//if true then for string values, only track jsa resolved strings (so hot spot strings)

public static final boolean ONLY\_TRACK\_JSA\_STRINGS = true;

## SourceCallInfoChain.java:

/\*\* Calculate the score for each entry in the call chain \*\*/

public void calculate\_scores() {

score = 0;

if (contents.length == 0) {

API api = API.v();

Set<InfoKind> source = api.getSourceInfoKinds(method);

Set<InfoKind> sink = api.getSinkInfoKinds(method);

if (is\_system (method)) {

if (api.isSafeMethod(method))

score = 0;

else if (api.isSpecMethod(method))

score = 5;

else if (api.isBannedMethod(method))

score = 6;

if (!source.isEmpty())

score += 1;

else if (!sink.isEmpty())

score += 2;

}

return;

}

Score is used to identify whether the source call info chain is a safe method, a spec method, a banned method, or a method with many sources/sinks.

## SourceCallChainBuilder:

/\*\* timer so we can timeout after a reasonable amount of time \*\*/

private StopWatch timer = new StopWatch();

/\*\* Timeout (milliseconds). The output will be incomplete \*\*/

private int timeout;

/\*\* just ignore duplicate methods rather than merging call chains \*\*/

private boolean ignore\_dup\_methods = false;

## Files and the places that generate the file:

InterAppSourceFlows.gson 🡪 android.droidsafe.analyses.interapp. GenerateInterAppSourceFlows.java

Configurations: createRCFG, produceInterAppFlowsFile (writeinterappflows)

reachable-user-class-methods.txt 🡪 android.droidsafe.analyses.rcfg.RCFG.java

high-level.txt 🡪 android.droidsafe.speclang.SecuritySpecification.java

(number of srcKind -> sinkKind)

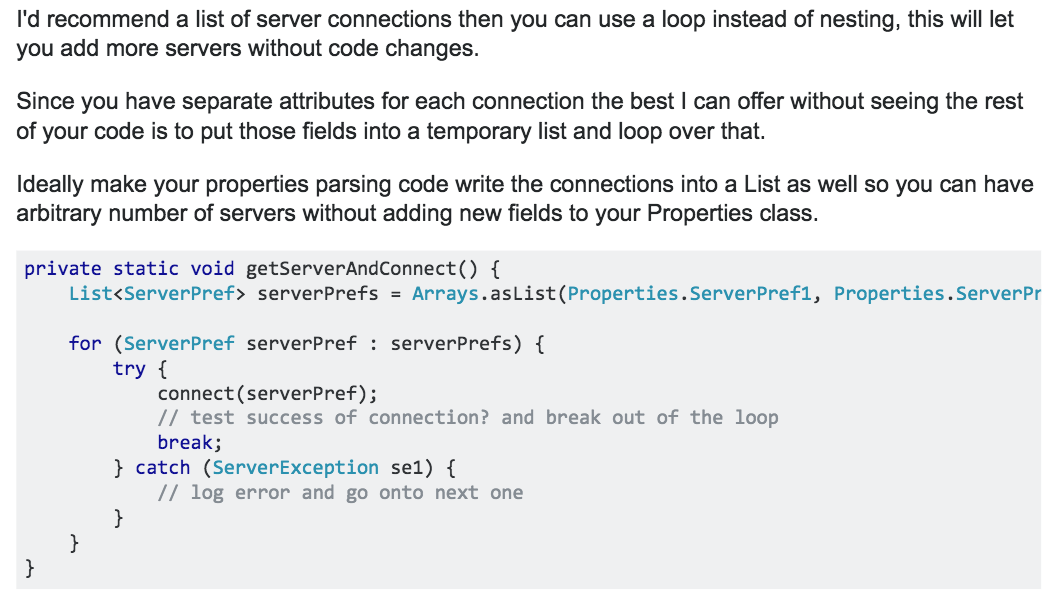
## Main.java:

AfterTransform(arg…): Called after one or more transforms to recalculate any underlying analysis. (Running PTA, Finished PTA)

## Callback && Fallback

Callback: Your app wants to download a file from some remote computer and then write to to a local disk. The remote computer is the other side of a dial-up modem and a satellite link. The latency and transfer time will be huge and you have other things to do. So, you have a function/method that will write a buffer to disk. You pass a pointer to this method to your network API, together with the remote URI and other stuff. This network call returns 'immediately' and you can do your other stuff. 30 seconds later, the first buffer from the remote computer arrives at the network layer. The network layer then calls the function that you passed during the setup and so the buffer gets written to disk - the network layer has 'called back'. Note that, in this example, the callback would happen on a network layer thread than the originating thread, but that does not matter - the buffer still gets written to the disk.

