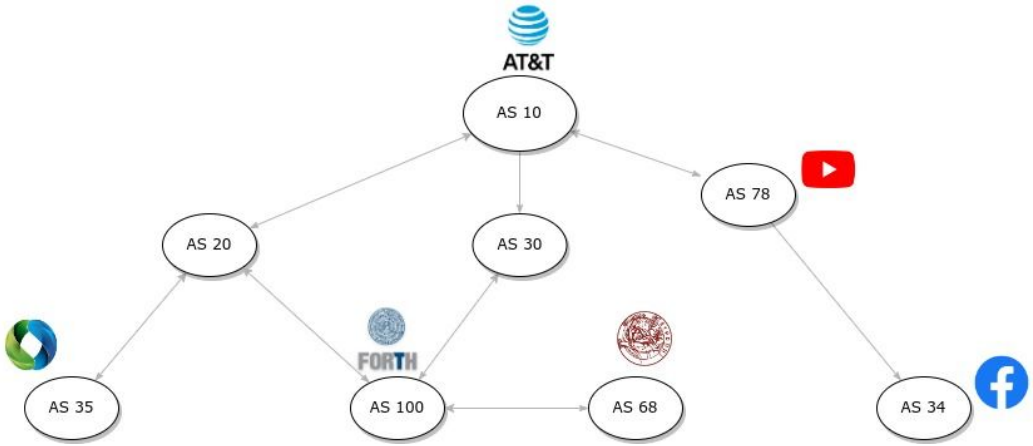
BGP Hijacks

CS-436

What is BGP?

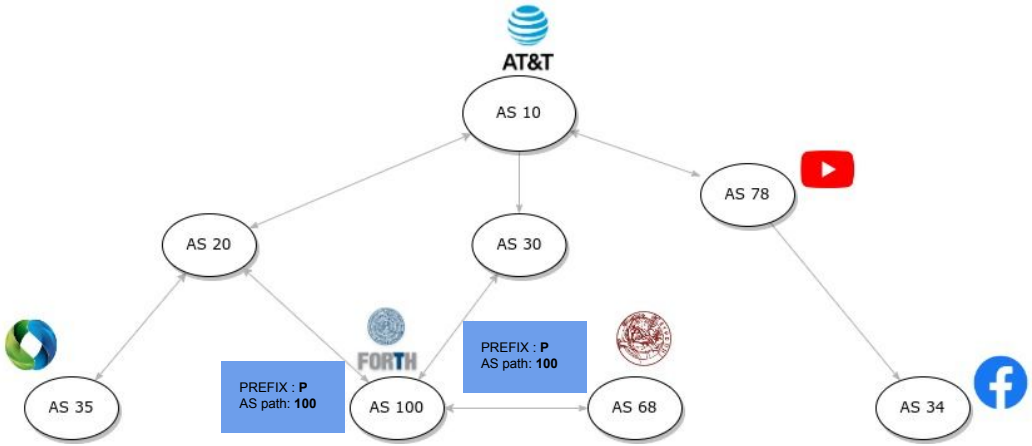
- BGP stands for Border Gateway Protocol
- Is the de facto inter-domain routing protocol
- Enables exchanging routing information between Autonomous Systems (AS)
- Each AS can advertise its IP prefixes



BGP Announcements

One AS can announce its prefixes to BGP

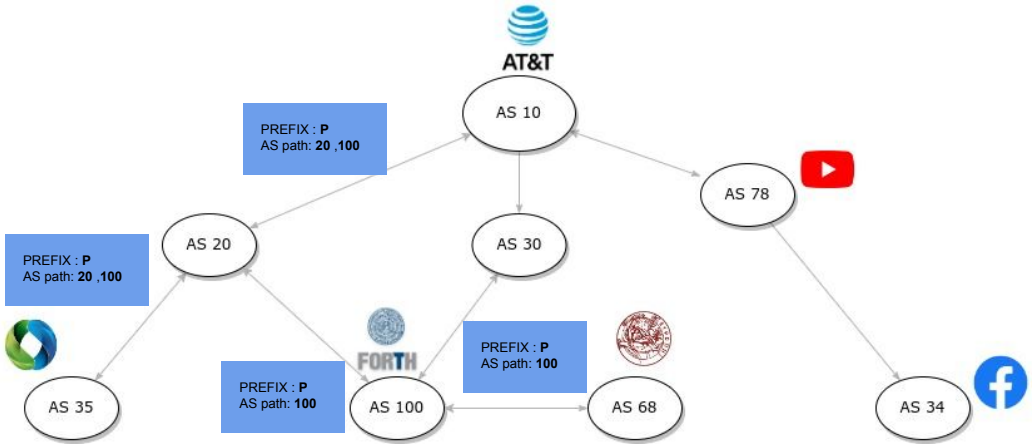
For Example AS 100 advertises its IP prefix to its peers AS 20 and AS 68.



