How Secure are Secure Interdomain Routing Protocols?

Sharon Goldberg, Michael Schapira, Peter Hummon, Jennifer Rexford, SIGCOMM 2010

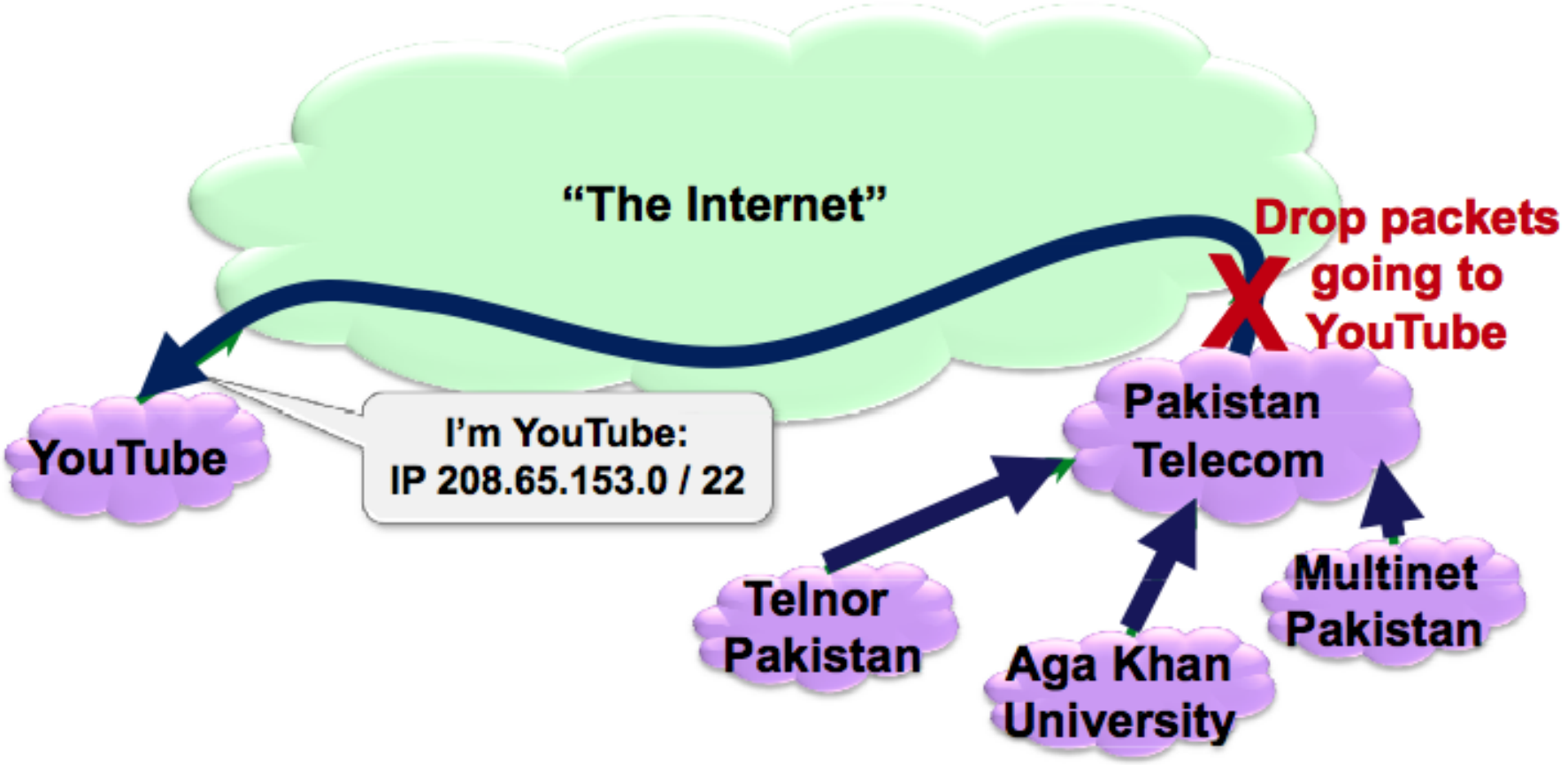
Presented by Colin Scott

How Secure is Routing on the Internet Today? (1)

February 2008 : Pakistan Telecom hijacks Youtube

How Secure is Routing on the Internet Today? (2)

