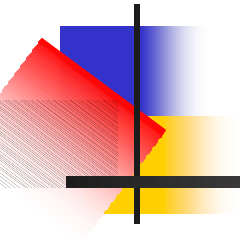
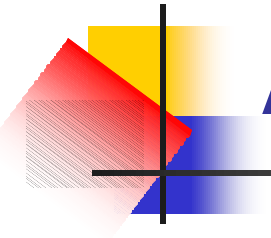


IP Hijacking

David J. Bowie

CISSP

david.bowie@level3.com

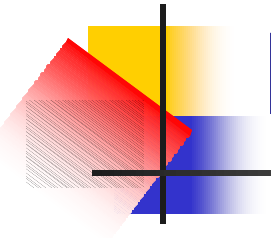


Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking made easy
- Impact on the community
- Recourse and recovery

IP and AS assignment

- IANA (under the ICANN) assigns IP addresses to networks via RIRs. (APNIC, ARIN, RIPE, LACNIC)
  - www.iana.org
- Each collection of networks managed as a system is assigned an AS (Autonomous System) number by their respective RIR.
- Each AS is responsible for routing policy and delegation of IPs within their network.
- Each AS shares information about their network with other AS's.
  - This is referred to as PEERING.

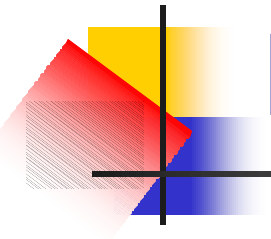


Private networks

- "Private Use" IP addresses:
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255
    - Defined in RFC 1918
    - These addresses should NEVER be announced to the public internet.
    - Not to be confused with unallocated or reserved space.

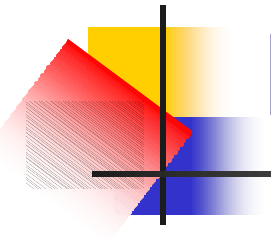
IGP and EGP

- IGP (Interior Gateway Protocol) defines the manner in which Networks within an autonomous system communicate routing information to each other.
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First).
- EGP (Exterior Gateway Protocol) the original protocol was defined by BBN in 1982 (RFC 827) as the method for AS's to share information about their routing policies.
  - BGP, BGP-4
  - EGP-2
  - EGP(1) defined an "Autonomous System" as a 16-bit field, hence the maximum of 65534 AS's.



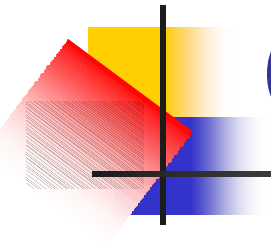
BGP

- Border Gateway Protocol
  - RFC 1771
  - The routing protocol currently used to exchange routing information between Autonomous Systems.
  - BGP-4 implemented support for CIDR notation eliminating the ‘class’ of network.
  - BGP is a destination-based set of rules.
    - A router forwards a packet based solely on the destination address carried in the IP header of the packet
    - Announcements to neighboring ASs contain only those routes that the announcing AS uses



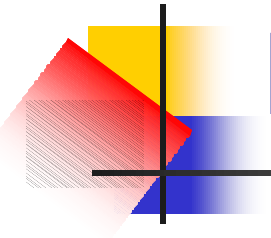
BGP threats

- Configuration error
- Fraudulent origination
- Fraudulent modification
- Compromised routers
- Routing by miscreants
- Packet sniffing and injection



Consequences

- Disruption
- Deception
- Disclosure

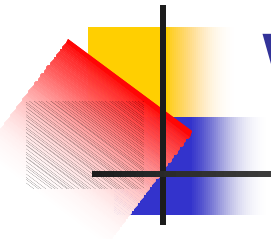


BGP assumptions

- Each AS announces only those prefixes for which they are responsible
- Source of a BGP-update has the authority to announce the prefix
- The announced AS path is correct
- TCP provides a secure transmission between BGP peers

