情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

모바일 클라우드 서비스의 보안위협 대응 방안 연구*

장 은 영[1†], 김 형 종[1‡], 박 춘 식[1], 김 주 영[2], 이 재 일[2]
[1]서울여자대학교 컴퓨터학과, [2]한국인터넷진흥원

The study on a threat countermeasure of mobile cloud services

Eun-Young Jang,[1†], Hyung-Jong Kim[1‡], Choon-Sik Park[1], Joo-Young Kim[2], Jae-il Lee[2]
[1]Seoul Women's University Computer engineering, [2]Korea Internet & Security Agency

요 약

스마트 폰의 보급이 확장되면서 데스크톱의 성능과 모바일 특성이 적용된 다양한 모바일 서비스가 증가하고 있다. 모바일 서비스는 모바일 단말의 메모리, 컴퓨팅 파워, 저장 공간 부족과 모바일 단말의 플랫폼에 종속되는 한계를 갖는데 이를 극복할 수 있는 클라우드 컴퓨팅 서비스가 적용된 모바일 클라우드 컴퓨팅 서비스가 최근 각광받고 있다. 모바일 클라우드 서비스는 모바일 서비스와 무선네트워크, 클라우드 서비스가 융합된 서비스로 다양하고 확장된 서비스를 제공하지만, 보안 위협요소가 복합적으로 상속되는 위험이 잠재되어 있다. 그러므로 보안위협이 제거된 안전한 서비스를 배포하고 위협 발생 시 적절하게 대응하기 위한 방안이 필요하다. 본 연구에서는 모바일 단말, 무선네트워크, 클라우드 컴퓨팅 서비스의 위협을 분석하여 모바일 클라우드 서비스의 위협과 위협에 대응하기 위한 방안을 정의하였으며, 위협시나리오를 기반으로 잠재된 위협을 예상하고 대응할 수 있는 방안을 제시하였다.

ABSTRACT

Mobile services which are applied PC performance and mobile characteristics are increased with spread of the smartphone. Recently, mobile cloud service is getting the spotlight as a solution of mobile service problems that mobile device is lack of memory, computing power and storage and mobile services are subordinate to a particular mobile device platform. However, mobile cloud service has more potential security threats by the threat inheritance of mobile service, wireless network and cloud computing service. Therefore, security threats of mobile cloud service has to be removed in order to deploy secure mobile cloud services and user and manager should be able to respond appropriately in the event of threat. In this paper, We define mobile cloud service threats by threat analysis of mobile device, wireless network and cloud computing and we propose mobile cloud service countermeasures in order to respond mobile cloud service threats and threat scenarios in order to respond and predict to potential mobile cloud service threats.

Keywords: Threat of Mobile Cloud Computing, Countermeasure of Mobile Cloud Computing

I. 서 론

최근 국내외 클라우드 컴퓨팅 서비스의 도입이 증가하고 있으며, 스마트 폰 서비스 이용자들이 증가하고 있다. 사용자들은 데스크톱에서 이용하는 서비스를 스마트 폰에서 동일하게 제공받길 원하면서 기존 데스크톱 서비스가 모바일 단말의 이동성과 개인적 소유의 특성이 적용된 모바일 서비스로 제공되고 있다. 모바일 단말이 발전되었지만, 메모리, 컴퓨팅 파워 및 전력 사용의 한계와 정보 저장 문제와 분실 및 도난 문제, 특히 모바일단말 플랫폼에 종속되는 모바일서비스

접수일(2010년 12월 3일),게재확정일(2011년 1월 27일)
* 본 연구는 방송통신위원회가 출연하고 한국인터넷진흥원에서 위탁시행 한 모바일 클라우드 서비스 보안 침해 대응 방안 (KISA-WP-20100063)사업 결과에 의한 것입니다.
† 주저자, elishajey@swu.ac.kr
‡ 교신저자, hjkim@swu.ac.kr

의 문제가 발생하였다. 이러한 기존의 모바일서비스의 문제를 클라우드 서비스의 적용으로 해결되면서 현재 모바일 클라우드 서비스가 각광받고 있다. 그러나 클라우드 자원을 이용하는 웹기반 모바일 컴퓨팅을 수행하는 모바일 클라우드 서비스는 모바일 서비스와 클라우드 서비스가 융합된 형태이기 때문에 각각의 위협이 복합적으로 파생되어 발생하므로 모바일과 무선네트워크, 클라우드서비스 중 하나의 자원에 문제가 발생하면 정상적인 서비스 수행이 불가능하며 공유된 자원의 무선네트워크를 이용하는 서비스이기 때문에 문제가 전파되는 영역이 커진다. 그러므로 보안위협이 제거된 안전하고 신뢰할 수 있는 모바일 클라우드 서비스를 배포해야 하며, 위협이 발생하였을 때 신속하게 대처해야 한다.

본 연구에서는 향후 발생 가능한 모바일 클라우드 서비스의 위협을 예상하기 위해 모바일 단말 위협과 무선네트워크 위협, 클라우드 위협을 통해 모바일 클라우드 서비스의 위협을 정의하고 각 위협이 악용한 취약점과 위협영향을 분석하였으며, 각 위협에 대한 대응방안을 정의였다. 또한 위협 간 상관관계를 파악하여 위협시나리오를 통해 잠재된 위협을 예상하고 대응하는 정보보호대책을 제시하였다.

