특집 05

모바일 클라우드 보안 이슈 및 대응기술 요구사항

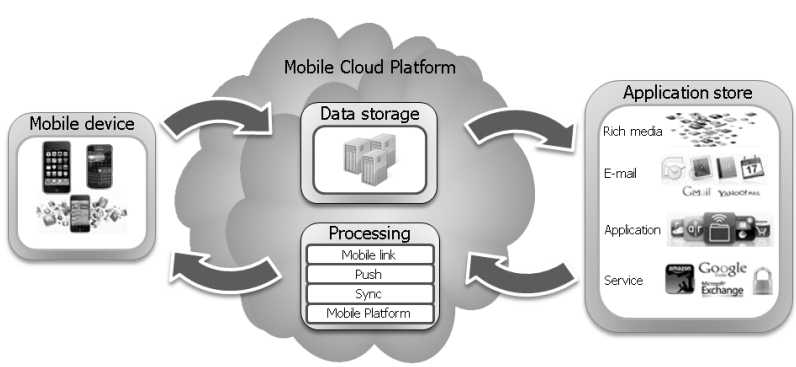
김환국·정현철·원유재 (한국인터넷진흥원)

목 차 »

1. 서 론

모바일 클라우드 서비스는 언제 어디서나 인터넷에 접속할 수 있는 모바일 단말을 통해 클라우드 서비스를 제공하는 것으로서, 모바일 기기의 컴퓨팅 처리 성능 한계, 저장 공간 제약 등으로 인해 모바일 단말에서 처리해야할 작업 및 데이터의 일부를 클라우드 환경으로 이동시켜 처리하는 서비스이다[1]. 최근에는 스마트폰, 테블릿 PC 등 모바일 기기 보급이 확산되고 기업, 개인, 콘텐츠의 클라우드화가 가속화되면서, 클라우드 컴퓨팅 기술과 적용된 모바일 클라우드 서비스에 관심이 고조되고 있다.

국내 클라우드 시장은 '14년까지 2조원 규모로 급성장할 것으로 예상하는 반면, 모바일 클라우드 서비스 활성화의 장애요인으로 서비스의 안정성에 대한 우려, 데이터의 보안성 및 기밀성에 대한 불안감 등 보안에 대한 우려가 높다. 특히 모



(그림 1) 모바일 클라우드 서비스

바일 서비스와 클라우드 서비스가 융합되어, 각각의 위협이 복합적으로 파생되어 발생될 것으로 예상되나, 모바일 기기의 분실로 인한 정보유출, 외부에 위탁한 정보에 대한 접근통제 우회, 가상화 취약성을 이용한 공격, 자원 집중화에 따른 DDoS 서비스 장애 등 클라우드 환경에 위한 보안 위협에 대해 기존 IT 보안 기술로도 충분히 대응이 가능한지와 모바일 클라우드 특성에 최적화된 보안 기술에 대한 요구사항에 대한 분석이 구체화되지 못하고 있는 실정이다.

이에 본 논문에서는 2장에서 모바일 클라우드 서비스 특성을 기존 IT 서비스와 비교하고, 3장에서 모바일 클라우드 특성에 따른 보안 이슈를 살펴보고, 제4장에서는 모바일 클라우드 보안기술에 대한 요구사항을 정리한다.

2. 모바일 클라우드 서비스 특성

IT 서비스 환경이 개인용 PC 환경에서 클라우드 컴퓨팅으로 변하면서, 인터넷을 통해 대용량의 컴퓨터 집합(Cloud)에 접속하여 애플리케이션, 스토리지, OS 등 필요한 IT 자원을 원하는 시점에 필요로 하는 만큼 골라서 사용하는 IT 서비스 패러다임이 변화 하였다. 이에 따라, 기존의 컴퓨팅 환경에서는 이용자가 데이터 및 컴퓨팅 자원, 소프트웨어를 직접 소유・관리해야 했지만, 클라우드 컴퓨팅 환경에서는 컴퓨팅 자원 및 소프트웨어를 클라우드 서비스 사업자로부터 임대하여 사용한다. 다시 말해, 이용자는 모든 자원을 가상화된 형태로 인터넷을 통해 제공받을 수 있다.

