
WPKI 기반 Kerberos 인증 메커니즘 설계

이철승* · 박찬모** · 이호영*** · 이준****

Design of Kerberos Authentication Mechanism based on WPKI

Cheol-seung Lee* · Chan-mo Park** · Ho-young Lee*** · Joon Lee****

요 약

본 논문은 WPKI 환경에서 Kerberos V5 인증 프로토콜을 이용한 사용자 인증 문제를 해결하고자 한다. WAP Forum에서 정의한 보안구조 및 요소, 기존 인증 시스템과 관련된 각종 암호 기술을 살펴본 후, 무선 공개키 기반 구조와 전송 계층 보안등을 이용하여 응용 계층에서의 사용자 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 E2E 보안상 취약점을 찾아 대안을 제공한다. 인증 프로토콜인 Kerberos V5와 그 단점을 보완 할 수 있는 무선용 X.509 V3을 결합한 후, 보안성이 우수한 WIM을 인증서 저장 매체로 활용한 올바른 인증 방법 해결책을 제시하고자 한다.

ABSTRACT

In this paper we challenge the user Authentication using Kerberos V5 authentication protocol in WPKI environment. this paper is the security structure that defined in a WAP forum and security and watches all kinds of password related technology related to the existing authentication system. It looks up weakness point on security with a problem on the design that uses wireless public key-based structure and transmission hierarchical security back of a WAP forum, and a server-client holds for user authentication of an application level all and all, and it provides one counterproposal. Therefore, We offer authentication way solution that connected X.509 V3 with using WIM for complement an authentication protocol Kerberos V5 and its disadvantages.

키워드

WPKI, Authentication, Kerberos V5, X.509 V3

1. 서 론

무선 인터넷 기술이 가속화되면서 유선상에서 제공받았던 멀티 콘텐츠들을 무선상에서 제공받을 수 있게 되었지만, 정보의 공유와 개방화를 목표로 개발된 인터넷의 기본적인 취약성, 열악한 무선 네트워크 환경과 무선 단말기의 제약성 때문에 유선상의 멀티 콘텐츠를 그대로 수용할 수 없

는 문제가 발생하게 되었다. 이에 WAP(Wireless Application Protocol) Forum은 무선 인터넷의 기본적 취약점을 극복하고 효율적인 무선 네트워크 자원을 사용할 수 있도록 프로토콜을 정의하였다.

그러나 WAP구조는 WTLS(Wireless Transport Layer Security)구간과 SSL(Secure Socket Layer)구간의 프로토콜 변화를 수행할 게이트웨

*조선대학교 대학원 컴퓨터공학과

**초당대학교 정보통신공학과

접수일자 : 2003. 7. 23

**광주 과학기술원 Post Doc.

****조선대학교 전자정보 공과대학 컴퓨터공학부

이에서 E2E(End to End)보안의 취약점을 지남으로써, 실제 보안이 필요한 여러 응용 계층에서 WAP을 적용하기 힘들게 되어, WAP을 채택한 무선 인터넷 인프라스트럭처에 커다란 문제점으로 지적되고 있다.

본 논문은 기존 인증 시스템과 관련된 각종 암호 관련 기술을 살펴본 후 WAP Forum의 무선 공개키 기반 구조와 전송 계층 보안을 이용하여 응용 계층에서의 사용자 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 E2E 보안상 취약점을 찾아 대안을 제공한다.

인증 프로토콜로는 Kerberos V5[1]와 그 단점을 보완할 수 있는, X.509 V3을 결합한 후 보안성이 우수한 WIM(Wireless Identifier Module)[2]을 인증서 저장 매체로 활용한 올바른 인증 방법 해결책으로 “KXWTestRootCA”를 제시한다.

