情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

무선 LAN 정보보호 기술 표준화 동향

김 신 효*, 강 유 성*, 정 병 호*, 조 현 숙*, 정 교 일*

요 약

최근 무선에서의 보안 결함이 밝혀지고, 무선 환경에서의 개인 프라이버시 침해 문제가 사회적인 현안으로 등장하였다. 본 고에서는 무선 기반 공중 망의 보안성 강화를 위하여 국제 표준화기구에서 논의하고 있는 무선 LAN 정보보호 기술과 키관리 기술 및 가입자 인증 기술 동향과 향후 전망에 대해서 분석해 보고자 한다.

Ⅰ. 서 론

다양한 멀티미디어의 송수신이 가능하여 꿈의 이동통신으로 불리웠던 3세대 이동 통신(IMT-2000) 서비스의 상용화 시기가 늦어지고 있다. 또한 상대적으로도 현저히 빠르지 않은 전송속도와 음성이 아닌 데이터의 전송에 고가의 통신 비용을 지불하여야 한다는 단점으로 인하여 무선LAN이 초고속 무선인터넷의 좋은 대안이 될 수 있다는 인식이 급속히 확산되기 시작하였다. 기존의 인터넷사업자들 역시 핫스팟 지역에 무선LAN을 설치하여 값싼 초고속 멀티미디어 무선인터넷 서비스를 제공하는 방향으로 유무선 통합망을 구축하고 있으며, 이동통신사업자들 역시 이동통신과 무선을 연동하는 방향으로 유무선 통합망을 구축하기 위한 노력을 진행하고 있다.

이러한 유무선 통합망을 이용한 무선인터넷 사용자들은 이동중에도 무선으로 전자메일, 물건 구입 및 인터넷 전화 등의 편리한 서비스도 받으면서, 프라이버시 정보를 보호받고 싶은 보안성 욕구도 함께 증가하고 있다. 무선LAN이 유무선 통합망의 중요한 요소로 자리매김하기 위해서는 무선LAN 고유의 브로드캐스팅 특성으로 인하여 엿듣기 등 무선LAN 데이터 프라이버시에 대한 취약성 해소를 위해 보안성을 강화함은 물론, 공중망에서 사용되기 위해 필요한 네트워크 접속 기술과의 결합이 필요하다. 특히 무선LAN 기반 유무선 통합망 구축시 보안성이 가장 중요한 영역으로 인식되고 있으며, 단말의 이동에 따른 보안 체계의 복잡성을 어떻게 해결해야 하는가도 큰 이슈중의 하나이다[1].

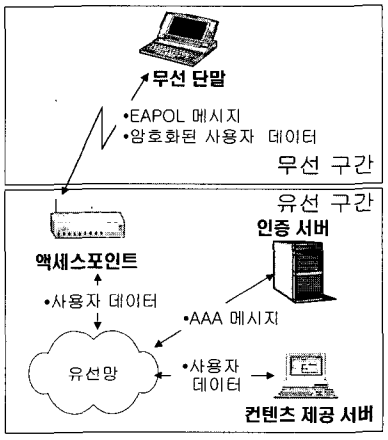
무선LAN이 공중망에서 차지하는 비중이 점차 높아가고, Mobile IP를 이용한 무선인터넷 서비스의 주 타겟 망이 무선LAN이 될 가능성이 높아지면서 IEEE, IETF, ETSI, 3GPP(3rd Generation Partnership Project) 등 국제 표준화 기구에서도 이와 관련된 표준화를 진행하거나 계획하고 있다. 무선LAN 표준화의 대표적인 IEEE 802에서는 대표적인 보안 표준으로 IEEE 802.11i(Specification for Enhanced security)와 IEEE 802.1X(Port-based Network Access Control)를 발표하였다. IEEE 802.11i(이하 802.11i)는 무선LAN MAC(Media Access Control)레이어에서 무선단말과 액세스포인트간의 장비 인증과 데이터에 대한 암호화를 담당하고 있으며, IEEE 802.1X(이하 802.1X)는 유선까지 아우르는 MAC레이어 상위에서 사용자에 대한 인증서비스 제공을 위한 프레임워크에 관련된 표준을 다룬다. 802.11i 태스크그룹은 무선LAN 인프라망과 Ad-Hoc망에 적용할 수 있는 새로운 형태의 보안 아키텍쳐(RSN: Robust Security Network)를 제안하고 이를 구체화하고 있다[2]. RSN은 다수의 액세스포인트가 연결된 핫스팟에서 802.1X 기반 가입자 인증을 통한 네트워크 접속 제어, 보안 세션 관리, 패킷당 키관리, 그리고 새로운 암호 알고리즘 도입을 통한 무선 접속구간 보안을 강화하는데 이용된다. IEEE 802.11워킹 그룹은 최근 802.11i와 802.1X를 결합시키는 작업을 진행하고 있으며, 상당한 진전을 이루었다[2-4].

* 한국전자통신연구원({shykim, youskang, cbh, hsch, kyoil}@etri.re.kr)

본 고에서는 먼저 기존의 무선LAN 망에서의 보안 문제점이 무엇인지를 2장에서 정리하고, 3장에서는 802.1X와 인증서버를 통한 키분배 방식을, 그리고 4장에서는 새로운 무선 보안 구조인 RSN을 통한 보안 협상 방법에 대해서 살펴보겠다. 그리고, 마지막 5장에서는 결론을 맺겠다.

II. 무선LAN 보안의 문제점

무선LAN 보안 서비스를 제공하는 서비스 망은 무선단말과 액세스포인트 및 인증서버로 구성된다. 무선단말과 액세스포인트 간은 무선 접속구간이며, 유선망에 연결되어 타 네트워크와 연동하는 브리징 기능을 수행하는 액세스포인트와, 사용자 단말에게 인증 서비스를 제공하는 인증 서버는 유선구간에 위치한다(그림 1). 무선 단말은 인증과 관련된 정보는 EAPOL(Extended Authentication Protocol Over LAN)프레임 형태로 액세스포인트로 전달하고 액세스포인트는 이들 메시지들 중에 인증서버로 전달하여야 하는 메시지는 AAA(Authentication, Authorization and Accounting) 메시지 형태로 변환하여 전달하고 인증과정을 수행된다.

