Routing in the Future Internet

Marcelo Yannuzzi

Graduate Course (Slideset 8)
Institute of Computer Science
University of the Republic (UdelaR)

August 31st 2012, Montevideo, Uruguay

Department of Computer Architecture
Technical University of Catalonia (UPC), Spain

Institute of Computer Science
University of the Republic (UdelaR), Uruguay

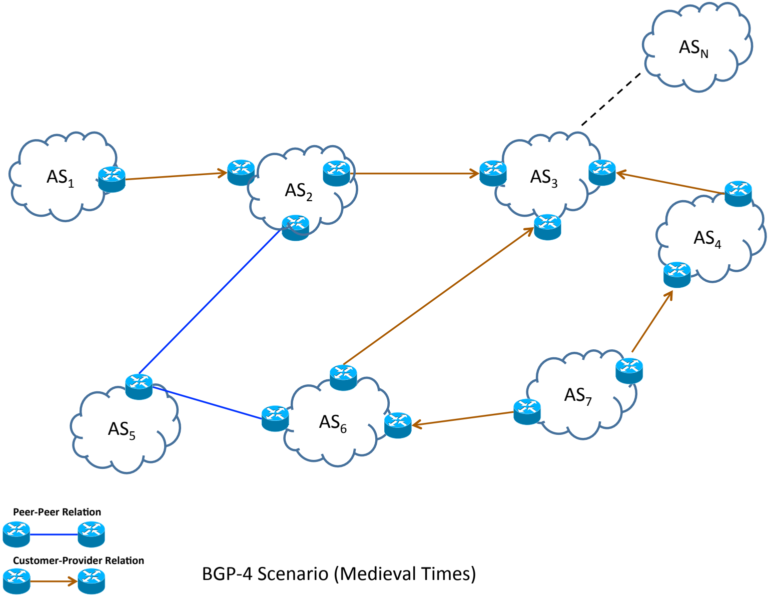
Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Outline

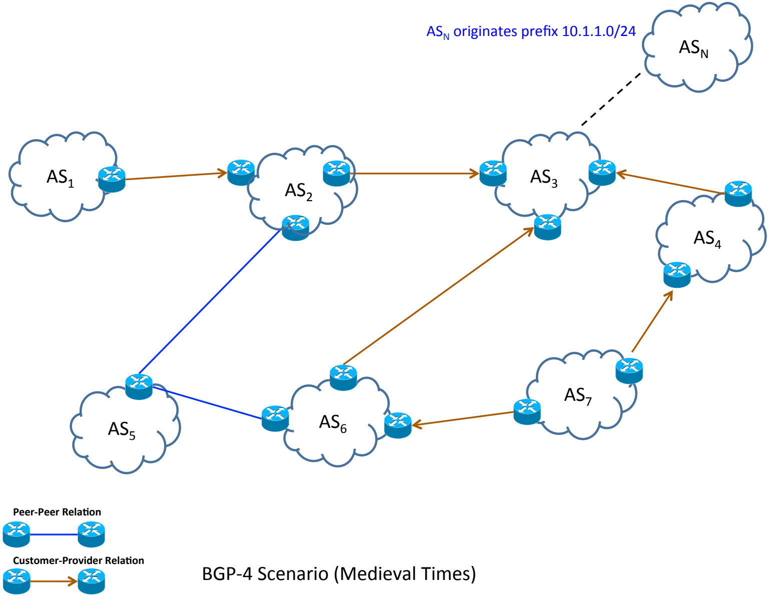
1. **Prefix Hijacking: RPKI and ROA**
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Prefix Hijacking



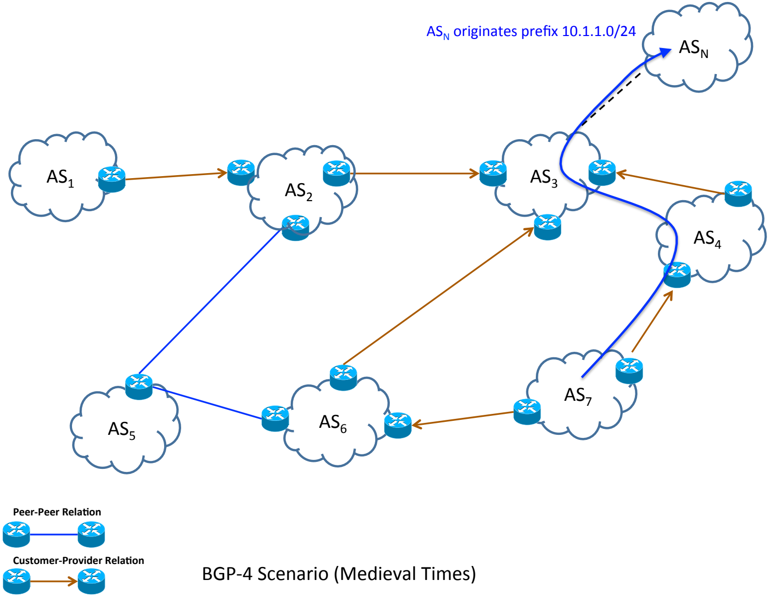
BGP-4 Scenario (Medieval Times)

Prefix Hijacking



BGP-4 Scenario (Medieval Times)

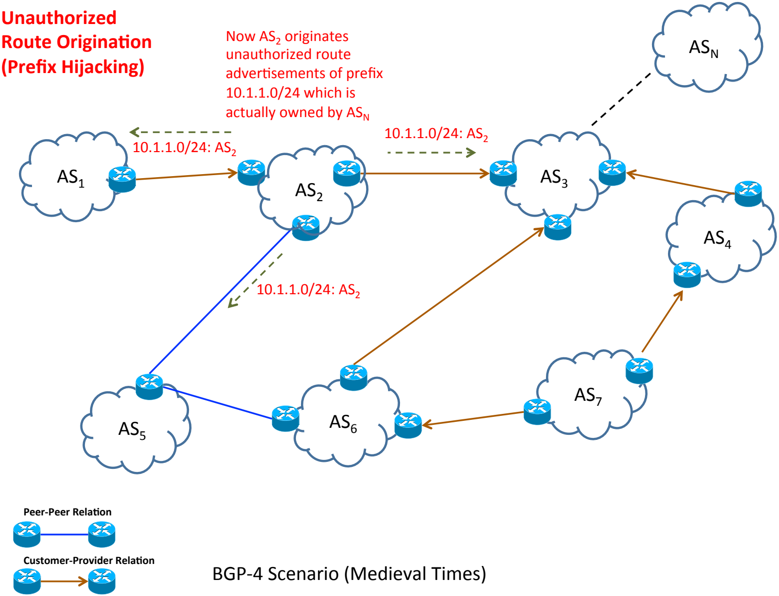
Prefix Hijacking



BGP-4 Scenario (Medieval Times)

Prefix Hijacking

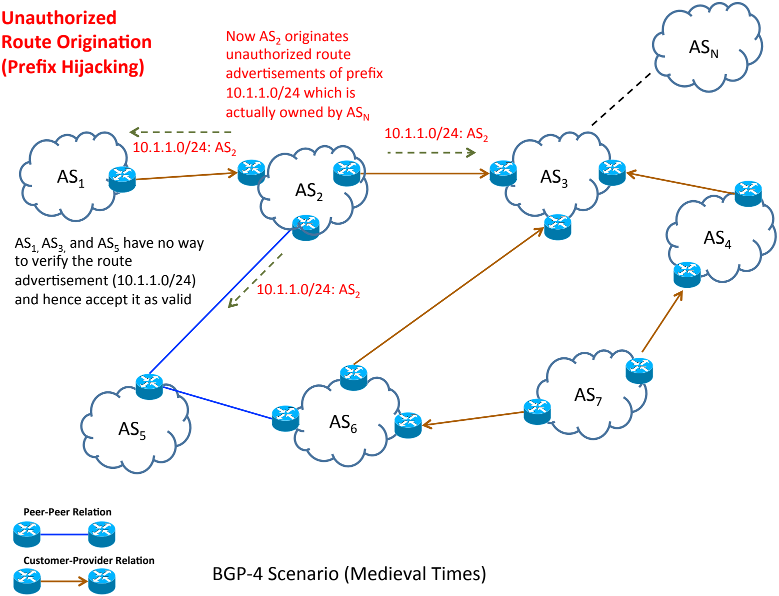
Unauthorized Route Origination (Prefix Hijacking)


Now AS_2 originates unauthorized route advertisements of prefix 10.1.1.0/24 which is actually owned by AS_N
AS_N
10.1.1.0/24: AS_2
10.1.1.0/24: AS_2
AS_1
AS_2
AS_3
AS_4
10.1.1.0/24: AS_2
AS_5
AS_6
AS_7
Peer-Peer Relation
Customer-Provider Relation

BGP-4 Scenario (Medieval Times)

Prefix Hijacking

Unauthorized Route Origination (Prefix Hijacking)



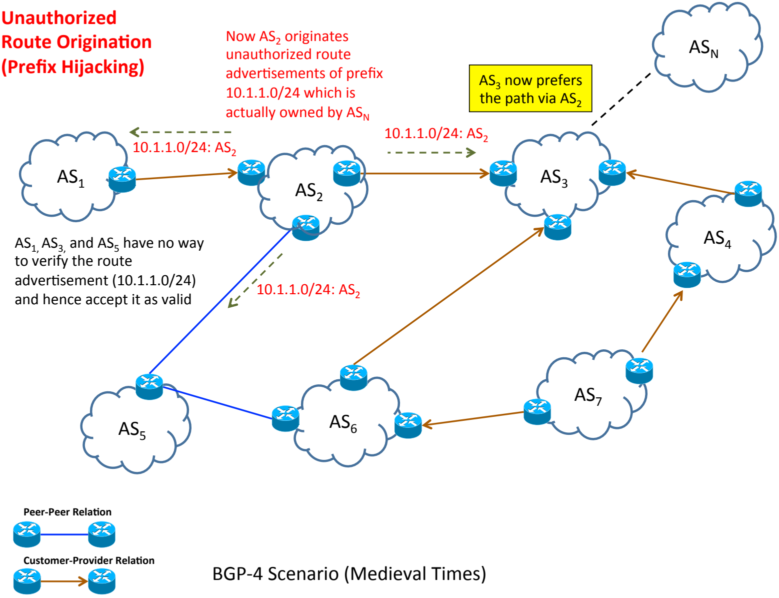
Now AS_2 originates unauthorized route advertisements of prefix 10.1.1.0/24 which is actually owned by AS_N
AS_N
AS_1
10.1.1.0/24: AS_2
AS_2
10.1.1.0/24: AS_2
AS_3
AS_4
10.1.1.0/24: AS_2
AS_5
AS_6
AS_7
Peer-Peer Relation
Customer-Provider Relation

AS_1, AS_3, and AS_5 have no way to verify the route advertisement (10.1.1.0/24) and hence accept it as valid

BGP-4 Scenario (Medieval Times)

Prefix Hijacking

Unauthorized Route Origination (Prefix Hijacking)



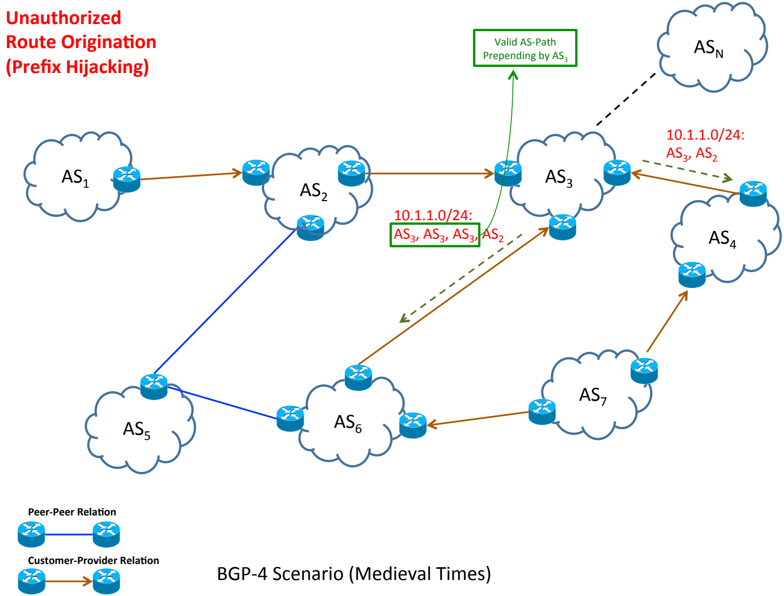
Now AS_2 originates unauthorized route advertisements of prefix 10.1.1.0/24 which is actually owned by AS_N

AS_3 now prefers the path via AS_2

AS_1, AS_3, and AS_5 have no way to verify the route advertisement (10.1.1.0/24) and hence accept it as valid

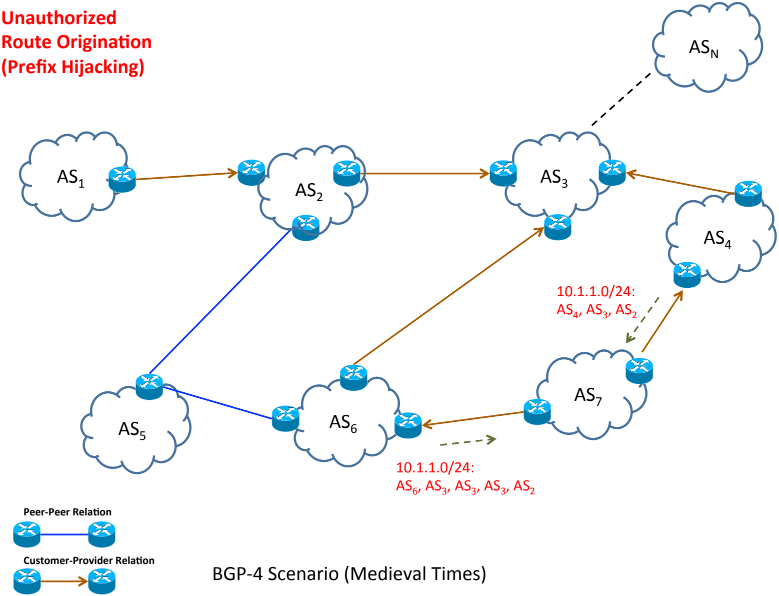
BGP-4 Scenario (Medieval Times)

Prefix Hijacking



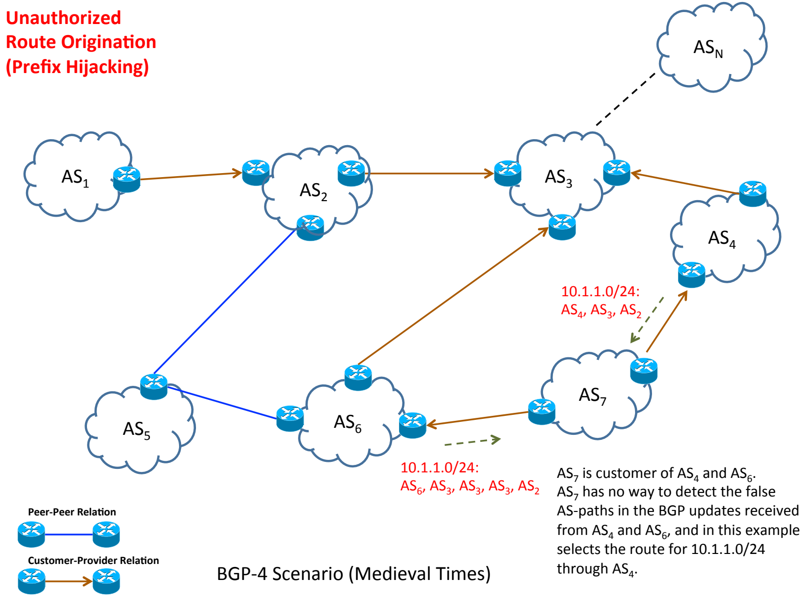
BGP-4 Scenario (Medieval Times)

Prefix Hijacking



BGP-4 Scenario (Medieval Times)

Prefix Hijacking

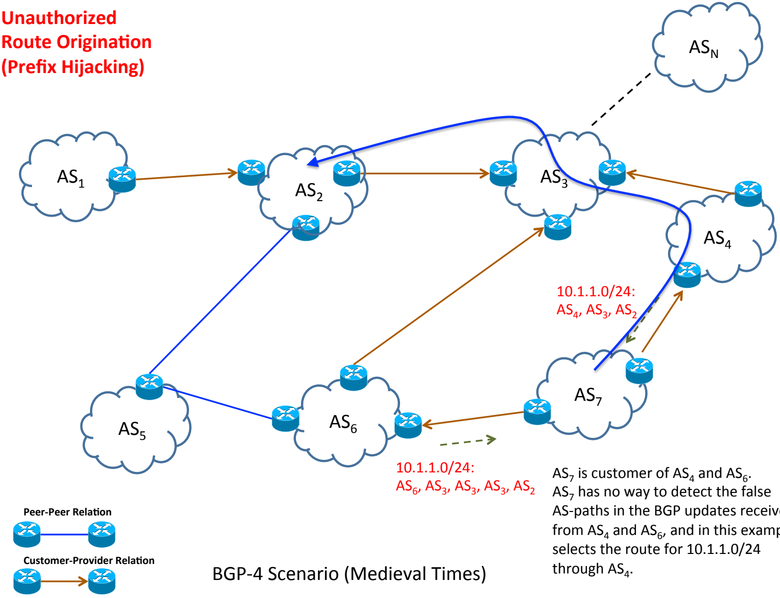

Unauthorized Route Origination (Prefix Hijacking)
AS_N
AS_1
AS_2
AS_3
AS_4
AS_5
AS_6
AS_7
10.1.1.0/24: AS_4, AS_3, AS_2
10.1.1.0/24: AS_6, AS_3, AS_3, AS_3, AS_2
Peer-Peer Relation
Customer-Provider Relation

AS_7 is customer of AS_4 and AS_6. AS_7 has no way to detect the false AS-paths in the BGP updates received from AS_4 and AS_6, and in this example selects the route for 10.1.1.0/24 through AS_4.

BGP-4 Scenario (Medieval Times)

Prefix Hijacking

Unauthorized Route Origination (Prefix Hijacking)

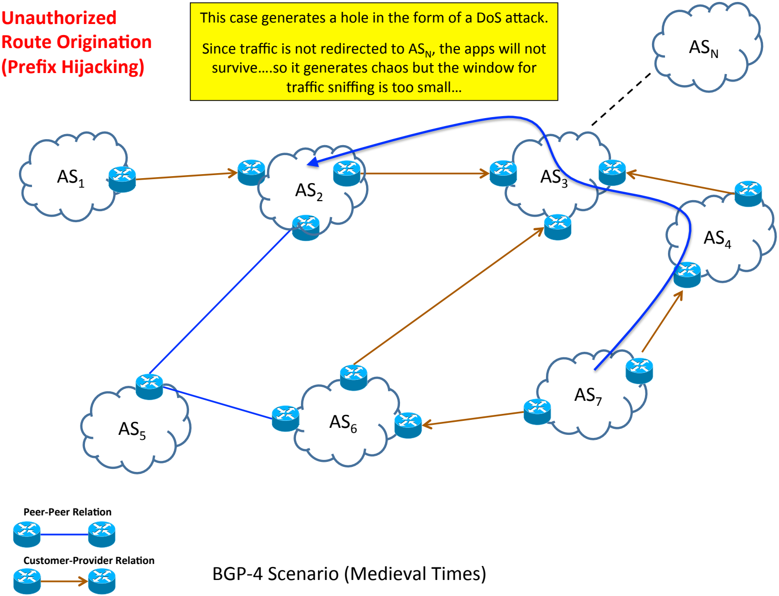


AS_7 is customer of AS_4 and AS_6. AS_7 has no way to detect the false AS-paths in the BGP updates received from AS_4 and AS_6, and in this example selects the route for 10.1.1.0/24 through AS_4.

BGP-4 Scenario (Medieval Times)

Prefix Hijacking

Unauthorized Route Origination (Prefix Hijacking)



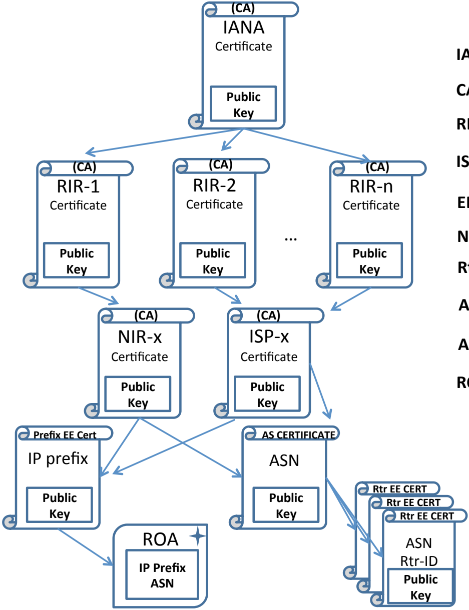
This case generates a hole in the form of a DoS attack.

