

Memory Safety

Memory Safety

In this section, we will be looking at software security—problems associated with the software implementation. You may have a perfect design, a perfect specification, perfect algorithms, but still have implementation vulnerabilities. In fact, after configuration errors, implementation errors are probably the largest single class of security errors exploited in practice.

In particular, we will look at a particularly prevalent class of software flaws, those that concern *memory safety*. Memory safety refers to ensuring that attackers cannot read or write to memory locations other than those intended by the programmer.

Because many security-critical applications have been written in C, and because C is not a memory-safe language, we will focus on memory safety vulnerabilities and defenses in C.