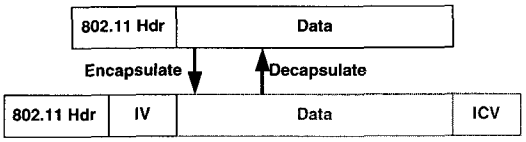


〔그림 1〕 무선LAN 서비스 구성도

무선LAN은 유선LAN과는 달리 기본적으로 모든 단말에 데이터를 뿌리는 브로드캐스팅 망이므로, 액세스포인트의 비콘 수신 영역 내에 있는 모든 단말은 다른 사람의 송수신 데이터 내용을 청취할 수 있으므로, 수신자 이외의 다른 사람으로부터 데이터를 보호하기 위해서는 기밀성 및 무결성 서비스와 상호 인증 서비스가 매우 중요하다. 하지만 현존하는 무선 LAN서비스에서는 몇 가지 점에서 보안성이 취약하다. 본 절에서는 사용자와 액세스포인트사이의 무선 접속구간에서의 보안 문제점과 유선 구간에서 존재하는 인증서버의 한계에 대하여 살펴보도록 한다.

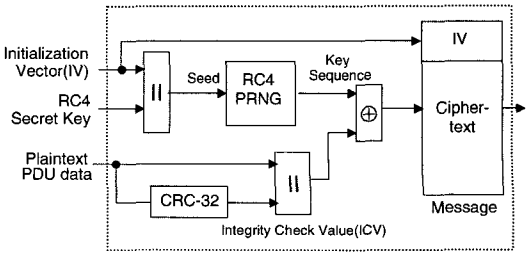
1. 무선 접속 구간 보안의 문제점

암호화된 무선LAN 프레임은 802.11 헤더 및 사용자 데이터 이외에 데이터 암호화에 사용된 IV (Initialization Vector)를 추가하고 메시지 확인을 위한 ICV(integrity Check Value)를 마지막에 부가한다. 헤더와 IV를 제외한 사용자 데이터와 ICV는 암호화된 형태이며, 이러한 메시지 형태를 (그림 2)에 도시하였다.



〔그림 2〕 802.11의 메시지 프레임 구조

현재까지의 무선LAN에서 데이터에 대한 보안을 위해서는 기존의 WEP(Wired Equivalent Privacy)보다 개선된 WEP2 알고리즘의 사용을 권고하고 있다. WEP2 알고리즘은 무선LAN 사용자 데이터의 보안성을 제공하기 위한 암호화 기법으로써, 데이터의 암복호화에 동일키를 사용하는 스트림 암호 방식이다. 액세스포인트의 서비스를 받는 모든 단말은 128비트 크기의 암호키를 미리 공유하고 있다. 액세스포인트는 단말을 인증하기 위해 random challenge를 보내면, 단말은 공유하고 있는 128비트의 암호키와 128비트의 IV를 결합하여 이를 RC4 암호화 알고리즘에 입력시켜 의사 난수 키 스트림을 생성하고, 이를 이용해 평문을 암호화하여 전송한다(그림 3). 액세스포인트는 이를 복호화하여 단말을 인증한다[5].



〔그림 3〕 WEP2의 암호화 방식

WEP2 알고리즘은 기존의 WEP 보다는 암호키와 IV의 크기를 늘려 보안성이 강화된 것은 분명하지만, IV를 암호화되지 않은 평문으로 전송되며, 암호키는 액세스포인트에 연결된 모든 단말이 공유하는 값으로, 실시간 공격과 도청으로 인한 평문의 노출 등으로 암호학적으로는 여전히 취약하다[6].

2. 인증서버의 문제점

유선 구간에서는 RADIUS (Remote Authentication Dial In User Service)나 TACACS+ (Terminal Access Controller Access Control System) 프로토콜을 이용하여 사용자 인증을 통한 보안성을 제공하고 있다[7-8].

최근의 무선LAN 환경은 핫스팟 지역에서 액세스포인트를 통해 직접 인터넷에 접속하는 형태로, PPP 접속에서의 NAS(Network Access Server)와는 다른 방식이므로 기존의 클라이언트/서버 모델 기반의 RADIUS를 인증 및 과금 서버로 사용하기에는 적합하지 않다. 즉, 인증 서버에 접속하기 위한 NAS로 동작하는 액세스포인트는 PC 통신 서버의 수에 비해서 상대적으로 매우 많고 이를 관리하는 주체도 대단히 많을 것으로 예상되는 상황에서 단순한 프록시 기능만을 지닌 RADIUS를 이용하여 이들을 효과적으로 상호 연계시키는 것이 현실적으로 어렵고, 무선LAN의 다양한 운용 환경(예를 들면, 공용망에서의 불특정 다수에 의한 단독망, 공용과 단독망의 혼합된 형태의 운용)에 따라서 다른 서비스를 제공하는 것도 쉽지 않을 것이며, 큰 규모의 적용환경에 취약한 것으로 알려져 있다[9]. 또한 중요한 무선인터넷 접속 기반 구조로 활용된 IMT-2000에서도 인증 서버로 Diameter를 채용하는 최근의 경향을 반영하여 상호운용성을 고려한다면, 무선LAN 상에서의 인증 및 과금 서버로는 Diameter가 현재로서는 유일한 대안으로 여겨진다.

Diameter 인증 서버는 AVP(attribute value pair) 코드 필드의 증가로 AVP의 추가가 용이하고 메시지의 길이 제한이 적으므로 확장이 용이하고, 신뢰할 수 있는 하부 프로토콜(예를 들면 SCTP: Stream Control Transmission Protocol)의 사용이 가능하고 브로커 기반의 Peer-to-peer 기반 프로토콜로써 다수 구성요소 간의 상호 연계가 용이할 것이다. 또한 상위의 응용에 상관없이 통합된 과금 기능을 지원할 수 있으며, 서버에 의한 강제적인 메시지의 전송이 가능하므로 과금 정책에 의한 사용자의 서비스 제한도 용이하여 서버에 의한 다양한 과금 및 컨텐츠의 제공이 가능하다는 장점을 가지고 있다[10].