따라서 기존의 컴퓨팅 환경에서는 이용자가 모든 자원의 구매, 환경 구축 및 폐기까지의 전 과정을 직접 처리해야 했다. 하지만 클라우드 컴퓨팅 환경에서는 이용자가 온라인으로 필요한 자원을 신청하기만 하면 된다. 구축된 환경을 빠르고 손쉽게 제공받을 수 있는데다 폐기의 과정 또한 간단하다는 이점이 있다.

또한 클라우드 컴퓨팅 환경에서 제공되는 스토리지 제공 서비스, 소프트웨어 임대 서비스의 경우 웹하드, SBC(Server Based Computing), ASP (Application Service Providing) 등 기존의 응용인터넷 서비스와 유사해 보일 수 있다. 하지만, 클라우드 서비스는 동기화 및 데이터 가공 등 가상화 서버를 기반으로 새로운 기능 제공이 가능한, 다시 말해 서비스 제공자가 구축하는 고정적인 형태의 기존 응용서비스들과 다르다. 특히, 사용자별로 본인의 환경을 간편히 구성할 수 있고 수시로 변경 가능한 장점이 있다.

〈표 1〉 컴퓨팅 환경의 비교

컴퓨팅 환경	개인용 컴퓨팅 환경	인터넷 환경	클라우드 환경
데이터 위치 및 컴퓨팅 주체	개인용 PC, 노트북	서버/클라이언트	클라우드 서버(온라인)
자원 구매/폐기	이용자	이용자	서비스 제공자
사용자 컴퓨터 설치 S/W	OS, 응용S/W	OS, 응용S/W, 클라이언트	클라이언트(웹브라우져)
데이터의 소유 및 관리	소유와 관리가 동일	소유와 관리가 일부 분리	소유와 관리 분리 ※ 소유 : 이용자 ※ 관리 : 서비스 제공자
제공 서비스	오프라인 컴퓨팅 서비스 ※ 문서작성, 통계 계산, 그래픽 작업 등	– 기본 인터넷 서비스 ※ 웹, FTP, 이메일 등 – 응용 인터넷 서비스 ※ 웹하드, SBC, ASP 등 – IT 융합서비스 ※ VoIP, IPTV 등	– 가상 서버/데스크탑 서비스 – 스토리지 제공 서비스 – S/W 임대서비스 등

