Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.165

프록시 모바일 네트워크를 위한 계층적 인증 기법*

김 경 준,[1†] 백 재 종,[2] 송 주 석[1‡]
[1]연세대학교, [2]대한민국 해군

A Hierarchical Authentication for Proxy Mobile IPv6 Networks*

KyungJoon Kim,[1†] JaeJong Baek,[2] JooSeok Song[1‡]
[1]Yonsei University, [2]Republic of Korean Navy

요 약

본 연구에서는 프록시 모바일 IPv6 환경에서의 인증 지연시간을 최소화하기 위하여 계층적인 인증 기법을 제시한다. AAA 서버의 인증 기능을 LMA와 MAG에 분산하여 해당 LMA 또는 MAG가 모바일 노드에 관한 정보를 가지고 있는 경우 AAA 서버를 거치지 않고 빠르게 인증을 하여 인증 지연 시간을 줄일 수 있는 기법을 제시한다. AAA 서버는 인증을 위한 모든 것을 담당하고 있기 때문에 AAA 서버에 서비스 거부 공격 등으로 인한 단일 고장점 문제가 발생할 경우 모바일 노드는 더 이상 프록시 모바일 IPv6 네트워크에 접속할 수 없는 문제가 발생한다. LMA와 MAG에 인증 기능을 분산함으로써 이러한 단일 고장점 문제에 대응하고 보다 가까운 네트워크 장비에서 보다 가벼운 인증을 수행함으로써 인증 지연시간을 줄일 수 있다.

ABSTRACT

In this paper, a hierarchical authentication protocol is proposed to minimize authentication delay in proxy mobile IPv6 networks. The authentication function of the AAA server is distributed to the LMAs and the MAGs. If the LMAs or the MAGs have authentication information of the MNs, they authenticate the MN on behalf of the AAA servers. Therefore, the authentication delay is reduced. The AAA server is vulnerable to denial-of-service attack. If the AAA server is down, MNs cannot access the proxy mobile IPv6 network until they are authenticated. The proposed scheme reduces the load on the AAA server by distributing the authentication function to the LMAs and the MAGs.

Keywords: PMIPv6, EAP-AKA, Authentication, Key agreement

I. 서 론

국제 인터넷 표준화 기구 (IETF)에서 표준화된 모바일 IPv6 (mobile IPv6) 프로토콜[1]은 모바일 노드가 위치에 구애받지 않고 통신을 하기 위해 제시되었다. 하지만 모바일 단말에서 모바일 IPv6 기능을 수행함으로 인하여 단말의 계산 자원과 배터리를 소모하고 시그널링(signaling) 메시지가 무선 링크를 통해서 전달이 되어 무선 링크의 자원을 소모하는 단점이 있다. 이러한 문제점을 보완하기 위하여 프록시 모바일 IPv6 (proxy mobile IPv6) 프로토콜[2]이 제시되었다. 프록시 모바일 IPv6 프로토콜에서는 모

접수일(2013년 12월 11일), 수정일(2013년 12월 16일), 게재확정일(2013년 12월 16일)
* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2012R1A1B3004161)
* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2012R1A1B3004161)
† 주저자, theboy@emerald.yonsei.ac.kr
‡ 교신저자, jssong@emerald.yonsei.ac.kr (Corresponding author)

바일 노드가 모바일 IPv6 기능이 없더라도 프록시 모바일 IPv6 네트워크에서 단말의 이동성을 관리해서 위치에 상관없이 모바일 단말이 네트워크에 접속을 유지할 수 있도록 한다.

프록시 모바일 IPv6 네트워크에서의 단말 인증은 AAA(Authentication・Authorization・Accounting) 서버가 수행한다. AAA 서버는 EAP-AKA' 프로토콜[3]을 통해서 모바일 단말을 인증한다. 단말이 인증을 받기 전에는 EAP-AKA' 프로토콜 이외의 메시지는 보낼 수 없다. 따라서 이동 단말의 핸드오버 지연시간을 최소화하기 위해서는 인증 지연 시간 단축이 필수적이다. 또한, 인증・인가・과금 서버가 고장이나 분산 서비스 거부 공격(distributed denial-of-service attack)을 받아서 인증이 불가능한 경우, 단말은 더 이상 인증을 받지 못하고 프록시 모바일 네트워크에 접속할 수 없게 된다. 본 논문에서는 AAA 서버의 인증 기능을 프록시 모바일 네트워크에 분산시켜서 AAA 서버 장애시 대처하고 인증 지연 시간도 줄일 수 있는 인증 기법을 제시하고자 한다.

