일회성 속성인증서의 바인딩 메커니즘

정회원 박 종 화*, 이 상 하**, 김 동 규***

A Binding Mechanisms Using One-Time Attribute Certificates

Chong-Hwa Park*, Sang-Ha Lee**, Dong-Kyoo Kim*** *Regular Members*

요 약

공개키 기반구조에서 공개키인증서는 신분확인을 위한 인증서로서 인증기관(Certificate Authority : CA)에서 전자적으로 서명되어 진다. 또 속성인증서(Attribute Certificate : AC)는 사용자의 속성 정보를 저장 관리하는 인증서로서 속성인증기관(Attribute Certificate Authority : ACA)에 의해 전자적으로 서명된다. 웹 상의 많은 응용에서 이들이 사용되기 위해서는 속성인증서를 적절한 신분인증서에 결합하는 바인딩 메커니즘이 필요하며, 이 인증서들 간에 종속성이 유지되어야 한다. 본 논문에서 잘 알려진 바인딩 메커니즘인 선택적 철회 방식과 암호적 바인딩 방식을 분석하고, 위의 방식들이 갖고 있는 문제점을 해결하기 위한 하나의 대안으로 일회성 속성인증서를 사용하는 새로운 방식을 제안한다.

Key Words : Attribute Certificates; dependencies; Binding Mechanism; Authorization

ABSTRACT

An ID certificate is digitally signed by a certificate authority for authentication and an attribute certificate is digitally signed by an attribute certificate authority for authorization. In many applications in web, there should be a mechanism to bind attributes to proper identities. The dependencies between them should be maintained. So we analyzed some known binding methods, selective revocation methods and cryptographic binding methods. And we proposed a binding mechanism using one-time attribute certificates in order to solve their problems.

I. 서 론

최근 인터넷의 급격한 성장에 따라 전자상거래는 기존의 상거래를 보안하거나 대체하면서 급속한 성장을 보이고 있다. 그러나 인터넷은 공개 네트워크(Open Network)라는 특성으로 인해 정보의 변조, 위조, 누설 등의 위협에 노출되어 있다. 따라서 인터넷상의 정보보호는 전자상거래의 활성화를 위해 필수적인 요소로 자리잡고 있다. 이러한 정보보호를 제공하기 위해 많은 연구가 진행되고 있으며, 특히 최근에는 사용자에 대한 인증 정보를 제공하는 PKI (Public Key Infrastructure)[1]에 대한 연구 및 개발이 활발히 진행되고 있다.

PKI는 사용자에 대한 공개키 소유여부에 대한 인증 정보를 제공하며 정보에 대한 인증(Authentication), 무결성(Integrity), 비밀성(Confidentiality), 부인방지(Non-repudiation) 기능의 제공을 통하여 정보보호 기반구조로 활용되고 있다. 그러나 일반 응용 환경에서는 이와 같은 정보보호 기능뿐만 아니라 사용자에 대한 권한관리를 요구한다. 즉, 일반적으로 전자상거래에서 사용자가 어떤 물품을 주문했을 때, 서버 시스템에서 물품을 배달할 것인지 결정하는 과정은 물품을 주문한 사용자에 대한 신분확

* 세명대학교 소프트웨어학과(chpark@semyung.ac.kr), ** 동서울대학 정보통신과(shyi@dsc.ac.kr)
*** 아주대학교 정보 및 컴퓨터공학부(dkkim@ajou.ac.kr)
논문번호 : 030270-0624, 접수일자 : 2003년 6월 24일

인을 수행하는 인증 정보뿐만 아니라 사용자가 주문한 물품의 대금을 지불할 능력이 있는지를 확인하는 인가(Authorization)정보가 매우 중요하다. 따라서, 물품을 구입하기 위해서는 두 가지의 정보, 즉, 인증정보와 이와 연관된 인가정보가 물품을 배달할 응용 서버 시스템에 제공되어야 한다.

초기에 사용자의 권한과 같은 인가정보는 인증정보와 함께 공개키인증서(Public Key Certificate : PKC)를 통해 제공하려는 연구가 수행되었다. 그러나 공개키에 대한 발급주체가 사용자의 속성을 발급하는 주체와 다르고 공개키의 유효기간과 사용자 속성의 유효기간이 서로 다르기 때문에 실제 활용되지 못하고 있다. 따라서 최근에 사용자의 임무, 지위, 역할, 접근권한 등과 같은 속성 정보를 별도의 속성인증서(Attribute Certificate : AC)[2,7]에 저장 관리하며 유통하는 속성인증서에 대한 연구가 활발히 진행되고 있다.

