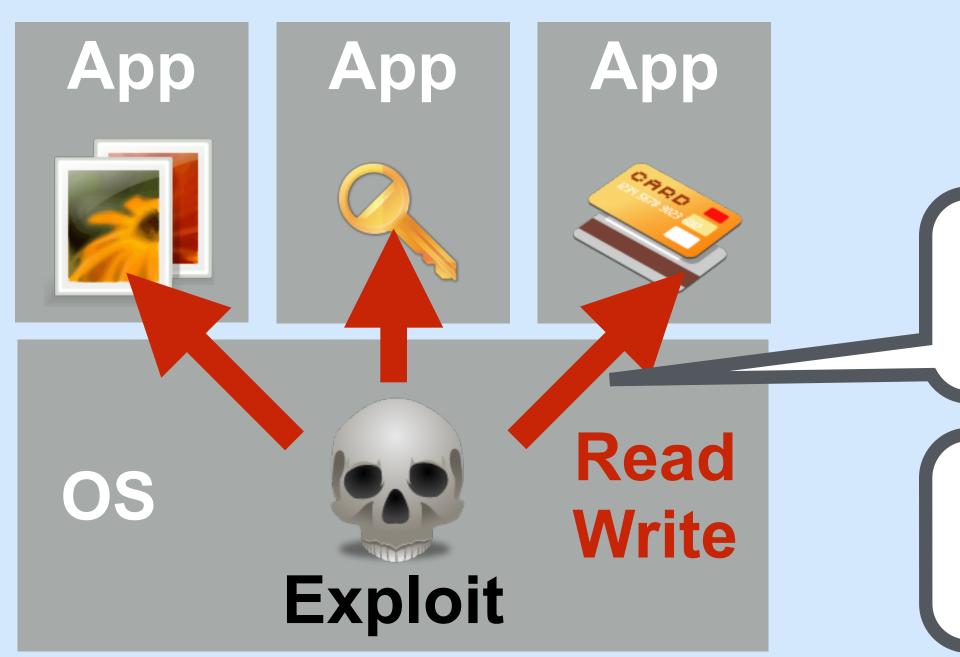
Exit-Less solated Execution

Yushi Omote Japan Society for the Promotion of Science

Takahiro Shinagawa The University of Tokyo

Kazuhiko Kato **University of Tsukuba**

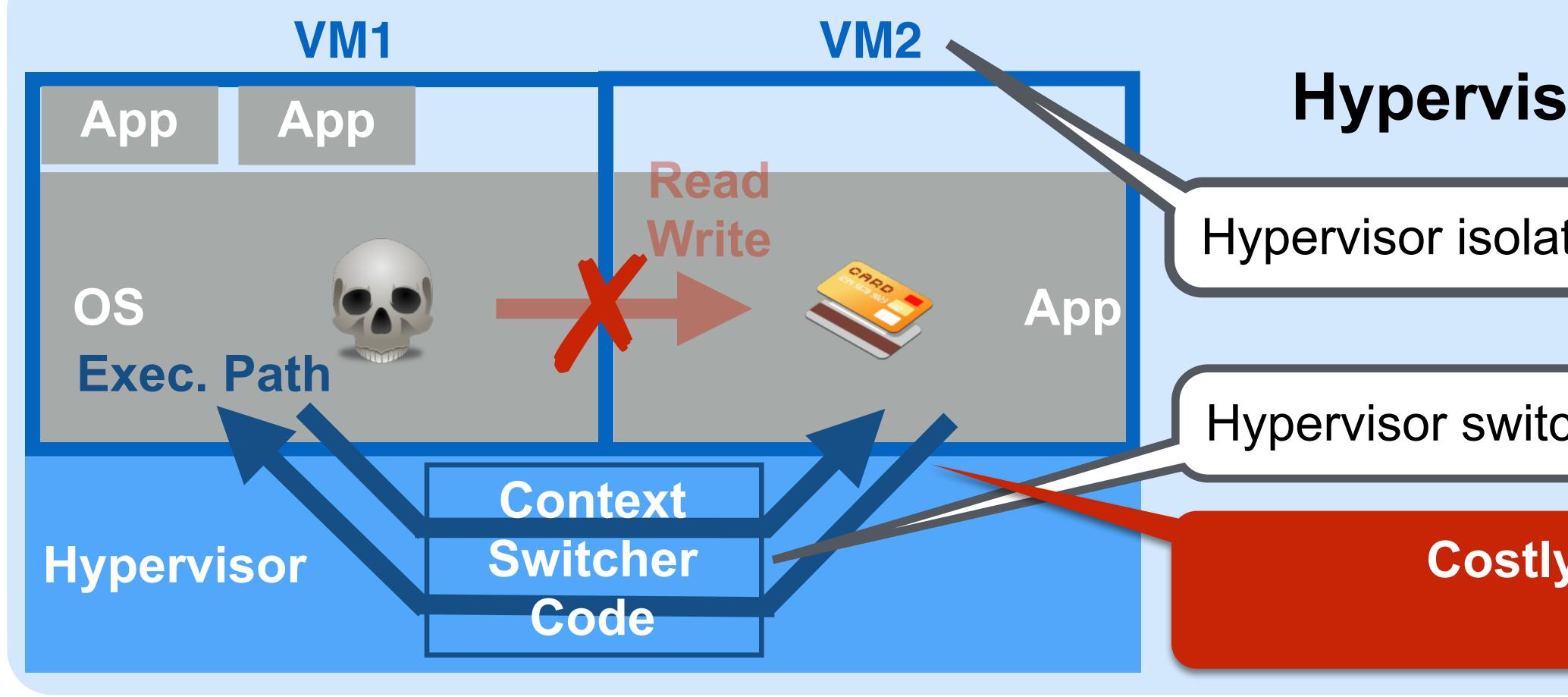


Vulnerability of OSs

Background

OSs have many vulnerabilities and attack surfaces but have unrestrained access to sensitive info. in Apps.

