HABITAT - Hardware-Accelerated Binary Translator

Sing Hin To (Jason)[1], Tom Spink[2]

[1]School of Computer Science, University of St Andrews, St Andrews, UK

[2]School of Computer Science, University of St Andrews, St Andrews, UK

sht2@st-andrews.ac.uk

Abstract

Emulators are widely used to allow a host system to run software designed for a different guest system. They have been essential in supporting legacy systems, future prototypes, and programs compiled for other architectures.

However, software-based solutions often suffer from performance and scalability issues, considering that the host system is responsible for both the translation & execution of foreign programs. This drastically limits the scope of possible scenarios for emulation & raises the entry barrier for such technology.

This project aims to explore potential improvements through hardware acceleration with broad support across multiple architectures, while remaining accessible to most existing systems.

In this talk, we will introduce our early work on offloading the binary translation stage from the CPU using a PCIe FPGA dynamic binary translator (DBT). We will also introduce Architecture-Independent Representation (AIR), a unified format that encapsulates foreign instructions (e.g., RISC-V, ARM) before translating them into host instructions.

Currently, we have established a draft of the AIR to support RV64GC (RISC-V), along with a software-based DBT that elaborates most of the instruction set. The DBT can run statically linked C programs on Linux and perform arithmetic operations with standard I/O.

We have also created a JSON-based format to encode details about instruction formats that can be expanded into a procedurally generated software decoder [1]. The JSON-based format can encode variable instruction lengths and irregular instructions.

This project is still in its early stages, and we welcome any feedback from the community.

References

[1] Katsumi Okuda and Haruhiko Takeyama. Decision tree generation for decoding irregular instructions. In *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1592–1597, 2016.