Android Malware Analysis and Detection

Analysis

- Static Analysis
  - Automated static analysis system
  - Manual static analysis
- Dynamic Analysis
  - Sandbox
  - Taint
  - Manual Dynamic Analysis

Detection

- ES DB
- CRC
- AI

Static Analysis

Automated static analysis system

Step1. Dex2Smali

Step2. Set the SDK whitelist

Step3. Custom malicious code rules

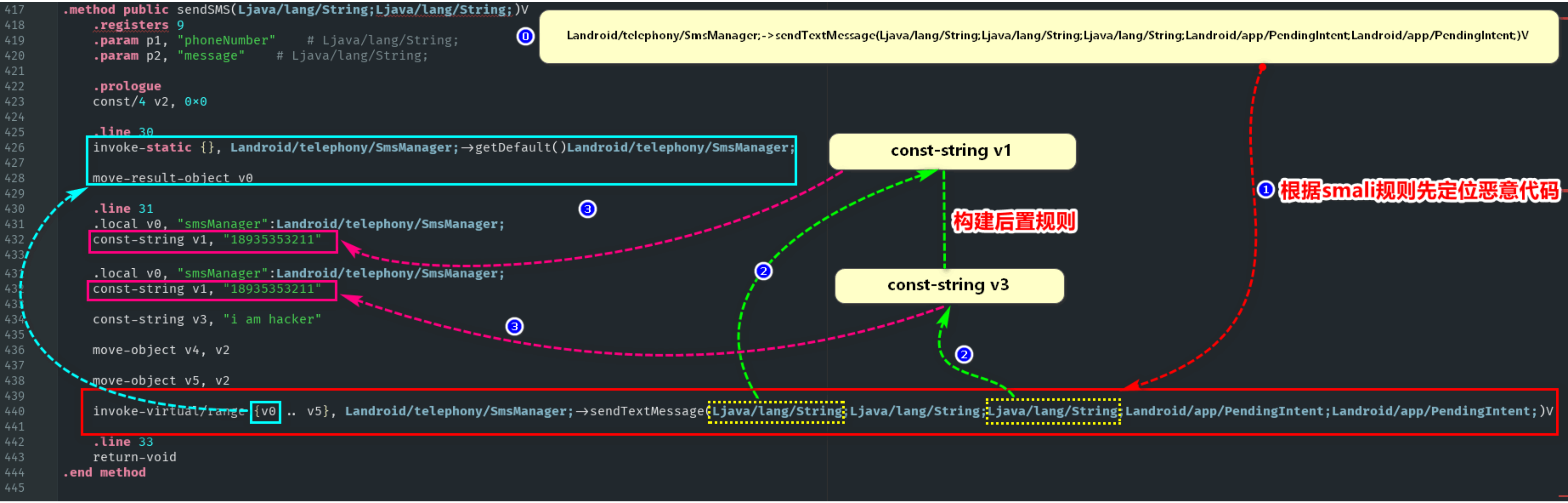
Step4. Scan

Q: How to dex2smali?
A: apktool, etc…

Q: Why do we need sdk whitelist?
A: Quick scan and Reduce false positives

Q: What is the rule format ?
A: Smali code and Regular expression

E.g

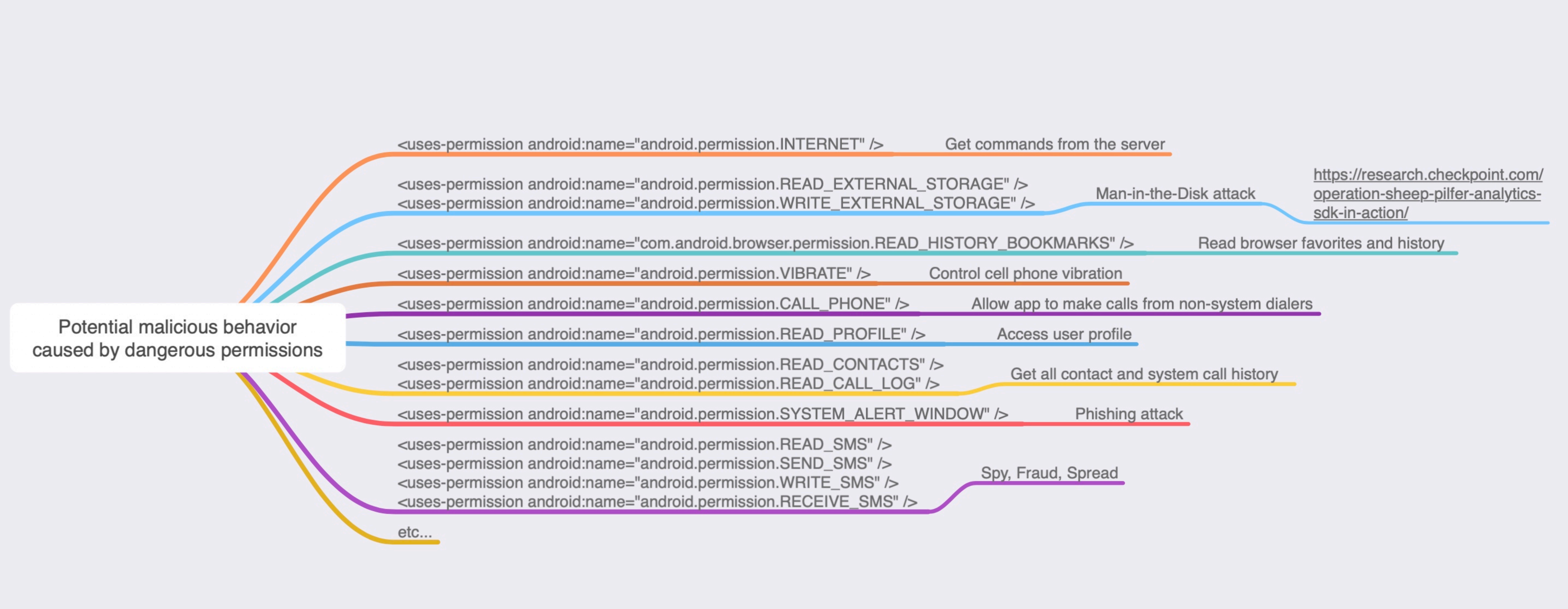


```
.method public sendSMS(Ljava/lang/String;Ljava/lang/String;)V
    .registers 9
    .param p1, "phoneNumber"    # Ljava/lang/String;
    .param p2, "message"    # Ljava/lang/String;

    .prologue
    const/4 v2, 0×0

    .line 30
    invoke-static {}, Landroid/telephony/SmsManager;→getDefault()Landroid/telephony/SmsManager;

    move-result-object v0

    .line 31
    .local v0, "smsManager":Landroid/telephony/SmsManager;
    const-string v1, "18935353211"

    .local v0, "smsManager":Landroid/telephony/SmsManager;
    const-string v1, "18935353211"

    const-string v3, "i am hacker"

    move-object v4, v2

    move-object v5, v2

    invoke-virtual/range {v0 .. v5}, Landroid/telephony/SmsManager;→sendTextMessage(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Landroid/app/PendingIntent;Landroid/app/PendingIntent;)V

    .line 33
    return-void
.end method
```

```
Landroid/telephony/SmsManager;->sendTextMessage(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Landroid/app/PendingIntent;Landroid/app/PendingIntent;)V
```

Manual Static Analysis

- Tools
  - JEB
  - IDA
  - R2
  - Hopper
  - Jadx
  - Charles
  - Other
- Skill
  - Get malicious code location based on permissions



Potential malicious behavior caused by dangerous permissions

<uses-permission android:name="android.permission.INTERNET" /> Get commands from the server

