University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

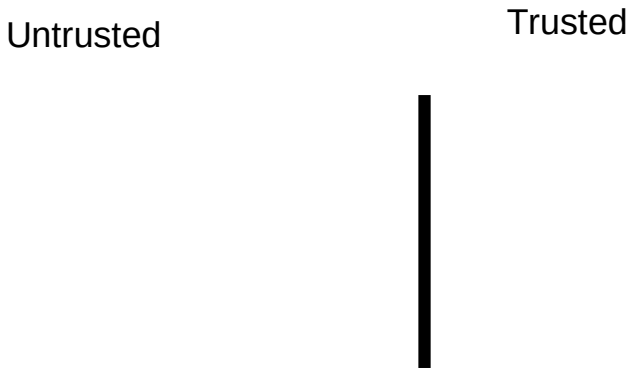
bristol.ac.uk

University of BRISTOL

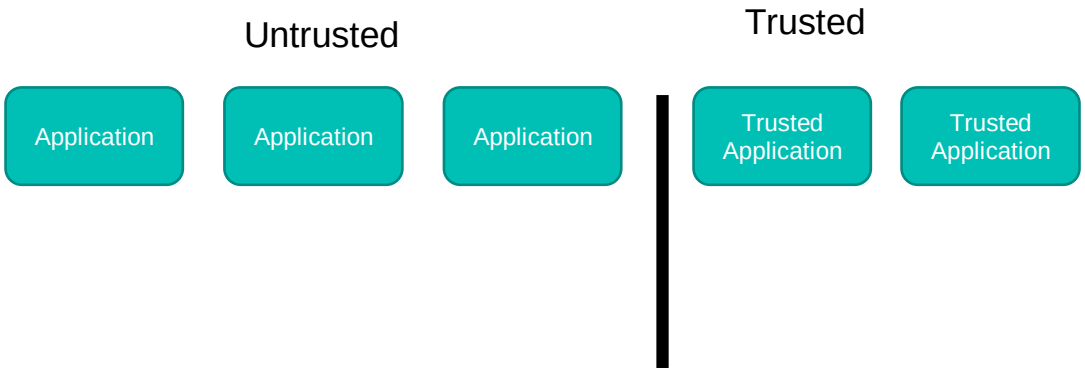
ARM Trustzone

bristol.ac.uk

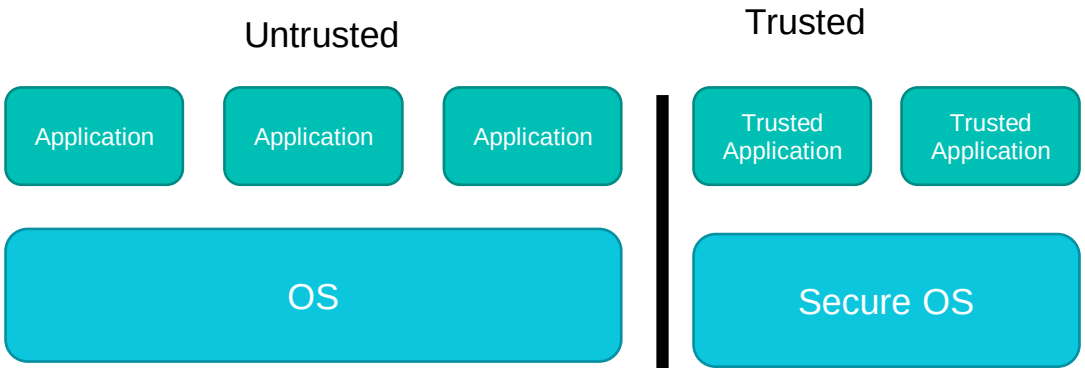