II. 관련 연구

프록시 모바일 네트워크는 MAG(Mobile Access Gateway)와 LMA(Local Mobility Anchor)로 구성되어있다. MAG는 모바일 노드 대신 모바일 노드의 이동성을 관리하며 LMA는 프록시 모바일 IP 도메인 내에서 홈 에이전트 역할을 한다. MAG는 모바일 노드가 자신의 네트워크에 들어오게 되면 인증을 시작한다. 모바일 노드가 인증을 통과하면 MAG는 모바일 노드 대신 LMA에 바인딩 업데이트 (binding update) 메시지를 보내고 LMA와 MAG 사이에 양방향 터널이 형성된다. MAG는 모바일 노드에 router advertisement 메시지와 모바일 노드가 사용할 보조 주소 (care-of address)를 보내면 모바일 노드는 모바일 IPv6 기능이 구현되지 않은 모바일 노드도 이동성을 제공받을 수 있게 된다.

이러한 프록시 모바일 IPv6 기능은 3GPP(3rd Generation Partnership Project) 네트워크에서 비 3GPP 네트워크와의 연동에 사용된다. 이때 모바일 노드의 인증은 EAP-AKA' 프로토콜을 이용해 이루어진다. EAP-AKA'은 EAP-AKA의 향상된 버전으로 SHA-1 대신 SHA-256을 사용하여 보안성을 강화하였다. EAP-AKA' 프로토콜은 EAP-AKA 프로토콜과 동일하게 인증 지연시간 단축을 위하여 빠른 인증 모드를 제공한다. 재인증 시에 이전에 사용한 일부 키를 재사용함으로써 지연 시간을 단축할 수 있다. 하지만 여전히 인증에 AAA 서버의 개입이 필요하다.

Kim 등[4]은 디피-헬만 기반의 프록시 네트워크 인증 기법을 제시하였다. 하지만 공개키 방식의 특성상 단말이 복잡한 연산을 수행해야 하는 단점이 있다.

Chen 등[5]은 Relay 키를 도입하여 수신 신호의 세기를 이용 새로운 기지국으로의 패킷 전달을 통하여 핸드오버 지연시간을 줄이려는 시도를 하였다. 하지만 단말의 핸드오버 예측이 빗나갈 경우 문제가 발생하게 된다.

III. 제안 기법

본 연구에서는 EAP-AKA'을 기반으로 프록시 모바일 네트워크의 계층적 인증 기법을 제시한다. EAP-AKA'에서 생성되는 키 중 확장 마스터 키(EMSK)는 여분의 키로 다양한 목적을 위하여 사용될 수 있다[3,6]. 이 확장 마스터키를 이용하여 LMA와 MAG에서 사용할 보조키를 생성하여 AAA 서버를 거치지 않고 인증과 키 분배가 가능한 경우 LMA 또는 MAG가 인증을 수행할 수 있도록 한다. Fig.1.은 제안 프로토콜을 보여주고 있다.

3.1 초기 인증 (AAA 서버에 의한 인증)

AP(Access Point)에서는 주기적으로 EAP-Request/Identity 메시지를 보낸다. 모바일 노드는 이 메시지를 수신하고 EAP-Response/Identity 메시지를 통해 사용자의 식별번호 NAI(Network Access Identifier)를 제공한다. AP, MAG, LMA는 먼저 자신이 해당 NAI에 대한 인증 정보를 가지고 있는지 검색하여 없는 경우에는 상위 개체에 넘기게 된다. 초기 인증 시에는 AP, MAG, LMA는 해당 정보를 가지고 있지 않기 때문에 AAA 서버에 전달된다. AAA 서버는 EAP-AKA'을 통하여 모바일 노드의 인증을 수행한다.

