COL788: Advanced Topics in Embedded Computing

Lecture 18 – Trusted Computing (Cont.)

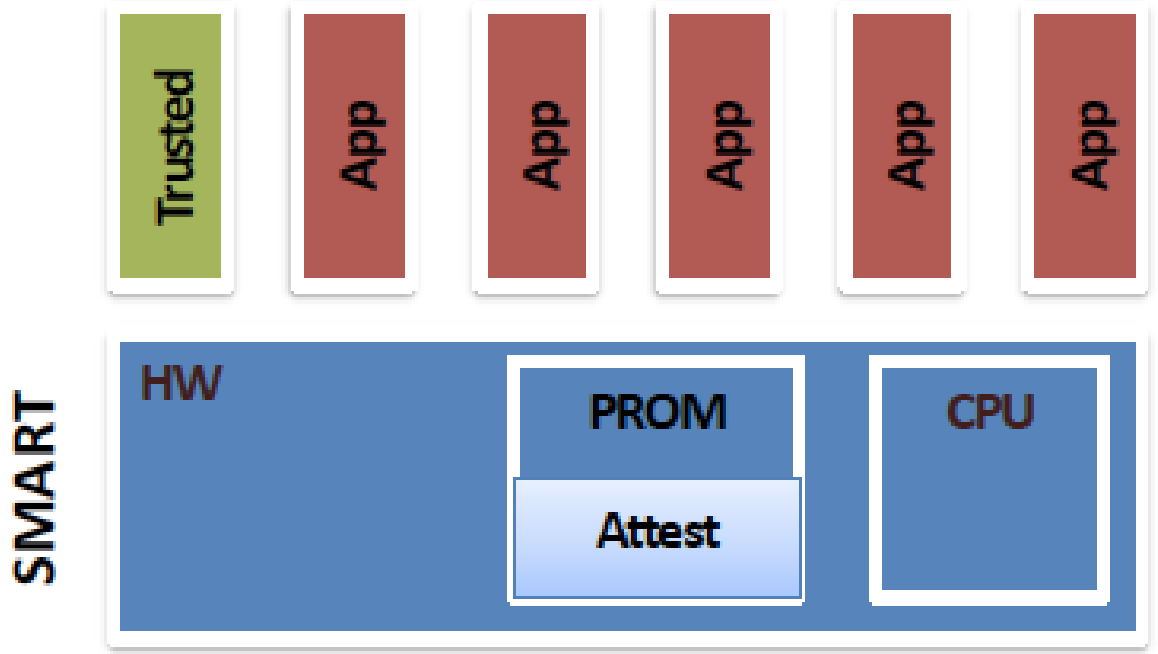
Vireshwar Kumar
CSE@IITD

September 21, 2022

Semester I
2022-2023

Basic Architecture