II. 인증 시스템 기반 기술

2.1 WIM

WIM은 ISO/IEC7816과 PKCS#15기반 스마트카드 규격으로 설계됐다. 또한 WAP기반에 사용할 수 있는 스마트카드의 규격 외에 무선 단말기와 스마트카드간의 인터페이스를 갖춘 인증·보안 모듈이며, WPKI(Wireless Public Key Infrastructure)와 전자서명 기능을 담고 있어, 유선 상의 PKI(Public Key Infrastructure)와 동급의 기밀성, 무결성, 거래 안정성을 유지하면서도 무선 방식의 편리함을 누릴 수 있다. 또한 전송 계층 보안을 위한 WTLS 핸드셰이킹과 응용 계층에서의 전자서명을 지원하는 역할을 수행한다.

2.2 Kerberos V5

Kerberos는 중앙집중식으로 하나의 안전한 인증 서버를 두어 사용자들을 인증할 수 있도록 한 인증 서비스이며, 보안 결함을 수정하여 V5가 Internet draft 표준(RFC1510)으로 발표되었다[8].

Kerberos V4는 Ticket을 적용하여 사용 및 시간제한을 통해 인증을 하였으며, Kerberos V5에서는 영역(Realm) 개념을 도입하여 Kerberos 서

버와 다수의 클라이언트, 그리고 다수의 응용 서버로 구성된 완전한 Kerberos환경을 구성하였다. 그리고 Kerberos의 6단계의 인증 절차는 Fig. 1과 같다.

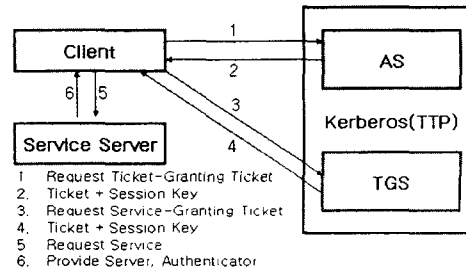


그림 1. Kerberos V5 인증
Fig. 1 Kerberos V5 authentication

2.3 X.509 V3

X.509 V3는 각 사용자와 관계된 공개키 인증서를 말하며, CA(Certificate Authority)에 의해 발행된 인증서는 사용자와 CA에 의해 디렉토리에 위치하고, 인증서에 표현되는 정보는 사용자ID, 사용자 공개키, CA정보, 서명으로 크게 구성된다.

인증서는 CA의 비밀키로 전자서명을 생성하여 첨부하며, 디렉토리 서버는 공개키의 생성이나 인증 기능에 대한 책임이 없으며, 단지 사용자가 인증서를 쉽게 얻을 수 있는 접속 장소를 제공할 뿐이다[3].

2.4 기존 인증 시스템 문제점

무선 인터넷 환경에서 대부분의 인증 프로토콜은 비밀키 기반을 사용하기 때문에 방대한 규모의 네트워크에서 효과적으로 키를 관리하기가 불가능하며, WAP 게이트웨이에서 암호화된 문서를 복호화 한 후 다시 암호화하는 과정에서 정보가 손실되거나 제3자에게 도청 가능성 기회를 제공하게 된다. 이로 인해 WAP Forum의 신뢰성 있는 무선 공개키 암호화 기법 사용에 대한 적합성 여부가 새로운 문제점으로 제시되었으나, 무선 인터넷 환경의 좁은 대역폭, 낮은 전송률 무선 단말기의 열악성 때문에 공개키 암호화 기법은 무선 환경에 맞지 않으며, WML이 HTML과 필터링을 통한 호환이 가능하지만, 현재의 WAP 프로토콜

이 운용되는 곳만 WTLS가 운영되어 웹 서버와 단말기 간 보안 인증은 제공되진 못한다. 또한 네트워크 부하 및 프로토콜 변환을 위한 WAP 게이트웨이 구축에 추가적인 하드·소프트웨어 설치가 불가피 하는 문제점이 발생하였다[6].

