Defending Against BGP Man-In-The-Middle Attacks

Black Hat DC 2009
Arlington, Virginia
February 2009

Clint Hepner
Earl Zmijewski
Renesys Corporation

Overview

- Every organization owes its Internet connectivity to one protocol: BGP4. **There are no alternatives**.
- BGP4 has longstanding vulnerabilities that **cannot be fixed,** and can only be monitored carefully.
- In this presentation, we will describe a *recent* vulnerability: BGP Man-In-The-Middle (MITM).
- Takeaway messages:
  1) Everyone who connects to the Internet is currently exposed to various routing risks: **downtime, hijacking** and now even **wholesale traffic interception**.
  2) Very few people understand these risks, so they are not being **measured** or **managed** appropriately.

Outline

1) BGP Routing Basics
   - Enough to understand and identify the threat
2) The Man-In-The-Middle Attack
   - Review of the DEFCON BGP exploit
3) Detecting the Attack
   - Methods for observing the attack in the wild
4) Case Studies
   - Analyzing historical data for attack evidence

Part 1: BGP Routing Basics

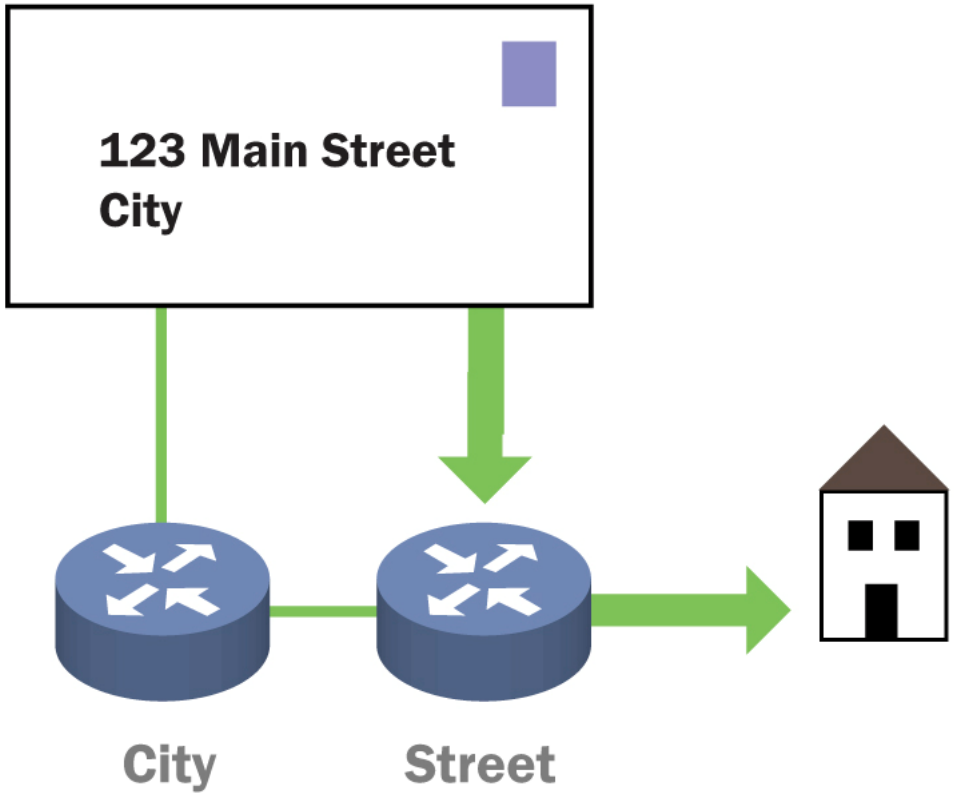
- Basics of routing and the inherent threats
  - Prefixes
  - ASNs
  - Routing updates
  - Route attributes
  - Vulnerabilities
  - Typical historical attacks

Internet Routing – Prefixes

- **Internet routing** is orchestrated via blocks of IP addresses
- **A network prefix** is a block of contiguous IP addresses:
  - **11.1.18.0/24** contains 256 addresses, namely,
    11.1.18.0, …, 11.1.18.255
  - **11.1.16.0/20** contains 4096 addresses, namely,
    11.1.16.0, …, 11.1.31.255
  - **11.1.18.0/24** is **more specific** than **11.1.16.0/20**
- IP addresses in the same prefix are routed in the same way.

Internet Routing – most specific route wins

BGP favors **more specific** routes to an address over **less specific** ones. A packet of data is like a letter sent through the mail. It contains the full address of its destination, but prefers the most specific available route to that address.



Internet Routing – ASNs

Global Internet routing relies on the Border Gateway Protocol.

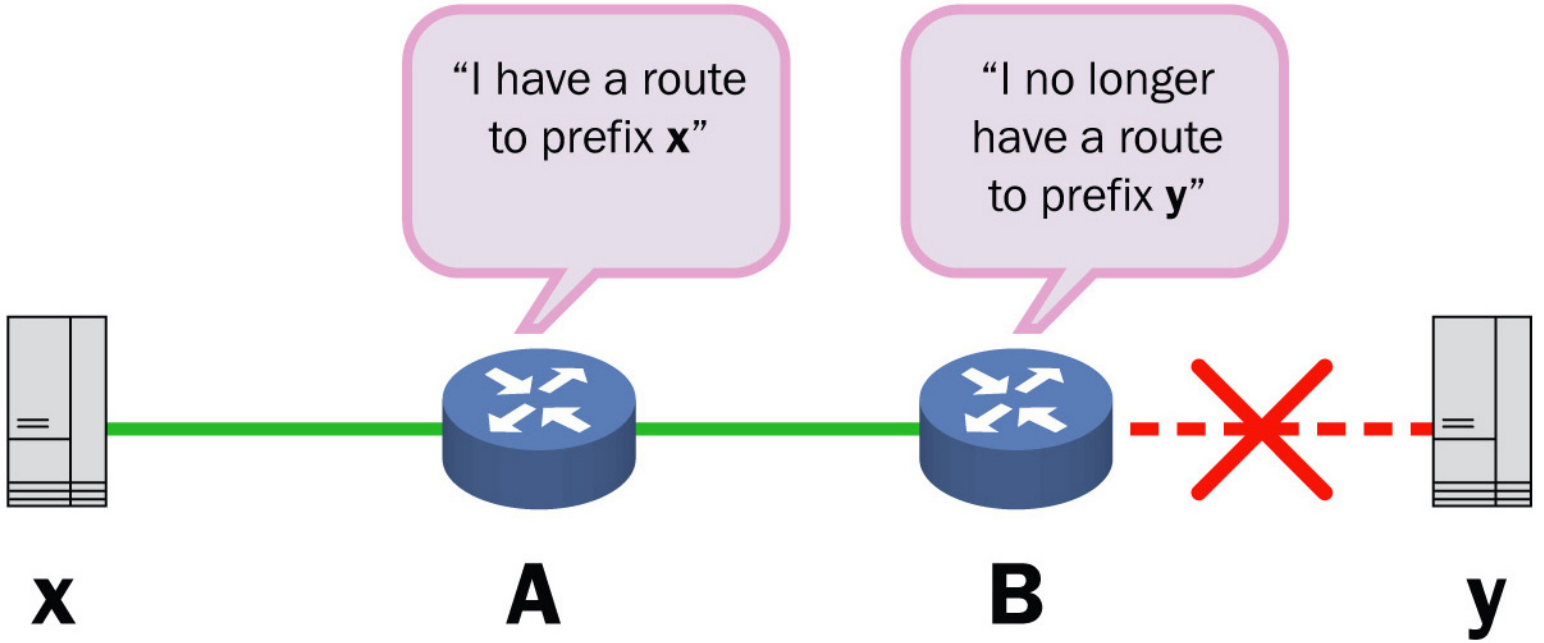
Each organization participating in BGP is assigned:

- A unique **Autonomous System Number** or **ASN** (integer)
- One or more **prefixes** (range of IP addresses)

Example ASNs

Routers talk to neighboring routers via **BGP**

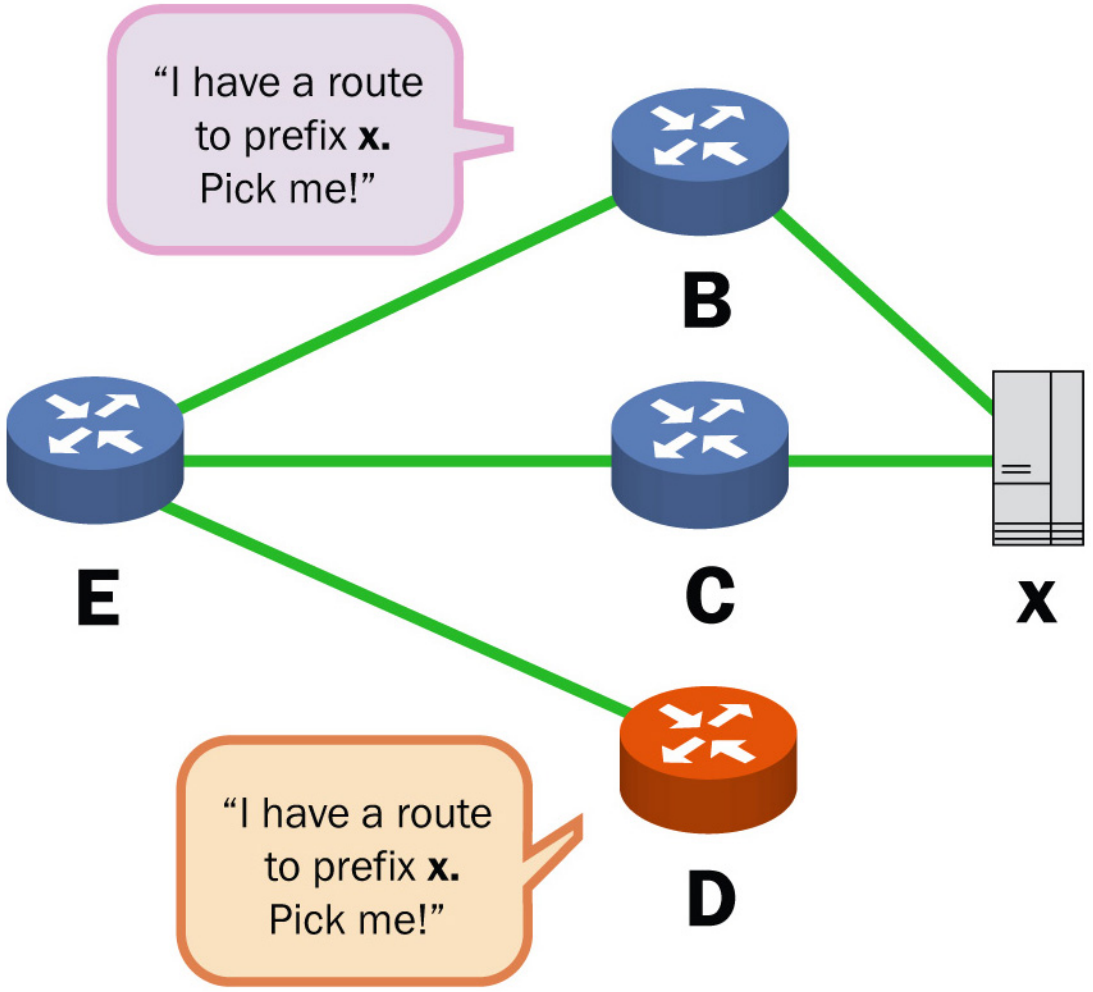
(Border Gateway Protocol) - That's how global routing is established



Typical messages that routers send to each other.

All routing decisions are local

Each router decides on the "best" route to each prefix from all the possibilities it learns about. It may also choose to inject ***bogus*** routes.

