Securing a Service Provider's Public Route-views Routers:

Limiting information available to the unauthenticated user

James DeMong
Submitted for GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b (Option 2)
July 27, 2004

Abstract:

Looking glasses, traceroute servers and route-views servers are invaluable trouble shooting tools installed and maintained by Service Providers as a public service to the Internet community. Route-views routers can be used to determine the reachability of a host or subnet from outside one's own network as well as how the subnet appears in BGP beyond a network's borders. However, the unauthenticated user should not be provided information that could be easily used for reconnaissance of a service provider's network.

This paper examines the network topology and router specific information that is available on a Service Provider's route-views routers, the risk that information poses and the steps taken to reduce the information available to unauthenticated users of the route views routers.

Background:

Border Gateway Protocol version 4 or BGP-4 has been described as "the protocol that glues together the largest, most stable, and most complex network ever created."[1] BGP-4 allows directly connected networks to exchange routes. Reachability of a network depends on whether its routes have been advertised properly and propagated beyond the directly neighboring networks. BGP-4's proper operation is critical to the smooth operation of the Internet itself.

When the Internet was a kinder, gentler place and the operator community was a small group of like minded individuals, looking glasses, traceroute servers and the like were set up as a courtesy for other operators to verify that their BGP routes were reachable on the Internet from beyond their network's borders. The users of these resources did not have to authenticate and the users were not afforded any privileges on the equipment other than being able to execute "show" (Cisco IOS) or equivalent, traceroute and ping commands.

Having a route-views router is way for a service provider (SP) to distinguish itself as not all SPs have route-views routers. Providing a route-views router is a public service. Providing one could also be looked upon as providing some level of operational credibility.

Typically, route-views routers participate in a full iBGP mesh with the other BGP routers within the autonomous system. This gives the route-views router an excellent BGP view of the Internet from the SP's network perspective, which is very handy when trouble shooting BGP issues. To phrase it another way: information about the SP's network is provided to the public with no authentication required. Suddenly it sounds like a bad thing.

[1] Greene, "BGPv4 Security Essentials" p.1

In the next section, the operational deployment of a Service Provider's route-views routers and its potential risks are examined.

Before:

The setting for this case study is a large national service provider (SP). The network is peered with many other ISPs. The Service Provider has a large residential broadband customer base as well as enterprise customers and government entities. The SP also carries long distance voice traffic for its national telephony network. Security is a priority to the SP especially with respect to its backbone.

The route-views routers were set up with scrounged equipment outside of normal processes. While this is an effective way to "get things done", it bypasses formal policies and peer scrutiny. Although some concerns were expressed with the amount and type of information available about the SP backbone, the potential risk was considered to be low by some and believed to be outweighed by the operational usefulness of the route-views routers. The SP's operations staff would log into the route-views servers to do BGP trouble-shooting since it didn't require a username and password versus to logging in to one of many of the SP's BGP routers.

The main security concern when the route-views routers were deployed was restricting the ability of the unauthenticated user to configure the router. In Cisco IOS (Internetworking Operating System) version 10.3 and above, a command called "privilege" is available.[2] It is used to limit available commands based on the privilege level of the user. For the route-views routers, privilege was used to remove the "enable" command from the allowed commands for the unauthenticated user. The result of this is that no matter what the unauthenticated user does, they are not able to enter privileged exec mode and configure the router.

There were 24 other commands that were elevated to the privileged user. Among these, telnet was removed so the unauthenticated user could not telnet from the route-views router to another host.

"Show logging" was also assigned to the privileged user. The "show logging" command lists the current log buffer and the IP addresses of the syslog servers configured. In this case, the logging servers happened to be the same servers used for production equipment. If an attacker were able to attack these syslog servers, he might be able to obscure a brute force attack or cover his tracks after a successful attack.

The secondary security concern was one of routing information integrity. The route-views routers should never be able to advertise routes into BGP. Their

[2] "CISCO IOS SOFTWARE RELEASES 12.0 MAINLINE: Passwords and Privileges Commands"

function is to listen to BGP only and no routes should ever originate from these routers. The BGP peers of the route-views routers were configured to deny any incoming routes from the route-views routers. Even if the route-view router were compromised and configured to advertise bogus routes into internal BGP, its peers would drop the updates. This is an application of defense-in-depth.

