

## Interdomain Routing Security

Mike Freedman

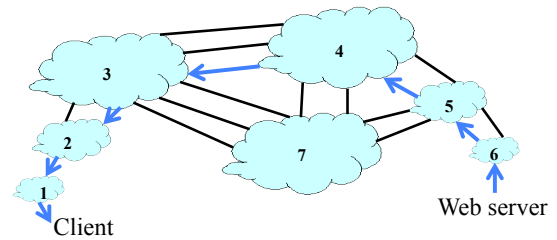
COS 461: Computer Networks

Lectures: MW 10-10:50am in Architecture N101

<http://www.cs.princeton.edu/courses/archive/spr13/cos461/>

## Interdomain Routing

- AS-level topology
  - Nodes are Autonomous Systems (ASes)
  - Edges are links and business relationships



## Border Gateway Protocol (BGP)

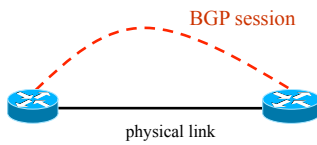
- ASes exchange reachability information
  - Destination: block of addresses (an "IP prefix")
  - AS path: sequence of ASes along the path
- Policies configured by network operators
  - Path selection: which of the paths to use?
  - Path export: which neighbors to tell?



## BGP Session Security

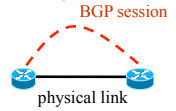
## TCP Connection Underlying BGP Session

- **BGP session runs over TCP**
  - TCP connection between neighboring routers
  - BGP messages sent over TCP connection
  - Makes BGP vulnerable to attacks on TCP



## Attacks on Session Security

- **Confidentiality**
  - Eavesdropping by tapping the link
  - Inferring routing policies and stability
- **Integrity**
  - Tampering by dropping, modifying, adding packets
  - Changing, filtering, or replaying BGP routes
- **Availability**
  - Resetting the session or congesting the link
  - Disrupting communication and overloading routers



## Defending Session Security is Easy

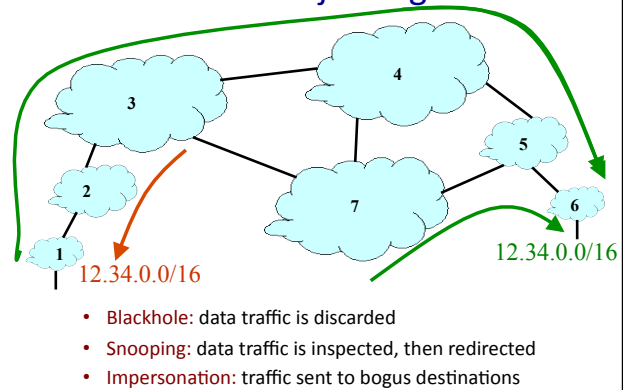
- **BGP routing information is propagated widely**
  - Confidentiality isn't all that important
- **Two end-points have a business relationship**
  - Use known IP addresses and ports to communicate
  - Can agree to sign and encrypt messages
- **Limited physical access to the path**
  - Direct physical link, often in same building
- **Low volume of special traffic**
  - Filter packets from unexpected senders
  - Can give BGP packets higher priority

Validity of the routing information:  
Origin authentication

## IP Address Ownership and Hijacking

- **IP address block assignment**
  - ICANN -> Regional Internet Registries -> ISPs
- **Proper origination of a prefix into BGP**
  - By the AS who owns the prefix
  - ... or, by its upstream provider(s) in its behalf
- **However, what's to stop someone else?**
  - Prefix hijacking: another AS originates the prefix
  - BGP does not verify that the AS is authorized
  - Registries of prefix ownership are inaccurate