〈표 2〉 클라우드 서비스와 기존 응용인터넷 서비스의 차이점

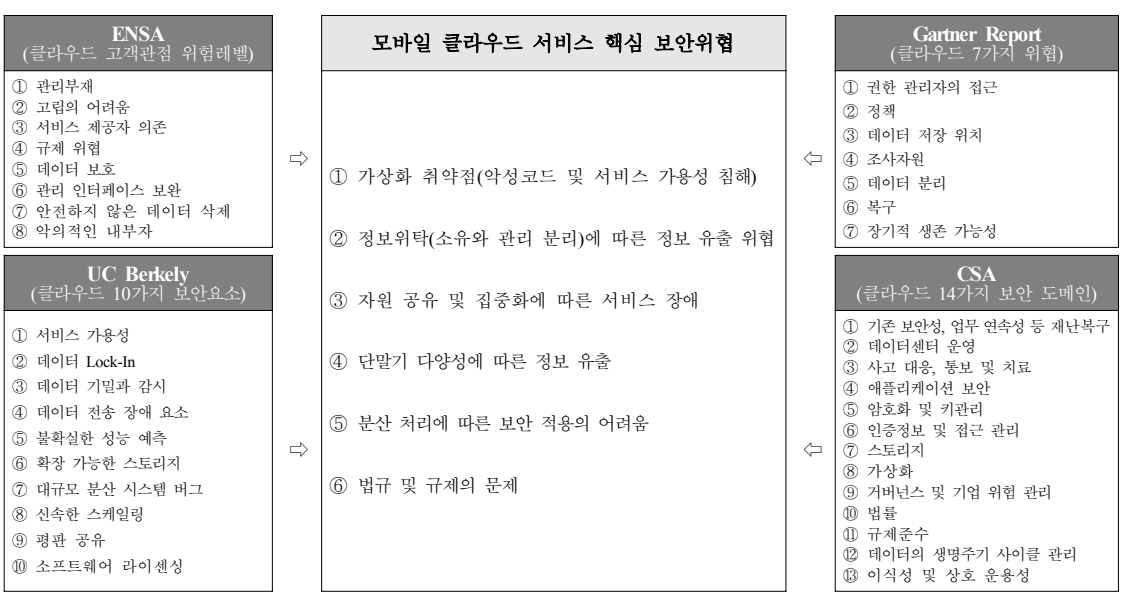
기존 인터넷 서비스		클라우드 서비스
• 웹하드 – 단순 파일 저장 기능 – 파일 다운로드 후 개인PC에서 가공	⇒	• 스토리지 제공 서비스 – 다양한 단말기와 데이터 동기화 서비스 지원 – 서버에서의 데이터 가공 서비스 지원
• SBC – 단일서버로 서비스 제공자가 특정 사용자를 대상으로 환경 구축 후 사용 – 사용자에 의한 컴퓨팅 환경 변경 불가	⇒	• 가상 서버/데스크탑 서비스 – 가상화된 서버 그리드로 서비스 제공자는 서비스 제공을 위한 공통 플랫폼만 구축 – 사용자 환경설정이 사용자에 의해 간편하게 이루어짐
• ASP – 사업자가 지원하는 고정적인 형태의 서비스만 사용 가능	⇒	• 소프트웨어 제공 서비스 – 사용자가 원하는 S/W들로 사용환경을 동적으로 구성할 수 있는 기능 제공

3. 모바일 클라우드 보안 이슈

3.1 보안 위협 분류

모바일 클라우드 서비스의 주요 특성은 SaaS, PaaS, IaaS 서비스를 구성하는 요소와 방법에 따라 효율적인 자원의 활용을 위해 하나의 물리적인 자원을 논리적으로 여러 사람이 공유하기 위해 통합/재분배하여 사용하는 IT자원의 가상화 및 자원공유, 고객의 정보가 서비스 제공자의 클라우드 서버에 위치하는 정보 위탁, PC, 스마트폰, 테블릿 PC 등 다양한 형태의 단말기를 통한 접속의 특성을 가지고 있다.

이러한 특징에 따라 모바일 클라우드 서비스 상에서는 정보 유출, 서비스 장애 등 다양한 보안 위협이 발생할 수 있으며, 보안위협은 주체와 관점에 따라 다양한 방법으로 분류되고 있다. CSA[2], NIST[3], UC Berkely[4], 가트너[5] 등에서 제시하는 대표적 보안위협 분석사례에서 클라우드 서비스의 핵심 보안요소를 도출하면 (그림 2)



(그림 2) 모바일 클라우드 서비스 핵심 보안 위협

〈표 3〉 모바일 클라우드 구간 별 보안 위협

모바일 기기	네트워크	클라우드 플랫폼
• 모바일 악성코드 감염 • 모바일 기기 분실 및 도난 • 단말 암호 크랙 • 크로스 서비스 공격 • 기업 내부 정보 유출	• 무보안 무선랜을 통한 도청 • DDoS 공격 • 개인 감시 • 비인가 접근	• 가상머신 악성코드 감염 • 고객 정보 유출, 유통, 가공 • 가상머신 해킹 • 멀티테넌시 취약성 • 서비스거부공격

와 같다.

