

Darwin’s Secure BGP?

An Open Platform for the Evolution of Routing Security

Dan Wendlandt - Carnegie Mellon University - dwendlan@cs.cmu.edu

For the past decade, operators and researchers have struggled with how to respond to well-known security vulnerabilities in BGP. Despite many strong technical proposals, an agreed upon and deployed solution remains distant [2]. Instead of focusing on selecting and globally deploying a particular secure routing proposal (s-BGP vs. so-BGP, etc.), we advocate the creation of a generic interface for selecting routes capable of interpreting data generated by any routing security approach. The specific mechanism used to generate the data can change, allowing the infrastructure to “evolve” over time as additional attack resistance is needed.

1 Creation vs. Evolution (In BGP Security)

In an ideal world, the “creation” of a single secure protocol that remedies the vulnerabilities in BGP would let operators flip a switch and never again worry about BGP security. While enticingly simple, we feel that such a “no security to full security” approach is unrealistic for two reasons:

(1) Past secure routing proposals differ greatly on a fundamental trade-off: mechanisms that provide the greatest attack resistance commonly have the highest costs for deployment and use. Given the many interested parties, each with diverse needs, arriving at one “blessed” solution will be difficult. Additionally, a security vs. cost trade-off that makes sense today may prove ill-advised in the future when the perceived threat grows.

How evolution can help: Instead of “baking” a particular cost vs. security trade-off into the routers, evolvable routing security lets operators start with simple protections (e.g., eliminating most BGP misconfigurations), while leaving the door open to future improvements. The flexibility of an evolutionary mechanism also helps individual ASes tailor their routing security mechanisms to a locally desirable cost/security trade-off.

(2) Secure versions of BGP often present high barriers to entry, yet provide few security benefits until widely deployed. As a result, investing money to deploy a new protocol as an early adopter can be unattractive for an AS, since costs are high, but benefits depend entirely on the willingness of others to participate. The result is a cyclic dependency that can stall deployment.

How evolution can help: An evolutionary approach to routing security can break deployment into many steps, each of which provides incrementally more security. Because each step is small, the cost (and associated risk) of participation is greatly reduced. This, in turn, minimizes the effect of cyclic dependencies.

2 Sources of Data in Evolutionary Routing Security

Data used to select more secure routes can come from many *information sources*. In an evolutionary approach, data initially comes from readily, though less authoritative, sources. Over time, operators can add data that is more comprehensive and/or more trusted in order to resist attacks. Likely sources include:

- **Route History:** Significant past research demonstrates that BGP paths change infrequently. As a result, approaches like PG-BGP [6] and PHAS [7] use history to infer AS connectivity and prefix ownership, letting them recognize and (temporarily) avoid suspicious routes. In practice, large providers or entities like Renesys may collect and compile historical BGP data on behalf of small ISPs.
- **Bilateral Trust:** Providers often limit customer announcements, filtering all but a registered set of prefixes. Sharing such “local” data with BGP neighbors provides an additional source of routing trust information.

- **Authoritative PKI or Registries:** Routing data may be authenticated using trust rooted at authoritative entities like region registries, tier-1 ISPs, or CAs like Verisign. It is quite possible that a routing PKI would have multiple roots or that several route registries will co-exist, meaning that ASes may trust some information sources more than others [5, 3].
- **Data-Plane Probing/Monitoring:** Data-plane probing can “reality-check” paths prior to their selection in the control plane. Schemes like Listen [8] catch obvious black-holes, while more sophisticated mechanisms can detect hijacks in real-time [4] or reveal the presence of compromised data-path elements [1].

3 Properties of a Generic “Route Selector”

We argue that any routing security mechanism, from so-BGP to Listen & Whisper, can be abstracted as an *information source* that represents its decision-making as a set of “filters”, not unlike BGP ACLs used today. Provided with a trust ranking for each information source (i.e., each set of filters), a generic route selector can apply these filters to choose more trusted routes *without regard to how the filters themselves where generated*.

A key difference compared to BGP ACLs, however, is that in the evolutionary approach, data is not assumed to be complete or authoritative. Below we outline the basic properties, beyond those already provided by BGP ACLs, that this generic route selector should support:

1. **Per-Prefix Trust Thresholds:** Given a trust ranking of all information sources, for each prefix the route selector should chose only the route(s) validated by the *most trusted source* to validate any route for that prefix. Because the existence of highly trusted authentication information for a route causes less trusted paths for that prefix to be rejected, individual prefix owners have an incentive to publish more authoritative data.
2. **Path Plausibility Testing:** Given a database of AS-AS connectivity pairs the selector should be capable of determining “AS-path plausibility” for a route announcement (i.e., does each AS hop exist in the database?). This so-BGP style model is a simple way to express data from BGP history or route registries.
3. **Combining Data from Multiple Sources:** Combining data from multiple sources can support stronger trust statements (e.g., this route was validated by independent data sources) or allow different sources to “work together” by filling in each other’s knowledge gaps.
4. **Dynamic Update:** The cost of adding or removing individual “filters” must not be prohibitive.

A generic route selection mechanism provides greater flexibility for operators to choose how routing data is authenticated. The ability for routing security mechanisms to evolve over time is a practical way to realize the benefits of the many novel routing security techniques proposed in past years.

References

- [1] I. Avramopoulos and J. Rexford. Stealth Probing: Securing IP Routing through Data-Plane Security. Technical Report TR-730-05, Princeton University, 2005.
- [2] S. M. Bellovin, J. Ioannidis, and R. Bush. Position paper: Operational requirements for secured BGP. In *Proc. DHS Secure Routing Workshop*, Mar. 2005.
- [3] B. Christian and T. Tauber. *BGP Security Requirements*. IETF, Feb. 2007. Internet Draft: draft-ietf-rpsec-bgpsecrec-07.txt.
- [4] X. Hu and Z. M. Mao. Accurate real-time identification of ip hijacking. Technical Report CSE 516-06, Univ. Michigan CSE, 2006.
- [5] Y.-C. Hu, D. McGrew, A. Perrig, B. Weis, and D. Wendlandt. (R)Evolutionary bootstrapping of a global PKI for securing BGP. In *Proc. 5th ACM Workshop on Hot Topics in Networks (Hotnets-V)*, Nov. 2006.
- [6] J. Karlin, S. Forrest, and J. Rexford. Pretty good BGP: Improving BGP by cautiously adopting routes. In *Proc. International Conference on Network Protocols*, Nov. 2006.
- [7] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang. PHAS: A prefix hijack alert system. In *Proc. 15th USENIX Security Symposium*, Aug. 2006.
- [8] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz. Listen and whisper: Security mechanisms for BGP. In *Proc. USENIX NSDI*, Mar. 2004.