AAA 서버는 EAP-AKA' 알고리즘을 통하여 AV(Authentication Vector)를 생성한다. AV는 다양한 값으로 구성되는데 AT_RAND는 서버가 생성한 난수($RAND_{AAA}$), AT_AUTH는 키 생성 방법, AT_KDF_INPUT은 네트워크 이름, AT_MAC은 EAP메시지의 무결성을 보장하기 위한 메시지 인

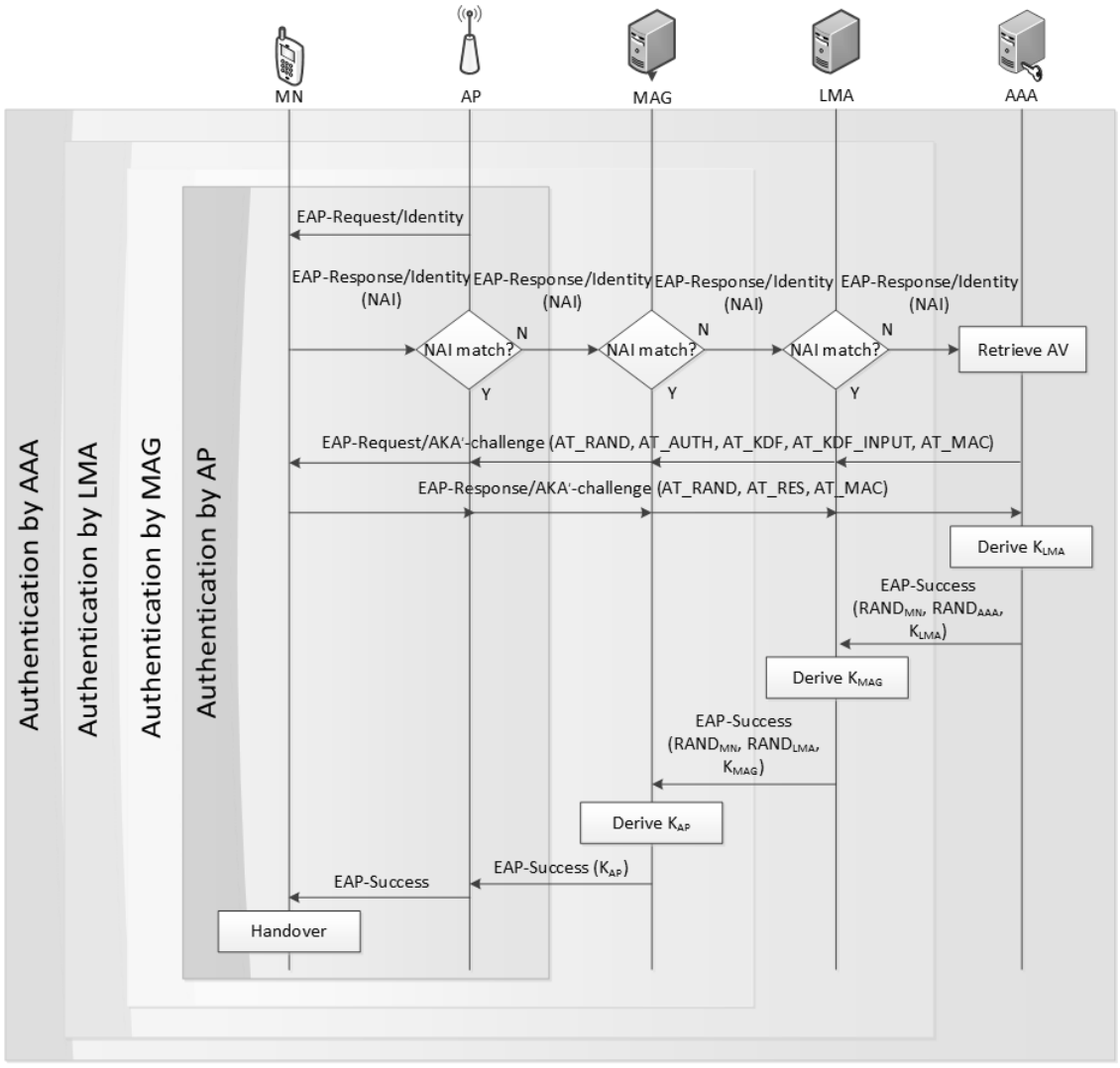

Fig.1. The hierarchical authentication procedure

증 코드이다. 해당 정보들은 EAP-Request /AKA'-Challenge 메시지를 통해 AV를 단말에 전달한다. 단말은 AAA가 생성한 AV를 같은 방식으로 생성하여 AT_MAC를 통해 무결성을 검증하고 AAA 서버가 제시한 도전(challenge)에 대한 응답(response)으로 AT_RES를 생성하고 메시지 인증 코드를 생성하여 EAP-Response/AKA'-Challenge 메시지를 통하여 AAA 서버에 전달한다. 이때 재전송 공격(replay attack)에 대한 보안성 향상을 위하여 추가적으로 단말이 생성한 난수($RAND_{MN}$)를 AT_RAND으로 전달한다. AAA 서버는 AT_MAC을 검사하여 무결성을 검증하고 AT_RES 값을 검증함으로써 단말을 인증한다.