Since traffic is not redirected to AS$_N$, the apps will not survive….so it generates chaos but the window for traffic sniffing is too small…

BGP-4 Scenario (Medieval Times)

Preventing Prefix Hijacking: RPKI and ROA

Preventing Prefix Hijacking: RPKI and ROA



IANA = Internet Assigned Numbers Authority

CA = Certification Authority

RIR = Regional Internet Registry

ISP = Internet Service Provider

EE Cert = End-Entity Certificate

NIR = National Internet Registry

Rtr = Router

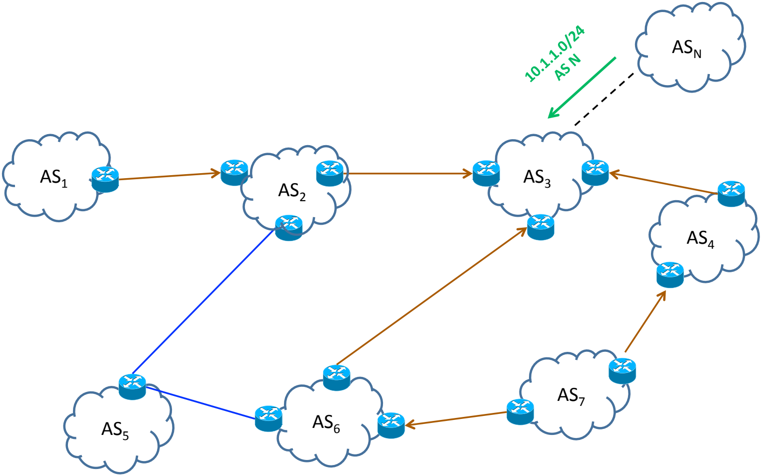
AS = Autonomous System

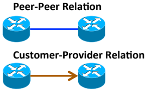
ASN = Autonomous System Number

ROA = Route Origin Authorization (RFC 6482)

Administrative Resource Allocation Hierarchy

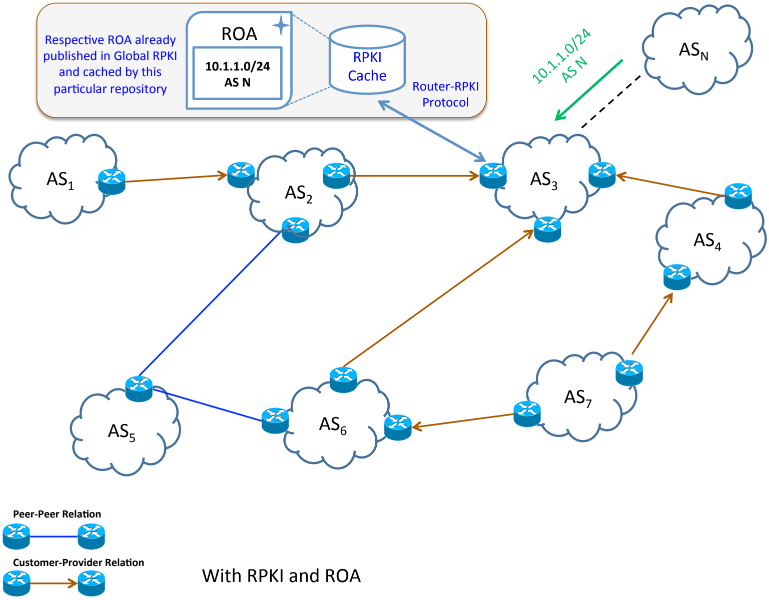
Preventing Prefix Hijacking: RPKI and ROA





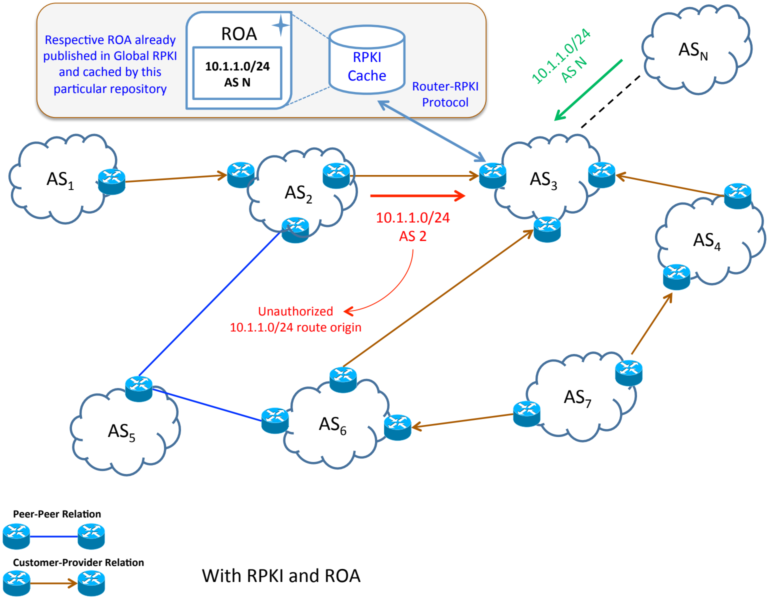
With RPKI and ROA

Preventing Prefix Hijacking: RPKI and ROA



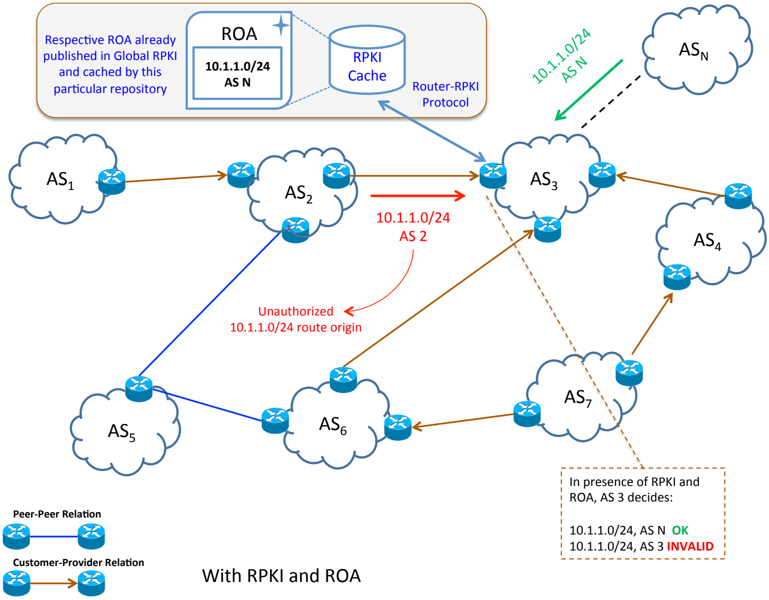
With RPKI and ROA

Preventing Prefix Hijacking: RPKI and ROA



With RPKI and ROA

Preventing Prefix Hijacking: RPKI and ROA



Respective ROA already published in Global RPKI and cached by this particular repository

In presence of RPKI and ROA, AS 3 decides:

10.1.1.0/24, AS N **OK**
10.1.1.0/24, AS 3 **INVALID**

Unauthorized 10.1.1.0/24 route origin

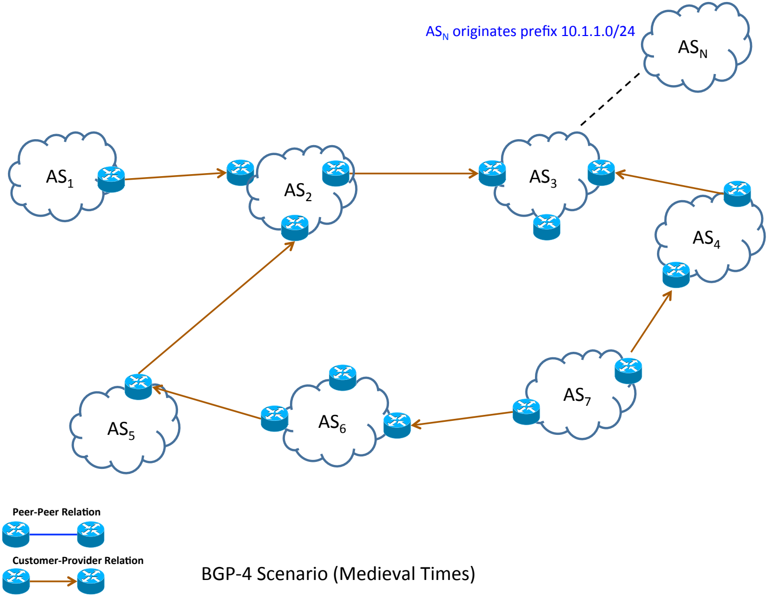
With RPKI and ROA

Outline

1. Prefix Hijacking: RPKI and ROA
2. **Route Hijacking: BGPSEC**
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

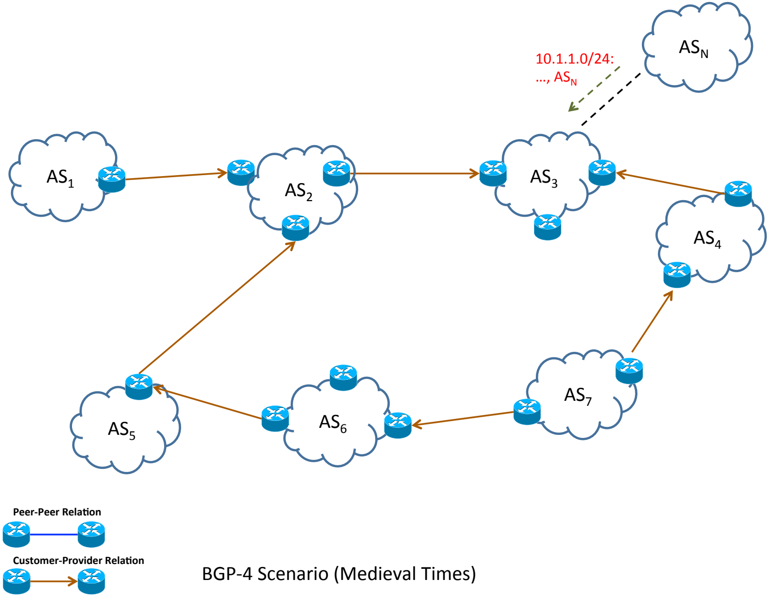
Fake (invalid) BGP paths

Route Hijacking: case 1



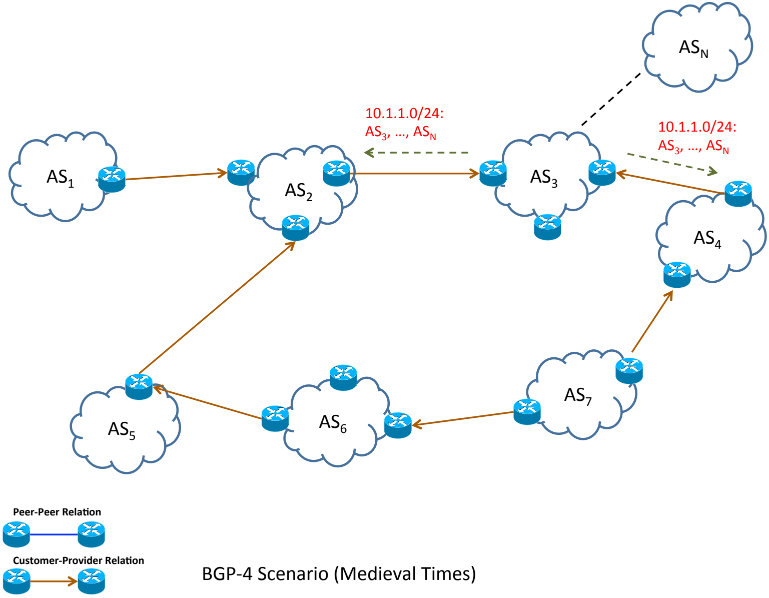
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



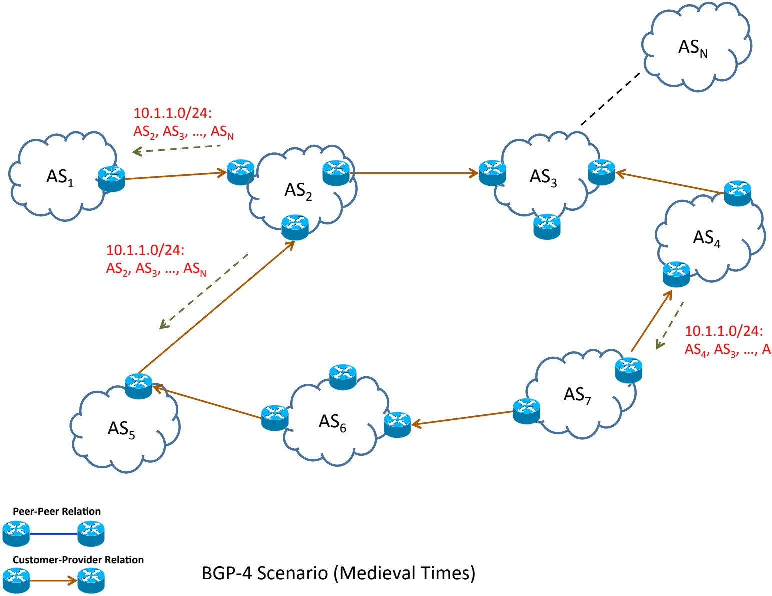
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



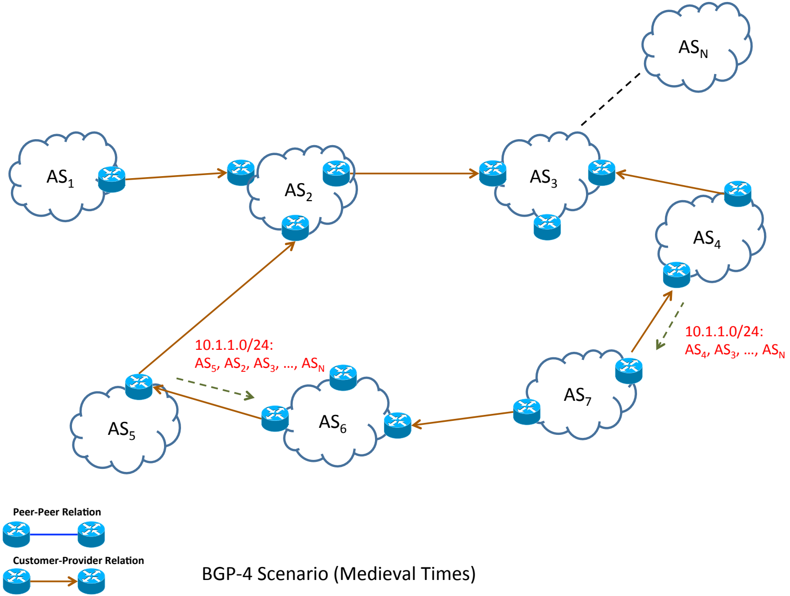
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



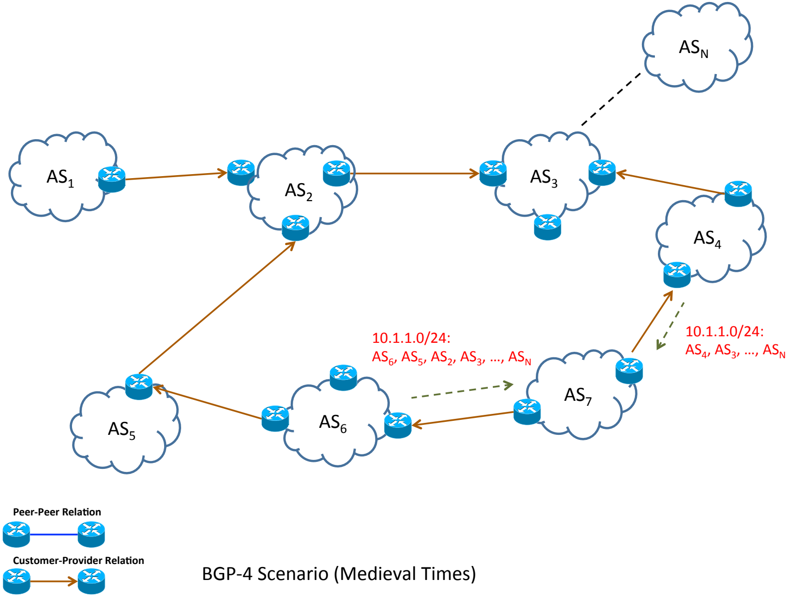
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



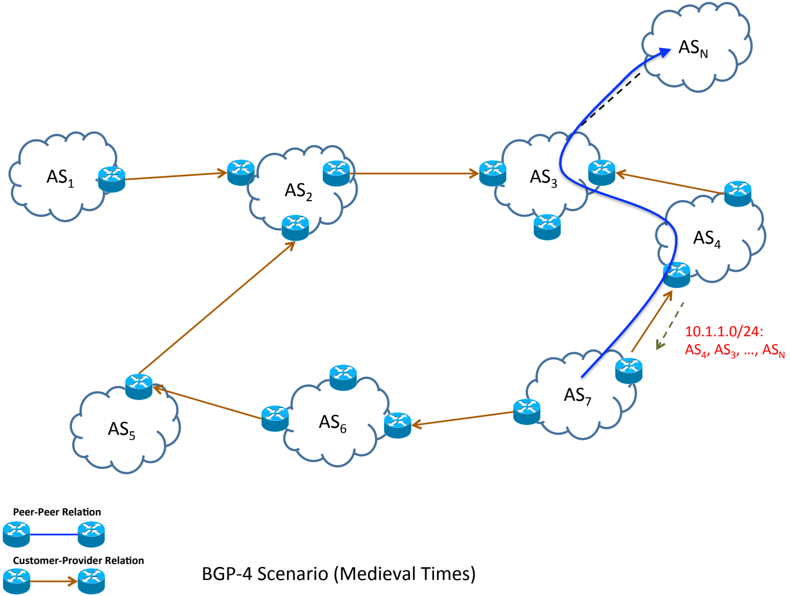
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1


AS_N
AS_1
AS_2
AS_3
AS_4
10.1.1.0/24:
AS_6, AS_5, AS_2, AS_3, ..., AS_N
10.1.1.0/24:
AS_4, AS_3, ..., AS_N
AS_7
AS_6
AS_5
Peer-Peer Relation
Customer-Provider Relation

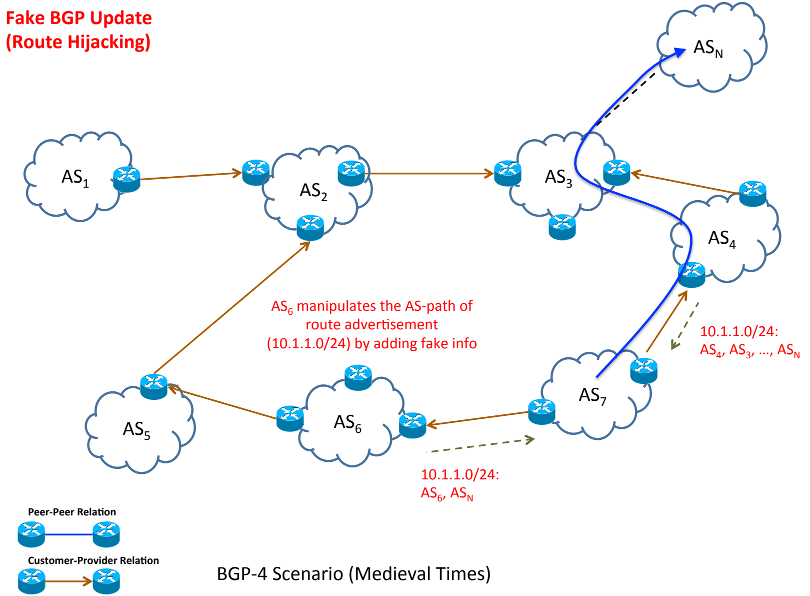
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



BGP-4 Scenario (Medieval Times)

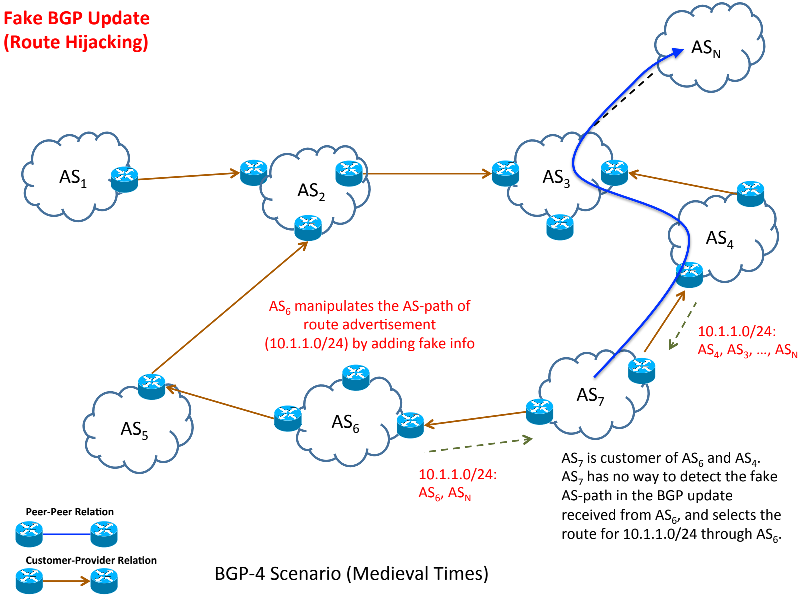
Route Hijacking: case 1



Fake BGP Update
(Route Hijacking)
AS_N
AS_1
AS_2
AS_3
AS_4
AS_5
AS_6
AS_7
AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info
10.1.1.0/24: AS_4, AS_3, ..., AS_N
10.1.1.0/24: AS_6, AS_N
Peer-Peer Relation
Customer-Provider Relation

BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1

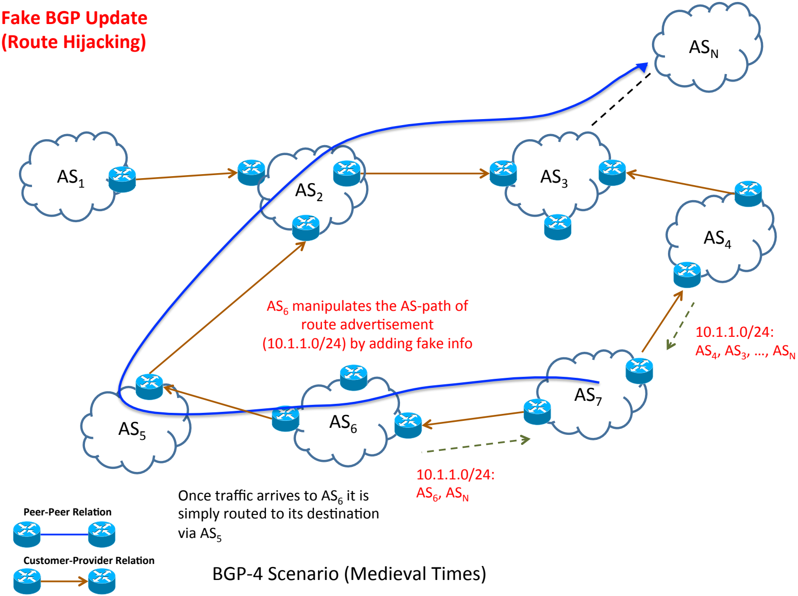


AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info

AS_7 is customer of AS_6 and AS_4. AS_7 has no way to detect the fake AS-path in the BGP update received from AS_6, and selects the route for 10.1.1.0/24 through AS_6.

BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1



Fake BGP Update (Route Hijacking)

AS$_6$ manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info

10.1.1.0/24: AS$_4$, AS$_3$, ..., AS$_N$

10.1.1.0/24: AS$_6$, AS$_N$

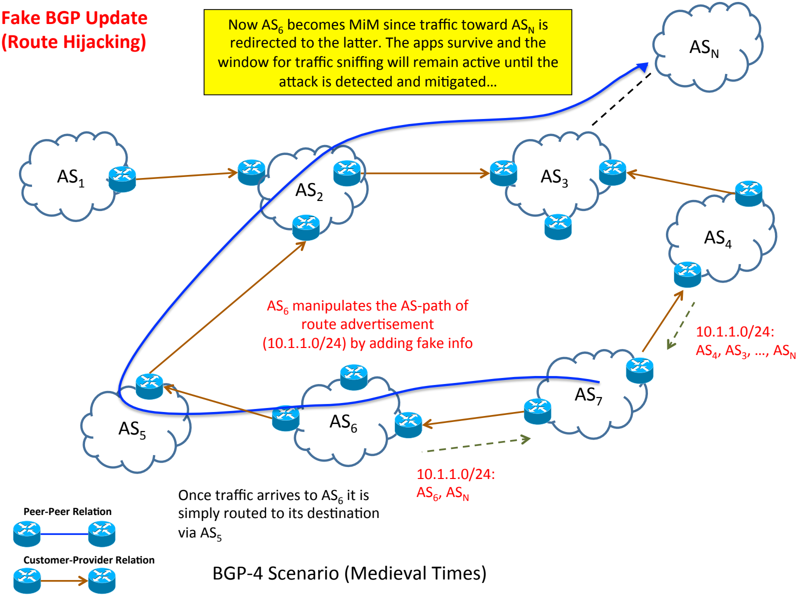
Once traffic arrives to AS$_6$ it is simply routed to its destination via AS$_5$

BGP-4 Scenario (Medieval Times)

Route Hijacking: case 1

Fake BGP Update (Route Hijacking)

Now AS_6 becomes MiM since traffic toward AS_N is redirected to the latter. The apps survive and the window for traffic sniffing will remain active until the attack is detected and mitigated…



AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info

10.1.1.0/24:
AS_4, AS_3, …, AS_N

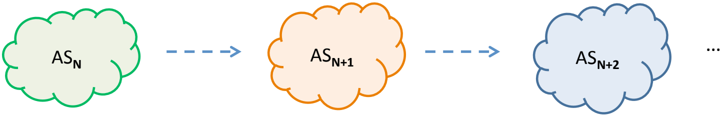
10.1.1.0/24:
AS_6, AS_N

Once traffic arrives to AS_6 it is simply routed to its destination via AS_5

BGP-4 Scenario (Medieval Times)

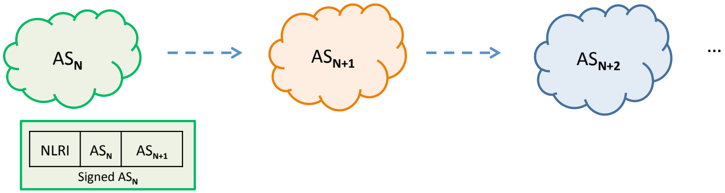
Preventing Route Hijacking: BGPSEC (with forward signing)

Preventing Route Hijacking: BGPSEC



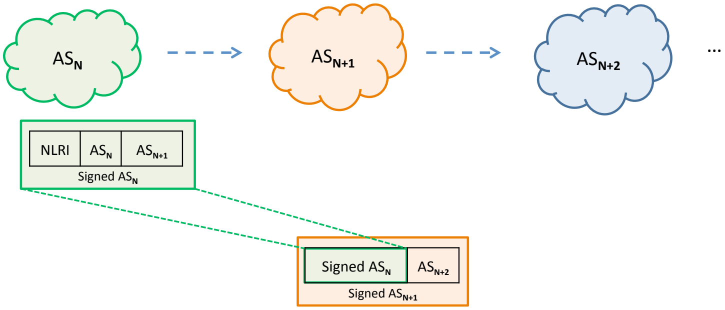
BGPSEC Update Forward Signing

Preventing Route Hijacking: BGPSEC



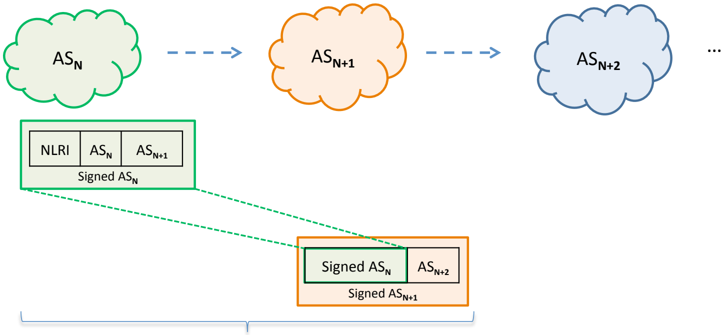
BGPSEC Update Forward Signing

Preventing Route Hijacking: BGPSEC



BGPSEC Update Forward Signing

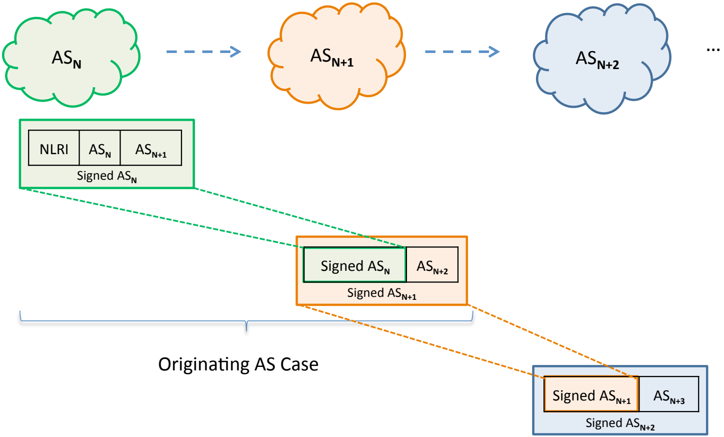
Preventing Route Hijacking: BGPSEC



Originating AS Case

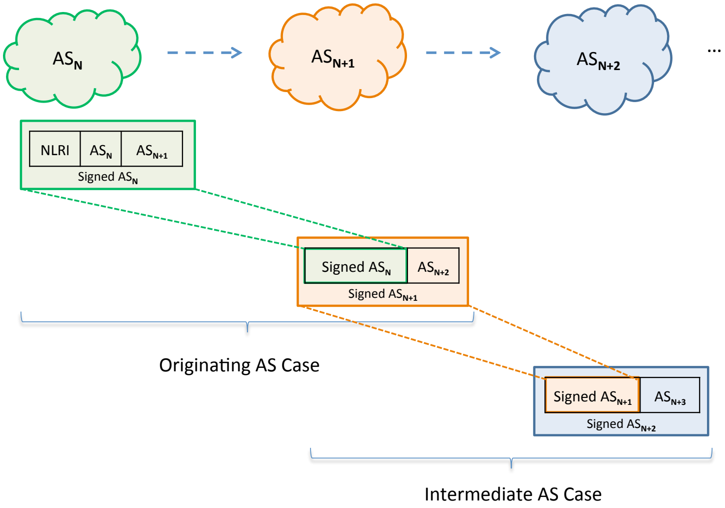
BGPSEC Update Forward Signing

Preventing Route Hijacking: BGPSEC



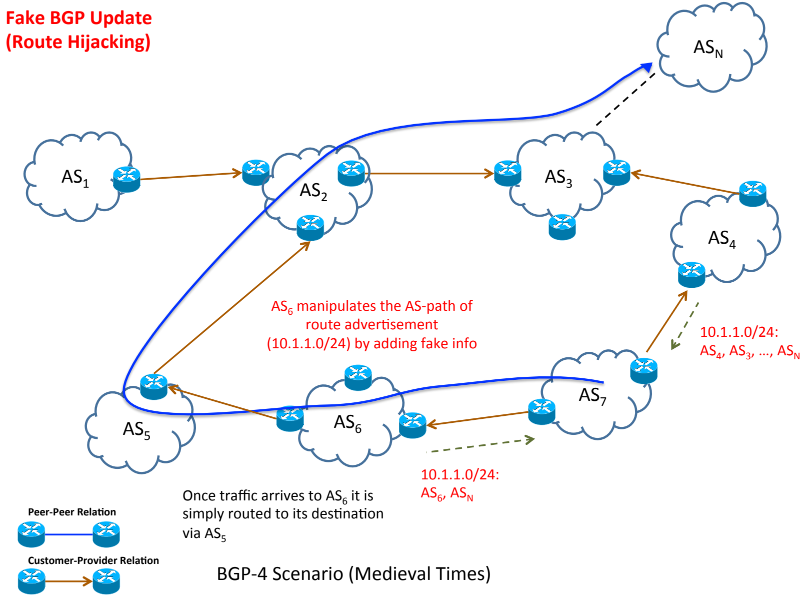
BGPSEC Update Forward Signing

Preventing Route Hijacking: BGPSEC



BGPSEC Update Forward Signing

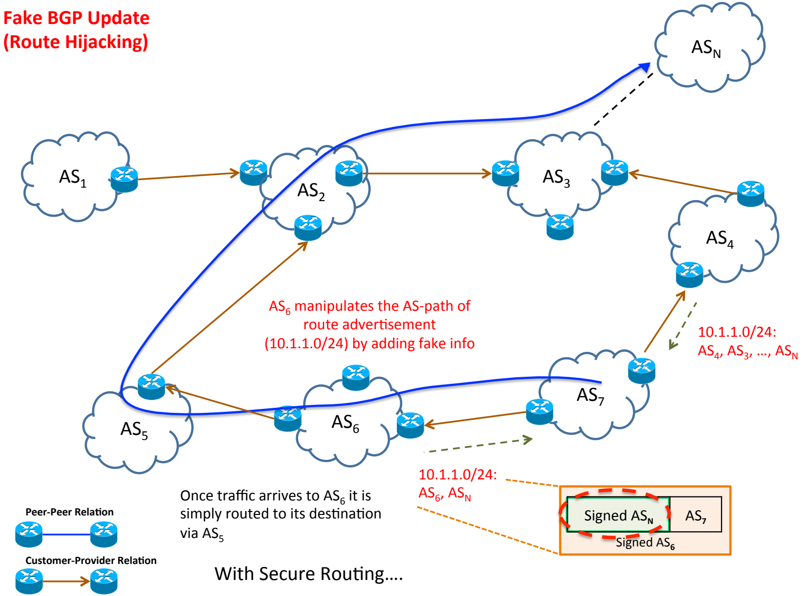
BGPSEC (with forward signing)



Fake BGP Update
(Route Hijacking)
AS_N
AS_1
AS_2
AS_3
AS_4
AS_5
AS_6
AS_7
AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info
10.1.1.0/24:
AS_4, AS_3, ..., AS_N
10.1.1.0/24:
AS_6, AS_N
Once traffic arrives to AS_6 it is simply routed to its destination via AS_5
Peer-Peer Relation
Customer-Provider Relation

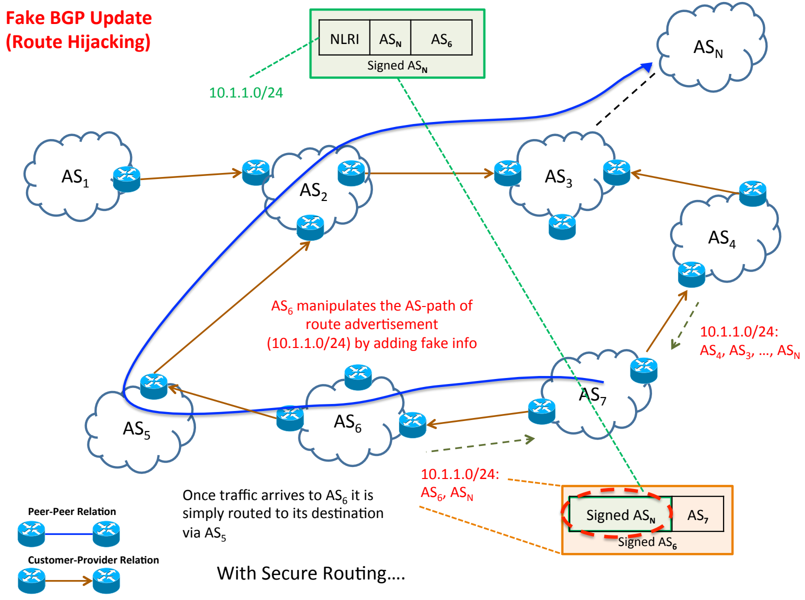
BGP-4 Scenario (Medieval Times)

BGPSEC (with forward signing)



Fake BGP Update
(Route Hijacking)
AS_N
AS_1
AS_2
AS_3
AS_4
AS_5
AS_6
AS_7
AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info
10.1.1.0/24: AS_4, AS_3, ..., AS_N
10.1.1.0/24: AS_6, AS_N
Signed AS_N
AS_7
Signed AS_6
Once traffic arrives to AS_6 it is simply routed to its destination via AS_5
Peer-Peer Relation
Customer-Provider Relation
With Secure Routing....

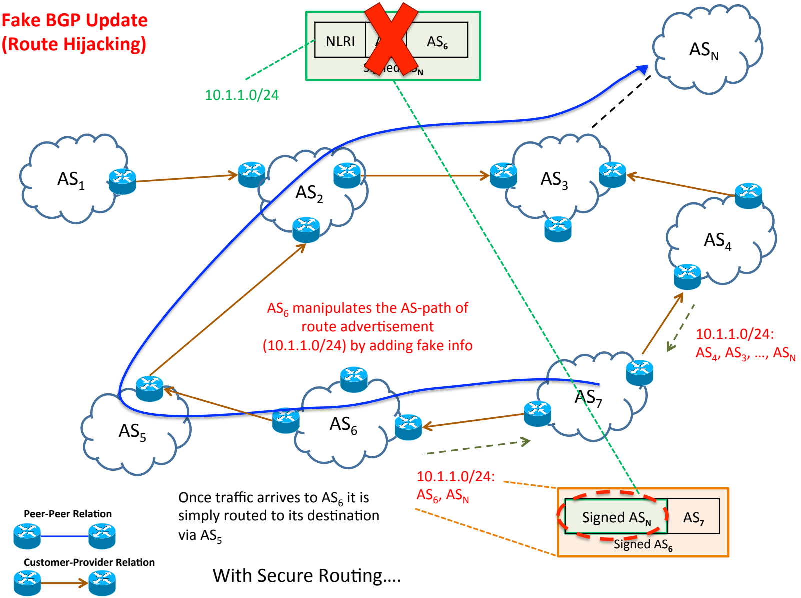
BGPSEC (with forward signing)



Once traffic arrives to AS_6 it is simply routed to its destination via AS_5

With Secure Routing....

BGPSEC (with forward signing)



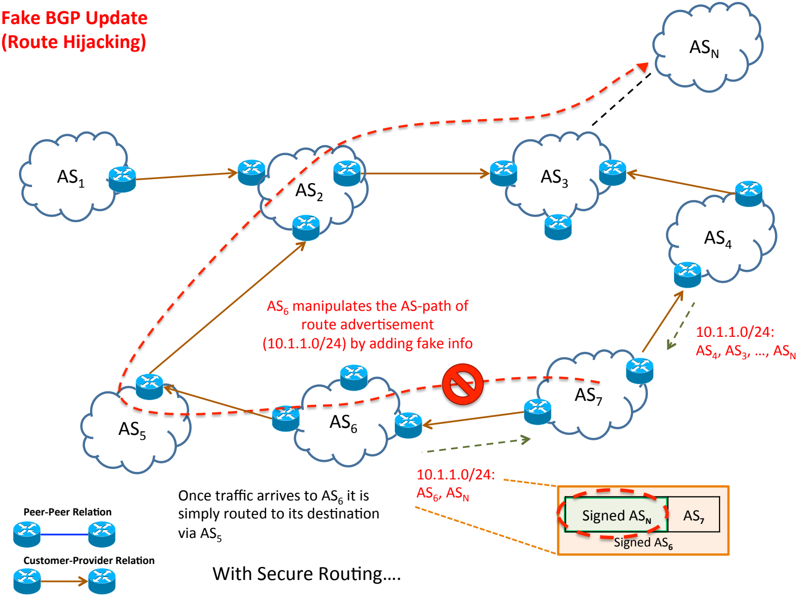
Fake BGP Update (Route Hijacking)

AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info

Once traffic arrives to AS_6 it is simply routed to its destination via AS_5

With Secure Routing....

BGPSEC (with forward signing)



Fake BGP Update (Route Hijacking)

AS_6 manipulates the AS-path of route advertisement (10.1.1.0/24) by adding fake info

10.1.1.0/24: AS_4, AS_3, …, AS_N

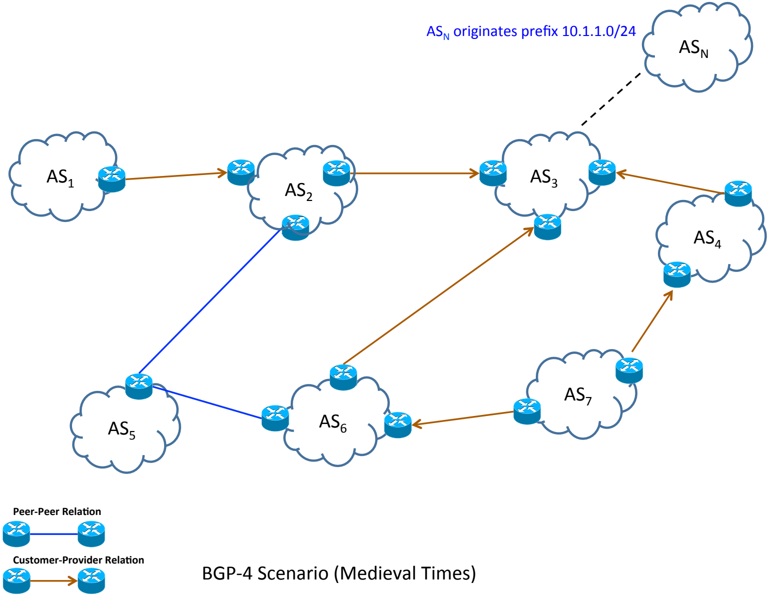
10.1.1.0/24: AS_6, AS_N

Once traffic arrives to AS_6 it is simply routed to its destination via AS_5

With Secure Routing….

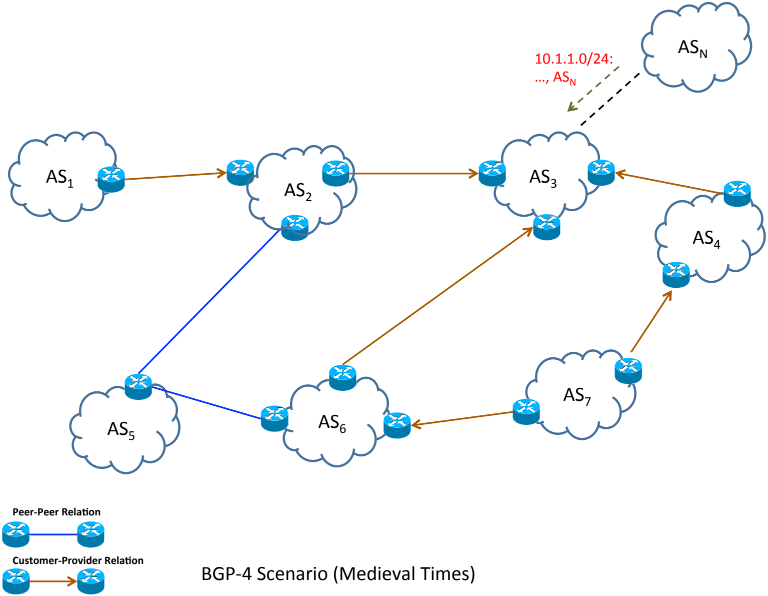
AS-path Shortening (valid BGP paths)

Route Hijacking: case 2



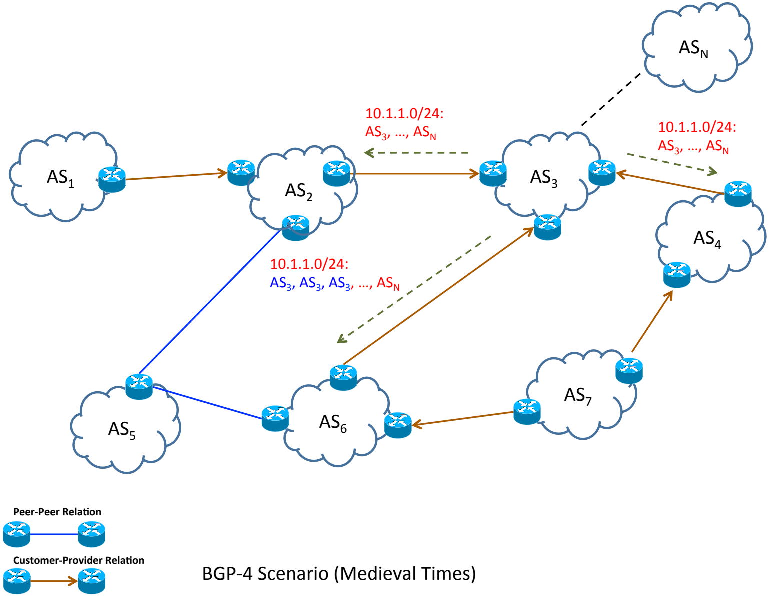
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 2



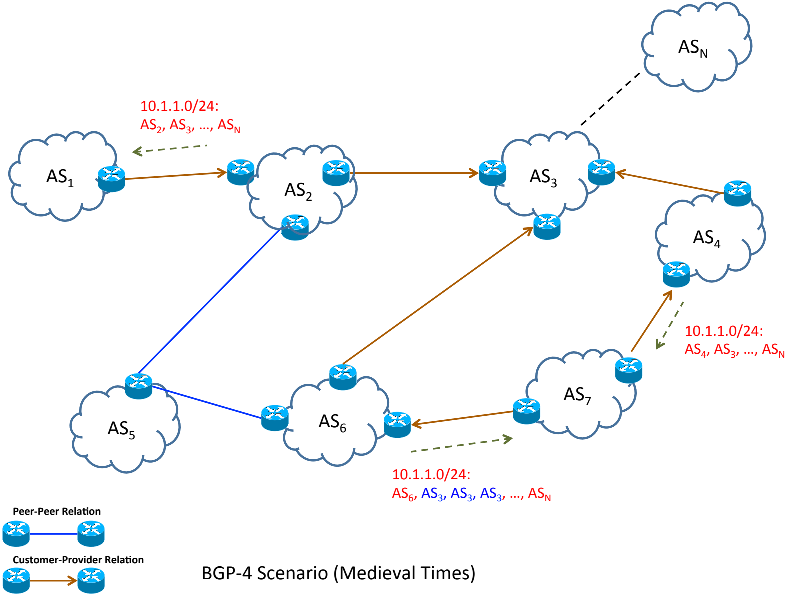
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 2



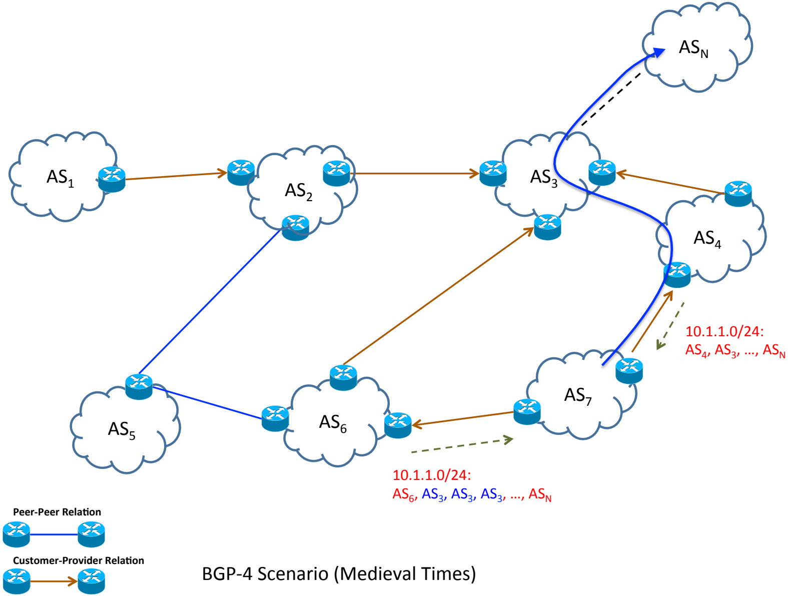
BGP-4 Scenario (Medieval Times)

Route Hijacking: case 2


AS_N
10.1.1.0/24:
AS_2, AS_3, ..., AS_N
AS_1
AS_2
AS_3
AS_4
10.1.1.0/24:
AS_4, AS_3, ..., AS_N
AS_5
AS_6
AS_7
10.1.1.0/24:
AS_6, AS_3, AS_3, AS_3, ..., AS_N
Peer-Peer Relation
Customer-Provider Relation

BGP-4 Scenario (Medieval Times)

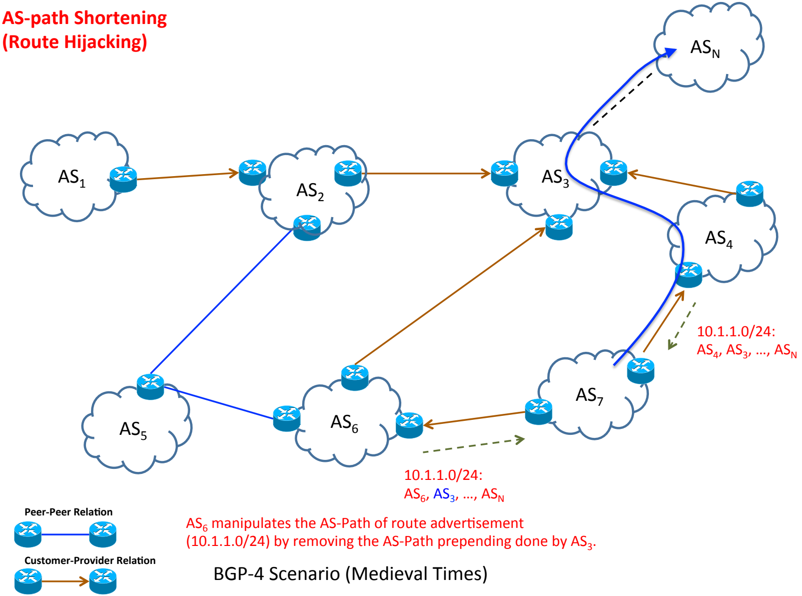
Route Hijacking: case 2


AS_N
AS_1
AS_2
AS_3
AS_4
AS_5
AS_6
AS_7
10.1.1.0/24:
AS_4, AS_3, …, AS_N
10.1.1.0/24:
AS_6, AS_3, AS_3, AS_3, …, AS_N
Peer-Peer Relation
Customer-Provider Relation

BGP-4 Scenario (Medieval Times)

Route Hijacking: case 2

AS-path Shortening (Route Hijacking)



10.1.1.0/24: AS$_4$, AS$_3$, …, AS$_N$

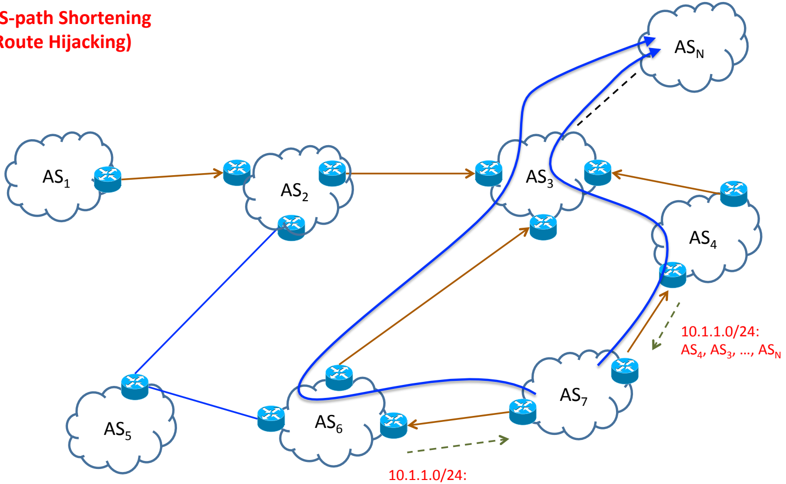
10.1.1.0/24: AS$_6$, AS$_3$, …, AS$_N$

AS$_6$ manipulates the AS-Path of route advertisement (10.1.1.0/24) by removing the AS-Path prepending done by AS$_3$.

BGP-4 Scenario (Medieval Times)

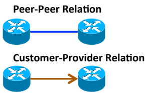
Route Hijacking: case 2

AS-path Shortening (Route Hijacking)



10.1.1.0/24:
AS_4, AS_3, …, AS_N

10.1.1.0/24:
AS_6, AS_3, …, AS_N



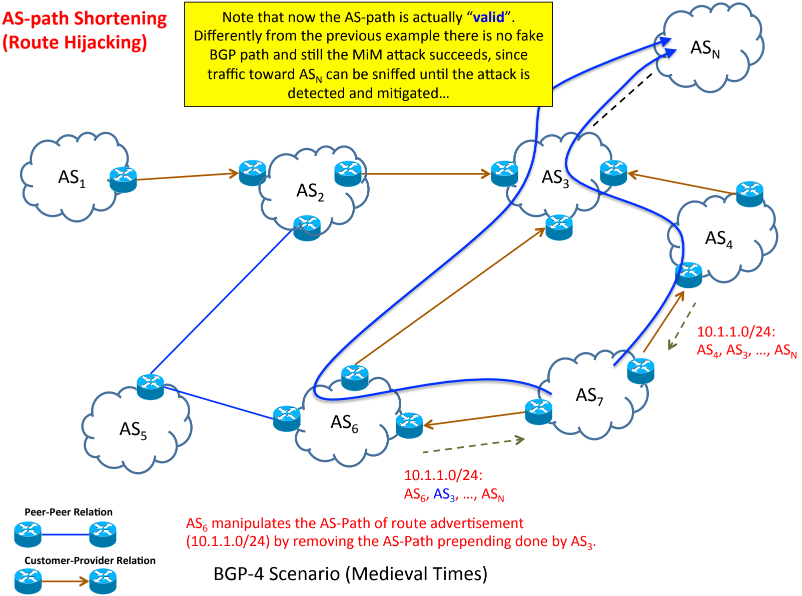
AS_6 manipulates the AS-Path of route advertisement (10.1.1.0/24) by removing the AS-Path prepending done by AS_3.

BGP-4 Scenario (Medieval Times)

Route Hijacking: case 2

AS-path Shortening (Route Hijacking)

Note that now the AS-path is actually "**valid**". Differently from the previous example there is no fake BGP path and still the MiM attack succeeds, since traffic toward AS_N can be sniffed until the attack is detected and mitigated…

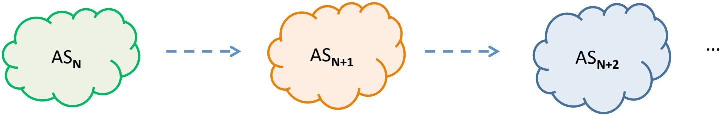


AS_6 manipulates the AS-Path of route advertisement (10.1.1.0/24) by removing the AS-Path prepending done by AS_3.

BGP-4 Scenario (Medieval Times)

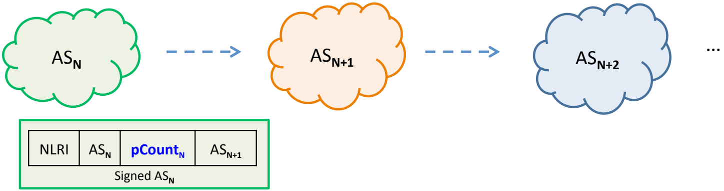
Preventing Route Hijacking: BGPSEC (with forward signing and pcount)

BGPSEC (with forward signing and pcount)



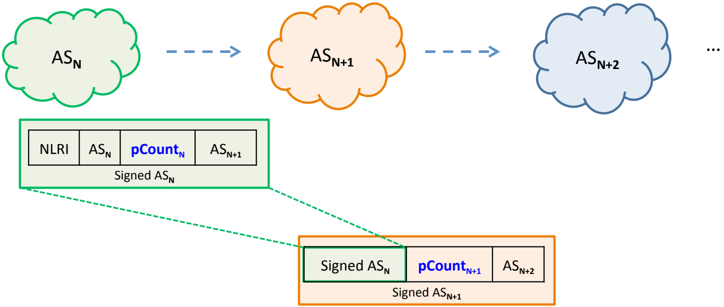
BGPSEC Update Forward Signing (with pcount)

BGPSEC (with forward signing and pcount)



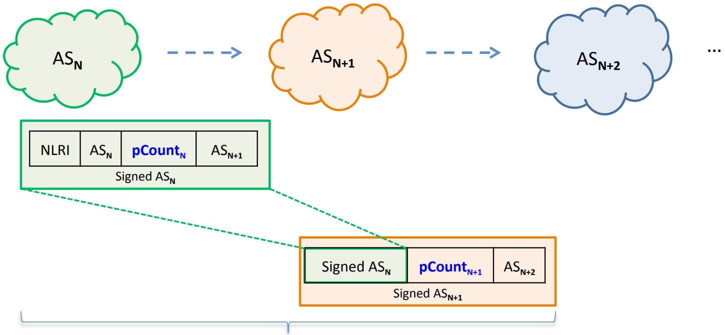
BGPSEC Update Forward Signing (with pcount)

BGPSEC (with forward signing and pcount)



BGPSEC Update Forward Signing (with pcount)

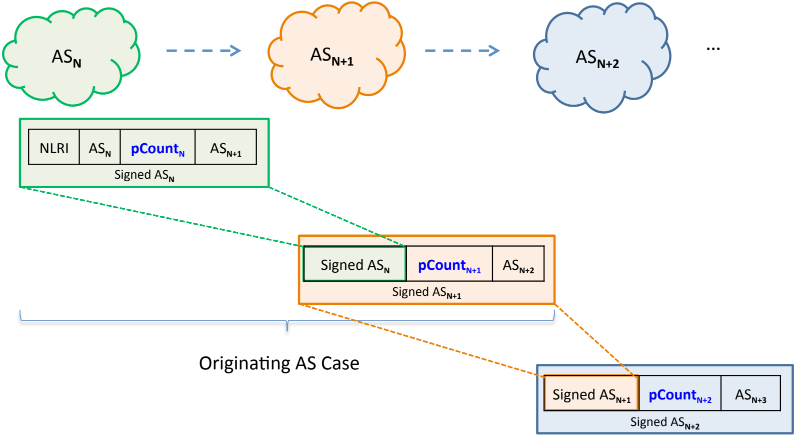
BGPSEC (with forward signing and pcount)



Originating AS Case

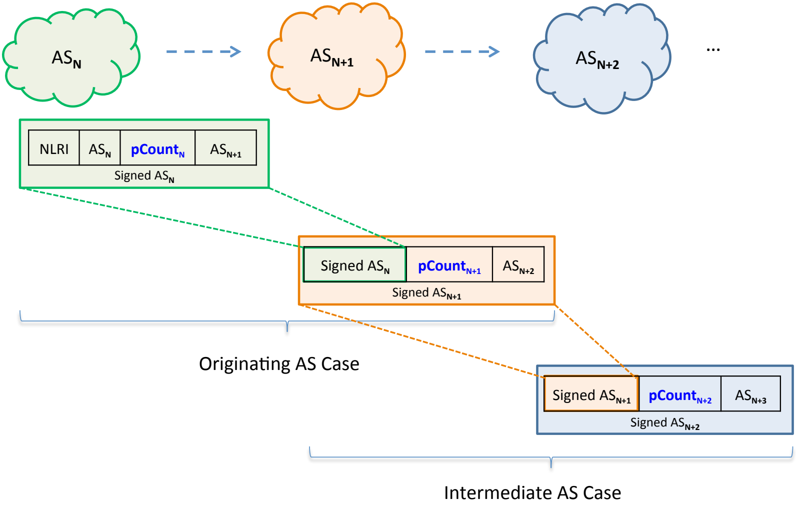
BGPSEC Update Forward Signing (with pcount)

BGPSEC (with forward signing and pcount)



BGPSEC Update Forward Signing (with pcount)

BGPSEC (with forward signing and pcount)



AS_N AS_{N+1} AS_{N+2} …

NLRI | AS_N | $pCount_N$ | AS_{N+1}

Signed AS_N

Signed AS_N | $pCount_{N+1}$ | AS_{N+2}

Signed AS_{N+1}

Originating AS Case

Signed AS_{N+1} | $pCount_{N+2}$ | AS_{N+3}

Signed AS_{N+2}

Intermediate AS Case

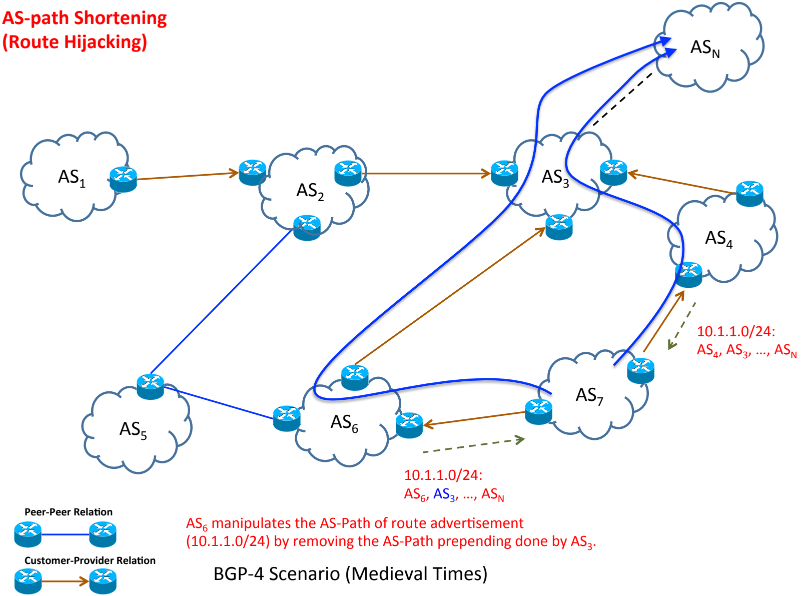
BGPSEC Update Forward Signing (with pcount)

Basic operation of pcount...

- Formerly in BGPSEC:
  - AS-PATH : X Y Z Z Z (required 5 signatures)
- Now:
  - AS-PATH : X Y Z
  - pCount :   1 1 3 (requires only 3 signatures)
- AS-path length now is the sum of the pcount...
- Note that it requires “expanding" the AS-path when sending an update from a BGPSEC speaker to a non-BGPSEC speaker.
- Route Servers and IXPs may set pCount to 0....to avoid moving traffic away from them due to the increased AS-PATH length.
- **Security Threat:** Entities that are neither Route Servers nor IXPs could set pCount = 0 to bias traffic towards them ... so if the peer is not a one of those and sends an update with pCount = 0, the update should be dropped ...

BGPSEC (with forward signing and pcount)

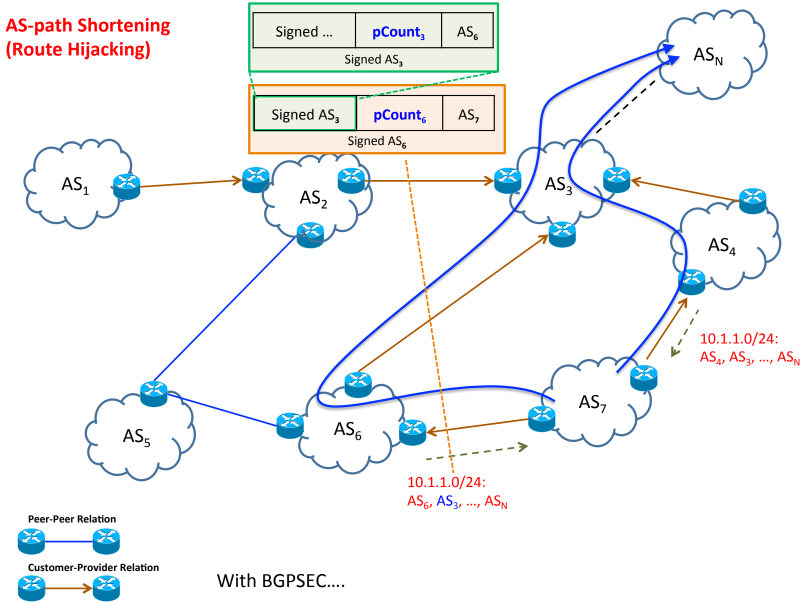
AS-path Shortening (Route Hijacking)



AS_6 manipulates the AS-Path of route advertisement (10.1.1.0/24) by removing the AS-Path prepending done by AS_3.

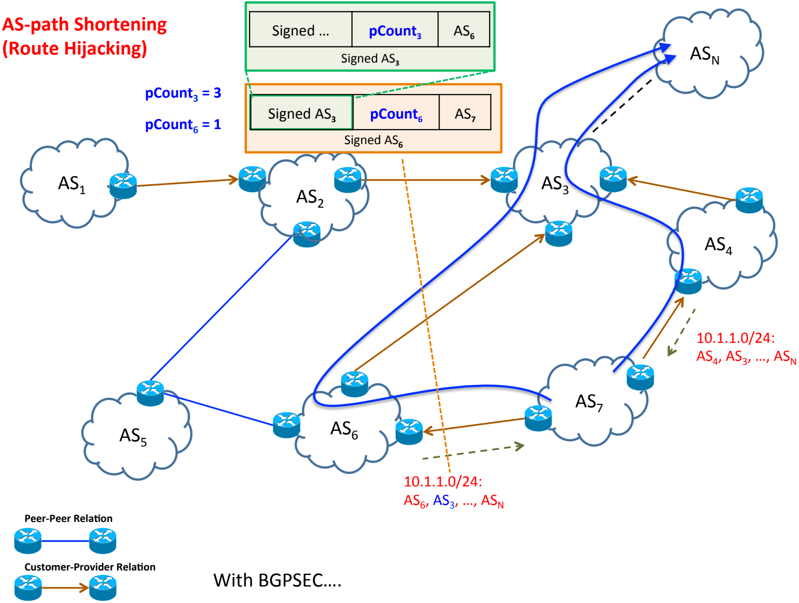
BGP-4 Scenario (Medieval Times)

BGPSEC (with forward signing and pcount)



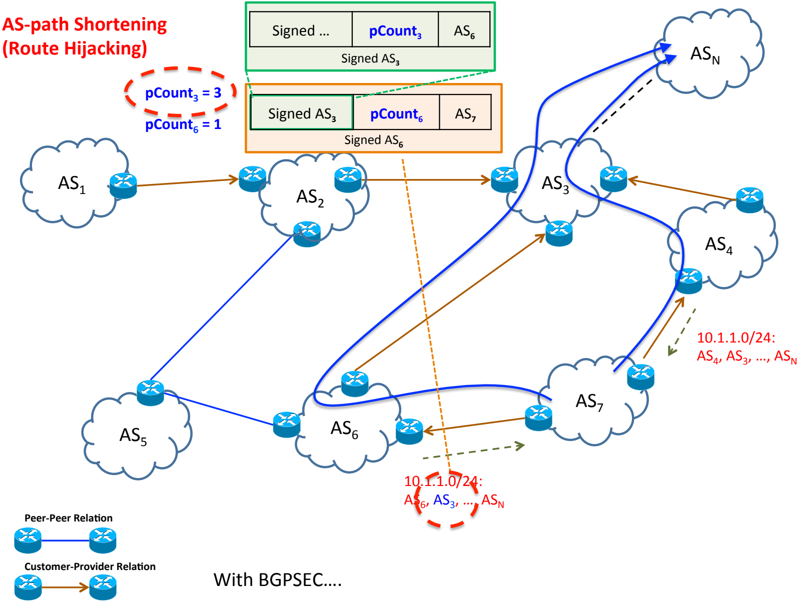
With BGPSEC….

BGPSEC (with forward signing and pcount)



With BGPSEC....

