Software Requirements Specification

Calculate Trust Value for Android Device

Feature Extraction in Installed Applications

<<Any comments inside double brackets such as these are *not* part of this SRS but are comments upon this SRS example to help the reader understand the point being made.

Refer to the SRS for details on the purpose and rules for each section of this document.

This work is based upon the submissions of Calculate Trust Value for Android Device project. The student who submitted this document is Chathuranga K.B.L. (IT13048624). >>

Table of Contents

1.0. Introduction

1.1. Purpose

The Internet of Things (IoT) is one of the new emerging technologies. The main limitation that might threaten the growth of IoT will be the difficulties in the Security. Since IoT is composed of various heterogeneous smart devices, the security vulnerabilities in IoT are very high because the number of malware that can affect will also be higher. Although there are many studies carried out on trust evaluation, normal trust evaluation methods will not serve due to the high diversity of the IoT devices. This paper state of a machine learning mechanism to determine the trust of the devices involved in IoT by looking at various aspects that indicate the presence of malware in a device which will ultimately diminish trust. The features we collect are based on Network Information, Application information, Operating System Information and User Information. By considering many parameters from these features, the overall trust of the device is determined. Our ultimate goal is to build a trust network by connecting devices with higher trust values, so that sensitive information can be exchanged through IoT. These computations will be done using a Machine Learning algorithm and we plan to present simulation results that support our work.

1.2. Glossary

Term	Definition
Android device	Message sender who wants to confirm that message receiver is a secured device to send sensitive information.
Target Android device	Message receiver
Google Android	
Google Play Store	

1.3. References

IEEE. *IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications.* IEEE Computer Society, 1998.

1.4. Overview of Document

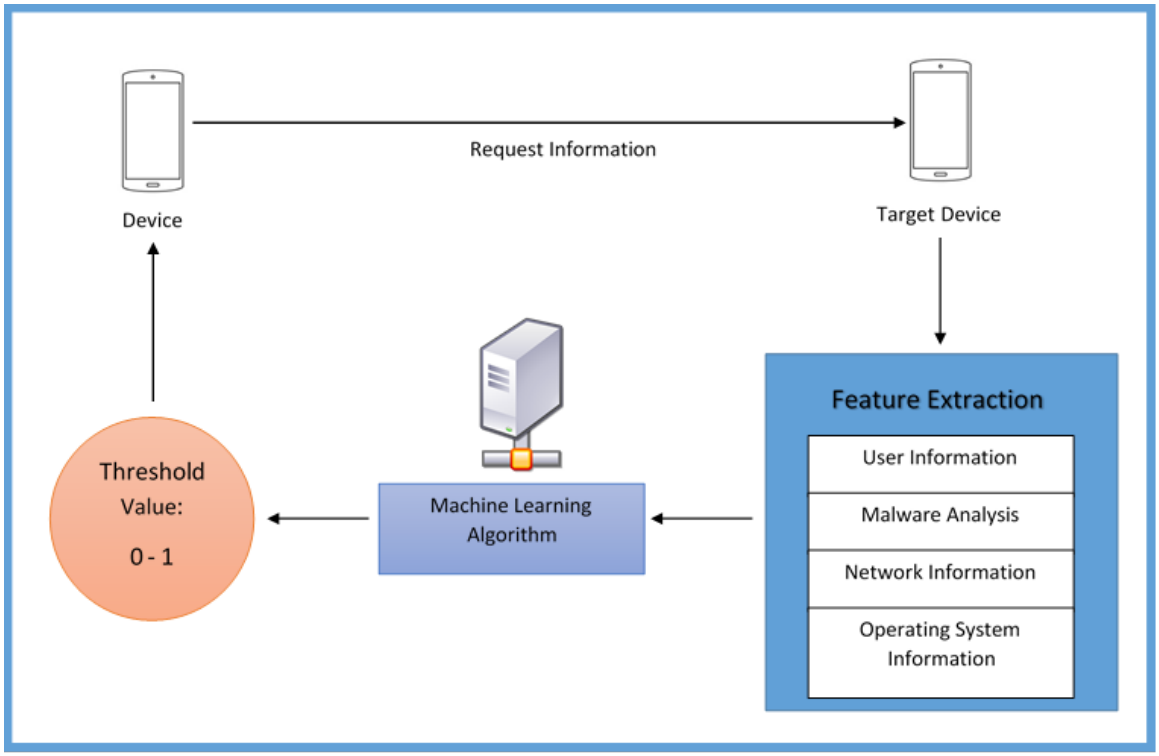
The next chapter, the Overall Description section, of this document gives an overview of the functionality of the product. It describes the informal requirements and is used to establish a context for the technical requirements specification in the next chapter.

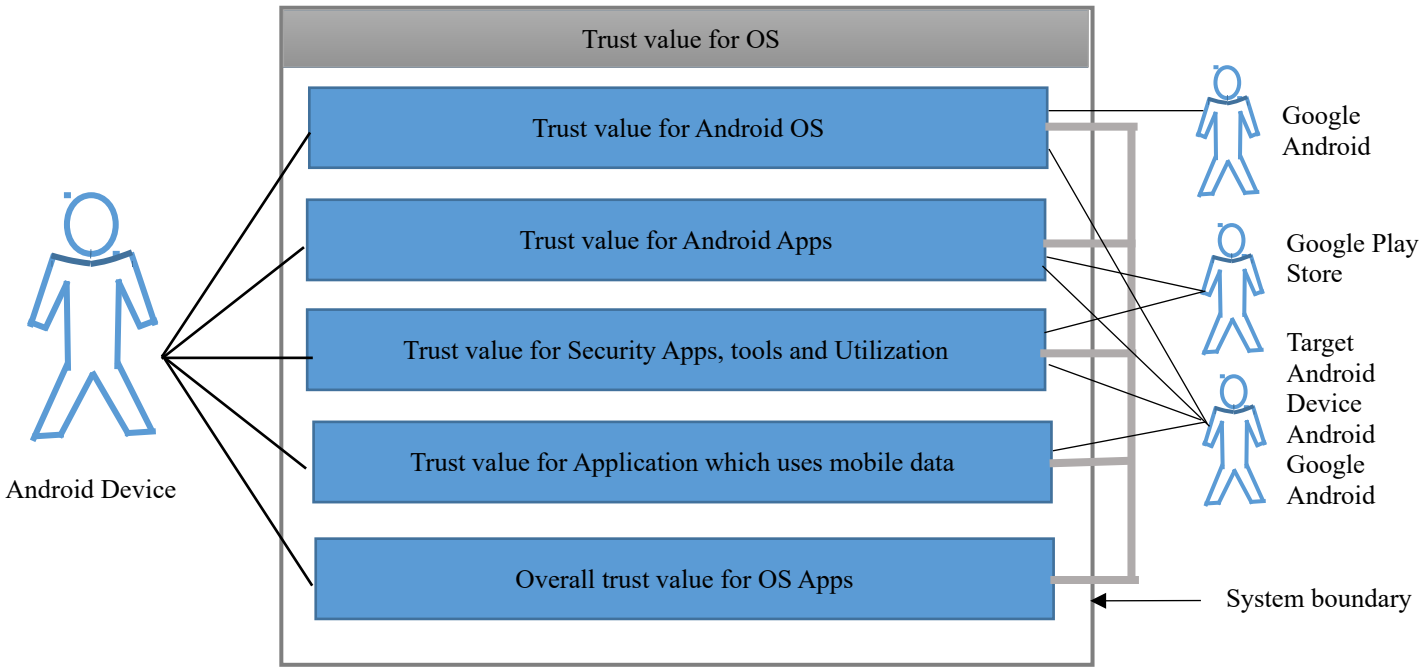
The third chapter, Requirements Specification section, of this document is written primarily for the developers and describes in technical terms the details of the functionality of the product.

Both sections of the document describe the same software product in its entirety, but are intended for different audiences and thus use different language.

