현하기 위해 제안되었다[1]. 또한, 독립적인 개체로서 UMTS 모바일 뿐만 아니라 3G 모바일과 WLAN의 상호 네트워크 작용에도 적용될 수 있다.

(그림 3)에서 보여주고 있듯 IDM3G의 프로토콜은 과거 IP Network상에서 서비스 제공자들간의 SSO를 구현하기 위한 사용자 인증 프로토콜들이(대표적으로 Microsoft .Net Passport) 그러하듯 대부분 사용자를 인증한 이전 SP와 새로운 SP간의 ID 인증교환 과정을 거칠 수 밖에 없는데서 발생하는 다수의 메시지 교환의 과정을 MO와 MO에서 만들어지는 Ticket{SP_IP, RND, IMSI}, TMSI를 SP에게 전달함으로써 줄일 수 있을 뿐 아니라 모바일 네트워크의 특성상(Serving Network) MO간의 핸드오버까지 고려된 것이다. IDM3G는 4개의 독립적인 개체로 이루어지는데 사용자(U), 사용자 장비에 연결된 USIM(USIM/UE), MO(MO - 인프라스트럭처에 연관된 모든 컴포넌트) 그리고 서비스 제공자(SP)가 그것이다. Liberty Alliance 프로토콜에 의하면 주체는 사용자와 USIM/UE의 조합이고 ID공급자는 MO, 서비스 제공자는 SP로 정의하고 있다[16]. IDM3G USIM/UE는 MO가 공유하는 TMSI와 UMTS-AKA의 인자들로 Ticket을 만들고 이 인자값들을 SP에게 보내게 되는데 MO의 측면에서는 자신이 가진 USIM/UE의 정보(Ticket)으로 만들어 인증 요청을 대기하다가 SP로부터 SAML로 요청 받은 정보(그림 3의 7단계)를 비교하는데 이것이 IDM3G의 프로토콜의 핵심 프로세스이다. 이와 같은 핵심 프로세스를 통해서 <표 2>와 같은 프로토콜의 보안성을, <표 3>과 같은 프로토콜의 성능 개선을 달성할 수 있다.

〈표 2〉 IDM3G의 보안 성능 요약

IDM3G 요소	보안적 성능
TMSI	프라이버시 보호
UE/USIM & MO	상호 인증
Cipher Key (UMTS-AKA)	신뢰 / 무결성 보호
TMSI, Timer in MO	리플레이 보호
Entity Impersonation Protection	MITM Aattack 보호
No Password Protocol	Brute Force & Dictionary Attack 보호
CK, IK by UMTS protocol	키 배분 정책
IETF Randomness Recommand	난수 생성

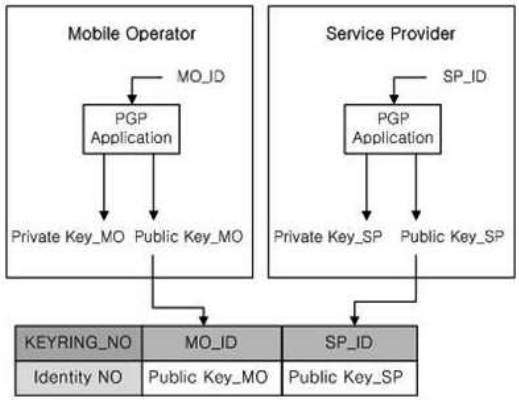
〈표 3〉 프로토콜간 메시지 교환 수 비교

프로토콜 구분	UE와의 메시지 교환 회수	메시지 교환 회수 총합
Liberty artefact profile for SSO	8	10
Liberty browser Post profile for SSO	8	8
Liberty-enabled client & proxy profile for SSO	6	12
Microsoft .Net Passport	8	8
IDM3G	5	7

본 논문에서는 IDM3G 프로토콜의 단계별 상세한 설명은 생략하기로 한다.

3. 제안하는 I²DM 프로토콜

I²DM은 IDM3G 프로토콜을 근간으로 성능적인 면과 보안적인 면의 개선을 제안한다. 특히, IDM3G는 사용자를 인증하기 위하여 USIM/UE의 정보를 SP로부터 받는 과정에 타이머가 작동함에 따라 MO 자체에 많은 부하를 예상할 수 있다. (그림 3)은 SP가 MO와 USIM/UE로부터 전달받는 암호화된 Ticket을 인증하기 위한 사전적 신뢰기반의 원리에 대해 간략하게 설명하고 있다. 프로토콜의 작동원리는 MO와 SP의 공개키를 사전에 등록하고 신뢰/관리 관계를 수립하는데 그 기반을 두고 있다.

