Listen and Whisper: Security Mechanisms for BGP
Review by Frank Fetters

The main problem is the creation and propagation of invalid routes on high level routers. The two main sources for these invalid routes are malicious adversaries and mis-configurations in other routers. This paper discusses two tools used to detect and reduce the effect of these invalid routes.

These tools are Listen and Whisper, two non-invasive tools which will reduce the effectiveness of invalid routes. Listen is basically a listener which double checks that all the routes advertised actually work the way they are supposed to. Whisper uses more advanced techniques to make sure that the route advertised is accurate.

Whisper will take the many advertisements for a new route and test them all to make sure they are consistent. Its main feature is all of the ways it tests path consistency. Listen basically watches traffic and updates and if a trouble spot comes up, Listen is able to signal the existence of the problem.

A neat technique is the penalty based route selection. When you are caught generating a bad route, anyone who got that bad route will give you a penalty point. The more points you have the less likely another router will use your route. Pretty soon, it becomes obvious which router’s have problems.

This paper effectively shows how these two methods can be combined to successfully slow down and stop isolated adversaries and many misconfigurations. More techniques will need to be added to stop a large group of colluding adversaries.