http://dx.doi.org/10.14400/JDC.2014.12.10.299

Efficient Security Method Using Mobile Virtualization Technology And Trustzone of ARM

Hwi-Min Choi[*], Chang-Bok Jang[**], Joo-Man Kim[*]

Dept. of IT Engineering, Pusan National University[*] R2soft co., LTD.[**]

모바일 가상화 기술과 ARM의 Trustzone을 사용한 효율적인 보안 방법

최휘민[*], 장창복[**], 김주만[*]

부산대학교 IT응용공학과[*], (주)R2soft[**]

Abstract Today, a number of users using smartphone is very rapidly increasing by development of smartphone performance and providing various services. Also, they are using it for enjoying various services(cloud service, game, banking service, mobile office, etc.). today's mobile security solution is simply to detect malicious code or stay on the level of mobile device management. In particular, the services which use sensitive information, such as certificate, corporation document, personal credit card number, need the technology which are prevented from hacking and leaking it. Recently, interest of these mobile security problems are increasing, as the damage cases been occurred. To solve the problem, there is various security research such as mobile virtualization, ARM trustzone, GlobalPlatform for mobile device. Therefore, in this paper, I suggested efficient method that uses the mobile virtualization techniques of certification, security policy and access control, password/key management, safe storage, etc. and Trustzone of ARM for preventing information leakage and hacking.

Key Words : Mobile Virtualization, Trustzone, Mobile Security, GlobalPlatform

요 약 최근, 스마트폰의 사용자 수는 스마트폰 성능 향상 및 다양한 서비스 제공으로 인해 매우 빠르게 증가하고 있다. 스마트폰 사용자들은 클라우드 서비스, 게임, 뱅킹 서비스, 모바일 서비스 등의 다양한 서비스를 사용한다. 오늘날의 모바일 보안 솔루션은 악성코드를 검출하거나 모바일 장치를 관리하는 수준에 그치고 있다. 이에 인증서, 법인 문서, 개인의 신용 카드 번호와 같은 보안에 민감한 정보에 대해 서비스 해킹 및 누설을 방지하는 기술이 필요하다. 모바일 보안 기술은 피해가 발생한 사례가 있었던 만큼 최근에 관심이 증가하고 있다. 이러한 문제를 해결하기 위해서 모바일 가상화, ARM Trustzone, Globalplatform과 같은 다양한 모바일 장치의 보안 기술이 연구되었다. 따라서 본 논문에서는 정보 유출 및 해킹을 방지하기 위한 인증, 보안 정책 및 액세스 제어, 암호/키 관리, 세이프 스토리지 등의 모바일 가상화 기술과 ARM의 Trustzone의 효율적인 방법을 제안한다.

주제어 : 모바일 가상화, Trustzone, 모바일 보안, GlobalPlatform

Received 12 August 2014, Revised 19 September 2014
Accepted 20 October 2014
Corresponding Author: Joo-Man Kim
(Pusan National University)
Email: joomkim@pusan.ac.kr

ISSN: 1738-1916

1. Introduction

Recently, a number of government agency and corporation to build smartwork environment is increasing for effective conduction of business work. So, cases which introduce the mobile office application which can be operated on mobile devices(smartphones, tablet PC, etc.) are also on the rise in that you can easily build smartwork environment without much cost. But today's mobile security solution is simply to detect malicious code or stay on the level of mobile device management. In order to overcome these limitations of mobile security and the problems, it is needed that mobile virtualization-based security technology which fuses mobile security technologies with virtualization technology, can be run on a variety of mobile devices, and can be operated on the latest Android and Linux operating system for smartwork environment[1,2,3,4]. Various method has studied to solve the mobile security problem, and I proposed security method to fit smartwork environment through research about mobile security technology.

2. Related Works

2.1 Virtualization Technology

Mobile virtualization technology has been used across many different embedded systems. Its technology has been represented by a very thin software abstraction layer called virtual machine monitor (VMM) or hypervisor[1,2,6,7]. A common platform comprises hardware, operating system, and user applications in the vertical order. But hypervisor enables a single device to look like multiple devices. Thus, different operating systems can run independently and simultaneously on each virtual machine created by VMM. So, two different domains simply refer to two separate operating systems on each own machine that could be physically identical or not. One of main purposes to use it is to maximize the hardware utilization in a single device[1,2].