ARM Trustzone



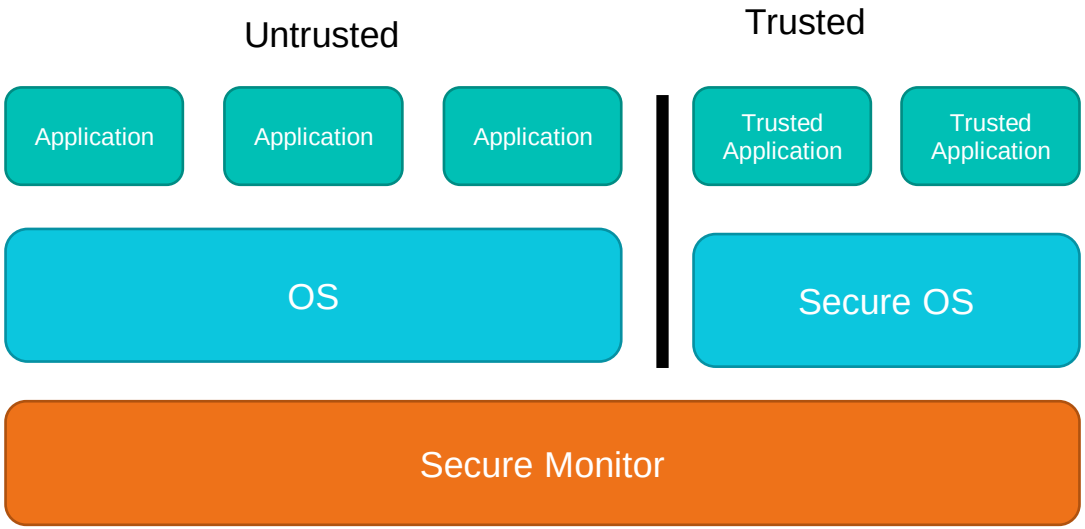
ARM Trustzone



ARM Trustzone

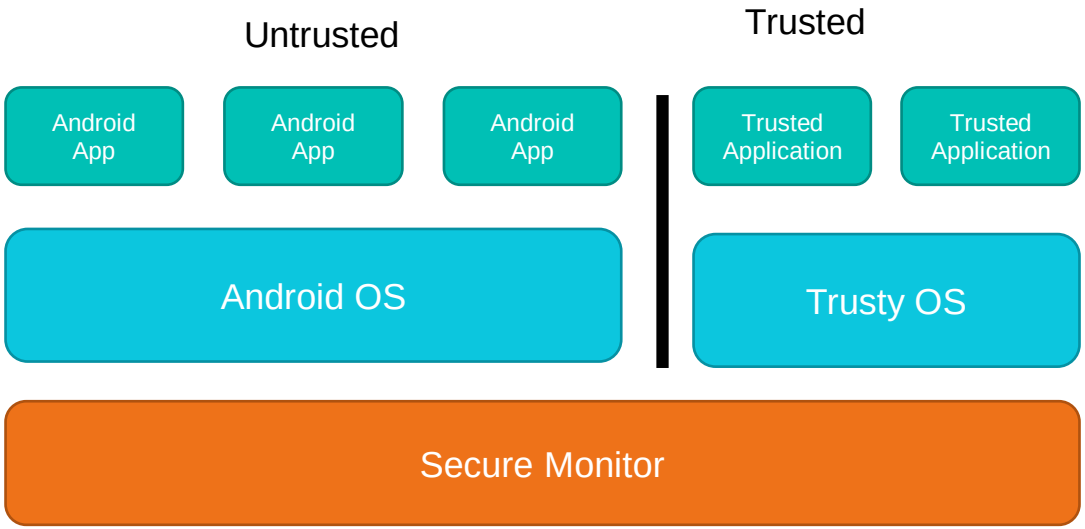


ARM Trustzone

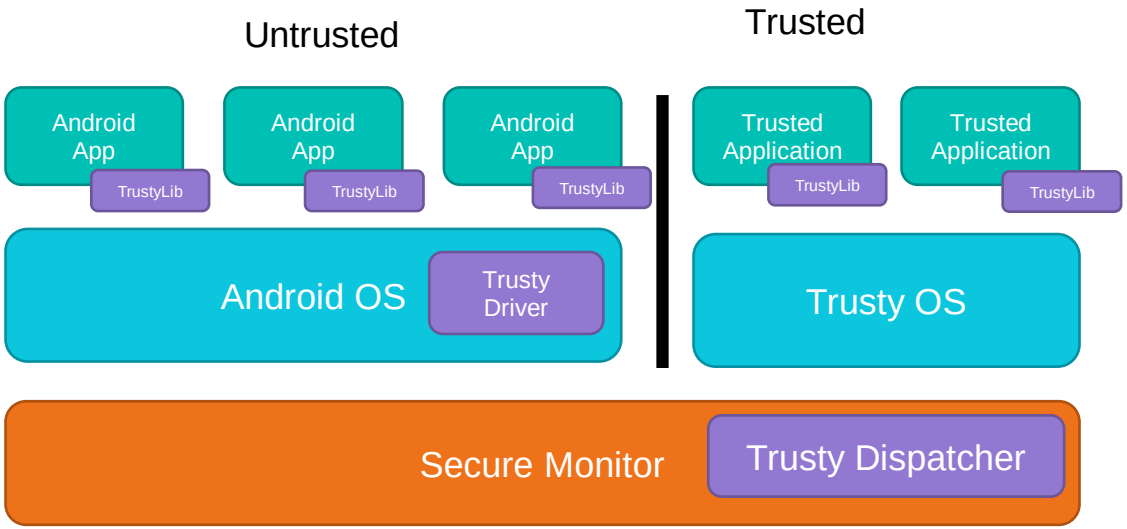


Own processor
Own RAM address
Own devices
etc…