139.91.0.0/16 ->P

BGP Announcements

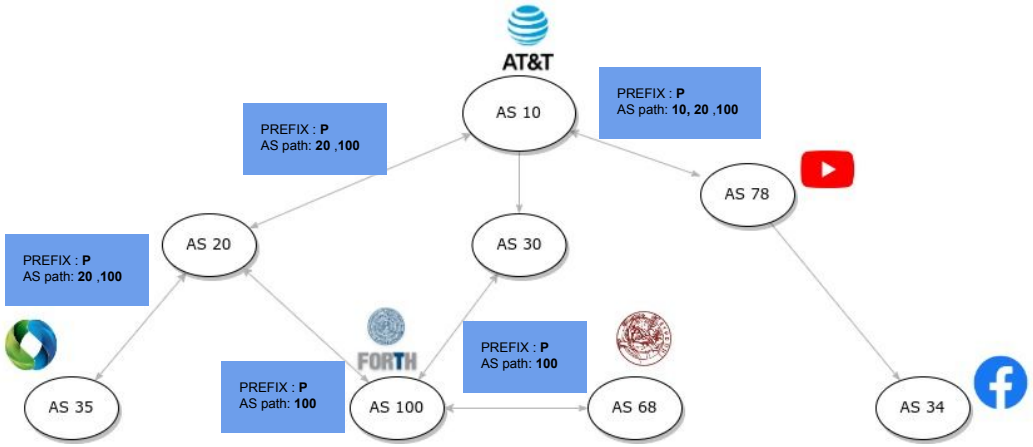
Then AS 20 announces a path to AS 100 to its neighbors with its ASN added to the path.



139.91.0.0/16 ->P

BGP Announcements

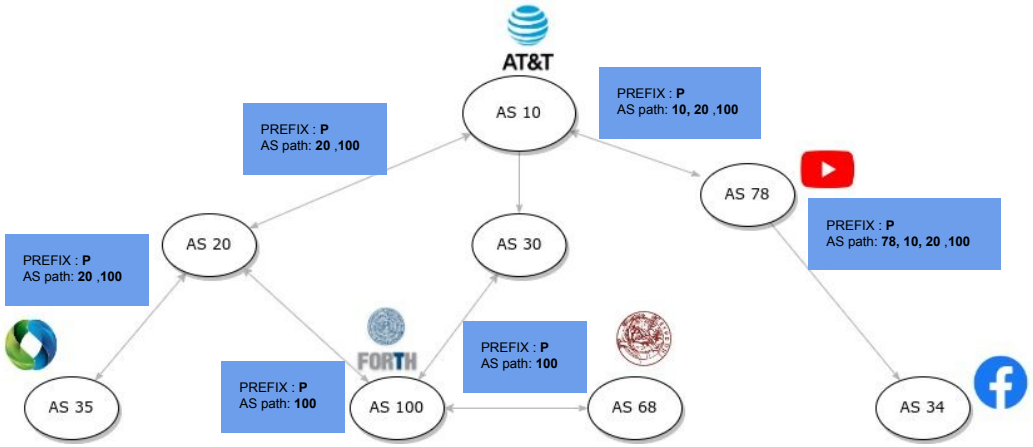
Then AS 20 announces a path to AS 100 to its neighbors with its ASN added to the path.



