https://doi.org/10.33778/kcsa.2022.22.2.043

‘스마트 폰’의 보안 취약요인에 관한 연구★

전 정 훈*

요 약

모바일 기기는 이미 일상생활에 있어, 삶의 필수도구가 되었다 해도 과언이 아니다. 이러한 모바일 기기 중에 대표적인 스마트폰은 신제품이 출시될 때마다 새로운 기능과 서비스를 선보이며 시장을 과열시키고 있다. 하지만 대부분의 사용자들은 제조사나 서비스, 기능에 따라 다양한 취약점들이 있는 것을 모른 채 사용하고 있으며, 취약점들을 악용한 공격들로 인해 피해가 발생하고 있다. 이에 대한 연구는 이미 진행되어왔지만, 새로운 기기와 운영체제, 서비스, 기능에 따라 다양한 차이를 갖고 있어, 예측하기란 매우 어렵다. 이러한 까닭에 새로운 취약요인에 대해 지속적인 모니터링과 연구가 필요하다. 따라서 본 연구를 통해 이제까지의 연구 및 취약점, 공격기술, 대응기술을 고찰해 보고, 대응 방안을 제안함으로써 향후 시스템 및 대응기술 개발의 기초 자료로 활용될 수 있을 것으로 기대한다.

A Study on the Security Vulnerability Factors of Smart Phones

Jeon Jeong Hoon*

ABSTRACT

It is no exaggeration to say that mobile devices have already become an essential tool in our daily life. Among these mobile devices, a representative smart phone is overheating the market by introducing new functions and services whenever a new product is released. However, most users do not know that there are various vulnerabilities depending on the manufacturer, service, or function, and damage is occurring due to attacks that exploit the vulnerabilities.Research on this has already been conducted, but it is very difficult to predict because there are various differences depending on new devices, operating systems, services, and functions. For this reason, it is necessary to continuously monitor and study new vulnerable factors. Therefore, through this study, research so far, vulnerabilities, attack technology, and response technology were considered. In addition, it is expected that it can be used as basic data for the development of systems and response technologies in the future by proposing countermeasures.

Key words : Mobile Device, Smart Phone, Vulnerability Factors, Voice phishing, Smishing, OWASP

접수일(2022년 05월6일), 수정일(1차: 2022년 05월21일), 게재확정일(2022년 06월 18일)

★ 이 논문은 2020년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교/컴퓨터학과(주저자)

1. 서 론

최근 4차 산업혁명의 기반 기술들이 이슈화 되고 있는 가운데, 이 기술들을 제어하고 응용하는데 모바일 기기가 널리 사용되고 있다[1]. 모바일 기기는 단순 통신 기기에 그치지 않고 일상생활에 없어서는 안 될 필수 기기가 되어 버린 지도 오래다. 특히 모바일 기기 중 대표적인 스마트폰은 신품 출시에 따른 다양한 기능 및 서비스의 생성과 소멸 주기가 짧아 진화 속도가 매우 빠른 특징을 갖고 있다. 이러한 여러 장점들도 있지만, 보안취약점 또한 빠르게 진화하고 있음도 간과해서는 안될 것이다. 취약요인은 여러 관련 연구 자료들을 통해 찾아볼 수 있지만, 변화에 따른 지속적인 대응이 필요한 실정이다[2][3].

따라서 본 논문은 연구 자료들을 토대로 취약요인 연구와 공격 그리고 악성코드의 대응 방안을 제안해 봄으로써, 향후 모바일 기기의 하드웨어 및 소프트웨어의 개발뿐 아니라 대응기술 개발에 기초 연구 자료로 활용될 수 있을 것으로 기대한다. 본 고의 논리적 구성을 위해 2장은 기존의 연구와 공격, 대응, 동향과 보안취약점을 알아보고, 3장에서는 대응 방안을 제안한다. 그리고 4장은 성능비교 및 개선 효과에 대해 알아보고, 마지막 5장의 결론으로 글을 마치도록 한다.

