AZERIA LABS

This is a personal project that is meant to contribute to the InfoSec community by helping interested folks to understand the concepts of rather complex topics and is split into two parts: ARM Assembly Basics and ARM Exploit Development. The ARM Assembly Basics section of this site is meant for people who want to get the familiar with the ARM Assembly language. These tutorials do not require prior knowledge about the ARM platform and are a good starting point for future ARM reverse engineers or exploit developers. The ARM Exploit Development section is for those who have enough knowledge about ARM assembly language and are looking forward to develop their first exploits.

Writing ARM Assembly

An introduction into ARM assembly basics covering the following topics: differences between Intel processor and ARM processor, how assembly works under the hood, and how to compile an ARM assembly program.

Data Types and Registers

Learn about ARM data types, the different types of ARM registers, and the usage of the CPSR (Current Program Status Register) in conditional execution.

ARM and Thumb Instruction Set

Learn about the differences between the ARM and Thumb instruction set and the most common instructions used for writing ARM assembly code.

Memory Instructions: Load and Store

This chapter describes LDR/STR instructions covering three offset forms: **Immediate** value as the offset, **Register** as the offset, and **Scaled register** as the offset.

Load and Store Multiple

This chapter describes how to Load and Store multiple values at once using the instructions LDM and STM. You will also learn how PUSH and POP are being used on ARM.

Conditional Execution and Branching

Learn how to use condition codes for conditional execution in ARM and Thumb mode and how to use conditional branch instructions to jump to other functions.

Stack and Functions

In this part we will look into a special memory region of the process called the Stack and explore how functions work on the ARM platform.

START HERE

ARM Exploit Development

Due to rapid increase of ARM based devices it is necessary to properly evaluate the security of such devices. One way of doing this is through direct exploitation of identified security issues. To do so one needs to be able to understand the basics of ARM Assembly language, know at least the most common vulnerabilities, be capable of writing exploits and flexible when it comes to adjusting the payload. Our site is intended to give the basic knowledge in these areas of ARM Exploit Development with a hope that the gained skills will be used for increasing the security of ARM devices that are out there.

Writing ARM Shellcode

Learn how to trace system functions and how to use your knowledge about ARM assembly basics to write your first shellcode in ARM assembly.

LEARN MORE

Memory Corruptions

Learn how the memory layout of a process looks like and what memory corruptions are. This section covers Stack memory corruptions and Heap memory corruptions in more detail.

LEARN MORE