International Journal of Distributed Sensor Networks, 5: 23, 2009
Copyright © Taylor & Francis Group, LLC
ISSN: 1550-1329 print / 1550-1477 online
DOI: 10.1080/15501320802508543

An Efficient Worm Defense System Based Signature Extraction

HAO TU[1,2], ZHITANG LI[1,2], BIN LIU[1,2], and YEJIANG ZHANG[1]

[1]Network and Computer Centre, HuaZhong University of Science and Technology, P.R. China
[2]College of Computer Science and Technology, HuaZhong University of Science and Technology, P.R. China

The fast spread of a worm is a great challenge to Internet security. Most current defense systems use a signature matching approach while most signatures are developed manually. It is difficult to catch a variety of new worms promptly. An efficient worm defense system is designed and implemented to provide early warning at the moment the worms start to spread in the network and to contain or slow down the spread of the worm by automatically extracting a signature that could be used by firewalls or Intrusion Prevention Systems. Several recent efforts to automatically extract worm signatures from Internet traffic have been done, but the efficiency is an unsolved problem especially in real high-speed network. In this paper, we proposed an efficient worm defense system based signature extraction. The input of the system is all traffic crossing an edge network and its output is a database of worm signatures which can be used by content-based defense. There are three main stages to extract signatures from network traffic. First, a clustering stage uses multidimensional traffic mining based IP header to identify significant traffic volume. We propose a binary clustering algorithm and this leaves a preferred policy to improve the front traffic filter, which can reduce the traffic to be processed and enhance its purity. After clustering, nonsignificant traffic volume is stored in an innocuous packet pool and significant traffic volume is further classified using address dispersion as suspicious or innocuous. After this stage, only a small portion of the packets captured from the edge network are analyzed in third stage, signature extraction. A position-aware signature generation method based bloom filter is proposed to extract more accurate signatures with less CPU time and memory consumption. To minimize false positives, the signatures will be verified based on the innocuous packet pool. Both trace data and tcpdump data are used to test the prototype system. Experiment results show that the system can efficiently filter through suspicious traffic with high purity and extract more accurate signature, which can well support popular content-based defense system such as Snort.

This research was supported by the National Natural Science Foundation of China grant 60573120 and the National High Technology Research and Development Program of China grant 2007AA01Z420.

Address correspondence to Hao Tu, HuaZhong University of Science and Technology, China, E-mail: tuhao@hust.edu.cn

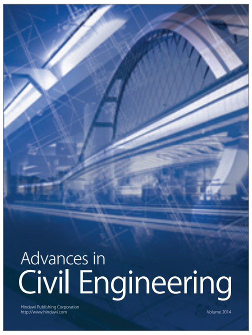
Journal of Engineering

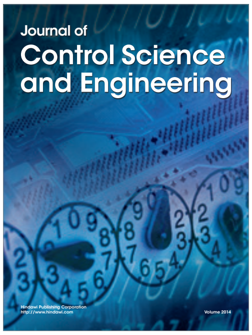
The Scientific World Journal

International Journal of Rotating Machinery

Journal of Sensors

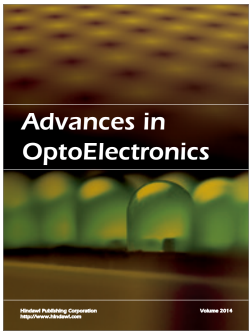
International Journal of Distributed Sensor Networks


Advances in Civil Engineering


Journal of Control Science and Engineering

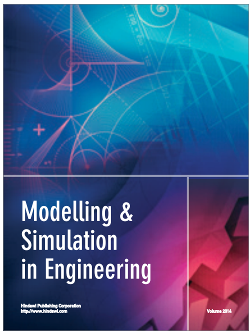
Journal of Robotics

Journal of Electrical and Computer Engineering

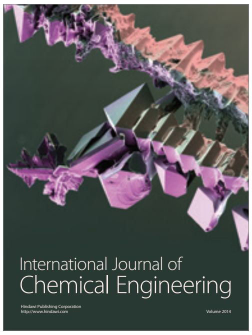

Advances in OptoElectronics

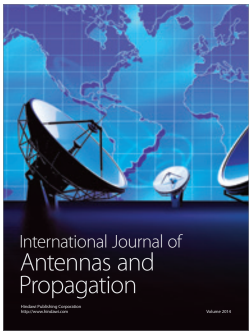
VLSI Design

International Journal of Navigation and Observation

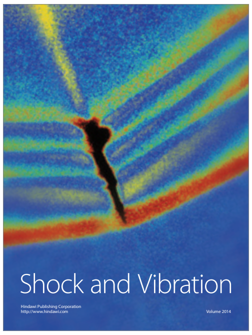

Modelling & Simulation in Engineering

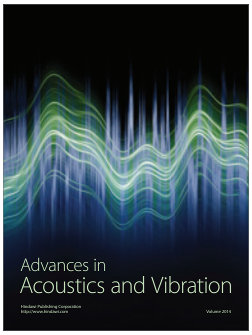
International Journal of Aerospace Engineering


International Journal of Chemical Engineering


International Journal of Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in Acoustics and Vibration