Local host

In-process attacks
(memory corruption, ROP attacks)

Enclave data

Enclave code

Exchange attestation

Remote service or enclave

Host OS

OS attacks (e.g., rootkits)

Enclave creation

Off-chip hardware

Hardware attacks
(e.g., cold-boot attacks)

Intel CPU

☐ ⇨ Trusted

▨ ⬛ Untrusted