클라우드 보안 개요

권혁찬, 정도영, 정병호, 김정녀
한국전자통신연구원

요 약

현재 아마존을 선두로 하여 구글, MS, 애플 등 글로벌 기업들이 클라우드 서비스 시장에 사활을 걸고 뛰어 들고 있으며, 미국, 영국, 일본 등 각국 정부도 클라우드 서비스 활성화를 위한 정책을 수립하는 등 IT 환경이 클라우드 환경으로 급속히 진화하고 있다. 본 고에서는 클라우드 기술을 소개하고 클라우드 환경에서의 보안 위협 및 이에 대응하는 보안기술 및 향후 전망 등에 대해 살펴 본다.

Ⅰ. 서 론

기존 IT환경은 하드웨어 자원을 가상화하여 확장성, 가용성, 민첩성, 가시성 및 경제성을 보장하는 클라우드 가상화 환경으로 급속히 진화하고 있다. 해외의 경우, 아마존이 독식하고 있는 클라우드 시장에 구글, IBM, MS, 애플 등 글로벌 기업들이 사활을 걸고 뛰어들고 있으며, 미국, 영국, 일본 등 각국 정부도 클라우드 서비스 활용에 박차를 가하고자 지원정책을 펴고 있는 상황이다. 미국의 정보기관인 중앙정보국(CIA)과 미국항공우주국(NASA)도 아마존의 클라우드 서비스를 이용하고 있다. 가트너는 2015년까지 보안 기업용 제품 기능 중 10%가 클라우드로 공급될 것이며, VPN/방화벽 시장의 20%가 물리적 보안 장비 대신 하이퍼바이저 상의 가상 스위치에 구축될 것이라고도 전망한다. 또한 가트너가 발표한 2014년 10대 전략기술 중 4개는 클라우드 관련 기술이기도 하다.

국내의 경우에도, 2015년 국내 클라우드 산업 발전을 위한 법적 근거인 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률안(클라우드 발전법)'이 제정되는 등 클라우드 산업 활성화를 위해 다각적인 노력을 기울이고 있는 상황이다.

그러나 클라우드 컴퓨팅 환경에는 가상화 영역을 통한 해킹, 서비스 거부 공격(DoS), 계정탈취는 다양한 형태의 보안 위협이 존재한다. 2015년 10월 미국 정부는, 정부의 민감한 정보를 호스팅하는 클라우드 컴퓨팅 서비스 제공업자에 대한 보안 통제기본사항을 제시하는 가이드라인을 발표하기도 하였고(2015. 01), 2013년 12월 영국에서는 공공부문 조직이 클라우드 제품 및 서비스 도입을 위해 고려해야 하는 보안 원칙에 대한 G-Cloud 가이드라인을 발표하기도 하였다. North Bridge Venture Partners에서 아마존, MS, 우분투 등을 포함한 다양한 산업군을 중심으로 조사한 결과, 클라우드 사용의 가장 큰 부담으로 응답자의 46%가 '보안'을 선택하기도 하였다[1] CSA(Cloud Security Alliance)는 2011년 클라우드 보안을 위한 10종의 구현가이드[2] 문서를 발표하기도 하였다.

이처럼 정부, 기업 등에서 클라우드 도입, 구축을 위해 선결되어야 할 가장 중요한 문제로 바라보는 것은 바로'보안'이다.

본 원고에서는 클라우드 보안에 대한 전반적인 개요를 살펴본다. 먼저 2장에서는 클라우드 컴퓨팅이 무엇인지 그리고 관련 서비스 현황을 살펴 본다. 3장에서는 클라우드 보안 취약점을 살펴보고 4장에서 현재의 클라우드 보안 기술들을 간략히 소개한다.

Ⅱ. 클라우드 컴퓨팅 개념 및 서비스 현황

클라우드 컴퓨팅이란 IT자원을 직접 설치할 필요 없이 '원격으로 빌려 쓰는 서비스' 형태로 제공하는 新 컴퓨팅 패러다임으로, 인터넷상의 서버군을 통하여 데이터 저장, 네트워크, 콘텐츠 사용 등 IT 관련 서비스를 한 번에 사용할 수 있는 컴퓨팅 환경이다. 사용자가 필요로 하는 컴퓨팅 자원(네트워크, 서버, 스토리지, 애플리케이션과 서비스)를 필요로 하는 시점에 즉각적으로, 필요로 하는 양을 유동적으로 제공(On-Demand)하여 컴퓨팅 자원을 효율적으로 활용할 수 있게 해준다.