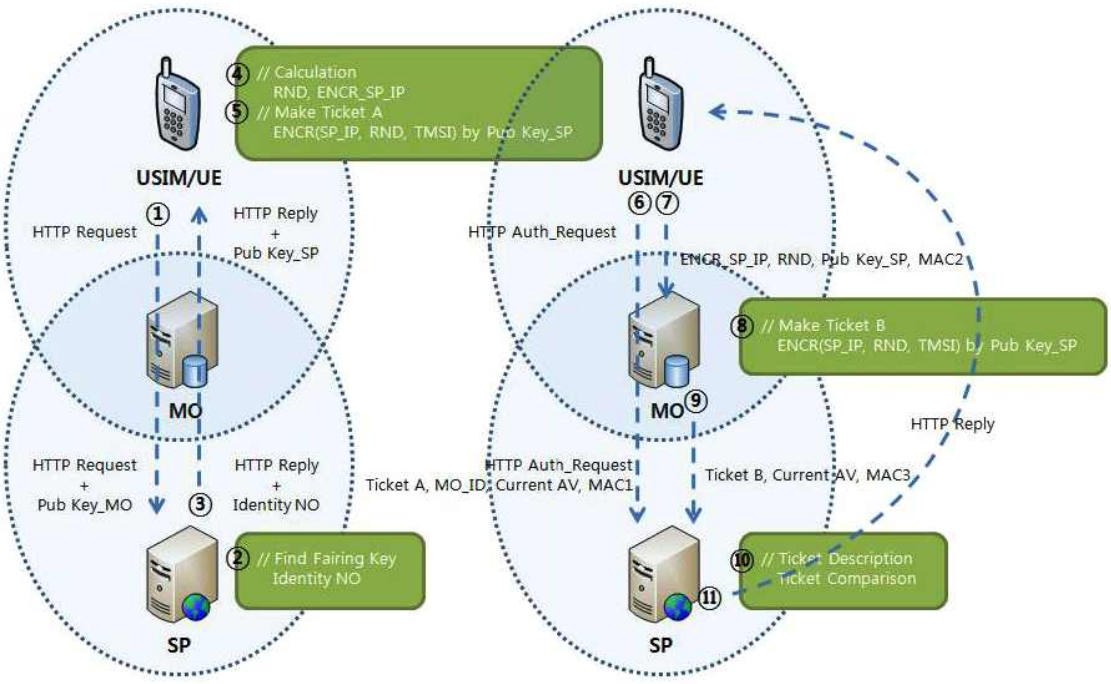


(그림 4) MO와 SP의 공개키 교환과 관리

(그림 4)과 같이 SP와 MO간에 PGP 알고리즘을 이용하여 SP의 공개키를 등록하고 MO는 SP를 쌍으로 등록함으로써 SP에 대한 신뢰를 높이고 서비스 제공자로써의 SP를 효과적으로 관리할 수 있다. 이 때 공개키의 인증은 MO에서 제공하는 제3의 인증기관을 활용할 수 있다. 미국의 경우를 예를 들면, PGP의 공개키는 Network Associates에서 300,000개의 등록된 공개키를 가지고 있는 LDAP/HTTP 공개키 서버를 유지하고 있고 이 서버는 전세계의 다른 사이트에 미러링되어 있으며 이를 통해 디지털 서명과 같은 효과를 유지할 수 있다.

I²DM 프로토콜은 다음 사항을 가정한다.

첫째, MO와 SP사이에는 확고한 비즈니스적 합의와 신뢰의 관계(안전한 경로를 포함하여)이다. MO와 사용자간의 비니지스적 신뢰와 합의는 MO와 사용자간의 사용계약으로 이



(그림 5) I²DM 프로토콜

루어지며 사용자의 ID는 MO에게만 알려진다. 단말기 사용자의 신원이 계약자와 동일하지 않을 수 있으나 이것은 계약당사자의 책임이며, 모바일 장비의 실제 사용여부는 생체기술로 해결할 수 있다[17].

둘째, SP가 MO의 사용자에게 서비스를 개시하려면 MO의 규약에 의해 사전에 PGP 알고리즘에 의한 키 교환과 ID Ticket을 비교하는 알고리즘을 채택해야 한다. 이러한 규약은 ID 제공자(MO)와 서비스 제공자(SP)간에 공유된다. MO는 이렇게 등록된 SP의 공개키를 관리하고 분배해야 한다. 이와 같은 과정을 통하여 MO와 SP는 신뢰관계를 획득할 수 있다.

