Listen and Whisper

L. Subramanian, V. Roth, I. Stoica, S. Shenker, R. H. Katz

Presented by Ashish Vulimiri
Focus on invalid routes
- Invalid routes in the control plane
- Invalid routes in the data plane

Solution: both control and data plane verification
Requirement: Path Verification

Actual Guarantee:

*If an AS receives at least one valid path to AS A, receipt of an invalid path to A will trigger an alarm*
Discussion

Is this a good property to provide?
Suppose two paths received, A and B
Build loop out of these paths
Source-route along loop (in both directions)
When D receives path CBA from C
- Signature received: $S = h(B, h(A, h(z)))$
- D computes $h(C, S)$ before sending onwards

Authors suggest two schemes for computing and using these hashes
Secondary Requirement:

*If an AS sends out “too many” invalid paths, it will be identified*

Actual Mechanism:

Count how many times AS is in a problem-path
Listen: Data Plane

Requirement:
Check if data plane path matches control plane path

Actual Guarantee:
Check if data plane path reaches destination
Can you do anything better with end-to-end feedback?
Listen: Mechanism

- Mechanism: passive probing
  - Why?
- Raise alert if too many \((N)\) unsuccessful TCP connection attempts in time \(T\)
- \(T\) proportional to popularity of destination
  - Popularity measured by MTBA
Listen: Mechanism

- **False negatives**
  - Suggest values for $N$ based on experimental results

- **False positives**
  - Drop packets on m paths
  - Observe these m and an additional n
  - Expected: retransmissions on m, none on n
  - If not, raise alert
What they list as potential misbehaviour:

- End-hosts collude with adversary, generate fake valid TCP connections
- Port scanners: false positives

What else could happen?
Authors do not assume malicious attempts to game Listen/Whisper

Independent adversaries: if 1000 largest ASes deploy L/W, then in worst-case
- 8% of all nodes affected w/o penalties
- 1% with penalties
Colluding adversaries

Figure 8: The effects of colluding adversaries in the current Internet.
Summary

- Path verification in the control plane
- Reachability analysis in the data plane
- They remove existing vulnerabilities
- ... and then add their own
- Still, could be a net improvement
Questions?