II. 관련연구

2.1 모바일 클라우드 서비스

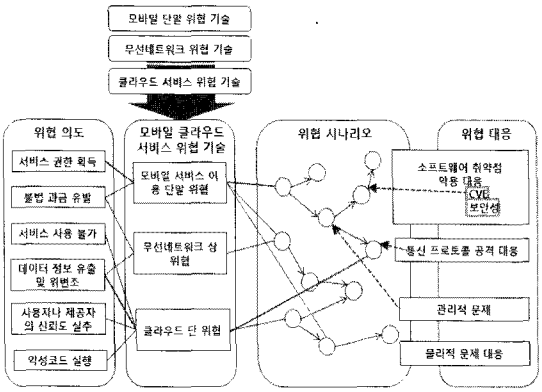
모바일 클라우드 서비스는 모바일 단말에서 처리해할 작업 및 데이터 저장의 일부를 클라우드 컴퓨팅 환경으로 이동시켜 처리하고 모바일 단말에서 처리결과를 보여주는 애플리케이션이다[1]. 모바일 클라우드 서비스는 모바일 단말의 기능과 특징과 클라우드 서비스의 특징을 통해 연계 서비스와 이동성 서비스로 분류 할 수 있다. 연계 서비스란 모바일 단말에서 데스크톱 서비스를 언제 어디서나 끊임없이 이용할 수 있는 모바일 클라우드 서비스이며, 검색 서비스, 동기화 서비스, U-health, 공공 서비스 실시간 조회, 기업형 모바일 서비스, 엔터테이먼트 서비스로 분류 할 수 있다. 클라우드 컴퓨팅 환경을 기반으로 모바일 서비스의 한계를 극복한 대표적인 서비스인 동기화 서비스는 Mobile Me, My phone 서비스가 있다. 또한 실시간 업무를 가능하게 하는 기업 형 모바일 서비스는 Sonnr, thinkfree office mobile, Enterprise disk, 삼성 모바일 클라우드 서비스가 있다. 기존 모바일 서비스에 모바일 단말의 이동성 특징이 적용된 서비스는 구글 맵 네비게이션, ShopSavvy, Foursqure, Gowalla, Yelp가 있으며, 증강현실 서비스는 Layar, Acrossair가 있다. 소셜 네트워크 서비스는 두가 서비스 유형에 모두 속하는 서비스로 이동환경이 적용된 연계된 실시간 공유 및 검색 서비스 기능이 추가된 모바일 블로그 서비스이며 대표적으로 Loopt, Twitter가 있다. 현재 위의 모든 모바일 서비스가 클라우드 형태로 제공되고 있지 않지만, 점차 모바일 클라우드 서비스로 변화하고 있다. 모바일 클라우드 서비스는 이동환경에서 개인이 소유한 단말의 특성을 강화 시키고 모바일 단말의 제약을 극복할 수 있는 다양한 서비스를 제공한다.

2.2 클라우드 컴퓨팅 서비스의 위협

CSA(Cloud Security Alliance)는 클라우드 컴퓨팅의 위협요소를 다음과 같이 도출하였다[2][3][4]. 클라우드 서비스 확장을 위한 프로모션 서비스 제공으로 인해 공격자들이 클라우드 자원을 비도덕적으로 사용하고 자원을 남용하는 것이 가능하다. 클라우드 컴퓨팅 사업자의 클라우드 서비스의 관리와 상호작용을 위한 소프트웨어 인터페이스나 API를 제공으로 클라우드 서비스의 보안요소가 종속된다. 또한, 통합되고 공유되는 클라우드 서비스 도입은 관리자 요소가 더 심각한 중요성을 가진다. 클라우드 사업자가 클라우드 가상화 기술을 이용한 자원 공유로 공유 인프라 구조를 만드는 기본 컴포넌트들은 멀티-테넌트 구조를 위해 강력한 격리와 방어를 제공하지 않는다. 게다가 데이터가 클라우드 사업자에게 의해 관리되기 때문에 삭제나 변경, 백업, 레코드 연결 해제, 데이터 암호화 문제가 중요하다. 암호학적인 개인정보와 비밀번호의 재사용으로 인해 사용자의 계정이나 서비스 인스턴스들이 공격자에 유출 될 수 있다. 클라우드 서비스의 프로파일정보는 보안 상태를 평가하기 위한 중요한 요소이다. 서비스 사용자는 이 정보를 알아야 하며, 명확한 프로파일 제어와 운영이 필요하다. 위와 같은 위협은 모바일 클라우드 서비스에서도 발생할 수 있는 위협이므로 모바일 클라우드 서비스를 배포하고 관리하는데 중요한 요소이다.

III. 모바일 클라우드 서비스의 위협과 취약점

모바일·클라우드 서비스의 보안 침해 조사와 분석



〔그림 1〕 모바일 클라우드 서비스의 위협과 대응

을 통해 모바일 클라우드 서비스 이용 단말의 위협, 무선네트워크 상의 위협기술과 클라우드 단의 위협기술을 도출하였다. 공격자의 위협의도에 따라 위협 기술로 공격이 수행되고, 이러한 위협 기술들은 연관관계를 가질 수 있으므로 잠재적인 위협 발생을 야기한다. 이와 같은 위협 기술 간 관계는 위협시나리오(위협 패턴)와 같이 나타낼 수 있다. 본 연구에서는 모바일 클라우드 서비스의 취약점을 분석을 기반으로 〔그림 1〕과 같이 위협시나리오의 위협 기술이 악용한 취약점을 도출하였다.

위협은 사고와 실수로 인해 발생하는 결과가 아니라 시스템을 정상적으로 수행하지 못하는 결과를 야기하는 것을 말한다. 모바일 클라우드 서비스는 모바일 단말을 통하여 클라우드 서비스를 제공받으므로 모바일 서비스, 모바일 무선네트워크와 클라우드 서비스가 갖는 위협을 복합적으로 상속받을 것이다.

3.1 모바일 단말 위협

모바일 단말은 특정 사용자의 개인적인 민감한 정보가 저장되며 이동성으로 인해 음성 및 데이터의 노출과 분실 및 도난의 위험이 크다〔5〕〔6〕〔7〕〔8〕〔9〕. 또한 개방형 모바일 환경에서 제공하는 소프트웨어 및 콘텐츠의 사용으로 데스크톱에 비해 신뢰성 낮은 서비스를 이용하게 된다. 이러한 특성은 개개인이 요구에 맞게 실제 환경과 접목된 서비스를 제공받을 수 있지만 물리적 장치와 모바일 서비스, 플랫폼 및 개인정보가 많은 위협에 노출되는 환경을 제공한다. 모바일 단말의 위협은 〔표 1〕과 같이 메시지, 메일 오용 및 남용, 서비스 거부, 데이터 손실 및 유출, 서비스 기반 위협, 보안체계 위협과 악성코드로 분류 및 정의할 수 있다.

