Preventing Route Leaks using a Decentralized Approach: An experimental Evaluation

Miquel Ferriol Galmés (mferriol@ac.upc.edu)
Albert Cabellos-Aparicio (acabello@ac.upc.edu)
Roger Coll Aumatell (roger.coll.aumatell@est.fib.upc.edu)
Shoushou Ren (renshoushou@huawei.com)
Xinpeng Wei (weixinpeng@huawei.com)
Bingyang Liu (renshoushou@huawei.com)
Context
Border Gateway Protocol (BGP)

- Routing protocol that **glues** the Internet
- Provides **reachability** and **path selection**
Border Gateway Protocol (BGP)

- Routing protocol that **glues** the Internet
- Provides **reachability** and **path selection**

As the Internet and **business-oriented** Autonomous Systems (AS) began to provide connectivity, the different policies started to be:

- More **complex**
- More **rich**
- More **fine-grained**
Example
Example
Example
Example

- BGP is based on trust
- This protocol is vulnerable to a different number of security threads
- An important BGP security threat are Route Leaks
Route Leaks
Route Leaks

- Route leaks occur when one AS **violates** the routing policies agreed with another AS.
- This policies are based according to the **business relationship** between them.
- This violations can lead to:
  - Traffic redirection, traffic loss, traffic hijacking, prefix blackholding...
Route Leaks

AS link

Original route of the traffic

BGP Update

Traffic after route leak
Route Leaks

- Route leaks are a **simple** problem but **hard** to fix:
  - BGP protocol lacks of cryptographic-based security mechanisms
  - Inter-domain routing lacks a standard mechanism to communicate routing policy
BGP Communities

- **Transitive attribute** attached to BGP messages
- Used for **tagging** routes and for **modifying** BGP routing decisions
- Can be **added**, **removed**, or **modified** as the message travels from AS to AS
- Represent an important **attack vector**
Proposed Solution
Architecture

- Take advantage of BGP communities to address the challenges of route leaks
- Propose an architecture that provides a formal definition of routing policy
- Secure mechanism to communicate it to participating ASes (Block-chain based)
Formal language

Contains 5 parameters:

- **ASN**: AS number
- **CN**: Community number
- **Rule**: The policy to be applied (e.g., LOCALPREFERENCE, PREPEND...)
- **Value** (optional): It normally defines the quantity of a given effect.
- **To**: what the rule refers to.
Distributed ledger

- Set of requirements:
  - Authentication
  - Permissioned
  - Privacy and confidentiality
How the policies are uploaded to the Distributed Ledger?

- **Execute** a transaction and verify its correctness
- **Order** transactions via a **consensus protocol**
- **Validate** a transaction against a specific **endorsement policy** before committing them to the ledger
Architecture

1. Policy upload

LEDGER

CN: 123 RULE: NO_EXPORT
TO: USA
Architecture

1. Policy upload

2. The compiler generates the BGP route filter
Architecture

**LEDGER**

1. Policy upload

CN: 123  RULE: NO_EXPORT
TO: USA

2. The compiler generates the BGP route filter

AS1 ——— AS2 ——— AS3

3. The installed route filters stop the propagation of the BGP update that would cause the route leak.

p1: AS1, ...

AS1:123
Experimental Evaluation
Prototyping the Distributed Ledger
How scalable is the ledger?

<table>
<thead>
<tr>
<th>Variable 1</th>
<th>Variable 2</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain size</td>
<td>Number of communities</td>
<td>Linear</td>
</tr>
<tr>
<td>Time to add a new community</td>
<td>Number of endorsers</td>
<td>Linear</td>
</tr>
<tr>
<td>Compiling time</td>
<td>Number of communities</td>
<td>Linear</td>
</tr>
</tbody>
</table>
Preventing Route Leaks in a Realistic Topology
Dataset

- 27 Ases
- 458 BGP Communities
- Transformed to the formal language
Real Topology
Experimental Results
Conclusions

- Open-source\textsuperscript{[1]} prototype of a blockchain-based solution to prevent route leaks
- Scales linearly with respect to relevant metrics and that introduces negligible delay
- Prototype in a real-world scenario by preventing a route-leak in a 10 ASes topology

\textsuperscript{[1]} https://github.com/MiquelFerriol/SecuringBGP
Thank you for watching