BGPSEC (with forward signing and pcount)

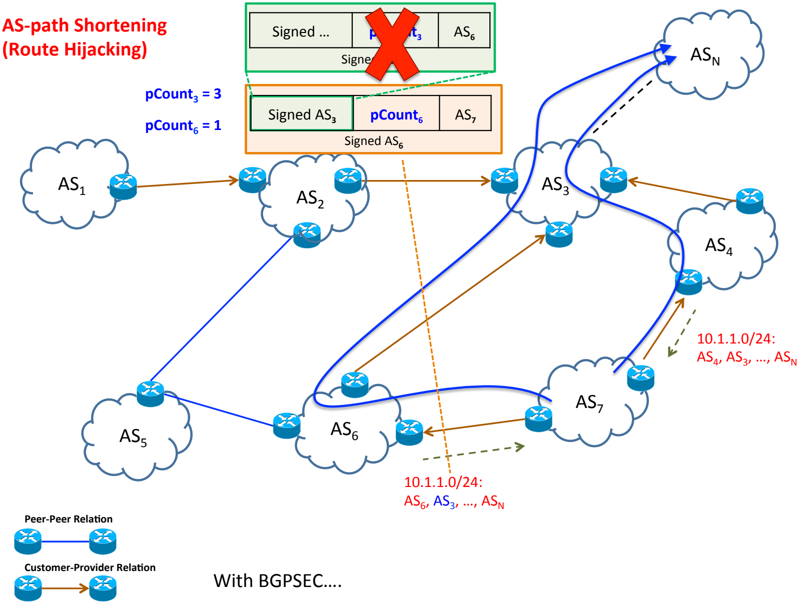


AS-path Shortening (Route Hijacking)

With BGPSEC….

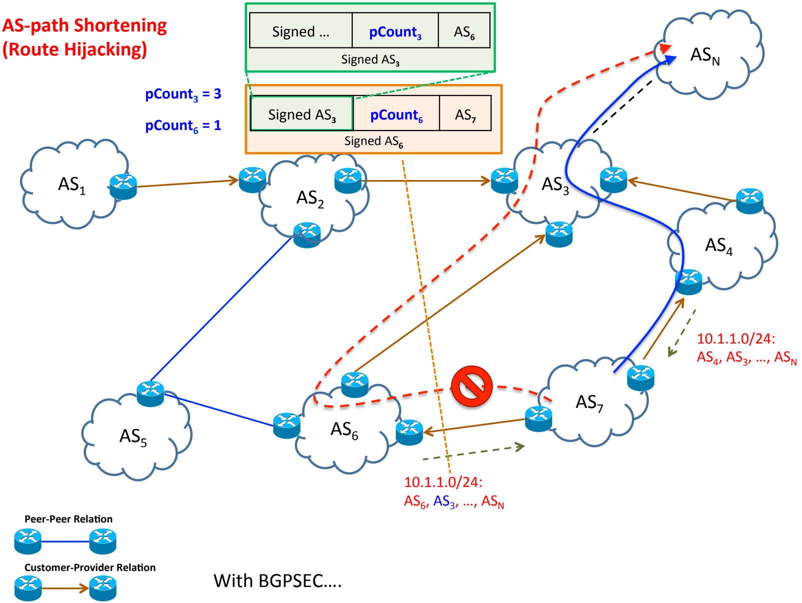
BGPSEC (with forward signing and pcount)

AS-path Shortening (Route Hijacking)



With BGPSEC….

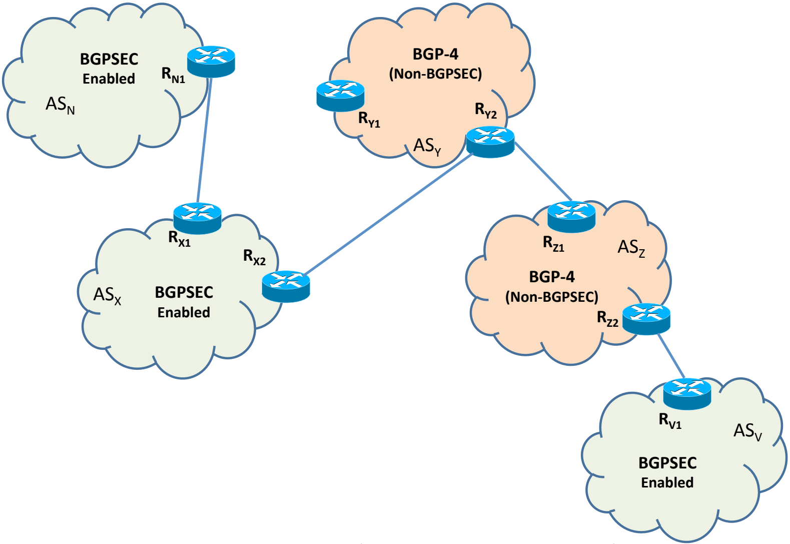
BGPSEC (with forward signing and pcount)



With BGPSEC….

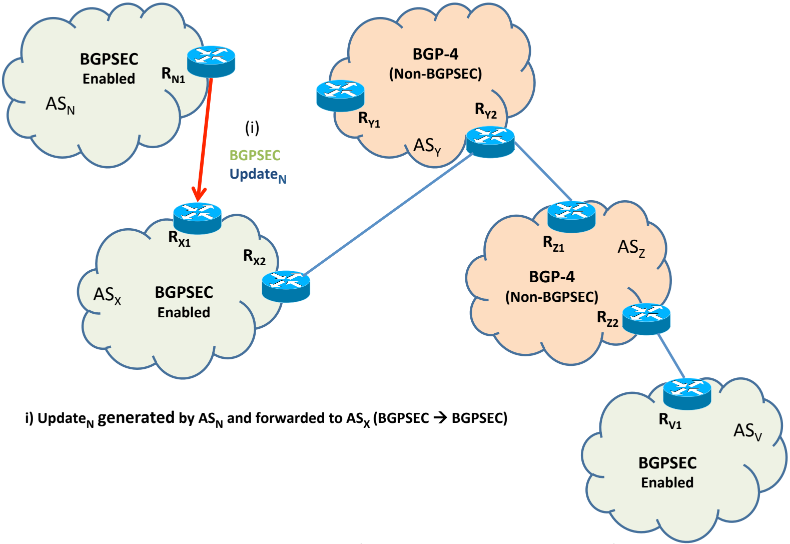
BGPSEC (Partial Deployments)

BGPSEC (Partial Deployments - Scenario I)



BGPSEC Partial Deployment Scenario I (BGPSEC Originated Update)

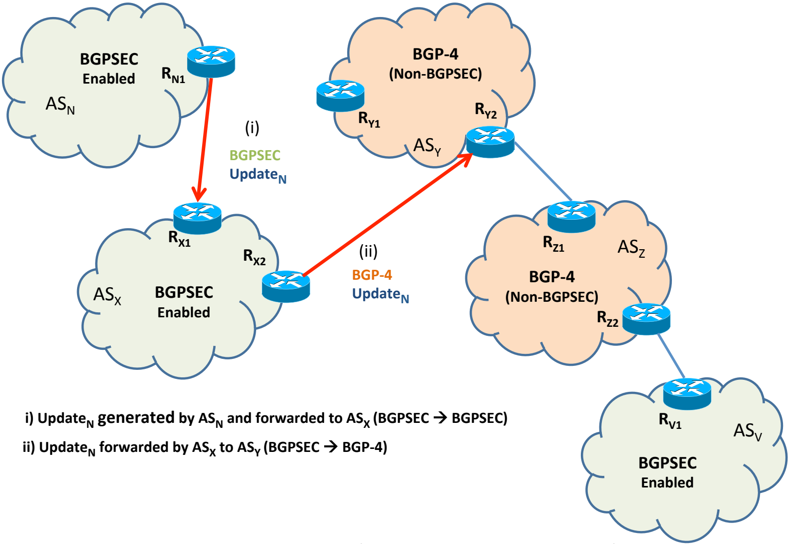
BGPSEC (Partial Deployments - Scenario I)



i) $Update_N$ generated by AS_N and forwarded to AS_X (BGPSEC → BGPSEC)

BGPSEC Partial Deployment Scenario I (BGPSEC Originated Update)

BGPSEC (Partial Deployments - Scenario I)

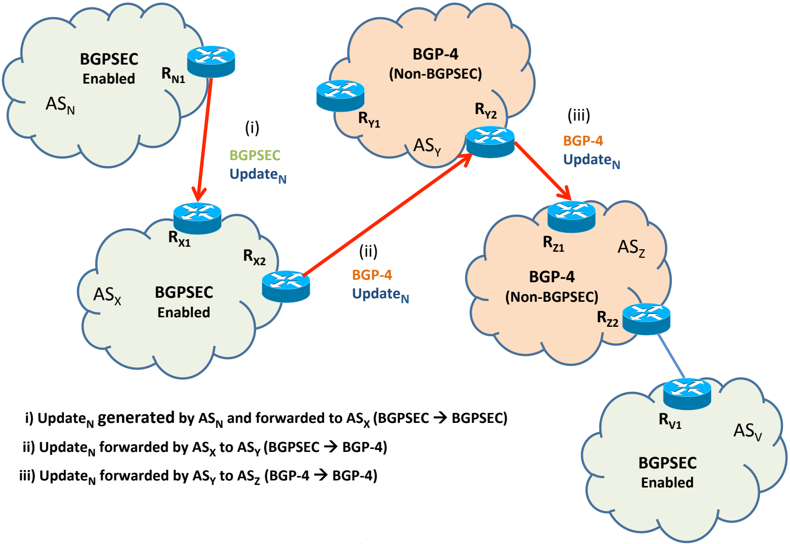


i) $Update_N$ generated by AS_N and forwarded to AS_X (BGPSEC → BGPSEC)

ii) $Update_N$ forwarded by AS_X to AS_Y (BGPSEC → BGP-4)

BGPSEC Partial Deployment Scenario I (BGPSEC Originated Update)

BGPSEC (Partial Deployments - Scenario I)



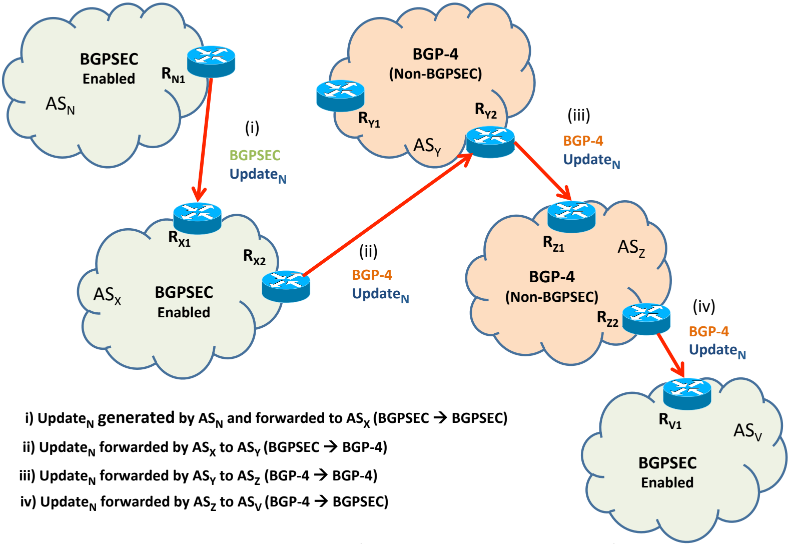
i) $Update_N$ generated by AS_N and forwarded to AS_X (BGPSEC → BGPSEC)

ii) $Update_N$ forwarded by AS_X to AS_Y (BGPSEC → BGP-4)

iii) $Update_N$ forwarded by AS_Y to AS_Z (BGP-4 → BGP-4)

BGPSEC Partial Deployment Scenario I (BGPSEC Originated Update)

BGPSEC (Partial Deployments - Scenario I)



i) Update$_N$ generated by AS_N and forwarded to AS_X (BGPSEC → BGPSEC)

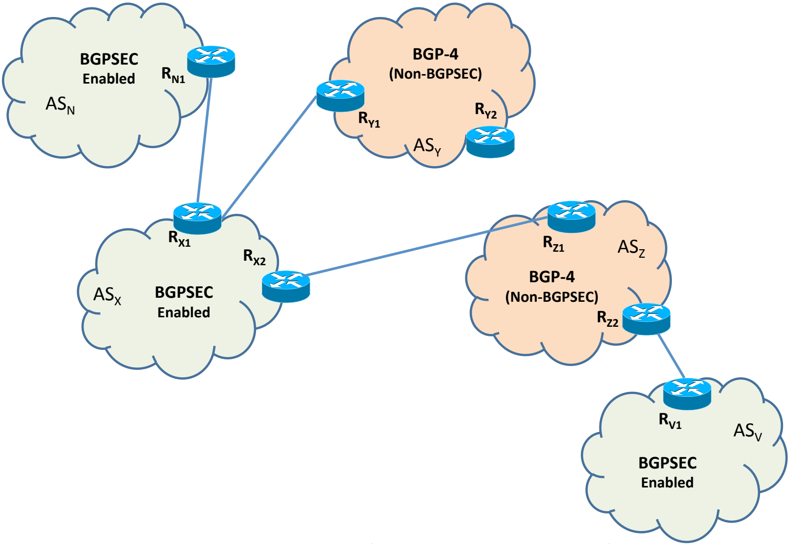
ii) Update$_N$ forwarded by AS_X to AS_Y (BGPSEC → BGP-4)

iii) Update$_N$ forwarded by AS_Y to AS_Z (BGP-4 → BGP-4)

iv) Update$_N$ forwarded by AS_Z to AS_V (BGP-4 → BGPSEC)

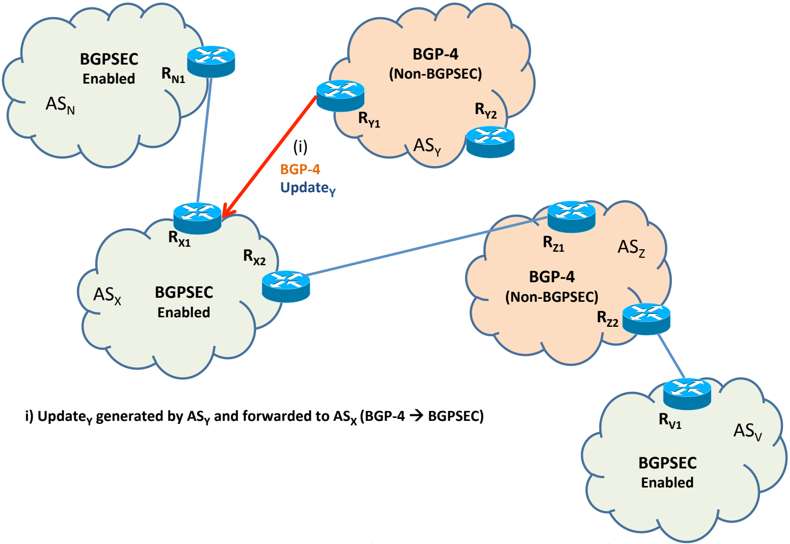
BGPSEC Partial Deployment Scenario I (BGPSEC Originated Update)

BGPSEC (Partial Deployments - Scenario II)



BGPSEC Partial Deployment Scenario II (BGP-4 Originated Update)

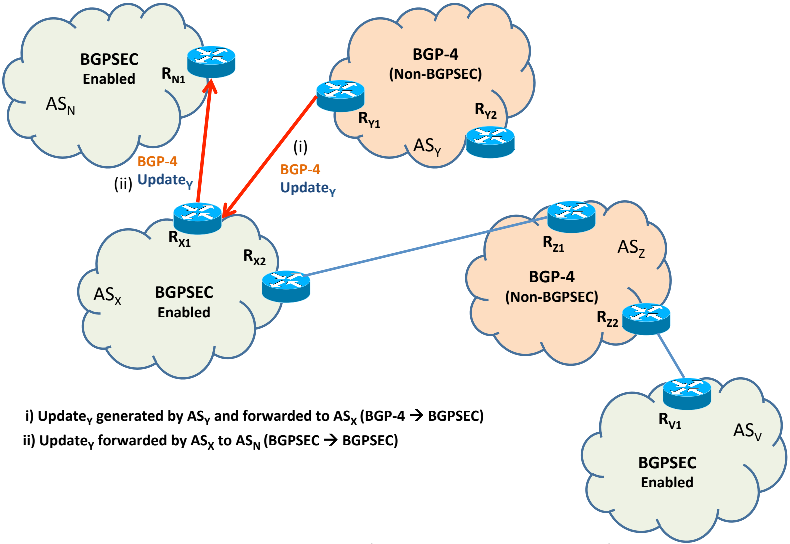
BGPSEC (Partial Deployments - Scenario II)



i) $Update_Y$ generated by AS_Y and forwarded to AS_X (BGP-4 → BGPSEC)

BGPSEC Partial Deployment Scenario II (BGP-4 Originated Update)

BGPSEC (Partial Deployments - Scenario II)

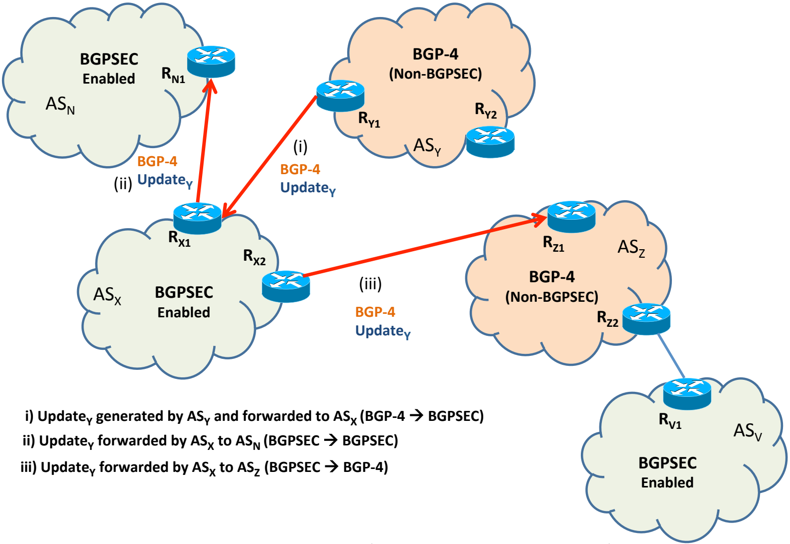


i) $Update_Y$ generated by AS_Y and forwarded to AS_X (BGP-4 → BGPSEC)

ii) $Update_Y$ forwarded by AS_X to AS_N (BGPSEC → BGPSEC)

BGPSEC Partial Deployment Scenario II (BGP-4 Originated Update)

BGPSEC (Partial Deployments - Scenario II)



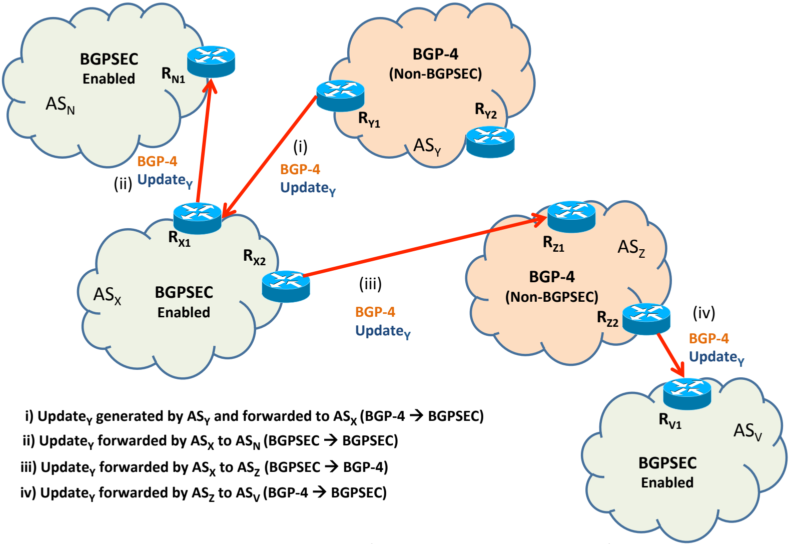
i) $Update_Y$ generated by AS_Y and forwarded to AS_X (BGP-4 → BGPSEC)

ii) $Update_Y$ forwarded by AS_X to AS_N (BGPSEC → BGPSEC)

iii) $Update_Y$ forwarded by AS_X to AS_Z (BGPSEC → BGP-4)

BGPSEC Partial Deployment Scenario II (BGP-4 Originated Update)

BGPSEC (Partial Deployments - Scenario II)



i) $Update_Y$ generated by AS_Y and forwarded to AS_X (BGP-4 → BGPSEC)
ii) $Update_Y$ forwarded by AS_X to AS_N (BGPSEC → BGPSEC)
iii) $Update_Y$ forwarded by AS_X to AS_Z (BGPSEC → BGP-4)
iv) $Update_Y$ forwarded by AS_Z to AS_V (BGP-4 → BGPSEC)

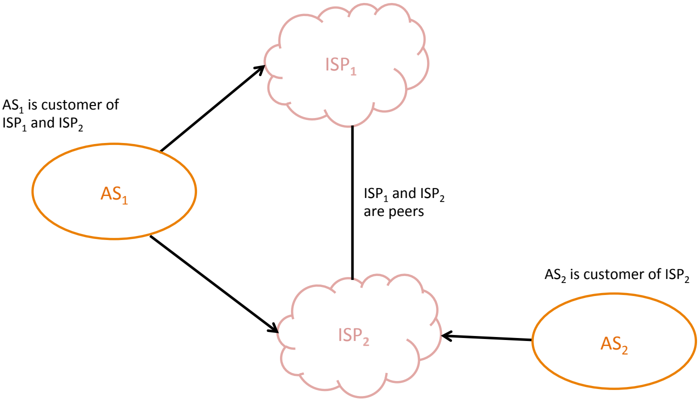
BGPSEC Partial Deployment Scenario II (BGP-4 Originated Update)

Outline

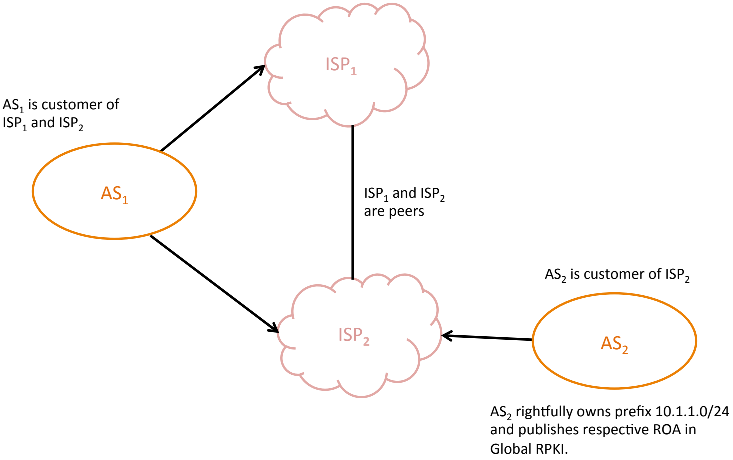
1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. **Route leaks**
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Route Leaks: Customer Case

Route Leaks: Customer Case


ISP$_1$
AS_1 is customer of ISP_1 and ISP_2
AS_1
ISP_1 and ISP_2 are peers
AS_2 is customer of ISP_2
ISP_2
AS_2

