Virtual Honeynet을 이용한 신종공격 탐지기술 개발

강대권* · 엄익채** · 김천석***

A Development of Novel Attack Detection Methods using Virtual Honeynet

Dae-kwon Kang* · Ieck-chae Euom** · Chun-suk Kim***

요 약

지난 수년간 Honeynet은 공격자의 공격 도구, 공격 기법 및 공격동기를 배울 수 있는 보안 메커니즘으로서의 가치가 충분히 입증되었다. 이러한 정보는 다양한 위협에 대한 조직의 대응을 위한 핵심 정보로 활용되어 보다 효율적인 보안을 위한 기초자료가 되고 있다. 그러나 Honeynet활용의 문제점 중 하나는 구축에 많은 자원이 요구되며, 구축 및 운영관리가 어렵다는 문제이다. Honeynet 구축을 위해서는 다수의 시스템들과 다양한 보안 메커니즘을 필요로 한다. 본 논문에서는 최근 IT분야의 화두로 떠오르고 있는 가상화(Virtualization) 기술을 이용하여 기존의 Honeynet의 가치를 그대로 유지하면서도 기존 Honeynet의 자원문제, 구축 및 운영관리문제를 줄일 수 있는 Virtual Honeynet 모델을 제시하고자 한다.

ABSTRACT

A honeynet is a closely monitored computing resource that we want to be probed, attacked or compromised. More precisely, a honeypot is "an information system resource whose value lies in unauthorized or illicit use of that resource

The value of honeynet is weighed by the information that can be obtained from it. but It's very difficult to deploy Honeynet in Real World, So I focused on Virtual Honeynet. The strength of virtual honeynet is scalability and ease of maintenance. It is inexpensive to deploy and accessible to almost everyone. Compared with physical honeypots, this approach is more lightweight. Instead of deploying a physical computer system that acts as a honeypot, we can also deploy one physical computer that hosts several virtual machines that act as honeypots.

키워드

Virtual Honeynet, Honeypot, High-Interaction Honeypots

Ⅰ. 서 론

오늘날 거의 모든 비즈니스는 컴퓨터와 네트워크에 의해서 이루어지므로 이들에 대한 보안의 중요성이 나날이 증가하고 있다. 수십 년간의 연구와 실제 경험을 가지고 있음에도, 우리는 여전히 안전한 컴퓨터 시스템(Secured Computer System)을 만들어내고 있지 못하고 있으며, 컴퓨터 시스템의 보안 수준을 정확히 측정조차하고 있지 못하는 상황이다. 공격자(Attacker)는 공격 코드의 자동화 및 취약점의 스캐닝을 통하여 시스템 취약점을 알아냄과 동시에 컴퓨터 시스템을 장악하고 있다. 이러한 스캔공격 및 공격 코드로부터 보안을 강화할 수 있는 한 가지 방법은 네트워크상에 침해가 예상되는 컴퓨터를 설치하여 이를

* 전남대학교 전자통신공학과(kang7233@kdn.com) ** 한전KDN 정보보호사업팀(ice@kdn.com)
*** 교신저자 : 전남대학교 전자통신공학과(kim1000s@chonnam.ac.kr)
접수일자 : 2010. 06. 24 심사(수정)일자 : 2010. 07. 15 게재확정일자 : 2010. 08. 05

모니터링 함으로써 공격자의 새로운 공격기법이나 공격도구에 대해서 배우는 것이다[3],[7]. 이러한 컴퓨터 시스템을 Honeypot이라하고 다수의 Honeypot으로 구성된 네트워크를 Honeynet이라고 한다. 공격자의 공격 기법이나 도구에 대해서 학습하기 위해서는 그러한 컴퓨터들에 대한 모든 연결에 대해 로깅하고 모니터링 하여야 하며 알려진 취약점들에 대해서 알고 있어야 한다. 낮은 상호작용(low-interaction) Honeypot은 일부 서비스나 TCP/IP의 일부 특성만을 시뮬레이션 한다. 높은 상호작용(high-interaction) Honeypot은 운영체제의 모든 측면을 시뮬레이션 하므로 보다 풍부한 정보를 얻을 수 있는 반면, 분석 및 관리가 어려워지는 심각한 부작용이 내포되어 있다. 즉, 공격자가 Honeypot을 장악하는 경우, 해당 시스템은 타 시스템을 공격하는 데에 이용될 수 있다. 따라서 높은 상호작용 Honeypot은 보다 세밀한 관리 및 주의가 필요하다[3],[7].

