안드로이드 악성앱 정적 분석기

윤용호
서울대학교 프로그래밍연구실

악성앱

- 다양한 악성앱들이 쏟아지지만 뚜렷한 해결책이 없음
- 기존의 연구는
  - 케이스 스터디 수준이거나
  - 알려진 악성 코드의 지문 검출 방식이거나
  - 개인정보 누출 분석에만 치중

악성 행동들*

- 유저 몰래 루트 권한 획득(Exploit)
- 개인정보 누출
- 수신한 SMS 훔치기 / 사용자 몰래 SMS 발신하기
- 좀비폰으로 만들어 다른 공격에 활용하기(Botnet)

악성 행동

숨기기

- 진짜 악성 행동을 하는 다른 앱을 설치하도록 유도
- 앱간 통신을 이용한 개인정보 누출
  - 앱1에서 개인정보를 꺼내고 앱2로 보낸 후 앱 2에서 내보냄
- 문자열 연산을 적극적으로 활용
  - AES/DES 암호화 및 reflection

DroidKungFu1: 28176bc34e54e087e90bbbaba0c846ec9182db17

```
class com.google.ssearch.SearchService {
  getPermission1() {
    s = "/gjsvro";
    fname = "/data/data/" + packageName + s;
    Utils.copyAssets(ctx, s, fname);

    cmd = "/system/bin/chmod";
    arg = "4755 " + fname;
    Utils.oldrun(cmd, arg);

    cmd2 = fname + " /data/data/" + packageName;
    Utils.oldrun(cmd2, "");
  }
}
```

*Plankton: 202252e3767456e95b27d0476ae29bcc11253c1e

```
class SMSBroadcastReceiver extends BroadcastReceiver {
  onReceive(ctx, intent) {
    …
    arr = (Object[]) intent.getExtras().get("pdus");
    marr = new SmsMessage[arr.length];
    for(i=0;i<arr.length;i++) {
      buf = (byte[])arr[i];
      msg = SmsMessage.createFromPdu(buf);
      marr[i] = msg;
    }
    s = marr[0].getMessageBody();
    s2 = SharedPreference.getString
         ("sms_keyword", "Bring me back my droid");
    if(!s.equalsIgnoreCase(s2)) return;
    abortBroadcast();
    …
  }
}
```

*Yajin Zhou, and Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution", Proceedings of the 33rd IEEE Symposium on Security and Privacy (Oakland 2012)

ScanDal

- 앱 개인정보 누출 분석기
- 개인정보 누출만 분석하기엔 좀 아쉬움
  - 의미 분석을 꽤 깊이 하기 때문에
- 조금씩 고쳐서 다른 분석에도 유용하게 사용할 수 있을 것 같음
- 코드를 정리 및 공개 하고 싶음

코드 재정비

- 파싱 및 번역 결과물을 쉽게 가져다 쓸 수 있도록
- 다양한 도메인을 구현해서 쉽게 적용할 수 있도록
- 다양한 분석 스펙을 쉽게 조절해볼 수 있도록
  - Context Sensitivity, Widening, 스파스 분석, etc.
- 분석 결과를 보기 쉽도록
- …

방향

목표

- 새로운 분석을 만들 때 손쉽게 만들어볼 수 있는 프레임워크
- 안드로이드 앱 분석에 새로 뛰어드는 동료가 쉽게 알아볼 수 있고 활용할 수 있는 코드 제공
- SOOT처럼 다양하게 활용되는 것이 꿈

안드로이드 악성앱 정적분석기

- 정비된 정적 분석 프레임워크 코드 구현과
- 실행의미 기반 악성앱 검출 분석 구현
- … 을 진행중입니다.
- 곧 코드 오픈 됩니다

Coming Soon!

Programming Research Laboratory
Seoul National University
ROSAEC center
Research On Software Analysis for Error-free Computing
소프트웨어 무결점 연구센터 NRF ERC