139.91.0.0/16 ->P

BGP Announcements

After a while all ASes know how to route traffic towards prefix P



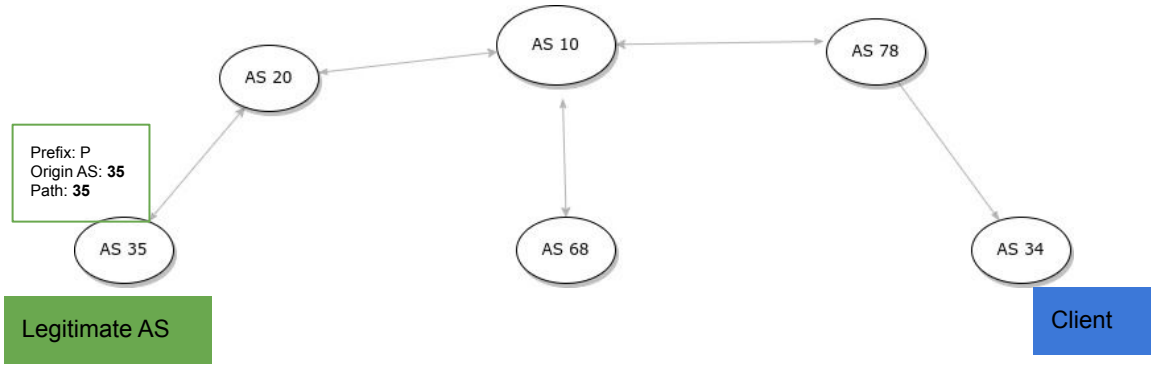
139.91.0.0/16 ->P

What is BGP Hijack?

- BGP hijacking is when attackers maliciously reroute Internet traffic.
- Hijackers accomplish this by falsely announcing ownership of groups of IP addresses that does not belong to them.

