USING TRUSTED EXECUTION ENVIRONMENTS ON HIGH-PERFORMANCE COMPUTING PLATFORMS

Ayaz Akram, Anna Giannakou, Venkatesh Akella, Jason Lowe-Power, Sean Peisert
Secure High-Performance Computing

How to compute with large sensitive data?
Biomedical data
Proprietary data

Secure from both external and internal threats
Integrity or confidentiality or both
High-Performance Computing Workloads

Common characteristics
- Large data sets (10s–100s GB per node)
- Limited user interaction (batch)
- Often highly multithreaded

Dedicated (super computers) or shared (cloud) nodes

Diverse compute, memory, and security requirements
We Analyze Two TEEs

<table>
<thead>
<tr>
<th>Technology</th>
<th>Ensures Integrity</th>
<th>TCB Size</th>
<th>Secure Memory Size</th>
<th>Application Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel SGX</td>
<td>Yes</td>
<td>Small</td>
<td>128 MB (useable: 94MB)</td>
<td>Required</td>
</tr>
<tr>
<td>AMD SEV</td>
<td>No</td>
<td>Large</td>
<td>Up to RAM size</td>
<td>Not Required</td>
</tr>
</tbody>
</table>

Methodology

• Benchmarks used: NAS parallel benchmarks, LightGBM and GAPBS
• Platforms used: Intel Core i7-8700 (12 threads/socket) for SGX and AMD EPYC 7451 (dual socket with 48 threads/socket) for SEV study
• Use of SCONE (SGX) and Kata (SEV) containers
• Measured slowdown of the used workloads under secure execution on both platforms
• Relate the slowdown to other collected metrics
Performance Impact of SGX

High slowdown, especially for graph workloads

NPB (Class C)  GAPBS (synth)  GAPBS (road)  LGBM (mslr)
Enclave Page Cache (EPC) Faults

Threads=6

NPB (Class C)  GAPBS (synth)  GAPBS (road)  LGBM (mslr)

Threads=6

EPC Faults (PMI)

360  500

Slowdown

npb  gapsbs_synth  gapbs_road  lgbm_mstr

gmean

Slowdown

npb  gapsbs_synth  gapbs_road  lgbm_mstr

gmean
Enclave Page Cache (EPC) Faults

All the benchmarks have large resident memory except ep & tc_synth
Impact of Increasing Execution Threads (under SGX)

Don't scale well, as they have large resident memory
Impact of Increasing Execution Threads (under SGX)

Scales normally under SGX and has a small memory footprint
Performance Impact of SEV

NPB (Class C) | GAPBS (synth) | GAPBS (road) | LGBM (mslr)
Virtualization appears to be the biggest reason of slowdown
Preliminary Takeaways

Future TEEs should support HPC apps

Smaller slowdowns for SEV

Performance issues for SGX
  EPC faults
  Multiple execution threads

Dynamic choice of threat model