# 안전한 인터넷 경매시스템 설계

박진호* 안성진**
*대덕대학 인터넷정보기술계열 **성균관대학교 컴퓨터교육학과

## 요 약

인터넷이 보다 대중화되면서 웹을 통한 다양한 서비스가 창출되고 있다. 경매분야도 예외는 아니어서 현재 국내외의 여러 사이트에서 인터넷 경매가 활발하게 진행중이다. 그러나, 대부분의 인터넷 경매시스템은 보안기능이 취약해서 사용자에게 큰 피해를 초래할 수 있다. 본 논문에서는 사용자에게 보다 안전하면서 편리한 인터넷 경매 환경을 제공하기 위한 안전한 인터넷 경매시스템을 설계하였다.

# Design of an Secure Internet Auction System

Jinho Park* Sungjin Ahn**

## ABSTRACT

Becoming Internet is public, various services using Web are created . Internet auction is not exceptional but make rapid progress. Internet auction system damages user because its security is not perfect and faultless. In this paper, we propose a design of internet auction system providing more secure and convenient environment.

## 1. 서 론

인터넷 사용량의 급속한 증가로 2005년에는 전 세계 인터넷 사용자 수가 3억 5천만에 육박할 것으로 전망된다[1]. 이에 따라 사람들이 정보를 얻는데 있어 인터넷에 의존하는 비율이 더욱 높아지게 되었다. 인터넷을 통해 제공되는 서비스 형태의 종류는 그 수를 헤아릴 수 없을 만큼 많아지고, 그 중 홈뱅킹이나 전자상거래는 그 범위가 급속하게 넓어지고 있다. 이러한 서비스중의 하나로 인터넷 경매를 생각할 수 있다.

경매는 공지된 물품에 대해 구매를 요구하는 구매자들이 구매하려는 가격을 제시함으로써 낙찰자를 결정하는 방법이다. 예전에는 규모가 큰 물품이나 소장가치가 있는 일부 귀중품에 한해 시행되었으나, 인터넷의 발전으로 웹상에서 일반 사용자들을 위한 생활용품에 까지 그 범위를 넓히고 있다. 그러나 기존의 경매는 시간과 공간적 제약을 많이 받고 있어, 일반 소비자들이 경매에 참가하기란 그렇게 쉬운 일이 아니었다. 최근 들어 일부에서는 이를 전산화함으로써 특정 계층이 아닌 일반소비자에게도 경매에 참가하도록 유도하려는 움직임이 일고 있다. 그러나, 단순히 경매를 위한 웹 페이지만을 구축하고, 경매 물품만 공고한다고 해서 완벽한 경매 시스템을 구축했다고 말할 수는 없는 것이다. 인터넷 상에서 경매서버를 운영하기 위해서는 경매에 참가하는 사용자들에 대한 완벽한 보호, 경매 진행시에 경매내용에 대한 안전성과 투명성을 보장해야만이 완벽한 인터넷 경매시스템이라 할 수 있을 것이다. 이에 본 논문에서는 인터넷 상에 구축함으로써 고려해야 할 사용자 보호와 인증을 보장할 수 있는 안전한 인터넷 경매 시스템을 설계하고자 한다.

## 2. 인터넷 경매 시스템의 요구사항

경매는 돈과 결부되어 있기 때문에 정당한 사용자가 아니면 반드시 경매에 참여시켜서는 안되며, 정당한 사용자라 하더라도 인터넷의 특성상 그 내용이 인터넷에 연결된 제 3자에게 그대로 노출될 수 있기 때문에 이를 보호해 줄 도구가 필요하다. 이러한 보안서비스를 위해 암호화 통신이 요구된다[2][3].

### 2.1 기밀성 및 무결성

인터넷 상거래의 가장 기본이 되는 부분이 바로 보안문제이다. 인터넷은 그 특성상 네트워크를 통해 전송되는 모든 정보를 네트워크에 존재하는 모든 사람들이 읽고 변경할 수 있다. 상거래를 위해서 이 정보들은 상거래에 참여하고 있는 당사자들 이외에는 그 누구도 읽거나 변경할 수 없어야 한다. 경매도 인터넷 상거래의 일종으로써 경매를 진행하는 동안 사용자의 개인 정보에 대한 암호화가 선행되어 내용의 불법적인 노출 및 변경을 방지해 주어야 한다. 현재 인터넷 상에서 운영되고 있는 대부분의 경매 사이트들은 이 부분이 완전히 배제되어 있거나, 구현되어 있다 하더라도 브라우저에서 기본적으로 제공하고 있는 암호 모듈을 그대로 사용하고 있는 실정이어서 이를 방치한다면 경매 사이트를 이용하고 있는 사용자들에게 불이익이 돌아갈 것으로 예측된다.

