이동전화기를 이용한 Diffie-Hellman 키 교환기법의 개선방안

이윤진* · 이재근* · 조인준**

Enhanced Diffie-Hellman Key Distribution using Mobile-phone

Yoon-Jin Lee* · Jae-Guen Lee* · In-June Jo**

요 약

대칭암호시스템은 빠른 속도로 암·복호를 행하는 장점을 지니지만 안전하게 비밀키를 분배하는 방법에 문제점이 있다. 특히, 비밀통신을 원하는 불특정 사용자가 공통으로 가져야 할 비밀키를 분배하는 방안이 핵심쟁점이 되어왔다. 이러한 문제의 해결 방안으로 Diffie-Hellman 키 교환방법이 제안되었다. 하지만 이 스킴은 중간공격자(MITM, Man In The Middle)공격에 취약한 것으로 판명되었다.

본 논문에서는 이러한 문제점을 해결하기 위한 하나의 방안으로 널리 사용되는 이동전화 채널을 이용하여 강화된 Diffie-Hellman 키 교환방법을 제안하였다. 제안방안은 이동전화를 통해 교환된 인증번호와 생성된 Diffie-Hellman 키를 합성하여 송신자와 수신자에게 세션키를 분배하는 방안이다. 이렇게 함으로써 Diffie-Hellman 키 교환방법에서 쟁점이 된 중간공격자 공격을 실용적인 방법으로 방어할 수 있다.

ABSTRACT

Although a symmetric cryptographic system has many advantages in speed of encryption · decryption, the security problems with the distribution method of secret keys have been still raised. Especially, the distribution method of secret keys for unspecified individuals who want secret communication is becoming a core issue. As a simple solution to this issue, Diffie-Hellman key exchange methods were proposed, but proved to be insufficient in depending MITM (Main In The Middle) attacks.

To find effective solution to problems mentioned above, this paper proposes the strengthened Diffie-Hellman key exchange methods applied for the mobile-phone channel which are widely used. This paper emphasizes the way to distribute the synthesized session keys to the sender and the receiver, which are created with authentication numbers exchanged between the mobile-phones and Diffie-Hellman key. Using proposed ways, MITM attacks can be effectively defended.

키워드

키 교환방법, 대칭 암호시스템, Diffie-Hellman Key, 이동전화 인증번호

Key word

key exchange, symmetric cryptographic system, Diffie-Hellman key, authentication numbers

* 배재대학교 컴퓨터공학과

** 배재대학교 컴퓨터공학과 (교신저자)

접수일자 : 2009. 09. 29

심사완료일자 : 2009. 10. 26

Ⅰ. 서 론

대칭암호시스템은 빠른 속도로 암·복호를 행하는 장점을 지니지만, 비밀통신을 원하는 불특정 사용자간에 공통으로 가져야하는 비밀키를 안전하게 분배하는 방법에는 문제점이 있다.

지금까지 알려진 대칭암호시스템에서 키 분배방안은 첫째, 송신자와 수신자가 사전에 키를 분배하는 방법, 둘째, 키 분배센터(KDC, Key Distribution Center)를 이용하는 방법, 셋째, 공개키 암호시스템을 사용하는 방법, 넷째, D-H(Diffie-Hellman) 키 분배 방안을 들 수 있다[1]. 이중에서 D-H 키 분배 방법은 불 특정인사이에 공개적으로 협의절차를 거쳐 서로 간에 비밀키를 공유할 수 있다는 장점을 지닌다. 하지만, 이 방식은 중간공격자(MITM, Man In The Middle)공격에 취약하다는 문제점을 지니고 있어 이의 활용에 제약 요인이 되고 있다. 이러한 문제점을 해결하기 위한 방안으로 송신자와 수신자간에 인증을 위해 전자서명 프로토콜을 보완적으로 추가하는 방안이 제시되었다. 하지만, 이러한 접근법에서는 전자서명 인프라를 구축해야 하기 때문에 부가적인 시스템 요소가 추가되어 키 분배의 부담요인이 되었다[2][3].

본 논문에서는 이러한 문제점들을 해결하기 위한 하나의 방안으로 이동전화를 이용하여 강화된 D-H 키 분배 방법을 제안하였다. 제안방안은 이동전화를 통해 부여된 인증번호와 분배된 D-H 키를 합성하여 송신자와 수신자에게 키를 분배한다. 이러한 방법에 따라 분배된 키는 D-H 키 분배 프로토콜의 최대 취약점인 중간공격자 공격을 무력화시킬 수 있다.

