Efficient authentication mechanism for defending against reflection-based attacks on domain name system

ABSTRACT

Domain Name System (DNS) is one of few services on the Internet which is allowed through every security barrier. It mostly depends on the User Datagram Protocol (UDP) as the transport protocol, which is a connectionless protocol with no built-in authentication mechanism. On top of that, DNS responses are substantially larger than their corresponding requests. These two key features made DNS a fabulous attacking tool for cybercriminals to reflect and amplify a huge volume of requests to consume their victim's resources. Recent incidents revealed how harsh DNS could be when it is abused with great complexity by attackers. Moreover, these events had proven that any defense mechanism with single point deployment couldn't accurately and efficiently overcome an attack volume with high dynamicity. In this paper, we proposed the Efficient Distributed-based Defense Scheme (EDDS) to overcome the shortcomings of a centralized-based defense mechanism. By using an authentication message exchange, which is a Challenge-Handshake Authentication Protocol (CHAP)-based authentication mechanism. It is deployed on multiple nodes to determine the legitimacy of the DNS request. Moreover, it significantly reduces the impact of the amplification factor for the fake DNS requests without having any side effects on legitimate ones. Then, a Stateful Packet Inspection (SPI)-based packet filtering is proposed to distinguish legitimate requests from fake ones by considering the results of the authentication procedure. Both authentication-message exchange and SPI-based filtering are introduced to provide detection accuracy without reducing the quality of service for legitimate users. As the simulation results show, the proposed mechanism can efficiently and accurately detect, isolate, and discard the bogus traffic with minimal overhead on the system.

Keyword: DNS; Reflection/Amplification attacks; Amplification factor; CHAP; Source authentication