Security in Border Gateway Protocol (BGP)

Suvradip Chakraborty
Jadavpur University, India

Bhaskar Sardar
Jadavpur University, India

INTRODUCTION

Border Gateway Protocol (BGP) is a dynamic routing protocol that routes inter domain traffic, connecting Autonomous Systems (AS's) to form the decentralized backbone of the Internet (Rekhter, et. al., 2006). BGP provides reachability information to the ASs and disseminates external information internally within an AS. With the exponential growth of ASs, BGP has become one of the most critical components of the Internet's infrastructure. Unfortunately, the limited guarantees provided by BGP sometimes contribute to serious instability and outages. While many routing failures have limited impact and scope, others may lead to significant and widespread damage. Most of the risk to BGP comes from accidental failures, but there is also a significant risk that attackers could disable parts or all of network, disrupting communications, commerce, and possibly putting lives and property in danger. BGP's mutual trust model involves no explicit presentation of credentials, no propagation of instruments of authority, nor any reliable means of verifying the authenticity of the information being propagated through the routing system. Hostile attackers can attack the network by exploiting this trust model in inter domain routing to meet their own ends (Butler et. al, 2010). For example, on May 2005, an AS falsely claimed to originate Google's prefix and parts of the internet could not reach Google's search engine for roughly an hour as traffic was misdirected to the attacking AS. This article focuses on the various kinds of attacks on BGP and studies the solutions both in use and proposed to overcome the security vulnerabilities of BGP and discusses the open research issues. The next section provides background information on inter-domain routing and BGP. Subsequent sections focus on the security issues and attacks on BGP and their countermeasures.

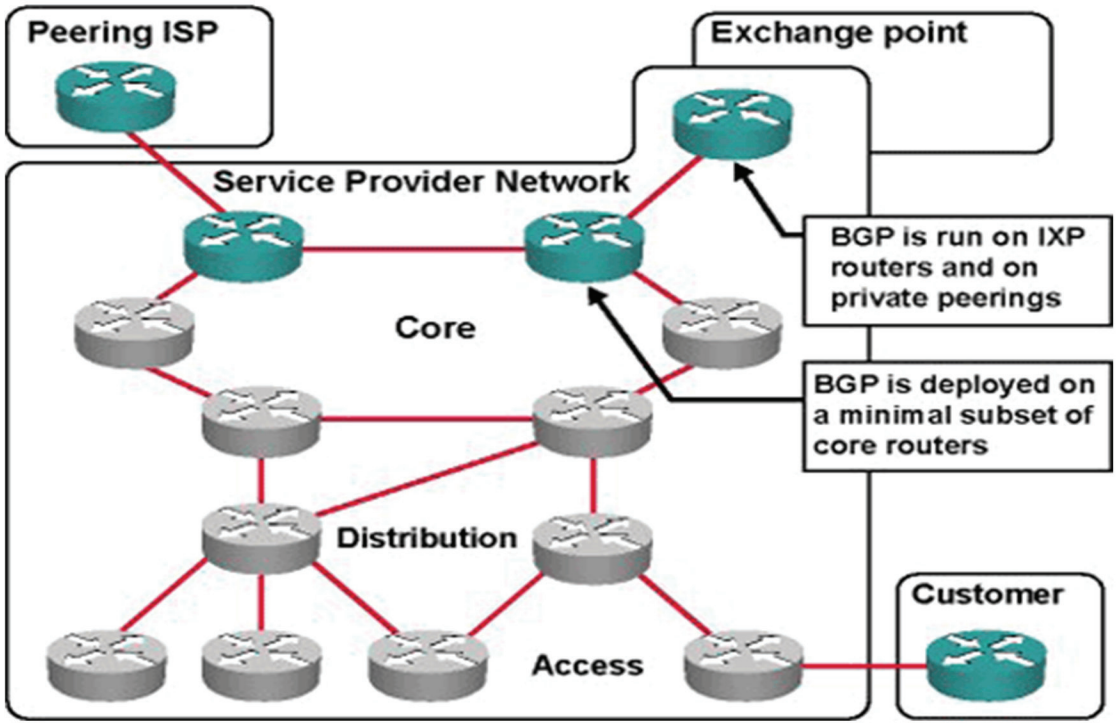
BACKGROUND

The Internet is composed of large number of ASs, which relay traffic to each other on behalf of their customers. The process of routing within an AS is called *intra-domain routing* which is mainly carried out by the Interior Gateway Protocols (IGPs), while routing among the ASs is called *inter domain routing*. BGP is the de-facto interdomain routing protocol that uses *path vector* form of distance vector routing algorithm. All major ISPs use BGP to distribute global routing information, internally and between each other. Figure 1 shows the connectivity model of BGP.

BGP neighbors, called *peers*, are established by manual configuration between routers to create a TCP session on port 179. TCP adds reliability and flexibility to BGP. Once the TCP connection is established between the peers, OPEN messages are exchanged by which BGP speakers can negotiate optional capabilities of the session, including multiprotocol extensions and various recovery modes. Once the OPEN message is acknowledged by the peer router, UPDATE messages are used to exchange reachability information. The other BGP messages include NOTIFICATION message which is sent by a router to indicate the termination of a BGP peering session, ROUTE REFRESH message that is sent to request a retransmission of routing information. A BGP speaker sends 19-byte KEEP-ALIVE message every 30 seconds to maintain the connection. Each BGP route object is a prefix and a set of attributes: <ASPath vector, Origin, Next Hop, Local Preference, Atomic Aggregate…>. One of the most critical attribute for BGP is *ASPath* which is an

DOI: 10.4018/978-1-4666-5888-2.ch682

Figure 1. Border Gateway Protocol (BGP)



ordered enumeration of AS values that form the path of ASs from the origin AS to the current AS across all possible paths. The originating AS adds it's AS number to the ASPath at first. Each of the transit AS, which imports the route, appends its own AS number to the ASPath before advertising the route to its peers. When a BGP speaker is presented with multiple paths to the same address prefix from a number of peers, the BGP speaker selects the *"best"* path to use which can be influenced by a number of factors and attributes- both *mandatory* which includes shortest ASPath, next hop attributes and *discretionary* (optional) such as local preference, community attribute, atomic aggregate, multi-exit discriminator etc.

BGP SECURITY ISSUES AND THREAT MODEL

BGP does not gaurantee security and privacy of routing traffic. The flaws of BGP have contributed to several major Internet outages. These problems are likely to get worse because cyber warriors, criminals, and even script kiddies have the potential to exploit BGP to deny service, sniff communications, misroute traffic to malicious networks, map network topologies, and trigger network instabilities. The numbers of attacks against BGP are on the rise. A recent attack was targeted against Spamhaus, an organization based in Switzerland responsible for maintaining IP addresses, which is reportedly the largest distributed denial of service attack in the history which saw 300 Gbps of traffic related to this attack.

BGP does not protect integrity, freshness, and origin authentication of messages. It neither validates an AS's authority to announce reachability information nor it ensures the authenticity of path attributes announced by an AS. There are no mechanisms in verifying correctness of routing information. The attacks on BGP can be categorized into the following categories: