DNS Amplification Attack Detection via Flexible Flow (sFlow)

A. A. A. M. ATAN, M. N. M. M. NOOR, M. N. ISMAIL

Abstract

High availability plays a vital role in the Information Age. Ensuring availability involves the protection against network threats that could lead to unavailability, such as a Distributed Denial of Service (DDoS) attack. Relatively, Domain Name System (DNS) amplification attack is one of the biggest DDoS to date. The attack takes advantage of the circumstance that a small DNS query can cause amplified DNS replies. In regard to today's rapid networks, recent defense approaches have focused more on flowbased analysis as alternative countermeasure due to its efficacy in monitoring anomalous behaviour against fast-paced data streaming. However, fixed flow-monitoring application (i.e. NetFlow) is apparently known for its deferred processing mode which causes prominent delays in DDoS detection. Conversely, this paper proposed a method of detecting DNS amplification attack via flexible flow analysis. Preliminary results are based on the utilization of s Flow, immediate cache, and extended flow values involving DNS attributes.