

Agenda

- Protocol evolution
- Major threats and operational issues
- Current situation
- BGP security requirements
- Mechanism specifications
- Threat scenarios
- Future developments

State Diagram

1. initial state is DISCONNECT
2. OPEN - SEND



longhead@cisco.com
yakov@IBM.COM

415-326
(914) 045-3836

1989

1. link type error in open
- my view of current link type (1 byte)
2. unknown auth type code
- no data
3. authentication failure (no data)
4. update error - data is block is

~~routing trap in update~~
~~two phase error in update~~

data is subcode (2 byte) follows
update block is variable (1 byte)

- subcodes -
1. invalid network field
 2. invalid first hop gw
 3. invalid direction code
 4. invalid AS
 5. routing loop
 6. two-phase error

5. reconnection out of sync - data is lost (TCP close after packet sent)
6. open continued
7. invalid block type (data is 1 byte)
8. invalid version number (data is 1 byte)

B.G.P	block number	2 bytes	
	block length	1 byte	
Boundary Gateway Protocol	version number	1 byte	(reserved)
	block type	2 bytes	(minutes)
	holddown timer	2 bytes	(minutes)

types:

- open - 1
- update - 2
- notification - 4
- keepalive - 8

version is currently 1

open:

- my AS = 2 byte
- link type 1 byte
- up - 1
- down - 2
- interval - 4
- H-link - 8

(not used in update database field)

auth type code 1 byte

- 0 - none

authentication variable

update:

- network id 4 bytes
- first hop gateway 4 bytes
- metric 2 bytes
- count of AS 1 byte
- direction 1 byte
- AS # 2 bytes

repeat "count" times

notification:

- open/closed 2 bytes
- data variable

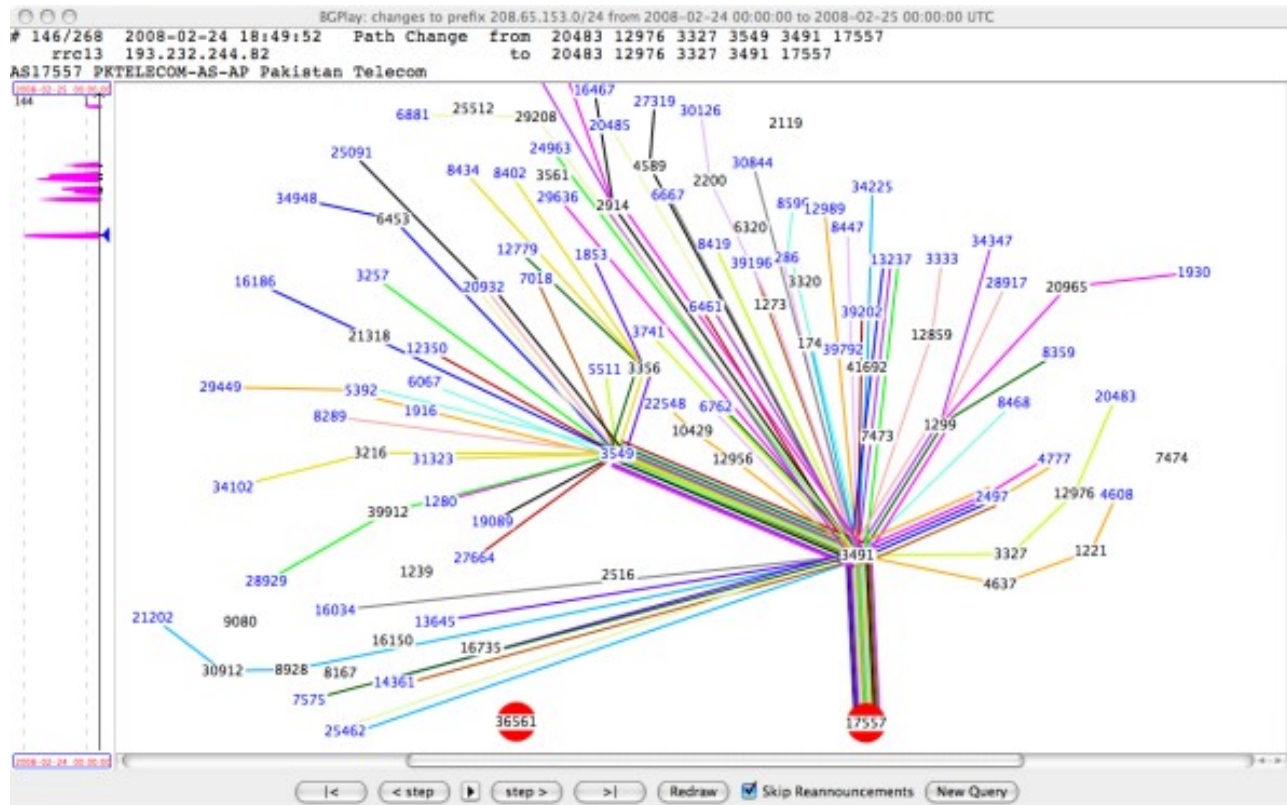
0 27 JUL 2011 07:17:28.174

1989 - 2011

- June 1989 - RFC 1105 - A Border Gateway Protocol (BGP)
- March 1995 - RFC 1771 - A Border Gateway Protocol 4 (BGP-4)
- January 2006 – RFC 4271 - A Border Gateway Protocol 4 (BGP-4)
- November 2008 - BGP Security Requirements

Latest major incidents

- 2008 - YouTube Hijacking: Pakistan Telecom (AS17557) started an unauthorized announcement of the prefix 208.65.153.0/24

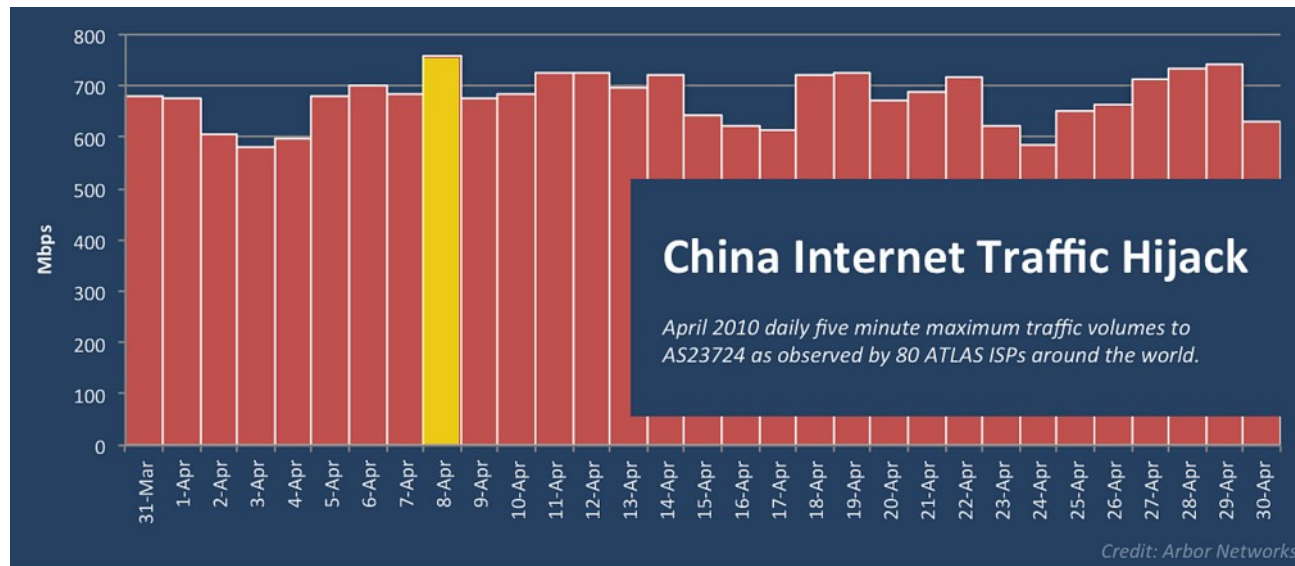


http://www.youtube.com/watch?v=IzLPKuAOe50&feature=player_embedded#!