이와 같이 신분인증 정보가 공개키인증서를 통해서, 그리고 사용자의 임무, 지위, 역할, 접근권한 등과 같은 속성 정보가 속성인증서를 통해 제공할 때에, 이 들 사이에 적절한 바인딩 메커니즘이 제공되어야하며, 또 이들 인증서들 간에 종속성이 유지되어야 한다. 즉 신분인증서를 기초로 발급된 속성인증서는 그 공개키인증서가 철회될 때 함께 철회되어야 한다. 본 논문에서는 짧은 유효기간으로 인해 원천적으로 종속성 유지 문제가 발생하지 않는 일회성 속성인증서의 바인딩 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 기술들을 설명하고, 3장에서는 잘 알려진 종속성을 유지하는 바인딩 메커니즘인 선택적 철회 방식(selective revocation methods)[5]과 암호적 인증서 바인딩 방식(cryptographic certificate-binding methods)[3]을 분석하고, 제안된 방식인 일회성 속성인증서를 이용한 도메인 내에서의 접근권한과, 도메인간의 접근권한에 대해서는 4장에서 제안하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 기술

1. 공개키인증서

공개키인증서는 인증기관(Certificate Authority : CA)이 발행하는 전자서명 정보로, 특정 공개키가 특정 사용자에게 연관되어 있음을 증명한다. 일반적으로 공개키를 신뢰성 있게 사용하기 위해서는 특정 공개키가 특정 사용자에게 정확히 결합되어 있다는 것을 증명할 필요가 있다. 따라서 사용자 신분정보와 사용자 공개키가 암호학적으로 안전하게 결합될 필요가 있다. 이렇게 하기 위해서는 공개키와 신분 정보를 포함하는 데이터에 대한 무결성, 결합 증거가 제3의 기관에 의해서 이루어 졌음을 나타내는 인증성, 부인방지의 특성을 요구한다. 이를 제공하기 위한 암호학적 메커니즘이 전자서명이다. 즉, 사용자의 신분 정보와 사용자의 공개키를 포함하는 문서에 대하여 서명이 요구된다.

ITU(International Telecommunication Union)과 ISO(International Organization for Standardization)은 1988년 X.509 표준[1]을 발표하였고, IETF (International Engineering Task Force)에 의해 채택되었다. X.509는 현재 가장 널리 사용되는 공개키인증서에 대한 데이터 양식이며, 인증기관 사용을 기초로 한다.

X.509 인증서는 공개키를 특정 개인에게 연결하기 위해 사용되며, 공개키가 이 인증서의 소유자(주체)에 연결되어 있음을 확인하기 위하여 인증기관에 의한 전자서명이 이루어진다.

2. 속성인증서

속성인증서는 사용자의 속성정보를 저장 관리하는 인증서로서 기존 공개키인증서가 사용자의 공개키 정보를 통해 인증 정보를 제공하는 것과는 달리 사용자의 지위, 권한, 임무 등과 같은 다양한 권한 정보를 제공한다. 또한 한 사용자는 하나의 공개키 인증서와 연관된 여러 개의 속성인증서를 가질 수 있는 특징을 가진다. 모든 응용은 인증을 첫 번째 절차로 시작하기 때문에 속성인증서는 사용자의 공개키인증서와 응용에 따라 상호 정보를 연결한다.

속성인증서에 대한 표준화 작업은 ANSI[2], Open Group, ITU-T, IETF 등과 같은 국제 단체에서 진행되고 있다. 이 중 ITU-T는 X.509 Version 4에서 속성인증서와 이를 이용한 권한관리기반구조 PMI (Privilege Management Infrastructure)에 대하여 기술하고 있다. 또한 IETF에서는 Attribute Certificate Profile에 대하여 표준을 제정하고 있으며 현재 Version 9 드래프트가 발표되었다. 인터넷상의 전자상거래 정보보호를 위해 일반적으로 복잡한 ITU-T 표준보다 IETF의 RFC나 드래프트가 활용되고 있는 것이 현실이다.

