Audio Capture, Technique T1429 - Mobile

Archived: 2026-04-02 10:44:49 UTC

Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Examples of audio information adversaries may target include user conversations, surroundings, phone calls, or other sensitive information.

Android and iOS, by default, require that applications request device microphone access from the user.

On Android devices, applications must hold the `RECORD_AUDIO` permission to access the microphone or the `CAPTURE_AUDIO_OUTPUT` permission to access audio output. Because Android does not allow third-party applications to hold the `CAPTURE_AUDIO_OUTPUT` permission by default, only privileged applications, such as those distributed by Google or the device vendor, can access audio output.[1] However, adversaries may be able to gain this access after successfully elevating their privileges. With the `CAPTURE_AUDIO_OUTPUT` permission, adversaries may pass the `MediaRecorder.AudioSource.VOICE_CALL` constant to `MediaRecorder.setAudioOutput`, allowing capture of both voice call uplink and downlink.[2]

On iOS devices, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file to access the microphone.[3]

Source: https://attack.mitre.org/techniques/T1429