본 논문에서는 최근 IT분야에서 주목을 받고 있는 가상화 (Virtualization) 기술을 응용하여 기존의 높은 상호작용 Honeypot의 장점을 살리는 동시에 단점을 보완할 수 있는 새로운 Virtual Honeynet의 모델 및 방법을 제시하고자 한다.

II. 현재의 Honeynet 기술

2.1 Honeypot 개요

Honeypot이란 네트워크 침해를 유도하고 이를 상세히 분석하여 공격자의 공격의도, 기법, 도구 등을 분석하여 신종 공격기법에 대한 분석 및 대응을 통하여 보안을 강화하기 위한 도구로 정의 할 수 있다[3]. Honeypot은 임의의 운영체제 및 임의의 서비스를 설정할 수 있다. Honeypot의 가치는 Honeypot을 통하여 수집하는 정보의 양과 종류에 직접적으로 비례한다. 정보 수집과는 별개로, Honeypot은 공격자가 보다 가치 있는 시스템을 공격하는 것으로부터 혼선을 줄 수 있다는 장점과 신종 공격 또는 공격 동향에 대한 조기 경보 시스템으로서의 장점 그리고 공격자의 공격 기법 및 도구에 대한 심도 있는 분석이 가능하다는 장점이 있다. 또 다른 기능으로서는 공격자가 시스템을 침해할 때, 시도했던 모든 행위를 수집할 수 있다. 앞서 설명한대로, 낮은 상호작용 및 높은 상호작용의 두 가지 수준의 Honeypot이 있으며 다음 두 가지 종류의 Honeypot 구성이 가능하다: 물리적(Physical) Honeypot은 실제 IP주소를 가지는 시스템을 사용하는 것이며, Virtual Honeypot은 하나의 시스템에 여러 대의 가상 시스템을 시뮬레이션 하는 방식이다[7]. 물리적 Honeypot은 흔히 높은 상호작용으로 분류되는데 그 이유는 완전하게 침해될 수 있으며, 설치 및 유지 관리 비용이 많이 들기 때문이다. 예를 들면, 일정범위의 IP주소들을 모두 Honeypot으로 사용하기 위해서는 각각의 IP주소와 1대1로 매핑되는 Honeypot을 설치하여야 한다. Virtual Honeypot은 흔히 낮은 상호작용으로 분류되는 데, 그 이유는 구현 및 유지관리 비용이 낮고, 하나의 Virtual Honeypot은 여러 대의 운영체제, 서비스 및 TCP/IP stack을 한 대의 물리적 시스템에서 시뮬레이션할 수 있기 때문이다. 그러나 엄밀한 의미에서 Virtual Honeypot도 2가지로 구분할 수 있는데, 첫번째는 Honeyd와 같은 단일 프로그램을 이용하여 여러 개의 운영체제, 서비스, TCP/IP stack을 시뮬레이션 하는 낮은 상호작용 방식과 최근 IT분야의 화두로 떠오르고 있는 가상화 기술을 이용하여 물리적 Honeypot과 같은 서로 다른 실제 시스템을 한 대의 시스템에 설치하여 관리하는 높은 상호작용방식으로 구분할 수 있다[3], [7].

이 절에서는 후자의 방식을 이용한 Honeynet의 구성, 정보 수집 및 분석 이슈에 대하여 논의하고자 한다.

2.1.1 가상화를 이용한 Virtual Honeynet 구성

Virtual이라는 용어는 여러 개의 서로 다른 운영체제가 여러 대의 서로 다른 컴퓨터에서 실행되는 것과 동일한 효과를 한 대의 컴퓨터에서 달성하는 것을 의미하며 따라서 Virtual Honeynet은 한 대의 컴퓨터에서 모든 것을 실행시킨다. 이러한 개념이 가능한 이유는 가상화 소프트웨어를 이용하여 한 대의 컴퓨터에서 여러 대의 가상 컴퓨터를 시뮬레이션하고 그 위에 여러 개의 실제 운영체제를 실행 시키는 것이 가능하게 되었기 때문이다. 근본적으로 Virtual Honeynet은 새로운 개념은 아니며 단지 Honeynet 기술을 가상화 소프트웨어를 이용하여 한 대의 컴퓨터에 구현하는 개념이다. 이러한 접근 방식은 기존의 Honeynet과 비

교할 때 고유의 장점과 단점을 가지게 된다. 장점은 명백한 비용절감과 유지 관리가 용이하다는 점이며, 단점은 현재의 가상화 소프트웨어가 Intel X86계열의 하드웨어 시뮬레이션만이 가능하므로 해당 아키텍처를 지원하는 제한된 운영체제만을 지원한다는 점과 공격자가 가상화 소프트웨어를 장악할 경우, 전체 Honeynet이 공격자에 의해 장악될 수 있다는 점 그리고 Honeynet이 가상화 소프트웨어 위에서 실행되고 있다는 점을 공격자가 알아낼 수 있다는 점이다.

