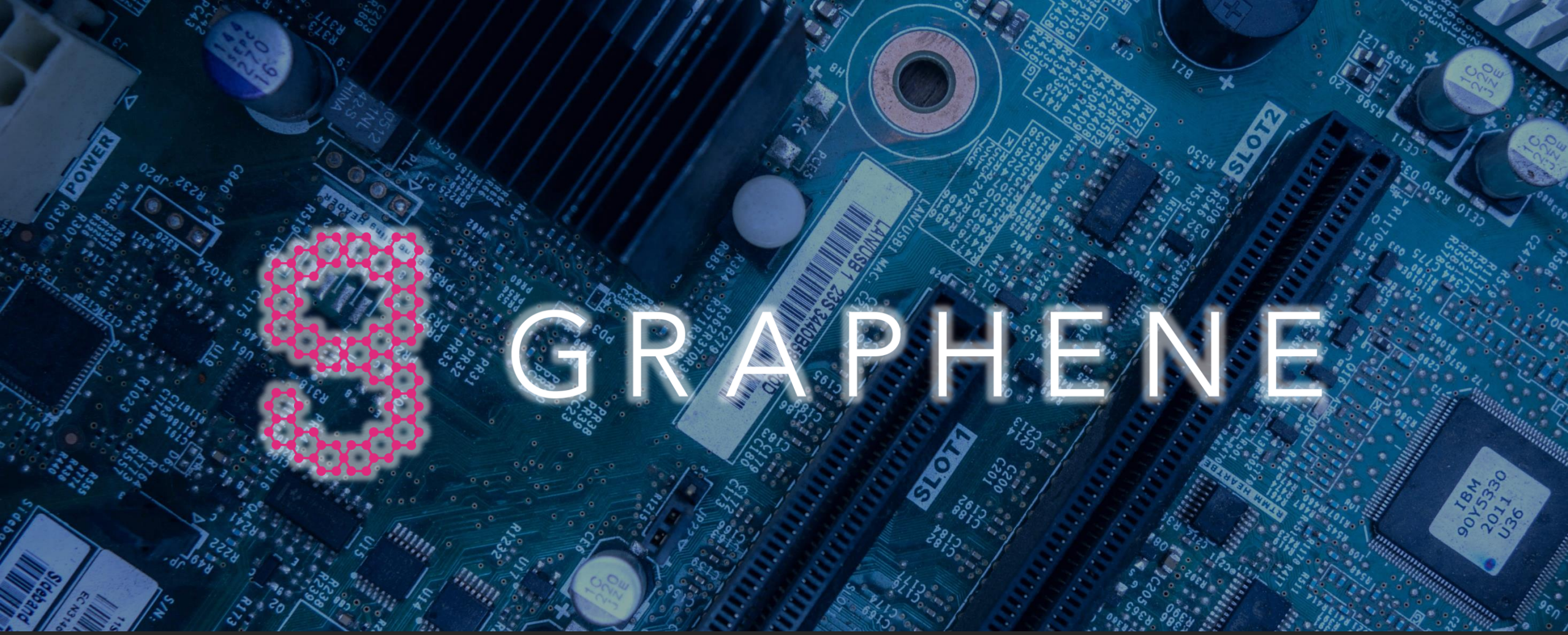


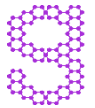
Graphene v1.0: Toward A Reliable, Open-Source Library OS for SGX

CHIA-CHE TSAI

TEXAS A&M / GRAPHENE PROJECT

This Talk Includes:

1. WHAT's Graphene, WHY, and HOW
2. Latest updates
3. Our future roadmap



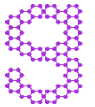
GRAPHENE

SGX Is Not For "Dummies"

Developing a SGX application is hard

- Setup and configuration
- Porting legacy code
- OS interfaces and libraries
- Security implications
- Debug and performance tuning

You have to be a:
system admin
+ Linux/libc maintainer
+ security expert
+ computer architect?

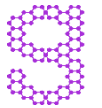


GRAPHENE

What IS Graphene?

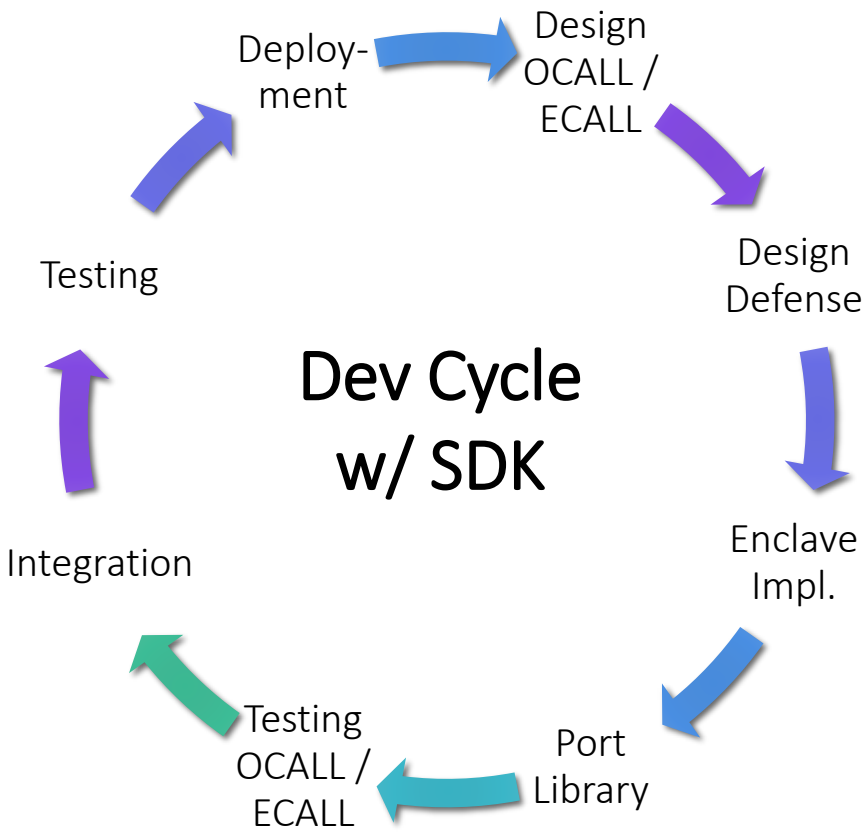
A system that runs unmodified* Linux apps on platforms like SGX.

