Analyzing the Deployment of Secure Routing Protocols at Internet Scale

Braden Hollembaek, Kevin Butler

Computer and Information Science Department, University of Oregon

With large-scale attacks occurring at an alarming rate, the current state of Internet routing security has proven to be inadequate. Various security modifications to the current protocols have been proposed to help mitigate this problem, but none have seen widespread support due to the lack of investigative research performed. By creating software capable of simulating all of the world's routing traffic, we are able to test the impact of multiple security enhanced routing protocols. This research will strengthen the Internet by providing the critical analysis needed to discern the feasibility of deploying secure routing protocols across the highest levels of the Internet and help us to better understand which security features are the best candidates for adoption.

The State of BGP Security

To combat the known problems with BGP security, the Secure Inter-Domain Routing workgroup was formed and designed BGPsec, which creates a chain of provenance for a route that can guarantee to an AS that the route was originated by a trusted entity and that the path to reach the destination contains only trusted parties. Unfortunately, BGPsec has failed to see widespread adoption. This is due, in part, to the high demands of bandwidth and cryptographic processing power required by the protocol. Each signature added to the BGP route advertisement significantly increases its size. Each signature also needs to be verified, burning CPU time. This raises concerns about congesting networks and overloading router processors.

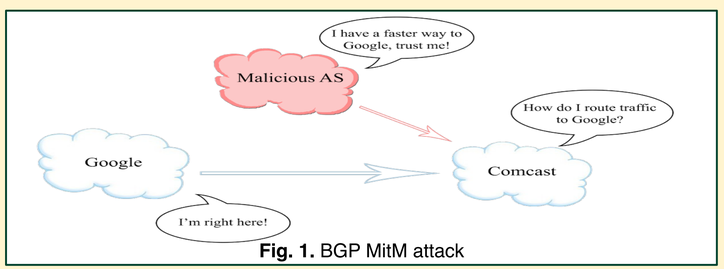

Fig. 1. BGP MitM attack

Large Scale eBGP Simulator

To date, no study has attempted to simulate the entirety of the Internet's AS infrastructure with regards to modeling the costs BGP security enhancements. Using real routing data recorded from Internet traffic by the Oregon Route Views project, we are able to use custom simulator software to predict the effects of BGPsec as implemented on a global scale. The simulator is a Java program that is capable of running over 40,000 concurrent threads to replicate the global AS topology. It can be run as a single node or distributed across multiple machines with a synchronized logging system to maximize hardware resources. This functionality enables us to emulate real world BGP and BGPsec traffic at an unprecedented scale. The simulator has the ability to test multiple signing and verification schemes as well as alternative protocol implementations.

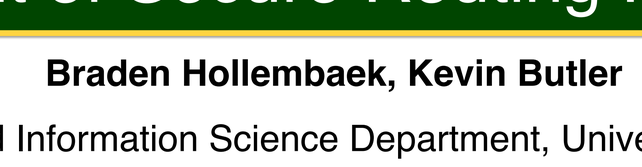

Fig. 2. BGPSEC Signing Procedure

Preliminary Results

While testing of the full scale data set is still in progress on the ACISS cloud platform, sample results in the difference in bandwidth usage of control messages between BGP and BGPsec has been analyzed. Using a simple RSA-2048 signing mechanism during a short simulation between just 55 ASes, we have observed an increase in bandwidth usage from BGP to BGPsec totaling over 3600%. This figure shows the need for optimization.

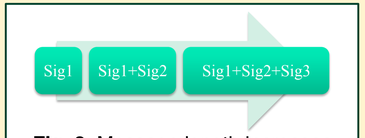

Fig. 3. Message length increases

The Simulator in Action

```
1397197861545 47 RECV SEC-WITHDRAW 1.0.0.0/8 path=[50 53 52 48 6 11 13 10 7 5 2 1 ] >>
1397197861545 47 RECV SEC-UPDATE 1.0.0.0/8 path=[50 53 52 48 6 5 7 9 12 8 3 1 ] >>
1397197861545 47 received a secure update for path [50 53 52 48 6 5 7 9 12 8 3 1 ] from 50 >>
1397197861545 31 received a secure update for path [30 27 24 21 13 10 7 5 2 1 ] from 30 >>
1397197861546 31 RECV SEC-UPDATE 1.0.0.0/8 path=[63 68 26 22 12 13 11 6 2 1 ] >>
1397197861546 69 received a secure update for path [72 68 63 61 64 81 80 10 7 4 3 1 ] from 72 >>
1397197861546 69 RECV SEC-UPDATE 1.0.0.0/8 path=[72 68 26 25 22 12 9 7 5 2 1 ] >>
1397197861546 29 RECV SEC-UPDATE 1.0.0.0/8 path=[32 28 23 21 13 10 7 9 12 8 3 1 ] >>
1397197861546 29 received a secure update for path [32 28 23 21 13 10 7 9 12 8 3 1 ] from 32 >>
1397197861546 32 RECV SEC-UPDATE 1.0.0.0/8 path=[33 30 27 24 21 22 12 13 11 6 2 1 ] >>
1397197861546 32 received a secure update for path [33 30 27 24 21 22 12 13 11 6 2 1 ] from 33 >>
```

This figure shows an excerpt from the simulation log. From left to right, we see the timestamp, AS number, message type, the IP range being advertised, and the AS path to it.

Conclusion

At the conclusion of this study, we will have mined a significant amount of data that can tell us the total increase in network traffic, processor workload, and overall coverage of BGPsec in such an environment where not all ASes are using BGPsec. The simulations will also investigate the efficacy of various proposed signature mechanisms. From this, we will be able to provide definitive information on which mechanisms are well-suited for use at internet scale and which will require further refinement. The tests are being ran on the University of Oregon's ACISS supercomputer.

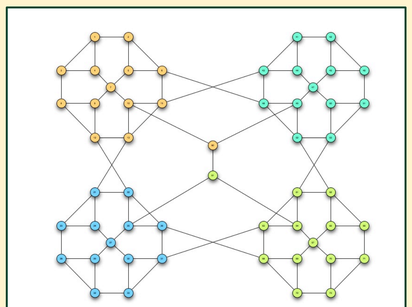

Fig. 4. Demo AS Infrastructure

OSRIS Oregon Systems Infrastructure Research & Information Security Laboratory

For further information, contact Braden Hollembaek (*bhollemb@cs.uoregon.edu*).