이로 인해 무선용 X.509 V3 인증서를 통한 사용자 인증에 대한 연구가 활발히 진행 중에 있지만, X.509 V3 인증서에 전자서명을 하는 곳은 CA이기 때문에 사용자는 반드시 전자서명을 확인하기 위해 CA의 고유 공개키를 가지고 있어야 하며, 사용자의 인증서를 확인하려면, 공개키는 사용자에게 무결성과 인증이 제공되는 어떤 저장 매체를 통해서 분배되어야 하는 문제점이 발생하였다[7].

III. 무선 인터넷 환경의 인증 메커니즘

3.1 KXW 인증 시스템

본 장에서는 WPKI 기반 KXW(Kerberos V5, X509 V3, WIM) 사용자 인증 메커니즘을 설계한다. 기존 인증 시스템 기술 및 인증 시스템의 문제점과 KXW 인증 시스템의 요구 사항과 구성 요소들을 고려한 후, 무선 환경의 적합성 여부를 평가 및 분석을 한다.

기존 유선용 CA솔루션들은 RSA알고리즘을 이용한 인증서를 발급한다. 이를 무선 환경에 적용시 성능 저하로 현실적으로 이용할 수 없다. 그러므로 빠른 Kerberos V5 알고리즘을 이용한 X.509 V3 인증서 발급이 무선 환경의 보안 인프라를 구축하는데 가장 시급한 문제이다.

Kerberos V5는 Realm과 상호작용을 위해 반드시 $[N(N-1)]/2$ 개의 비밀키가 사전에 교환되어야 하며, 이는 키 관리의 문제점을 발생시킨다. 그러나 공개키 방식의 X.509 V3 디렉토리 인증 서비스를 이용하여 외부 영역의 수가 10,000개가 되어도 비밀키를 10,000개만 보유하면 쉽게 해결할 수 있다.

KXW 인증 시스템은 CA에서 인증한 사용자 정보를 무선 인터넷 환경에서 유효기간 내에 직접 인증이 가능하도록 해주며, WIM을 적용한 이유

는 내부 패스워드, 암호키 등을 안전하게 저장할 수 있어 보안성이 우수하고, 대규모 정보 기억에 유용하며, 휴대 및 대중화가 유리하기 때문이다.

KXW 인증 시스템은 WPKI 기반 구조에서 인증 사슬에 의한 외부 영역의 상호 인증 개념을 도입하며, Kerberos V5 인증 프로토콜 절차를 응용하여 사용자가 이용하려는 서비스 서버를 통제하여 서버에 대한 보안성을 강화하였다.

가입자는 인증서를 발급 받기 위해 등록 기관에서 직접 대면을 통한 신원 확인을 하며, 본인 확인을 위한 참조 코드(ID/Password)를 부여받은 후, 전자서명 생성키(Private Key)를 생성한다. 전자서명 검증키와 개인 정보를 담은 인증서 발급 요청 정보를 작성하여 CA로 발급 요청을 한다. CA는 자신의 전자서명 생성키로 가입자의 전자서명 검증키에 대하여 서명함으로써, 가입자 인증서를 생성하여 가입자에게 인증서를 발행하게 된다[4].

3.2 Kerberos v5 와 X.509 V3 결합

3.2.1 접속 및 사용자 인증

사용자는 Kerberos 인증서버(AS)에게 자신의 인증과 원하는 티켓승인서버(TGS)에 관한 메시지를 전송한다. KerberosAS는 사용자 데이터베이스(UserDB)에서 사용자 정보를 검색한 후, 정당한 사용자라면 요청한 TGS가 어느 영역에 있는지를 디렉토리 서버(DirServer)에서 검색하게 된다. 만약 동일한 영역 내에 있는 TGS라면, 타 영역과의 인증 및 외부 영역에 있는 DirServer들의 공개키를 얻는 과정은 필요가 없다.

3.2.2 외부 영역과 디렉토리 연결

사용자가 원하는 TGS가 타 영역에 있을 경우 X.509 V3을 이용한 타 영역까지 경로를 연결하는 과정은 Fig. 2와 같다.