본 논문의 구성은 제 1장에 서론, 제 2장에 D-H 프로토콜의 문제점 분석, 제 3장에 제안 프로토콜 설명, 제 4장에 제안 프로토콜의 특성 및 고찰, 그리고 제 5장에 결론을 기술하였다.

Ⅱ. D-H키 분배 프로토콜 분석

2.1 D-H 키 분배 프로토콜

이 프로토콜의 목적은 메시지 암·복호를 위해 송신자와 수신자가 안전하게 키를 교환하는데 있다. 이 프로토콜의 근본적인 원리는 이산대수 계산의 어려움을 활용한 것이다. RFC 2630에서는 특성이 서로 다른 3가지 D-H 스킴을 제시하고 있다[4][5].

본 논문은 3가지 스킴 중에서 Ephemeral-Ephemeral D-H을 기반으로 제안한 것이기 때문에 이를 설명하면 다음과 같다.

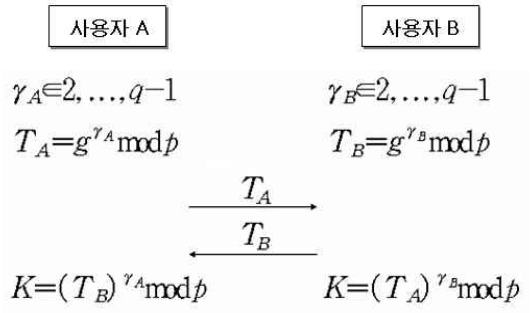

그림 1. Ephemeral-Ephemeral D-H 스킴
Fig 1. Ephemeral-Ephemeral D-H scheme

상기에서 사용자 A와 사용자 B는 매개변수g와p를 공개변수로 알고 있다. 여기에서p는 소수이고 g는 p의 원시근이다.

이와 같은 조건에서 사용자 A와 사용자 B는 자신의 개인값과 공개값을 계산할 수 있다. 즉, 사용자 A의 개인값은 r_A이고 공개값은 T_A이다. 이와 같은 방법으로 사용자 B의 개인값은 r_B이고 공개값은 T_B이다. 이렇게 계산된 개인값은 자신이 비밀스럽게 유지하고 공개값은 일반채널을 통해 공개적으로 교환한다. 사용자 A와 B는 교환된 공개값과 자신이 유지하고 있는 개인값, 공개변수p를 이용하여 그림 1. 처럼 세션키 K를 생성한다. 생성된 세션키 K값은 동일하게 계산되기 때문에 이를 사용하여 송수신자가 대칭암호시스템에서 메시지 암·복호를 할 수 있게 된다[6].

2.2 Ephemeral-Ephemeral D-H의 문제점

이 프로토콜은 사용자 A와 B간에 공개값을 아무런 안전조치 없이 서로 교환하여 이를 근간으로 최종적인 세션키를 계산하게 된다. 이는 중간공격자 공격에 취약성을 보인다. 그림 2.에서 이를 설명한다.