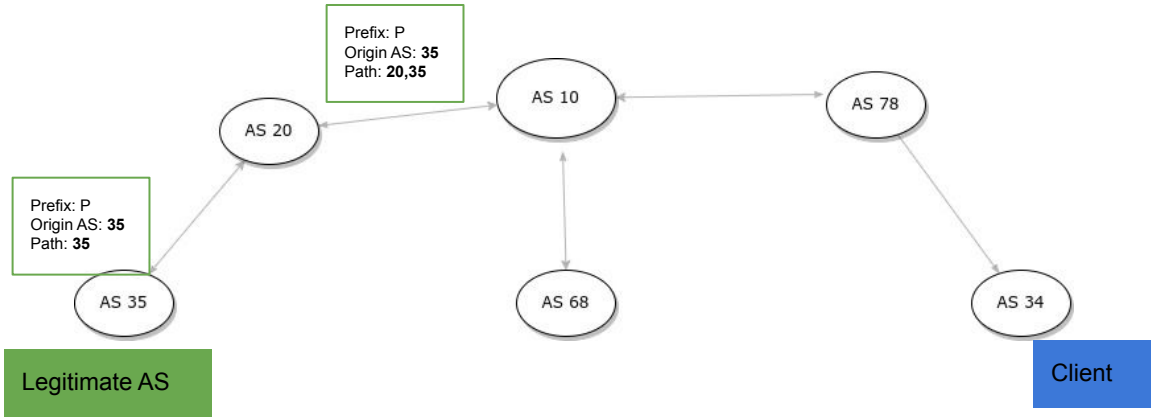
BGP hijacking Example

- AS 35 announces its prefix P



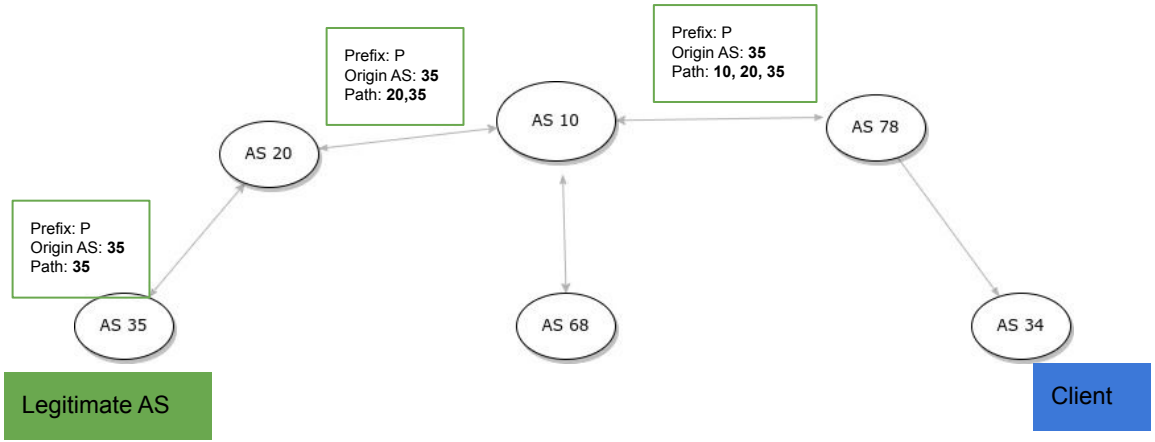
BGP hijacking Example

- AS 35 announces its prefix P



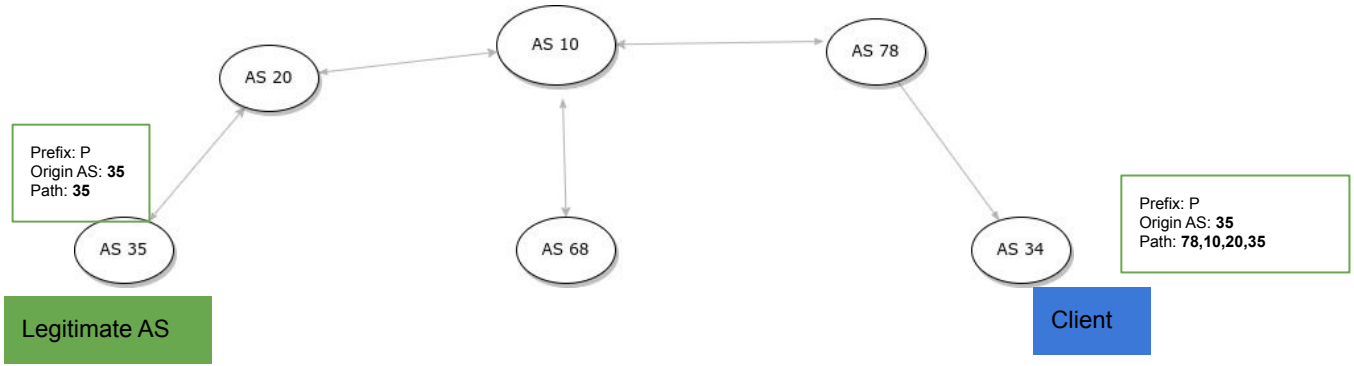
BGP hijacking Example

- AS 35 announces its prefix P



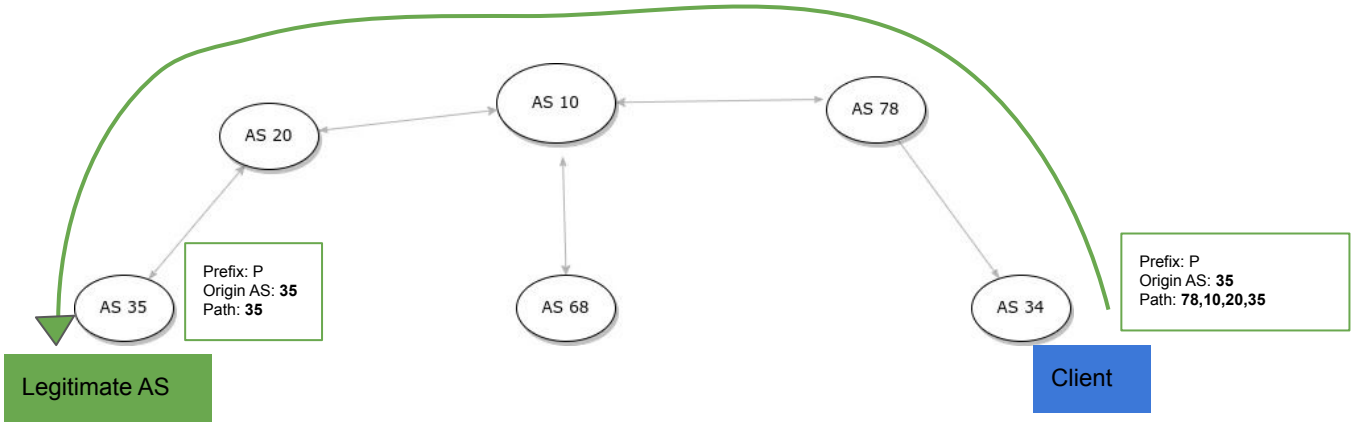
BGP hijacking Example

