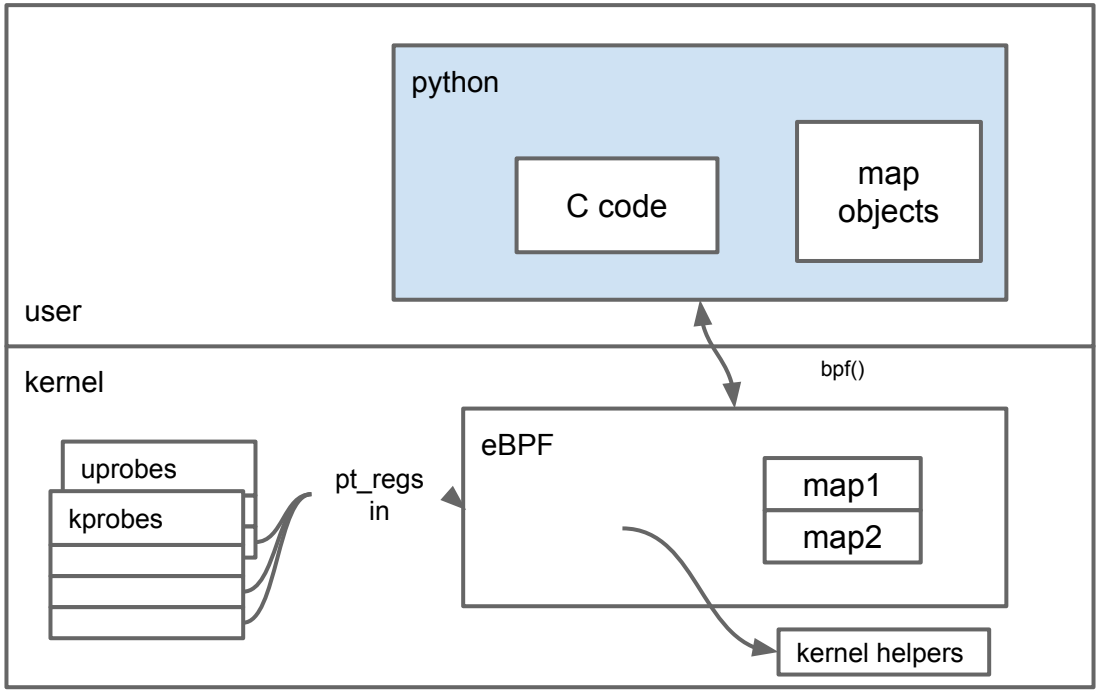
Definitions

- **BPF** (Berkeley Packet Filter) - Bytecode interpreter inside the kernel, now widely applicable besides original tcpdump use case
- **JIT** (Just In Time) - Converts BPF bytecode to native instructions
- **BPF Verifier** - Runtime sanitizer in the kernel that guarantees safety of bytecode
- **KProbe** - “Breakpoint” inside the kernel, can be set at nearly any function or instruction
- **UProbe** - Generic userspace breakpoint similar to kprobe, works without gdb and friends
- **Tracepoint** - Pre-defined kernel tracing locations, can be enabled through /sys/kernel/debug/tracing/events

IO Visor Block Diagram



Hello, World!

```
#!/usr/bin/python
from bcc import BPF
BPF(text='''void kprobe__sys_clone(void *ctx) {
    bpf_trace_printk("Hello, World!\\n");
}''').trace_print()
```

Requirements

- >= 4.0 kernel
- python-bcc (github.com/iovisor/bcc)
- Kernel header files
- *Don't* need kernel debug symbols
- *Don't* need kernel sources