클라우드 컴퓨팅은 빌려쓰는 자원의 종류에 따라, XaaS(X as a Service)로 분류한다. 클라우드 컴퓨팅이 발전함에 따라 다양

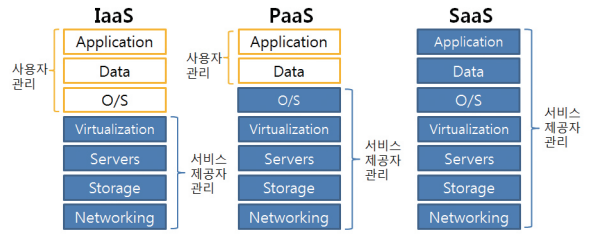

그림 1. IaaS, PaaS, SaaS의 비교

한 분류법이 등장하였으나, SaaS[1], PaaS[2], IaaS[3]로 분류하는 것이 일반적이다. 서비스 제공자가 관리해주는 영역과 사용자가 관리하는 영역에 따라 SaaS, PaaS, IaaS를 비교하면 〈그림 1〉과 같다. SaaS, PaaS, IaaS를 서비스의 대상과 관련제품으로 분류하자면 〈표 1〉과 같다.

표 1. 서비스 대상 및 관련제품

종류	대상	관련제품
SaaS	End-User	Google Apps, Taleo, Salesforces, Dropbox,
PaaS	Developers	Google AppEngine, Windows Azure, force.com
IaaS	System Manager	Amazon AWS, Rackspace

IaaS는 연산능력(CPU + RAM), 저장공간, 네트워크 자원을 가상화하여 사용자에게 제공한다. PaaS는 IaaS에 더하여 OS 환경을 가상화하여 사용자에게 제공한다. SaaS는 PaaS 상에 어플리케이션(및 어플리케이션에서 생성/활용하는 데이터)를 가상화 자원으로 제공한다.

또 다른 분류법으로는 클라우드 컴퓨팅의 기반이 되는 인프라(서버, 스토리지, 네트워크 등)의 소유에 따라 사설(Private), 공용(Public), 혼용(Hybrid)으로 분류하는 방법이 있다. 사설 클라우드는 기업체와 같이 정보의 유출이 민감한 기관에서 선호하는 방식으로 인프라의 소유자와 클라우드 컴퓨팅의 사용자가 동일하다. 공용 클라우드는 일반 사용자가 흔히 접하는 방식으로, 일정한 요금(또는 무료)을 지불하고 사업자가 제공하는 인프라를 사용한다. 혼용은 공용과 사설 클라우드가 혼재되어 있는 방식이다.

미국 NIST는 Cloud Definition Framework를 통해, 클라우드 컴퓨팅의 배치모델(Private, Public, Hybrid), 서비스모델(SaaS, PaaS, IaaS), 주요특성(On-Demand 등), 공통특성을 제시하였다. 이에 대한 개념도는 〈그림 2〉와 같다.

1 Software as a Service
2 Platform as a Service
3 Infrastructure as a service

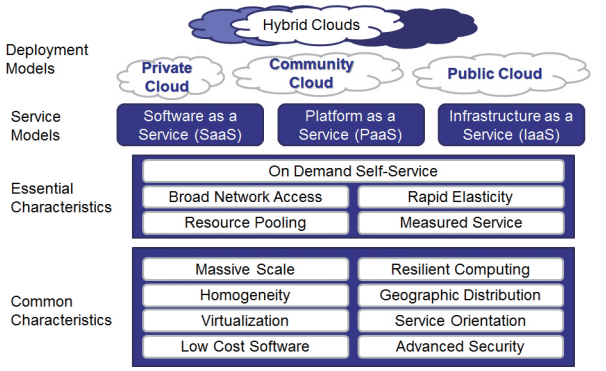

그림 2. The NIST cloud definition framework [3]

클라우드 컴퓨팅이 발전함에 따라 클라우드 서비스 제공자(Cloud Service Provider) 또한 우후죽순으로 등장하고 있으며, 제공하는 서비스의 종류도 다양해지고 있다. 최근에는, 제공하는 서비스의 다양성을 넘어, 서로 다른 클라우드 플랫폼 자원의 공유, 거래를 제공하는 브로커, 거래소까지 등장하고 있다. 대표적인 클라우드 서비스 제공자인 Amazon(AWS, Amazon Web Service), Microsoft(Azure), Google(Google Docs, Drive), Salesforce 또한 계속 시장을 확대해 나가고 있다.