〔표 1〕 모바일 단말 위협

위협	요약	위협 기술
메시지, 메일 오용 및 남용	모바일 메시지를 다양한 위협 형태로 악용하여 바이러스 유포 및 서비스와 단말의 사용 제약	메시지 스푸핑
		스팸 메시징
		메시지 피싱
		악성 메시지 배포
		다량의 메시지 전달
		악의적인 콘텐트
서비스 거부	모바일 단말이 타깃이 되어 작업 수행을 못하거나 좀비가 되어 서버나 다른 모바일 단말을 위협	서비스 과다요청
		모바일 단말 파괴
		배터리 소진
		저장 공간 소진
		컴퓨팅 파워 소진
		악의적인 포맷 스트링
		오버플로우
데이터 손실 및 유출	모바일 단말의 고성능화와 이동성, 서버의 모바일 데이터를 보유하는 특성으로 인한 데이터 손실 및 유출의 위협	모바일 단말 분실 및 도난
		서버의 데이터 손실 및 유출
		모바일 화면, 통화 내용 노출
		모바일 정보 유출
		부적절한 네트워크 접근
서비스 기반 위협	정상적인 모바일 서비스의 방식 및 내용을 악용하거나 위장하여 다른 모바일 서버, 플랫폼, 단말, 데이터 등을 위협	크로스 서비스 위협
		사용자 위치 불법 추적
		논리 오류 발생 및 코드 삽입
		불법 통화 시도
보안 체계 위협	모바일 단말의 암호화, 인증 등을 무력화시키는 위협	모바일 단말 암호 크랙
		데이터 암호화 보호 크랙
		인증 우회 및 크랙
악성코드 위협	모바일 단말을 감염시켜 데이터를 유출하고 시스템 파괴, 원격 제어 등 악의적인 행동하는 코드	바이러스
		웜
		트로이 목마
		스파이웨어

3.2 무선 네트워크 위협

웹기반 모바일 서비스는 3G, Wi-Fi, WiBro, Bluetooth를 이용하므로 무선네트워크를 통한 위협이 잠재한다[11][12]. 무선네트워크는 물리적 매체 대신 전파나 빛을 이용하므로 연결 링크가 끊어지거나 다중경로, 쉐도우와 같은 문제점이 나타날 수 있다. 또한 무선 공유기의 노출과 네트워크 수신자 지정의 어려움, 물리적 위치의 자유로움 등으로 인해 많은 위협에 노출되어 있다. 무선네트워크의 위협은 [표 2]와 같이 도감청, 프로파일링 및 추적, 불법 인증 위협, 서비스 거부, 네트워크 통신정보 유출 및 변조와 세션 가로채기로 분류 및 정의 하였다.

[표 2] 무선 네트워크 위협

위협	요약	위협 기술
도·감청	패킷을 불법으로 수집하여 내용 유출	음성 도감청
		메시지 도감청
		패킷 도감청
프로파일링 및 추적	네트워크 통신 정보를 수집하고 추적	블루투스 프로파일링
		무선랜 프로파일링
		WiBro 프로파일링
불법 인증 위협	SSID, MAC주소 노출 등으로 불법 인증된 사용자가 접근	비인증 접근점
		서비스 식별자 노출
		WEP 키 노출
		이더넷 물리적 주소 노출
서비스 거부	시스템 자원 고갈 및 비정상 패킷의 다량 발송 등 정상적인 서비스 거부	플러딩 위협
		전파 차단 및 방해
		모바일 단말 파괴
네트워크 통신정보 유출 및 변조	사용자의 등록정보를 조작하거나 불법 통신망으로 서비스 접속을 유인하여 사용자 정보 유출	네트워크 통신정보 스푸핑
		메시지 피싱
세션 가로채기	사용자의 세션 제어권한 등을 획득	세션 가로채기

3.3 클라우드 컴퓨팅 서비스의 위협

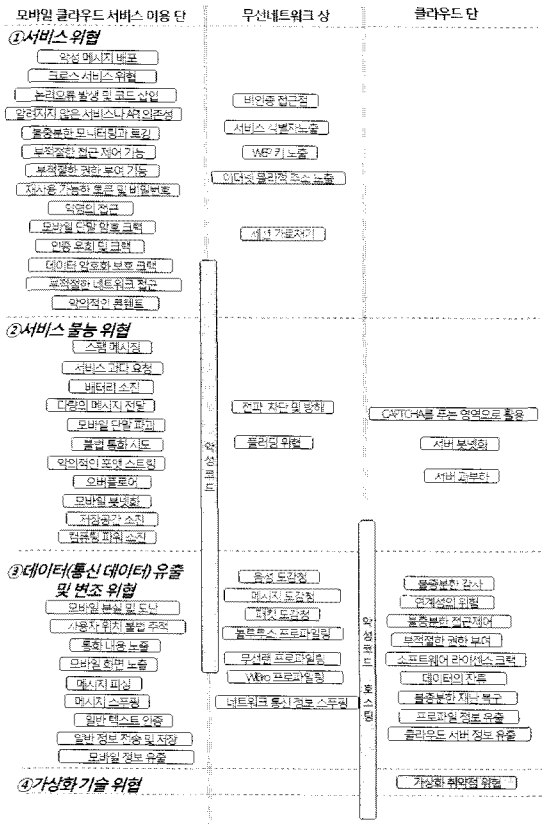
클라우드 컴퓨팅 서비스는 통합되고 공유된 IT 자원을 가상화 기술을 이용하여 관리하고 다양한 서비스 형태로 제공된다. 그러나 보안 가이드라인의 부재와 접근제어 관리, 데이터 암호화, 가용성 및 무결성 보장 기술 등의 적용 부족으로 많은 위협에 노출되어 있다[2][3][4]. 클라우드 컴퓨팅 서비스는 [표 3]과 같이 서비스 오남용, 데이터 손실 및 유출, 애플리케이션의 위협, 관리 시스템의 취약점과 가상화 기술의 취약점으로 인한 위협으로 분류된다.

