Evaluating Disassembly of Android Apps Compiled to Binary OATs Through the ART

Jakob Bleier, Martina Lindorfer – SecLab TU Wien

EuroSec ‘23
Evaluating Disassembly of Android Apps Compiled to Binary OATs Through the ART

Jakob Bleier, Martina Lindorfer – SecLab TU Wien

EuroSec ‘23
How did we get here?

Computers

Idea: Study Android Ecosystem

2020

now

Present about Android Ecosystem
How did we get here?

Computers

2020

Idea: Study Android Ecosystem

2019

R8 becomes default dexter

Present about Android Ecosystem

now
int fooBar(int a) {
    int x = halve(a);
    int y = a*3;
    int z = 0;
    if (a > 111) {
        z = fooBar(x);
    } else {
        z = a-2;
    }
    return x+y+z;
}

int halve(int a) {
    return a/2;
}

invoke-virtual {v3, v4},
    int [..].halve(int)
movere-result v0
mul-int/lit8 v1, v4, #+3
const/16 v2, #+111
if-le v4, v2, +7
invoke-virtual {v3, v0},
    int [..].fooBar(int)
movere-result v3
goto +3
add-int/lit8 v3, v4, #-2
add-int/2addr v0, v1
add-int/2addr v0, v3
reterrn v0
How did we get here?

Computers

2014
ART replaces Dalvik VM

2019
R8 becomes default dexer

2020
Idea: Study Android Ecosystem

Present about Android Ecosystem

now
### Java (/Kotlin)

```java
int fooBar(int a) {
    int x = halve(a);
    int y = a*3;
    int z = 0;
    if (a > 111) {
        z = fooBar(x);
    } else {
        z = a-2;
    }
    return x+y+z;
}

int halve(int a) {
    return a/2;
}
```

### Dalvik

```dls
invoke-virtual {v3, v4},
    int [..].halve(int)
move-result v0
mul-int/lit8 v1, v4, #+3
const/16 v2, #+111
if-le v4, v2, +7
invoke-virtual {v3, v0},
    int [..].fooBar(int)
move-result v3
goto +3
add-int/lit8 v3, v4, #-2
add-int/2addr v0, v1
add-int/2addr v0, v3
return v0
```

### Binary

```
[..]
mov x22, x1
mov x23, x2
[..]
cmp w23, #0x6f (111)
b.le #+0x20 (addr 0x7f0730)
mov x2, x0
mov x1, x22
mov x25, x2
[..]
mov x25, x0
sub w0, w23, #0x2 (2)
add w1, w25, w24
add w0, w25, w1
[..]
ret
```
Evaluate Disassembly

APKs → dex2oat → OATs → IDA Pro, Ghidra, Binary Ninja, radare2, angr → Function Boundaries

oatdump
Function Boundaries

- full match: offset + size match
- (only) offset matches
- superfluous functions at unexpected offsets
Function Boundaries

![Diagram showing function boundaries for different tools: oatdump (ground truth), Ida Pro, Ghidra, Binary Ninja, radare2, angr, Ida ProBE, GhidraBE, Binary NinjaBE. The diagram compares the full match, offset match, and superfluous segments across the tools.]
Function Boundaries

Soot: 1,261 (94.17%)

SootUP: 1,339 (100%)
Failed on 7 functions in 5 apps
Of Ahead Time: Evaluating Disassembly of Android Apps Compiled to Binary OATs Through the ART

Jakob Bleier, Martina Lindorfer – SecLab TU Wien

● APK to OAT compilation and Disassembly possible at scale
● Differences in decompilers re: Function boundaries, but promising results

Ongoing work:

● Downstream tools for full app analysis
● Open source pipeline for extendable benchmark with robust ground truth
Extra slides
Lifetime of an Android App