A Survey of BGP Security

KEVIN BUTLER
Systems and Internet Infrastructure Labratory
Pennsylvania State University
TONI FARLEY
Arizona State University
PATRICK MCDANIEL
Systems and Internet Infrastructure Labratory
Pennsylvania State University
and
JENNIFER REXFORD
Princeton University

The Border Gateway Protocol (BGP) is the *de facto* interdomain routing protocol of the Internet. Although the performance BGP has been historically acceptable, there are mounting concerns about its ability to meet the needs of the rapidly evolving Internet. A central limitation of BGP is its failure to adequately address security. Recent outages and security analyses clearly indicate that the Internet routing infrastructure is highly vulnerable. Moreover, the design and ubiquity of BGP has frustrated past efforts at securing interdomain routing. This paper considers the vulnerabilities of existing interdomain routing and surveys works relating to BGP security. The limitations and advantages of proposed solutions are explored, and the systemic and operational implications of their design considered. We centrally note that no current solution has yet found an adequate balance between comprehensive security and deployment cost. This work calls not only for the application of ideas described within this paper, but also for further introspection on the problems and solutions of BGP security.

Categories and Subject Descriptors: C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*; C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Routing protocols*; C.2.5 [**Computer-Communication Networks**]: Local and Wide-Area Networks—*Internet*

General Terms: Security

Additional Key Words and Phrases: authentication, authorization, BGP, border gateway protocol, integrity, interdomain routing, network security, networks, routing

This work was performed while Farley and Butler were interns at AT&T Labs.
Authors' addresses: T. Farley, Information and Systems Assurance Laboratory, Arizona State University, 1711 S. Rural Road, Goldwater Center, Tempe, AZ 85287, USA; email: toni@asu.edu. K. Butler and P. McDaniel, Systems and Internet Infrastructure Laboratory, Pennsylvania State University, 344 Information Sciences and Technology Building, University Park, PA 16802, USA; email: {butler, mcdaniel}@cse.psu.edu.

1. INTRODUCTION

The Internet is a global, decentralized network comprised of many smaller interconnected networks. Networks are largely comprised of end systems, referred to as hosts, and intermediate systems, called routers. Information travels through a network on one of many paths, which are selected through a routing process. Routing protocols communicate reachability information (how to locate other hosts and routers) and ultimately perform path selection. A network under the administrative control of a single organization is called an autonomous system (AS) [Hawkinson and Bates 1996]. The process of routing within an AS is called *intradomain routing*, and routing between ASes is called *interdomain routing*. The dominant interdomain routing protocol on the Internet is the Border Gateway Protocol (BGP) [Rekhter and Li 1995]. BGP has been deployed since the commercialization of the Internet, and version 4 of the protocol has been in wide use for over a decade. BGP works well in practice, and its simplicity and resilience have enabled it to play a fundamental role within the global Internet [Stewart 1999]. However, BGP has historically provided few performance or security guarantees.

The limited guarantees provided by BGP often contribute to global instability and outages. While many routing failures have limited impact and scope, others lead to significant and widespread damage. One such failure occurred on 25 April 1997, when a misconfigured router maintained by a small service provider in Virginia injected incorrect routing information into the global Internet and claimed to have optimal connectivity to all Internet destinations. Because such statements were not validated in any way, they were widely accepted. As a result, most Internet traffic was routed to this small ISP. The traffic overwhelmed the misconfigured and intermediate routers, and effectively crippled the Internet for almost two hours [Barrett et al. 1997].

Loss of connectivity on the Internet can be manifested as anything from an inconsequential annoyance to a devastating communications failure. For example, today's Internet is home to an increasing number of critical business applications, such as online banking and stock trading. Significant financial harm to an individual or institution can arise if communication is lost at a critical time (such as during a time-sensitive trading session). As the number of critical applications on the Internet grows, so will the reliance on it to provide reliable and secure services. Because of the increased importance of the Internet, there is much more interest in increasing the security of its underlying infrastructure, including BGP. Such assertions are not novel: the United States government cites BGP security as part of the national strategy for securing the Internet [Department of Homeland Security 2003].

Current research on BGP focuses on exposing and resolving operational and security concerns. Operational concerns relating to BGP, such as scalability, convergence time (the time required for all routers to have a consistent view of the network), route stability, and performance, have been the subject of much effort. Similarly, much of the contemporary security research has focused on the integrity, authentication, confidentiality, authorization, and validation of BGP data. These two fields of operational issues and security research are inherently connected. Successes and failures in each domain are informative to both communities.

This paper explores current research in interdomain routing security, exposing the similarities and differences in proposed approaches to building a more secure Internet. The next section provides a brief overview of interdomain routing and BGP. Subsequent sections examine current research addressing BGP and interdomain routing security issues.

2. OVERVIEW OF INTERDOMAIN ROUTING

The autonomous systems that collectively comprise the Internet are controlled by individual organizations. They vary in size, from large national and multinational networks owned by corporations and governments, to small networks servicing a single business or school. The *lingua franca* of the Internet is the Internet Protocol (IP) [Postel 1981], allowing communication between disparate networks. There are three types of ASes: stub, multihomed, and transit. Stub ASes are communication endpoints, with connections to the rest of the Internet only made through a single upstream provider. Multihomed ASes are similar to stub ASes, but possess multiple upstream providers. Transit ASes have connections to multiple ASes and allow traffic to flow through to other ASes, even if the traffic does not originate or terminate within them. These ASes are often Internet Service Providers (ISPs), providing connectivity to the global Internet for their customers. The relationship between stub, multihomed and transit ASes is illustrated in Figure 2. ISPs can form *peering* relationships with each other, where they mutually forward their customer traffic over common links.

2.1 Routing within and between Autonomous Systems

Within an AS, routers communicate with each other through the process of intradomain routing. This is accomplished using an interior gateway protocol (IGP) such as the Routing Information Protocol (RIP) [Malkin 1994], the Open Shortest Path First protocol (OSPF) [Moy 1998], and the Intermediate System to Intermediate System protocol (IS-IS) [Callon 1990]. ASes communicate routing information via an external gateway protocol (EGP). The *de facto* standard EGP in use on the Internet is BGP version 4, which has obsoleted previous versions and the original ARPANET EGP protocol [Mills 1984]. While other interdomain routing protocols and architectures exist (e.g., [Alaettinoglu and Shankar 1995] and [Castineyra et al. 1996]), we restrict our discussion to BGP. However, many issues related to interdomain routing are independent of the protocol in use.

A router running the BGP protocol is known as a BGP *speaker*. BGP speakers communicate across TCP and become *peers* or *neighbors*. TCP is a reliable connection-oriented protocol and by employing it, BGP does not need to provide error correction at the transport layer [Minoli and Schmidt 1999]. Each pair of BGP neighbors maintains a *session*, over which information is communicated. BGP peers are often directly connected at the IP layer; that is, there are no intermediate nodes between them. This is not necessary for operation, as peers can form a *multi-hop* session, where an intermediate router that does not run BGP passes protocol messages to the peer. This is a less commonly seen configuration.

BGP peers within the same AS (internal peers) communicate via internal BGP (IBGP). External BGP (EBGP) is used between speakers in different ASes (external peers). The routers that communicate using EBGP, which are connected to routers