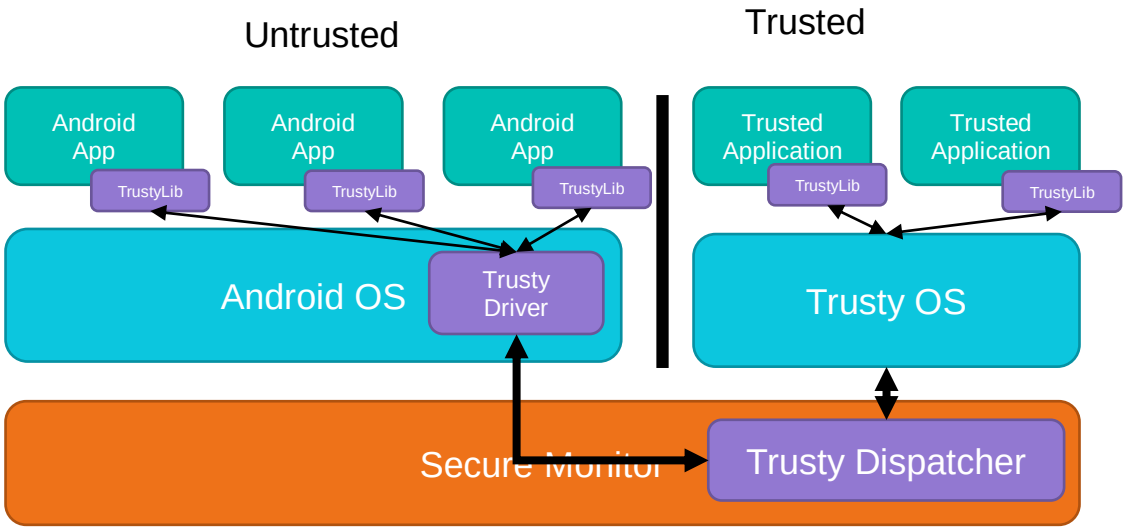
ARM Trustzone



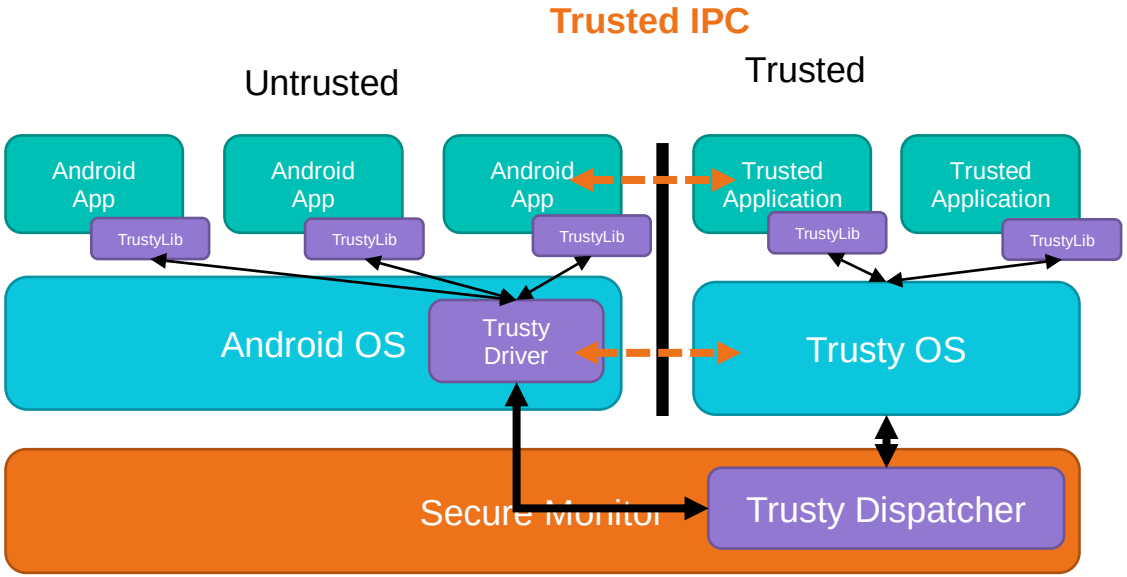
ARM Trustzone



ARM Trustzone



ARM Trustzone



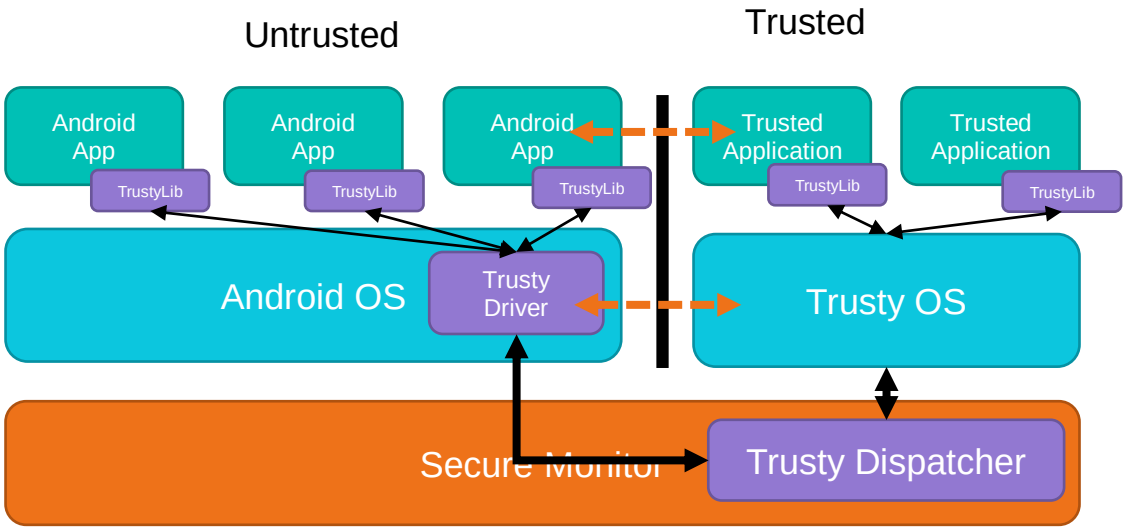
Trusted IPC example

- connect(path, flags)
- send_msg(handle, msg)
- get_msg(handle, *msg_info)
- read_msg(handle, id, offset, *msg)

Trusted service declare endpoints
Untrusted apps can connect and exchange with truted apps

Occur through driver + secure monitor

ARM Trustzone



Examples:
DRM
Secure banking
Multi-factor authentication
etc…