Tiefenbohrung

Decompilieren von Android-Applikationen mit Java-Mitteln

Thomas Ronzon

Haben Sie schon einmal das Bedürfnis gehabt, sich eine Android-Applikation, aus welchen Gründen auch immer, ein wenig näher anzusehen, ohne den Quellcode zu haben? Nichts leichter als das!

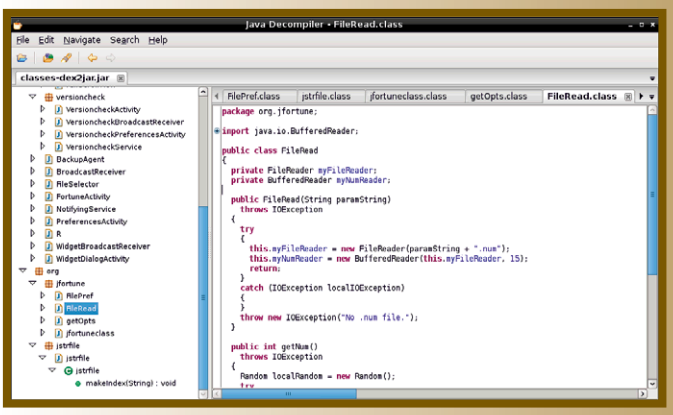

Abb1: Screeenshot JD-GUI

Wie Sie wissen, werden Android-Applikationen in Java geschrieben. Allerdings werden diese nach der Compilierung in einen speziellen Bytecode übersetzt, welcher dann von der Dalvik VM [DVM] ausgeführt werden kann. Wenn man nun diese Umsetzung des Bytecodes wieder so rückgängig macht, dass Bytecode im Format der Java VM [JVM] entsteht, kann man diesen mit bekannten Decompilern wieder einsehen. Doch der Reihe nach.

Nehmen wir einmal an, dass Sie eine Android-Applikation als apk-Datei vorliegen haben. Als Beispiel verwende ich hier eine Applikation, welche den unter Unix bekannten Sprücheklopfer „Fortune“ [Fortune] für Android zur Verfügung stellt. Laden Sie einmal die apk-Datei hier herunter [Download]. Ein

```
ronzon@star:~/Downloads> file AndroidsFortune-1.1.8-for-1.5.apk
```

ergibt

```
AndroidsFortune-1.1.8-for-1.5.apk: Zip archive data, at least v1.0 to
  extract Java Jar file data (zip)
```

Aha, also eine Jar-Datei, welche ich mit

```
ronzon@star:~/Downloads/Fortune>
  jar xvf AndroidsFortune-1.1.8-for-1.5.apk
```

entpacken kann. Neben den Grafiken und ein paar xml-Dateien findet sich hier auch die Datei **./classes.dex**

```
ronzon@star:~/Downloads/Fortune> file classes.dex
classes.dex: Dalvik dex file version 035
```

In dieser Datei wird der Bytecode der Dalvik VM gespeichert. Unter [DEX] finden Sie die genaue Dateispezifikation des Dalvik Executable Format.

Ich jedoch finde es viel zu umständlich, diese Datei selbst zu zerlegen. Hier hilft uns das Tool *dex2jar* weiter, welches Sie unter [Dex2Jar] herunterladen können. Nach dem Entpacken genügt der Aufruf

```
ronzon@star:~/Downloads/Fortune> d2j-dex2jar.sh classes.dex
dex2jar classes.dex -> classes-dex2jar.jar
```

Und schon haben wir eine jar-Datei. Möchte ich diese nun schnell analysieren, verwende ich gerne *jd-gui*, welcher native für verschiedene Betriebssysteme unter [JDGUI] heruntergeladen werden kann. Anschließend genügt ein

```
ronzon@star:~/Downloads> ./jd-gui Fortune/classes-dex2jar.jar
```

und ich kann in aller Ruhe die Quellen analysieren. Es ist schon erstaunlich, wie gut der Code in Abbildung 1 lesbar ist.

Fazit: Nicht immer müssen es spezielle Android-Tools sein, um im Android-Umfeld arbeiten zu können. Mit etwas Kreativität kann man eine Menge der gewohnten Tools weiterverwenden.

Links

[DEX] `http://source.android.com/devices/tech/dalvik/dex-format.html`
[Dex2Jar] `http://code.google.com/p/dex2jar/`
[Download] `https://launchpad.net/androidsfortune/+download`
[DVM] `http://de.wikipedia.org/wiki/Dalvik_Virtual_Machine`
[Fortune] `http://de.wikipedia.org/wiki/Fortune_(Computerprogramm)`
[JDGUI] `http://jd.benow.ca/`
[JVM] `http://de.wikipedia.org/wiki/Java_Virtual_Machine`

Thomas Ronzon ist seit mehr als zehn Jahren bei der w3logistics AG in Dortmund als Projektleiter bei diversen Logistik-Projekten beschäftigt.
E-Mail: ronzon@w3logistics.de