ANALYSIS OF SANDBOX-EVADING MALWARE IN ANDROID

Nicolas Biojo, David Erazo,
Daniela Llano, Sara Ortiz Drada

OBJETIVOS

O1.

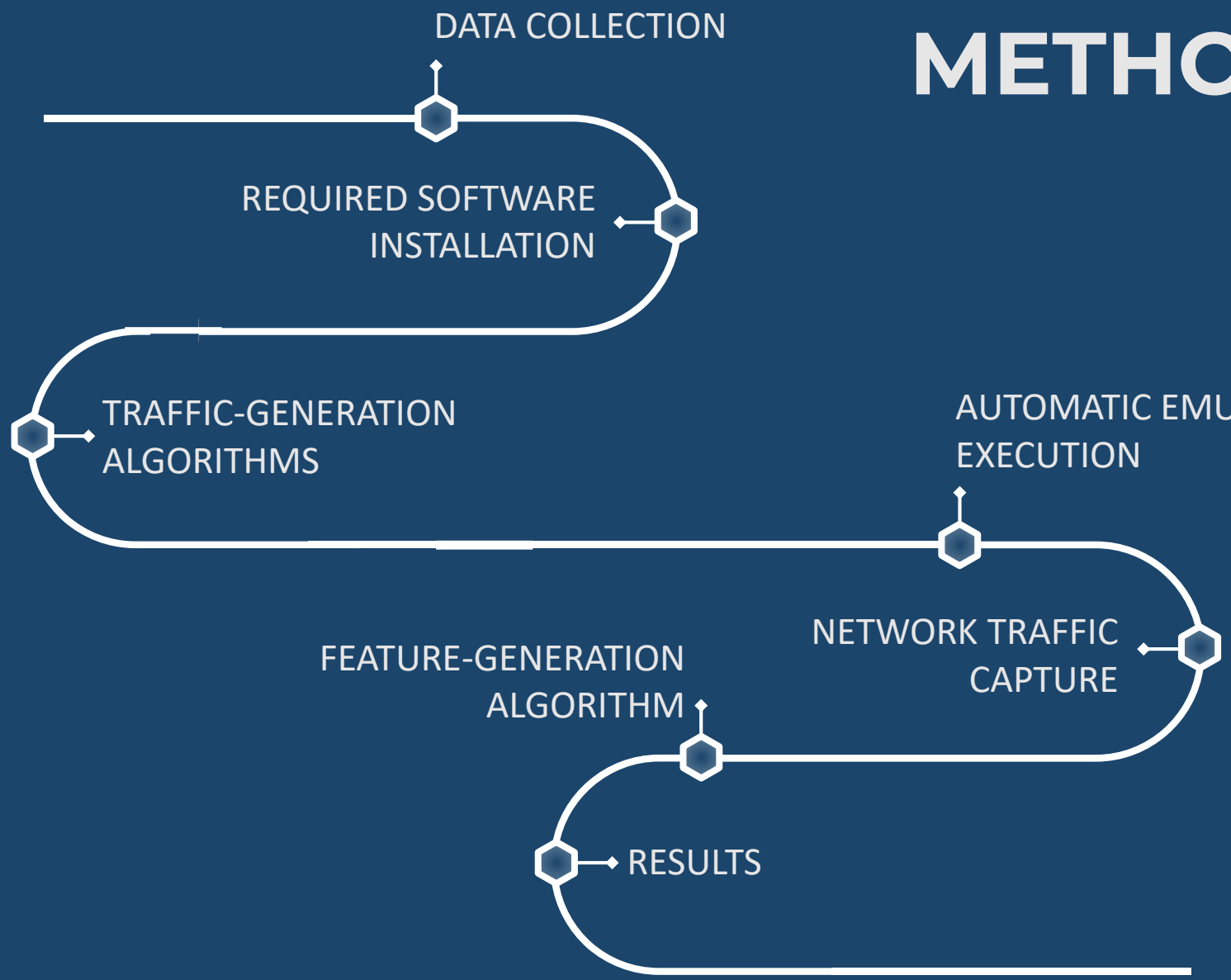
Determinar las características de un data ser de malware que tiene la capacidad de detectar que está siendo emulado en un entorno virtual a través de el análisis estático y dinámico.

