1 Native Client

1.1 Jumping from Untrusted Code to Trusted Code

- The untrusted text segment is unwritable.

- The untrusted code can only jump within its own region because jumps are checked.

- A special region acts as a trampoline into the trusted region. Different slots are used to jump into different entry points in the trusted region. Note that the trampoline is inserted at load time and contains trusted code placed in the untrusted text segment.

![Diagram showing the use of trampolines to jump into trusted code](image)

Figure 1: Using trampolines to jump into trusted code
1.2 Returning from Trusted Code to Untrusted Code

- Returns from trusted code seem straightforward at first. However, there is a possibility of the module putting a rogue return address on the stack which can cause problems.

- A special region called a springboard handles a return.

1.3 Trampolines and Springboards

These special regions contain trusted code that enforce the calling convention between a module and the NaCl runtime.

1.3.1 Trampoline responsibilities

- Switch to trusted stack
- Move arguments and return address to trusted stack
- Jump to trusted code

1.3.2 Springboard responsibilities

- Switch to module stack
- Copy return values
- Check that return address is aligned and within range
- Jump to return address