모바일 앱과 클라우드 서비스 연동에서 발생하는 보안 취약점 2

BCG 장건희

02/28

목차

- 하드코딩
- 어플리케이션 해킹 유형
    - ios생태계에서의 방법
- 앱 패키지 분석으로 기술적 정보 파악하기
- 크리덴셜 정보 관리
- 모니터링 비용 감축의 위험성

참조

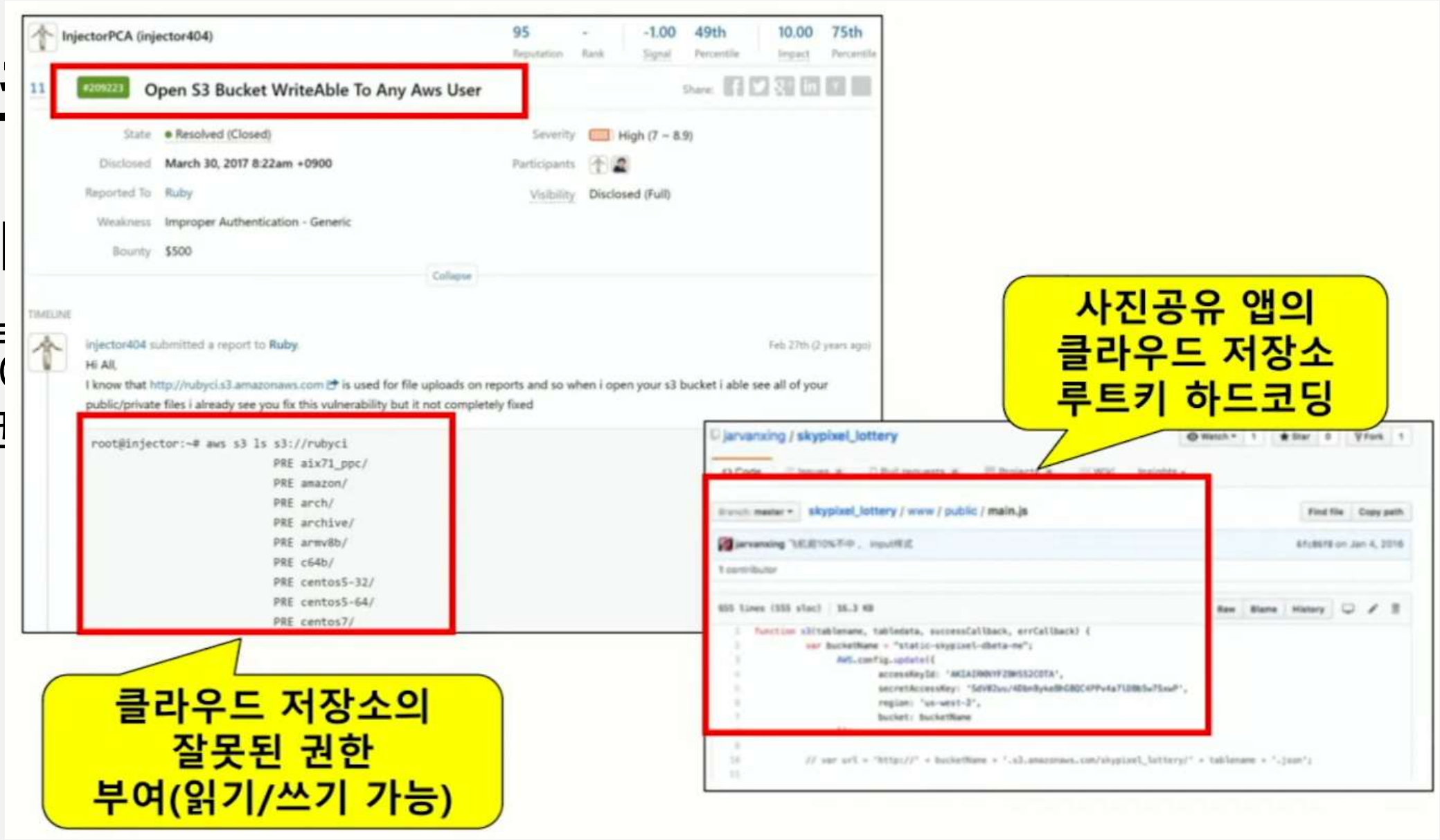
- NHN Cloud On 웨비나 10 | 모바일 해킹에 대응하는 강력한 앱 보안 솔루션 https://youtu.be/69vFnVR3Nu0?si=Jc-WjIAXeQynbJDy
- 2020 공개SW 페스티벌 Track1_Session7 "모바일 앱의 클라우드 보안취약점과 대응방안" 박현준(네이버) https://youtu.be/gS6ErctP8hQ?si=ZBpqwcdq-2v490ev
- Zimperium(짐페리움) 모바일 앱 보호와 소스코드 난독화 https://youtu.be/VM2bbfVccRg?si=t1yXcFhHsVacZ7su
- 모바일 취약점 진단을 할 때 꼭 봐야 할 가이드 (영상 자막) https://youtu.be/LmsSDylsPN8?si=0f3nlDZOazp4CZK9