셋째, 사용자는 3GPP의 사양에 따라 PIN을 보냄으로써 USIM을 인증하고[18-19] UMTS-AKA 메커니즘은 이미 설명한 바와 같이 USIM과 MO의 상호 인증을 위해 배치된다. 이 단계에서 CK(데이터 암호화)와 IK(독립 보호)는 USIM과 MO 모두에 의해 계산되고 TMSI는 MO에 의해 암호화되어 USIM에 전달된다.

(그림 5)와 같이 사전에 신뢰관계를 맺은 SP의 정보는 MO를 거치면서 SP의 인증이 요구되는(특정 IP를 Hold한) 지점에 사용자가 접속을 시도할 때 I²DM의 프로토콜이 초기화된다. 프로토콜은 다음 단계로 구성되어 있다.

1단계 : USIM/UE(사용자)가 SP에 서비스를 요청하기 위한 표준 HTTP Request를 MO를 거쳐 전송할 때 MO는 사용자로부터 요청받은 SP의 공개키에 페어링(Paring)된 MO의 공개키를 찾아 함께 SP로 전달한다.

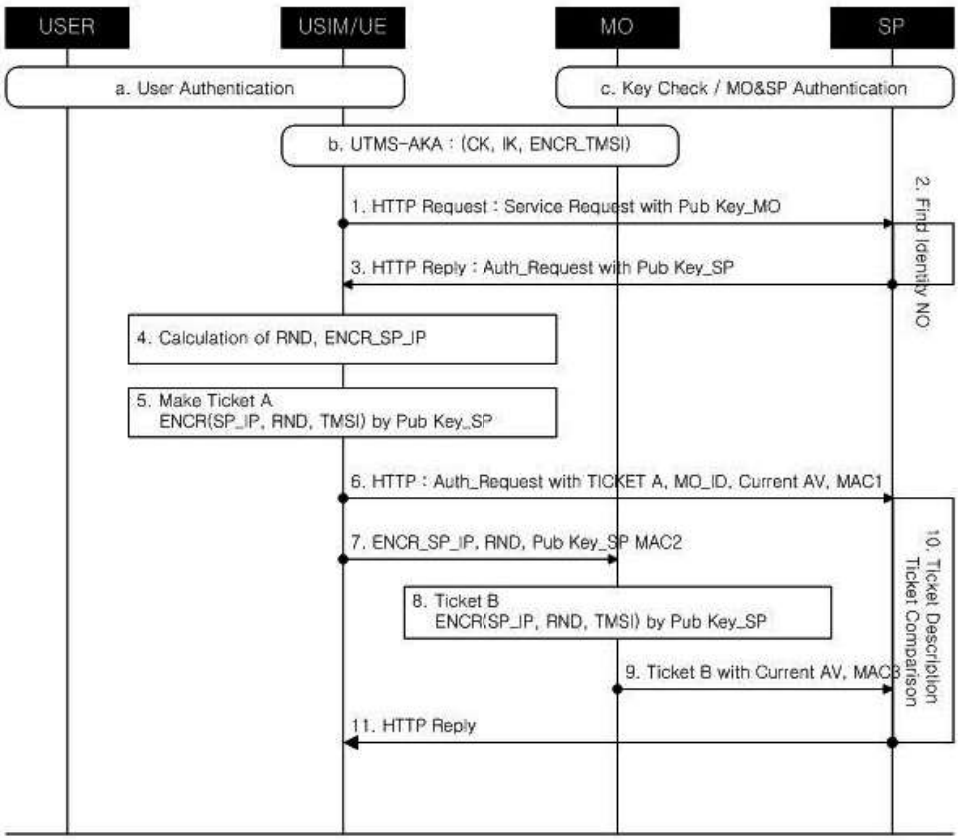
2단계 : USIM/UE(사용자)의 서비스 개시를 위하여 SP는 MO에서 보내온 공개키(Pub Key_MO)를 이용해 맵핑되는 Identity NO를 찾아서 자신의 공개키(Pub Key_SP)로 보낼 준비를 한다.

3단계 : SP는 USIM/UE(사용자)에 인증을 요구하는 표준 HTTP Reply를 자신의 공개키(Pub Key_MO)전달한다.

