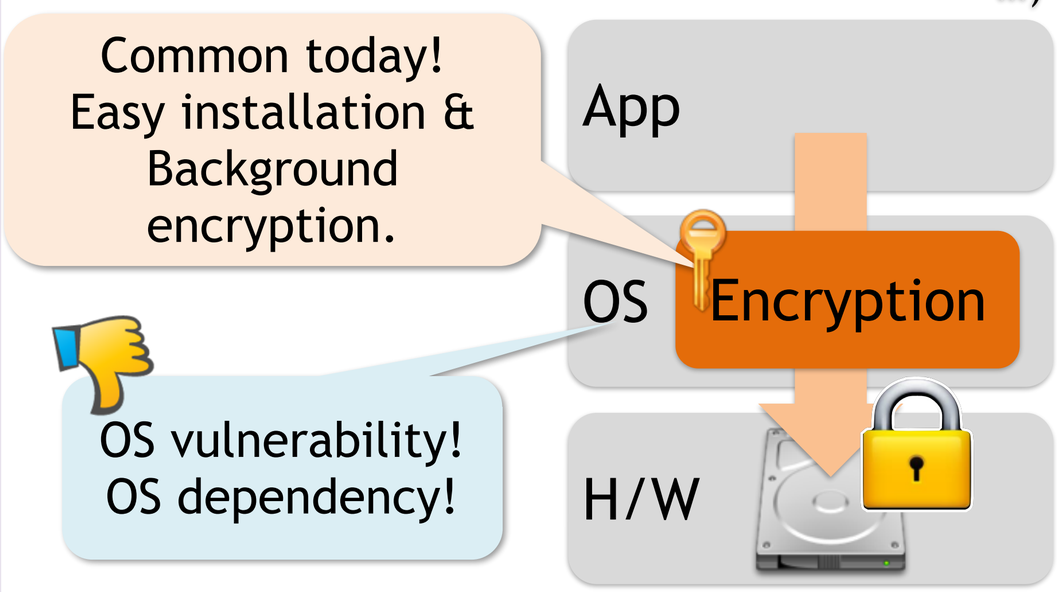
Hypervisor-based Background Encryption

Yushi Omote, University of Tsukuba

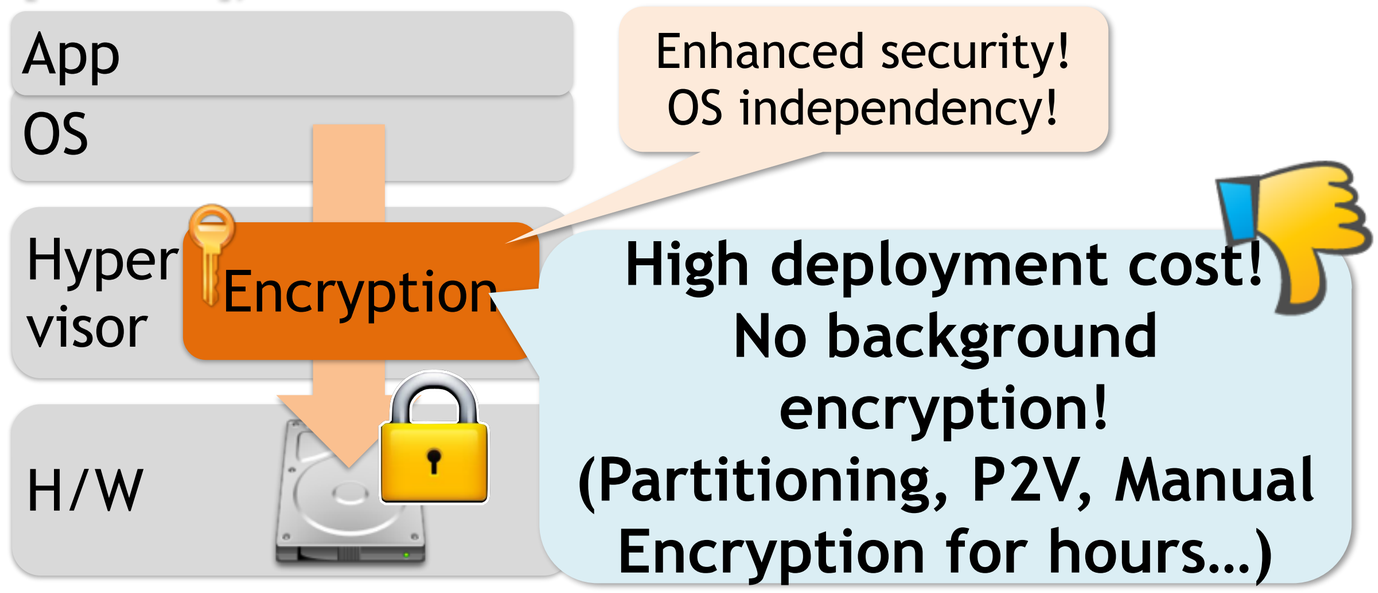
Background & Problem

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

OS-based Approach (BitLocker, Compusec, …)