2. 관련 연구

2.1 연구 동향

모바일 기기의 취약요인에 관한 연구가 본격적으로 시작된 시기는 관련 연구와 사용이 증가하기 시작한 2007년, 애플 스마트폰의 출시 이후로 볼 수 있다. 초기 모바일 기기의 등장 이후 무선 취약성을 이용한 공격으로 시작해, 점차 개인정보를 타겟(target)으로 하는 공격으로 진화했다. 하지만 모바일 기기의 보안성과 안전성이 높아짐에 따라, 취약요인의 감소를 기대하였지만 그렇지 않은 것이 현실이다. 이에 <표 1>은 취약요인에 대한 이전 연구들을 요약한 것이다. <표 1>을 살펴보면, 초기 연구는 기존 통신주파수와 와이파이(wifi) 등의 무선 통신 환경과 개방성, 휴대성, 저성능 등에 따른 기능 중심의 연구가 진행되었음을 알 수 있다[4].

<표 1> 취약요인 관련 연구 동향

년도	취약요인에 관한 연구
2010	스마트폰 주파수 변조를 이용한 전파교란 취약점 연구[5]
	스마트폰 환경하에 소셜 개인 방송서비스의 취약점 연구[6]
2011	윈도우 CE기반기술 스마트폰의 SMS 관리 취약점 연구[7]
	인터넷과 SNS에서의 저작권 관련 문제연구[8]
	안드로이드 어플리케이션 보안취약점에 관한 연구[9]
	스마트폰용 모바일 웹페이지에 대한 취약점 분석[10]
2012	스마트폰에서 NFC를 이용한 융.복합 하이브리드 취약점[11]
	스마트폰뱅킹을 위한 공인인증서 복사 프로토콜의 취약점 분석[12]
	사용자 중심의 스마트폰 보안 취약성 분석 어플리케이션 개발[13]
	HTML5 차세대 웹표준 환경에서의 보안 이슈[14]
2013	안드로이드 스마트폰 뱅킹 앱 무결성 검증 기능의 취약점 연구[15]
	스마트폰에서의 SSL/TLS 전송구간 취약점 연구[16]
2017	SMS 기반 인증의 보안 취약점을 개선한 스마트폰 소유 및 위치 확인 기법[17]
2018 ~ 현재	스마트폰 동적 가상키보드의 취약점 분석[18]
	시나리오 기반의 스마트폰 취약점에 대한 보안방안[19]

2011년에는 모바일 기기의 활성화에 따른 애플리케이션의 증가와 물리적 도난 및 분실에 따른 연구가 되었다[20]. 이후 2012~2017년에는 전자상거래의 활용이 증가하면서, 인증과 결재 서비스가 주요 요인으로 다루어졌으며[21], 2018년부터~현재까지는 다양한 플랫폼과 서비스에 따른 취약요인에 대해 연구되었다[22]. 결과적으로 2012년 이전 연구들은 기기나 기능 위주의 연구에서 점차 서비스로 진화해 가고 있음을 알 수 있다.

2.2 공격기술 동향

<표 2>는 앞서 연구 자료를 토대로 모바일 기기의 공격유형들을 요약하였다. <표 2>를 살펴보면, 초기 무선 환경의 장애나 배터리 소진, 과금 등 기기나 기능을 대상으로 하는 공격에서 정보나 서비스를 대상으로 하는 공격으로 점차 옮겨감에 따라, 보다 지능화된 공격으로 변화해 가고 있음을 알 수 있다[4].

<표 2> 공격 관련 동향

공격분류	공격유형
악성코드 공격 (2010~)	초기 단말 장애 유발형
	초기 배터리 소모형
	초기 과금 유발형
	정보 유출형
	크로스 플랫폼형
네트워크 공격 (2011~)	DoS 공격
	무선 네트워크의 데이터 도청 및 위변조
사용자 (2012~)	도난과 분실, 피싱, 보이스피싱, 스미싱

최근 공격은 사용자 정보를 획득하기 위한 보이스피싱이나 스미싱 등이 주를 이루고 있으며, 무작위 대상에서 특정 대상으로 집약되고 있다. 이제 모바일 기기는 더 이상 단순 통신 기기로서의 역할만이 아니라, 사용자의 다양한 정보를 수집함과 동시에 공격대상이 되고 있음을 알 수 있다[20][22].