Ⅲ. 클라우드 보안 취약점

클라우드 환경에서는 다양한 보안 위협이 존재하며 실제로 클라우드 서비스 관련 사고 들이 종종 보고되고 있다.

가상머신 자원의 유연한 할당 · 증감, 가상머신 간 상호연결 · 연계 및 다른 호스트 간 · 클라우드 간 가상머신 이동(VM Migration) 등의 특성으로 인하여 다양한 공격 경로가 존재한다.

구체적으로는 가상머신 간 도청, 악성코드 전이, 자원고갈 공격, 의도적인 가상머신 할당 후 이를 활용한 서비스 거부 공격이 있으다. 또한 하이퍼바이저가 악성코드에 감염될 경우 동일 하이퍼바이저 상의 가상머신들에게 악성코드가 감염되어 확산

그림 3. 클라우드 9개 보안 위협 (CSA, 2013)

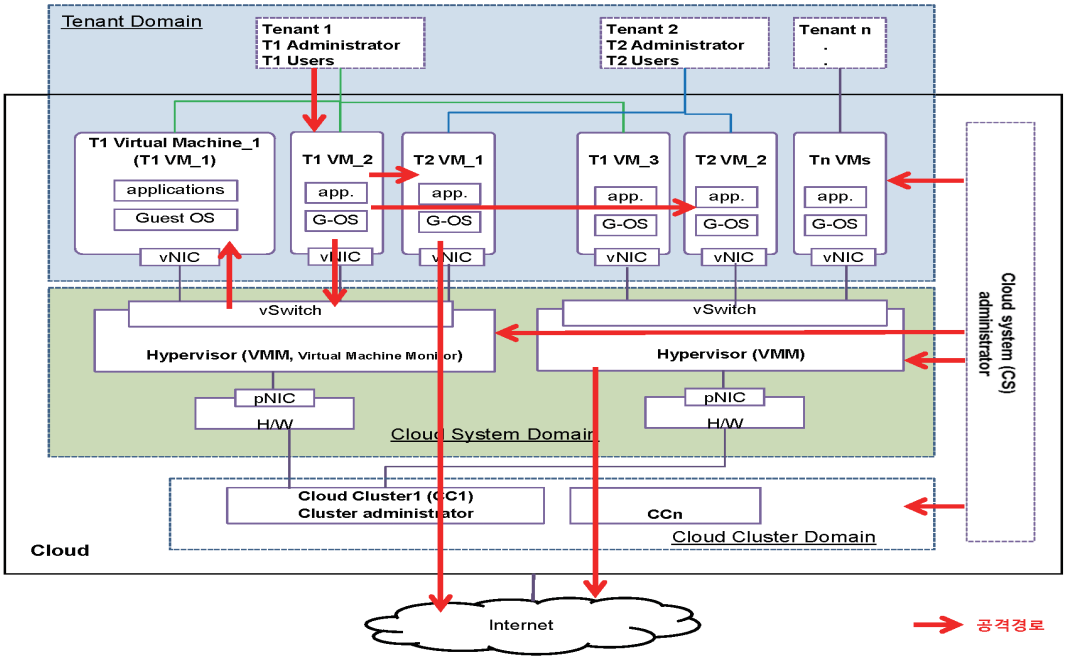

그림 4. 클라우드 공격 경로

될 수 있다. 악성코드가 감염되거나 보안패치가 안 된 가상머신의 이동(VM Migration)에 따라 다른 물리적인 플랫폼으로 위험이 전이될 수도 있다. 가상머신 이동 시 가상머신 이미지 조작, 가상머신 상의 파일 또는 프로세스의 임의 상태 변경 등의 위협 등을 예로 들 수 있다.

〈표 2〉에서는 주요 클라우드 서비스에 대한 보안 사고 발생 사례를 보여주며, 〈그림 3〉에서는 CSA[4]에서 정의한 클라우드 9대보안 위협을 보여준다[4].

〈그림 4〉는 클라우드 구성도 및 공격 경로를 보여준다. 〈그림 4〉 보안 위협을 위협주체별로 분류하여 정리하면 다음과 같다.

