論文
5-1-6

Single Sign-On을 적용한 네트워크 보안 모델링 (A Study on Network Security Modeling using Single Sign-On)

서희석(Hee-Suk Seo)[1] 김희완(Hee-Wan Kim)[2]

요 약

인터넷 사용의 급증에 따라 대부분의 사용자들은 여러 웹 서버의 서비스를 사용하고 있으며 각 서버의 접속 사용자 ID 및 패스워드의 상이함으로 인해 혼선을 초래하기도 한다. 이러한 문제를 해결하기 위한 방법이 SSO(Single Sign-On)이다. 본 논문은 네트워크에 존재하는 다양한 서버 및 호스트에 접근하기 위한 SSO를 적용하여 침입 탐지 시스템과 침입 차단 시스템 등과 같은 보안 시스템의 관리를 수월하게 하고 네트워크 사용 및 관리를 효과적으로 수행하기 위한 모델링 방법을 제안한다. 본 연구진이 제안하는 방법은 소규모 네트워크에서 적용하여 사용하기 수월하도록 구성하였으며 조직의 여러 데이터를 효과적으로 처리할 수 있도록 구성되었다. SSO의 구성은 인증서 기반의 PKI (Public Key Infrastructure)를 사용하여 구성하였으며 인증 통신을 위한 데이터 암호화를 SSL (Secure Socket Layer) 기반의 SHTTP (Secure Hyper Text Transfer Protocol)을 적용한다.

ABSTRACT

With the growing usage of the networks, the users in the Internet uses some kinds of web server. They confused that each web server uses the different user ID and passwords. To solve these problems, SSO (Single Sign-On) solution is introduced. We presents the modeling methods which are efficiently constructed the network management models. We constructed the intrusion detection systems and firewalls using the SSO. This architecture is efficient to manage the network usage and control. SSO solution designed on the small scale Intranet. CA server in the SSO that depends on PKI (Public Key Infrastructure) is used to issue the certificates. SHTTP based on SSL (Secure Socket Layer) is used to protect the data between certificate server and the intranet users.

1) 정회원 : 성균관대학교 정보통신공학부 박사과정
2) 정회원 : 삼육대학교 컴퓨터과학과 조교수

논문접수 : 2003. 12. 26.
심사완료 : 2004. 1. 5.

1. 서론

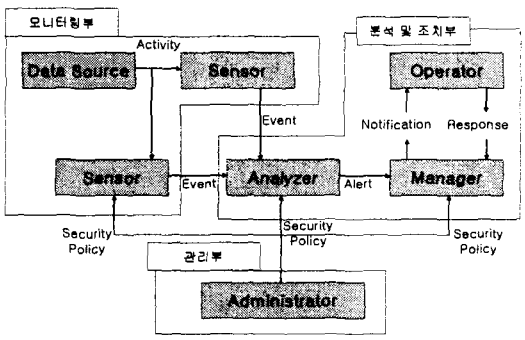
컴퓨터와 인터넷을 통한 전자 상거래는 경제 활동의 새로운 패러다임으로서 우리의 일상 생활 속에 이미 깊숙이 들어와 있다. 앞으로는 전자 상거래를 통하지 않고는 기업 간, 혹은 기업과 고객 간의 거래를 이룰 수 없는 세상이 될 것이다. 전자 상거래 이외의 분야에서도 우리는 이미 인터넷의 포로가 되어 있다고 해도 과언이 아니다. 행정, 교육, 국방, 치안 등등 우리 일상의 모든 활동이 인터넷에 의존되어 있는 실정이다. 이러한 가운데 많은 인터넷 사용자들은 서비스를 제공하는 인터넷/인트라넷 웹 사이트에 접속하면 사용자 ID 및 패스워드를 요청받는 경험을 하게 된다. 인터넷 사용자의 급증에 따라 대부분의 사용자들은 여러 웹 서버에 접속할 때마다 서로 다른 사용자 ID와 패스워드를 입력해야 한다. 특히 인트라넷에서는 기관 내의 서비스별로 사용자 ID를 관리하고 있어 한 서버에 접속하여 회사의 속한 사원임을 인증 받았다 해도 다른 서버에 접속하면 같은 방식의 인증 확인 절차를 반복하거나 심지어 서버마다 ID와 패스워드가 달라 사용자의 혼선을 초래하기도 한다. 이러한 문제를 해결하기 위하여 SSO 기술이 사용되는데, SSO란 한번의 로그인을 통해 모든 서버에 좁속할 수 있는 권한을 갖게하는 개념이다. SSO 구현을 위한 방법으로는 기존 ID/패스워드 방식이 구현하기가 용이하나 사용자의 인증 정보들이 네트워크에서 노출될 가능성이 많이 때문에 X.509에 의한 인증서(Certificate) 기반의 강력한 인증 기법이 적용되고 있다 [1-3]. 또한 SSO를 적용한 솔루션의 형태는 SSO 본연의 기능인 통합 로그인 기능에서 인증 정보 유지, 개인화 서비스 제공, 다양한 관리 기능 등이 포함되며, 접근 권한 관리 기반 구조인 PIM (Privilege Management Infrastructure)와 함께 통합되어 EAM (Extranet Access Management)으로 확대 발전되고 있다 [4].

