Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.2.261

국내 보안관제 체계의 현황 및 분석

박시장* · 박종훈**

Current Status and Analysis of Domestic Security Monitoring Systems

Si-Jang Park* · Jong-Hoon Park**

요 약

국내 보안관제센터들의 현황을 검토하였으며, 보안관제 체계의 특징인 패턴기반 보안관제체계와 중앙집중형 보안관제 체계에 대한 분석과 장단점을 분석하였다. 또한 국내 보안관제 체계 발전방안에서는 기존 패턴기반의 중앙집중형 관제 체계가 가지고 있는 문제점을 개선하기 위해 이상행위 탐지기반의 허니넷과 다크넷을 분석하여 이를 적용한 발전 방안을 기술하였다.

ABSTRACT

The current status of domestic monitoring centers was reviewed and the pattern-based security monitoring system and the centralized security monitoring system, both of which are the characteristics of security monitoring systems, were analyzed together with their advantages and disadvantages. In addition, as for a development plan of domestic security monitoring systems, in order to improve the problems of the existing pattern-based centralized monitoring system, Honeynet and Darknet, which are based on anomalous behavior detection, were analyzed and their application plans were described.

키워드

Security Monitoring, Darknet, Honeynet, IDS, Anomaly detection, Behavior Detection
보안관제, 다크넷, 허니넷, 침입탐지시스템, 이상탐지, 행위기반탐지

Ⅰ. 서 론

국내 대다수 보안관제센터들은 공통적으로 사이버 공격들의 특징을 추출하여 제작한 패턴을 탐지에 활용하는 패턴기반 보안관제를 근간으로 다수의 소속기관을 모니터링하고 사이버 공격에 대응하는 패턴기반 중앙집중형 보안관리체계를 가지고 있다[1].

이러한 방식은 침입자로부터의 공격을 탐지/차단하기 위해 미리 정의된 침입규칙에 의거해 정형화된 단순 침입시도로부터 내부 시스템과 네트워크등의 자원을 비교적 안전하게 보호할 수 있으나[2], 분석 작업이 선행되어야 하는 특징 때문에 첨예화·지능화 되어가는 해킹에 신속한 대응이 어려운 문제를 안고 있다.

따라서 올바른 현황파악을 위해서 주요 보안관제센터들의 역할 및 특징 등에 대해 분석하고, 문제점 도출을 위해 보안관제센터들이 공통적으로 활용하고 있는 패턴기반 중앙집중형 보안관리체계를 분석하여 장점과 한계점을 파악하고 이를 개선하기 위한 방안 마련을 위해 이상행위 분석과 관련된 연구들을 검토하고 분석한다. 이상행위 분석과 관련된 연구는 크게 허

* KT전남고객본부 SMB컨설팅센터(sijan.park@kt.com)
** 교신저자(corresponding author) : 중부대학교 컴퓨터학과 교수(jhpark@joongbu.ac.kr)
접수일자 : 2013. 11. 13 심사(수정)일자 : 2013. 12. 22 게재확정일자 : 2014. 02. 11

니넷(Honeynet)을 활용하는 방안과 다크넷(Darknet)을 활용하는 방안이 있다. 허니넷은 초기구축 및 지속적인 기술연구 및 유지보수를 위한 비용과 노력을 요구하지만 다크넷은 큰 부담없이 구축이 가능하고 추가적인 관리의 부담도 적어 본 논문에서는 다크넷 기반 보안관제를 권고한다.

II. 국내 보안관제 체계의 특징

일반적인 기관의 정보보호 시스템 구축 경향은 각각의 침해유형에 대처하기 위해 침입차단 시스템(Firewall), 침입방지 시스템(IPS), 유해트래픽 분석 시스템(TMS), DDoS 전용장비 등을 이용하여 보안체계를 구성하였으나 점차 고도화되고 지능적인 공격유형에 대처하기에는 한계점이 나타나게 되었다.

이에 대한 해결책으로 국내에서는 보유하고 있는 다양한 보안장비(Firewall, IDS, IPS, VPN 등)들과 다양한 솔루션을 연동하여 실시간으로 침해위협 트래픽을 모니터링 하는 EMS을 구축하고[3], EMS을 통해 발생하는 보안 이벤트들 사이의 연관성을 분석해 신종공격(Zero-day 공격) 및 대규모 사이버공격 조기탐지 연구를 지속적으로 수행하고 있으며[4], 이를 기반으로 효과적인 공격 탐지가 가능한 패턴기반 보안관제를 근간으로 중앙집중형 보안관리체계를 채택하여 운용중에 있다.

