High Performance Networks and
Architectures Laboratory
University of Castilla-La Mancha
Albacete, Spain

March 30, 2020

Dear Editor:

Please find enclosed our manuscript entitled "*Automatic Analysis Architecture of IoT Malware Samples*" by Javier Carrillo-Mondéjar, Juan Manuel Castelo Gómez, Carlos Núñez Gómez, José Roldán Goméz and José Luis Martínez, which we would like to submit for publication in *Security and Communication Networks.*

The weakness of the security measures implemented on IoT devices, added to the sensitivity of the data that they handle, has created an attractive environment for cybercriminals to carry out attacks. To do so, they develop malware to compromise devices and control them. The study of malware samples is a crucial task in order to gain information on how to protect these devices, but it is impossible to manually do this due to the immense number of existing samples. Moreover, in the IoT there exist multiple hardware architectures, such as ARM, PowerPC, MIPS, Intel 8086 or x64-86, which enlarges even more the quantity of malicious software.

In this regards, this paper proposes a modular solution to automatically analyze IoT malware samples from these architectures is proposed. In addition, the proposal is subjected to evaluation, analyzing a testbed of 1500 malware samples, proving that it is an effective approach to rapidly examining malicious software compiled for any architecture.

On behalf of my co-authors, I declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere. I also confirm that the manuscript has been read and approved for submission by all the named autors.

Yours sincerely,

Javier Carrillo-Mondéjar