All-IP망에서 다기종 Mbile단말기 간 보안개선에 관한 연구

변 병 길, 이 기 영

인천대학교 정보통신공학과

A Study on the security improvement between different mobile terminal Using All-IP in Wireless Network

Byung kil-Byun* □ Ki Young-Lee**

*University of Incheon

E-mail : bgbyun@stu.ac.kr

요 약

인터넷 프로트콜에 적용가능한 모든 Mobile단말은 데이터, 통신들의 상호 편리하고 자유로운 커뮤니케이션의 급속한 발전을 가져왔으나 이때 가장 취약한 점이 바로 보안부분이다. 현재 제시되고 있는 각망의 연동기술의 현황을 분석하고 단말및 이종 네트워크간의 상이한 보안체계의 연동과정에서 발생가능성 있는 취약성및 예상가능한 각종 보안위협에 대하여 대응책등을 고려하려 보다 강화된 보안기술 및 성능분석을 제시하고자 한다.

ABSTRACT

Mobile handsets with all applicable Internet Protocol brought communication channels between the easy and rapid development. But this time that the security is part of the most vulnerable points. All IP-network currently being presented to analyze the current state of integration technology, and two kinds of terminal interworking between networks of different security systems are likely to occur in the course of the various security threats, vulnerabilities and expectations regarding possible measures to consider more stringent security technologies and performance analysis the present study.

키워드

wireless security, w-lan, All-Ip

Ⅰ. 서 론

1983년 모토로라에서 처음 출시된 다이나택(핸드폰)이 무선환경에 등장한 이래로 2009년 3월 현재 이동통신 전화기의 총 가입자 가 41억 3500만명으로 26년만에 전세계 인구의 68%가 무선환경을 살아가고 있다.

IP(Internet Protocol)의 개발과 WWW의 만남을 경험한 이들에게 언제 어디서나 선 없이 WEB 서비스를 사용하고 싶은 욕구를 충족 시키고자 무선랜, 3G분야 또한 크나큰 발전을 이루었다.

이러한 무선 네트워크 기반이 충족되다보니 노트북 외에 스마트폰등의 수요가 증가하였다. 휴대폰과 노트북을 오가며 communication과 정보를 주고 받을수 있도록 진화하고 있다. 사용자들이 PC작업을 하고 있을때 인터넷을 통해 PC로 전화를 받고 집밖을 나서면 새로 오는 전화는 자동으로 스마트폰으로 연결되고 차를 운전할 즈음에는 사무실로 차안의 인터넷 장치를 통하여 전화를 걸어 회의를 잡고 화상회의 도중에는 주소록을 찾아서 다른 사람들로 하여금 회의에 참가하도록 콜을 하고 다른 사람들은 어떠한 환경에 있더라도 인접한 단말을 통하여 통신이 connection 되는 것을 기대하는 것은 공상과학소설에나 있을법한 이야기가 아닌 이미 존재하고 있는 제품과 기술들이다.

그러나 이러한 기대를 충족시키기 위해서는 인증,권한부여, 과금,로밍서비스에 있어서 기존의 사업자위주의 개별화된 방식을 넘어 상호 협약을 통한 통합된 형태가 되어야 할것이다. 아울러 음성, 데이터, 멀티미디어 서비스가 끊어짐없이 제공되어야 하며 QoS등 품질에 대한 고급화가 필수 요건이라고 할수 있다.

위와 같은 고급서비스에 구현되어야 하는 모든 Mobile단말은 데이터, 통신들의 상호 커뮤니케이션을 통한 매체접근이 이슈가 되었다.

각 단말기는 하드웨어로 구성되어있고 그속에서 운영되는 소프트웨어,데이터가 서로 연결되어 원하는 서비스를 제공해야 하는 근본적으로 취약한 구조가 컴퓨터이다.[1)]

사용자들의 편리성을 충족시키면서 취약한 구조 가운데 보안을 실제에 적용하는 것이 어려운 것이 바로 그 이유이다.

정책과 관리입장에서는 기존 개별 네트워크에 대한 보안 수준을 넘어 Wi-Fi, 3G, 4G등과 연동되는 네트워크상에서 보안을 제공할 수 있는 새로운 보안기술 체계가 요구되고 있다. 이러한 보안기술의 구현을 위해서는 개별 네트워크 보안 체계가 가지는 취약성, 각 단말및 이종 네트워크간의 상이한 보안체계의 연동 과정에서 발생 가능성이 있는 취약성 그리고 예상 가능한 각종 보안위협에 대한 대응책등을 고려하여 보다 강화된 보안기술의 개발이 요구되고 있다.[2)]

그러나 보안은 사용자들의 편의성에 밀려 스마트폰의 경우 2009년 4월부터는 멀티미디어 보안 프로토콜인 drm을 해제하고 출시되고 있고 사용자들또한 백신의 효과에 대한 부정적영향으로 인해 정부가 2007년 관계법령(개인정보보호법)의 발효로 본인뿐 아니라 타인의 정보에 대해서도 취급부주의시에는 3년이하의 징역등 형사처벌하는등의 보안 법규를 강화한 바 있으나 지켜지지 않고 있다. 이는 사용자들은 편의성이 수반된 보안서비스에 대한 기대가 높은 것이다.