- AS 34 learns a path towards AS 35 for its prefix P



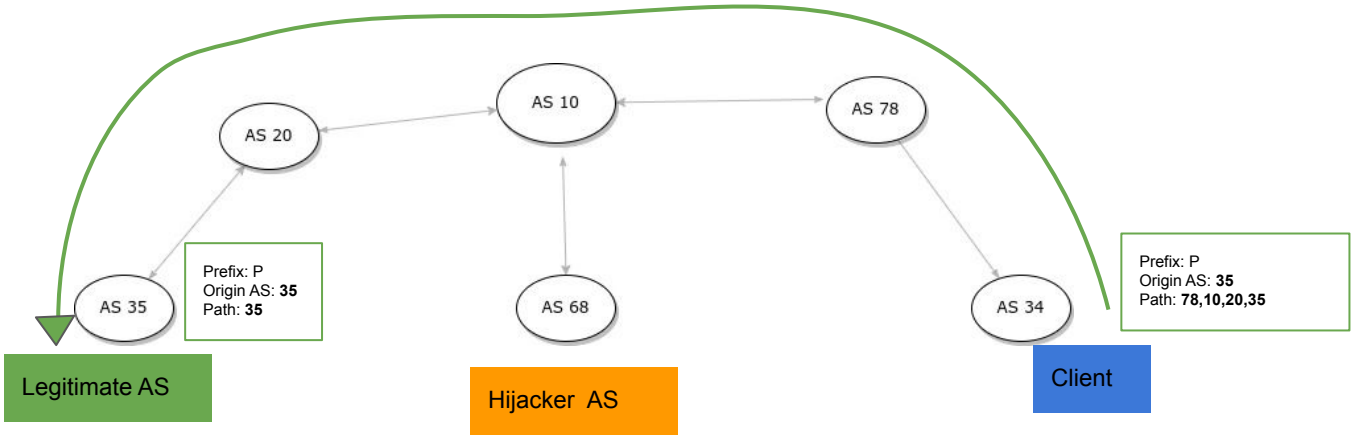
BGP hijacking Example

- AS 34 learns a path towards AS 35 for its prefix P



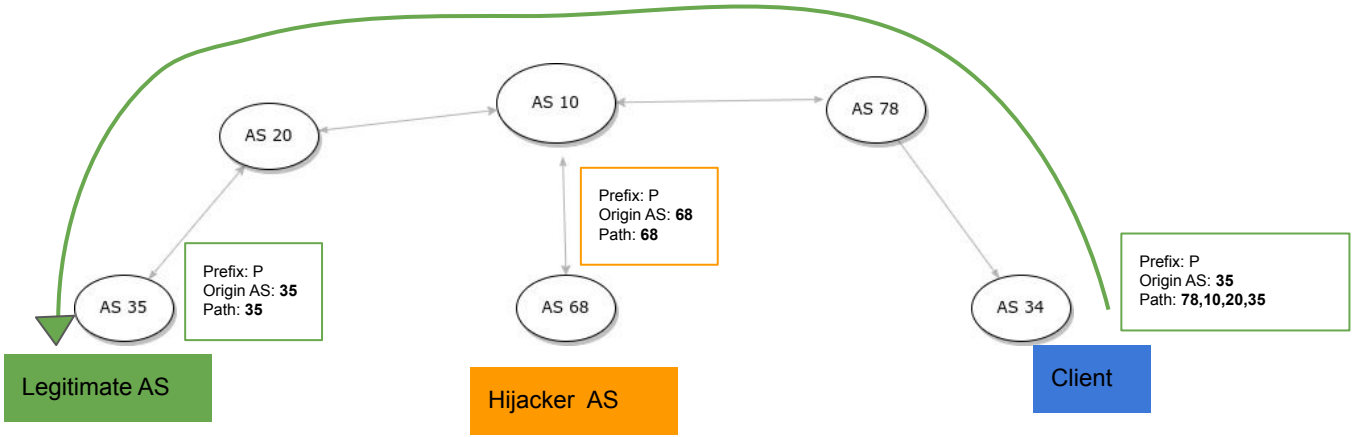
BGP hijacking Example

- But BGP does not have any build in security feature to prevent a malicious AS from announcing one prefix that does not belong to its prefixes !!



