SWINBURNE UNIVERSITY OF TECHNOLOGY

Securing BGP - A Literature Survey

Geoff Huston, Mattia Rossi, Grenville Armitage

gih@apnic.net, mrossi@swin.edu.au, garmitage@swin.edu.au

Centre for Advanced Internet Architectures (CAIA)
Swinburne University of Technology

Outline

What is routing?

- Internet is decentralised network
- End hosts and routers
- Hosts generate IP packets, routers direct packets to destination
- Internet topology changes continuously, routing needs to be dynamic
- Routers propagate location of addresses to each other in order to allow consistent and optimal packet forwarding decisions
- Routing protocols are used to perform this information propagation

Some BGP background

- Intra-domain routing (RIP, OSPF) within Autonomous System (AS) vs. inter-domain routing (BGP) between AS
- BGP is the sole Inter-domain routing protocol since the late 1980's
- BGP is crucial for the operation and security of the Internet
- BGP relies on informal trust models to provide reliable and correct results
- Design was based on homogeneous and mutually trusting Internet of the 80's
- Not designed for negotiated trust models and for robustness against hostile actors

A trust problem

- BGP is vulnerable as Internet grows and risk of hostility increases
- BGP trust model lacks of:
  - explicit presentation of credentials
  - propagation of instruments of authority
  - any reliable means of verifying the authenticity of the information being propagated through the routing system
- Possible hostile actions are difficult to detect:
  - false routing information may be injected
  - valid routing information removed
  - information altered to cause traffic redirection

What could happen?

- Aims of attacks:
  - prevent the correct operation of applications
  - conduct fraudulent activities
  - disrupt the operation of part (or even all) of the network in various ways
- Effects of attacks:
  - from relatively inconsequential
  - through to catastrophic
- Real examples:
  - “7007 Incident”, 1997
  - “Con Edison steals the Net”, 2006
  - “Youtube Accident”, 2008
  - “The Internet’s Biggest Security Hole” Wired Magazine, 2008

Requirements to resist to subversion of integrity

- BGP speaker needs:
  - Sufficient information to verify the authenticity and completeness of the information received
  - The ability to generate authoritative information for others to verify the authenticity of routing information
- BGP scalability has to be considered!

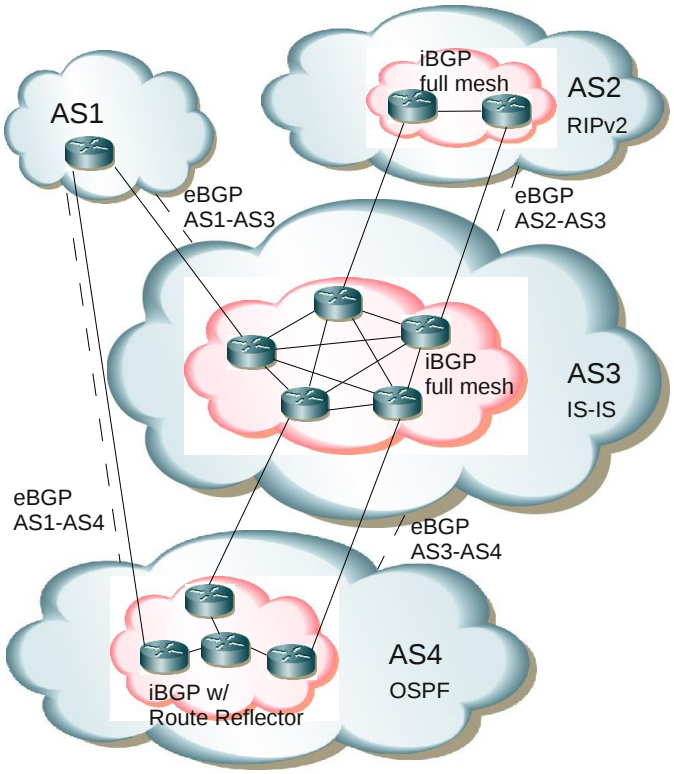
How the Internet works

- Internet is based on the Internet Protocol (IP)
- Decoupled framework consisting of:
  - IP addresses
  - forwarding system (data plane)
  - routing system (control plane)
  - routing protocols
- Addresses are identity not location, numerical adjacency $\neq$ topological adjacency
- Forwarding system selects the interface on a local router depending on information from the routing system (local view)
- Routing system provides information of address location between ASes using inter-domain routing protocols (global view)
- ASes can be single routers or a complex system of routers (peers) using an intra-domain routing protocol

