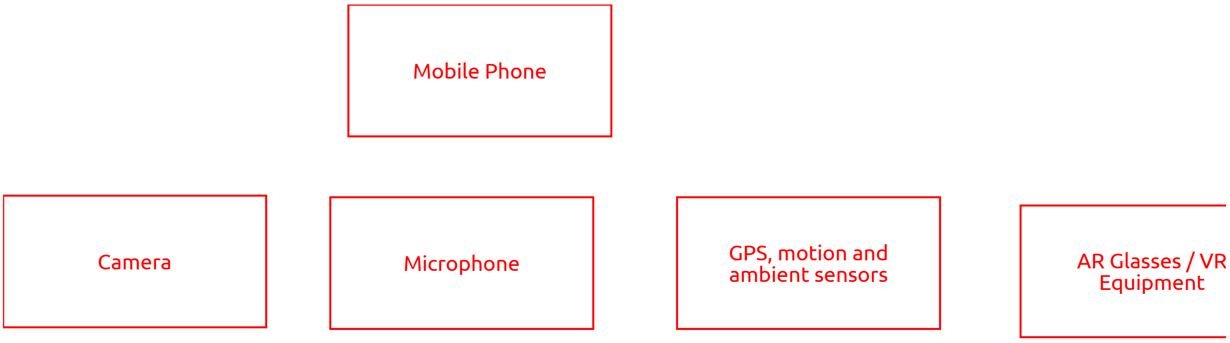
Threat model report for Sensors

Owner:
Francesco Galassi
Reviewer:
Contributors:

High level system description

AR app for school pupils

sensors on mobile



Mobile Phone

Camera

Microphone

GPS, motion and ambient sensors

AR Glasses / VR Equipment

Mobile Phone (External Actor)

Description:

Phone controlled

Tampering, Open, High Severity

Description:
Take control of the mobile hardware and/or software with a virus or app to gain control, grant access or alter any behaviour

Mitigation:
install antivirus, anti malware on the phone to protect the phone

TDos

Denial of service, Open, High Severity

Description:
A Telephony Denial of Service (TDoS) attack is an attempt to make a telephone system unavailable to the intended users. (Source cisecurity.org)

Mitigation:
block any connection if the app does not behave as expected

elevation of privilege vulnerability

Elevation of privilege, Open, Medium Severity

Description:
Exploiting some phones vulnerabilities that exist for examplo in Windows Mobile Devicesmight allow attacker to bypass access restrictions to delete files. (source msrc.microsoft.com)

Mitigation:
Be sure the app has the lowest permissions granted

Camera (External Actor)

Description:

camera misuse

Spoofing, Open, Medium Severity

Description:
Use camera access from the app to take photo, record or see what framed by the phone

Mitigation:
Ask the user permission for camera use every time the app is on

Camera offline for other apps

Denial of service, Open, Medium Severity

Description:
Elements might be put offline denying use of them from other applications

Mitigation:
limit the resource to the app

Microphone (External Actor)

Description:

overhearing

Information disclosure, Open, High Severity

Description:
Similar to the camera, the app has access to the microphone which can hear or save what the microphone listen to

Mitigation:
release persmission every time the app is closed or paused and ask again for permisisons

Microphone offline for other apps

Denial of service, Open, Medium Severity

Description:
Elements might be put offline denying use of them from other applications

Mitigation:
limit the resource to the app

GPS, motion and ambient sensors (External Actor)

Description:

User position

Information disclosure, Open, High Severity

Description:
the app knowing the user position can inform an attacker where the user is

Mitigation:
grant position only when wished by the user working with permissions

sensors offline for other apps

Denial of service, Open, Medium Severity

Description:
Elements might be put offline denying use of them from other applications

Mitigation:
limit the resource to the app

AR Glasses / VR Equipment (External Actor)

Description:

equipment offline

Denial of service, Open, Medium Severity

Description:
Elements might be put offline denying use of them from other applications

Mitigation:
limit the resource to the app