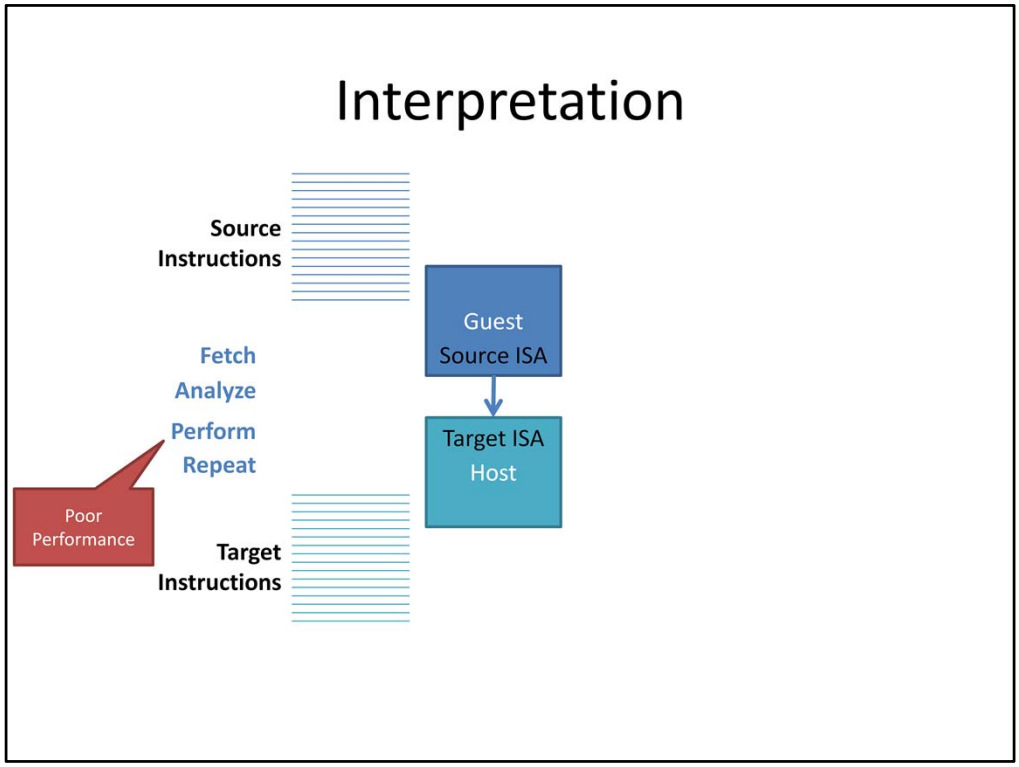
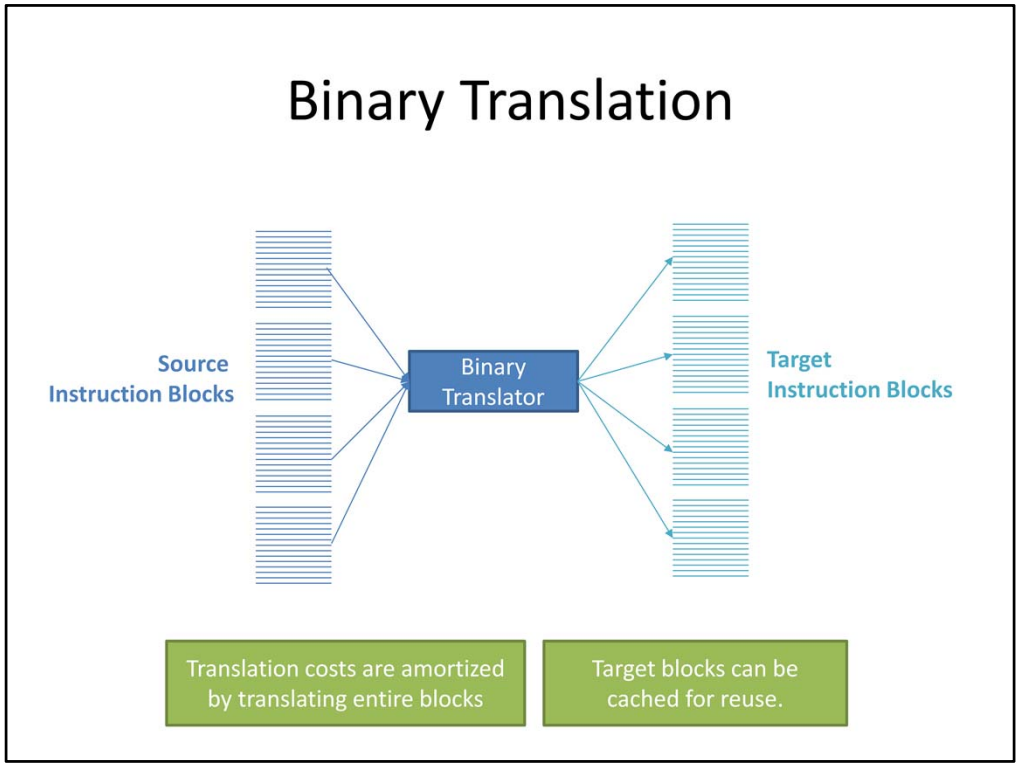
Binary Translation