4단계 : USIM/UE(사용자)는 RND, ENCR_SP_IP를 계산한다.

5단계 : 4단계에서 계산된 RND와 ENCR_SP_IP와 USIM/UE(사용자)의 TMSI를 3단계에서 전달받은 SP의 공개키(Pub Key_SP)로 암호화하여 Ticket A를 만든다.

6단계 : USIM/UE(사용자)는 SP의 인증요구에 대하여 5단계에서 생성된 Ticket A와 UMTS-AKA의 인증벡터(Current AV)를 패킷의 데이터 무결성 확인을 위한 메시지 인증 코드(MAC1)와 함께 SP로 전달한다. 이때의 메시지 인증코드(MAC1)와 파라미터인 RND는 재사용을 방지하기 위해 한번만 유효하다. SP는 USIM/UE(사용자)가 보내온 Ticket A의 무결성을 확인하고(MAC1) 자신의 개인키(Private Key_SP)로 복호화함으로써 USIM/UE(사용자)로부터 받은 인증 파라미터를 확인한 다음 Ticket B와 비교하기 위해 대기한다. 이 때 두 패킷을 비교하기 위한 세션시간을 제한할 수 있다.



(그림 6) I²DM 메시지 전달절차

7단계 : USIM/UE(사용자)는 4단계에서 계산한 RND, ENCR_SP_IP와 2단계에서 SP로부터 전달받은 Pub Key_SP와 함께 MO로 전달한다. 이 때 무결성 확인을 위한 메시지 인증 코드(MAC2)와 UMTS-AKA의 인증벡터(Current AV)를 함께 전달한다.

8단계 : MO는 전송받은 RND, ENCR_SP_IP 그리고 SP의 공개키(Pub Key_SP)를 MO가 이미 가지고 있는 USIM/UE(사용자)의 TMSI 정보와 함께 SP의 공개키(Pub Key_SP)로 암호화하여 Ticket B를 생성한다.

9단계 : MO는 8단계에서 생성된 Ticket B를 UMTS_AKA의 인증벡터(AV), 메시지 인증 코드(MAC3)와 함께 SP로 전달한다.

10단계 : SP는 USIM/UE(사용자)가 보내온 Ticket B의 무결성을 확인하고(MAC3) 자신의 개인키(Private Key_SP)로 복호화함으로써 MO로부터 받은 USIM/UE(사용자)의 인증 파라미터를 확인한 다음 Ticket A의 정보와 비교하여 일치하는지 여부를 확인하며 두 Ticket이 일치하면 인증이 완료된다.

11단계 : 10단계에서 인증이 완료되면 서비스를 요청한 USIM/UE(사용자)에게 즉각 제공한다(HTTP Reply).

(그림 6)는 I²DM 프로토콜의 구조를 통신주체별 메시지 전달절차를 설명한 것이다.

4. I²DM 프로토콜 평가

I²DM 프로토콜은 설계단계에서 IDM3G를 분석하여 제안한 것으로 IDM3G의 보안적 평가, 성능 측면의 평가, 구현 복잡도 측면의 분석 기법을 그대로 따른다. 이러한 보안과 프라이버시에 대한 분석 기법은 RFC의 보안 및 프라이버시 문제 해결을 위한 IETF 권고안에 따라 분석되며 추가로 I²DM과 IDM3G의 상호 성능을 비교 분석한다.

4.1 보안분석

IETF의 10가지 제시 항목에 대한 보안 분석은 다음과 같다.

1) 프라이버시 : I²DM 프로토콜은 도·감청은 물론 사용자의 신원정보를 보호할 수 있다. IMSI는 SP로 전송되지 않으며 TMSI 역시 PGP 알고리즘에 의해 단방향으로 암호화 전송 처리된다. MO로 전송된 메시지의 경우 임시 ID로 MO와 SP에서 식별한다. SP로 보내지는 정보들은 사용자의 서비스에 접속하는 권한과 연관된 정보를 스스로 발급한 공개키에 대칭되는 개인키로 복호화한다.

