Special Issue on “Cyber-Physical System Security”

Cyber-Physical Systems (CPS) consist of large-scale interconnected systems of heterogeneous components interacting with their physical environments. There exist a multitude of CPS devices and applications deployed to serve critical functions in our lives thus making security an important non-functional attribute of such systems.

This special issue solicits original contributions from both academia and industry on all areas of cyber-physical system security. The submission will undergo rigorous peer review and accepted articles will be published within the journal as a collection.

Topics include but are not limited to:

- Attack detection for CPS
- Attestation and assessment of CPS
- Authentication and access control for CPS
- Availability and resilience of CPS
- Critical infrastructure protection
- Modelling and analysis of CPS
- Recovery of CPS from cyber attacks
- Testbeds and experimental facilities for CPS security research

Key Dates
Paper submission: August 15, 2020
1st round notification: October 31, 2020
Revision due: December 15, 2020
Final notification: January 31, 2021

Guest Editor
Jianying Zhou <jianying_zhou@sutd.edu.sg>
Singapore University of Technology and Design (SUTD), Singapore

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: http://www.editorialmanager.com/cyse/default.aspx.

To ensure that you submit to the correct thematic series please select the appropriate thematic series ‘Cyber-Physical System Security’ 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 Cyber-Physical System Security.