■ 위협주체: 악의적인 사용자/공격자

- Tenant VM[5]의 취약점 분석 · 해킹, 악성코드 감염
  - → VM을 통해 VMM[6]을 해킹하여 privileged domain 및 호스트 OS에 불법 접근
  - → 다른 tenant VM들에 대한 DoS 공격
  - → 다른 tenant VM들의 자원(memory, CPU, DB 등) 고갈 공격
  - → VM을 정상 임대하여 DoS 공격 수행
- VMM의 취약성 분석 · 해킹
  - → Privileged domain 콘솔 불법 접근
  - → VMM 자원 스케줄러를 해킹(exploit)하여 인접 VM의 자원을 고갈

표 2. 클라우드 서비스 보안 사고 사례

서비스 제공자	보안사고 사례
구글	태국의 ISP를 이용한 세션 하이재킹 공격 발생
	2011년 2월 27일, 50만명의 이용자가 메시지 및 주소록이 사라지는 사고 발생 (원인규명 안됨)
MS	2010년 12월, 서비스 환경설정 오류로 인해 클라우드상의 기업정보가 타인에게 열람
아마존	2011년 아마존의 가상서버 임대서비스(EC2)에 가명으로 가입 후 가상서버를 대여해 소니 플레이스테이션 네트워크 해킹
애플	2014년 유명 여배우들의 계정 탈취를 통한 누드사진 유출
	2012년 iCloud, Gmail, Twitter 계정분석을 통한 맷호난 기자의 계정 탈취 및 모든 개인자료 삭제
VMWare	2012년 Vmware Image에 CRISIS 악성코드 삽입
Dropbox	2012년 사용자 이메일 명단 유출 및 스팸전송
에버노트	백도어 활동, C&C 서버의 수집정보 은닉 장소로 에버노트 이용 (2013.2)
Vaserv.com	가상화 플랫폼(Hyper-VM)에 대한 제로데이 공격으로 10만 고객사 웹사이트 삭제 (2009.6.8.)
ZenDesk	2013년 2월 ZenDesk 시스템 해킹을 통한 개인정보 유출
DreamHost	2012년 1월 DreamHost DB 해킹으로 인한 개인정보 유출

4 Cloud Security Alliance

5 VM: Virtual Machine, 가상머신

6 VMM: Virtual Machine Monitor. 하드웨어 위에서 여러 가상 머신을 구동시키는 중간 계층으로 하이퍼바이저와 동일한 개념

→ signature wrapping, XSS technique 등을 통해 제어 인터페이스를 해킹하여 공격대상에 대한 완벽한 제어권 획득

- 고도화된 계정탈취, 불법 권한 상승, 취약점 악용을 통한 해킹 공격

■ 위협주체: 악의적인 클라우드 시스템 관리/운영자

- tenants의 runtime state information에 불법 접근 (예: Xen의 Dom0)
- tenant VM의 개인키(private key)를 추출하고, 이를 통한 중간자 가로채기(MITM) 공격
- 다른 tenant의 VM 트래픽 도청, 유출, 위변조
- VM 이미지 위변조, 삭제

■ 위협주체: 악의적인 가상머신

- 침해된 tenant VM이 위장 주소를 이용하여 공격 트래픽 발생 (ICMP flood, UDP flood, TCP SYN flood, Smurf attacks)
- 하이퍼바이저에 루트킷[7] 설치
- 악성코드를 다른 VM으로 전이
- 외부 host에 대한 DoS 공격tenants의 runtime state information에 불법 접근 (예: Xen의 Dom0)

IV. 클라우드 보안 기술 개요

1. 가상화 자원 모니터링 기반 보안 기술

클라우드 컴퓨팅 환경에서는 가상화 기술을 바탕으로 노드(물리적인 컴퓨터) 상에 다수의 가상머신이 동작한다. 하이퍼바이저는 가상머신의 생성/소멸/관리를 담당하며, 가상머신의 관리를 위하여 VMI(Virtual Machine Introspection) 인터페이스가 존재한다. VMI 인터페이스는 가상머신의 CPU 점유율, 메모리 사용량과 하이퍼바이저의 상태정보를 제공하는 인터페이스로, 이를 통해 가상자원의 상태정보를 수집 · 분석하여 위협을 탐지할 수 있다. 〈그림 5〉에서는 가상화 자원 모니터링 기반 보안 기술 개념도를 보여준다. Introspection 엔진은 일반적으로 하이퍼바이저에 탑재되어 위협을 탐지하게 된다.

