A Distributed Cryptographically Generated Address Computing Algorithm for Secure Neighbor Discovery Protocol in IPv6

Authors : M. Moslehpour, S. Khorsandi

Abstract : Due to shortage in IPv4 addresses, transition to IPv6 has gained significant momentum in recent years. Like Address Resolution Protocol (ARP) in IPv4, Neighbor Discovery Protocol (NDP) provides some functions like address resolution in IPv6. Besides functionality of NDP, it is vulnerable to some attacks. To mitigate these attacks, Internet Protocol Security (IPsec) was introduced, but it was not efficient due to its limitation. Therefore, SEND protocol is proposed to automatic protection of auto-configuration process. It is secure neighbor discovery and address resolution process. To defend against threats on NDP&rsquo;s integrity and identity, Cryptographically Generated Address (CGA) and asymmetric cryptography are used by SEND. Besides advantages of SEND, its disadvantages like the computation process of CGA algorithm and sequentially of CGA generation algorithm are considerable. In this paper, we parallel this process between network resources in order to improve it. In addition, we compare the CGA generation time in self-computing and distributed-computing process. We focus on the impact of the malicious nodes on the CGA generation time in the network. According to the result, although malicious nodes participate in the generation process, CGA generation time is less than when it is computed in a one-way. By Trust Management System, detecting and insulating malicious nodes is easier.

Keywords : NDP, IPsec, SEND, CGA, modifier, malicious node, self-computing, distributed-computing
Conference Title : ICICS 2016 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 09-10, 2016

Open Science Index, Computer and Systems Engineering Vol:10, No:06, 2016 publications.waset.org/abstracts/45747.pdf