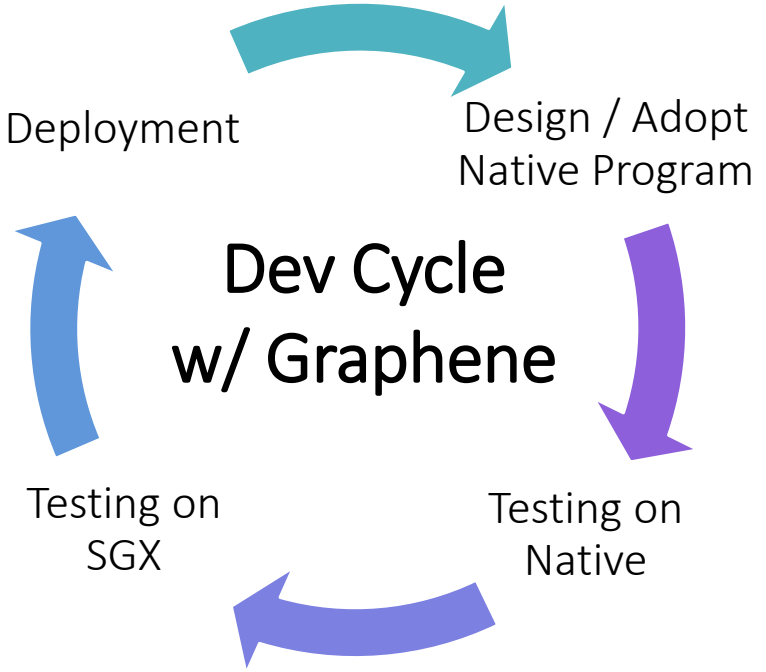
* Native binaries, no code change, no recompile



GRAPHENE

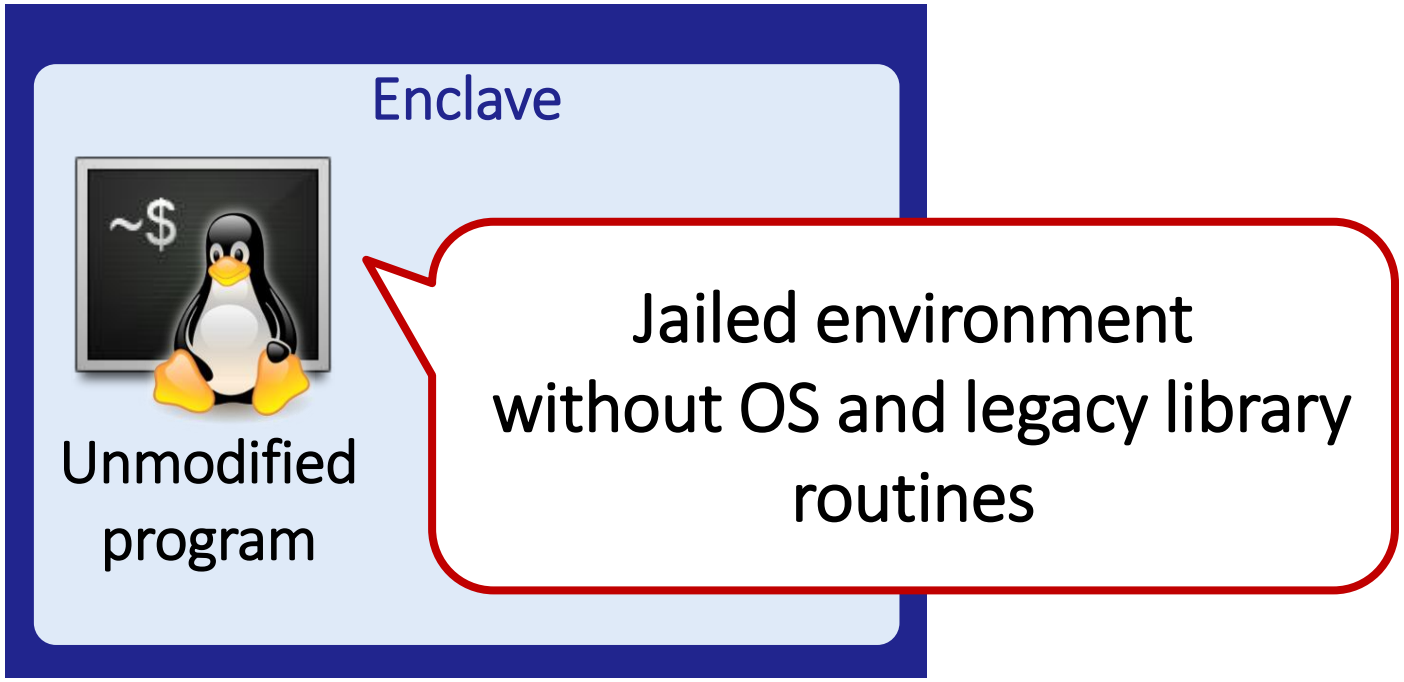
Can We Improve the Dev Cycles?





