Paper Review 0

- Reviewer: CPT Roy Ragsdale
- Paper Title: Secure Border Gateway Protocol (S-BGP) — Real World Performance and Deployment Issues
- Authors: Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo

Did you like this paper? Why?

I thought this paper addressed an interesting and important topic but was very light on the security implications. Also I felt that given the large number of assumptions they made the resulting recommendation, that collocated hardware could address performance concerns, was relatively weak.

What problem is this paper solving?

This paper is an analysis of a proposed system specifically looking at S-BGP and focusing on performance characteristics. It uses an experimental methodology of a network testbed to reply real world traffic to determine the overhead that S-BGP incurs relative to BGP. The stated aim is to provide feedback on the feasibility of deploying S-BGP.

What are the strengths of this paper?

A strength of this paper is that it provides a thorough analysis of many performance characteristics of an S-BGP implementation, including network overhead, storage, and processing requirements. This analysis of characteristics which contribute to the overall feasibility of deployment will be valuable for evaluating any proposed future optimizations. Another strength
of this paper is that they provide an concrete recommendation for achieving feasibility of a deployment. Unfortunately the bound they were able to determine requires the use of additional collocated hardware which is a substantial impediment.

What are the main weaknesses in the paper?

A primary weakness of this paper is the lack of addressing security considerations. In the few areas where they specifically address security, the paper seems takes the approach that as long as S-BGP is correctly operated then security guarantees will be achieved. Additionally the paper makes a number of assumptions concerning AS local operations that could be relevant to the overall security, and certainly the end result of users receiving the correct routes. Though these consideration may not be addressed by S-BGP, relying on local security policies to be correct seems to lend itself to the same potential for Byzantine failures the protocol is attempting to prevent.

Next Steps?

The key aspect that I think this paper missed is failing to address attacks that
could occur even in the face of a successful S-BGP deployment. By equating correctness with security and assuming secure AS local policies and operations I think the paper fails to make a strong security argument. Additionally because the proposed recommendation of adding additional hardware sets a relatively high bar it is left unclear how much they deployment of S-BGP would tangibly improve end user security. Specifically the paper makes the claim that S-BGP would only need to be deployed to "just the BGP routers of the half a dozen or so major ISPs", but then does not address how secure operations are then extended to end users. Another area where the paper makes a number of assumptions, thus leaving room for future work,

is regarding the bootstrapping steps of the PKI infrastructure. The paper repeatedly claims that Address Announcements (AA) and certificates can be effectively distributed and validated out of band to reduce the protocol overhead, but this assumption should be validated or at the very least demonstrated to match a similar out of band process that currently exists. A final thought that is possible given the passage of time is that the paper underestimates the likelihood of partial deployments that require additional collocated hardware. Since 16 years later S-BGP still does not appear to have wide deployment this deployment issue seems
to have dominated.

How to Read a Paper

1. Category

This paper is an analysis of a proposed system. Specifically looking at S-BGP and focusing on performance characteristics. It uses an experimental methodology of a network testbed to reply real world traffic to determine issues with performance.

2. Context

This paper is most related to work that identified vulnerabilities/attacks existing against BGP. Also it builds upon the theoretical foundations that went into developing the S-BGP protocol. Though it provides an overview of the protocol it doesn't focus on the correctness or security of it, but rather on the performance and deployment impediments.

3. Correctness

This work assumes that correctness guarantees security. While surely having BGP operate correctly (aka according to spec) is desirable, I'm not sure that this correctness property ensures any specific security guarantees. I think that would require reasoning about the protocol itself. The experimental methodology does seem to be robust and valid as long as you can rely on the CARIN testbed to accurately reflect real world network behavior.

4. Contributions

This paper's main contributions are in providing empirical data on how S-BGP would preform when tested against real world traffic loads. This leads to the recommendation that additional hardware is sufficient to get started on deploying S-BGP.

5. Clarity

This paper is well written and provides appropriate figures and graphics to understand the underlying system that is proposed. Additionally the level of detail provided is sufficient to inform further implementation and exploration.