Reading papers

1) What is the problem being addressed?
   - Does the paper succeed?
   - How well do they evaluate success?

2) What is the contribution?
   - How important is the contribution?

3) How does the paper relate?
   - Any obvious extensions?
   - Project ideas?
4) How would you address the problem?

5) What is unclear?

6) What are the holes/weaknesses/assumptions made by the paper?

Amer) What surprised you most?

Evan

ACM → Import Zotero → Mendele

DBLP → BibDesk

Ad-hoc text files

(Hard copy)
FlowDroid

Problem: Static taint analysis of Android applications

Challenges:

1) Program entry points - "main"
   - Android lifecycle

2) [Native code, Reflection, ...]
   - Usual yucky stuff everyone ignores

3) Callbacks

4) Aliasing
Contributed

- MV per program location
- MV: separated per field
- o.f., o.g are separate
- context, flow, field, object sensitive
- (not path sensitive)
- + callbacks / lifecycle

```
x: a
  x.f(c)
```

```
y: a
  y.f(c)
```

"context-sensitivity with receiver objects"
Lifecycle

1) Based on the component "type" like Activity
   onCreate(), ...
   Build a call graph per component

2) Registered callbacks per component are added next
Taint Analysis

1) Find tainted sources (forwards)

2) Propagate to aliases (backwards)

IPDS

Abstract domain element whose reachable heap

\( U \) set of access paths that may be tainted

[per program location]

e.g. \( \{ x.f \} \)

\( Y \in S \) means no tainting in the reachable heap

from \( y \).
IFDS

Interprocedural, Finite, Distributive, Subset

Dataflow Analysis

1) supergraph of the program

CF6s plus call/return edges

CFG for f

entry

exit

CF6 for g

2) finite set of "dataflow facts" D

FlowDroid set of all program access paths

3) a meet operator

\( \Join \) (abs interpretation)
4) distributive data flow function


\[ f : 2^D \rightarrow 2^D \]

\[ \forall d \in 2^D \]

\[ f(\hat{d}_1 \sqcap \hat{d}_2) = f(\hat{d}_1) \sqcup f(\hat{d}_2) \]

"precision"

solves MRP w/o loss precision

& "realizable paths"
"Exploded super graph"

\[ \text{supergraph} / \text{CFG} \times \text{dataflow facts} \]

\[ 2^D \]

\[ O(D) \]