Route Leaks: Customer Case



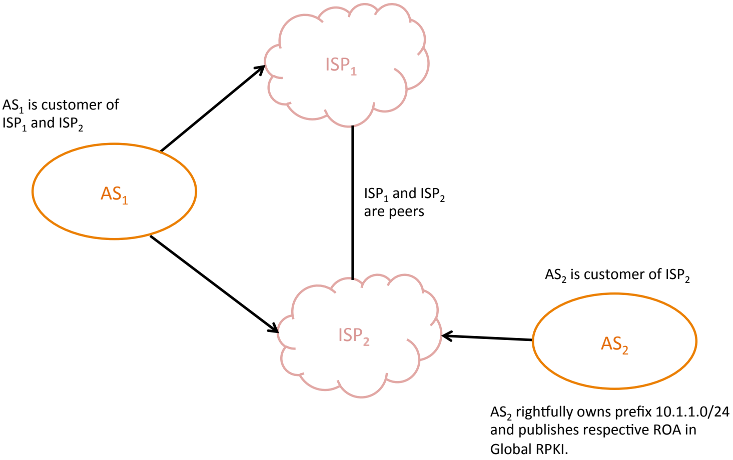
AS$_1$ is customer of ISP$_1$ and ISP$_2$

ISP$_1$ and ISP$_2$ are peers

AS$_2$ is customer of ISP$_2$

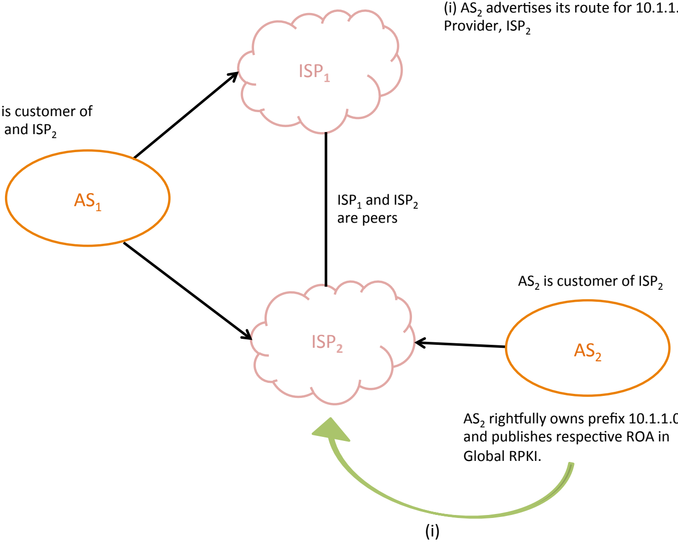
AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: Customer Case


ISP$_1$
AS$_1$ is customer of ISP$_1$ and ISP$_2$
AS$_1$
ISP$_1$ and ISP$_2$ are peers
AS$_2$ is customer of ISP$_2$
ISP$_2$
AS$_2$
AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Note: Assuming complete presence of RPKI and that the route advertisement is carried out using BGPSEC and ROA, even then route leaks can occur. **This is because RPKI, BGPSEC and ROA only secure the operations of BGP and not the BGP polices among the various ASes.**

Route Leaks: Customer Case



(i) AS$_2$ advertises its route for 10.1.1.0/24 to its Provider, ISP$_2$

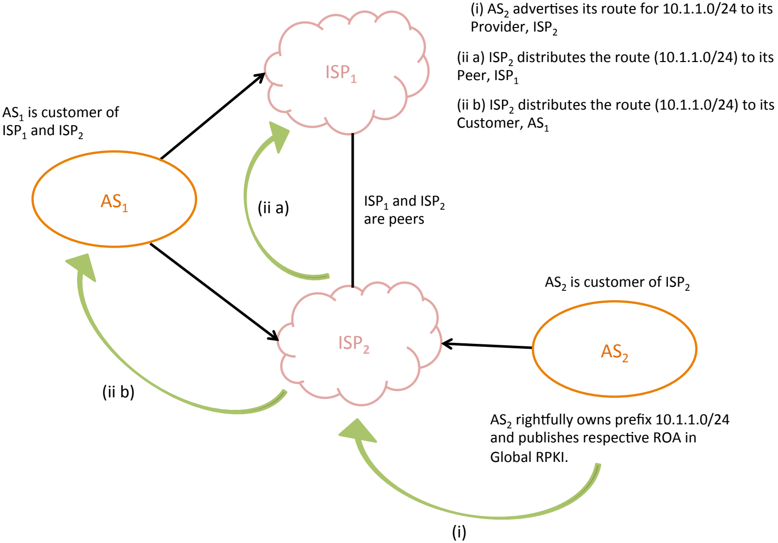
AS$_1$ is customer of ISP$_1$ and ISP$_2$

ISP$_1$ and ISP$_2$ are peers

AS$_2$ is customer of ISP$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: Customer Case



(i) AS_2 advertises its route for 10.1.1.0/24 to its Provider, ISP_2

(ii a) ISP_2 distributes the route (10.1.1.0/24) to its Peer, ISP_1

(ii b) ISP_2 distributes the route (10.1.1.0/24) to its Customer, AS_1

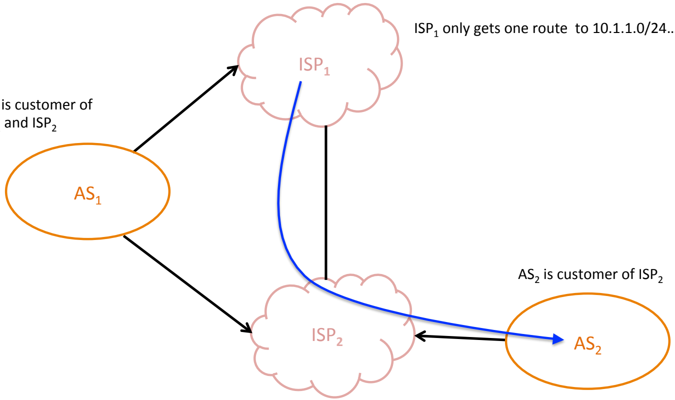
AS_1 is customer of ISP_1 and ISP_2

ISP_1 and ISP_2 are peers

AS_2 is customer of ISP_2

AS_2 rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: Customer Case



ISP$_1$ only gets one route to 10.1.1.0/24…via its peer

AS$_1$ is customer of ISP$_1$ and ISP$_2$

AS$_2$ is customer of ISP$_2$

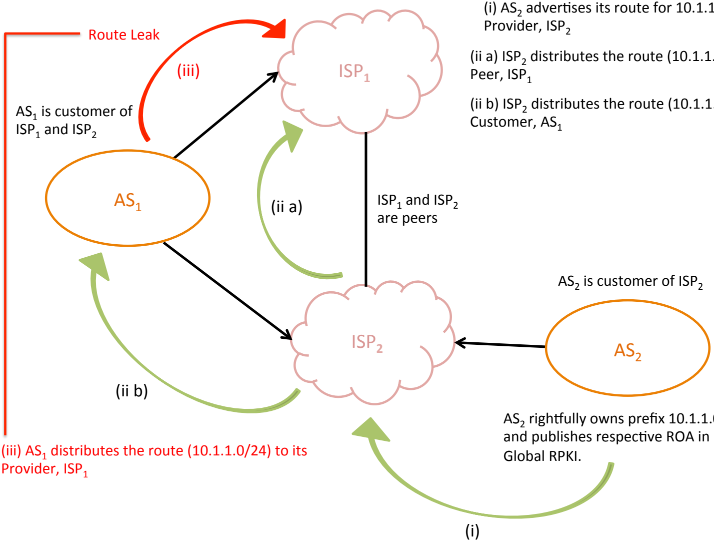
AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: Customer Case

(i) AS_2 advertises its route for 10.1.1.0/24 to its Provider, ISP_2

(ii a) ISP_2 distributes the route (10.1.1.0/24) to its Peer, ISP_1

(ii b) ISP_2 distributes the route (10.1.1.0/24) to its Customer, AS_1



Route Leak

(iii)

AS_1 is customer of ISP_1 and ISP_2

ISP_1

AS_1

(ii a)

ISP_1 and ISP_2 are peers

AS_2 is customer of ISP_2

ISP_2

AS_2

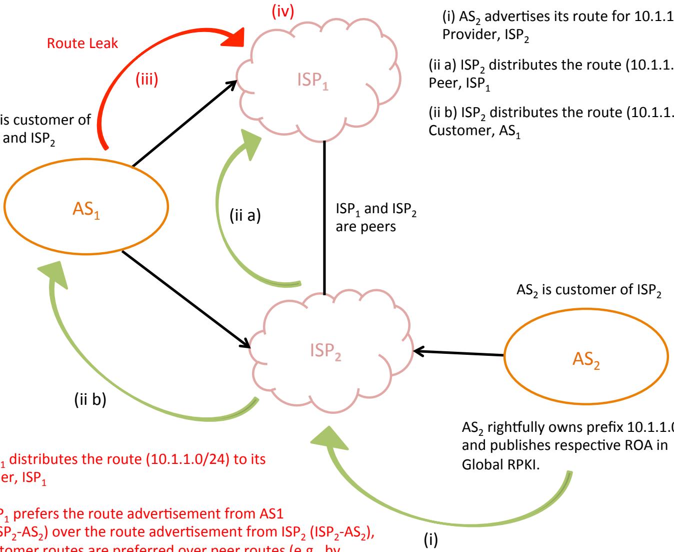
(ii b)

AS_2 rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

(i)

(iii) AS_1 distributes the route (10.1.1.0/24) to its Provider, ISP_1

Route Leaks: Customer Case


(iv)
Route Leak
(iii)
ISP$_1$
AS$_1$ is customer of ISP$_1$ and ISP$_2$
AS$_1$
(ii a)
ISP$_1$ and ISP$_2$ are peers
AS$_2$ is customer of ISP$_2$
ISP$_2$
AS$_2$
(ii b)
(i)

(i) AS$_2$ advertises its route for 10.1.1.0/24 to its Provider, ISP$_2$

(ii a) ISP$_2$ distributes the route (10.1.1.0/24) to its Peer, ISP$_1$

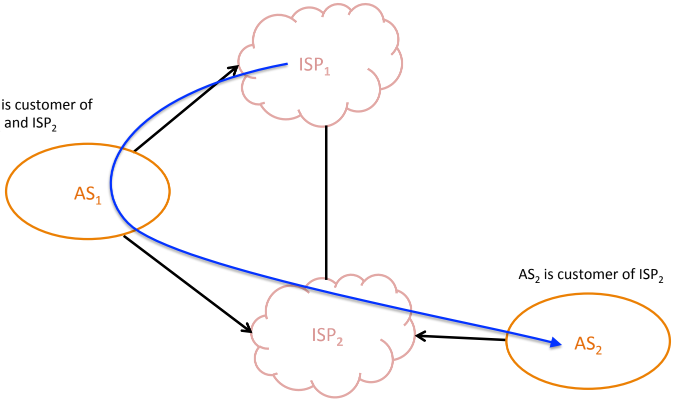
(ii b) ISP$_2$ distributes the route (10.1.1.0/24) to its Customer, AS$_1$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

(iii) AS$_1$ distributes the route (10.1.1.0/24) to its Provider, ISP$_1$

(iv) ISP$_1$ prefers the route advertisement from AS1 (AS$_1$-ISP$_2$-AS$_2$) over the route advertisement from ISP$_2$ (ISP$_2$-AS$_2$), as customer routes are preferred over peer routes (e.g., by policies enforced using communities) …. even though the path length of the latter is greater than the former.

Route Leaks: Customer Case

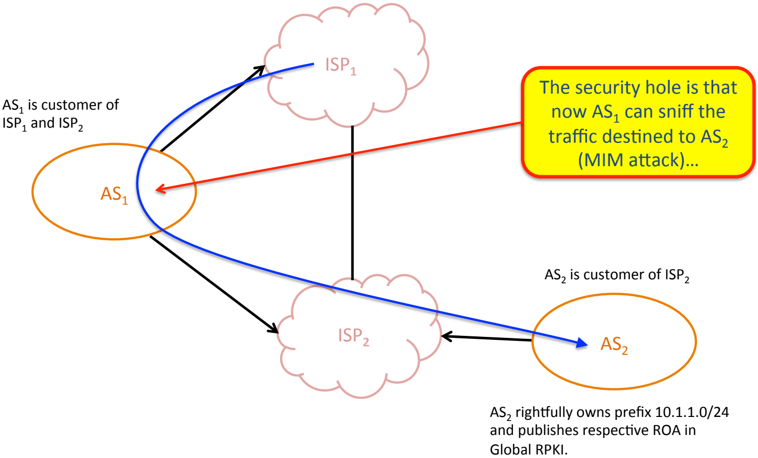


AS$_1$ is customer of ISP$_1$ and ISP$_2$

AS$_2$ is customer of ISP$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: Customer Case



AS$_1$ is customer of ISP$_1$ and ISP$_2$

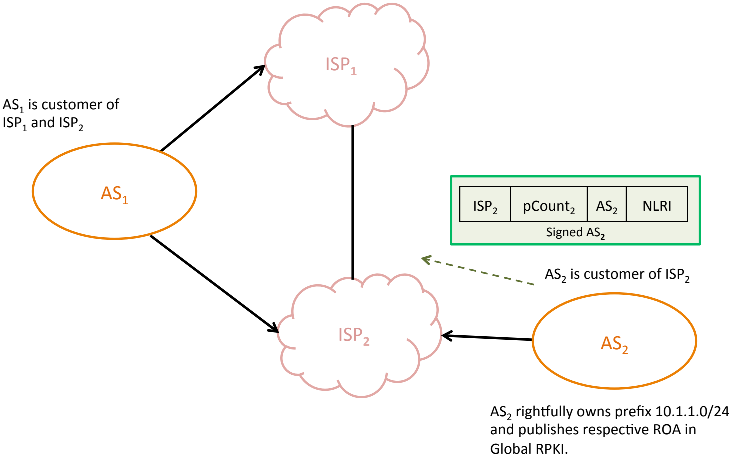
The security hole is that now AS$_1$ can sniff the traffic destined to AS$_2$ (MIM attack)...

AS$_2$ is customer of ISP$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

Route Leaks: RPKI, ROA, and BGPSEC are not sufficient...

RPKI, ROA, and BGPSEC can't help....



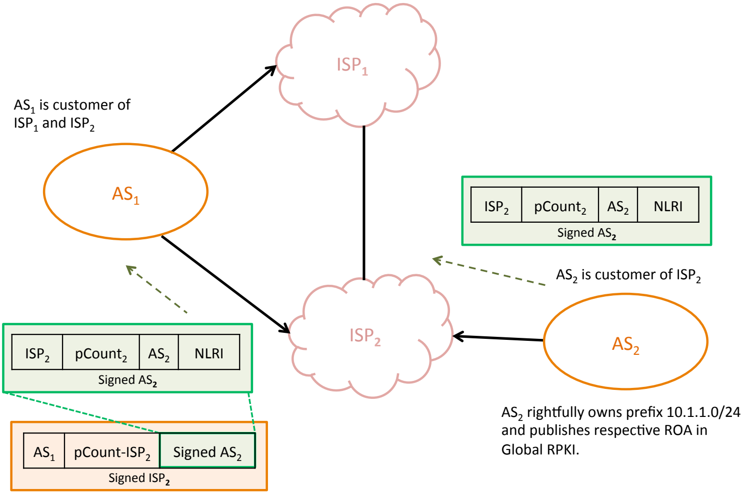
ISP$_1$
AS$_1$ is customer of ISP$_1$ and ISP$_2$
AS$_1$
ISP$_2$
AS$_2$ is customer of ISP$_2$
AS$_2$

ISP$_2$	pCount$_2$	AS$_2$	NLRI

Signed AS$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

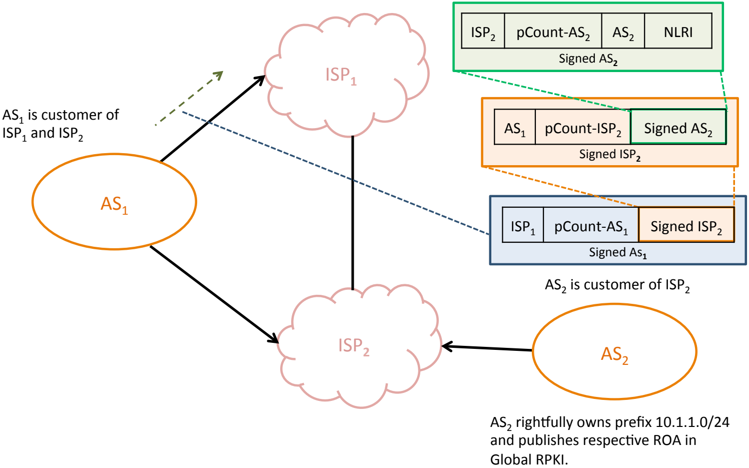
RPKI, ROA, and BGPSEC can't help....



ISP_1
AS_1 is customer of ISP_1 and ISP_2
AS_1
ISP_2 | $pCount_2$ | AS_2 | NLRI
Signed AS_2
AS_2 is customer of ISP_2
ISP_2
AS_2
ISP_2 | $pCount_2$ | AS_2 | NLRI
Signed AS_2
AS_1 | pCount-ISP_2 | Signed AS_2
Signed ISP_2

AS_2 rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

RPKI, ROA, and BGPSEC can't help....



ISP$_2$	pCount-AS$_2$	AS$_2$	NLRI

Signed AS$_2$

AS$_1$	pCount-ISP$_2$	Signed AS$_2$

Signed ISP$_2$

ISP$_1$	pCount-AS$_1$	Signed ISP$_2$

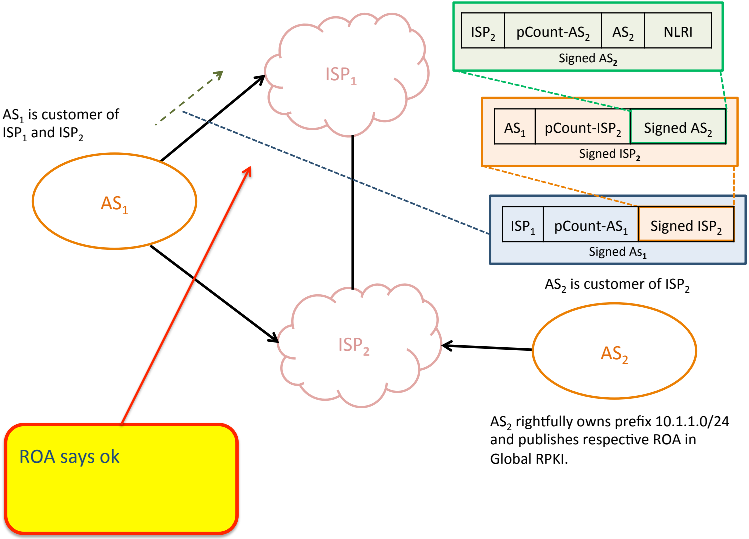
Signed As$_1$

AS$_1$ is customer of ISP$_1$ and ISP$_2$

AS$_2$ is customer of ISP$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

RPKI, ROA, and BGPSEC can't help....



ISP_2 | pCount-AS_2 | AS_2 | NLRI
Signed AS_2
AS_1 | pCount-ISP_2 | Signed AS_2
Signed ISP_2
ISP_1 | pCount-AS_1 | Signed ISP_2
Signed As_1
ISP_1
ISP_2
AS_1
AS_2

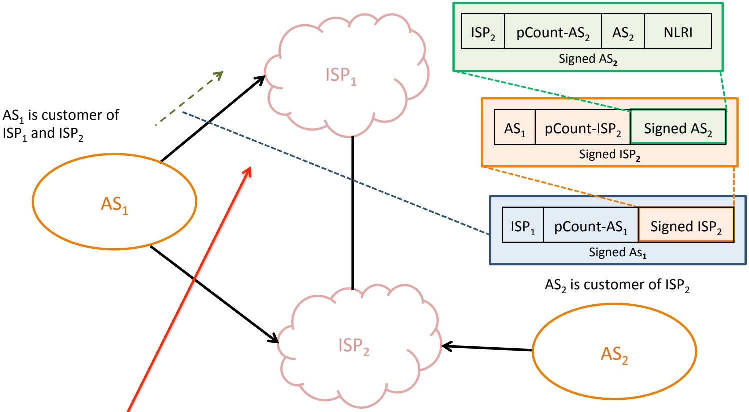
AS_1 is customer of ISP_1 and ISP_2

AS_2 is customer of ISP_2

AS_2 rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

ROA says ok

RPKI, ROA, and BGPSEC can't help....

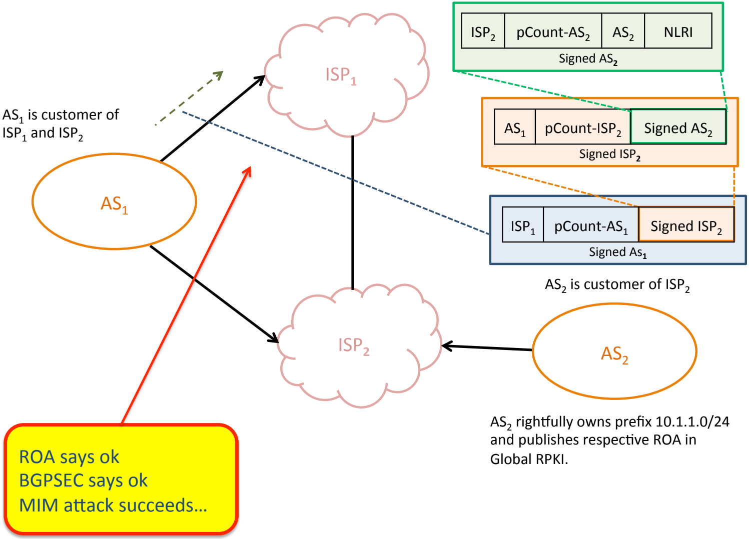


ISP$_2$ | pCount-AS$_2$ | AS$_2$ | NLRI
Signed AS$_2$
AS$_1$ | pCount-ISP$_2$ | Signed AS$_2$
Signed ISP$_2$
ISP$_1$ | pCount-AS$_1$ | Signed ISP$_2$
Signed As$_1$
ISP$_1$
AS$_1$ is customer of ISP$_1$ and ISP$_2$
AS$_1$
ISP$_2$
AS$_2$ is customer of ISP$_2$
AS$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

ROA says ok
BGPSEC says ok

RPKI, ROA, and BGPSEC can't help....


