Adding Memory Safety to the Mac OS X Kernel

Billy Lau, University of Illinois at Urbana-Champaign

ADVISOR: Vikram Adve

Background

Secured Virtual Architecture (SVA) Overview

Ensure memory safety for Mac OS X

- Accurate Array Bounds Check
  ensure that array dereferencing stays within bounds
- Make Dangling Pointers Harmless
  dangling pointer dereferences access objects of the correct type
- Sound compiler analysis for kernel code
- Type safety for subset of kernel objects

Ultimately prevents exploits and attacks originating from memory error vulnerabilities in kernel

Fundamental Questions/Challenges

- Design difference between Linux and Darwin increases the complexity and adds to the challenge of this project.
- There are custom kernel allocators that require special handling.
- There are also performance/safety trade-off issues to be considered.
- What to do when a buffer overflow is detected in the kernel remains a question for future research to answer.

Research Plan

- Identify all available memory allocators in Darwin Kernel.
- Determine which allocators should be pool allocators and which should be general heap allocators.
- Modify appropriate memory allocators to allow for pool registration.
- Port Darwin to the SVA instruction set.

Research Results

- Successfully identified all available memory allocators in Darwin and compared with those of Linux.
- Successfully incorporated runtime initialization functions for Memory Safety Engine into the kernel during the boot sequence.
- Darwin zone allocators have been modified to register objects with the Memory Safety Engine. Further testing is yet to be done.
- Adapted the Memory Safety Engine to support multi-core chips.

Related Work/Interaction with Other Projects

- LLVM (Low-Level Virtual Machine)
  www.llvm.org
- SAFECode
  developed techniques used by Memory Safety Engine
- DSA (Data Structure Analysis)
  extremely fast recursive identification of data structures & their properties
- SVA for Linux
  pioneer project that provides memory safety to Linux via a compiler-based virtual machine