2.0. Overall Description

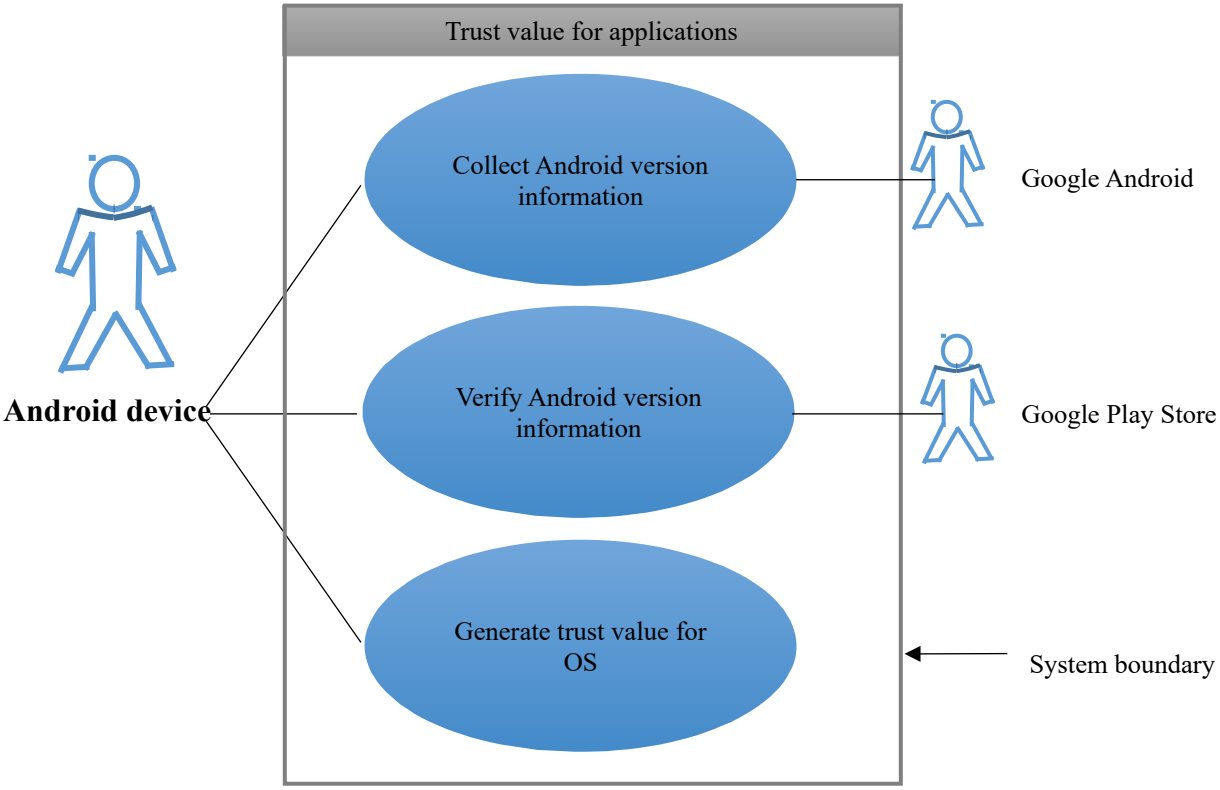
2.1 System Diagram





2.2 Functional Requirements Specification

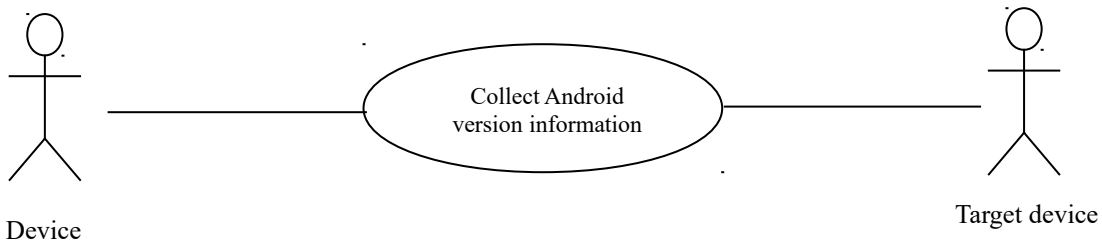
This section outlines the use cases for Android device separately. The target Android device, the Google Android and the Google Play Store have use cases while the Android is main actor in this system.



2.2.1 Android device Use Case

Use case: **Collect Android version information**

Diagram:



Brief Description
The Android device collects the Android operating system version information of the Target Android device. This information includes Android version, Security software version, Model number etc.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to collect the Android version information.

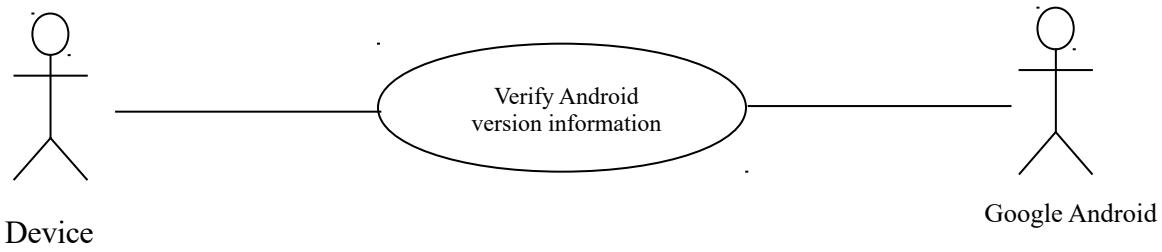
1. The Android device requests collect Android version information of the Target Android device.
2. The Target Android device sends the information to the system.
3. The System collects the Android version information from the Target Android device.
4. The System presents the Android version information of the Target Android device to the Android device.
5. The System checks the received information.
6. The System stores the Android version information for the comparison.

Xref: Section 3.2.1, Collect Android version information.

2.2.2 Android device Use Case

Use case: **Verify Android version information**

Diagram:



Brief Description
The System needs to confirm that the target Android device's OS is updated. The system collect information from Google Android which includes latest Android version, latest Security software version etc. for the particular target Android device model. Then system compares latest Android version and exiting Android version of the target Android device.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to verify the latest Android version information.

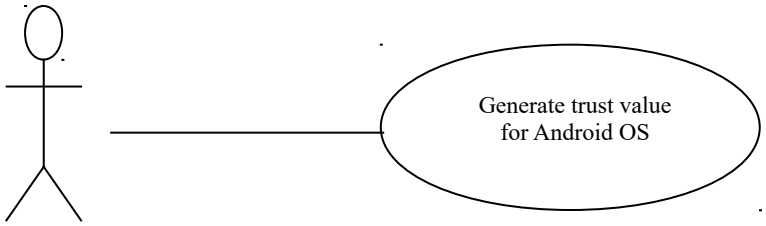
1. The Android device requests collect latest Android version information from Google Android.
2. The Google Android sends the related information to the system.
3. The System collects the latest Android version information from the Google Android.
4. The System compares latest Android version with stored Android version details such as
    a. Android version
    b. Baseband version
    c. Kernel version
    d. Security software version
5. The System generates a fraction after the comparison.

Xref: Section 3.2.2, **Verify Android version information**

2.2.3 Android device Use Case

Use case: **Generate trust value for Android OS**

Diagram:

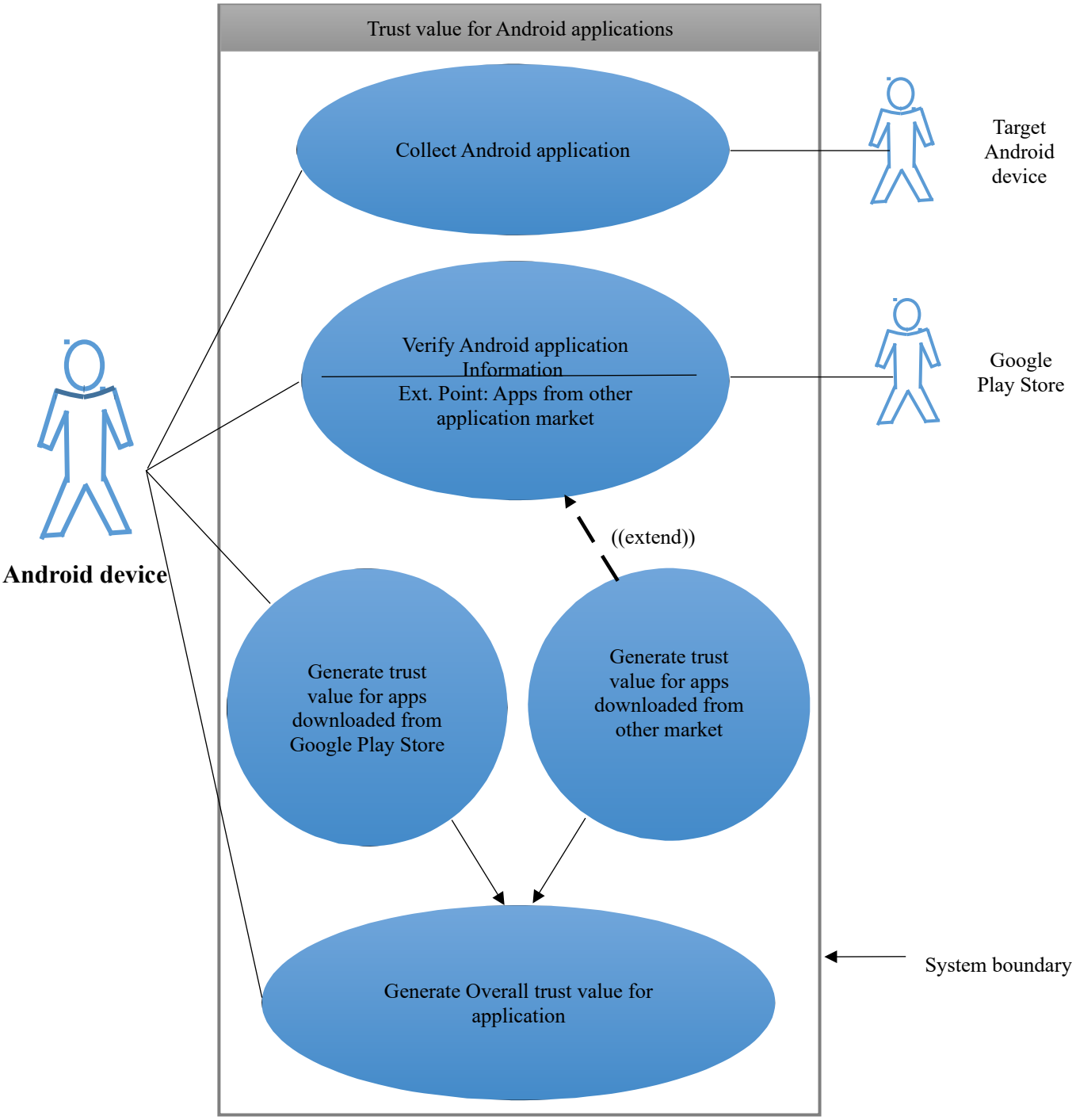


Brief Description
After the verification of the Android version details, the system will generate threshold value for the verification of Android OS.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate trust value.

1. The Android device requests to generate a threshold value for Android version.
2. The System converts the fraction into threshold value.
3. The System presents threshold value.

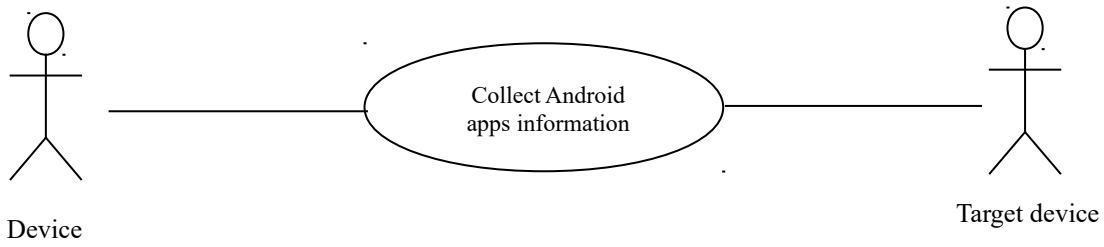
Xref: Section 3.2.3, Generate trust value for Android OS


Trust value for Android applications
Collect Android application
Verify Android application Information
Ext. Point: Apps from other application market
((extend))
Generate trust value for apps downloaded from Google Play Store
Generate trust value for apps downloaded from other market
Generate Overall trust value for application
Android device
Target Android device
Google Play Store
System boundary

2.2.4 Android device Use Cases

Use case: **Collect Android application information**

Diagram:



Brief Description
The System collects the Android application information which are installed in Target Android device. This information includes Application name, Application version, Access permissions etc.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to collect the Android application information.

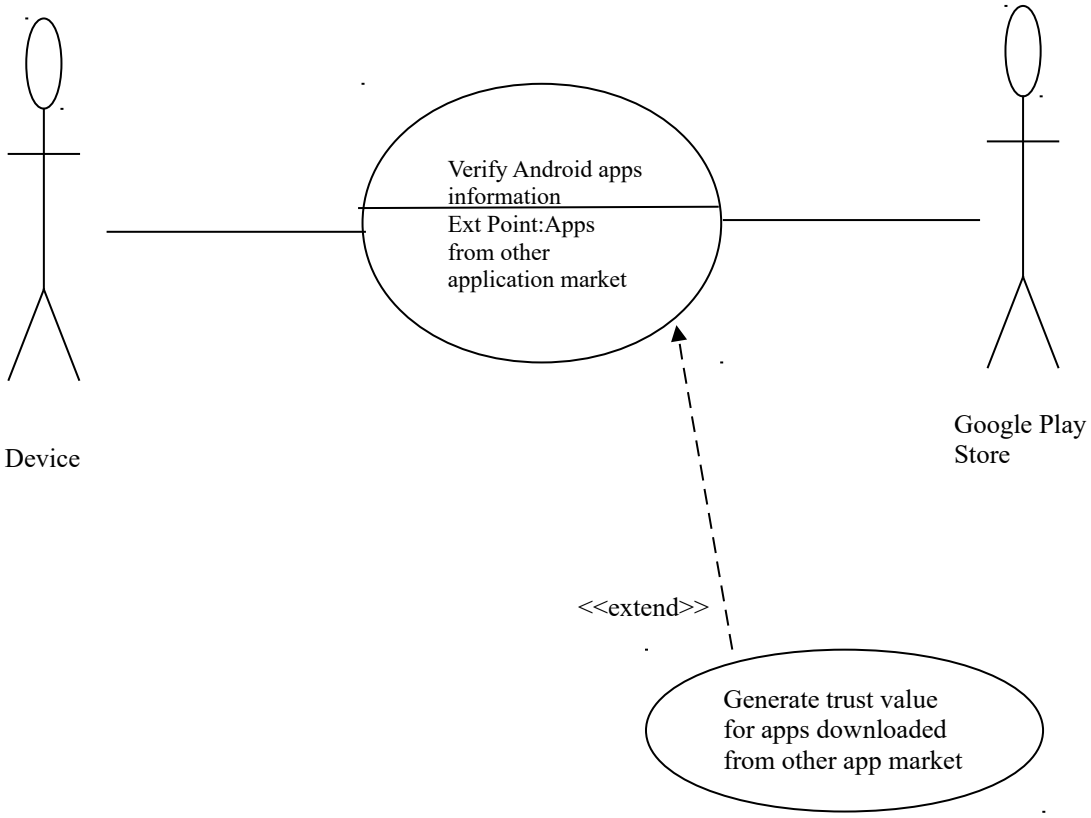
1. The Android device requests collect Android application information which are installed in Target Android device.
2. The Target Android device sends the information to the system.
3. The System collects the Android application information from the Target Android device.
4. The System presents the Android application information of the Target Android device to the Android device.
5. The System checks information.
6. The System stores the Android application information for the comparison.

Xref: Section 3.2.4, Collect Android application information.

2.2.5 Android device Use Cases

Use case: **Verify Android application information**

Diagram:



Brief Description
The System needs to confirm that the target Android device's applications are updated and not a malicious application. The System collects information of application from Google Play Store which includes application name, version, access permission etc. for the installed application on Target Android device. Then system compares application information with stored application information of the Target Android device.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to verify the Android application information.

1. The System differentiate applications which are downloaded from Google play Store and Other android application markets.
2. If the application downloaded from Google Play Store, Then

a. The System requests collect last version of Android application information from Google Play Store.
b. The Google Play Store sends the related information to the system.
c. The System collects the latest version of Android application information from the Google Play Store.
d. The System compares latest version of Android application with stored Android application information.
e. The System compares Android application version, number of installs, number of reviews, score, developer and permissions with the stored Android application information.
f. The System generates a fraction after the comparison.

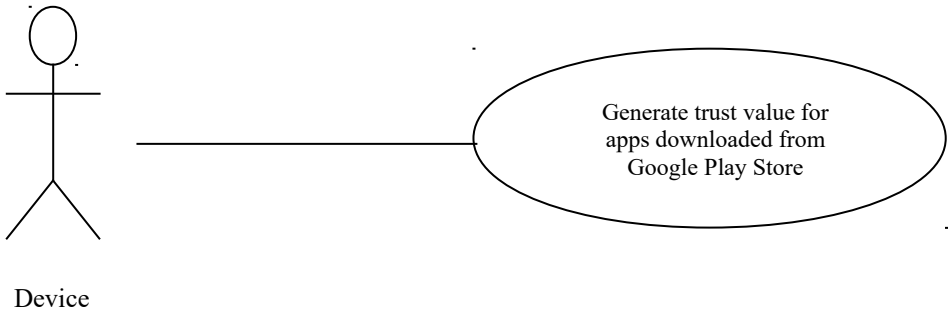
3. If the application downloaded from Other android application market, Then
    a. The System generates threshold trust value for applications.

Xref: Section 3.2.5, Verify Android application information.

2.2.6 Android device Use Cases

Use case: **Generate trust value for Android application downloaded from Google Play store**

Diagram:



Brief Description
After the verification of the Android application information which are downloaded from Google Play Store, the system will generate threshold value for the verification.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate the Android application information.