O2.

Verificar si las magnitudes de los permisos más comunes usados por los diferentes malwares también se conservan en otro conjunto de datos.

DYNAMIC ANALYSIS

METHODOLOGY



KOODOUS

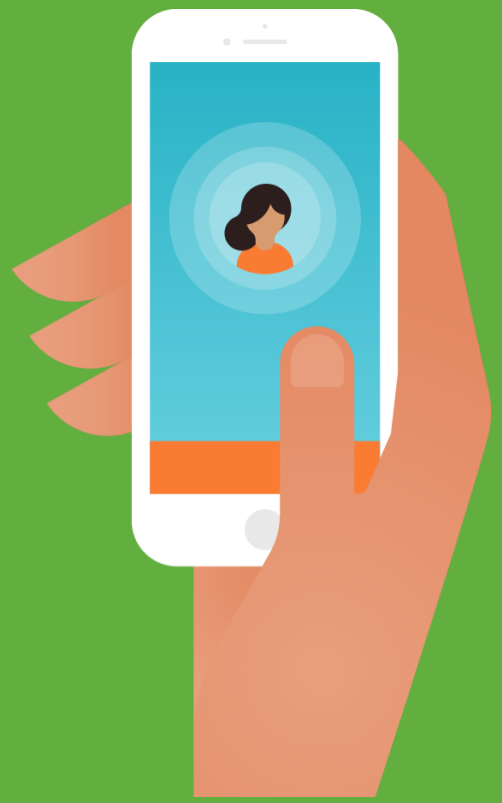
Collection of APK's from the Koodous repository (Trojan malware)

Android Studio

Software installation

ubuntu

Algorithms execution: Traffic generator



1

`eliminarPaquetes.py`

2

File .txt with paths of the APK's

3

`instalacionApp.py`

4

Random actions (touch down, touch up)

5

Network protocol analyzer

`While monekeyR.py`

NETWORK LAYER ANALYSIS

TCP exchange

Counts the number of TCP packets sent and received during communication.

Different TCP packets

Is the total number of packages that have ports other than those exposed in TCP.

Remote IP's

Represents the number of external IP addresses to which the application communicated.

App bytes

Is the number of bytes sent from the application to external sites.

UDP packets

Total number of UDP packets transferred in the communication.

Source app packets

It is the number of packets sent from the application to a remote server.

Remote app packets

Number of packets received from sources external to the application.

Source app bytes

This is the volume (in bytes) of the communication between the application and the server

Remote app bytes

This is the volume (in bytes) of the data from the server to the emulator

DNS query times

Number of DNS queries.

NETWORK LAYER ANALYSIS

TCP exchange	Different TCP packets	Remote IP's	App bytes	UDP packets
195	189	8	62174	1
1634	1586	12	178615	1
268	231	11	80281	0
391	186	9	78967	0

