Zraniteľnosti a forenzná analýza smartfónov na platforme Android.

JÁN PARASKA

DOC. RNDR. JOZEF JIRÁSEK, PHD.

ÚINF

Motivácia

- Android – najrozšírenejšia mobilná platforma (88%)
- Veľké množstvo osobných údajov (SMS, e-mial, heslá, ...)
- Vysoká konektivita (Wi-Fi, 3G, 4G, ...)
- Malá miera bezpečnosti
  - Vysoký počet aplikácií (2.8 mil)
    - Automatická kontrola (Bouncer – kontroluje škodlivosť aplikácií, nekontroluje využiteľné slabiny)
    - Kontrola oprávnení ponechaná na zákazníka
      - 70% Aplikácií žiada oprávnenia nesúvisiace s činnosťou
      - 97% Užívateľov nedbá na žiadané oprávnenia
  - Open source

Bezpečnostné problémy a nedostatky

- Eskalácia oprávnení
  - Často sú využité verejne známe medzery v implementácii Androidu
  - Prístup k zdrojom, ktoré sú za bežných okolností chránené pred aplikáciami aj užívateľom
- „Prebaľovanie“ aplikácií
  - Rozbalenie súboru *.apk* legitímnej aplikácie (napr. pomocou ApkTool)
  - Vloženie škodlivého kódu
  - Zabalenie aplikácie (napr. pomocou ApkTool) a podpísanie pomocou *jarsigner*
    - Gemini, KungFu
- DoS – nadmerná záťaž CPU, pamäte, siete, batérie, ...
- „Colluding“ – zdieľanie oprávnení

Súčasný stav

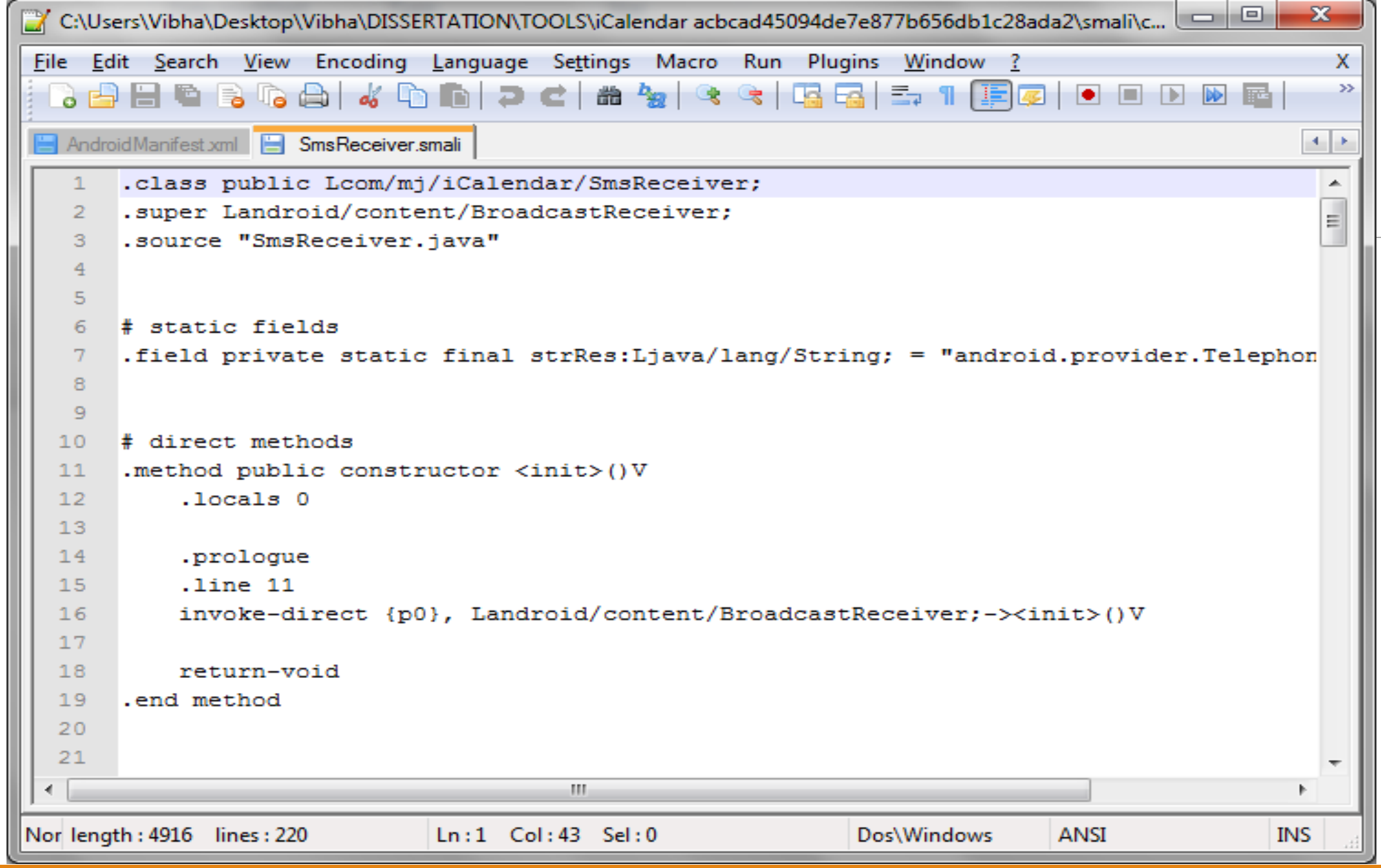
- Statická analýza
  - Podpis – porovnávanie vzorov v aplikácii oproti slovníku známych malvérov
  - Povolenia – hodnotenie rizík žiadaných oprávnení
  - „Control Flow“
    - AndroSimilar, RiskRanker, Kirin
- Dynamická analýza - analýza správania sa aplikácie počas behu
  - RecDroid, FireDroid, MockDroid, AppGuard
- „Crowdsourcing“ – analýza spätnej väzby od používateľov
  - CrowDroid, RickMoon