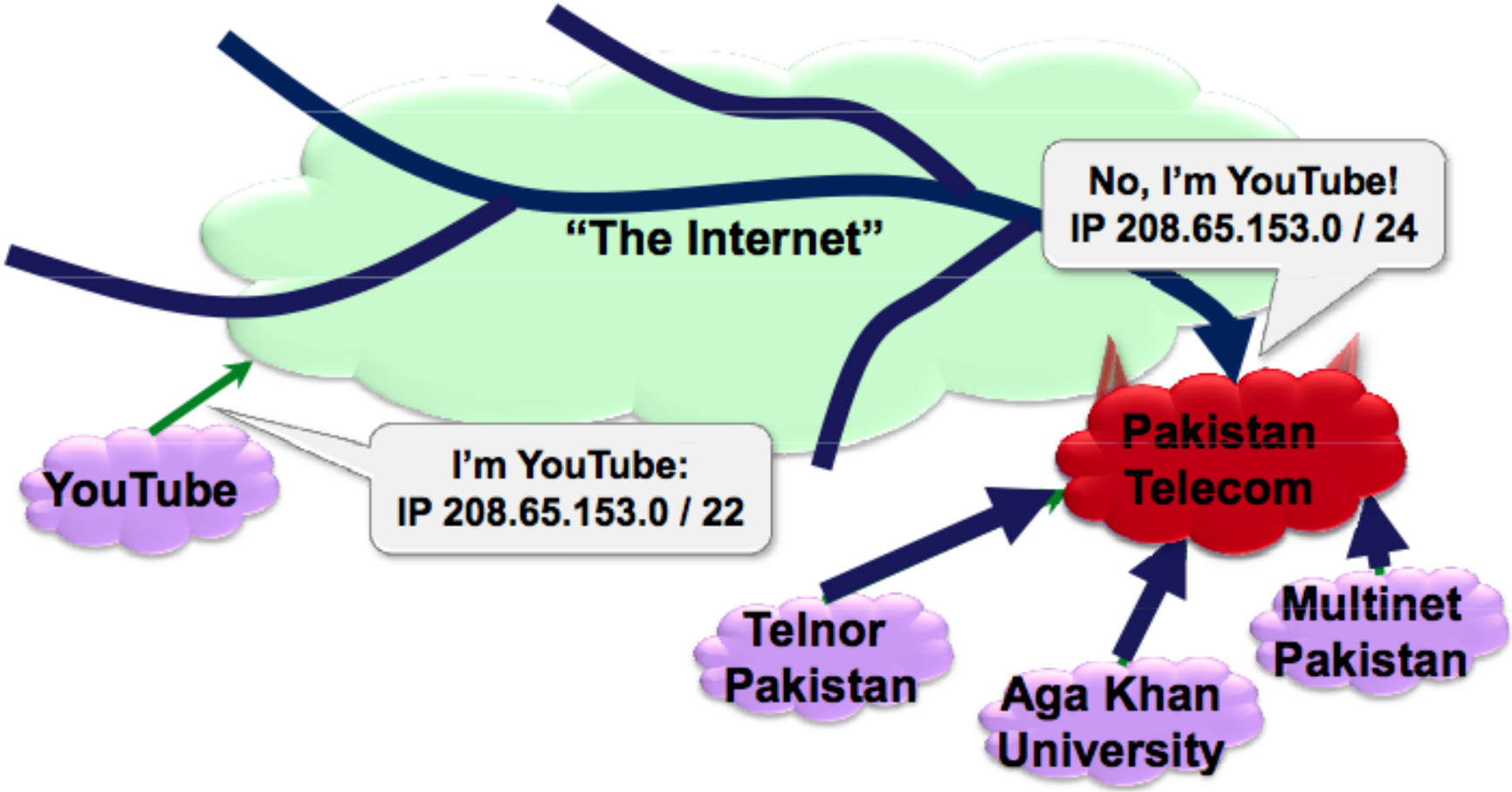
Here's what should have happened....



Block your own customers.

How Secure is Routing on the Internet Today? (3)

But here's what Pakistan ended up doing…



Draw traffic from the entire Internet!