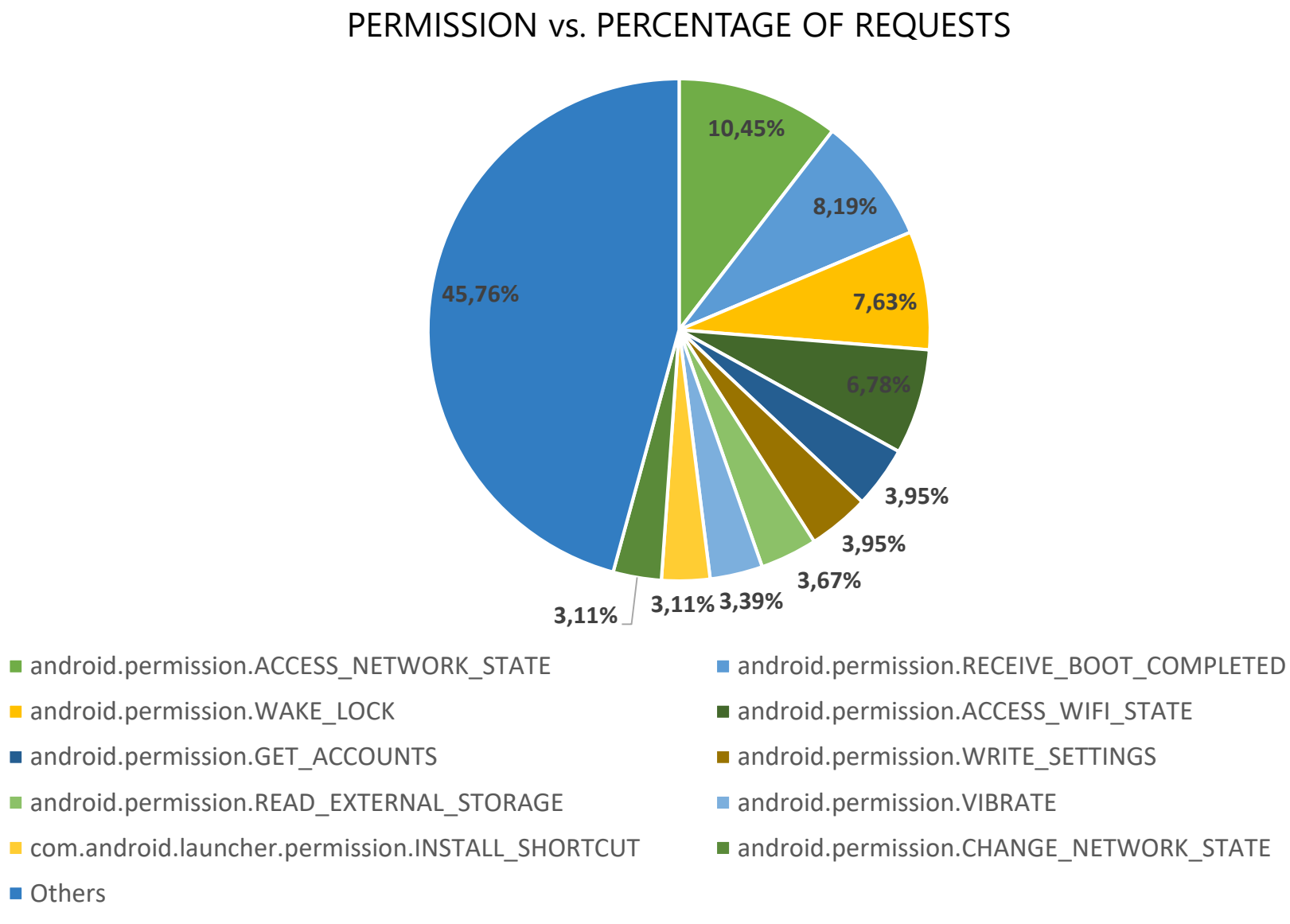
Source app packets	Remote app packets	Source app bytes	Remote app bytes	DNS query times
212	235	167632	63476	16
1656	3424	4745650	180281	21
290	318	194461	82045	22
409	533	409711	80403	18