2. 네트워크 보안 요소

2.1 침입 탐지 시스템

침입 탐지 시스템은 컴퓨터나 네트워크 자원에 대한 악의적인 행위들에 대해 확인하고 그에 대해 응답하는 시스템으로 다음과 같은 작업을 수행한다 [9].

- 다양한 시스템 소스로부터 정보를 수집.
- 오용이나 비정상적인 행위 패턴에 대한 정보를 분석.
- 자동적으로 탐지된 행위에 응답
- 탐지 프로세스에 대한 출력 기록



<그림 1> 침입 탐지 시스템의 구성도

<그림 1>는 침입 탐지 시스템의 구성을 나타낸다. 침입 탐지 시스템은 크게 모니터링부, 분석 및 조치부, 관리부로 구성된다.

1. 모니터링부

이 단계의 작업은 정보 수집 단계로 호스트나 네트워크로부터 데이터를 수집하며 수집된 데이터는 특정 패턴을 검출하기 위해 다음 단계로 넘겨짐.

2. 분석 및 조치부

- 정보 가공 및 축약 단계 : 수집된 정보에 대한 분석은 시스템 설정과 패턴 생성기에 의해서 생성된 패턴 데이터베이스의 설정에 따라 정보 분석기에서 수행됨.
- 분석 및 침입 탐지 단계 : 침입 탐지 시스템의 핵심적인 단계로 기존의 가공된 정보와 축약을 거친 데이터를 기반으로 침

입 여부를 결정
- 보고 및 조치 단계 : 보고 및 조치는 침입으로 규정된 행위가 발생할 경우 수행되는 역할로서 실제적인 관리자에게 보고

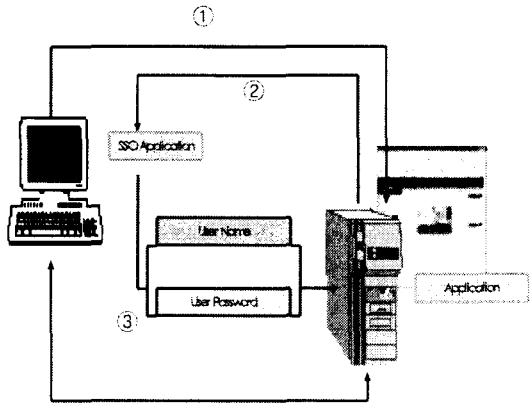
3. 관리부

관리부는 모니터링부와 분석 및 조치부에 대한 통제 및 관리 기능과 이들에 대한 보안 정책을 제공하는 기능을 수행한다. 만일 대규모 네트워크를 위한 침입 탐지 시스템을 구성하는 경우에 있어서의 보안 정책은 중앙 시스템의 관리부로부터 각 분산된 침입 탐지 시스템의 관리부로 전달될 수 있으며, 각 분산된 침입 탐지 시스템의 운영자들로부터의 취합된 침입 탐지 정보는 중앙 시스템의 운영자에게 전달되어 전체적으로 통제할 수 있는 형태로 구성할 수 있다 [10-12].