Generally, those domains are isolated each other and are not permitted by the illegal access between separate hardware machines. The domain isolation is valuable for security and reliability of the software systems. The reason VMMs hold great potential for security is that they can play an important role in creating separate domains in a physically single machine[1,2].

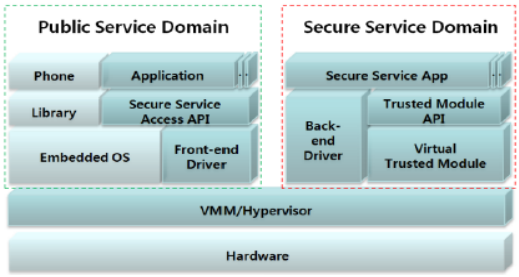
Various techniques have been proposed to implement VMMs according to their design principles such as compatibility, performance, and simplicity[1,2,4,5].

2.2 Mobile Security Technology

Recently, mobile virtualization techniques have been used for reinforcing the system security and reliability because they provide isolated domains on which various systems with different security policies reside simultaneously[1,2,11]. Several studies are effective virtualization to analyze malicious code or to prevent mobile device from trying hacking. Access control technology deployed in the VMM or hypervisor to authorize the permission of an access to the hardware resource, for enhancing the security of this virtualized environment[9,10]. Recently, it has been worked that research which uses Near Field Communication (NFC) to enforce strict security policy in a separate hardware that is apart from the application processor. A technique which security functions are inside the dedicated USIM card provide a high secure environment for the high security demanding services such as mobile payment, banking, etc. However, mobile device's resource is limited and its power is deficient to process various services[11]. One of the traditional trusted computing platforms on desktop or server computing was to use security coprocessor or secure crypto processor. Among them, TCG's Mobile Trusted Module published a specification detailing facilities mobile device should offer. Such a TPM, this mobile

hardware module has some roots of trust for integrity measurement[12], status, and report for platform integrity as well as key information and primitives for cryptographic functions. MTM can be an alternative implementation of the Virtual Trusted Module inside the Secure Service Domain[8].

2.3 TEEMO Technology

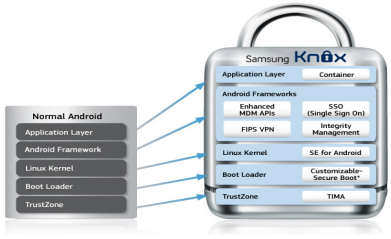


[Fig. 1] TEEMO Architecture

TEEMO is virtualization-based secure execution environment for mobile platform which was suggested in ETRI[1, 2]. The object of their design is to provide two separate domains with different security policies and to offer secure service from a isolated virtual machine in a safe way. Isolated domains, secure service, virtual trusted module, and inter-domain communications were explained as major design principles towards the realization of the goal. On top of that, three different service modes possible for the various secure service models are provided inside the Secure Service Domain.

2.4 Samsung KNOX Technology

Samsung KNOXTM is the comprehensive enterprise mobile solution for work and play[13]. With the increasing use of smartphones in businesses, Samsung KNOX addresses the mobile security needs of enterprise IT without invading the privacy of its employees. Samsung KNOX addresses platform security with a comprehensive three-pronged strategy to secure the system: Customizable Secure Boot*, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA), and a kernel with built-in Security Enhancements for Android (SE for Android) access controls. Customizable Secure Boot ensures that only verified and authorized software can run on the device. Customizable Secure Boot is a primary component that forms the first line of defense against malicious attacks on devices with Samsung KNOX. In addition, Samsung Knox's Secure Boot technology allows the switch of the secure boot root certificate in a secure manner after the devices are shipped. As a result, customers that have high security requirements can purchase regular consumer devices and switch the root-of-trust used for secure boot to better protected ones. Customizable Secure Boot availability varies depending on hardware specification. TIMA runs in the secure-world and provides continuous integrity monitoring of the Linux kernel. When TIMA detects that the integrity of the kernel or the boot loader is violated, it takes a policy-driven action in response. One of these policy actions disables the kernel and powers down the device. ARM and TrustZone are registered trade marks of ARM Limited in the EU and elsewhere. Security Enhancements for Android provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. Security Enhancements for Android isolates applications and data into different domains so that threats of tampering and bypassing of application security mechanisms are reduced while the amount of damage that can be caused by malicious or flawed applications is minimized.



