Secure Systems Group, Aalto University

Shohreh Hosseinzadeh, Hans Liljestrand, Andrew Paverd, Ville Leppänen, N. Asokan

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

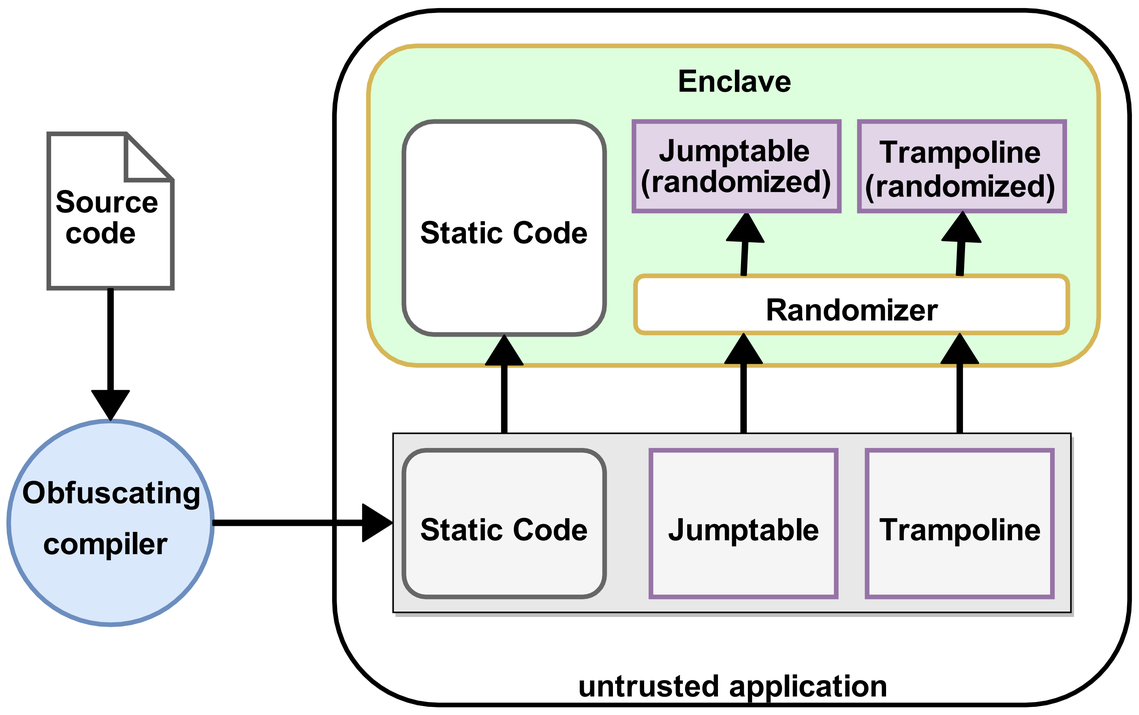

Figure 1: System design

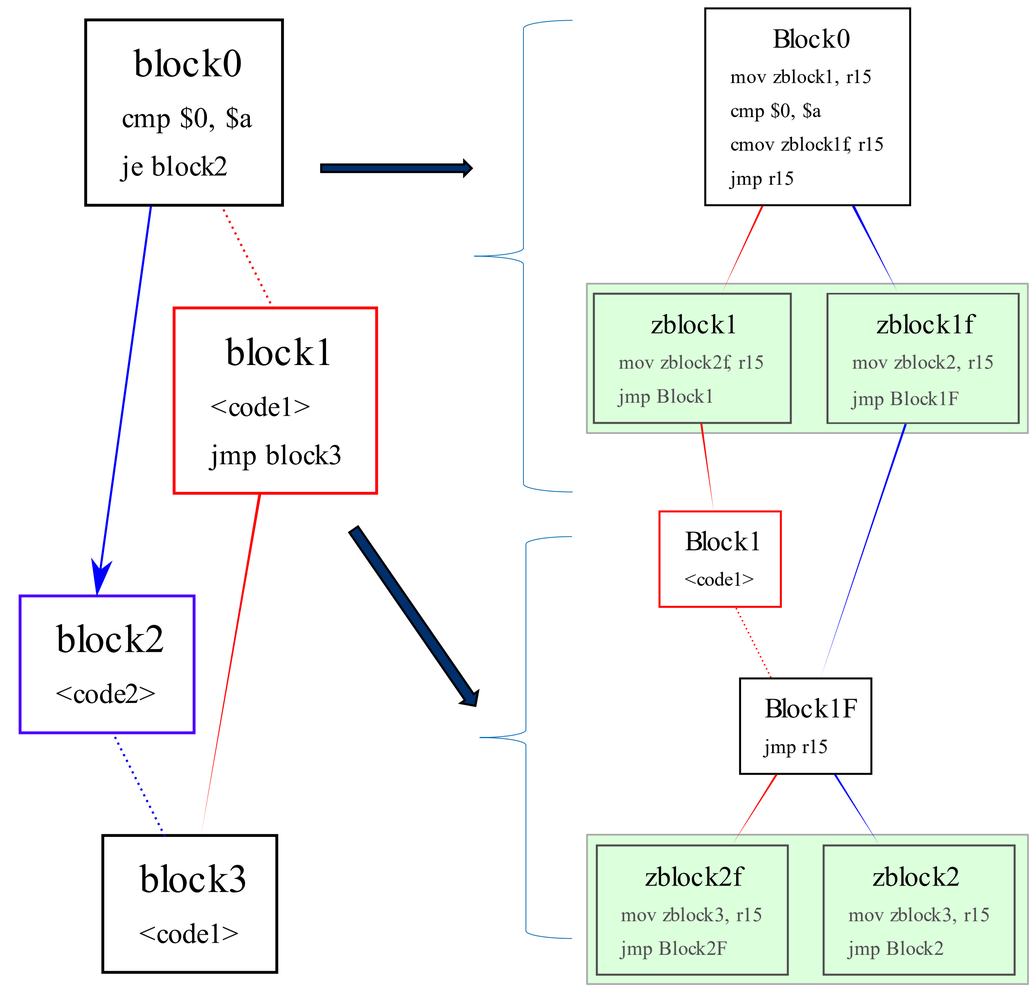

Figure 2: original and modified control flow graph of the program