2.2 침입 차단 시스템

침입 차단 시스템은 기본적으로 방어를 목적으로 하는 장치이고, 주요 목적은 불법 사용자로부터 내부 네트워크를 보호하는 것이다. 외부 네트워크는 신뢰할 수 없으며, 보안 침해의 원천이 될 수 있다 [13-15]. 네트워크를 보호한다는 것은 정당하지 않은 사용자가 중요한 데이터에 접근하는 것을 막고, 정당한 사용자가 네트워크 자원을 방해 없이 접근하도록 하는 것이다. 일반적으로 보호하고자 하는 네트워크는 사용자가 속한 기관의 네트워크이고 불법 사용자는 외부의 네트워크에 있는 사용자로 간주된다. 침입 차단 시스템의 기능은 다음과 같다.
- 접근 통제 : 허용된 서비스와 전자 우편 서버나 공개 정보 서버와 같은 특정한 호스트를 제외하고는 외부에서 내부 네트워크래 접속하는 것을 패킷 필터링 등을 사용하여 통제.
- 사용자 인증 : 침입 차단 시스템을 지나가는 트래픽에 대한 사용자들의 신분을 증명.
- 감사 및 로그 : 모든 트래픽에 대한 접속 정보 및 네트워크 사용에 따른 유용한 통계 정보를 기록하는 감사 및 로그 기능.
- 프라이버시 보호 : 프라이버시와 관련된 정보의 누출을 막고 공격자로부터 보호.
- 서비스 통제 : 안전하지 못하거나 위험성이 존재하는 서비스를 필터링함으로써 내부 네트워크의 호스트가 갖는 취약점 감소.

2.3 SSO



<그림 2> SSO의 동작

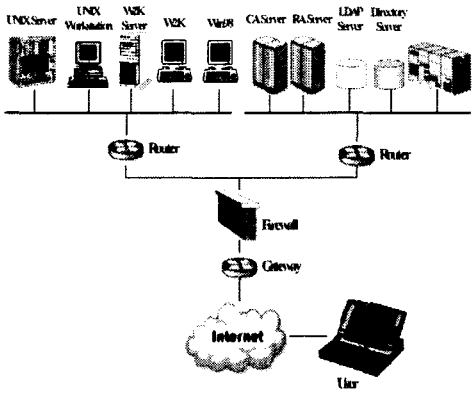
기존의 방식에서는 사용자가 응용 서비스를 요구할 때마다 응용 서버에 매번 로그인을 시도하여야 하나, <그림 2>과 같이 SSO 솔루션을 도입할 경우, SSO가 사용자 대신 로그인 과정을 처리한다 [16-19]. SSO를 사용함으로써 얻을 수 있는 효과는 다음과 같다.

- 기업의 업무 효율성 증대 : Help desk 비용 감소 (Password 분실 처리 등의 계정관련 문의 업무 감소)
- Log on 회수 감소 (Log on 시간 절약,)
- 중앙 집중식 인증/권한 관리 가능
- 보안성 증대 : 네트워크상의 정보에 대한 접근 제어
- 사용의 편리성

3. 대상 네트워크

3.1 대상 네트워크의 구조

대상 네트워크는 <그림 3>와 같이 구성되어 있다. 방화벽 안의 내부 네트워크의 구성은 크게 서버 및 호스트가 존재하는 네트워크와 PKI 인증을 해 줄 수 있는 Authentication Components로 구성되어 있다.



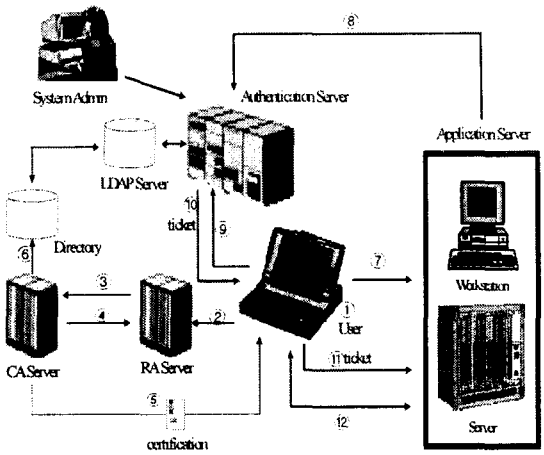
<그림 3> 대상 네트워크의 구조

서브 네트워크에는 Unix 시스템, Windows NT 서버 및 여러 PC들이 존재하며, Authentication Components에는 CA (Certificate Authority) server, RA (Registration Authority) server, LDAP (Lightweight Directory Access Protocol) server, directory server로 구성된다.