III. Diameter 인증서버의 동작과 802.1X를 통한 키 분배

1. 802.1X와 802.11i

2001년 6월에 승인된 802.1X는 무선 가입자의 상호인증 방법과 무선 접속구간 보안에 필요한 마스터 세션 키를 동적으로 분배하기 위한 방법을 정의한 규격이다. 여기에 802.11i 표준화의 요구 조건을 수용하기 위하여 2002년 7월에 802.1X 문서에 대한 'Amendment 1: Technical and Editorial Corrections'로써 IEEE 802.1aa draft version 3.0 문서를 발표하였다[4].

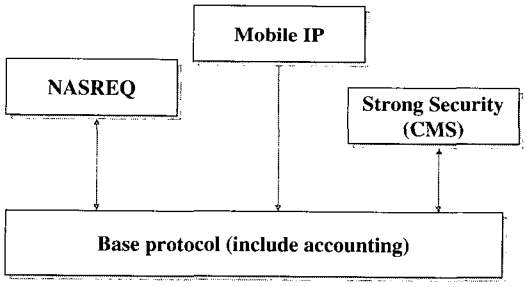
802.1X가 마스터 세션 키 분배 및 이를 통한 무선 사용자와 액세스포인트 사이의 상호인증을 정의하고 있는 반면, 무선 접속구간의 데이터 암호화를 위한 암호 알고리즘의 정의 및 암호 키 분배에 대한 표준화는 802.11i 태스크그룹에서 담당하고 있다. 2002년 7월 현재 802.11i 태스크그룹에서는 802.11i draft version 2.2 문서를 작성했다. 이 문서에서는 무선 구간 암호 알고리즘으로써 WEP, TKIP (Temporary Key Integrity Protocol), AES (Advanced Encryption Algorithm) 알고리즘을 제안하고 있으며, 무선 구간 암호 키 분배를 위하여 무선 사용자와 액세스포인트 사이의 4-way handshake 키 분배 프로토콜을 제안하고 있다. 4-way handshake 키 분배 프로토콜은 기본적으로 802.1X의 인증 프로토콜을 통한 마스터 세션 키 획득을 전제로 하고 있다.

802.1aa 문서에서는 802.11i 에서 제안하고 있는 4-way handshake 키 분배를 위한 key descriptor를 수용하기 위하여 802.1X key descriptor 형태를 확장이 가능하도록 재구성하였다. 그리고, 무선 단말 사용자와 액세스포인트사이의 암호 키 분배가 완료되면 해당 무선 채널이 안전하다는 것을 나타낼 수 있는 방법을 구체화하여, 기존에 정의된 state machine을 변경하거나 추가하였다.

2. Diameter 인증서버의 동작

Diameter의 기본 구조는 (그림 4)에서와 같이

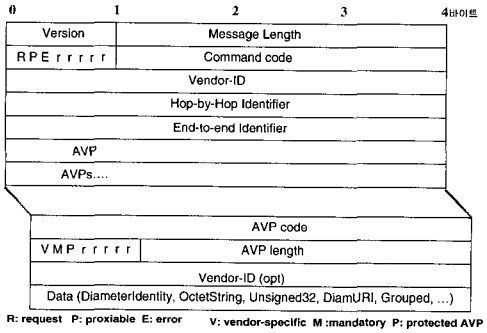
과금 기능을 포함한 기반 프로토콜(Base protocol)[10]과 상위의 다양한 응용 기술로 나뉠 수 있다. Diameter의 기반 프로토콜은 응용에서 필요로 하는 세션 또는 과금에 대한 관리 등의 기본적인 서비스를 제공하고, AVP의 전달, 노드의 능력(Capabilities)에 대한 협상 및 에러 통고 등의 기능을 부가적으로 수행한다. 현재 정의되어 있는 응용으로는, PAP/CHAP등의 전통적인 인증 방식 또는 EAP를 이용한 네트워크 인증 응용(Diameter NASREQ Application)[11], Mobile IPv4 응용(Diameter Mobile IPv4 Application)[12], 노드간 보안 및 종단간 보안을 위한 Diameter CMS Security[13] 응용이 있다. 또한 Diameter는 RADIUS의 단점으로 지적받은 확장성을 보장하기 위해 새로운 응용 식별자(Application Identifier)와 사업자에 의한 특정 AVP의 추가가 용이한 프레임워크를 가지고 있다. 그 기본구조를 (그림 4)에 도시하였다.



〔그림 4〕 Diameter의 기본 구조

Diameter 메시지 구조는 (그림 5)와 같다. 메시지 헤더에는 버전 정보, 전체 메시지 길이, 명령 코드와 요구/응답을 나타내는 비트, 중간의 프록시에 의해 전달 가능함을 표시하는 비트, 에러를 나타내는 비트들이 존재한다. 2002년 7월 갱신된 Diameter base protocol 규격[10]에서는 기존의 optional field였던 Vender-ID 대신에 Application-ID를 메시지 헤더에 추가하여 헤더에 의한 응용 메시지의 구분을 명확히 하였다. 더불어 노드간의 메시지 전달을 분명히 하기 위한 Hop-by-Hop ID 및 종단간 메시지 전달을 위한 End-to-End ID가 존재한다. Hop- by-Hop ID는 각 노드에 따라 변경하지만 End- to-End ID는 메시지가 최종단에 전달될 때까지 변경되지 않는 값이다. 이 ID이후에는 AVP 리스트가 올 수 있으며, 하나의 AVP는 AVP 코드와 메시지 길이와 다양한 형태의 데이터가 전달되며, AVP의 상태를 나타내는 비트들이 존재한다. 특히 CMS에 의해 보호되고 있는 AVP인 경우에 P 비트는 셋팅되어야 하며, 각 노드에서 변경 가능한 AVP인 경우에 이 비트는 셋팅되어서는 안된다. 기반 프로토콜은 AVP들에 대한 기본적인 에러 확인을 한 후 상위의 응용으로 데이터를 올려보낸다.

기반 프로토콜은 능력 협상을 위한 메시지, 연결 설정을 위한 watchdog 동작 및 해제, 세션 중지와 세션 종결 연결 해지, 재인증을 위한 메시지와 과금 기능을 수행하는 메시지로 세분된다.



〔그림 5〕 Diameter 메시지 구조

또한 NASREQ 응용에서는 EAP 인증 메시지 처리와 PAP/CHAP 인증 메시지 처리를 담당하고 CMS 응용에서는 보안 어소시에이션(Security Association)을 처리하기 위한 두 종류의 메시지가 존재한다. 마지막으로 Mobile IP(MIP) 응용에서는 Mobile Node에 대한 인증 처리를 위한 메시지를 처리한다. Diameter 기반 및 상위 응용에서 정의된 메시지 종류는 표 1에 자세히 표시하였다.