인증이 완료되면 AAA서버는 LMA를 위한 보조키(K_{LMA})를 확장 마스터키로부터 다음과 같이 생성한다.

$$K_{LMA} = PRF(EMSK[0\text{-}255], \text{“KLMA\0”} | LMAID | NAI | RAND_{AAA} | RAND_{MN}).$$

PRF는 EAP-AKA'에서 사용되는 SHA-256함수이다. PRF(K, S)는 SHA-256 함수에 문자열 S를 키 K를 사용한 해쉬 함수 결과이다. 이때 확장 마스터키 중 처음 256비트가 키로 사용된다. LMAID는 LMA의 식별번호이다. 본 논문에서는 AT_KDF_INPUT 항목에 LMAID를 추가함으로써 단말이 이 정보를 획

득할 수 있다고 가정한다. Network Access Identifier (NAI)는 사용자의 고유번호이다. $RAND_{AAA}$는 AAA가 생성하여 EAP-Requst/AKA'-Challenge 메시지를 통해 전달된 난수이다. $RAND_{MN}$는 단말이 생성한 난수로 EAP-Response/AKA'- Challenge 메시지에 포함된 것과 같은 값이다. 이렇게 생성된 K_{LMA}는 단말과 AAA 서버가 생성한 난수와 함께 EAP-Success 메시지를 통해 LMA에 전달된다. LMA는 K_{LMA}로부터 MAG를 위한 보조키 K_{MAG}를 다음과 같이 생성한다.

K_{MAG} = PRF(K_{LMA},"KMAG\0"|MAGID| NAI|$RAND_{AAA}$|$RAND_{MN}$).

MAGID는 MAG의 식별자로 마찬가지로 AT_KDF_INPUT을 통해 단말에 전달한다. MAG에서 새로운 난수를 생성하지 않고 AAA 서버가 생성한 값을 재사용하는 이유는 인증 지연시간을 줄이고 통신비용을 절약하기 위해서이다. 만약 LMA가 새로운 난수를 생성하여 K_{MAG}를 생성할 경우 상위 키와 AAA가 생성한 난수가 노출되더라도 LMA가 생성한 난수를 모를 경우 K_{MAG}를 알 수 없지만 난수가 평문으로 전달되기 때문에 보안성을 높여준다고는 볼 수 없다. 또한 LMA가 생성한 난수를 별도로 단말에 전달해야 되기 때문에 이에 대한 통신비용이 추가로 발생한다.

이렇게 생성된 K_{MAG}는 EAP-Success 메시지를 통하여 MAG에 전달된다. MAG는 이를 바탕으로 AP와 이동 단말 사이에 사용될 세션키 K_{AP}를 다음과 같이 생성한다.

K_{AP} = PRF(K_{MAG},"KAP\0"|APID| NAI|$RAND_{AAA}$|$RAND_{MN}$).

이때 APID는 AP 식별번호로 MAC (Media Access Control) 주소 등이 사용될 수 있다. 이렇게 생성된 KAP는 EAP-Success 메시지를 통하여 AP에 전달된다. 단말은 같은 방식으로 순차적으로 K_{LMA}, K_{MAG}, K_{AP}를 생성하고 AP와의 통신에서 세션키로 KAP를 사용한다. 이러한 과정을 통하여 인증과 키 분배가 완료된다.

3.2 AP에 의한 인증

프록시 모바일 IP 네트워크는 주기적으로 단말의 인증을 수행한다. 또한 단말이 잠시 전원이 꺼지는 등의 이유로 원래 접속했던 AP에 재접속을 시도하는 경우도 발생한다. 이 경우 AP가 이미 단말의 인증 정보를 가지고 있기에 AP에서 재인증이 수행된다. 이 때 AT_KDF_INPUT 값으로 APID가 있는 경우 단말은 AP에 의한 재인증임을 감지할 수 있다. 또한 그리고 AP가 생성한 난수가 AT_RAND로 전달된다. 단말과 AP는 서로 공유한 K_{AP}를 이용하여 AT_RES로 전달할 RES를 다음과 같이 생성한다.