그래서 본 논문에서는 다기종 Mobile단말기간 보안개선에 관하여 실제 현장에서 적용가능한 보안 적용사례를 연구해 보고자 한다.

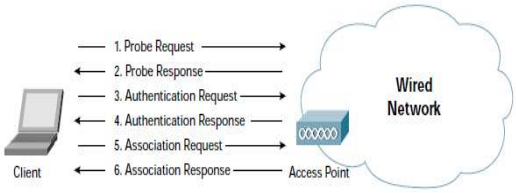
II 관련연구

2.1 무선랜 보안 요소

무선lan은 1999년 IEEE 802.11b표준으로 승인된후 유선으로 설치가 어려운 망 환경에서 광범위하게 이용되고 있다. 비교적 단순한 유선 Ethernet Protocol과 달리 무선 lan은 무선 주파수(RF)데이터가 송출되는 것을 Client Station에서 수신하게 되므로 이과정을 보호하는 보안 메카니즘이 요구되고 있다.

이때 SSID인증, 802.11스테이션인증,공유키인증,맥인증 등이 사용되고 있으며 인증 프로세스는 다음과 같다.

1. 클라이언트가 모든 채널에서 프로브 요청 프레임을 송출
2. 범위 내에 있는 액세스 포인트가 프로브 응답 프레임을 통해 응답.
3. 클라이언트가 액세스에 가장 적합한 액세스 포인트(AP)를 결정한 후 인증 요청을 전송.
4. 액세스 포인트가 인증 응답을 전송.
5. 인증이 성공하면 클라이언트가 액세스 포인트에 연결 요청 프레임을 전송.
6. 액세스 포인트가 연결 응답을 통해 응답.
7. 클라이언트가 액세스 포인트로 트래픽을 송신.[3)]



2.1.1 사용자인증, 접근제어, 권한 검증

IEEE 802.1x를 사용하여 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속포트에 기반한 접근제어 기능을 정의, 무선구간 보안에 필요한 마스터 세션키를 분배 접속허가자가 접속요구단말을 각각의 포토로 관리하여 인증서버로부터 각 포트별로 접속 허가여부를 전달받아서 접속요구단말의 네트워크 접근을 제어하는 것이다. 그러나 네트워크 관리자 영역에 접속 요구단말에 대한 인증정보를 가지고 있는 인증서버가 존재하거나 엑세스 포인트 자체적으로 인증서버 기능을 내장하고 있어야 한다.[4)]

2.1.2 데이터 기밀성, 데이터 무결성, 부인방지

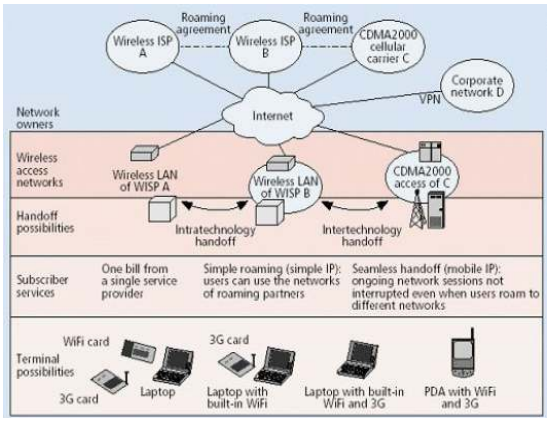
IEEE 802.11i 무선랜 시스템이 가지는 무선구간 보안 취약점을 해결하고자 IEEE 802.1x/1aa기반의 접근제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 무선구간데이터 보호를 위한 새로운 대칭키 암호 알고리즘의 적용등을 내용으로 담고 있다.

2.1.3 보안 취약성

위와 같은 보안요소중 현재 무선랜의 보안요소는 접근제어에 따른 사용자인증과 데이터기밀성에 관한 WEP알고리즘[5][6]이 실제에 적용되는 상위의 보안적용인바, 현재 무선망에서 보안에 관한 802.11, 802.1x, EAP프로토콜에서 메시지에 대한 인증 부족으로 인해서 세션 하이재킹과 MIM공격이 가능하다. 예를 들어 합법적인 사용자와 AP 사이에 EAP메시지 교환을 통한 인증이 이루어진 후, 임의의 시점에서 공격자가 AP로 위장하여 사용자에게 disassociate 메세지를 보내 사용자 연결이 끊어진것 처럼 하고 자신이 그 세션을 이용한 트래픽으로 도청한다. 이는 IEEE 802.11표준에서 관리 프레임에 대한 무결성 보호를 하지 않기 때문이다.