Routing Protocols

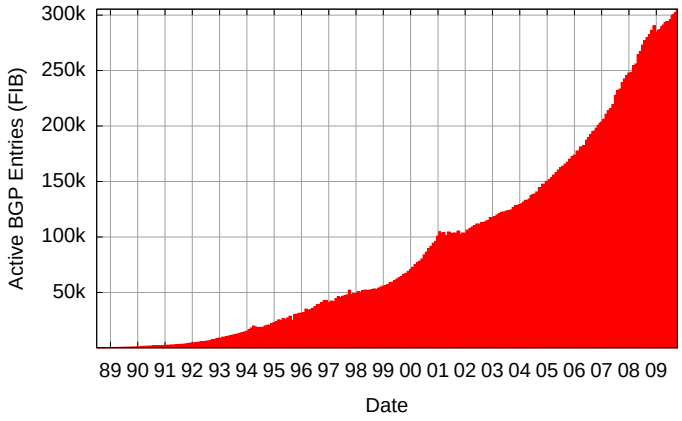
- Different routing protocols:
  - Intra-domain: Interior Gateway Protocols (IGPs) - RIP, RIPng, OSPF, OSPFv2, IS-IS
  - Inter-domain: BGP
- Two types of BGP:
  - iBGP for BGP peering between edge routers of an AS
  - eBGP for inter-AS peering
- **iBGP $\neq$ IGP!**
- iBGP needs full mesh to maintain BGP information consistent
- Full mesh has scalability problem $=>$ route reflector

An example topology



History of BGP

- Current Version: BGP-4 - Current Standard: RFC4271 (January 2006)
- Version 1: RFC1105 - 1989, Version 2: RFC1163 - 1990, Version 3: RFC1267 - 1991
- Version 4: RFC1771 - March 1995, refined in RFC4271
- Grown from 20000 routes to 300000 routes

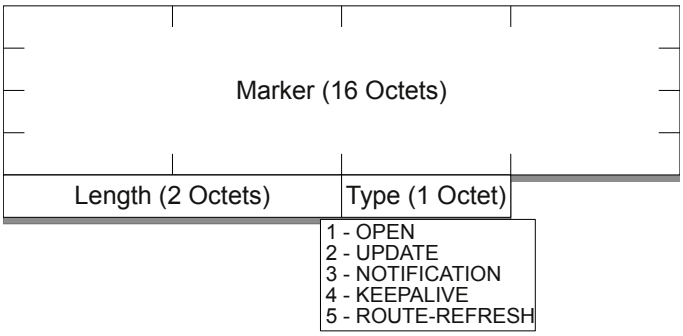


BGP and TCP

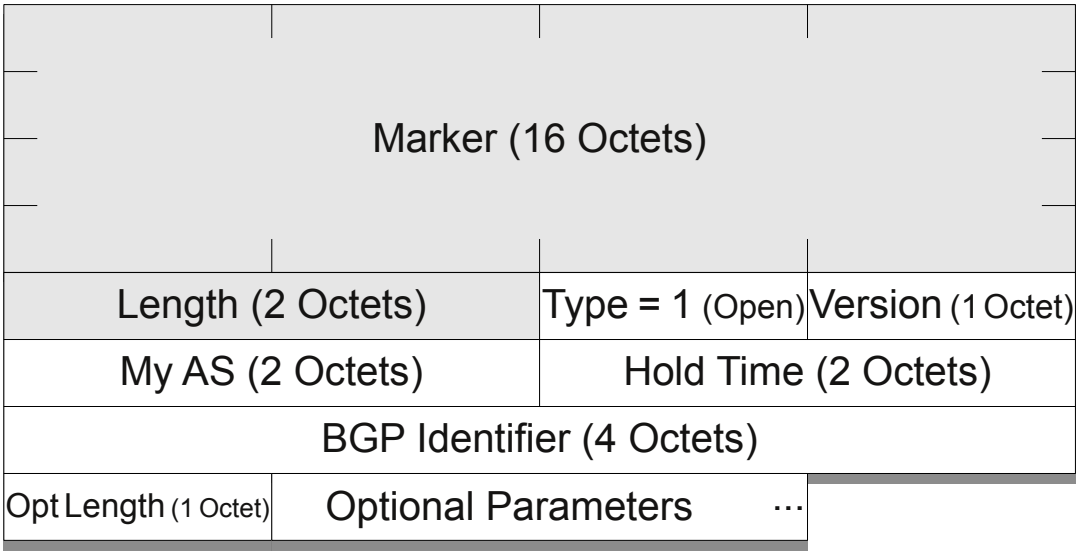
- BGP uses TCP to exchange routing updates
- Assumption of the existence of a functional IP forwarding environment at link level
- Allows to operate across logical connections on the same sub-net, LAN or Internet
- BGP messages use markers for identification and are between 19 and 4096 bytes long
- Use of TCP omits overhead of ensuring reliable packet delivery by the routing protocol
- Use of reliable transport protocol also omits the need to periodically refresh the routing table
- Only incremental updates are needed after sending the initial routing table.

