SVV: Policy-Constrained Speculative Execution

ACSAC 2005 NSPW Panel
Michael E. Locasto
Columbia University NSL
{Sidiroglou, Keromytis}

December 8th, 2005
Last Word

- push common security monitoring functionality down the system stack closer to and into the hardware
  - provide implicit supervision
  - export a policy-driven interface for that monitoring mechanism
  - provide foundation for automatic response
Pumpkin Pie

• Lesson
  - outsource execution observe results
  - take credit if things go well
  - else, patch up (grape jelly)

• requires policy to inform detection

• fixing is interesting, may need to resort to bakery
Motivation

● hardware often lacks primitives for tasks in which raw speed is not the primary goal.

● There is little architectural support for monitoring execution at the instruction level, and no mechanisms for assisting an automated response.
Main Contribution

• A set of architectural components for speculatively executing the entire instruction stream

• 2 phases
  − 1: speculate that the instructions are benign
  − 2: verify the results and optionally re-write if harmful
Goals

• Obtain time to ROAR

• Provide low-level, general functionality to support automatic remediation
  – instruction stream re-writing
  – plus basic response strategies
  – others can be learned, programmer supplied, compiler supplied, administrator supplied
Insight

- Need to have or otherwise obtain enough lead time to ROAR. Need to create a time bubble or buffer so that application looks like it operates normally to the user and attacker, but in reality is looking into a crystal ball
Details

• Add another pipeline stage
  – verify (Read/Decode, Execute, Write, Commit)

• other components
  – Policy Constraint Unit + instrumentation
  – VERU (virtual emulator)
  – VB (verification buffer)
  – IRWU (instruction re-write unit)
Challenges

• The problem of scope
  - how large is the buffer
  - how patient are those waiting for the fixed pie?

• Implementation (is this feasible)

• How far to propagate a micro-patch

• How to make sure a response is correct
Last Word

• push common security monitoring functionality down the system stack closer to and into the hardware
  - provide implicit supervision
  - export a policy-driven monitoring mechanism
  - provide foundation for automatic response
Questions

- I think there are some very interesting, multi-disciplinary issues to be addressed here
- Thank you very much for your kind attention