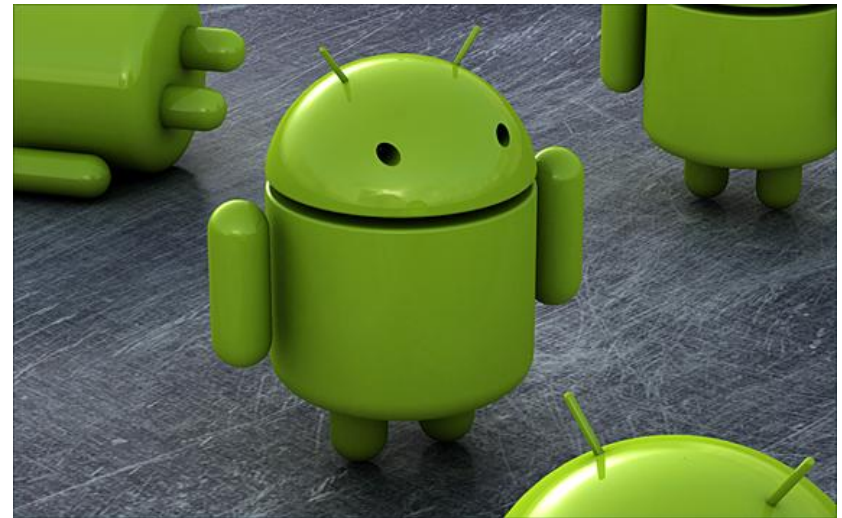


inversion Mobile. Case “Android”. apply IHsecurePolicy...

Jinseong Jeon &
Youngil Kim

CMSC 631 term project

ANDROID



- A mobile OS
 - based on Linux kernel
- A complete set of software for mobile devices
 - OS, middleware, and applications
- “All applications are created equal.”