STATIC ANALYSIS

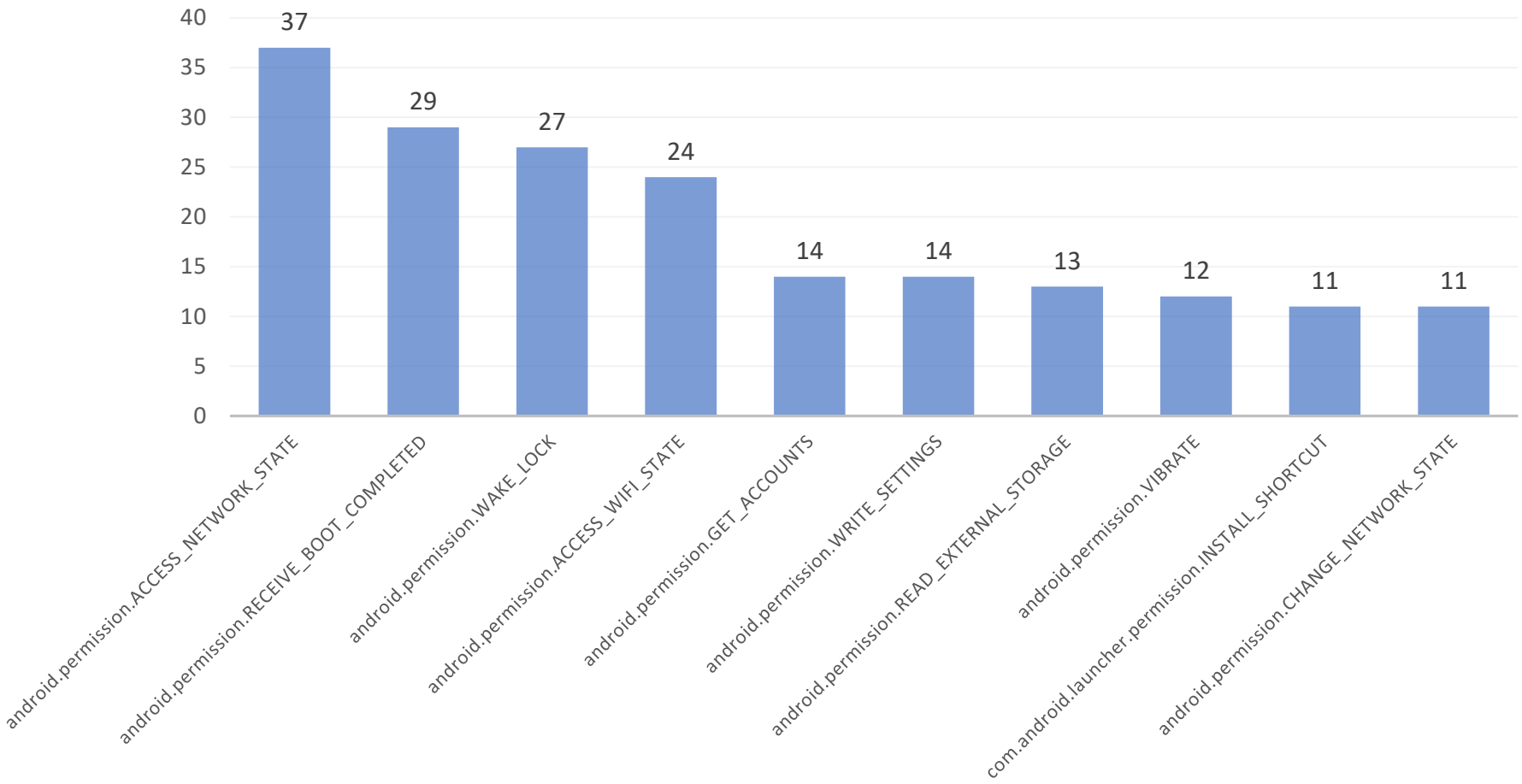
PERMISSIONS

ALLOWS AN APPLICATION TO VIEW THE STATUS OF ALL NETWORKS

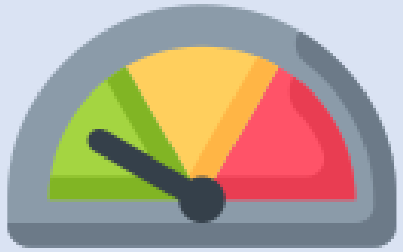
PERMISSIONS



PERMISSIONS

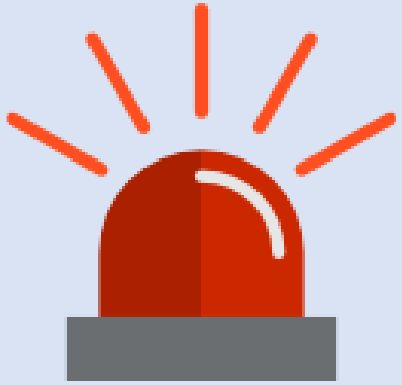


PROTECTION LEVELS



NORMAL

A lower-risk permission.
Gives requesting applications access to isolated application-level features, with minimal risk to other applications, the system, or the user.
Automatically permission at installation.



