September Week2

PROGRESS

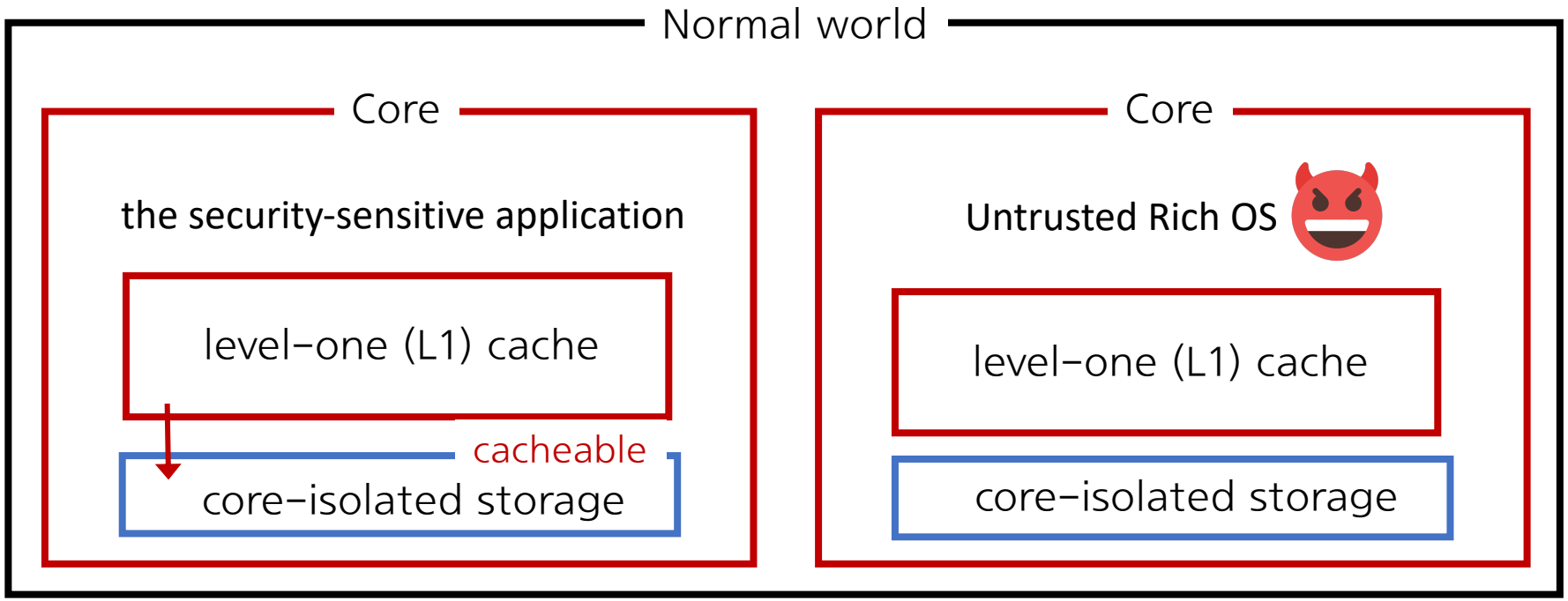
2020019252 김나현

Cache-in-the-Middle (CITM) Attacks: Manipulating Sensitive Data in Isolated Execution Environments

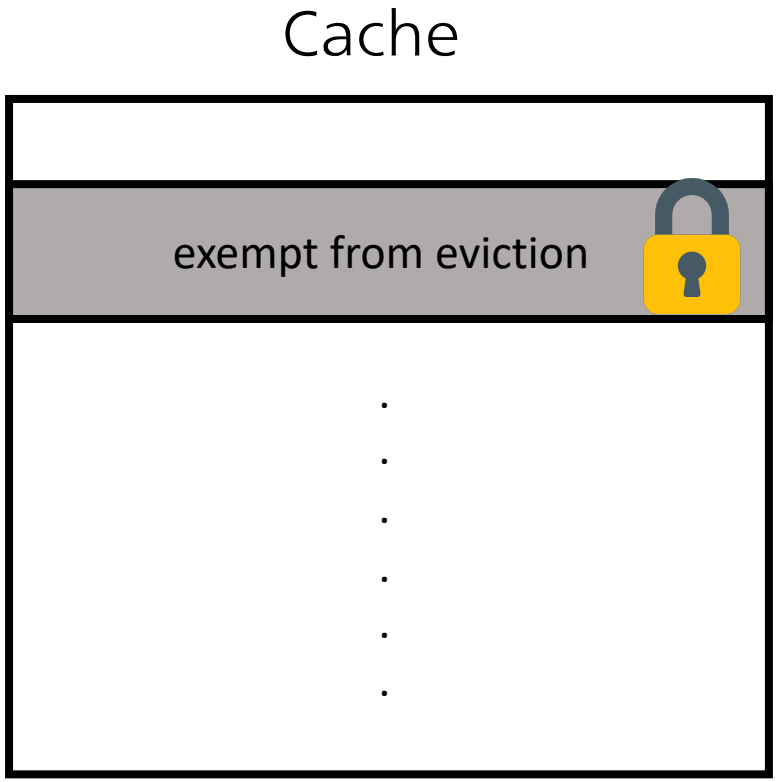
CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications SecurityOctober 2020