 - no diff. between core app. and 3rd party app.
 - no barriers to accessing individual information

Security

“Midnight Survival” using
Google latitude



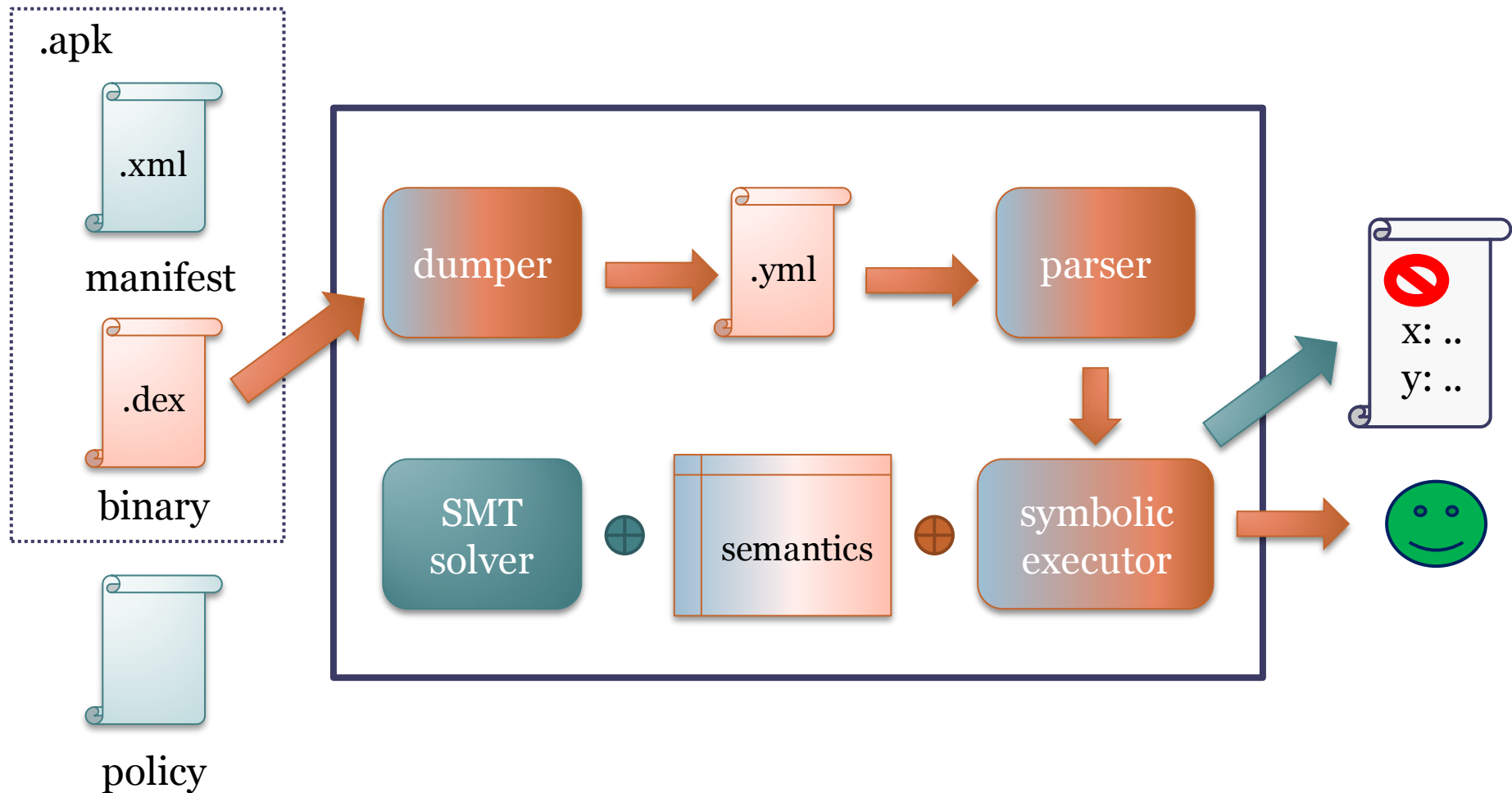
- Apps can leak your private info
 - calendar
 - contacts, call logs, or favorites(!)
 - geographic location