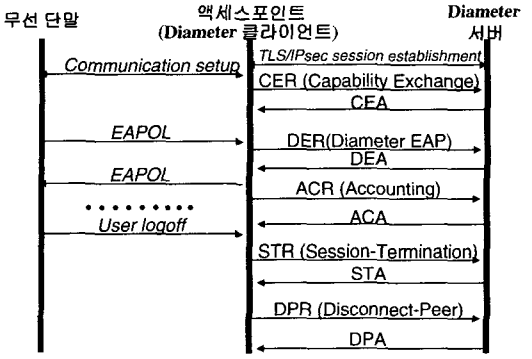
〔표 1〕 메시지 종류 및 역할

위 치	명령 이름	역할
Base Protocol	CER CEA	Capabilities-Exchange Request / Capabilities-Exchange Answer
	DPR DPA	Disconnect-Peer Request / Disconnect-Peer Answer
	DWR DWA	Device-Watchdog Request / Device-Watchdog Answer
	RAR RAA	Re-auth Request / Re-auth Answer
	ASR ASA	Abort-Session Request / Abort-Session Answer
	STR STA	Session-Termination Request / Session-Termination Answer
	ACR ACA	Accounting Request / Accounting Answer
NAS REQ	DER DEA	Diameter EAP Request / Diameter EAP Answer

NAS REQ	DER DEA	Diameter EAP Request / Diameter EAP Answer
Application	AAR AAA	AA Request / AA Answer
CMS Application	DSAR DSAA	Diameter Security Association Request / Diameter Security Association Answer
	PDSR PDSA	Proxy Diameter Security Association Request / Proxy Diameter Security Association Answer
MIP Application	AMR AMA	AA Mobile Node Request / AA Mobile Node Answer
	HAR HAA	Home Agent MIP Request / Home Agent MIP Answer

무선LAN 사용자의 인증과 권한 제어 및 과금을 위해서는 802.1X에 정의된 Authenticator PAE 즉, 액세스포인트는 인증 서버인 Diameter의 클라이언트 기능을 수행한다. 이 Diameter 클라이언트는 단말로부터의 EAPOL메시지에서 EAP 메시지를 추출하고, 인증 서버로 전달하기 위한 AAA메시지의 하나인 DER(Diameter EAP Request) 메시지로 재구성한다. 인증서버는 이에 대한 응답으로 DEA(Diameter EAP Answer) 메시지를 액세스포인트를 통해 무선 단말에 EAPOL 형태로 전달함으로써 가입자 인증을 수행한다. 또한 과금을 위해서 Diameter 서버와 클라이언트는 과금 정보의 저장과 관리 기능을 수행함은 물론 ACR(Accounting Request)과 ACA(Accounting Answer) 메시지를 사용하여 과금 데이터를 송수신한다.

무선 단말이 액세스포인트에 접속 요청을 시작으로 가입자 인증을 거치고, 과금을 수행하고 사용자 로그오프 이후 세션의 종료와 연결 해제의 전 과정을 메시지의 흐름으로 일반적인 예로 도시하면 (그림 6)과 같다. 무선 단말과 액세스포인트는 비콘 신호의 송수신으로 통신을 설정하고 이후 사용자에 의한 액세스포인트 접속요청을 받아야 한다. 이후 단말과 액세스포인트는 인증정보의 제공과 사용자 로그오프 등의 일련의 과정을 EAPOL형태로 메시지를 송수신한다. 액세스포인트는 가장 먼저 인증서버와 안전한 통신 채널의 설정을 위해 TLS(Transport Layer Security) 또는 IPSec을 이용한 세션을 설정한 후 AAA 메시지 교환을 시작한다. CER/CEA 메시지를 이용하여 자신이 NASREQ 서비스가 가능함을 클라이언트에게 알리고, 사용자로부터의 EAP를 DER/DEA 메시지로 변환하고 이를 EAPOL로 무선 단말에 전달하여 검증하게 함으로써 사용자에 대한 인증과 권한제어 기능을 수행한다. 즉, 사용자로부터 받은 가입자 신원 정보는 EAP-payload로 DER 메시지[9]에 담겨져서 인증 서버에게 전달되고, 최종적으로 액세스포인트는 인증서버로부터 인증 성공/실패 DEA 메시지를 받으면 인증과정이 종료된다. 이 때 인증과정에서 생성한 마스터 세션키는 다시 액세스포인트로 전달된다[10]. ACR과 ACA를 이용한 과금 정보의 수집과 전달은 서비스 도중에 이루어지며 사용자의 로그오프이후에는 세션의 종료(STR/STA)와 연결 해제(DPR/DPA)의 순서로 모든 서비스를 마치게 된다.



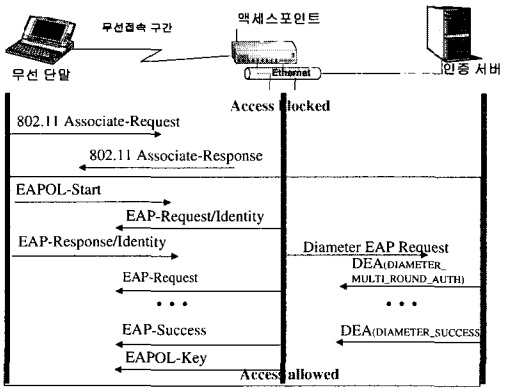
〔그림 6〕 가입자 인증 메시지의 흐름(예)

그리고 이들 메시지들에 대한 보안성 제공을 위해 DSAR(Diameter Security Association Request) / DSAA(Diameter Security Association Answer) 메시지와 PDSR(Proxy Diameter Security Association Request) / PDSA(Proxy Diameter Security Association Answer) 메시지를 사용할 수 있다.