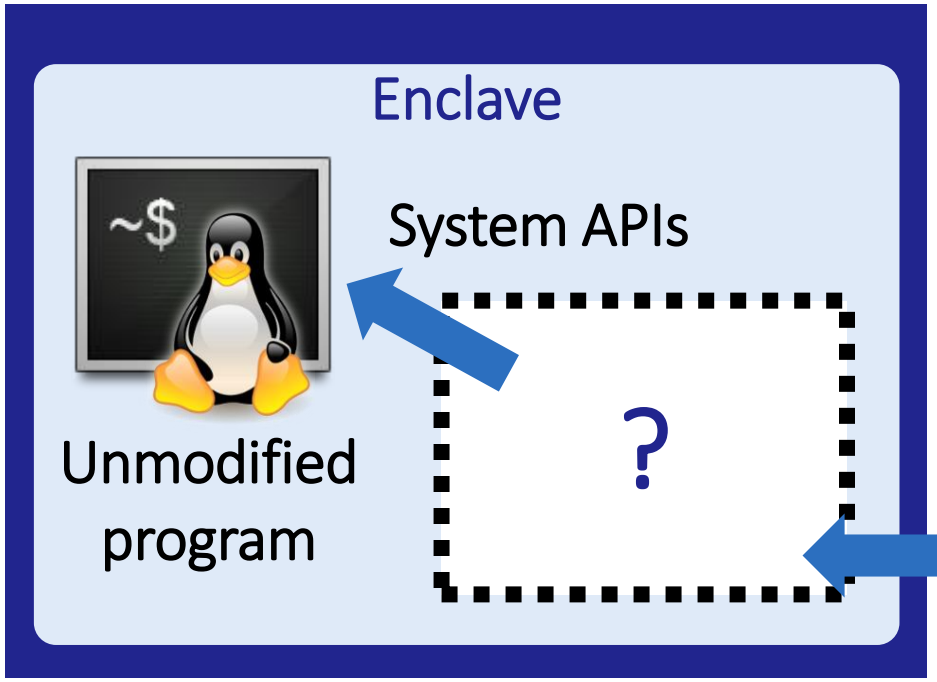
GRAPHENE

The LibOS Approach



GRAPHENE

The LibOS Approach



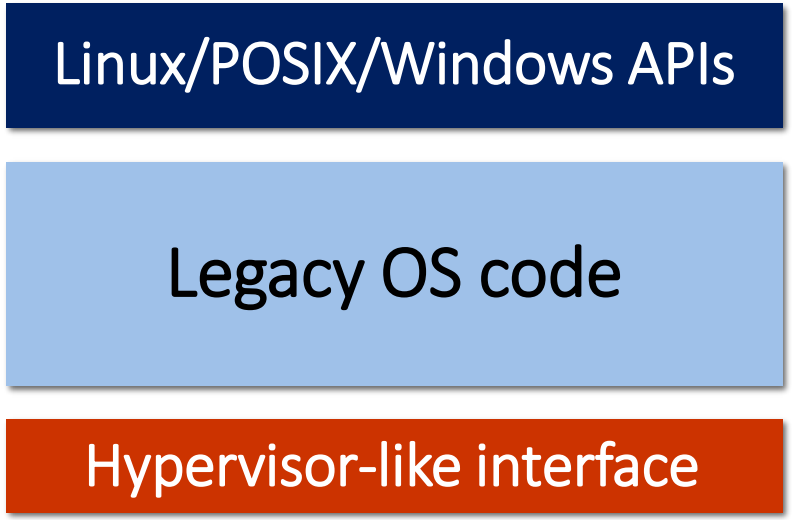
Broadly speaking,
lots of SGX frameworks qualify
for this definition
(Haven, SCONE, SGX-LKL, …)

Untrusted
Host OS

GRAPHENE

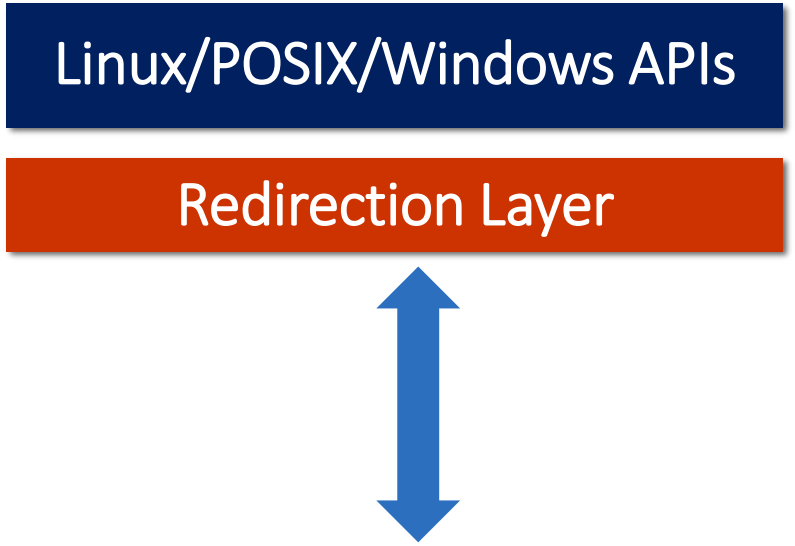
How Are "LibOSes" Generally Built?

