Automating binary code reverse engineering with black-box solutions

Vidal Attias*[1,2]

[1]Laboratoire Instrumentation Multi-TEChnique (CEA, LIST) – Département d'instrumentation Numérique (CEA, LIST) – France

[2]Laboratoire Lorrain de Recherche en Informatique et ses Applications – Institut National de Recherche en Informatique et en Automatique, Université de Lorraine, Centre National de la Recherche Scientifique, Centre National de la Recherche Scientifique : UMR7503 – France

Résumé

We motivate in this document the need for alternative code simplification techniques. We show that the traditional white-box approach get rapidly get mitigated and has fundamental semantical limitations. Our work builds upon an emerging field of deobfuscation based on black-box techniques and demonstrate that although current state of the art solutions outperform white-box techniques, it is necessary to improve and support additional capabilities.

*Intervenant