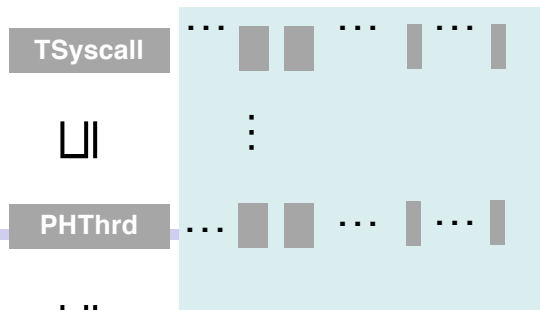
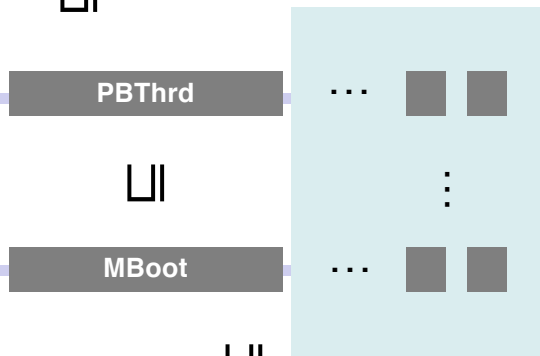


CertiKOS Structure

(2) Section 5.2



(3) Section 5.3



(1) Section 5.1



(4) Section 5.4

 : Environments

CertiKOS Theorems

$$\llbracket \mathbf{Tsyscall}[tid, \varepsilon'_{tid}] \langle \mathbf{Ctxt} \rangle \rrbracket_{\text{mach}_{\text{HAsm}}}$$

$$\llbracket \mathbf{PHThrd}[tid, \varepsilon_{tid}] \langle \mathbf{CertiKOS}_{\text{td}} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\text{mach}_{\text{HAsm}}}$$

$$\llbracket \mathbf{PBThrd}[cid, \varepsilon'_{cid}] \langle \mathbf{CertiKOS}_{\text{td}} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\text{mach}_{\text{LAsm}}}$$

$$\llbracket \mathbf{MBoot}[cid, \varepsilon_{cid}] \langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\text{mach}_{\text{LAsm}}}$$

$$\llbracket \mathbf{MBoot} \langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\text{mach}_{\text{x86}}}$$

(where $\mathbf{CertiKOS} := \mathbf{CertiKOS}_{\text{cpu}} \oplus \mathbf{CertiKOS}_{\text{td}}$)

Connect CompCertX interface

Optimize
environmental context

Introduce per-CPU machine

Introduce partial machine
and prove linking theorem

Introduce hardware scheduler

$$\text{Mach}_{\text{LAsm}}(\text{MBoot}[cid, \varepsilon_{cid}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{sep}}(\text{MBoot}[cid, \varepsilon_{\text{sep}}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{reorder}}(\text{MBoot}[cid, \varepsilon'_{\text{reorder}}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{reorder}}(\text{MBoot}[cid, \varepsilon_{\text{reorder}}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{split}}(\text{MBoot}[cid, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{si_big}}(\text{MBoot}[cid, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{si_big}}(\text{MBoot}[cid, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{si}}(\text{MBoot}[cid, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{env}}(\text{MBoot}[cid, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{env}}(\parallel_{si \in \text{CoreSet}} \text{MBoot}[\text{CoreSet}, \varepsilon_{si}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{oracle}}(\text{MBoot}[\varepsilon_{\text{CoreSet}}]) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

$$\sqcup$$

$$\text{Mach}_{\text{mc}}(\text{MBoot}) \vdash \llbracket \text{CertiKOS} \oplus \text{Ctxt} \rrbracket$$

Connect CompCertX Interface

$$\text{Mach}_{\text{HAsm}}(\text{PHThrd}[tid, \varepsilon_{tid}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$

\sqcup

$$\text{Mach}_{\text{TAsm}}(\text{PHBThrd}[tid, \varepsilon_{tid}^{MTLink}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$

\sqcup

Introduce
per-thread machine

$$\text{Mach}_{\text{IEAsm}}(\text{PHBThrd}[tid, \varepsilon_{tid}^{MTLink}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$

\sqcup

Introduce
multithreaded machine and
prove linking theorem

$$\text{Mach}_{\text{IEAsm}}(\parallel_{tid \in T_{[cid]}} \text{PHBThrd}[cid, \varepsilon_{tid}^{MTLink}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$

\sqcup

$$\text{Mach}_{\text{EAsm}}(\parallel_{tid \in T_{[cid]}} \text{PHBThrd}[cid, \varepsilon'_{cid}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$

\sqcup

$$\text{Mach}_{\text{LAsm}}(\text{PBThrd}[cid, \varepsilon'_{cid}]) \vdash \llbracket \text{CertiKOS}_{\text{thrd}} \oplus \text{Ctxt} \rrbracket$$