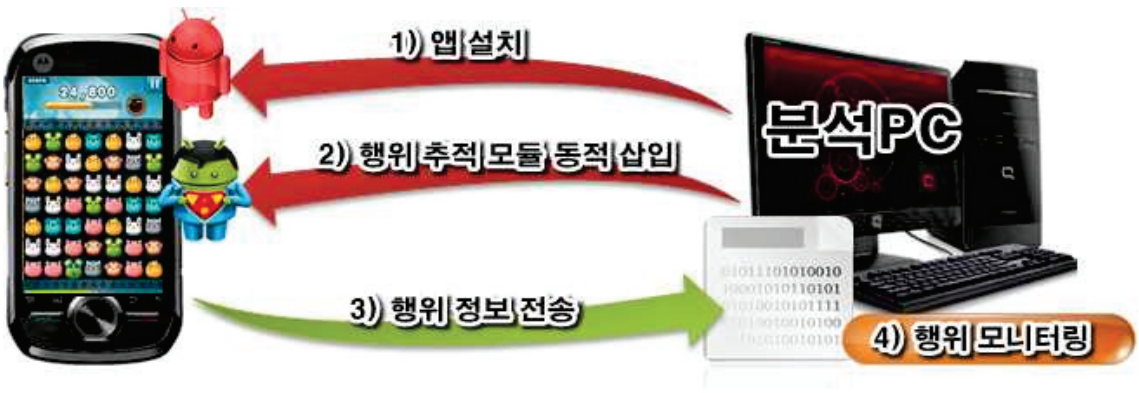
스마트폰 앱 행위 모니터링 기술

기술키워드	안드로이드, 비루팅, 행위 모니터링								
지식재산권	출원 1건(미국) / 등록 1건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	**시제품 신뢰성평가**	시제품 인증	상용품

기술개요

- 스마트폰 앱 행위 모니터링 기술
  - 루팅되지 않은 일반 스마트폰에 앱을 실행시켜 해당 앱의 행위를 실시간 추적 및 GUI를 통한 모니터링
  - 앱 실행 시 동적으로 DEX를 로딩하는 행위를 추적 및 대응하며, 자바 리플렉션 등 행위 모니터링 방해 기술에 대응
  - 앱 모니터링 결과를 함수 단위로 그룹화하여 의미 분석
- 앱의 데이터 추적 기술
  - 앱이 실행하며 사용하는 함수 인자, 타입, 이름, 데이터 등을 자동으로 추적
  - 실시간으로 앱에서 생성한 파일을 추출하여 획득 가능
- 기술 구성도



기술성

- 기존 모니터링 기술은 안드로이드 펌웨어를 수정하거나 루팅을 해야하며, API가 아닌 개발자가 개발한 함수는 모니터링이 불가능하나 본 기술은 일반 스마트폰에서 루팅없이 모든 API 및 개발자 함수도 모니터링 가능
- 기존에는 모니터링 기술을 만든 개발자가 정해놓은 함수와 데이터 만 추적 가능했으나 본 기술은 분석가가 원하는 함수와 모든 데이터를 추적 가능
- 특히 본 기술은 안드로이드의 Native 단의 행위 및 외부 서비스와의 연동 모두 추적 가능

기능		Scalpel	DroidBox	Anubis
행위 모니터링	플랫폼 변경	불필요	필요	필요
	앱 코드 수정	불필요		
안드로이드 API 추적		O	O	O
데이터 객체 추적		O		
Native 코드 추적		O		O
사용자 정의 메소드 추적		O		
선택적 행위 분석		O		

시장성

- 안드로이드 앱 정적 분석 도구인 JEB(PNF Software)는 $1,000에 팔리고 있으며 국내 앱 분석하는 대부분의 사람이 사용하고 있음
  · PC 정적 도구인 IDA 와 유사하여 선도적인 기술이 시장을 장악
- PC의 행위 모니터링 도구인 GFI Sandbox, Norman Sandbox는 수천만 원을 넘고 있으며, 모바일에서의 행위 모니터링 도구는 아직 제품화되어 판매되지 않고 있음
- 모바일 악성코드 전용 분석 도구 확보로 모바일 분석 도구 시장 선점 필요
  · 모바일 환경에 맞는 특화된 기능(앱과 Native 모듈 연동, 코드 은닉 대응 등)으로 공개 분석 도구 대비 경쟁력 확보

기술 응용 분야

- 기본 API뿐만 아니라 앱 개발자에 의해 개발된 함수를 모니터링하여 앱의 모든 행위 분석
- OS와 앱 코드 수정 없이 앱의 내부 정보 추출 및 조작

관련 특허 등 지식재산권

- (등록) 10-1666176(2016. 10. 7. 대한민국) "안드로이드 플랫폼 기반의 어플리케이션 모니터링 장치 및 방법"
- (출원) 14/939507(2015. 11. 12. 미국) "안드로이드 플랫폼 기반의 어플리케이션 모니터링 장치 및 방법"