Fallback: more like a backup mechanism;



addFallbackModeling:

android.droidsafe.transforms.CallBackModeling.java

public void run() {

//go through all user classes and find method that override system methods that are not called

//create a method for each class that calls inherited methods that are not reachable (and not verified)

//for each allocation of one of these classes, call the fallback callback method

findDeadCallbackAndCreateFallbackMethod();

//call the methods that we have created at each allocation

callFallBackMethods();

//check for components that are not created anywhere

findAndCreateUnallocedComponents();

}

android.droidsafe.reports.InfoFlowReportNoRCFG.java: Generate information flow result with RCFG. Only assume that PTA and information flow analysis has completed.

stmt-flows.txt

reachable-app-methods.txt

all-sources.txt (printSensitiveSources())

android.droidsafe.reports.InformationFlowReport.java: Create an information flow report that lists sensitive sinks if a sensitive source flows into a receiver or argument.

info-flow-results.txt (// format is: \*\*|<entry-method>|<sink>/<cat>/line|rx-src|<source\_rx/cat\_list>|arg-src|<src\_arg list)

info-iflow-results.txt (Config.v().implicitFlow) (iflow\_create(SecuritySpecification spec): Create an information flow report that lists sensitive sinks from sensitive sources via implicit flow.)

check-info-flow.txt (Config.v().checkInfoFlow)

## android.droidsafe.reports.SensitiveSources.java:

(building indicator, writeJSONReports() in Main.java)

sensitive\_sources.json

## android.droidsafe.analyses.value.ValueAnalysis.java:

va-results.log&va-errors.log

## pta packages:

SPARK: A PTA bridge for the SPARK points to analysis. Right now the analysis is context insensitive.

Config.v().dumpPta 🡪 pta.txt; Config.v().dumpCallGraph 🡪 callgraph.gexf; dumpReachablesAndAllocNodes () 🡪 spark-dump.log; dumpOutdegreesCSV() 🡪 reachables-outdegree.csv; dumpCallGraphReachablesCSV() 🡪 reachables-count.csv

PaddlePTA:

GeoPTA: Config.v().dumpPta 🡪 pta.txt; Config.v().dumpCallGraph 🡪 callgraph.dot

## PTAPaper.java & Method.java:

int flowsIntoSinksArgs = 0;

int flowsIntoSinksArgsPrecise = 0;

int flowsIntoSinksMem = 0;

int flowsIntoSinksRec = 0;

## android.droidsafe.stats.IntentResolutionStats.java:

icc-resolution-stats.txt

## android.droidsafe.stats.FindAPICallsWithNonLocalEffects.java:

non-local-api-methods.txt

## android.droidsafe.stats.AveInfoFlowSetSize.java:

info-set-size.txt (totalSet, totalSetsSize)

android.droidsafe.reports.AnalysisReport.java:

This class stores data and produces a report for an analyst of any issues encountered during the analysis that are suspicious or could lead to imprecision or inaccuracy in the results.

