Special Issue on “Binary Analysis”

In this thematic Series, we solicit original contributions on binary analysis, and encourage all international researchers and practitioners to present novel theories and techniques in analyzing binary executables (including binary or byte code in PC and servers, mobile and IoT devices, industrial control systems, automotive, etc.). All submissions will undergo rigorous peer review and accepted articles will be published within the journal as a collection.

Topics of interest include but not restricted to:
- Malware analysis and detection
- Exploit and security patch generation
- Vulnerability discovery and diagnosis
- Firmware analysis
- Reverse engineering
- Code obfuscation and de-obfuscation
- Decompilation
- Formal verification

Key Dates
Paper Submission: May 1, 2020
1st round notification: June 15, 2020
Revision due: July 15, 2020
Final notification: July 31, 2020

Guest Editors
Zhenkai Liang, liangzk@comp.nus.edu.sg, National University of Singapore, Singapore
Dinghao Wu, dinghao@psu.edu, Pennsylvania State University, USA
Heng Yin, heng.yin@ucr.edu, University of California, Riverside, USA

Submission Instructions
Prospective authors are invited to prepare and submit manuscripts following the instructions at:
https://cybersecurity.springeropen.com/submission-guidelines
the complete manuscript should be submitted through:

To ensure that you submit to the correct thematic series please select the appropriate thematic series ‘Binary Analysis’ in the ‘Additional Information’. In addition, indicate within your cover letter that you wish your manuscript to be considered as part of the thematic series on Binary Analysis.