2.3 대응 동향

<표 3> 대응 방안[5]

분류	대응 방안
무선 네트워크	초기 무선 AP 보안관리
	개인 위치정보 측위 방지
악성코드	초기 마켓 애플리케이션의 보안 검증
	안티바이러스 백신
	원격서비스, 폰 장금장치, 초경량 암호화 알고리즘

<표 3>은 대응 방안에 대한 연구를 요약하였다. 초기 무선 환경의 취약요인에 대해 AP(access point) 보안으로 대응 방안을 제시하였고, 점차 증가하는 악성코드의 근원이었던 앱(app) 마켓은 보안 검증과 백신으로 대응 방안을 제시하였다. 그리고 개인정보의 공격은 인증 및 권한, 암호를 통해 대응하였다[20]. 하지만 점차 증가하고 있는 멜웨어 및 바이러스에 대해서는 백신만으로 대응이 어렵고, 보안 검증을 하지 않는 앱에 대해서도 완전한 대응이 불가한 실정이다. 꾸준히 성장하고 있는 스마트 시장을 고려해볼 때, 피해는 더욱 커질 것으로 예상된다.

2.4 보안 취약점

2.4.1 OWASP

<표 4> OWASP 2010, 2014년 취약요인

구분	취약요인
네트워크	▪ Weak Server-Side Control ▪ Client Side Injection ▪ Insufficient Transport Layer Protection ▪ Inappropriate Session Handling
데이터	▪ Side Channel Data Leak ▪ Insecure Data Storage ▪ Broken Encryption ▪ Lack of Binary Protections
인증/권한	▪ Incorrect Authorization and Authentication
개발/사용자	▪ Security Decisions through Untrusted Input ▪ Sensitive Information Disclosure

<표 5> OWASP 2016~2020년도 취약요인

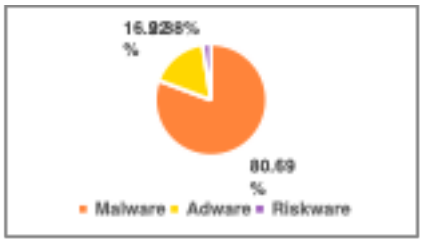
구분	취약요인
네트워크	M3: Insecure Communication
데이터	M2: Insecure Data Storage M5: Insufficient Cryptography
인증/권한	M4: Insecure Authentication M6: Insecure Authorization
개발	M10: Extraneous Functionality M1: Improper Platform Usage M7: Client Code Quality M8: Code Tampering M9: Reverse Engineering

OWASP(The Open Web Application Security Project)는 '개방 웹 애플리케이션 보안 프로젝트'로서는 2004년부터 약 3~4년 간격으로 보안에 영향을 줄 수 있는 취약점 10가지를 선정하고 있다. 특히 모바일 관련해서는 2010년부터 모바일 취약점 Top 10을 발표해 왔다[25][26]. <표 4>는 2010년과 2014년도의 취약요인들을 요약 정리한 것으로 2010년 이후, 초기 공격유형들에 따른 취약요인이 구체적으로 분류되었다면, <표 5>는 유사 요인들을 범주에 따라 체계화하고 있음을 알 수 있다. 특히 항목 중, '개발' 부분은 악성코드에 관한 것으로 항목이 늘어나 있는 것을 볼 때, 악

성코드로 인한 공격이 다양화되고 있음을 말해준다.

2.4.2 멜웨어(malware)

최근 모바일 공격은 정보 유출을 목적으로 하는 피싱이나 보이스피싱, 스미싱 공격이 대부분을 차지한다. 이러한 공격유형들은 단독 실행이 아니라 멜웨어나 애드웨어 같은 악성코드에 의해 시도되어 역시 취약요인이 된다[27]. (그림 1)은 모바일 기기 공격에 사용된 소프트웨어의 분포로 멜웨어가 80.6%를 나타냈고, 애드웨어(adware)는 16.92%를 나타냈다[27].