Virtual Honeynet은 두 가지로 분류할 수 있는데, 독립모델과 혼합모델로 나눌 수 있다. 독립 모델은 단일 컴퓨터에 Honeynet을 설치하는 방식이며, 혼합모델은 데이터 수집 및 데이터 통제를 별도의 Gateway에서 처리하며, Honeynet은 별도의 서버에서 실행하는 방식이다. 각각은 고유의 장점과 단점을 가지게 된다[3], [7]

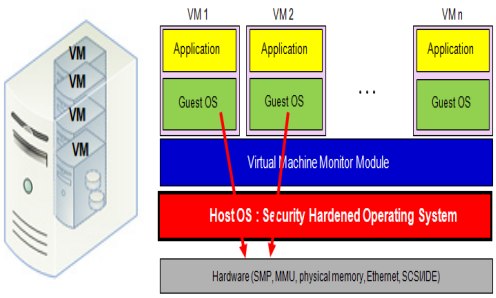

그림 1. Virtual Honeynet 독립모델의 구조
Fig. 1 Separate Model Structure of Virtual Honeynet

독립모델의 장점은 :

- 이동성(Portability)이 높다(한 대의 컴퓨터에 Honeynet을 탑재하여 어디든 가지고 다닐 수 있다)
- 임의의 네트워크 구간에 설치하여 공격을 탐지/분석할 수 있다.
- 적은 비용으로 구축할 수 있다.

단점으로는:

- 단일 실패점이 될 수 있다. 즉, 컴퓨터가 고장인 경우, 전체 Honeynet을 사용할 수 없게 된다.
- 모든 Honeynet이 가상화 소프트웨어를 공유 하므로 Hoeynet의 다른 부분(예 : 방화벽)도 영향을 받을 수 있으므로 보안측면에서 불리하다.
- 운영체제의 선택이 제한적이다. (Intel X86지원)

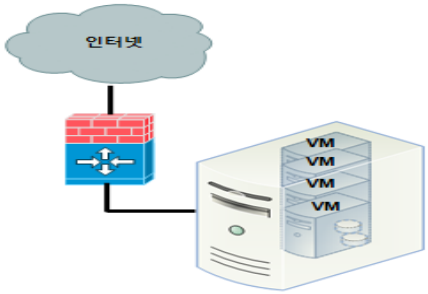

그림 2. Virtual Honeynet 혼합모델의 구조
Fig. 2 Hybrid Model Structure of Virtual Honeynet

혼합모델의 장점은:

- 보안성이 높다. 즉, 공격자는 Honeynet내 다른 Honeypot만 접근가능하다.
- 유연성이 높다. 즉, 데이터 통제를 위해서 다양한 보안 솔루션을 사용할 수 있다. 또 Honeypot이외의 다른 Physical 서버를 둘 수 있다.

단점으로는:

- 여러 대의 컴퓨터로 구성되므로 이동성이 낮다.
- 구축비용이 높다
- 운영관리가 복잡하다. 하지만 실제세계에서는 독립모델이 보다 일반적이다.

현재 수많은 가상화 소프트웨어가 존재하므로 다양한 방식으로 Virtual Honeynet을 구성할 수 있다. 아래 표 1은 가용한 가상화 소프트웨어의 일부를 보여준다[4].

