Security and Predictability: Two Missing Pieces in BGP

Lakshmi Subramanian
UC Berkeley

1 Introduction

BGP, the current inter-domain routing protocol, is a critical piece responsible for the functioning of the Internet. Two essential components which are missing from BGP are: *security* and *predictability*.

Lack of Security: BGP's resilience against attack is essential for the security of the Internet. BGP currently enables peers to transmit route announcements over authenticated channels, so that adversaries cannot impersonate the legitimate sender of a route announcement. This approach, which verifies *who* is speaking but not *what* they say, leaves the current infrastructure extremely vulnerable to both unintentional misconfigurations and deliberate attacks. While misconfigurations are a known occurrence, routers are surprisingly vulnerable to deliberate attackers. Some have *default passwords* [2, 7], others use standard interfaces like telnet and SSH, and so routers share all their known vulnerabilities. Deliberate attacks can involve an *isolated adversary* (i.e., a single compromised router) or *colluding adversaries* (i.e., a set of compromised routers). The spectrum of problems we need to secure against, in order of increasing difficulty, are *misconfigurations*, *isolated adversaries* and *colluding adversaries*. It is particularly difficult to secure against colluding attackers.

Lack of Predictability: BGP has evolved into such a complex protocol with several policy knobs and features that its dynamics have been hard to comprehend. Without a good understanding of these dynamics, efforts to address BGP's shortcomings have become essentially a black art. First, it is difficult for providers to determine how to configure the BGP protocol, since it is difficult to predict the effects of such a change. Second, only recently have several problems including those related to BGP route oscillations and convergence problems been brought to light. It is unclear whether these represent the entire spectrum of possible problems with BGP. Hence, it may be difficult for router manufacturers and researchers to suggest modifications to the BGP protocol, since the exact cause of many routing anomalies are not known. Additional modifications may further increase the complexity of the protocol and may trigger a new set of problems currently unknown to the community (*e.g.*, selective route flap dampening was introduced to address a convergence problem with the basic route flap dampening mechanism). In order to improve predictability, it is necessary to have a better understanding of the fundamental causes of routing changes observed at a router. In other words, we need answers for two questions: (1) *why does a routing change occur?* (2) *Where does a routing change originate?*

2 Improving the Security Model

To deal with misconfigurations and malicious adversaries, several sophisticated BGP security measures have been proposed, most notably S-BGP [5]. However, these approaches typically require an extensive cryptographic key distribution infrastructure and/or a trusted central database (*e.g.*, ICANN [1]). Neither of these two crucial ingredients are currently available, and so these security proposals have not moved forward towards adoption.[1] In our work, we abandon the goal of "perfect security" and instead seek "significantly improved security" through more easily deployable mechanisms. To this end we propose two measures, Listen and Whisper [6], that require neither a public key distribution nor a trusted centralized database.

Listen detects invalid routes in the data plane by checking whether data sent along routes reaches the intended destination. Whisper checks for consistency in the control plane. While both these techniques can be used in isolation, they are more useful when applied in conjunction. The extent to which they provide protection against the three threat scenarios can be summarized as follows:

Misconfigurations and Isolated Adversaries: Whisper guarantees *path integrity* for route advertisements in the presence of misconfigurations or isolated adversaries; *i.e.*, any invalid route advertisement due to a misconfiguration or

[1] There is much debate about whether their failure is due to the lack of a PKI and trusted database, or onerous processing overheads, or other reasons. However, the fact remains that neither of these infrastructures are available, and any design that requires them faces a much higher deployment barrier.

isolated adversary with either a fake AS path or with any of the fields of the AS path being tampered (*e.g.,* addition, modification or deletion of AS's) will be detected. Path integrity also implies that an isolated adversary cannot exploit BGP policies to create favorable invalid routes. In addition, Whisper can identify the offending router if it is propagating a significant number of invalid routes. Listen detects reachability problems caused by errors in the data plane, but is only applicable for destination prefixes that observe TCP traffic. However, none of our solutions can prevent malicious nodes already on the path to a particular destination from eavesdropping, impersonating, or dropping packets. In particular, countermeasures (from isolated adversaries already along the path) can defeat Listen's attempts to detect problems on the data path.

Colluding Adversaries: None of our techniques can prevent two colluding nodes from pretending there is a direct link between them by tunneling packets. Moreover, colluding nodes can exploit the current usage of BGP policies to create large scale outages without being detectable by either Listen or Whisper. To deal with this problem, we suggest simple modifications to the BGP policy engine which in combination with Whisper can largely restrict the damage that colluding adversaries can cause. In the absence of complete knowledge of the Internet topology, these two problems also exist in the case of heavy-weight security solutions like Secure BGP [4].

3 Improving Predictability

We believe that a first step towards improving the predictability of BGP is to develop a formal methodology for analyzing routing changes and inferring *why* they happen and *where* they originate. Answers to these questions can provide useful insights into the sources of routing instabilities. We have built a *BGP health monitoring system* [3], which continuously infers the state of the network by merely observing routing updates from multiple vantage points. In particular, our system determines the set of events that triggers each route update. Such inferences may then be used: (a) *offline* for network performance monitoring and troubleshooting; or (b) *online* to improve path selection and damping of instability. Since inferences that can be made from a single vantage point may be limited, we require updates from multiple vantage points to improve the accuracy of our inferences.

By analyzing route updates from Routeviews and RIPE for over 18 months, our system could detect several interesting anomalous routing events. A few examples include:

1. **Peering link instability:** On July 21 2003, the peering link between AS 1239 and AS 701 underwent a large number of session-reset like events, affecting the reachability of over 20,000 prefixes. Among the affected domains include cnet.com, excite.com, and weather.com. During this period of time, the AS paths traversed by these prefixes cycled through several paths, occasionally interspersed with withdrawals. Sprint's web site notes outages during this period of time but does not reveal the size or specifics of the event. The event affected routing tables in many AS's, and was visible from several viewpoints.
2. **Misconfiguration:** On June 26 2003, AS 2500 advertised paths for over 500 prefixes it did not own. This event affected prefixes owned by several major providers, including AT&T WorldNet Services, NTT, and Cable&Wireless. The instability was short-lived, lasting about 15 minutes.
3. **Reroutes:** On January 23 2003, an event on the peering link between AS 2914 and AS 3561 abruptly caused over 6000 prefixes to change to alternate paths. These prefixes abruptly returned to their original paths one hour later. Prefixes owned by several major providers were affected by this event including Bell Atlantic, Nortel, and Cable&Wireless.

References

[1] Internet Corporation for Assigned Names and Numbers. `http://www.icann.org/`.

[2] Trends in dos attack technology. `http://www.cert.org/archive/pdf/DoS_trends.pdf`.

[3] M. Caesar, L. Subramanian, and R. H. Katz. *Root Cause Analysis of BGP Dynamics*. Technical Report, UC Berkeley, 2003.

[4] S. Kent, C. Lynn, and K. Seo. Design and analysis of the Secure Border Gateway Protocol (S-BGP). In *Proc. of DISCEX '00*.

[5] S. Kent, C. Lynn, and K. Seo. Secure Border Gateway Protocol (Secure-BGP). *IEEE Journal on Selected Areas of Communications*, 18(4):582–592, Apr. 2000.

[6] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz. *Listen and Whisper: Security Mechanisms for BGP*. Technical Report, UC Berkeley, 2003.

[7] R. Thomas. `http://www.cmyru.com`.