[표 3] 클라우드 컴퓨팅 서비스의 위협

위협	요약	위협 기술
서비스 오남용	클라우드 자원을 악의적인 목적으로 오용 및 남용	데이터 암호화 보호 크랙
		서비스 과부하
		서버, 모바일 봇넷화
		악성코드 호스팅
		CAPTCHA를 푸는 영역으로 활용
데이터 손실 및 유출	통합되고 공유된 자원이 악의적 접근에 노출되거나 데이터 사이 구분의 불명확함	불충분한 접근제어
		부적절한 권한 부여
		불충분한 감사
		소프트웨어 라이센스 크랙
		연계성의 위험
		클라우드 서버 정보 유출
애플리케이션의 위협	결함이 있는 클라우드 서비스 제공자에게 종속되는 애플리케이션의 위험	익명의 접근
		재사용 가능한 토큰이나 비밀번호
		일반 텍스트 인증
		일반 정보 전송 및 저장
		부적절한 접근제어 기능
		부적절한 권한부여 기능
		불충분한 모니터링과 로깅
		알려지지 않은 서비스나 API의존성
관리 시스템의 취약점	클라우드 관리자의 보안성 부재와 관리 부족	프로파일 정보 유출
		불충분한 재난복구
		데이터의 잔류
가상화 기술의 취약점	가상화 기술의 특성을 악용	가상화 취약점 위협

3.4 모바일 클라우드 서비스의 위협

모바일 클라우드 서비스는 모바일 단말을 이용하여 웹을 통해 클라우드 서비스를 이용하므로 모바일 단말과 모바일이 이용하는 무선네트워크, 클라우드 서비스의 위협이 복합적으로 발생 할 수 있다. 모바일 클라우드 서비스는 기존 모바일 서비스와 달리 무선네트워크를 통해 클라우드 서버에 데이터 대부분을 저장하고 처리한다. 그러므로 기존의 모바일 서비스에서 발생할 수 있는 위협 중 모바일 단말 분실 및 도난으로 인한 데이터 손실과 단말 암호 크랙과 같은 물리적 위협은 상대적으로 감소할 것이며 무선네트워크 통신 불능으로 인한 위협은 증가할 것이다.



〔그림 2〕 모바일 클라우드 서비스 위협

모바일 클라우드 서비스의 위협은 〔그림 2〕와 같이 모바일 단말, 무선네트워크, 클라우드 컴퓨팅 서비스의 위협을 기반으로 정의하였다. 모바일 클라우드 서비스는 기존의 데스크톱에서 이용하는 클라우드 서비스를 모바일 단말에서 이용하기 때문에 클라우드 서비스의 위협은 모바일 클라우드 서비스 이용 단의 서비스 위협으로 나타난다. 악성코드와 악성코드 호스팅은 모든 영역에 악의적인 영향을 끼칠 수 있다.

모바일 클라우드 서비스의 위협은 공격자가 위협하는 객체를 기준으로 시스템 상 위협 기술과 정보 유출 및 변조에 대한 위협으로 분류할 수 있다. 모바일 클라우드 서비스의 시스템 상 보안 위협은 모바일 서비스의 전체적인 작업 처리 방식과 관련된 자원의 위협을 의미하며, 서비스 자체에서 발생하는 공격과 서비스 단에서 제공되는 보안 체계 및 관리에서 발생하는 서비스 위협과 정상적인 서비스 수행을 불가능하게 하는 서비스 불능 위협, 클라우드 자원의 가상화 기술 위협으로 나뉜다. 모바일 클라우드 서비스의 정보 위협은 모바일 단말에 저장된 데이터와 클라우드 자원에 저장된 데이터, 무선네트워크에서 송수신되는 데이터의 유출 및 변조 위협을 의미한다.

3.5 모바일 클라우드 서비스의 위협 시나리오

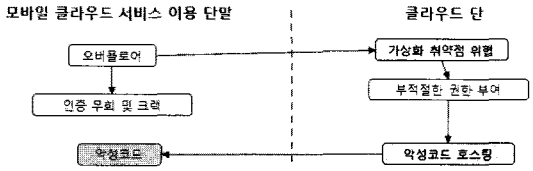
모바일 클라우드 서비스 위협을 기반으로 잠재되어 있고 발생 가능한 〔그림 2〕와 같은 위협 기술을 예상하기 위해 공격자의 위협의도에 따라 위협시나리오를 도출하였다. 이는 잠재적인 상태에 머물러 있거나 사용자가 인식하지 못하는 복잡해진 위협 기술을 예상하기 위한 위협 기술 연쇄추론 방법이다.

피해자가 공격자의 위협의도를 파악하지 못한다면, 모든 IT 자원의 취약점 내재 여부를 밝혀야 하며 공격 탐지 및 방지를 위해 모든 보안기술 및 관리를 동원해야 한다. 그러므로 공격자의 행동을 추측하여 잠재 위협과 위협의 발생 경로를 파악하여 제한된 시간과 비용 내에 효율적인 보안침해 대응방안을 마련해야 한다. 공격자의 위협의도에 따른 모바일 클라우드 서비스의 위협시나리오는 〔표 4〕와 같다.

