Abstract

The unprecedented growth of the Internet over the last years, and the expectation of an even faster increase in the numbers of users and networked systems, suggest that in the near future the Internet may become the single integrated communication media. However, as the dependence on the networking infrastructure grows, its security becomes a major concern, in light of the increased attempt to compromise the infrastructure. In particular, the routing operation is a highly visible target that must be shielded against a wide range of attacks. The current interdomain routing protocol, the Border Gateway Protocol (BGP), is limited in implementations of universal security. Because of this, it is vulnerable to many attacks at the Autonomous System (AS) to AS routing infrastructure. Initially, the major concern about BGP security is that malicious BGP routers can arbitrarily falsify BGP routing messages and spread incorrect routing information. Recently, some authors have pointed out another kind of attack, called malicious dropping attack that has not studied before. The malicious draping attack can result in data traffic being blackholed or trapped in a loop. However, the authors did not elaborate on how one can detect such attacks. In this paper, we discuss and analyse a method that can be used to detect malicious dropping attacks in the Internet.
In this paper, we describe the formatting guidelines for IJCA Journal Submission.

Reference

- A. Heffernan, “Protection of BGP sessions via the TCP MD5 signature option”, RFC 2385, SRI Network Information Center, August, 1998

Index Terms

Computer Science Network Security

Key words

AS

BGP

Malicious Dropping Attacks

Monitoring point

Instability