Emulacja 8086 używając nowoczesnego języka C++

Patryk Kaniewski

2021-05-17

Promotor

dr Cezary Bolek

Cel

Zbudowanie biblioteki do emulacji 8086 w C++20 i na jej podstawie zbudowanie emulatora.

Motywacja

8086 jest jednocześnie dosyć prostą architekturą (ograniczona liczba instrukcji w porównaniu do nowoczesnego x86 z dużą liczbą rozszerzeń) i posiada tylko realmode bez seperacji uprawnień oraz ochrony pamięci.
Kolejnym dużym plusem 8086 jest bardzo dobra dokumentacja (zarówno od producenta jak i duża ilość funkcjonalnych analiz zewnetrznych tego ISA)

Używane technologie

- C++20
- GCC
- cmake
- tinyasm (port)
- ncurses/qt (frontend)

Spis czynnosci

- disasembler (tokenizacja) 8086
- PoC
- zbudowanie toolchaina (używajac tinyasm) do latwego assemblowania i uruchamiania kodu 8086
- zbudowanie systemu debugowania (register dump, memory dump, single step)
- interpretacja instrukcji 8086
- implementacja części funkcjonalnosci systemowych DOS/BIOS

Spis tresci

Referencje

Verifying x86 Instruction Implementations

https://arxiv.org/abs/1912.10285

Intel 8086 Family User's Manual

https://edge.edx.org/c4x/BITSPilani/EEE231/asset/8086_family_Users_Manual_1_.pdf

Apple][Emulation on an AVR Microcontroller

https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/858/file/thesis_strauch_final.pdf

Referencje (kont.)

The INTEL® 8087 numeric data processor

https://dl.acm.org/doi/10.1145/1500518.1500674

Formal Specification of the x86 Instruction Set Architecture

https://publikationen.sulb.uni-saarland.de/handle/20.500.11880/26394

Emu8086

Implementacja referencyjna