또한 이용자가 모바일 클라우드 서비스를 구성하는 모바일 기기, 네트워크, 클라우드 플랫폼 단계별로 <표 3> 과 같은 보안위협이 존재한다.

3.2 모바일 클라우드 사고 사례

최근 아마존 EC2 장애 등 일시적으로 서비스가 중단되는 장애와, 데이터 손실 등의 사고가 빈번이 발생하고 있다. 하지만, 클라우드 서비스 제공자들은 사고 발생 경위에서부터 원인 및 중단 시간, 피해규모 등을 명확히 밝히지 않고 있으나, 주로 시스템(장비) 에러 및 교체, 관리자 부주의, 자연재해에 의한 것으로 이는 클라우드 컴퓨팅 서비스가 아직 활성화되지 않았기 때문으로 모든 정보가 한 곳에 집중화 되는 서비스 특성상 클라우드 컴퓨팅 서비스가 본격적으로 확산되면 많은 해커들의 주 대상이 될 것으로 예상된다.

〈표 4〉 클라우드 장애 사고 사례

구분	일시	유형	주요 내용
구글	'09.9	서비스 장애	Gmail 2시간 서비스 장애 반복 발생
	'11.2	데이터 손실	50만명의 메일 이용자의 메일내용 및 주소록이 삭제
MS	'09.10	서비스 장애	스마트폰 서비스 사이드킥 서비스 중단
	'10.12	데이터 유출	서비스 환경설정 오류로 인해 기업정보가 타인에게 공개
eBay	'09.8	서비스 장애	페이팔 자불결제 시스템 에러로 서비스 2시간 중단
아마존	'11.4	서비스 장애	아마존 EC2 서비스를 이용하는 190여개 서비스가 11시간 장애
	'11.8	서비스 장애	벼락으로 인한 정전사고로 아마존 EC2 장애 (유럽지역 수천개 기업 최대 이틀간 접속장애)

3.3 기술적·관리적 보안 이슈

모바일 클라우드 보안 위협은 가상화, 자원공유, 정보위탁, 다양한 단말기의 접속 등 특성에 따라 기술적 · 관리적 보안 이슈는 다음과 같다.

3.3.1 가상화 시스템 해킹

가상화 기술을 통해 고객의 가상머신들이 상호 연결되어 다양한 공격경로가 존재하며, 하이퍼바이저[1] 해킹 시 타 가상머신의 통제권이 상실될 수 있다. 또한 특정 가상머신이 악성코드 감염될 경우, 가상환경 내부로 쉽게 확산될 수 있는 가능성이 존재하며, 최근에는 클라우드 가상화 플랫폼 CVE 보안 취약성이 꾸준히 발견되고 있다.[1]

3.3.2 자원공유로 인한 비인가자의 정보 접근

고객 정보가 원격의 클라우드 서버에 저장되고 관리되므로, 동일 컴퓨터에 타 고객 사 정보가 혼재되어 설정오류, 취약한 패스워드 사용, 계정도용 등으로 인해 클라우드 자원에 대한 비 인가자

1) 하이퍼바이저: 하나의 컴퓨터에서 서로 다른 여러 개의 운영체제를 동시에 구동시킬 수 있게 하기 위한 HW와 고객들의 가상머신 사이에 위치하는 SW로서, 고객의 가상 OS와 HW를 논리적으로 연결

의 정보 접근이 가능하다.

3.3.3 내부자에 의한 고객 정보 유출 및 오용

내부 직원의 고의적, 관리 부주의로 고객 정보에 대한 접근 및 유출과 내부 관리자의 부주의로 고객의 계정과 가상서버가 삭제되거나 손실될 수 있다.