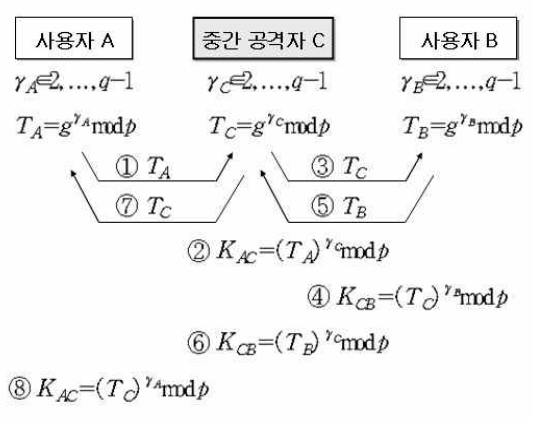

그림 2. 중간 공격자의 공격
Fig 2. Man In The Middle Attack

그림 2. 에서 보듯이 중간 공격자 C는 사용자 A가 사용자 B에게 전달하는 T_A값을 탈취한다. 이를 이용하여 사용자 A와 중간공격자 C간에 사용할 세션키로 K_{AC}를 생성한다(①). 그리고 사용자 B에게는 자신의 T_C 값을 보낸다. 이를 수신한 사용자 B는 중간공격자 C와 사용자 B간에 사용할 세션키로 K_{CB} 를 생성한다(④). 그리고 사용자 B는 사용자 A에게 전달할 목적으로 T_B를 보낸다. 이 과정에서 중간공격자 C가 이를 탈취한다. 이를 이용하여 중간 공격자 C는 사용자 B간에 사용할 세션키 K_{CB}를 생성한다(⑥). 공간공격자 C는 사용자 A에게 T_B를 보내지 않고 자신의 공개값 T_C를 보낸다. 이를 수신한 사용자 A는 중간공격자 C간에 사용할 세션키로 K_{AC}를 생성한다(⑧). 이와 같이 Ephemeral-Ephemeral D-H 에 의한 키 분배에서 중간 공격자의 공격이 이루워지면, 사용자 A와 B간에 송수신되는 모든 메시지를 중간 공격자가 탈취하여 해독이 가능하다. 이것은 두 사용자간의 키 분배 과정에서 서로를 인증하는 절차가 생략되었기 때문이다. 이 문제점을 해결하는 방안으로 전자서명을 통한 인증기법이 제시되고 있다[1]. 하지만, 이는 공개키 암호시스템과 같은 기반설비 즉, 전자서명 인프라를 구축해야 하기 때문에 부가적인 시스템 요소가 추가되어 키 분배의 부담요인이 되고 있으며 활용에 많은 제약이 된다.

본 논문에서는 전자서명 인프라와 같이 기반설비에 부담이 되지 않는 Ephemeral-Ephemeral D-H 스킴에 이동전화 기반시설을 활용하여 인증절차를 거쳐 중간공격자를 방어하는 새로운 기법을 제안하였다.

Ⅲ. 제안 프로토콜

3.1 제안프로토콜의 동작 개요

제안 프로토콜은 다음과 같은 가정을 전제로 동작한다.

가정) 사용자는 서버응용에 자신의 이동전화번호를 등록하고 이동전화를 항상 소지하여 문자 메시지를 확인할 수 있다.

제안된 프로토콜은 Ephemeral-Ephemeral D-H 스킴에 사용자 인증을 위한 SMS(Shortest Message System) 인증번호를 전송받기위해 이동전화 채널을 활용하도록 고안되었다. 따라서 이와 같은 가정 하에 제안 프로토콜은 그림 3. 과 같은 동작과정을 거쳐 세션키를 분배한다.

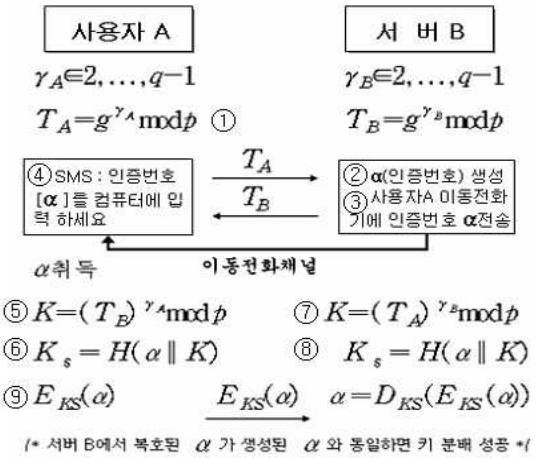

그림 3. 제안 키 분배 방안
Fig 3. Proposes the key exchange methods

<제안 프로토콜의 동작 과정>

① 사용자 A는 공개키 값 $T_A=g^{\gamma_A} \bmod p$ 을 계산하고 T_A를 서버 B에게 전송한다.

② 서버는 랜덤한 α(인증번호)값을 생성한다.
③ 서버 B는 이동전화 채널을 이용하여 사용자 A에게 α가 입력된 SMS를 전송한다.
④ 사용자 A는 수신한 α를 컴퓨터에 입력한다.
⑤ 서버로부터 수신한 공개값 T_B와 자신의 개인키 값으로 $K=(T_B)^{r_A} \bmod p$ 값을 계산한다.
⑥ 사용자 A는 α와 키 값 K를 해쉬함수(H)에 입력하여 세션키 $K_S=H(\alpha \| K)$를 계산한다.
⑦ 서버 B는 사용자 A의 공개키 값과 자신의 개인키 값으로 $K=(T_A)^{r_B} \bmod p$ 값을 계산한다.
⑧ 서버 B는 자신이 생성해 A에게 전송한 α와 킷값 K를 해쉬함수(H)에 입력하여 세션키를 $K_S=H(\alpha \| K)$ 계산한다.
⑨ 사용자 A와 서버 B는 생성한 세션키의 검증 과정을 거친다.
* A는 α를 암호화하여 $E_{KS}(\alpha)$ 값을 서버 B에게 전송한다.
* A에게 받은 암호문을 $\alpha=D_{KS}(E_{KS}(\alpha))$ 복호화를 통해 α를 취득한다.
* A가 보낸 α값이 자신이 생성했던 인증번호 α값과 일치하는지 확인한다.