### 2.2 인증

서로의 얼굴을 마주보고 물품을 경매하는 실세계의 경매와는 달리 인터넷 경매는 서로를 확인 할 수 없는 상황에서 경매를 진행해야 한다는 커다란 부담을 안고 있다. 기존의 인터넷 경매는 정당한 사용자임을 확인하기 위해 미리 등록과정을 마치고, 그 등록과정에서 발급된 사용자 ID와 password로써 진위 여부를 확인하고 있다. 이 방

법은 매우 초보적인 방법으로써 악의의 제 3자가 얼마든지 도청해서 재 사용할 수 있고 또한 경매에 불법으로 참가한 후 경매 가격을 조작한다거나 임의로 낙찰시켜 낙찰 후, 경매 물품에 대한 사용자와 서버간의 분쟁을 일으킬 수 있어, 이에 따른 심각한 피해를 야기할 수 있는 단점이 있다. 그럼에도 불구하고 현재 인터넷 상에서 이루어지고 있는 대부분의 경매 시스템은 이 메카니즘을 보편적으로 사용하고 있다. 인터넷 상에서 안전한 인터넷 경매 시스템을 구축하기 위해서는 이러한 Basic Authentication의 틀을 벗어나 서버와 사용자간에 진정으로 믿을 만한 인증 메커니즘, 즉 메시지와 사용자에 대한 전자서명 기술이 절실히 요구된다.

### 2.3 송/수신 부인봉쇄

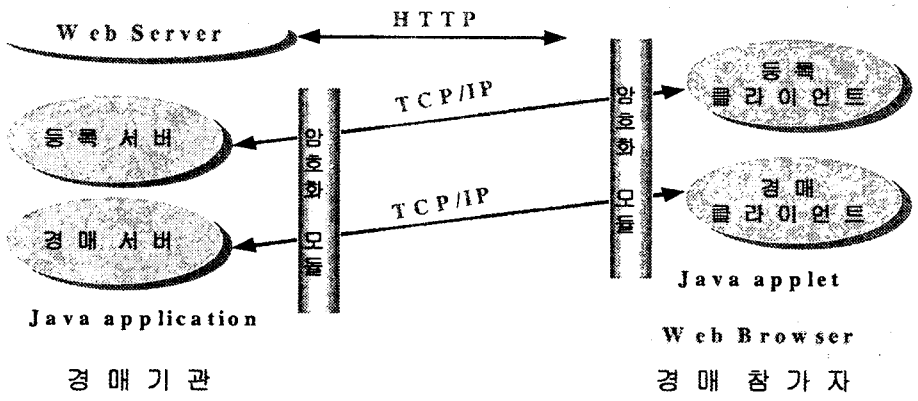
네트워크상에서 발생하는 모든 거래에 대해 필요한 것으로 부인봉쇄가 있다. 경매에서도 참가자가 제시한 가격에 대해 참가자가 전송 사실을 부인하거나 서버가 수신 사실을 부인하면 정상적인 경매 진행이 불가능해진다. 그러므로, 경매가 진행되는 동안에 통신되는 중요한 정보에 대한 전자서명이 추가되어 송/수신부인 봉쇄가 가능해져야 한다.

### 2.4 실시간 처리

실제의 경매는 물품에 대한 공고가 올라간 후 경매가 시작되면 경매 시간이 빠르면 수분, 아무리 늦어도 1시간을 넘어가는 경우가 없다. 그러나 현재 인터넷 경매의 경우에는 물품 공고가 올라간 후 경매 시간이 짧으면 1시간, 보통의 경우 일주일 정도가 된다. 경매를 통해 빠른 시간내에 물품을 구매하기를 원하는 사용자들에게는 이보다 불편한 일이 없을 것이다. 경매 서버측에서도 낙찰자가 결정된 이후에 낙찰자가 정당한 사용자인지, 지불 능력이 있는지 등을 전화나 E-mail을 통해 다시 한번 체크해야 하므로 경매 진행 과정이 상당히 길어질 수 밖에 없었다. 이러한 모든 일들을 신속하게 처리함으로써 보다 빠른 경매 라이프 사이클을 유지해 경매 문화의 확산을 유도할 필요성이 생겨나게 되었다.