Background

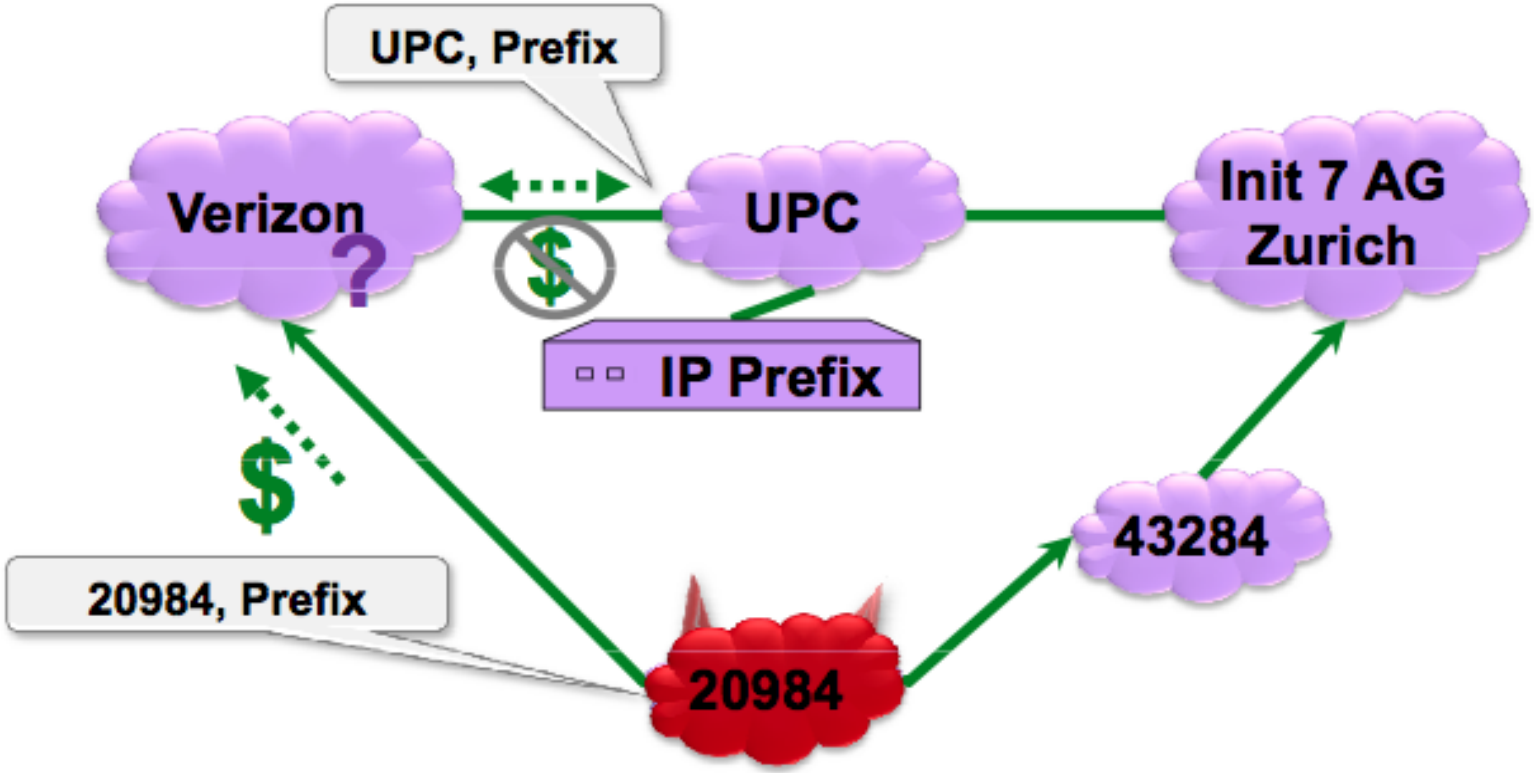
- "Traffic Attraction" attacks can cause major problems
- Many proposals to fix BGP:
  - Origin Authentication (ROA) < soBGP < S-BGP
  - (+ Defensive filtering)

Contribution

- This paper seeks to *quantify* and *compare* the different proposals using simulation

Traffic Attraction Attacks (1)

