Security in Mobile Systems - UE/EX

FH Hagenberg, WS 2017
DI Dr. Erik Sonnleitner

Exercise 6: Reverse Engineering

Exercise 6: Reverse Engineering

(1) Reverse engineer the following Dalvik bytecode snippet into high-level Java code, and explain what the code does.

```
.method private mymethod([II)V
  aget          v0, v3, v4
  add-int/lit8 v1, v4, 0x1
  aget          v1, v3, v1
  aput          v1, v3, v4
  add-int/lit8 v1, v4, 0x1
  aput          v0, v3, v1
  return-void
.end method
```

- Notes:
  - First argument passed to method is `v3`, and of type `[I`
  - Second argument passed to method is `v4`, and of type `I`

Exercise 6: Reverse Engineering

(2) Reverse engineer the following Dalvik bytecode snippet into high-level Java code, and explain what the code does.

```
.method private mymethod2(Ljava/io/InputStream;)I
.catch Ljava/io/IOException; {:try_start_0 .. :try_end_0} :handler_0
  :try_start_0
  invoke-virtual {v2},Ljava/io/InputStream/read
  move-result v0
  :try_end_0
  return v0
  :handler_0
  move-exception v0
  const/4 v0,15
  goto :try_end_0
.end method
```

Exercise 6: Reverse Engineering

(3) Choose any Android application from the Google Play store, download and disassemble it. Analyze (and possibly modify) the SMALI bytecode in order to achieve a particular goal. If your goal requires code modification, re-package the APK and run it on an Android system. Interesting goals include, but are not limited to:

- Removing ad banners
- Transforming a "free" to a "paid" application (for research purposes only)
- Bypass authentication,
- Analyze code in order to understand authentication, credential storage,
- etc.

Fully describe your goal and the exact process what you did, what you found, what problems you faced, etc. Note that some companies may have explicitely used code obfuscation techniques (e.g. non-human-readable class/method names) - you may have to test a few apps.

(4) Solve enough SMS-CTF levels (from the pool 06 to 19), to achieve a total of at least **9 stars** with regard to the level's difficulty rating. You can choose the particular levels yourself, but do not forget to explititely refer to them in your submission! Hand in a step-by-step walkthrough how each level can be solved using your solution.