Related Work

- SCanDroid
 - modular data-flow analysis
 - extracts security specs from manifests
 - checks data-flows are consistent with such specs
- TaintDroid
 - an extension of Android platform
 - labels (taints) data from privacy-sensitive sources
 - tracks and logs when such data are transmitted over the network or leave the system

FEDEX: Fast symbolic Executor for DEX

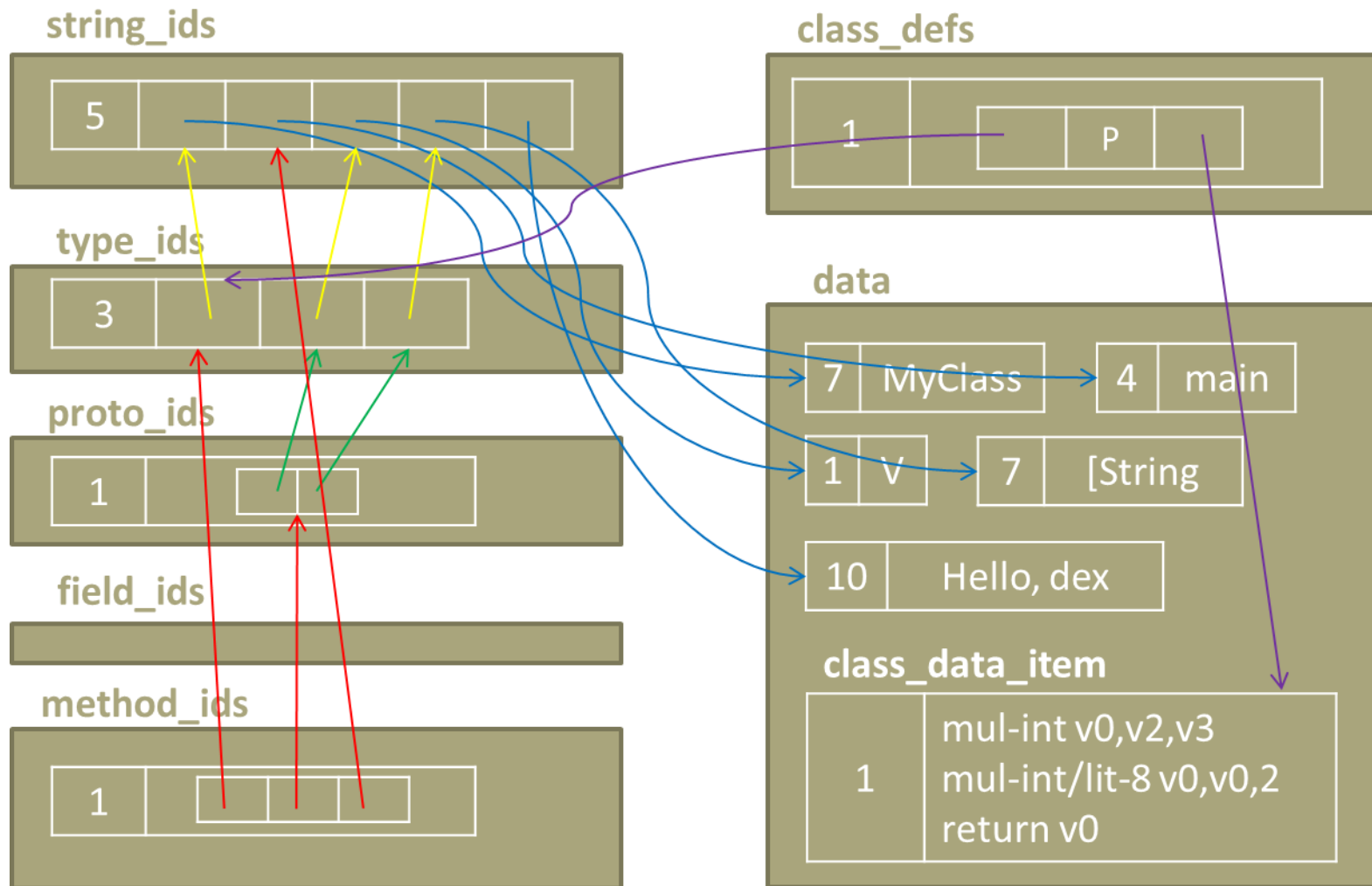


DEX: Dalvik Executable

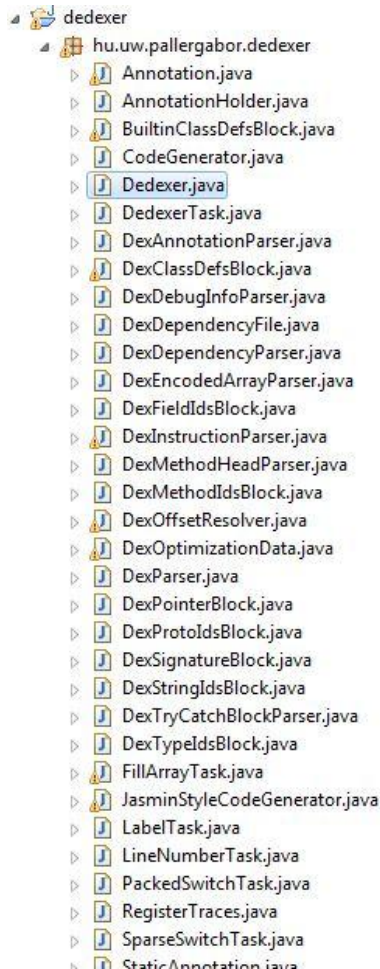


- Shared Constant Pool
 - to avoid repetition
- Either Links or Data
 - header
 - indicates where other sections are
 - e.g. string_ids
 - constant string
 - name for class, field, and method
 - a list of offsets to a location in data section