2.1 패턴기반 보안관제체계

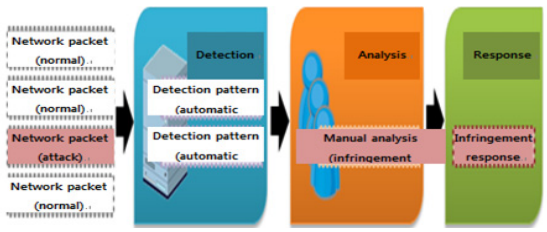

그림 1. 패턴기반 보안관제 개념도
Fig. 1 Conceptual diagram of pattern-based security monitoring

앞에서 언급한 국내 부문보안관제센터들은 패턴기반의 중앙집중형 보안관제체계를 가지고 있다. 패턴기반의 보안관제체계는 그림 1과 같이 탐지, 분석, 그리고 대응 프로세스를 거쳐 사이버 공격을 확인하고 대응하는 체계이다.

① 탐지 : 사전에 알려진 공격들을 분석, 특징을 추출해 만든 탐지패턴들과 네트워크에 유입된 트래픽을 비교분석하여 사이버공격 위험이 존재하는 보안 이벤트들을 자동 검출하여 보안관제 모니터링 시스템 및 보안관제 요원에게 제공한다.

② 분석 : 기존에 분석된 사고이력과 비교분석, 보안관제 인력의 노하우 활용 등의 과정을 거쳐 탐지된 보안 이벤트들이 실제 사이버 공격과 연관이 있는지를 확인한다.

③ 대응 : 분석과정에서 '사고'로 판단되는 항목들에 대하여 보안 이벤트가 탐지된 관제대상기관에 통보하고 대응방안 마련을 권장한다. 통보내용에는 판단의 근거가 되는 분석 자료와 사고조치에 필요한 대응방안 등의 정보를 포함한다.

2.2 중앙집중형 보안관제체계

중앙집중형 보안관제체계는 그림 2와 같이 보안관제 대상기관의 백본 네트워크에 전용 보안장비를 설치하고 이를 통해 보안이벤트를 실시간으로 수집하여 침해대응 활동을 수행하고 있다.

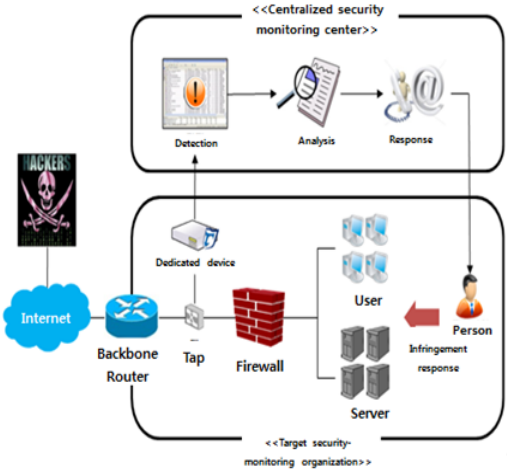

그림 2. 중앙집중형 보안관제체계도
Fig. 2 Centralized security monitoring system diagram

체계를 구성하는 중앙관제센터와 대상기관의 역할은 다음과 같다.

① 중앙관제센터
- 대상기관으로부터 수집된 보안 이벤트를 취합하고 관제인력에게 제공하는 통합 관리 시스템 구축
- 보안 이벤트 탐지를 위한 패턴 개발 및 공유
- 24시간 보안 이벤트 모니터링/분석 (관제인력)
- 사고인지 시 대상기관에 통보 및 대응지원

② 대상기관
- 관제구간 정의 및 전용장비 배치
- 중앙관제센터에서 제공하는 탐지패턴 전용장비에 적용
- 사고통보 수신 시, 사고 시스템 분석 및 대응 조치 수행 중앙집중형 보안관제체계는 관제체계 구축예산, 보안 전문인력 등을 중앙 관제센터에서 제공하므로 예산 효율성과 부족한 보안인력 수급 문제해결 효과가 특징이다.

