Hypervisor-based Background Encryption

Yushi Omote, University of Tsukuba

Background & Problem

Full-Disk Encryption (FDE) is an effective technique for prevention of data breach!

OS-based Approach (BitLocker, Compusec, ...)

- Common today!
- Easy installation & Background encryption.
- OS vulnerability!
- OS dependency!

Hypervisor-based Approach (BitVisor [VEE'09], TCVisor [ICITST'10])

- Enhanced security!
- OS independency!
- High deployment cost!
- No background encryption!
- (Partitioning, P2V, Manual Encryption for hours...)

Approach

Pass-through-based Thin Hypervisor.

- No P2V!
- No Partitioning!

Hypervisor-based Background Encryption!

- No Manual Encryption!

Challenge 1: Storage sharing with guest OS.
1.) Carefully insert hypervisor’s I/O requests between guest’s I/O requests.
2.) Prevent data corruption by I/O scheduling.

Challenge 2: Encryption-speed moderation.
Monitor guest activities from the hypervisor layer (Interrupt freq., I/O freq.) to determine the encryption speed.

Evaluation Results

1.) Several minutes installation of hypervisor-based encryption!
2.) Reasonable disk throughput with moderation!
3.) Good application benchmark result!

- Read
- Write
- Unencrypted

- 1M Seq.
- 4K Rand.

Future work

Auto optimization of criteria for encryption-speed moderation.

Intel Core 2 Quad Q9550 2.83GHz / 4GB RAM / 1TB HDD 7200rpm / Windows 7 32bit. Benchmark Tools: Crystal Disk Mark, PCMark.