Haven / SGX-LKL



Untrusted Host OS

SCONE

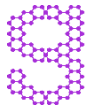


Untrusted Host OS

GRAPHENE

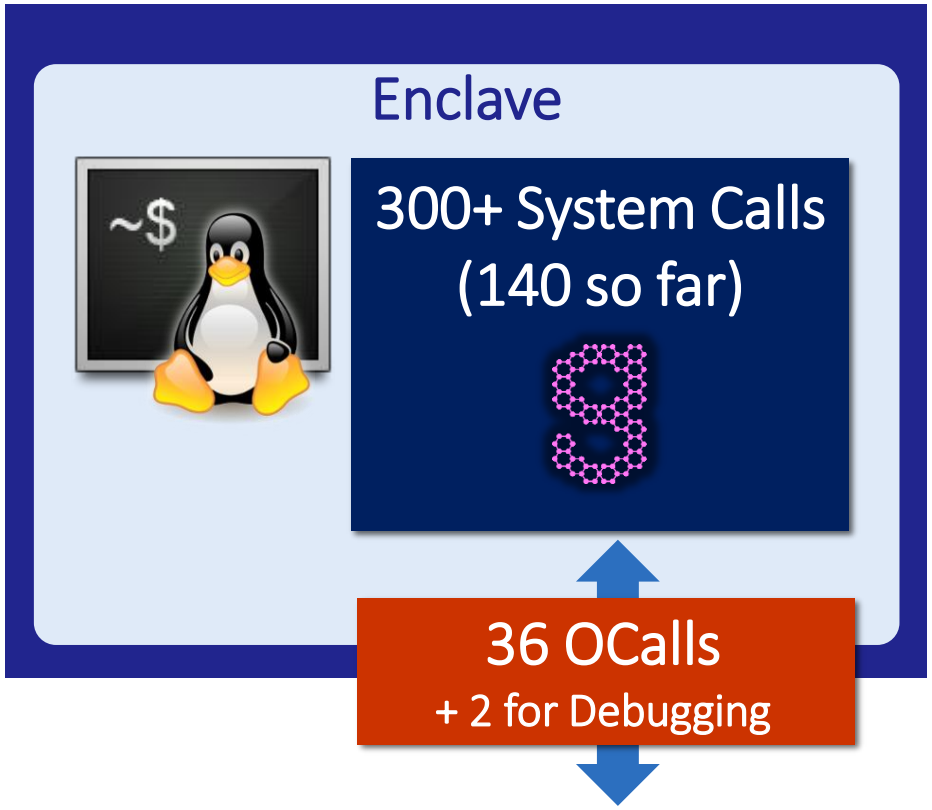
How is Graphene Different?

