World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:06, 2022

Cyber Security Enhancement via Software Defined Pseudo-Random Private IP Address Hopping

Authors : Andre Slonopas, Zona Kostic, Warren Thompson

Abstract : Obfuscation is one of the most useful tools to prevent network compromise. Previous research focused on the obfuscation of the network communications between external-facing edge devices. This work proposes the use of two edge devices, external and internal facing, which communicate via private IPv4 addresses in a software-defined pseudo-random IP hopping. This methodology does not require additional IP addresses and/or resources to implement. Statistical analyses demonstrate that the hopping surface must be at least 1e3 IP addresses in size with a broad standard deviation to minimize the possibility of coincidence of monitored and communication IPs. The probability of breaking the hopping algorithm requires a collection of at least 1e6 samples, which for large hopping surfaces will take years to collect. The probability of dropped packets is controlled via memory buffers and the frequency of hops and can be reduced to levels acceptable for video streaming. This methodology provides an impenetrable layer of security ideal for information and supervisory control and data acquisition systems.

Keywords : moving target defense, cybersecurity, network security, hopping randomization, software defined network, network security theory
Conference Title : ICAITTC 2022 : International Conference on Advances in Internet of Things Technologies and Cybersecurity
Conference Location : Oslo, Norway
Conference Dates : June 23-24, 2022