CS 423
Operating System Design: Process VMs

Professor Michael Bailey
Spring 2018
 Goals for Today

• **Learning Objective:**
  • Conclude discussion of virtualization w/ process VMs

• **Announcements, etc:**
  • Midterm scores and debrief will come over spring break
  • MP2 extension: **now due on March 25th (UTC-11)**
  • MP3 released March 27th
  • MP2.5 (Extra Credit) release on March 27th also

**Reminder:** Please put away devices at the start of class
Dynamic Binary Translation

Start with SPC

Look up SPC→TPC in map table

Hit in Table?

Yes

Branch to TPC and execute block

No

Translate new block

Store new SPC→TPC entry in table

Get SPC of next block

Edit: The original automata didn’t execute the current block unless there was a hit!
Translation Chaining

• Translation chaining
  – The counterpart of threading in interpreters
  – The first time a jump is taken to a new destination, go through the emulation manager as usual
  – Subsequently, rather than going through the emulation manager at that jump (i.e., once destination block is known), just go to the right place.
• What type of jumps can we do this with?
  • Fixed Destination Jumps Only!!!
Indirect Jump Caching

• Jump destination depends on value in register.
• Must search map table for destination value (expensive operation)
• Solution?
  – Caching: add a series of if statements, comparing register content to common jump source program counter values from past execution (most common first).
  – If there is a match, jump to corresponding target program counter location.
  – Else, go to emulation manager.
• Present the abstraction of a different machine and OS to a *process*. 
• Creation of an isomorphism that maps a virtual guest system to a real host:
  – Maps guest state $S$ to host state $V(S)$
  – For any sequence of operations on the guest that changes guest state $S_1$ to $S_2$, there is a sequence of operations on the host that maps state $V(S_1)$ to $V(S_2)$
Virtualization Isomorphism

“State Equivalence”
• Process state equivalence at the point of interaction with the “external world”
  – When control transfers from guest process to host OS, state equivalence must hold
  – When control transfers back to guest process, state equivalence must hold (both of user managed and OS managed state)

• Consequences:
  – State does not need to be mapped correctly in between interactions with OS
State Mapping

- **Guest registers** → **Host registers/Memory**
  - Guest context (and context switch)
  - Depends on who has more registers

- **Memory address space mapping**
  - Guest application (virtual) address space
    → Host application (virtual) address space
Translation Table

Guest Address Space

Translation Table

64K blocks

Host (Virtual) Address Space

Software translates guest to host virtual addresses. Disadvantage?
Direct Access Translation

Offset Translation

Guest Application Address Space

Host Virtual Address Space

Runtime

Mapped Guest Application Address Space

Direct Translation

Guest Application Address Space

Host Virtual Address Space

Runtime

Host Virtual Address Space

Mapped Guest Application Address Space
Direct Translation

Offset Translation

Guest Application Address Space

Mapped Guest Application Address Space

Runtime

Host Virtual Address Space

Limitations?

Direct Translation

Guest Application Address Space

Guest Application Address Space

Mapped Guest Application Address Space

Runtime

Host Virtual Address Space

Host Virtual Address Space
• Host OS Offers:
  – A system call to set memory protection (specifies page and access privileges)
  – A signal for a memory protection violation that can be delivered to the application (runtime)

• Memory protection
  – Each page has protection bits such as read/write or read/write/execute (e.g., you cannot execute data, or overwrite code)
  – What if guest architecture has read/write/execute protection whereas host has read/write only?
Page Size Issues

• What if page size on guest is a multiple of page size on host?
• What if page size on host is a multiple of page size on guest?
Page Size Issues

- What if page size on guest is a multiple of page size on host?
  - No problem. Just replicate page protection

- What if page size on host is a multiple of page size on guest?
  - Different guest pages mapped to same host page?
    - Problems?
  - Pad guest pages to size of host page?
    - Problems?
Page Size Issues

• What if page size on host is a multiple of page size on guest?
  – Different guest pages mapped to same host page? Problems?
    • What if pages have different protection?
    • Use the more conservative bits and handle violations accordingly
  – Pad guest pages to size of host page?
    • Makes address translation more difficult
    • Wastes resource
• Interpretation versus binary translation?
  – Interpretation:
    • no startup overhead
    • High overhead per instruction
  – Binary translation:
    • High startup overhead
    • Low overhead per instruction
  – Can we combine the best of both worlds?
• Interpretation versus binary translation?
  – Interpretation:
    • no startup overhead
    • High overhead per instruction
  – Binary translation:
    • High startup overhead
    • Low overhead per instruction
  – Can we combine the best of both worlds?
    • Small program: Do interpretation
    • Large program: Do binary translation
• Initially assume small program
  – Do Interpretation
• Count the number of times each block is executed
• If a block is executed more than N times, do binary translation on this block
Interrupts Emulation

• Two types:
  – Traps (caused by instructions in the program)
  – Hardware interrupts (caused by asynchronous external events)
• For Traps and Exceptions:
  – Ensure that all instructions prior to trap have been executed
  – Ensure that none of the instructions after the trap have been executed
• For Interrupts:
  – Emulated code must be in interruptible state...
• How to detect them?
  – Both guest and host support same trap (e.g., page fault). Map guest trap to host trap: capture trap signal, execute the translated guest handler
  • Runtime intercepts all signals and handles them
  – Guest supports trap/exception that host does not support (or does not deliver to the application). Check for exception conditions in the emulated software explicitly
• When an interrupt occurs:
  – Interpretation: When an interrupt occurs, finish interpreting the current instruction and execute the interrupt handler
  – Binary translation: When an interrupt occurs, the emulated code may be in non-interruptible state (what does that mean?)
    • Need well-defined boundaries where emulated code is interruptible.
    • What is a suitable boundary?
    • When interrupt occurs, execute emulated guest code until boundary is reached, then execute the interrupt handler.
Interrupts

• When an interrupt occurs:
  – Interpretation: When an interrupt occurs, finish interpreting the current instruction and execute the interrupt handler
  – Binary translation: When an interrupt occurs, the emulated code may be in non-interruptible state (what does that mean?)
    • Need well-defined boundaries where emulated code is interruptible.
    • What is a suitable boundary? BLOCK BOUNDARIES
    • When interrupt occurs, execute emulated guest code until boundary is reached, then execute the interrupt handler.
Interrupts

• When an interrupt occurs:
  – Interpretation: When an interrupt occurs, finish interpreting the current instruction and execute the interrupt handler
  – Binary translation: When an interrupt occurs, the emulated code may be in non-interruptible state (what does that mean?)
    • Need well-defined boundaries where emulated code is interruptible.
    • What is a suitable boundary? **BLOCK BOUNDARIES**
    • When interrupt occurs, execute emulated guest code until boundary is reached, then execute the interrupt handler.

What if blocks are chained?
• When an interrupt occurs, the emulated code may be in non-interruptible state
  – Determine which block is currently running
  – Unchain the block from the next by replacing the jump at the end of the block to a transfer of control to the emulation manager.
  – Let the block finish
  – Control is transferred to emulation manager which invoked interrupt handler.
• Does not have to translate guest OS instructions one a time
  – Translate entire functions into equivalent ones
  – Example: replace a disk I/O system call on the guest with an equivalent disk I/O call on the host

• Not all guest system calls need to be translated to host calls; some are handled by the runtime.
  – Example: Calls installing a new signal handler may be handled by the runtime since runtime intercepts all signals and maintains their handlers.

• Generally an ad hoc process (case-by-case).