Undocumented Instructions in Microprocessors

Smole, Vid (School: Upper Secondary School of Electrical and Computer Engineering and Technical Gymnasium Ljubljana)

Meznar, Urban (School: Upper Secondary School of Electrical and Computer Engineering and Technical Gymnasium Ljubljana)

The aim of our research was to find out if the ATMega328p processor contains undocumented instructions, and if it does, how they effect and change the registers and contents of RAM. In order to explore the field, we had to learn assembly for the ATMega328p microprocessor, which can be found on the Arduino Uno. We used Python scripts to inject potentially undocumented instructions into the assembly programs, which were then compiled with Atmel's compiler (avrasm2) to Intel HEX and uploaded to the Arduino Uno using a batch script. The program on the ATMega performed a memory dump, executed the injected instruction and once again sent the contents of the memory. The memory dumps were then analyzed with Python and C# programs. In the end, based on the differences between the memory dumps, before and after execution of the injected instruction, we could determine if an instruction really is an undocumented instruction. In total we’ve discovered over 120 undocumented instructions and proved that they can be found even in such simple processors.

Awards Won:

Innopolis University : Full tuition scholarships for the Bachelor program in Computer Science

Innopolis University : Full tuition scholarships for the Bachelor program in Computer Science