

모바일 금융거래 애플리케이션의 보안대책 우회 기법

2014년 9월 4일

에이쓰리시큐리티 보안기술팀

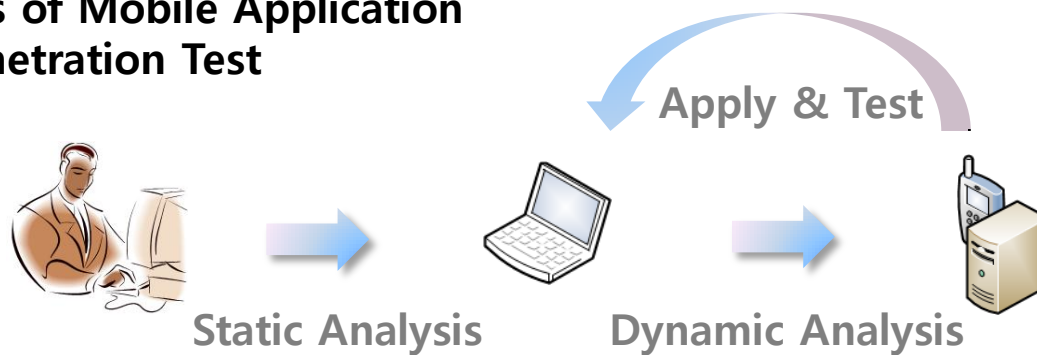
정대근 팀장

1. 모바일 애플리케이션 분석 방법

모바일 애플리케이션과 관련된 분석 방법은 크게 정적 분석 및 동적 분석으로 분류 가능

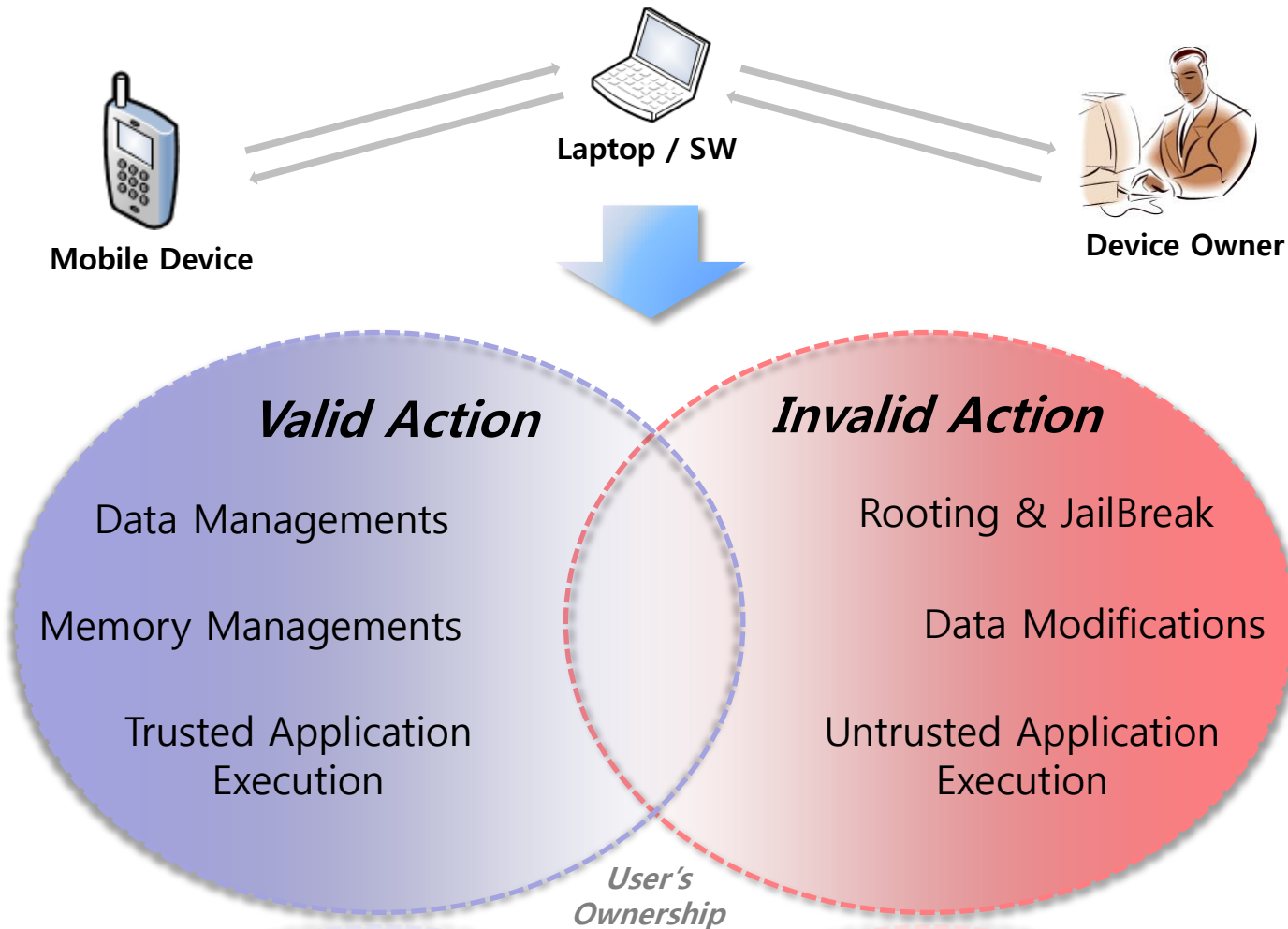
Static Analysis	Dynamic Analysis
Decompile	Function Hooking
Disassembly	Network Data Modification
Binary Patch	Memory Contents Modification
Resource Modification	Decrypting of the Encrypted Data