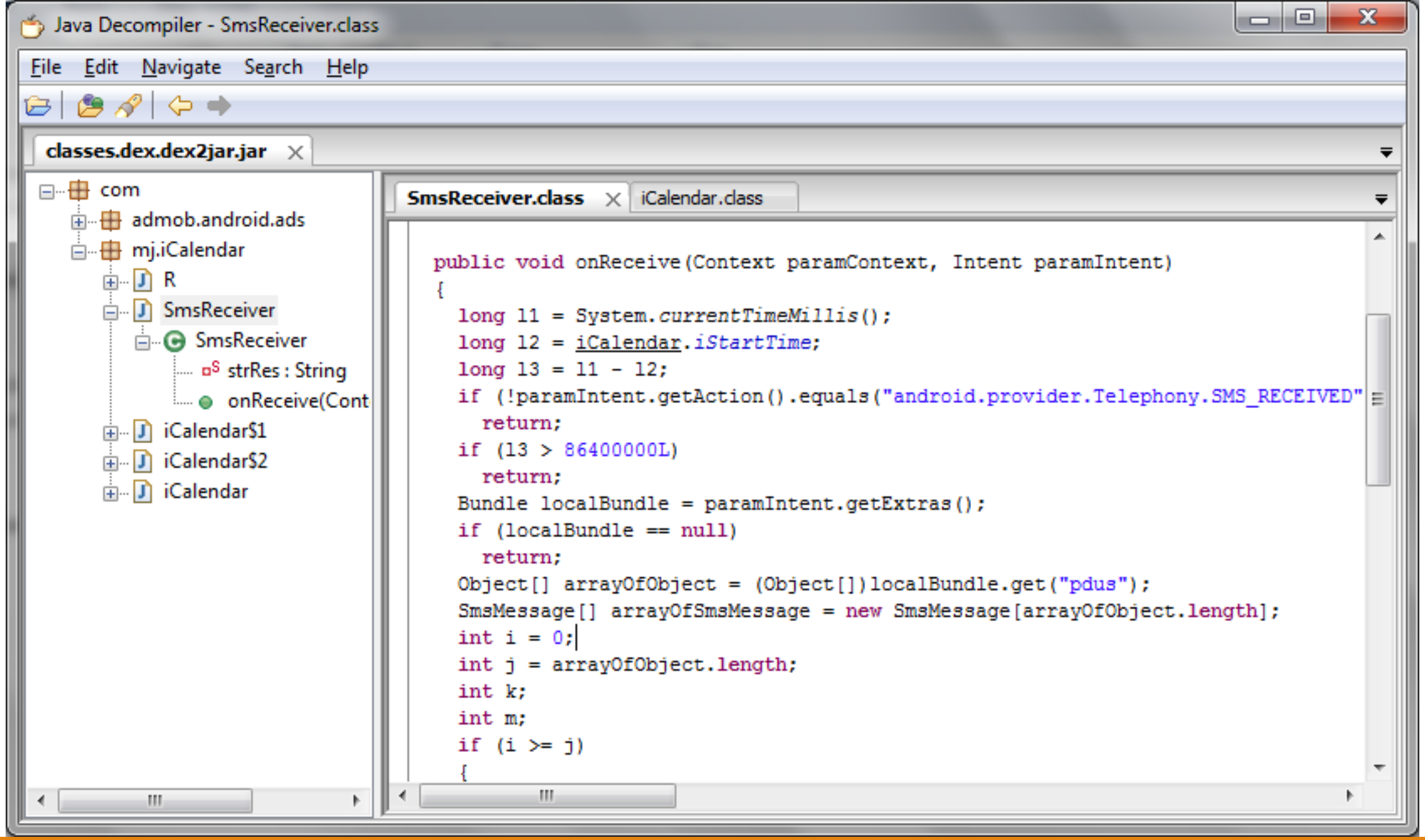
Ciele?