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

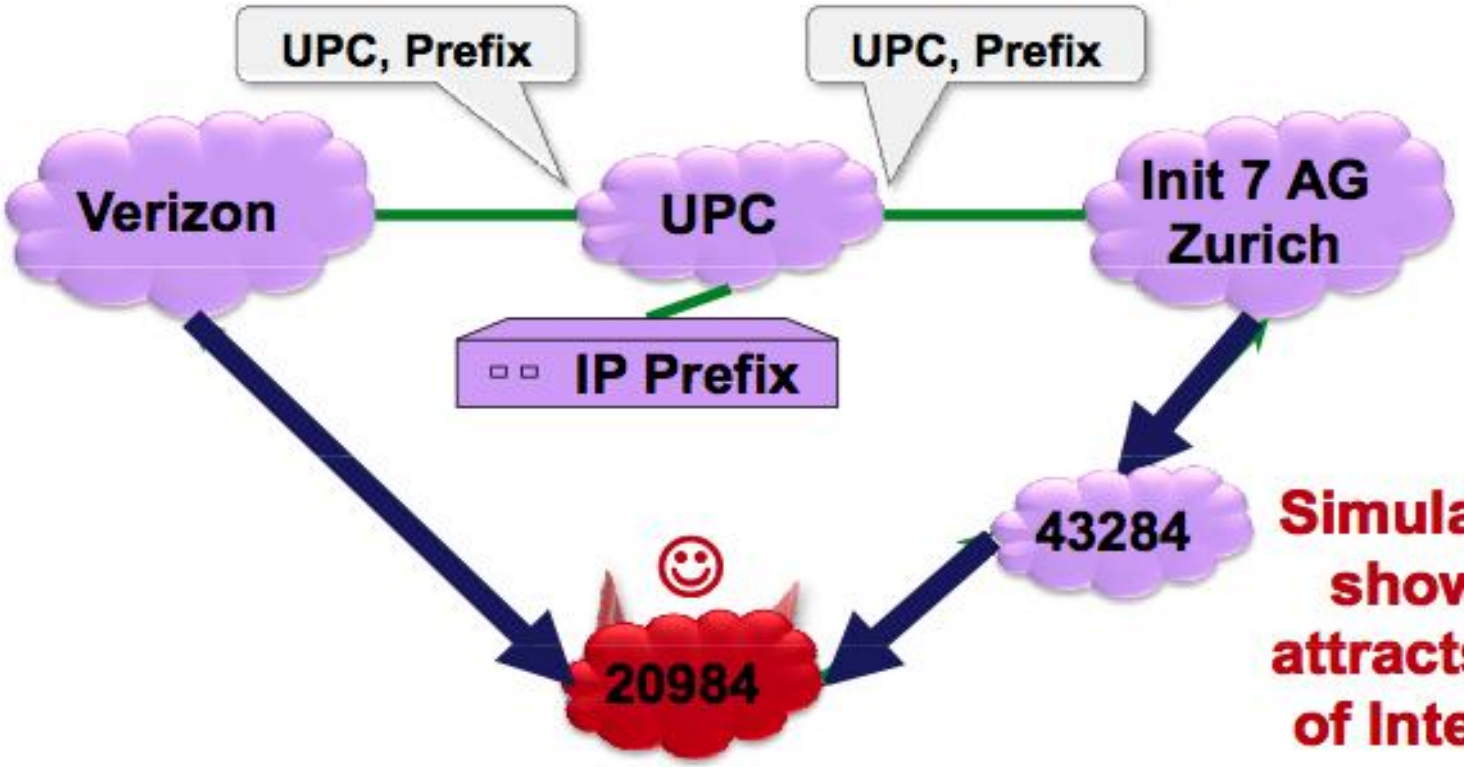


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Traffic Attraction Attacks (5)

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)



Simulations show he attracts 62% of Internet!

A model of routing decisions:

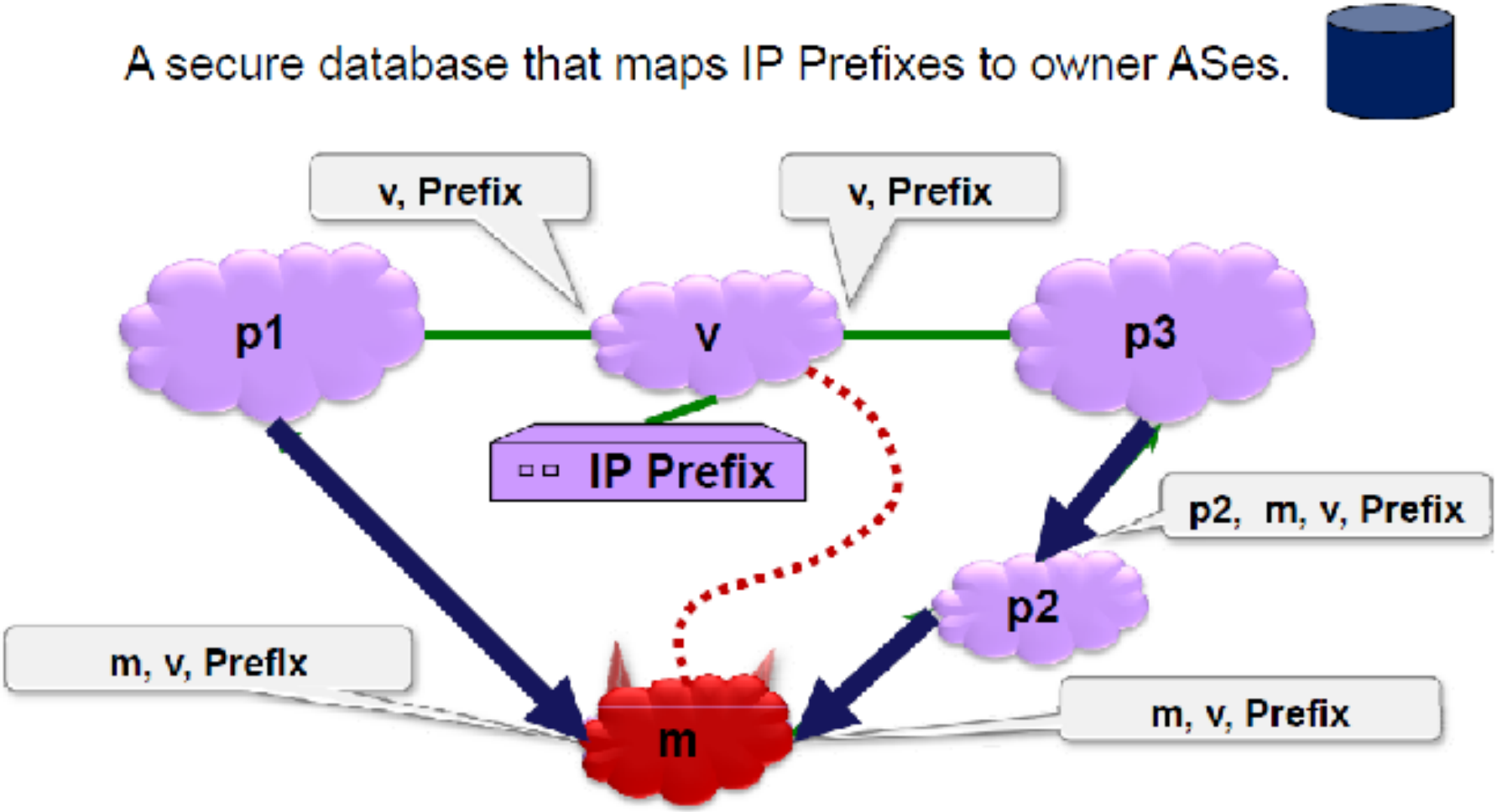
- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Origin Authentication