Ⅲ. 속성인증서와 공개키인증서 간의 종속성

어떤 개체에 대하여 접근권한이 없는 사용자에게 접근제어에 관한 문제의 주 요인은 속성인증서를 통하여 분배된 그 접근권한(그룹의 membership, 위임 등)이 그 속성인증서를 발행하기 위해 사용된 공개키인증서의 철회와 무관하게 유지되고 있다는 것이다. 그림 1에서 사용자는 CA_1로부터 공개키인증서$_1$를 받고, 그 공개키인증서$_1$을 통하여 속성인증서를 발급 받는다. 그런데 만약 공개키인증서$_1$이 철회된다면, 그로 인해 발급된 속성인증서도 당연히 철회되어야 한다. 그때 속성인증서가 철회되지 않았다면, 사용자는 다른 CA_2로부터 발급 받은 공개키인증서$_2$를 가지고 그림 1과 같이 접근권한 없이 접근하게 된다. 속성인증서의 유효성과 신분인증서의 유효성 사이에 종속관계가 유지된다면, 공개키인증서가 철회된 후에 접근권한을 계속 유지하는 일의 문제점이 가능하지 않을 것이다.

접근권한 없는 사용자를 제어하기 위한 공개키인증서와 속성인증서와의 종속성에 대하여 현재 제안된 방법은 선택적 철회 방식[5]와 암호의 바인딩 방식[3] 등이다. 이 장에서는 각 방식들을 비교 분석한다.

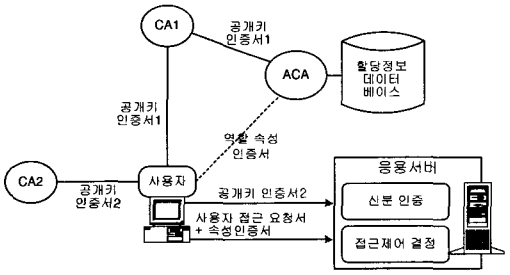


그림 1. 권한 없는 접근권한의 유지

1. 선택적 철회 방식(selective revocation methods)

선택적 철회 방식은 접근권한이 없는 사용자의 접근권한 유지 문제에 대한 해결의 한 방법으로 Himanshu와 Virgil[5]이 제안하였다. 이 선택적 철회 방식을 지원하기 위해서는 인증서와 연관된 서버들 사이에 동적인 링크의 유지가 요구되는 데, 이 링크들은 분산 시스템에서 선택적 철회를 적용하기 위해 서버들간에 적절한 메시지를 보내기 위해 사용되어 진다. 이 방식에서 각각 인증서와 연관된 서버들은 시간이 기록된 기본적인 사건들(즉, 보낸 메시지와 받은 메시지)의 순차적인 기록들을 유지한다. 그리고 선택적 철회의 적용은 이 기본적인 사건들에 기초한 보내는 메시지를 포함된다. 하나의 ACA (Attribute Certificate Authority)는 사용자에게 속성인증서를 발급할 때는 언제든지 그 사용자의 공개키인증서를 발급했던 CA에게 속성인증서 분배 사실을 메시지로 보내야한다. 그 때 이 메시지는 CA의 기록으로 유지될 것이다. 또 CA가 그 사용자의 신분을 나타내는 공개키인증서를 철회하고자 할 때 CA는 그 철회에 대하여 ACA에게 메시지를 보내어 ACA로 하여금 그 사용자의 속성인증서를 선택적으로 철회 할 수 있게 한다. 이 방식은 인증서들의 분배와 철회에 대하여 인증서와 연관된 서버들 간에 동적인 링크들의 유지를 요구하는데, 이 방식은 추가적인 통신비용의 원인이 된다.

2. 암호적 인증서 바인딩 방식 (cryptographic certificate-binding methods)

선택적 철회의 다른 방식으로, 암호적 인증서 바인딩 방식이 Park과 Sandhu[3]에 의해서 제안되었다. 이 방식은 강결합(strong binding)에 기초하는데, 강결합은 하나의 유일한 공개키인증서가 속성인증서에 의해 분배된 접근권한에 연결되어 바인딩 되는 것이다. 만약 그 공개키인증서가 철회되었다면, 사용자는 다른 공개키인증서를 통해 접근하는 일이 발생하지 않을 것이다. 즉 권한없는 사용자의 접근권한 유지 문제가 제거되어진다.

이 방식에 의한 종속성 적용에서는 모든 접근 요청에 대하여 서버는 공개키인증서와 속성인증서가 미리 정의된 것과 맞는지를 확인하여야한다. 즉, 서버에서 매 접근 요청에 대해 그의 공개키인증서와 속성인증서의 정당성을 확인해야만 한다. 따라서 이 방식은 모든 접근 요청에 대하여 추가적인 연산시간을 요구하며, 이것이 접근권한 할당과 권한허용에 따른 추가적인 부하가 될 것이다.

