


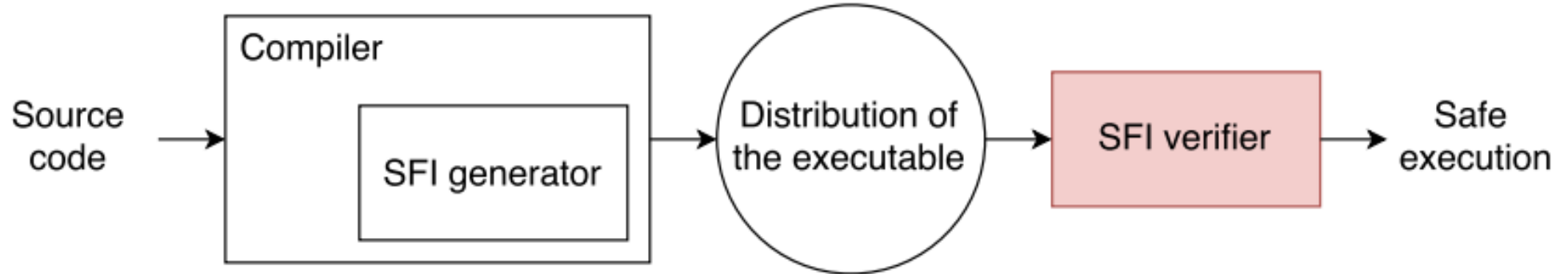
WASM SANDBOX

The security model of WebAssembly has two important goals: (1) protect users from buggy or malicious modules, and (2) provide developers with useful primitives and mitigations for developing safe applications, within the constraints of (1).

- WebAssembly Design

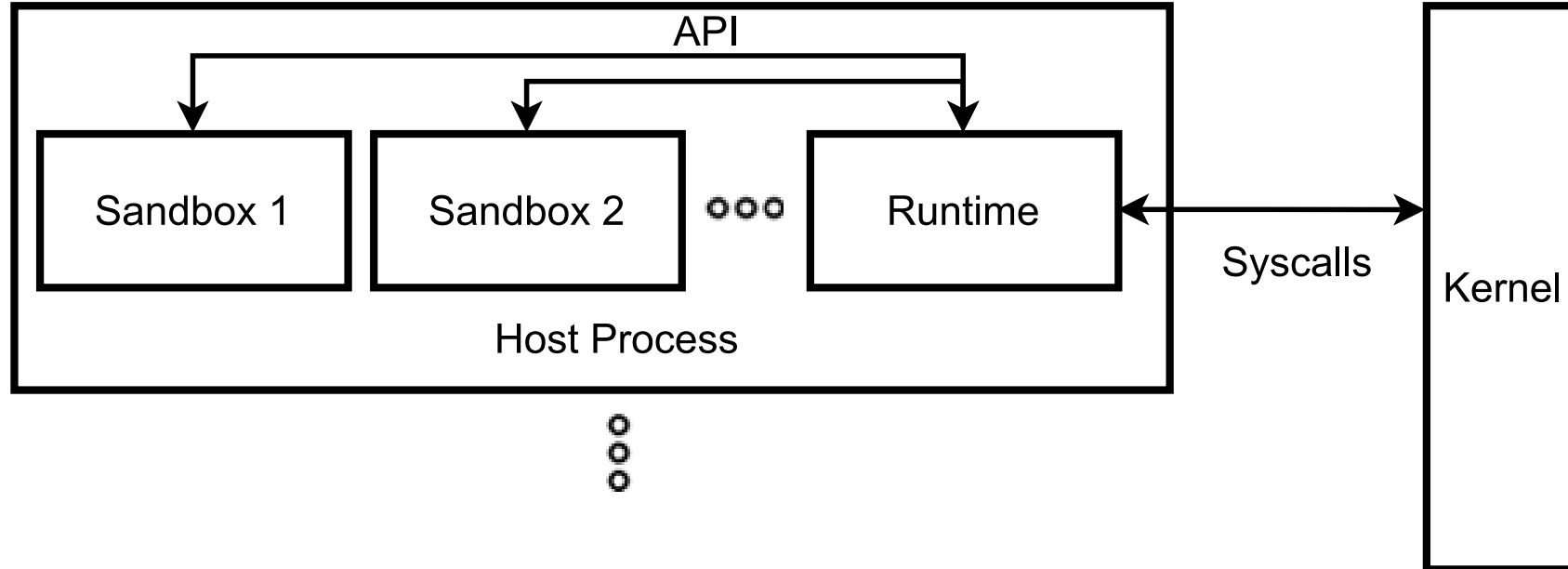
FIRST STEP TO SANDBOXING

 Trusted Computing Base



HOW DOES WASM GO ABOUT THIS

- Needs to be implemented by the runtime
- A runtime could potentially be implemented to give it full access to host



MEMORY IN WASM

- Linear memory is a continuous buffer of unsigned bytes
- Modules with potentially harmful code are prevented from accessing data outside their assigned linear memory space.
- The runtime system constantly monitors the size of each module's memory. It checks whether any memory access attempt by a module is confined within its pre-allocated memory boundaries.
- A module in WebAssembly is unable to intrude into the memory spaces of other modules, the runtime environment, or the operating system of the runtime, unless it has been explicitly authorized to do so.

```
use wasm_bindgen::prelude::*;

const WASM_MEMORY_BUFFER_SIZE: usize = 2;
static mut WASM_MEMORY_BUFFER: [u8; WASM_MEMORY_BUFFER_SIZE] = [0;
WASM_MEMORY_BUFFER_SIZE];

#[wasm_bindgen]
pub fn store_value_in_wasm_memory_buffer_index_zero(value: u8) {
    unsafe {
        WASM_MEMORY_BUFFER[0] = value;
    }
}

#[wasm_bindgen]
pub fn get_wasm_memory_buffer_pointer() -> *const u8 {
    let pointer: *const u8;
    unsafe {
        pointer = WASM_MEMORY_BUFFER.as_ptr();
    }

    return pointer;
}

#[wasm_bindgen]
pub fn read_wasm_memory_buffer_and_return_index_one() -> u8 {
    let value: u8;
    unsafe {
        value = WASM_MEMORY_BUFFER[1];
    }
    return value;
}
```

CONTROL-FLOW INTEGRITY

Safeguard against:

- Direct function calls: When a program directly calls a function.
- Indirect function calls: When a program calls a function indirectly, without specifying the exact target.
- Returns: When a function returns control back to the caller.

NOT A FREE LUNCH

- Memory Monitoring
- Control-flow integrity
- Unmapped pages
- And more...