Computer Security and Electronic Payment System

Final Report : cores

Team members : 강희영 2001003
기준백 2001009
김범주 2001020
정대민 2001115

< 목 차 >

1. Abstracts

최근 인터넷의 이용이 폭발적으로 증가되면서 언제, 어디서나 쉽게 인터넷을 이용할 수 있는 방법들이 많이 제시되고 있다. 그 중에서도 모바일폰을 이용한 인터넷의 활용이 크게 주목을 받고 있다. M-커머스는 사용자들의 편리함을 추구하고 삶의 질을 향상시킬 수 있다. 하지만 무선 인터넷을 활용하는 이른바 M-커머스가 보다 확산되기 위해서는 핵심 문제의 하나인 대금 결제와 관련한 보안 문제가 해결되어야만 할 것이다.

유·무선을 막론하고 프라이버시와 기밀성(confidentiality)은 점점 중요한 이슈가 되어 가고 있다. 보안 문제의 핵심은 암호화 이다. 암호화는 보내고자 하는 메시지에 프라이버시와 무결성(integrity)를 제공해 준다. 그러나 만약 암호화가 충분히 강력하고 어떠한 단말기에서도 유용한 상태라 할 지라도 이 것이 범죄자의 손에 의해 악용되었을 때 공공의 안전은 심각한 위험에 처할 수 있는 것이다.

우리 팀은 지난 기간의 발표를 통해서, m-커머스 상의 문제와 여러가지 보안관련 취약점들을 찾아 보았고, 그것에 대한 대안을 찾고자 하였다. 이미 살펴본 바와 같이, 현재 무선 단말기의 낮은 전원, 제한된 컴퓨팅 파워 등을 고려해 볼 때 비대칭키 암호 알고리즘은 그리 좋은 방법이 아닐 수 있다. 비록 WPKI 와 같은 모바일 단말기용 프로토콜이 제안되고 있지만 그 부담은 모바일 단말기에서 쉽게 해결할 수 있을 것으로 보이지 않는다.

아마도 대안은 전통적인 대칭키 암호 알고리즘이 되지 않을까 생각한다. 여러 논문과 제안을 분석한 결과 End-to-end 보안과 non-repudiation 이라는 기능을 제공할 수 있는 Session Key Sharing 방식'이 가능한 대안이 되지 않을까 생각한다.

이 글은 먼저 모바일 e커머스의 정의로 시작한다. 유무선 인터넷의 내용을 살펴본 후 다음으로 무선망을 통한 인터넷 접근의 대표적 표준 규약인 WAP의 전체적인 개요에 대해서 살펴 본고 모바일 e 커머스와 관련된 문제점들을 살펴 본 뒤 대안을 제시하고 국내 기업에서 실제로 어떤 식으로 적용되는지 알아 보고자 한다.

또한 이는 기존의 layer stack 을 건드리지 않는 application layer 계층에서 동작하는 모델이 될 것이다. S사의 사례와 상세한 프로토콜을 그 예로 들었다.

2. Introduction

최근 들어 모바일 인터넷에 대한 관심이 폭증하고 있다. 물론 아직까지는 구체적인 수익모델이나 이렇다 할 매력적인 서비스를 제공하고 있진 못하다. 하지만 그 적용범위가 조금씩 확대되고 있으며, 앞으로는 무선 인터넷이 유선 인터넷보다 인기가 있고 크게 유행되리라 생각된다. 그 근거로는 전세계적으로 가정이나 사무실에 있는 전화의 회선 수가 10 억 개에 달할 때 까지는 장장 1 백년 이상 걸렸다. 이에 비해 휴대 전화 대수는 불과 10 년 만에 3 억대를 넘어선 점을 보면 짐작할 수 있다.

오늘날 지하철이나 버스에서 양손으로 휴대폰을 부여잡고 뭔가에 열중하는 10대들의 모습은 이제 낯설지 않다. 이들 사이에서 거론되는 「몇 백 타」는 일반 데스크 톱 PC 자판에서의 속도를 의미하지 않는다. 양 엄지 손가락의 움직임이 눈에 보이지 않을 정도로 빠름도 당연하다. 채팅에 한창이라고 생각하기 쉽지만 자세히 보면 이들 중 적지 않은 수는 채팅이 아닌 게임에 열중하고 있음을 알 수 있다. 유료게임을 다운로드 받아 혼자 게임에 몰두하고 있는 것이다. 한동안 「달리는 채팅」 문화가 지배했던 10대들의 무선인터넷 서비스 틈새로 모바일커머스(M커머스)는 이처럼 소리없이 번지고 있다. 10대들이 이용하는 M커머스의 주종이 게임이라면 20 30대에게는 단연 예매 서비스가 인기 종목이다. 휴대폰을 이용해 항공권이나 콘도 또는 공연 티켓을 예매하는 서비스는 이제 일반화돼있다. 국내 한 인터넷 전문 쇼핑몰은 티켓예매 사이트에서 올리는 수익의 비중이 전체 쇼핑몰에서 절반 이상을 차지할 정도다. 이처럼 커뮤니케이션에서 시작된 휴대폰의 기능은 점차 「거래 수단」으로 변하고 있다. 단순히 이동 중 전화통화를 할 수 있는 통신수단의 기능으로 시작된 휴대폰이 이제는 상거래를 발생시키는 주요 인프라로 탈바꿈하고 있다.

2.1 모바일 e커머스의 정의

모바일 e 커머스란 Mobile Commerce 의 약자로 전자상거래의 일종. 가정이나 사무실에서 유선으로 인터넷에 연결,물건을 사고 파는 것과 달리 이동 중에 이동전화기나 무선인터넷정보단말기 등을 이용해 거래를 하는 것을 말한다. 이 때 이동전화기는 인터넷사이트를 검색할 수 있는 웹브라우저를 내장하고 있어야 한다.

'카드 가맹점 조회기의 선이 사라진다" 레스토랑에서 식사를 마친 후 손님은 계산을 위해 카운터로 갈 필요가 없다. 웨이터가 들고 온 무선카드 결제기를 이용해 앉은 자리에서 곧바로 요금을 계산하면 된다. 음식배달을 주문한 후

배달원이 휴대한 무선카드결제기로 현장에서 카드결제도 가능하다. 최근 들어서는 택시에 무선카드 결제기를 부착해 운행요금을 카드로 받는 사례도 늘어나고 있다. 카드결제가 가능한 포장마차도 등장해 손님들의 호응을 얻고 있다. 이처럼 설치장소나 환경에 구애 받지 않고 언제 어디서나 간편하게 카드요금을 결제할 수 있는 무선 신용카드결제서비스가 인기이다.

최근 인터넷의 이용이 폭발적으로 증가되면서 언제, 어디서나 쉽게 인터넷을 이용할 수 있는 방법들이 많이 제시되고 있으며, 모바일 폰을 이용한 인터넷의 활용이 크게 주목을 받고 있다. 이를 '모빌 인터넷 서비스'라고 하며, 사용자가 임의의 장소로 이동하면서도 무선이동통신 서비스망에 접속하여 인터넷 서비스를 받는 것으로 모빌인터넷의 응용 범위는 무수히 많다. 달리는 차 속이나 여행지에서, 상담 중에 어디에서든지 인터넷을 사용할 수 있는 방법이 개발되고 있는데, 즉 디지탈 모바일 폰에 노트북 컴퓨터를 연결하여 세계 각지와 인터넷의 E-Mail 을 주고 받고, 웹서핑을 즐기며, 신속히 정보를 교환할 수 있는 방법들이 구체적으로 실용화되어 일반 사람들도 쉽게 사용할 수가 있게 되었다.