## 3. 인터넷 경매시스템의 구성

인터넷 경매시스템의 각 구성요소 및 역할들은 다음과 같다.




(그림 1) 전자 경매시스템 구성도

(1) 웹 서버(Web Server)
- 경매 물품을 공고한다.

(2) 등록 서버(Registration Server)
- 등록을 희망하는 사용자들로부터 등록 접수를 받는다.
- 등록 희망자들의 정보를 데이터베이스에 유지하고 관리한다.
- 등록 희망자들에게 유일한 ID를 발급한다.

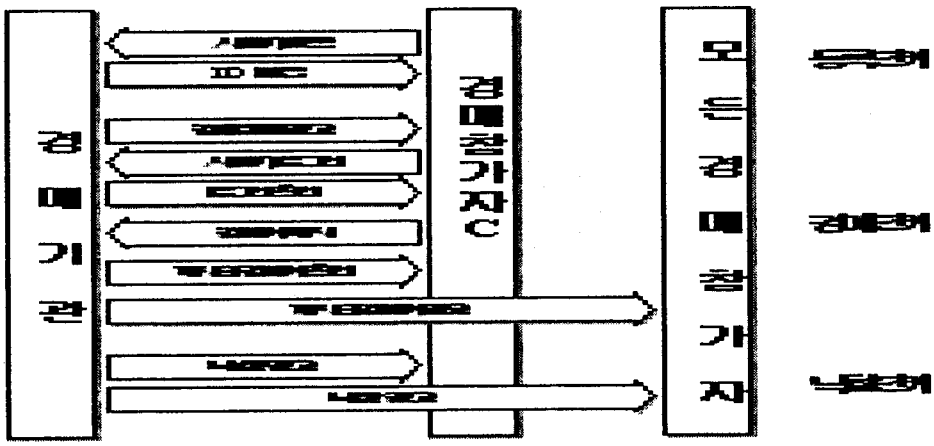
(3) 경매 서버(Auction Server)
- 이미 등록한 자들로부터 경매 참가 신청을 접수한다.
- 경매 참가자 데이터 베이스를 유지하고 관리한다.
- 경매시 참가자들의 모든 경매정보를 관리 및 감시한다.
- 경매 참가자들이 제시한 경매가를 이용해서 낙찰자를 결정/통보한다.
- 경매진행 전반에 대한 데이터 처리를 담당한다.

(4) 등록 클라이언트(Registration Client)
- 등록 신청서의 데이터를 암호화하여 등록 서버에 전송한다.
- 서버의 공개키를 로컬 컴퓨터에 저장한다.
- 클라이언트를 위한 비밀키와 공개키를 생성한 후, 로컬 컴퓨터에 각각의 키를 저장한다.
- 등록 서버가 발급한 ID를 로컬 컴퓨터에 저장한다.

(5) 경매 클라이언트(Auction Client)
- 경매 참가자로부터 경매서버로 전송하는 데이터를 암호화 및 서명한 후 전송한다.
- 현재 제시되고 있는 모든 경매 상황을 경매 참가자에게 알려준다.

## 4. 안전한 경매 프로토콜 설계

본 시스템은 <그림 2>과 같이 등록, 경매, 낙찰의 3단계로 이루어진다. 등록단계에서는 경매에 참가하고자 하는 희망자가 경매서버에 등록을 하고 ID를 발급받는 단계이다. 경매단계는 경매서버에서 경매 물품 공고가 나오면 경매에 참여하고자 하는 참가자가 경매서버에 로그인을 한 후, 경매가격을 제시함으로써 실제 경매를 진행하는 단계이다. 낙찰단계는 경매물품에 대한 낙찰자를 결정하고, 그 결과를 모든 참가자에게 알려주는 단계이다.




(그림 2) 인터넷 경매 프로토콜

인터넷 경매 프로토콜을 구현하기 위해서는 메시지의 기밀성과 무결성, 전자서명을 위한 관용키/공개키 알고리즘을 사용한다. 각 단계에서 사용되는 암호화와 해쉬함수의 표기는 <표 1>과 같다.