* The Process of Mobile Application Penetration Test



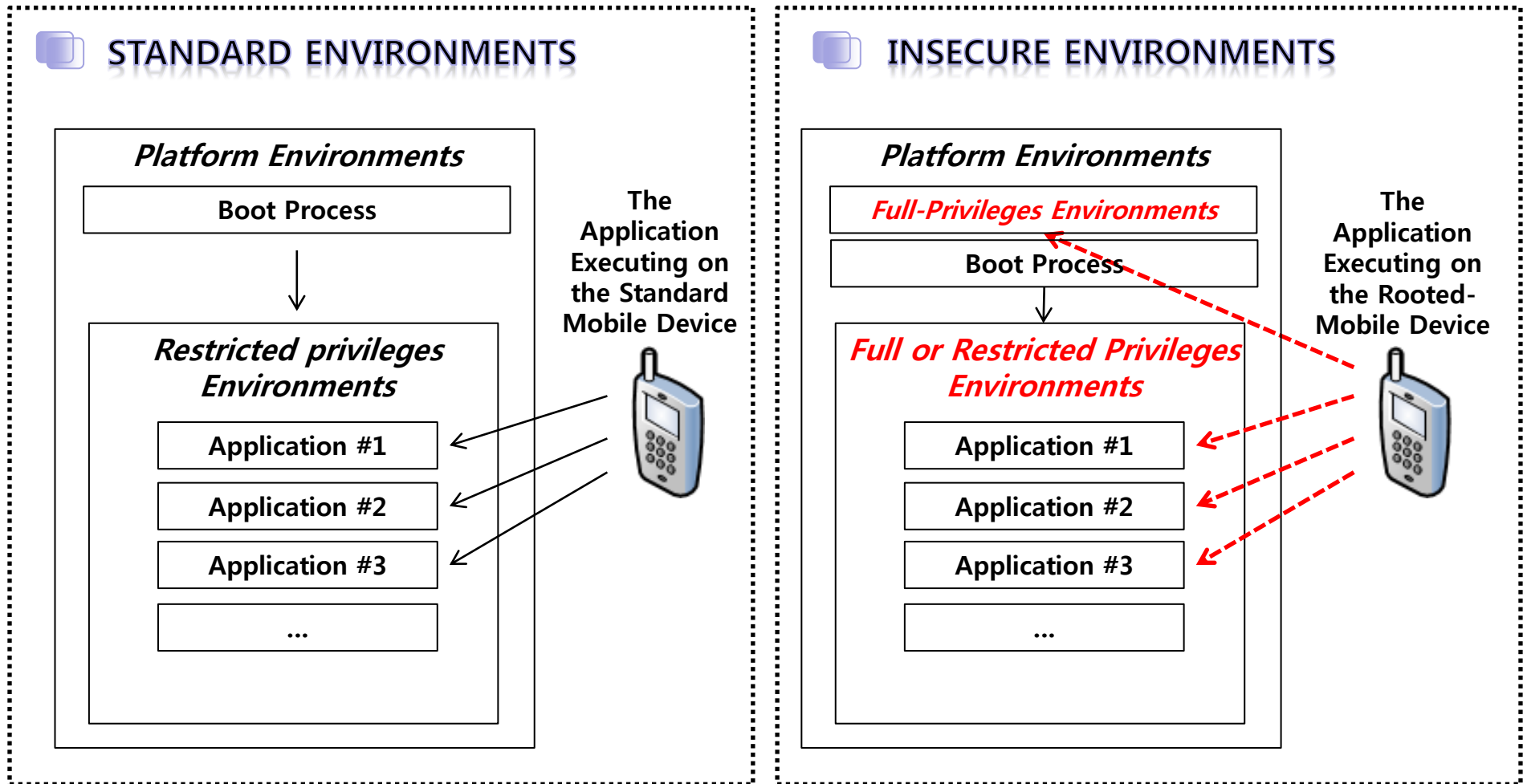
2. 모바일 애플리케이션 동작 환경

모바일 애플리케이션이 동작하는 디바이스는 