3.2 인증 과정

<그림 4>는 <그림 3>에서 구성된 Authentication Components를 통해서 인증을 수행하는 과정을 나타낸다.

① User : 서명용 키 쌍을 생성
② 등록 신청
③ 인증서 발급 요청
④ 결과 응답
⑤ User에게 인증서 발급
⑥ 인증서를 Directory Server에 저장
⑦ User가 Application Server에게 접속 시도
⑧ Application server가 Authentication server에게 user의 접속 시도를 알림
⑨ User가 인증서 password를 입력하여, 자신의 신분을 확인시킴
⑩ AS가 User에게 valid ticket 발행
⑪ User는 ticket을 이용해 Application Server에게 service 요청
⑫ Application Server는 이 ticket의 유효성 확인 후 user에게 접속 권한을 주어, service를 이용케 함

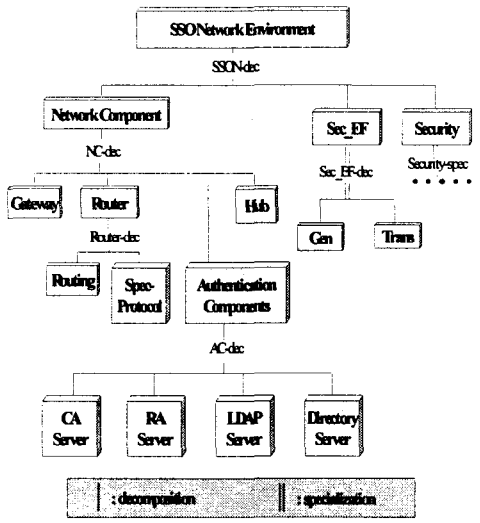


<그림 4> PKI-based SSO 인증 과정

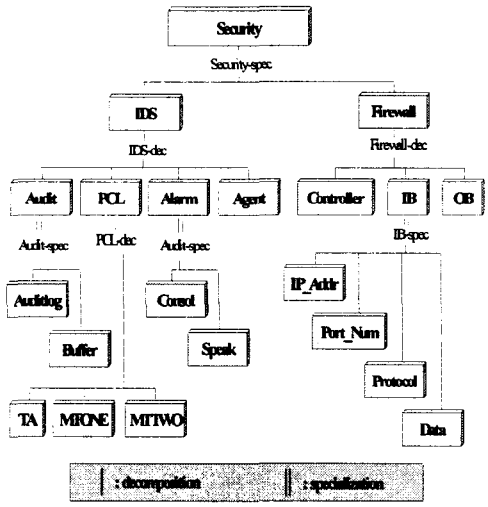
4. 네트워크 모델링 방법론

4.1 대상 네트워크의 SES

<그림 5>은 <그림 3>의 대상 네트워크 구조를 기반으로 구성한 대상 네트워크의 SES이다. 구성된 SSO 네트워크는 크게 Network Component 모델, Sec_EF 모델과 Security 모델로 구성된다. Network 모델은 Gateway 모델, 네트워크 상의 트래픽을 라우팅하는 Router 모델, PKI 기반의 인증 서비스를 제공하기 위한 Authentication Component 모델과 Hub 모델로 구성된다. Sec_EF 모델은 구성된 네트워크에 대한 시뮬레이션 운용을 위해 사용되는 모델로서 패킷을 재생성하기 위한 Gen 모델과 시뮬레이션 수행에 따른 결과를 분석하기 위해 필요한 Trans 모델로 구성된다. Security 모델은 침입 탐지 시스템과 침입 차단 시스템을 포함하고 있는 모델이다. 모델 베이스에는 <그림 5>에 구성된 모델들이 기본 모델과 결합 모델의 형태로 존재하게 된다. 네트워크를 구성하여 시뮬레이션을 수행하고자 한다면 SES를 통해 구조를 만들고 그에 맞는 모델들을 호출하여 시뮬레이션을 수행할 수 있다.