표 1. 주요 가상화 (Virtualization) 소프트웨어 비교
Table 1. The comparison of Main Virtualization Software

제품명	제조사	지원 Host CPU	지원 Guest CPU	Host OS	지원 Guest OS	라이센스 형태
SUN xVM Server	SUN	X86-64bit SPARC	X86-64bit, SPARC	필요 없음 (Baremetal기반)	WindowsXp-2003, Linux, Solaris	무료 (GPL-Version3)
SUN xVM VirtualBox	SUN	X86-32bit X86-64bit	X86-32bit X86-64bit	Windows, Linux, Solaris, MAC OS	DOS, Windows Linux,FreeBSD Solaris	무료 (GPL-Version2)
VMWare ESX Server	VM ware	X86-32bit X86-64bit	X86-32bit X86-64bit	필요없음 (Baremetal기반)	Windows,Linux Netware,Solaris FreeBSD	유료

VMWare Server	VM ware	X86-32bit X86-64bit	X86-32bit X86-64bit	Windows, Linux	DOS, Windows Linux,FreeBSD Solaris,V-Appliance	유료
VMWare Workstation6.0	VM ware	X86-32bit X86-64bit	X86-32bit X86-64bit	Windows, Linux	Windows,Linux Netware,Solaris V-Appliance	유료
VMware Player 2.0	VM ware	X86-32bit X86-64bit	X86-32bit X86-64bit	Windows, Linux	Windows,Linux Netware,Solaris V-Appliance	배포 무료
User Mode Linux	Jeff Dike	X86-32bit X86-64bit PowerPC	X86-32bit X86-64bit PowerPC	Linux	Linux	무료 (GPL-Version2)

2.2 Virtual Honeynet을 이용한 Data 수집 및 분석

Honeypot 모니터링은 모든 Honeypot에서 필수적인 부분이다. 전통적으로는 네트워크 기반의 모니터링과 호스트 기반의 모니터링 2가지 접근 방법을 동시에 사용하고 있다. 네트워크 기반의 모니터링은 Honeynet으로 유입/유출되는 모든 트래픽을 수집하여 이를 TCPDUMP 및 Ethereal 등으로 스니핑하는 방법을 사용하며, 호스트 기반 모니터링에서는 Honeypot 내부에 특수한 센서를 설치하여 관심 있는 이벤트를 수집하는 방법을 사용한다[3],[6]. 위의 두 가지 방법은 상호보완적 기능을 수행하므로 유용한 정보의 분석을 위해서는 두 가지를 사용하는 것이 바람직하다. 본 절에서는 기존의 호스트 기반 및 네트워크 기반 데이터수집 및 분석에 관한 접근 방법을 살펴보고 본 논문에서 제시하는 데이터 수집 및 분석의 새로운 접근 방법을 제시하여 Honeypot의 효율성을 극대화 할 수 있는 방안에 대해서 논의하고자 한다.

2.2.1 호스트 기반 데이터 수집 및 분석 방법

호스트 기반 데이터 수집방법에는 여러 가지 방법이 있을 수 있으나, 높은 상호작용 Honeypot에서 가장 널리 사용되고 있는 Sebek에 대해서 살펴보면: (1) 우선 Sebek은 자신을 loadable kernel module로서 원래 운영체제의 민감한 system calls 대체한다[6], [8]. 즉, 약 11가지 system calls: sys open, sys read, sys readv, sys pread64, sys write, sys writev, sys pwrite64, sys fork, sys vfork, sys clone, sys socketcall. 이러한 System call을 intercept하여 해당 system table 엔트리를 겹쳐 쓴다. (2) 겹쳐쓰기가 성공할 경우, 대체된 system call handler는 해당 system call의 매개변수 및 context 정보 (예: UID 또는 PID)를 수집하고 본래 system call 서비스를 완료한다. (3) 마지막으로 수집된 정보를 분석을 위하여 은밀하게 신뢰하는 서버로 전송한다.

2.2.2 네트워크 기반 데이터 수집 및 분석 방법

네트워크 기반의 모니터링은 Honeynet으로 유입/유출되는 모든 트래픽을 수집하고 이를 TCPDUMP 및 Ethereal 등으로 스니핑하는 방법을 사용하며 분석을 위해 서버로 전송한다[6],[8]. 이러한 정보는 원시 데이터이므로 유용한 정보를 추출하기가 매우 어렵다. 그 이후에 개발되어 Honeynet의 De facto Standard로 사용되고 있는 Hflow는 perl로 작성된 데몬으로 각종 네트워크 기반 데이터 종합에 사용되는데, 주요 기능은 (1) IDS 이벤트, Sebek의 socket 통신 기록, p0f 운영체제 핑거프린팅, Flow 데이터를 종합하여 관계형 데이터베이스에 저장한다. (2) 이러한 데이터를 이용하여 네트워크에 접속한 상대방 운영체제 정보 인식, 네트워크 연결이후 발생한 IDS 이벤트 호스트 상의 사용자나 프로세스 감시 등을 수행한다[7], [9].