1. Host interface defined with portability and security in mind
2. Rich functionality for Linux apps



GRAPHENE

Graphene: A Tailored LibOS

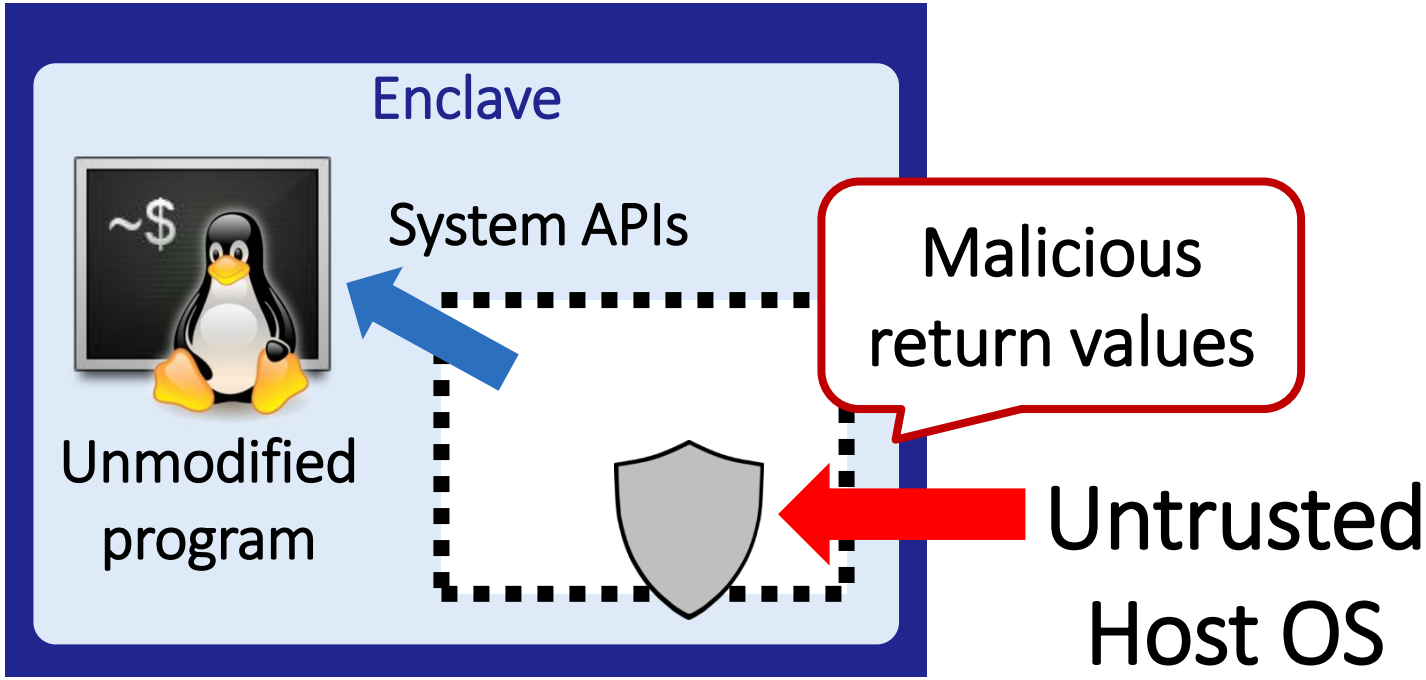


Step 1.
Define a host interface

Step 2.
Reimplement Linux APIs from scratch

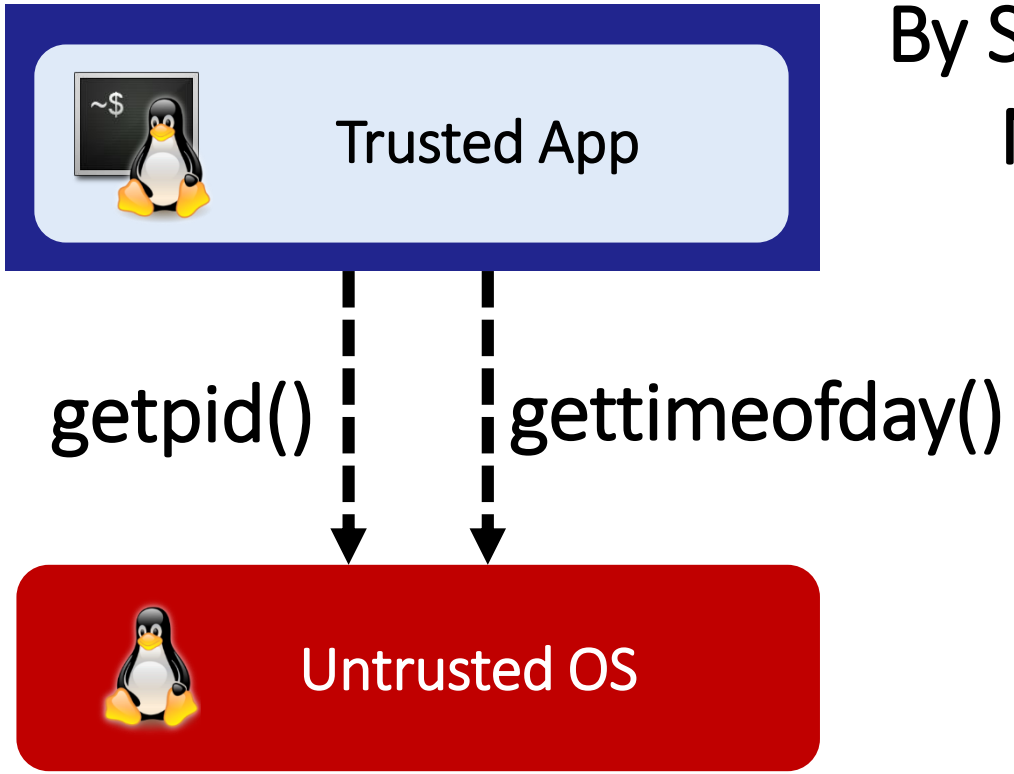
GRAPHENE

Why Host Interface Matters?



GRAPHENE

Iago Attacks [ASPLOS 2013]



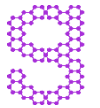
By SGX / Inktag / Overshadow / Nexus / Virtual Ghost / …

App uses malicious results for sensitive operations:
Example:
Seed the RNG with (PID|TIME)

GRAPHENE

In A Nutshell

Iago attacks are semantics vulnerabilities caused by mistrusting legacy APIs

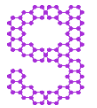


GRAPHENE

More Examples

Iago attacks are pervasive and often hard to mitigate

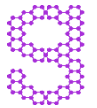
- File system metadata
- System time
- IPC (signals, message queues, shared memory)
- Scheduling
- System info (/proc, /sys, getrusage)
- Exception handling