<표 1> 암호 관련 기호

| 구분 | 의 미 |
|---|---|
| Ex | 키 x로 메시지 암호화<br>예) $E_{KS}$ : 세션키(관용키)로 암호화 |
| C | 참가자 |
| S | 서버 |
| KSx | x가 생성한 세션키<br>예) KSc : 참가자의 세션키, KSs : 서버의 세션키 |
| Kux | x의 공개키<br>예) KUc : 참가자의 공개키, KUs : 서버의 공개키 |
| KRx | x의 비밀키<br>예) KRc : 참가자의 비밀키, KRs : 서버의 비밀키 |
| H[M] | 메시지 M에 대한 해쉬값 |
| $C_{ID}$ | 참가자 C의 ID |
| $P_{ID}$ | 경매물품의 ID |

### 4.1 등록 단계

● 사용자 등록

경매에 참가를 희망하는 사용자가 경매를 위해 미리 서버에 등록하는 단계이다. 경매참가 희망자는 해당 양식에 자신의 인적사항을 입력한 후 등록서버에 제출한다. 제출시 사용자의 인적사항과 기타 등록사항은 네트워크 상의 제 3자에게 노출되어서는 안되고, 또한 악의의 3자가 정당한 사용자를 사칭하여 거짓 등록을 하지 못하도록 등록정보를 사용자의 세션키(관용키)로 암호화하고, 사용자의 서명을 같이 서버에 전송하여야 한다. 등록정보를 암호화한 관용키는 서버의 공개키로 암호화되어 안전하게 전달된다. 또한 사용자의 인증서는 경매서버에 등록하기 전에 서로 교환할 수 있어야 한다. 본 논문에서는 등록단계에 사용자와 서버간에 서로의 인증서를 미리 교환하고 있음을 전제로 한다. 내용은 다음과 같다.

$$E_{KS_C}[\text{사용자의인적사항}] \| E_{KU_S}[KS_C] \| E_{KR_C}[H(\text{사용자의인적사항})]$$

● ID 발급

경매 기관은 등록을 요청한 경매 참가 희망자의 자격을 심사한 후, 희망자에게 유일한 ID를 부여한다. 이때 ID는 서버의 전자서명을 붙여 전달한다. 사용자의 ID를 암호화하지 않는 이유는 사용자의 ID만을 가지고 네트워크 상에서 제 3자가 사용자의 정보(이름이나 기타 등록사항)을 알 수 없기때문이다. 또한 ID에 서버의 전자서명을 붙이는 이유는 서버에서 발급한 ID가 정당한 것이고, 중간에 변경이 없음을 확인하기 위해서이다. ID발급단계에서 서버가 사용자에게 전송하는 내용은 다음과 같다.

$$C_{ID} \| E_{KR_S}[H(C_{ID})]$$

### 4.2 경매 단계

● 경매 물품 공고

서버는 웹서버를 통하여 사용자에게 경매물품을 공고하고, 경매 시작시간을 공고한다. 경매에 참가하고자 하는 사람은 경매 시작시간 전에 경매 서버에 접속해야 한다. 이때 경매에 참가할 수 있는 사용자는 등록서버에 등록되어 있는 사용자들이고, 자신의 ID와 전자서명을 이용해서 경매 서버에 로그인 할 수 있다.

● 사용자 로그인

경매에 참가하고자 하는 사용자는 경매서버에 정당한 참가자임을 증명하기 위해 서버에 로그인을 해야한다. 기존의 방식에서 사용자의 ID와 패스워드를 가지고 등록할 경우 제 3자가 이를 갈취해 서버에 정당한 사용자로 로그인 할 수 있는 문제점이 있다. 이를 해결하기 위해 본 시스템에서는 사용자의 ID와 ID에 대한 서명으로써 서버에 로그인을 하게 된다. ID에 대한 서명만으로 로그인을 할 경우 네트워크상의 제 3자가 이 정보를 보관하고 있다가, 나중에 서버에 이 정보를 그대로 사용할 수 있는 재전송 공격이 가능하므로 ID와 TimeStamp를 동시에 사용함으로써 이를 방지할 수 있다. 서버는 사용자의 서명값을 사용자의 공개키로 복호화하여 ID와 TimeStamp값을 비교해 봄으로써 사용자의 정당성을 확인할 수 있다. 사용자가 서버에 로그인 시 전송되는 내용은 다음과 같다.