우리가 흔히 사용하는 모바일 폰으로 전화를 주고 받는 것 이외에 인터넷에 접속하여 비즈니스의 효율을 극대화하고, 멀티미디어의 효율성을 찾는다면 대단히 획기적으로 비즈니스는 물론 일상 생활에서도 크게 도움될 것이다. 특히 모바일 폰을 이용한 무선인터넷은 개인용 컴퓨터에서의 인터넷과는 전혀 다른 특성을 가진다. 무엇보다도 모바일 폰은 언제나 켜져 있다. 그리고 항상 이용자의 호주머니 속에 들어 있다. 모바일 폰은 철저히 개인용이며 값비싼 컴퓨터에 비해 쉽게 구입할 수 있다. 이런 특성들을 바탕으로 만들어 낼 수 있는 새로운 서비스는 그 다양성의 끝을 알 수 없을 정도이다.

하지만 무선 인터넷이 성장하기 위해서는 몇 가지 넘어야 할 문제점들이 있다. 모바일 인터넷에 대한 장애는 기술적인 제약 때문에 생각보다는 더뎌질 것이라고 전망했는데, 이는 전체적인 새로운 모바일 네트워크를 구축하기 위해 투자되는 대규모의 자금투자가 불확실하며 현재 모바일에 대한 표준화 작업도 미비하기 때문이다. 보다 중요한 것은 M-커머스가 점차 확산되고 있기는 하나 핵심인 대금결제와 관련한 보안 문제가 아직 최대 장애가 되고있다. 무선망을 통한 인터넷 접근의 대표적 표준 규약인 WAP 의 경우에도 그 예외는 아니다.

2.2 무선 인터넷

WAP(Wireless Application Protocol)에 대해 알아보기 전에 우선, 무선 인터넷에 대한 이해가 필요하므로 무선 인터넷의 전반적인 이해로부터 시작해보자.

더 이상 설명할 필요가 없을 만큼 우리의 일상생활 속으로 깊이 들어와 있는 인터넷을 둘로 나눈다면 케이블과 같이 눈에 보이는 고정된 선을 사용하는 유선 인터넷과, 같은 인터넷을 무선 휴대폰과 같은 이동통신 공중망을 이용하는 무선 인터넷으로 나눌 수 있다.

무선 인터넷은 사실 인터넷을 활용하는 사용자 입장에서 보면 유선 인터넷과 별다른 차이가 없을지도 모른다. 하지만 이를 개발하는 사람의 입장에서 보면 그렇지가 않다. 그렇다면 우선 무선 인터넷에 대해 바르게 이해 하는 것이 중요하다.

2.3 유선 인터넷과 무선 인터넷의 차이점

	유선 인터넷	무선 인터넷
전송속도	56K ~ Mbps	14.4Kbps ~ 64Kbps
화면	640*480 Pixels 이상	4*16chars(일반 폰) 8*16chars(스마트 폰)
인터페이스	키보드, 마우스 등 다양한입출력 장치	액정화면 소프트버튼 등
휴대성	불가	가능
통신 에러율	낮음	높음
프로토콜	TCP/IP	TCP/IP, WAP
컨텐츠 형태	HTML	HTML, WML,WMLScript cHTML, sHTM

2.4 무선 인터넷의 발전

이동통신망은 기술에 따라 초기 1세대에 아날로그 셀룰러 이동 전화 시스템으로 FDMA(Frequency Division Multiple Access)전송기술을 이용하는 AMPS(Advanced Mobile Phone Service)망을 이용한 셀룰러 방식의 디지털 이동 통신 네트워크 CDPD(Cellular Digital Packet Data)에서 발전하여 현재의 2세대인IS-95/GSM(Global System for Mobile Communication)을 거쳐 앞으로 3세대인 IMT-2000으로 발전 중에 있다

현재 2세대 이동통신망 기반으로 WAP, ME, i-mode 등의 무선응용 프로토콜을 사용하여 무선인터넷 서비스를 제공 중에 있다

최종적으로는 무선인터넷은 차세대 이동통신망인 All-IP 망을 기반으로 전개될 전망이다

2.5 무선 인터넷의 제한 사항

?? **전송용량 및 속도에 제한**

무선 이동통신이 사용하고 있는 망의 대역폭(Bandwidth)이 유선에 비해 상대적으로 낮으며 한번에 전송할 수 있는 데이터의 양도 그만큼 적어 전체적인 전송속도를 저하시키고 있다.
향후 IMT-2000 을 기반으로 하는 초고속 무선망을 사용하여 무선 인터넷 사용의 전송 속도에 대한 단점은 해결될 것으로 예상하고 있다.

?? **단말기 화면크기의 제한**

인터넷 환경을 그대로 접목하기에는 적은 크기의 LCD 화면을 가진 단말기는 무리가 있다.

?? **비효율적이 무선망으로 인한 비용의 부담**

현재의 음성 위주의 무선망 시스템은 회선 방식으로 운용되고 있는데 이를 이용하는 것은 효율적인 면에서 많은 비용이 소요되며 이때 발생하는 비용의 부담은 곧 사용자의 사용 요금 부담으로 이어지고 있는데 이의 해결을 위해서 현재의 회선 방식의 무선망을 새로운 패킷 방식의 시스템을 사용하는 데이터 트래픽 중심의 시스템으로 진화시키는 노력이 요구되고 있다.

3. 보안과 WAP Security

WAP 의 보안과 관련한 여러 기술들은 기존의 유선인터넷 상에서 사용되는 보안 관련 기술을 최대한 활용하는 것을 기본 원칙으로 하였다. 그러나, 이러한 기존 유선 인터넷상의 보안 기술의 적용에도 불구하고, WAP 은 WAP Gateway 의 존재로 인하여 기존의 유선 인터넷에서 제공되는 보안에 비해 제한적인 범위에서만 보안을 보장한다. 앞으로 보안의 역할과 보안의 기본요소 들에 대한 전반적인 내용을 설명하고자 한다.

3.1 보안의 역할

보안은 크게 두 가지 측면의 역할을 수행한다고 볼 수 있다. 한편으로는 **사용자로 하여금 허가되지 않은 작업은 못하게 하는(Disabling Technology) 관점**에서, 다른 한편으로는 **사용자로 하여금 안전하게 작업을 수행할 수 있게 하는(Enabling Technology) 두 가지 관점**의 역할을 수행하는 것이다. Disabling Technology 관점의 보안은 외부자 침입 등의 방지를 들 수 있을 것이고, Enabling Technology 관점의 보안은 적법한 사용자 여부를 파악하는 인증 등을 생각할 수 있다.

