Exploiting the hard-working DWARF

Trojan and Exploit Techniques With No Native Executable Code

Agenda

Soruces

DWARF Summary

- Old school: typical exploitation techniques are trying to insert shellcode (since 1980's)
- Newer: trying to "borrow" necessary executable code snippets from target (end 1990/early 2000)
- Current: generalization, s.t. Turing-completeness is achieved (ROP)
- Other kinds of exploitable bugs: Int-overflow, parsing (mis)interpretation...
- **DWARF exploitation** as an alternative exploitation technique
  - In despite to return oriented programming (ROP) which is using its native code
  - DWARF allows an attacker to create a trojan payload for ELF executables without any native binary code.

Sources I