2.3 국내 보안관제체계의 장·단점

국내 부문보안관제센터들은 위에서 언급된 패턴기반 보안관제체계와 중앙집중형 보안관제체계를 결합해 사용하고 있다. 따라서 국내 보안관제체계는 두 체계의 분석을 통해 이뤄질 수 있다. 앞서 살펴본 두 체계의 특징을 미루어 살펴본 국내 보안관제체계의 장점은 다음과 같다.

① 효용성 : 보안관제 대상기관 백본 네트워크에서 수집되는 전체 보안이벤트를 수집함으로써 보안관제 영역에 대한 전반적인 침해위협 동향 수집·분석이 용이하다.

② 일관성 : 전용 보안장비를 활용하여 보안이벤트를 수집하기 때문에 보안정책(탐지패턴) 개발·적용이 용이하고 이를 통해 일관성 있는 침해대응활동을 수행할 수 있다.

③ 신속성 : 해킹공격에 대한 사전징후 포착 시 전용 보안장비에 대한 보안정책 일괄적용이 용이하며, 동일한 구성이기 때문에 특정 기관에서 발생한 구조적 문제 또는 해킹사례를 분석하여 보안관제 영역 전반에 신속히 전파할 수 있다.

그러나, 해킹 기술의 진화와 함께 해킹 시도가 지속적으로 증가하면서 기존 보안관제체계는 다음과 같이 다양한 한계점을 보이고 있다.

① 신·변종 공격 대응 : 탐지패턴의 특성 상 새로운 기법이 도입된 신종 공격이나 패턴 우회 등을 목적으로 일부 코드, 암호화 기법 등을 조작한 변종 공격에 대한 대응방안이 전무하다. 사이버 공격의 기법은 꾸준히 발전하고 있고, 탐지우회 시도가 증가하고 있는 실정에서 신·변종 공격에 대한 탐지 및 대응방안의 필요는 절실하다.

② 대규모 공격 대응 : DDoS나 스팸공격과 같은 대규모 보안 이벤트를 발생시키는 공격은 신속한 분석과 대응조치를 필요로 한다. 이러한 대규모 공격은 급속히 증가하고 있는 실정이나 보안 이벤트를 건별로 분석하는 패턴기반 보안관제체계에서는 신속한 대응이 어렵다.

③ 이상징후 대응 : 사회공학 기법, 은닉 채널 통신, 맞춤형 악성코드, 제로데이 취약점 등을 활용한 APT공격은 공격대상 사전분석, 시스템 장악 등의 행위가 사전에 이뤄지며 공격이 발생하는 시점에는 사전 확보된 경로를 통해 시스템 마비, 목표정보 획득 등의 행위가 이뤄진다. 공격 이전에 발생하는 이상 징후들은 패턴을 통한 탐지가 어려운 것이 특징이며, 탐지가 이뤄진다 하더라도 직접적인 피해가 없는 것으로 간주되어 사고처리가 이뤄지지 않는 케이스가 대부분이다.

④ 정탐과 오탐 : 공격 시도가 아닌데 공격으로 오인하는 현상, 즉 정탐(False Positive)이 발생할 수 있다. 패턴 매치 기법은 알려진 공격 패턴을 기록한 룰을 통해 트래픽 패턴을 비교하는 방식이지만 정보를 구성하는 문장의 맥락을 이해하지 못하고 룰에 기록된 패턴과의 일치 여부만을 검사함으로써 발생할 수 있는 가장 전형적인 오류라고 볼 수 있다. 또한 공격 시도를 탐지하지 못하는 현상, 즉 오탐(False Negative)의 발생이다. 알려진 공격 패턴이 없으면 룰을 만들 수 없고, 룰이 없으면 당연히 트래픽 패턴과 비교할 대상이 없기 때문에 탐지가 불가능하다.

위 패턴기반 보안관제와 중앙집중형 보안관제는 침입자로부터의 공격을 탐지/차단하기 위해 미리 정의된 침입규칙에 의거하여 시스템과 네트워크를 감시를 통해 효율성, 일관성, 신속성의 기능을 제공하지만 신·변종 공격 대응, 대규모 공격 대응, 이상징후 대응 및 정탐과 오탐 등과 같은 다양한 유형의 공격과 침입규칙에 포함되지 않은 새로운 공격방식에 대한 대처가 불가능하며, 침입대응 시간에서 많은 문제점을 가지고 있다[5].