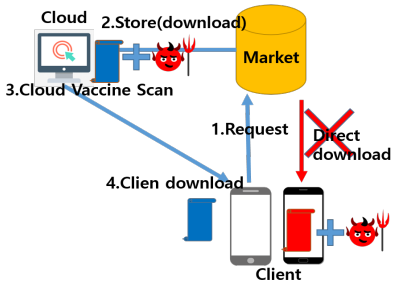
(그림 1) 모바일 공격에 사용된 SW 2021

결과적으로 스마트폰의 주요 보안 취약요인은 악성코드가 되고 있음을 알 수 있다. 따라서 악성코드의 유입경로를 선별하고, 이를 우회하여 차단함으로써 스마트폰의 보안성을 높일 수 있을 것이다.

3. 클라우드를 이용한 악성코드 차단 방안의 제안

3.1 제안 방안의 시나리오

앞서 2장을 통해 악성코드의 비중이 커지고 있음을 알 수 있었다. 이에 스마트폰의 악성코드 취약요인은 사용자가 파일을 직접 내려받는 방식에 있다. 따라서 플랫폼의 클라우드를 이용한 대응 방안을 제안하고자 한다. 시나리오의 주요 내용은 (그림 2)와 같다. 사용자가 플랫폼으로부터 파일을 내려받고자 할 때, 플랫폼은 클라우드를 백신의 샌드박스(sendbox)와 같이 사용함으로써, 악성코드의 직접 유입경로에 대한 위험을 경감 하고자 한다. 다음은 (그림 2)의 제안 내용을 단계별로 설명한다.



(그림 2) 클라우드를 경유한 다운로드

① 플랫폼 기업인 '마켓(Market)'은 사용자의 다운로드 요청에 응답한다.
② 마켓은 파일을 자신들의 클라우드에 복사한다.
③ 클라우드는 백신을 통해 악성코드의 검색 및 제거를 수행하며 사용자에게 준비화면을 제공한다.
④ 클라우드는 검색을 마친 파일을 사용자에게 전송하며 다운로드 화면을 제공한다. 전송 후, 파일은 정책에 따라 삭제한다.

3.2 클라우드 공간의 활용 방안 제안

스마트폰의 보안취약점은 악성코드 유입경로인 다운로드를 통해 직접 파일을 내려받는데 있다. 따라서 플랫폼 기업의 클라우드와 플랫폼을 이용해 사용자가 내려받는 파일을 클라우드에 임시 저장하고, 복사본을 사용자에게 전송 후 삭제함으로써 직접 다운로드로 인한 악성코드 유입 문제를 해결하도록 제안한다.

3.3 클라우드의 자원 활용 방안 제안

스마트폰 상에서 백신과 같은 소프트웨어들을 수행할 경우, 적지 않은 시스템 부하로 성능저하를 초래하여 다른 서비스의 사용에 영향을 미치게 된다. 따라서 앞서 3.2절과 같이 복사본의 전송 전에 악성코드에 대한 검색 및 제거를 수행함으로써 스마트폰의 효율적인 자원 활용을 제안한다.

3.4 클라우드의 저장소 관리 방안 제안

클라우드의 사용자 요청 파일은 효율적인 관리가 필요하다. 파일의 저장 방식은 크게 공용 또는 사용자별 관리로 나눠 볼 수 있으며, 이는 악성코드의 검색

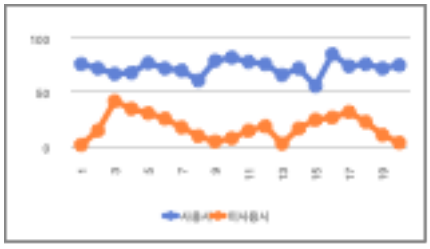
시간과 자원 사용에 영향을 미친다. 저장 공간의 사용 권한은 플랫폼에 부여하되, 감염위험으로 파일의 실행(execute)을 제외한 읽기(read)와 쓰기(write)만을 허용한다. 복사본은 하드웨어의 수명을 고려해 실시간 삭제보다는 용량 하한 설정을 통한 방법을 제안하며, 접근권한은 플랫폼의 접근만으로 제한한다.