2) 상호 인증 : 상호 인증은 독립된 개체들의 프로토콜 사이에 성립된다. UE/USIM과 MO는 UMTS-AKA 메커니즘을 통해 상호 인증한다. MO와 SP간의 상호 인증은 프로토콜 작업의 전제조건 즉, 두 독립된 개체간의 비즈니스적인 동의에 의한 안전한 경로의 확보가 포함되어 있으며 MO와 SP의 PGP 키 관리 매커니즘을 통해 직접적 혹은 제 3의 인증을 통해 성립된다. 사용자와 USIM 간의 인증은 3GPP 사양에 따라 PIN을 통해 구현된다[20]. 더 나아가 잘 디자인된 생체 컴포넌트가 배치된다면 더욱 강력한 인증 메커니즘이 실행될 수도 있다. IETF의 권고안에는 이러한 3G 모바일과 WLAN 간의 상호작용에 생체 인증을 하는 직접적인 예가 나타나 있다.

3) 기밀성 : CK를 이용한 대칭 암호화를 통해 기밀성이 성립된다. 암호화 메커니즘의 강도는 3GPP 사양의 UMTS-AKA를 통해 승계된다.

4) 무결성 : UMTS-AKA 알고리즘에 기반한 메시지인증 코드(MAC)에 의해 무결성 보호가 구현된다. MO와 UE/USIM의 메시지 교환 간에 MAC의 계산이 IK를 이용하여 이루어지며, PGP 알고리즘에 의거한 PKI 방식도 무결성을 확인한다.

5) Replay 공격 : Replay 공격 보호는 4가지 요소로 구성된다. 첫째, CK와 IK의 변조를 일으키는 UMTS-AKA의 전체 인증 절차에서 인증벡터 비교(3GPP 명시), 둘째, TMSI의 비교(UMTS-AKA 메커니즘에 명시), 셋째, MAC의 무결성 보호를 위해 계산할 때 따라오는 RND의 계산이다. RND는 특정 Ticket을 구분하고 특정 시간 프레임 동안 단일하다. (TMSI의 최대 수명보다 훨씬 길어야 함. 추가적으로 SP는 MO와 UE의 두 Ticket을 인증하는 시간간격을 비즈니스 및 네트워크 환경에 따라 사전에 협의함으로써 제한을 두어 보호할 수도 있다.)

6) MITM(Man-in-the-middle) 공격 : 해커가 공격의 가운데에 존재하게 되는 하이재킹 공격 세션과 독립성 유지는 위에서 설명된 무결성, 기밀성, Replay 공격 보호와 상호 인증과 연결되어 이루어진다. 아울러 I²DM은 MITM에 강하도록 상호 인증을 기반으로 설계되어 있다. 아울러 PGP의 메커니즘을 이용하여 SP의 공개키를 비교하는 방식은 피싱(Phishing)이나 파밍(Farming)과 같은 사회 공학적 공격에 강하다.

7) Brute force / Dictionary 공격 : UMTS-AKA는 패스워드 프로토콜이 아니다. 따라서 I²DM는 근본적으로 Dictionary 공격이나 Brute force 공격에 강하다. 단, 일반적인 GSM (Global System for Mobile Communications)의 COMP128 암호화 알고리즘이 가진 약점으로 2G 시스템에서는 SIM 복제에 도달하는 비밀 키를 추출해낼 수 있다[21]. 이러한 공격은 강화된 알고리즘과 보안 대책을 탑재한 3G에서 해결할 수 있다[22].

8) 키 유도 보호 : UMTS 프로토콜의 보안레벨에서 물려받은 암호화된 키인 CK와 IK는 UMTS-AKA 사양을 기반으로 하고 있다. MO와 SP간의 비대칭 키는 PGP 알고리즘과 키 교환 구조에 기반을 두고 있다.

9) 랜덤 숫자 생성 : 보안 프로그램에 쓰이는 RND는 IETF 임의성의 권장[23]에 따라 생성된다.

10) DoS 공격 보호 : 다양한 유형의 DoS 공격이 올 수 있다[24]. I²DM에 가장 적절한 공격 중의 하나는 연관된 통신 주체들에게 잘못된 오류 메시지들을 보내는 것으로, 현재 수준의 프로토콜에 대한 설명은 에러의 경우와 그에 해당하는 에러 메시지들은 포함하지 않고 있다. 이것은 차후에 진행할 연구이슈들 중에 하나이다.

<표 4>에서 IETF의 방법론에 따르는 IDM3G와 I²DM간의 보안 성능을 비교하여 보여준다.