III. 국내 보안관제 체계의 발전방안

2장에서 설명한 기존 보안관제의 한계점을 극복하기 위하여 네트워크 상의 이상행위를 조사·분석하는 다양한 연구가 진행되고 있다. 이상탐지(Amomaly Detection) 기법은 비정상 탐지라고도 불리며, 모니터링하는 트래픽이 트레이닝 데이터를 사용하여 구축된 정상 트래픽 프로필과 일치하지 않는 경우 이를 공격으로 간주하여 탐지하는 방식이다. 따라서, 통계적인 접근(전문가 시스템, 신경망, 데이터마이닝, Hidden Markov Models 등)을 통해 새로운 공격 탐지확률을 높일 수 있는 반면 평균적인 오탐율도 동반하여 증가한다는 단점을 갖는다.

또한, 네트워크 상에서 발생되는 다양한 악성행위 정보를 수집하기 위하여 가장 보편적으로 활용되는 방법은 허니넷(Honey-Net) 또는 다크넷(Darknet)이다. 허니넷이란 공격자를 함정에 빠뜨리기 위한 '꿀딴지'를 의미하며, 공격자의 관심을 유발하는 네트워크 자원을 고유하여 침입을 유도하는 네트워크를 의미하기도 한다. 이에 반해, 허니팟은 컴퓨터 프로그램에 침입한 스팸과 컴퓨터바이러스, 공격자를 탐지하는 가상컴퓨터로 침입자를 속이는 최신 침입탐지기법을 통해 마치 실제로 공격을 당하는 것처럼 보이게 하여 침입자를 추적하고 정보를 수집하는 역할을 수행하는 시스템을 의미한다.

일반적으로 허니팟은 공격자의 정보를 얻기 위한 하나의 개별 시스템으로 구성되어 있어 자신에게 보내진 패킷만 처리하기 때문에 비교적 구성이 간단하고 고성능의 시스템이 요구되진 않지만 해당 포트로 유입되는 패킷만 수집하기 때문에 네트워크 전반에 대한 침입정보를 분석할 수 없는 단점이 있다. 또한 공격자가 허니팟을 발견한 후 이 시스템의 접근을 피하거나 허니팟을 마비시키는 공격을 가할 수도 있으며, 허니팟이 침해를 당하고 다른 시스템 공격에 사용된다면 전체 조직의 보안에 위험을 줄 수 있다.

이에 반해, 허니넷은 그림 3과 같이 허니팟, 호스트, 보안 솔루션을 포함한 하나의 네트워크 구조로 구성되어 있다[6].

허니넷은 실제 적용에 있어 유연성이 있으며 데이터 수집 및 경보 능력이 아주 뛰어나 다양한 시스템 및 응용프로그램에 적용할 수 있는 확장성을 지니고 있다. 하지만, 공격자와의 높은 상호작용으로 인해 보안의 위험성이 따를 수 있으며 설정 및 구축이 복잡하여 관리운영을 위한 전담인력을 필요로 한다는 단점이 있다[5].

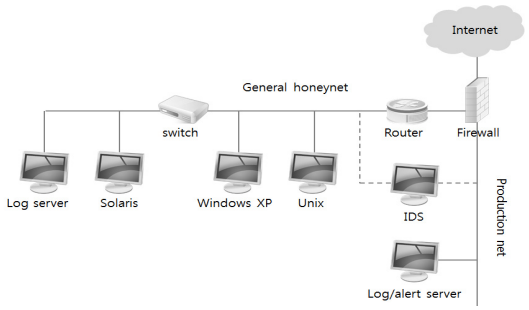

그림 3. 허니넷 구성도
Fig. 3 Structural diagram of honeynet

다크넷은 그림 4와 같이 할당(사용)되지 않은 IP주소공간을 의미하며, 일반적으로 해당 IP대역에서 발생하는 네트워크 트래픽을 모니터링 하는 인터넷 시스템이라는 의미로도 쓰인다[7].