4. 성능 분석 및 개선 효과

4.1 성능 분석

4.1.1 스마트폰의 자원 소모 측정

실험은 스마트폰에서 백신을 사용할 경우, CPU의 변화를 측정하고자 한다. 측정 소프트웨어의 멀티 창 수행이 불가하여 유사한 모바일 기기장치인 Nexus 2. 5Ghz core 2를 사용했으며, 측정 도구는 “CPU/GPU Meter & Notification” 앱과 백신은 ‘Avira’를 사용하였다. 그리고 백신의 사용과 미사용 시, CPU 값을 각각 20회 측정하였다.



(그림 3) CPU 변화 측정값

(그림 3)의 가로축은 횟수, 세로축은 사용률(%)을 나타낸다. (그림 3)의 결과는 불규칙한 흐름을 보였지만 사용과 미사용 시의 자원 사용률의 차이가 매우 큼을 알 수 있다.

4.1.2 서비스 사용에 따른 소모자원 측정

백신 동작 중 다른 서비스의 사용 시, CPU의 변화를 측정하였다. 4.1.1의 실험환경과 동일 조건에서 횟수를 10회로 하였으며, 백그라운드 수행이 가능한 멀티미디어 서비스 수행 시 측정하였다.

(그림 4) 서비스 사용 시 측정값

(그림 4)의 측정 결과는 예상된 결과였지만 다소 불규칙한 흐름을 보였다. 초기 자원 사용이 80%를 넘는 CPU 사용률을 보임으로써 다른 서비스의 사용에 매우 큰 영향을 미치고 있음을 알 수 있었다.

4.1.3 경로 우회에 따른 소요 시간 분석

클라우드로 경로를 우회할 경우, 얼마의 지연이 발생하였는지를 알아본다. 지연시간은 기존 플랫폼으로부터 파일을 내려받을 경우, 소요 시간을 ‘t’ 초라 한다면, 제안 방식은 (그림 2)의 2단계로 복사본을 클라우드로 전송하는데 ‘a’ 초가 발생하고, 백신 소프트웨어로 검색 시 걸리는 시간이 ’T‘초에 최종 사용자가 내려받는 시간을 더 해준다. 이를 정리해보면 기존 방식은 ’t’ 초, 제안 방식은 최소 ($a+T+t$) 초가 소요된다. 여기에는 클라우드와 플랫폼 간의 네트워크와 백신의 검색 대상 파일의 크기가 변수로 작용하여 소요 시간은 더 늘어날 수 있다.

4.1.4 제안 방식의 비교 분석

기존 방식은 스마트폰 상에 파일을 내려받고자 할 때, 악성코드의 위험과 시스템 자원의 소모는 커지며, 다른 서비스에도 영향을 미친다. 그리고 소프트웨어와 환경에 따라 시스템 자원 소모에 차이를 가질 수 있으며, 성능은 저하된다. 반면 제안 방식은 백신의 샌드박스(sendbox)와 같이 클라우드로 전송함으로써, 스마트폰의 자원 소모는 없으며, 악성코드의 위험도 없다. 단지 클라우드로부터 파일을 내려받을 경우, 기존 파일을 직접 받을 때와 마찬가지로 일부 자원 소모가 발생한다. 결과적으로 4.1.3절과 같이 내려받는 시간이 늘어나는 단점은 있지만, 악성코드를 검색하는데 자원을 사용하지 않기 때문에 안정적인 스마트폰 서비스를 지속할 수 있으며, 무엇보다도 악성코드의 유입을 차단할 수 있다.

4.2 개선 효과

기존 방식과 제안 방식의 비교 시, 어떤 개선된 효과가 있는지를 <표 8>로 정리하였다.

