The SPIKE Fuzzer

Technically speaking, SPIKE is actually a fuzzer creation kit, providing an API that allows a user to create their own fuzzers for network based protocols using the C programming language. SPIKE defines a number of primitives that it makes available to C coders, which allows it to construct fuzzed messages called «SPIKES» that can be sent to a network service to hopefully induce errors. SPIKE was specifically designed to focus on finding exploitable bugs, so it's an excellent choice for our purposes.

There are also a number of papers and presentations available on SPIKE, with one of the most interesting being an older presentation from SPIKE author «Daily» Dave Aitel. (This presentation is available here https://www.immunitysec.com/downloads/usingspike3.ppt) While the presentation is rather lacking in detailed examples, it does outline a lot of the things that make SPIKE such a great fuzzer to use for discovering software vulnerabilities. Let's discuss some of these features, and see how they might be useful to us.