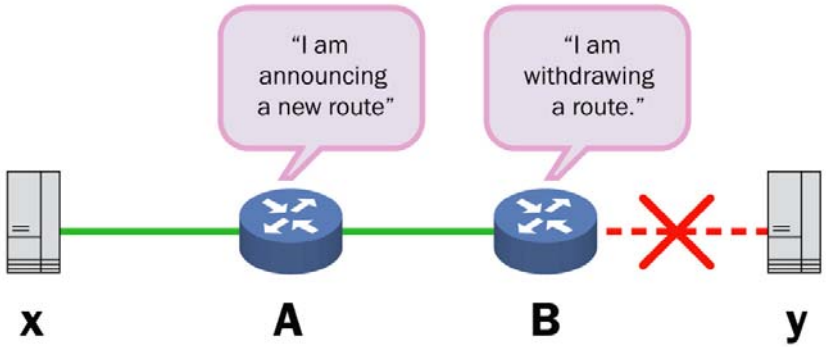


BGP Update Messages

- **An UPDATE** message announces a new route or withdraws a previously announced route.

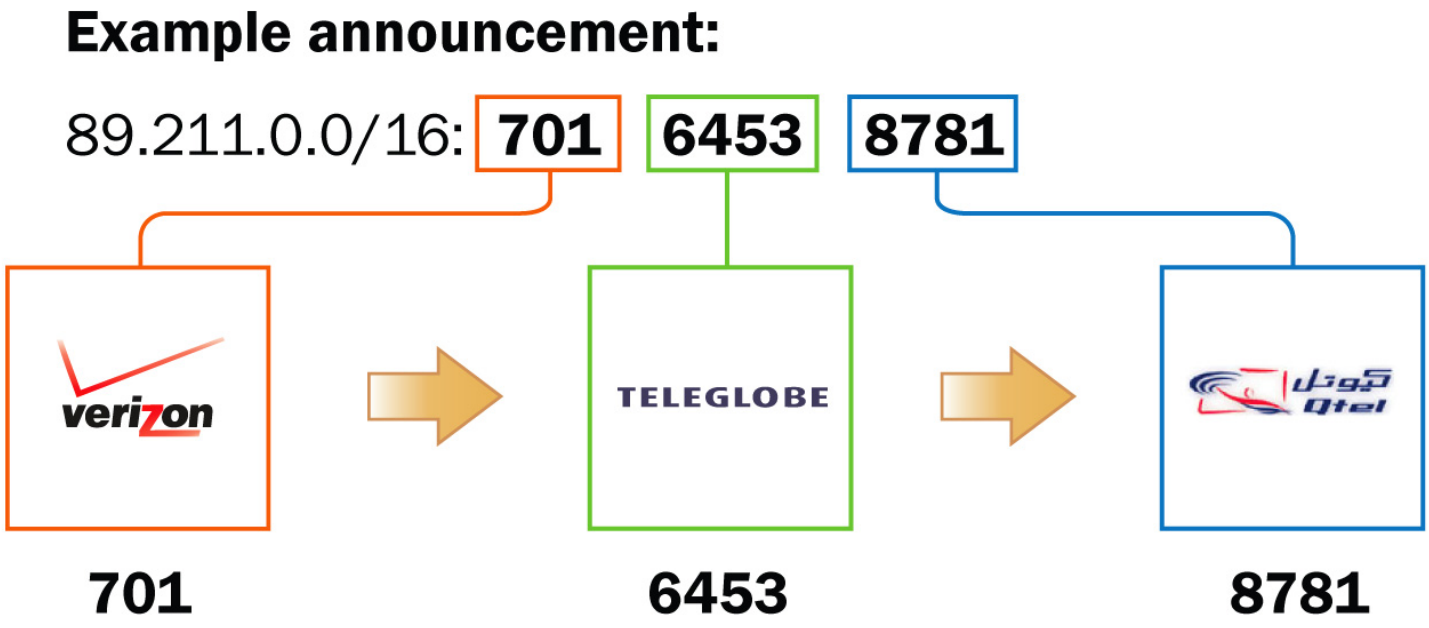
  UPDATE = prefix + route attributes

- Adjacent routers chatter constantly with each other as routes come and go. Globally, Renesys observes 45,000+ updates per minute when things are quiet!



BGP Attributes

- **Routing announcements have attributes …**
  many possibilities but the (hopefully valid) ***AS path*** to the announced prefix is always present.



Key to routing vulnerabilities

- No single authoritative source of who should be doing what.
  - If there were, you could filter out the errors / hijacks.
  - As a result, filtering by ISPs is not common or easy.
- All of Internet routing is based on *trust*.
  - Anyone can announce any IP space they want.
  - Anyone can prepend any ASN to any path that they want.
- No mechanism in place to handle ASNs who go ***rogue***. There are no Internet police!

Two typical types of hijacks

- **No operational impact**
  - **Hijack *unused* (but maybe assigned) IP space**
    - Potentially harms the reputation of the owner
    - But does not disrupt any legitimate traffic on the Internet
- **Obvious operational impact**
  - **Hijack *currently used* IP space**
    - Legitimate traffic diverted to the hijacker
    - Victim can be effectively taken off the Internet
    - Very disruptive and very obvious
- **Both types of hijack allow an attacker to attract *all traffic* bound for the hijacked space.**

Hijacking unused (but assigned) space

Examine three US DoD networks and their more-specifics

DoD owns but does not announce 7.0.0.0/8, 11.0.0.0/8, 30.0.0.0/8 and others. These networks are "free for the taking" without any impact on **DoD.**

A Sampling of **Hijacks**: 2008

Prefix	Date(s)	Origination (AS)	Country	Duration
30.30.40.0/24	Aug 6-9, Nov 11-26	Telefonica (AS 10834)	Argentina	20 days
11.42.51.0/24	July 16-17	Telstra Pty (AS 1221)	Australia	11.6 hours
11.11.11.0/24	May 17	Teknoas (AS 42075)	Turkey	6.5 minutes
11.11.11.0/24	May 10, July 9	INDO Internet (AS 9340)	Indonesia	6.4 minutes
11.0.0.0/24	April 25-26	ITC Deltacom (AS 6983)	US	16 hours
7.7.7.0/24	March 7	Posdata (AS 18305)	S. Korea	16 minutes
11.1.1.0/24	**March 5-29**	**Helios Net (AS 21240)**	**Russia**	**3.5 weeks**
11.11.11.0/24	January 5	Hutchinson (AS 9304)	Hong Kong	1.1 hours

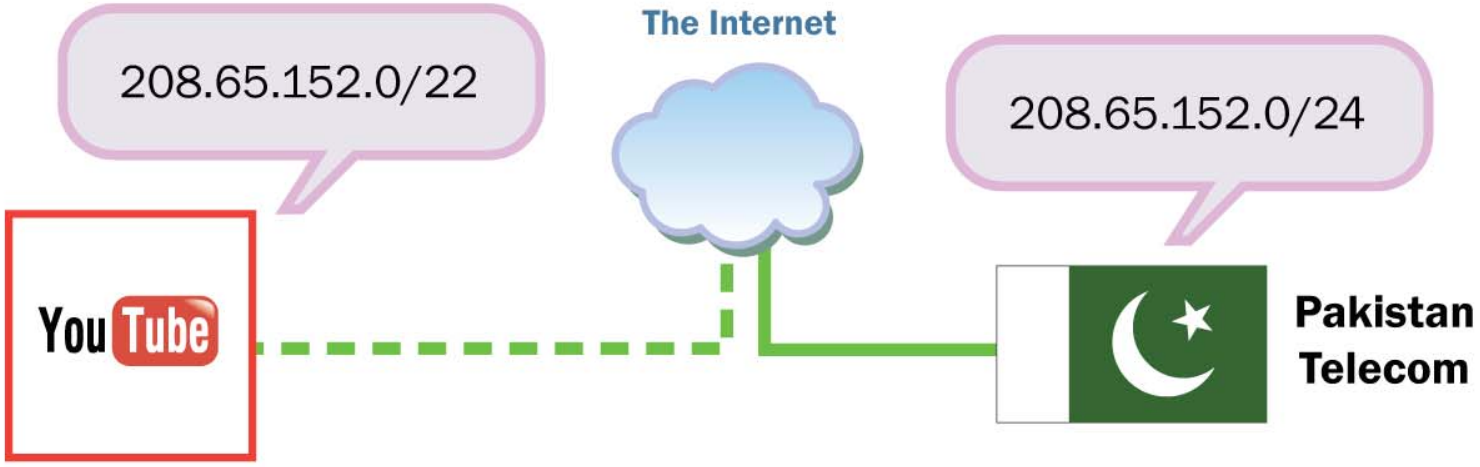
Every announcement in this space is a hijack.

Hijacking Used Space – YouTube: Feb ’08

- YouTube owns 208.65.152.0/22
  - This contains the more-specific 208.65.153.0/24
  - The above /24 *used* to contain all of YouTube’s
    - DNS Servers (have since moved)
    - Web Servers (have since added additional IP space)
  - YouTube announced only the /22

Hijacking Used Space – YouTube: Feb ’08

- Pakistan Telecom announces the /24
  - In BGP, most specific route to an IP address wins!
  - Pakistan Telecom gets all traffic intended for YouTube
  - YouTube is globally unreachable for 2 hours



None of this is new

- Hijacking has been going on for over 10 years!
- No incremental or comprehensive solutions
- Solutions lack economic drivers
  - Doesn’t happen daily and universally
  - Avoiding negative publicity is not necessarily compelling
  - Impact poorly understood by management
- Miscreants are actively hijacking now
  - To send spam from “clean” IP blocks
  - To cover their other nefarious activities
    - What good are your firewall/IDS logs now?
    - Need historical global routing data to identify hijackers

Part 2: The Man-In-The-Middle Attack

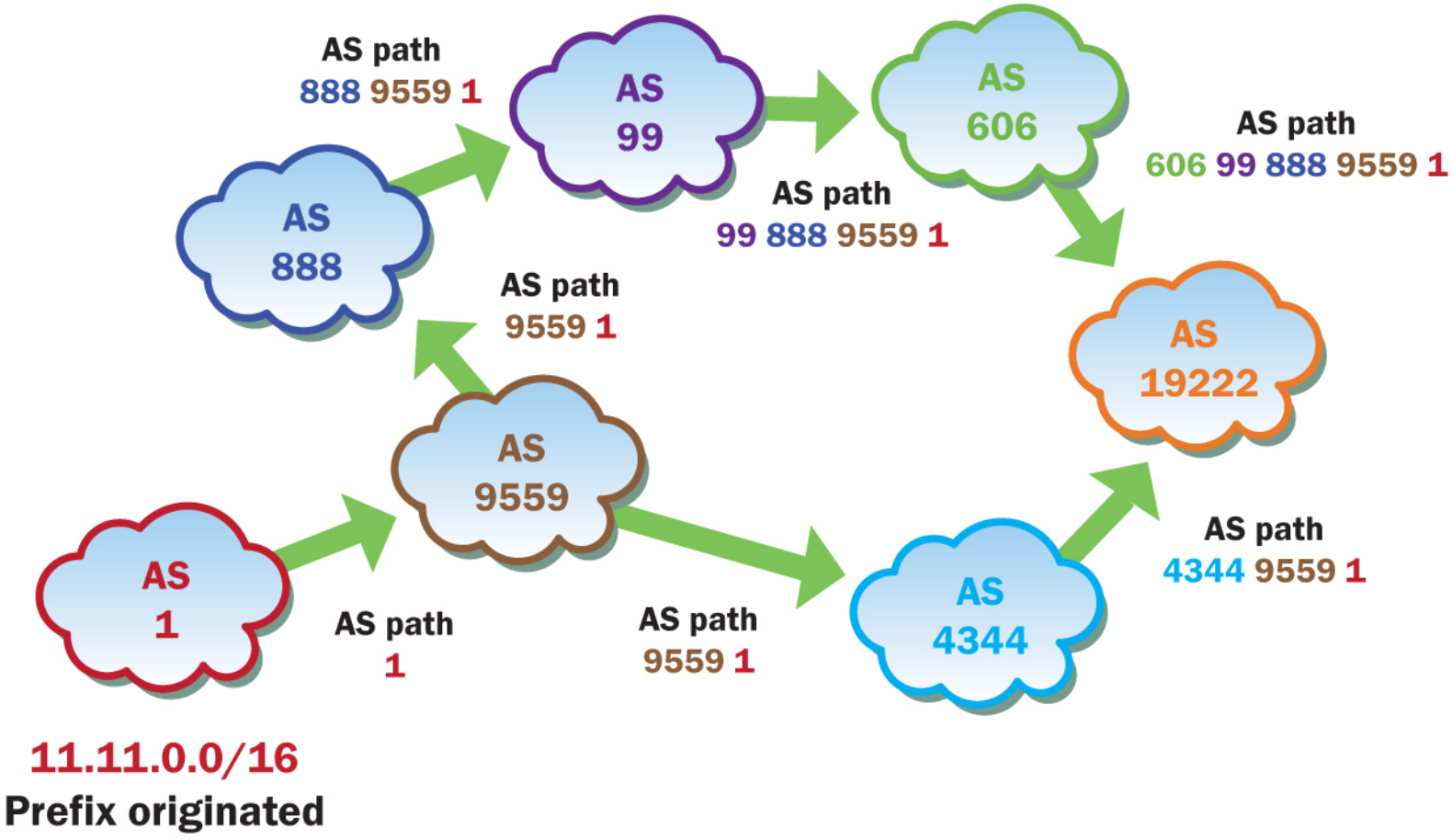
- Review of the MITM exploit presented at DEFCON
  - AS path attribute
  - AS loop prevention
  - MITM attack technique
  - Obscuring the MITM attack with TTL adjustment