2. 가상화 네트워크 보안 기술 (Virtual IPS)

하이퍼바이저 상의 가상머신들은 가상화 네트워크를 통해 통신한다. 실제 네트워크와 유사한 위상(topology)으로 가상 네트워크 카드(vNIC), 가상 스위치 (vSwitch) 및 가상 게이트웨이(vGateway)로 구성된다. 가상 네트워크의 가상 스위치와 가상 게이트웨이 단에서는 네트워크 패킷을 수집 · 분석하여 위험을 탐지하는 가상 IPS기술이 개발되어 일부 서비스에 적용되고 있다. 유선 네트워크의 IDS/IPS와 유사한 기능을 가상화 네트워크에서 수행한다고 보면 된다.

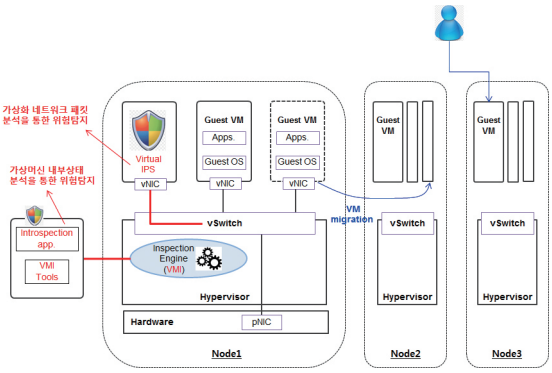

그림 5. 가상화 자원 보안 모니터링 및 가상 IPS 개념도

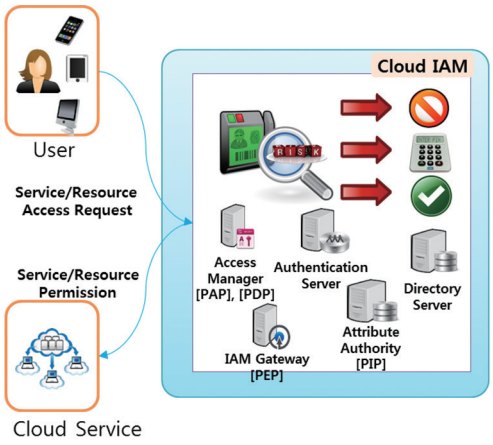

그림 6. 클라우드 IAM 개념도

본 기고문 4.1절의 가상화 자원 모니터링 기반 보안 기술 및 4.2절의 가상화 네트워크 보안 기술에 대한 보다 상세한 내용은 본지의 "안전한 클라우드 환경구축을 위한 가상화 보안 이슈 및 기술 동향" 기고문을 통해 살펴볼 수 있다.

3. 클라우드 IAM

관리자 계정, 가상머신, 데이터 등 자원에 대한접근제어 및 인증을 통하여 인가된 사용자만이 서비스에 접근하고 사용할 수 있도록 하는 기술이다. IAM[8]의 구성요소는 접근제어 정책

7 루트킷(Rootkit): 백도어 기능과 악성행위 은닉 기능을 가진 악성코드

8 Identity Access Management

및 접근제어 대상 자원과의 관계에 따라, PDP[9], PEP[10]등으로 분류된다.

현재에도 클라우드 서비스를 위한 인증/접근제어 기술이 적용되고 있으나, 현 방식은 사회공학적 기법 등을 이용한 고도화된 계정탈취 공격 등에 대응 한계가 있으므로 향후 클라우드에 특화되며 다양한 형태의 계정탈취공격에 대응 가능한 IAM에 대한 요구가 증가할 것으로 예측된다. 클라우드 IAM기술에 대한 상세 내용은 본지의 "클라우드 기반 IAM 기술동향"기고문에 기술되어 있다.

V. 결 론

본고에서는 클라우드 기술을 소개하고 클라우드 환경에서의 보안 위협 및 대응 보안기술에 대해 살펴보았다.

현재 다양한 보안 기술이 개발 및 적용되고 있으나 여전히 보안사고가 계속 보고되는 등 기술적 대책이 필요한 상황이다. 클라우드 환경은 모든 정보가 집중화되어, 보다 강도 높은 인증·접근제어가 요구되지만, 피싱, 소셜 계정 정보연계, 관리적 취약점 이용 등 사회공학적 기법을 포함하여 점점 인증수단 탈취 기법이 다양해지고 있어 이에 대한 기술적 대책도 필요하다.