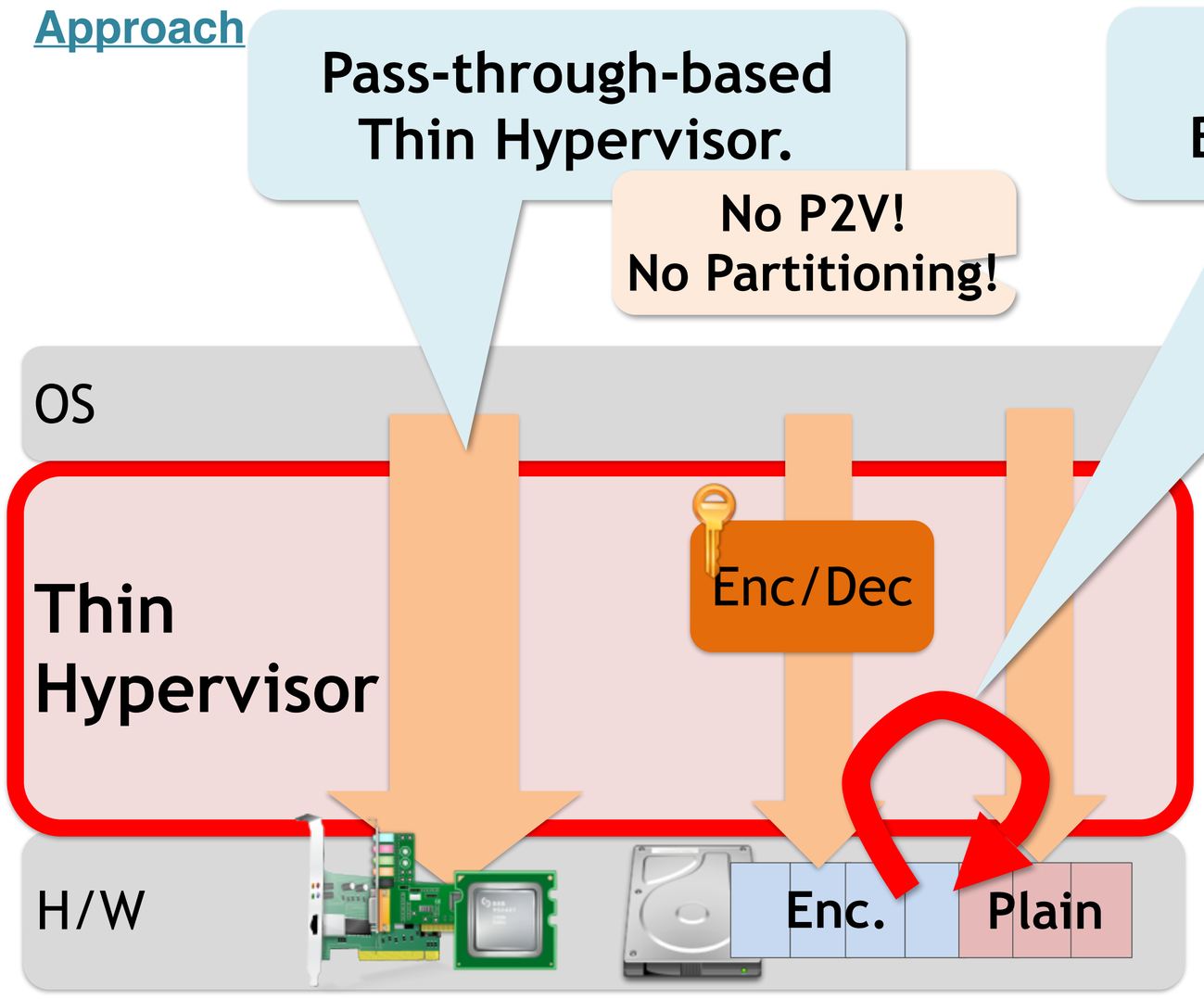


Hypervisor-based Approach (BitVisor [VEE'09], TCVisor [ICITST'10])



Goal Quick deployment of hypervisor-based encryption.

Approach



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.