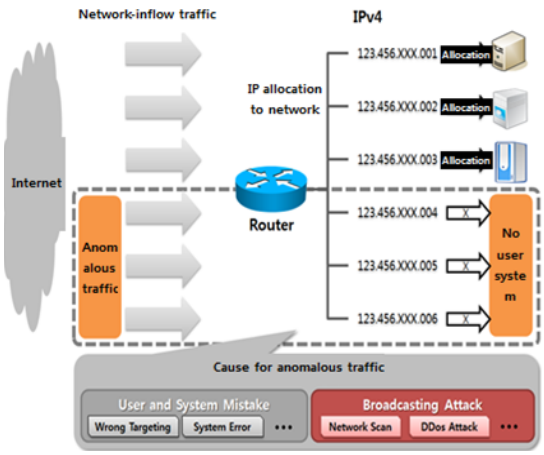

그림 4. 다크넷 시스템 구성도
Fig. 4 Structural diagram of darknet system

일반적으로 허니넷과 동일한 목적으로 구성하지만 실제 시스템이 존재하지 않는 유휴 주소자원을 할당하기 때문에 2차 피해를 사전에 방지할 수 있다는 장점을 가지고 있다.

따라서, 보안관제 체계 발전방안으로는 대규모 네트워크 상에서 발생되는 알려지지 않은 해킹시도인

이상행위를 수집하기 위하여 다크넷(Darknet) 개념을 확장하고, 수집된 이상행위 정보를 기반으로 기존의 패턴기반의 보안관제 체계와 추가적인 다크넷 기반의 이상행위 통계적 기법을 통해 해킹공격에 대한 상세 분석을 수행하는 보안관제 모델을 권고한다.

다크넷 트래픽은 정상적인 트래픽을 거의 포함하고 있지 않아 필터링 등의 1차 가공 없이 즉시 분석에 활용이 가능하다. 이를 통해 해킹 유형별 침해대응 이원화를 통해 효율적인 보안관제 서비스 제공을 기반을 마련하였으며 그림 5와 같이 기존 관제 대비 10% 이상의 침입탐지위협을 검출할 수 있는 것으로 파악되었다.

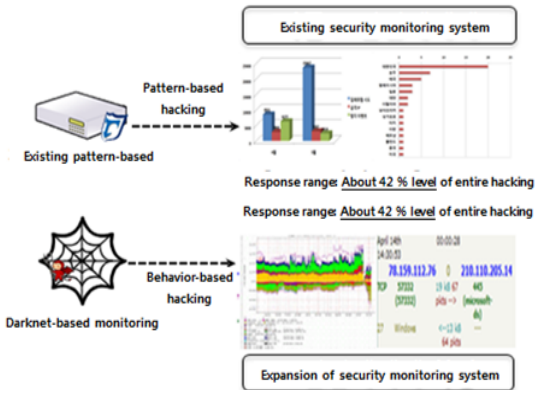

그림 5. 다크넷 시스템을 활용한 침해사고 대응범위 확장

Fig. 5 Expansion of response range to infringement accidents based on darknet system

또한, 선행연구들을 통해 해킹 기술에 대한 능동적·체계적 탐지 기반을 확보하여 기존의 탐지패턴 기반의 해킹탐지 기술과 신규 구축된 행위 기반의 해킹탐지 기술의 효율적인 연계를 통해 그림 6, 그림 7과 같이 DoS공격 및 IP위변조 공격 등에 대한 신종·변종 및 대규모 사이버공격에 대한 조기 탐지를 감지할 수 있다.

이처럼 다크넷 트래픽을 활용하면 실시간으로 진행되는 사이버 공격의 유형, 공격 트래픽 크기, 공격 근원지 정보 등 네트워크 침해사고 현황을 쉽게 알 수 있어 선진국에서는 허니팟·허니넷 기술과 함께 이상징후 탐지 및 분석 분야에 다양하게 활용되고 있다.