During:

My role was to provide a solution balancing usability with security and get agreement from the operations team before I implemented the changes to the route-views routers.

The method used to determine what information was being provided to unauthenticated users was to log on to the route-views router as an unauthenticated user and take notes of what information was available.

The first item of note was the banner that greeted the unauthenticated user. The banner identified the router as a route-views router providing a view into the Service Provider's BGP table. It also provided three personal email addresses for contacting persons who were responsible for the router-views router. The personal emails addresses at this Service Provider were of the form firstname.lastname@serviceprovider.net. This information could be used for social engineering. An attacker could phone up or email the NOC and have them make a change to BGP by either saying he was one of those people or giving one of the names as the authorizer for the change. The worst-case scenario is that the change causes an outage that violates a customer's SLA (Service Level Agreement). For some SLAs, the SP refunds money back to the customer if the SLA is not met.

Too much information was available to the unauthenticated user through the CLI (Command Line Interface). Although the unauthenticated user could not "enable", he could use every variation of the "show" commands.

The "show cdp" command derivatives display information from Cisco Discovery Protocol. This Cisco proprietary protocol is used to communicate device specific information between equipment with Layer 2 connectivity. For example, on one of the route-views routers, the "show cdp neighbor" command provided the specific hardware platform, IOS version and IP address of the directly connected router. All of it is none of the unauthenticated user's business.

The "show version" command provides information about the router itself. The command lists the IOS version, the hardware platform, router uptime and the last restart reason. At best, this information is not examined by the unauthenticated user. At worst, this information could be used to subvert the route-views router.

"Show users" and "show hosts" on the route-views server provided similar information. "Show users" normally displays a list of the users that are currently logged into the router. In case of the route-views router where usernames are not required, the list is of the IP addresses or host names of the persons that are currently connected to the route-views router. “Show hosts” displays the most recent names resolved by the router. The unauthenticated user could find out details of what another user was checking connectivity to. The chances are a little remote that he could put much together, but once again, we are better off not providing that information.

The “show ntp associations” command was one I did not think was a big deal at first. When I looked more closely at it, I noticed that the ntp servers were part of the SP’s management network. The public should not know the specifics of the ntp servers since if the servers were attacked it could wreak havoc with the logs. Often a service provider’s ntp servers are also used for other management functions. The servers were protected behind firewalls but it is better to not provide the IP addresses to the public and wait for them to discover an exploit.

Another of these “show” commands allows the unauthenticated user to see the source and destination ports used for BGP TCP sessions to the route-reflectors. In light of the TCP RST vulnerability,[3] the “show ip bgp neighbor” command has potential for danger since it shows details of the TCP sessions used for BGP with the route-reflectors. A posting to the NANOG mailing list provided details on how to use this information to attack the router peering with a public route-views router with TCP RST vulnerability. [4] One would use the TCP RST exploit on the route-views router and then check to see what ports the next TCP connection established itself over. The port used on the remote router could indicate what ports it was using for other BGP TCP connections since Cisco IOS TCP implementation does not use truly random ephemeral ports. In the SP’s network, an attacker gaining information about the route reflector’s BGP connection might be able to cause havoc. The TCP MD5 signature is a viable work around provided by Cisco.[5] TCP MD5 signature option computes a 16-byte MD5 digest using the TCP pseudo header, the TCP header, the TCP segment data, and independently specified password.[6] Cisco IOS has an option to apply the TCP MD5 signature to BGP TCP connections. When a BGP peering router receives a TCP BGP data segment, it validates the MD5 digest before it attempts to process the packet. If the MD5 digest is invalid, the segment is discarded. This provides another layer of protection for the BGP session from being reset by a spoofed packet. (The primary layer of defense is ingress filtering to block packets from entering the SP’s network from outside if they have source IP addresses from within the SP’s network.) The SP’s route-reflectors did not have the TCP MD5 signature configured on all of their BGP sessions. This had been remedied on the route-reflectors prior to the application of the changes specified.

The “show tcp” command provides information similar to “show ip bgp neighbor”.

[3] Watson

[4] Luyer, “RE: TCP/BGP vulnerability - easier than you think.”

[5] “Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products.”

