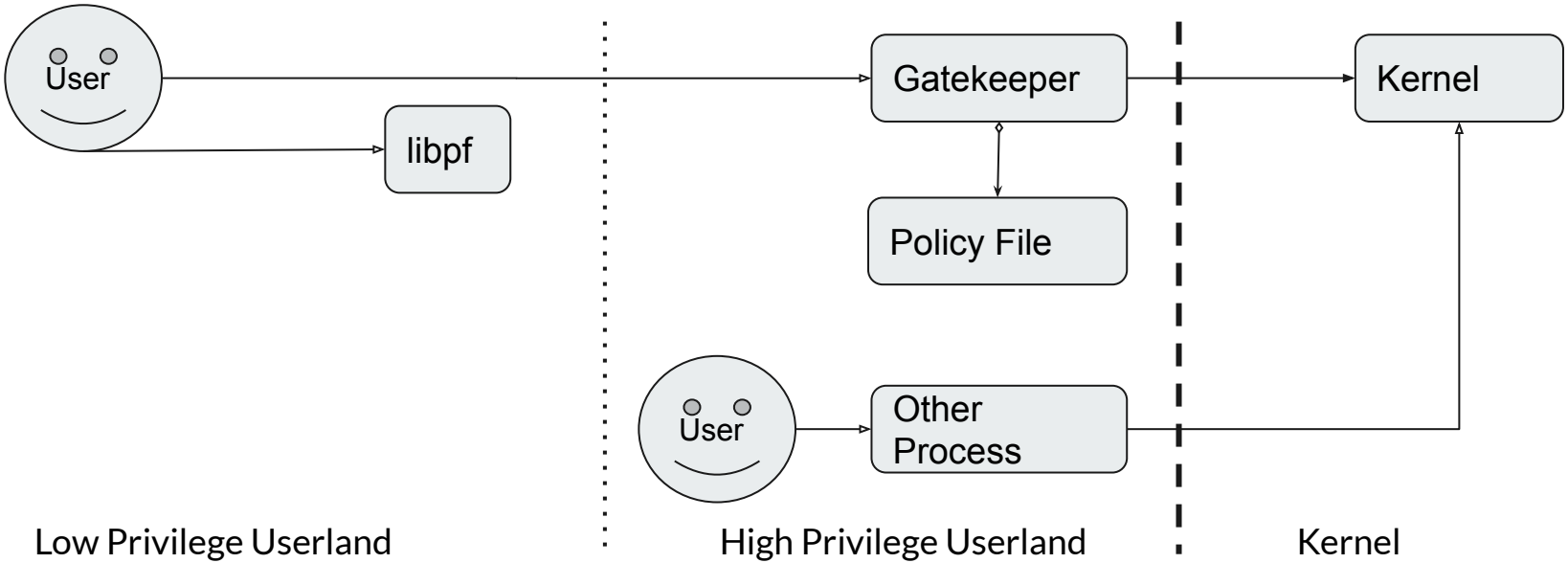
EBPF Policy

Signatures might be the answer

Motivation

- Allow for identity based policy
- Allow for capabilities to be added for granular restrictions
- Allow restrictions for program intent
- Allow for less privileged tasks to initiate eBPF?
    - This may could be dangerous

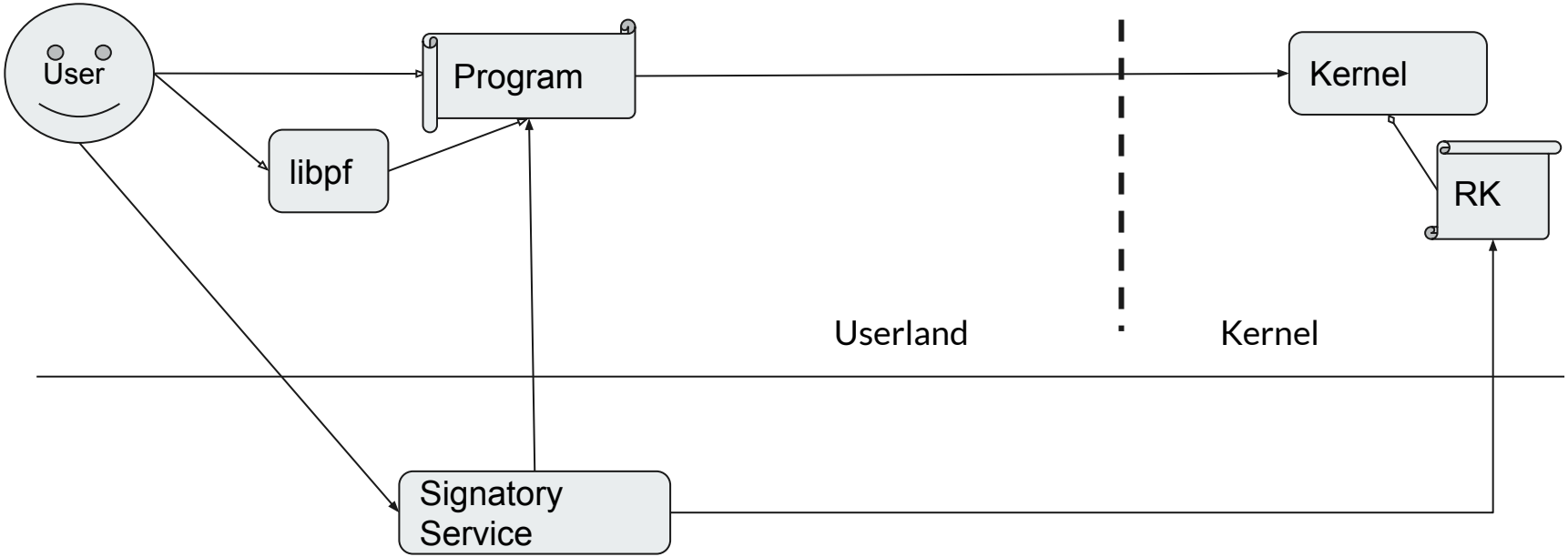
Partial Workflow - Gatekeeper



Signature High Level Idea

- Add an instruction to indicate code signing to the byte code
- Format would be something like
- CodeSign Instruction + Signature + Signature Extensions + eBPF Program
- Signed Payload should be extensible (Policy & Identity)
    - Allow for capability restrictions signed with eBPF program
    - Allow binding identity
    - Allows for a lower privilege user to run a vetted program
- Kernel flags for enforcing signatures and the default trusted public key

Possible Workflow - Signed



Open Questions

- Does the identity model break down somehow with cgroups?
- Revocation lists?
- Time bounded credentials?