New type of hijacking: BGP MITM
- BGP Man-In-The-Middle (think “wiretapping”)

- Presented at **DEFCON** 16, August 10, 2008
  - “Stealing the Internet” – Alex Pilosov and Tony Kapela
- Basic Idea
  - Hijack someone’s traffic, but then ultimately send it on to them
    - Allows an attacker to alter, log, misdirect or simply observe somebody else’s incoming Internet traffic.
  - The attacker “blinds” some of the Internet to the hijack, in order to construct a viable path to the victim
    - Abuse AS path loop detection to blind some ASes

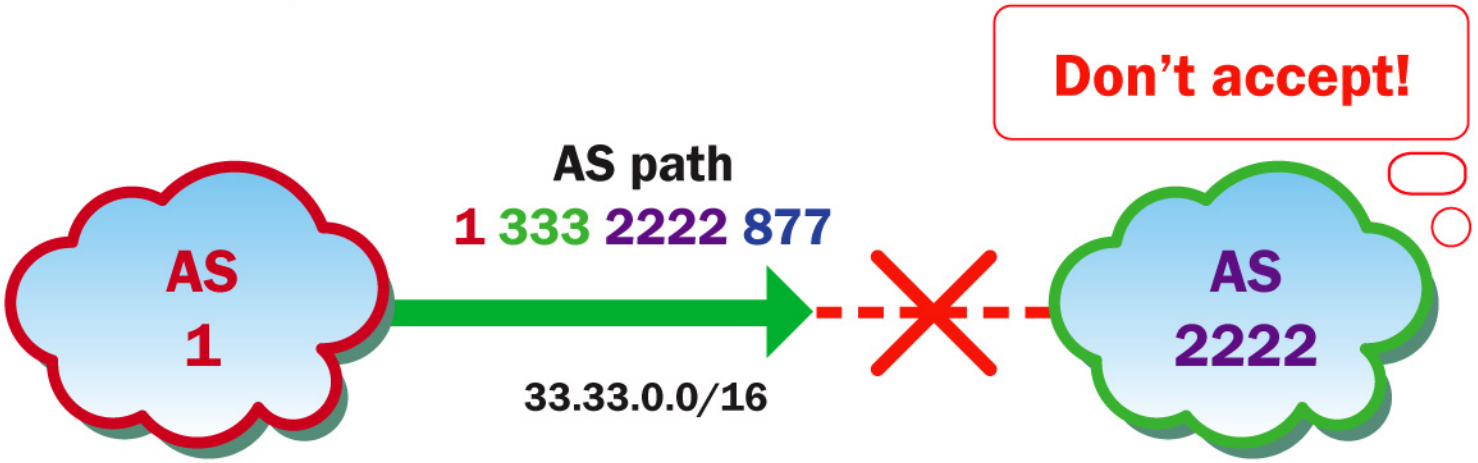
AS Path Attribute

Paths grow as announcements propagate



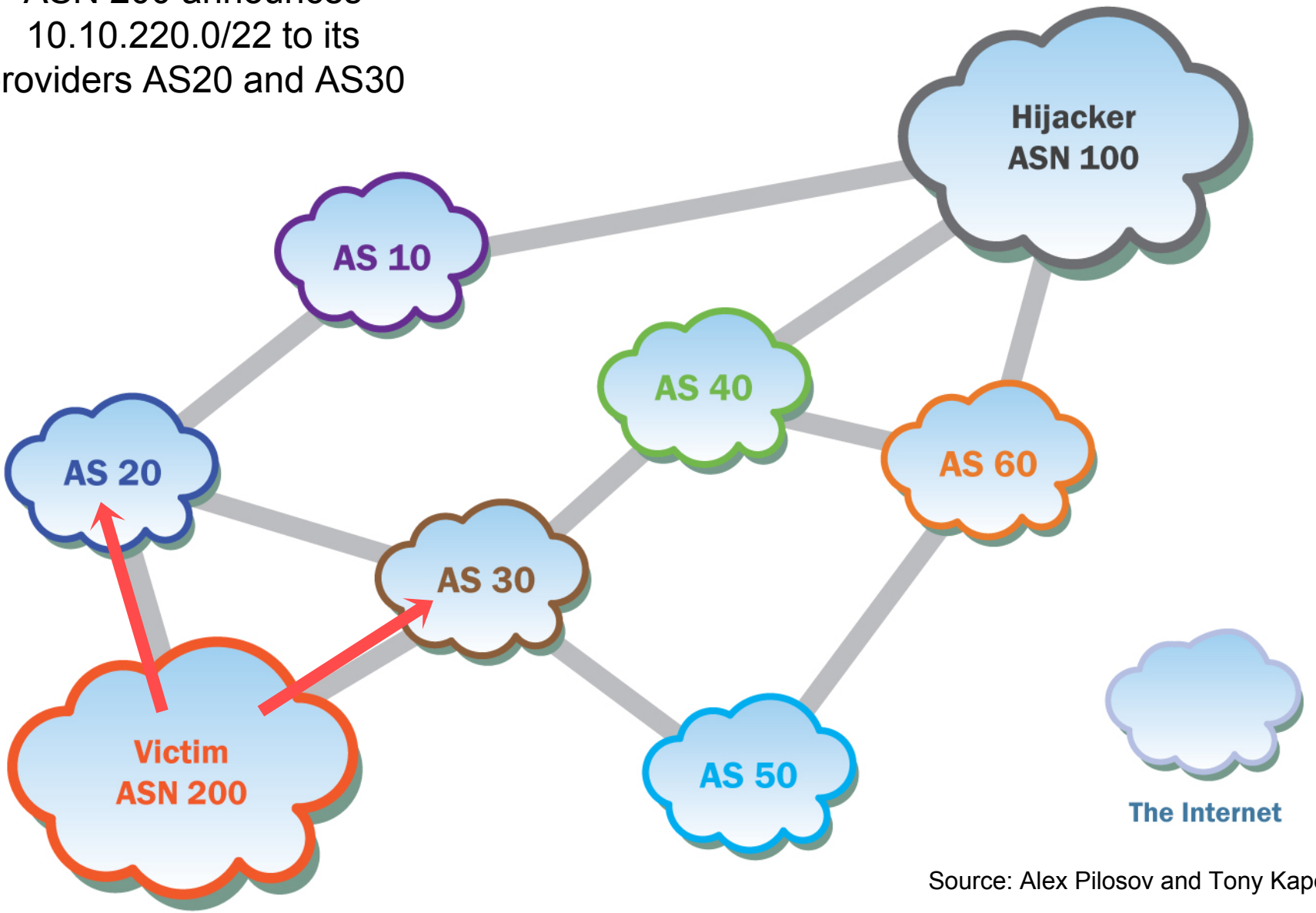
BGP Loop Prevention via AS Path attribute

AS X will not accept a route with **X** on its AS path.
For example,



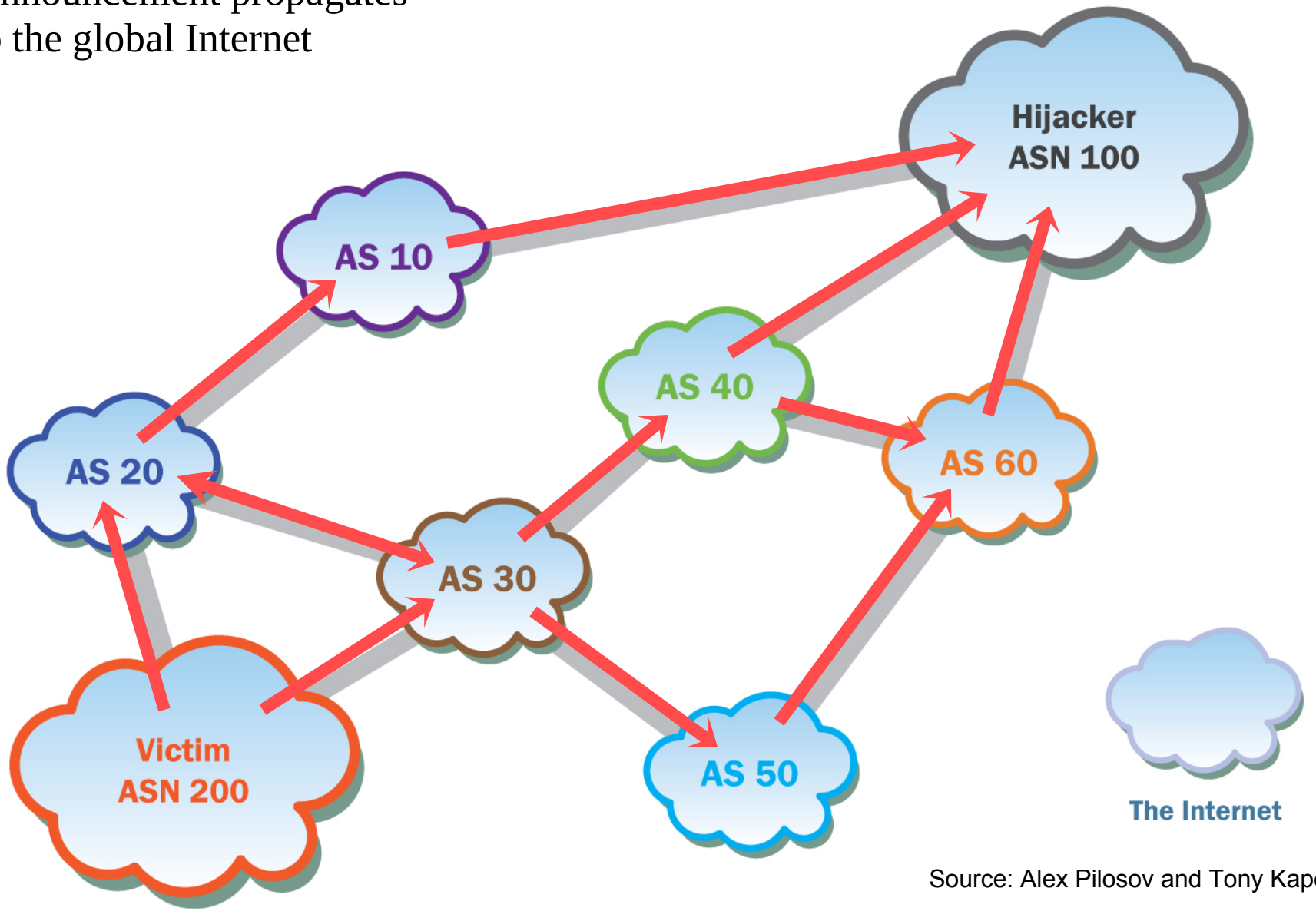
Note: such rejected routes are not logged and are only visible by putting the router into "debug" mode.