III. 개선된 Honeynet 시스템

3.1 서비스 공격 의도(Intention) 확인 기반의 Data 수집 및 분석 기법

2.2절에서 소개한 전통적인 호스트 및 데이터 네트워크 기반의 데이터 수집 및 분석 기법은 매우 유용하다. 하지만, 의심스러운 이벤트에 대한 분석을 위해서는 운영자의 많은 데이터를 분석하여야 하며 또 전문적인 지식을 필요로 한다. 따라서 본 논문에서는 전통적인 데이터 수집 및 분석 기법과 차별화 되는 공격 의도 확인 기반의 데이터 수집 및 분석 기법을 제시함으로써 분석해야할 데이터양을 최소화하고 분석을 최대한 자동화하는 동시에 Honeynet의 데이터 수집능력을 극대화하는 기법을 제시하고자 한다.

3.1.1 서비스 공격의도(Intention) 확인 기반의 호스트 기반 데이터 수집 및 분석 기법

Sebek에서 주요 system call을 가로채어 데이터를 수집하는 방법과는 달리, 서비스 공격의도 확인 기반의 호스트 기반 데이터 수집 및 분석 기법에서는

TCP, UDP, ICMP에서 각각 66,535개의 포트를 이용하여 서비스를 제공한다는 점에 착안하였다. 즉, 공격자나 악성 코드의 전파행위를 위해서는 사전에 각각의 서비스 제공여부를 스캐닝을 하게 되는데, 초기 스캐닝에서는 아무런 서비스가 제공되지 않는 것처럼 보이도록 한다.

이후에 같은 포트(서비스)에 대해 추가적인 스캐닝을 하는 경우, 해당 서비스를 제공하고 있는 것처럼 서비스를 시뮬레이션하고, 이후에 공격자나 공격코드의 모든 행위를 수집하는 방식이다. 이러한 방식은 집요하지 않은 공격자를 배제하는 동시에, 공격의도를 가진 공격자나 자동화된 악성코드(예: 웜)의 반복적인 전파행위만을 파악하고 이후에 발생하는 모든 행위를 기록할 수 있다는 장점을 가지게 된다. 이러한 접근방식을 통하여 전통적인 호스트기반 데이터 수집방식에서의 데이터양의 문제와 전문성이 요구되는 분석의 어려움을 획기적으로 개선할 수 있게 된다. 즉, 공격의도를 가진 공격자와 악성코드에 대한 데이터를 선발하고 선발된 행위에 대해서만 집중적으로 데이터를 수집하고 수집된 데이터를 자동화할 수 있게 된다. 이러한 데이터 수집 및 분석 방식을 위해서는 Sebek과 마찬가지로 특수한 센서를 Honeypot내에 설치하여야 함은 동일하나, 공격의도를 가진 공격만을 선별하여 데이터를 수집함으로써 수집 데이터 량을 최소화 할 수 있으며, 분석을 자동화 할 수 있으므로 Honeypot의 효율성을 극대화 할 수 있다.

3.1.2 서비스 공격의도 확인 기반의 네트워크 기반 데이터 수집 및 분석 기법

3.1절의 서비스 공격의도 확인 기반의 호스트 기반 데이터 수집 및 분석 기법에서는 공격의도를 가진 공격만을 선별하여 데이터를 수집함으로써 수집 데이터 양을 최소화 할 수 있으며, 분석을 자동화 할 수 있는 기법을 제시 하였다. 이러한 호스트 기반 데이터에서 의심스러운 행위에 대한 풍부한 분석 데이터를 제공하기 위해서는 Honeynet으로 유입/유출되는 모든 트래픽 데이터를 수집한다. 수집 후에는 전통적인 Honeypot에서 제공하였던 TCPDUMP 및 Ethereal 등으로 스니핑하는 방법을 사용한다. 하지만 Honeynet으로 유입/유출되는 트래픽 데이터를 모두 수집하고, 호스트 기반 분석에서 분석할 데이터 량을 최소화 하였음에도 불구하고 네트워크 데이터 분석의 어려움은 여전히 존재한다. 보다 효율적인 데이터 분석 및 문제에 빨리 접근하기 위하여 본 논문에서는 Focus-oriented 분석 기법을 사용하였다. 즉, 호스트 기반 데이터 수집 및 분석부에서 추출한 관심 데이터에 대해여 보다 상세한 분석을 원할 경우, 수집된 네트워크 기반 데이터 Pool에서 분석하여야 한다. 이러한 경우, 호스트 기반 데이터를 이용하여 네트워크 기반 데이터 Pool을 검색할 경우, 추출된 결과 데이터 Pool위에 Focus를 좁혀서 다시 분석할 수 있으며, 이러한 구조는 원하는 분석 결과를 얻을 때까지 반복적으로 수행할 수 있다. 이렇게 함으로써 운영자는 분석 범위를 최소화 할 수 있으므로 보다 효율적으로 원하는 결과에 보다 빨리 도달 할 수 있게 된다.

