SEV-SNP Live Migration and VMM/KVM API Implications

Pankaj Gupta & Tom Lendacky
Migration Initialization

1. Dest QEMU started
   - SVSM generates public/private key pair
   - SVSM generates attestation report
     - Hash of public key as report data
   - SVSM provides attestation report, public key, and certificate data (collectively, migration data)

2. Src QEMU initiates migration
   - SVSM receives Dest SVSM migration data
   - SVSM validates Dest SVSM attestation report
   - SVSM initializes migration state
   - SVSM generates transport key, encrypts using Dest SVSM public key, and sends to Dest SVSM
Migration of Pages

1. Src QEMU
   - Shared pages
     - Transfers in traditional manner
   - Private pages
     - SVSM encrypts page with transport key
     - SVSM returns page with metadata
     - SVSM provides encrypted page and metadata

2. Dest QEMU
   - Shared pages
     - Handles in traditional manner
   - Private pages
     - SVSM processes page based on metadata
Migration Completion

1. Src QEMU
   - Remaining memory pages that still need to be migrated
   - Private state
     - SVSM prepares vCPU pages
     - SVSM prepares required SVSM state
     - Transfers encrypted pages and metadata

2. Dest QEMU
   - Handles remaining memory pages
   - Private state
     - SVSM processes final metadata
New APIs

VMM
• Migration Initiation
  • Provide migration verification data
  • attestation report, etc.
  • Send migration transfer data
  • transport key, etc.

• Migration
  • Support for GMEM allows VMM to know what pages are Shared vs. Private
  • For Private pages
    • Need VMM API to send and receive the private page metadata and wrapped page(s)

• Migration Completion
  • Need VMM to receive final state

KVM
• Migration Initiation
  • Generate migration verification data
  • attestation report, etc.
  • Validate and create migration transfer data
  • transport key, etc.

• Migration
  • For Private pages
    • Need KVM API to package an encrypted page (transport encrypted with metadata)
    • Need KVM API to receive and process metadata and wrapped page(s)

• Migration Completion
  • Need KVM API to package final guest state (vCPU data, etc.) and any SVSM state (vTPM, etc.)
  • Need KVM API to process final state