Ⅳ. 일회성 속성인증서 접근권한

1. 도메인 내에서의 접근권한

선택적 철회방식과 암호학적 바인딩 방식의 문제점을 해결하기 위하여 본 논문에서는 일회성 속성인증서를 이용한 공개키인증서와 속성인증서의 바인

딩 방법을 제안한다. 그림 2는 본 논문에서 제안한 도메인 내에서 일회성 속성인증서를 사용한 접근제어의 전형적인 모습을 보인다. 여기서 접근권한을 얻기 위하여 사용자는 CA에 의해서 서명된 사용자의 신분정보를 인증하는 공개키인증서를 CA로부터 발급 받는다. 그리고 사용자는 자신의 개인키로 서명한 접근 요청서를 자신이 접근하고자 하는 객체를 가진 서버에 제출함과 동시에 ACA에게 자신의 공개키인증서와 함께 일회성 속성인증서에 대한 요청서를 보내다. 이 때 ACA는 사용자의 공개키인증서를 확인하고, 서버와 보안정책을 고려한 일회성 속성인증서를 발급한 다음, 사용자의 공개키인증서와 함께 서버에게 직접 보내게 된다. 이 때 일회성 속성인증서가 사용자를 통하여 서버에 보내지는 것이 아니기 때문에 3장에서 언급한 접근권한이 없는 사용자의 접근권한 유지와 같은 문제는 사전에 차단 할 수 있다.

응용 객체에 대한 접근은 서버에서 유지되는 ACL(Access Control List)에 의해서 관리된다. 일반적으로 공개키인증서에는 사용자의 이름과 개인키에 의해 서명된 요청서의 그 개인키와 연관된 공개키를 포함한다. 속성인증서는 사용자가 어느 단체에 소속된 회원임을 정의하며, 사용자가 그 단체에 연관되었음을 나타낸다. 공개키인증서는 CA에 의해서 발급되고, 속성인증서는 ACA에 의해서 발급된다. 이때 ACA는 속성인증서를 발급하기 전에 CA를 통해 사용자의 공개키인증서가 정당한 것인지를 확인한다.

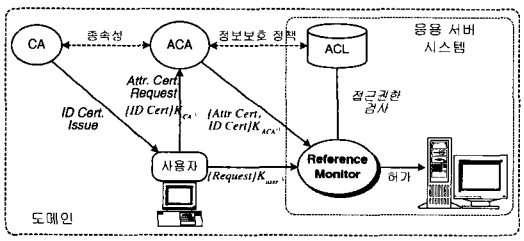


그림 2. 일회성 속성 인증서를 이용한 접근권한

접근요청서를 받은 서버는 그 요청서에 대하여 그 사용자의 공개키인증서와 속성인증서의 정당성을 확인하고, 또 그 요청서에 표시된 특정 객체에 대한 접근권한과 ACL이 요청한 접근권한에 허가한 그룹과 연관되는지를 확인하는 것에 의해 권한을 부여한다. 모든 확인 과정을 끝낸 후에 서버는 객체에 대한 사용자의 요청을 수행한다. 이 전형적인 프로토콜로부터 사용자의 속성인증서는 공개키인증서에 바인딩 되어야 하고, 이 인증서들 간에 종속성까지도 유지되어야 한다. 즉, 사용중인 공개키인증서가 철회 됐을 경우, 그 공개키인증서에 따른 속성인증서도 반드시 철회되어야 한다. 그것은 접근요청이 서버에 의해서 접근권한(속성인증서)이 등록된 사용자(공개키인증서)에게 분배됐다고 확인될 때만 승인되어지기 때문이다.

본 논문에서 제안한 일회성 속성인증서는 일회성으로서 공개키인증서가 철회되기 전에 그 사용의 유효성을 다하기 때문에 종속성 유지 문제는 발생하지 않으며, 또 서버에서 매 접근 요청에 대해 공개키인증서와 속성인증서 간의 바인딩을 위한 추가적인 연산을 요구하지 않는다.

2. 도메인간의 접근권한

그림 2에서 CA와 ACA가 서로 다른 인증서를 부여하는 기능을 갖는 것을 보였다. 이 두 CA와 ACA가 하나의 서버에 존재할 수 있다. 하나의 서버에 두 CA와 ACA를 두고 관리하는 것이 인증절차를 단순하게 할 수 있다. 그러나, 신분인증기관과 속성인증기관을 분리해서 운영하는 것이 여러 면에서 이점이 있음을[6]에서 보이고 있다. 그 이점들은 다음과 같다.