3. 802.1X 프로토콜 동작

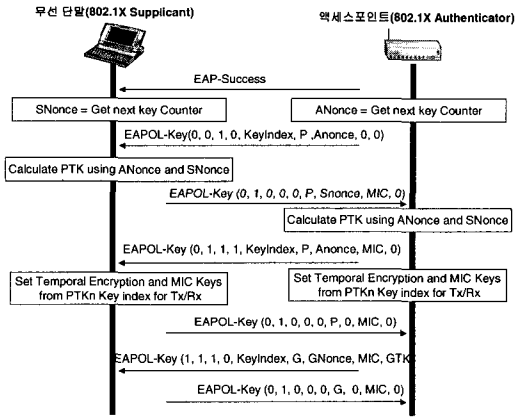
802.1X의 Supplicant는 망접속을 요청하는 단말이고, Authenticator는 단말과 인증서버 간의 인증과정을 중계하고, 인증 결과에 따라 컨트롤을 수행하는 주체 (PAE: Port Access Entity)가 된다. 컨트롤 주체인 액세스포인트는 어소시에이션 식별자(Association ID)와 같은 논리적인 포트를 이용하여 가입자의 접속을 제어한다. 즉 패킷 필터링을 통하여 인증받은 포트로 송수신되는 데이터 전송만을 허용하는 방식이다.

사용자(Supplicant PAE)가 먼저 접속을 시도하는 경우, EAPOL-Start 메시지를 액세스포인트(Authenticator PAE)에게 보낸다. 액세스포인트는 이 EAPOL-Start 메시지를 받으면 가입자 인증에 필요한 가입자 신원(ID) 정보를 단말에게 요청한다. 이 때 가입자의 글로벌 로밍과 과금을 지원하기 위해서는 가입자 ID가 E-mail주소 표기와 같은 NAI (Network Access ID) 형식을 따라야 한다.[14] NAI형식을 준수해야 만이 가입자의 홈 인증서버의 위치를 알 수 있어서 분산 인증이 가능하게 된다. 이와 관련된 규격은 IETF 에서 표준화를 진행하고 있다[14-15].



〔그림 7〕 802.1X와 인증서버를 이용한 안전한 무선 접속 과정

무선 단말은 EAPOL-Key 메시지를 이용한 키 교환과 EAP-Success의 수신으로써 자신이 인증되었고, 무선 채널이 안전하다는 것을 판단할 수 있다(그림 7). 무선 단말과 액세스포인트가 키를 교환하게 되면, 그 키의 사용 시점을 동기화하는 것이 필요하다. 또한 무선 단말은 EAP-Success를 수신함으로 인증된 controlled port를 사용할 수 있기 때문에 EAP-Success의 수신과 키 사용 시점의 동기화는 중요한 표준화 기술의 대상이다. 2002년 7월 현재 802.11i 태스크그룹에서는 인증서버로부터 Access-Accept 메시지와 함께 마스터 세션 키를 수신한 액세스포인트가 먼저 EAP-Success 메시지를 무선 단말에게 송신하고, 그리고 나서 (그림 8)의 4-way handshake를 통하여 무선구간 암호 키 교환과 그룹 키 갱신을 하는 것으로 표준화를 진행하고 있다. 이 후부터 단말과 액세스인트는 동적으로 분배된 키를 이용하여 무선 데이터 구간에 대한 프라이버시를 보장받을 수 있다.



〔그림 8〕 4-way handshake 과정(예)

802.11 기반 무선LAN 시스템의 보안 기술의 실용화를 위해서는 사용자(Supplicant), 액세스포인트(Authenticator) 그리고, 인증서버(Authentication Server)가 각각 처리해야 할 데이터의 전송 프레임이 표준화되어야 한다. 따라서 IEEE의 무선 구간 표준화와는 별도로 액세스포인트와 인증서버 사이의 프레임 구조는 IETF에서 담당하고 있으므로, 상호 유기적인 협력은 당연하다. 2002년 1월, 802.11 및 11i 워킹그룹의 의장은 IETF/IESG 의장에게 마스터 세션 키 생성을 위한 EAP 인증 방식 중 특정 방식에 대한 정의, EAP keying 프레임 타입의 정의, 그리고 RADIUS keying attribute의 정의 등에서 상호 협조가 요구됨을 알린바 있다[16].

802.1X에서는 EAP를 가입자 인증 데이터 전송을 위한 표준 프로토콜로 이용하고 있다[17]. EAP 프로토콜은 초기 IETF의 EAP워킹그룹(Point-to-point Protocol Extensions 워킹그룹으로 시작하였으나 지금은 EAP 관련된 표준화 작업을 주로 진행함)에서 ID/패스워드, 인증서, 스마트카드, Kerberos 등 다양한 인증 방식을 지원하기 위한 encapsulation 알고리즘으로 시작하였으나, 최근에는 EAP를 표준화하고, 다른 워킹 그룹에서도 각 인증 알고리즘을 이용한 세션 키 생성 방법의 표준화을 추진하고 있다.

IETF EAP 워킹그룹에서 표준화중인 EAP 인증 방식(EAP-method) 중에서 EAP-MD5[18]는 유일하게 mandatory로 정의된 방식이다. 구현이 단순하나 단방향으로 가입자 인증만을 지원하고, 무

선 접속구간 보안에 필요한 마스터키 생성 방식을 정의하고 있지 않는다는 문제가 있다. EAP-TLS[19]는 사용자와 인증서버가 인증서를 이용하여 상호 인증하고, 세션 기반의 동적인 WEP키를 생성하여 분배하는 대표적인 인증 방식이다. EAP-TTLS (Tunneled TLS Authentication Protocol)[20]는 EAP-TLS의 확장 형태이다. EAP-TTLS는 열악한 무선 환경에서 무거운 인증서를 보관하고 전송하여야 하는 부담을 줄이기 위하여 단말 인증은 비밀번호로 수행하고 서버 인증은 인증서를 이용하여 인증하는 방식이다. 사용자 정보는 TLS 프로토콜을 통해서 안전하게 터널링 함으로써 무선링크를 포함한 인증서버 까지 외부 도청자에 대한 익명성이 보장된다. EAP-AKA(Authentication and Key Agreement)[21]는 3GPP에서 IMT-2000용으로 제안한 인증 및 키 일치(AKA) 메커니즘을 EAP에 적용한 인증 방식이다. 이러한 인증 방식 중에 EAP-MD5는 패스워드 기반으로 양방향 인증을 제공하지 못하고, EAP-TLS는 양방향 인증은 제공하지만 인증서를 사용하여야 하므로 현재의 무선에서의 적용은 어려우므로 802.11 응용에서 마스터 세션 키 생성에 적절한 새로운 EAP 인증방식을 선정할 필요가 있다.