- BGP + Origin Authentication: magic database in the sky to verify correct origin AS

Security Mechanism: Origin Authentication RPKI/ROA

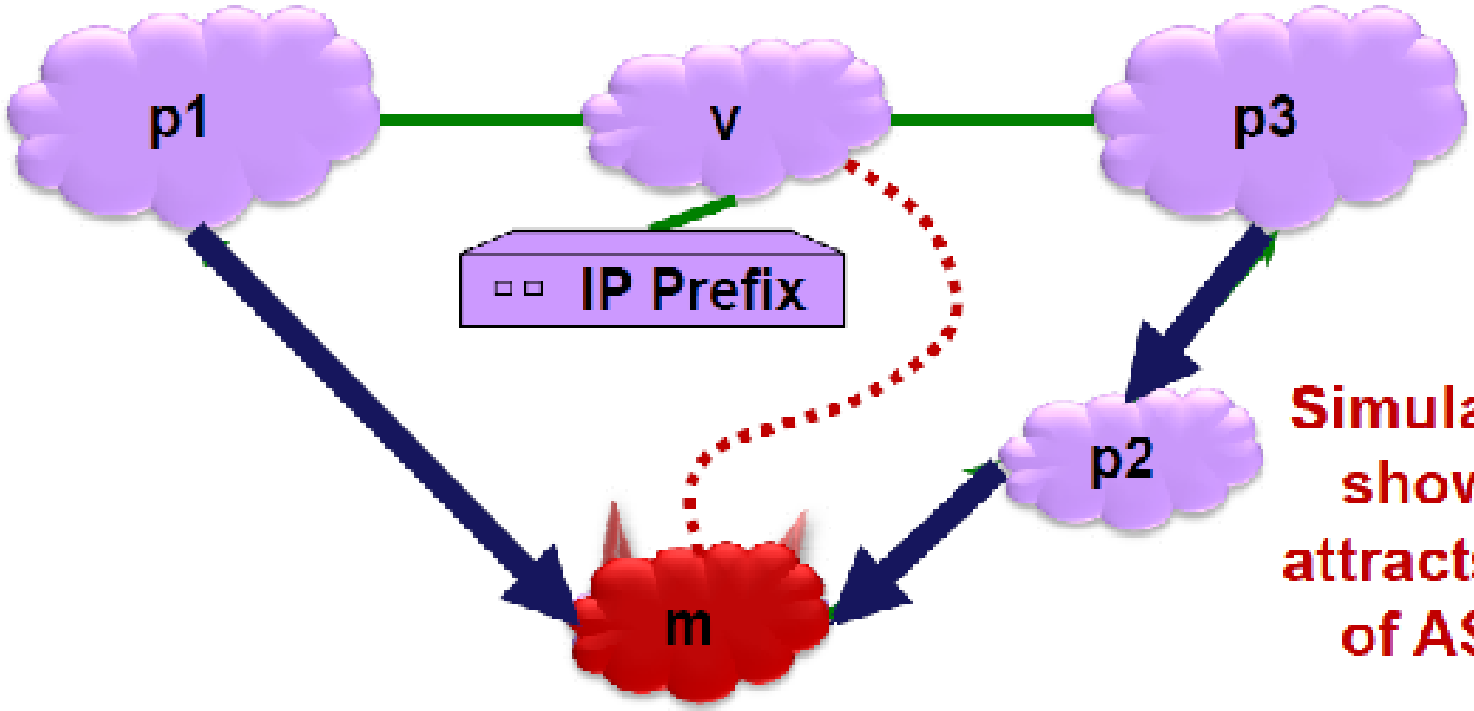
A secure database that maps IP Prefixes to owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication RPKI/ROA

A secure database that maps IP Prefixes to owner ASes.



Simulations show he attracts 58% of ASes!