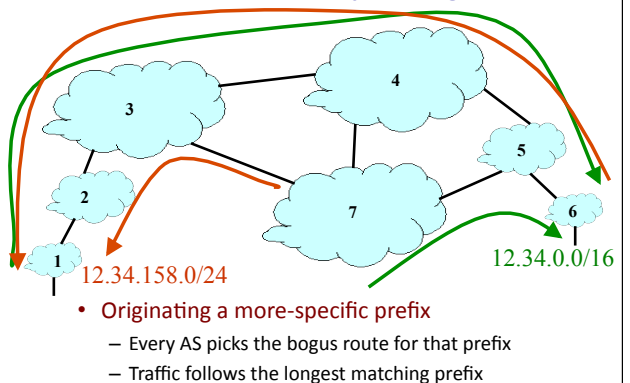
## Prefix Hijacking



## Hijacking is Hard to Debug

- **The victim AS doesn't see the problem**
  - Picks its own route, might not learn the bogus route
- **May not cause loss of connectivity**
  - Snooping, with minor performance degradation
- **Or, loss of connectivity is isolated**
  - E.g., only for sources in parts of the Internet
- **Diagnosing prefix hijacking**
  - Analyzing updates from many vantage points
  - Launching traceroute from many vantage points

## Sub-Prefix Hijacking



## How to Hijack a Prefix

13

- **The hijacking AS has**
  - Router with BGP session(s)
  - Configured to originate the prefix
- **Getting access to the router**
  - Network operator makes configuration mistake
  - Disgruntled operator launches an attack
  - Outsider breaks in to the router and reconfigures
- **Getting other ASes to believe bogus route**
  - Neighbor ASes do not discard the bogus route
  - E.g., not doing protective filtering

## YouTube Outage on Feb 24, 2008

14

- **YouTube (AS 36561): 208.65.152.0/22**
- **Pakistan Telecom (AS 17557)**
  - Government order to block access to YouTube
  - Announces 208.65.153.0/24 to PCCW (AS 3491)
  - All packets to YouTube get dropped on the floor
- **Mistakes were made**
  - AS 17557: announce to everyone, not just customers
  - AS 3491: not filtering routes announced by AS 17557
- **Lasted 100 minutes for some, 2 hours for others**

## Timeline (UTC Time)

15

- 18:47:45: First evidence of hijacked /24 route in Asia
- 18:48:00: Several big trans-Pacific providers carrying route
- 18:49:30: Bogus route fully propagated
- 20:07:25: YouTube advertising /24 to attract traffic back
- 20:08:30: Many (but not all) providers are using valid route
- 20:18:43: YouTube announces two more-specific /25 routes
- 20:19:37: Some more providers start using the /25 routes
- 20:50:59: AS 17557 starts prepending (“3491 17557 17557”)
- 20:59:39: AS 3491 disconnects AS 17557
- 21:00:00: Videos of cats flushing toilets are available again!

## Another Example: Spammers

16

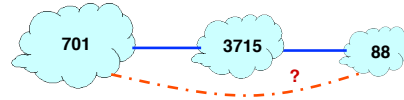
- **Spammers sending spam**
  - Form a (bidirectional) TCP connection to mail server
  - Send a bunch of spam e-mail, then disconnect
- **But, best not to use your real IP address**
  - Relatively easy to trace back to you
- **Could hijack someone’s address space**
  - But you might not receive all the (TCP) return traffic
- **How to evade detection**
  - Hijack unused (i.e., unallocated) address block
  - Temporarily use the IP addresses to send your spam

## BGP AS Path

17

## Bogus AS Paths

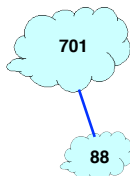
- Remove ASes from the AS path
  - E.g., turn “701 3715 88” into “701 88”
- Motivations
  - Attract sources that normally try to avoid AS 3715
  - Help AS 88 look like it is closer to the Internet’s core
- Who can tell that this AS path is a lie?
  - Maybe AS 88 *does* connect to AS 701 directly



18

## Bogus AS Paths

- Add ASes to the path
  - E.g., turn “701 88” into “701 3715 88”
- Motivations
  - Trigger loop detection in AS 3715
    - Denial-of-service attack on AS 3715
    - Or, blocking unwanted traffic coming from AS 3715!
  - Make your AS look like it has richer connectivity
- Who can tell the AS path is a lie?
  - AS 3715 could, if it could see the route
  - AS 88 could, but would it really care?