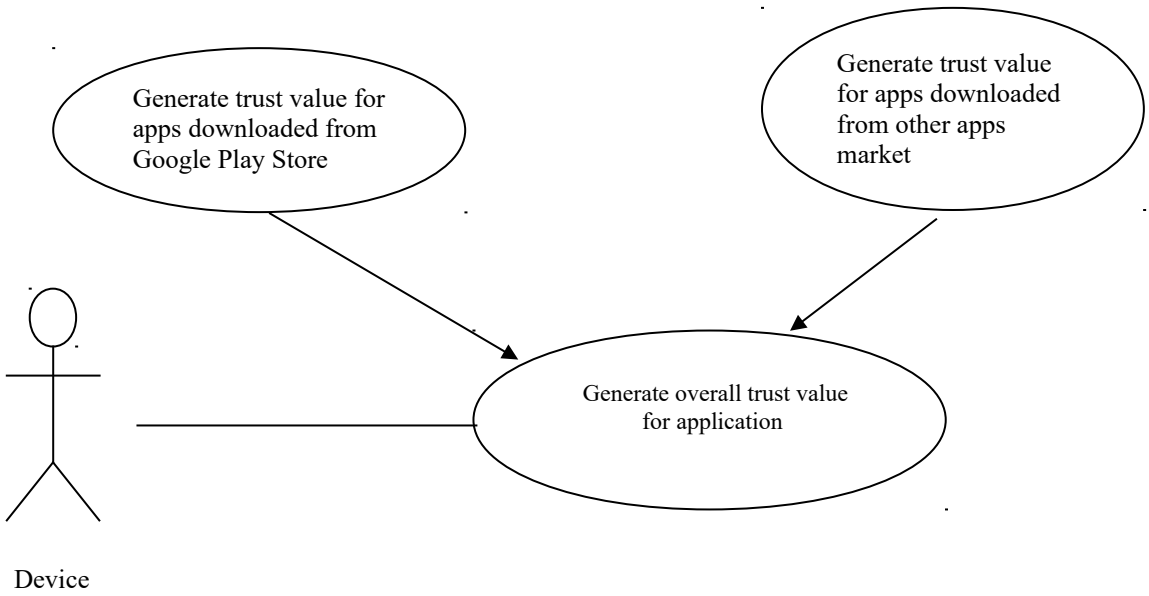
1. The Android device requests to generate a threshold value for Android applications which are installed in target Android device.
2. The System converts the fraction into threshold value.
3. The System presents threshold value.

Xref: Section 3.2.6, Generate trust value for Android application downloaded from Google Play Store

2.2.7 Android device Use Cases

Use case: **Generate overall trust value for Android application**

Diagram:

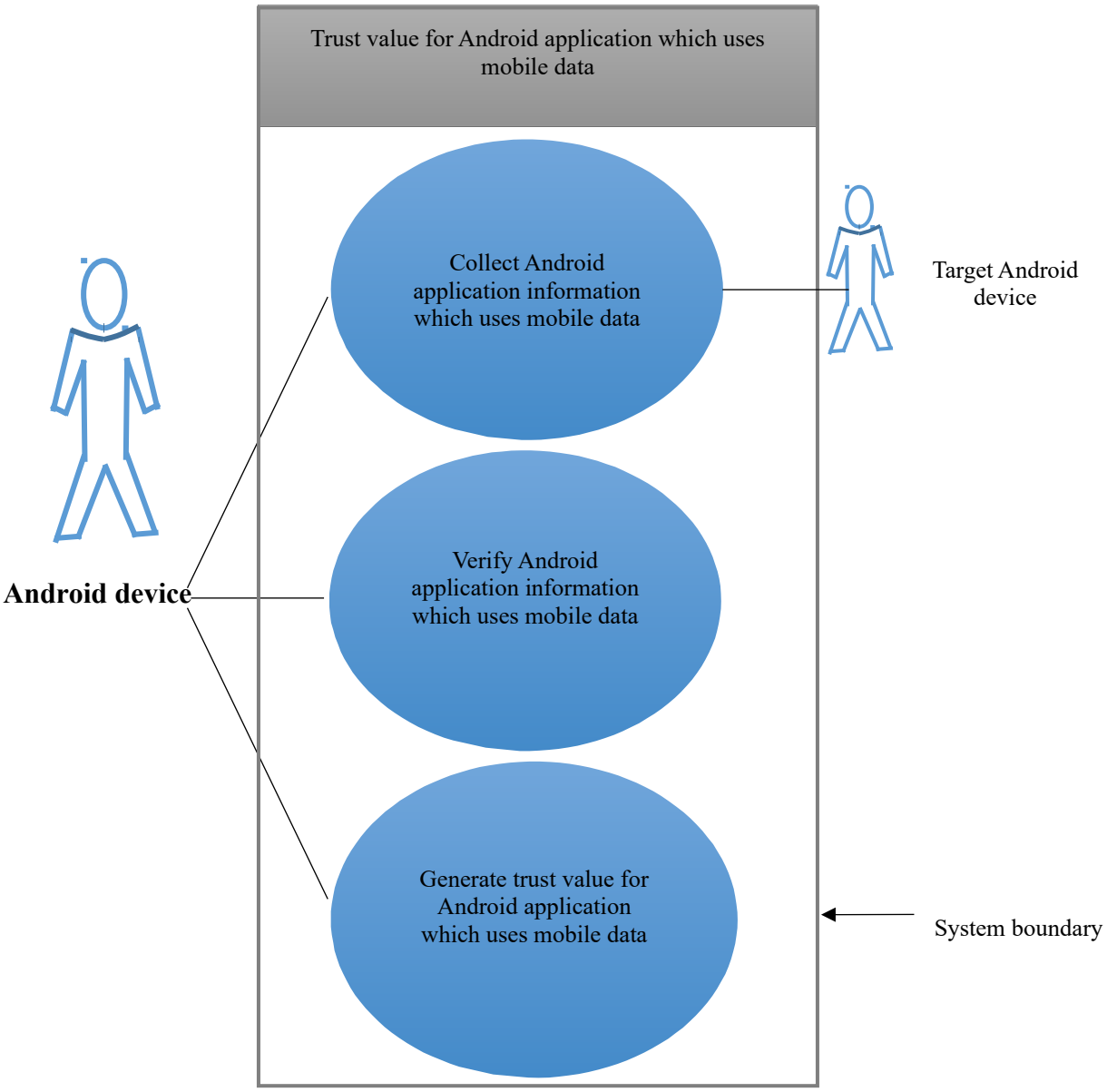


Brief Description
After the verification of the all Android application information, the system will generate overall threshold value for the all application.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate the Android application information.

1. The Android device requests to generate an overall threshold trust value for Android applications.
2. The System adds the each threshold value and converts it to single threshold trust value (0-1).
3. The System presents overall threshold value for application.

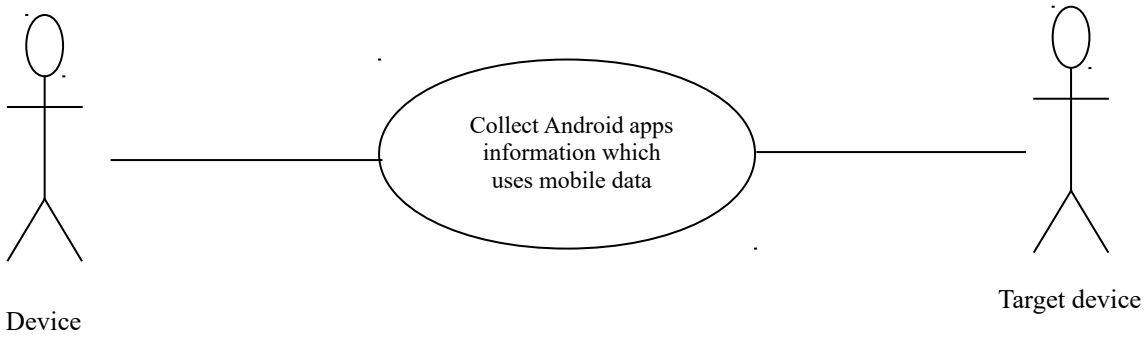
Xref: Section 3.2.7, Generate overall trust value for Android application


Trust value for Android application which uses mobile data
Collect Android application information which uses mobile data
Verify Android application information which uses mobile data
Generate trust value for Android application which uses mobile data
Android device
Target Android device
System boundary

2.2.8 Android device Use Cases

Use case: **Collect Android application information which uses mobile data**

Diagram:



Brief Description
The Android device collects the Android application information which uses mobile data for their function in Target Android device. This information includes Foreground mobile data usage and Background mobile data usage.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to collect the Android application information which uses mobile data.

