A Software-Defined Networking approach to enhance BGP security

Regivaldo Costa
Prof. Fernando Ramos (Advisor)

LaSIGE, Faculdade de Ciências
Universidade de Lisboa, Portugal

NavTalk, June/2017
Outline

1. Objective
2. Motivation
3. Background
4. BGP Security problems
5. Related work
6. Proposal
7. Evaluation
8. Conclusion
Objective

Motivation

Background

BGP Security problems

Related work

Proposal

Evaluation

Conclusion
Objective & Goals

Objective of this work: design, implementation and evaluation of an SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security.

Our goals:
- Provide Origin Authentication and Path Validation to avoid prefix hijacks and other fake BGP announcements.
- Promote deployment.
A SDN approach to enhance BGP security

1. Objective
2. Motivation
3. Background
4. BGP Security problems
5. Related work
6. Proposal
7. Evaluation
8. Conclusion
Motivation (BGP Security)

Some solutions to improve BGP security having been proposed in the past two decades [ProcIEEE’10], but the most effective security solutions have not seen widespread deployment [SIGCOMM’14]:

- Proposed solutions require changes to BGP.
- Proposed solutions represent a high computational burden to routers.
- Network operators are not given the right incentives to migrate to a secure solution, and have concerns about the disclosure of business relationships considered private.
3 Background

4 BGP Security problems

5 Related work

6 Proposal

7 Evaluation

8 Conclusion
Background - Internet infrastructure/routing
Background (Internet infrastructure/routing)

Internet interconnection

A SDN approach to enhance BGP security
Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

<table>
<thead>
<tr>
<th>Continental Region</th>
<th># IXPs</th>
<th>Continental Region</th>
<th># IXPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>186</td>
<td>Africa</td>
<td>38</td>
</tr>
<tr>
<td>North America</td>
<td>131</td>
<td>Australia/New Zealand</td>
<td>27</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>92</td>
<td>Middle East</td>
<td>9</td>
</tr>
<tr>
<td>Central/South America</td>
<td>62</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some IXPs are very large:
- DE-CIX has more than 600 connected networks.
- AMS-IX has more than 700 connected networks.
- CIX and AMS each have a network traffic around 5 terabits/s.
Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

<table>
<thead>
<tr>
<th>Continental Region</th>
<th># IXPs</th>
<th>Continental Region</th>
<th># IXPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>186</td>
<td>Africa</td>
<td>38</td>
</tr>
<tr>
<td>North Americ</td>
<td>131</td>
<td>Australia/New Zealand</td>
<td>27</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>92</td>
<td>Middle East</td>
<td>9</td>
</tr>
<tr>
<td>Central/South America</td>
<td>62</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some IXPs are very large

DE-CIX has more than 600 connected networks.
AMS-IX has more than 700 connected networks.
CIX and AMS have each one a network traffic around 5 terabits/s.
Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

<table>
<thead>
<tr>
<th>Continental Region</th>
<th># IXPs</th>
<th>Continental Region</th>
<th># IXPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>186</td>
<td>Africa</td>
<td>38</td>
</tr>
<tr>
<td>North Americ</td>
<td>131</td>
<td>Australia/New Zealand</td>
<td>27</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>92</td>
<td>Middle East</td>
<td>9</td>
</tr>
<tr>
<td>Central/South America</td>
<td>62</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some IXPs are very large

- DE-CIX has more than 600 connected networks.
- AMS-IX has more than 700 connected networks.
- CIX and AMS has each one a network traffic around 5 terabits/s.
Background (Internet infrastructure/routing))

IXPs visual distribution around the world (source: telegeography.com)
Route propagation along the path (UPDATE message)
Route propagation along the path (*UPDATE* message)
Route propagation along the path (UPDATE message)
Background (BGP route announcement)

Route propagation along the path (UPDATE message)
Background - Software-Defined Networking
Background (SDN overview)

Traditional and SDN network architecture

Traditional

SDN
Background (SDX = SDN + IXP)

Software-Defined Exchange [SIGCOMM’14][NSDI’16]
4. **BGP Security problems**
BGP Security Problems - Prefix Hijacking
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security problems

Prefix/Sub Prefix Hijacking

A SDN approach to enhance BGP security
BGP Security Problems - Path manipulation
BGP Security problems

Path manipulation (path-shortening)
BGP Security problems

Path manipulation (path-shortening)

A SDN approach to enhance BGP security
Related work

A SDN approach to enhance BGP security
A SDN approach to enhance BGP security
Related work: Origin Authentication (RPKI) [RFC6480]

A trusted DB is used to guarantee that an **AS cannot falsely claim** to be the rightful owner for an IP prefix (Route Origin Authorization - **ROA**) [RFC6482].