Need protecting Apps from compromised OSs. (while preserving compatibility for commodity OSs or OS transparency)



Existing Solution

Hypervisor-based Isolated Execution

Hypervisor isolates Apps in different VMs.

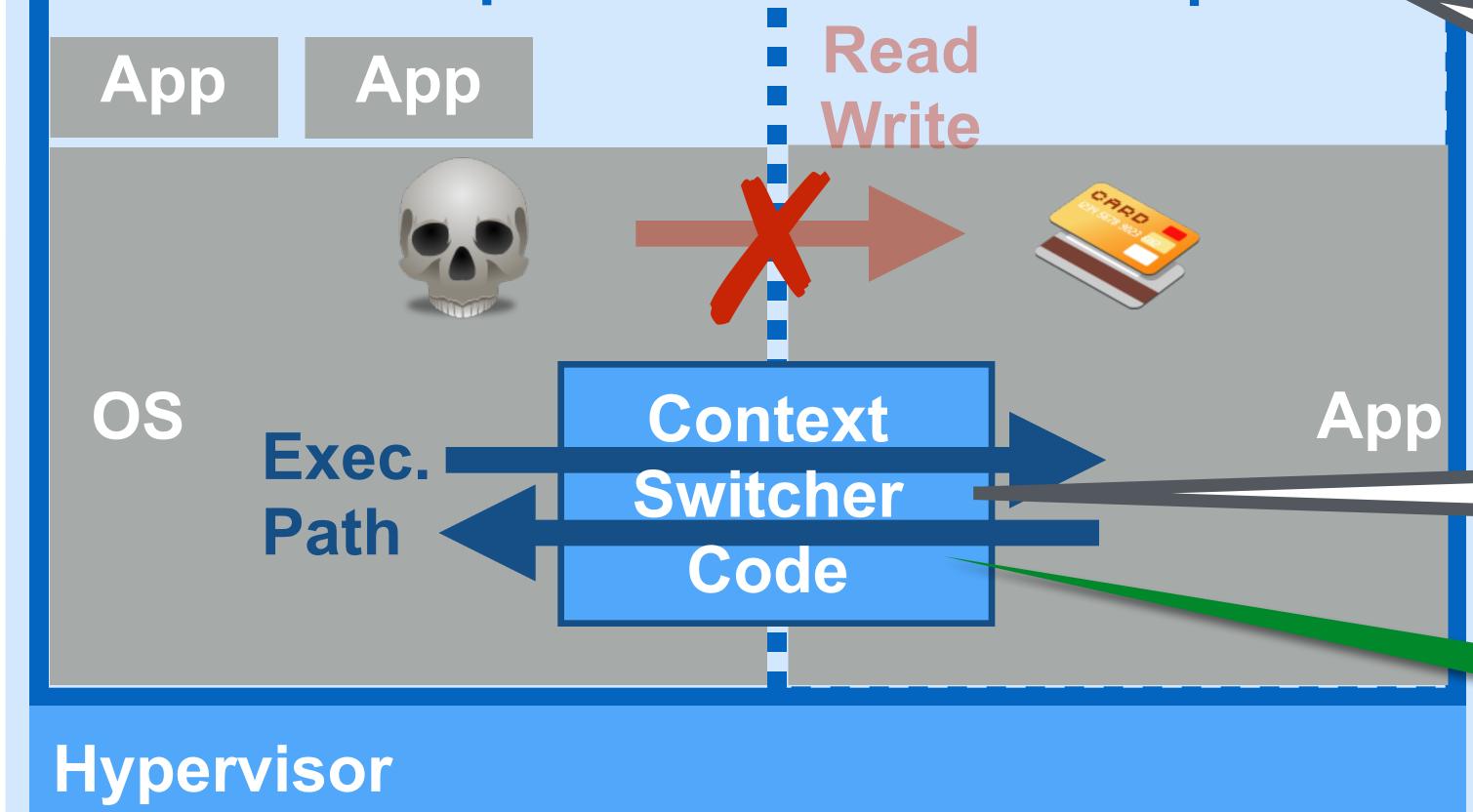
Hypervisor switches VMs for OS/App context switching.

