안드로이드 환경의 개인정보 보호를 위한 보안기법 분석

이대희*, 박석천**, 김용희***
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
***KCC정보통신 연구소 수석연구원
e-mail : daehei87@gmail.com

Analysis of Security Techniques for Privacy Information Protection in Android Environment

Dae-hee Lee*, Seok-Cheon Park**, Yong-Hee Kim***
*Dept. of Mobile Software, Gachon University
**Dept. of Computer Engineering, Gachon University(Corresponding Author)
***Principal Research Engineer, KCC Information & Communication

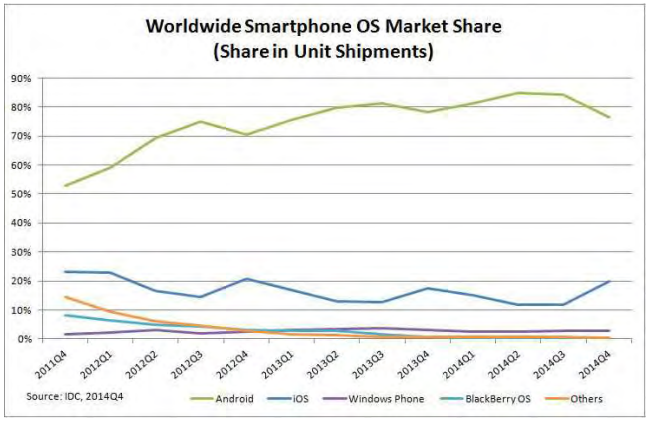
요 약

2014년을 기준으로 안드로이드 OS기반 태블릿이 전체 태블릿 시장의 67.4%를 차지하고 있고, 스마트폰은 약 80%에 육박하는 시장 점유율을 가지고 있으므로 스마트폰 사용자 5명 중 4명은 안드로이드 스마트폰을 사용한다. 스마트폰이 가진 편리성으로 인해 급속도로 확산되고 있는 스마트폰 중 특히 안드로이드 환경의 스마트폰의 보안 취약점을 이용한 보안사고가 꾸준히 증가하고 있다. 스마트폰에는 주소록, SMS, 위치 정보 등의 많은 개인정보들이 담겨 있는데, 스마트폰이 가지고 있는 다양한 종류의 보안 취약점을 이용하여 개인 정보를 갈취하고 악용하는 등의 악의적인 목적의 공격들이 끊임없이 발생하고 있다. 따라서 본 논문은 개인정보의 유출을 막기 위한 다양한 보안 기법에 대해 살펴보고자 한다.

1. 서론

스마트폰은 처음 시장에 등장한 이후 꾸준히 가파른 성장세를 보이며 성장하면서 현재에는 전 세계적으로 약 2억대가 넘는 디바이스들이 사용되고 있다. 다양한 OS별 스마트폰 시장 점유율은 (그림1)에서 그 비율을 확인할 수 있다. 안드로이드 OS기반의 스마트폰은 꾸준히 60%에서 많게는 80%까지 점유율을 차지하고 있고 압도적인 비율을 차지하고 있다는 것을 알 수 있다. 안드로이드 OS기반 스마트폰 사용자가 그만큼 증가하면서 오픈소스 기반인 안드로이드 스마트폰을 사용하는 사용자들의 개인정보 유출 및 그에 따른 피해가 증가하고 있다. 단적으로 알약 안드로이드 2014 하반기 스미싱 동향을 보면 2014년 한 해에만 24만건의 스미싱이 신고 되었고, 이는 알약 안드로이드에 접수된 것만 집계한 것으로, 실제 스미싱 공격은 더욱 큰 규모로 확대되어 여전히 스마트폰 사용자의 개인정보에 대한 보안을 위협하고 있는 것으로 보인다. 또한 안드로이드 환경의 모바일 단말의 보안을 위협하는 다른 공격 즉 플랫폼 공격, 네트워크 공격, 어플리케이션 공격, 단말기 공격 등의 다양한 공격을 추가하면 실제 안드로이드 환경의 스마트폰 사용자들의 개인정보 유출로 인한 피해는 심각한 수준인 것으로 예상된다[1~3].

따라서 다양한 공격에 대응하는 다양한 보안 기법들이 필요한 상태이고 점점 발전해가는 공격 방식에 유동적으로 대처할 수 있는 보안 기법이 필요한 실정이다. 이에 본 논문은 이러한 개인정보 유출을 통한 피해를 방지하기 위하여 현재 발생하고 있는 다양한 보안 위협들에 대처하기 위한 최근의 보안기법들에 대해 분석 하고자 한다.



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
Q4 2014	76.6%	19.7%	2.8%	0.4%	0.5%
Q4 2013	78.2%	17.5%	3.0%	0.6%	0.8%
Q4 2012	70.4%	20.9%	2.6%	3.2%	2.9%
Q4 2011	52.8%	23.0%	1.5%	8.1%	14.6%

Source: IDC, 2014 Q4

(그림 1) 세계 스마트폰 운영체제 시장 현황

2. 안드로이드 환경 공격 방식

2.1 공격대상에 의한 분류

공격대상에 의한 분류는 <표1>과 같이 플랫폼 공격, 어플리케이션 공격, 네트워크 공격 및 단말기 분실 등으로 인한 공격이 존재한다[4].