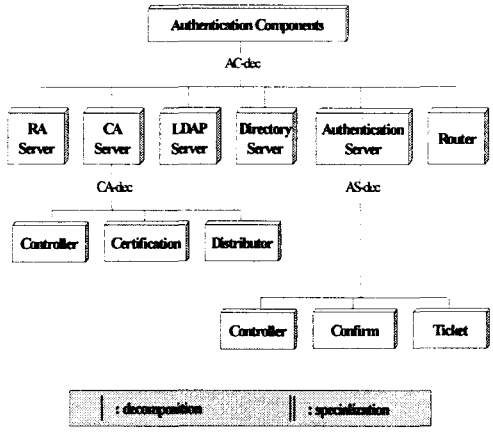
<그림 5> SSO 네트워크의 SES



<그림 6> Security 모델의 SES

<그림 6>은 <그림 5>에 구성되어 있는 Security 모델을 좀 더 자세하게 표현한 SES이다. 본 연구진이 구성한 Security 모델은 크게 IDS 모델과 Firewall 모델로 구성된다. 네트워크 상의 침입을 탐지하기 위한 IDS모델은 Audit 모델, PCL (Packet Classify Library) 모델, Alarm 모델과 실제 침입을 탐지하게 되는 Agent 모델로 구성된다. Audit 모델은 침입 탐지 시스템이 갖고 있는 감사 기능을 위해 구성한 모델로 로그 정보와 같은 Audit 정보를 저장하는 Audit 모델과 네트워크 상에서 수집한 패킷을 임시로 저장하고 각 처리 모듈 간의 이동에 필요한 다양한 종류의 Buffer 모델이 존재한다. PCL 모델은 네트워크 상의 패킷을 본 연구진이 분류한 패킷의 종류에 따라 분류를 해 주는 모듈로서 TA (Task Allocator) 모델과 MTONE 모델, MTTWO 모델로 구성된다. Alarm 모델은 침입이 발생한 경우 관리자에게 알리기 위한 방법을 갖고 있는 모델로서 소리로서 알리기 위한 Speak 모델과 화면에 메시지를 보여 주는 Consol 모델을 구성하였다.

Firewall 모델은 방화벽을 구성한 모델이다. Firewall 모델은 크게 Controller 모델과 IB (Inbound) 모델, OB (Outbound) 모델로 구성된다. IB 및 OB 모델은 다시 4가지의 모듈로 나뉘는데, 각 모델은 패킷의 어떠한 정보에 따라 필터링을 수행할 지를 결정할 수 있다. 패킷의 주소에 의한 필터링은 IP_Addr 모델을 통해 필터링을 수행하고, 포트 정보를 이용한 필터링은 Port_Num 모델이 담당한다. 프로토콜에 의한 필터링은 Protocol 모델이 담당하고, 패킷의 데이터에 의한 필터링은 Data 모델이 그 역할을 수행하게 된다.



<그림 7> Authentication Components 의 SES

<그림 7>은 <그림 5>에 구성되어 있는 Authentication Components 모델을 좀 더 자세하게 표현한 SES이다. Authentication Components 모델은 RA Server 모델, CA Server 모델, LDAP Server 모델, Diectory 모델, Authentication Server 모델과 Router 모델로 구성된다. CA Server 모델은 Controller 모델, Certification 모델과 Distributor 모델로 구성되고 Authentication Server 모델은 Controller 모델, Confirm 모델과 Ticket 모델로 구성된다.

5. 결론

시스템마다 별개로 수행되었던 사용자 계정의 등록/수정/삭제 작업과 권한 설정,접근제어 설정 작업을 중앙에서 한번에 수행할 수 있으며, 모든 사용자 정보가 중앙에 통합됨으로써 시스템 사이의 정보 불일치를 피할 수 있는 인증서 기반의 SSO를 연구하였다. 본 연구진이 제안하는 방법은 소규모 네트워크에서 적용하여 사용하기 수월하도록 구성하였으며 조직의 여러 데이터를 효과적으로 처리할 수 있도록 구성되었다. SSO의 구성은 인증서 기반의 PKI (Public Key Infrastructure)를 사용하여 구성하였으며 인증 통신을 위한 데이터 암호화를 SSL (Secure Socket Layer) 기반의 SHTTP (Secure Hyper Text Transfer Protocol)이 적용되었다. 침입 탐지 시스템 및 침입 차단 시스템의 관리자는 SSO를 사용하여 안전하고 쉽게 네트워크 설정 환경에 접속할 수 있으며 인트라넷의 사용자 역시 네트워크의 서비스를 쉽게 이용할 수 있었다.

향후 과제로는 좀 더 복잡하고 구성 요소가 많은 환경에서 SSO 및 보안 요소들이 동작되도록 구성할 것이며 좀 더 쉬운 사용자 환경을 구성하여 보다 쉽게 SSO를 사용하도록 할 것이다.

