Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.59 – 65

RESEARCH ARTICLE

An Integrated Approach to Detect and Limit IP Spoofing

Tanmay A. Abhang[1], Uday V. Kulkarni[2]
[1]M. Tech. Student, CSE Dept., SGGS IE&T, Nanded-431606, India
[2]Professor & HOD, CSE Dept., SGGS IE&T, Nanded-431606, India

[1] tanmay2abhang@gmail.com; [2] uvkulkarni@sggs.ac.in

Abstract— Transmission Control Protocol/Internet Protocol (TCP/IP) is the suite of communication protocols used to connect hosts on the Internet. IP address spoofing or IP spoofing is the creation of IP packets with a forged source IP address, with the purpose of hiding the identity of the sender or impersonating another computing system in order to gain unauthorised access. There are number of types of attacks that successfully employ IP spoofing. So it is mandatory for today's network scenario that there must be some mechanism present to avoid IP spoofing which ultimately causes different kinds of network and resource attacks. Many attempts are made to prevent from such attacks at router or network level. We employ an approach to control IP spoofing at Autonomous System (AS) level or at interdomain level by making use of implicit information contained in border gateway protocol (BGP) messages transferred between border routers of different ASes.

Key Terms: - IP spoofing; AS; BGP

Full Text: http://www.ijcsmc.com/docs/papers/July2013/V2I7201326.pdf