Secure Extension of BGP by Decoupling Path Propagation and Adoption

draft-zhang-idr-decoupling-01

Mingui Zhang
mingui@huawei.com

Bin Liu
Tsinghua University

Dacheng Zhang
Huawei

Beichuan Zhang
The University of Arizona
False Routing Announcements

- Interrupt the Internet service
- Source
  - Malicious attack
  - Mis-configuration
- Attacker can do
  - Black holing
  - Interception
Solutions

- **Prevention**
  - based on PKI, act before attacks

- **Detection**
  - monitoring & reaction, act after attacks

- **Mitigation**
  - filtering on my own, act during attacks
Traditional Mitigation

- The idea
  - A historical data base for trusted paths is set up on each AS router.
    - Not trusted ones will be identified as suspicious.
  - Block suspicious (most likely bogus) paths for certain time (e.g., 1 day).
    - Attacks will be clean up in this time.

- Benefits
  - Mitigate the impact of attacks
  - Prolong the time for operators to delete the bogus paths

- Disadvantage 1: Due to the inevitable false positive, some legitimate paths will be suspected and blocked hop by hop.
  - The total propagation delay can be very long, which is proportional to the length of AS_PATH.

- Disadvantage 2: Blocks the view of monitors in detection systems.
  - Can not detect and stop the real attack in time.
The optional transitive path attribute DAS_PATH

- Decoupling path propagation and path adoption in BGP (DBGP)
  - Don’t use the suspicious paths for data forwarding, but still inform neighbors about them through DAS_PATH which is the newly defined optional transitive path attribute contained in the same update message with AS_PATH.
  - DAS_PATH is used as an informational field. It will never be used for real data delivery.

- Legitimate paths can be validated in parallel during false positives.

- The monitors obtain the attack information through DAS_PATH, therefore the detection systems still work.
In BGP, the bogus path is used directly. The data will be redirected to the attacker AS X.

‘A’, ‘B’, ‘C’, ‘D’ and ‘X’ are used to denote the AS numbers while ‘p’ is the prefix.
Traditional Mitigation

Block the suspicious path for one day.

Adj-RIBs-In

7/10
DBGP-The New Mitigation Scheme

- (B X) is suspected and propagated using the DAS_PATH attribute. A DAS_PATH will only used as information rather than real data delivery!

- If (B X) is actually a legitimate path, the propagation in fact enable parallel validation.
  - A can start to validate it. When B propagate it to A as legitimate path one day later, A has already finished the validation in advance and can accept it directly.
Evaluation—How effective against attacks?

- DBGP is implemented in SSFNet-2.0.
  - Including “no-valley” and “customer-first” routing policy
  - An AS-level topology of 23718 nodes and 94468 links

- The figures also indicate that DBGP can be incrementally deployed across the network.
Conclusion

- DBGP protects data delivery in face of false routing announcements by decoupling path adoption and propagation.

- DBGP complements existing detection systems.

- DBGP reduces the delay of legitimate announcements.