ASN 200 announces 10.10.220.0/22 to its providers AS20 and AS30



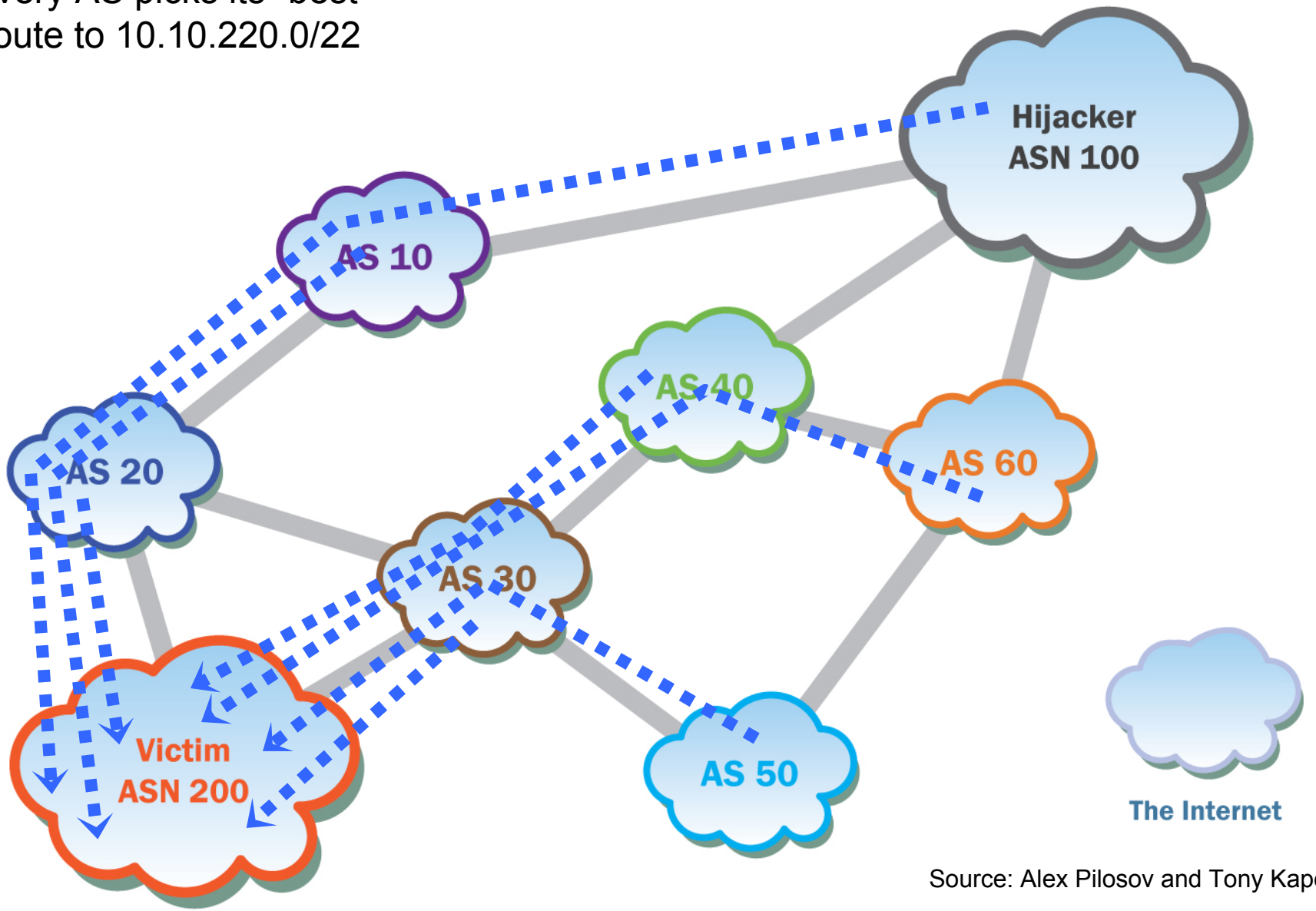
Source: Alex Pilosov and Tony Kapela

Announcement propagates
to the global Internet



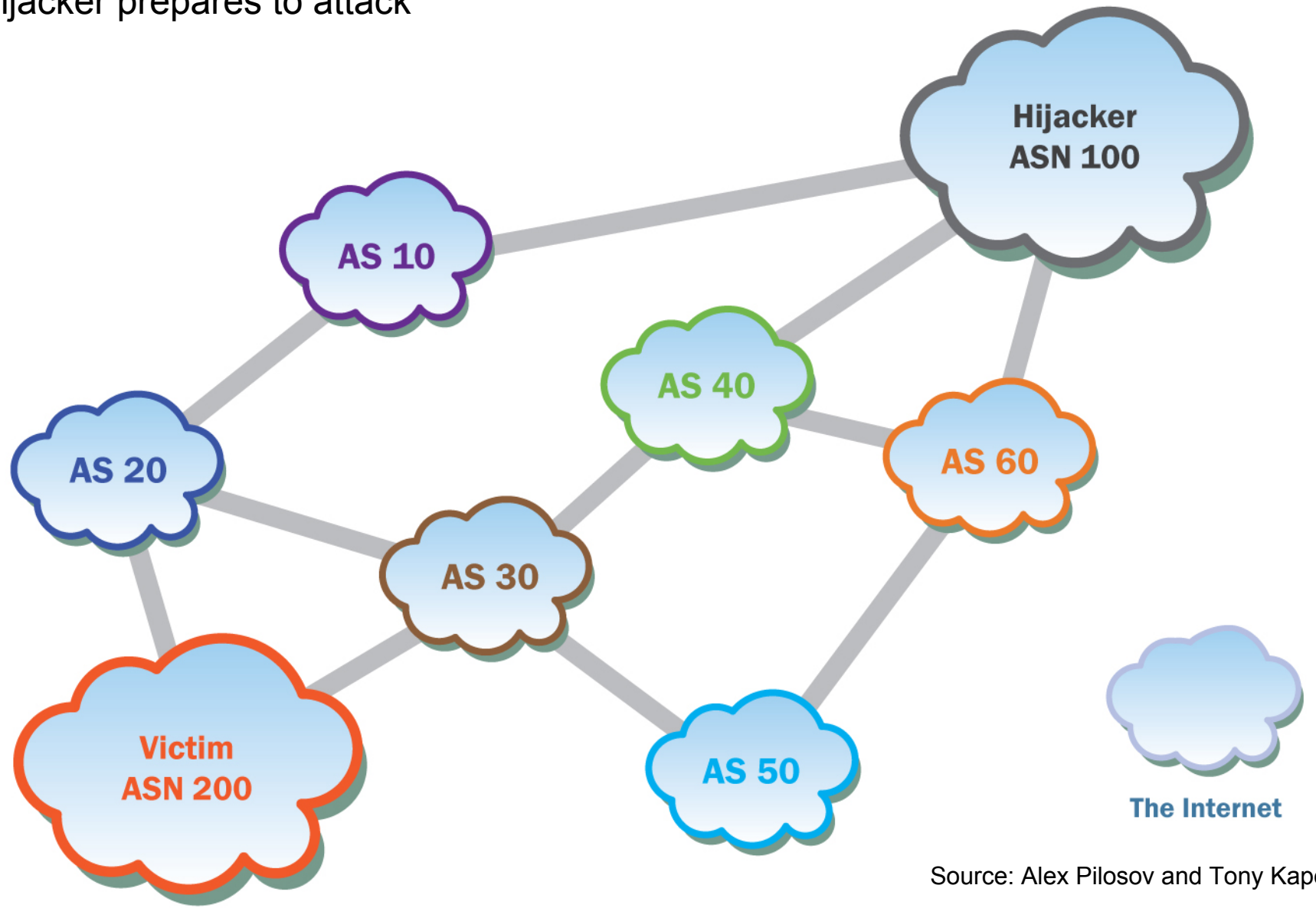
Source: Alex Pilosov and Tony Kapela

Every AS picks its “best” route to 10.10.220.0/22



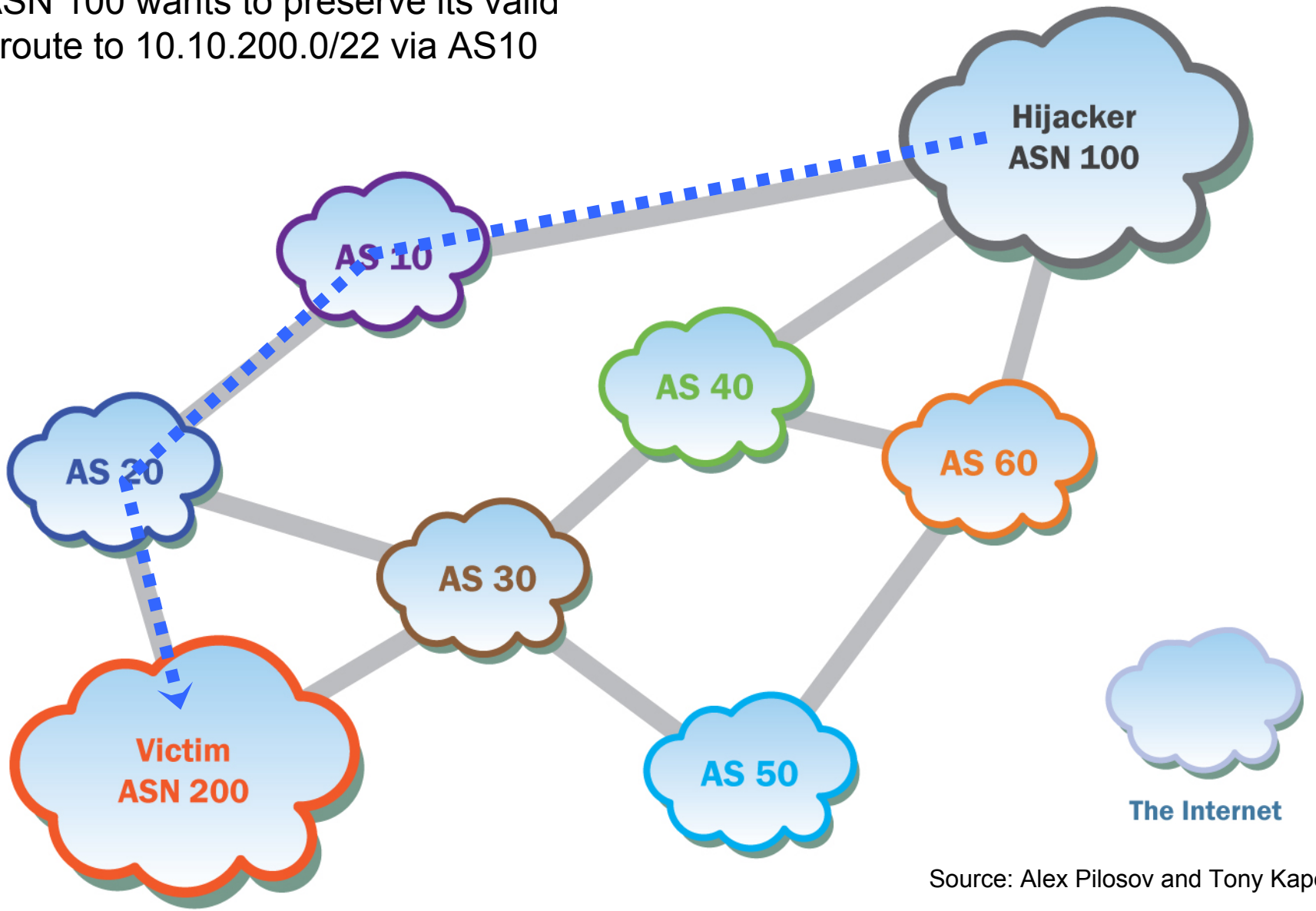
Source: Alex Pilosov and Tony Kapela

Hijacker prepares to attack



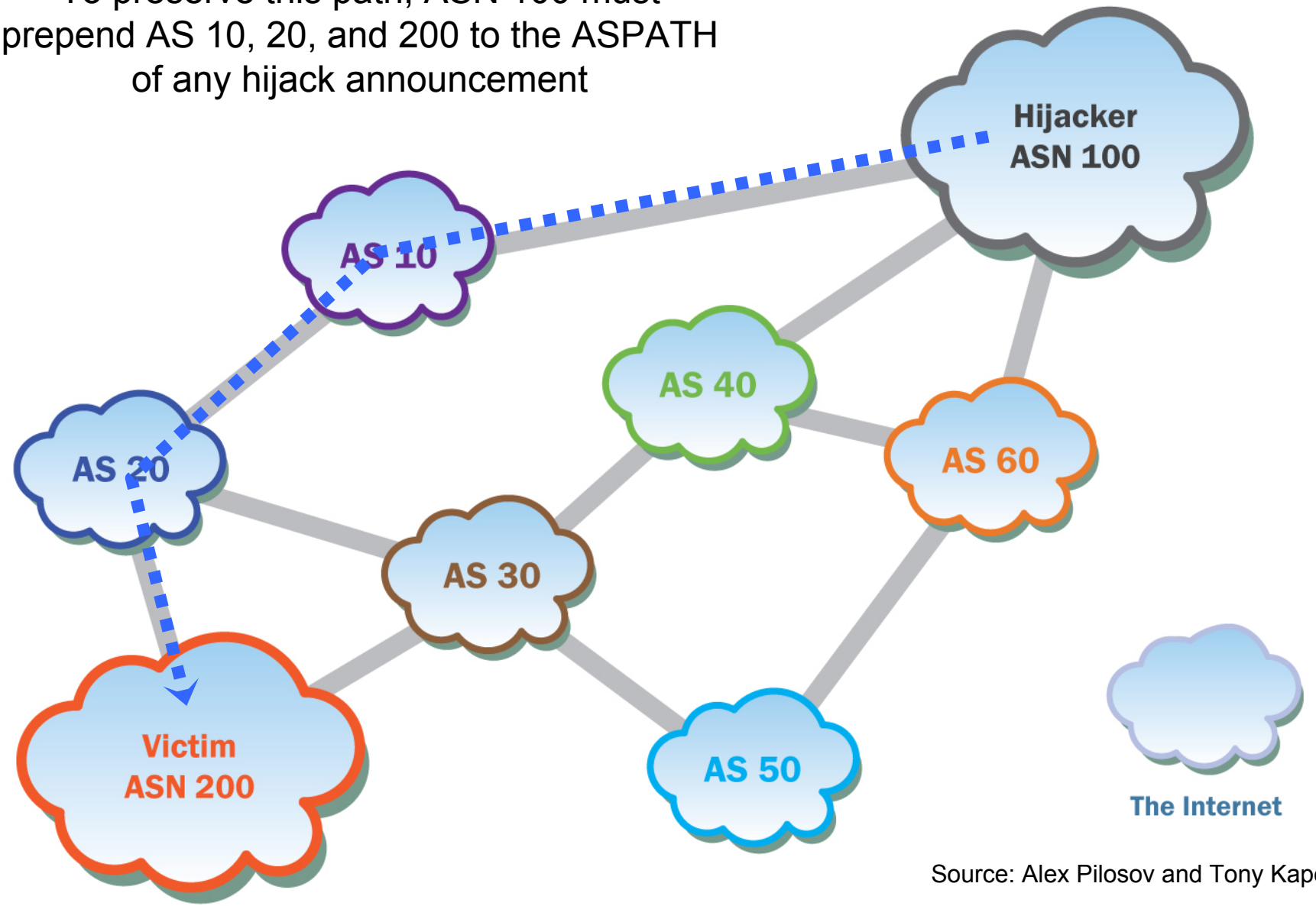
Source: Alex Pilosov and Tony Kapela

ASN 100 wants to preserve its valid route to 10.10.200.0/22 via AS10



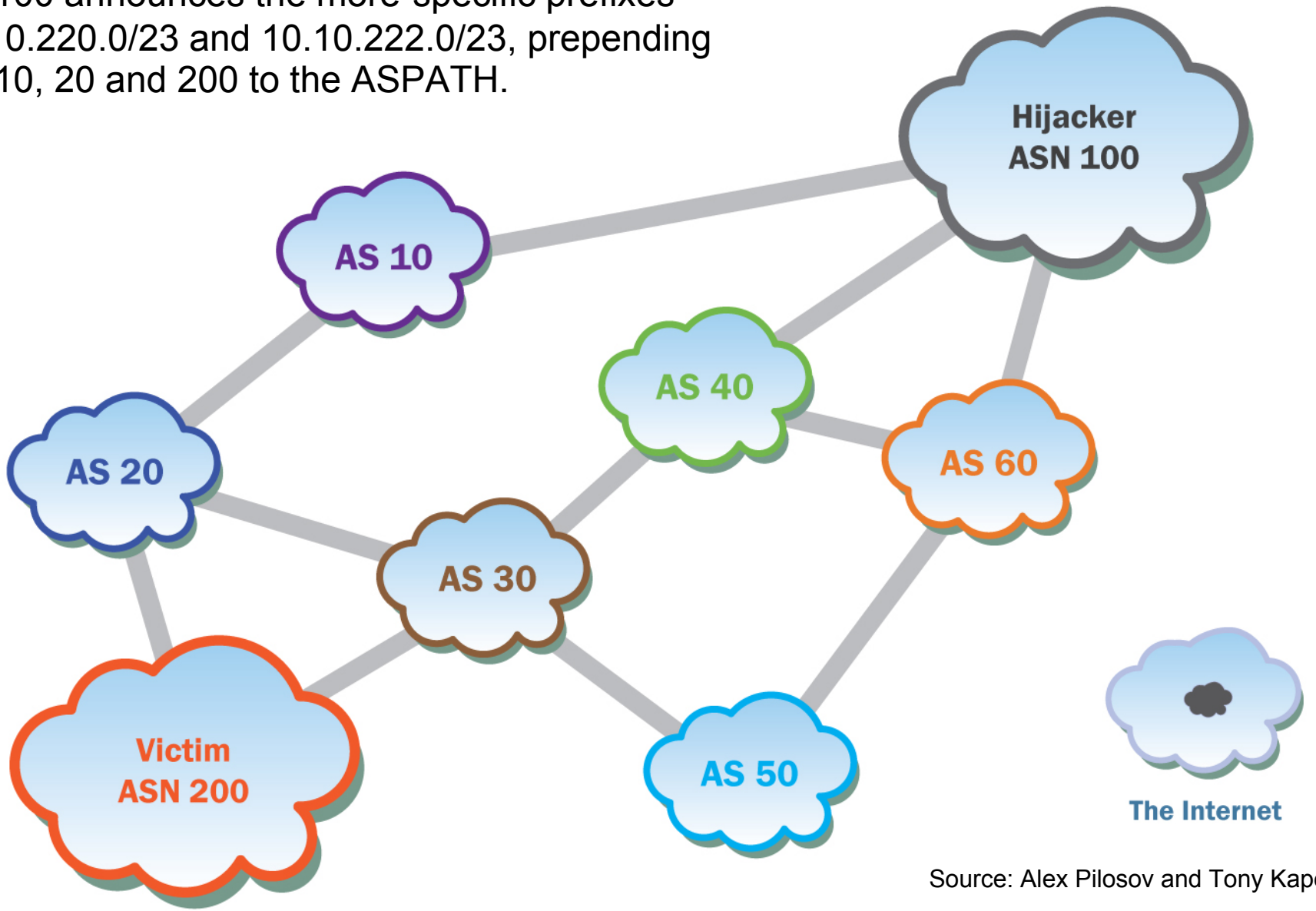