- SMART: Secure Minimal Architecture for (Establishing a Dynamic) Root of Trust



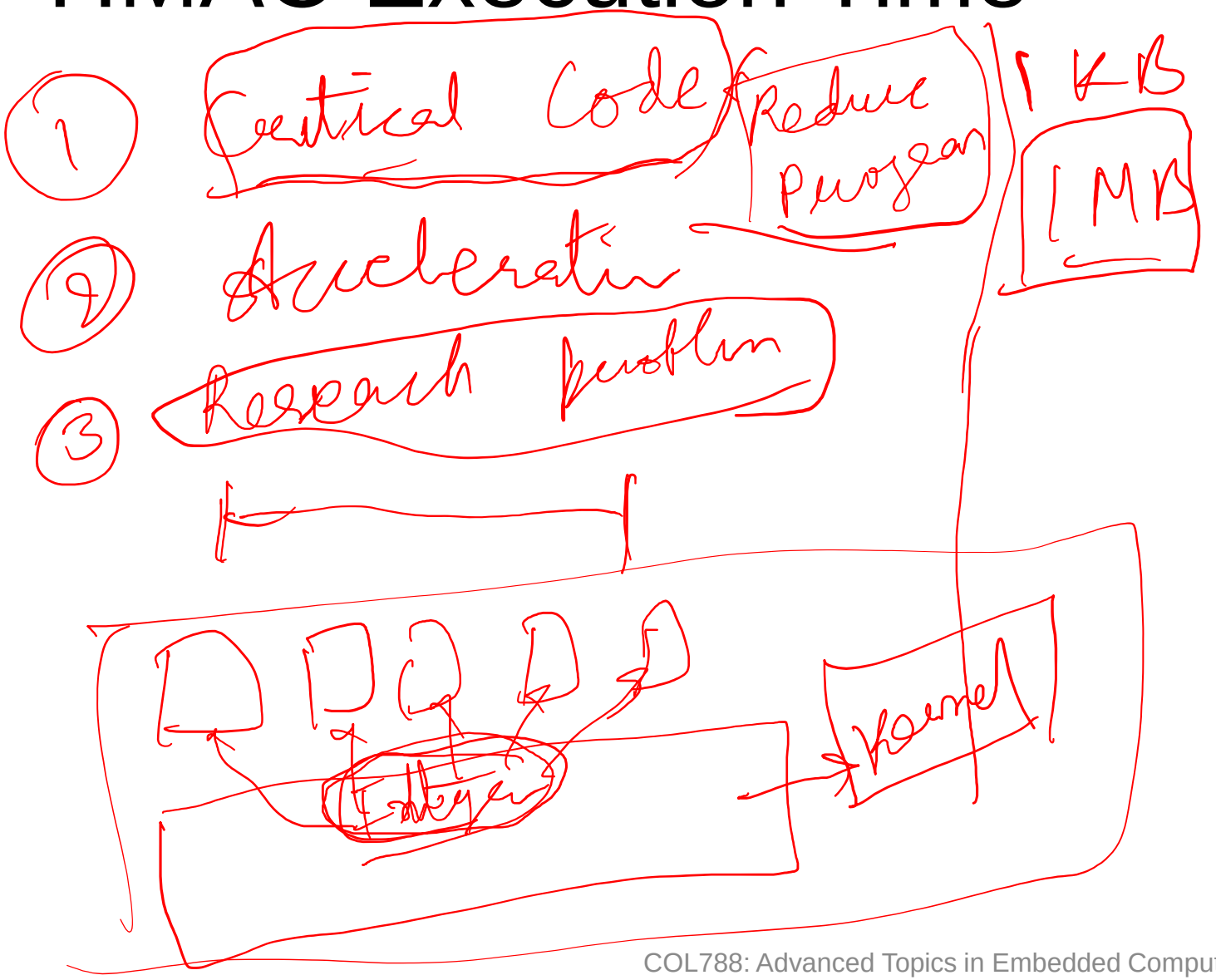
Threat Model

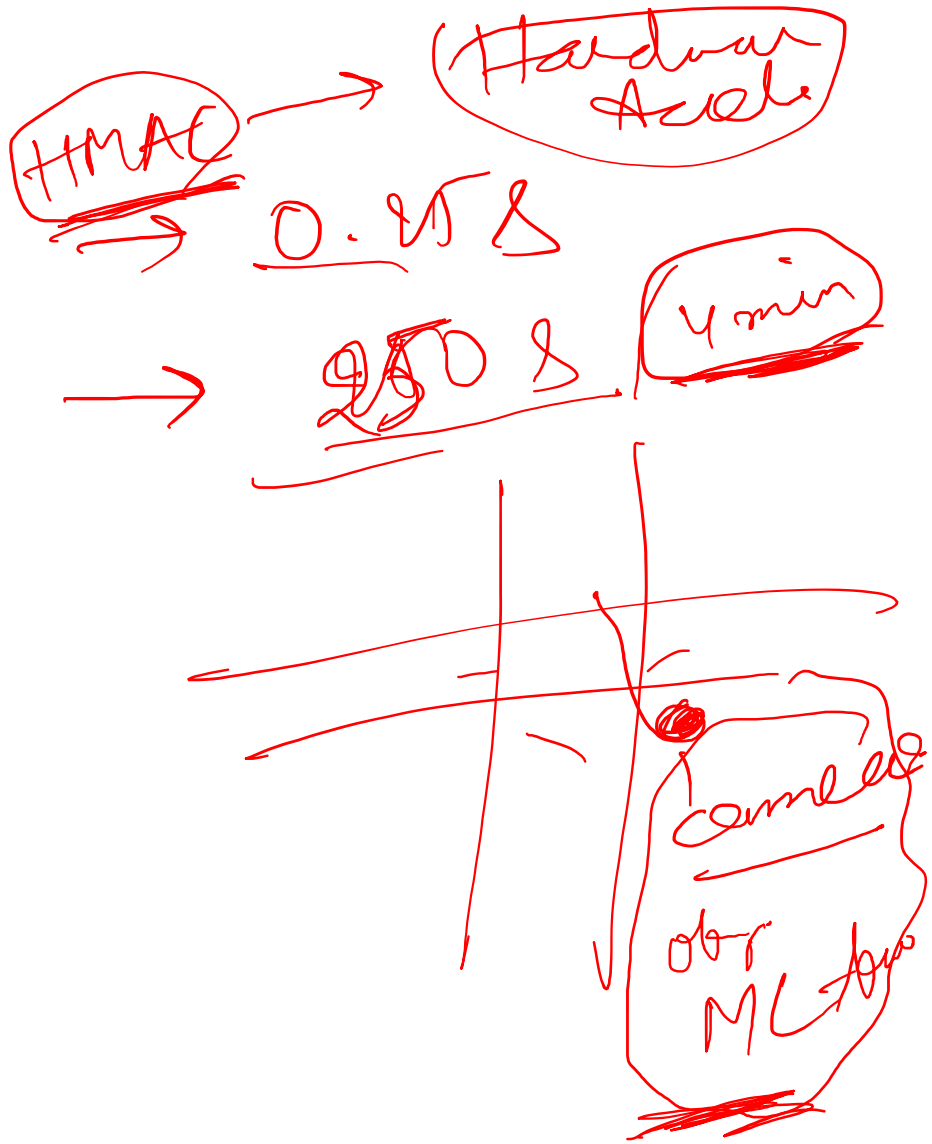
- System
  - Immutable ROM
  - RAM erased at reset