3.3.4 집중화로 인한 서비스 장애의 대형화

고객의 중요정보가 서비스 제공자의 클라우드 서버에 모여 있기 때문에 해커의 집중적 공격 대상이 될 수 있으며, 공격 경유지로 악용될 수 있어 침해사고 발생 시 해당 자원을 공유하는 타 고객 서비스까지 연쇄적으로 확산되고 피해가 대형화 될 수 있다.

3.3.5 보안관리 책임소재 불분명 및 정책의 복잡화

사업자는 고객의 IT 자원 및 데이터 보호를 완벽하게 보장하기 않기 때문에 보안 관리에 대한 책임소재가 불분명하고 대용량 데이터가 분산파일 시스템을 통해 많은 서버들에 분산 저장・관리됨에 따라 데이터 암호화, 이용자 인증, 접근제어 등의 어려움이 증가한다. 또한, 관리시스템의 위치 노출 시 악의적인 해킹, 이용자의 데이터 손실・유출, 관리자나 해당 기업의 관계자에 의한 정보 유출 등과 같은 보안위협이 존재한다.

3.3.6 단말기 다양성에 따른 정보 유출

다양한 모바일 기기를 통해 클라우드 데이터에 접속하게 되므로 유선환경과는 상대적으로 보안이 취약하게 된다. 모바일 단말기는 사용자의 개인적인 민감한 정보가 저장되며, 이동성으로 인해 음성 및 데이터의 노출과 분실 및 도난으로 인한 정보유출의 위협이 존재한다.

4. 모바일 클라우드 보안 기술 요구사항

4.1 기존 보안기술과의 차이점 및 특성

모바일 클라우드 보안 기술은 기존 보안기술과 크게 차이가 있지 않으나, 가상화, 자원공유, 정보 위탁, 멀티테넌시, 소유관계 및 역할 분담 등의 고려가 되어야 하며, <표 5>는 기존 보안기술과의 차이점을 정리하였다.

〈표 5〉 기존 보안 기술과 클라우드 보안기술의 특성

구분	기존보안기술	클라우드 보안기술의 특성
네트워크 방화벽	물리적 경계 네트워크에서 접근제어, DDoS 공격 등을 탐지/차단	가상 머신(VM) 간 DDoS, 악성코드 등 전파 방지 VM 간 트래픽에 대한 접근제어 하이퍼바이저 보호, 침해사고 피해 VM 격리
침입탐지 (백신 등)	단일 에이전트로 물리적 서버 보호	논리적 가상 머신 환경에서 동작
인증 및 권한관리	DBMS 테이블 수준의 접근제어 역할에 따른 권한 접근제어 객체, 주체(프로세스, 소속, 역할 등)	다수의 데이터 및 사용자가 혼재 특성 상세한 자원 접근 통제/분리 보안상황이 다른 환경(재택, 사내 등) 접근 상황
데이터 암호화	주로 PC 환경 어플레케이션/데이터 보호	클라우드 자원 속 Invisible 데이터 저장 위치 외부 사업자에게 위탁한 민감한 데이터 관리
보안관리	물리적 관리 대상 명확	가상화 계층 증가로 보안관리 요소 증가 위탁한 자원에 대한 감사/모니터링, 불법접근 추적 등

4.2 보안 기술의 요구사항

모바일 클라우드 도입 시 정보유출, 서비스 장애 등 우려가 커서, 클라우드 보안 기술에 대한 관심이 크며, 클라우드 환경에 기존 보안 기술을 그대로 탑재하는 단계에서 가상화 방화벽 등 가상화 환경 특성을 고려한 클라우드 전용 보안기술(For the Cloud) 제품이 출시되고 있다. 향후에는, 보안기술을 클라우드 환경에서 서비스 형태로 제공(In the Cloud)하는 기술로 발전될 것으로 예상되며, 모바일 클라우드 보안 기술이 가져야 한 요구사항은 다음과 같다[6,7].

