An Infrastructure Supporting Secure Internet Routing

Stephen Kent

BBN Technologies
Cambridge, MA 02138 USA

Abstract. The Border Gateway Protocol (BGP) [1] is the foundation of inter-domain Internet routing. A number of papers have described how BGP is highly vulnerable to a wide range of attacks [2, 3], and several proposals have been offered to secure BGP [4, 5, 6, 7, 8]. Most of these proposed mechanisms rely on a PKI, to provide trusted inputs for routing security mechanisms, to enable BGP routers to reject bogus routing advertisements. This paper provides a detailed proposal for a PKI, including a repository system, representing IP address allocation and Autonomous System number assignment,. This infrastructure offers a near term opportunity to improve routing security, since it does not require changes to routers, while also setting the stage for more comprehensive BGP security initiatives in the future.

1 Background

Inter-domain Internet routing is effected via a distributed system composed of many routers, grouped into management domains called Autonomous Systems (ASes), each identified by an AS number. Routers at the perimeter of each AS are called border routers, and BGP is the protocol executed between them. Routing information, most importantly AS path information (described below), is propagated between ASes using BGP UPDATE messages. Enabling border routers to verify that routes propagated via these messages are "valid" is the primary focus of several proposed BGP security technologies [4, 5, 6, 7, 8].

Although these proposals differ in may respects, all rely on the existence of a PKI attesting to resource holdings, specifically address blocks and AS numbers. Two of the proposals, S-BGP and soBGP, have provided details of how to organize such a PKI, while other proposals have either assumed the existence of the S-BGP PKI or have ignored PKI details and focused on digital signature optimization. To date, there has been essentially no progress in deploying any BGP security enhancements. Some require that more memory, and possibly crypto accelerator hardware, be added to border routers. In the current economic climate for ISPs, this is a very difficult expenditure to justify. The major router vendors no longer garner most of their revenue from sales to ISPs, so they are reluctant to invest in developing routers targeted toward the ISP market. Thus it may be a long time before such BGP security technologies can be deployed.

However, the sort of infrastructure that these security mechanisms assume as an underpinning can offer improved security prior to the deployment of such mechanisms. Creation of the infrastructure described below can be viewed as a first step toward

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 116 – 129, 2006.

more comprehensive security mechanisms. A concerted effort is now (2006) underway to secure agreement on design and deployment details for such a PKI. Staff from all five Regional Internet Registries (RIRs) are meeting to refine the design, and trials are underway. This paper describes the current design, derived from the S-BGP PKI model [9], noting new design aspects and details.

2 Securing Route Origination

Even if one does not deploy a BGP security solution that relies on such an infrastructure, the availability of the infrastructure would allow ISPs to detect bogus route origination. Bogus route origination occurs whenever an AS advertises itself as the origin AS for a prefix, without being authorized to do so by the (legitimate) holder of the prefix. This appears to be one of the most common forms of routing errors today, often arising from configuration errors by network operators. It also can arise from technical or social engineering attacks against ISPs, causing an ISP to advertise a route for a prefix that is not legitimately associated with a subscriber of the ISP. Some spam attacks are facilitated by this so-called "prefix hijacking." In either case, the bogus route origination will propagate through the Internet if neighboring ISPs do not filter UPDATEs to remove such errors.

Some ISPs use Internet Routing Registry (IRR) data to configure route filters, in an effort to reject bogus routes of various forms. However, network operators complain that the extent and quality of IRR data varies considerably by geopolitical region. There are no intrinsic quality controls on the IRR data, i.e., each ISP or multi-homed subscriber enters its own data into an IRR and, not surprisingly, errors arise. No authority is responsible for quality control of IRR data. Thus the ability to use such data in an automated fashion to create accurate route filters is limited. In contrast, the infrastructure described in this paper provides intrinsic controls on the data to which it attests, allowing automated detection of many forms of errors, as well as protection against attacks on the integrity or authenticity of the data.

The proposed security infrastructure consists of three components: a PKI, route origination authorizations (ROAs), and repositories. The PKI represents the allocation of address blocks and AS numbers to organizations. The ROAs enable an organization to explicitly authorize one or more ASes to originate routes to its address blocks. Repositories provide the means of distributing the PKI and ROA data to interested parties. The intent is that network operators upload to repositories any PKI or ROA data as it changes, and periodically download (e.g., on a daily basis) data uploaded by others. From this data, operators can extract authenticated address prefix origination data, which can be used to construct route filters in a more secure fashion than is currently offered via the IRR system. The following sections describe in greater detail how this data is represented, maintained, and processed.

3 Address Block Allocation and AS Number Assignment

IP addresses and AS numbers are allocated via a geopolitical, tree-structured scheme that ensures uniqueness. The root of the tree is the Internet Assigned Numbers Authority (IANA), which performs this and other operational functions on behalf of