104. INTRODUCING HIGH SECURITY IN CYBERSPACE USING MIMICKING ATTACKS AND ANTI-ATTACKS

D.JULIA JEMILA(PG STUDENT)P.PREETHY REBECCA(ASSISTANT PROFESSOR)
Department of computer science and engineering,St.Peter's college of engineering and technology

Botnets have become major engines for malicious activities in cyberspace recent days. To sustain their botnets and disguise their malicious actions, botnet masters are mimicking legitimate cyber behavior to fly under the radar. This poses a critical challenge in anomaly detection. In this study, use web browsing on popular web sites as an example to tackle this problem. First establish a semi-Markov model for browsing behavior. Based on this model, find that it is impossible to detect mimicking attacks based on statistics if the number of active bots of the attacking botnet is sufficiently large (no less than the number of active legitimate users). Still, it is hard for botnet owners to satisfy the condition to carry out a mimicking attack most of the time. With this finding, mimicking attacks can be discriminated from genuine flash crowds attack using second order statistical metrics. The aim of this project is to perform legitimate cyber behavior mimicking attacks from large scale botnets and also able to discriminate mimicking attacks from legitimate cyber events. Our real world data set experiments andsimulations confirm our theoretical claims. This finding can be widely applied to similar situations in other research fields.

ISBN 978-81-904760-6-5