3.2 보안 - 전자상거래의 성공을 위한 전제 조건

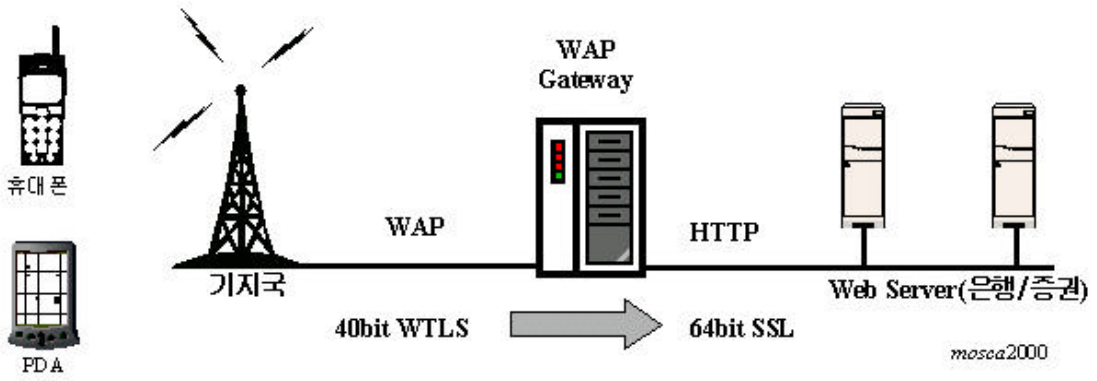
최근 인터넷이 각광 받으면서 전자 상거래가 수많은 .com 들의 초미의 관심사로 떠오르고 있다. 인터넷 기업들의 수익의 원천으로서 전자상거래는 핵심적인 issue 일 것이다. 이러한 전자상거래 성공의 전제조건은 보안이다. 직접 상점에 가서 Credit Card 와 신분증을 꺼내 본인임을 확인하고 신용카드 전표에 사인하는 등의 작업들이 전자상거래에서도 필요한 것이다. PC 나 무선단말기 상의 browser 를 통해서 이루어지는 E-Commerce 와 M-Commerce 의 성공을 가능케 하기 위해서는 보안은 필수 불가결한 요소이다.

3.3 보안의 기본요소

Authentication	사용자의 진위를 파악하는 인증 작업이다. Unix machine 이나 NT 에서의 로그인 과정이 기본적인 authentication 의 한 예이다.
Confidentiality	정보의 내용을 허가 받지 않은 자는 이해하지 못하도록 변환하는 것을 일컫는다. Confidentiality 는 암호화(Encryption)를 통해 주로 달성된다고 볼 수 있다.
Integrity	정보의 내용이 변형되어지거나 위조되지 못하도록 하는 것을 일컫는다. 정보의 내용을 토대로 추출되는 Hash 값(Hash Function 을 이용하여 추출)을 가지고 정보의 임의 수정 여부를 판단한다.
Authorization	사용자가 특정작업에 대해 권한을 가지고 있는지를 결정하는 과정을 일컫는다. Unix machine 에 로그인한 사용자가 특정 파일에 대해서 가질 수 있는 권한은 사용자에 따라 읽기, 쓰기 등의 다양한 권한을 가질 수 있다. 예를 들어 은행계좌로부터 출금할 권한이 있는지 여부를 결정하는 일등이 이에 속한다.

3.4 WAP 에서의 보안-유선인터넷과의 차이점과 한계

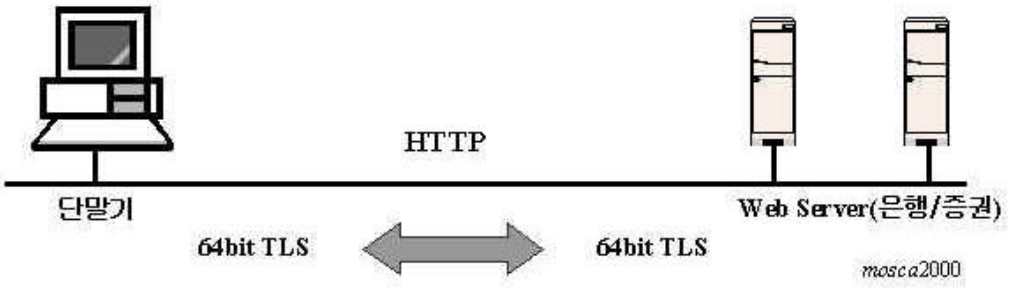
유선 인터넷 상에서는 64bit SSL(Secure Socket Layer)를 사용하여 암호화를 한다. 무선 인터넷에서도 이와 같은 보안 알고리즘으로 40 bit WTLS(Wireless Transport Layer Security)가 표준화되어 있다. 현재의 무선인터넷 구조는 다음 그림과 같이 되어 있다.



그림에서 보는 바와 같이 WAP G/W 는 무선구간의 WTLS 와 유선 구간의 SSL(TLS)를 연결해 주기 위해서 사용자로부터 전달된 데이터(이 데이터는 Binary data 로 구성되어 있다)를 해독하고(WAP G/W 는 사용자로부터 전달된 데이터를 "해독"할 수 있는 구조상의 위치를 차지하고 있다는 것에 주목하자.) 다시 SSL 로 암호화하여 Web server 로 전달하게 된다. Web server 에서 사용자에게 전달되는 데이터도 마찬가지 과정을 거친다. WAP G/W 가 암호화된 데이터를 자유자재로 복호화하고 다시 암호화하는 과정에서 무선인터넷의 End-To-End 보안의 허점이 발생하는 것이다. WAP G/W 를 운영하는 자(일반적으로 이동통신업자일 것이다)를 신뢰할 수 있다라는 전제가 있다면 End-To-End 보안이 성립된다고 볼 수 있는 것이다. 따라서 End User 쌍방간의 진정한 의미의 완벽한 보안이 제공되지 못하는 것이다.

4. 유선 인터넷 보안과 무선 인터넷 보안

4.1 유선인터넷 보안



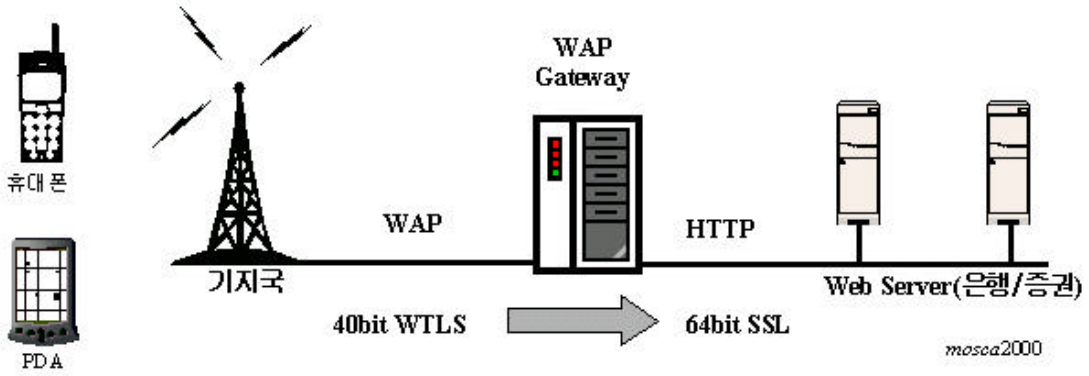
위의 그림에서 보는 바와 같이 유선인터넷에서 보안은 사실상의 표준으로 자리잡은 Transport Layer Security(TLS) Protocol 을 사용하여 이루어 진다. Public key 와 Private key 를 이용한 Key Exchange 기법을 이용하여 Client 와 Server 쌍방이 Session key 를 안전하게 공유한 다음, Client 와 Server 간 모든 데이터 전송은 공유된 Session key 를 이용하여 암호화/복호화되는 것이다. End To End 보안이 보장되어 완벽한 보안이 제공될 수 있다.

