PAIRS: Control Flow Protection using Phantom Addressed Instructions
Mohamed Tarek Ibn Ziad, Miguel A. Arroyo, Evgeny Manzhosov, Vasileios P. Kemerlis*, Simha Sethumadhavan
{mtarek,miguel,.evgeny,simha}@cs.columbia.edu, *vpk@cs.brown.edu
Columbia University, *Brown University

PAIRS is a novel technique that protects against Code-Reuse Attacks.
PAIRS randomizes execution path of the program without performance overheads or binary modifications.

**Problem Statement**
- Complete Memory Safety has prohibitive cost for deployment (energy/performance)
- Most solutions require new hardware and recompilation of codebase
- Many low-cost/Embedded/IoT devices are 32b and left out by State-of-Art solutions

**Goals**
- Provide a solution that works for 32/64b devices
- Backward compatibility and zero overheads

**Approach**
- Populate Virtual Address Space with multiple phantoms of original program
- Randomize Program execution flow between phantoms and original program
- Resolve phantoms to original program at run time

**Results**
- PAIRS has no performance penalty, unlike Pointer Encryption (ARM PAC) or SW Execution Path Randomization
- Enhanced PAIRS (PAIRS+TRAP) allows security exceptions at the cost of 4% performance overheads on average
- Adding a lite variant of pointer encryption: trading 2% (total 6%) performance for encryption of virtual pointers
- RIPE benchmark: (60.4+5.8)% attacks fail, however, most of the attacks have length of 1-2 gadgets

Evgeny Manzhosov
Computer Science, Columbia University