GRAPHENE

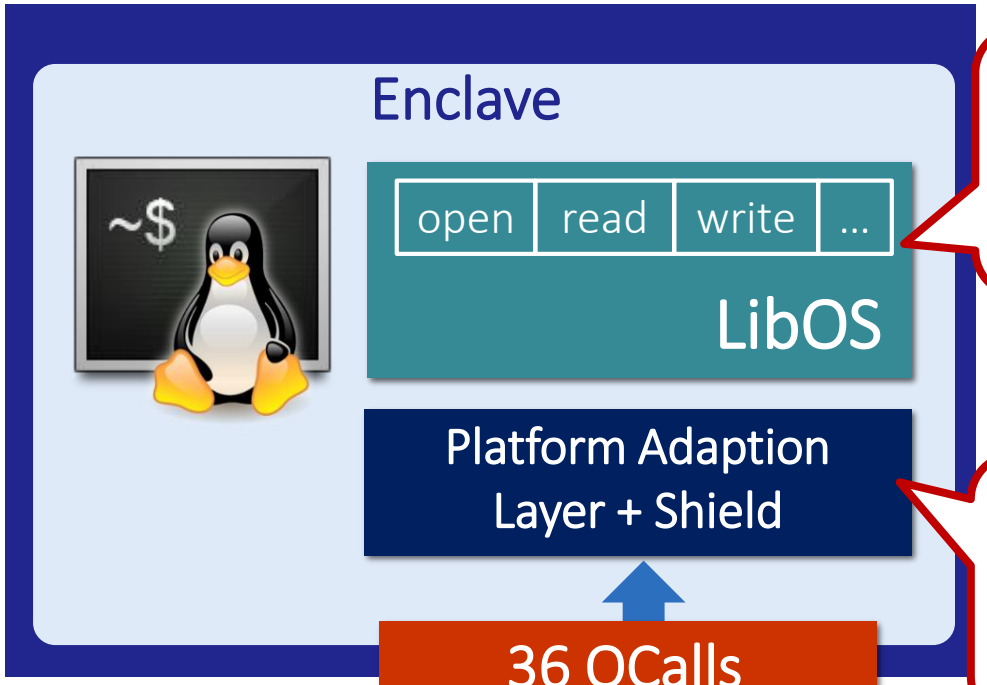
Myths About Iago Attacks

1. Only system calls can suffer Iago attacks - wrong
2. Just leave to app developers - wrong
3. Orthogonal to system/runtime design - wrong



GRAPHENE

Decouple Shielding & Linux APIs

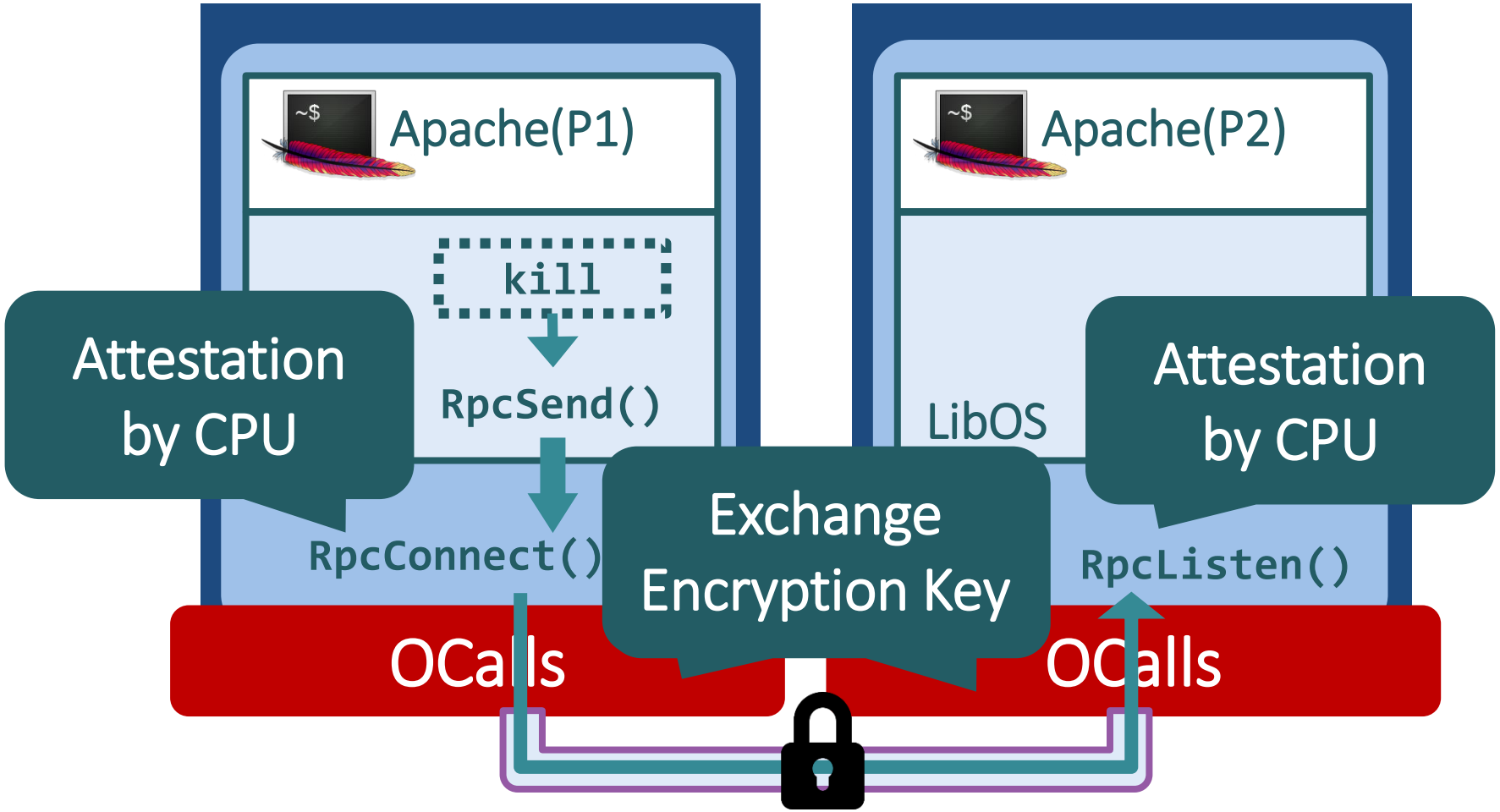


Linux functionality

Portability & shielding
(Explicit semantics + crypto checks)