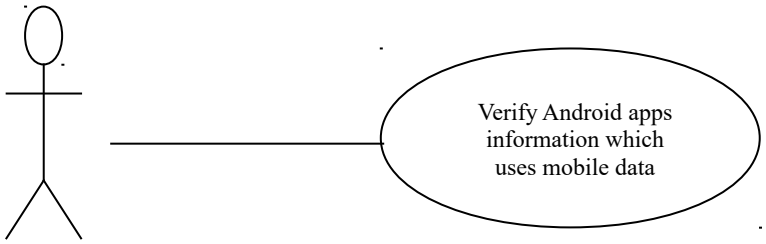
1. The Android device requests collect Android application information uses mobile data for their function in Target Android device.
2. The Target Android device sends the information to the system.
3. The System collects the Android application information from the Target Android device.
4. The System presents the Android application information of the Target Android device to the Android device.
5. The System checks information.
6. The System stores the Android application information for the comparison.

Xref: Section 3.2.8, Collect Android application information which uses mobile data.

2.2.9 Android device Use Cases

Use case: **Verify Android application information which uses mobile data**

Diagram:



Brief Description
The Android device needs to confirm that the target Android device doesn't have malicious application. The system verifies application's foreground mobile data usage and background mobile data usage. If the background mobile data usage is greater than foreground mobile data usage, the particular application may be malicious application.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to verify the Android application information which uses mobile data.

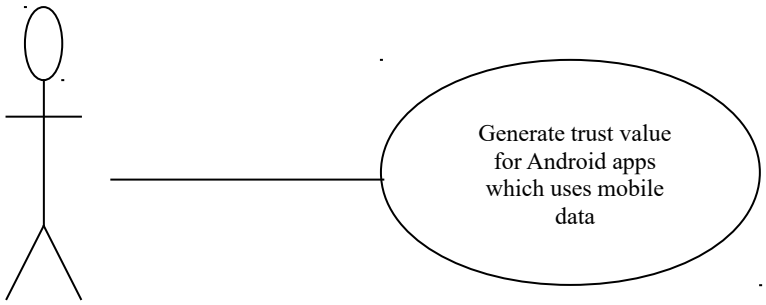
1. The Android device requests analyze mobile data usage of Android application which uses mobile.
2. The System compares the foreground mobile data usage and background mobile data usage of each application.
3. The System generates a fraction after the comparison.

Xref: Section 3.2.9, Verify Android application information which uses mobile data.

2.2.10 Android device Use Cases

Use case: **Generate trust value for Android application which uses mobile data**.

Diagram:

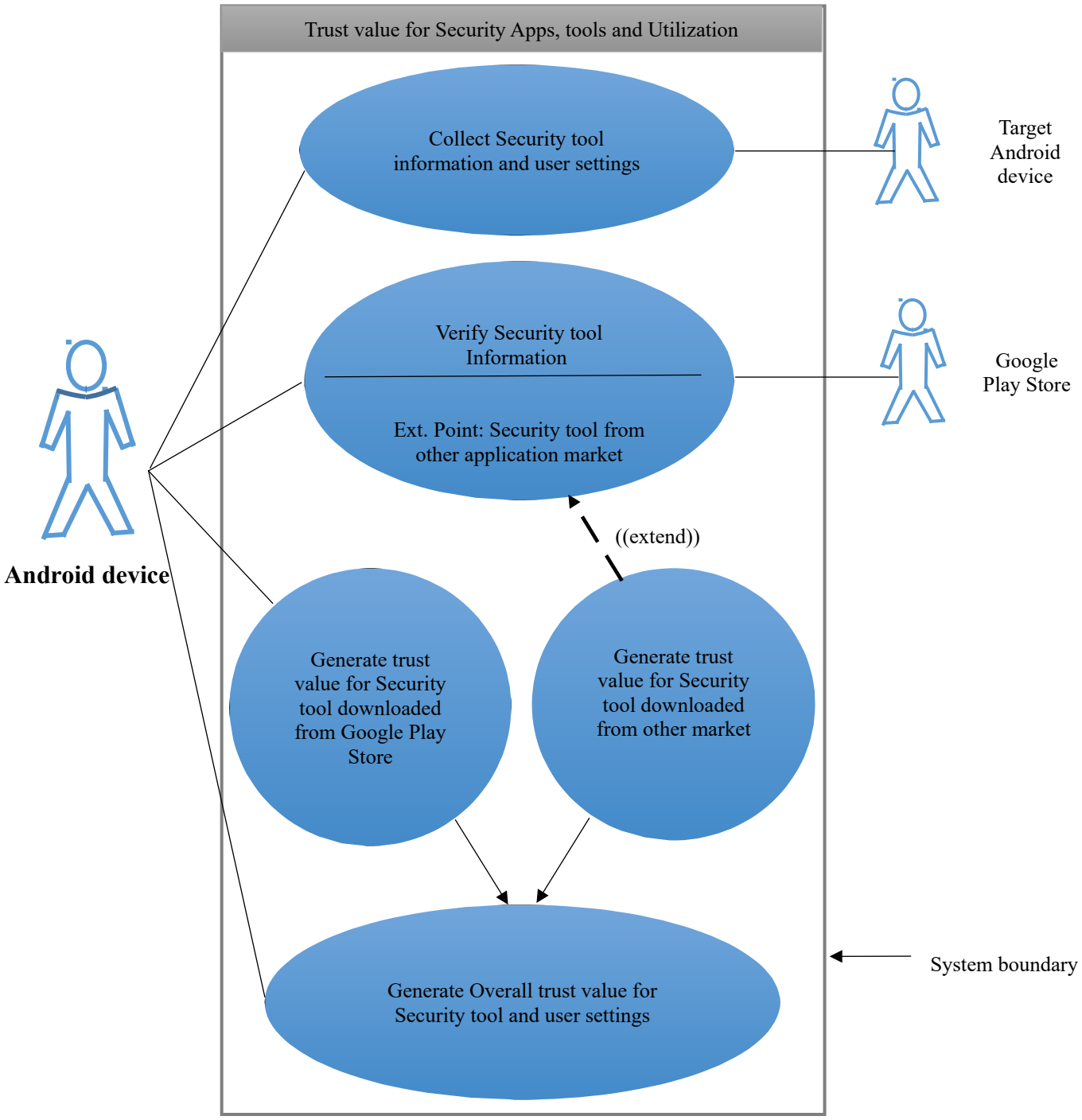


Brief Description
After the verification of the Android application's mobile data usage information, the system will generate threshold value for the verification.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate the Android application information which uses mobile data.

1. The Android device requests to generate a threshold value for Android applications which uses mobile data in their functions in target Android device.
2. The System converts the fraction into threshold value.
3. The System presents threshold value.

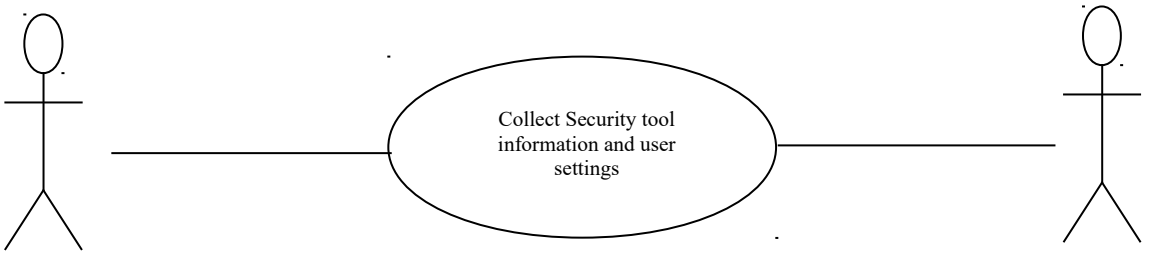
Xref: Section 3.2.10, Generate trust value for Android application which uses mobile data.


Trust value for Security Apps, tools and Utilization
Collect Security tool information and user settings
Verify Security tool Information
Ext. Point: Security tool from other application market
((extend))
Generate trust value for Security tool downloaded from Google Play Store
Generate trust value for Security tool downloaded from other market
Generate Overall trust value for Security tool and user settings
Android device
Target Android device
Google Play Store
System boundary

2.2.11 Android device Use Case

Use case: **Collect Security tool information and user settings.**

Diagram:



Brief Description
The Android device collects the Security tool information and the user settings of the Target Android device. The information includes Security tool name, how the security tool has been utilized on the target Android device.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to collect the Security tool information and user settings.

