Requirements for Secure MMAP File Descriptor

These revised requirements are based on discussions with Zach Riggle and Mark Brown.

1/31/19 GOOGLE, Phil Burk, Zach Riggle

Overview

The AAudio API in Android is a new low-latency path that is recommended for all new native applications. It uses the ALSA MMAP mode to allow reading and writing the PCM buffer. In EXCLUSIVE mode, the app can write directly into the MMAP buffer so it requires access to an ALSA file descriptor. This is a security risk if the FD is the full ALSA FD that includes STATUS and CONTROL.

Requirements

1. The HAL must be able to create an ALSA MMAP file descriptor with access to STATUS and CONTROL for use only by the HAL. This FD will be used to query the hardware read/write position.
2. The HAL must be able to create a second file descriptor that only allows access to the PCM buffer and nothing else. That limited FD will be passed through Binder to the application.
3. It must be impossible for the permissions of this limited FD to be increased by code running at the application level.
4. The FD should be of type “anon_inode:*”. It can be, for example, “anon_inode:dmabuf” or “anon_inode:snd-pcm-buffer”.
5. The changes must ultimately be available as open source in ALSA so that Android partners can make use of it.
6. Google would like to make patches available to SOC partners for review, and possible adoption, before final acceptance in the upstream kernel.
7. The patches must pass a review by the Android Security team before they can be used in an Android device.