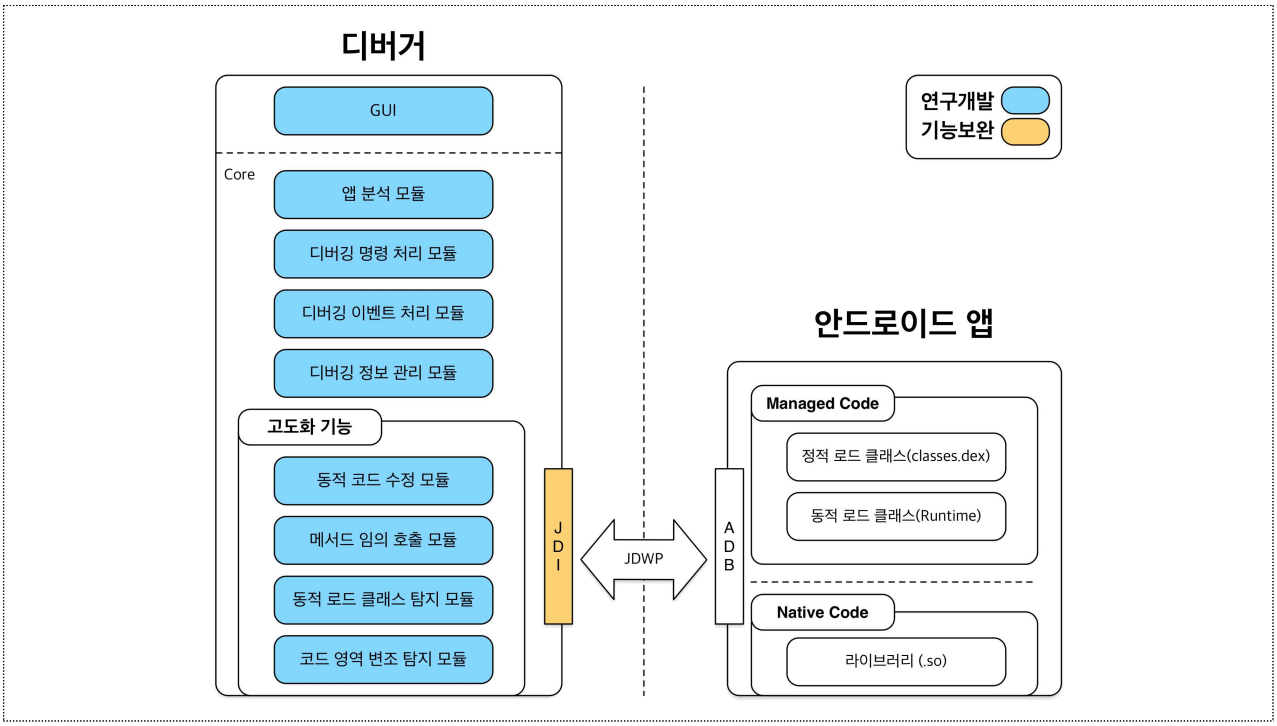
안드로이드 앱 역공학 관점 디버깅 기술

기술키워드	모바일 악성코드, 모바일 보안, 안드로이드 앱 역공학								
지식재산권	등록 1건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	**시제품 신뢰성평가**	시제품 인증	상용품

기술개요

- 안드로이드 앱을 실시간으로 역공학 관점에서 디버깅하기 위한 기술
  - 정적으로 추출한 실행코드가 아닌 실제 메모리상의 실행 코드를 디버깅하기 위한 기술로, 디버깅을 위한 안드로이드 실행 파일 해석 기술, 앱 디버깅 전처리 자동화 기술, 메모리상의 동적 변화를 실시간 반영 기술을 개발하여 고도화된 모바일 악성코드에 대응 가능한 기술임
- 기술 구성도



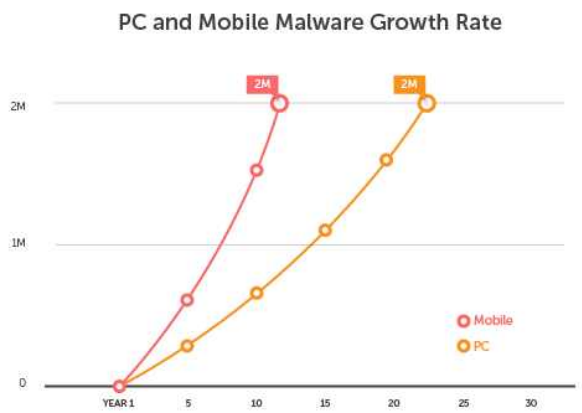
기술성

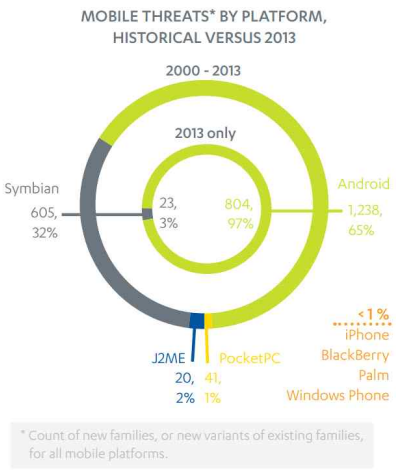
- 현재 시장에 나와 있는 디버깅 기술은 정적으로 추출한 실행 코드를 디버깅에 활용하는 수준으로 동적으로 코드가 변경되는 악성코드에 대응 할 수 없음
- 본 기술은 실제로 실행되고 있는 실행 파일을 디버깅하여 메모리상의 변화를 탐지하여 반영하거나 분석가가 임의로 코드를 수정하는 등 현재 안드로이드 앱 디버깅을 위해 차용하고 있는 자바 디버거의 한계를 극복함

기능	DABiD	Smali-Debugging	IDAPro
디버깅을 위한 전처리 및 설정 자동화	O		
정적으로 추출한 DEX 디버깅	O	O	O
메모리에서 추출한 DEX 디버깅	O		
동적 코드 변화 탐지 (자가변조, 동적로딩)	O		
동적 코드 수정	O		

시장성

- TrendMicro의 조사에 따르면 모바일 악성코드의 증가 속도는 PC 악성코드 증가 속도의 2배 이상으로 앞으로도 모바일 환경을 타겟으로 한 악성코드가 더욱 증가 할 것으로 예상됨
- 모바일 악성코드의 대부분은 안드로이드 악성코드로 2013년에는 97%의 모바일 악성코드가 안드로이드 플랫폼을 타겟으로 하고 있음
- 모바일 분야는 악성코드의 증가 속도 및 그로 인한 피해에 비하여 역공학을 위한 전용 분석 도구가 부족한 상황이며 따라서 전용 분석 도구의 수요가 높은 것으로 추정됨





기술 응용 분야

- 백신업체 등 모바일 악성코드에 의한 사고 시 대응이 필요한 업체에서 앱 정밀 분석에 활용 가능
- 국가·공공기관, 군 등 모바일 앱 배포 기관에서 배포 전 앱 정밀 검사 시 활용 가능
- 통신사 등 앱 마켓 운영 주체에서 배포 전 앱 정밀 검사 시 활용 가능

관련 특허 등 지식재산권

- (등록) 10-1724412(2017. 4. 3. 대한민국) "확장 코드를 이용한 어플리케이션 분석 장치 및 방법"