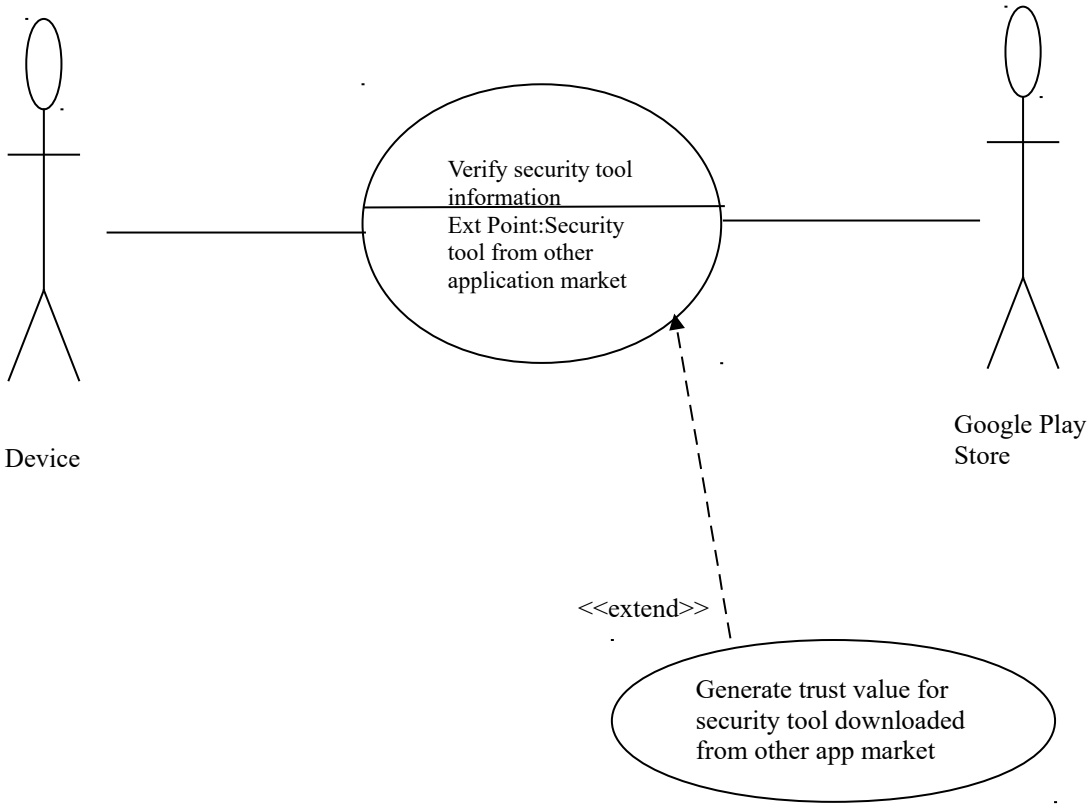
1. The Android device requests collect Security tools information and the user settings of the Target Android device.
2. The Target Android device sends the information to the system.
3. The System collects the Security tools information and the user settings from the Target Android device.
4. The System presents the Security tools information and the user settings of the Target Android device to the Android device.
5. The System checks information.
6. The System stores the Security tools information and the user settings for the comparison.

Xref: Section 3.2.11, Collect Security tool information and user settings.

2.2.12 Android device Use Cases

Use case: **Verify Security tool information**

Diagram:



Brief Description
The Android device needs to confirm that the target Android device is secured by Anti-virus tool. The system verifies security tool which is installed in Target android device and how the user utilized the security tool. If the target android device uses LookOut security tool and user enables every security option in the tool, it's a secured device to connect.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to verify the Security tool information and user settings.

1. The Android device requests verify Security tools information and the user settings of the Target Android device.
2. The System analyze security tools information.
3. If the Security tool downloaded from Google Play Store, Then

a. The Android device requests collect last version of Security tool information from Google Play Store.
b. The Google Play Store sends the related information to the system.
c. The System collects the latest version of Security tool information from the Google Play Store.
d. The System compares latest version of Security tool with stored Security tool information.
e. The System compares Security tool version, number of installs, number of reviews, score, developer and permissions with the stored Security tool information.
f. The System generates a fraction after the comparison.

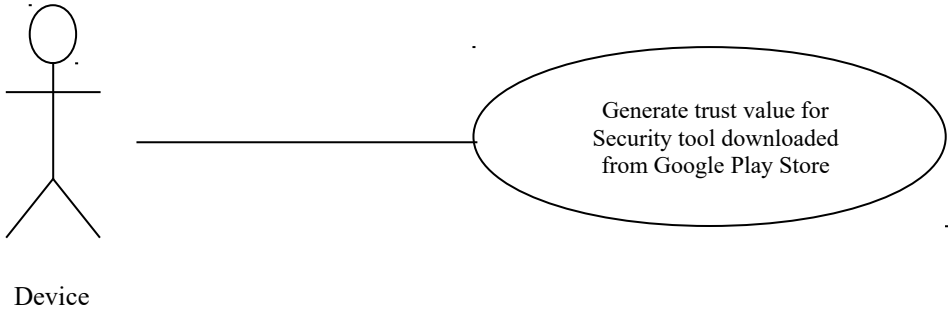
4. If the security tool downloaded from Other android application market, Then
    a. The System generates trust value for the security tool.

Xref: Section 3.2.12, Verify Security tool information and user settings.

2.2.13 Android device Use Cases

Use case: **Generate trust value for Security tool downloaded from Google Play tore**

Diagram:



Brief Description
After the verification of the Security tool and user settings information which downloaded from Google Play Store, the system will generate threshold value for the verification.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate trust value for Security tool information and user settings.

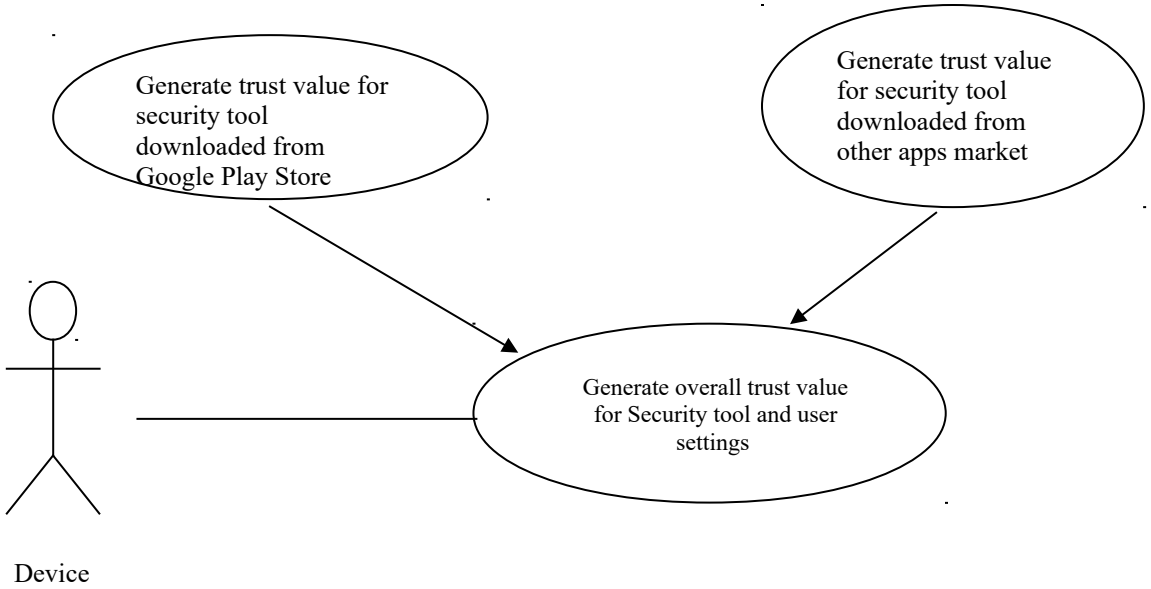
1. The Android device requests to generate a threshold value for Security tool and user settings in target Android device.
2. The System converts the fraction into threshold value.
3. The System presents threshold value.

Xref: Section 3.2.13, Generate trust value for Security tool downloaded from Google Play Store.