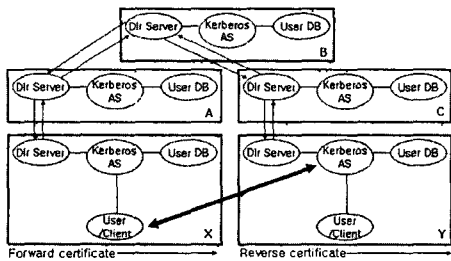


그림 2. 디렉토리간의 인증후 X-Y영역 연결
Fig. 2 X-Y area connection after authentication between directory

많은 Kerberos영역이 있을 경우, 각 영역의 Dir-Server는 단지 연결 설정의 역할만 할 뿐 인증에 관한 제반 사항은 AS에서 전담한다.

X영역에서 Y영역의 공개키(PKY)를 얻고자 할 경우 Y영역의 TGS를 사용하여 전방인증체인을 생성한다.

이와 반대로 Y영역에서 X영역의 공개키(PKX)를 얻고자 할 때는 후방인증체인을 생성한다.

그 후 X영역과 Y영역의 직접적인 연결이 이루어지며, PKY를 X영역에서 알게 되었으므로, X영역의 사용자는 PKY로 자신의ID, 원하는 TGS등을 암호화하여 전송하게 된다[5].

전방인증체인 : A<>B<<C>>C<<Y>>
후방인증체인 : C<>B<<A>>A<<X>>

3.2.3 두영역간 키 교환

X영역과 Y영역간의 연결이 직접적으로 이루어졌으면, 사용자를 인증하는 절차는 Fig. 3과 같다.

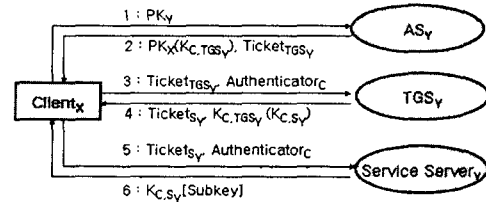
사용자는 Y영역의 인증서버(AS_Y)에게 X.509 V3를 이용하여 얻은 PKY로 사용자 인증 정보를 암호화하여 전송한다.

AS_Y는 자신의 비밀키로 수신된 메시지를 복호화한 다음 다시 Client_X에게 PK_X로 Client_X와 TGS

간 공유하는 세션키(K_{c, TGS_Y})를 암호화하여 전송한다. 이때 Y영역의 TGS 접근 승인 티켓($Ticket_{TGS_Y}$)도 함께 보내는데, 역시 여기에도 세션키 K_{c, TGS_Y} 가 포함되어 있다.

이는 사용자와 Y영역의 TGS에게 은밀한 방법

으로 세션키를 분배하는 방법으로, 이후부터 두 영역간의 공개키를 사용하지 않고, 비밀키로 메시지 인증 교환 단계를 하게 된다. 나머지 과정은 Kerberos V5의 메시지 교환 절차와 같다.



$Ticket_{TGS_Y}$ = Y영역의 티켓 승인 티켓
 $Ticket_{S_Y}$ = Y영역의 서비스 승인 티켓
Authenticator = 클라이언트의 인증자

그림 3. X-Y 영역간 키 교환
Fig. 3 Key exchange between X-Y area

3.2.4 제안 알고리즘

제안한 KXW시스템의 특징은 서버 클라이언트 환경에서 AS 및 TGS를 두어 다단계 인증 서비스를 제공하는 메커니즘이다.

즉, Kerberos V5의 다단계 인증 서비스 장점을 활용하였으며, X.509 V3를 Kerberos V5와 접목하면서 DirServer가 Realm의 역할을 대신하여 영역들의 구분을 해주어 외부 영역과의 상호 연결을 한다.