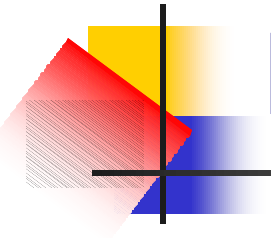
Mitigating the BGP threat

- IPSEC
  - secure point-to-point between BGP speakers
- Implement RFC2385
  - MD5 validation of TCP sessions
  - Optional extension is BGP MD5
    - Handles inter-As validation of routes
- Filters to ensure your neighbors only announce their own space (RFC 2827)
- BGP configuration checks and balances in house



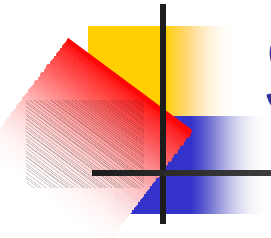
What about S-BGP

- BGP updates are digitally signed
- Address-based PKI used to validate signatures
- Signing party certifies next hop
- Validates BGP speakers, AS identity, and ownership of IP blocks.



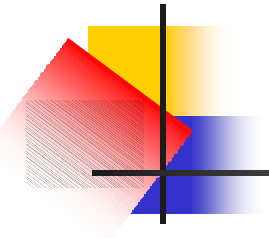
Limitations of S-BGP

- Cost
  - Increased CPU and memory requirement
  - Increased bandwidth
  - PKI implementation per AS
- Coordination of PKI infrastructure
- Need for router upgrades
- Acceptance by ISPs



SO-BGP

- Secure Origin BGP
  - Cisco response to S-BGP
    - Verifies the AS-Path as announced in updates
  - Adds BGP security message as an extension to BGP
    - Uses distributed processing and trust
    - Certificates shared between routers
    - Incremental deployment is possible



Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking Made easy
- Impact on the community
- Recourse and recovery

Who are you

- Each Regional Internet Registry (RIR) is responsible for maintaining documentation on the allocation and use of IP space within their region. (RFC2050)
- Registration includes the IP space, AS number, organization name, and points of contact.
- Each RIR is allocated blocks of IP space from IANA (initially defined in RFC 1466)
  - http://www.iana.org/assignments/ipv4-address-space

WHOIS information

- Each RIR maintains a searchable WHOIS registry.
  - ARIN
    - North America, Africa, & leftovers
  - APNIC
    - Asia Pacific
  - RIPE
    - European
  - LACNIC
    - Latin America and Caribbean
  - AFRINIC (under development)
  - DODNIC (not really an RIR)
    - .mil

SWIP (ARIN-specific)

- ARIN distinguishes IP address allocation from IP address assignment.
  - ISPs receive allocations, while end-users receive assignments.
    - Assignments are not sub-delegated
    - Allocations are sub-delegated to downstream ISPs
- ISPs receiving IP blocks must use either SWIP (Shared WHOIS Project) or a RWhois server (Referral WHOIS) to provide reassignment or reallocation information for /29 and larger blocks to their RIR.
  - RWHOIS is defined in RFC 2167

Maintenance of WHOIS data

- RIRs have recently undertaken a clean-up effort on their databases.
- It is the responsibility of the RIR to ensure that the Direct Allocation information is correct.
- It is the responsibility of the ISP to ensure that SWIP data is correct.

Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking made easy
- Impact on the community
- Recourse and recovery

Zombie blocks

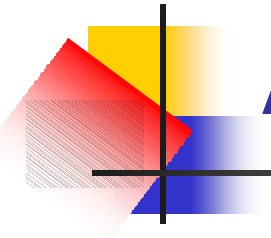
- Any routable IP block not in current use on the Internet.
- Blocks of assigned IP space forgotten or ignored and not returned to the RIR.
  - Bankruptcy or ceased operation
  - Forgotten allocations
  - Decreased demand after initial allocation
  - “Private” IP space used only internally.

Bogon IP space

- A bogon prefix is a route that should never appear in the Internet routing table
- Commonly found as the source addresses of DDoS attacks
- Bogon list contains RFC1918 space, IANA reserved space (RFC 3330), and known unrouted IP space.