The RPKI provides a trusted mapping - a **whitelist** - from allocated prefixes to ASes by establishing a cryptographic hierarchy of authorities.
Related work: Origin Authentication (RPKI) [RFC6480]

- Pros & Cons:
  - Offline cryptography.
  - Low computational burden to routers.
  - No changes to BGP.
  - Protects from BGP hijacks.
  - Does not avoid path manipulation.
  - RPKI coverage is small.
Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons:**
  - (+) Offline cryptography.
Pros & Cons:

(+): Offline cryptography.
(+): Low computational burden to routers.

(-): Does not avoid path manipulation.
(-): RPKI coverage is small.
Related work: Origin Authentication (RPKI) [RFC6480]

**Pros & Cons:**

- (+) Offline cryptography.
- (+) Low computational burden to routers.
- (+) No changes to BGP.
Pros & Cons:

- Offline cryptography.
- Low computational burden to routers.
- No changes to BGP.
- Protects from BGP hijacks.

Does not avoid path manipulation.
RPKI coverage is small.
Related work: Origin Authentication (RPKI) [RFC6480]

**Pros & Cons:**

- (+) Offline cryptography.
- (+) Low computational burden to routers.
- (+) No changes to BGP.
- (+) Protects from BGP hijacks.
- (-) Does not avoid path manipulation.

RPKI coverage is small.
Pros & Cons:

- Offline cryptography.
- Low computational burden to routers.
- No changes to BGP.
- Protects from BGP hijacks.

- Does not avoid path manipulation.
- RPKI coverage is small.
In addition to origin authentication, it uses cryptographically-signed routing announcements to provide path verification.

It comprises a set of nested signature which need to be verified.
Pros & Cons:

- Protects from BGP hijacks.
- Protects from path manipulation.
- High computational burden to routers.
- Requires changes to BGP.
- Benefits only with large deployment.
Pros & Cons:

(+) Protects from BGP hijacks.
Pros & Cons:

- (+) Protects from BGP hijacks.
- (+) Protects from path manipulation.
Related work: BGP security extension (BGPSEC) [RFC-Draft]

**Pros & Cons:**

- (+) Protects from BGP hijacks.
- (+) Protects from path manipulation.
- (-) High computational burden to routers.
Pros & Cons:

- (+) Protects from BGP hijacks.
- (+) Protects from path manipulation.
- (-) High computational burden to routers.
- (-) Requires changes to BGP.

Related work: BGP security extension (BGPSEC) [RFC-Draft]
Pros & Cons:

(+) Protects from BGP hijacks.
(+ ) Protects from path manipulation.

(-) High computational burden to routers.
(-) Requires changes to BGP.
(-) Benefits only with large deployment.
A SDN approach to enhance BGP security
Proposal - Design requirements
We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don’t require changes to BGP.
We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don’t require changes to BGP.
- Remove computational burden from routers.
We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don’t require changes to BGP.
- Remove computational burden from routers.
- Creates incentives to ASes and removes disincentives.
Peer which receives the advertisement makes queries on each AS of the path to validate the announcement.

In the queries, for a legitimate advertisement is returned VALID, otherwise INVALID.

Queries uses RESTful over HTTPS.

Queries in blockchain uses JSON-RPC (based in key/value).
Each peer have its blockchain and are synchronized with each other. No proof-of-work is required to include transactions. To avoid malicious peer is used a permission policy.

To validate OA/PV, the AS makes queries in its own blockchain.

To avoid synchronization problems, queries may be performed on the remote peer using JSON-RPC (HTTPS or SSL/TCP-Socket).
BGPSECx design (Inter-IXP queries)

A SDN approach to enhance BGP security
BGPSECx design - OA/PV validation

Secure BGP for Internet Exchange Points - **BGPSECx**

A SDN approach to enhance BGP security
A SDN approach to enhance BGP security
We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.
We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.
- HTTPS/RESTful to provide IXP collaboration.
We have implemented BGPSEClx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.
- HTTPS/RESTful to provide IXP collaboration.
- Multichain approach to support blockchain.
A SDN approach to enhance BGP security
Empirical analysis: methodology

- Data-driven simulations using empirical data: public BGP routing information and IXP datasets.
  