<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" /> Man-in-the-Disk attack https://research.checkpoint.com/operation-sheep-pilfer-analytics-sdk-in-action/

<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" /> Read browser favorites and history

<uses-permission android:name="android.permission.VIBRATE" /> Control cell phone vibration

<uses-permission android:name="android.permission.CALL_PHONE" /> Allow app to make calls from non-system dialers

<uses-permission android:name="android.permission.READ_PROFILE" /> Access user profile

<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.READ_CALL_LOG" /> Get all contact and system call history

<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" /> Phishing attack

<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" /> Spy, Fraud, Spread

etc...

  - Get malicious code location based on intent
  - Get malicious code location based on string
  - Other

Permissions

android.permission.RESTART_PACKAGES
android.permission.WRITE_APN_SETTINGS
android.permission.ACCESS_NETWORK_STATE
android.permission.WRITE_SETTINGS
android.permission.READ_CALL_LOG
android.permission.INSTALL_PACKAGES
android.permission.RECEIVE_SMS
android.permission.WRITE_CONTACTS
android.permission.CHANGE_WIFI_STATE
android.permission.WRITE_SMS_VIBRATE
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_HISTORY_BOOKMARKS
android.permission.ACCESS_LOCATION
android.permission.WRITE_CONTACTSWRITE_CONTACTS
android.permission.ADD_SYSTEM_SERVICE
android.permission.RECEIVE_BOOT_COMPLETED

android.permission.WRITE_CALL_LOG
android.permission.EXTRA_COMMANDS
android.permission.WAKE_LOCK
android.permission.READ_PHONE_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.READ_SMS
android.permission.GET_TASKS
android.permission.SET_WALLPAPER
android.permission.CAMERA
android.permission.GET_ACCOUNTS
android.permission.SEND_SMS
android.permission.ACCESS_COARSE_LOCATION
android.permission.SYSTEM_ALERT_WINDOW
android.permission.CHANGE_NETWORK_STATE
android.permission.DEVICE_POWER
android.permission.DISABLE_KEYGUARD

Q & A