2.2.14 Android device Use Cases

Use case: **Generate overall trust value for Security tools and user settings**

Diagram:

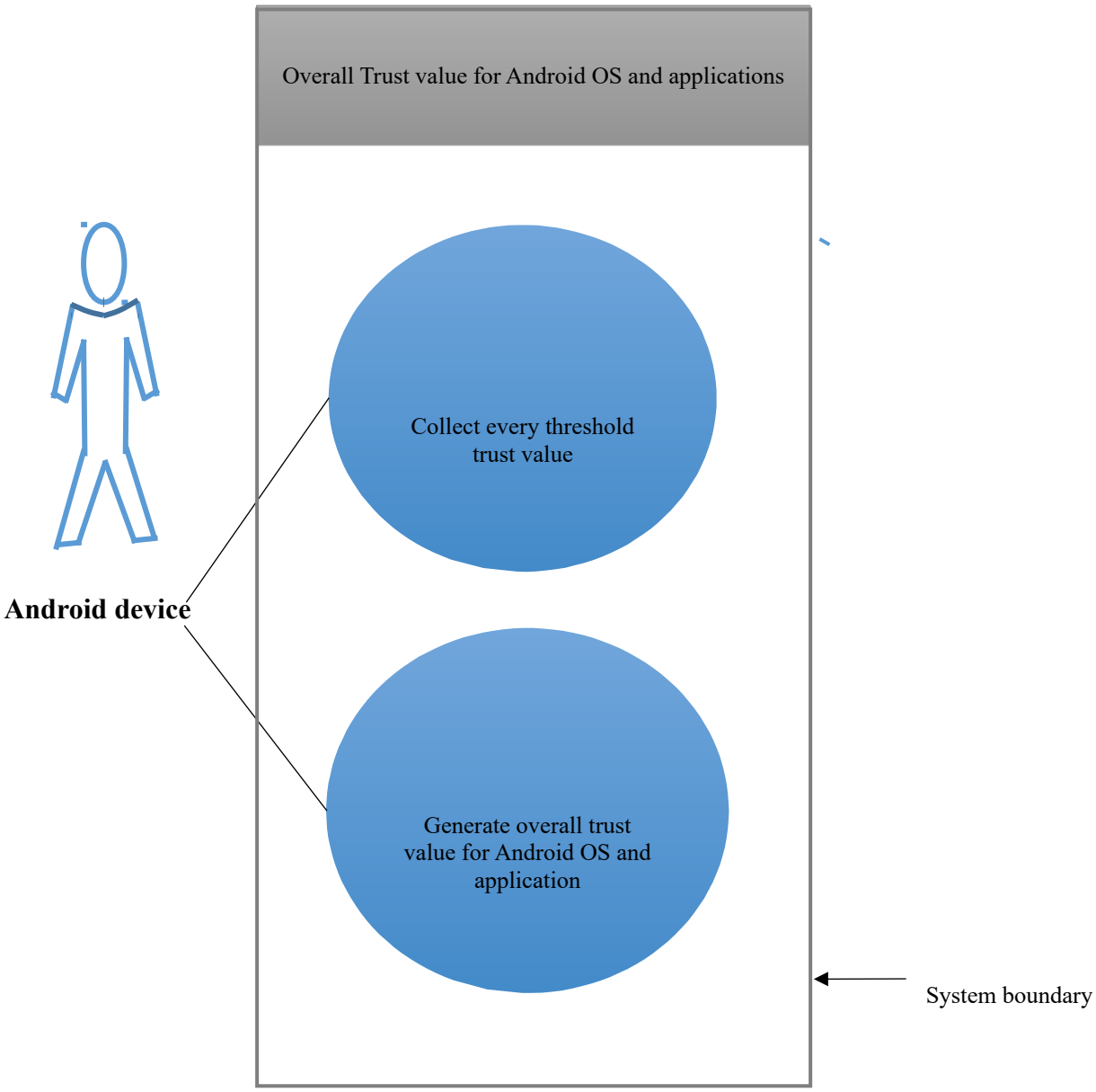


Brief Description
After the verification of the Security tool information, the system will generate overall threshold value for the Security tool and user settings.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate trust value for Security tools and user settings

1. The Android device requests to generate an overall threshold trust value for Android applications.
2. The System adds the each threshold value and converts it to single threshold trust value (0-1).
3. The System presents overall threshold value for application.

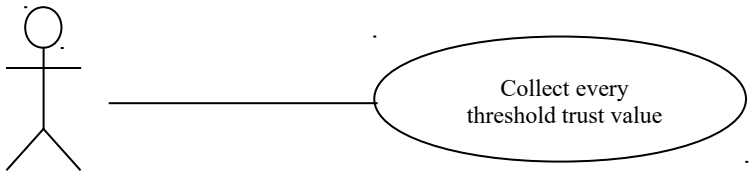
Xref: Section 3.2.14, Generate overall trust value for Security tool and user settings.


Overall Trust value for Android OS and applications
Collect every threshold trust value
Android device
Generate overall trust value for Android OS and application
System boundary

2.2.15 Android device Use Cases

Use case**: Collect every threshold trust value**

Diagram:



Device

Brief Description
After the four subparts verification (Trust value for Android OS, Trust value for Android application, Trust value for Android application which uses mobile data and Trust value for Security tool and user settings), the system needs collect each trust value from the sub parts.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to collect the trust value of sub parts.

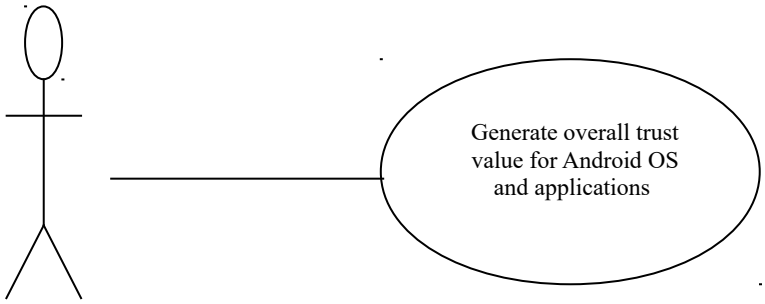
1. The Android device requests to collect a threshold trust value from
    a. Trust value for Android OS
    b. Trust value for Android application
    c. Trust value for Android application which uses mobile data
    d. Trust value for Security tool and user settings
2. The System collects the threshold trust value from each field.
3. The System stores each threshold trust value for addition.

Xref: Section 3.2.15, Collect every threshold trust value

2.2.16 Android device Use Cases

Use case**: Generate overall trust value for Android OS and application**

Diagram:



Brief Description
After collecting each threshold trust value from each field, the system needs to combine these trust value and generate an overall trust value for Android OS and applications. This overall threshold trust value is the final outcome of this total system.

Initial Step-By-Step Description
Before this use case can be initiated, the Android device has already requested to generate overall trust value of Android OS and application.

1. The Android device requests to generate an overall threshold trust value for Android OS and applications.
2. The System adds the each threshold value and converts it to single threshold trust value (0-1).
3. The System presents overall threshold value.

Xref: Section 3.2.16, Generate overall trust value for Android OS and applications.

3.1 Functional Requirements

The Logical Structure of the Data is contained in Section 3.3.1.

3.1.1 Collect Android version information

Use Case Name	Collect Android version information
Actor	Android device, Target Android device
XRef	Section 2.2.1, Collect Android version information
Trigger	The Android device requests the trust value for Android OS
Precondition	Target android device will send all required information to the system.
Basic Path	1. The Android device requests collect Android version information of the Target Android device. 2. The Target Android device sends the information to the system. 3. The System collects the Android version information from the Target Android device. 4. The System presents the Android version information of the Target Android device to the Android device. 5. The System checks the received information. 6. The System stores the Android version information for the comparison.
Alternative Paths	None
Postcondition	System receives and stores Target android device's Android version information.
Exception Paths	None
Other	None

3.1.2 Verify Android version information

Use Case Name	Verify Android version information
Actor	Android device, Google Android
XRef	Section 2.2.2, Verify Android version information
Trigger	The Android device requests the trust value for Android OS
Precondition	Google Android will send all required information to the system.
Basic Path	1. The Android device requests collect latest Android version information from Google Android. 2. The Google Android sends the related information to the system. 3. The System collects the latest Android version information from the Google Android. 4. The System compares latest Android version with stored Android version details such as a. Android version b. Baseband version c. Kernel version d. Security software version 5. The System generates a fraction after the comparison.
Alternative Paths	None
Postcondition	The fraction generated
Exception Paths	None
Other	None

3.1.3 Generate trust value for Android OS

Use Case Name	Generate trust value for Android OS
Actor	Android device
XRef	Section 2.2.3, Generate trust value for Android OS
Trigger	The Android device requests the trust value for Android OS.
Precondition	System has the fraction for the conversion.
Basic Path	1. The Android device requests to generate a threshold value for Android version. 2. The System converts the fraction into threshold value. 3. The System presents threshold value.
Alternative Paths	None
Postcondition	Threshold trust value for Android OS
Exception Paths	None
Other	None

3.1.4 Collect Android application information

Use Case Name	Collect Android application information
Actor	Android device, Target Android device
XRef	Section 2.2.4, Collect Android application information
Trigger	The Android device requests the trust value for Android application.
Precondition	Target android device will send all required information to the system.
Basic Path	1. The Android device requests collect Android application information which are installed in Target Android device. 2. The Target Android device sends the information to the system. 3. The System collects the Android application information

	from the Target Android device. 4. The System presents the Android application information of the Target Android device to the Android device. 5. The System checks information. 6. The System stores the Android application information for the comparison.
Alternative Paths	None
Postcondition	System receives and stores Target android device's application information.
Exception Paths	None
Other	None