4.2.1 가상화 보안 기술

가상화 인프라의 하이퍼바이저에서 가상머신 간의 채널을 통한 공격 트래픽의 탐지 및 차단, 가상 네트워크 변화에 따른 동적 네트워크 보안 기능 등 가상화 환경에 따른 보안 기술이 요구된다.

4.2.2 클라우드 환경을 고려한 강력한 인증 및 접근제어

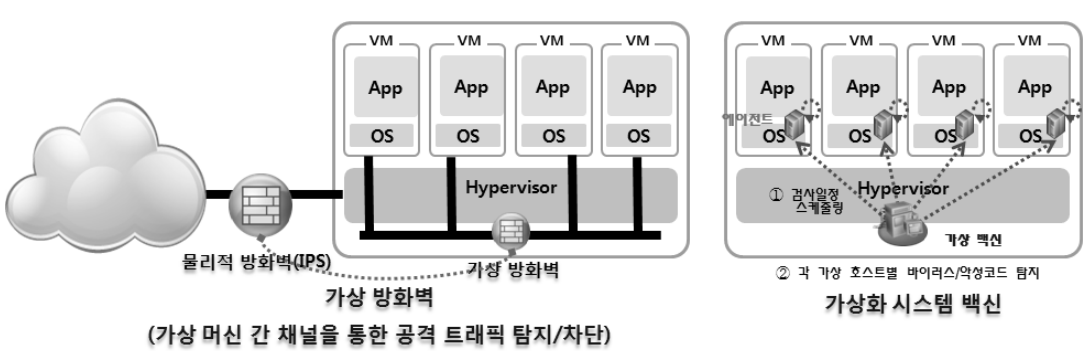
사용자, 관리자 외에 서비스 제공자가 개념이 포함된 역할기반의 권한관리와 기업 내부뿐만 아니라 외부 클라우드 사업자에게 위탁한 자원까지 관리 대상이 확대되어야 한다. 기업용 프라이빗 클라우드 제공 시 VPN 인증, 암호화 통신, 사용자 IP 기반의 접근제어가 필요하며, 특히 와이파이 등 유선 환경보다 보안이 취약한 접속 환경에서 접속하는 모바일 기기에 대한 차등적인 접근제어 통제가 필요하다.

4.2.3 클라우드 데이터 암호화

클라우드 서버에 저장된 데이터에 대한 적절한 암호화 사용과 확장성을 지원하는 키 관리가 제공되어야 하며, 데이터 암호화를 통해 자원 접근에 대한 보호와 개인정보와 같은 중요 데이터에 대한 보호가 이뤄져야 한다.

4.2.4 클라우드 보안 관제 및 침해사고 대응

기존의 물리적 보안 영역과 가상화 관리 영역을 통합적으로 보안관리 기능을 제공하여야 한다. 특히, 클라우드 가상화 영역까지 인증, 자원 할당 등 보안 이벤트 로그 정보를 수집하고 분석하는 클라우드 보안 모니터링을 확대하여 과도한 자원 할당, 과부하에 의한 시스템 장애, 권한 외 자원 접근 시도, 계정 도용으로 인한 정보유출 시도 등을 이상 징후를 종합적으로 분석하고 탐지하는 기능이 요구된다.



(그림 3) 가상화 보안 기술

5. 결 론

국내 스마트폰 등 모바일 기기 보급 확산 및 비용절감, 확장성 등의 장점으로 클라우드 도입이 확대되고 있는 실정이나, 정보유출 악성코드 감염, 서비스 장애 등 보안 위협에 대한 우려가 여전히 높기 때문에 보안 문제에 대한 보장이 없이 모바일 클라우드 서비스 확대에는 한계가 있을 수 밖에 없다. 모바일 클라우드 서비스 특성상 정보가 한 곳으로 집중되고, 다양한 모바일 기기를 통한 접속이 가능하기 때문에, 향후 클라우드 서비스가 급속도로 활성화 될 경우 많은 해커들의 주 공격대상이 될 가능성이 크다. 그로 인한 피해 규모가 커질 것으로 예상되기 때문에 안전한 모바일 클라우드 서비스를 이용하기 위해서는 신규 보안위협 및 사고 발생에 대한 대응이 필요하다.