19

## Bogus AS Paths

- Adds AS hop(s) at the end of the path
  - E.g., turns “701 88” into “701 88 3”
- Motivations
  - Evade detection for a bogus route
  - E.g., by adding the legitimate AS to the end
- Hard to tell that the AS path is bogus...
  - Even if other ASes filter based on prefix ownership



20

## Invalid Paths

21

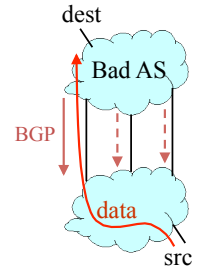
- **AS exports a route it shouldn't**
  - AS path is a valid sequence, but violated policy
- **Example: customer misconfiguration**
  - Exports routes from one provider to another
- **Interacts with provider policy**
  - Provider prefers customer routes
  - Directing all traffic through customer
- **Main defense**
  - Filtering routes based on prefixes and AS path



## Missing/Inconsistent Routes

22

- **Peers require consistent export**
  - Prefix advertised at all peering points
  - Prefix advertised with same AS path length
- **Reasons for violating the policy**
  - Trick neighbor into “cold potato”
  - Configuration mistake
- **Main defense**
  - Analyzing BGP updates or traffic for signs of inconsistency



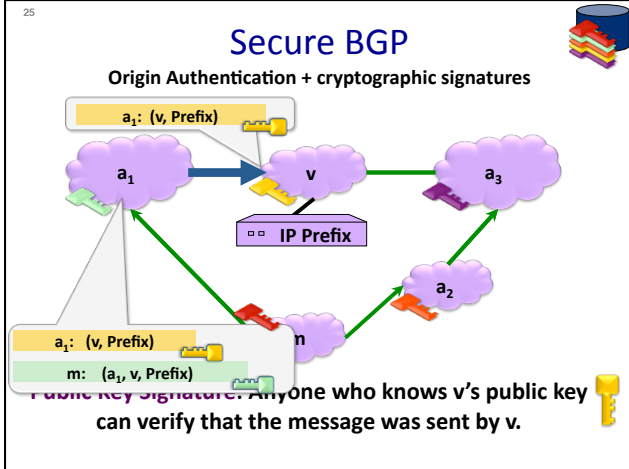
## BGP Security Today

23

- **Applying “best common practices” (BCPs)**
  - Securing the session (authentication, encryption)
  - Filtering routes by prefix and AS path
  - Packet filters to block unexpected control traffic
- **This is not good enough**
  - Depends on vigilant application of BCPs
  - Doesn't address fundamental problems
    - Can't tell who owns the IP address block
    - Can't tell if the AS path is bogus or invalid
    - Can't be sure the data packets follow the chosen route

## Proposed Enhancements to BGP

24



- 26
- ## S-BGP Secure Version of BGP
- **Address attestations**
    - Claim the right to originate a prefix
    - Signed and distributed out-of-band
    - Checked through delegation chain from ICANN
  - **Route attestations**
    - Distributed as an attribute in BGP update message
    - Signed by each AS as route traverses the network
  - **S-BGP can validate**
    - AS path indicates the order ASes were traversed
    - No intermediate ASes were added or removed

- 27
- ## S-BGP Deployment Challenges
- **Complete, accurate registries of prefix "owner"**
  - **Public Key Infrastructure**
    - To know the public key for any given AS
  - **Cryptographic operations**
    - E.g., digital signatures on BGP messages
  - **Need to perform operations quickly**
    - To avoid delaying response to routing changes
  - **Difficulty of incremental deployment**
    - Hard to have a "flag day" to deploy S-BGP

- 28
- ## Incrementally Deployable Solutions?
- **Backwards compatible**
    - No changes to router hardware or software
    - No cooperation from other ASes
  - **Incentives for early adopters**
    - Security benefits for ASes that deploy the solution
    - ... and further incentives for others to deploy
  - **What kind of solutions are possible?**
    - Detecting suspicious routes
    - ... and then filtering or depreferencing them

## Detecting Suspicious Routes

- **Monitoring BGP update messages**
  - Use past history as an implicit registry
- **E.g., AS that announces each address block**
  - Prefix 18.0.0.0/8 usually originated by AS 3
- **E.g., AS-level edges and paths**
  - Never seen the subpath “7018 88 1785”
- **Out-of-band detection mechanism**
  - Generate reports and alerts
  - Internet Alert Registry: <http://iar.cs.unm.edu/>
  - Prefix Hijack Alert System: <http://phas.netsec.colostate.edu/>

