COL788: Advanced Topics in Embedded Computing

Lecture 17 – Trusted Computing

Vireshwar Kumar
CSE@IITD

September 19, 2022

Semester I
2022-2023

Agenda

- Need for Trusted Computing

- Trusted Execution Architecture

- Example: Remote Attestation

Problem: Digital Right Management

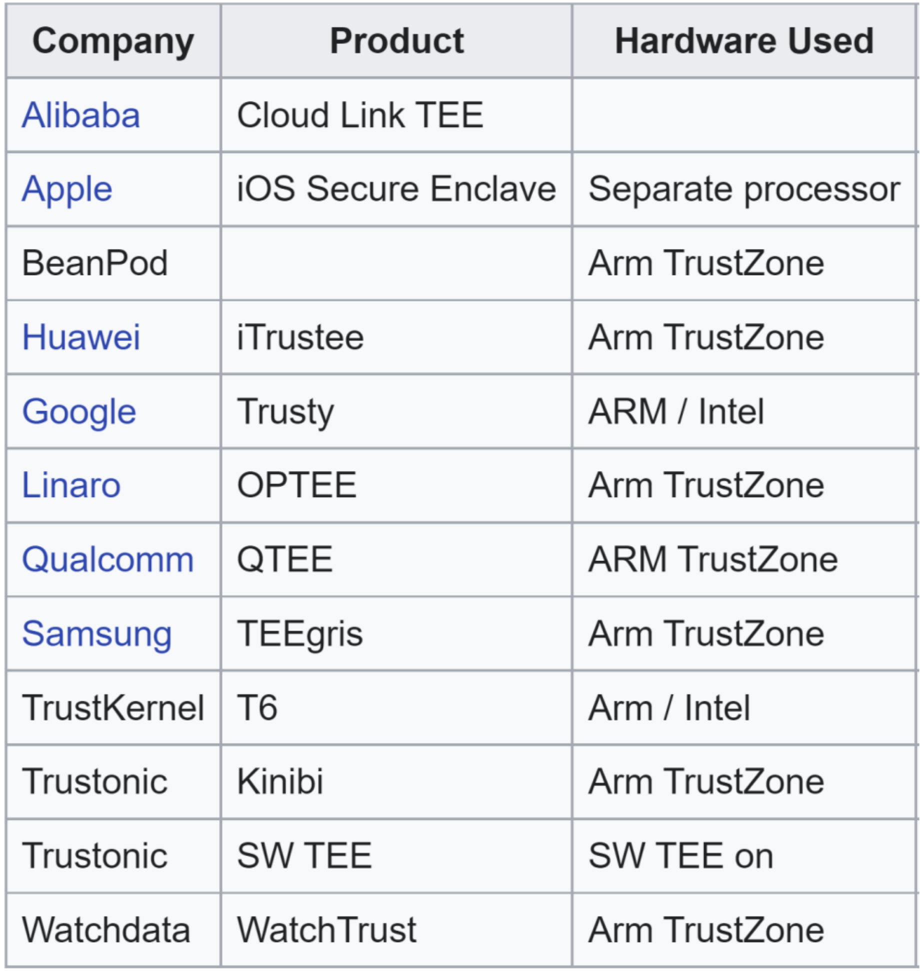
Problem: Robust Security

Idea: Trusted Computing

- Features
  - Isolation from the regular OS
  - Hardware-based security guarantees
  - Reconfigurability

