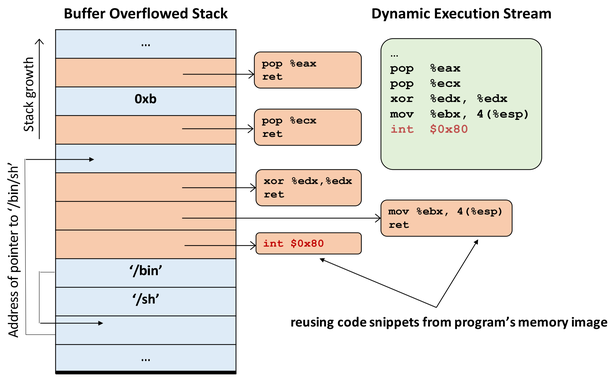
HIPStR – Heterogeneous-ISA Program State Relocation

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

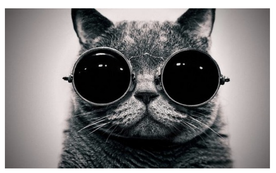
Harnessing ISA Diversity: Escape from ROP

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

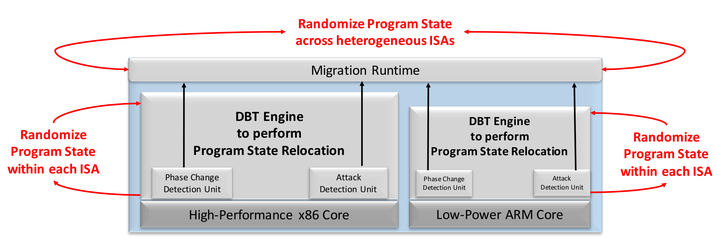
Massive Attack Surface Reduction (99.09%)



Outperforms JIT-ROP Competition by 15.6%

Removes one of the last remaining "constants" available to the attacker -- knowledge of the ISA

Heterogeneous-ISA Program State Relocation

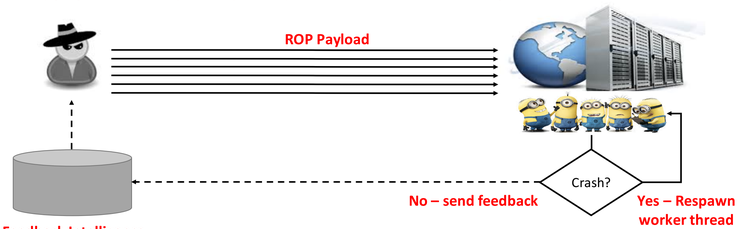


Synergistically combines two strong and independent defense techniques:

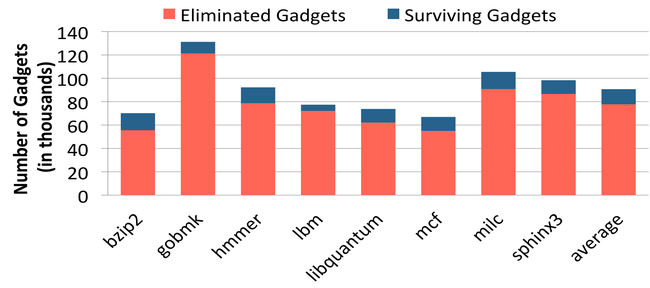
- Binary Translation driven Program State Relocation
- Non-deterministic Execution Migration across Heterogeneous-ISAs

Brute Force Attacks on HIPStR

Goal: Construct a simple 4-gadget shellcode exploit.
i.e., populate %eax, %ebx, %ecx, and %edx with attacker-provided values.



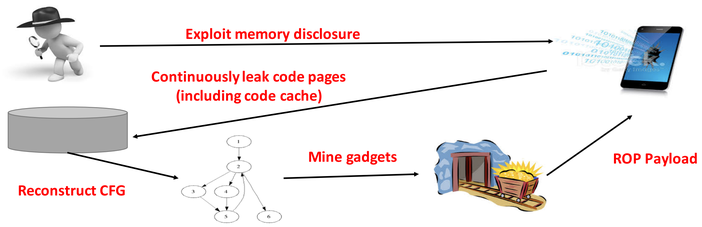
Need just 20 minutes to accomplish all of this



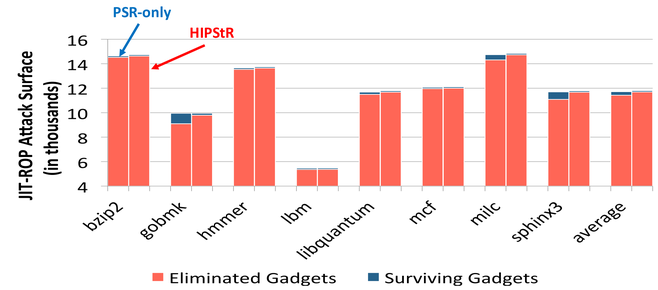
Best Case Scenario: Need 56 trillion years to break HIPStR

JIT-ROP Attacks on HIPStR

Goal: Construct a simple 4-gadget shellcode exploit.
i.e., populate %eax, %ebx, %ecx, and %edx with attacker-provided values.



Thousands of gadgets in just 23 seconds.

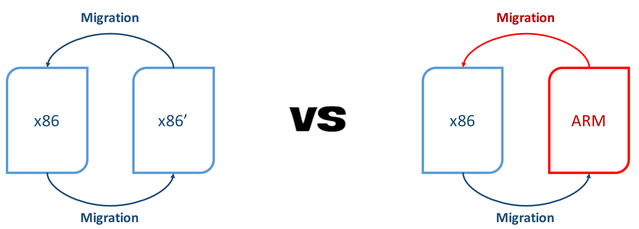


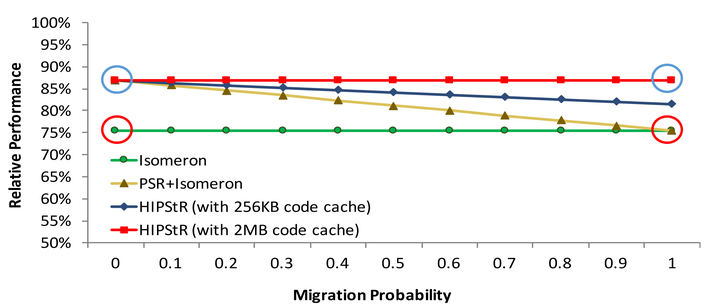
Only 27 gadgets bypass migration – insufficient to construct a simple shellcode exploit.

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?



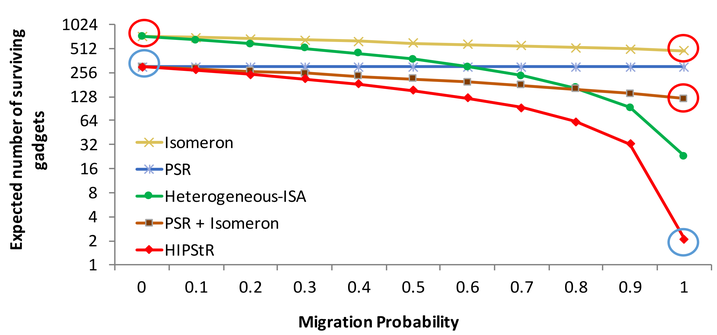


HIPStR outperforms Isomeron by an average of 15.6%

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.



Hundreds of gadgets survive Isomeron, but only 2 gadgets survive HIPStR