Call for Papers

Special Issue on "Advanced Malware Analysis in IoT"

Scope: Malware analysis is an ever-green research area which is becoming challenging day by day with the evolution of new technologies such as Cloud Computing, Internet of Things (IoT), Mobile Cloud, Edge & Fog Computing, Virtualization, etc. The emergence of new technologies opens new doors for the attackers because of the introduction of new vulnerabilities and threats. The conventional security tools and approaches may not be sufficient enough to deal with the emerging threats and vulnerabilities. In fact, the attackers are now shifting their target from conventional computer systems to IoT devices, virtualization servers, mobile cloud platforms and end-user devices etc. Moreover, due to extensive exploitation of the Android platform in the IoT devices creates a task challenging of securing such kind of malware activities. The IoT applications are integrated with cloud servers and android devices; data privacy and security have become a very strong concern. As a real-world large-scale blackout, one can refer the malware against smart cities is the ransomware in health system in Ireland in May 2021 which affected the healthcare system over the country, putting the life of people in danger. The detection and prevention of the new malware variants becomes more difficult due to the invisible aspects, introduced by emerging technologies.

The purpose of the special issue is to publish high-quality papers addressing state-of-the-art ideas from various advanced computing domains in order to combat the new malware attacks with emerging technologies. We are soliciting original contributions, of leading researchers and practitioners from academia as well as industry, which address a wide range of theoretical and application issues in this domain. Topics may include, but are not limited to:

- IoT security framework for automated malware detection and response
- Deep Learning and soft computing for IoT malware detection/analysis
- Malware analysis in android applications, integrated with IoT devices
- AI based systems for securing IoT nodes against attacks
- Distributed microservice architecture for IoT security
- Virtualization security frameworks to design secure IoT
- Memory forensics approaches to deal with IoT malware
- Hypervisor security frameworks/architectures to secure Cloud in IoT ecosystem
- Cloud malware attack analysis and defensive solutions in IoT ecosystem
- IoT Botnet attack analysis and defensive solutions
- Memory acquisition techniques and analysis for IoT malware

Submission Guidelines

Submitted articles must not have been previously published or currently submitted for publication elsewhere. Submissions the journal guidelines will be summarily rejected. The journals must be submitted online at https://mc.manuscriptcentral.com/ieee-sj. The author guidelines can be found at https://ieeesystemsjournal.org/author-instructions/. Select the paper type "SI: Advanced Malware Analysis in IoT" upon submission to ensure that the article is considered for this special issue. Authors must also mention the same in their submission coverletter.

Important Dates

Submission Deadline: Jan 31, 2022

First round of review: April 01, 2022

Second round of review: May 30, 2022

Final Decision: Jun 30, 2022

For further information, please contact any of the Guest Editors.

Guest Editors

Dr. Preeti Mishra, Doon University Dehradun, India; Email: scholar.preeti@gmail.com

Dr. Nour Moustafa, University of New South Wales (UNSW)'s UNSW Canberra, Australia; Email: nour.moustafa@ieee.org

Prof. (Dr.) Pierluigi Siano, University of Salerno, Italy psiano@unisa.it

Dr. Hassan Haes Alhelou, University College Dublin, Ireland, alhelou@ieee.org

Prof. (Dr.) Vijay Varadharajan, University of Newcastle, Callaghan, Australia; Email: Vijay.Varadharajan@newcastle.edu.au

Dr. Md Zakirul Alam Bhuiyan, Fordham University, Bronx, NY USA, Email: mbhuiyan3@fordham.edu