BGP Messages

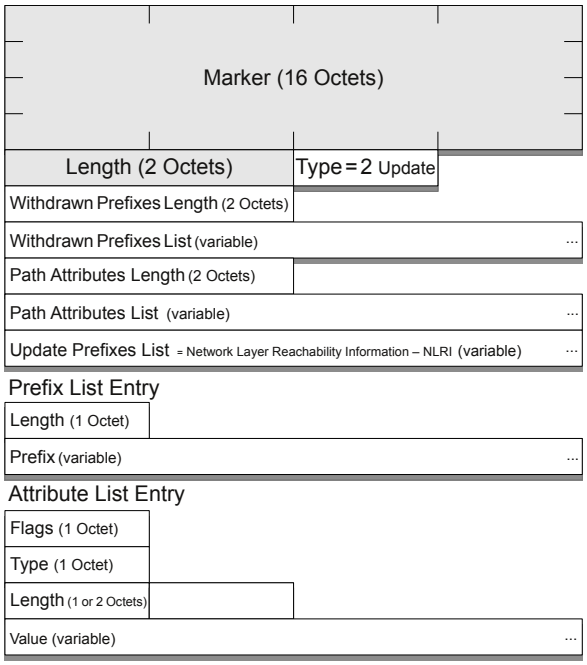
- 5 message types using a common Header:
  - OPEN - to start a BGP peering session
  - UPDATE - to exchange reachability information
  - NOTIFICATION - used to convey a reason code prior to termination of the BGP session
  - KEEPALIVE - to confirm the continued availability of the BGP peer
  - ROUTE-REFRESH - to request a resend of the routing information
- BGP common header:



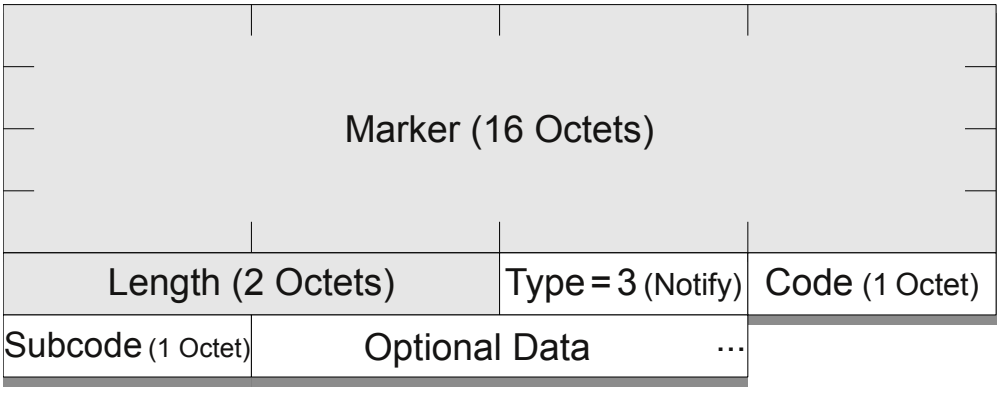
OPEN Message



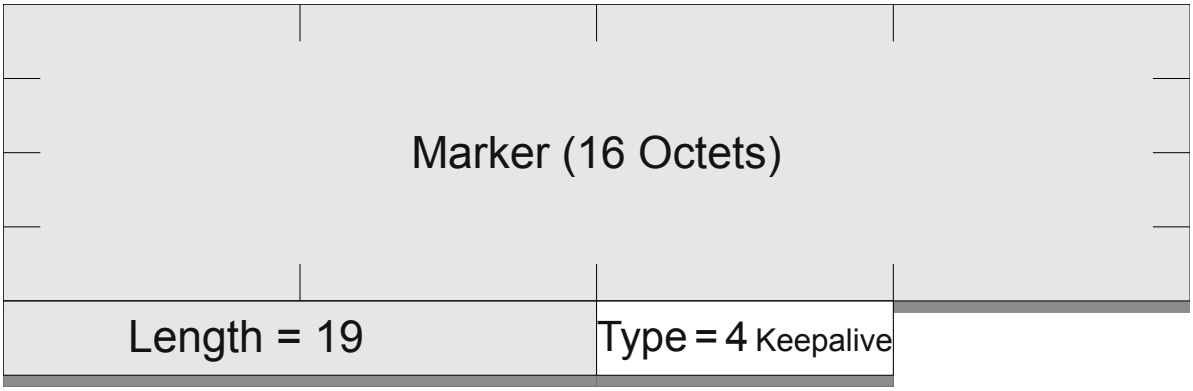
UPDATE Message



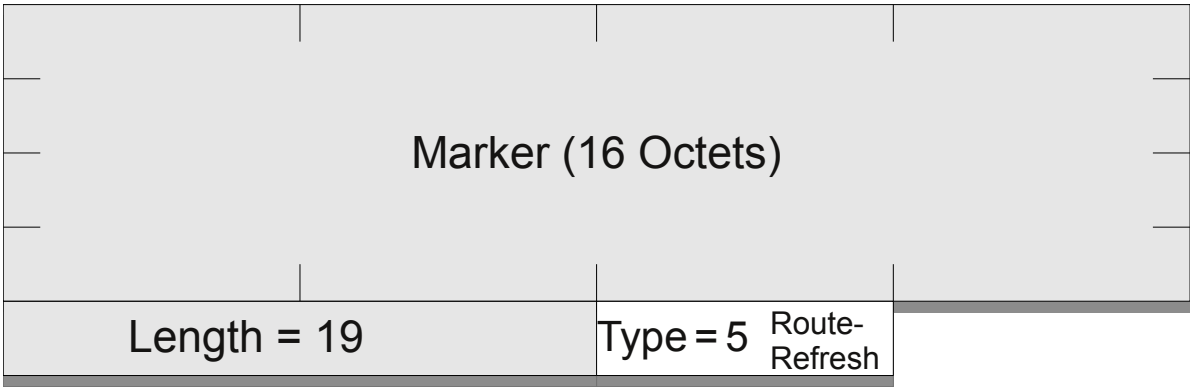
NOTIFICATION Message



KEEPALIVE Message



ROUTE-REFRESH Message



Route selection

- BGP can receive announcements for the same prefix from different peers
- Best path needs to be selected through decision process:
  - Select the route object with the highest value for LOCAL-PREF attribute value
  - Select the route object shortest AS_PATH attribute length
  - Select the lowest MULTI_EXIT_DISCRIMINATOR attribute value
  - Select the minimum IGP cost to the NEXT_HOP address given in the route object
  - Select eBGP over iBGP-learnt routes
  - If iBGP select the lowest BGP Identifier value.
- General rule: more specific prefix is preferred over a covering prefix
- Behaviour can be changed by network administrator

Analysing BGP communication

- How do we talk?
- Whom am I talking to?
- What are you saying?
- Should I believe you?
- How recent is your information and is it still valid?