DANGEROUS

A higher-risk permission.
Gives the requesting application access to private user data or control over the device.

SIGNATURE

The requesting application is signed with the same certificate as the application that declared the permission.

PERMISSIONS

ACCESS_NETWORK_STATE

Allows applications to access information about networks.

RECEIVE_BOOT_COMPLETED

Allows an application to receive the Intent. ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.

WAKE_LOCK

Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.

ACCESS_WIFI_STATE

Allows applications to access information about Wi-Fi networks.

GET_ACCOUNTS

Allows access to the list of accounts in the Accounts Service.

PERMISSIONS

WRITE_SETTINGS

Allows an application to read or write the system settings.

READ_EXTERNAL_STORAGE

Allows an application to read from external storage.

VIBRATE

Allows access to the vibrator.

INSTALL_SHORTCUT

Allows an application to install a shortcut in Launcher.

CHANGE_NETWORK_STATE

Allows applications to change network connectivity state.

Malicious applications, in this case Trojans, have greater access to the following features:

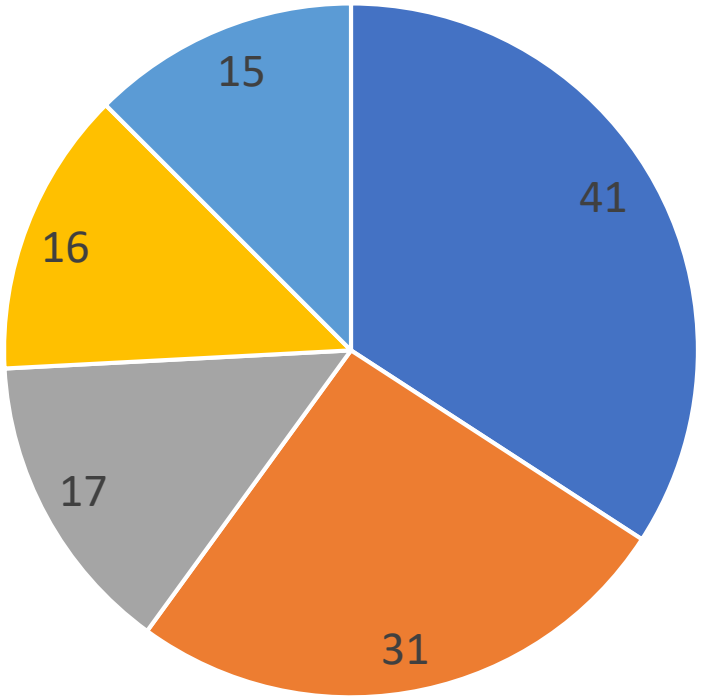
	DREBIN	Features to Detect Android Malware*	OUR ANALYSIS
1. android.permission.INTERNET	96.1%	97.99%	70%
2. android.permission.READ_PHONE_STATE	89.1%	95.48%	63,33%
3. android.permission.ACCESS_NETWORK_STATE	65.7%	83.92%	61,7%
4. android.permission.WRITE_EXTERNAL_STORAGE	66.6%	68.34%	56,67%
5. android.permission.SEND_SMS	54.2%		55,00%

