BGP Security: Threats and Solutions

KEVIN BUTLER AND PATRICK MCDANIEL

BGP

The Border Gateway Protocol (BGP) provides the means by which the independent networks that comprise the Internet communicate with each other. In BGP, networks are organized into autonomous systems (ASes) that exchange IP prefixes to each other. As BGP is a path vector protocol, prefixes with the shortest path length are chosen as the preferred method for getting to a destination. Path attributes can further influence policy decisions.

Threats to BGP

BGP is susceptible to threats from a global level. Prefix hijacking involves an AS advertising routes belonging to another AS. A malicious AS could then drop the traffic that is has misdirected (creating a black hole) or impersonate the victim AS to potentially damaging ends. This is an example of an attack against origins. Real-world instances of this have brought down large portions of the Internet for hours at a time. Attacks against paths can be similarly damaging; the path describing how a prefix is transited to its origin can be forged or modified, allowing denial of service attacks and consuming router resources. In addition, ASes colluding together can create worm-holes, or illusory connectivity.

Origin Authentication

We create a number of proof systems showing that, contrary to previous results, on-line origin authentication is possible due to significantly reduced computational burdens. Our results are based on analysis of the address delegation hierarchy which shows that as few as 16 organizations perform 80% of address delegations on the Internet. Our authenticated delegation lists, and particularly delegation trees, exploit these properties to substantially reduce the number of signature validations required.

Address Usage

This quad chart gives a graphical depiction of the current address use in the Internet and provides insights into address delegation.

BGP Path Authentication

Through data-driven analysis, the cryptographic constructions that we devise reduce signature validation costs by as much as 97.3% over existing proposals. We also provide formal analysis of our solution by proving the security of the proof scheme against existential forgery and replay, and prove the security of the route attestation tags that provide the path authentication. This scheme exploits the inherent reference locality that we found in BGP paths, based on the analysis of hundreds of millions of routes over a two-year period.

Large-Scale BGP Simulation

BGP spans a massive number of networks, with over 20,000 ASes currently comprising the Internet. Our Isb simulator allows us to simulate the entire eBGP protocol with real data traces from repositories such as RouteViews and RIPE. We can model the operation of the Internet from any time in the past through repository data, and show the effects of attacks across the Internet with our attack generator. This will additionally allow us to accurately model the effect of security solutions on BGP operations and performance.

RESEARCH SUPPORTED BY AT&T, NSF, DARPA & DHS