[6] Heffernan, p.2

The command shows every TCP connection the router has along with detailed statistics. The “show tcp” command cannot be completed from the command line in user exec mode for the IOS version used but it was available.

Providing the full BGP routing table can cause information to be leaked to the route-views router inadvertently. Since the routers used for the route-views routes were scrounged, the amount of memory available wouldn’t support iBGP peering directly with the BGP speakers individually, the route-views routes were made route-reflector clients of the production route reflectors. This weakness of this configuration is that the BGP information being passed to the route-view router cannot be easily filtered since a route-reflector does not modify the attributes of the reflected BGP route before reflecting it.[7] There is critical information that an attacker could obtain from the route-views routers.

There are a couple of features of a route-reflector environment that are intended for loop prevention but provide a lot of identifying information to an outsider. The route-reflector adds two attributes to the BGP route prior to reflecting it for loop prevention: ORIGINATOR_ID and CLUSTER_LIST.[8] The ORIGINATOR_ID is the ROUTER_ID of the router that originated the BGP route. If a route-reflector client receives a route with its router id as the originator id, it discards the route. The ROUTER_ID is the loopback address of the router in common practice and in the SP’s network so it identifies a target for DoS. The CLUSTER_LIST contains the cluster ids of each route-reflector that the route has been passed through. If a route received at a route reflector has its own cluster id in the CLUSTER_LIST, the route is discarded. In the SP’s environment, the cluster id of the route reflector is its Router ID which is the IP address of the loopback interface. If the route-reflectors are DoSed, the entire BGP for SP’s network could be taken out. Without routing, the SP’s network would be useless.

```
route-views>sh ip bgp 131.149.0.0/16
BGP routing table entry for 131.149.0.0/16, version 14000920
Paths: (2 available, best #1)
  64512 14177 11085
    192.168.51.24 (metric 1012) from 192.168.11.103 (192.168.11.103)
      Origin IGP, metric 10, localpref 100, valid, internal, best
      Originator: 192.168.51.24, Cluster list: 192.168.11.103, 192.168.11.175
  64512 14177 11085
    192.168.51.24 (metric 1012) from 192.168.11.224 (192.168.11.224)
      Origin IGP, metric 10, localpref 100, valid, internal
      Originator: 192.168.51.24, Cluster list: 192.168.11.224, 192.168.11.175
```

Example of Originator and Cluster List in a BGP route on the route-views routers

[7] Bates,et al., p.6
[8] Ibid.

The SP makes use of remote triggered blackhole routes to mitigate DoS attacks[9] against itself and its customers. These routes are propagated in BGP inside the SP. Although the SP's BGP communities that would easily identify the route as blackholed are not passed on to the route-views router, the next-hop is unique to all the blackhole routes and the subnet mask is usually a /32 bit mask. Attackers could gauge the effectiveness of an attack by the appearance or the existence of blackhole routes. If the host or subnet being attacked shows up as a blackholed route, the attack is successful because the black hole route drops all traffic destined to the end host or subnet. In addition, the time lag between when an attacker started a DoS and when the blackhole route showed up on the route-views router could also be used by the attacker to benchmark the response time of the SP's security team.

Another bit of information that could be derived from the BGP routes on the route-views routers was which subnets were likely to be populated without having to scan for them. Outside of the SP's network on the Internet, only the SP's large CIDR (Classless InterDomain Routing) blocks are visible. It is not clear which parts of the large address blocks are in active use. From the route-views router, an attacker could do reconnaissance since he can easily view the smaller blocks that are advertised within the SP's network. If a class B has several blocks with subnet masks longer than 16 bits, it is very likely that the smaller address blocks are populated with hosts. Instead of scanning the whole /16, the attacker can focus on scanning the smaller blocks within that /16 that are routed.

The SP's operations group wanted to continue to provide public route-views routers so shutting them down was not an option. The senior network specialist welcomed my offer to specify and to implement the changes as he agreed that the route-views routers provided too much information. I was a little surprised to hear that from an operations guy. The goal was to limit the information available while still providing a useful view of the SP's BGP table and Internet connectivity.

The personal email addresses in the login banner were replaced with a generic public group email address.