X.509 V3 디렉토리 인증 표준을 이용하여 인증 서비스 교환 단계에서 패스워드의 평문 전송 없이 상대방 공개키로 암호화 전송하여, AS로부터 도청 및 가로채기 위협이 없는 사용자 인증을 받을 수 있도록 하였다.

WIM의 접목은 제안한 시스템의 보안성을 강화시켰고, WIM을 위조하기 위해서는 CA의 인증서를 위조해야 하기 때문에 안전하다고 할 수 있다.

제안한 인증 시스템은 RSA전자서명 알고리즘과 Kerberos V5 인증 프로토콜, 그리고 X.509 V3 디렉토리 표준 프로토콜을 기본으로 하고 있으며, 사용자와 서버 사이에서 인증 정보가 교환되는 알고리즘은 Table 1.과 같다.

표 1. 제안 알고리즘
Table 1. Proposal algorithm

① $Client_X \Rightarrow AS_X$ $M([Option], ID_C, ID_{TGS_Y}, Times, Nonce1)$
② $AS_X \Rightarrow Client_X$ $M(ID_C, EK_C(PK_Y, Times, Nonce1, ID_{TGS_Y}))$
③ $Client_X \Rightarrow AS_Y$ $M(EPK_Y([Option], ID_C, ID_{TGS_Y}, Times, \sim Nonce2))$
④ $AS_Y \Rightarrow Client_X$ $M(ID_C, Ticket_{TGS_Y}, EPK_X(K_{C,TGS_Y}, Times, \sim Nonce2))$ $Ticket_{TGS_Y} = EK_{TGS_Y}([Flags], K_{C,TGS_Y}, \sim ID_C, AD_C, Times)$
⑤ $Client_X \Rightarrow TGS_Y$ $M([Option], Ticket_{TGS_Y}, Authentication_C, \sim Times, Nonce3, ID_{S_Y})$ $Authentication_C = EK_{C,TGS_Y}(ID_C, TS1)$
⑥ $TGS_Y \Rightarrow Client_X$ $M(ID_C, Ticket_{S_Y}, EK_{C,TGS_Y}(K_{C,S_Y}, Times, \sim Nonce3, ID_{S_Y}))$ $Ticket_{S_Y} = EK_{S_Y}([Flags], K_{C,S_Y}, ID_C, \sim AD_C, Times)$
⑦ $Client_X \Rightarrow Server_Y$ $M([Option], Ticket_{S_Y}, Authentication_C)$ $Authentication_C = EK_{C,S_Y}(ID_C, TS2, \sim [Subkey, Seq#])$
⑧ $Server_Y \Rightarrow Client_X$ $M(EK_{C,S_Y}(TS2, [Subkey, Seq#]))$

IV. 인증 시스템 평가 및 분석

제안 알고리즘을 이용한 KXW 인증 시스템 구성도는 Fig. 4와 같다.

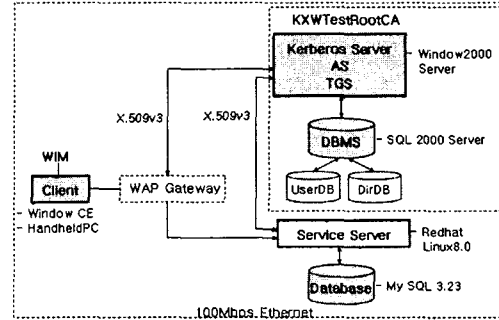


그림 4. 제안 시스템 구성도
Fig. 4 The diagram of proposal system structure

사용자는 인증서 발급을 위해 KXWTestRootCA의 UserDB에 사용자 명칭, 사용자의 전자서명, 인증서 발급에 사용되는 전자서명 방식, 인증서의 일련번호, 인증서 유효 기관, 공인 인증 기관 명칭 등을 저장한 후 KXWTestRootCA로부터 본인 확인을 위한 참조 코드를 부여받는다.

사용자는 KXWTestRootCA와 공유되어 있는 특정 서비스 서버를 이용하기 위해 Window CE HandheldPC를 이용하여 KXWTestRootCA의 AS에게 TGS에 관한 메시지를 전송한다.