DEX Example

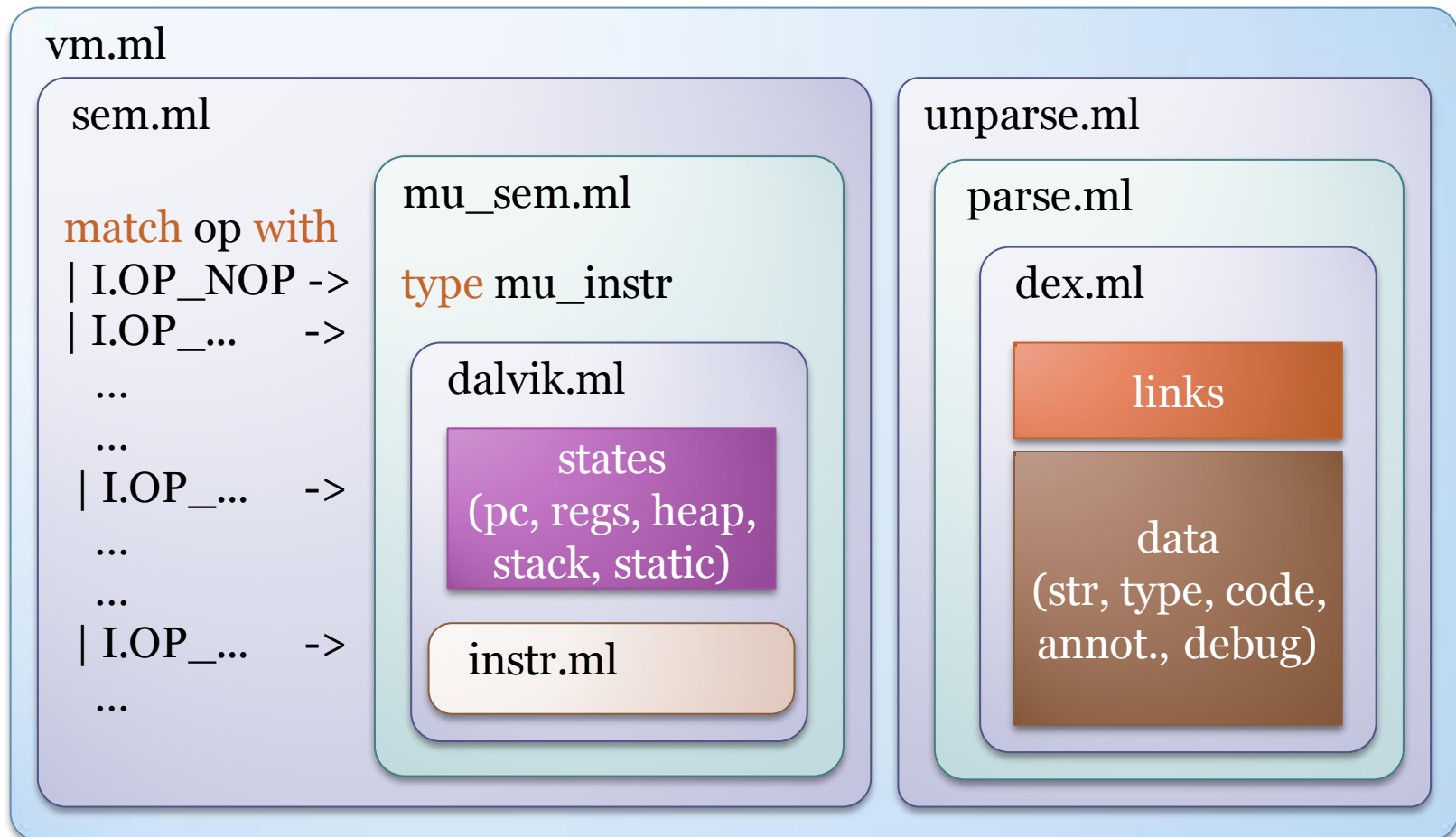


Dumpers



- dexdump
 - from Dalvik VM
 - written in C
 - try to mimic “objdump”
- baksmali
 - from smali project
 - written in Java
 - build source trees in smali format
- dedexer
 - yet another open source project
 - written in Java

Dalvik VM



Micro Semantics

```
(* step: Dk.state -> I.instr -> Dk.state *)
let step pre ins =
  let op = fst ins and opr = snd ins in
  match op with
  | I.OP_NOP -> pre
  | ...

  | I.OP_ADD_INT
  | I.OP_ADD_INT_LIT16
  | I.OP_ADD_INT_LIT8
  | I.OP_ADD_IND_2ADDR ->
    MU.step pre (MU.MU_BOP (MU.MU_ADD opr))
  | ...
```

sem.ml

```
type mu_instr =
  | MU_GOTO of Instr.offset
  | MU_CONST of Instr.operand list
  | MU_MOVE of Instr.operand list
  | MU_COMP of bop * Instr.operand list
  | MU_BOP of bop * Instr.operand list
  | ...

type bop

val step: Dalvik.state -> mu_instr
      -> Dalvik.state
```

mu_sem.mli

- original opcodes:
 - 1 nop, 3 moves, 4 consts, 12 comps, 3 gotos, 41 bops
- micro: 5 opcodes + (6 relations + 11 bops)

Demo

augustus:1 (jsjeon)