(1) 인증에 책임이 있는 인증기관과 권한을 부여하는 속성인증기관 사이의 독립성을 유지할 수 있다.
(2) 비교적 유효기간이 긴 공개키인증서에 영향 없이 속성인증서를 회수하는 것에 의해서 접근권한 할당을 쉽게 바꿀 수 있다.
(3) 다양한 도메인 사이에서 자원을 공유하는 도메인간의 네트워크에서는 신분인증기관과 속성인증기관의 분리가 필요하다.

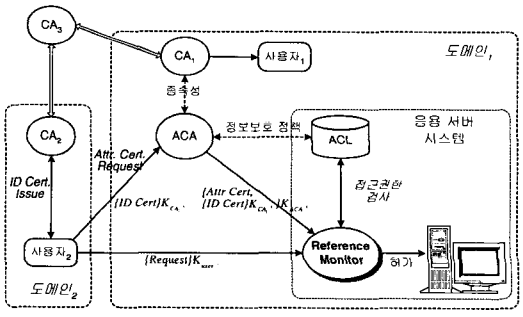


그림 3. 일회성 속성인증서를 갖는 도메인간의 접근권한

그림 3은 두 개의 자치적인 도메인을 포함하는 네트워크를 보이고 있다. 하나의 자치적인 도메인은 독립적인 인증과 도메인 내의 사용자 등록 및 공개키인증서 부여 등을 수행하는 도메인 자체 CA를 소유한다. 자치적인 도메인은 또한 도메인간의 네트워크의 관리가 자치 도메인 내의 사용자의 등록에 관여하지 않음과 다른 자치도메인 내의 사용자 등록에도 관여하지 않음을 함축한다. 따라서 자치 도메인들은 독립적으로 그리고 자치적으로 관리되므로, 도메인간의 네트워크 관리는 자치 도메인 내에 누가 등록된 사용자인지 조차도 알지 못한다.

그림 3에서 보이는 네트워크는 새로운 가상의 도메인을 구성하는데, 이 새로운 가상 도메인은 도메인$_1$과 도메인$_2$의 사용자와 자원들(즉, 서버들과 객체들)을 경로의 일회성으로 유지한다. 예를 들어, 도메인$_1$은 사용자$_1$을 그리고 도메인$_2$는 사용자$_2$를 등록하고 이들이 구성원으로 전체 가상 도메인을 구성한다. 이 가상 도메인의 네트워크에서 인증은 각 도메인의 인증기관인 CA_1과 CA_2에 의해서 부여하는 공개키인증서에 기초하는데, 이 공개키인증서는 각 도메인의 인증 정책에 기초한다. 자치적인 도메인은 다른 지역의 사용자 등록과 인증 정책을 지원하므로 지리적으로 멀리 떨어져 있을 수 있으며, 가상 도메인의 네트워크는 사용자 등록과 지역 인증 목적을 위하여 각 자치 도메인 구성원을 믿어야만 한다.

가상 도메인 네트워크에서 다른 도메인의 자원에 대한 접근은 인증서 체인을 통해 발급 받은 공개키인증서와 접근하고자 하는 도메인의 ACA으로부터 서버로의 일회성 속성인증서 발급 요청 그리고 개인키에 의해 서명된 요청서(Request)를 접근하고자 하는 도메인의 서버에게 제출함으로서 이루어진다. 예를 들면, 그림 3에서 도메인$_2$의 사용자$_2$가 도메인$_1$의 서버시스템에 접근하고자 할 때에, 우선 사용자$_2$는 CA_2으로부터 도메인$_1$의 공개키인증서를 상호인증인 인증서체인(CA_2, CA_3, CA_1)을 통해 발급 받는다. 그리고 사용자$_2$는 그 공개키인증서를 이용하여 도메인$_1$의 ACA에게 일회성 속성인증서를 발급하여 공개키인증서와 함께 도메인$_1$의 서버에게 보낼 것을 요청함과 동시에 자신의 개인키로 서명한 접근요청서를 도메인$_1$의 응용서버에게 보낸다. 이와 같은 일련의 절차가 접근권한 허용 처리 과정에서 일어난다.