〔표 4〕 모바일 클라우드 서비스의 위협 시나리오

위협 의도	위협 시나리오
서비스 권한 획득	불법 인증을 통한 악성코드 감염
	서비스 악용을 통한 악성코드 전파
	클라우드 자원의 악성코드 감염으로 인한 악성코드 전파
	오버플로어를 통한 서비스 권한 획득
불법 과금 유발	비정상적인 서비스 제어로 인한 과금 발생
	비밀번호 유출로 인한 불법 과금
	권한 오용을 통한 불법 과금 침해
	네트워크 취약점을 악용한 과금 우회
서비스 사용 불가	모바일 단말 파괴를 야기하는 서비스 거부
	클라우드 자원을 위협하는 서비스 거부
	악의적 메시지로 인한 배터리 소진 위협
	클라우드 자원 악용으로 인한 서비스 거부
데이터 정보 유출 및 위변조	부적절한 애플리케이션 사용
	모바일 단말의 분실 및 도난
	통신 내용 도감청 및 섹션 가로채기
	스팸 메시지를 통한 민감한 정보 획득
	데이터 통신 정보 수집을 통한 데이터 유출
	가상화 취약점을 악용한 프로파일 정보 유출
	모바일 관리 서버 해킹 후 악성코드 배포
	무선 네트워크의 도감청을 통한 데이터 유출
	비인증 접근점을 통한 데이터 유출
	서비스의 취약성으로 인한 데이터 유출
	연계성의 위험으로 인한 데이터 유출
공급자의 신뢰도실추	신뢰성 낮은 서비스 개발로 인한 보안 침해

모바일 클라우드 서비스의 위협시나리오는 모바일 클라우드 서비스의 위협 기술의 상관관계로 구성된다. 각각의 위협 기술은 공격자가 취약점을 악용하여 발생하며 다른 위협을 야기할 수 있다. 다음은 대표적인 모바일 클라우드 서비스의 위협시나리오를 설명하고 CVE(Common Vulnerability and Exposures) 기반으로 취약점을 분석하였다.



〔그림 3〕 오버플로어를 통한 서비스 권한 획득

공격자는 모바일 단말에서 수행되는 모바일 클라우드 서비스에서 요구되는 값을 초과하여 입력하여 모바일 단말에서 수행하는 모바일 클라우드 서비스에 대한 인증 우회 및 크랙 가능하다. 또한 오버플로우 위협을 통해 가상화 취약점을 위협하여 클라우드 단에서 정의된 가상머신의 특정 메모리 영역을 넘는 값 전달 한 후, 특정 가상머신에 대한 권한을 획득 할 수 있다. 해당 가상머신에 악성코드 호스팅이 될 경우, 해당 모바일 클라우드 서비스를 이용하는 악성코드 취약점을 가진 모든 모바일 단말이 악성코드에 감염되어 모바일 단말의 좀비로 제어 가능해 진다.

〔표 5〕 오버플로어를 통한 서비스 권한획득 시나리오 분석

위협 기술	대상	취약점 예
오버플로어	아이폰	CVE-2009-2795
	안드로이드	CVE-2009-1442
	윈도우즈 모바일	CVE-2010-2990
	심비안	CVE-2009-2538
인증 우회 및 크랙	아이폰	CVE-2009-2795
	윈도우즈 모바일	CVE-2008-4540
	안드로이드	CVE-2009-2692
가상화 취약점 위협	RHEV	CVE-2010-0431
	MS VM	CVE-2010-1225
	virtualBoX	CVE-2009-3940
	Xen	CVE-2008-3687
부적절한 권한 부여	MS VM	CVE-2009-1542
	VMware	CVE-2007-2491
	virtualBoX	CVE-2009-0876
	Xen	CVE-2008-3687
악성코드 호스팅	HP VM	CVE-2010-1035
	VM ware	CVE-2009-1244
	Xen	CVE-2008-3687
악성코드	아이폰	CVE-2010-1797
	안드로이드	CVE-2009-1442
	윈도우즈 모바일	CVE-2010-2990

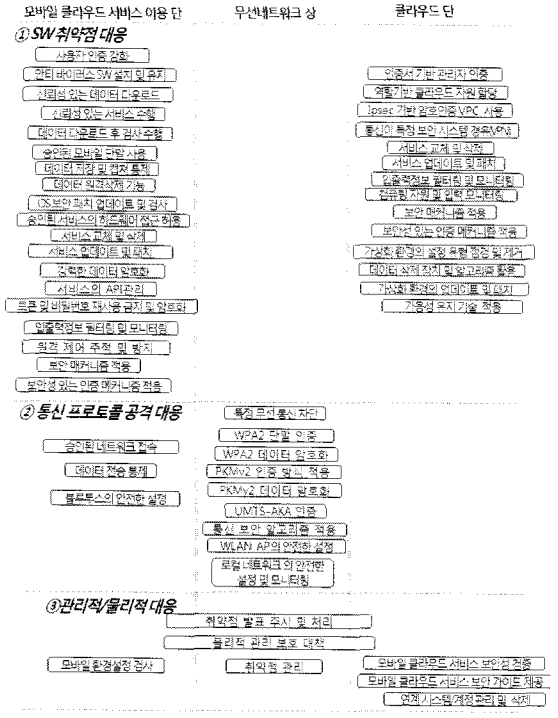
〔그림 3〕의 오버플로우를 통한 서비스 권한 획득 시나리오의 실제 취약점을 〔표 5〕와 같이 분석하였다. 아이폰의 CVE-2009-2795는 오버플로우 위협을 통해 인증 우회 및 크랙의 위협 기술을 수행하여 공격자가 서비스 권한을 획득하였다. 공격자는 모바일 클라우드 서비스의 권한을 획득한 후, Xen의 CVE-2008-3687과 같이 오버플로우 위협을 통해 가상화 취약점에 위협 후 부적절한 권한 부여 위협을 통해 서버 권한을 획득하고 악성코드에 감염될 수 있다. 그러므로 아이폰에서 Xen이 설치된 클라우드 자원을 이용하는 모바일 클라우드 서비스를 실행한다면, 공격자는 오버플로우 공격으로 인증을 우회하고 클라우드 단에 오버플로우 공격으로 가상화 취약점을 위협하여 모바일과 클라우드 단의 권한을 획득할 수 있다. CVE-2010-1797 취약점을 가진 다른 아이폰의 모바일 클라우드 사용자가 감염된 클라우드 자원에 접근한다면 급속도로 악성코드에 감염 될 것이다.