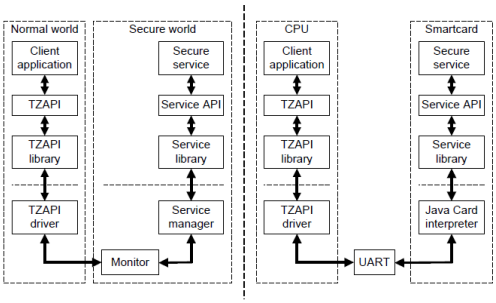
[Fig. 2] KNOX Architecture

2.5 MDM(Mobile Device Management) Technology

Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises[14]. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc. This applies to both company-owned and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers[15][16]. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime[17]. With mobile devices becoming ubiquitous and applications flooding the market, mobile monitoring is growing in importance[18]. Numerous vendors help mobile device manufacturers, content portals and developers, test and monitor the delivery of their mobile content, applications and services. This testing of content is done real time by simulating the action of thousands of customers and detecting and correcting bugs in the applications. Companies are alarmed at the rate of employee adoption of mobile devices to access corporate data. MDM is now touted as a solution for managing these devices in the workplace. The primary challenge is the ability to manage the risks associated with mobile access to data while securing company issued and BYOD (Bring Your Own Device) mobile devices.

2.6 Trustzone of ARM

The TrustZone API (TZAPI) is a programming interface that allows client applications to communicate with an abstract security service in a manner which is independent of the implementation of both the security environment and the security service itself. An implementation of the API can ensure that the communications interfaces are implemented on top of the most suitable underlying physical mechanism available on the hardware platform[19].



[Fig. 3] Two possible systems using the TrustZone API

Client's point of view, the TZAPI decomposes the security environment into four functional blocks[20]:

2.6.1 TrustZone API implementation:

- The nature of the TZAPI implementation is platform-specific, but will typically include a component that exists as library code within the client memory space and a portion within the privileged memory of the host operating system. The component within the operating system, commonly called a driver, is more trusted than the component in the client memory space and may be capable of making some limited security decisions, for example the derivation of client identity to provide login credentials.

2.6.2 Device:

- A single logical device forms the basis of each security environment available on the system. The device provides the entry point to the security environment and manages all connections between the

client and other components of the environment.

2.6.3 Service manager:

• A logical management component that can be used to query installed services, and change the services that are installed within the device.

2.6.4 Services:

• Any number of services running within the security environment, exposing high level security functionality to client applications.

Most of the functions in the TZAPI are designed to enable clients and services to communicate in a robust and efficient manner. Clients and services can communicate through two mechanisms: structured messages, and shared memory. Shared memory is client memory that is mapped directly into the memory space of service.

Structured messages can be used to robustly pass small quantities of data, while shared memory is particularly useful for minimizing the overhead when a service has to deal with large data buffers.

Note that the availability of genuine shared memory depends on the nature of the security environment; some hardware platforms, such a smartcard-based secure environment, cannot support direct mapping of client memory. In these systems the implementation of shared memory may require a memory copy.

• Control functions
- TZDeviceOpen
- TZDeviceClose
- TZDeviceGetTimeLimit
- TZOperationPrepareOpen
- TZOperationPrepareInvoke
- TZOperationPrepareClose
- TZOperationPerform
- TZOperationRelease
- TZOperationCancel
- TZSharedMemoryAllocate
- TZSharedMemoryRegister
- TZSharedMemoryRelease
- TZSystemGetPropertyList
- TZSystemGetProperty