앞에서 언급한 도메인 내에서 그리고 도메인 간의 일회성 속성인증서 메커니즘을 제안하였다. 속성인증서는 일회성으로 인해 공개키인증서가 철회되기 전에 그 사용을 다하기 때문에 종속성 유지 문제는 발생하지 않았으며, 또 서버에서 매 접근 요청에 대해 공개키인증서와 속성인증서 간의 바인딩을 위한 추가적인 연산 부하도 발생하지 않는다.

V. 결 론

인터넷상의 정보보호는 전자상거래의 활성화에 필수적인 요소로 자리잡고 있다. 정보보호를 제공하기 위해서는 사용자의 신분에 대한 인증정보와 사용자의 접근권한과 같은 접근허용 정보가 제공 되어야한다. 이 때 신분 인증정보는 공개키인증서를 통해서, 그리고 접근권한 허용정보는 속성인증서를 통하여 제공되며, 이 들이 사용되기 위해서는 속성인증서는 공개키인증서에 바인딩 되어야 하며, 이 인증서들 간에 종속성이 유지되어야 한다.

본 논문에서 잘 알려진 바인딩 메커니즘인 선택적 철회 방식[5]과 암호적 바인딩 방식[3]에서 인증서들간에 종속성을 어떻게 유지하고 있는지를 보이고, 이들 방식들의 대안으로 일회성 속성인증서를 사용한 새로운 방식을 제안하였다. 일회성 속성인증서는 사용자의 요청에 의해 속성인증기관에 의해 발행되어 사용자가 접근하고자 하는 서버에 직접 보내지기 때문에 접근권한 없이 개체 접근에 사용되지 않으며, 단 한번 사용되는 짧은 유효기간으로 인해 종속성 유지 문제가 발생하지 않는다.

참 고 문 헌

[1] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January 1999.

[2] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[3] Joon S. Park and Ravi Sandhu,"Binding Identities and Attributes Using Digitally Signed Certificates", 16th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, December 11-15, 2000.

[4] Joon S. Park and Ravi Sandhu, "Smart Certificate : Extending X.509 for Secure Attribute Services on the Web", NISSC, 1999.

[5] Himanshu Khurana and Virgil D. Gligor, "Enforcing Dependencies between PKI certificates in ad-hoc Networks, IEEE International Conference on Telecommunications, Buchartest, Romania, pp. 293-298, June 2001.

[6] J. Lim, M. Nystrom, "Attribute Certification : On enabling technology for delegation and role-based controls in distributed environments", Proceedings Fourth ACM Workshop on Role-Based Access Control, 1999.

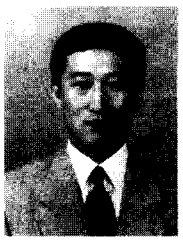
[7] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models", IEEE Computer, Volume 29, Number 2, February 1996.

박 종 화(Chong-hwa Park) 정회원

1974년 2월 : 숭실대학교 전자공학과 졸업
1990년 1월 : 미국 Syracuse 대학교 컴퓨터공학과 석사
1976년~1978년 : (주)CDC
1979년~1981년 : 전자통신연구원
2002년 : 아주대학교 컴퓨터공학과 박사수료
1994년 3월~ 현재 : 세명대학교 소프트웨어학과 조교수

<관심분야> 정보보호, 시스템 소프트웨어 보안, 네트워크 보안

이 상 하(Sang-Ha Yi) 정회원



1987년 2월 : 울산대학교 전자계산학과 졸업
1991년 2월 : 아주대학교 컴퓨터공학과 졸업 석사
1991년~1992년 : (주)큐닉스컴퓨터
1993년~1999년 : (주)케이엔아시스템
2002년 8월 : 아주대학교 컴퓨터공학과 박사
2000년 3월~현재 : 동서울대 정보통신과 전임강사

<관심분야> 정보보호, 네트워크 관리 및 보안, 분산처리 시스템 보안

김 동 규(Dong-Kyoo Kim) 정회원

1973년 2월 : 서울대학교 공과대학 응용수학과 졸업
1979년 2월 : 서울대학교 자연과학대학원 전자계산학과 석사
1984년 : 미국 Kansas State University 전자계산학과 박사
1986년~IEEE 802.4, 802.6, 802.10 Working Group Member
1979년~현재 : 아주대학교 정보 및 컴퓨터공학부 교수, Asiacrypt '96 조직위원장, 건설교통부 항공교통관제소 신공항 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국정보보호학회 부회장 역임

<관심분야> 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링