위와 같이 TLS 를 이용, 사용자와 서버 양쪽을 연결해주는 유선인터넷은 다음의 보안요소 들을 충족시킨다. 우선, 로그인 과정을 통해 사용자의 당사자 여부를 판단하는 Authentication 이 보장 받게 되며, Session key 를 알지 못하는 제 3 자는 Client 나 Server 에서 암호화된 데이터의 내용을 알 수 없으므로 Confidentiality 가

보장이 된다. Client 에서 암호화된 데이터는 Server 에 도착하는 동안 누군가에 의해 가로채어 질 수 있지만 데이터를 임의로 변화시키게 되면 데이터의 Hash 값이 변하게 되므로 Integrity 가 보장된다. 인증을 받은 특정 사용자에 대해 적절한 권한 부여를 하여 Authorization 을 최종적으로 수행한다.

4.2 무선인터넷 보안

무선인터넷에서의 보안은 아래 그림에서 보는 바와 같은 구조를 갖는다. 무선구간에서는 WTLS 를 이용하여, 유선구간에서는 기존 유선인터넷의 TLS(SSL)를 그대로 적용하여 유선, 무선 각각에서 보안을 달성할 수 있도록 구성되어 있다.



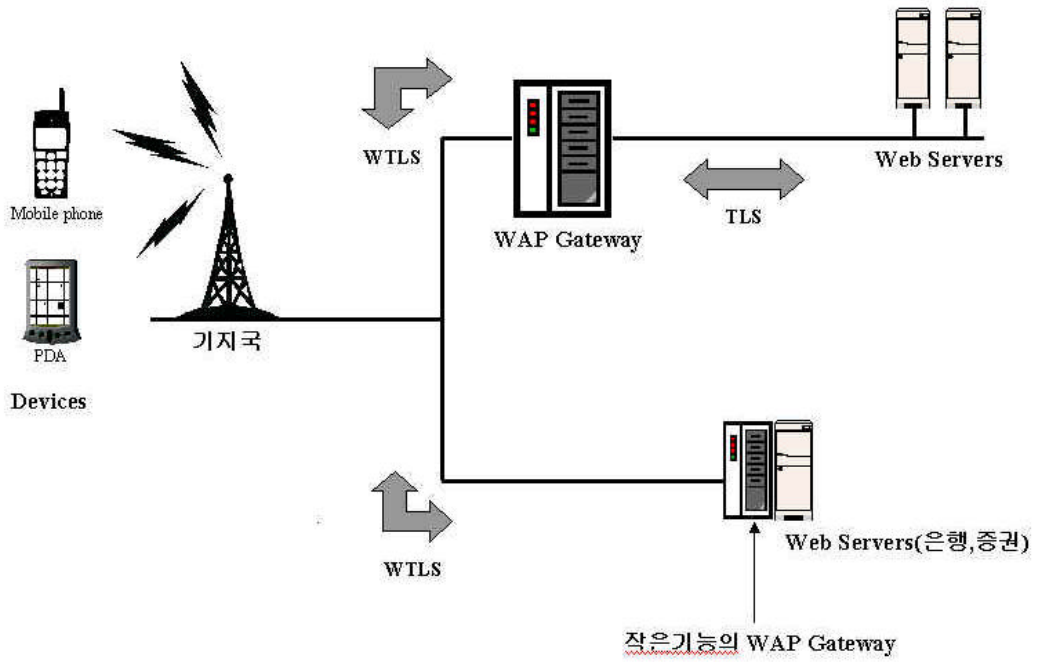
하지만, 무선 인터넷 보안에서의 문제점은 유무선 각 구간별 보안에서 발생하는 것이 아니라, 안전한 유무선 구간 쌍방을 연결하는 WAP G/W 에서 발생할 수 있다. WAP G/W 는 무선 구간의 WTLS 와 유선 구간의 TLS 를 연결해 주기 위해서 사용자로부터 전달된 데이터를 해독하고 다시 암호화하여 Web Server 로 전달하며, 반대로 Web Server 로부터 전달된 데이터를 해독하고 이를 다시 암호화하여 사용자에게 전달한다. 이 과정에서 WAP G/W 는 사용자와 서버간 전달되는 데이터의 모든 내용을 해독하므로 보안의 허점이 발생할 수 있는 것이다. 물론 통신사업자가 WAP G/W 의 대부분을 운영하는 현 상황에서 통신사업자를 어느 정도는 신뢰할 수 있지만 Business 에 따라서는 이러한 "어느 정도의 신뢰"도 사업상 큰 risk 로 작용할 수 있다. 따라서 Wireless Internet 에서는 "어느 정도 신뢰 있는 보안"을 제공하되 Wired Internet 과 같은 완벽한 End To End 보안은 제공하지 못하는 것이다.

(※ WAP G/W 는 유선인터넷의 Proxy server 와 시스템구조 상의 위치는 유사하지만, 유선인터넷의 Proxy server 와 동일한 기능을 한다고 생각해서는 안된다. 유선인터넷 상에서의 Proxy server 는 WAP G/W 와 달리 데이터를 복호화하는

기능이 없으므로 암호화된 데이터의 내용을 알 수가 없다. 따라서 유선인터넷 상에서는 무선인터넷 상에서 발생하는 보안문제가 발생하지 않는 것이다.)

5. 무선인터넷에서의 보안문제 해결방안

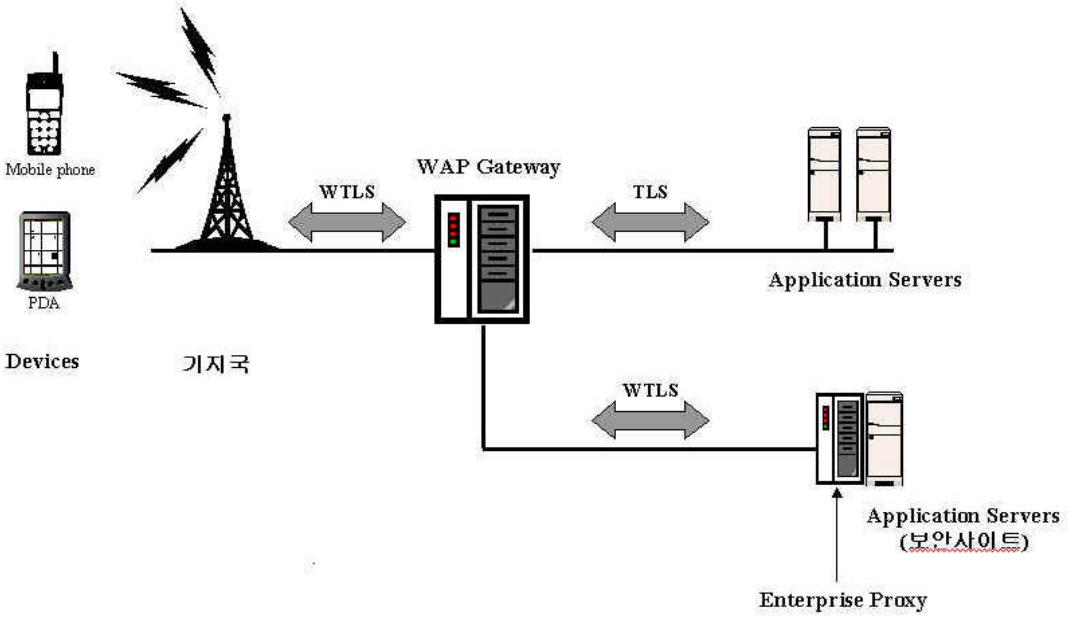
5.1 WAP G/W 를 거치지 않는 방법



위 그림과 같이 단말기에서 은행이나 증권사 같은 보안에 대한 요구가 많은 사이트를 접속할 경우에는 WAP G/W 의 IP address 대신에 보안 사이트의 Web Server IP address 를 입력하여 직접 접속하는 방법이 있다. 위 그림에서는 WAP G/W 를 거치지 않기 때문에, WTLS/TLS 의 변환 과정이 필요가 없고 암호화된 데이터를 중간에서 WAP G/W 에서 처리하지 않기 때문에 데이터의 암호화를 보장할 수 있다. 단, 위 그림에서 보는 바와 마찬가지로 웹 서버에서는 단말기로부터 전송된 Binary 데이터를 변환하여 이를 처리할 수 있는 능력을 가지고 있어야 한다(작은 기능의 WAP G/W 기능을 가지는 Web server). 기지국에서 Web server 로, Web server 에서 기지국으로 가는 데이터는 Binary 데이터이기 때문이다. 이러한 방법의 최대 단점은 사용자가 사용하기 어렵다는 점이다. 즉, 사용자는 보안 사이트를 접속하고자 할 경우에는 항상 IP address 를 바꾸어