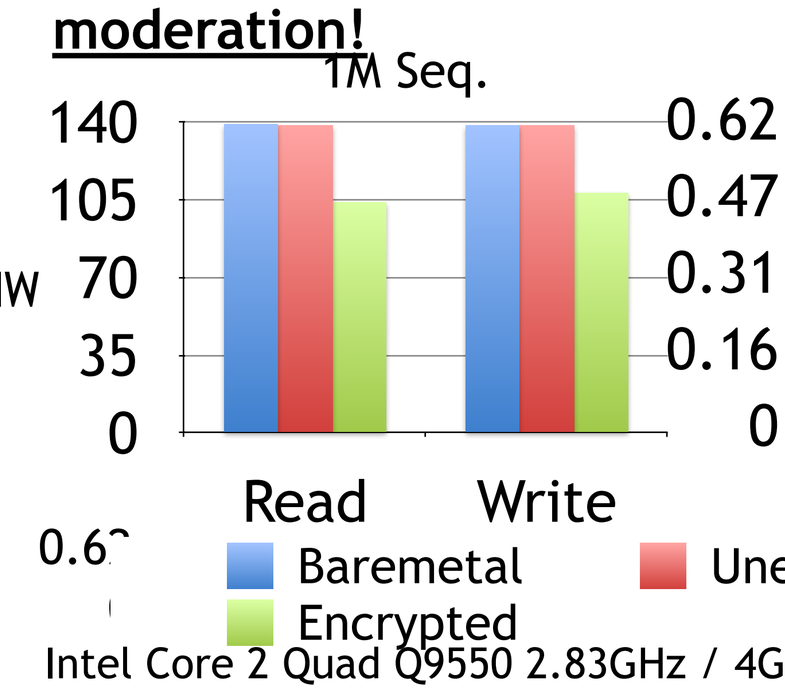
Challenge 2 Encryption-speed moderation.

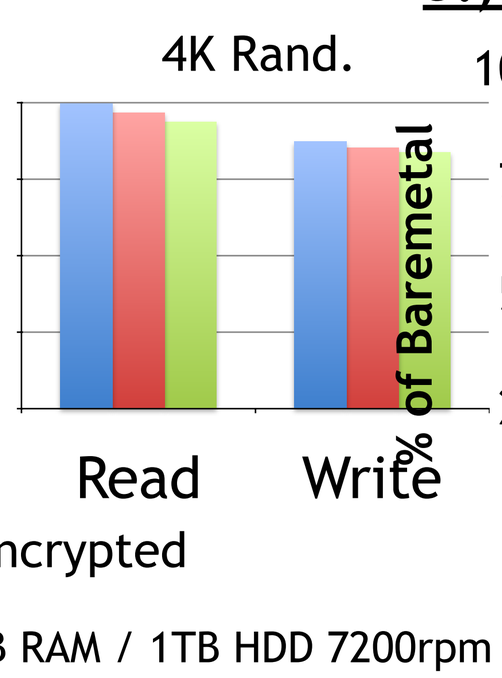
Monitor guest activities from the hypervisor layer (Interrupt freq., I/O freq.) to determine the encryption speed.

Evaluation Results

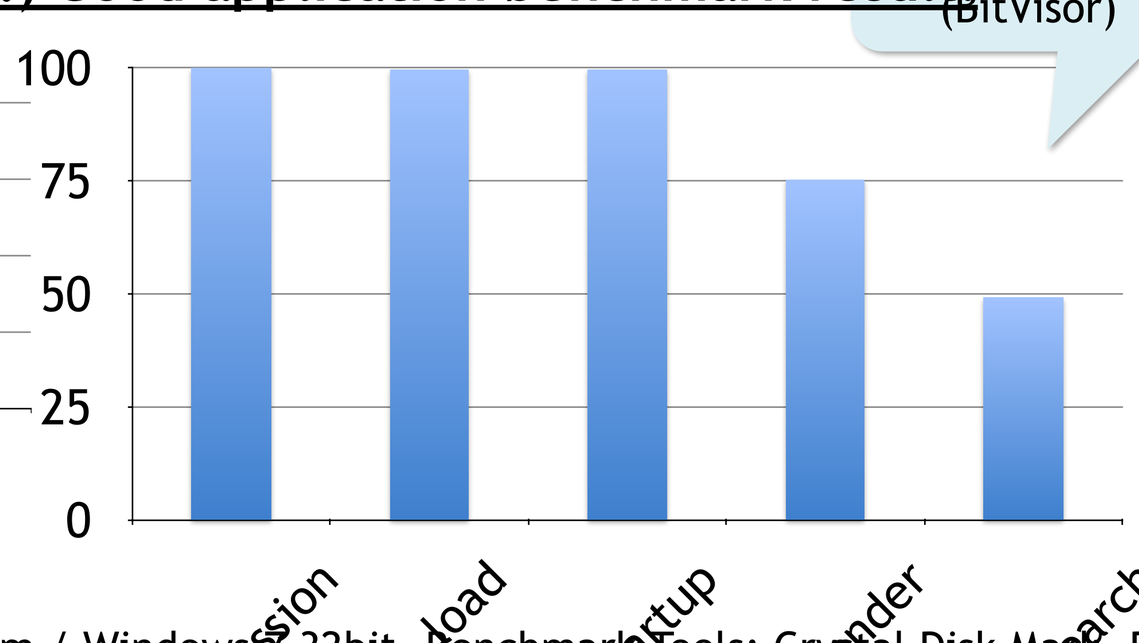
1.) Several minutes installation of hypervisor-based encryption!

2.) Reasonable disk throughput with moderation!





3.) Good application benchmark result!



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

Future work Auto optimization of criteria for encryption-speed moderation.

omote@osss.cs.tsukuba.ac.jp
Laboratory of Advanced Research B Room 1128, University of Tsukuba, 1-1-1, Tenno-dai, Tsukuba, Ibaraki, 305-8573, Japan