CLOUD COMPUTING APPLICATIONS

Virtualization: Binary Translation

Prof. Reza Farivar

Binary Translation

- Binary translation modifies sensitive instructions on the fly to virtualizable instructions
  - we only need to translate kernel code that is executing in ring 0
    - Depending on the workload, this is a small fraction of the total code
  - Examine the executable code of the virtual guest for "unsafe" instructions
  - Translate these into "safe" equivalents
  - Execute the translated code

- Direct Execution
  - most code is executed directly on the CPU, and only the code that needs to be translated is actually translated

- Binary translation is performed on the binary code that gets executed on the processor it does not require changes to the guest operating system kernel

Binary Translation

- Binary translation was first described in a paper from 1992 by [Digital Equipment Corporation](#) (DEC)

- Original VMWare Workstation 1.0 in 1999
  - BT support deprecated since 2016

- Somewhat similar to Just in Time compilation for Java Virtual Machine (JVM), Javascript (V8 in Chrome), PHP 8 (since November 2020)