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

Jinseong Jeon & Youngil Kim
CMSC 631 term project
• 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

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>header</td>
</tr>
<tr>
<td>string_ids</td>
</tr>
<tr>
<td>type_ids</td>
</tr>
<tr>
<td>proto_ids</td>
</tr>
<tr>
<td>field_ids</td>
</tr>
<tr>
<td>method_ids</td>
</tr>
<tr>
<td>class defs</td>
</tr>
<tr>
<td>data</td>
</tr>
</tbody>
</table>
DEX Example

string_ids

5

type_ids

3

proto_ids

1

field_ids

method_ids

1

class_defs

1

P

data

7 MyClass

4 main

1 V

7 [String

10 Hello, dex

class_data_item

1 mul-int v0,v2,v3

mul-int/lit-8 v0,v0,2

return v0
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

```
match op with
| I.OP_NOP   ->
| I.OP_...   ->
   ...
| I.OP_...   ->
   ...
| I.OP_...   ->
   ...
| I.OP_...   ->
   ...
```

- `vm.ml`
- `sem.ml`
- `unparse.ml`
- `parse.ml`
- `mu_sem.ml`
- `mu_instr`
- `dalvik.ml`
- `states`
  - `(pc, regs, heap, stack, static)`
- `instr.ml`
- `dex.ml`
- `links`
- `data`
  - `(str, type, code, annot., debug)`
Micro Semantics

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

```java
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
```

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

• 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

• **Dalvik VM**
  [http://android.git.kernel.org/?p=platform/dalvik.git;a=tree;hb=master](http://android.git.kernel.org/?p=platform/dalvik.git;a=tree;hb=master)

• **dedexer**

• **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.