Source: Alex Pilosov and Tony Kapela

To preserve this path, ASN 100 must prepend AS 10, 20, and 200 to the ASPATH of any hijack announcement



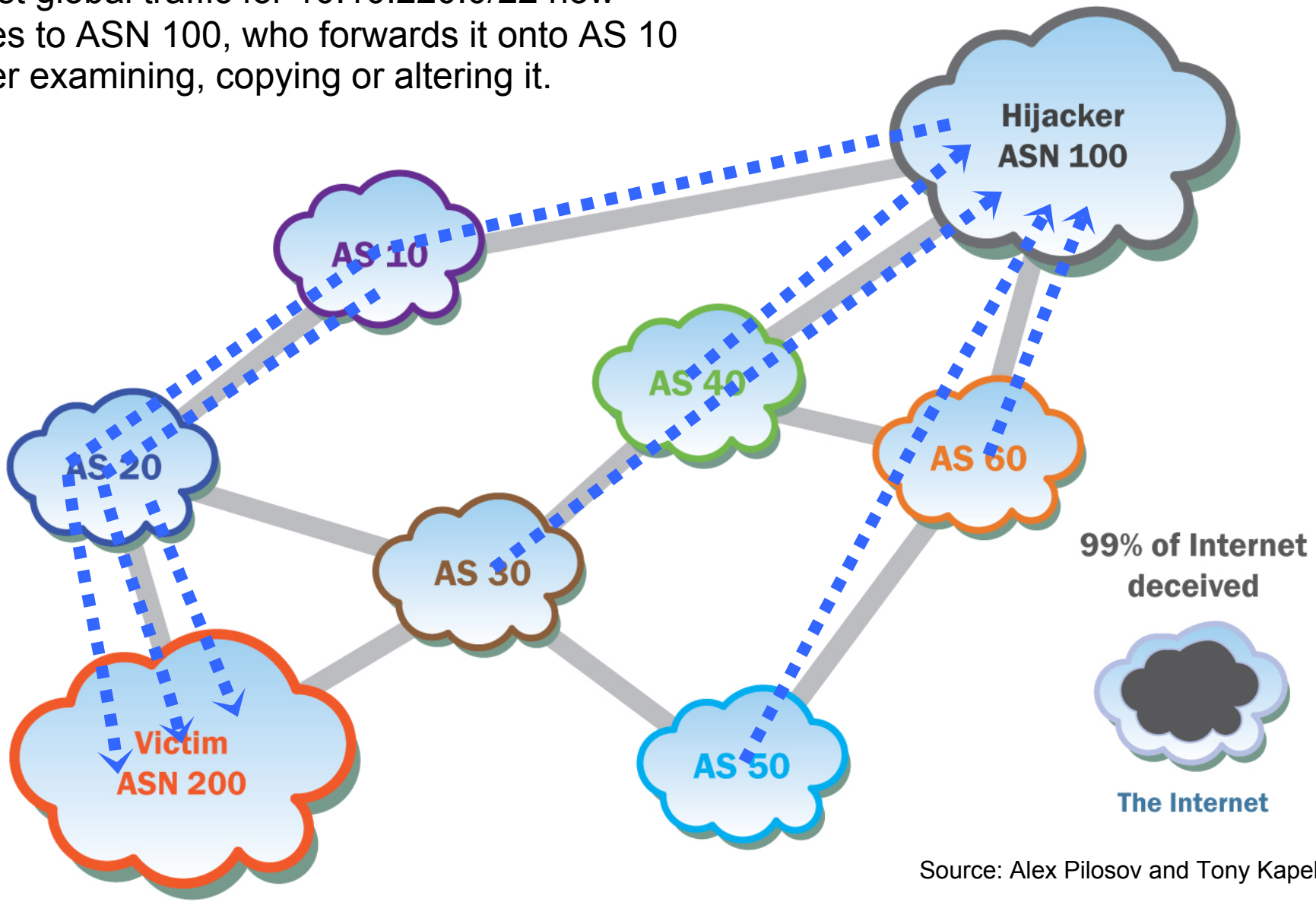
Source: Alex Pilosov and Tony Kapela

AS 100 announces the more-specific prefixes 10.10.220.0/23 and 10.10.222.0/23, prepending AS 10, 20 and 200 to the ASPATH.



Source: Alex Pilosov and Tony Kapela

Most global traffic for 10.10.220.0/22 now goes to ASN 100, who forwards it onto AS 10 after examining, copying or altering it.



Source: Alex Pilosov and Tony Kapela

How can the victim observe this?