<http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

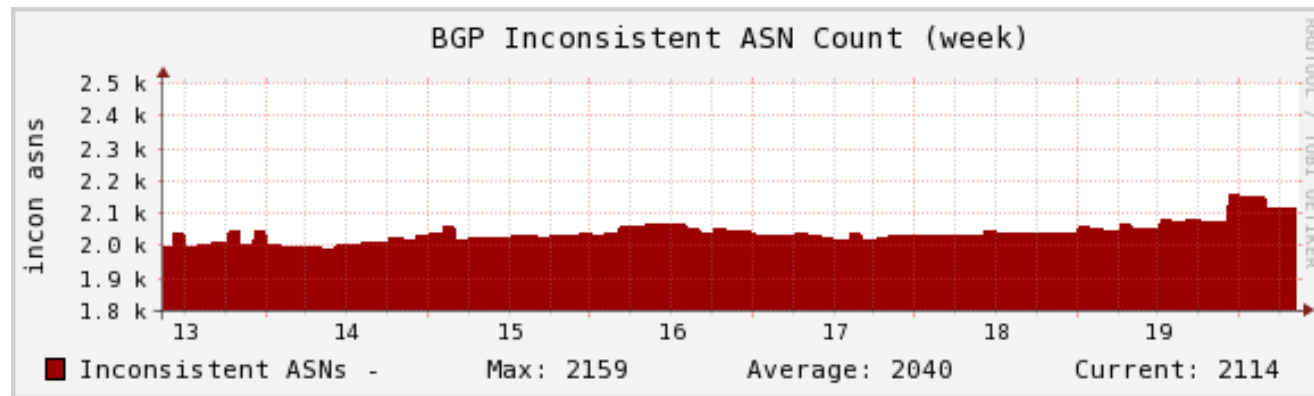
Latest major incidents

- 2010 - China Hijack: a Chinese Internet provider announced 40,000 routes belonging to other ISPs / enterprises around the world



Daily misconfigurations

- Advertised yet unassigned addresses
- Unassigned, reserved and private ASNs in use
- Prefixes from private and non-routed address space
- Unregistered ASNs



BGP Security solutions 2010

System	Type	Reference Implementation	Deployed
GTSM	session security only	Yes ⁷	Yes
sBGP	crypto	Yes ⁸	No
soBGP	crypto/anomaly	No ⁹	No
psBGP	crypto	No	No
IRV	crypto/anomaly	No	No
SPV	crypto	No	No
pgBGP	anomaly	Yes ¹⁰	Yes
iSPY	anomaly	No	No
PHAS	anomaly	No ¹¹	No
Secure Traceroute	crypto	No	No
Fatih	anomaly	No	No
Listen & Whisper	crypto/anomaly	No	No

TABLE I
DEPLOYMENT AND IMPLEMENTATION STATUS OF BGP SECURITY
APPROACHES

G. Huston, M. Rossi, e G. Armitage, «Securing BGP-A Literature Survey», Communications Surveys & Tutorials, IEEE, no. 99: 1–24.

BGP security requirements

- provide data to AS operators to enable BGP speakers to reject advertisements (UPDATE messages) that are not valid.
- secure:
 - the data payload of the protocol
 - data semantics of the protocol.

BGP possible verification

- Contents of the UPDATE message SHOULD be authenticated in real-time as the UPDATE message is processed.
- The route information base MAY be authenticated periodically or in an event-driven manner by scanning the route-table data and verifying the originating AS and the validity of the AS_PATH list.

BGP deployment requirements

- per-peer basis
- backward compatibility
- secured and non-secured
- incremental deployment scenarios
- transition free of service interruption

BGP other requirements

- SHOULD NOT require connections to external systems, beyond those directly involved in peering relationships, in order to return to full service
- Local controls for secure UPDATE acceptance:
 - MUST support a range of possible outputs for local determination of the trust level for a specific route so that routing preference and policy can be applied to its inclusion in the RIB.
 - The security system SHOULD allow the operator to determine whether speed of convergence is more important than security, or whether security is more important than the speed of convergence.

BGP AS_PATH requirements

1. Authorization of Originating AS
 2. Announcing AS Check
 3. AS_PATH Feasibility Check
 4. Update Transit Check
- MUST be capable of distributing security information at the same rate as the BGP announcements and withdrawals propagate.

BGPsec

- RPKI
- Route Origination Authorization (ROA) allows holders of IP address resources to authorize specific ASes to originate routes to these resources
- BGPSEC router certificate, binds an AS number to a public signature verification key, the corresponding private key of which is held by one or more BGP speakers within this AS
- BGPSEC_Path_Signatures, new optional (non-transitive) attribute, in the UPDATE msg and protects:
 - Network Layer Reachability Information (NLRI)
 - the AS number of the originating AS,
 - the AS number of the peer and consecutive new AS to whom the update message is being sent
- Subject Key Identifier (SKI) used to select the public key (and selected router certificate data)
- Negotiated separately (sec/nonsec – Ipv4/IPv6 - send/receive)
- Does not disclose new info about topology
- Assume additional capabilities in the routers
- AS's eBGP speaking