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Next Attempt

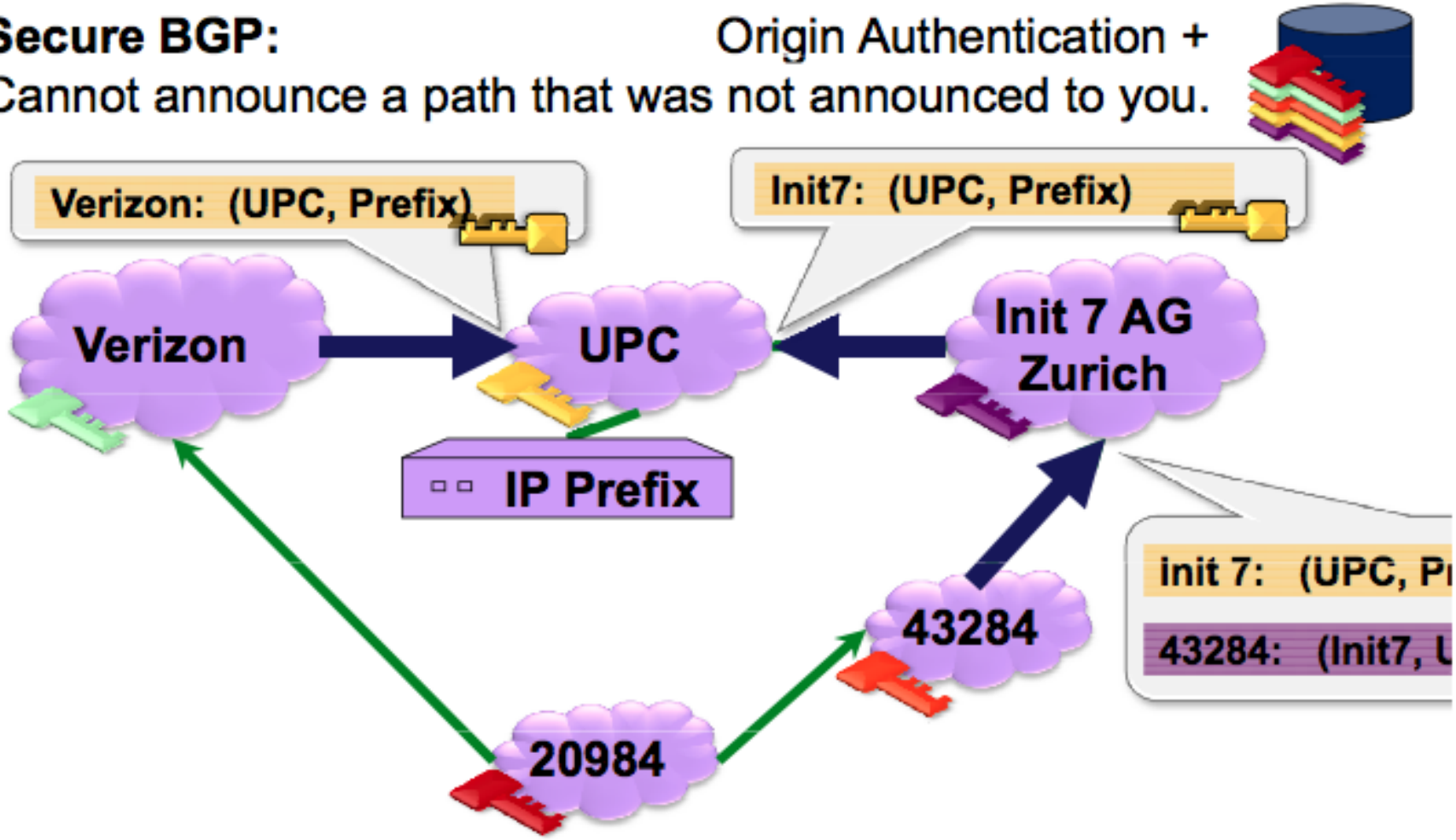
- soBGP ('secure origin'): authenticate origin + verify existence of path
  - Hack!: Bad guy can announce fake (unused) paths through real Ases

Better Attempt

- S-BGP: each AS cryptographically signs routing advertisement -> authentication for every hop
  - This should fix it, right?

Security Mechanism: "Secure BGP" [KLS98]

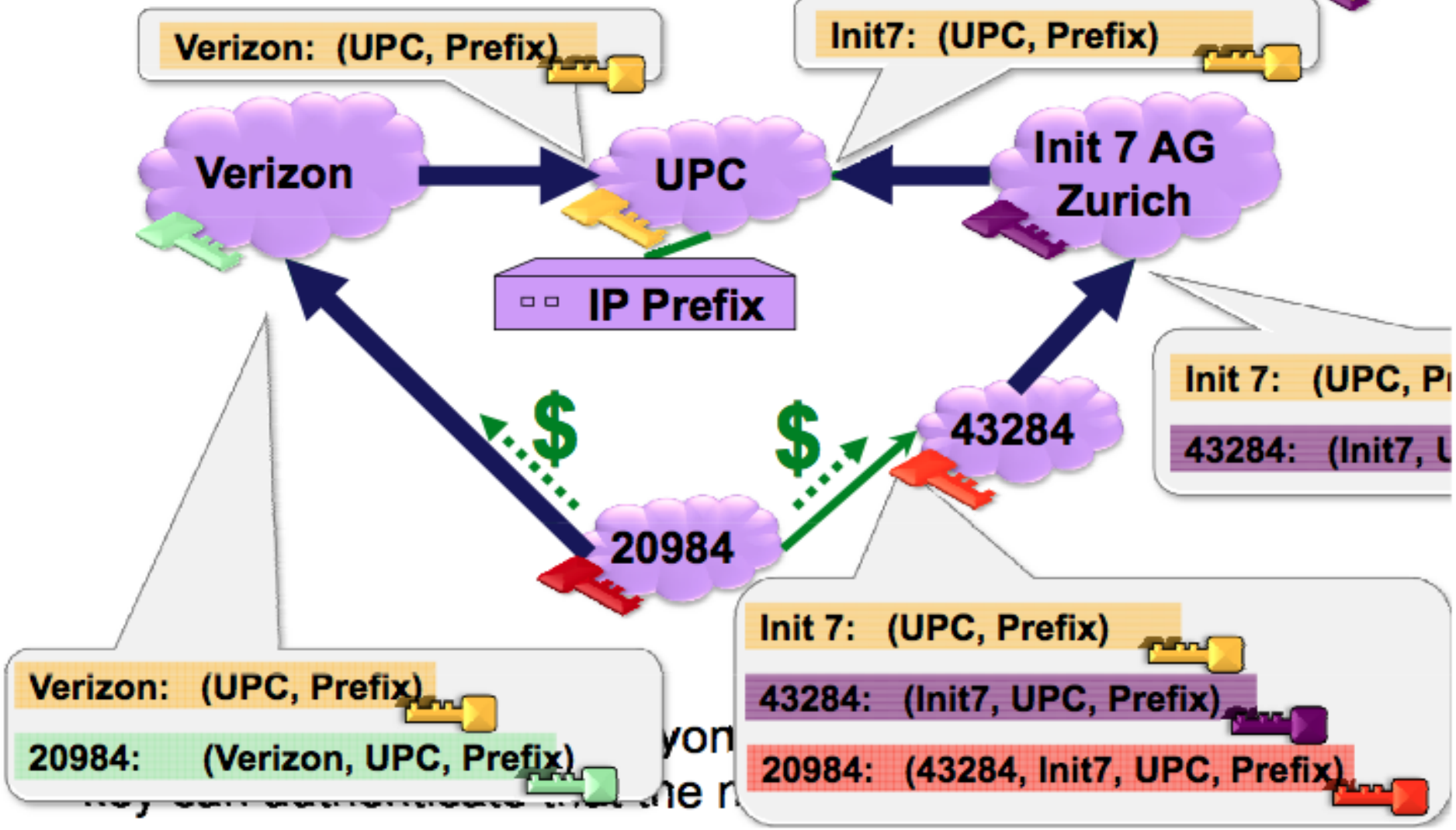
Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



Public Key Signature: Anyone who knows UPC's public key can authenticate that the message was sent by UPC.

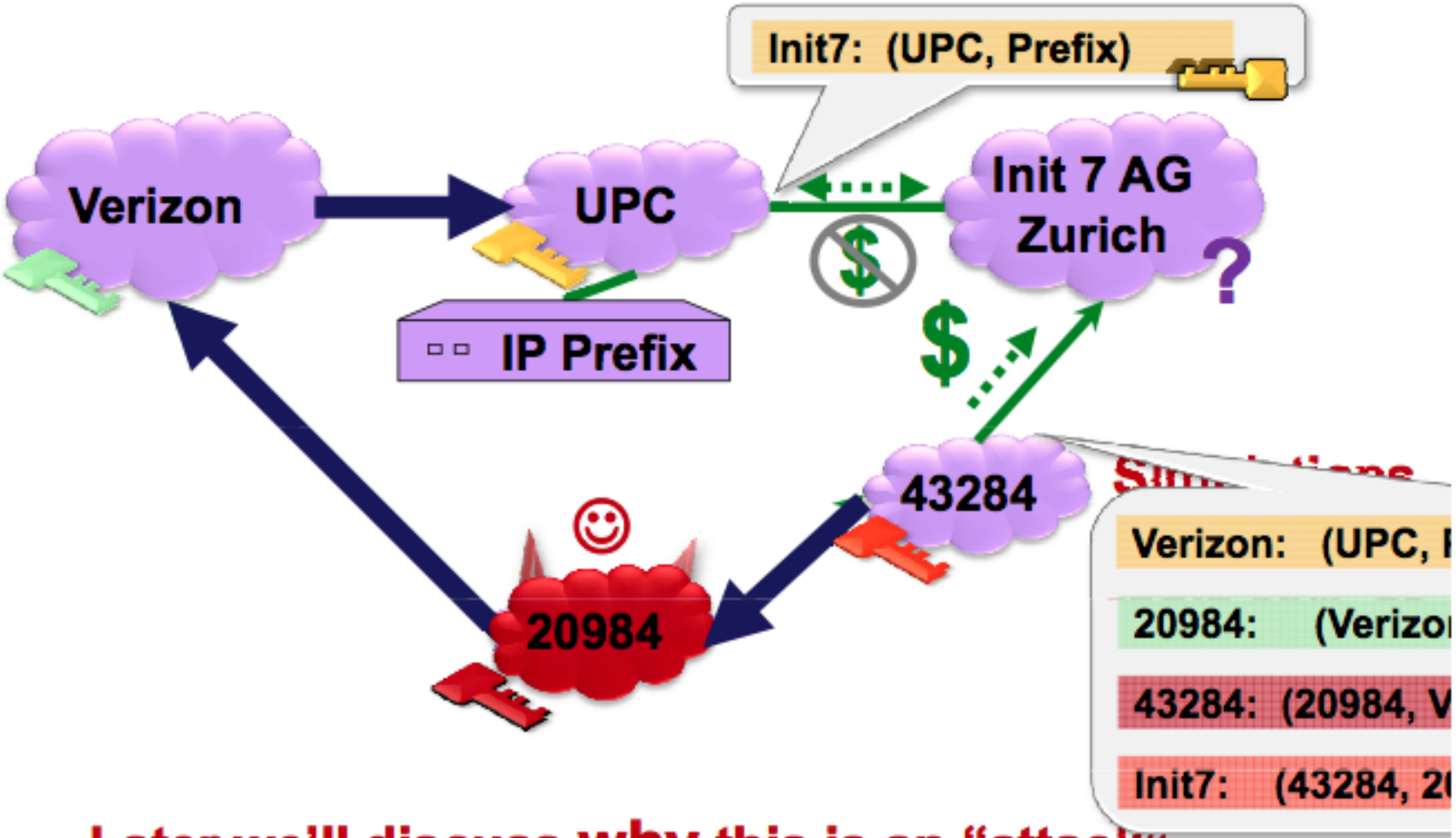
Security Mechanism: "Secure BGP" [KLS98]

Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



Are attacks still possible with Secure BGP? (3)

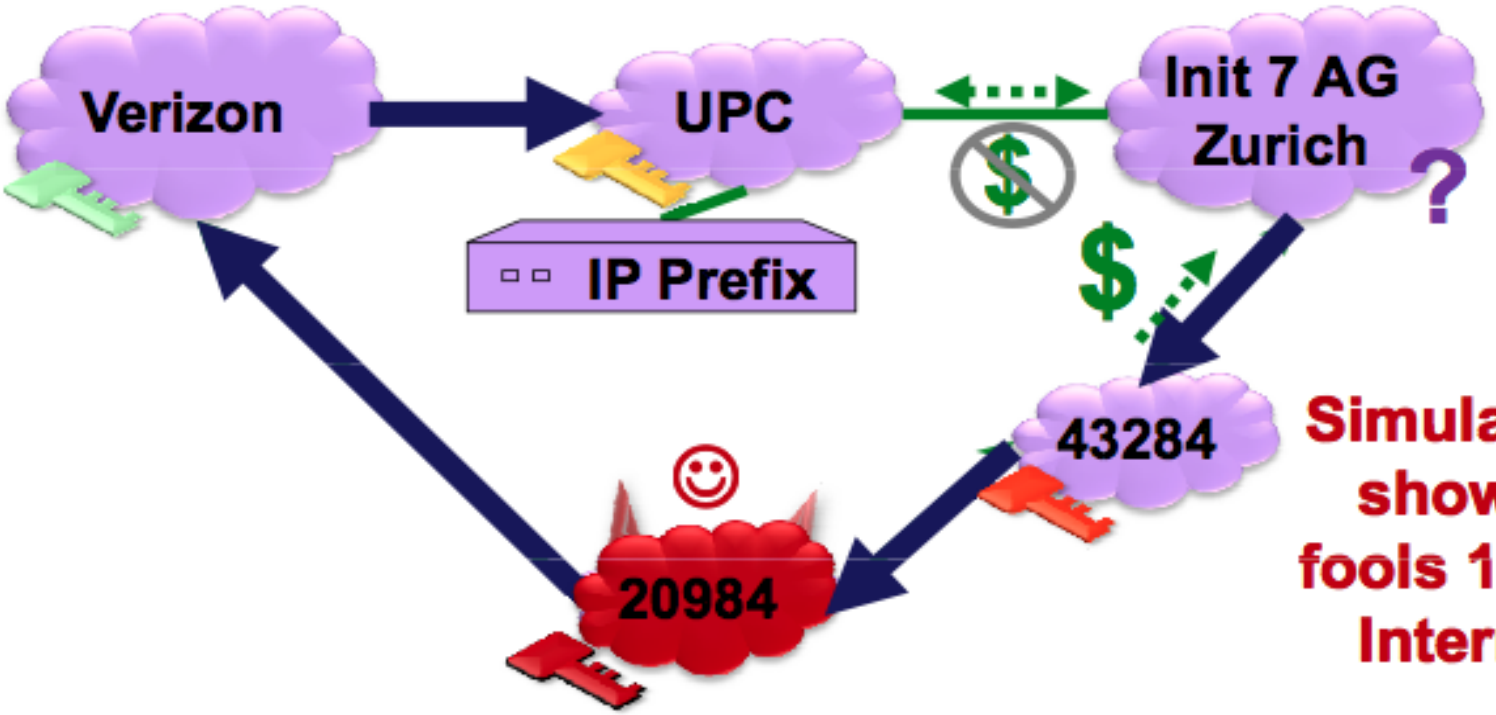
Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Later we'll discuss why this is an "attack"

Are attacks still possible with Secure BGP? (4)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Simulations show he fools 16% of Internet!

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only carry traffic if it earns you money.

Conclusion

- Several security proposals for BGP:
  - Origin authentication < so-BGP < S-BGP
- Paper quantified and compared proposals using simulation
- Showed that *export policies* are as important as 'legitimacy' of routes
- (Other results as well, not shown here)