〈표 4〉 IDM3G와 I²DM과의 보안 성능 비교

IETF 보안권고항	IDM3G 보안원리	I²DM 보안원리	보안성능 비교
(1) 프라이버시	TMSI	TMSI	동일
(2) 상호 인증	USIM/UE	USIM/UE + MO/SP	I²DM 우세
(3) 기밀성	UMTS-AKA	UMTS-AKA	I²DM 우세
(4) 무결성	UMTS-AKA	UMTS-AKA + RSA(PKI)	I²DM 우세
(5) Replay 공격	TMSI, MO Timer	TMSI, Limited Ticket	동일
(6) MITM 공격	(2)(3)(4)	(2)(3)(4)	I²DM 우세
(7) Brute force / Dictionary 공격	No PW	No PW	동일
(8) 키 유도	UMTS-AKA	UMTS-AKA + RSA(PKI)	I²DM 우세
(9) 랜덤숫자생성	UMTS-AKA	UMTS-AKA	동일
(10) DoS 공격	취약	취약	동일

4.2 성능 측면에서의 평가

프로토콜의 작동에 있어서 중요한 매개변수는 실제로 모바일 사용자의 장비가 네트워크 통신에 있어 한정된 성능을 가지고 있다는 점이다. I²DM의 성능을 측정하기 위해서는 이런 USIM/UE의 장비 환경이 조사되어야한다. USIM/UE와 다른 프로토콜의 독립적인 개체들 간에 교환된 메시지의 숫자도 평가에 포함되어 있다. I²DM는 미리 계산된 값들의 세트를 활용하고 (UMTS-AKA 메커니즘 기반의 상호 인증 네크워크 액세스 동안에 얻어짐) 작업 동안 값들의 세트가 계산된다. 이 기능은 4단계에서 랜덤 번호 생성, SP_IP 암호화, 그리고 10단계에서의 Ticket 비교가 SP에서 이루어짐으로서 MO의 작업 부하를 줄여준다. 난수생성기를 포함한 이러한 계산들은 3GPP 사양에 호환되는 USIM 제품에 의해 적절하게 통제된다. 연관된 통신주체들 간에 교환된 메시지의 숫자에 관해서는, I²DM는 .NET Passport 프로토콜과 Liberty Alliance의 ID관리 프로토콜 프로필을 비교한다[25-27]. 사용자 클라이언트와 다른 통신주체들이 각 프로토콜을 통해 주고받은 메시지의 숫자는 물론 각 프로토콜에서 주고받은 메시지 수의 총 합도 계산된다. 같은 조건이 모든 프로토콜에 고려되며 이는 서비스 제공자와 ID 제공자가 이미 상호 인증을 거쳤으며 이에 연관된 메시지는 계산되지 않는다는 전제조건을 포함한다. Liberty Alliance 프로토콜은 .NET Passport 프로토콜과는 상반되게 사용자가 이미 ID 제공자에게 인증을 받았다고 가정하고, 이 인증 메시지들을 포함한다는 점과 SP와 MO가 등록과정을 통해 상호 인증되어 있다는 점을 강조해야만 한다. 결과를 일반화시키기 위해서는 Liberty Alliance 프로토콜의 5가지 주요 메시지들(인증 요청과 인증 응답)에 적어도 2가지 메시지가 추가되어야 한다. 3G 모바일 아키텍처와 ID 제공자로서 MO의 역할 통합과 SP로의 부하 분산을 위해 I²DM은 이런 메시지들을 요구하지 않는다. <표 5>는 IDM3G와 I²DM 두 프로토콜간의 통신 주체별 메시지에 대한 비교 결과를 제시하고 있다.

〈표 5〉 IDM3G & I²DM 통신주체별 메시지 수 비교

통신주체별 메시지 분석	IDM3G	I²DM
UE/SP간 메시지 총합	5	5
USIM/MO/SP간 메시지 총합	7	6
MO/SP or MO/UE 메시지 총합	2	1
전 과정의 메시지 통과 주체 총합	18	16

I²DM는 Liberty Alliance나 .NET Passport 프로토콜과 비교하여 사용자 장비에 상당히 낮은 숫자의 메시지들을 수반하며 총 메시지 교환 숫자의 총합도 가장 적다. 이것은 통신주체단의 성능 개선 속도를 고려하고 3G 인프라스트럭처의 프로토콜 기능을 통합시켜 통신주체간 상호 신뢰 매커니즘을 적용한 결과이다.

4.3 구현 복잡성 분석

I²DM는 간단하지만, 기존의 표준을 기반으로 쉬운 구현과 사용자 터널 장비의 기술적인 기능과의 호환성을 보장한다. 프로토콜 구현의 복잡성 및 연관된 통신주체들과 관련한 요구사항을 아래와 같이 분류/분석하였다.