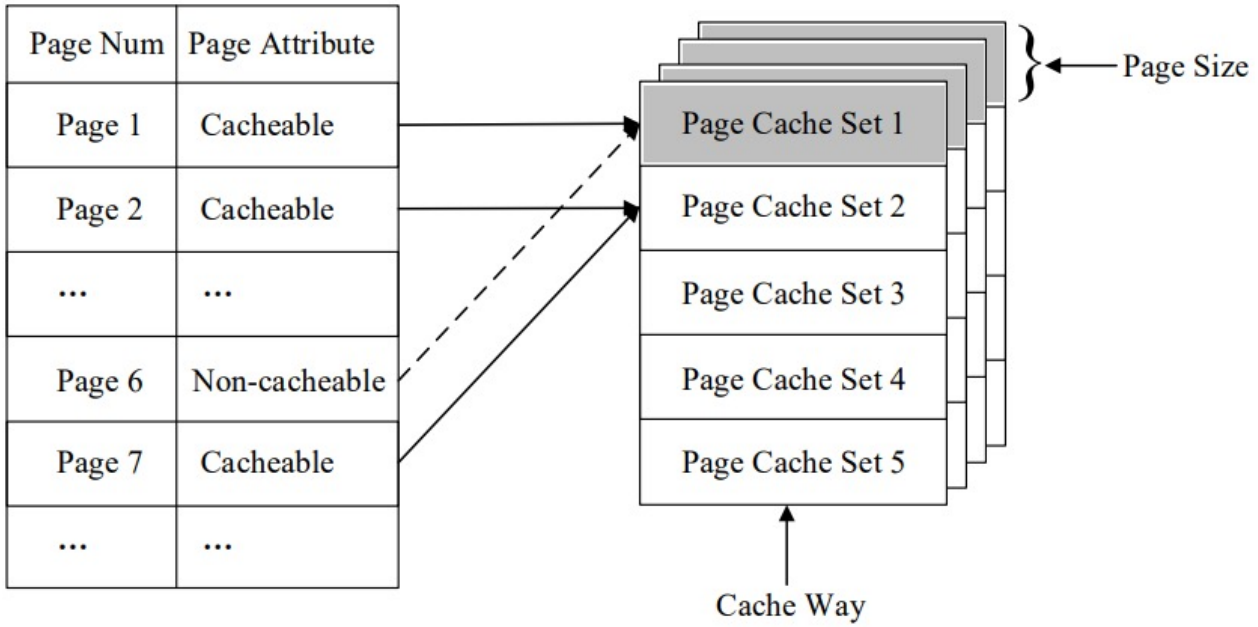
Type II. Bypassing security measures during IEE "switch out" process