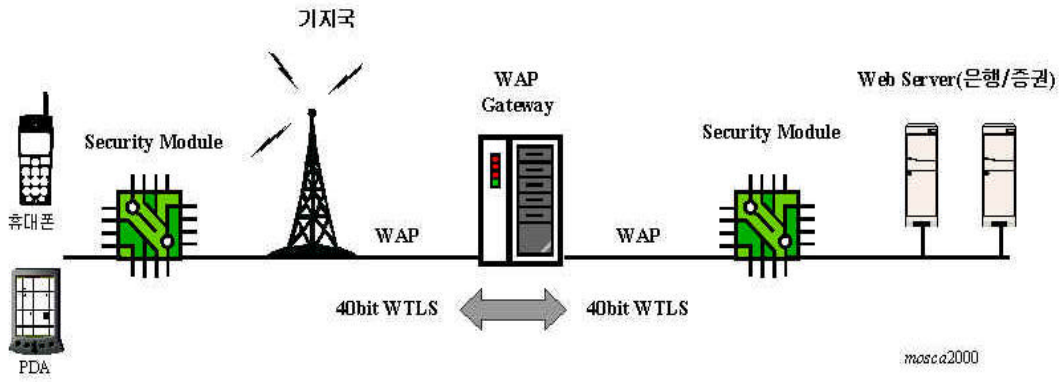
입력해야 한다. 또한 현재 국내의 WAP 단말기는 Browser 에서 접속하는 WAP G/W 의 IP address 를 사용자가 입력하지 못하도록 설정되어 있기 때문에 국내 통신 환경상으로도 비현실적인 방법이다.

5.2 보안 데이터에 대한 Bypass 기능을 이용하는 방법



1 번에서 설명한 단말기에서 IP address 입력에 의한 사용자 서비스 불편을 없애기 위한 방법으로 위 그림과 같은 방법이 사용될 수도 있다. 위 그림에서는 보안 사이트에 대한 데이터일 경우에 WAP G/W 에서 이 데이터를 Bypass 하는 방법이다. 각 보안 사이트의 Web server 앞에는 Enterprise Proxy server 가 위치하여 Bypass 된 데이터를 처리하는 역할을 한다. 이 경우에는 기존의 사용자들의 단말기를 변경하지 않고도 완벽하게 End-to-End Security 를 지원할 수 있는 장점이 있다. 현재 이와 같은 방법으로 Phone.com을 비롯한 많은 WAP G/W 개발 업체들이 무선 인터넷의 보안 문제를 해결하는 solution 을 제시하고 있다. 그러나, WAP G/W 에 연결된 보안 사이트마다 설치해야 하는 Enterprise Proxy Server 의 비용이 문제가 된다. 이러한 비용을 이동통신사가 떠 안아야 하는 것인지, 각 보안사이트를 운영하는 contents 업체가 떠 안아야 하는 지도 매우 민감한 문제이다. 즉 기술적으로는 완벽한 솔루션이 될 수 있으나 비즈니스적인 측면에서 많은 비용문제가 가장 큰 걸림돌이 된다.

5.3 특정한 데이터 Type 을 이용하는 방법



이 방법에서는 무선 인터넷 사이트를 일반 사이트와 보안 사이트로 구분하지 않는다. 따라서 보안 사이트의 웹 서버는 일반 사이트 웹 서버와 마찬가지로 동작한다. 다만, 일반 사이트와는 달리 보안 사이트에서는 암호화하고자 하는 데이터를 단말기와 미리 약속된 방법으로 암호화하고 전송한다. 마찬가지로 단말기에서는 암호화된 데이터를 미리 약속된 방법으로 이를 처리할 수 있다. 단말기에서 웹 서버로 전송하는 데이터의 경우도 마찬가지로 처리한다. 이러한 미리 약속된 방법을 처리하는 기능을 제공하는 Security 모듈을 단말기와 Web server 에 설치하여 이러한 기능을 구현할 수 있다. 단말기와 보안 사이트 간의 미리 약속된 방법을 사용하는 예로 mimetype 을 이용한 방법을 들 수 있다. 무선단말기에는 특정 mimetype 을 처리할 수 있는 Security 모듈이 내장되며 Web server 에서도 동일한 기능을 가지는 모듈을 이용하여 End-To-End 보안 문제를 해결할 수 있다.

6. 우리의 제안 ? 개선된 symmetric key 를 이용한 종단간 보안

무선 기술의 성장과 더불어 다양한 애플리케이션과 서비스가 시장에 전개되고 있다. E-commerce 가 무선 시장에서 빠르게 성장함에 따라 종단간 보안(end-to-end security)이 필수적인 것이 되었다. 그러나 GSM, WAP 중 어느 것도 end-user 간의 보안을 보장하고 있지 않다. 구체적으로 휴대폰과 기지국 사이를 오가는 [1]메시지들은 안전하다고 얘기할 수도 있지만 (꼭 그렇지만은 않다.), 유선 네트워크를 오가는 메시지들은 완전히 노출이 되어 있는 셈이다. 따라서 향후 더 많은 숫자의 무선 통신 가입자들이 좀더 사적이고 상업적인 정보들을 무선 네트워크에 흘려넣게 되면 무선통신 사업자들이 이런 정보들을 손쉽게 획득할 위험이 있는 것이다.

6.1 E-commerce requirement

전자상거래는 많은 비즈니스에서 전통적인 구매 행위를 변화시키는데, 전자상거래는 다음과 같은 보안성을 요구한다. (1) 메시지 전송의 프라이버시 (2) 메시지 전송 중 종단간 보안(end-to-end security)의 기밀성과 무결성 (3) 부인방지 서비스 (non-repudiation service) 등이 그것이다.

무선 네트워크는 많은 편리함을 제공하긴 하지만 무선이 원래 신뢰도가 떨어지는 매체이기 때문에 새로운 문제들이 끊임 없이 발생한다. 누군가가 공중을 오가는 메시지는 몰래 청취할 수도 있는 것이다. 만약 이 취약한 매체에 뭔가 적절한 보안대책이 가해지지 않는다면 누군가가 접근하여 메시지의 무결성에 흠집을 낼 수도 있는 것이다.

보안을 위해서 암호화 기법(encryption)이 사용되어 진다. 근데 강력한 암호화 기법은 칼의 양면성과 같은 성격이 있다. 개인정보를 보호한다는 면에서는 좋으나 만약 이 철저한 보안성이 범죄자에 의해 이용된다면 수사 당국도 이를 추적할 수 없는 어려움도 있다. 이를 피하기 위해 법원에서 승인한 감청이 가능한 형태의 보안이어야 할 것이다.