Disconnect Options Clipboard Record Send Ctrl-Alt-Del Refresh

Applications Places System

Mon Nov 29, 9:05 PM

jsjeon@augustus:~/2010_fall/631/fedex

File Edit View Terminal Tabs Help

```

0x000001D3: [sort: string_data, size: 2, data: "VL"]
0x000001D7: [sort: string_data, size: 19, data: "[Ljava/lang/String;"]
0x000001EC: [sort: string_data, size: 4, data: "exit"]
0x000001F2: [sort: string_data, size: 4, data: "main"]
0x00000178: [sort: type_list, size: 1, list: [0]]
0x00000180: [sort: type_list, size: 1, list: [5]]
0x0000020D: [sort: class_data_item, static_fields_size: 0, instance_fields_size: 0, direct_methods_size: 2, virtual_methods_size: 0, direct_methods_list: [[method_id: 0, access_flag: 65537, code_off: 0x0000011C], [method_id: 1, access_flag: 9, code_off: 0x00000134]] ]
0x0000011C: [sort: code_item, registers_size: 1, ins_size: 1, outs_size: 1, tries_size: 0, debug_info_off: 504, insns_size: 2, insns_list: [0x0000012C, 0x00000132] ]
0x0000012C: [sort: instruction, op: invoke-direct, opr: [v0, 2] ]
0x00000132: [sort: instruction, op: return-void]
0x00000134: [sort: code_item, registers_size: 6, ins_size: 1, outs_size: 1, tries_size: 0, debug_info_off: 509, insns_size: 16, insns_list: [0x00000144, 0x00000146, 0x0000014A, 0x0000014E, 0x00000150, 0x00000152, 0x00000156, 0x00000158, 0x0000015C, 0x0000015E, 0x00000162, 0x00000168, 0x0000016A, 0x0000016C, 0x00000170, 0x00000176] ]
0x00000144: [sort: instruction, op: const/4, opr: [v4, 1] ]
0x00000146: [sort: instruction, op: const/16, opr: [v0, 631] ]
0x0000014A: [sort: instruction, op: const/16, opr: [v1, 16] ]
0x0000014E: [sort: instruction, op: const/4, opr: [v2, 0] ]
0x00000150: [sort: instruction, op: move, opr: [v3, v0] ]
0x00000152: [sort: instruction, op: if-gt, opr: [v1, v3, 0x0000015E] ]
0x00000156: [sort: instruction, op: sub-int/2addr, opr: [v3, v1] ]
0x00000158: [sort: instruction, op: add-int/lit8, opr: [v2, v2, 1] ]
0x0000015C: [sort: instruction, op: goto, opr: [0x00000152] ]
0x0000015E: [sort: instruction, op: if-gt, opr: [v1, v3, 0x00000168] ]
0x00000162: [sort: instruction, op: invoke-static, opr: [v4, 3] ]
0x00000168: [sort: instruction, op: mul-int/2addr, opr: [v1, v2] ]
0x0000016A: [sort: instruction, op: add-int/2addr, opr: [v1, v3] ]
0x0000016C: [sort: instruction, op: if-eq, opr: [v0, v1, 0x00000176] ]
0x00000170: [sort: instruction, op: invoke-static, opr: [v4, 3] ]
0x00000176: [sort: instruction, op: return-void]

```

"Demo.dump.yml" 72L, 3751C 72,2 Bot

jsjeon@augustus:~/2010_fall/631/fedex

File Edit View Terminal Tabs Help

```

import java.lang.System;

public class Demo {

    public static void main (String[] args) {
        int n, d;
        n = 631;
        d = 16;

        int r = n, q = 0;
        while (d <= r) {
            r = r - d;
            q++;
        }

        if (d <= r)
            System.exit(1);

        if (n != (q * d + r))
            System.exit(1);
    }
}