사용자 A가 암호화하여 서버 B에게 보낸 α값이 서버 B가 생성해서 사용자 A에게 보냈던 α값과 일치하면 세션키 분배가 종료된다.

3.2 중간공격자 공격 방어

제안 프로토콜의 동자절차를 그림 3. 에서 보였다. 그리고 원래의 Ephemeral-Ephemeral D-H 스킴에서 약점인 중간공격자 C의 공격절차를 그림 2.에서 보였다. 그림 2에서 보듯이 중간 공격자 C가 송신자 A로 위장하여 수신자 B에게 자신의 공개값을 제공하고 이를 활용하여 중간공격자 C와 B간에 동일한 세션키를 생성한다. 똑같은 방법으로 송신자 B로 위장하여 A에게 자신의 공개값을 제공하고 B의 정보를 탈취하여, 중간공격자 C와 A간에 동일한 세션키를 생성하게 된다.

이러한 결과는 A와 B간에 전송되는 모든 메시지들이 중간 공격자 C에 의해 해독이 된다. 이렇게 취약점이 존재하게 된 이유를 Ephemeral-Ephemeral D-H 스킴의 동작 과정에서 찾아보면 송수신하는 사용자 간에 서로를 인증하는 절차 없이 공개값이 교환되기 때문이다. 하지만, 제안 프로토콜에서는 서버측에서 PRNG(Pseudo Random Number Generator)를 통해서 인증번호를 생성하고, 이를 서버측에 미리 등록된 이동 전화번호를 통해 클라이언트 이동전화에 인증번호를 송신한다. 이동전화 단문메시지를 통해서 수신된 인증번호를 클라이언트의 컴퓨터에 입력하도록 하여 입력된 인증번호와 원래의 Ephemeral-Ephemeral D-H 스킴에 의해 계산된 키를 해쉬함수에 입력하여 양자간에 동일한 세션키를 생성하는 방안이다[7]. 이는 이동전화 채널을 활용하여 해당 이동전화기에 만 인증번호가 전송되기 때문에 서버가 이동전화기를 통해서 클라이언트를 인증하는 방식이다. 따라서, 중간공격자는 송수신자간에 전송되는 공개값은 취득할 수 있지만 이동전화기를 통한 인증번호는 취득할 수 없기 때문에 중간공격자가 송수신자에게 분배된 세션키를 생성할 수 없다. 따라서, 송수신자간에 전송되는 메시지를 해독할 수 없게 되어 중간공격자 공격을 방어할 수 있다.

Ⅳ. 제안프로토콜의 특성 및 고찰

제안프로토콜의 특성을 분명히 하고자 다음과 같이 5가지 측면에서 기존의 Ephemeral-Ephemeral D-H 스킴과 전자서명을 통한 사용자 인증 D-H 스킴과 비교 검토를 하였다.

첫째, 키 분배 속도측면을 고려할 수 있다.

원래의 Ephemeral-Ephemeral D-H 스킴의 키 분배 속도는 인증절차 없이 키 분배가 이루어지기 때문에 속도면에서 가장 빠르다. 반면 전자서명 인증 D-H 스킴은 서버가 클라이언트를 인증하는 절차에서 소요되는 시간으로 인해 속도 면에서는 느리다. 제안한 스킴 또한 이동전화기에서 인증번호를 확인하고 이를 클라이언트에 입력하는 과정을 거쳐야 하기 때문에 키 분배 속도는 원래의 Ephemeral-Ephemeral D-H스킴 보다 느리다.

둘째, 스킴의 복잡도 측면을 고려할 수 있다.