Attacks over the communication channel

- BGP peer session is a long-held TCP session and thus vulnerable to
  - eavesdropping
  - session reset
  - session capture
  - message alteration
  - denial of service attacks
- BGP has no enforced minimum level of message protection

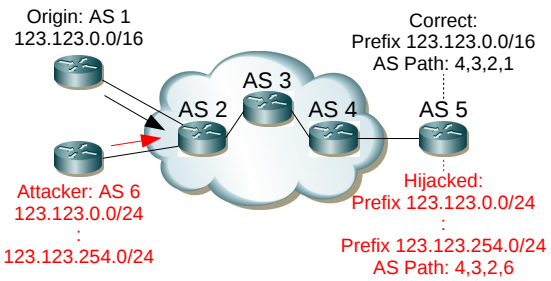
Attacks over the communication channel

- Possible attacks are:
  - Man in the middle attack: filter traffic from both sides and alter messages
  - Message injection: inject false routing information
  - Delay messages: timing is important, BGP peer could fall out of sync and start distributing bogus routing information
  - Replay Attack: Replay withdrawals after announcements and trigger route flap damping (RFD)
  - Saturation Attack: insert bogus TCP messages, causing Denial of Service (even worse if MD5 or IPSEC is used due to decryption overhead)

Verifying BGP Identity

- Verify the authenticity and completeness of the routing information
- A local BGP speaker believes everything sent from a remote peer, unable to detect bogus information
- Threats:
  - Suppression of routing information
  - Alteration of the route object that is passed on
  - Invention of spurious route objects.
  - Assertion that an AS Path is genuine when it reflects an artificial path
  - Originate an advertisement for a prefix when, in fact, no such authority exists (prefix hijacking)

Prefix Hijacking



- Prefix hijacking types:
  - Stealing a whole prefix by announcing it with special attributes to bias the route selection process
  - Announcing more specific prefixes which together completely cover the larger prefix
  - Announcing an unallocated prefix
- May happen due to operational misconfiguration
- Difficult to detect, specially if sub-prefix is hijacked
- BGP cannot verify the authenticity of prefixes and attributes

Attacks to the Data Plane

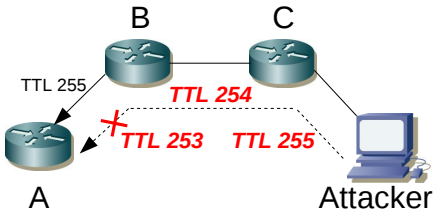
- Forwarding table is usually generated by lookups to the routing table
- Forwarding table can be inconsistent with routing table
- BGP is missing a mechanism to verify the consistency
- Possible threats:
  - subversion of local policies
  - theft of carriage capacity
  - deliberate denial of service
  - potential to eavesdrop on a conversation
  - support the interception and alteration of application level transactions
  - potential to masquerade, steal addresses and obscure identity (fake DNS, generate SPAM)
- Secure control plane $=$ secure routing but routing $\neq$ forwarding

BGP is vulnerable

- Vulnerable and exposed to previously listed threats
- Routers can be compromised (in 2001 some deployed default passwords)
- Not possible to prevent routers from generating false messages, if routers can be compromised
- Consequence: there is no mechanism that limits the extent to which a misbehaving router can make false claims about reachability

Securing BGP - Basics

- Tools protecting the TCP session (implementations exist):
  - Generalized TTL security mechanism (GTSM): Limits the radius of an attacker and can protect against SYN-flooding and similar attacks



  - TCP-MD5: potentially dangerous and weaker as IPSEC, but faster
  - IPSEC: potentially dangerous, slower than MD5, but has key rollover capacity, thus more secure

Securing BGP - Basics - continued

- Securing the routing information (implementations do not exist):
  - Use of shared secrets is not possible, as information only partially transitive and can change
  - Digital signatures needed - X.509 certificates
  - Authority needed to verify signatures - Public Key Infrastructure (PKI)

What are the requirements for secure routing?

- Secure the payload data:
  - Ensure the packet has not been tampered with while on the wire
- Secure the semantics:
  - Selected fields of the BGP messages need to be signed and authenticated (prefix, AS path)
- Allow piecemeal deployment:
  - Unsigned messages might not necessarily be wrong
- Make sure to avoid routing loops
- Do not delay convergence

