Abstract: RECON: Reconstruction of Protocol Parsing Module for Smart Fuzz Testing

Hyoung Chun Kim and Young Han Choi*
The Attached Institute of Electronics and Telecommunications Research Institute(ETRI)
{yhch,khche}@ensec.re.kr

Abstract

Smart fuzz testing is a methodology for finding security holes in a software system by inserting fault data into the input of the software with consideration of protocol format. Nevertheless, protocol analysis is a tedious and error-prone work. Therefore, a method is needed that can analyze a protocol specification automatically. In this paper, we propose a novel methodology that can reconstruct a protocol parsing module at assembly code-level to efficiently perform automatic protocol reverse engineering. After tracing a protocol parsing process without protocol information, our methodology can reconstruct the control-flow of a protocol parsing module using debug information. Using our methodology, we can perform smart fuzz testing focusing on only the codes related to the parsing module. We developed a practical tool, RECON, for our methodology using the WinDbg extension. Experimental result shows that RECON can reconstruct a parsing module sufficiently.