오버플로우의 취약점을 가진 안드로이드의 CVE-2009-1442는 인증 우회 및 크랙의 위협기술이 나타나지 않고 악성코드 위협 기술이 발생했지만 공격자 검거가 어렵다면, 부적절한 권한 부여와 인증 우회 및 크랙의 위협이 잠재되어 있다고 볼 수 있다.

IV. 모바일 클라우드 서비스의 위협 대응

4.1 모바일 클라우드 서비스의 위협 대응 방안

모바일 클라우드 서비스의 안전한 수행을 위해서는 〔그림 2〕와 같은 위협과 〔표 5〕와 같은 취약점의 악순환을 방지해야 한다. 클라우드 서비스 관리자는 공격기법에 대응하는 기술적 대책을 고려해야하여 소프트웨어와 프로토콜의 취약점의 악용을 차단해야 하며, 알려진 취약점을 제거하는 보안 관리를 통해 위협 수행을 막아야한다. 또한 관리자의 지속적인 관리적 물리적 대응이 이루어져야 한다. 〔그림 2〕의 모바일 클라우드 서비스의 위협은 〔그림 4〕의 모바일 클라우드 서비스 위협 대응과 같이 각 모바일 클라우드 서비스 이용 단, 무선네트워크 상, 클라우드 단에서 소프트웨어 취약점과 통신프로토콜 공격, 관리적/물리적인 방식으로 위협에 대응 할 수 있다.



〔그림 4〕 모바일 클라우드 서비스 위협 대응

○ 사용자 인증 강화 : 모바일 단말의 이동성으로 인해 분실 및 도난의 위험이 크므로 이에 대비한 사용자 인증 강화

○ 안티바이러스 소프트웨어 설치 및 유지 : 웹기반 서비스는 악성코드 감염과 전파의 위험이 크므로 안티바이러스 소프트웨어를 설치하고 최신 엔진상태를 유지하며, 주기적으로 모바일 단말의 검사를 수행

○ 신뢰성 있는 데이터 다운로드 : 신뢰할 수 있는 웹에서 검증된 데이터를 다운로드, P2P와 웹 하드 사용 금지

○ 신뢰성 있는 서비스 수행 : 신뢰할 수 있는 마켓을 통해 검증된 애플리케이션을 다운로드

○ 데이터 다운로드 후 검사 수행 : 다운로드 한 서비스 및 데이터를 안티바이러스를 통해 검사 수행

○ 승인된 모바일 단말 사용 : 승인된 모바일 단말과 저장매체 사용

○ 데이터 저장 및 캡쳐 통제 : 민감한 정보의 업무용 서비스의 경우 모바일 단말의 데이터 저장과 화면 캡처를 통제

○ 데이터 원격삭제 기능 : 모바일 단말 분실 및 도난으로 데이터 유출 위험을 방지하기 위해 서비스와 데이터를 원격으로 삭제

○ OS 보안 패치 업데이트 및 검사 : 모바일 단말의 OS의 보안 패치와 환경을 최신상태로 유지

○ 승인된 서비스의 하드웨어 접근 허용 : 중요한 모바일 단말의 하드웨어 대해서는 승인된 서비스만 접근할 수 있도록 통제

○ 서비스 업데이트 및 패치 : 서비스 및 가상화 환경의 응용프로그램의 취약점 위험을 제거하기 위해 지속적인 업데이트 및 패치

○ 서비스 교체 및 삭제: 업데이트 및 패치로 수정 불가능한 서비스 및 가상화환경의 응용 프로그램은 삭제 후 재설치

○ 입출력정보 필터링 및 모니터링 : 네트워크를 통해 모바일 단말과 서비스에 공격 정보 필터링 및 모니터링하여 오버플로어 및 악성코드 입력 방지

○ 보안 메커니즘 적용 : 경쟁조건과 소프트웨어 디자인 오류를 해결하기위해 보안 메커니즘 적용

○ 보안성 있는 인증 메커니즘 적용 : 적절하지 않은 인증 수단이나 인증이 적용되지 않은 경우 데이터 유출 및 변조를 해결하기위해 추가 적용

○ 인증서기반 관리자 인증 : 클라우드 자원의 내부관리자의 접근을 인증서 기반으로 강화

○ 역할기반 클라우드 자원할당 : 클라우드 자원을 역할 기반으로 할당함으로써 자원에 대한 인증과 자동화된 과금과 사용자의 상태와 개인적 특성 적용 가능하며, 자원의 상태 모니터링 및 대응 가능

○ Ipsec기반 암호인증 VPC(Virtual Private Cloud) 사용 :네트워크의 VPN(Virtual Private Network) 게이트웨이와 고객 네트워크의 게이트웨이 사이의 안전한 데이터 통신

○ 통신이 특정 보안 시스템 경유(VPN) : 특정 단말이 설정 외의 지역에 있다면 VPN 기술을 활용하여 특정 보안 시스템을 경유하도록 설정

○ 컴퓨팅 자원 및 입력 모니터링 : 클라우드 자원에 저장되는 정보와 자원 간 전송 되는 입력 모니터링

○ 가상화 환경 설정 점검 및 제거 : 가상화 환경의 예상 치 못한 설정으로 인한 종료를 해결하기 위해 설정에 대한 점검

○ 데이터 삭제 장치 및 알고리즘 활용 : 디스크의 중요정보 삭제 시 별도의 삭제 장치나 알고리즘 활용

○ 가상화 환경의 업데이트 및 패치 : 새로운 취약점에 대한 위험을 해결하기 위해 지속적인 가상화 환경에 대한 패치 설치 업데이트

○ 강력한 데이터 암호화 : 데이터 암호화를 위한 강력한 키 선택

○ 서비스의 API 관리 : 서비스 뿐 아니라 API의 취약점에 대응하기 위해 리스트 관리

○ 토큰 및 비밀번호의 재사용 금지 및 암호화 : 토큰 및 비밀번호 재사용 설정 해지 및 암호화

○ 원격제어 추적 및 방지 : 봇넷을 구성하는 경우 원격 서버를 추적하여 봇넷 제어 방지

○ 가용성 유지 기술 적용 : 가상화 서버들에 대한 고가용성 기술 및 작업부하관리 기술 적용

○ 데이터 전송 통제 : 모바일 단말과 데스크톱 간 악성코드 전파를 예방하기위해 무선네트워크와 USB를 통한 데이터 전송 통제

○ 승인된 네트워크 접속 : 모바일 단말의 네트워크 접근 설정을 통한 비인증 접근점 접속제어

○ 블루투스의 안전한 설정 : Discovery 모드 해제, 패스키 기반 통신 Pair(쌍) 생성 모드 활성화

○ 특정 무선 통신 차단 : 블루투스는 암호해독이 쉬운 PIN코드와 확인되지 않은 모바일 단말의 연결로 악성코드 감염 및 원격접속의 위험에 노출, 보안이 필요한 특정 지역에 대한 무선 통신 차단하여 제한