RES = f2(K_{AP}, $RAND_{AP}$)

f2는 EAP-AKA'에서 RES 생성을 위해 사용하는 함수이다. AP는 AT_RES값을 확인하여 인증을 수행한다. 본 연구에서는 EAP-AKA' 프로토콜과의 통일성을 위해서 RES 생성에 f2를 사용한다. KAP는 f5 함수를 통하여 무결성 검사를 위한 AT_MAC 생성에도 사용된다.

3.3 MAG내부 핸드오버 인증

단말이 동일한 MAG에 속한 다른 AP로 핸드오버를 수행한 경우 AP가 단말의 인증 정보를 가지고 있지 않지만 MAG가 인증정보를 가지고 있다. 이 경우 MAG가 인증을 수행한다. RES 값을 다음과 같이 생성하여 인증을 수행한다.

RES = f2(K_{MAG},$RAND_{MAG}$).

AP가 사용할 키는 보조키 KAP는 다음과 같이 생성되어서 AP에 전달이 된다.

K_{AP} = PRF(K_{MAG},"KAP\0"|APID| NAI|$RAND_{MAG}$|$RAND_{MN}$).

3.4 LMA내부 핸드오버 인증

단말이 동일 LMA내 다른 AP로 이동한 경우 LMA가 인증을 수행한다. 이때 RES는 다음과 같이 생성된다.

RES = f2(K_{LMA},$RAND_{LMA}$).

RES가 일치하는 경우 인증이 완료되고 MAG를 위한 보조키가 다음과 같이 생성된다.

K_{MAG} = PRF(K_{LMA},"K_{MAG}\0"|MAGID| NAI|$RAND_{LMA}$|$RAND_{MN}$).

MAG는 이를 바탕으로 AP를 위한 보조키를 다음과 같이 생성한다.

K_{AP} = PRF(K_{MAG},"KAP\0"|APID| NAI|$RAND_{LMA}$|$RAND_{MN}$).

IV. 보안성 분석

Table 1.은 EAP-AKA'와 제안 기법의 보안성을 비교하고 있다. EAP-AKA'에서 재전송 공격은 서버에서 생성한 난수와 서버와 단말 사이에 공유한 일련번호(Sequence number)에 의하여 보호된다. 하지만 일련번호의 경우 완전히 일치하지 않더라도 허용범위에 들어오는 경우 인증이 진행된다. 따라서 서버에서 보낸 EAP-Request/AKA'-challenge 메시지를 재전송 하는 경우 단말은 일련번호의 범위에 들어오는 경우 인증을 진행하는 문제가 발생한다. 제안 기법에서는 단말에서도 난수를 발생시켜 인증을 수행하기 때문에 재전송 공격에 보다 강하다고 할 수 있다.

EAP-AKA'에서는 AAA서버와 단말이 가지고 있는 일련번호가 허용범위를 벗어난 경우 동기화가 필요하다. 하지만 제안 기법에서는 일련번호의 동기화는 초기의 AAA서버에 의한 인증에서만 요구된다. 보조키의 생성에서 일련번호를 사용하지 않기 때문에 동기화를 요구하지 않는다.

제안된 기법에서는 LMA 또는 MAG에서 인증이 수행되기 때문에 보다 인증 지연시간이 감소된다.

표준 문서[7] 에서는 서비스 거부 공격을 고려하여 시스템을 설계할 것을 권고하고 있다. 이에 대한 하나의 해법으로 본 논문에서와 같이 MAG와 LMA에서 인증 기능의 분산을 통해 서비스 거부 공격에 대응할 수 있다.