6.2 Current wireless network approach

GSM 의 경우는 SIM card(Subscriber Identity Module) 을 사용하여 휴대폰 복제 문제를 해결하고 안전한 전송을 위하여 몇가지의 암호 키들을 이용한다. SIM 카드에 저장되어 있는 비밀키는 매 세션마다 다른 형태의 알고리즘을 가진 암호키를 생성해 낸다. 그러나 GSM 시스템도 종단간 보안을 제공하지는 않는다. 단말기

[1] 작년 국정감사 때도 제기된 문제지만 현재의 감청 기술로 충분히 휴대폰 단말기와 기지국 사이를 오가는 암호화된 정보도 풀어낼 수 있다고 알려져 있다. 검찰도 cdma 타입의 휴대폰 통신을 감청할 수 있는 장비를 가지고 있는 것으로 보도되고 있으며 군 당국도 성남 근처의 정보부대에서 이러한 장비들로서 감청을 행하고 있다고 보도된 바 있다.

와 기지국 사이를 오가는 메시지는 안전하다고 말할 수 있으나 유선 네트워크를 오가는 메시지는 결코 안전하지 않은 것이다.

음성 서비스외에 부가서비스나 애플리케이션들도 급격하게 오늘날 성장하고있다. WAP(Wireless Application Protocol)은 실시간 정보나 인터넷 검색을 위한 플랫폼을 제공한다. WAP 에서 보안 서비스를 제공하는 것은 STK(SIM Toolkit)과 WTLS(Wireless Transport Layer Security) 이다. STK 는 특히 가입자와 은행가의 종단간 보안을 제공하나, 이런 경우 가입자는 미리 지정된 하나의 은행만 이용이 가능하다.

WTLS는 WAP application 에서 메시지 전송을 위한 대안책을 제시한다. WTLS는 인터넷 환경에서 사용되어 지는 SSL(Secure Socket Layer)와 TLS(Transport Layer Security)에 근간을 두고 있다. 그러나 이도 종단간 보안이라 할 수 없는 "가입자-WAP gateway "간 보안 수준만을 제공하고 있다.

6.3 End to end secure protocol for digital mobile users

위에서 살펴봤듯이 실제로 종단간 보안을 제시하는 모델은 없다. 따라서 여기서 제시되는 것은 단말기의 제한된 컴퓨팅 파워를 고려한 대칭키를 사용한 모델이다. 이로써 우리는 종단간 보안과 부인 방지라는 보안 서비스를 제공할 수 있다.

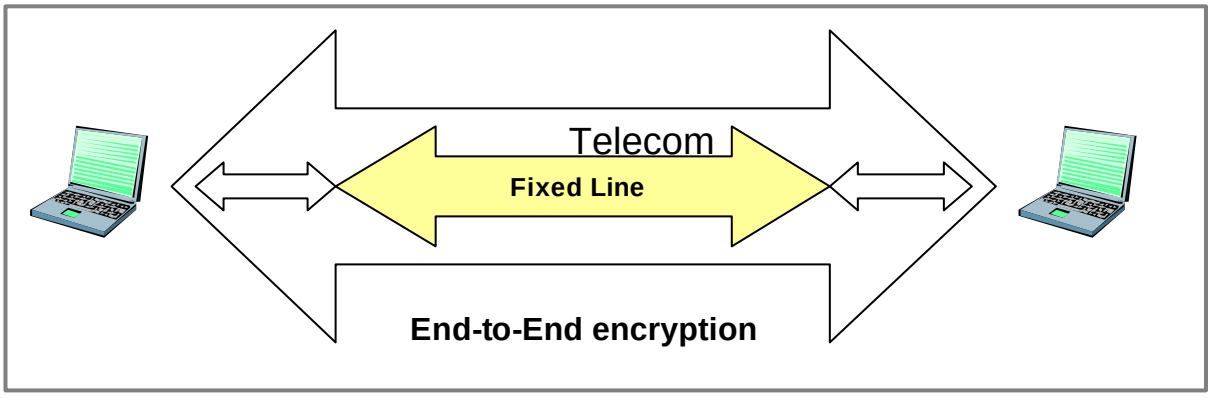


Figure 1.1 End-to-end security for improved wireless communications

휴대폰을 위한 무선 네트워크는 어디서나 정보를 전달하고 교환할 목적으로 확장되어져 왔다. 그러나 이 무선 네트워크는 현재 프라이버시나 공공의 안전을 보장해 주지 못한다. 좀 더 구체적으로 말해서는 종단간 보안이나 부인 방지 서비스를 제공해 주지 못하는 것이다. 종단간 보안은 특히 전자상거래가 활성화 되기 위해서는 꼭 갖춰져야 될 것 중 하나다.

최근의 무선 네트워크에서 데이터들은 physical link 계층에 놓여지기 전에 암호화

된다. 네트워크 운영자들은 링크를 공유하고 유니크한 키를 공유한다. 암호화는 라디오 링크를 통해서 메시지를 보호한다. 그러나 메시지는 네트워크 운영자들에게는 항상 노출되어 있는 것이다.

조금 개선된 휴대폰 기반의 무선 통신 시스템의 도해를 보자. 그림 2는 보안측면에서 강화된 휴대폰 무선 네트웤을 보여준다.

육각형은 하나의 셀을 나타내며 이 셀의 집합들은 local area 라고 부른다. (sub-domain)으로 분류되어 지기도 한다. 이 sub-domain 은 MCC(Mobile Control Center) 에 의해 컨트롤 되어진다. 각각의 MCC 는 [2] VLR(Visitor Location Register)를 가진다. VLR 은 네트워크 내에서 이동 중에 있는 MS(Mobile Station : 단말기) 에 대한 임시 정보를 저장한다. Mobile Station(MS) 는 고정적인 MS 에 대한 정보를 가지는 HLR(Home Location Register)에 연동되어져 있다. HLR 은 단말기가 이전 VLR에서 새로운 VLR 로 이동해 감에 다라 업데이트되는 위치 정보를 저장한다. AUC (Authentication center) 는 기밀 정보를 저장하는 보안이 유지되는 데이터 베이스다.

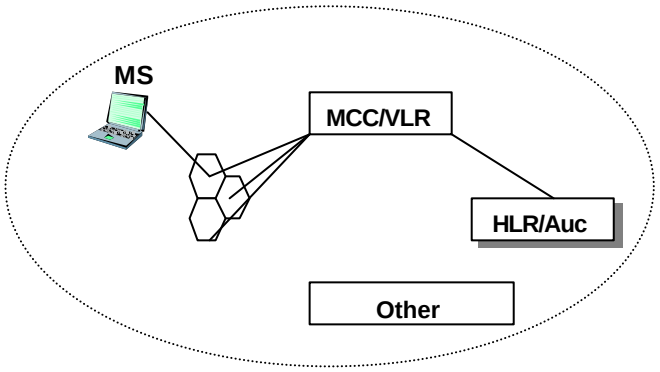


Figure 2 : Improved wireless network infrastructure

6.4 System architecture

PCS(Personal Communication Systems)는 여러 종류의 서비스와 정보를 어디서나 가능한 접속 서비스와 함께 제공한다. 가입자의 인증과 함께 이에 상응하는 보안 기능은 요구한 가입자에게 제공된다. 따라서 가입자를 인증하는 기능은 가입자가 네트워크에 접근하기 이전에 요구 되어진다.