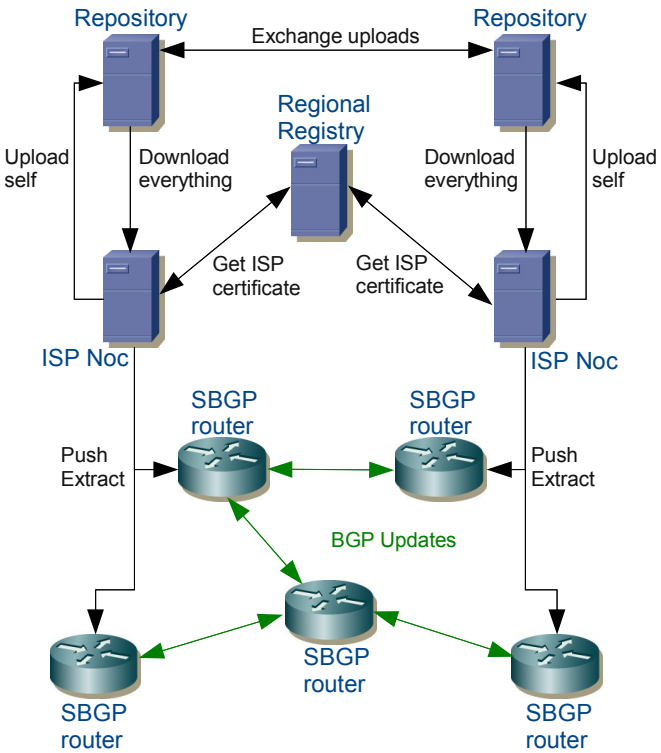
Some approaches to secure BGP

- Full security suites:
  - Most complete solution: Secure BGP (sBGP) - uses signatures and PKI - puts high load on routers
  - Secure Origin BGP (soBGP) - Cisco - signatures and PKI
  - Pretty Secure BGP (psBGP) - tries to avoid hierarchical PKI, but assumes its existence... inconsistent
  - Inter-domain Route Validation (IRV) - uses Internet routing registries
- Partial security solutions and Research:
  - Pretty Good BGP (PG-BGP) and Quarantine BGP (Q-BGP)
  - Prefix Hijacking Alert System (PHAS)
  - Multiple Origin Autonomous System (MOAS) detection and more...
- Lots of security mechanisms (Chained Hash Functions, Secure Path Vector routing (SPV),...)

sBGP

- Very complete and elaborated, uses signature on UPDATE messages and complex system for authentication
- Issues:
  - Puts high load on routers
  - High load on session restart
  - Piecemeal deployment impossible
  - Requirement that the BGP UPDATE message has to traverse the same AS sequence as that contained in the UPDATE message

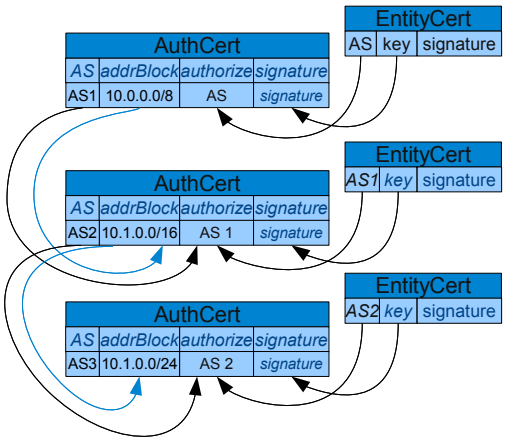
sBGP

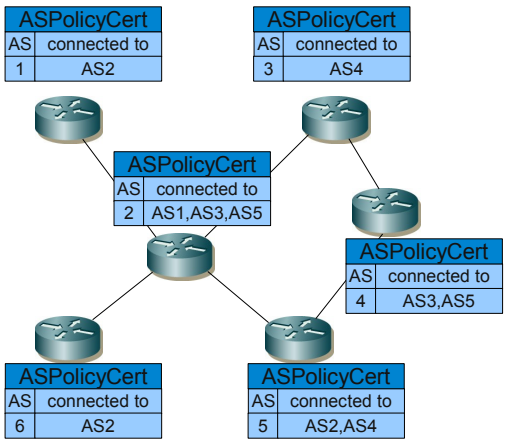


soBGP

- Less complicated than sBGP - ensures originator of prefix is authenticated
- Checks AS-Path only for feasibility - AS peer check
- uses EntityCerts (AS), AuthCerts (Prefix) and ASPolicyCerts (AS peer check)
- Issues: Does not tell how to establish trust anchors for validation of Certificates