Ⅳ. 결 론

Honeypot은 공격자나 악성코드에 의한 네트워크 기반 공격을 탐지하고 분석하는 데 있어 매우 유용한 도구로 사용되어 왔다. 그러나 Honeypot의 설치 및 운영에는 많은 물리적 비용과 시간적, 지적 비용이 발생한다. 따라서 신종 공격에 대한 공격의도, 공격기법, 공격도구 등을 파악하여 보안에 효율성을 기할 수 있다는 엄청난 가치에도 불구하고 유지운영이 용이하지 않다는 문제점이 있다. 본 논문에서는 가상화 기술을 이용하여 물리적 비용을 최소화할 수 있는 방안을 제시하였고, 공격의도확인 기반의 데이터 분석 수집 및 분석 기법 그리고 Focus-oriented분석 기법을 제시하여 운영에 필요한 비용을 최소화할 수 있는 Virtual Honeynet의 모델을 제시하였다. 본 논문에서 제시된 Virtual Honeynet은 공격의 분석 측면에서는 데이터 양의 최소화 그리고 분석 비용의 최소화를 달성하였다. 그러나 공격자가 가상화 기술의 사용여부를 어렵지 않게 파악 할 수 있으므로 현재에는 자동화된 악성코드나 초중급 공격자에 적용될 수 있다. 고급 공격자에게도 적용할 수 있기 위해서는 가상화 기술의 사용여부를 은닉할 수 있는 기법, 악성코드 수집 및 분석 기술은 향후에도 개선되어야 할 점으로 남아있다.

참고 문헌

[1] F. Raynal et el, Honeypot Forensics Part I: Analyzing the Network, IEEE(Security&Privacy), pp105-121, 2004.

[2] F. Raynal et el, Honeypot Forensics, Part II: Analyzing the Compromised Host, IEEE(Security&Privacy),pp10-25, 2004.

[3] Honeynet Project: Know Your Enemy: Defining Virtual honeynets, http://www.honeynet.org, 2003.

[4] Wikipdeia, Comparison of platform virtual machines, http://en.wikipedia.org/wiki/Comparison_of_platform virtual_machines

[5] E. Alata1 et el, Lessons learned from the deployment of a high-interaction honeypot, Eurécom, pp12-50, 2006.

[6] X. Jiang, et el."Out-of-the-box" Monitoring of VM -based High-Interaction Honeypots, RAID, pp84-96, 2007

[7] The Honeynet Project. http://www.honeynet.org.

[8] Sebek. https://projects.honeynet.org/sebek/

[9] HFlow, https://projects.honeynet.org/hflow/

[10] G. Bednarski et el, Understanding Network Threats through Honeypot Deployment, CMU, pp 273-306, 2004.

저자 소개

강대권(Dae-kwon Kang)

1984년 2월 광운대학교 전자통신공학과 졸업(공학사)
1988년 8월 한양대학교 산업대학원 전자공학과 졸업(공학석사)
2010년 5월 현재 : 전남대 전자통신공학과 박사과정
현재 : 한전KDN(주) 진주지점장
※ 주 관심분야 : 정보보호, 전력IT컨설팅

엄익채(Ieck-chae Euom)

2003년 8월 전남대학교 컴퓨터정보공학과 졸업(공학사)
2003년 8월 ~ 2007년 9월 LG이노텍 신뢰성S/W Lab
2007년 10월 ~ 현재 : 한전KDN 정보보호사업팀
저서 : Start Up! 웹마스터 (2002, 웅보출판사)
※ 주 관심분야 : 인프라 가상화 분야 정보보호

김천석(Chun-suk Kim)

1980년 9월 광운대학교 전자공학과(공학사)
1982년 9월 건국대학교 대학원 전자공학과(공학석사)
1998년 경남대학교 대학원 전자공학(공학박사)
1982년 11월 ~ 현재 : 전남대학교 전자통신공학과 교수
※주 관심분야 : 수중통신, 정보통신분야