원래의 Ephemeral-Ephemeral D-H 스킴의 복잡도가 가장 낮다. 전자서명을 통한 사용자 인증이 부가된 D-H 스킴은 PKI(Public Key Infrastructure)를 전제로 하기 때

문에 복잡한 인증서 관리 등의 부담이 수반되어 복잡도가 가장 높다. 제안 스킴은 간단히 이동전화를 통해서 인증이 이루어지기 때문에 전자서명을 통한 인증방식을 채택한 D-H 스킴 보다는 복잡도면에서 낮다.

셋째, 생성된 세션키의 안전성에 대해 고려 할 수 있다.

원래의 Ephemeral-Ephemeral D-H 스킴에서 생성된 세션키는 송・수신자 모두 비밀스럽게 유지하는 비밀값에의해 키의 안전도가 좌우된다. 제안 스킴은 원래의 Ephemeral-Ephemeral D-H 키와 인증번호를 해쉬함수에 넣어 그 결과 값이 세션키가 되기 때문에 각자의 비밀값이 공격자에게 노출이 되었어도 인증번호를 취득하지 못하면 세션키를 계산하기가 어렵다. 따라서, 세션키의 안전도 면에서는 제안방안에서 분배된 세션키가 Ephemeral-Ephemeral D-H에서 생성된 세션키보다 안전하다.

넷째, 스킴의 견고성 측면을 고려할 수 있다.

원래의 Ephemeral-Ephemeral D-H 스킴은 가정 사항이 공개값과 비밀값을 정의하고, 공개값은 일반채널을 통해서 공개적으로 교환하고, 비밀값은 자신만이 유지한다는 전제하에서 동작된다. 따라서 전송 중에 발생할 수 있는 공개값의 손상에 유무에 따라 스킴의 견고성이 영향을 받는다고 볼 수 있다. 제안방안에서는 이러한 공개값 교환과 더불어 추가적으로 이동전화 채널을 통한 인증번호 송신이 이루어진다. 이는 클라이언트에게 안전한 인증번호를 송신하기 위해서는 서버에 클라이언트의 이동전화번호가 안전하고 신뢰성 있게 등록되어 있어야 한다는 전제가 필요하다. 또한 서버와 클라이언트간의 이동전화 채널도 중간 공격자가 도청할 수 없는 안전한 채널을 가정한다. 따라서 제안한 스킴의 견고성은 Ephemeral-Ephemeral D-H 스킴보다 낮다고 볼 수 있다. 전자서명 인증서를 활용하여 사용자를 인증하는 방식에서는 추가적으로 인증서 발급, 인증서 폐기 등의 복잡한 인증서 관리 절차가 수반된다. 또한 매번 인증서를 추가적인 매체에 보관하여 유지하고, 사용 시 마다 이를 컴퓨터에 인식시키기고 검증하는 절차를 거치기 때문에 이 스킴의 견고성은 제안 방안보다는 낮다고 판단 할 수 있다.

다섯째, 응용측면에서 스킴의 실용성을 고려할 수 있다.

실용성이 가장 좋은 것은 인증기능이 빠진 원래의 Ephemeral-Ephemeral D-H 방식일 것 이다. 하지만 전자서명 인증방식을 Ephemeral-Ephemeral D-H 스킴에 추가한 스킴을 생각할 수 있다. 이 경우에는 송수신자에게 안전하게 세션 키가 분배되지만, 전자서명에 필요한 공개키 기반구조에서 안전하게 인증서가 관리되어야 하는 부담을 지니게 된다. 따라서, 이는 PKI가 전제되어야 하기 때문에 실용성이 떨어진다고 할 수 있다. 이에 반해 제안방안에서는 기존의 이동전화 채널을 사용하여 간단하게 클라이언트를 인증하는 스킴이 Ephemeral-Ephemeral D-H 스킴에 추가된 것이기 때문에 실용성이 높다고 할 수 있다.