AS는 UserDB를 이용하여 정당한 사용자인지를 검색한 후 사용자가 원하는 TGS를 DirDB에서 검색하고, 적법한 사용자라면 X.509 V3 인증서를 전송한다.

사용자는 인증서 저장 매체로 WIM을 선택하고, 인증서 발급을 위해 새로운 암호를 입력한 후 인증서를 발급 받는다. 사용자는 발급 받은 인증서를 이용하여 다른 외부 영역에 있는 서비스 서버를 이용하게 된다.

KXW 인증시스템의 암호화 알고리즘 수행 성능 검증을 위해 HandheldPC의 수행 성능을 Table. 2에 비교하였다.

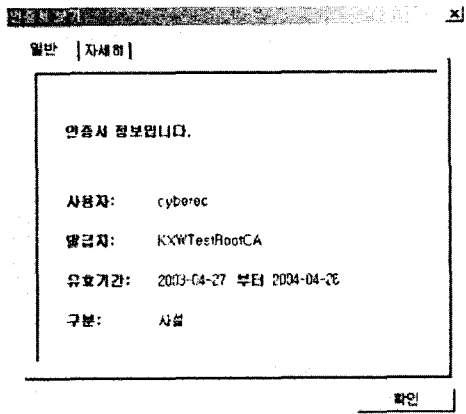


그림 5. KXWTestRootCA의 인증서
Fig. 5 Authentication of KXWTestRootCA

표 2. 암호화 알고리즘 비교
Table. 2 Encryption algorithm comparison

	키생성	서명	검증
RSA-1024bit	5.243	0.253	0.010
ECDSA(ECC)-160bit	0.022	0.022	0.034
KXW-160bit	0.143	0.012	0.023

(단위 : ms)

전자서명에 가장 널리 사용되고 있는 RSA의 경우에는 키 생성시 많은 시간이 소요되며, ECDSA와 KXW는 RSA와 같은 보안 수준을 제공할 때 키의 길이가 작아 키 생성 소요 시간이 짧다는 것을 확인할 수 있었으며, ECDSA 경우 소수 분해와 같은 과정이 필요치 않아 KXW보다 키 생성 시간이 짧다는 것을 확인할 수 있었다. 가장 문제가 되는 검증의 문제는 RSA가 ECDSA나 KXW보다 유리한 것으로 나타났다. 그러나 무선 단말기의 연산 능력을 고려해볼때 RSA는 무선 환경에 적합하지 않으며, 제안한 KXW는 ECDSA보다 서명 및 검증 부분에서 유리한 것을 알 수 있었다.

그리고 KXW 인증 시스템은 방대한 규모의 네트워크에서 키 관리를 용이하게 하여 네트워크의 개방 효과를 예방하였다.

비밀키 암호 방식을 사용하는 기존의 무선 인터넷 환경의 인증은 타 영역과 상호 인증에 있어서 키를 많이 관리해야 했지만, KXW 인증 시스템에서는 세션키를 분배하는데 있어 공개키 암호

화 방식으로 문제를 해결하였다. 그러나 제안 시스템은 공개키 암호 방식을 사용하므로 기존 Kerberos보다 인증 정보를 암호화하여 전송하는 속도가 느리며, X.509 V3에서 필요로 하는 디렉토리 서버, WIM, CA등의 추가적인 비용과 노력이 든다는 단점이 발생하였다.

V. 결론 및 향후 연구 방향

본 논문은 무선 인터넷 환경의 사용자 인증에 대해 분석하고, 기존 인증 시스템에 대한 문제점을 찾아 KXW인증 시스템을 제안하였다.