$$C_{ID} \| TimeStamp \| E_{KR_C}[H(C_{ID} \| TimeStamp)]$$

● 경매 시작 및 사용자의 경매가 제시

경매 시작시간이 되었거나, 경매에 참가할 수 있는 사용자 수가 다 찼으면 곧바로 경매가 시작된다. 경매 참가자는 자신의 로컬 컴퓨터에 저장되어 있는 자신의 비밀키를 passphrase를 이용해 얻고, 애플릿에서 제공하는 경매 폼에 의해 경매를 진행할 수 있다. 참가자가 서버에 제시하는 경매정보는 경매물품의 ID (PID)와 그에 해당하는 경매제시가격이다. 경매 참가자가 경매정보를 서버에 전송하는 경우, 경매정보의 해쉬값을 구한 뒤 참가자의 서명을 붙임으로써 메시지의 무결성을 보장할 수 있고, 송신부인방지가 가능하다. 이때 해쉬값을 구할 때의 입력값은 사용자의 ID, 경매정보(경매물품ID, 경매제시가), 그리고 메시지의 재사용을 막기 위한 타임스탬프등이 된다. 서버에 전송되는 내용은 다음과 같은 형태가 된다.

$$MsgOfC = C_{ID} \| \text{경매정보}(P_{ID}, \text{경매제시가}) \| \text{TimeStamp} \| E_{KR_C}[H(C_{ID} \| \text{경매정보} \| TimeStamp)]$$

● 제시된 경매가 확인

경매서버는 경매 참가자 C가 제시한 경매정보에 대한 서명을 확인한 후, 경매가가 정당한 것임을 사용자에게 확인시켜줄 필요가 있다. 만일 이 사항을 경매가격을 제시한 참가자에게 확인시켜주지 않는다면 참가자는 자신이 현재 제시한 경매가가 제대로 반영되었는지 확인할 수가 없고, 경매가 완료된 후에 사용자가 제시한 경매가를 서버가 받지 못했다고 주장할 수 있기 때문이다. 이처럼 수신부인봉쇄를 실현하기 위해 서버는 사용자의 메시지 (MsgOfC)에 자신의 서명을 붙여 경매가 제시자에게 전송한다.

$$MsgOfC \| E_{KR_S}[H(MsgOfC)]$$

● 제시된 경매가 공고

참가자 C가 경매가를 제시했을 때 현재 경매에 참가하고 있는 모든 참가자에게 현재 경매가를 공고함으로써 참가자들이 현재 경매가보다 더 높은 경매가를 제시하도록 해야한다. 참가자는 현재 경매가를 확인 후, 더 높은 가격을 제시하면 된다. 만일 제시한 경매가가 현재 경매가보다 낮거나 같은 경우, 제시된 경매가는 받아들여지지 않고 다시 가격을 제시할 것을 요구한다. 이때 제시된 경매내용이 서버에 의해 조작/변조되는 것을 방지하기 위해 참가자 C가 전송한 메시지 (MsgOfC) 전체에 서버의 서명을 붙여 모든 참가자들에게 전송하는 방법을 이용한다. 이렇게 함으로써 각 참가자는 서버로부터 전송된 메시지의 서명을 확인하고, 필요한 경우 경매가를 제시한 참가자의 인증서를 이용해 경매가에 대한 정당성을 확인해 볼 수 있다. 이때 불법적인 제 3자가 예전에 사용되었던 사용자의 경매제시가를 재사용하여 불법적으로 더 높은 가격을 모든 참가자

에게 제시함으로써 경매가를 높일 가능성이 있다. 이를 방지하기 위해 서버는 현재 경매정보에 TimeStamp를 첨가하여 서명함으로써 이 문제를 해결할 수 있다. 서버가 각 참가자에게 전송하는 경매확인 메시지의 내용은 다음과 같다.

$$MsgOfC \| TimeStamp \|$$
$$E_{KR_S}[H(MsgOfC \| TimeStamp)]$$

### 4.3 낙찰 단계

일정 시간동안 경매가가 올라가지 않거나, 1명을 제외한 모든 참가자가 경매포기 메시지를 보냈을 경우 낙찰자가 결정되며, 최종 낙찰가는 가장 마지막에 제시된 낙찰가가 된다. 낙찰에 관한 정보는 최종 낙찰가와 함께 모든 참가자에게 알려지게 되는데, 역시 최종 낙찰자로 선택된 참가자의 낙찰가와 서버의 전자서명을 붙여 모든 참가자에게 보냄으로써 낙찰가가 조작 및 변조되지 않았음을 확인할 수 있다. 참가자들에게 보내지는 낙찰정보의 내용은 다음과 같다.

