BGP Route Selection Notice*

Wang Lijun, Xu Ke, and Wu Jianping

Department of Computer Science and Technology,
Tsinghua University, Beijing, China
{wlj, xuke}@csnet1.cs.tsinghua.edu.cn, jianping@cernet.edu.cn

Abstract. The present Internet is not trustworthy, partially because the routing system forwards packets only according to destination IP address. Forged packets with mendacious source IP address will also be brought to the destination, which can be utilized to compromise the destination machine. In this paper, we propose to enhance BGP by adding Route Selection Notice functionality. With BGP Route Selection Notice, Autonomous Systems can validate the authenticity of incoming IP packets and filter out improper packets to make routing infrastructure offer support to trustworthy service. BGP Route Selection Notice does not impair the routing function of BGP and with proper design its bandwidth cost and convergence delay is acceptable which is proved by our simulation.

1 Introduction

The next generation Internet is necessary to be more trustworthy to sustain many security-sensitive applications. As an important Internet infrastructure, the present routing system provides *best effort* service which forwards packets only according to destination IP address. When a host receives a packet from network, it identifies the remote sender by the source IP address. However, the host can not tell the source IP address is mendacious or genuine, which makes Internet not trustworthy. To meet the need of Internet development, service provided by the routing system should be enhanced to be trustworthy, which will includes two aspects: forwarding IP packets to destination properly and guaranteeing the packets forwarded are genuine.

Internet routing has two levels, intra-domain routing and inter-domain routing. BGP [1] is the *de facto* standard of the latter which is used among Autonomous Systems(ASes).To construct the trustworthy Internet, routing system firstly should be able validate the genuineness of packets on a coarse granularity, that is ASes only permit in or transmit packets coming from the ASes where the packets should come from. This paper concentrates on inter-AS validation which makes hosts can not disguise hosts in other ASes or use other improper source address, such as not assigned IP address, to serve the devil. Indeed, this

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No. 2003CB314801, and Hi-tech research and development program of China under Grant No. 2005AA112130.

I. Chong and K. Kawahara (Eds.): ICOIN 2006, LNCS 3961, pp. 440–449, 2006.

can only guarantee the packet comes from the true AS but not the true host, but we think this is the first step toward the trustworthy Internet.

We think over to guarantee packets validity according to the hierarchy of Internet routing system. Compare to intra-domain routing, inter-domain routing is not so much dynamic in despite of the instability observed in [2]. So routing-based Distributed Packet Filtering(DPF) [3] is a more practical method used in inter-domain routing than in intra-domain routing. On another aspect, routing system mainly can be divided into data plane and control plane. The packets forwarding function of data plane is support by routing protocols. The packets validation is implemented in data plane, it is also reasonable that the control plane provides the information used by the validation. So, we prefer to extend BGP to provide the validation criterion to be used in border routers.

Route is propagated like a rumor in BGP: the receiving AS is not sure the received route is true or not and the propagating AS is not sure whether the routes sent to neighbors are selected or not. For the latter, if a route of specific destination is not selected by a neighbor, then no packets to the destination should come from the neighbor, otherwise, packets going to the destination should be forwarded through the propagator. But in current BGP, the propagator knows nothing about the route sent to other ASes, including whether is selected and if selected, selected by ASes with what IP address space. A border router just receives whatever sent from neighbor ASes and forwards them to destinations properly. So the present inter-domain routing has no guard against potential threat which makes Internet untrustworthy.

In this paper we bring forward extending BGP with Route Selection Notice function. The main idea is if an AS selects a route from a neighbor, it sends a message containing the destination prefix of the route and the IP address space of its AS to the propagator, which informs the propagator that packets to the destination are valid only if the source addresses is in that address space. We design a new BGP message, SelectionNotice, to complete this function. SelectionNotice messages pass through the reverse path of BGP route propagation until reach the original AS of the route. Each border router along the path records the address space in the message and all such information store in border routers as Route Selection Information which is used to construct packets validation criteria. In the design, bandwidth cost and convergence time of Route Selection Information are the main concerns we think over. Selection Notice timer is introduced to improve the performance by piggyback more source address space of different ASes for a route. In simulation, we found the extension has little negative impact on routing function of BGP.

The rest of this paper is organized as follows. In the next section, we give a summary of related works. The design principles of Route Selection Notice are introduced in Section 3. In the following Section, we present the architecture of the extended BGP in detail. Simulation result will be presented in Section 5. Several issues relating to Route Selection Notice is discussed in Section 6. Finally, we conclude this paper in the last Section.