- Victim's routes and those of at least one provider will **look normal**
- Traceroute from a public looking glass to the victim's IPs will show the hijacker
  (assuming the looking glass hasn't been blinded to the attack).
  - Traceroute depends on incrementally increasing **TTL**s
    (TTL: Time to Live – number of transmissions a packet can experience before being discarded.)
  - Hijacker can hide his presence by silently increasing TTLs for packets intended for the victim
    - Hides hijacker's routers
    - Hides hijacker's outbound routes to victim

Without TTL Adjustment

The ten hops (10-19, below) are the hijacker's **detour** through his own network. The hijacker has not obscured his tracks.


```
 2 12.87.94.9 [AS 7018] 4 msec 4 msec 8 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 4 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 8 msec 4 msec 8 msec
 5 192.205.35.42 [AS 7018] 4 msec 8 msec 4 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 24 msec 16 msec 28 msec
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 28 msec 28 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 28 msec 32 msec 32 msec

10 colo-69-31-40-107.pilosoft.com (69.31.40.107) [AS 26627] 32 msec 28 msec 28 msec
11 tge2-3-103.ar1.nyc3.us.nlayer.net (69.31.95.97) [AS 4436] 32 msec 32 msec 32 msec
12 * * *   (missing from trace, 198.32.160.134 – exchange point)
13 tge1-2.fr4.ord.llnw.net (69.28.171.193) [AS 22822] 32 msec 32 msec 40 msec
14 ve6.fr3.ord.llnw.net (69.28.172.41) [AS 22822] 36 msec 32 msec 40 msec
15 tge1-3.fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 84 msec 84 msec 84 msec
16 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 96 msec 96 msec 80 msec
17 tge1-1.fr4.lax.llnw.net (69.28.171.117) [AS 22822] 88 msec 92 msec 92 msec
18 tge2-4.fr3.las.llnw.net (69.28.172.85) [AS 22822] 96 msec 96 msec 100 msec
19 switch.ge3-1.fr3.las.llnw.net (208.111.176.2) [AS 22822] 84 msec 88 msec 88 msec

20 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 84 msec 88 msec 88 msec
21 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
22 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 88 msec 88 msec 88 msec
23 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 84 msec 84 msec
```

With TTL Adjustment

The hijacker has erased the ten hops (10-19) which went through his network.
The hijacker has obscured his tracks.


```
 2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
 3 tbr1.cgcil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 8 msec
 4 ggr2.cgcil.ip.att.net (12.123.6.29) [AS 7018] 4 msec 8 msec 4 msec
 5 192.205.35.42 [AS 7018] 8 msec 4 msec 8 msec
 6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 16 msec 12 msec *
 7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 32 msec 32 msec
 8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
 9 208.175.194.10 [AS 3561] 32 msec 32 msec 32 msec
```

Clue: a jump in **latency** from **32 msec** to **88 msec**
Depends on the distance from hijacker to victim.

```
10 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 88 msec 88 msec 84 msec
11 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
12 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 84 msec 84 msec 88 msec
13 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 88 msec 88 msec
```

Part 3: Detecting the Attack

- Is this generally visible?
- Attacker profile
- Difficulties with detection
  - You know the correct routing policies (easy)
    - Generally limited to networks under your control
    - Review of available alarm services
    - Can you attack the alarm services?
  - You don’t know the routing policies (hard)
    - A proposed global detection technique

Difficulties in observing the MITM attack

- Most Internet routers will see and prefer the hijacked routes
  - Won't be obvious among their 270,000+ routes
- Traceroutes won't show the hijacking (with TTL adjustments)
  - Independent of source location
- Latency to the victim will increase
  - Could be slight if the hijacker isn't far from the victim
- Route alarming services *might* see this if …
  - AS loop detection is disabled.
    - Otherwise the attacker can blind the alarming service itself
    - Implies service does collection only, no routing.
  - Good geographic coverage with full routes from peers.

Why the MITM attack doesn't break routing

- Content of AS paths are *not* used in routing
  - Loop detection only – avoiding endless circulation of routes
  - Length of path *might be* used in route selection – shortest preferred
- So AS paths can be arbitrary
  - Well-behaved BGP speaker prepends only its own ASN
  - Clever attacker does *not* prepend own ASN
- BGP receiver of routes
  - Retains NEXT_HOP attribute for learned routes
  - NEXT_HOP is the attribute used for actual routing
  - Only the BGP speakers adjacent to the attacker can be certain of his identity
    - Sounds a bit like DoS attacks from private IP space

Attacker profile, assume the worst …

Attacker is smart, does everything possible to avoid detection

- Ensures initial part of AS paths look legitimate
  (Uses victim's ASN and legitimate transit pattern.)
  → Victim's prefixes will appear to be announced from the correct origin
  → Victim's prefixes will appear to have the correct upstreams
- Ensures own ASN (attacker's) does not appear on paths
  → Attacker does not appear in BGP data
- Implements TTL adjustment and is "close" to the victim
  → Attacker does not appear in traceroute data
  → Negligible timing changes
- Ensures victim continues to receive traffic on all Internet connections
  → Victim will not see zero incoming traffic on any connection
  → Exercise left to the reader for victims with multiple connections

Implications for detection

- Incoming traffic to the victim
  - Looks normal to victim
  - No obvious traffic shifts or slowdowns
- Traceroutes
  - Look normal to everyone
  - No odd paths or obvious timing delays
- BGP Routes
  - Look normal to victim and victim's providers
  - Others may see a change

Victim must use an external BGP alarming service to detect the detour

Two questions to consider

- Can I detect MITM for *my* network?
  - Easy: Routing policy is presumably known or at least knowable.
- Can I detect MITM for the Internet at large?
  - Much harder: Routing policies are *not* known and probably *unknowable* for all 270,000+ prefixes

Let's start with the easy case

- Can I detect MITM for *my* network?
  - BGP MITM relies on announcing more-specifics of one or more of your prefixes.
  - You must know how *all* of your prefixes are announced.
    - Not necessarily easy in large organizations
  - You must use an external BGP alarming service, configured with the exact prefixes you expect to be seen.
  - Your alarming service must then alert you *immediately* for any unauthorized more-specifics that it sees.
    - You must then investigate any such alerts with high priority.
  - *Vigilance is key*: You have to keep your internal configuration in-sync with the configuration stored on the service.

How do BGP alarming systems work?

- All rely on BGP data feeds from *donors*.
  - BGP peering sessions are established with cooperating networks.
  - Routing updates are sent from the donors to the alarm service or to some intermediary.
  - Updates are used for data mining only, not traffic propagation.
  - Multiple donors are generally used and data is correlated to find events of interest.

Can such alarming be defeated?

- Potential attacks on alarming
  - Blind the alarming service:

    Possible only if they do not disable AS loop detection.
  - Blind the peers of the alarming service:

    Practical only for a limited number of peers.
  - Limit the scope of the attack:

    Possible only in geographies with limited points of egress and no peers for the alarming service.

Generally with a well-designed alarming system such attacks will be either impossible or extremely difficult. Not worth considering further.

BGP Alarming Services

- IAR (Internet Alert Registry)
- PHAS (Prefix Hijack Alert System)
- RIPE NCC MyASN Service
- BGPmon
- WatchMY.NET
- Renesys Routing Intelligence

All of these services will do the job, but …

there are significant differences:

- cost: free vs. commercial
- support: 24x7 vs. “as-is”; SLA vs. nothing
- redundancy: wrt data centers and personnel
- response time: seconds vs. hours or even days
- alarm types: basic vs. advanced vs. arbitrary regular expressions
- data sources: scope and diversity
- initial configuration: manual vs. auto-discovery
- configuration updates: manual vs. API access
- accuracy: rate of false positives

So what is the big deal?

- The problem is solved, right? Pick a service, configure it and sleep soundly.
  - Not exactly. How do you identify an attacker?
  - And the entire planet is *not* going to start using a BGP alarm service tomorrow.
- Enterprises and governments have an interest in knowing if partners, agencies, countries and others are under attack.
  - If I send data to you, I certainly do not want it reach you via a hostile third party.

This brings us to our second question

- Can I detect MITM for the Internet at large?
  - Routing policy is *not* known for any random set of networks.
  - Establish a baseline by observing the networks of interest over some time period: a day, a week, a month …
  - Use this baseline to configure an alarming system
  - Alarm on changes from baseline, such as new more-specifics
  - Re-establish new baseline periodically.
- Does this work?
  - No. Too many new more-specifics.
  - How do you differentiate legitimate traffic engineering from attacks?

Need more information

- When you know correct routing policy, you need *only one fact* to set off an alarm:
  - A more-specific of one of my prefixes has been announced on the Internet which wasn't authorized my me!
  - Ring the alarms! No false-positives here! Fire in the hole!
- Without correct policy, the situation is more complicated.
  - You notice a more-specific you haven't seen before. So what?
    - Over the last 7 months, the *median daily* number of "new" more-specifics that weren't active the previous day: 700
  - Need more information to determine if something new is hostile.
    - We have all the AS paths seen via the more-specific.
    - What can they tell us?

AS Paths from MITM Attacks

- Each AS path on a hijacked more-specific will consist of *two segments*:
  - Artificial Segment

    AS segment created by the attacker to blind certain others
  - Real Segment

    Created as the more-specific leaves the attacker and propagates through the Internet.

What can be wrong with these AS paths?

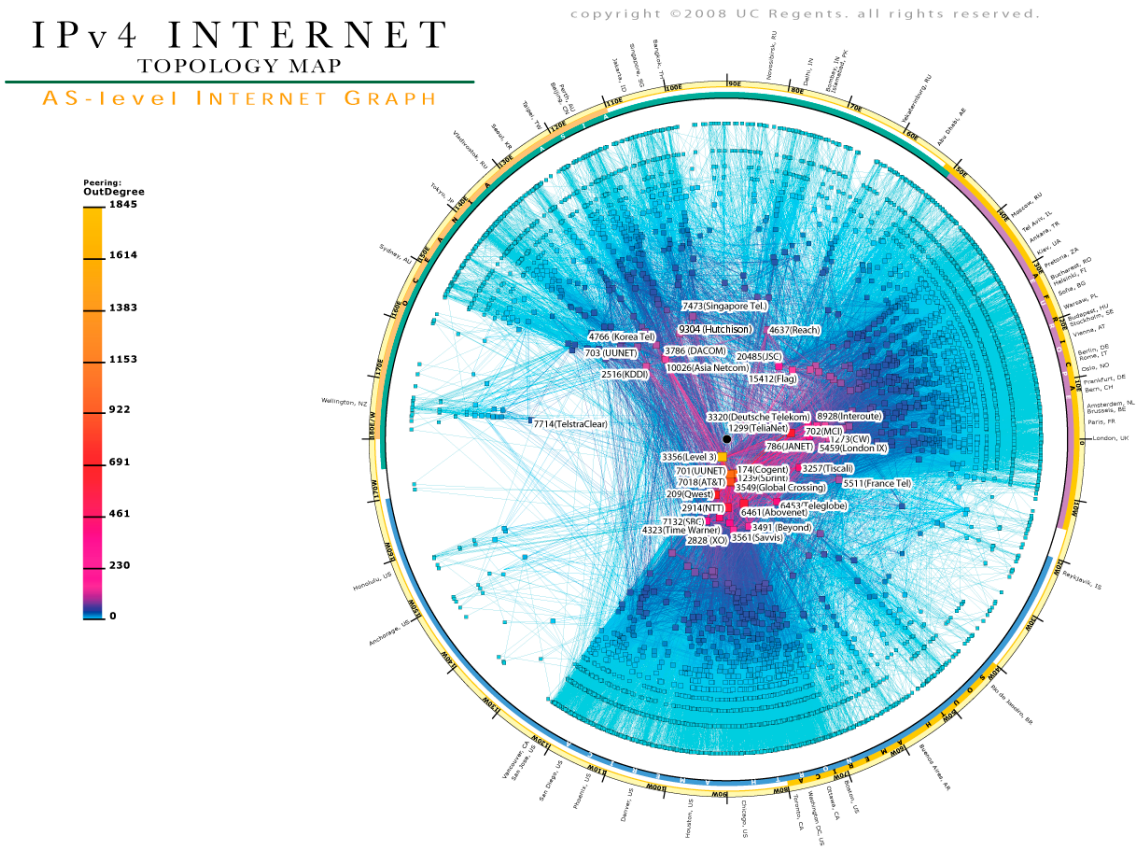
- Artificial segment looks “real” as it was constructed to conform to a transit pattern from the victim, but …
  - *None* of the ASes on the artificial segment will have seen or propagated the new more-specific prefix.
  - Transition from Artificial to Real segments *may* introduce a never before seen AS-AS adjacency.
- Real segment was created organically
  - And so is quite legitimate. Not useful here.
- But the two segments (or sub-segments thereof) might “look strange” together.

What can be wrong with these AS paths?