- 사용자 터미널 장비 : UE는 Liberty Alliance 프로토콜에 정의된 기본 요구사항, HTTP와 WML 지원을 충족해야 한다[28]. USIM의 표준 기능은 프로토콜의 기능들을 구현하는데 충분하고 USIM의 기능을 이용하여 이미 존재하는 브라우저의 통신 프로토콜의 기능들을 조합하는 것으로 I²DM를 구현할 수 있다.
- MO : MO들은 이미 그들의 사용자들에 대한 개인정보를 관리할 강력한 보안 메커니즘으로 보호된 인프라스트럭처를 가지고 있다. 그런 의미에서 MO는 ID 제공자와 SP의 PGP 공개키 분배 및 관리의 역할에 이상적이다. 기존 인프라스트럭처의 확장에 필요한 사용자의 속성을 더한 테이블과 기존 사용자 데이터베이스의 확장으로 SP 키 관리 및 MO와 서비스 제공자간의 안전한 통신 경로를 구현할 수 있다.
- 서비스 제공자 : 서비스 제공자는 모바일 운영자와 통신할 안전한 경로와 그들의 권리에 접근하기 위해서 MO가 제공하는 PGP 메커니즘과 Ticket 비교 알고리즘을 구현

해야 하고 기존 사용자 관리 및 서비스 제공자의 인프라스트럭처도 확장해야한다.

<표 6>은 I²DM를 구현하기 위해 쓰이는 기반기술을 보여준다.

〈표 6〉 통신주체별 구현복잡성 분석

구분	I²DM 구현의 기반기술
USIM/UE	Liberty Alliance with HTTP, WML
MO	MO - SP Secure communication RSA Key Derivation PGP infrastructure
SP	MO - SP Secure communication RSA Algorithm Secure Ticket Comparison Method

5. 결 론

모바일 단말의 성능향상은 모바일 네트워크 대역의 사용량을 급증시키는 결과를 가져왔고 사업자들은 새로운 신규시장에 집중하게 됨으로써 양적, 질적인 팽창이 진행 중이지만 감청이나 개인정보 도용과 같은 보안적인 요소는 많이 고려되어지지 않고 있는 것이 현실이다. I²DM은 기존의 IDM3G가 가지고 있는 최대 약점인 MO 프로세싱의 집중현상을 최대한 SP로 분산하여 네트워크 비용을 절감하였으며 사회공학적 공격에 대응하기 위한 기반을 강화하였을 뿐 아니라 IDM3G의 장점을 최대한 살려 모바일 네트워크에서 그 특유의 투명성, 기밀성을 제공하는 ID관리의 용이성을 제공한다. 이때, I²DM은 인증의 주체를 MO에서 SP로 옮기면서 기존의 IDM3G에서 SP로 제공하지 않았던 USIM/UE의 정보들에 대하여서는 256비트 키와 RSA기반의 PGP 메커니즘을 이용하여 보안성을 획득하였다.

I²DM은 기존의 IDM3G에 비해 MO의 데이터 처리량 감소와 네크워크 대역폭 부하를 줄여 전반적인 네트워크 비용을 감소시켜 소비가 증대되고 있는 모바일 네트워크에서의 MO의 가용성을 강화했다. 아울러 강력한 SP 관리와 함께 관리의 용이성도 함께 제공하였다. 그러나, 보안 프로토콜인 I²DM의 연구에서 프로토콜 자체의 실질 성능 평가와 DoS 공격에 대한 연구는 계속적으로 진행되어야하며 PGP 알고리즘을 구현하기 위한 추가적인 연구와 보안성 확보를 위해 SP 자유도를 제한함에 따라 발생하는 비용감소에 대한 연구 그리고 실질적인 성능 평가가 추후의 연구과제로 남았다.

참 고 문 헌

[1] Wisely D, Eardley P, and Burness L. IP for 3G - networking technologies for mobile communications, John Wiley & Sons, 2002.

[2] 3rd Generation Partnership Project. TS 23.234 - 3GPP system to wireless local area network (WLAN) interworking; system description v2.4.0, 2004.

[3] Mont M, Pearson S, and Bramhall P., "Towards accountable management of identity and privacy," Proceedings of 14th international workshop on database and expert systems applications, 2003.

[4] Bonatii P and Samarati P., "A unified framework for regulating service access and information release on the web," Computer Security Journal, Vol.10(3), pp.241-72, 2003.