2.2 3GPP 연동기술 표준

2.2.1 무선랜과 이동통신 연동기술

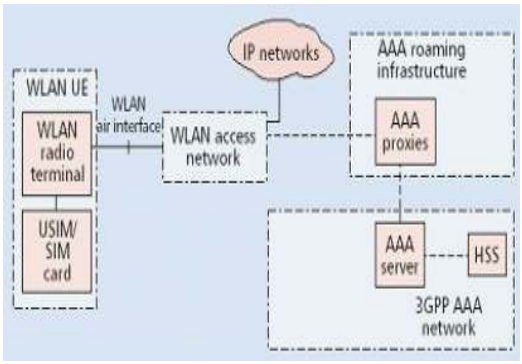


그림에서와 같이 이동통신의 네트워크 구조 또한 단말기에서 AP를 거쳐 콘트롤러까지 가는 WiFi와 유사한 프로세스를 가지며 3G의 경우 단말에서 고강도의 Radio주파수 콘트롤러까지 연결되고 이는 이동통신용 라우터인 PDSN을 통해 인터넷망과 연결된다.

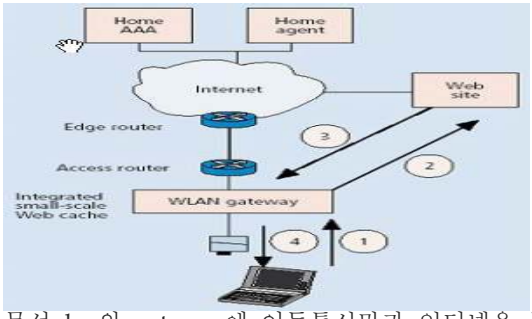
WiFi에서와 같은 프로세서로서 회선사업자A의 망지역에서 벗어나서 회선사업자B지역으로 이동할 때 끊김없는 Handoff가 지원되어야 하므로 회선 사업자와 통신사업자간의 로밍에 관한 규약선행이 필수적이다.

2.2.2 tightly coupled 연동

무선lan을 이동통신망의 무선 접속망의 일부로 간주하여 단말내에 radio-terminal과 ip로 연결된 wlan망의 Wr과 3G망의 AAA프록시서버와 참조점을 통해 접속되어 인증과 키값을 신호로 보내는 RADIUS EAP프로토콜이 사용된다.



2.2.3 loosely coupled 연동



무선 lan의 gateway에 이동통신망과 인터넷을 통해 접속하는 기능을 구현하고 gateway에 Web cache와 FA를 내장함으로써 사용자가 빠른 웹서비스를 받을수 있도록 할수 있게하였다. 단말에서는 WiFi,3G,Ethernet카드,IS-835 shim, virtual MIP adaptor 프로토콜이 지원된다. [7]

2.3 보안결함 및 취약공격

WEP, dynamic-WEP보다 보안강화되어 알려진 EAP인증의 경우 EAP-MD5의 경우 단방향 인증만 제공되고 데이터 암호화를 지원하지 않고 EAP-TLS[8]의 경우 많은 단계를 거쳐야 함에 따른 트래픽 발생 하고 서버의 인증서를 단말에 미리 설치되어 있어야 하는 문제점이 EAP-TTLS와 함께 제기되고 있다.

물리적인 AP or Server등의 Interruption(Dos 중단 : 시스템 자원을 사용할수 없게 하는 것), Interception(가로채기: 권한부여없이 시스템의 assets에 접근하는 것)의 보안 위협이 있고 전송되는 망에서는 데이터에 대하여 Interruption, Interception, Modification, Fabrication의 취약성을 갖고 있다.

III. 무선환경에서의 보안 성능개선 방안

본 논문에서는 서론과 2.3에서 기술한 바와 같이 구현된 여러 프로토콜이 실제 망 현장에서 적용되지 못하는 한계성을 보완할뿐만 아니라 오히려 보안을 강화하고도 이용하기에 편리한 개선안에

대하여 제안하고자 한다.

3.1 보안 구동 방법

step1 MS는 자신의 id, pwd를 입력하고 공개키에 해당하는 11자리 핸드폰 번호(CPN)를 암호화하여 전송한다.

step2 ap에서는 해당값을 넘겨받고 이를 암호화하여 인증서버로 인증요청을 한다.

step3 인증서버는 데이터베이스에 저장된 MS의 id/pwd를 비교하여 값이 일치하면 세션키와 MS의 공개키(CPN)를 암호화하여 AAA서버로 송부한다.