جامعة كارنيجي ميلون في قطر
Carnegie Mellon University Qatar

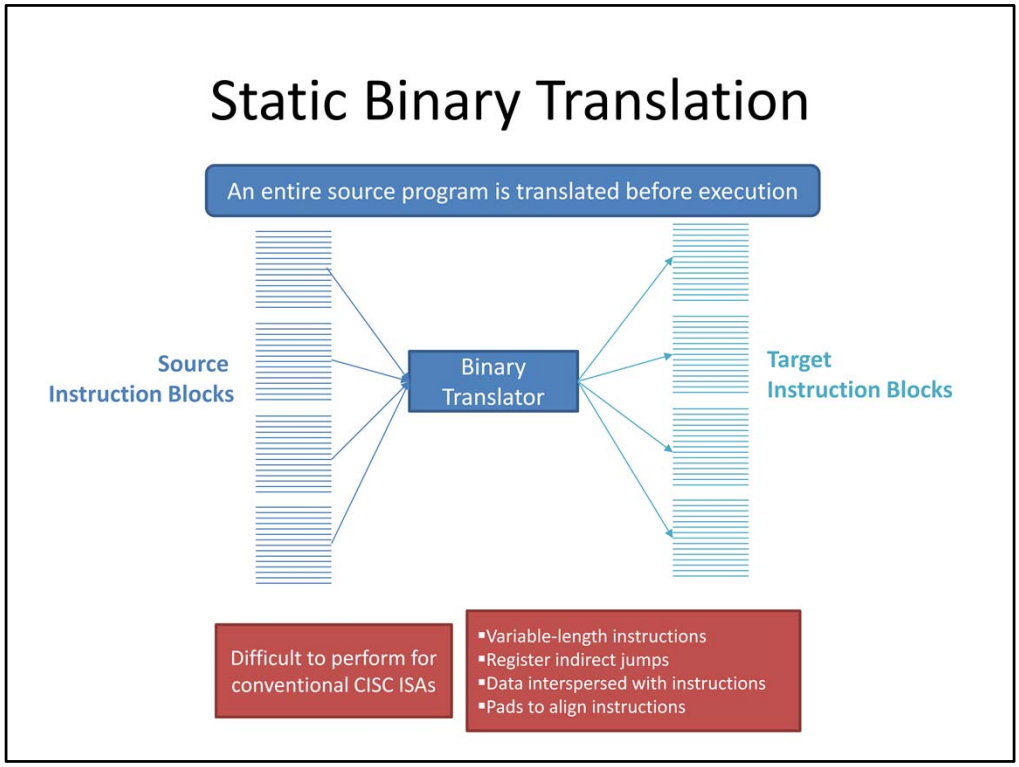
In this video, we'll explain binary translation, an emulation technique that targets the limitation of interpreters.



In interpreters, a source instruction stream is interpreted instruction by instruction into a target instruction stream. This leads to poor performance.



With binary translation, entire blocks of instructions are translated into target instruction blocks, in binary. Binary translators seek to amortize translation costs by translating an entire block at a time. More importantly, performance can be improved by caching these translated blocks for reuse when an identical source instruction block is encountered again.



In static binary translation, an entire source program is translated prior to execution. This is difficult to perform for conventional CISC architectures such as Intel x86 due to the complexity of the instructions, which can contain variable length instructions, register indirect jumps, data interspersed with instructions and pads to align instructions to the instruction width.