- Analýza známych útokov na implementácie systému Anadroid
- Klasifikácia a charakteristika zraniteľnosti smartfónov na platforme Android
- Možnosti a postupy forenznej analýzy smartfónov na tejto platforme?

Analýza malvéru

- ApkTool
  - XML definujúce rozloženia, atribúty, ...
  - Android Manifest File
  - Zdrojový kód vo formáte .smali (dá so otvoriť v NotePad++)
- Dex2Jar
  - Pracuje so súbormi vo formáte .dex (Dalvik Executable)
  - classes.dex.dex2jar.jar
  - Súbor .jar sa dá otvoriť pomocou JD-GUI


C:\Users\Vibha\Desktop\Vibha\DISSERTATION\TOOLS\iCalendar acbcad45094de7e877b656db1c28ada2\smali\c...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
AndroidManifest.xml
SmsReceiver.smali
1 .class public Lcom/mj/iCalendar/SmsReceiver;
2 .super Landroid/content/BroadcastReceiver;
3 .source "SmsReceiver.java"
4
5
6 # static fields
7 .field private static final strRes:Ljava/lang/String; = "android.provider.Telephon
8
9
10 # direct methods
11 .method public constructor <init>()V
12 .locals 0
13
14 .prologue
15 .line 11
16 invoke-direct {p0}, Landroid/content/BroadcastReceiver;-><init>()V
17
18 return-void
19 .end method
20
21
Nor length : 4916 lines : 220
Ln : 1 Col : 43 Sel : 0
Dos\Windows
ANSI
INS


Java Decompiler - SmsReceiver.class
File Edit Navigate Search Help
classes.dex.dex2jar.jar
com
admob.android.ads
mj.iCalendar
R
SmsReceiver
SmsReceiver
strRes : String
onReceive(Cont
iCalendar$1
iCalendar$2
iCalendar
SmsReceiver.class
iCalendar.class
public void onReceive(Context paramContext, Intent paramIntent)
{
long l1 = System.currentTimeMillis();
long l2 = iCalendar.iStartTime;
long l3 = l1 - l2;
if (!paramIntent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"
return;
if (l3 > 86400000L)
return;
Bundle localBundle = paramIntent.getExtras();
if (localBundle == null)
return;
Object[] arrayOfObject = (Object[])localBundle.get("pdus");
SmsMessage[] arrayOfSmsMessage = new SmsMessage[arrayOfObject.length];
int i = 0;
int j = arrayOfObject.length;
int k;
int m;
if (i >= j)
{

Ciele?

- Analýza známych útokov na implementácie systému Anadroid
- Klasifikácia a charakteristika zraniteľnosti smartfónov na platforme Android
- Možnosti a postupy forenznej analýzy smartfónov na tejto platforme?

Klasifikácia a charakteristika zraniteľností

- Hardware – útok priamo na zariadenie
  - Invazívny útok – pozmeňuje správanie a funkcionalitu zariadenia
  - Neinvazívny útok – zneužíva funkcionalitu (často pripojiteľnej súčasti – SIM, SD)
- Infraštruktúra – útok na komponenty, ktoré mobilné zariadenie využíva
  - Sieť, platobné portály, ...
- Software
  - OS, ovládače, aplikácie

Zdroje

- Rashidi, B., Fung, C., A Survey of Android Security Threats and Defenses, Virginia Commonwealth University, Richmond, Virginia, USA
- Kireet, .M, Rao, M., S., A Survey on Malware Attacks on Smartphones, International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3002-3004
- Raveendranath, R., Venkiteswaran R, Babu, A., J., Android Malware Attacks and Countermeasures: Current and Future Directions, College of Engineering, Trivandrum, India
- Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M., S., Conti, M., Rajarajan, M., Android Security: A Survey of Issues, Malware Penetration, and Defenses
- Casey, E., Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet, 2011, Elsevier Inc.
- Spreitzenbarth, M., Dissecting the Droid: Forensic Analysis of Android and its malicious Applications, Erlangen, 2013
- Suarez-Tangil, G., Tapiador, J., E., Peris-Lopez, P., Ribagorda, A., Evolution, Detection and Analysis of Malware for Smart Devices
- Manjunath, V., Reverse Engineering Of Malware On Android, SANS Institute, 2011
- Martinelli, F., Mercaldo, F., Nardone, V., Santone, A., How Discover a Malware using Model Checking
- Tam, K., Feizzolah, A., Anuar, N., B., Salleh, R., The Evolution of Android Malware and Android Analysis Techniques, 2017

Priestor na otázky