○ WPA2(Wi-Fi Protected Access v2) 단말 인증 : WLAN에서 사전에 공유키를 설정하여 세션을 맺는 WPA2-PSK(Pre-shared Keys)와 인증 서버를 통해 인증을 수행하는 WPA2-EAP(Extensible Authentication Protocol)을 통해 단말 인증

○ WPA2 데이터 암호화 : WLAN에서 AES (Advanced Encryption Standard)를 이용한 CCMP(Counter mode with CVC-MAC Protocol)로 더 강화된 데이터 암호화 제공

○ PKMv2(Privacy Key Management) 인증 방식 적용 : WiBro에서 RSA(Rivest Shamir Adleman)의 양방향 인증과 인증 서버를 이용하는 EAP(Extensible Authentication Protocol) 기반으로 단말인증 강화

○ PKMv2 데이터 암호화 : Wibro에서 데이터 및 TEK(Traffic Encryption Key) 교환을 위한 암호화 알고리즘 적용

○ UMTS-AKA(Universal Mobile Telecommunications System - Authentication and Key Agreement)인증 : HSDPA에서 단말의 USIM과 네트워크상의 인증센터가 비밀 키를 가지고 있다고 전제하고 무선구간에서 암복호화 및 무결성 확인을 위한키를 Chllenge/Response 방식으로 공유

○ 통신 보안 알고리즘 적용 : HSDPA에서 3GPP(3rd Generation Partnership Project)의 보안 구조의 보안 알고리즘 적용

○ WLAN AP(Access Point)의 안전한 설정 : 서비스 식별자 브로드캐스팅 기능 해제

○ 로컬 네트워크의 안전한 설정 및 모니터링 :ARP(Address Resolution Protocol)메시지 관리 및 IP/DNS/ARP 스푸핑 사전 방지 기술 적용

○ 취약점 발표 주시 및 처리 : 소프트웨어 대한 취약점을 제거하고 취약점을 악용하는 공격 기법들이 작동하지 못하도록 주시하고 대책마련

○ 취약점 관리 : 서비스 사용자와 네트워크 서비스 제공자 및 서비스 제공자 사이의 상호협력을 통한 취약점 확인 및 관리

○ 물리적 관리 보호 대책 : 클라우드서비스 제공자는 IDC운영자의 관리적 보호대책을 따라야 하며 가상화환경과 모바일단말에 대한 물리적 관리체계 적용

○ 모바일 환경설정 검사 : 위치 추적, 제한 없는 데이터 수락 및 인증 우회 등을 불가능하게 하기 위한 안전한 모바일 환경설정

○ 모바일 클라우드 서비스 보안성 검증 : 모바일 응용에 대한 적절한 보안 심사과정 도입

○ 모바일 클라우드 서비스 보안 가이드 제공 : 모바일 응용 개발자에게 안전한 프로그래밍 가이드 제공

○ 연계시스템/계정 관리 및 삭제 : 클라우드 서비스와 신뢰 관계를 갖는 연계 시스템 혹은 계정을 만들지 않도록 관리

4.2 위협 시나리오 기반 대응 방안

〔표 6〕 오버플로어를 통한 서비스 권한획득 위협대응

위협기술	위협대응
오버플로어	서비스 업데이트 및 패치 입력 정보 필터링 및 모니터링
인증 우회 및 크랙	사용자 인증 강화 서비스 업데이트 및 패치
가상화 취약점 위협	가상화 환경의 설정 유형 점검 및 제거 가상화 환경의 업데이트 및 패치 보안 메커니즘 적용
부적절한 권한 부여	사용자 인증 강화 인증서 기반 관리자 인증 역할기반 클라우드 자원 할당 보안성 있는 인증 메커니즘 적용
악성코드 호스팅	컴퓨팅자원 및 입력 모니터링 서비스 업데이트 및 패치/서비스 교체
악성코드	안티바이러스 설치 및 유지

모바일 클라우드 서비스의 위협기술에 대응하는 정보보호대책은 위협 시나리오를 기반으로 〔표 6〕과 같

다. 공격자의 오버플로어의 위협은 모바일 클라우드서비스에서 입력에 대한 필터링을 통해 방지할 수 있다. 이러한 입력 필터링 기능은 모바일 클라우드 서비스에서 제공해야 하며, 업데이트 및 패치로 최신기능으로 유지되어야 한다. 모바일 클라우드 서비스에서 기능을 제공하지 않을 경우 별도의 입력 모니터링이 수행되어야 한다. 인증 우회 및 크랙은 비밀번호와 인증 패턴이 정책적 결정을 따르고 일부에게 모바일 단말에 저장되는 인증정보를 제공하는 사용자 인증 강화로 대응할 수 있으며, 서비스의 취약점으로 인증정보 관리가 제대로 안될 경우는 서비스 업데이트 및 패치로 대응할 수 있다. 가상화 취약점 위협은 가상화 환경의 설정 유형을 지속적으로 점검하고 불안 요소를 제거하며, 업데이트 및 패치를 항상 수행해야 한다. 또한 보안성 강화를 위해 보안 메커니즘을 적용할 수 있다. 부적절한 권한 부여의 위협은 모바일 클라우드 서비스 이용 단의 사용자 인증강화와 클라우드 단의 인증서 기반 관리자 인증, 역할기반으로 관리자 인증, 권한 부여를 할당을 보안성 있는 인증 메커니즘을 적용하여 대응할 수 있다. 모바일 단말과 클라우드 단의 악성코드 감염 및 좀비화는 악성코드 입력을 지속적으로 모니터링하고 서비스를 업데이트 및 패치하며 서비스 이상 발생 시 신속하게 교체해야 한다. 또한 악성코드를 탐지 할 수 있는 안티바이러스 설치와 유지를 지속적으로 해야 한다.

