Welcome to Computer Architecture Exploitation and Security

Clear and detailed understanding of the architecture of a system under attack, or the system to be attacked, is crucial to determining the most effective ways to either prevent or detect the attack, or to facilitate the attack. In this course, you will learn about the two ubiquitous computer architectures used in most personal computers and Internet of things devices – the Intel x86 and the ARM. You will learn how individual instructions are executed and how data flows through the processor.

This course is composed of 50% lectures and 50% labs. The elements of the architectures will be introduced in the lectures, and you will work through the examples to gain a solid understanding of the material. Various programming tools will be introduced, with emphasis on the open source tools in the Linux environment. You will use text editors, compilers, assemblers and debuggers to write, compile and execute your own code.

In the labs, you will practice each concept introduced in the lectures. While the instructor will be available to answer your questions and to assist with the labs, you will be directed to study the available materials as well as to do your own research. The material in this course cannot be learned by reading a book about it. It requires hands-on practice – writing the code and debugging it for each assigned task.

**Topics**

There are nine modules that cover the following topics:

* Architecture of a general-purpose processor (GPP)
* The x86 hardware architecture
* The x86 software architecture
* Using x86 programming tools
* The ARM hardware architecture
* System on Chip (SoC) hardware architecture
* The ARM software architecture
* Using ARM programming tools
* Instruction sequences for reverse engineering

Tips for Success

* Practice using version control whenever it is appropriate.
* Practice C and assembly programming.
* Actively participate in the labs and discussions.