<표 10> 개선 효과

	스마트폰 기반	클라우드 기반
안전성	불안정	안정
효율성	비효율적	효율적
지연성	비교적 짧음 t 시간	긴 지연발생 최소$(a+T+t)$시간
차단성	낮음	높음

- 안정성(stability) : 제안 방식은 다운로드를 통한 스마트폰의 악성코드 유입을 경감시킬 수 있고, 시스템 자원의 효율적인 사용이 가능하여 안정적이라 할 수 있다. 특히 백신을 설치하지 않은 사용자의 부주의로 인한 악성코드 유입에 대응이 가능하다.
- 효율성(efficiency) : 사용자 기기의 사양에 따라 차이를 가질 수 있지만, 제안 방식은 사용자의 시스템 자원을 악성코드 검색에 소모하기보다는 원하는 서비스에 사용할 수 있어, 높은 자원 효율성이 예상된다.
- 지연성(delay) : 제안 방식은 기존보다 최대 2배 이상의 지연시간이 소요된다. 이는 경로변경으로 인한 지연시간이 추가로 발생하기 때문이며, 시스템 및 네트워크 상황에 따라 추가 지연이 발생할 수 있다.
- 차단성(blockability) : 제안 방식은 클라우드의 저장 공간을 사용함으로써 스마트폰에 대한 직접적인 악성코드 유입을 차단하는 효과를 갖는다.

5. 결 론

스마트폰은 대표적인 모바일 기기로 점차 일상생활에 없어서는 안 될 필수도구가 되었다. 그리고 사용 연령대는 낮아지기도 하였지만, 또한 높아지기도 하여 폭넓은 연령층을 갖게 되었다. 이러한 가운데 사용자는 다양한 서비스와 편의 기능을 제공받게 되었고 제공자는 사용자의 정보들을 요구하는 관계가 되면서, 모바일 기기는 점차 정보의 수집 도구가 되어갔다. 최근 사용자에 대한 보이스피싱과 스미싱 공격으로 인한 피해가 급증하고 있는 가운데, 보안 문제는 매우 심각한 수준에 이르게 되었다. 스마트폰에 저장하고 있는 각종 정보는 공격의 빌미를 제공해줌으로써, 악성코드에 대한 대응이 필요하다. 이에 악성코드의 유입경로 중, 다운로드의 대응 방안을 제안하였지만, 보다 실효성 있는 대응을 위해서 제도적인 지원이 전제되어야 할 것이며, 기업들의 협력이 필요함을 알 수 있었다.

따라서 본 고는 취약요인들을 분류하고 악성코드 유입 차단을 위한 방안을 제안해 봄으로써, 향후 보다 효과적인 대응 및 기술 개발에 기여할 수 있을 것으로 기대한다. 그러나 활용성과 함께 취약요인도 증가하고 있어, 사용자 중심의 취약요인의 지속적인 연구가 필요한 가운데 이에 따른 대응 방안 마련도 병행되어야 할 것이다.

참고문헌

[1] 경향신문 “스마트폰 없인 못살아” 67%, TV는 30%…방통위 2020 방송매체 이용행태조사,“ http:// biz.khan.co.kr/khan_art_view.html?artid=202102021130001&code=920100, 2021.2.2.

[2] 악성앱 이용한 스마트폰 해킹 공포, https://www.boannews.com/media/view.asp?idx= 96073, 보안뉴스, 2021..3.11.

[3] Search mobile computing, “Top 4 mobile security threats and challenges for businesses,” https://searchmobilecomputing.techtarget.com/tip/Top-4-mobile-security-threats-and-challenges-for-businesses, techtarget. 2021.5.11.

[4] 강동호 외6인, “스마트폰 보안위협 및 대응기술,” ETRI 전자통신동향분석, Vol. 25, No 3, 2010.6.

[5] 김인범 외2인, “스마트폰 주파수 변조를 이용한 항공 통신 시스템 전파교란 취약점,” 정보·보안논문지, Vol. 10, No. 4, pp. 49-59, 2010.12