하드코딩

- 상수나 변수에 들어가는 값을 소스코드에 직접 쓰는 방식
- 모바일 앱 실행 시 사용자에게 받을정보를 소스코드에 입력하거나 변수, 아이디, 비밀번호, 대칭키 등 중요 정보를 주석 처리하는 것도 하드코딩.

하드

- 상수니
- 모바일
  변수, (
  하드코



정적분석

- 소프트웨어를 실행할 필요가 없음
- 소스코드를 분석

- 언패키징 - 분석 - 리패키징 과정을 거침

동적분석

- 디버깅
- 실제 프로그램을 분석

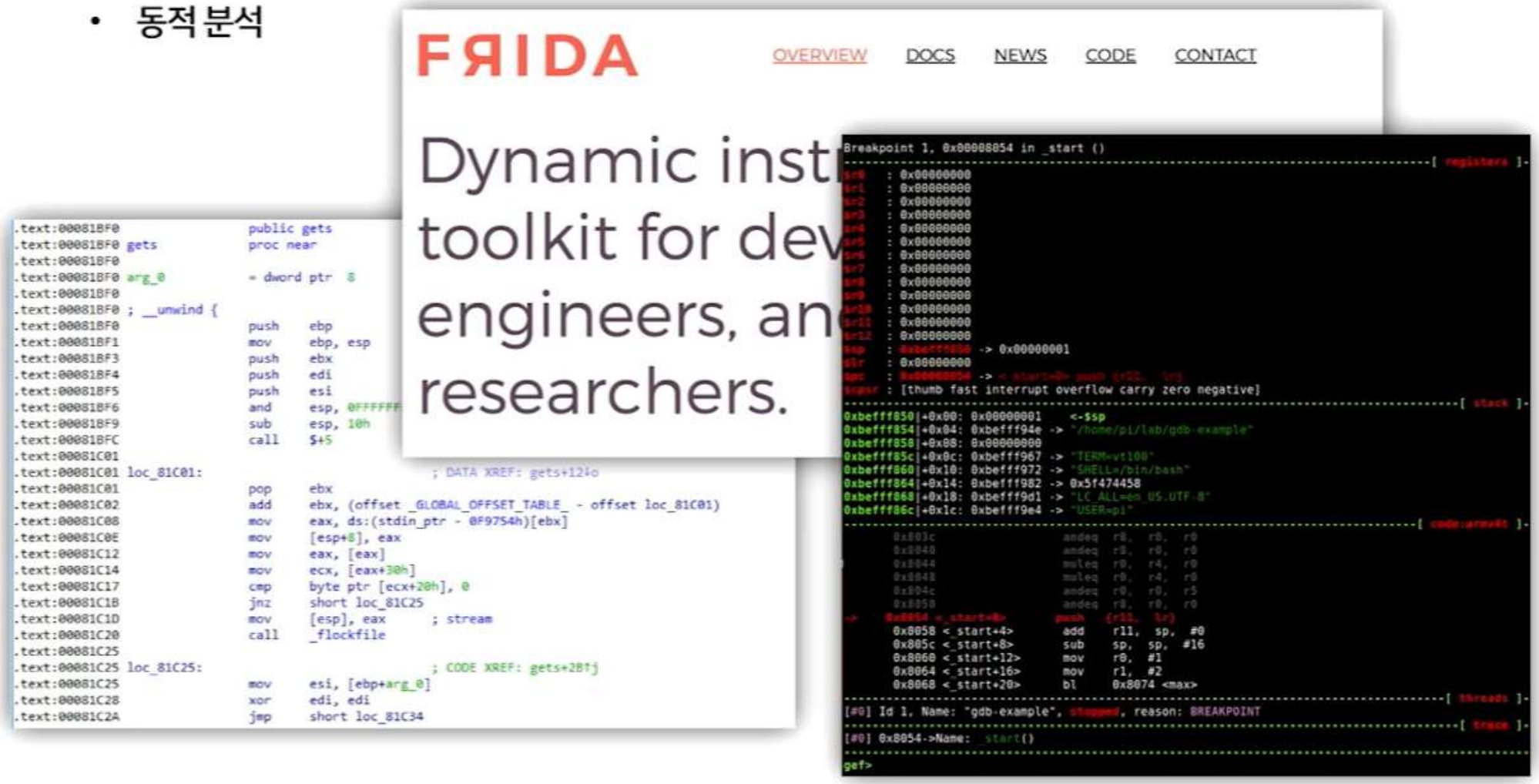
- 스트레스 테스트