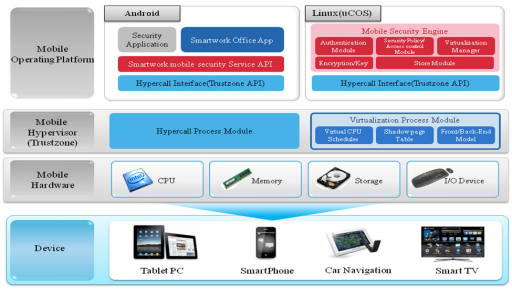
• Encoder and decoder functions
- TZEncodeUint32
- TZEncodeArray
- TZEncodeArraySpace
- TZEncodeMemoryReference
- TZDecodeUint32
- TZDecodeArraySpace
- TZDecodeGetType
- TZDecodeGetError

• Service manager functions
- TZManagerOpen
- TZManagerClose
- TZManagerGetServiceList
- TZManagerGetServicePropertyList
- TZManagerGetServiceProperty

• Asynchronous operations
- TZOperationAsyncStart
- TZOperationAsyncGetResult

• Run-time download and removal of services
- TZManagerDownloadService
- TZManagerRemoveService

3. System Architecture



[Fig. 4] Architecture of MVSP(Mobile Virtualization Security Platform)

In this paper, I have researched the components required to provide security service using mobile virtualization technology in smartwork environment as follows.

3.1 Certificate Component

In order to provide security service in smartwork environment, it needs components to verify user access through the methods of user certification or application certification. In Mobile virtualization-based security technology, two domains (Normal Domain, Security Domain) are divided by mobile virtualization technology. When the Normal Domain users or applications tries to use system resources or security functions in the Security Domain, the system certifies users or applications and creates data to be used in access control. After the system certifies users or applications, the availability of system resources and security functions which belong to the Security Domain should be decided through controlling access of the relevant users or applications. The certification method and means on the users and applications are as follows.

- Certification method
- User certification only
- Application certification only
- User certification + Application certification

- User certification means
- Password entered when the user uses the application
- Password entered when the user log-in the device
+ Password entered when the user uses the application

- Application certification means
- Unique number of the application
- Application hash value

In order for the application which operates in the Normal Domain to access in the Security Domain, it should deliver the certification information to security service supply module in the Security Domain. Based on the certification information, the certification of the users or applications is carried out. If the certification succeeds, various security services can be provided by offering protection of user's certification information and safe services.

3.2 Security Policy and Access Control Component

In order to provide security service in smartwork environment, when it uses security functions in the Security Domain and tries to access resource including important data, components are neccessary to protect.

Even though the process of certification succeeds, the access to relevant security functions and system resources should be differentiated by security policy and access control components. Security policy and access control component functions can be classified into Security Policy Management, Access Authority Decision, and Access Control Authority Execution.

- Security Policy Management Function
- Registration and management of user certification information

- Registration and management of application certification information
- Settings and management of differentiated access authority according to application types
- Certification of users and applications, storage and management of access log information

• Access Authority Decision Function
- Access control level decision of applications according to the security policy
- Access control level decision of users according to the security policy

• Access Control Authority Execution Function
- Security functions & access control permission and execution according to access control authority of applications about important data
- Security functions & access control permission and execution according to access control authority of users about important data

3.3 Password/Key Management Component

As one of core functions to protect important data in the device environment, various password algorithm and key management functions should be provided as security services in smartwork environment. Therefore, the security-related algorithm should be provided as follows:

■ Block Password
- Symmetrical encrypting method: a password is created in each block unit by dividing a plain sentence into regular unit
- International standard password algorithm (AES), Korean password algorithm(ARIA, SEED)
- Support DES and T-DES which are used in existing password system, even though they are not well used these days.

■ Hash Function
- Input message of random length is compressed into output value of fixed length
- SHA method is widely used and default hash algorithm in the Internet.
- MD5 should be included to be compatible with existing application even though this is not well used these days.

■ Public Key Password
- RSA algorithm: the most representative algorithm in public key encrypting method
- ECC algorithm: small-sized key with same security function. Memory and bandwidth can be saved as well as fast calculation speed and low electric consumption compared with RSA. It is suitable for mobile or wireless environment.

■ Key Sharing (Key Exchange)
- In order to operate security function in smartwork devices, safe key distribution is needed between transmitter and receiver. For the key distribution method, Diffie-Hellman Key Exchange Protocol is used. This protocol is designed to a share secret key by using public key password method. It is widely used in common security software these days.