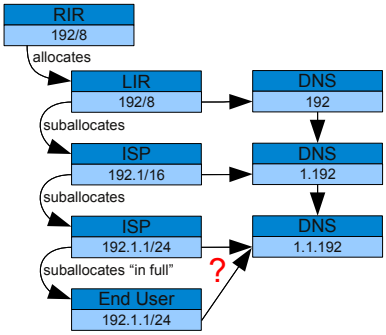
soBGP



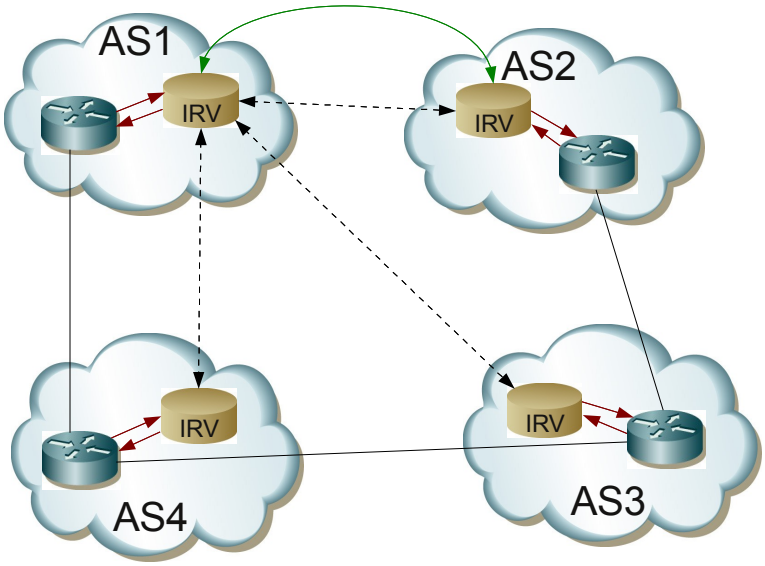


IRV

- Uses Internet routing registries (IRR) to verify authenticity via IRV server
- Does not modify the BGP protocol
- One IRV server per AS
- DNSSEC isomorphism
- Same problem:



IRV



Origin AS verification

AS Path verification

BGP router – IRV information lookup

BGP information exchange

Anomaly detection

- Only implementation: PG-BGP and Q-BGP:
  - Detection of prefix hijacking and sub-prefix hijacking
  - Detection of anomalous routes by analysing update data of one week
  - Delaying of suspect/anomalous updates for 24h (PG-BGP)
  - Anomalous updates are sent but not implemented for 24h (Q-BGP)

Securing the Data Plane

- Status of BGP forwarding table is not always consistent with routing table (8% inconsistency)
- Providers can steal traffic - pretext of “Traffic Engineering“
- No real solution
- Secure Traceroute:
  - Checks the data path and compares to AS path in routing tableofcontents
  - Uses PKI and signatures
  - Incremental deployment impossible
- Fatih:
  - Uses traffic summary functions and compares the results of neighbouring ASes
  - Not feasible on routers with billions of packets per second
- Listen and Whisper:
  - Combination of control plane security (Whisper) and data plane anomaly detection (Listen)
  - “Just too late” type of detection
  - Not feasible as it follows TCP flows

The current Status

System	Type	Implemented	Deployed
GTSM	session sec.	Yes (Quagga)	Yes
sBGP	crypto	Yes (old)	No
soBGP	crypto/anomaly	No	No
psBGP	crypto	No	No
IRV	crypto/anomaly	No	No
SPV	crypto	No	No
pgBGP	anomaly	Yes (Quagga)	Yes
iSPY	anomaly	No	No
PHAS	anomaly	No	No
Sec. Traceroute	crypto	No	No
Fatih	anomaly	No	No
Listen&Whisper	crypto/anomaly	No	No

Conclusions

- BGP has proved surprisingly resilient in terms of its longevity of useful operational life
- Early predictions favoured IDRP over BGP - (The OSI Inter-Domain Routing Protocol)
- BGP Security: Some network operators use TCP-MD5, some GTSM
- Overall picture of BGP security is unchanged
- Ample evidence of use of unregistered addresses and spamming
- BGP is abused in various ways
- Current efforts to mitigate problems are inadequate
- Deployment of PKI seems to be a good start
- BGP routing system is at risk - Internet is at risk!

Questions

THANK YOU FOR YOUR ATTENTION
Questions?