*

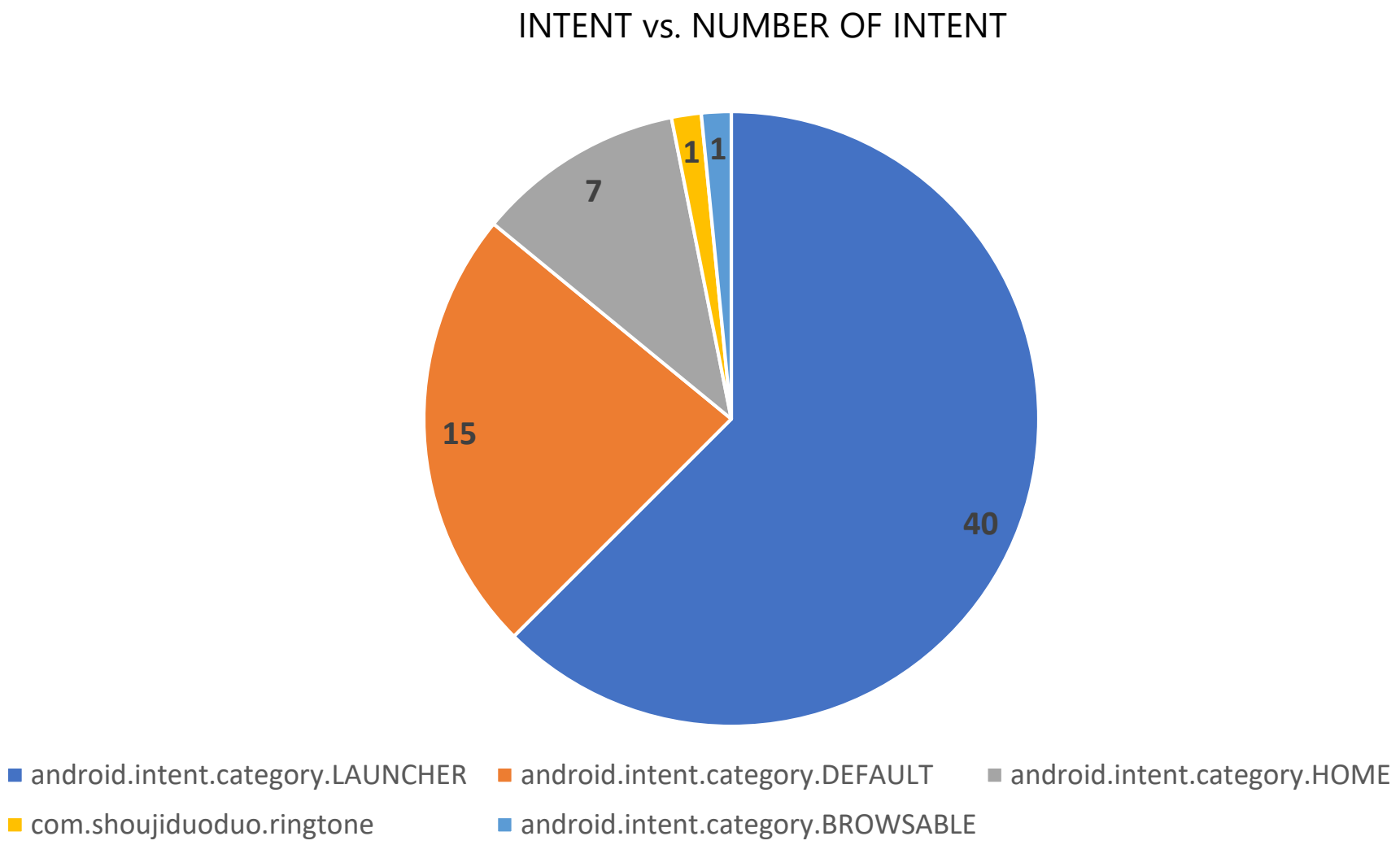
INTENTS

Is an abstract description of an **operation** to be performed.

BY ACTION


15
41
16
17
31
android.intent.action.MAIN
android.intent.action.BOOT_COMPLETED
android.provider.Telephony.SMS_RECEIVED
android.app.action.DEVICE_ADMIN_ENABLED
android.intent.action.USER_PRESENT

BY CATEGORY


INTENT vs. NUMBER OF INTENT
40
15
7
1
1
android.intent.category.LAUNCHER
android.intent.category.DEFAULT
android.intent.category.HOME
com.shoujiduoduo.ringtone
android.intent.category.BROWSABLE

Thank YOU!