HIPStR – Heterogeneous-ISA Program State Relocation

Ashish Venkat  Sriskanda Shamasunder  Hovav Shacham  Dean Tullsen
University of California, San Diego

Return-Oriented Programming

- Return-Oriented Programming can perform malicious computation without injecting malicious code
- ROP is proven to be Turing complete for multiple ISAs and a wide range of workloads

Harnessed ISA Diversity: Escape from ROP

ROP thrives on 4 fundamental characteristics:
- Ability to hijack control flow
- Prior knowledge of gadget locations
- Requires program state (registers/memory) to perform computation
- Knowledge of the underlying ISA

Brute Force Attacks computationally infeasible on even future Exascale Processors

- Outperforms JIT-ROP Competition by 15.6%
- Massively Attack Surface Reduction (99.09%)

Harnessing ISA Diversity: Refuge from ROP

- Synergistically combines two strong independent defense techniques:
  - Binary Translation driven Program State Relocation
  - Non-deterministic Execution Migration across Heterogeneous-ISAs

Heterogeneous-ISA Program State Relocation

- Synergistically combines two strong independent defense techniques:
- Binary Translation driven Program State Relocation
- Non-deterministic Execution Migration across Heterogeneous-ISAs

Software Diversity vs ISA Diversity

Isomeron (NDSS 2015):

- Why not migrate execution to a randomized version (isomer) of the same ISA at the flip of a coin?

Tailored Diversification Attacks

- Goal: Stitch together gadgets across heterogeneous-ISAs (or isomers)
  - NOP gadgets: Gadget performs useful operation in one ISA (isomer) and acts as a NOP in another.
  - Immutable gadgets: Gadget performs the same operation on both ISAs (isomers) without clobbering any previously stored values.

HIPStR outperforms Isomeron by an average of 15.6%