3.1.5 Verify Android application information

Use Case Name	Verify Android application information
Actor	Android device, Google Play Store
XRef	Sec 2.2.5 Verify Android application information
Trigger	The Android device requests the trust value for Android application.
Precondition	Google Play Store will send all required information to the system.
Basic Path	1. The System differentiate applications which are downloaded from Google play Store and Other android application markets. 2. If the application downloaded from Google Play Store, Then a. The System requests collect last version of Android application information from Google Play Store. b. The Google Play Store sends the related information to the system. c. The System collects the latest version of Android application information from the Google Play Store. d. The System compares latest version of Android application with stored Android application information. e. The System compares Android application version, number of installs, number of reviews, score, developer and permissions with the stored Android application information. f. The System generates a fraction after the

	comparison.
Alternative Paths	None
Postcondition	The fraction generated
Exception Paths	1. If the application downloaded from Other android application market, Then a. The System generates threshold trust value for applications.
Other	None

3.1.6 Generate trust value for Android application downloaded from Google Play Store

Use Case Name	Generate trust value for Android application downloaded from Google Play Store
XRef	Section 2.2.6, Generate trust value for Android application downloaded from Google Play Store
Trigger	The Android device requests the trust value for Android application.
Precondition	System has the fraction for the conversion.
Basic Path	1. The Android device requests to generate a threshold value for Android applications which are installed in target Android device. 2. The System converts the fraction into threshold value. 3. The System presents threshold value.
Alternative Paths	None
Postcondition	Threshold trust value for application downloaded from Google Play Store
Exception Paths	None
Other	None

3.1.7 Generate overall trust value for Android application

Use Case Name	Generate overall trust value for Android application
Actor	Android device
XRef	Section 2.2.7, Generate overall trust value for Android application
Trigger	The Android device requests the trust value for Android application.
Precondition	System has Threshold trust value for Google Paly Store apps and other apps
Basic Path	2. The Android device requests to generate an overall threshold trust value for Android applications. 3. The System adds the each threshold value and converts it to single threshold trust value (0-1). 4. The System presents overall threshold value for

	application.
Alternative Paths	None
Postcondition	Threshold trust value for all applications.
Exception Paths	None
Other	None

3.1.8 Collect Android application information which uses mobile data.

Use Case Name	Collect Android application information which uses mobile data.
Actor	Android device, Target Android device
XRef	Section 2.2.8, Collect Android application information which uses mobile data.
Trigger	The Android device requests the trust value for Android application which uses mobile data.
Precondition	Target android device will send all required information to the system.
Basic Path	1. The Android device requests collect Android application information uses mobile data for their function in Target Android device. 2. The Target Android device sends the information to the system. 3. The System collects the Android application information from the Target Android device. 4. The System presents the Android application information of the Target Android device to the Android device. 5. The System checks information. 6. The System stores the Android application information for the comparison.
Alternative Paths	None
Postcondition	System receives and stores Target android device's application information which uses mobile data.
Exception Paths	None
Other	None

3.1.9 Verify Android application information which uses mobile data

Use Case Name	Verify Android application information which uses mobile data
Actor	Android device
XRef	Section 2.2.9, Verify Android application information which uses mobile data
Trigger	The Android device requests the trust value for Android application which uses mobile data.
Precondition	System has foreground and background mobile data usage information.
Basic Path	1. The Android device requests analyze mobile data usage of Android application which uses mobile. 2. The System compares the foreground mobile data usage and background mobile data usage. 3. The System generates a fraction after the comparison.
Alternative Paths	None.
Postcondition	The fraction generated
Exception Paths	None.
Other	None.

3.1.10 Generate trust value for Android application which uses mobile data

Use Case Name	Generate trust value for Android application which uses mobile data
Actor	Android device
XRef	Section 2.2.10, Generate trust value for Android application which uses mobile data
Trigger	The Android device requests the trust value for Android application which uses mobile data.
Precondition	System has the fraction for the conversion.
Basic Path	1. The Android device requests to generate a threshold

	value for Android applications which uses mobile data in their functions in target Android device. 2. The System converts the fraction into threshold value. 3. The System presents threshold value.
Alternative Paths	None.
Postcondition	Threshold trust value for applications which uses mobile data.
Exception Paths	None
Other	None

3.1.11 Collect Security tools information and user settings

Use Case Name	Collect Security tools information and user settings
Actor	Android device, Target Android device
XRef	Section 2.2.11, Collect Security tools information and user settings
Trigger	The Android device requests the trust value for Security tools & Utilization.
Precondition	Target android device will send all required information to the system.
Basic Path	1. The Android device requests collect Security tools information and the user settings of the Target Android device. 2. The Target Android device sends the information to the system. 3. The System collects the Security tools information and the user settings from the Target Android device. 4. The System presents the Security tools information and the user settings of the Target Android device to the Android device. 5. The System checks information. 6. The System stores the Security tools information and the user settings for the comparison.
Alternative Paths	None.
Postcondition	System receives and stores Target android device's security tool information.
Exception Paths	None
Other	None

3.1.12 Verify Security tools information

Use Case Name	Verify Security tools information
Actor	Android device, Google Play Store
XRef	Section 2.2.12, Verify Security tools information
Trigger	The Android device requests the trust value for Security tools & Utilization.
Precondition	Google Play Store will send all required information to the system.
Basic Path	1. The Android device requests verify Security tools information and the user settings of the Target Android device. 2. The System analyze security tools information. 3. If the Security tool downloaded from Google Play Store, Then a. The Android device requests collect last version of Security tool information from Google Play Store. b. The Google Play Store sends the related information to the system. c. The System collects the latest version of Security tool information from the Google Play Store. d. The System compares latest version of Security tool with stored Security tool information. e. The System compares Security tool version, number of installs, number of reviews, score, developer and permissions with the stored Security tool information. f. The System generates a fraction after the comparison.

Alternative Paths	None.
Postcondition	The fraction generated
Exception Paths	1. If the security tool downloaded from Other android application market, Then The System generates trust value for the security tool.
Other	None

3.1.13 Generate trust value for Security tools downloaded from Google Play Store

Use Case Name	Generate trust value for Security tools downloaded from Google Play Store
Actor	Android device, Google Play Store
XRef	Section 2.2.13, Generate trust value for Security tools downloaded from Google Play Store
Trigger	The Android device requests the trust value for Security tools & Utilization.
Precondition	System has the fraction for the conversion.
Basic Path	1. The Android device requests to generate a threshold value for security tool which is installed in target Android device. 2. The System converts the fraction into threshold value. 3. The System presents threshold value.
Alternative Paths	None
Postcondition	Threshold trust value for security tool downloaded from Google Play Store
Exception Paths	None
Other	None

3.1.14 Generate overall trust value for security tool information and user settings

Use Case Name	Generate overall trust value for security tool information and user settings
Actor	Android device
XRef	Section 2.2.14, Generate overall trust value for security tool information and user settings
Trigger	The Android device requests the trust value for Security tools & Utilization
Precondition	System has Threshold trust value for Google Paly Store security tool or other security tool

Basic Path	1. The Android device requests to generate an overall threshold trust value for security tool. 2. The System receives the threshold value (0-1). 3. The System presents overall threshold value for application.
Alternative Paths	None
Postcondition	Threshold trust value for all applications.
Exception Paths	None
Other	None

3.1.15 Collect every threshold trust value

Use Case Name	Collect every threshold trust value
Actor	Android device
XRef	Section 2.2.15, Collect every threshold trust value
Trigger	The Android device requests the overall trust value for Android OS and applications
Precondition	System has Threshold trust value for each field separately
Basic Path	1. The Android device requests to collect a threshold trust value from a. Trust value for Android OS b. Trust value for Android application c. Trust value for Android application which uses mobile data d. Trust value for Security tool and user settings 2. The System collects the threshold trust value from each field. 3. The System stores each threshold trust value for addition.
Alternative Paths	None
Postcondition	System receives and stores threshold trust value for each field.
Exception Paths	None
Other	None

3.1.16 Generate overall trust value for Android OS and application

Use Case Name	Generate overall trust value for Android OS and application
Actor	Android device
XRef	Section 2.2.16, Generate overall trust value for Android OS and application
Trigger	The Android device requests the overall trust value for Android OS and applications
Precondition	System has Threshold trust value for each field
Basic Path	1. The Android device requests to generate an overall threshold trust value for Android OS and applications.

	2. The System adds the each threshold value and converts it to single threshold trust value (0-1). 3. The System presents overall threshold value.
Alternative Paths	None
Postcondition	Threshold trust value for Android OS and application
Exception Paths	None
Other	None