A few different options for altering the route-views routers were explored. One option was to make the route-views routers into ping and traceroute servers only, without a view of BGP. The autonomous system or AS path describes how a route has been advertised to the Service Provider's network. The AS path is a list of the AS's that the route has been advertised through. It is useful to a member of the Internet community to ascertain how the Service Provider hears their route and what AS's or networks traffic will traverse between the networks. Removing all BGP information was dismissed as it went too far.

A second option was to set up a web server with a CGI to interact with the route-

[9] Greene, "Remote Triggered Blackhole Routes"

views routers. This could provide excellent granularity in the information provided to unauthenticated users. However, the operations group that maintains the route-views routers does not maintain any other external web servers. The maintenance of the web server is critical for security. Based on the cost benefit, this option was dismissed at this time.

A third option was to peer directly with all of the routers originating BGP routes with the SP's backbone. This has the advantage of providing an excellent view into the BGP of the SP since the routes would not be watered down by a route-reflector deciding which were the "best paths." Unfortunately, the route-views routers didn't have enough RAM to support the number of BGP sessions required to peer with each of the routers directly.

A fourth option was to configure the route-views routers to be in a private AS "outside" of the SP's backbone. The advantage of this approach is that BGP route attributes that are transitive will not be propagated beyond the SP's AS[10]. ORIGINATOR_ID and CLUSTER_LIST (as well as MULTI_EXIT_DISC and LOCAL_PREF) will not be propagated to the route-views routers. Since the BGP session between the route-views router will be eBGP, it was no longer required to be peered with the route-reflector to get the entire BGP table, any BGP speaker would be sufficient. This was considered to be an advantage as it lowered the profile of the route-reflectors to the Internet at large. This option was selected and implemented with TCP MD5 signature protecting the BGP TCP session.

Next, the CLI commands available to the unauthenticated user were examined. Using the command completion feature of the IOS user exec CLI, it was confirmed that only the "enable" command had been removed from the unauthenticated user. Every other user exec command was available including many derivatives of the IOS "show" command, some harmless, some not.

Applying the Least Privilege Principle, the available commands should be limited to "ping," "traceroute" and "show ip bgp". The privilege command was enlisted to elevate all other commands to the enabled user.

```
privilege exec level 15 show ip bgp filter-list
```

Example of the privilege command used

This command only allows a user of exec level 15 to execute the command or its derivatives. The unauthenticated user, at exec level 1, is not able to execute these commands or even see they are present with IOS command line completion. The privilege command was used to elevate 137 additional commands and derivatives. The specific forms of the commands to be allowed were applied to exec level 1. The commands to allow the unauthenticated user to view a particular prefix in the BGP table, ping a host or traceroute are:

[10] Li, & Yakov (Eds.), p.20.

```
privilege exec level 1 show ip bgp
privilege exec level 1 show ip
privilege exec level 1 show
privilege exec level 1 traceroute
privilege exec level 1 ping
```

The privilege commands used for the unauthenticated user

Since the allowing the unauthenticated user full access to ping and traceroute has the unintended effect of providing ping flooding and spoofing capabilities (discovered through trial and error of command line completion while implementing), these commands were further limited by configuring the extended forms of the commands to privilege level 15.

Validating the changes made was an important final step to the process. The unauthenticated user should only be able to use “ping”, “traceroute” and “show ip bgp …”. After I had applied the changes, I connected to the box in the same way an anonymous user from the Internet would. I attempted to use command line completion to see what other commands were available. I saw the following:

```
route-views.>?
Exec commands:
  <1-99>      Session number to resume
  exit        Exit from the EXEC
  help        Description of the interactive help system
  logout      Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
  traceroute  Trace route to destination
```

The commands I saw were acceptable since some of them could have privilege set on them. Next I attempted to execute commands that should not be available and the CLI identified them as unrecognized commands. I then tried the show commands that I had identified previously and assigned to the privileged exec mode. All were also unrecognized by the CLI.

When I checked the variations of the commands that I had intended to allow to the unauthenticated user, I found a problem. I had made a mistake with how I privileged the “ping” and “traceroute” command. My first attempt at allowing the commands for the unauthenticated user had actually allowed extended ping and traceroute capability. By assigning the commands explicitly to exec level 1, I had assigned all commands that start with “ping” to exec level 1. The result was that an unauthenticated user could use the extended version of the commands to flood and to spoof. I had to remove the “ping” and “traceroute” privilege commands for exec level 1 as that had allowed the extended versions of the commands. (When privilege is used to move a command to an exec level, it allows the command and all of its derivatives.) Restoring the default versions of the commands for exec level 1 was exactly what I had wanted in the first place.