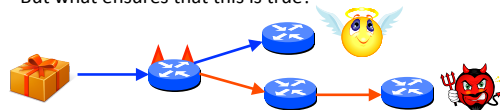
## Avoiding Suspicious Routes

- **Soft response to suspicious routes**
  - Prefer routes that agree with the past
  - Delay adoption of unfamiliar routes when possible
- **Why is this good enough?**
  - Some attacks will go away on their own
  - Let someone else be the victim instead of you
  - Give network operators time to investigate
- **How well would it work?**
  - If top ~40 largest ASes applied the technique
  - ... most other ASes are protected, too

## What About Packet Forwarding?

## Control Plane vs. Data Plane

- **Control plane**
  - BGP security concerns validity of routing messages
  - I.e., did the BGP message follow the sequence of ASes listed in the AS-path attribute
- **Data plane**
  - Routers forward data packets
  - Supposedly along path chosen in the control plane
  - But what ensures that this is true?





## Data-Plane Attacks, Part 1

33

- **Drop packets in the data plane**
  - While still sending the routing announcements
- **Easier to evade detection**
  - Especially if you only drop some packets
  - Like, oh, say, BitTorrent or Skype traffic
- **Even easier if you just slow down some traffic**
  - How different are normal congestion and an attack?
  - Especially if you let traceroute packets through?

## Data-Plane Attacks, Part 2

34

- **Send packets in a different direction**
  - Disagreeing with the routing announcements
- **Direct packets to a different destination**
  - E.g., one the adversary controls
- **What to do at that bogus destination?**
  - Impersonate the legitimate destination
  - Snoop on traffic and forward along to real destination
- **How to detect?**
  - Traceroute? Longer than usual delays?
  - End-to-end checks, like site certificate or encryption?

## Data-Plane Attacks are Harder

35

- **Adversary must control a router along the path**
  - So that the traffic flows through him
- **How to get control a router**
  - Buy access to a compromised router online
  - Guess the password, exploit router vulnerabilities
  - Insider attack (disgruntled network operator)
- **Malice vs. greed**
  - Malice: gain control of someone else's router
  - Greed: Verizon DSL blocks Skype to encourage me to use (Verizon) landline phone

## What's the Internet to Do?

36

## BGP is So Vulnerable

37

- **Several high-profile outages**
  - <http://merit.edu/mail.archives/nanog/1997-04/msg00380.html>
  - [http://www.renesys.com/blog/2005/12/internetwide\\_nearcatastrophela.shtml](http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml)
  - [http://www.renesys.com/blog/2006/01/coned\\_steals\\_the\\_net.shtml](http://www.renesys.com/blog/2006/01/coned_steals_the_net.shtml)
  - [http://www.renesys.com/blog/2008/02/pakistan\\_hijacks\\_youtube\\_1.shtml](http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml)
  - [http://www.theregister.co.uk/2010/04/09/china\\_bgp\\_interweb\\_snafu/](http://www.theregister.co.uk/2010/04/09/china_bgp_interweb_snafu/)
- **Many smaller examples**
  - Blackholing a single destination prefix
  - Hijacking unallocated addresses to send spam
- **Why isn't it an even bigger deal?**
  - Really, most big outages are configuration errors
  - Most bad guys want the Internet to stay up

## BGP is So Hard to Fix

38

- **Complex system**
  - Large, with around 40,000 ASes
  - Decentralized control among competitive Ases
- **Hard to reach agreement on the right solution**
  - S-BGP with PKI, registries, and crypto?
  - Who should be in charge of running PKI & registries?
  - Worry about data-plane attacks or just control plane?
- **Hard to deploy the solution once you pick it**
  - Hard enough to get ASes to apply route filters
  - Now you want them to upgrade to a new protocol

## Conclusions

39

- **Internet protocols designed based on trust**
  - Insiders are good guys, bad guys on the outside
- **Border Gateway Protocol is very vulnerable**
  - Glue that holds the Internet together
  - Hard for an AS to locally identify bogus routes
  - Attacks can have very serious global consequences
- **Proposed solutions/approaches**
  - Secure variants of the Border Gateway Protocol
  - Anomaly detection, with automated response
  - Broader focus on data-plane availability