all reads/write
are with in the
range
Specific
Entry point

Inline Reference Monitor

Untrusted data
Untrusted txt
Trusted data
Trusted txt

Un-writable
All jumps to 32 byte aligned targets

Control Trusted to/from Trusted Code

Untrusted code region:

Check return address

Untrusted code

Trusted code

Ssp
Jmp func
untrusted

Trusted

Filled by run time linker
Generated at load time by the user
Trampoline

Returns:

- Trusted code can just jump back
  - Better check R.A.
  - 2 stack: trusted & untrusted

Trampoline

Switch stack (Push to ssp)
Move pram & R.A. to spring board
foo

In Caller module

SSP: contains return address to switch back
+ return by only the trampoline
In a multithreaded application, every thread would have its own copy of ssp.

What's the win of two modules that don't trust each other? Faster context switching.