Control Flow Obfuscation to Mitigate Branch-Shadowing Attack on Intel SGX

Intel Software Guard Extensions
• Hardware-based trusted execution environment that enables secure computation
• Protects against malicious privileged software

Branch shadowing attack
• Critical side channel attack on Intel SGX that reveals fine-grained control-flow of enclave
• Can reveal program secret
• Probes the branch prediction and infers:
  • if conditional branch is taken or not
  • If unconditional branch is executed
  • target of indirect branch instruction

The proposed approach
• Hides the secret dependent control flow
• Obfuscates and flattens the control flow at compile time by replacing branch instructions
• Using trampoline trampoline when branching
• Randomizing trampoline layout inside enclave

References