본 논문에서는 가상화 및 자원공유, 정보 위탁, 다양한 형태의 단말기를 통한 접속 등 모바일 클라우드 환경 특성에 따른 보안 이슈를 분석하고, 기존 IT 환경의 보안기술과 클라우드 환경의 보안기술에 대한 비교를 통해, 물리적인 보안뿐만 아니라 가상화 환경까지 영역을 확대하여야 하며, 다양한 기기를 통해 접근하는 사용자 위치나 보안 상황에 따라 접근제어를 강력히 통제할 수 있는 모바일 클라우드 보안 기술에 대한 요구사항을 도출하였다.

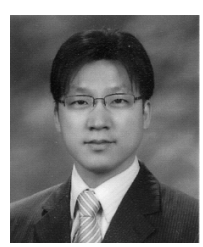
Acknowledgement

본 연구는 방송통신위원회의 정보보호원천기술개발사업인 “모바일 클라우드 통합인증 및 권한관리 기술개발사업”의 연구결과로 수행되었음 (KCA-2011-11914-06002)

참 고 문 헌

[1] 장은영, 김형종, 박춘식, 김주영, 이재일, “모바일 클라우드 서비스의 보안위협 대응 방안 연구”, 정보보호학회논문지, 제21권 제1호, pp.176-186, 2011년 2월.
[2] CSA, “Top Threats to Cloud Computing”, CSA, March, 2010.
[3] Wayne Jansen, Timothy Grance, “Guidelines on Security and Privacy in Public Cloud Computing”, NIST, January, 2011.
[4] Michal Armbrust etc, “Above the Clouds: A Berkeley View of Cloud Computing”, UC at Berkeley, Feburary, 2009.
[5] Jon Brodkin, “Gartner: Seven Cloud-computing securit risks”, Network World, July, 2008.
[6] 정현철, 김환국, “클라우드 보안 대비 서둘러야 한다”, 컴퓨터월드, 2011년 6월호.
[7] 차명석, “e-Bay 클라우드 서비스 보안 전략”, 2011.9.

저 자 약 력



김 환 국
이메일 : rinyfeel@kisa.or.kr

- 1998년 한국항공대학교 전자계산학 학사
- 2000년 한국항공대학교 컴퓨터공학 석사
- 2002년~2006년 한국전자통신연구원(ETRI) 정보보호연구단 연구원
- 2007년~현재 한국인터넷진흥원(KISA) 인터넷침해대응센터 연구개발팀/책임연구원
- 2009년~현재 고려대학교 경영정보공학대학원 박사과정(정보보호)
- 관심분야 : 네트워크 보안, 인터넷전화 보안, 클라우드 보안

정 현 철

이메일 : hcjung@kisa.or.kr

- 1996년 서울시립대학교 전산통계(이학사)
- 1999년 광운대학교 전자계산(이학석사)
- 1996년~현재 한국인터넷진흥원 인터넷침해대응센터 연구개발팀장
- 2006년~현재 고려대학교 정보보호대학원 박사과정
- 관심분야 : 웹취약성 분석, 인터넷전화 보안, 악성코드 분석, 클라우드 보안

원 유 재

이메일 : yjwon@kisa.or.kr

- 1985년 충남대학교 학사
- 1987년 충남대학교 석사
- 1998년 충남대학교 전산학과 박사
- 1987년~2001년 한국전자통신연구원 책임연구원/팀장
- 2001년~2004년 안랩유비웨어/안철수연구소 CTO
- 2004년~현재 한국인터넷진흥원 인터넷침해대응센터 본부장
- 관심분야 : 정보보호, 멀티캐스트 보안, 인터넷전화 보안