[5] Damiani E, De Capitani di Vimercati S, and Samarati P., "Managing multiple and dependable identities," IEEE Internet Computing, Vol.7(6), pp.29-37, 2003.

[6] Siemens, "Identity management for micropayments in a mobile environment," Paycircle, 2003.

[7] Christos K. Dimitriadis and Despina Polemi, "An identity management protocol for Internet applications over 3G mobile networks," Computers & Security, Vol.25, pp.45-51, February, 2006.

[8] Ed Gerck, Secure Email Technologies X.509 / PKI, PGP, IBE, and ZMAIL, in Chapter 12, Corporate Email Management, ICFAI University Press, pp.171-196, 2007.

[9] http://www.gnupg.org

[10] http://www.3gpp.org

[11] 3rd Generation Partnership Project. TS 33.102 - 3G security; security architecture v6.0.0, 2003.

[12] 3rd Generation Partnership Project. TS 33.234 - 3G security; wireless local area network (WLAN) interworking security v6.0.0, 2004.

[13] OASIS. Glossary for the OASIS security assertion markup language(SAML) v1.1, 2003.

[14] Liberty Alliance. Liberty ID-FF protocols and schema specification v1.2, 2003.

[15] Liberty Alliance. Liberty ID-FF architecture overview v1.2, 2003.

[16] http://www.sdl-forum.org/MSC/index.htm

[17] Dimitriadis C and Polemi D., "A protocol for incorporating biometricsin 3G with respect to privacy," 7th international conference on enterprise information systems (ICEIS2005), pp.123-135, 2005.

[18] 3rd Generation Partnership Project. TS 31.101 - UICC terminal interface; physical and logical characteristics v6.2.0, 2003.

[19] 3rd Generation Partnership Project 2. S.R0082 enhanced packet data air interface security v1.0, 2003.

[20] Urien P, Pujolle G, EAP-support in smartcard draft-urien-eap-smartcard-21.txt, IETF draft, 2011.

[21] Rao J, Rohatgi P, Scherzer H, and Tinguely S., "Partitioning attacks: or how to rapidly clone some GSM cards," IEEE symposium on security and privacy, 2002.

[22] Khan M, Ahmed A and Cheema A.R, "Vulnerabilitis of UMTS Access Domain Security Architecture", Software

Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08, Ninth ACIS International Conference on
[23] Eastlake D, Crocker S, Schiller J., "Randomness recommendations for security," IETF RFC 1750, 1994.
[24] Fry M, Fischer M, Karaliopoulos M, smith P and Hutchison D, "Challenge identification for network resilience", Next Generation Internet(NGI), 2010 6th EURO-NF Conference on, pp.1-8, 2010
[25] Liberty Alliance. Liberty ID-FF bindings and profiles specification v1.2, 2003.
[26] Microsoft Corp. Microsoft.NET passport review guide, <http://www.passport.net>.
[27] Pfitzmann B and Waidner M, "Analysis of liberty single-sign-on with enabled clients," Internet Computing, IEEE, Vol.7, Issue:6, pp.38-44, 2003.
[28] Liberty Alliance. Liberty trust models guidelines v1.0, 2003.
[29] IDC, Worldwide Identity Theft Black Market 2006-2010 Forecast, 2006.
[30} Liberty Alliance Project, http://www.projectliberty.org/
[31] Microsoft, Introducing Windows CardSpace, http://msdn.microsoft.com/
[32] OpenID, http://openid.net/
[33] Security Assertion Markup Language(SAML) OASIS Standard Specification, Version 2.0, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[34] Higgins Project, http://www.eclipse.org/higgins/

박 인 신

e-mail : shinpd@gmail.com
2001년 명지대학교 산업공학과(공학사)
2006년 (주)네오플 연구소 책임연구원
게임보안팀장
2009년 성균관대학교 정보보호학과
석사과정
관심분야 : 게임해킹대응, 정보보호, 모바일 APP보안, 모바일 네트워크 보안 등

정 종 필

e-mail : jpjeong@ece.skku.ac.kr
1997년 성균관대학교(공학사)
2003년 성균관대학교 정보통신공학부
(공학석사)
2008년 성균관대학교 정보통신공학부
(공학박사)
관심분야 : Mobility Management, Proxy Mobile IPv6, IEEE 802.16e, Seamless Handover, IPTV, NGN, Home Networking IMS, Networking, IMS, Network Security