위의 다섯 가지 측면의 비교를 통해 제안 프로토콜은 기존의 다른 두 스킴에 비해 실용성이 좋으며, 중간 공격자로부터 공격을 방어 할 수 있어 안전성도 좋은 것으로 나타났다고 판단할 수 있다. 현재 가장 안전한 방식으로 인식되는 전자서명 인증방식은 중간공격자 공격에 안전하지만, 인증서를 활용해 사용자를 인증하는 과정을 거쳐야하고, 인증서를 분배, 관리하는 복잡한 절차와 전자서명 인프라를 구축하고 관리하는데 많은 비용이 든다는 문제가 있다. 하지만 제안 방안은 기존의 이동전화 채널을 그대로 활용하므로 따로 인프라를 구축할 필요가 없다. 또한 키를 분배과정 중에 세션키를 생성을 위해 필요한 인증번호를 이동전화 SMS를 활용해 세션키를 생성한 사용자를 인증하는 절차를 거치므로 중간 공격자 공격에 안전하다 할 수 있다. 따라서 실용성과 안전성 면에서 좋아 현재 인터넷 상거래에서 일상적으로 사용되는 이동전화를 이용한 소액결제시스템을 본 시스템으로 대체할 경우 보다 안전한 전자상거래가 이루어질 것으로 판단된다.

Ⅴ. 결론

본 논문에서는 D-H 키 분배 방식의 최대 약점인 중간 공격자 공격을 방어할 수 있는 방안을 제안하였다. 제안 방안에서는 중간공격자의 공격을 방어하기 위해 인터넷 채널을 통해서는 D-H 공개 값을 송수신하고 통신을 원하는 사용자 인증을 위해서는 이동전화 채널을 사용하여 전송한 인증번호를 가지고, 계산된 D-H 키와 수신된 인증번호를 해쉬함수에 입력하여 세션키를 생성하였다. 이렇게 생성된 세션키로 인증번호를 암호화하여

인증번호를 보낸 서버에 보내고 이를 수신한 서버가 자신이 계산한 세션키로 복호화 하여 복호화 된 인증번호와 보냈던 인증번호가 같은지를 확인하는 검증과정을 거쳐 양자간에 세션키 분배를 완료한다

제안 방안은 D-H 키 분배방식에서 중간공격자를 방어하는 다른 방안에 비해 단순하다. 전자서명과 같이 복잡하고 비용이 발생하는 인프라를 따로 구축할 필요가 없이, 상용화되어 일상적으로 사용되는 이동전화 인프라를 변경 없이 그대로 활용함에 따라 실용성이 다른 스킴에 비해 강화된 것으로 판단된다. 또한 인터넷 채널과 이동전화 채널을 2중으로 사용하여 제안 프로토콜이 동작되기 때문에 중간공격자의 공격을 견고하게 방어할 수 있다고 판단된다.

참고문헌

[1] 윤종호, “원도우 서버와 프로토콜 분석기를 활용한 네트워크 보안 프로토콜”, 교학사, pp.31-57. 2004.

[2] 정익래. 권정옥. 이동훈. 홍도원. "표준모델에서 안전한 Diffie-Hellman 키 교환 프로토콜“ 정보과학회논문지, 정보통신 제35권 제6호 pp.465-473. 2008.

[3] K. Imamoto and K. Sakurai, "Design and Analysis of Diffie-Hellman-Based Key Exchange Using One-time ID by SVO Losic", Electronic Notes In Theoretical Computer Science, pp79-94, 2005.

[4] Tsuyoshi Abe, Hiroki Itoh, and Kenji Takahashi, "Implementation Identity Provider on Mobile Phone", Proc. ACM Workshop on Disital Identity Management (ACM DIM), ACM press, pp46-52. 2007.

[5] E. Rescola, "Diffie-Hellman Key Agreement Method" RFC2631. June 1999.

[6] Diffie W., Hellman H.: New directions in cryptography. IEEE transactions of Information Thory, vol.22(6): pp644-654. 1976.

[7] http://securitytechnet.com/resource/research/techreport/std-summary/node6.html

저자소개

이윤진(Yoon-Jin Lee)

1996년 배재대학교 응용수학과 (이학사)
2000년 배재대학교 컴퓨터공학과 (공학석사)
2003년～배재대학교 컴퓨터공학과(박사수료)
※관심분야 : 정보보호, 네트워크보안

이재근(Jae-Guen Lee)

2008년 배재대학교 컴퓨터공학과 (공학사)
2008년～배재대학교컴퓨터공학과 (석사과정)
※관심분야 : 정보보호, 컴퓨터네트워크

조인준(In-June Joe)

1982년 전남대학교 계산통계학과 (공학사)
1985년 전남대학교 전자계산학과 (공학석사)
1999년 아주대학교 컴퓨터공학과(공학박사)
1983～1994 한국전자통신연구원 선임연구원
1994년～현재 배재대학교 컴퓨터공학 교수
※관심분야 : 정보보호, 컴퓨터네트워크, 전산조직 운용