Table 1. Security analysis

	EAP-AKA'	Proposed scheme
Prevention of replay attack	△	O
Requirement of synchronization	O	△
Localized authentication	X	O
Prevention of Denial-of-service Attack	X	△

V. 비용 분석

Table 2.는 EAP-AKA'과 제안 기법의 인증 비용을 분석한 표이다. EAP-AKA'은 빠른 재인증을 제공하고 있다. EAP-AKA' 빠른 재인증에서는 일부키를 재사용함으로써 인증 비용이 조금 줄어드는 효과가 있다. EAP-AKA'에서는 인증 메시지가 AAA와 단말 사이에서 교환되지만 제안 기법에서는 단말에서 조금 더 가까운 네트워크 장비에서 인증이 이루어지기 때문에 지연 시간이 짧다. 또한 인증 프로토콜 자체도 EAP-AKA' 보다 가벼운 것을 볼 수 있다. 하지만 이를 위해서는 단말에서 추가적인 보조키를 유지하여 함으로 이를 위한 메모리 비용이 발생한다.

VI. 결 론

본 연구에서는 프록시 모바일 네트워크에서의 인증 기능을 LMA와 MAG에 분산함으로써 빠른 인증을 통해 인증 지연시간을 줄이고 인증 절차를 간략히 하여 단말에서 연산을 줄였다. 또한 단말에 의한 추가 난수 생성을 통해 재전송 공격에 대한 보안성을 강화하였고 인증 트래픽의 분산을 통한 서비스 거부 공격에도 대응할 수 있도록 하였다. 하지만 이를 위해서는 LMA와 MAG에 인증 기능이 필요하고 단말은 추가

Table 2. Performance analysis

Cost	EAP-AKA' full authentication	EAP-AKA' fast re-authentication	Inter-AP handover	Inter-MAG handover	Inter-LMA handover
Communication cost	$5H_{MN-AAA} \times d$	$5H_{MN-AAA} \times d$	$5H_{MN-AP} \times d$	$5H_{MN-MAG} \times d$	$5H_{MN-LMA} \times d$
MN calculation	12h	9h	2h	3h	4h
Network entity calculation	12h	9h	2h	3h	4h

h : hash operation
d : transfer delay in one hop
H_{MN-AAA}: the hop count between MN and AAA server
H_{MN-LMA}: the hop count between MN and LMA
H_{MN-MAG}: the hop count between MN and MAG

적인 키를 위한 메모리가 필요하다. 또한 계층적인 키 생성으로 인하여 상위 키가 노출 될 경우 하위 키도 모두 노출될 수 있기에 신중한 키 관리가 요구된다.

References

〔1〕 C. Perkins, D. Johnson, and J. Arkko, "Mobility support in IPv6," IETF RFC: 6275, Jul. 2011.

〔2〕 S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," RFC 5213 Aug. 2008.

〔3〕 J. Arkko, V. Lehtovirta, and P. Eronen, "Improved extensible authentication protocol method for 3rd generation authentication and key agreement," RFC 5448, May 2009.

〔4〕 H. Kim and J. Lee, "Diffie-Hellman key based authentication in proxy mobile IPv6," Mobile Information Systems, pp. 107-121, Jan. 2010

〔5〕 Y. Chen, T. Juang, and Y. Lin, "A secure relay-Assisted handover protocol for proxy mobile IPv6 in 3GPP LTE systems," Wireless Pers Communications, pp. 629-656, Dec. 2011

〔6〕 J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," RFC 5247, Aug. 2008.

〔7〕 J. Arkko and H. Haverinen, "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," RFC 4187, Jan. 2006.

〈저 자 소 개〉

김 경 준 (KyungJoon Kim) 학생회원
2005년 8월: 연세대학교 컴퓨터산업공학과 졸업
2005년 9월~현재: 연세대학교 컴퓨터과학과 석박사통합과정
〈관심분야〉 정보보호, 이동성 관리

백 재 종 (JaeJong Baek) 종신회원
1996년 2월: 한밭대학교 전자계산학과 졸업
2001년 2월: 연세대학교 컴퓨터과학과 석사
2011년 8월: 연세대학교 컴퓨터과학과 박사
〈관심분야〉 인증, 스마트폰 보안, MIP 보안, 역공학, 정보전

송 주 석 (JooSeok Song) 종신회원
1976년 2월: 서울대학교 전기공학과 졸업
1979년 2월: 한국과학기술원 전기전자공학과 석사
1988년 2월: University of California at Berkeley 컴퓨터과학과 박사
1988년~1989년: 미국 Naval Postgraduate School 조교수
1989년 3월~현재: 연세대학교 컴퓨터과학과, 정교수
2006년 한국정보보호학회 회장 역임
〈관심분야〉 정보보호, 유무선통신 등