Security service

✍✍ Availability

[2] VLR : foreign agent 와 같은 개념

- Confidentiality
- Integrity
- Non-repudiation
- Location privacy
- New countersign generation

6.5 End-to-end security on application layer using symmetric key system.

RSA 는 인기 있는 비대칭키 알고리즘이다. 이는 기본적으로 소인수 분해의 어려움에 기반을 두고 있다. 그러나 여러가지 active attack 으로부터 보호하기 위해서는 두 소수(prime)는 어느 크기 이상 (대략 1024bit) 의 집단에서 선택되어져야 한다. 현재 휴대폰의 여러 가지 제약 조건 상 비대칭키 암호를 사용해서 전송될 메시지를 암호화 하는 것은 적절치 않아 보인다.

현재 휴대폰의 컴퓨팅 파워를 고려해서 대칭키 암호를 좀 더 개량하는 쪽의 선택이 더 적절해 보인다. 이러한 대칭키 방식을 흔히 'Session Key Sharing(SKS) '방식이라고 부른다. SKS 알고리즘은 종단간 보안과 부인방지 서비스를 구현하는 데 효과적일 것이다. 그리고 이 알고리즘은 애플리케이션 레이어 층에서 구현되는 것이 바람직할 것이다.

6.6 Traditional session key generation

현재의 보안 기술은 커뮤니케이션에서 어느 정도의 신뢰도는 보장한다. Secure communication을 하기 이전에 양측에서는 사전에 secret session key를 공유한다. 확실한 통신상의 보안을 보장하기 위해 매 세션마다 새로운 세션키의 사용이 필요하다. 전통적인 방법에서는 세션키를 생성하기 위해서 두가지의 방법이 있다.

<Case1> : 세션키는 Key Distribution Center (KDC)에서 생성된다. 여기서의 가정은 통신 쌍방이 KDC와 같이 세션키를 공유한다는 점이다. A가 B와 대화하기 전에 반드시 세션키를 이용하여 데이터의 전송을 보호해야 한다. KDC는 secret key Ka, Kb를 이용하여 세션키의 분배하고 보호 한다.

<Case2> : 통신 쌍방은 통신전에 세션키를 협의한다.

Case1 의 경우에 A,B간의 통신 내용은 KDC를 통해서 복호화될 수 있다. 그러나 Case2의 경우에는 만일 불법적인 내용을 통신한다 하더라도, 아무도 그러한 범죄적 행위에 대하여 알아낼 수 없게 된다.

6.7 Improved session key generation

만일 암호화 방법이 범죄자들의 통신 장비에서 쉽게 사용된다고 하면, 공공의 안

전은 심각하게 위협을 받게 된다.

Mobile phone 장비의 computing capability와 위에서 언급한 결점을 고려하여 지금까지의 대칭형 키 암호화 방법을 개선하여 end-to-end 보안과 부인방지 기능을 모든 통신에 적용할 수 있다.

'Sharing session key component'이라는 알고리즘이 그것이다. 통신 쌍방은 통신전에 세션키를 결정한다. 불법적인 통신에 사용하는 것을 막기 위하여 여러 개의 Key Escrow Trust Organization(KETO)으로 키가 분배되고 만일 해당 통신이 불법의 여지가 있다면, 법원시스템(CS:Court System)에 의해 키가 복원된다. KETO는 신뢰할 수 있는 상대자이고, 세션키의 Sharing component를 관리하지만 세션키를 복원하는 것은 불가하다. 법원은 공공의 안녕을 위하는 목적일 경우에 KETO를 통해서 세션키의 Sharing components를 얻어 세션키의 복원할 수 있다.

'Sharing session key component'에서 특별한 디지털 서명을 제공한다. 일반적인 디지털 서명이 아니라 분쟁발생 해결이나, 공공 안전을 위해 중재할 수 있다.

'Sharing session key component'을 표현하기 위해 사용하는 표기법을 먼저 소개한다.

1. closekey : private component of session key, 디지털 서명을 위해 사용
2. openkey : public component of session key, 해당 closekey에 종속된다.
3. N : 시리얼 번호
4. KEY(openkey,closedkey) : 세션키를 만드는 함수,
   $KEY(openkey_B,closedkey_A) = KEY(OPENKEY_A,CLOSEDKEY_B)$
5. Ks : A,B 사이에 공유되는 세션키
   $KEY(openkey_B,closedkey_A) = Ks = KEY(OPENKEY_A,CLOSEDKEY_B)$
6. SecH() : 1way hash function
7. K[] : encryption using key K
8. Kc : a key generator by GSM

모든 통신망이 확립된후 통화 쌍방이 키 한쌍을 생성하는데 openkey, closedkey로 구성된다. 즉 통신을 위해 한시적으로 사용할 세션키 쌍을 만들어 낸다.
일반적으로 모든 통신 양방간의 데이터는 기본적으로 cellular wireless network(ex. GSM) 에서 제공하는 보안 기능을 이용한다. 즉 이동통신 네트워크는 차별화 된 암호키(Kc)를 사용하여 통신 내용을 보호한다. 만약 Alice 가 Bob과 통신한다고 할 때, Alice 가 보내는 메시지는 Kc_Alice에 의해 암호화 된다. 그러면 네트워크 관리자가 Kc_Alice로 복호화 하고 다시 그 메시지를 Kc_Bob으로 암호화 하여 Bob에게 보낸다.

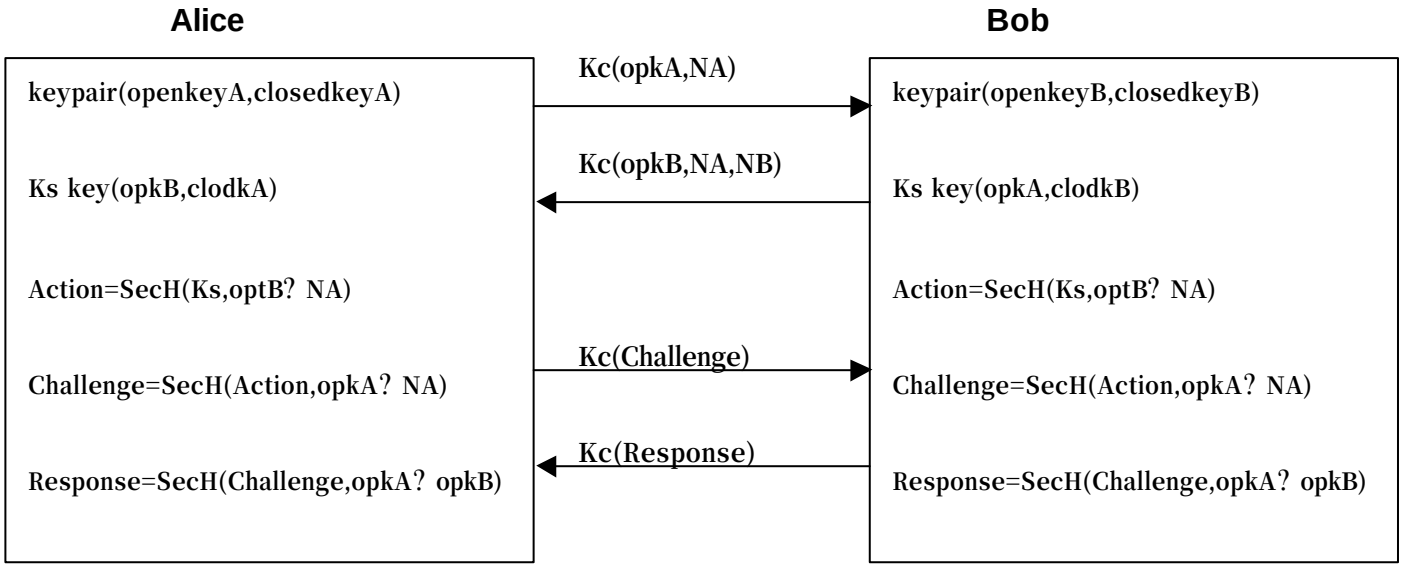


Figure 3 : Secure session key negotiated between Alice and Bob (? : exclusive OR)

Step1: Alice는 통신 기간동안 closedkeyA를 사용하고, Bob은 openkeyB를 만들어 통신기간동안 사용한다.