- Artificial segment looks “real” as it was constructed to conform to a transit pattern from the victim, but …
  - *None* of the ASes on the artificial segment will have seen or propagated the new more-specific prefix.
  - Transition from Artificial to Real segments *may* introduce a never before seen AS-AS adjacency.
- Real segment was created organically
  - And so is quite legitimate. Not useful here.
- But the two segments (or sub-segments thereof) might “look strange” together.

This is where peer selection for alarms matters

- The AS graph of the Internet is quite sparse, but its *core* is richly connected.



Source: caida.org

Internet AS Graph Statistics

- Globally, you can observe about …
  - 30,800 ASes
  - 105,000 AS-AS edges
  - 13,290 ASes announcing only one prefix, and
  - an average AS path length of 4.6
- With *at most a few hundred* carefully selected peers, it is possible to be *at most one hop away* from nearly every AS on the planet.
  - Implies most AS paths will contain several peers
  - Artificial segments are likely to contain a peer

  (Renesys observes at least 2 peers on more than 93% of the AS paths we receive.)

General MITM Detection Idea

- None of the ASes on the artificial segment will have seen or *propagated* the new more-specific.
- Detection idea:
  - When you see a new more-specific, check out all the associated AS paths for peers
  - Any peer *not announcing* the more-specific could indicate the presence of an artificially created AS path segment. (We'll call these *silent peers* with respect to this more-specific.)
  - Sound the alarm!

Can this result in false positives?

- Yes, when *BGP manipulation* is used for traffic engineering.
- Suppose you do *not* want a prefix to traverse a particular provider, say Sprint (AS 1239).
  - Prepend 1239 to the announcement.
  - Sprint will not see the announcement.
  - This is perfectly legitimate, although uncommon.

Part 4: Case Studies

- MITM Detection Algorithm
- The DEFCON attack
- Defense after detection?
- Seven-month historical search for MITM attacks
  - 1 July 2008 – 31 January 2009

MITM Detection Algorithm

For each day N

Determine all prefixes visible on day N-1.

(This is your *baseline*.)

For each prefix P seen on day N that is a *new more-specific* of a baseline prefix

For each AS path $\mathcal{P}$ associated with P

If $\mathcal{P}$ contains a silent peer wrt P and P was not quickly withdrawn (ignore short-lived announcements)

Sound the alarm!

DEFCON Attack – 10 August 2008

Legitimate prefix: 24.120.56.0/22

- Announced by Sparkplug Inc. (AS 20195)
- Sparkplug has one provider, SWITCH Comm. (AS 23005)

Hijacked more-specific: 24.120.56.0/24

- Announced by Pilosoft, Inc. (AS 26627)
- One path from Pilosoft and Sparkplug blinded to attack

DEFCON Attack – 10 August 2008, 19:33:18 UTC
(prior to attack)

Renesys observed announcements of 24.120.56.0/22

count		AS Paths		
90	R	19151	23005	20195
64	R	22822	23005	20195
37	R	3356	23005	20195
14	R		23005	20195
5	R	4323	23005	20195

… and many others

where R = any one of numerous Renesys peers
20195 = Victim (Sparkplug Las Vegas, Inc.)
23005 = Victim's sole provider (SWITCH Comm. Group)

DEFCON Attack – 10 August 2008, 19:34:47 UTC
(80 seconds later)

Renesys observed announcements of 24.120.56.0/24

count	AS Paths
23	R 3561 26627 4436 22822 23005 20195
21	R 3356 3561 26627 4436 22822 23005 20195
11	R 3549 3561 26627 4436 22822 23005 20195
8	R 1239 3561 26627 4436 22822 23005 20195
5	R 701 3561 26627 4436 22822 23005 20195

real segments | artificial segments

… and many others

where R = any one of numerous Renesys peers
20195 = Victim (Sparkplug Las Vegas, Inc.)
26627 = Attacker (Pilosoft, Inc.)
3561 = Attacker's provider (Savvis)

What is wrong with these AS paths?

Example path

R 3356 3561 26627 4436 22822 23005 20195

real segment artificial segment

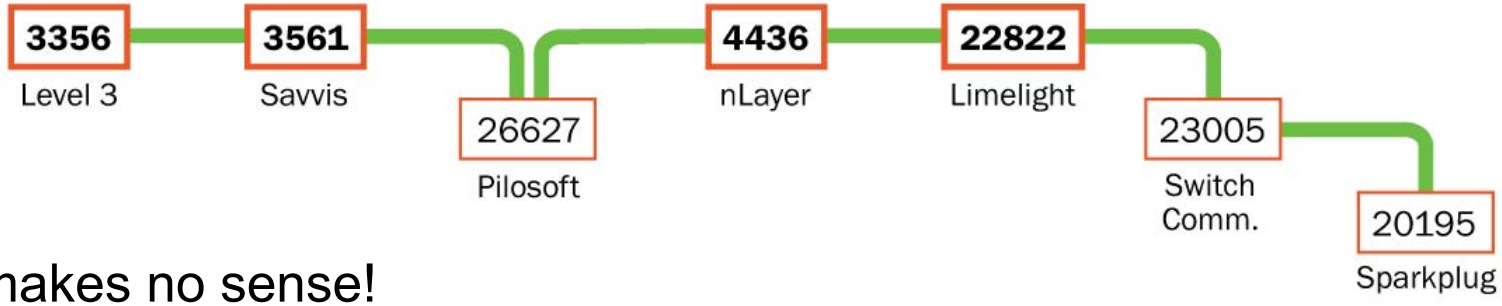
- Attack is easily detected
  - Silent Renesys peers exist
- Attacker is visible in the paths (AS 26627)
- More clever attack *might* have omitted AS 26627
  - But that would have introduced the *new edge* 3561_4436
- Artificial segment is *globally unvarying,* but …
  - AS 23005 had 4 different providers at the time
  - AS 22822 had 8 providers and 147 peers

What else is wrong with these paths?

Example path

R 3356 3561 26627 4436 22822 23005 20195

Draw the path with peers on the same level and customers hanging off of their providers. (Requires knowing all AS-AS relationships.)



Path makes no sense!

AS 26627 has 2 providers (AS 3561 & AS 4436), but is transiting traffic for unrelated AS 20195

Even hiding AS 26627, the path contains multiple peering links

Path violates *valley-free property*[1] of Internet routing

[1] The AS in the valley is transiting traffic for free, i.e., throwing out money.

Filtering out false positives

Proposed method generates too many false positives.

For suspected hijacks we need to consider:

- Noisy data
  - A more-specific might be seen by only a few peers
  - A silent peer might exist on only a few paths
- AS paths
  - Artificial segments should exist
    - Suspect paths should end with the same sequence of ASNs
  - Odd paths
    - Paths will almost certainly violate the valley-free property or introduce never before seen AS edges.

MITM Detection Improvements

Approach to handling these cases:

- Noisy data
  - More-specific must be seen by at least 15% of Renesys peers
  - 90% of related paths must have a silent peer
- AS paths
  - Artificial segments should exist
    - Ignore more-specifics unless 90% of paths end with the same 2 ASNs (artificial segment length > 2 unless victim and attacker share a provider)
  - Odd paths should exist
    - Ignore more-specifics unless *some paths* violate the valley-free property or introduce never before seen AS edges.

Historical search for MITM attacks
1 July 2008 – 31 January 2009 (215 days)

Filter (cumulatively applied)	**Count**
Original detection algorithm	10,442
Globally visible	209
Suspect artificial segment ≥ 2	178
Abnormal paths	3

Suspect Announcements

We are confident that the set of 178 suspect announcements *must* contain all *global* MITM attacks in this time period.

- Silent peers will be present due to Renesys coverage
- Hijack will be widely visible
- Artificial segments must be of length ≥ 2

Classifying the 178 Suspect Announcements

- Traffic Engineering
  - 119 originated in Costa Rica, all with single silent peer (Tier-1) on the paths. Costa Rica seems to be avoiding this provider.
  - 2 originated from HostMySite, blinding a major provider
- BGP Communities
  - 25 had silent peers since communities were used to limit the scope of their announcements.
- Miscellaneous
  - 29 had random other unsuspicious causes
- Abnormal Paths
  - 3 were in this category and warranted further investigation

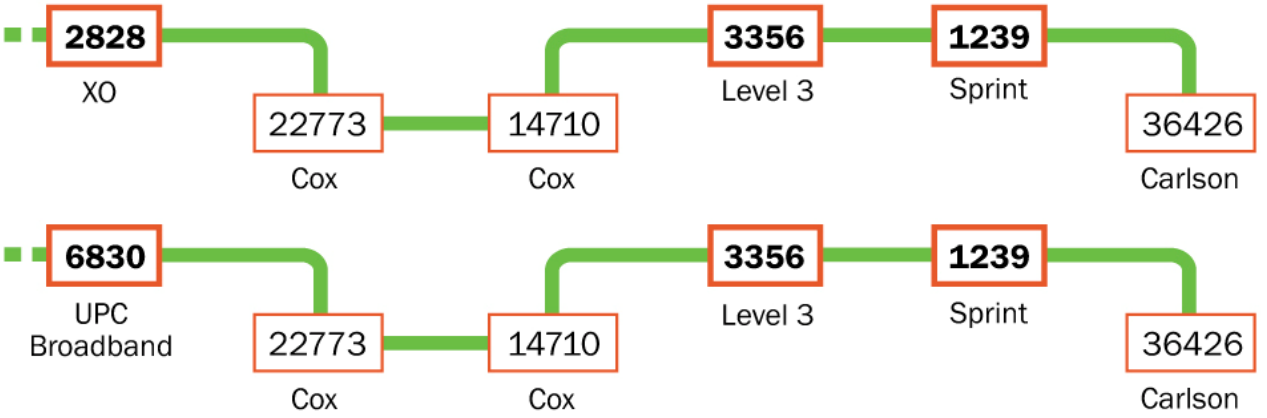
Highly Suspect Announcements

The three cases that satisfy *all* conditions:

- The DEFCON attack itself
  - 10 August 2008, 19:34:47 UTC
- Carlson Systems LLC (AS 36426)
  - 29 November 2008, 16:51:53 UTC
  - More-specific 63.161.162.0/24 of 63.160.0.0/12
  - 63.160.0.0/12 is originated by Sprint (AS 1239)
- Cizgi Telekomunikasyon (AS 34619)
  - 3 December 2008, 17:25:00 UTC
  - More-specific 94.73.129.0/24 of 94.73.128.0/18
  - 94.73.128.0/18 is originated by Cizgi

Carlson Systems LLC (AS 36426)

- Paths start out with long artificial segments.
- Paths are insane:



- Many frequent withdrawals and re-announcements
- Largely gone after 35 minutes
- Carlson claims to have been testing failover between Sprint and Cox at the time

Cizgi Telekomunikasyon (AS 34619)

- Paths all have the following form:

- Cizgi has both TTnet and ILETISIM as providers
- Largely gone after 20 minutes
- Traffic engineering on the part of Cizgi to avoid TTnet?

