Secured Routines:

Language-based Construction of Trusted Environments

Adrien Ghosn, James R. Larus, Edouard Bugnion
EPFL, Switzerland
TEE-Support Challenges

- **Performance**
  - TCB size
  - Coop
  - crossings

- **Security**
  - secret leak
  - syscalls

- **Usability**
  - Partition
  - legacy apps

Partition, Coop, syscalls, secret leak,
func main() {
    go foo()
    ...
}

Go Execution Model

Go Runtime
func main() {

gosecure foo()

...
}

Go Runtime

Trusted Runtime

Go channel
GOTEE

Compile-time
Run-time

Memory Isolation

Minimal TCB

Automatic code & data partitioning

cross-domain channels

Performance

Security

Usability

memory leaks

TCB size

Syscalls

Coop

Partition

crossings

Transparent syscalls

Runtime Cooperation

Minimal code changes

System cooperation

Minimal TCB

Automatic code & data partitioning

cross-domain channels