[6] 강장묵 외2인, “스마트폰 환경하에 소

셜 개인 방송서비스의 취약점 연구," 한국인터넷방송통신학회 논문지, Vol. 10, No. 6, pp. 161-167, 2010.
[7] 정진혁 외2인, "윈도우 CE 기반 스마트폰의 SMS 관리 취약점 분석," 한국정보과학회 논문지, Vol. 38, No. 2, pp. 147-156, 2011.4.
[8] 김병일, "인터넷과 SNS에서의 저작권 관련 문제연구," 한국언론법학회 논문지, pp. 105-133, 2010.12.
[9] 한찬규 외3인, "안드로이드 어플리케이션 보안 취약점에 관한 연구," 한국정보처리학회, Vol. 5, No. 11, pp. 854-857, 2011.4.30.
[10] 곽경주 외2인, "스마트폰용 모바일 웹페이지에 대한 취약점 분석," 한국정보처리학회, pp.866-868, 2011.4.30.
[11] 박창민 외1인, "스마트폰에서 NFC를 이용한 융.복합 하이브리드 취약점," 한국융합보안학회 논문지, Vol. 12, No. 4, pp. 3-8, 2012.
[12] 신동오 외3인, "스마트폰뱅킹을 위한 공인인증서 복사 프로토콜의 취약점 분석," 한국통신학 논문지, Vol. 137c, No. 9, pp. 841-850, 2012.
[13] 조식완 외2인, "사용자 중심의 스마트폰 보안 취약성 분석 어플리케이션 개발," 한국융합보안학회 논문지, Vol. 13, No. 2, pp. 7-12, 2012.
[14] 강석철 외1인, "HTML5 차세대 웹표준 환경에서의 보안 이슈," 정보보호학회지, Vol. 24, No. 4, pp. 44-55, 2014.8.
[15] 김순일 외2인, "안드로이드 스마트폰 뱅킹 앱 무결성 검증 기능의 취약점 연구," 정보보호학회논문지, Vol. 24, No. 4, pp. 743-755, 2013.
[16] 강원민 외2인, "스마트폰에서의 SSL/TLS 전송구간 취약점 연구," 한국정보처리학회, Vol. 24, No. 8, pp. 890-891, 2013.
[18] 권성재 외1인, "SMS 기반 인증의 보안 취약점을 개선한 스마트폰 소유 및 위치 확인 기법," 한국통신학회 논문지, Vol. 42, No. 2, pp. 349-357, 2017.
[18] 조태남 외1인, "스마트폰 동적 가상키보드의 취약점 분석," 한국정보처리학회 논문지, Vol. 8 No. 1, pp. 9-16, 2019.1
[19] 이재호 외2인, "시나리오 기반의 스마트폰 취약점에 대한 보안방안," 인문사회과학기술융합학회, Vol. 8 No. 6, pp. 835-844, 2019.1
[20] 서승현 외1인, "스마트폰 보안위협 및 대응전략," TTA Journal No. 135, pp. 44-48, 2010.
[21] 아시아타임즈, "올해의 '모바일 보안위협 트렌드'는?," https://www.asiatime.co.kr/85784, 2015.1.15.
[22] 전응렬 외3인, "스마트폰 보안위협과 대응기술 분석," 한국컴퓨터정보학회, Vol. 16, No. 2, pp. 153- 163, 2011.2.
[23] Forbes "5 Reasons Hackers Target Mobile Devices And How To Stop Them," https://www.forbes.com/sites/tmobile/2021/02/24/5-reasons-hackers-target-mobile-devices-and-how-to-stop-them/?sh=cbe6b717b283, 2021.2.24.
[24] Miguel Hernandez Bejarano, Luis Eduardo Baquero Rey, Celio Enrique Gil, "Ethical Hacking on Mobile Devices: Considerations and practical uses.," International Journal of Applied Engineering Research, 13(23), pp. 16637-16647, 2018.12.
[25] Guard Square, "The History of the OWASP Mobile Top 10 and What

Changes Mean to Developers," https://community.guardsquare.com/t/the-history-of-the-owasp-mobile-top-10-and-what-changes-mean-to-developers/276, 2020.10.
[26] OWASP 모바일 상위 10개 취약점 및 완화 전략, https://sectigostore.com/blog/owasp-mobile-top-1 0/ 2020.12.21.
[27] "모바일 악성코드 진화 2021," Kaspersky, 2022.2.
[28] 앱스토어 아키텍처, https://www.researchg ate.net/figure/The-APP-STORE-20-reference-architecture_fig1_315838209, 2017.

[저자소개]

전 정 훈 (Gil-dong Hong)
2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월 ~ 현 동덕여자대학교 컴퓨터학과 교수
email : nerdrandy@dongduk.ac.kr