■ Electronic Signature

This algorithm is used when certification is created and electronic signature is written in electronic documents. The electronic signature should satisfy the following conditions:

a. Forge impossibility condition: Only a legitimate signer should be able to create electronic signature on electronic documents.
b. Signer certification condition: Anyone should be able to verify the signer of the electronic signature.

c. Denial impossibility condition: The signer should not be able to deny the validity of his/her own signature after signing.
d. Change impossibility condition: The contents of the signed document cannot be changed.
e. Reusability impossibility condition: The signature of a electronic document cannot be used in other electronic documents.

3.4 Safe Storage Component

Safe Storage Component is to store sensitive information necessary to smartwork. By storing business information and document used in smartwork environment, it is essential component to protect important data against hacking. To restrict random uses of safe storage, it is needed to design only the application program(service) approved by certification can store (or withdraw) data in the safe storage.

4. Major API

〈Table 1〉 major API for functions

Function	Major API	Specification
Control	OPENCHANNEL	Channel Open
	CLOSECHANNEL	Channel Close
	OPENSESSION	Session Open
	CLOSESESSION	Session Close
Password/ Key Management	ND_GETSIGN_PSS ND_GETSIGN_PKCS 1_V15 ND_GETSIGN_KCDS A	Signature Algorithm
	ND_FILE_ENC	File Content Encrytion and Decrytion
Certificate	ND_GETCERTNBR	Certificate number search
	ND_GETCERT	Certificate search
	ND_GETPRIKEY	Private key Search
	ND_GETCERTNKEY	Certificate key Search
	ND_STORECERT	Certificate Store
	ND_STORECERTNK EY	Certificate key Store
	ND_REMOVECERT	Certificate Delete
	ND_REMOVECERTN KEY	Certificate key Delete
Safe Storage	ND_STOREFILE_WI THCONTENT	File Store
	ND_GETFILENBR	File Number Search
	ND_GETFILELIST	File List Search
	ND_GETFILENAME	File Name Search
	ND_GETFILE	File Content Search
	ND_GETFILE_WITH FILENAME	File Content and Name Search
	ND_REMOVEFILE	File Delete
Security Policy and Access Control	ND_CHECKLOGIN	Login Information Check
	ND_INITPIN	PIN Information Initialize
	ND_REGPIN	PIN Registration
	ND_CHANGEPIN	PIN Information Change
	ND_REMAINPIN	Remain Number of Correct PIN Input

5. Conclusion

In this paper, I have suggested efficient method of cloud resource management by using information of available physical resources(CPU, memory, storage, etc.) between mobile devices , and information of physical resource in mobile device. Suggested technology is possible to guarantee real-time process and efficiently manage resources.

Currently, services of server virtualization system in a cloud computing environment target only physical resources. However, in order to build a cloud computing environment, these initial costs, because it takes quite a lot of businesses that want to build a cloud computing environment or a burden on public authorities is another factor. Thus, the rapid development of the resources of the mobile devices that can be used in cloud computing environments is proposed cloud resource management plan. The cloud resource management practices in a variety of mobile devices scattered about the availability of resources, and owns most resources by configuring the device information, and to manage resources efficiently solve the problem.

Mobile virtualization in cloud computing devices available in the physical resources (CPU, Memory, Storage) and efficient management and cloud resources that can be processed in real-time management skills by offering a reduction in the cost of building a cloud computing environment, various embedded devices (TV, car, etc.) can effectively utilize the resources.

REFERENCES

[1] Changbok Jang, Euiin Choi, "Context Model Based on Ontology in Mobile Cloud Computing", Communications in Computer and Information Science, Vol. 199, pp. 146-151, 2011

[2] Hongbin Liang, "Resource allocation for security services in mobile cloud computing", Computer Communications Workshops(INFOCOM WKSHPS), pp. 191-195, 2011

[3] Guan Le, Ke Xu, Song Meina, Song, Junde, "A Survey of Research on Mobile Cloud Computing", Computer and Information Science (ICIS), pp. 387-392, 2011

[4] AMIT GOYAL and SARA DADIZADEH, "A Survey on Cloud Computing", University of British Columbia Technical Report for CS 508, 2009

[5] Young-Ho Kim, Jeong-Nyeo Kim, "Building Secure Execution Environment for Mobile Platform Computers", 2011 First ACIS/JNU International Conference, IEEE, pp.119-122, 2011.