$$MsgOfC_{\text{최종경매가제시자}} \| TimeStamp \|$$
$$E_{KR_S}[H(MsgOfC_{\text{최종경매가제시자}} \| TimeStamp)]$$

이상에서와 같이 본 논문에서 설계한 프로토콜은 공개키와 관용키 알고리즘을 모두 이용함으로써 기존 시스템에서 제공하지 못하는 메시지 암호화와 무결성, 전자서명 등을 제공함으로써 안전한 경매가 진행될 수 있는 기반을 마련하였다.

## 5. 결 론

인터넷의 급속한 확산과 정보 기술 발전은 일상생활과 비즈니스 관행을 근본적으로 변화시키고 있으며, 인터넷을 통한 다양한 비즈니스를 창출하고 있다. 그러나 보안상 매우 취약한 것으로 알려져 있는 인터넷상에서 사업이나 개인의 사생활과 관련된 민감한 정보에 대한 보안 대책이 미흡한 것이 사실이다. 이는 단순한 정보 누출이 아닌 범죄로까지 이어질 수 있는 매우 심각한 문제이다.

본 논문에서는 안전한 인터넷 경매 서비스를 제공하는 시스템을 설계함으로써 현재 실세계에서 행해지고 있는 경매 과정을 재현하며 비용감소와 안정성에 대한 새로운 방안을 모색하였다. 또한, 본 인터넷 경매시스템은 사용자의 디렉토리에 사용자의 공개키, 암호화된 비밀키, 서버의 공개키와 사용자의 ID를 모두 관리하고 있으므로, 이를 간단히 복사만 함으로써 이동성을 실현할 수 있기 때문에, 인터넷에 접속할 수 있는 곳이면 어디서든지 간단히 경매에 참여를 할 수가 있다. 이때, Passphrase를 알지 못하면 서명을 위한 비밀키를 복호화할 수 없으므로 사용자의 비밀키에 대한 기밀성이 보장된다. 현재 이 시스템은 인증서 발급과 지불 부분이 제외되어 있는데, 향후 두 부분이 개발된다면 보다 완벽한 경매시스템이 될 것으로 본다.

현재 경매는 일반인들에게는 익숙하지 않은 분야로 경매장소와 시간적 제약 때문에 많은 참여를 유도하지 못하고 있다. 하지만, 본 시스템은 인터넷상에서 쉽게 참여할 수 있으므로 많은 참여를 유도하여 경매를 보다 활성화 할 수 있는 가능성을 제공했다고 할 수 있다.

## 참고문헌

[1] 실리콘밸리 뉴스, http://www.svnews.com
[2] Bruce Schneier, "Applied Cryptography Second Edition", John Wiley & Sons Inc, 1996.
[3] William Stallings, "Network and

Internetwork Security", Prentice Hall International Edition, 1995.
[4] Gary Cornell & Cay S. Horstmann., "core JAVA", Sunsoft Press, 1998.
[5] IAIK-JCE, http://jcewww.iaik.tu-graz.ac.at/
[6] Scott Oaks, "Java Security ", O'Reilly & Associates Inc, 1998.
[7] JCE, http://java.sun.com/security

박 진 호

1995 대전대학교 전자계산학과(공학사)
1997 대전대학교 컴퓨터공학과(공학석사)
1997 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부(박사수료)
2000 ~ 2002 송호대학 정보산업계열 전임강사
2002 ~ 현재 대덕대학 인터넷정보기술계열 전임강사
관심분야 : 네트워크 관리, 보안

안 성 진

1988 성균관대학교 정보공학과 졸업(공학사)
1990 성균관대학교 대학원 정보공학과 졸업 (공학석사)
1998 성균관대학교 대학원 정보공학과 졸업 (공학박사)
1990 ~ 1995 한국전자통신연구원 연구 전산망 개발실 연구원
1996 정보통신 기술사 자격 취득
1999 ~ 현재 성균관대학교 컴퓨터교육과 조교수
관심분야 : 네트워크 관리, 트래픽 분석 , 보안관리