Expectation Management

You'll learn:

- How compilers implement exceptions
- How to reverse engineer them from a binary

This is not an exploitation talk.

About processor exceptions

During the normal flow of execution through a program, the program counter increases sequentially through the address space, with branches to nearby labels or branch and links to subroutines.

Processor exceptions occur when this normal flow of execution is diverted, to allow the processor to handle events generated by internal or external sources. Examples of such events are:

- externally generated interrupts
- an attempt by the processor to execute an undefined instruction
- accessing privileged operating system functions.

It is necessary to preserve the previous processor status when handling such exceptions, so that execution of the program that was running when the exception occurred can resume when the appropriate exception routine has completed.

Table 5.1 shows the seven different types of exception recognized by ARM processors.

Exception	Description
Reset	Occurs when the processor reset pin is asserted. This exception is only expected to occur for signalling powered up. A soft reset can be done by branching to the reset vector (`0x0000`).
Undefined Instruction	Occurs if neither the processor, or any attached coprocessor, recognizes the currently executing instru
Software Interrupt	This is a user-defined synchronous interrupt instruction.It allows a program running in User mode, for e