GRAPHENE

Multi-Process Applications

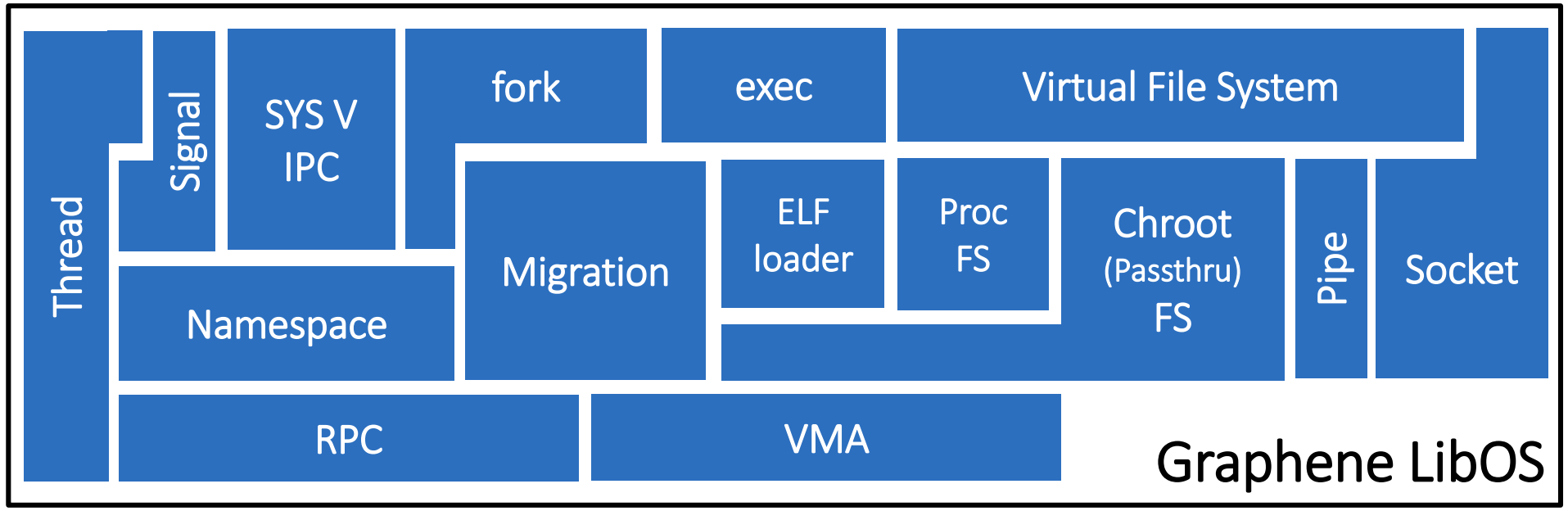


Distributed OS coordination

Supported:
fork/exec
signals
message queue
Semaphore

GRAPHENE

More LibOS Features



140 / 318 system calls
Implemented (core features)

63 KLOC
Source code

1.4 MB
Library size

GRAPHENE

Tested Applications

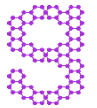
… and more.

See examples on: https://github.com/oscarlab/graphene

GRAPHENE

Graphene Project Updates

1. Open-source workgroup
2. Stable release plan (mid-August)
   - Reliability & Security improvements
   - New features



GRAPHENE

Graphene Workgroup

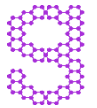
https://grapheneproject.io/

GRAPHENE

Stable Release (Mid-August)

Reliability improvements:

- 324 pull requests since Nov 2018
- Rewritten: memory mgmt., signal handling, IPC, and file system
- Data races and deadlock issues
- Better OCall interface and enclave initialization
- Documentation & UX improvements

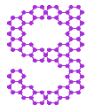


GRAPHENE

Stable Release (Mid-August)

Vulnerability fixes:

- Received multiple reports from KU Leuven and U. Birmingham
  - Untrusted argv/envp
  - Untrusted memory allocation
  - Untrusted argument copy for OCalls
  - TOCTOU for untrusted copy
  - Incorrect pointer validation
- **All fixed within 5 days**

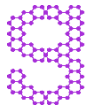


GRAPHENE

Stable Release (Mid-August)

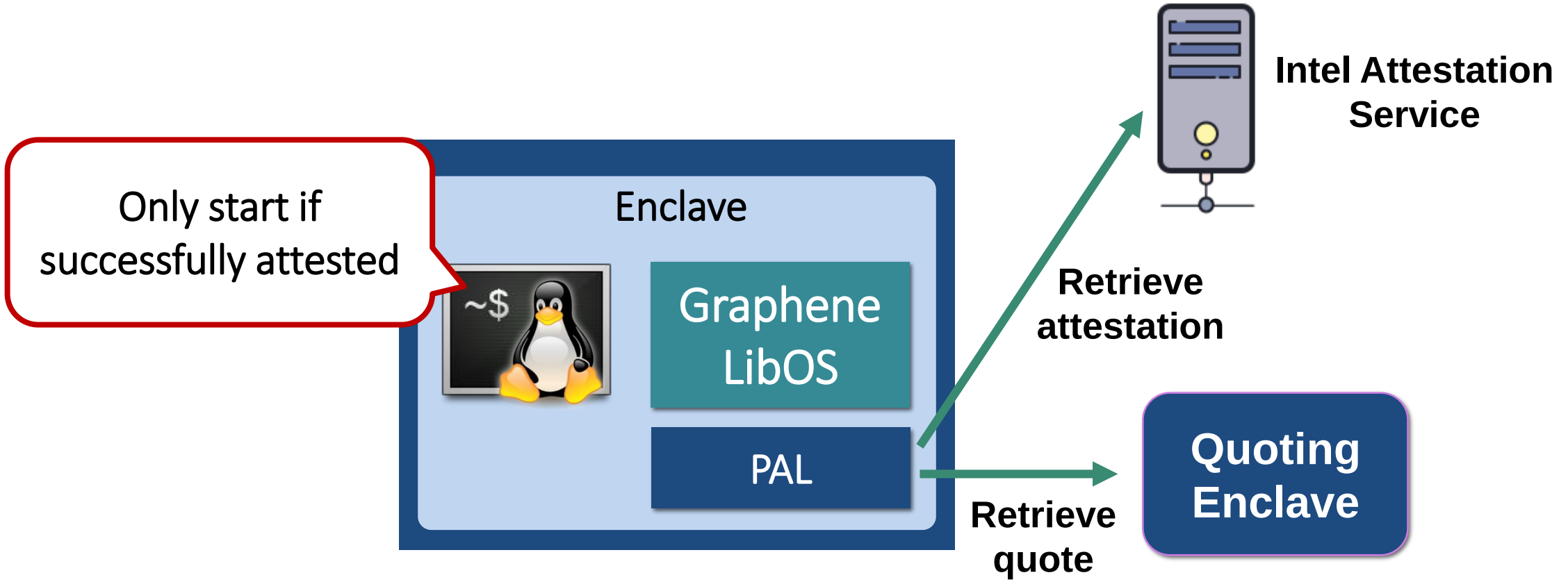
New features:

- Support for GLIBC 2.23 / 2.27 and Ubuntu 18.04
- Static binary support for Golang support
- Simple remote attestation
- EXPERIMENTAL:
  Docker integration (Graphene Secure Container)
- EXPERIMENTAL:
  File system & network shield (RA-TLS) plugins



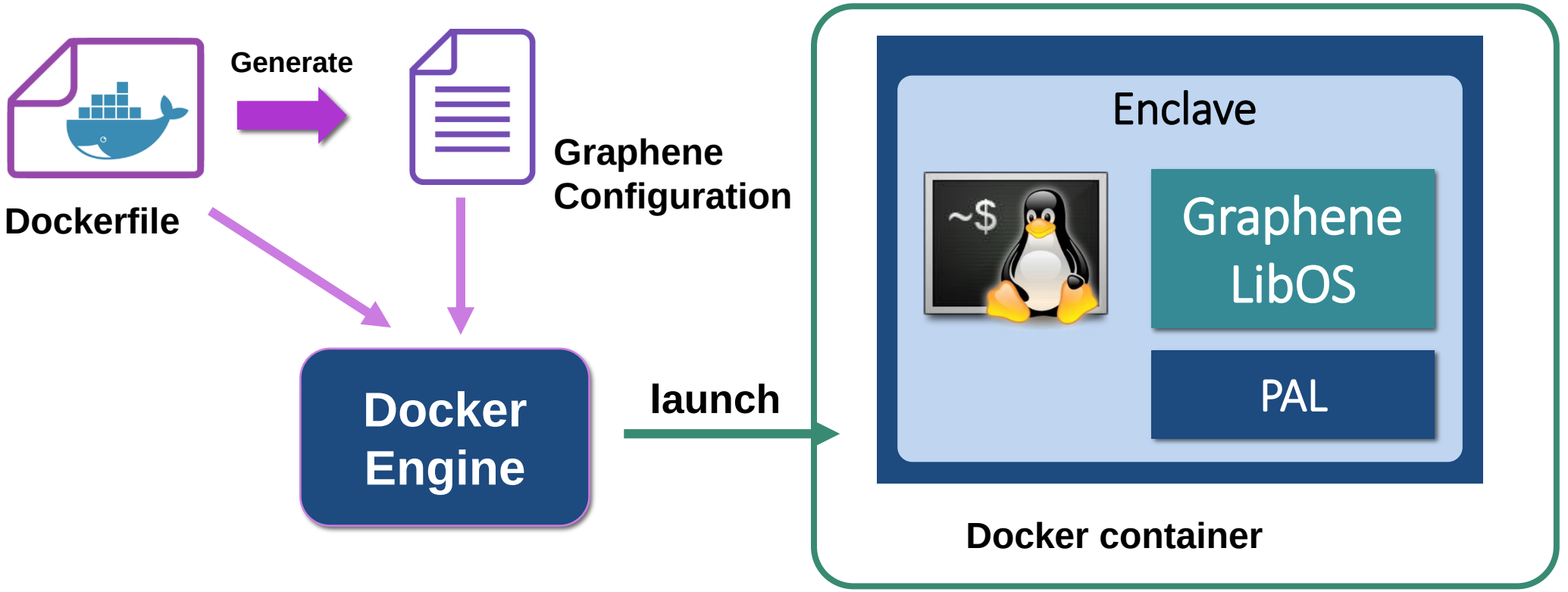
GRAPHENE

Remote Attestation



GRAPHENE

Docker Integration (EXPERIMENTAL)



GRAPHENE

Future Roadmap

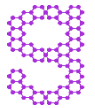
Periodic stable releases

File system shield and network shield (RA-TLS)

SGX2 (EDMM) support

Exitless enclave interface (optimization)

Support for upstream Linux driver



GRAPHENE

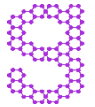
Conclusion

Why you should consider Graphene:

- Open-sourced (LGPL), good for customization and exploration
- Actively maintained by workgroup & community
- Tailored for small host interface and rich Linux functionality

https://grapheneproject.io

support@graphene-project.io



GRAPHENE