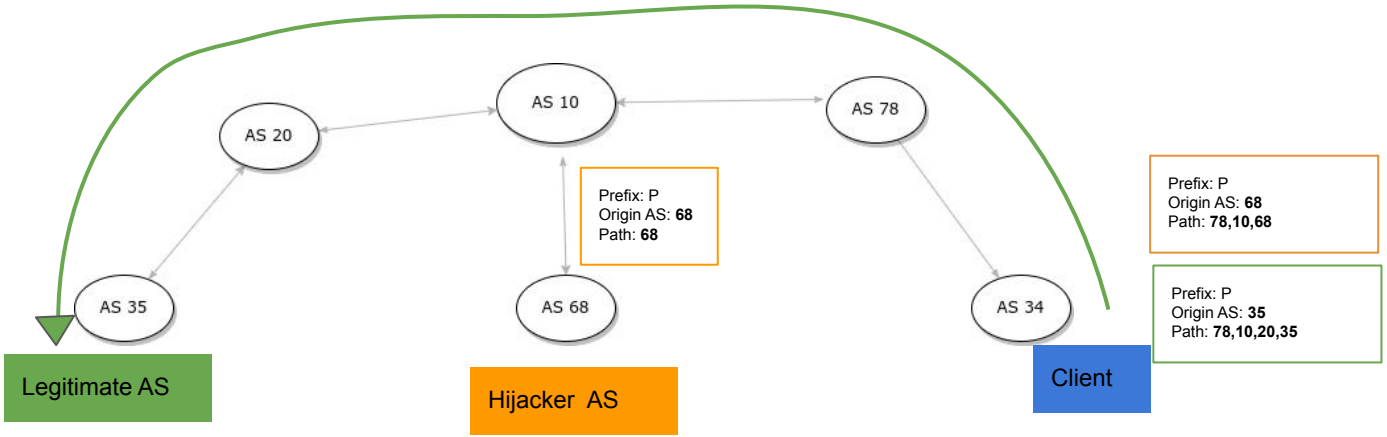
BGP hijacking Example

- So AS 68 can also announce prefix P



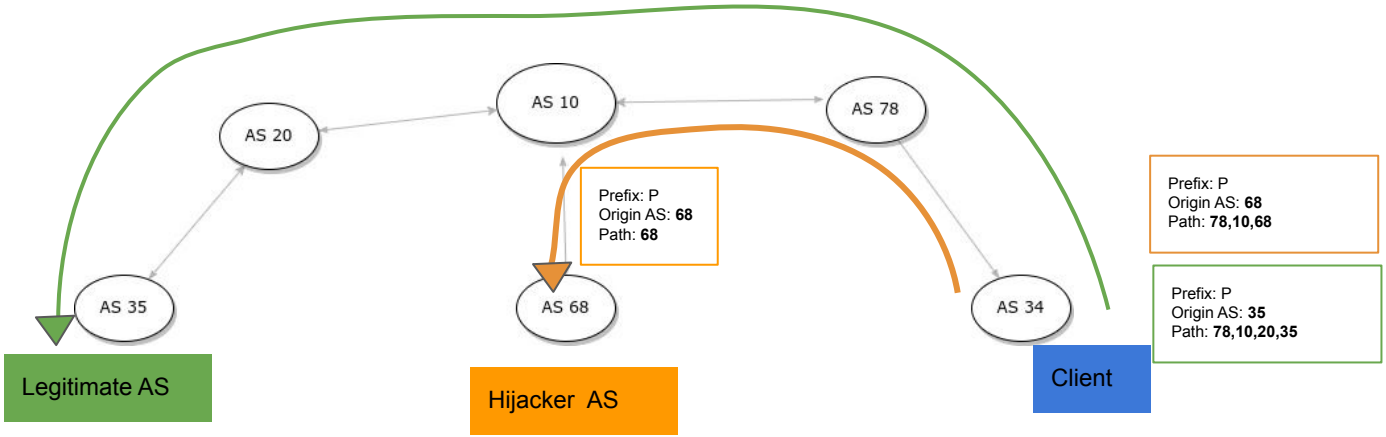
BGP hijacking Example

- AS 34 receives another BGP announcement for prefix P



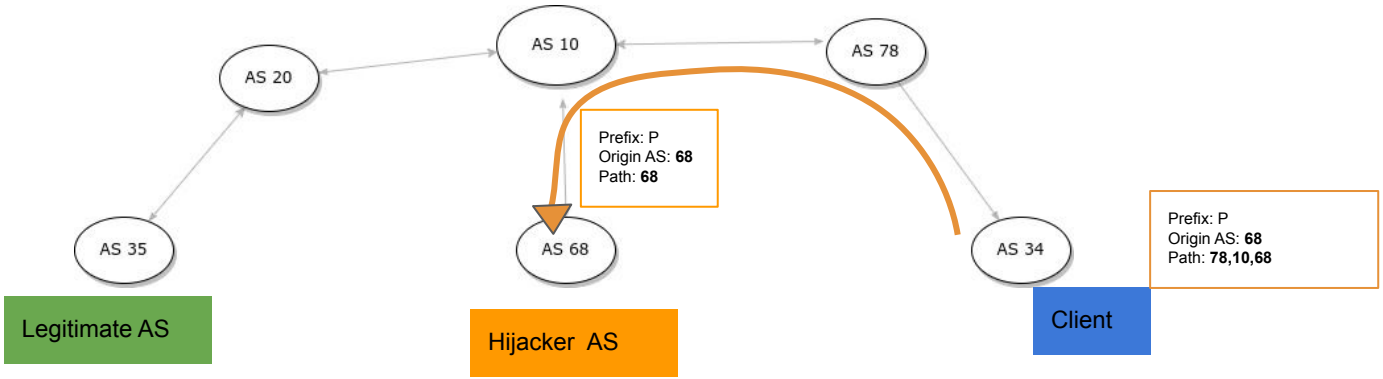
BGP hijacking Example

- Now AS 34 knows another (sorter) path for prefix P
- BGP prefers the “shortest” AS path



