Automated Detection and Classification for Packed Android Applications

Yibin Liao, Jiakuan Li, Bo Li, Guodong Zhu, Yue Yin, Ruoyan Cai

Network System and Security (NSS) Lab
University of Georgia (UGA)
Goal

• Detection
  – Automatically identify packed Android apps

• Classification
  – Automatically classify different packers into different groups
How Android App is Built and Run

Java Source Code (.java)

Java Compiler

Java Bytecode (.class)

Dex Compiler

Dalvik Bytecode (.dex)

Dalvik Executable

Dalvik VM
Packed Android App

Java Source Code (.java)

Java Compiler

Java Bytecode (.class)

Dex Compiler

Dalvik Bytecode (.dex)

Hiding

Dalvik Executable

Dalvik VM
Current problems

• Packed Android Malware
• Manual effort for analysis
  – Tedious
• Packers are evolving.
  – Unpacking approaches only works for a limited time, or particular type of packers.
Current packing techniques

- Code obfuscation
- Anti-debugging
- Bytecode hiding
- Dynamic code modification
- Dynamic loading
Our approach

Detection
• Combined Static and Dynamic analysis
  – Static
    • Static analysis tools (baksmali)
  – Dynamic
    • DVM instrumentation
  – Compare classes from static and dynamic analysis

Classification
• Runtime environment monitoring to capture the execution behavior pattern
  – System calls
    • Kernel modules
  – IPC transaction
    • Binder trace
  – Native-to-Java interaction
    • JNI trace
Overview

Detection Module

- Android Apps
  - Instrumented DVM
    - Dynamic Analysis
  - Baksmali
    - Smali files
    - Static Analysis

Comparer

- Classes

Classification Module

- Packed Apps
  - Packed Apps Set 1
  - Packed Apps Set 2
  - Packed Apps Set 3
  - Packed Apps Set N

- System Call Monitor
- Native-to-Java Monitor
- Binder Transaction Monitor

Classifier

Behavior Patterns
Overview

Detection Module

Instrumented DVM

Baksmali

Static Analysis

Dynamic Analysis

Comparer

Classes

Packed Apps

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Classification Module

Android Apps

Overview

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3...

Packed Apps Set N
Overview

Detection Module

Instrumented DVM

Baksmali

Static Analysis

Dynamic Analysis

Classes

Comparer

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Classification Module

Android Apps

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

Packed Apps Set N
Overview

Android Apps → Detection Module

Dynamic Analysis

Instrumented DVM → Classes

Baksmali → Smali files → Classes

Static Analysis

Comparer

Packed Apps

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Detection Module

Classification Module

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

Packed Apps Set N
Overview

- **Dynamic Analysis**
  - Instrumented DVM
  - Baksmali
  - Smali files
  - Classes

- **Static Analysis**
  - Classes

- **Detection Module**
  - System Call Monitor
  - Native-to-Java Monitor
  - Binder Transaction Monitor

- **Classification Module**
  - Behavior Patterns
  - Classifier

- **Packed Apps**
  - Set 1
  - Set 2
  - Set 3
  - ...
Overview

Dynamic Analysis

Instrumented DVM

Static Analysis

Baksmali

Smali files

Classes

Detection Module

Comparer

Packed Apps

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Classification Module

Detection Module

Classification Module

Android Apps

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

Packed Apps Set N
Overview

Detection Module

Detection of packed apps

Static Analysis

Baksmali

Smali files

Classes

Dynamic Analysis

Instrumented DVM

Classes

Comparer

Packed Apps

Classification Module

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

Packed Apps Set N
Overview

Android Apps

Detection Module

Instrumented DVM

Baksmali

Static Analysis

Dynamic Analysis

Smali files

Comparer

Packed Apps

Classes

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Classification Module

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

Packed Apps Set N
Overview

Detection Module

- Android Apps
  - Instrumented DVM
  - Baksmali

Comparer

- Dynamic Analysis
- Static Analysis

Classification Module

- Packed Apps
  - Set 1
  - Set 2
  - ...,
  - Set N

- Detected Classes
- Detected Smali Files

- System Call Monitor
- Native-to-Java Monitor
- Binder Transaction Monitor

Behavior Patterns

Classifier
Overview

Detection Module

Android Apps

- Instrumented DVM
- Baksmali

Static Analysis

Dynamic Analysis

Comparer

Packed Apps

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Classifier

Behavior Patterns

Classification Module

Packed Apps Set 1

Packed Apps Set 2

...
Overview

Android Apps

Detection Module

- Instrumented DVM
  - Dynamic Analysis
  - Classes

- Baksmali
  - Static Analysis
  - Small files
  - Classes

Comparer

Packed Apps

Classification Module

- System Call Monitor
- Native-to-Java Monitor
- Binder Transaction Monitor
  - Behavior Patterns
  - Classifier

Packed Apps Set 1
Packed Apps Set 2
Packed Apps Set 3
Packed Apps Set N
Overview

Detection Module

Android Apps

Instrumented DVM

Dynamic Analysis

Baksmali

Smali files

Static Analysis

Classes

Comparer

Packed Apps

Classification Module

System Call Monitor

Native-to-Java Monitor

Binder Transaction Monitor

Behavior Patterns

Classifier

Packed Apps Set 1

Packed Apps Set 2

Packed Apps Set 3

...
VM instrumentation (DVM)

- Unzip apk -> dex files
- Open and read dex file
- Initialize Classes
- Load classes

Insert codes to capture the class information (names, methods, fields, etc.)
Conclusion

• Implemented a detection module to identify packed Android Apps
• Proposed approaches to extract the execution behavior from different packers
Thank you

QA?