analysis-warning-report.txt

## modeling/api/droidsafe/annotations/DSSourceKind.java:

### DroidSafe source types:

GUI,

GUI\_TEXT,

ACCOUNT\_INFORMATION,

BLUETOOTH,

BLUETOOTH\_INFORMATION,

BROWSER\_INFORMATION,

CALENDAR,

CLIPBOARD,

CONTENT,

CONTACT\_INFORMATION,

DATABASE\_INFORMATION,

DATABASE,

EMAIL,

EXIF\_INFO,

FILE,

FILE\_INFORMATION,

IMAGE,

LOCATION,

MEDIA,

NETWORK,

NFC,

PREFERENCES,

SHARED\_PREFERENCES,

RESOURCE,

SCREEN,

SENSITIVE\_UNCATEGORIZED,

SMS\_MMS,

SECURITY\_INFO,

SYNCHRONIZATION\_DATA,

SYSTEM\_SETTINGS,

SYSTEM\_PROPERTY,

UNIQUE\_IDENTIFIER,

UNSPECIFIED,

UNMODELED,

REFLECTION,

RANDOM\_NUMBER,

SENSOR,

SERIALIZATION,

IPC,

IO,

AUDIO,

USER\_INPUT,

OS\_STATE,

OS\_PROCESS,

XML,

RESOURCES,

ANY\_MEMORY,

REMOTE\_APP,

CAMERA,

DATE\_TIME,

AD,

GOOGLE\_SERVICES, /\*a bit too generic \*/

GOOGLE\_DRIVE,

JSON,

WEB,

ENCODED

## modeling/api/droidsafe/annotations/DSSinkKind.java:

### DroidSafe sink types:

ACCOUNT\_SETTINGS,

AUDIO,

BLUETOOTH,

BROWSER\_INFORMATION,

CALENDAR,

CONTACT\_INFORMATION,

CONTENT, //content provider, resolver

EMAIL,

EXIF\_INFO,

FILE,

LOCATION,

LOG,

NETWORK,

NFC,

OS\_COMMAND,

PHONE\_CONNECTION,

PHONE\_STATE,

PREFERENCES,

SCREEN,

SENSITIVE\_UNCATEGORIZED,

SERIALIZATION,

SMS\_MMS,

SYNCHRONIZATION\_DATA,

SYSTEM\_SETTINGS,

SHARED\_PREFERENCES,

VOIP,

UNSPECIFIED,

USB,

REFLECTION,

IPC,

DATABASE,

RESOURCES,

IO,

PROCESS,

CLIPBOARD,

ANY\_MEMORY,

AD,

GOOGLE\_SERVICES,

GOOGLE\_DRIVE,

GUI,

EXEC,

ENCODER

## modeling/api/droidsafe/annotations/DSGenerator.java:

String tool\_name();

String tool\_version();

String generated\_on();

String hash\_original\_method();

String hash\_generated\_method();

## modeling/api/droidsafe/annotations/DSGeneratedField.java:

String tool\_name();

String tool\_version();

String generated\_on();

String hash\_original\_field();

String hash\_generated\_field();

## modeling/api/droidsafe/annotations/DSCat.java:

### //Safe Categories \*/

ANDROID\_ANIMATION,

ANDROID\_CALLBACK, //methods like onClick

OS\_GENERAL,

FS\_INFO,

DATA\_STRUCTURE,

DB\_CURSOR,

MEM\_BUFFER,

SAFE\_LIST,

GUI,

GRAPHICS,

NO\_ACTION,

DATA\_GENERAL,

SAFE\_OTHERS,

UTIL\_FUNCTION,

SOURCE,

### //Ban Categories

DALVIK,

PRIVATE\_METHOD,

REFLECTION,

CLASS\_LOADER,

SECURITY\_VIOLATION,

DROIDSAFE\_INTERNAL,

BAN\_OTHERS,

### //Spec Categories

ABSTRACT\_METHOD,

ANDROID\_ACCOUNT,

ANDROID\_ACTIVITY\_STARTING,

ANDROID\_APPLICATION,

ANDROID\_INTERNAL,

ANDROID\_INSTRUMENTATION,

ANDROID\_LOW\_LEVEL,

ANDROID\_MANAGER,

ANDROID\_NOTIFICATION\_STARTING,

ANDROID\_LOADER,

AUDIO\_CALL,

AUDIO\_RECORDING,

APP\_RESOURCE,

CALLBACK\_INVOKE,

CALLBACK\_REG,

BACKUP\_SUBSYSTEM,

BLUETOOTH,

NFC,

CONTACT,

CONTENT,

TO\_MODEL, //once the method is modeled, it will be safe

DATABASE, //database changing

DEFAULT\_MODIFIER,

DEVICE,

EXEC,

FILE\_SYSTEM,

MONITORING,

GPS,

INTERNET,

INTENT\_EXCHANGE,

INTERGUI\_ACTION,

IO,

IO\_ACTION\_METHOD,

IPC,

SERVICE,

JAVA\_SECURITY,

LOGGING,

LOCATION,

MEDIA\_RECORDER,

NETWORK\_STATS,

NETWORK,

NETWORKING,

OS\_LOW\_LEVEL,

PACKAGE\_INFO,

PACKAGE\_MANAGER,

PHONE\_CALL,

PHONE\_STATE,

POWER\_MANAGER,

RESOURCE,

RTP\_CALL,

SENSOR,

SIP\_REGISTRATION,

SMS,

SHARING,

STORAGE,

STORAGE\_STATE,

SYSTEM\_SETTING,

SYSTEM\_SERVICE,

STORAGE\_ACCESS,

SYSTEM,

SYSTEM\_PREFERENCES,

SHARED\_PREFERENCES,

SYSTEM\_SETTINGS,

SECURITY,

SERIALIZATION,

TELEPHONY,

XML,

THREADING, //threading/execution

TRIGGER,

URI\_EXCHANGE,

WIFI,

SPEC\_OTHERS,

TIME,

IPC\_CALLBACK,

### //Default value, not SAFE, BAN nor SPEC

UNSPECIFIED;

Droidsafe will model the Android system, while modeling the Android system, it categorizes all methds into the following types:

SAFE, SPEC, BAN

## DSOnlyType:

NOT\_VALID,

NOT\_USED,

DONTCARE

## Config-imprecisestrings:

tools/objsenspark/src/objsenspark/SparkPTA.java:

/\*\* comma separated list of classes in which no matter what the length of k

\* for object sensitivity, we want to limit the depth of the object sensitivity

\* to one. Also add subclasses of each

\*

\* Strings will be added if the precisestrings options is given

\*/

Check objsenspark tool:

Under tools/objsenspark