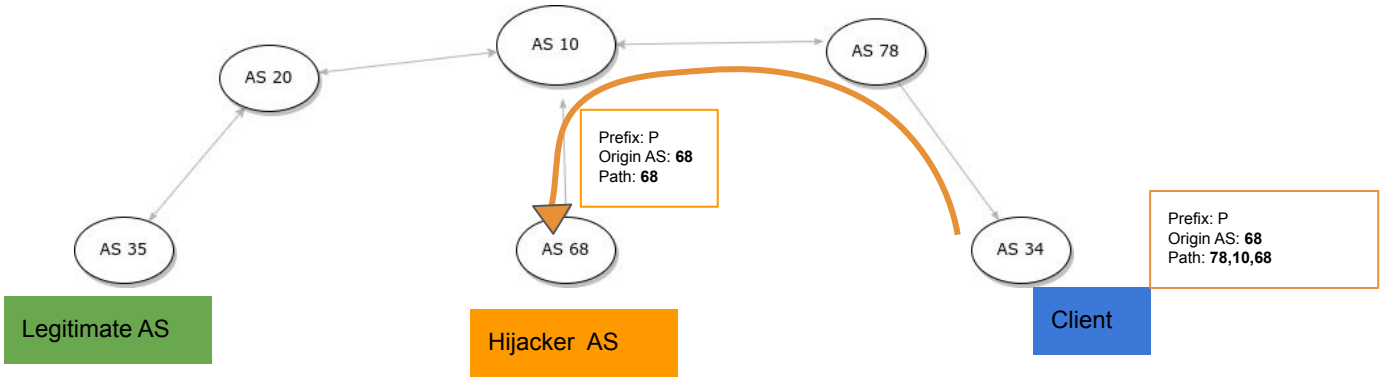
BGP hijacking Example

- The traffic for prefix P ends up to the AS 68



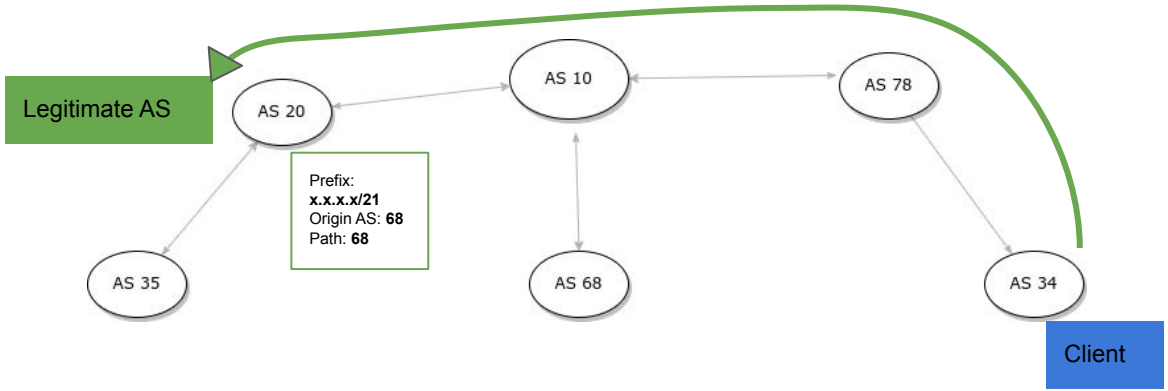
BGP hijacking Example

- This is an example of BGP **prefix Hijacking** or **Origin Hijacking**



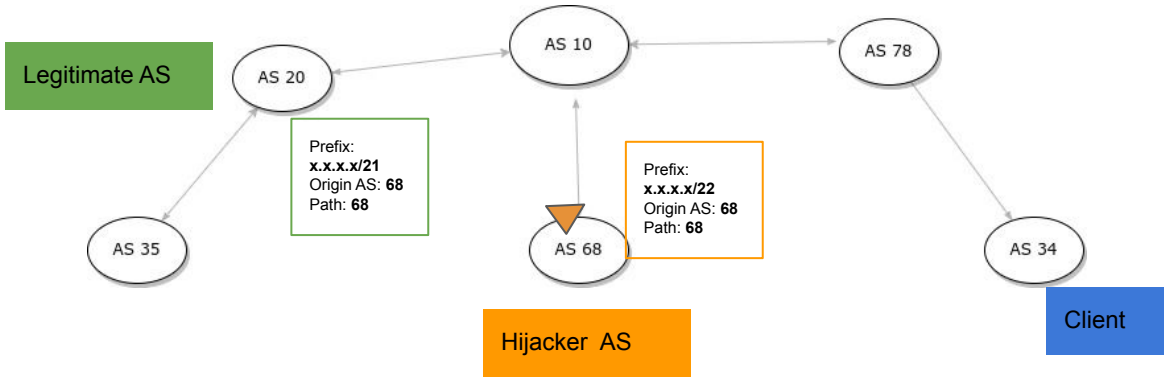
BGP hijacking Example

- AS 20 announces prefix x.x.x.x./21