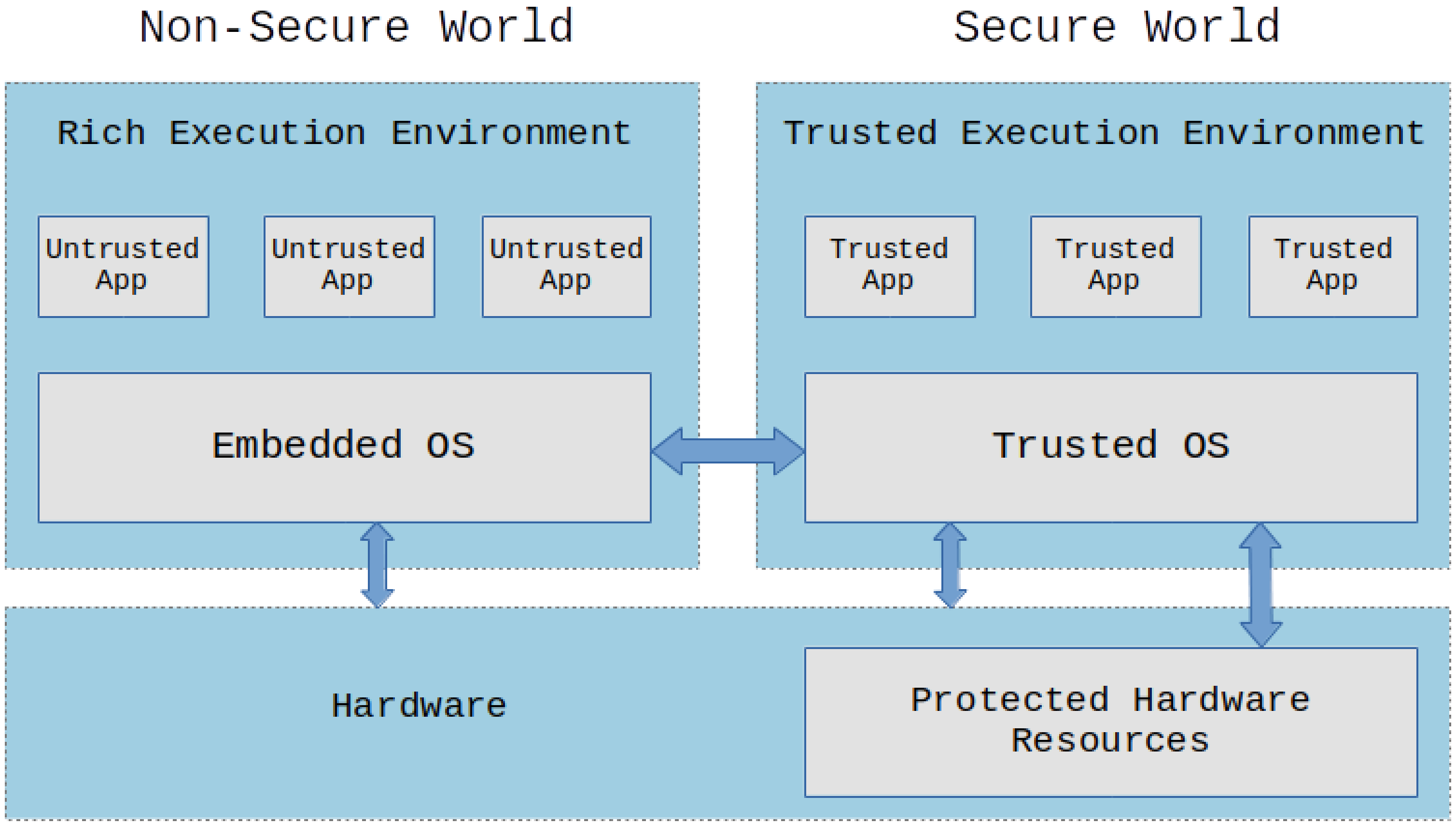
- Implications
  - Enhanced confidence in the device security
  - Ensures that the device performs the way it is supposed to
  - Recovery after a potential compromise
  - Secure storage

Trusted Execution Environment OS



Company	Product	Hardware Used
Alibaba	Cloud Link TEE	
Apple	iOS Secure Enclave	Separate processor
BeanPod		Arm TrustZone
Huawei	iTrustee	Arm TrustZone
Google	Trusty	ARM / Intel
Linaro	OPTEE	Arm TrustZone
Qualcomm	QTEE	ARM TrustZone
Samsung	TEEgris	Arm TrustZone
TrustKernel	T6	Arm / Intel
Trustonic	Kinibi	Arm TrustZone
Trustonic	SW TEE	SW TEE on
Watchdata	WatchTrust	Arm TrustZone

ARM TEE Architecture



Example: Remote Attestation

Example: Remote Update

What’s Next?

- Lecture 18
  - September 21, Wednesday, 11 am – 12 pm