- 모의 해킹
- 리버스 엔지니어링

동

- 소

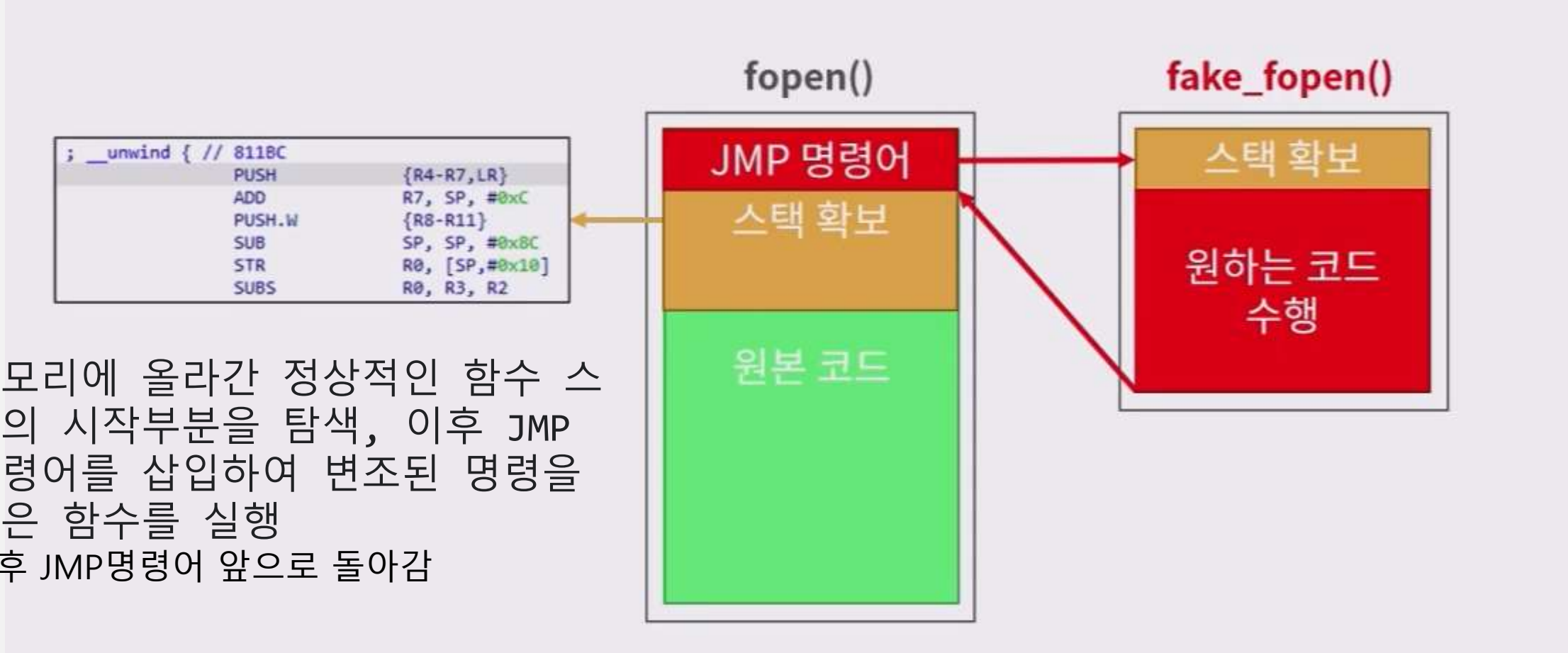
- **두 가지 분석 방법**
  - 정적 분석
  - 동적 분석

Frida(Dynamic Binary Instrumentation)동적 바이너리 계측 도구



동적 분석 원리 - 인라인 후킹

- 후킹 : 갈고리로 가로채는 이미지



메모리에 올라간 정상적인 함수 스택의 시작부분을 탐색, 이후 JMP 명령어를 삽입하여 변조된 명령을 담은 함수를 실행
이후 JMP명령어 앞으로 돌아감