The importance of testing cannot be stressed enough, even testing the obvious. After making the changes and retesting, the commands were restricted as required.

After:

The changes made to the route-views routers definitely enhanced the security of the SP's network. The login banner that greeted unauthenticated users now had a generic group email address rather than personal email addresses. The added benefit was that email inquiries about the route-views routers now went to the group that actually had responsibility for them. The route-views routers no longer peered with the route-reflectors directly. The amount of information available to unauthenticated users was strictly limited. The unauthenticated user could still use the ping and traceroute commands to verify connectivity and the "show ip bgp". The route-views routers now provided a view of BGP beyond the SP's AS so the SP's operations staff could also check that routes were BGP routes being advertised outside of the network.

Not everyone within the SP was happy with the extent of the changes. The concern was that placing the route-views severs into an external AS went too far. With the route-views routers in an external AS, the AS path of any BGP route has the SP's AS in the path where it did not prior to the change. The concerns were discussed with the operations group and the consensus was that the difference was mostly cosmetic and the increase in security outweighed the negatives.

In the interest of a timely resolution, there were several items that were ignored. Although the route-views boxes had always been syslogging to a log server, no one was analyzing the logs. The log information was not used for early warning purposes. The basic "show" command could still display the IOS image files on the flash memory even after locking down with "privilege" was completed. An attacker could derive the image version that the route-views router was running and possibly find vulnerabilities in the image. A possible solution to this would be to rename the image to a name that does not correspond to the actually image version. The image might still be able to be derived based on the size of the file.

Securing route-views routers is a necessary part of a service provider's complete security picture. The principle of least privilege applied to the unauthenticated user guided the strict limitation of commands allowed. The defense-in-depth approach also guided how to limit the knowledge of the network that an unauthenticated user could obtain. By limiting the information provided, the Service Provider's network was afforded extra protection. "An ounce of prevention is a worth pound of cure." Route-views servers can still be useful to the Internet community without giving the keys to the network away.

References:

1. Bates, Tony, et al. "RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP." April 2000. URL: http://www.ietf.org/rfc/rfc2796.txt (16 July 2004).

2. Butler, Kevin, et al. "A Survey of BGP Security." Technical Report TD-5UGJ33. June 2004. URL: http://www.patrickmcdaniel.org/pubs/td-5ugj33.pdf (16 July 2004).

3. "CISCO IOS SOFTWARE RELEASES 12.0 MAINLINE: Passwords and Privileges Commands" URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca5e6.html (22 July 2004).

4. "Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products." 2.0. 14 July 2004. URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml (16 July 2004).

5. Greene, Barry Raveendran. "BGPv4 Security Essentials." 0.5. 20 April 2004. URL: http://www.nanog.org/mtg-0206/ppt/BGP-Risk-Assesment-v.5.pdf (16 July 2004).

6. Greene, Barry Raveendran. "Remote Triggering Black Hole Filtering." 0.2. 2 August 2002. URL: ftp://ftp-eng.cisco.com/cons/isp/essentials/Remote%20Triggered%20Black%20Hole%20Filtering-02.pdf (26 July 2004).

7. Heffernan, Andy. "RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option." August 1998. URL: http://www.ietf.org/rfc/rfc2385.txt (16 July 2004).

8. Li, Tony & Rekhter, Yakov (Eds.). "RFC 1771 A Border Gateway Protocol 4 (BGP-4)." March 1995. URL: http://www.ietf.org/rfc/rfc1771.txt (16 July 2004).

9. Luyer, David. "RE: TCP/BGP vulnerability - easier than you think." NANOG mailing list archive. 21 April 2004. URL: http://www.cctec.com/maillists/nanog/historical/0404/msg00620.html (16 July 2004).

10. Watson, Paul. "4030: TCP Reset Spoofing." Open Source Vulnerability Database. 17 June 2004 URL: http://www.osvdb.org/displayvuln.php?osvdb_id=4030 (16 July 2004).