Scenarios

1. Bogon ASN and Bogus origins/path/attributes (unallocated, reserve and private - advertised yet unassigned addresses)
2. Unauthorized announcement / Prefix hijacking
3. Path spoofing
4. MITM
5. DoS

Scenario nr. 1:

Bogon ASN and Bogus origins/path/attributes (unallocated, reserve and private - advertised yet unassigned addresses)

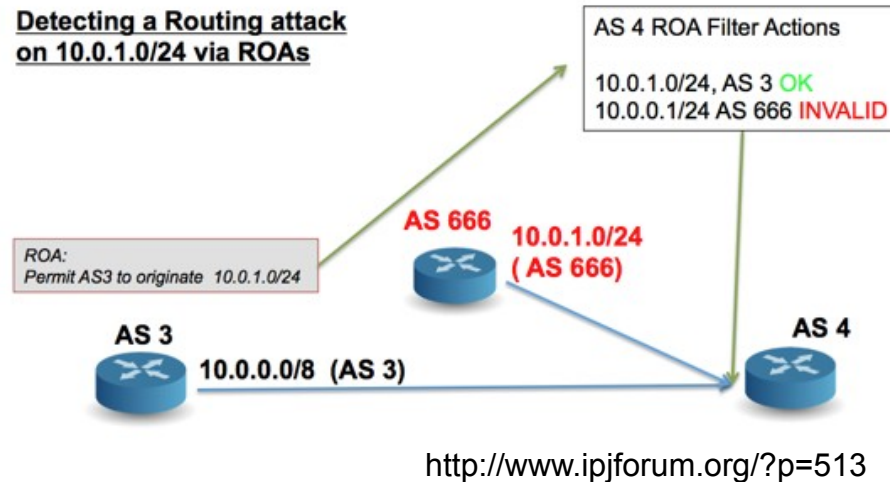
d000::/8 originated by AS28716

Advertisement of a massive bogon more general route in IPV6 from 13 Nov 2009 until 15 Jan 2010 – and noone noticed for 2 months!
A Provider's Perspective on BGP Security Techniques

BGPsec

- BGPSEC_Path_Signatures let recipient being able to detect that the update is invalid.
- Correspondence AS with public signature

Scenario nr. 2: Unauthorized announcement / Prefix hijacking



BGPsec

- RPKI:
 - ROA
 - BGPSEC router certificate
- Use signatures to protect the AS Path attribute of BGP update messages so that a BGP speaker can assess the validity of the AS Path in update messages that it receives.

Scenario nr. 3: Path spoofing

*Data traffic is forwarded through some router or network that is spoofing the legitimate address, thus enabling an active attack by affording the opportunity to modify the data.
RFC 4272*

BGPsec

- RPKI authentication
- Certification of the origin AS,path route advertisement
- Consistency of the legitimate address
- Use same technique

Scenario nr. 4: MITM

*BGP does not provide protection against man- in-the-middle attacks. As BGP does not perform peer entity authentication, a man-in-the-middle attack is child's play.
RFC 4272*

BGPsec

- Authentication of the origin ASN
- Path authentication
- Validate origin and path and reject unregistered ASNs routes
- Automatically invalid the route
- Do not allow further announcement

For more info

DEFCON 16: Stealing The Internet - A Routed, Wide-area, Man in the Middle Attack
<http://www.youtube.com/watch?v=S0BM6aB90n8>

Scenario nr. 5: DoS

While bogus routing data can present a denial of service attack on the end systems that are trying to transmit data through the network and on the network infrastructure itself, certain bogus information can represent a denial of service on the BGP routing protocol. For example, advertising large numbers of more specific routes (i.e., longer prefixes) can cause BGP traffic and router table size to increase, even explode.

RFC 4272

BGPsec

Blackhole traffic

- *Acknowledges the attack*

DoS with false source address

- Possible defense combined with reverse path filtering

BGPsec

- Original ideas from sBGP and DNSsec
- Path verification like Whisper
- Follows the hierarchical structure of the Internet
- Based on RPKI
- From 1st january 2011 all RIRs issue digital certificates along with the assignment or allocation of Internet number resources.
- Specification drafts are developed by the IETF SIDR WG
- Will be deployed in the next 10 -15 years

Future developments ?

*Think about what could happen
if somebody hijacked Google prefixes....*