<표 1> 공격대상에 의한 분류

분류	공격내용	공격방법
플랫폼 공격	바이러스/웜	Wi-Fi/블루트스/Web 등 여러채널을 이용한 전파 및 PC동기화(Active Sync)전파 • 단말기UI변경, 단말기파손(오류발생) • 배터리소모, 자동프로그램 삭제 및 설치
	시스템Unlock	Rootin, SecurityOff(WM)플랫폼 취약점 이용 (API 취약점 이용)
	키보드해킹	Rookit 같은 프로그램 악용
어플리케이션 공격	Malicious 앱 Fishing 앱	Web 다운로드, PC 동기화를 통한 설치 • 개인정보(파일, 일정, 주소록, SMS, 통화내역, 메모, 위치정보 등) 유출 • 인터넷뱅킹, 소액결제 등의 금융거래 정보, 업무용 파일 등 기밀정보 유출 • SMS의 부정사용 및 스팸문자 발송 오과금 발생 • 단말기 사용불능 발생, 좀비단말기발생 • 휴대전화 소액결제 악용 • 무선인터넷이용 유료 전화 서비스 악용
네트워크 공격	Wi-Fi/무선 네트워크 도청/변조	Wi-Fi/블루투스 네트워크 공격으로 인한 단말기 통신 도청/변조
	DDOS공격	• 특정사이트, 특정단말기, AP 등에 트래픽 유발 DOS공격 • 스마트폰 채널을 통한 직접적인 이동통신망에 대한 DDOS공격
단말기 공격	단말기 도난/분실	도난 및 분실
	Malicious 앱	이동 저장매체 감염

2.2 공격목표에 의한 분류

공격목표에 의한 분류는 크게 3가지 정보유출, 오작동, 과금회피로 분류할 수 있으며 세세한 사항은 다음 <표2>와 같다[4].

<표 2> 공격목표에 의한 분류

분류	공격내용	공격방법
정보 유출	정보의 유출 (개인/업무/위치 /금융거래 등)	• Malicious/Fishing 앱을 통한 SMS, 휴대폰정보, 주소록, 사진, 위치정보 등 탈취 • 아이디도용, SNS 피싱, 결제도용, 계좌정보유출 • 분실도난 • 바이러스/웜 • PC/Wi-Fi 동기화
오작동	단말기 사용불능 단말기 전력소모 DDOS 공격 SMS 과금유도	• 멀티태스킹에 의한 리소스 부족 및 악성코드의 동작 • 지속적인 단말기 접속이나 리소스 사용으로 단말기 배터리 소모 • Malicious/Fishing 앱 이용으로 인한 DDOS 공격 및 오과금 등 발생 • 바이러스/웜 동작
과금 회피	컨텐트 무단복제	Rooting, SecurityOff(WM) 등의 악의적인 컨텐트 제공

3. 개인정보 보호를 위한 보안 기법 분석

3.1 권한 연산 모니터링을 통한 악성 행위 탐지 기법

특정 앱이 개인 정보 요청과 관련된 연산을 호출할 때 전송되는 바인더 IPC 메시지를 분석하여, 개인 정보의 흐름을 모니터링 한다. 또한, 해당 앱의 외부 네트워크 연결 상황을 로그로 저장한다. 사용자는 로그 분석을 통해 해당 앱의 악성 행위 여부를 파악할 수 있다. 이 기법을 통해 과도한 권한을 가진 앱이 실제로 해당 권한을 사용하는지, 아니면 필요 없는 과도한 권한 설정인지 파악할 수 있다. 또한 해당 앱의 기능에 필요 없음에도 불구하고 개인 정보에 접근 가능한 권한들이 선언된 경우 이 기법을 통해 실제로 개인 정보가 추출되어 외부 네트워크와 연결이 이루어지는지 파악할 수 있다. 이 기법의 처리시간 오버헤드는 약 14%로, 이는 보안을 강화하기 위해서 허용할 만한 수준이다.

3.2 개인정보 유출 탐지 및 난독화된 악성 앱 클러스터링 연구

3.2.1 개인정보 유출 탐지 앱

API 간 상호 의존성 정보를 기반으로 출력한 그래프

에서 개인정보 탈취 노드와 개인정보 유출 노드간의 최단 거리를 계산하는 방법을 적용하여, 개인정보 유출의 가능성을 지닌 앱에 대한 탐지 방법을 적용한 개인정보 유출 탐지 도구인 LeakDroid가 구현되었다. LeakDroid의 개인정보 유출 탐지 능력은 가족군을 형성하고 있는 156개의 악성 앱이 포함된 총 250개의 악성 앱과 써드 파티 마켓으로부터 무작위로 수집한 1700개의 일반 앱을 대상으로 실험을 진행하여 증명되었다. 실험 결과 악성 앱에서는 96.4%의 높은 탐지율을 보임을 확인할 수 있다. 일반 앱의 경우 LeakDroid가 탐지 한 93개 중 수동으로 분석한 결과 68개의 앱에서 개인정보 유출관련 의심흐름을 확인할 수 있다.

