Abstract

Hackers have devised a recent technique of infiltrating critical infrastructure with wanton applications that gulp at the limited resources possessed by these infrastructure for meeting critical needs and deadlines. Also a reality is the fact that hackers could breach already existing and trusted applications or software on these critical infrastructure and bug them with malicious codes that plunge them into a state of wantonness; consuming limited, critical resources and making none (or insufficient) available for other, equally critical applications that depend on a fair portion of the same resources to meet their deadlines and critical requirements. This development portends the next generation of denial of service (DoS) and distributed denial of service (DDoS) attacks to critical infrastructure, where all that is required is to discover vulnerabilities in already trusted and running applications on critical infrastructure or deliver and escalate new applications on these critical infrastructure and plunge them into wantonness, consuming limited resources and resulting in a denial of service. Proposals already exist in literature that could forestall an occurrence of such attacks, but some of these have not
ResMon: Securing Resource Consumption of Critical Infrastructure from Wanton Applications

previously been tested; one of such being that documented by [1]. This research is an experimental implementation of the theoretical model proposed in the cited article, in order to test and validate its workability and results. An experimental prototype – codenamed “ResMon” – of the model proposed is built and validated within the Ubuntu Linux operating system environment.

References

in multiple scenarios. Proceedings of the 2011 International Conference on Communication,
Computing & Security (pp. 517-522). Rourkela, Odisha, India: Association for Computing
Machinery New York, NY, USA. doi:10.1145/1947940.1948047

Protection Network for the Detection of Flooding DDoS Attacks. IEEE/ACM TRANSACTIONS
ON NETWORKING, Volume 20(Issue 6), 1828-1841.


mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR):
Article No. 3, 39(1). doi:10.1145/1216370.1216373


Index Terms

Computer Science
System Architecture

Keywords

Critical Infrastructure, Computing Resources, DoS, DDoS.