Jumping back and forth between trampoline and code hides the real target.

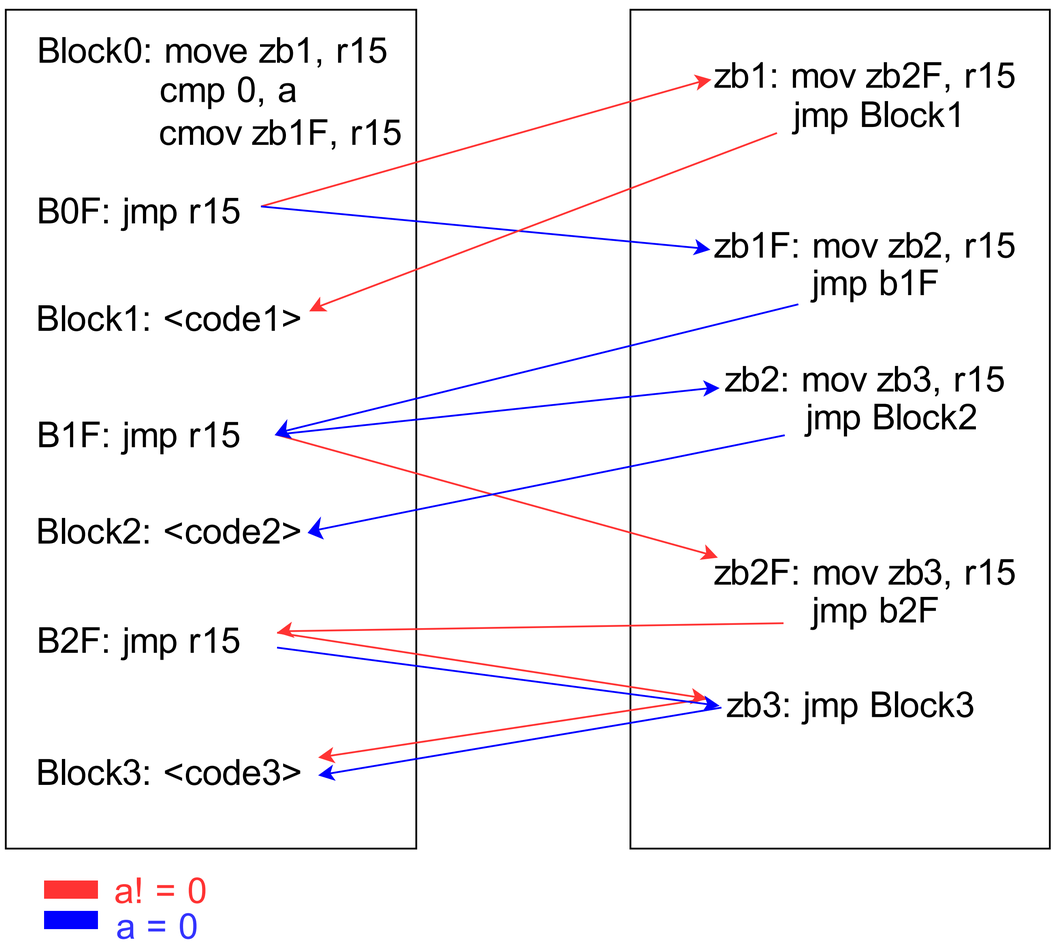

Figure 3: Modified code and redirecting the control flow using trampoline

References

[1] S. Lee, M.-W. Shih, P. Gera, T. Kim, H. Kim, and M.Peinado. 2016. Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing. CoRR abs/1611.06952 (2016).

Aalto University

Turun yliopisto
University of Turku