Costly CPU-mode changes, VM exits! (1500 cycles~)



Exit-Less Isolated Execution

Proposal



Hypervisor isolates Apps in different address spaces. (Using Nested Page Tables)

OS/App-level Code *transparently* inserted by Hypervisor switches address spaces without VM exits. (Using VMFUNC instruction)

> Lightweight switching without VM exits. (≈ 300 cycles)

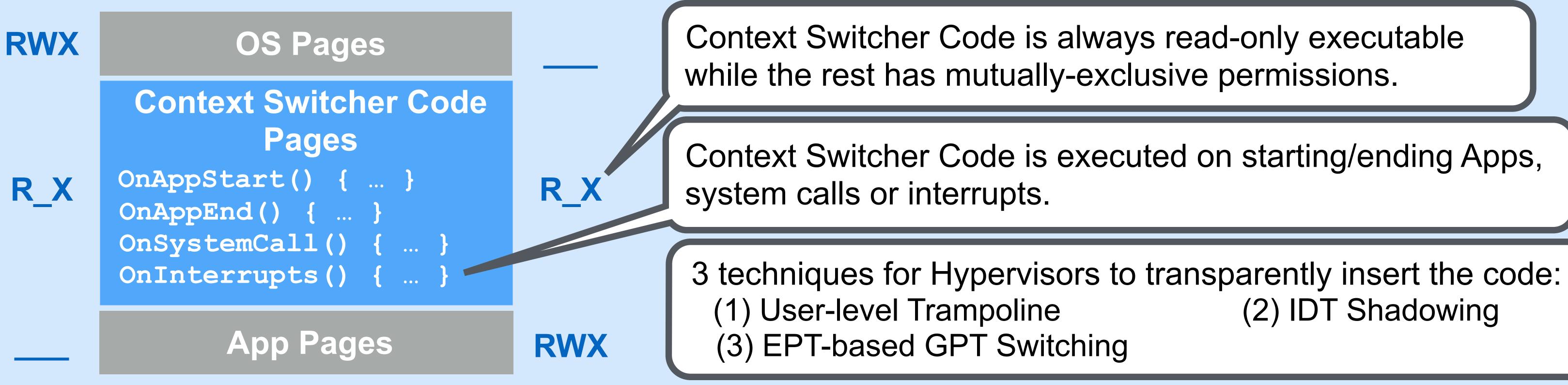
> > Implementation

AddressSpace1 **Page Permission**

AddressSpace2 **Page Permission**

OS-Transparent Exit-Less Context Switching

(2) IDT Shadowing



Contact Info: [Omote] <u>yushiomote@gmail.com</u>, [Shinagawa] <u>shina@ecc.u-tokyo.ac.jp</u>, [Kato] <u>kato@cs.tsukuba.ac.jp</u> Laboratory of Advanced Research B Room 1128, University of Tsukuba, 1-1-1, Tennodai, Tsukuba, Ibaraki, 305-8573, Japan.