Jumpstarting BGP Security

Sigcomm’16

Yossi Gilad
Joint work with: Avichai Cohen, Amir Herzberg, and Michael Schapira
BGP is insecure!

- Prefix/Subprefix Hijack

AS 1

My prefix is 1.2.0.0/16

AS 666

My prefix is 1.2.3.0/24

The Internet
BGP is insecure!

- Next-AS Attack

- AS 1
  - My prefix is 1.2.0.0/16

- The Internet
  - AS 1 is my neighbor
  - AS 666

- AS 1 is my neighbor
Current Paradigm: A Two Step Solution

- Origin Authentication (RPKI)
  - Periodic sync with trust-anchor, keeps BGP message format
  - Protects against prefix/subprefix hijacks
  - Slowly gaining traction (protects 6% of prefixes)

- Path Validation (BGPsec)
  - Real-time signature validation
  - Protects against false paths (e.g., next-AS attacks)
  - Builds on the RPKI
Problems with BGPsec

- Changes to BGP routers:
  - Online crypto requires new hardware
    [Goldberg’14, Comm ACM]
  - Different message format
    - legacy messages coexist with new format
- Meager benefits in partial deployment
  [Lychev et al., SIGCOMM’13]
  - Legacy routers force downgrade to (insecure) BGP
  - Attackers can advertise legacy BGP paths
- BGPsec is not “a small extension” of BGP
Our Goals

• Significant security benefits in partial deployment

• Avoid changes to routing infrastructure
Partial path signing (as described above) implies that the AS path is not rigorously protected. **Rigorous AS path protection is a key requirement of BGPSEC [RFC7353].** Partial path signing clearly reintroduces the following attack vulnerability: If a BGPSEC speaker can sign an unsigned update, and if signed (i.e., partially or fully signed) updates would be preferred to unsigned updates, then a faulty, misconfigured or subverted BGPSEC speaker can manufacture any unsigned update it wants (with insertion of a valid origin AS) and add a signature to it to increase the chance that its update will be preferred.
Path-end Validation

The Internet

AS 1
1.2.3.0/24

AS 10

AS 2
4.5.6.0/24

Router

AS 20

Router

RPKI Repository
Path-end Validation

PathEndRecord ::= SEQUENCE {
    timestamp Time,
    origin ASID,
    adjList SEQUENCE (SIZE(1..MAX)) OF ASID }

AS 1
1.2.3.0/24
Router

AS 10
Router

AS 2
Path-end Validation

The RPKI Repository

**Routing Policies**
- `ip as-path access-list as1 deny \[^{10|20}\]_1_`
- `ip as-path access-list allow-all permit`

AS 1
IP: 1.2.3.0/24

AS 10

AS 20

Router

Router
Router Configuration

- Compatible with today’s routers
- Only one rule per-AS
  - An order of magnitude less rules than origin authentication

The implementation can be found at:
https://github.com/yossigi/pathend
Intuition

• AS 666 wants to attract AS 3's traffic to IP prefix 1.2.3.0/24, but...
• It can't announce that it owns the prefix or is AS 1's neighbor
• It has to launch a 2-hop attack: (666,2,1,prefix)

AS 3 Attacker, AS 666 Victim, AS 1

MANY CLIENTS ARE ONE AS-HOP AWAY
FROM IMPORTANT CONTENT

Department of Computer Science, University of Washington

ABSTRACT

The Internet suffers from well-known performance, reliability, and security problems. However, proposed improvements have seen little adoption due to the difficulties of Internet-wide deployment. We observe that, instead of trying to solve these problems in the general case, it may be possible to make substantial progress by focusing on solutions tailored to the paths between popular content providers and their clients, which carry a large share of Internet traffic.

In this paper, we identify one property of these paths that may provide a foothold for deployable solutions: they are often very short. Our measurements show that Google connects directly to networks hosting more than 60% of end-user prefixes, and that other large content providers have similar connectivity. These direct paths open the possibility of solutions that sidestep the headache of Internet-of-networks. A second challenge is that the goal is to...
Path-end Validation vs. BGPsec

- Path-end validation is not just restricted BGPsec
  - Offline vs. online
  - Keep message format and use today's routers
- Important implication for security
  - AS 666 launches a next-AS attack against AS 1
    - Not prevented by BGPsec
    - Prevented by path-end validation
Simulation Framework

• Empirically-derived AS-level network from CAIDA
  • Including inferred peering links [Giotsas et al., SIGCOMM’13]

• Evaluate fraction of ASes an attacker can attract
  • For different adoption scenarios
  • For different types of attack

• Using the simulation framework in [Gill et al., CCR’12]
Simulation Results

![Graph showing simulation results for different deployment scenarios.](chart)

- **1. Next-AS**: Low attacker success rate.
- **2. BGPsec in partial deployment**: Moderate success rate.
- **3. 2-hop**: High success rate.
- **4. RPKI (full Deployment)**: Moderate success rate.
- **5. BGPsec (full deployment, legacy allowed)**: High success rate.
Additional Results

• Large content providers are typically connected via short paths and hence better protected
• Path-end validation mitigates high profile incidents
• Deployment by large ISPs within a geographic region protects local traffic
  • Governments may incentivize to protect local users
Conclusion

• Path-end validation
  • Is a modest extension to RPKI
  • Can significantly impact BGP security while avoiding BGPsec’s deployment hurdles

• We advocate
  • Incorporating path-end validation into the RPKI
  • Regulatory/financial efforts on gathering critical mass of adopters
Thank You!