또한, EAP인증 방식에는 EAP keying을 사용할 수 있다고 정의하고 있지만 이를 사용하기 위한 프레임워크가 없는 문제점을 지적하고 여기에 대한 해결책을 제시해 주기를 요구했다. EAP keying의 목적은 가입자와 인증서버가 EAP 인증방식을 이용한 상호인증 과정 이후 마스터 세션키를 생성하는 것이다. 그러나 EAP인증은 가입자와 인증서버 양단에서 동작하므로 무선단말과 액세스포인트가 RSN 협상 과정에서 어떤 cipher suite를 사용하기로 결정했는지 키 생성과 관련된 구체적인 키 요구사항을 상위 계층에서는 알 수 없다는 점이다. IETF AAA 워킹그룹와 EAP 워킹그룹에서 이와 관련한 표준을 다루고 있으나 아직 국제 규격은 없는 상태이므로 이에 대해 조속한 논의가 필요함을 지적하였다.

마지막으로 지적한 내용은, RADIUS의 AVP중에는 암호 키 정보의 전달을 위해서는 vendor-specific AVP를 이용할 수 밖에 없으므로, 새로운 RADIUS keying attributes를 필요로 한다. 즉, RADIUS keying attribute는 무선 사용자와 RADIUS 인증서버 사이에 설립된 마스터 세션 키를 RADIUS 인증서버가 액세스포인트에게 RADIUS 프레임 포맷에 실어 보내기 위해 필요한 attribute이므로, 기타 다른 프로토콜을 사용하는 인증서버라 하더라도 이와 유사한 기능을 담당하는 전송 프레임 구조는 반드시 필요하며, 이와 같은 내용을 IETF 표준화 과정에 반영하여야 함을 의미한다.

IV. 새로운 무선 보안 구조 RSN

1. RSN (Robust Security Network)

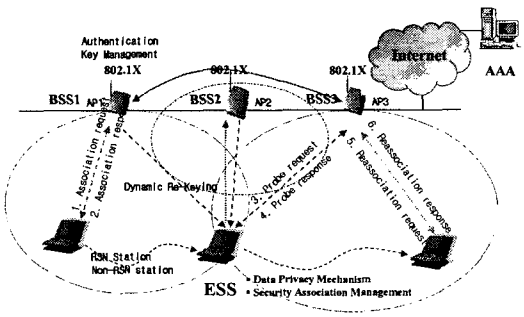
WEP 방식의 보안 문제점이 IV가 평문으로 전송되어 모두에게 알려지게 되며, 사용되는 암호 알고리즘(RC4)과 무결성 알고리즘(CRC-32)이 근본적으로 보안에 취약하다는 사실에 있음을 분석한 바 있다. 802.11i에서는 이러한 문제를 해결하는 방법으로 2가지 접근 방식을 제안하고 있다. 하나는 장기적인 관점에서 알고리즘 자체를 보안 강도가 높은 알고리즘(AES)으로 바꾸는 것인데, 이러한 방식은 MAC의 하드웨어 칩을 변경하여야 하므로 개발기간이 길고, 기존에 배치되어 사용중인 무선LAN 카드 및 액세스포인트에 backward compatibility를 보장 못하는 문제가 있다. 또 다른 하나는 단기적인 관점에서, 전술한 보안 문제점을 소프트웨어적으로 개선하는 TKIP 방식이다. 이 방식은 WEP 알고리즘을 개선할 수 있는 방법으로써, WEP 키를 고정적으로 사용하는 것이 아니라 key mixing과 MIC 과정을 WEP 알고리즘 앞단에 추가하여 WEP 키와 IV가 가지는 보안상의 약점을 보완하는 방식이다. 과도기적인 방식이긴 하지만 기존의 무선LAN 카드와 액세스포인트를 소프트웨어적으로 패치(patch)하여 사용할 수 있는 장점이 있다.

802.11 워킹그룹는 무선 보안의 문제점을 다음과 같이 정리하고 표준화에 반영하고 있다.

(1) RC4 WEP 알고리즘 자체가 알려진 평문 공격에 취약하다.
(2) 동적인 WEP키 분배 방법이 없다.
(3) 가입자 인증 및 접속 제어 방법이 없다.
(4) 공중망에 적용을 위한 중앙집중형 인증/과금/권한제어(AAA) 방법이 없다.
(5) 인증서, 보안토큰, ID/패스워드, SIM (Subscriber Identity Module)용 스마트카드 등을 지원하는 다양한 가입자 인증방식이 없다.
(6) 로밍 보안을 지원하지 못한다.

전술한 문제점 중에서 (1)과 (2)는 802.11i 태스크그룹에서 (3)은 802.1X에서 (4)는 IETF AAA 워킹그룹에서 (5)는 IETF EAP 워킹그룹에서 그리고 (6)은 IEEE 802.11f[22]와 802.11i 태스크그룹, IETF Seamoby와 Mobile-IP 워킹그룹에서 표준화를 진행하고 있다.

802.11i는 2002년 3월 RSN 보안 구조를 드래프트 표준에 반영함으로써, 무선에서의 데이터 프라이버시 기능을 더욱 강화하였다. RSN은 핫스팟에서 802.11과 802.11i를 지원하는 무선 액세스포인트들이 공존하는 환경에서, 802.1X를 이용한 가입자 인증 및 키관리 메커니즘과 빠르고 안전한 로밍 보안 프레임워크를 제시한 새로운 형태의 보안 구조이다(그림 9).



〔그림 9〕 RSN (Robust Security Network)

RSN이 지향하는 보안 목표는 첫째, 동적인 키갱신(dynamic rekeying) 등 무선 보안 강화(strong confidentiality) 기술을 이용한 보안의 취약성(기밀성, 무결성 등) 해결, 둘째, 다양한 무선망 환경 즉, 무선 인프라망과 Ad-Hoc망에 유연하게 적용할 수 있는 보안(flexible security) 프레임워크 제시, 셋째, 802.1X를 적용한 가입자 상호 인증 및 무선 망 접속제어 (port-based network access control), 넷째, 액세스포인트와 인증 서버를 분리함으로써 가입자의 제약없는 글로벌 로밍 보안 지원(ubiquitous security), 다섯째, 액세스포인트를 이동하는 가입자와 신규 서비스를 요청하는 가입자 수에 확장성이 있으면서 빠르고 안전한 재인증 메커니즘을 제공하는 것이다.