ISP$_2$ | pCount-AS$_2$ | AS$_2$ | NLRI
Signed AS$_2$
AS$_1$ | pCount-ISP$_2$ | Signed AS$_2$
Signed ISP$_2$
ISP$_1$ | pCount-AS$_1$ | Signed ISP$_2$
Signed As$_1$
ISP$_1$
ISP$_2$
AS$_1$
AS$_2$

AS$_1$ is customer of ISP$_1$ and ISP$_2$

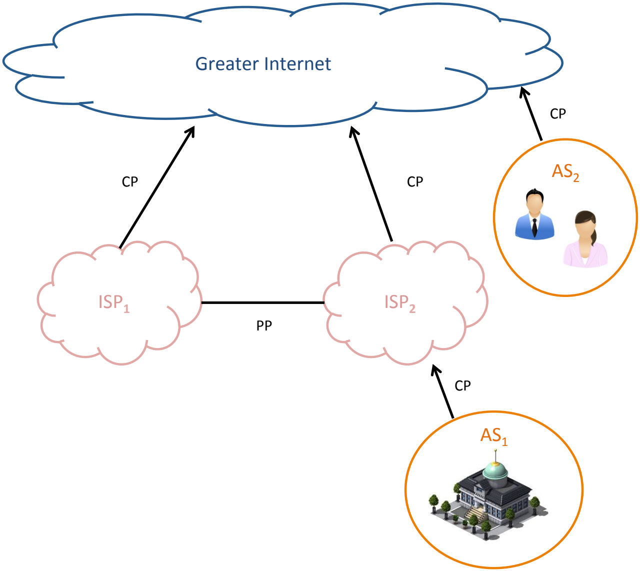
AS$_2$ is customer of ISP$_2$

AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

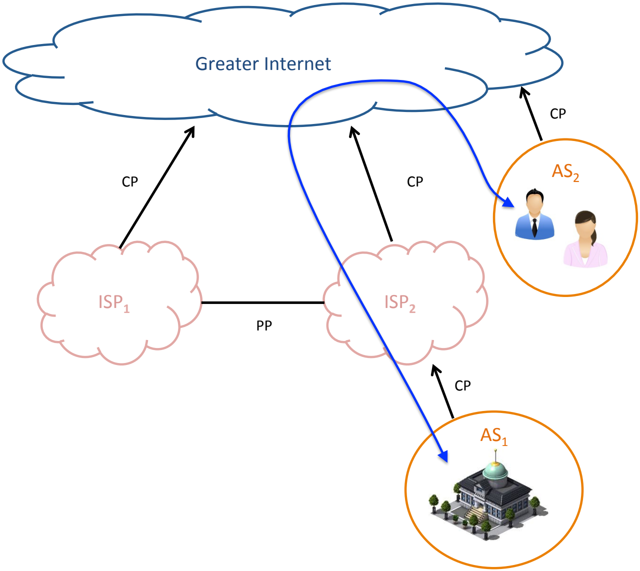
ROA says ok
BGPSEC says ok
MIM attack succeeds...

Route Leaks: Peer Case

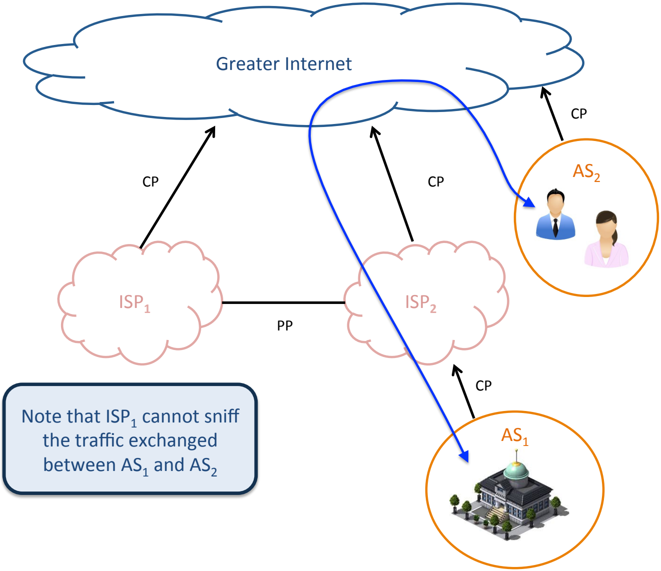
Route Leaks: Peer Case



Route Leaks: Peer Case

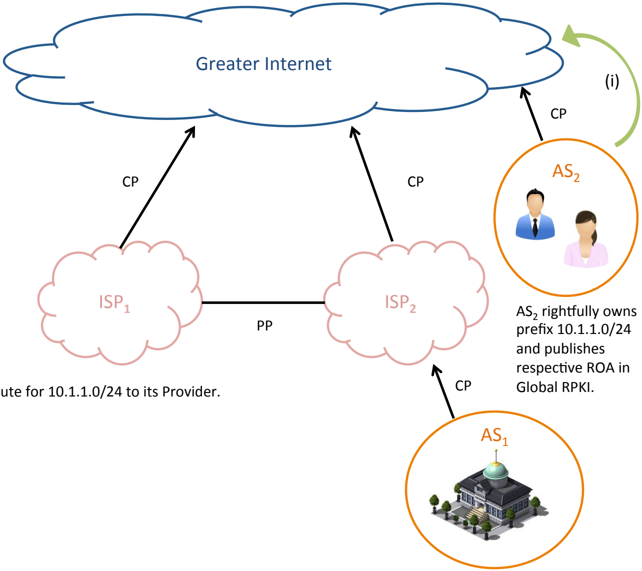


Route Leaks: Peer Case



Note that ISP$_1$ cannot sniff the traffic exchanged between AS$_1$ and AS$_2$

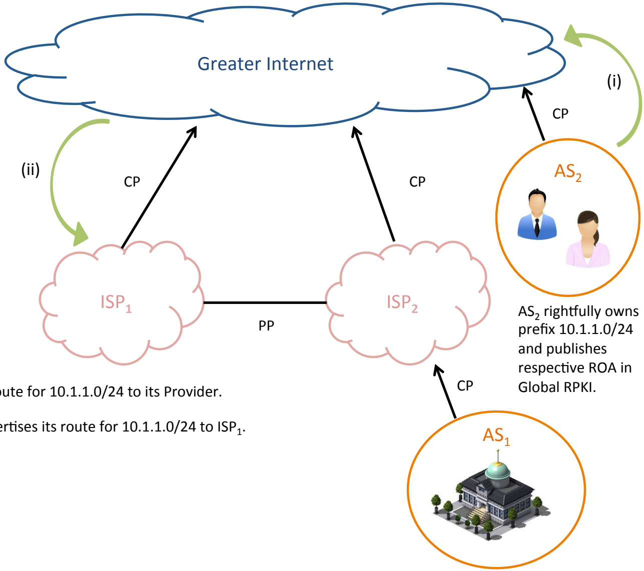
Route Leaks: Peer Case



AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

(i) AS$_2$ advertises its route for 10.1.1.0/24 to its Provider.

Route Leaks: Peer Case

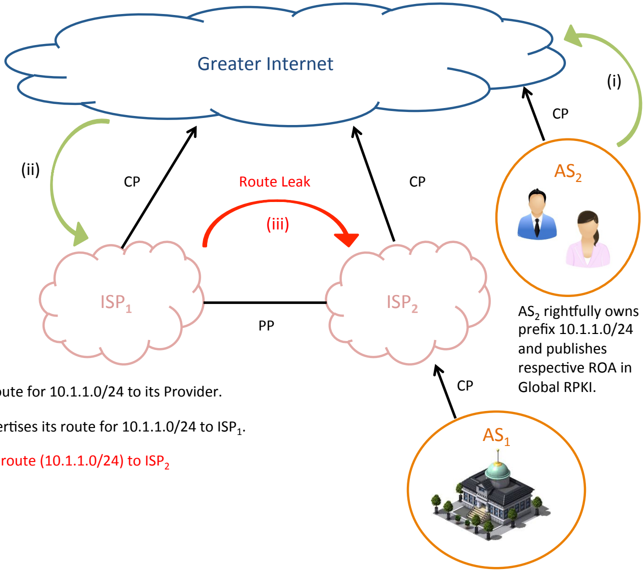


AS_2 rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

(i) AS_2 advertises its route for 10.1.1.0/24 to its Provider.

(ii) ISP_1's provider advertises its route for 10.1.1.0/24 to ISP_1.

Route Leaks: Peer Case



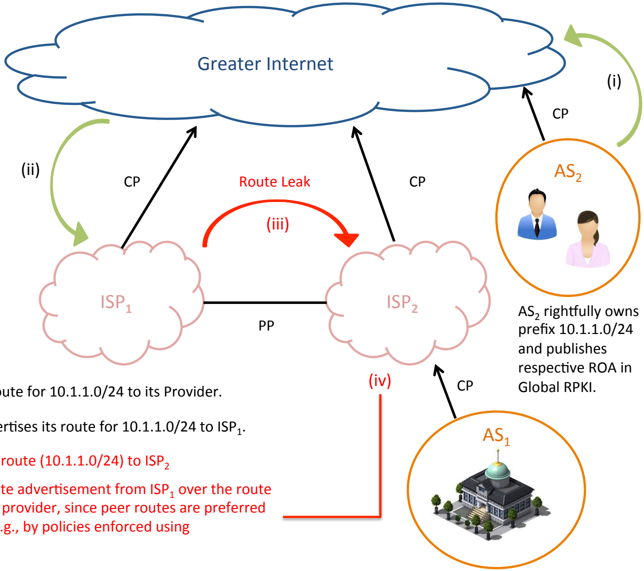
AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

(i) AS$_2$ advertises its route for 10.1.1.0/24 to its Provider.

(ii) ISP$_1$'s provider advertises its route for 10.1.1.0/24 to ISP$_1$.

(iii) ISP$_1$ distributes the route (10.1.1.0/24) to ISP$_2$

Route Leaks: Peer Case



AS$_2$ rightfully owns prefix 10.1.1.0/24 and publishes respective ROA in Global RPKI.

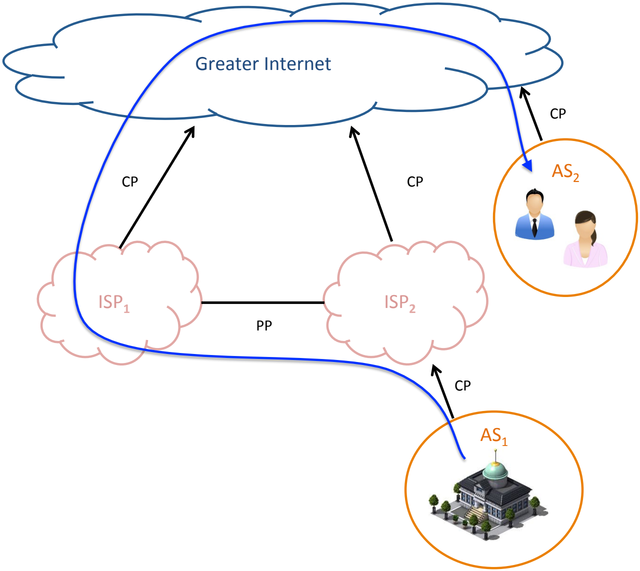
(i) AS$_2$ advertises its route for 10.1.1.0/24 to its Provider.

(ii) ISP$_1$'s provider advertises its route for 10.1.1.0/24 to ISP$_1$.

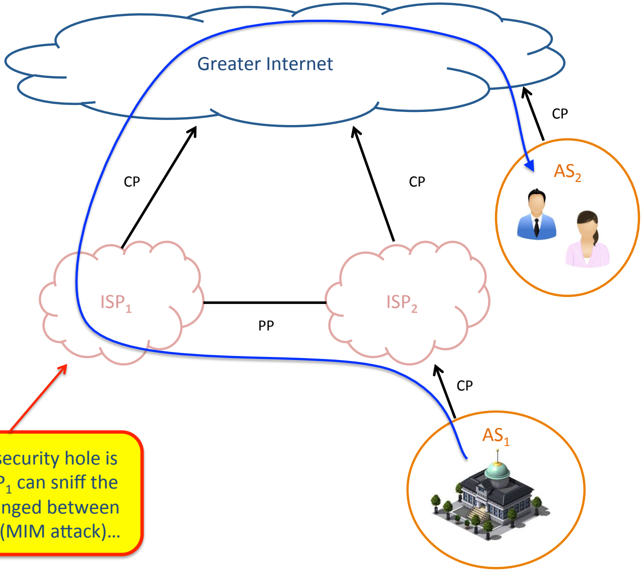
(iii) ISP$_1$ distributes the route (10.1.1.0/24) to ISP$_2$

(iv) ISP$_2$ prefers the route advertisement from ISP$_1$ over the route advertisement from its provider, since peer routes are preferred over provider routes (e.g., by policies enforced using communities).

Route Leaks: Peer Case

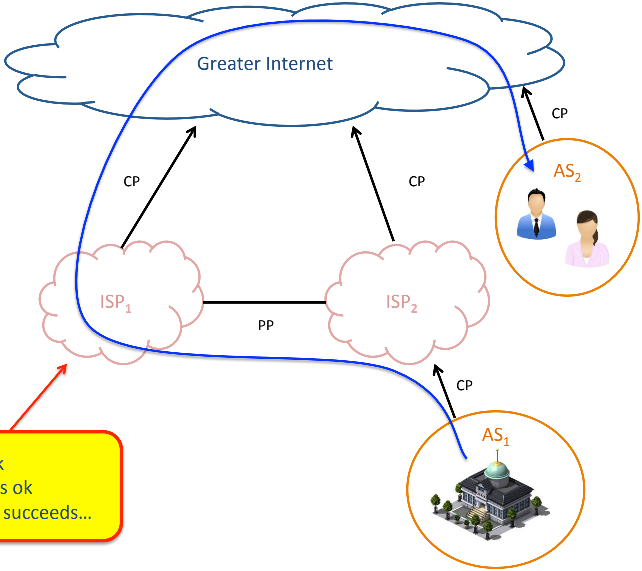


Route Leaks: Peer Case



Again…the security hole is that now ISP$_1$ can sniff the traffic exchanged between AS$_1$ and AS$_2$ (MIM attack)…

Route Leaks: Peer Case



ROA says ok
BGPSEC says ok
MIM attack succeeds...

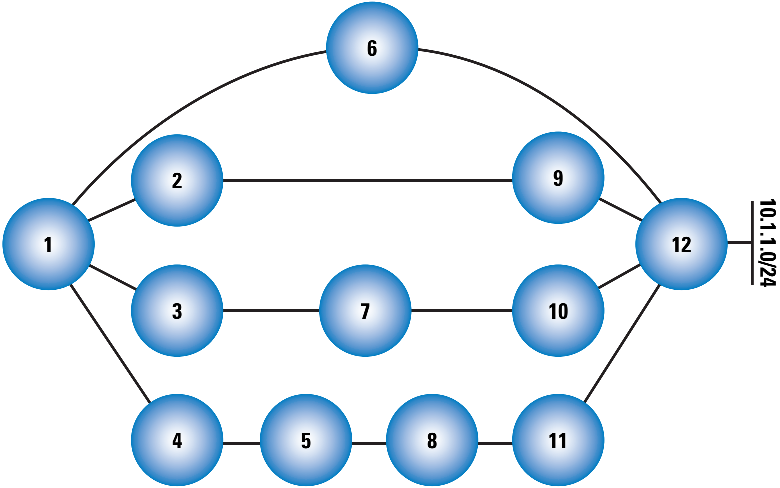
BGPSEC: Replay Attacks

- BGPSEC also attempts to “... prevent someone that you used to do business with from replaying stale information to keep attracting your traffic." (Matt Lepinski).
  - An expire-time mechanism to limit replay attacks
  - ....but validity periods should be long, since business relationships don’t change overnight...
  - ...this is still an open issue ..... for instance .... consider the case when my peer is filerting withdrawals from a third-party AS ...

Outline

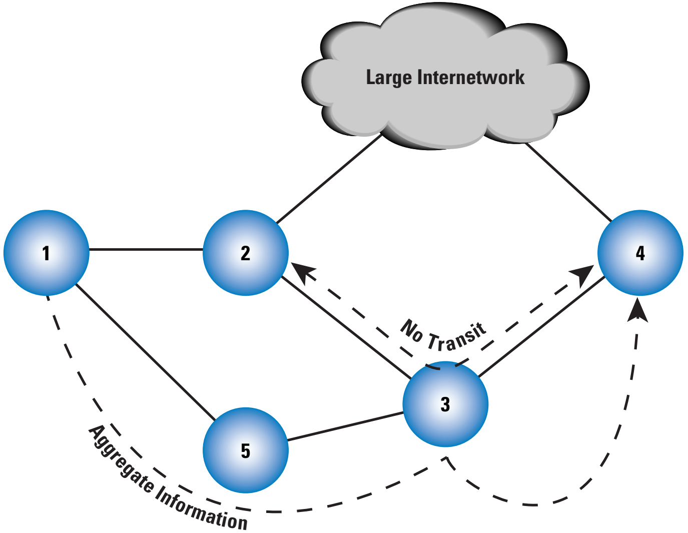
1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. **Overlay security, Bloom filters, etc.**
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Graph Overlays (R. White)



- Source: R. White, “Graph Overlays on Path Vector: A Possible Next Step in BGP,” in Internet Protocol Journal, Vol. 8, no. 2, June 2005.

Graph Overlays (R. White) (cont.)



- Source: R. White, “Graph Overlays on Path Vector: A Possible Next Step in BGP,” in Internet Protocol Journal, Vol. 8, no. 2, June 2005.

Overlays for IP Traceback

- Attackers have today a virtual guarantee of anonymity ...
- This AS-level IP-traceback system contrasts with previous works, since it requires neither a priori knowledge of the topology nor full deployments.
- A new IP-traceback BGP community attribute (a BGP extension) that enables information to be passed across ASes that are not necessarily involved in the overlay network.

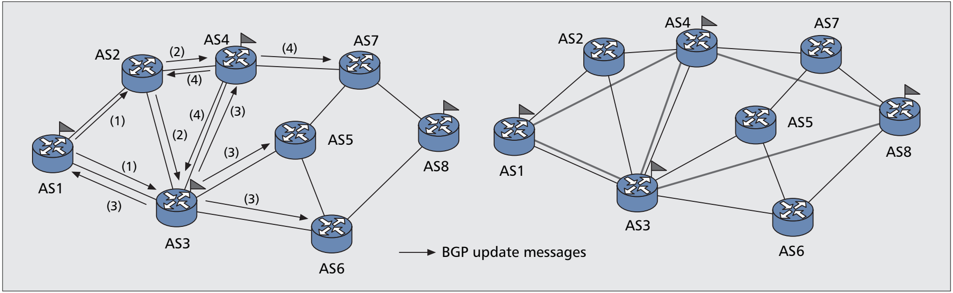
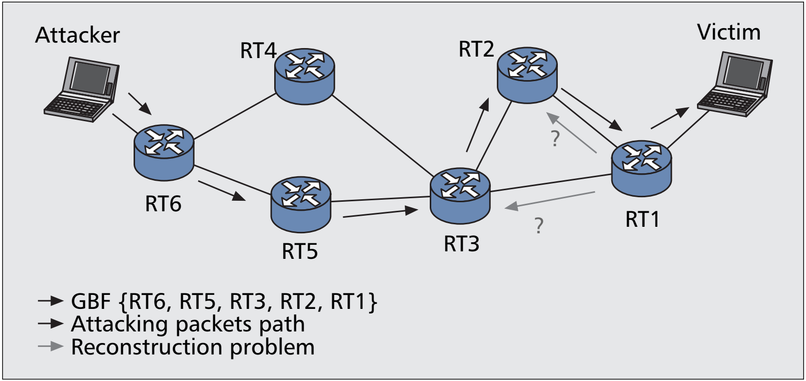


Figure 1. *Building the AS-level overlay network for IP traceback. a) BGP update messages with the IP Traceback Community; b) the resulting AS-level overlay network for IP traceback.*

- Source: André Castelucio et al., “An AS-Level Overlay Network for IP Traceback,” IEEE Network, January/February 2009.

Overlays for IP Traceback (cont.)

- The traceback system operates on border routers of ASes, and its main goal is the identification (at least partially) of the route(s) of attacker packets.
- The strength of BGP communities is that they represent optional transitive attributes in BGP.



■ **Figure 2.** *Illustration of the packet marking problem.*

- Source: André Castelucio et al., “An AS-Level Overlay Network for IP Traceback,” IEEE Network, January/February 2009.

Overlays for IP Traceback (cont.)

- A new sequence-marking process to remove ambiguities in the traceback path...

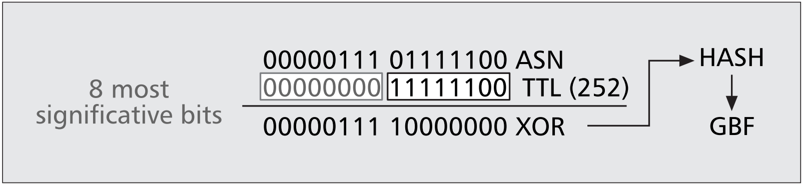


Figure 3. *Illustration of the AS sequence marking process that solves the packet marking problem.*

- Source: André Castelucio et al., “An AS-Level Overlay Network for IP Traceback,” IEEE Network, January/February 2009.

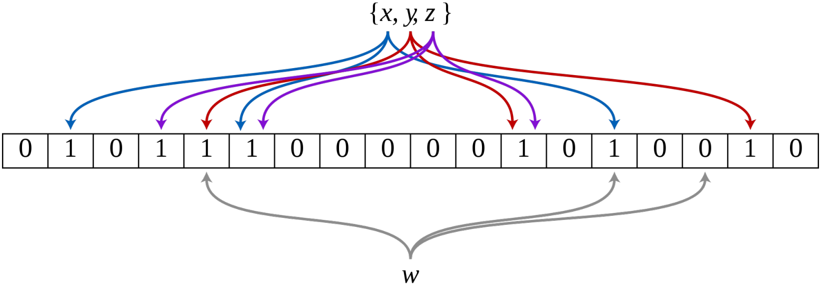
Bloom Filters

Bloom Filters

- A Bloom filter is a “space-efficient" probabilistic data structure that is used to test whether an element is a member of a set .... i.e., it supports membership queries (e.g., queries that ask: **“Is element X in set Y?”**).
- **False positives are possible** — Indicating that a given condition has been fulfilled, when it actually has not (queries might incorrectly recognize an element as member of the set, i.e., an element is indicated as member when it is actually not).
- **False negatives are not possible** — That is, a query returns either “inside the set” (which may be wrong) or “definitely not in set”.
- Elements can be added to the set, but not removed (though this can be addressed with a counting filter).
- In a set A of n elements, the more elements that are added to the set, the larger the probability of false positives....