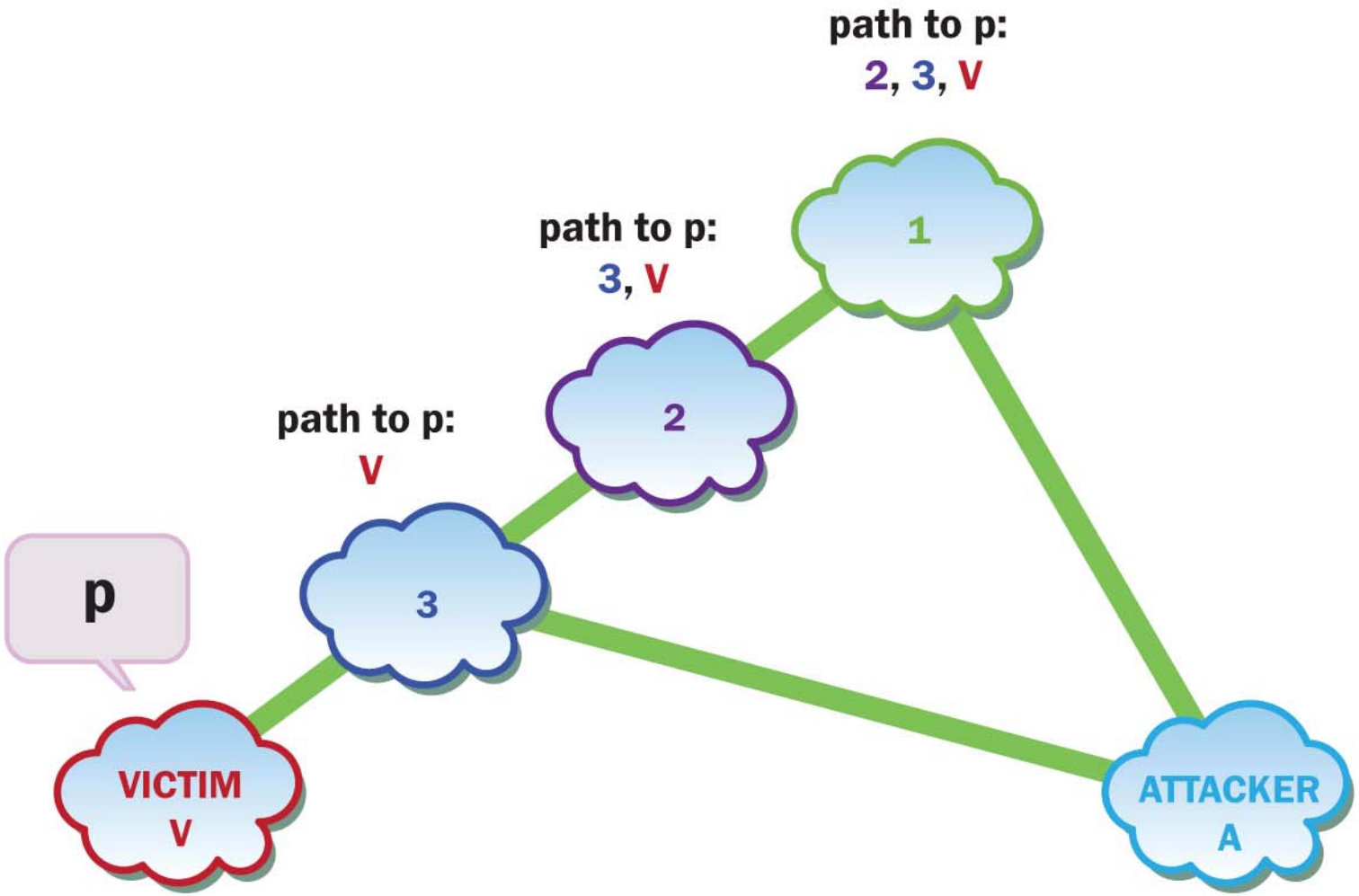
Defending against MITM
– You have detected an attack, now what?

As with any hijack, you have two options:

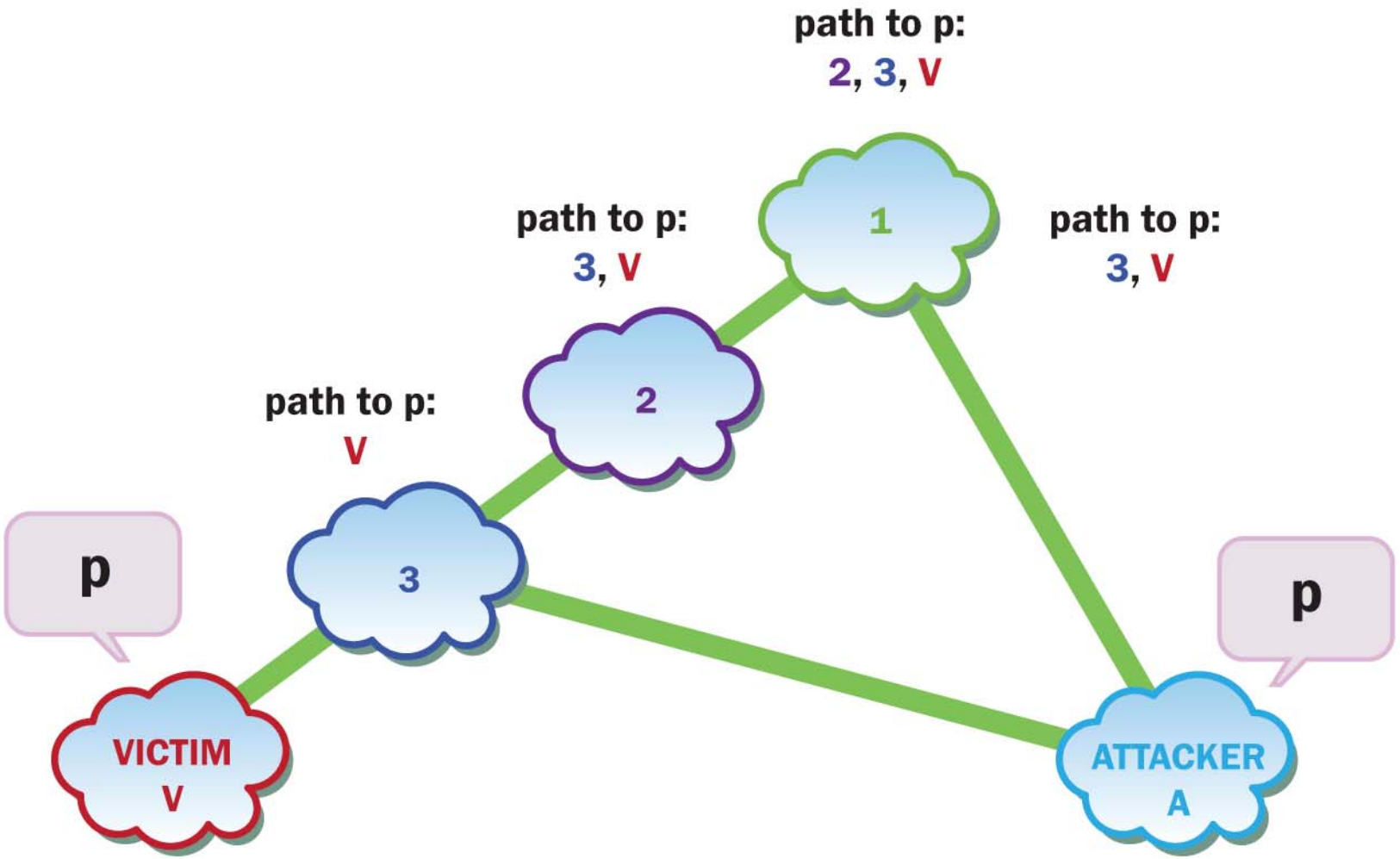
1) Announce more-specifics of the hijacked more-specific
   - Arms race, not a guaranteed win.
2) Get a cooperative upstream to filter the attacker –
   but who is the attacker?
   - Attacker ASN might not be on the AS paths
   - Examine all paths containing the more-specific
     - Differentiate real (varying) from artificial (constant) segments
     - Contact first non-varying provider on the real segment: this is the attacker's provider
     - Attacker's provider examines NEXT_HOP to definitively identify the attacker
     - Synthetic paths are the smoking gun: This wasn't an innocent error.

Can we avoid detection, even if the victim is alarming on changes?

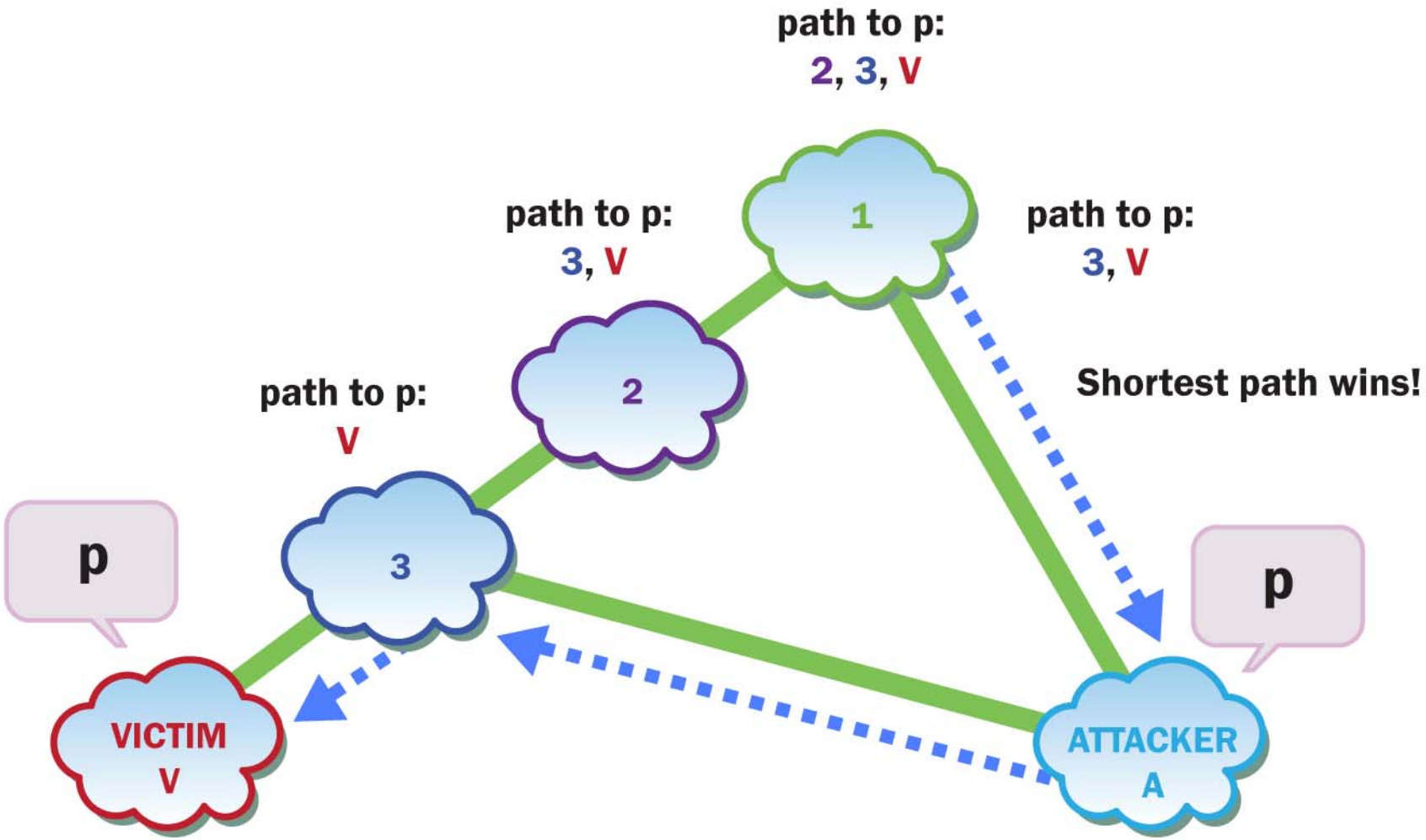
- More-specifics are our trigger for digging deeper
- Can I steal traffic *without* announcing a more-specific?
- Yes, if you are very lucky
  - Victim announces prefix P
  - Attacker announces the same prefix P
  - Who gets the traffic?
    - In the absence of specific overrides, shortest AS path wins.
    - As we saw, engineered AS paths can be rather long.
    - We can still steal traffic in this case, but success depends on …
      - attacker's distance from victim, and
      - victim's distance from the Internet's core



Victim V announces prefix "p" to its provider 3.



Attacker A announces prefix "p" to provider 1 with bogus path "3, V".



Provider 1 sends all of V's traffic to A, who passes it on to V via provider 3.

The Good News …

- MITM is not yet appearing in the wild.
- MITM did not appear in the wild in the month before its public disclosure at DEFCON.
- MITM is 100% detectable for *your* networks if you subscribe to an external service.
- MITM is also detectable for the global Internet.
- False positives are relatively rare.

Disclaimer: The above is universally true, except for carefully constructed corner cases.

The Bad News …

- As shown at DEFCON, *any* prefix can be hijacked without breaking end-to-end connectivity.
- This attack is still relatively unknown.
- You can only react to hijacks *after the fact*, using a service.
- Your service provider must satisfy many demands:
  - Enough sensors with *full routes* from enough places
  - Non-standard BGP configuration – no AS loop detection
  - Sophisticated real-time analytics
- This is very easy to get wrong and thereby miss attacks.
- There is no short-term fix here for BGP.

Thank You