iOS 생태계 유형1 - 탈옥

ios - tweak

Tweak : 비틀다

Cydia 라고 하는 탈옥 앱스토어 에서 설치,

정상 프로그램 실행시 메모리에 tweak을 삽입하여 메모리 어뷰징등의 허가되지 않은 동작을 실행

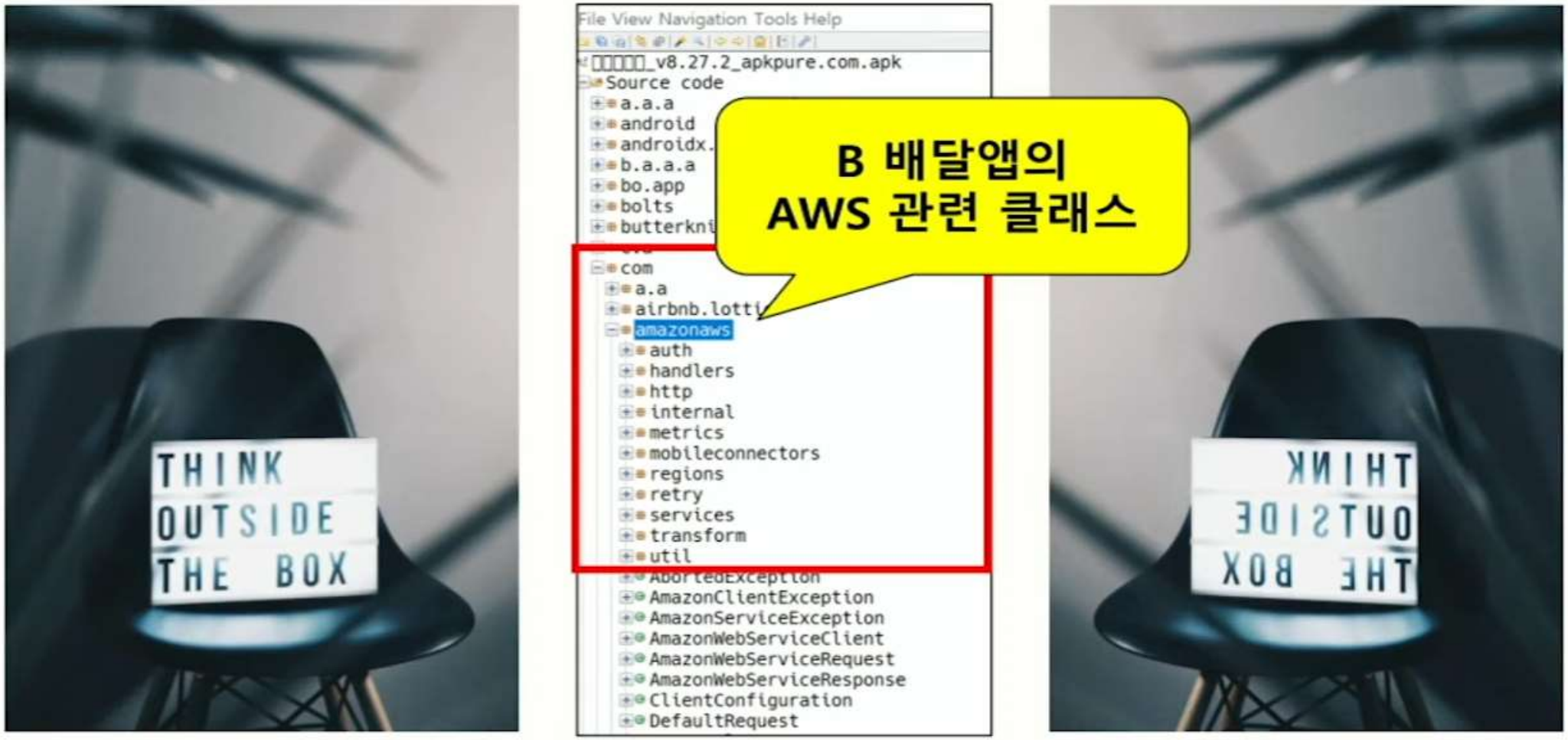
iOS 생태계 유형 2 - 앱 위변조

모바일 앱 분석

- Back-End 아키텍쳐 구성
  - 내장된 클라우드 SDK를 통해 서비스를 호출(REST API)
  - 사용자인증에 Credential (Access/Secret Key) 필요

모

- B



- 클라우드 SDK가 포함된 앱 : 클라우드 back-end 서비스가 연동
- 앱에서 클라우드 서비스 접근 시 Credential 정보를 사용

☞ **Credential을 훔칠 수 있다면 클라우드 자원에 접근 가능**

https://www.oss.kr/festival_speakers/show/b2b930df-7827-470b-acf2-9e9755cc7994

모니터링 비용 절감의 위험성

- 소규모 서비스일때는 큰문제가 없지만 서비스가 커지면서 모니터링 비용이 커질수가 있음.
- 대략적으로 중-대 규모의 서비스에서 월간 발생하는 로그 저장비용, 로그 수집비용, 모니터링 서비스 사용료등을 합치면 $500 - $2,000 정도의 비용이 나감.
- 하지만 기술장애나 보안 사고시에 기록이 없으면 사건 규명도 하지 못하므로 로그 저장비용을 절약하는 행위를 지양할 필요가 있음.

* AWS CloudWatch, Azure Monitor, Google Cloud Monitoring 등의 기본 적인 로그 서비스

보안을 생각하는 클라우드 사용

클라우드 키에 대한 적절한 권한 통제
  루트키 사용 금지
  키 하드코딩 금지

- 클라우드 보안에 대한 비용 투자
  로깅 + 모니터링

- 내부 토론, 보안 컨설팅을 통한 리스크 관리
  버그바운티 프로그램 참여