Dynamic Enforcement of Security Policies on Android Applications: A Case Study

Jinseong Jeon
Mobile Computing

Once upon a time...

recently
markets play a key role in booming a mobile industry, directly connecting developers with users.
Ultimatum

- All-or-nothing!
  - install the app, granting all the permissions it requires
  - or, revoke installation

- App Almighty
  - once granted, apps can use such permissions in *any way* they want.

- Privacy Problems
Happening

Hey George, yesterday I $#@!*&%^...

K**** messenger

Yay~ new smartphone~
Permission as Policy

- Currently, coarse-grained permissions
  - we call the current security model of Android resource-centric
  - i.e., too focused on HW and/or SW resources

- Towards fine-grained permissions
  - instead of full grant, specify the usage!
  - so that developers can assure that they use permissions safely
  - so that users can trust apps (guesses are no longer required.)

- E.g.,
  - Full Internet access vs. InternetURL(google.com)
  - Camera vs. ScanBarcodes
  - Fine (GPS) location vs. LocationBlock
Dynamic Enforcement

- Rewriting app. binary
  - user aspect: no source codes, easier than re-flashing OS
- Replacing libraries w/ trusted, fine-grained ones
Rewriting

DroidLib

policy extractor

policy analyzer

redexer+

xml

.zip

.dex

(xml)

(parser)

(modifier)

(dumper)
Demo

D/DroidLib Client(429): trying to bind
D/DroidLib Client(429): done bind method
D/DroidLib Client(429): status = true
D/dalvikvm(437): GC_EXPLICIT freed 114K, 53% free 2553K/5379K, external 716K/1038K
, paused 2725ms
D/DroidLib Service(437): onBind()
I/ActivityManager(65): Displayed com.nick.local/.RandomActivity: +25651ms
D/DroidLib Client(429): onServiceConnected end
D/sds(429): about to init service
W/KeyCharacterMap(429): No keyboard for id 0
W/KeyCharacterMap(429): Using default keymap: /system/usr/keychars/qwerty.kcm.bin
D/DroidLib Client(429): trying to connect to web
D/outputStream(429): the size is=0
D/outputStream(429): parcel sent
D/outputStream(437): buffer received
D/DroidLib Service(437): attempting to check
D/DroidLib Service(437): com.droidlib.permissions.URL.ucla_edu
D/DroidLib Service(437): try
D/DroidLib Service(437): permission=true
D/DroidLib Service(437): com.droidlib.permissions.URL.ucla_edu
D/DroidLib Service(437): try
D/DroidLib Service(437): connecting to url
D/inputStream(437): the size is=5792
D/inputStream(437): parcel sent
D/outputStream(437): the size is=0
D/outputStream(437): parcel sent
D/inputStream(429): buffer received
D/outputStream(429): buffer received
D/DroidLib Client(429): Count =5792
D/dalvikvm(65): GREF has increased to 401
W/InputMethodManager(65): Window already focused, ignoring focus gain of: com.android.internal.view.IInputMethodClientStub$StubProxy@40784348
D/dalvikvm(142): GC_EXPLICIT freed 60K, 51% free 2937K/5959K, external 2715K/3289K
, paused 241ms
Future Work

- More vocabularies for fine-grained permissions
- More libraries to support above
- More apps to explore this idea

- Evaluation methodology
  - rewriting overhead
    - in terms of file size, execution time, user experience
  - library efficiency
    - library exchange vs. inline monitor vs. no-op

- Differential privacy
  - tradeoff between privacy and functionality