Contribution ID: **254**   Type: **not specified**

Securely Migrating Untrusted Workloads with CRIU

Tuesday, 13 November 2018 15:15 (15 minutes)

While deploying a CRIU-based transparent checkpoint/restore task migration infrastructure at Google, one of the toughest challenges we faced was security. The infrastructure views the applications it runs as inherently untrusted, yet CRIU requires expansive privileges at times in order to successfully checkpoint and restore workloads. We found many cases where malignant workloads could trick CRIU into elevating their privileges during checkpoint/restore. We present our experience in securely checkpointing and restoring untrusted workloads with minimal Linux privileges while enabling the bulk of CRIU functionality. We'll discuss changes required to enable this usecase and make the case for an increased emphasis on security in checkpoint/restore.

I agree to abide by the anti-harassment policy

Presenter: BURNY, Radoslaw (Google)

Session Classification: Containers MC