  (a) Validating origin using RPKI
  
  (b) Validating origin using BGPSECx
  
  (c) Validating the full path using BGPSECx

  For BGPSECx we assume that:
  
  Only the 10% largest IXPs use BGPSECx (it represents IXPs with more than 50 ASes, totaling 4147).
  
  Only a random set of $X\%$ of peers connected to each IXP uses BGPSECx: $X = [1, 10, 25, 50, 75, 100]$.

  Running each experiment 10 times.
Empirical analysis: methodology

- Data-driven simulations using empirical data: public BGP routing information and IXP datasets.
- We simulate the process of validating each BGP update:
  - (a) Validating origin using RPKI
  - (b) Validating origin using BGPSECx
  - (c) Validating the full path using BGPSECx
Empirical analysis: methodology

- Data-driven simulations using empirical data: public BGP routing information and IXP datasets.

- We simulate the process of validating each BGP update:
  - (a) Validating origin using RPKI
  - (b) Validating origin using BGPSECx
  - (c) Validating the full path using BGPSECx

- For BGPSECx we assume that:
  - Only the 10% largest IXPs use BGPSECx (it represents IXPs with more than 50 ASes, totalizing 4147).
  - Only a random set of $X\%$ of peers connected to each IXP uses BGPSECx: $X = [1, 10, 25, 50, 75, 100]$.

- Running each experiment 10 times.
### Routing collector points and data volume (1/2)

<table>
<thead>
<tr>
<th>IXP/Locality</th>
<th># Updates</th>
<th># Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE (Amsterdam/NL)*</td>
<td>1176888</td>
<td>5886175</td>
</tr>
<tr>
<td>LINX (London/UK)</td>
<td>642095</td>
<td>3219512</td>
</tr>
<tr>
<td>AMS-IX (Amsterdam/NL)</td>
<td>802181</td>
<td>4021230</td>
</tr>
<tr>
<td>CIXP/CERN (Geneva/CH)</td>
<td>610684</td>
<td>2711758</td>
</tr>
<tr>
<td>VIX (Vienna/AT)</td>
<td>463082</td>
<td>2133931</td>
</tr>
<tr>
<td>JPIX (Otemachi/JP)*</td>
<td>141904</td>
<td>590750</td>
</tr>
<tr>
<td>NETNOD (Stockholm/SE)</td>
<td>918238</td>
<td>3350961</td>
</tr>
<tr>
<td>MIX (Milan/IT)</td>
<td>762713</td>
<td>3288810</td>
</tr>
<tr>
<td>NYIIX (New Yourk/US)*</td>
<td>897104</td>
<td>4344049</td>
</tr>
</tbody>
</table>
### Routing collector points and data volume (2/2)

<table>
<thead>
<tr>
<th>IXP/Locality</th>
<th># Updates</th>
<th># Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-CIX (Frankfurt/DE)</td>
<td>1524949</td>
<td>7004462</td>
</tr>
<tr>
<td>MSK/IX (Moscow/RU)*</td>
<td>1314165</td>
<td>4778407</td>
</tr>
<tr>
<td>PAIX (Palo Alto/US)</td>
<td>663323</td>
<td>3371273</td>
</tr>
<tr>
<td>PTTMetro (São Paulo/BR)*</td>
<td>1896335</td>
<td>12324785</td>
</tr>
<tr>
<td>NOTA (Miami/US)</td>
<td>259672</td>
<td>977813</td>
</tr>
<tr>
<td>CATNIX (Barcelona/ES)</td>
<td>84222</td>
<td>278400</td>
</tr>
<tr>
<td>NAP/JB (Johannesburg/ZA)*</td>
<td>437222</td>
<td>1820852</td>
</tr>
<tr>
<td>SwissIX (Zurich/CH)</td>
<td>2015867</td>
<td>7900807</td>
</tr>
<tr>
<td>FranceIX (Paris/FR)</td>
<td>1607568</td>
<td>7520597</td>
</tr>
</tbody>
</table>
Empirical analysis: simulation results