- Attacker
  - Full control over software
  - No invasive hardware attacks
  - No side-channel attacks

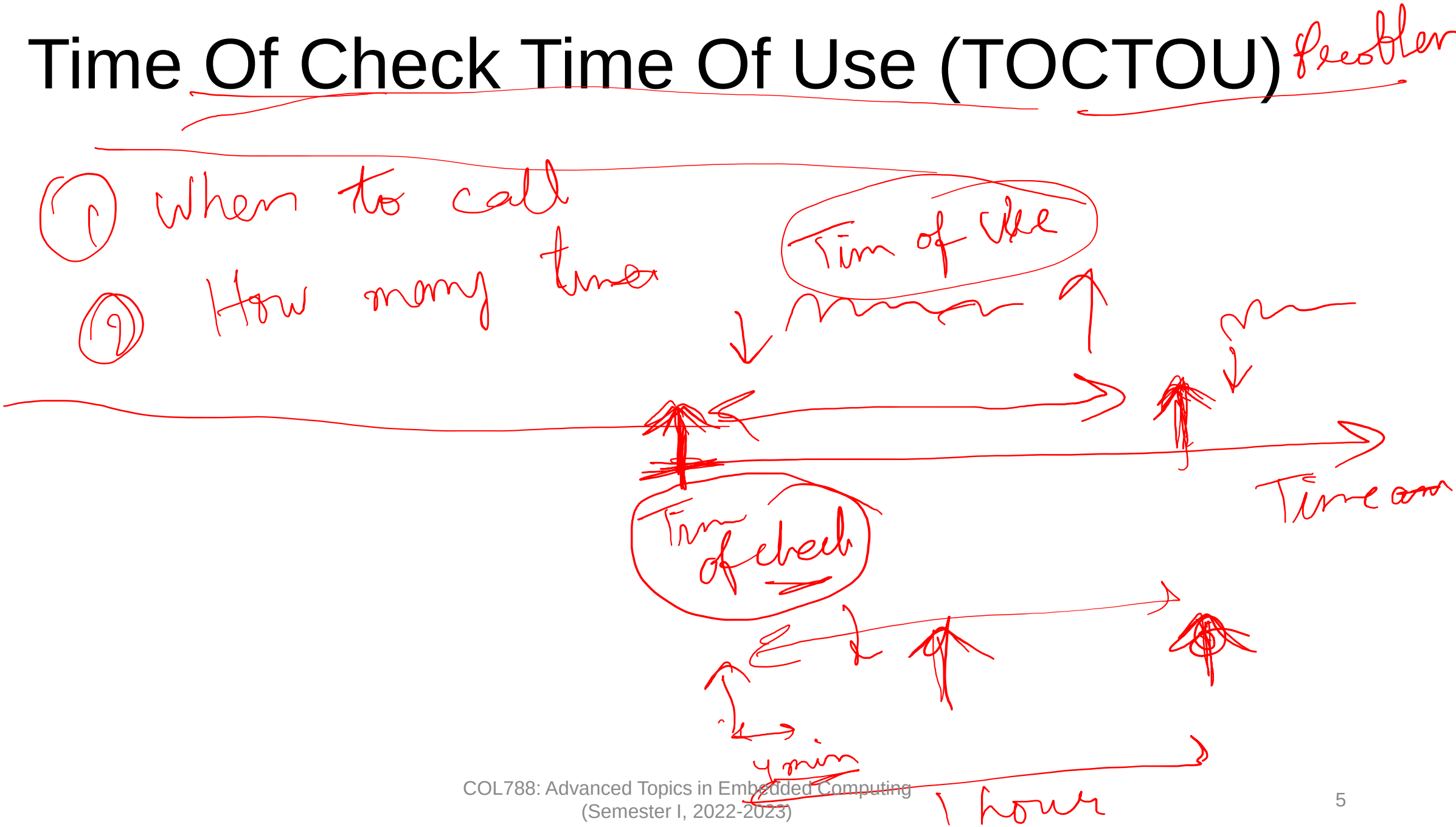
- Shared key between prover and verifier

HMAC Execution Time





Time Of Check Time Of Use (TOCTOU)



What Next?

- Lecture 19
  - September 22,Thursday, 12 pm – 1 pm