Bloom Filters (cont.)

- In a set A of n elements, Bloom filters describe membership information of A using a bit vector V of length m. For this, k hash functions, $h_1, h_2, \ldots, h_k$, with $h_i : X \to \{1, \ldots, m\}$ are used as described below:



0	1	0	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0

- "An example of a Bloom filter representing the set {x, y, z}. The colored arrows show the positions in the bit array that each set element is mapped to. The element w is not in the set x, y, z, because it hashes to one bit-array position containing 0. In this example, $m = 18$ and $k = 3$.

Bloom Filters (cont.)

False Positives

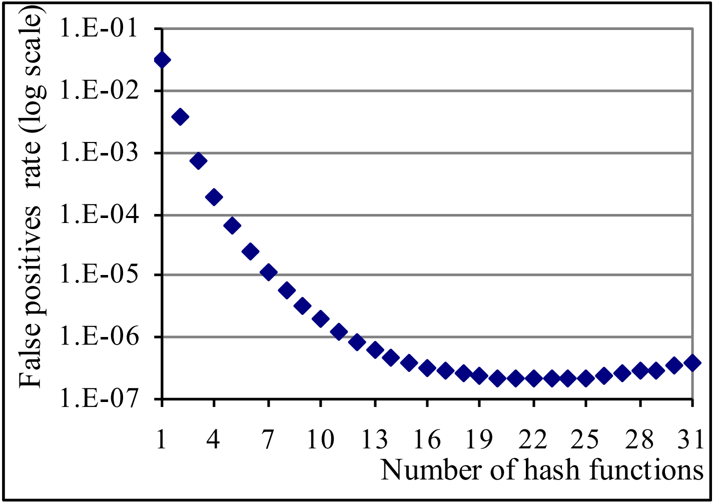
- The probability of a false positive, i.e., the probability that all k bits have been previously set to 1, is:

$$P_{error} = \left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^{k} \approx \left(1 - e^{-\frac{kn}{m}}\right)^{k}$$

- By minimizing, we can obtain the optimum value of k:

$$k_{opt} = \frac{m}{n} Ln(2)$$

Bloom Filters (cont.)



- Source: M. Ripeanu et al., “Bloom Filters — Short Tutorial” .

Overlays for IP Traceback (cont.)

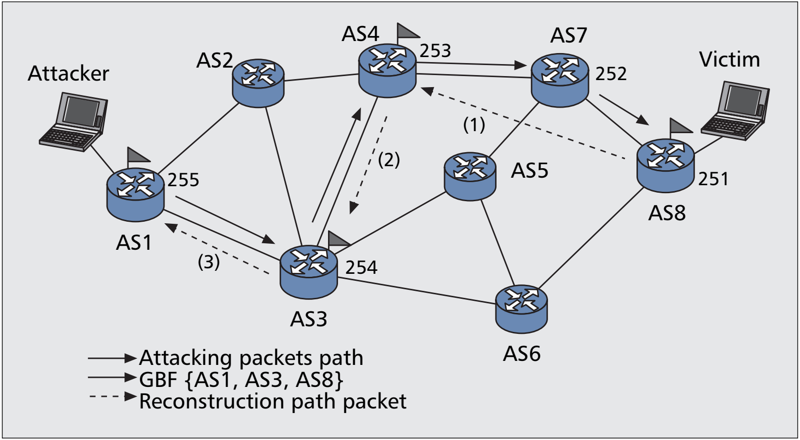


Figure 4. *IP traceback illustration.*

- Source: André Castelucio et al., "An AS-Level Overlay Network for IP Traceback," IEEE Network, January/February 2009.

IP traceback: reconstructing the path...

- The victim's AS (AS8) starts the traceback by checking its overlay table.
- From this table, it searches for GBF marks belonging to either AS3 or AS4, that is, its neighbors in the overlay network.
- To check where attacker packets come from (AS3 or AS4), AS8 proceeds as follows:
  1. An XOR operation is performed between the ASN of AS3 and the TTL of the packet increased by one (note that TTL at AS8 is 251; then the TTL at AS3 must be 252 or greater).
  2. The result of the XOR is hashed and compared against the GBF of the packet (because there is no match in this example, the procedure is now performed using the ASN of AS4).
  3. The result is negative for both, so the TTL is increased to 253, and the procedure is repeated until a match is found.
  4. In this case, the check is positive for AS4. Therefore, AS8 sends a reconstruction path packet to AS4 (step 1).
  5. AS4 increases the TTL (254) and repeats the process looking for marks belonging to either AS1 or AS3.
  6. The result is positive for AS3 (step 2). Then, the same procedure is repeated at AS3, and it finishes when the reconstruction path packet reaches AS1 (step 3).

IP traceback: reconstructing the path... (cont.)

- The traceback process could actually finish in two ways: when the TTL reaches 256 or when an AS cannot find marks of any other neighbor in the GBF, thus concluding it is the closest AS to the source of the attack.

Strategic versus Random Placement

- Strategic placement: the most connected ASs have a traceback system deployed first.

Overlays for IP Traceback (cont.)

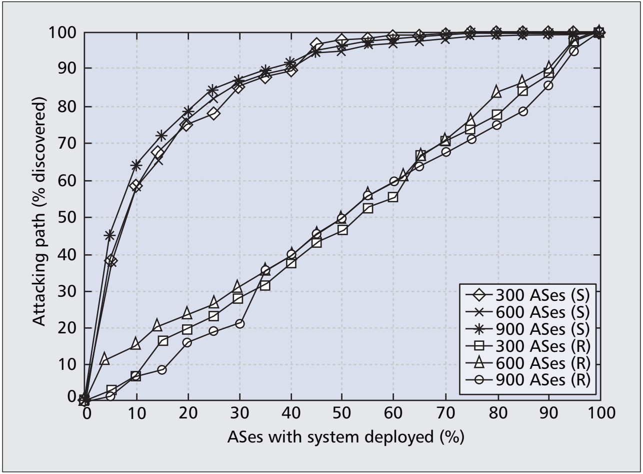
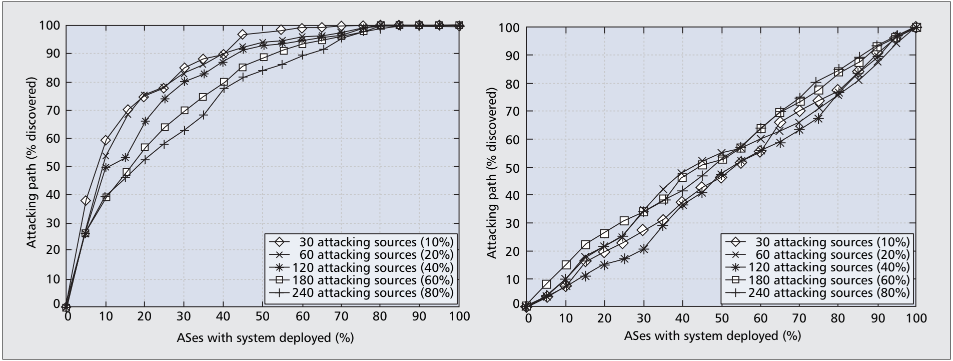


Figure 5. *Efficiency in discovering the attacking path with strategic (S) and random (R) placements.*

- Source: André Castelucio et al., “An AS-Level Overlay Network for IP Traceback,” IEEE Network, January/February 2009.

Overlays for IP Traceback (cont.)



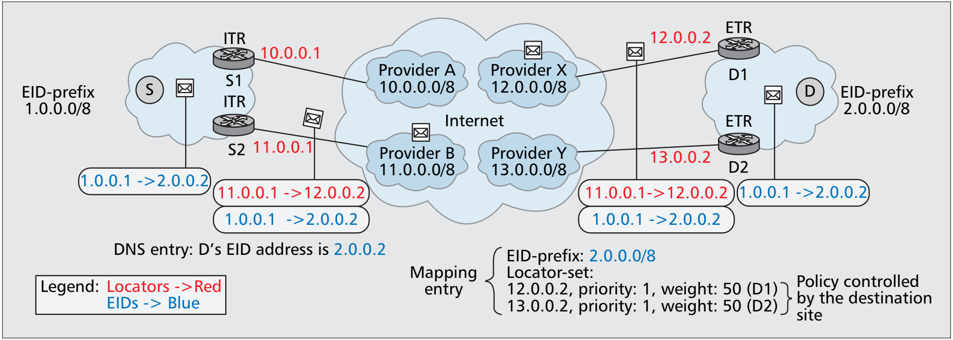
■ **Figure 6.** *Efficiency in discovering the attacking path with an increasing number of attacking sources. a) Strategic placement; b) Random placement.*

- Source: André Castelucio et al., “An AS-Level Overlay Network for IP Traceback,” IEEE Network, January/February 2009.

Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. **LISP: its initial goals, caches, mapping (DDT), etc.**
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

LISP



■ **Figure 3.** *The basics of LISP.*

- Source: M. Yannuzzi, X. Masip-Bruin, E. Grampin, R. Gagliano, A. Castro, M. German, “Managing Interdomain Traffic in Latin America: A New Perspective based on LISP," in IEEE Communications Magazine, Vol. 47, issue 7, pp. 40–48, July 2009.

LISP: Shrinking the FIBs

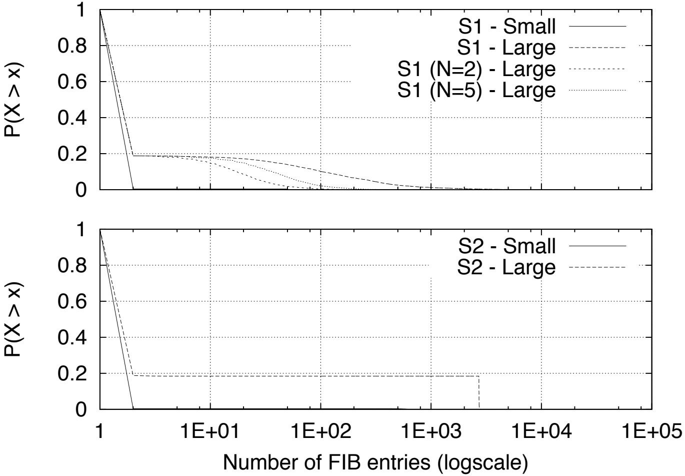


Figure 5: Number of per domain installed FIB entries.

- Source: B. Quoitin et al., “Evaluating the Benefits of the Locator/Identifier Separation," ACM MobiArch, Kyoto, Japan, August 2007.

LISP: Traffic Engineering Opportunities...

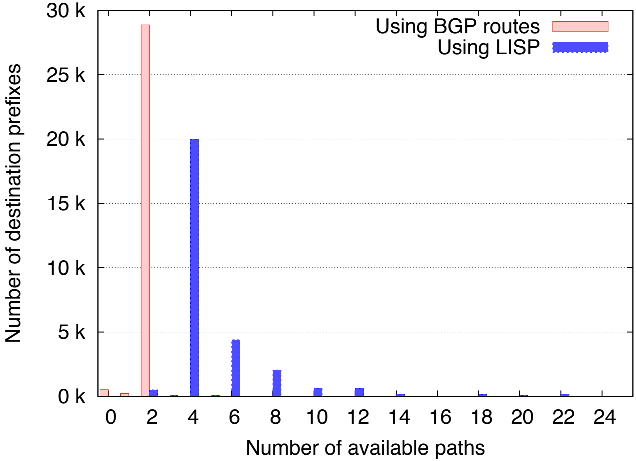
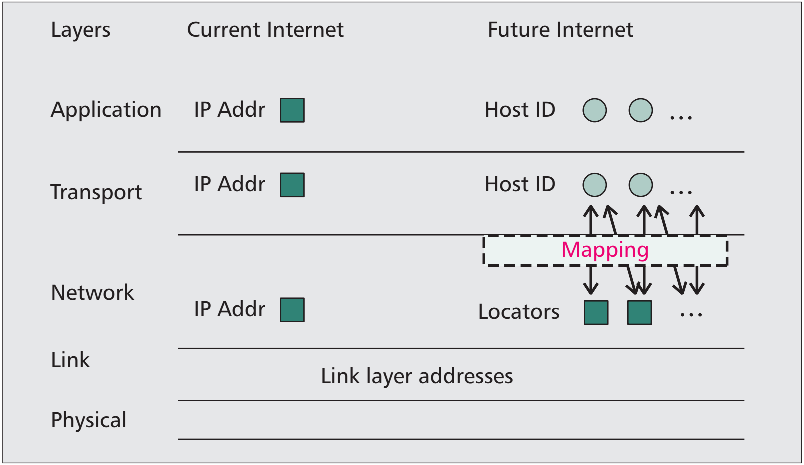


Figure 6: Path diversity when multihoming to RouteViews peers.

- Source: B. Quoitin et al., “Evaluating the Benefits of the Locator/Identifier Separation," ACM MobiArch, Kyoto, Japan, August 2007.

LISP (cont.)



Layers	Current Internet	Future Internet
Application	IP Addr	Host ID …
Transport	IP Addr	Host ID …
		Mapping
Network	IP Addr	Locators …
Link	Link layer addresses	
Physical		

Figure 1. *Host IDs and locators in the current and future Internet protocol stacks.*

- Source: V. P. Kafle ate al., “Introducing Multi-ID and Multi-Locator Into Network Architecture," in IEEE Communications Magazine, March 2012.

LISP (cont.)

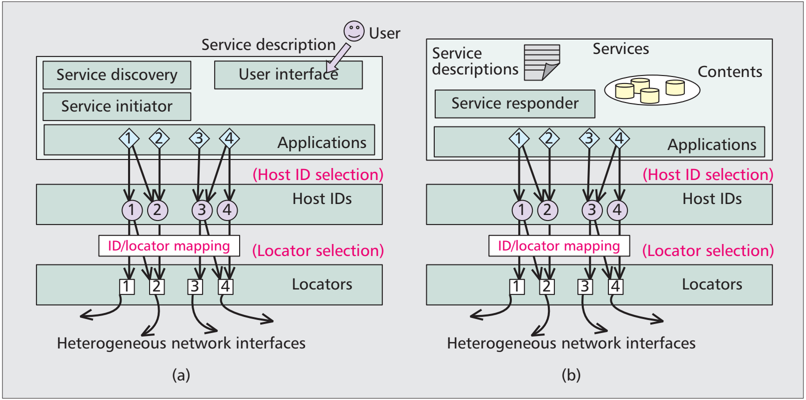


Figure 2. *a) Client host; b) server host functions in multi-ID and multi-locator architecture.*

- Source: V. P. Kafle ate al., “Introducing Multi-ID and Multi-Locator Into Network Architecture," in IEEE Communications Magazine, March 2012.

LISP (cont.)

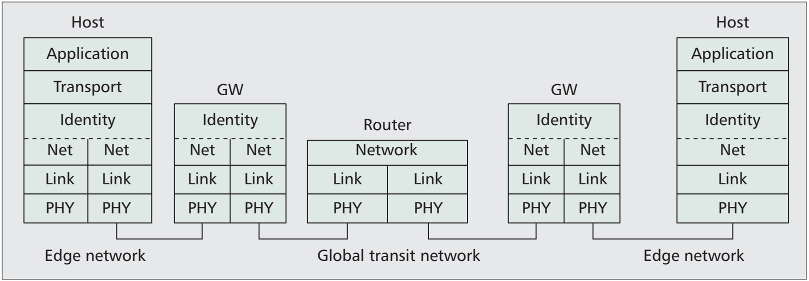


Figure 4. *Protocol stack of ID/locator split architecture.*

- Source: V. P. Kafle ate al., “Introducing Multi-ID and Multi-Locator Into Network Architecture," in IEEE Communications Magazine, March 2012.

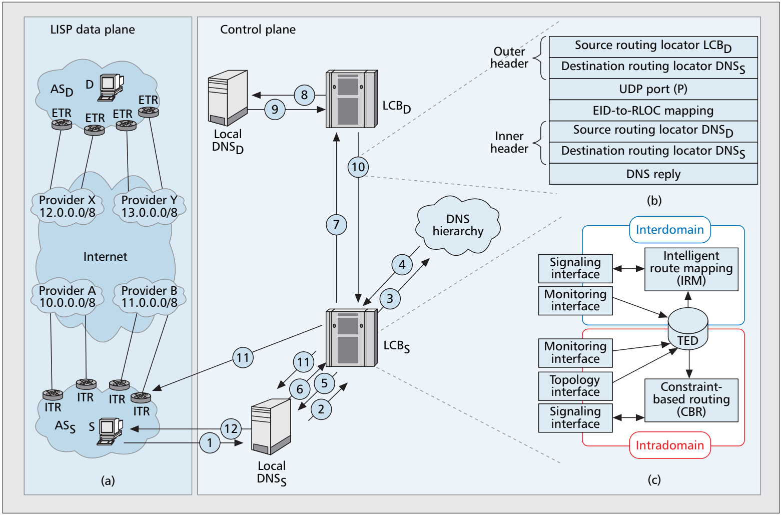
LISP: Main Advantages...

1. It does not introduce major changes to the routing system, and therefore it might be feasible to implement and deploy in the near future.
2. It has the potential to significantly reduce the size of the global routing table (previous works claim around 2 orders of magnitude).
3. The mapping system brings a wide set of TE opportunities, which in principle, can reach a granularity of a /32 prefix without impacting on the size or dynamics of the global routing table.

LISP: Main Weaknesses...

1. Special care must be taken, since LISP might end up moving the scalability issues from the global routing table to the global mapping system.
2. Dealing with the initial packets sent from a source EID to a destination EID at the ITR during the EID-to-RLOC mapping resolution (buffering, dropping, caching, mix of control and data planes, ...).
3. LISP might considerably increase the latency to start up the communication between end systems....
4. For each traffic flow from *S* to *D*, the egress ITR is also used as the local ETR for the packets sent from *D* to *S*. This is to avoid a two-way mapping resolution. Clearly, this introduces a limitation in terms of inbound TE, given that outbound and inbound traffic management policies typically do not match.

LISP (cont.)



Source routing locator LCB$_D$
Destination routing locator DNS$_S$
UDP port (P)
EID-to-RLOC mapping
Source routing locator DNS$_D$
Destination routing locator DNS$_S$
DNS reply

Figure 4. *Proposed control plane architecture.*

- Source: M. Yannuzzi, X. Masip-Bruin, E. Grampin, R. Gagliano, A. Castro, M. German, “Managing Interdomain Traffic in Latin America: A New Perspective based on LISP," in IEEE Communications Magazine, Vol. 47, issue 7, pp. 40–48, July 2009.

LISP (cont.)

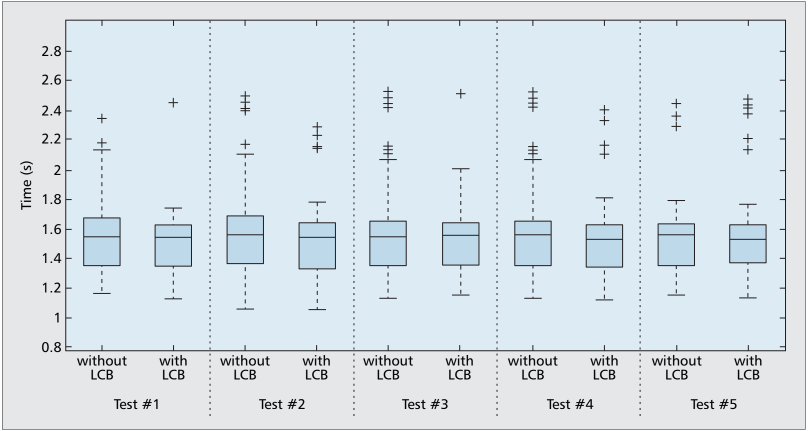


Figure 5. *Five tests showing the time distribution of a set of 1000 DNS lookups over the Internet. Each test corresponds to a round of 200 DNS lookups, 100 without LCBs, and 100 with LCBs.*

- Source: M. Yannuzzi, X. Masip-Bruin, E. Grampin, R. Gagliano, A. Castro, M. German, “Managing Interdomain Traffic in Latin America: A New Perspective based on LISP," in IEEE Communications Magazine, Vol. 47, issue 7, pp. 40–48, July 2009.

OpenLISP

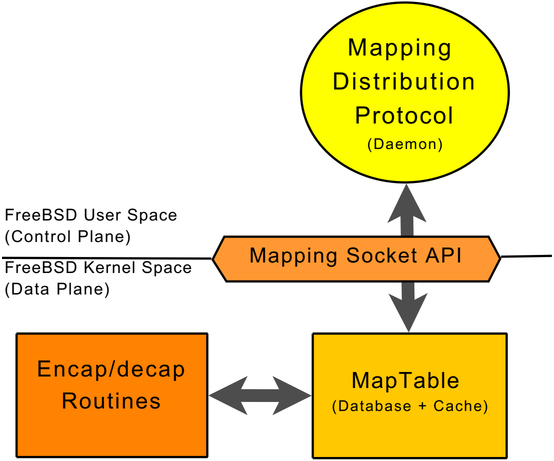


Fig. 2. OpenLISP architecture.

- Source: L. Iannone et al. “Implementing the Locator/ID Separation Protocol: Design and Experience," Computer Networks Journal (Elsevier), Vol. 55, no. 4, pp. 891–1036, March 2011. .

Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. **LISP evolution, LISP mobile (mobile phones become ITRs), etc.**
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. **LISPSEC**
8. Gap between BGPSEC and LISPSEC
9. Opportunities for overlays ...

Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. **Gap between BGPSEC and LISPSEC**
9. Opportunities for overlays ...

Outline

1. Prefix Hijacking: RPKI and ROA
2. Route Hijacking: BGPSEC
3. Route leaks
4. Overlay security, Bloom filters, etc.
5. LISP: its initial goals, caches, mapping (DDT), etc.
6. LISP evolution, LISP mobile (mobile phones become ITRs), etc.
7. LISPSEC
8. Gap between BGPSEC and LISPSEC
9. **Opportunities for overlays ...**

Questions?