참 고 문 헌

[1] Netscape manual, "Single Sign-On Deployment Guide," http://developer.netscape. com/docs/manuals/security/SSO/index.htm

[2] White Paper, "Single Sign-On in Windows2000 Networks," http://www.microsoft. com/TechNet/win2000/win2ksrv/prodfact/nt2ksso.asp

[3] White Paper, "Password Synchronization and Single Sign-On Between Multiple Platform," Microsoft.

[4] 연승호, 박현규, 오수희, 김영헌, 전병민, "공개키 기반 구조에서 KT Single Sign-On 설계," 정보과학회 논문지 : 컴퓨팅의 실제, 제 8권, 제 2호, pp 231-239, 2002.

[5] 이임영, 송유진, 현대암호, pp 109-134, 생능출판사, 1999.

[6] H.S. Seo and T.H. Cho, "An application of blackboard architecture for the coordination among the security systems", Simulation Modelling Practice and Theory, Elsevier Science B.V., vol. 11, issues 3-4, pp. 269-284, Jul. 2003.

[7] Tae H. Cho, Bernard P.Zeigler, "Simulation of Intelligent Hierarchical Flexible Manufacturing : Batch Job Routing in Operation Overlapping," IEEE Transactions on Systems, Man and Cybernetics-PART A : System and Humans, vol. 27, no.1, p.116-126, Jan., 1997.

[8] Zegler, B.P, Cho, T.H. and Rozenblit, J.W., "Knowledge Based System for Hierarchical Flexible Manufacturing System Modeling," IEEE Transactions on Systems, Man and Cybernetics-PART A, vol 26, no.1, p.81-89, Jan., 1996.

[9] 이만영, 김지홍, 송유진, 염흥열, 이임영, 인터넷 보안 기술, 생능출판사, 2002.

[10] E. Amoroso, Intrusion Detection-An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response, Intrusion.Net Books, 1999.

[11] S Mclure, J. Scambray and G. Kurtz, Hacking Exposed: Network Security Secrets

and Solutions, McGraw-Hill, 1999.
[12] R. Bace, Intrusion Detection, Macmillan Technical Publishing, 2000.
[13] E. D. Zwicky, S. Cooper and D. B. Chapman, Building Internet Firewalls second edition, O'reilly & Associates, 2000.
[14] Avolio and Blask, "Application Gateways and Stateful Inspection : A Brief Note Comparing and Contrasting," Trusted Information System, Inc., 1998.
[15] M. R. Lyu, K. Y. Lau, "Firewall Security : Policies, Testing and Performance Evaluation," Proceeding of CSAC 24th Annual International, pp. 116-121, Oct. 2000.
[16] 김지연, "PKI 구성 객체의 상호 연동을 위한 명세서 분석," 한국 정보보호 센터, 1998.
[17] Netscape manual, "Introduction to Public-Key Cryto graphy," http://developer.netscape.com/docs/mannuals/security/pkin/index.htm
[18] White Paper, "Windows 2000 public Key Interoperability," Microsoft.
[19] Netscape manual, "Access Control Programmer's Guide," http://developer.netscape.com/docs/manuals/enterprise/accessapi/contents.htm

서희석

2000. 2. 성균관대학교 산업공학과 졸업 (공학사).
2002. 2. 성균관대학교 전기전자 및 컴퓨터공학부 졸업 (공학석사).
2002. 3. ~ 현재 성균관대학교 정보통신공학부 박사과정 재학 중.
관심분야 : 네트워크 보안 시뮬레이션, 지능형 시스템, 취약성 분석.

김희완

1987년 광운대학교 전자계산학과 졸업(이학사).
1988년 한국전력공사 정보처리처(DBA)
1995년 성균관대학교 정보공학과(공학석사)
1996년 정보처리 기술사(정보관리 부문) 취득
1999년 정보시스템 감리인(한국전산원) 자격 취득
2002년 성균관대학교 전기전자 및 컴퓨터공학부 (공학박사)
1996년 삼육의명대학교 전산정보과 조교수
2001년 삼육대학교 컴퓨터과학과 조교수
관심분야 : 컴퓨터 및 네트워크 보안, 동시성 제어, 분산 DB, 보안 시뮬레이션