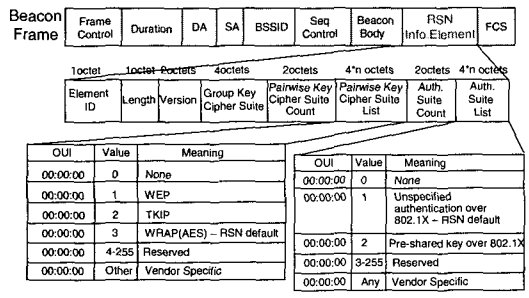
RSN의 주요 보안 요소는 802.1X 인증 메커니즘, 802.11i 데이터 프라이버시 메커니즘, 그리고 보안 어소시에이션 관리이다. 802.1X 인증 메커니즘은 EAP/EAPOL 프로토콜, EAP 인증 및 키분배 알고리즘, AAA 인증서버, 그리고 논리적인 포트 기반 무선 접속 제어기술로 대변된다. 802.11i 데이터 프라이버시 메커니즘은 WEP, TKIP, AES로 대변되는 3가지 cipher suite로 구성된다. 데이터 프라이버시 메커니즘의 cipher suite는 무선 데이터 프라이버시를 보장하는데 필요한 암호 알고리즘 세트를 의미한다. 이와는 별도로 802.11i에서는 무선 가입자 인증방식을 선택하기 위한 인증 cipher suite을 정의하고 있는데, 대표적인 방식인 802.1X 인증방식과 pre-shared key 인증방식이 있다. 현재 논의되고 있는 기본 인증방식 및 데이터 프라이버시 메커니즘은 802.1X 인증과 AES 암호 알고리즘이다. 2002년 7월에 있었던 802.11i 미팅에서 AES 동작 모드에 대한 논의의 결과로 AES-CCM 모드를 mandatory 구현으로 결정하고, AES-OCB 모드를 optional 구현으로 결정하였다. 보안 어소시에이션 관리는 동적인 키 생성 및 분배 메커니즘과 re-keying 프로토콜을 이용하여 단말과 액세스포인트 간에 특정 cipher suite에 맞는 보안 컨택스트를 설정하고 유지하는 과정이다.

2. RSN 보안 협상

RSN 보안 협상은 단말과 액세스포인트가 서로 간의 보안 요구사항(인증 메커니즘, unicast/ multicast 암호 알고리즘과 같은 cipher suite)을 일치시키는 절차로써, RSN 보안 프레임워크를 지원하기 위하여 2002년 3월 802.11i 규격에 새로이 추가된 부분으로써, 2002년 7월 현재 최적의 형태를 구성하기 위해 표준화가 진행중인 부분이다. RSN 보안 협상은 액세스포인트와 단말이 무선의 MAC association을 설정하는 과정에서 진행된다. 협상에 필요한 cipher suite 파라미터들은 (그림 10)에서 보는 바와 같이 RSNIE (RSN Information Element) 구조체로 표현되며, MAC management 프레임(beacon, association request, reassociation request, probe response 프레임)에 포함되어 단말과 액세스포인트 사이에 전달된다.

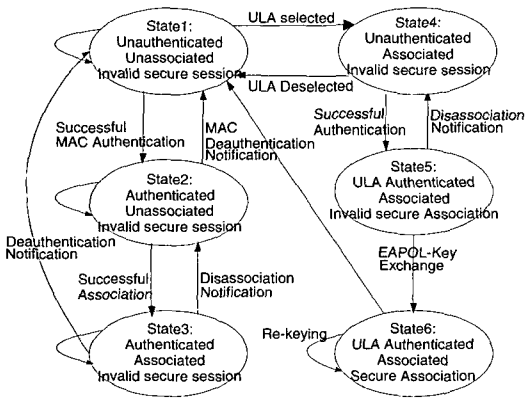
협상 절차는 다음과 같다. RSN을 인지하는 단말이 RSNIE를 포함하는 비콘 프레임을 받으면, 단말이 보안 어소시에이션 맺기를 희망하는 cipher suite의 값을 선택한다. 단말이 선택한 cipher suite는

(예를 들면 unicast 암호 알고리즘: TKIP, multicast 암호 알고리즘: AES, 인증방법: 802.1X) association request 프레임에 실려서 액세스포인트로 전달된다. 액세스포인트는 단말이 요구한 cipher suite에 대한 협상 결과를 association response 프레임을 통하여 알림으로써 단말과 액세스포인트 간의 보안 세션 설정을 개시한다. RSN 협상시 단말이 특별히 원하는 cipher suite를 제시하지 않으면 액세스포인트는 단말이 802.1X 인증 방식과 AES에 의한 데이터 프라이버시 보장을 요구한다고 가정하고 보안 세션 설정을 시작한다.



〔그림 10〕 RSN Beacon 프레임 구조

일단 RSN 보안 협상이 완료되면 단말은 협상된 인증 방식에 따라서 인증을 수행한다. 인증이 완료된 후에, 단말과 액세스포인트는 선택된 암호 알고리즘(WEP, TKIP, AES)을 동작시키는데 필요한 세부 키를 생성하고, 키교환 프로토콜을 이용하여 상호간의 키를 일치 시킴으로써 보안 어소시에이션을 설정한다. 이렇게 형성된 보안 어소시에이션과 cipher suite들은 단말이 액세스포인트 사이를 이동할 때 반드시 전달되어야 하는 기본적인 보안 컨텍스트가 된다. (그림 11)은 기존의 MAC 서비스에 RSN 보안 서비스를 제공할 수 있도록 확장해 본 상태 천이도이다.



〔그림 11〕 RSN 서비스 다이아그램

V. 결론 및 향후 전망

지금까지 본 고에서는 무선LAN의 개인 정보보호 취약점을 보완하기 위해 IETF AAA워킹그룹에서 논의중인 Diameter 인증서버와 IEEE 802 그룹에서 발표한 802.1x와 802.11i를 통한 무선LAN 보안 서비스에 대한 표준화 동향에 대하여 살펴보았다. 이 표준들은 아직까지 확정되지는 않았지만 많은 부분에 있어 의견일치를 이루어가는 상황이고, 무선LAN 서비스의 증가추세를 감안한다면 빠른 시일내에 표준이 확정될 것으로 예상된다.

