A Deep Adversarial Network based Industrial Control Protocol Fuzzing Framework from A Self-Attention Perspective

Wanyou Lv[1], Bohao Wang[1], Jianqi Shi[1]*, Yanhong Huang[1], and Zhihui Li[1]

[1] National Trusted Embedded Software Engineering Technology Research Center, East China Normal University
Shanghai, China
{wanyou.lv, bohao.wang, zhihui.li}@ntesec.ecnu.edu.cn
{jqshi, yhhuang}@sei.ecnu.edu.cn

Abstract. The Industrial Control Protocol (ICP) is the cornerstone of the communication of the Industrial Control System (ICS). However, the industrial control environment applicable to ICPs has a strong diversity, which is difficult for testers to formulate a series of universal security rules. Therefore, fuzz testing (fuzzing) has already become the main method of detecting vulnerabilities in ICPs. It is noticed that the process of fuzzing relies heavily on specifications of ICPs. And it will take a lot of time and manual engineering to analyze and understand specifications. In this paper, we propose a new simple and smart sequence generation neural network framework based on Improved Wasserstein GANs (WGAN-GP), called HexGANFuzzer, to solve problems. Moreover, we put forward a series of performance metrics to evaluate different models in the field of fuzzing. Compared with traditional methods, our framework can generate massive fake but plausible test protocol messages automatically in a short time without protocol specifications. Compared with other deep learning works for fuzzing, our framework can not only increase the probability of triggering vulnerabilities, but also be more parallelizable and require significantly less time to train. We evaluate its performance by testing several typical ICPs, including MQTT and Modbus. Extensive experiments demonstrate significant improvements of HexGANFuzzer on test effectiveness and efficiency.

Keywords: Deep adversarial learning · Self-attention · Fuzz testing · Industrial control protocol

Acknowledgments

This work is partially supported by Shanghai Science and Technology Committee Rising-Star Program (No.18QB1402000), Shanghai Municipal Ecnomic and Infomatization Commission Project (2018-GYHLW-02012), Science and Technology Commission of Shanghai Municipality Project (No. 18ZR1411600).

* Corresponding author: jqshi@sei.ecnu.edu.cn