Step2: Alice는 openkeyA와 , N_A 를 Bob에게 보낸다.

Step3: Bob은 openkeyB와 , N_B 를 Alice에게 보낸다.

Step4: 세션키 생성 함수에 의해 Alice는 openkeyB, closedkeyA로 세션 Ks를 만든다. Bob도 openkeyA, closedkeyB를 가지고 Ks를 만든다.
즉 $KEY(openkey_B,closedkey_A) = Ks = KEY(OPENKEY_A,CLOSEDKEY_B)$ 이 된다.

Step5: Alice는 Action 즉, Ks, openkeyB? NA 를 해쉬한 값을 만들어 낸다. 그리고 Action, openkeyA? NA로 hasing한 challenge를 만든다.
Bob도 똑같이 action을 만든후에 challenge에 대한 Response를 Chanllenge, openkeyA? openkeyB를 hashing 하여 만들어 낸다.

Step6: Alice는 challenge를 Bob에게 전송한다. Bob은 Challenge_A를 자신의 Challenge와 비교한다.만일 결과가 같으면 세션키 Ks 교환과 negotiate가 성공한 것이다. Bob은 만든 Response를 Alice에게 보낸다.

Step7: Alice는 Response_B를 자신의 Response와 비교한다. 만일 결과가 같으면 세션키 Ks 교환과 negotiate가 성공한 것으로 안다.

6.8 Realize end-to-end confidentiality and non-repudiation service.

세션키 Ks가 negotiate되고 난 후에 양방은 자신의 private components를 여러 KETOs에 KETO의 secret key를 이용하여 분배한다. 이것은 기존의 대칭키 암호 기

법을 개선한 것일뿐 아니라, 모든 거래에 있어서 non-repudiation 서비스를 가능하게 하는 특별한 디지털 서명의 기능도 가능하다.

세션키 Ks에는 두개의 필수적인 요소가 있다. 하나는 공개된 openkey, 또 하나는 비공개되는 closedkey이다. 쌍방의 통신에서 모든 메시지는 송신자 또는 수신자의 colsedkey로 자동적으로 서명이 된다. 따라서 법원의 결정에 따라 디지털 서명된 내용은 논쟁이나 공공의 안전을 위하여 확인 할 수 있다. 이 경우 non-repudiation 서비스가 가능해 진다.

Sharing session key component ' 알고리즘에서 세션키는 두개의 필수적인 openkey, colsedkey로 구성된다. 여기서 closedkey는 세개의 요소로 나뉘어 진다. closedkey = closedkey_1 ? closedkey_2 ? closedkey_3.

세션키 negotiation이 이루어 진후에 분리된 closedkey_1, closedkey_2, closedkey_3 은 자동적으로 Mobile Station(MS)이 KETO의 비밀키를 이용하여 여러 KETO로 분배시킨다. 만일 통신 내용이 분쟁이 되거나, 공공의 안전으로 확인해야 할 경우에 법원의 책임하에 세션키 Ks를 재 구성한다.

	Traditional symmetric key encryption	Public key algorithm	Improved symmetric key encryption
Key length	Short	Long	Short
Computing speed	Quick	Slow	Quick
Mobile device overhead	Low	High	Low
Bandwidth overhead	Low	High	Low
Key lifetime	Long,(the key doesn't change until it is damaged possibly)	Long,(same as left)	Key always changes as every communications
Key Management if there are n parties	(N*(N-1)) / 2	N	No, key is generated at the same
Confidentiality	Yes	Yes	Yes
Digital signature	No	Yes	Yes
Ensure public safety	No	No	yes
Non-repudiation	No	Yes	Yes

[TABLE 1] three kinds of encryption algorithm comparisom

6.9 Comparison of encryption algorithm

우리는 여기서 세종류의 암호 알고리즘을 비교하였다. 기존의 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 위에서 설명한 Sharing Session Key 알고리즘이 그것이다. 이것의 위의 [Table 1]에 설명하였다.

여기서 보여주듯이 개선된 대칭키 암호화 알고리즘은 모바일 기기의 overhead와 bandwidth를 증가시키지 않는다. 또한 key관리의 부하면에서도 공개키 암호화 방식에 비해 훨씬 쉽고, short key lifetime은 좀 더 안전하다고 할 수 있다.

더 좋은 점은 디지털 서명을 통해 non-repudiation 서비스를 제공할 뿐 아니라, 범죄자에 의해 암호 기법이 잘못 사용되는 것도 막을 수 있다.

7. Conclusion

무선에서의 부가기능 서비스와 기능이 급격하게 증가하고 있고 이에 따라 m-Commerce에서도 상호 인증, end-to-end 보안, 부인봉쇄등의 서비스가 요구되고 있다.

미래의 3rd 세대 시스템에서는 좀더 강하고 다양한 형태의 보안 서비스가 데이터 통신과 부가 기능 서비스에 필요로 한다. End-to-end 보안과 여러 서비스의 결합은 사용자 뿐만이 아니라 차기 e-Commerce 시스템을 위해서도 필요하다. 이것은 합법적인 법의 적용을 위해서도 필요한데, 만약 이것이 어렵다면, 전세계적인 상호 운영의 가능성은 희박하게 될 것 이다.

이것 이외에 end-to-end authentication의 기능이 필요한데, 데이터 통신과 부가 서비스 위주의 3세대 시스템에서는 이러한 기능이 더 요구 된다고 할 수 있다. 이것은 end-to-end 보안보다 한 단계 앞선 것으로 볼 수 있다. 상호 인증 없이 거래가 이루어 진다면 더 잦은 논쟁에 휩싸이게 될 것 이다.

새로운 wireless technology는 낮은 전력 사용, 컴퓨팅 파워의 증가, 메모리/사용자 인터페이스의 개선등 혁신을 가져올 것이다. 결국 이러한 것은 공개키 암호 시스템과 대칭키 암호 시스템이 데이터 통신과 부가 서비스 통신에 사용될 것임을 알 수 있다. 데이터의 기밀성과 정합성을 보장하면서 부인 봉쇄의 기능도 필요하지만 범죄자에 의한 잘못 된 사용이나, 법원이 인가한 합법적 해독의 여지도 남겨 놓아야 한다. 암호화 기법은 공공의 이익과 개인의 프라이버시 양쪽을 고려하며 적용되어야 한다.

아직까지 모바일 기술과 단말기 및 사용 프로토콜에 대한 개발의 여지는 많이 남아 있다. 지금까지 밝혀진 보안상의 문제와 열악한 사용자 인터페이스를 극복하고, 많은 편리성과 잇점으로 고객에게 가까이 가리라 기대한다.