사용자가 언제든지 조작 및 변경 가능한 환경



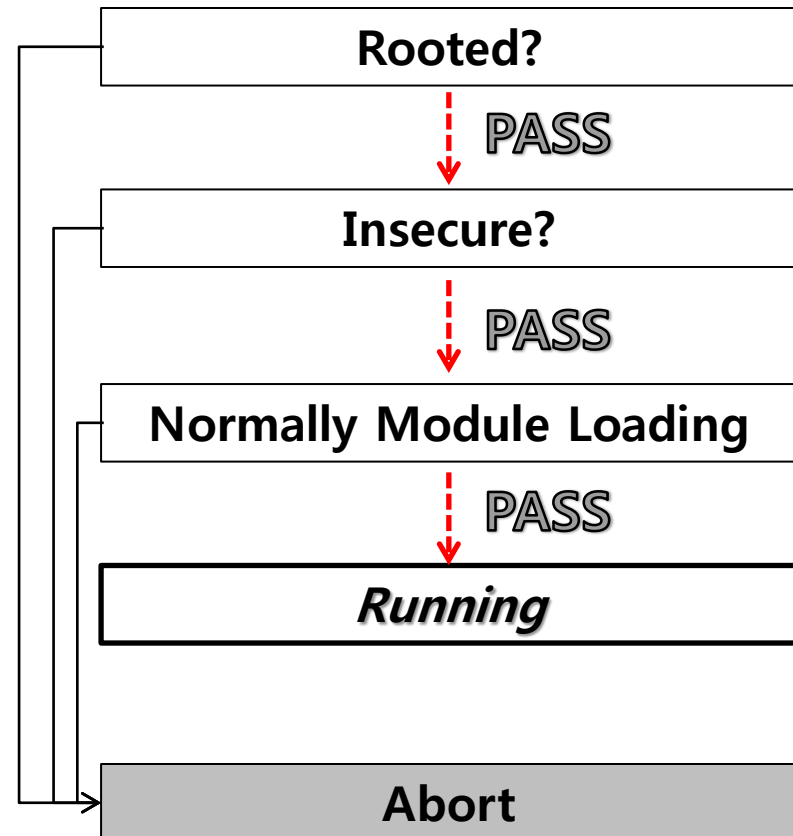
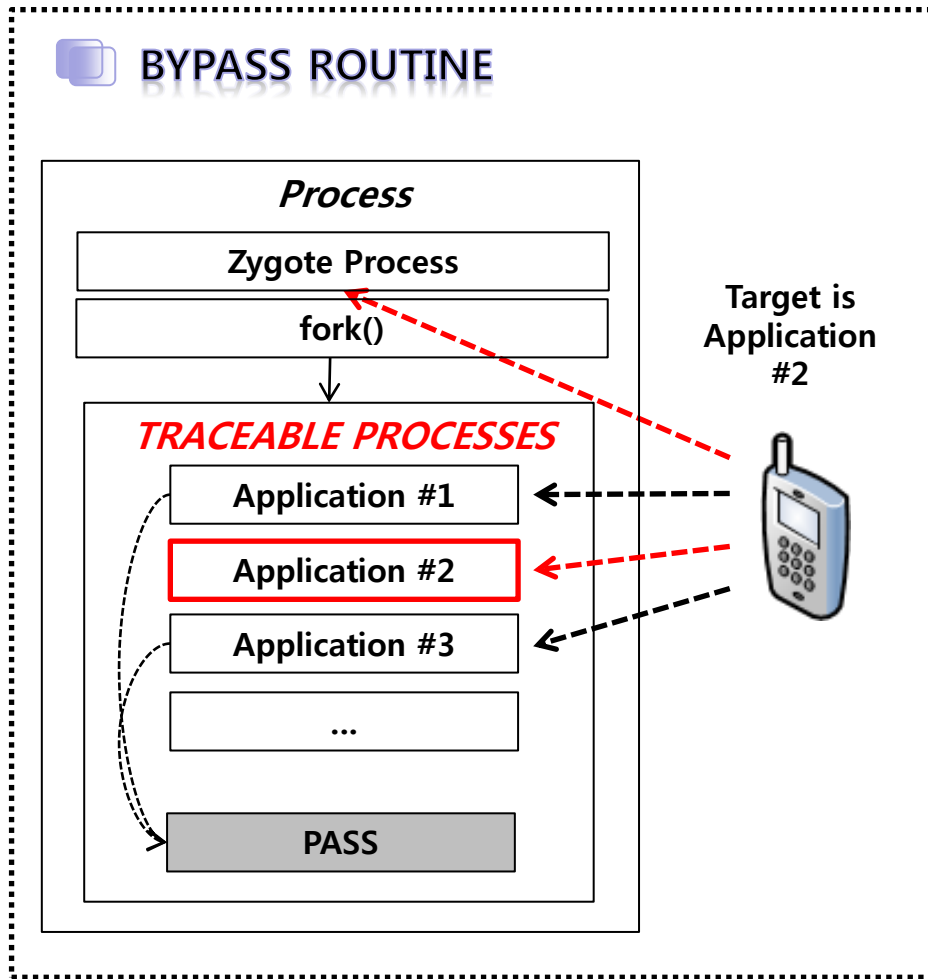
3. 안전하지 않은 모바일 애플리케이션 동작 환경

