30 Years into Scientific Binary Decompilation: What We Have Achieved and What We Need to Do Next

By Ruoyu “Fish” Wang

Abstract

Almost 30 years have passed since the very first seminal paper on decompiling C binaries by Dr. Cristina Cifuentes was published. Clearly, by 2022, the binary decompilation problem has yet been solved. What is
our progress on the binary decompilation problem over these years? What are our achievements and pitfalls? What do we need to do next so the problem of binary decompilation will be solved before 2052, 30 years from today? The talk will (attempt to) answer these questions with the goal of attracting and unifying research effort in the security, software engineering, and programming languages community.

A similar version of this talk was given at the 2022 NDSS Workshop of Binary Analysis Research (BAR) as a keynote.

Everyone welcome!

About the Speaker

Ruoyu "Fish" Wang is an Assistant Professor in the School of Computing and Augmented Intelligence at Arizona State University. He is a co-director of the Laboratory of Security Engineering For Future Computing (SEFCOM) at ASU. His research focuses on system security, especially on automated binary program analysis and software reverse engineering. He is the co-founder and a core developer of the binary analysis platform, angr.

Fish received his Ph.D. degree from the Department of Computer Science at the University of California, Santa Barbara, where he was advised by Dr. Giovanni Vigna and Dr. Christopher Kruegel. He was a core member of
the CGC team Shellphish CGC, with whom he won the third place in the Final Event of the DARPA Cyber Grand Challenge in 2016.