World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:5, No:1, 2018

Introducing a Polymorphic Machine Learning Defense for Cyber Attacks against Gibson Mainframe Computers

Authors : Dade Murphy, Kate Libby

Abstract : Gibson based mainframe computer platforms remain vulnerable to a specific class of buffer overflow first identified in 1988. Specifically, it is possible to corrupt the magnetic core memory stack by writing past the end of protected colonel memory. Code that does this is said to have 'Hacked the Gibson', causing a return from the routine to jump to a random address. This gives an attacker access to the superuser account, from where they have access to the whole system. As of writing, the only defense is to situate Gibson based mainframe computer behind seven or more proxies. Combining next generation, dynamic malware analysis techniques with polymorphic machine learning ZeroR classifiers, we demonstrate a 97.435% accuracy in detecting such attacks. Specifically, we designed four layered ZeroR classifiers which self-modify based on four distinct features present in malicious packets. Features consist of whether the packet has the FIN, URG and PSH flags set and how fragmented the packet is overall. We extensively evaluated our algorithm on a diverse spectrum of corpora with 81,337 malicious packets and 48,183 legitimate packets. Our results offer a promising advance in addressing a vulnerability which has existed for nearly three decades.

Keywords : buffer overflow, Gibson, polymorphic defense, ZeroR classifier
Conference Title : ICCWSS 2018 : 20th International Conference on Cyber Warfare and Security Systems
Conference Location : Amsterdam, The Netherlands
Conference Dates : January 22-23, 2018