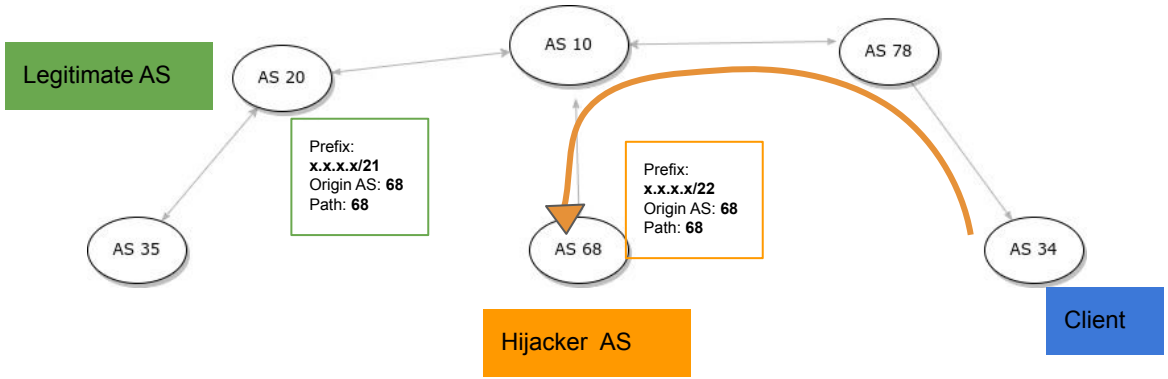
BGP hijacking Example

- AS 68 announces prefix x.x.x.x./22 which is a more specific prefix which is preferred in BGP



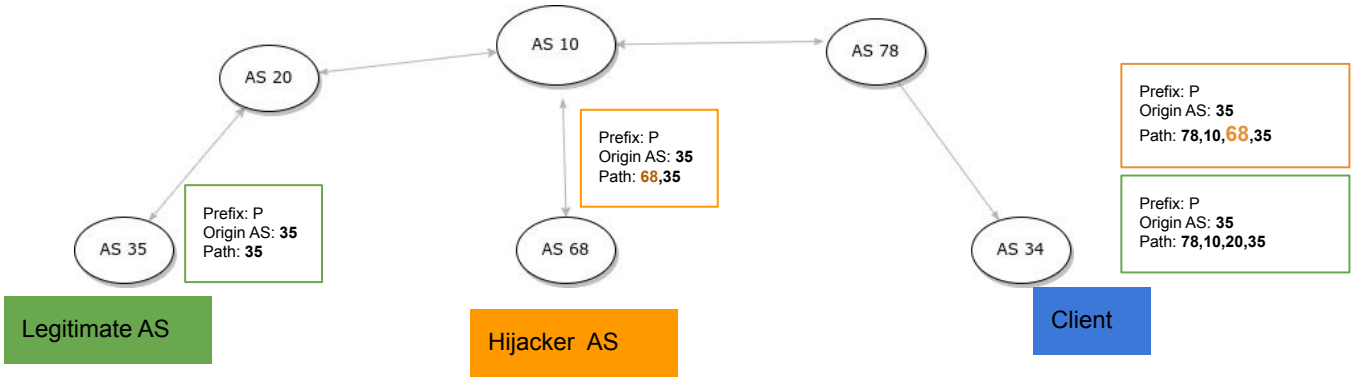
BGP hijacking Example

- This is an example of **Sub-prefix Hijacking**



BGP hijacking Example

- AS 68 can also announce a **fake path** towards AS 35



QUESTIONS ?