V. 결론

본 연구는 모바일 클라우드 서비스 보안위협 침해대응 방안을 제안하기 위해 모바일과 무선네트워크, 클라우드 서비스의 보안 위협을 조사 및 분석하고 이를 기반으로 모바일 클라우드 서비스에서 발생 가능한 보안 위협 요소를 도출하였다. 또한 공격자의 위협 의도 관점으로 위협 시나리오를 도출하고 이를 클라우드 서비스 위협 기술과 취약점 관계를 분석하였다. 모바일 클라우드 서비스의 위협기술에 대응하기위한 대응방안을 위협기술의 상관관계로 구성된 시나리오와 취약점을 기반으로 활용 가능한 정보보호기술을 대입하여 도출 하였다. 본 연구는 모바일 클라우드 서비스를 제공하는 사업자가 고려해야 할 보안 위협기술과 취약점을 고려하여 위협대응 기술을 적용할 수 있으며, 위협기술 발생 시, 해당 위협기술과 이로 인해 발생 할 수 있는 위협기술에 대한 대응방안을 마련하기 위한 지표로 활용 될 수 있다. 향후 위협 기술과 위협 시나리오를 추가 도출 할 것이며, 위험 정도에 따른 위협의 우선순위와 이에 요구되는 보안등급별 대응방안을 도출 할 것이다.

참고문헌

[1] F. Samimi, P. McKinley and S. Masoud Sadjadi, "Mobile Service Clouds : A Self-managing Infrastructure for Autonomic Mobile Computing Services", Lecture Notes in Computer Science, vol. 3996, pp. 130 - 141, June 2006.

[2] Dan Hubbard and Michael Sutton, "Top Threats to Cloud Computing V1.0", Cloud Security Alliance, March 2010

[3] Glenn Brunette and Rich Mogull, "Security Guidance for Critical Areas of Focust in Cloud Computing V2.1", Cloud Security Alliance, December 2009

[4] Z. Cheng. "Mobile Malware: Threats and Prevention" McAfee Avert Labs, 2007

[5] Hypponen and Mikko. "Malware Goes Mobile.", Scientific American, pp. 70 - 77, November 2006

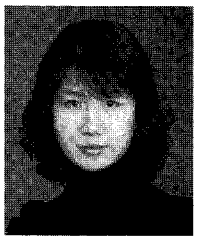
[6] Christopher Abad, "Taxonomy of Current and Potential Mobile Threats", CLOUDMARK, January 2007

[7] United States Computer Emergency Readiness Team "Cyber Threats to Mobile Device", TIP-10-105-01, US-CERT, April 2010

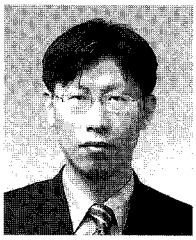
[8] Airwide Solutions, "Taking on the Challenge of Mobile Messaging Abuse", Airwide Solutions Inc, 2009

[9] Santosh K. Pandey, "Major Security Threats in Wireless Networks, The Institute of Chartered Accountants of India

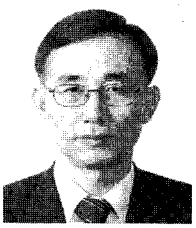
〈著者紹介〉



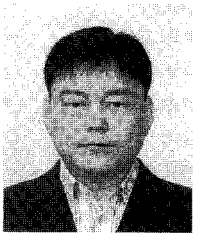
장 은 영 (Eun young Jang) 학생회원
2008년: 서울여자대학교 정보통신공학부 멀티미디어통신공학과(공학사)
2009년~현재: 서울여자대학교 일반대학원 컴퓨터학과 석사과정
〈관심분야〉 개인정보보호, 네트워크 보안, 취약점 분석 및 모델링, 클라우드컴퓨팅 보안



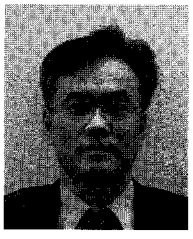
김 형 종 (Hyung Jong Kim) 종신회원
1996년: 성균관대학교 정보 공학과(공학사)
1998년: 성균관대학교 정보 공학과(공학석사)
2001년: 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
2001년~2007년: 한국정보보호진흥원 수석연구원
2004년~2006년: Carnegie Mellon University, USA Visiting Researcher
2009년~2010년: 한국시뮬레이션학회 편집위원장
2007년~현재: 서울여자대학교 컴퓨터학부 조교수
〈관심분야〉 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 인터넷전화 보안기술



박 춘 식 (Choon sik Park) 종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교 컴퓨터학부 교수
〈관심분야〉 개인정보보호기술, 클라우드컴퓨팅 보안



김 주 영 (Ju Young Kim) 정회원
2005년: 한양대학교 컴퓨터공학 석사
2002년 4월~현재: 한국인터넷진흥원 미래인터넷팀장
〈관심분야〉 미래인터넷보안, 클라우드컴퓨팅보안



이 재 일 (Jae Il Lee) 정회원
1988년: 서울대 계산통계학과 학사,석사
2006년: 연세대 컴퓨터과학과 박사
1991년~1996년: 한국 IBM 소프웨어연구소
1996년~2009년 7월: 한국정보보호진흥원 전자거래보호단장, IT기반보호단장
2009년 7월~2009년 12월: 한국인터넷진흥원 정책개발단장
2010년 1월~현재: 한국인터넷진흥원 인터넷융합단장
〈관심분야〉 인터넷, 정보보호