디바이스 사용자의 의도에 따라 동작 환경이 달라지며 보안 위협에 노출될 가능성 존재



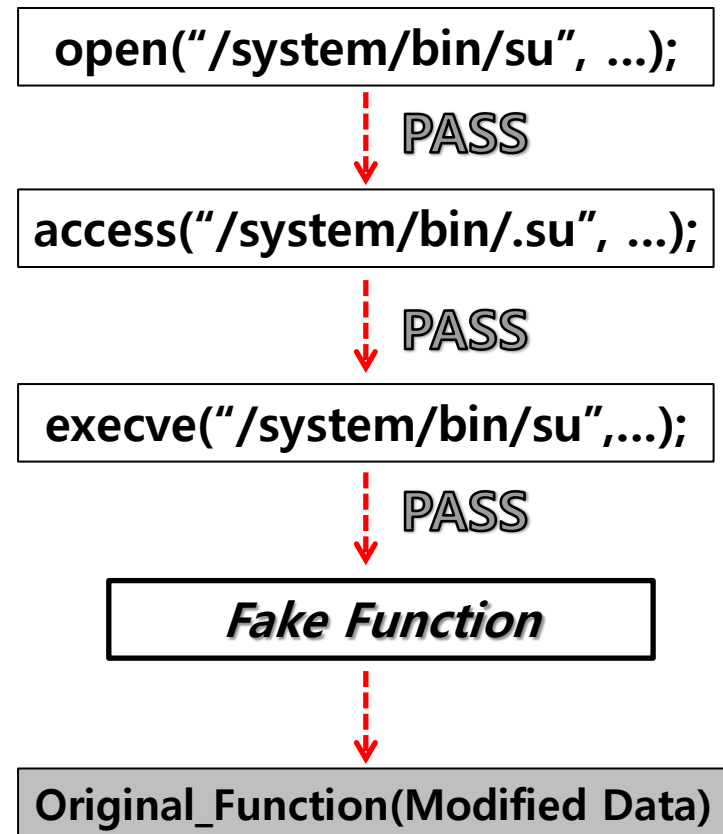
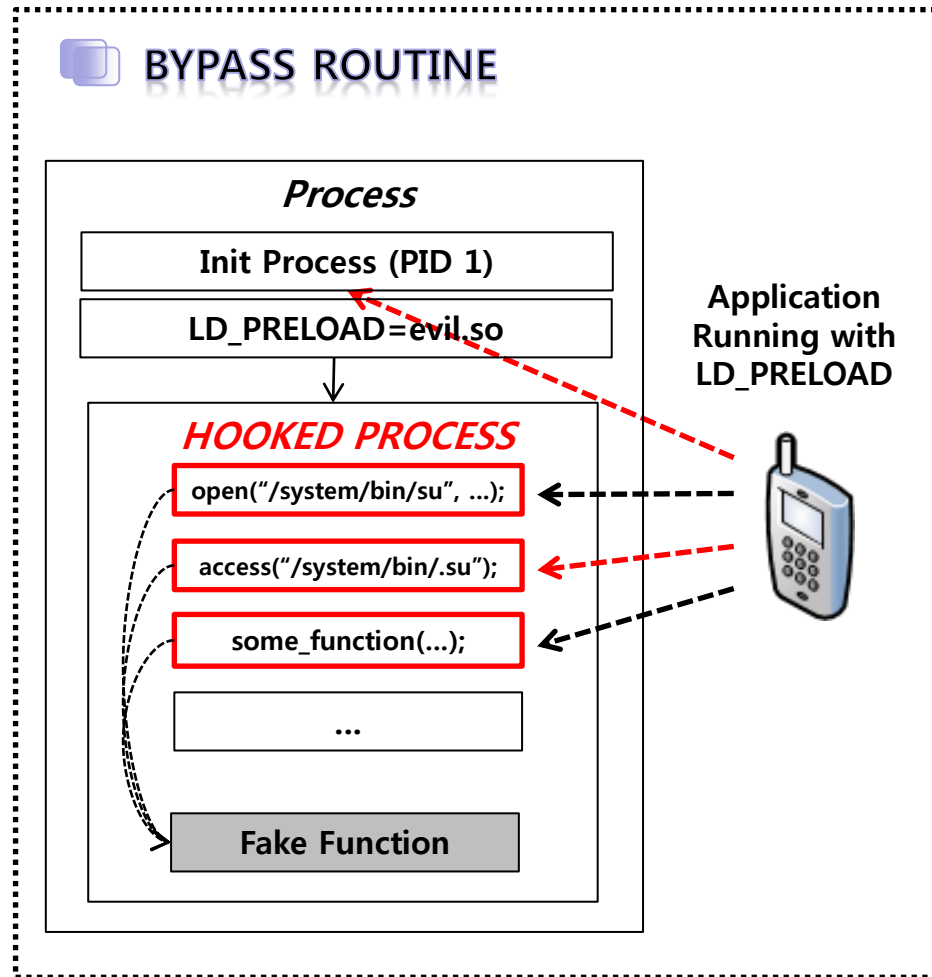
4. 임의의 시스템 콜을 사용한 모바일 앱 실행 플로우 변조

Zygote 프로세스의 저 수준(Low-Level) 시스템 콜을 탐지하며 특정 프로그램 실행 흐름을 변조



5. 임의의 함수 후킹을 통한 모바일 앱 실행 플로우 변조

우선순위를 가지는 모듈을 적재하여 특정 함수의 실행 흐름 변조





6. 시연

시연

7. 모바일 애플리케이션 보안의 현 주소

금융거래 애플리케이션을 포함한 많은 모바일 애플리케이션들이 보안 위협에 노출

금융거래 모바일 애플리케이션 보안 대책 항목	우회 및 무력화 가능 여부
모바일 애플리케이션 위/변조 방지	우회 가능
모바일 디바이스 위/변조 방지	우회 가능
종단간 통신 데이터 암호화	복호화 가능
민감한 사용자 입력 정보 보호	입력정보 보호 무력화 가능
모바일 백신 적용	백신 무력화 가능
난독화 및 패킹 등의 코드모듈 보호	무력화 가능
모바일 디바이스에 저장되는 데이터 등의 암호화	복호화 가능

-  개인 프라이버시 침해의 가능성이 있는 데이터 뿐만이 아니라 금융거래 정보도 보안 위협에 노출
-  민감한 정보 유출 시, 범죄에 악용될 가능성 및 피해 확산

감사합니다