인증서버는 세션키 생성 : SK

step4 키값을 전송받은 AAA서버는 난수를 생성하여 3G망으로 SafeSMS로 전송하고 난수를 해쉬한값을 인증서버로 전달합니다.

AAA서버는 2차검증에 사용될 난수 생성 : Ar

난수를 sms서버를 통하여 3gpp망으로 전송

step5 MS는 암호화된 SK(세션키)를 개인키(CPN)로 복호화하여 세션키 동기화를 완료한다.

3gpp망으로 전송받은 난수값을 암호화하여 인증서버로 권한및 과금요청.

stpe6 인증서버는 전송받은 값을 복호화하여 MS로부터 전송된 암호화된 값과 AAA서버 값을 비교하여 권한 및 과금 성공유무를 확인하여

①서버인증 성공시 응용서비스 지원

②인증 실패시 재인증 시도

step7 AS와 MS사이에 안전하게 공유된 Key를 사용하여 안전한 응용서비스 지원

3.2 제안방식 분석

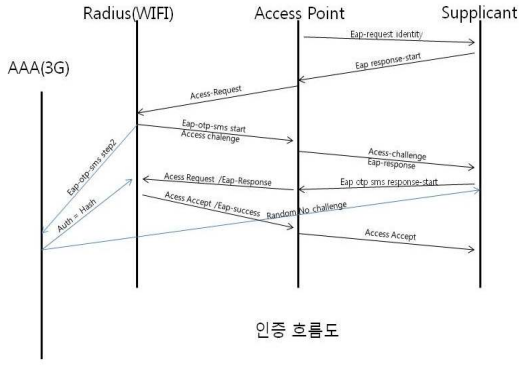
제안방식의 프로토콜을 3.1에서 언급한 안정성과 제3자의 공격에 대한 요구사항에 맞추어 분석하고, 통신에 따른 효율성을 분석하면 다음과 같다

기밀성(confidentiality) :통신에 사용된 키값은 공격자가 알지 못하게 하고 암호화된 값을 전송받고 이는 일회용 pwd이므로 공격자가 알수 없다

무결성(Integrity) Supllicant와 AP간 공격자가 이를 가로채어 위조,삭제,변조되지 않아야 한다. 제안방식에서는 Radius서버에서 중간에 값이 바뀌지 않았는지 암호화값을 비교검증하여 제공된다.

인증(Authentication) Supplicant를 사용하는 사용자가 전송하는 메시지가 본인의 것이 맞는지를 확인하여야 한다. 단말기에서는 ID/PWD로 AP에 승인요청을 보내면 AP는 단말기 데이터를 Radius서버로 보내고 승인결과 암호키를 AP로 보내서 1차 인증을 하고 최초에 전달된 CPN으로 AAA서버는 난수를 생성하여 CP으로 송부함과 동시에 해쉬값을 Radius서버로 송신하고 단말기에서는 값을 입력함으로 2차 인증을 시작하여 Radius는 AAA서버와 값을 비교하여 2차인증을 완료한다.

접근제어(Access Control):정당하지 않은 사용자는 서비스를 이용할수 없어야 하는 것에 대하여 본 제안은 1,2차 인증을 통하여 구현되었다.



인증 흐름도

결론 및 향후 방안

제안된 보안방법은 EAP-tls에서의 세분화된 알고리즘 보다 8단계를 줄이면서 트래픽부하를 줄였으며 EAP-ttls에서 지니고 있던 취약점을 개선하여 사용할수 있게 되었다.

또한 연동기술의 상호보완적인 접근과 일회용암호화라는 접근에 대해 사용자들의 인식도가 높아지는 즈음에 사용자들의 편리성을 충족시키고 보안을 강화할수 있는 일회용 패스워드(난수)의 사용에 대한 접근을 적극홍보하여 편리와 보안을 이룰수 있는 형태를 제안하였다. 현재 제안구현된 것은 비교적 작은 자체망에서 구현가능하게 설계되었는바 사업자간의 표준화협약등을 통해 보다 광범위한 적용이 향후 이루어야 할 과제라고 보여진다.

참고문헌

1) 변병길외, All-IP에서의 Mobile Terminal에 대한 인증고찰, 해양정보통신학회
2) 무선네트워크 연동 보안 기술 동향 100page
3) 802.11무선 LAN보안에 대한 포괄적 검토 및 Cisco Wireless Security Suite. Pejman Roshan
4) 익명성을 지원하는 ID기반 티켓을 이용한 AAA메커니즘,정보보호학회논문지,92page,2007
5) 정은희 외, 무선랜 환경에서 OTP를 이용해 사용자 인증을 강화시킨 보안시스템 설계,142p
6) Newsham, T. "Cracking WEP Keys." Presented at blackhat 2001.
7) 무선랜과 이동통신망 연동표준 한국정보통신기술협회 5,8p 2007
8) 신동훈, 무선랜 보안 표준 분석