우리나라의 유선통신 사업자인 KT, 하나로통신, 데이콤 등은 무선LAN을 이용한 초고속 무선인터넷 서비스를 계획하거나 진행중이지만, 아직까지는 무선LAN 보안 표준이 확정된 상태가 아니라 이들 업체에서의 보안서비스는 아직까지는 미미하다. 하지만 추후 사용자의 보안요구사항의 증가와 표준화가 이루어진다면 보안서비스를 제공하는 무선LAN 시장은, 이동성 제약을 극복하기 위해 무선LAN 사업자와 이동통신 사업자의 망사용 제휴를 통한 Mobile-IP 기반의 이동 인터넷 서비스까지 가능하다면 매우 큰 시장으로 형성될 것임은 분명하다. 액세스포인트 공유를 통하여 무선인터넷 사업자간의 글로벌 로밍 서비스가 제공되기 위해서는 분산인증 및 실시간 패킷과금에 대한 요구 또한 더욱 중요시된다. 이와 관련하여 이동통신과 무선이 연동되는 이동 인터넷 환경에 적합한 Diameter 인증서버 및 과금서버 기술은 매우 중요하다.

IETF Mobile IP 워킹그룹에서는 무선에서 빠른 핸드오프 지원를 위한 기술 표준화 논의를 활발하게 진행하고 있고, 802.11i와 802.11f에서는 무선의 공중망 적용에 필수 선결 과제인 안전한 무선망 보장을 위한 RSN 구성 및 동일한 서브넷에 위치한 액세스포인트들 간의 이동시 제공해야 할 로밍, 마이크로 이동 보안에 대한 표준화 논의를 진행하고 있다. 본 논문에서는 기술하지 않은 무선 로밍 및 이동보안, 그리고 무선 Ad-Hoc 보안 이슈와 인증/과금 서버와의 메시지 교환에 대한 지속적인 연구가 필요하다.

참고문헌

[1] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.

[2] IEEE Std 802.11i/D2.0, "Specification for Enhanced Security," July 2002

[3] IEEE Std 802.1X, "Port Based Network Access Control." June 2001

[4] IEEE Draft P802.1aa/D3, "Port Based Network Access Control - Amendment1: Technical and Editorial Corrections", July 2002

[5] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," 1999.

[6] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes," University of Maryland, Mar. 2001.

[7] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June 2000.

[8] C. Finscth, "An Access Control Protocol, Sometimes Called TACACS," IETF RFC 1492, July 1993.

[9] "http://www.interlinknetworks.com/references/Introduction_to_Diameter.html", Feb. 2002.

[10] P. Calhoun, J. Arkko, E. Guttman, G. Zorn, J. Loughney, "Diameter Base Protocol," draft-ietf-aaa-diameter-12.txt, IETF work in progress, July. 2002.

[11] P. Calhoun, Alan C. Rubens, J. Haag, G. Zorn, "Diameter NASREQ Application," draft-ietf-aaa-diameter-nasreq-09.txt, IETF work in progress, Mar. 2002.

[12] P. Calhoun, T. Johansson, C. Perkins, "Diameter Mobile IPv4 Application," draft-ietf-aaa-diameter-mobileip-09.txt, IETF work in progress, Mar. 2002.

[13] P. Calhoun, S. Farrell, W. Bulley, "draft-ietf-aaa-diameter-cms-sec-04," IETF work in progress, Mar. 2002

[14] B. Aboba, M. Beadles, "the Network Access Identifier," IETF RFC 2486, Jan. 1999.

[15] P. Calhoun, C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4 ,"IETF RFC 2794, Mar. 2000.

[16] http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-040.zip

[17] EAP Group Letter L. Blunk et al., "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, Mar. 1998.

[18] D. Potter et al., "PPP EAP MS-CHAP-V2 Authentication Protocol," http://www.rfc-editor.org/internet-drafts/draft-dpotter-pppext-eap-mschap-01.txt, Jan. 2002.

[19] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol," IETF RFC 2716,

[20] P. Funk et al., "EAP Tunneled TLS Authentication Protocol," http://www.potaroo.net/ietf/ids/draft-ietf-pppext-eap-ttls-01.txt, Feb. 2002.

[21] J. Arkko et al., "EAP AKA Authentication," http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-03.txt, Feb. 2002.

[22] IEEE Std 802.11f/D3, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," Jan. 2002.

〈著者紹介〉

김 신 효 (Sinhyo Kim)

1990년 : 전남대학교 전산학과 (이학사)

2000년 : 충남대학교 컴퓨터과학과 (이학석사)

1990년~현재 : 한국전자통신연구

원 무선인터넷보안연구팀 선임연구원
관심분야 : 무선LAN 정보보호, CAS, AAA보안, 보안 프로토콜

강 유 성 (Yu-Sung Kang)
1997년 : 전남대학교 전자공학과 (공학사)
1999년 : 전남대학교 전자공학과 (공학석사)
1999년~현재 : 한국전자통신연구원 무선인터넷보안연구팀 연구원
관심분야 : 무선인터넷 보안, 스마트카드, 보안 프로토콜

정 병 호 (Byong-Ho Chung)
1988년 : 전남대학교 컴퓨터과학과 (이학사)
2000년 : 충남대학교 컴퓨터과학과 (이학석사)
2001년~현재 : 충남대학교 컴퓨터과학과(박사과정)
1988년~2001년 : 국방과학연구소 선임연구원
2001년~현재 : 한국전자통신연구원 무선인터넷보안연구팀장
관심분야 : 무선인터넷 보안, 이동인터넷, 네트워크 보안

조 현 숙 (Kyun-Sook Jo)
종신회원
1979년 : 전남대학교 수학과(이학사)
1991년 : 충북대학교 대학원 전자계산학과(이학석사)
2001년 : 충북대학교 대학원 전자계산학과 (이학박사)
1982년~현재 : 한국전자통신연구원 정보보호기술연구본부 본부장 역임, 국책연구개발사업단 책임연구원
관심분야 : CAS, 이동인터넷보안, 네트워크 보안

정 교 일 (Kyo-il Chung)
정회원
본호의 "ITU SPU 정보보호 워크샵 보고" 저자 소개 참조.