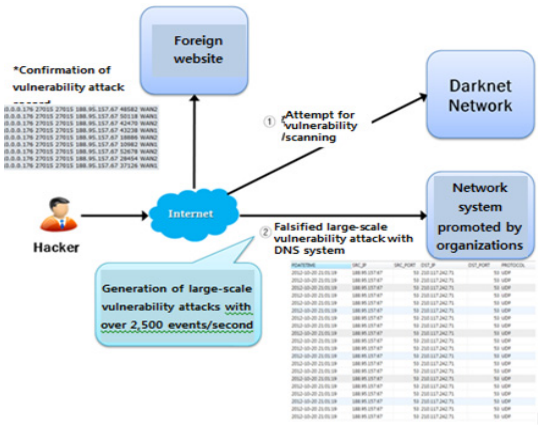

그림 6.서비스공격거부(DoS) 공격 탐지

Fig. 6 Detection of denial-of-service(DoS) attack

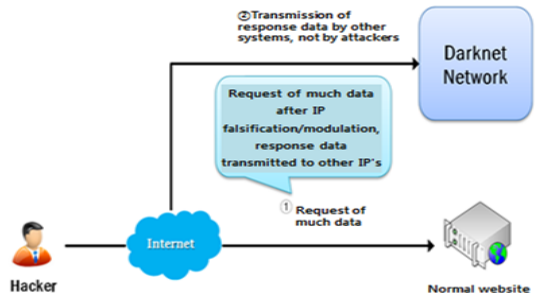

그림 7. IP 위변조 기반의 서비스거부공격(DoS) 시도 탐지

Fig. 7 Detection of dos attack attempts for IP falsification/modulation base

Ⅳ. 결 론

본 논문에서 국내 보안관제센터들의 현황을 검토하였으며, 보안관제 체계의 특징인 패턴기반 보안관제체계와 중앙집중형 보안관제 체계에 대한 분석과 장단점을 분석하였다. 또한 이에 대한 문제점을 개선하기 위한 국내 보안관제 체계 발전방안을 기술하였다. 보안관제 체계 발전방안으로 대규모 네트워크 상에서 발생되는 알려지지 않은 해킹시도인 이상행위를 수집하기 위하여 다크넷(Darknet) 개념을 확장하고, 수집된 이상행위 정보를 기반으로 통계적 기법을 통해 해킹공격에 대한 상세분석을 수행하는 보안관제 모델을 권고한다.

참고 문헌

[1] T. Nam, S. Kim, S. Lee, J. Ji, and S. Son, "Reliable Next Generation Network Security System," *Korea Information Protection Academic Association J.,* vol. 6, no. 5, 2003, pp. 1-12.

[2] W. Seo and M. Jun, "A Study on the Realization of Diskless and Stateless Security Policy Based High-speed Synchronous Network Infrastructure," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 6, no. 5, 2011, pp. 676-679.

[3] W. Seok and M. Jun, "A Study on the 3D-Puzzle Security Policy in Integrated Security System Network," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 5, no. 4, 2010, pp. 425-434.

[4] J. Song, H. Takakura, and Y. Kwon, "A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts," The 2008 Int. Symp. on Applications and the Internet(SAINT2008), *The IEEE CS Press,* Aug. 2008, pp. 51-56.

[5] C. Kim, D. Kang, and I. Euom, "The Case of Novel Attack Detection using Virtual Honeynet," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 7, no. 2, 2012, pp. 279-285.

[6] P. Mun, "Honeypot and Honeynet for Network Security Analysis," *Collected Papers of Pyeongtaek University,* vol. 16, 2002, pp. 353-363.

[7] T. Ban, L. Zhu, J. Shimamura, S. Pang, D. Inoue, and K. Nakao, "Behavior Analysis of Long-term Cyber Attacks in the Darknet," *ICONIP (5),* 2012, pp. 620-628.

저자 소개

박시장(Si-Jang Park)

2007년 호남대학교 인터넷소프트웨어학과 졸업(공학사)
2009년 호남대학교 소프트웨어공학과 졸업(공학석사)
2013년 호남대학교 컴퓨터공학과 졸업(박사수료)
1994년 한국전기통신공사 입사
2008년~현재 KT전남고객본부 SMB컨설팅 팀장
※ 관심분야 : U-City설계, VoIP, 정보보안

박종훈(Jong-Hoon Park)

1987년 광운대학교 전자계산기공학과 졸업(공학사)
1989년 광운대학교 대학원 컴퓨터공학과 졸업(공학석사)
1995년 광운대학교 대학원 컴퓨터공학과 졸업(공학박사)
1999년~현재 중부대학교 컴퓨터학과 교수
※ 관심분야 : XML웹서비스, 시맨틱 웹, 정보보안a