```

"Demo.java" 23L, 303C 2,0-1

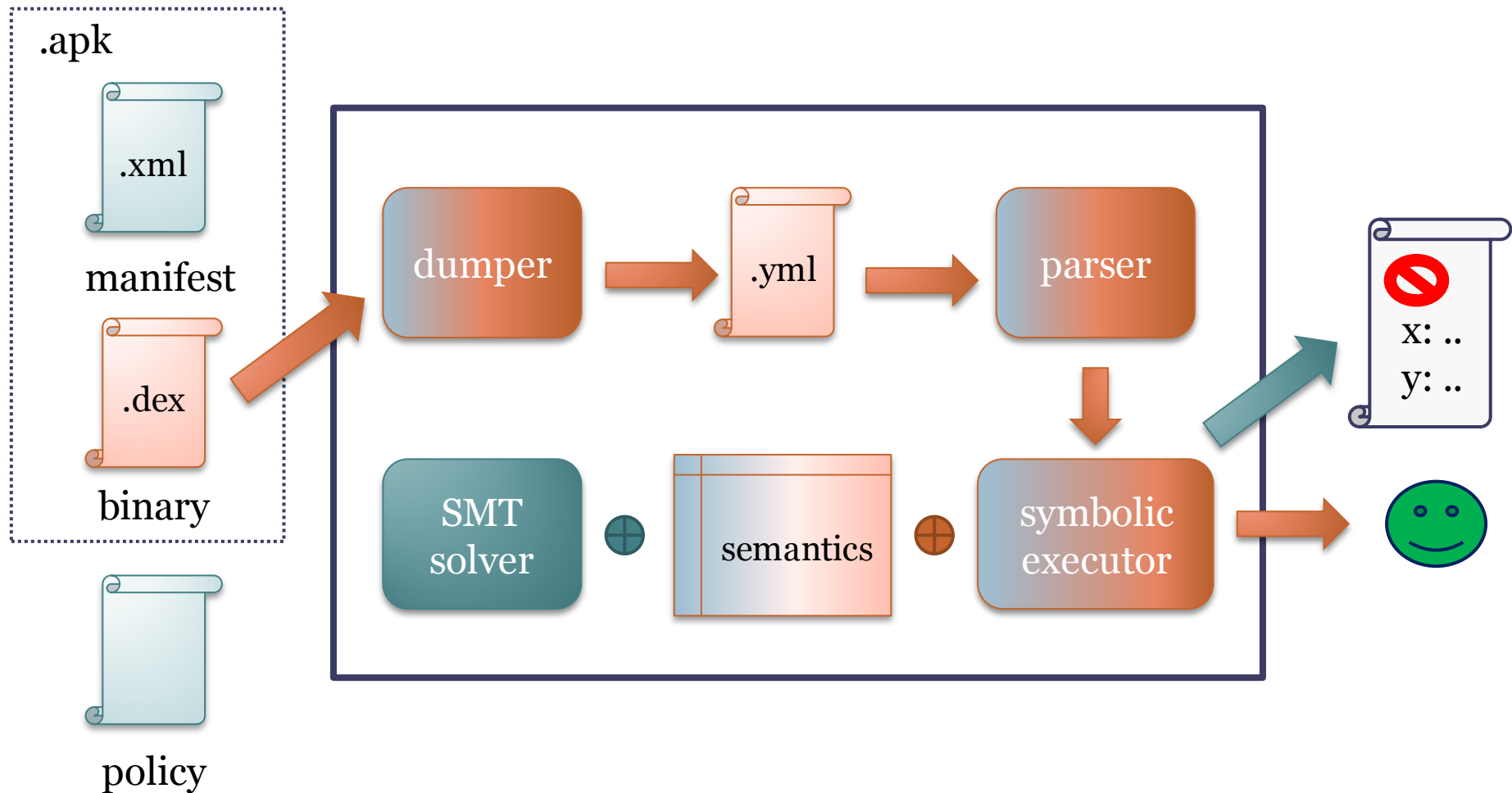
```

- !pc
pc : 0x00000176
- !registers
v0 : 631
v1 : 631
v2 : 39
v3 : 7
v4 : 1
- !stack
- !heap
- !static
Fatal error: exception Sem.SEM_Error("not handled yet: return-void")
[jsjeon@augustus fedex]$

```

jsjeon@augustus:~/2010_fall/631/fedex jsjeon@augustus:~/2010_fall/631/fedex jsjeon@augustus:~/2010_fall/631/fedex

Future Work



Reference

- Open Handset Alliance
<http://www.openhandsetalliance.com/>
- DEX Executable format
<http://www.netmite.com/android/mydroid/dalvik/docs/dex-format.html>
- bytecode for the Dalvik VM
<http://www.netmite.com/android/mydroid/dalvik/docs/dalvik-bytecode.html>
- YAML: YAML Ain't Markup Language
<http://www.yaml.org/>
- Syck bindings for Ocaml
<http://ocaml-syck.sourceforge.net/>

Reference

- **smali**: an assembler/disassembler for Android's dex format
<http://code.google.com/p/smali/>
- **Dalvik VM**
<http://android.git.kernel.org/?p=platform/dalvik.git;a=tree;hb=master>
- **dedexer**
<http://dedexer.sourceforge.net/>
- **SCanDroid**: Automated Security Certification of Android Applications. Adam P. Fuchs, Avik Chaudhuri, and Jeffrey S. Foster.
- **TaintDroid**: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, William Enck, et. al.