[6] Young-Ho Kim, Yun-Kyung Lee, and Jeong-Nye Kim. "TeeMo: A Generic Trusted Execution Framework for Mobile Devices", Computers, Networks, Systems, and Industrial Application International Conference, SERSC, Vol. 8, pp. 579-583, 2012

[7] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L. Iftode, "Rootkits on Smart Phones: Attacks, Implications and Opportunities," HotMobile '10 Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, pp. 49-54, 2010.

[8] Trusted Computing Group, TCG Specification Architecture Overview Specification, revision 1.4, Aug., 2007.

[9] C. Linn and S. Debray, "Obfuscation of Executable Code to Improve Resistance to Static Disassembly," CCS '03 Proceedings of the 10th ACM conference on Computer and communications security, pp. 290-299, Oct. 2003.

[10] P. Barham et al., "Xen and the Art of Virtualization," ACM SOSP '03 Proceedings of the nineteenth ACM symposium on Operating systems principles, pp. 164-177, Oct. 2003.

[11] TCG, Mobile Trusted Module Specification, ver. 1.0, revision 6, June 2008.

[12] S. M. Lee, S. B. Suh, and B. Jeong, S. Mo, "A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization," IEEE Consumer Communications and Networking Conference, pp. 251-256, Jan. 2008.

[13] J. Y. Hwang and S. B. Suh, "Xen-On-ARM: System Virtualization using Xen Hypervisor for ARM-based Secure Mobile Phones," IEEE Consumer Communications and Networking Conference, pp. 257-161, Jan. 2008.

[14] NFC mobile service standard consortium, "Dynamic management of multi-application secure elements," White Paper, 2008.

[15] R. Sailer, X. Zhang, T. Jeager, and L. Doorn, "Design and Implementation of a TCG-based Integrity Measurement Architecture," 13th USENIX Security Symposium, Vol. 13, Aug. 2004.

[16] T. Garfinkel and B. Pfaff, "Terra: A Virtual Machine-Based Platform for Trusted Computing," SOSP '03 Proceedings of the nineteenth ACM symposium on Operating systems principles, Vol. 37, No. 5, pp. 193-206, 2003.

[17] http://www.samsung.com/global/business/mobile/solution/security/samsung-knox

[18] http://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[19] ARM Security Technology : Building a Secure System using TrustZone Technology, April 2009, ARM
[20] TrustZone API Specification Version 3.0, February 2009, ARM

최 휘 민(Choi, Hwi Min)

- 2013년 2월 : 부산가톨릭대학교 멀티미디어공학과(공학사)
- 2013년 3월 ~ 현재 : 부산대학교 IT응용공학과 석사과정
- 관심분야 : 모바일 컴퓨팅, RTOS, 임베디드 시스템, 통신보안, 센서네트워크
- E-Mail : pololy90@gmail.com

장 창 복(Jang, Changbok)

- 2001년 2월 : 한남대학교 컴퓨터공학과(공학사)
- 2003년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2007년 2월 : 한남대학교 컴퓨터공학과(공학박사)
- 2007년 3월 ~ 현재 : R2soft 연구소장
- 관심분야 : 컨텍스트웨어 컴퓨팅, 유비쿼터스 컴퓨팅, 모바일 클라우드 컴퓨팅, 가상화 및 보안
- E-Mail : chbjang@r2soft.co.kr

김 주 만(Kim, Jooman)

- 1984년 2월: 숭실대학교 전자계산학(공학사)
- 1998년 8월 :충남대 컴퓨터공학(공학석사)
- 2003년 2월 :충남대 컴퓨터공학(공학박사)
- 1985년 1월 ~ 2000년 2월 : ETRI OS팀장(책임연구원)
- 1995년 7월 ~ 1996년 6월 : 미국 Novell사 객원연구원
- 2000년 3월 ~ 현재 : 부산대학교 IT응용공학과 교수
- 관심분야 : 임베디드 시스템, 실시간 시스템, 클러스터 컴퓨팅, 병렬분산 시스템
- E-Mail : joomkim@pusan.ac.kr