Verification results of OA/RPKI from NL, ZA, RU, JP and BR

<table>
<thead>
<tr>
<th>City</th>
<th>Percentage of verification (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amsterdam/NL</td>
<td>94.71</td>
</tr>
<tr>
<td>Joburg/ZA</td>
<td>96.83</td>
</tr>
<tr>
<td>Moscow/RU</td>
<td>96.24</td>
</tr>
<tr>
<td>New York/US</td>
<td>97.12</td>
</tr>
<tr>
<td>Otemachi/JP</td>
<td>96.01</td>
</tr>
<tr>
<td>São Paulo/BR</td>
<td>96.88</td>
</tr>
</tbody>
</table>

Verified:  
Not verified:
Empirical analysis: simulation results

Verification results of **OA/RPKI** from NL, ZA, RU, JP and BR

Conclusion: The RPKI is useful for less than 4% of all updates
Empirical analysis: simulation results

Verification results of **OA/BGPSECx** from NL, ZA, RU, JP and BR

![OA using BGPSecX](image)
Empirical analysis: simulation results

Verification results of **OA/BGPSECx** from NL, ZA, RU, JP and BR

1. **Even assuming that only 10% of ASes (~400 ASes) adhere to the BGPSECx service, BGPSECx is always better when compared to the RPKI.**

2. **If we assume all ASes connected to the selected IXPs adhere to the BGPSECx service (~4000 ASes), BGPSECx is always more than 10x better than the RPKI. Importantly, the RPKI has prefixes from a similar number of ASes (~4000 ASes), demonstrating that BGPSECx is more effective.**
Empirical analysis: simulation results

Verification results of **PV/BGPSECx** from NL, ZA, RU, JP and BR
Empirical analysis: simulation results

Verification results of **PV/BGPSECx** from NL, ZA, RU, JP and BR

In most scenarios **BGPSECx** is able to verify a higher % of full paths than RPKI is able to perform much "simpler" origin authentication.
1. Objective

2. Motivation

3. Background

4. BGP Security problems

5. Related work

6. Proposal

7. Evaluation

8. Conclusion
BGP is insecure.

Solutions for this problem remain largely undeployed for fundamental reasons:

1. They require changes to BGP.
2. They are computationally expensive for routers, and/or;
3. They do not give operators incentives for deployment.
4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:

  1. They require changes to BGP.
  2. They are computationally expensive for routers, and/or;
  3. They do not give operators incentives for deployment.
  4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Conclusion

- BGP is insecure.
- Solutions for this problem remain largely undeployed for 4 fundamental reasons:
  1. They require changes to BGP.
  2. They are computationally expensive for routers, and/or;
  3. They do not give operators incentives for deployment.
  4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:
- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  1. They require **changes to BGP**.
  2. They are **computationally expensive** for routers, and/or;
  3. They do not give operators incentives for deployment.
  4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
BGP is insecure.

Solutions for this problem remain largely undeployed for 4 fundamental reasons:

1. They require changes to BGP.
2. They are computationally expensive for routers, and/or;
3. They do not give operators incentives for deployment.
4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  1. They require changes to BGP.
  2. They are **computationally expensive** for routers, and/or;
  3. They do not give operators **incentives** for deployment.
  4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  1. They require **changes to BGP**.
  2. They are **computationally expensive** for routers, and/or;
  3. They do not give operators **incentives** for deployment.
  4. They create disincentives by disclosing business relationships.

- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:
Conclusion

- BGP is insecure.

- Solutions for this problem remain \textit{largely undeployed} for 4 fundamental reasons:
  1. They require \textit{changes to BGP}.
  2. They are \textit{computationally expensive} for routers, and/or;
  3. They do not give operators \textit{incentives} for deployment.
  4. They create disincentives by disclosing business relationships.

- Our proposal, BGPSECx, offers \textit{equivalent security} to the most complete secure BGP solution while:
  - Solving problems (1) and (2) by using an SDN-based approach.
Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.

- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:
  - Solving problems (1) and (2) by using an SDN-based approach.
  - Solving problem (3) by targeting (clusters of collaborating) IXPs.
Conclusion

BGP is insecure.

Solutions for this problem remain largely undeployed for 4 fundamental reasons:

1. They require changes to BGP.
2. They are computationally expensive for routers, and/or;
3. They do not give operators incentives for deployment.
4. They create disincentives by disclosing business relationships.

Our proposal, BGPSECx, offers equivalent security to the most complete secure BGP solution while:

- Solving problems (1) and (2) by using an SDN-based approach.
- Solving problem (3) by targeting (clusters of collaborating) IXPs.
- Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).
Thank you!