3.2.2 난독화된 악성 앱 클러스터링

바이오인포메틱스 분야에서 사용되는 기법 중 대표적인 기법인 서열 정렬 기법을 기반으로 악성 앱을 클러스터링 하고, 다양한 서열 정렬 기법 중 Smith-Waterman 알고리즘을 적용하여 유사도를 비교하는 방법으로 난독화된 악성 앱을 정확하게 구분했는지 확인하는 방식이다. 이 알고리즘을 적용하는 이유는 동일 가족군을 형성하는 악성 앱 이라고 할지라도 난독화 기법의 적용에 의해 악성 행위를 수행하는 특정 메서드의 길이가 서로 다를 수 있기 때문이다. 이 알고리즘의 경우 비교 대상이 되는 두 개의 시그니쳐가 서로 길이 또는 크기가 다를 경우에 이 두 개의 시그니쳐에서 공통부분을 찾는 것을 중점으로 수행하기 때문에 이 방식에서 얻고자 하는 결과에 가장 잘 부합한다.

시그니처를 추출할 대상 메서드를 선택하는 과정은 경험적 분석 방법의 비중이 크다. 그렇기 때문에 이를 자동화하였을 때 놓치는 악성 행위 패턴이 존재한다. 대표적인 패턴은 탈취한 개인정보를 변수에 담아 외부로 유출시키는 것이 아니라 안드로이드 내부 DB에 저장했다가 외부로 유출 시키거나 또는 원격지에서 특정 명령에 의해 악성 행위가 동작 할 때이다. 이와 같은 문제점을 해결하기 위하여 정적 분석에서의 정확한 데이터의 흐름을 파악할 수 있는 오염 분석 기법과 동적 분석에서의 특정 명령에 의한 이벤트를 탐지 및 추출할 수 있는 분석 기법들을 적절히 혼합하여 사용하는 연구를 지속해야 한다.

4. 결론

바이오인포메틱스 분야에서 사용되는 기법 중 대표적인 기법인 서열 정렬 기법을 기반으로 악성 앱을 클러스터링 하고, 다양한 서열 정렬 기법 중 Smith-Waterman 알고리즘을 적용하여 유사도를 비교하는 방법으로 난독화된 악성 앱을 정확하게 구분했는지 확인하는 방식이다. 이 알고리즘을 적용하는 이유는 동일 가족군을 형성하는 악성 앱 이라고 할지라도 난독화 기법의 적용에 의해 악성 행위를 수행하는 특정 메서드의 길이가 서로 다를 수 있기 때문이다. 이 알고리즘의 경우 비교 대상이 되는 두 개의 시그니쳐가 서로 길이 또는 크기가 다를 경우에 이 두 개의 시그니쳐에서 공통부분을 찾는 것을 중점으로 수행하기 때문에 이 방식에서 얻고자 하는 결과에 가장 잘 부합한다. 시그니처를 추출할 대상 메서드를 선택하는 과정은 경험적 분석 방법의 비중이 크다. 그렇기 때문에 이를 자동화하였을 때 놓치는 악성 행위 패턴이 존재한다. 대표적인 패턴은 탈취한 개인정보를 변수에 담아 외부로 유출시키는 것이 아니라 안드로이드 내부 DB에 저장했다가 외부로 유출 시키거나 또는 원격지에서 특정 명령에 의해 악성 행위가 동작 할 때이다. 이와 같은 문제점을 해결하기 위하여 정적 분석에서의 정확한 데이터의 흐름을 파악할 수 있는 오염 분석 기법과 동적 분석에서의 특정 명령에 의한 이벤트를 탐지 및 추출할 수 있는 분석 기법들을 적절히 혼합하여 사용하는 연구를 지속해야 한다.

사사의 글

본 연구는 2015년도 지식 경제부의 SW전문인력양성사업의 재원으로 정보통신산업진흥원의 고용계약형 SW석사과정 지원사업(H0116-15-1003)으로부터 지원받아 수행되었습니다.

참고문헌

[1] IDC, "Smartphone OS Market Share," 2014 Q4

[2] IDC, "Worldwide Quarterly Tablet Tracker," March 12, 2015

[3] 알약 블로그, http://blog.alyac.co.kr/226

[4] 문건환 "안드로이드 스마트폰 기반의 중요데이터 유출 방지를 위한 보안 메커니즘", 대전대학교 대학원, 2012

[5] 이환택 "안드로이드 권한 연산 모니터링을 통한 악성 행위 탐지 기법", 단국대학교 대학원, 2014

[6] 김도래 "안드로이드 애플리케이션의 개인정보 유출 탐지 및 난독화된 악성 앱 클러스터링 연구", 한양대학교 대학원, 2015