현재의 클라우드 보안 기술은 가상스위치에 탑재된 에이전트를 통한 네트워크 패킷 분석(가상 IPS) 또는 VMI를 통해 가상화 자원 상태정보를 수집/분석하여 위험을 탐지하여 대응하는 수준이다. 그러나 이러한 기술들은 클라우드 전체 플랫폼의 위협을 종합적으로 탐지하기에는 한계가 있다. 특히 최근 많이 보고되는 내부자에 의한 정보 유출 등 침해공격에 충분한 대응이 어렵다는 문제도 있다. 따라서 가상 네트워크, 가상화 자원, 물리적 호스트에 대한 보안상태 모니터링 및 연계분석을 통한 종합적 대응이 필요하며, 인증/접근제어를 위해서도 사용자의 행위 및 가상자원의 상태를 종합 연계 분석하여 위험도를 산정하고 이를 접근제어에 반영하는 등의 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] North Bridge Venture Partners, "Future of Cloud Computing Survey", 2013.6

[2] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, CSA Research, 2011

[3] NIST (2009). The NIST Cloud Definition Framework. Retrieved March 14, 2011 from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt

[4] Cloud Security Top Threats, CSA, 2013

[5] "VM escape" http://www.zdnet.com/blog/ security/us-cert-warns-of-guest-to-host-vm- escape-vulnerability/12471

[6] "Xen security advisory 19 (CVE-2012-4411). guest administrator can access QEMU monitor console." http://lists.xen.org/archives/html/xen-announce/2012-09/msg00008.html

[7] V. Varadarajan, et al., "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)," in Proc. 2012 ACM Comput. Commun. Security Conf.

[8] J. Somorovsky, et al., "All your clouds belong to us.security analysis of cloud management interfaces," in 2011 ACM Comput. Commun. Security Conf.

[9] Y. Zhang, et al., "Cross-VM side channels and their use to extract private keys," in 2012 ACM Comput. Commun. Security Conf.

[10] R. Beverly, R. Koga, and K. C Claffy, "Initial longitudinal analysis of IP source spoofing capability on the Internet," July 2013. http://www.internetsociety.org/doc/initial-longitudinal-analysis-ipsource-spoofing- capability-internet

[11] J. Idziorek, M. F. Tannian, and D. Jacobson, "The insecurity of cloud utility models," IEEE Cloud Comput., pp. 14.18, May.June 2013.

[12] Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1-37.

[13] Y. Shin, M. Yoon, K. Son, "Design of a Versatile Hypervisor-based Platform for Virtual Network-Host Intrusion Prevention", Proceedings of International Conference on Information Processing and Management (ICIPM), 2013

[14] VMware, "vCloud Networking and Security,"

9 Policy Decision Point

10 Policy Enforcement Point

http://www.vmware.com/products/datacenter-virtualization/vcloud-network-security/

약 력

권 혁 찬

2001년 충남대학교 컴퓨터과학과 박사
2001년~현재 한국전자통신연구원 ICT 융합보안연구실 책임연구원
관심분야: IoT 보안, 의료IT 보안, 융합보안, 무선보안

정 도 영

2012년 KAIST 전산학과 학사(2010), 이학석사
2012년~현재 한국전자통신연구원 ICT융합보안연구실 연구원
관심분야: IoT 보안, 클라우드/빅데이터 보안, 의료IT 보안, 무선보안

정 병 호

1998년~2000년 국방과학연구소 선임연구원
2000년~현재 한국전자통신연구원 ICT 융합보안연구실 실장/책임연구원
관심분야: 무선보안, 의료융합보안, IoT보안, 멀티미디어 보안 등

김 정 녀

1987년 전남대학교 전산통계학과 학사
2004년 충남대학교 컴퓨터공학과 석사, 박사
2005년 Univ. of California, Irvine Post-Doc.
1996년 OSF/RI 공동연구 파견(미국)
1988년~현재 한국전자통신연구원 사이버보안시스템연구부 부장/책임연구원
2015년~현재 과학기술연합대학원대학교(UST) 정보보호 공학과 교수
관심분야: IoT 보안, 모바일 보안, 시스템 · 네트워크 보안, 보안 OS 등