constrain the memory

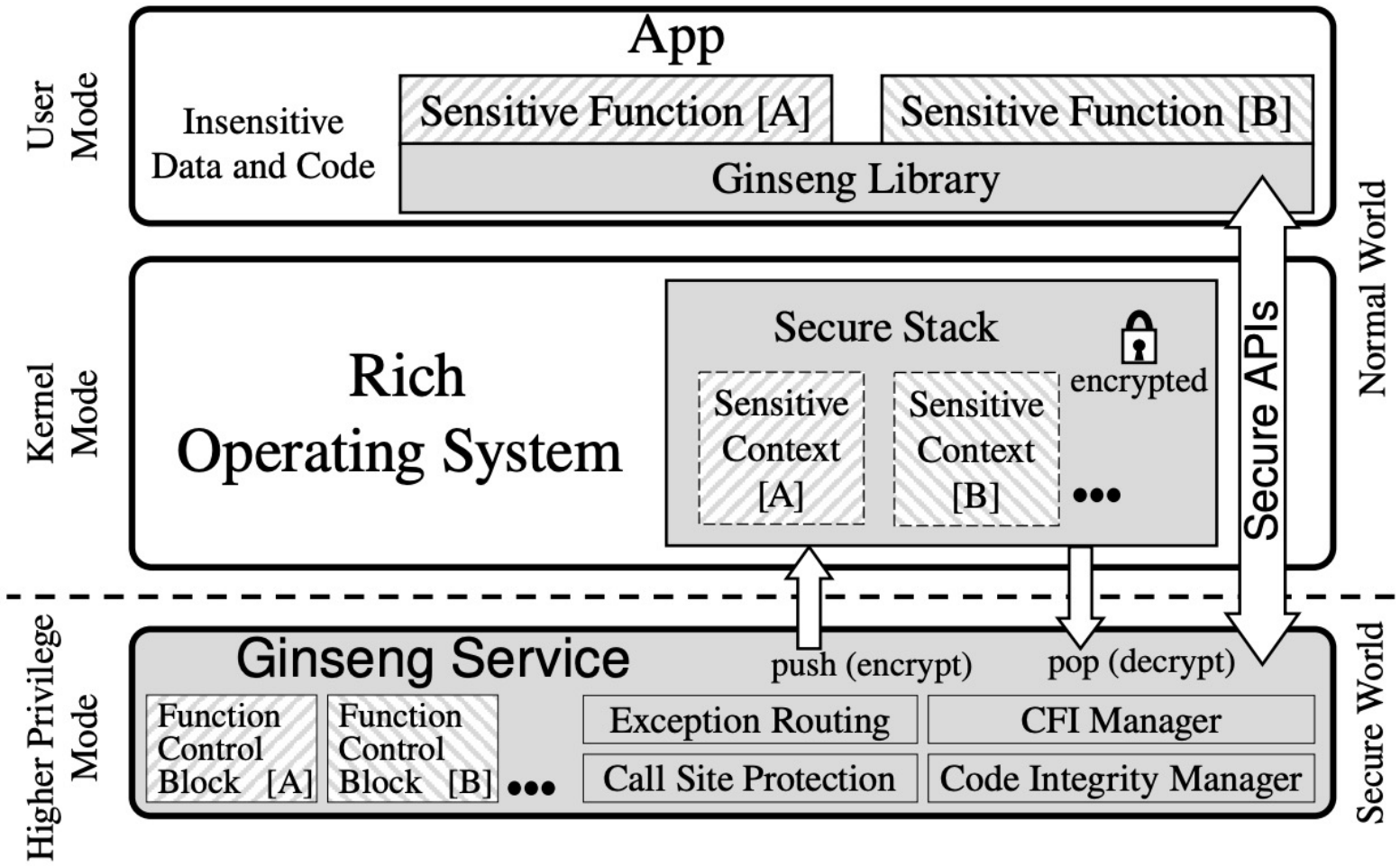


Cache Lockdown Technique

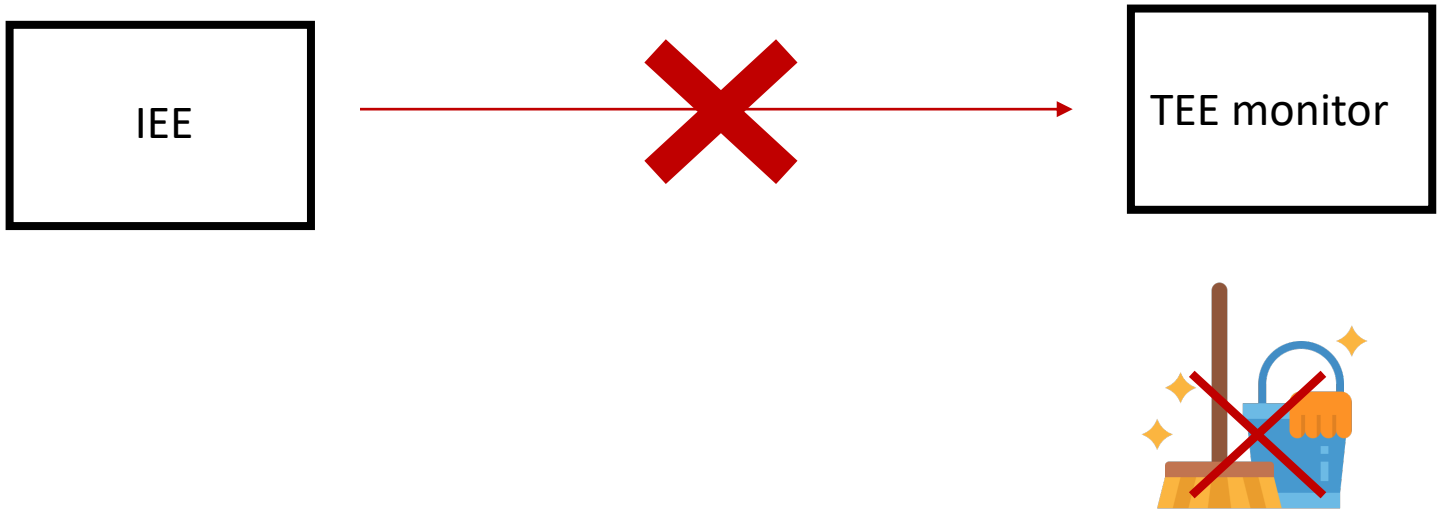




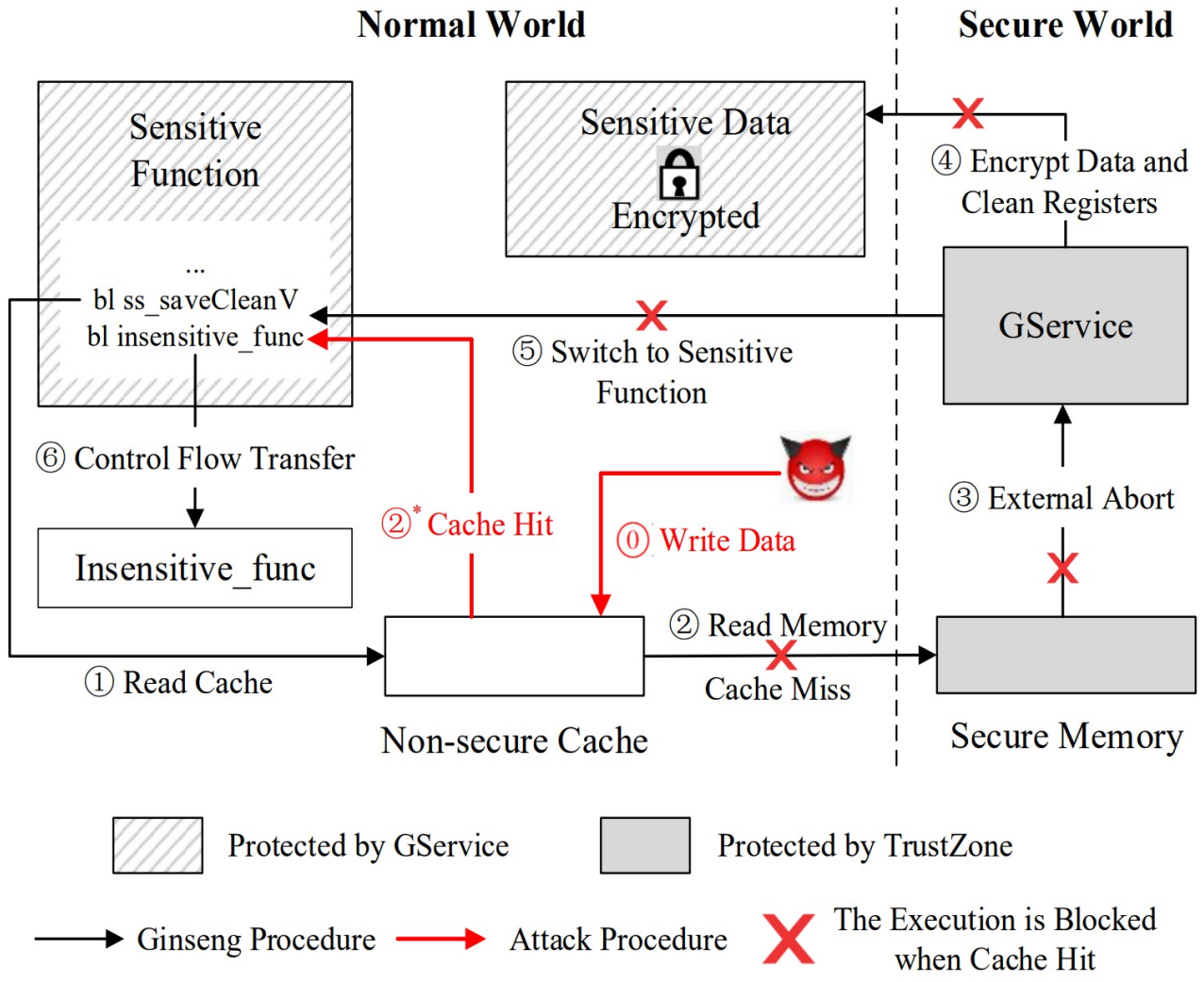
Ginseng: Mapping to Non-Secure Cache



bypass the data cleaning



Attacking Procedure



2. the reading and writing operations are not synchronized between memory and cache

(Type II attack)

-> synchronizing the reading and writing operations between memory and cache