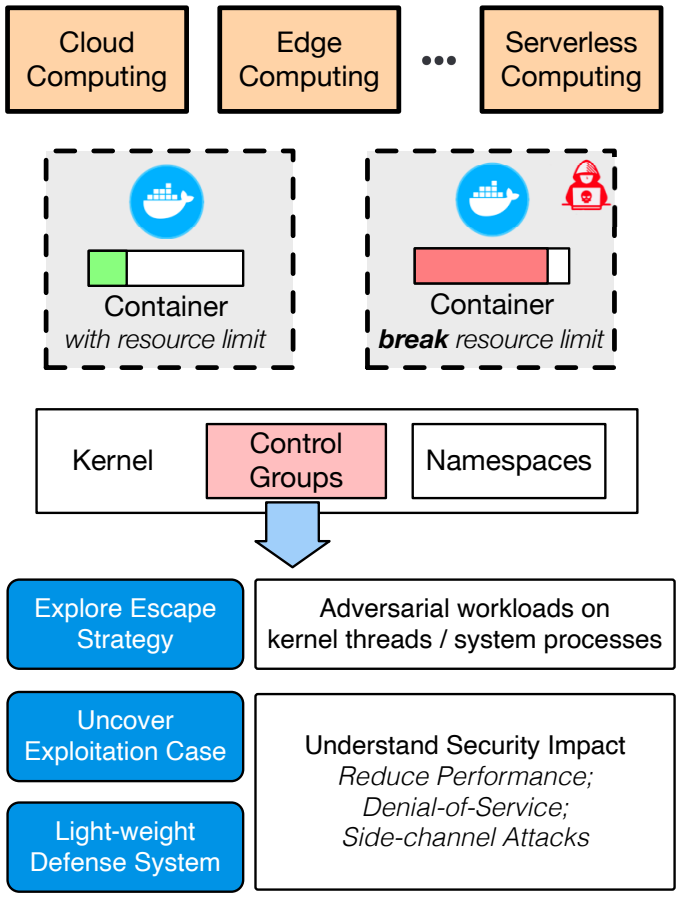
CRII: SaTC: Securing Containers in Multi-Tenant Environment via Augmenting Linux Control Groups

Challenge:

- Linux containers leverage control groups to apply resource limits to each container instance.
- Containers might break the resource rein of cgroups, generate extra workloads, and exhaust system resources.
- It is difficult to uncover potential exploitations available inside containers, understand their impact, and finally mitigate them.

Solution:

- Explore kernel mechanisms that can generate out-of-band workloads via processes de-associated from their originating cgroups.
- Develop automated testing-based framework to dynamically identify adversarial workloads using diverse strategies.
- Shrink attack surfaces by reinforcing cgroup inheritance mechanisms with advanced policies.



Scientific Impact:

- Enforce isolation mechanisms in Linux containers.
- New tools developed to uncover vulnerabilities in container technologies.
- Improve the awareness of security issues raised by shared resources in OS-level virtualization.

Broader Impact and Broader Participation:

- Benefit containerization component developers to enhance their products.
- Benefit cloud vendors to secure their services.
- Teach students about container techniques and their security issues.
- Multiple vulnerabilities reported and fixed in container runtime.

NSF CNS-2054657; PI: Xing Gao

Assistant Professor, Department of Computer and Information Sciences, University of Delaware

Website: https://xgao-work.github.io/