제안 시스템의 보안을 달성하기 위한 기술적인 방법은 암호기술, 해쉬함수, 전자서명, 키 관리 등과 같은 방법을 사용하였다. 그리고 인증 시스템의 구성 요소로 다단계 인증 서비스를 지원하는 Kerberos V5와 디렉토리 인증 프로토콜인 X.509 V3, 인증서 그리고 무선 단말기의 열악한 환경을 극복하기 위해 자체 연산 능력과 메모리를 보유하고 있는 WIM으로 구성하였다. KXW 인증 시스템은 기존의 Kerberos보다 보안성 및 키 관리의 효율성을 높여 CA와 무선 인터넷 환경의 강력한 인증 체인을 형성하였고, 보다 강화된 인증 서비스를 사용자에게 제공하여, 신뢰성 높은 무선 인터넷 환경에 적합한 인증 시스템을 제안하였다.

향후 연구 방향으로는 무선 인터넷 시장의 성장을 감안하여, 좀더 안전하고, 효율적인 무선 인터넷 환경 구현을 위해 BlueTooth기술을 접목시킨 연구를 통해 보안성 및 효율성이 강화된 강력한 무선 인터넷 환경과, 제안한 인증 시스템에서 발생한 문제점인 암호화 알고리즘 속도 향상을 위해 적절한 암호 알고리즘을 이용한 무선 단말기의 성능 및 속도 향상에 관한 연구가 필요할 것이다.

참고 문헌

- [1] K. Raeburn, "Encryption and Checksum Specifications for kerberos 5.", March 2003.
- [2] WAP Forum, WAP Identity Module Specification, 18 February 2000,

- [3] M.Myers, "X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol-OCSP." Network Working Group, 1999.
- [4] "Wireless Application Protocol Public Key Infrastructures Definition", WAP forum, Feb. 2000
- [5] R.Hously, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile." Network Working Group, RFC2459, January,
- [6] R. Housley and other, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile.", Jan, 1999.
- [7] P.Gutmann, "Internet X.509 Public Key Infrastructure operational protocols.", Internet Draft, <draft-ietf-pkix-certstore-http-05.txt>, 2003.
- [8] S.Hartman, K.Raeburn, "The Kerberos Network Authentication Service v5", Internet-Draft,

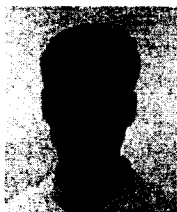
저자 소개



이철승(Cheol-Seung Lee)

2001년 2월 광주대학교 공과대학
컴퓨터학과 졸업(공학사)
2003년 8월 조선대학교 대학원
컴퓨터공학과 졸업(공학석사)

※ 관심분야 : 차세대 인터넷, 임베디드 시스템, 시스템보안, 인증



박찬모(Chan-Mo Park)

1997년 2월 조선대학교 대학원
컴퓨터공학과 졸업(공학석사)
2002년 2월 조선대학교 대학원
컴퓨터공학과 졸업(공학박사)

2002년 9월 - 현재 광주과학기술원 Post Doc.
※ 관심분야 : P2P Network, Overlay Multicast, 분산
객체, 차세대 인터넷, 보안



이호영(Ho-Young Lee)

1988년 2월 조선대학교 전산기
공학과 졸업(공학사)
1995년 2월 조선대학교 대학원
컴퓨터공학과 졸업(공학석사)

2000년 조선대학교 대학원 컴퓨터공학과 졸업
(공학박사)
2002년 - 현재 초당대학교 정보통신공학과 조교수
※ 관심분야 : 객체지향 프로그래밍, 분산 운영체제
컴퓨터 네트워크, 임베디드 시스템



이준(Joon Lee)

1979년 2월 조선대학교 전사
공학과 (공학사)
1981년 2월 조선대학교 대학원
전자공학과 (공학석사)

1997년 2월 숭실대학교 대학원 전자계산학과
(공학박사)
1982년 3월 - 현재 조선대학교 전자정보공과대학
컴퓨터공학부 교수
※ 관심분야 : 시스템 보안, 분산 운영체제, 프로그
래밍 환경