Bogon AS's

- Total number of unique ASNs : **15821**
  Total number of bogus ASNs: **11**
  - 8/18/03
- A Bogon AS is an announced AS with a valid path, but the AS is unassigned or reserved by IANA. (ex: AS64514)
  - ASNumber: 64512 - 65535
  - ASName: IANA-RSVD2



Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking made easy
- Impact on the community
- Recourse and recovery

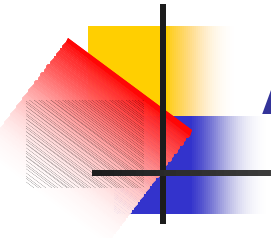
How to Hijack IP space

- Find a /24 or smaller that is not being used
- Change the data in the RIR WHOIS database
  - Change the nameserver to one you control
- Announce the block via BGP
  - Most ISPs don’t check ownership

Activity on Hijacked space

- Disruption
  - SPAM
  - DoS
- Deception
  - Selling or leasing IP address space

- Note: IP space is NEVER sold or leased!



Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking made easy
- Impact on the community
- Recourse and recovery

Impact to the community

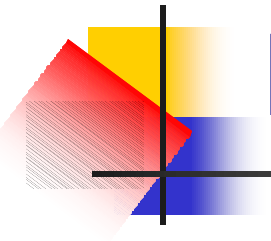
- Disruption
  - SPAM
    - Sourced from and advertising hijacked IPs
  - DoS
    - Injection of false route
- Deception
  - SPAM
    - Advertised domain on multiple hijacked IP space
- List of IPs currently hijacked:
  - http://www.completewhois.com/hijacked/index.htm

Sample of hijacked IP space

- 34.0.0.0/8 from Halliburton Oil Co
  - Grabbed by Gordon Lantz for reselling?
- 128.13.0.0/16 from DoD (ArpaNet)
  - Nameserver now is “goods-up4sale.com”
- 134.33.0.0/16 from CODEX (Motorola)
  - Scooped by VMX Networks for Spam services
- 146.20.0.0/16 from Erie Forge & Steel
  - Sub-delegated to spam organizations
- 203.26.80.0/24 from Motorola AU
  - Used for child/bestiality porn
- From a list of ~100 IP blocks being currently hijacked.

Agenda

- IP allocations and routing
- Hijacking whois
- Zombies and Bogons
- Hijacking made easy
- Impact on the community
- Recourse and recovery

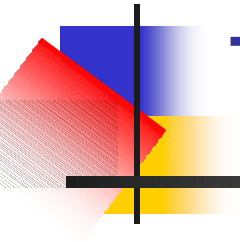


Recourse and Recovery

- BGP abuse
  - Use BCP 38 (RFC2827)
  - Announce only those networks you specifically list
  - Ensure validity of TCP on BGP speakers with MD5 (RFC2385)
  - Investigate S-BGP or SOBGP
  - Institute protections against human error

Recourse and Recovery (cont)

- IP Hijacking
  - Ensure all WHOIS information is correct and current
  - Report all offers to sell you IP space
  - Report and document all unauthorized use of IP space
  - Confirm IP space ownership before routing



Thanks – Q&A

david.bowie@level3.com
CISSP

(Yes - I am looking for a job.)

Links & References

- http://www.theregister.co.uk/content/55/31156.html
- http://www.cluecentral.net/pipermail/rbl/2003-April/000017.html
- http://www.ietf.org/internet-drafts/draft-ietf-ptomaine-nopeer-03.txt
- http://www.bgp4.as/links
- http://www.rpsec.org/
- http://www.completewhois.com/hijacked/hijacked_qa.htm
- http://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-dugan.pdf
- http://www.nanog.org/mtg-0306/pdf/bellovinsbgp.pdf
- http://www.psg.com/~randy/030603.nanog-sxbgp.pdf
- http://www.ir.bbn.com/projects/s-bgp
- http://www.nanog.org/mtg-0306/pdf/alvaro.pdf
- http://www.cymru.com/Bogons/