Asgn 03

Matteo Di Fabio: 264339

Luca Genovese: 264364

Why BGP?

Once upon a time, when the Internet was just a tiny cloud, there were only a few networks connected to each other. As a result, routing between network nodes was quite static. All that needed to be done to set up routing was to define network nodes and make connections between them as needed. As we know, the Internet didn't stay small for very long time; it began to incorporate more and more networks, which needed a more dynamic routing system. As the Internet continued to expand, it became increasingly difficult to keep track of all the routes from one network to another, for that reason the solution was to transition to an Autonomous System (AS) architecture.
An AS can be an Internet Service Provider, a university or an entire corporate network, including multiple locations (IP addresses); so each AS is represented by a unique number called ASN (Autonomous System Number). As the number of autonomous systems in the internet grew, the drawbacks of EGP (Exterior Gateway Protocol) became more pronounced; its hierarchical structure hampered scalability and made it difficult to connect new networks in an efficient manner. Consequently, it was necessary to define a new exterior routing protocol that would provide enhanced and more scalable capabilities.

In June 1989, the first version of this new routing protocol, known as the Border Gateway Protocol, was formalized; then since 1994 it has been in use on the Internet.
IPv6 BGP was first defined in RFC 1883 in 1995, and it was improved to RFC 2283 in 1998.
In these lasts year some AS adopted a new version: BGP4. Unfortunately the transition to this new version is not really adopted from a lot of autonomous system because it is not completely compatible with the previous version and because its integration is quite difficult and for that reason they prefer to wait.

What is BGP?

BGP (Border Gateway Protocol) is the protocol underlying the global routing system of the internet. When one network router is connected to other networks it cannot determine which network is the best network to send its data to by itself. Border Gateway Protocol considers all peering partners that a router has and sends traffic to the router that is closest to the data's destination. This communication is possible because, at boot, BGP allows peers to communicate their routing information and then stores that information in a Routing Information Base (RIB).
We can think about BGP as a postal service of the Internet. When someone drops a letter into a mailbox, the postal service processes that piece of mail and chooses a fast, efficient route to deliver that letter to its recipient. You can think of an autonomous system in the computer world as a city with many streets. A network prefix is similar to one street with many houses. An IP address is like an address for a particular house in the real world, while a packet is the equivalent of a car travelling from one house to another using the best possible route. So our postal service (BGP) to deliver as fast as can will determinate the best route by different factors, such as traffic congestion, roads temporarily closed for maintenance, etc. The path is calculated dynamically depending on the situation of the network nodes, which are like roads and junctions.
Analyzing BGP more in detail we can say that BGP is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (ASs).
Here we will present some of BGP characteristics:

- BGP routing information includes the complete route to each destination, it uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems.
- Uses the network reachability information to construct a graph of AS connectivity, which enables BGP to remove routing loops and enforce policy decisions at the AS level.
- Allows policy-based routing: in fact it is possible to use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information.
- Using TCP as its transport protocol, the port 179 establish connections, so running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing.
- Manages how packets get routed from network to network through the exchange of routing and reachability information among edge routers.
- Directs packets between autonomous systems (AS).
- Creates network stability by guaranteeing routers can adapt to route failures: when one path goes down, a new path is quickly found.
- Makes routing decisions based on paths, defined by rules or network policies set by network administrators.
- Offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down.
- Makes routing decisions based on paths, rules or network policies configured by a network administrator.
- Each BGP router maintains a standard routing table used to direct packets in transit.
- Uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the server.

What is an autonomous system?

An autonomous system (AS) is a set of routers that are under a single technical administration and normally use a single interior gateway protocol and a common set of metrics to propagate routing information within the set of routers. To other ASs, an AS appears to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it. If we continue to think of BGP as the postal service of the Internet, AS's are like individual post office branches. A town may have hundreds of mailboxes, but the mail in those boxes must go through the local postal branch before being routed to another destination. The internal routers within an AS are like mailboxes, they forward their outbound transmissions to the AS, which then uses BGP routing to get these transmissions to their destinations. The structure of the Internet is constantly changing, with new systems popping up and existing systems becoming unavailable. Because of this, every AS must be kept up to date with information regarding new routes as well as obsolete routes. This is done through peering sessions where each AS connects to neighboring AS's with a TCP/IP connection for the purpose of sharing routing information. Using this information, each AS is equipped to properly route outbound data transmissions coming from within.
Here's where part of our analogy falls apart: unlike post office branches, autonomous systems are not all part of the same organization. As such, they have no reason to be friendly to each other and are often times business competitors! For this reason, BGP routes sometimes will not only consider the shortest AS path to reach the destination but it will also take business considerations into account. Autonomous Systems often charge each other to carry traffic across their networks, and the price of access can be factored into which route is ultimately selected.

How BGP work?

To guarantee the reliability of transmission, BGP is encapsulated into a TCP connection, meaning that two routers that want to establish a BGP session must have prior IP reachability. After establishing a TCP connection, the two routers – hereafter called BGP peers – agree on the parameters to use in the BGP session via BGP open messages, and then start exchanging routes. These routes can be generated by the peer itself or they can be learned by the peer via other BGP sessions, and each of them is announced via BGP update messages. Whenever a route is received from an AS, the route is subject to a filtering process where it can be

discarded or accepted and, if required, its path attributes are manipulated. Then a BGP decision process is applied to select the best route for each IP destination network, since an AS may receive multiple routes toward the same IP network from different peers.
The BGP decision process is composed of a sequence of steps that allow the AS to choose the best route by analyzing the path attributes of each of the candidates, in order to apply criteria that range from pure commercial (e.g. prefer a cheaper provider over the other) to technical reasons (e.g. transit traffic to reach a destination via the smallest number of ASs). Each best route is then installed in the routing table of the router and used to forward traffic. Eventually, after a proper attribute manipulation, each best route is propagated to the all other BGP peers, or a subset of them depending upon the output filtering process applied.
Having this general knowledge about routing we are now able to understand how Border Gateway Protocol (BGP) works. Based on this general knowledge we now are able to discuss the specific security issues with BGP. The biggest problem, however, is that BGP is extremely vulnerable to both malicious attacks and human error.

Vulnerability

BGP protocol has allowed network operators to apply and enforce the most varied inter-AS routing policies during the past 30 years. It is clear that the Internet is vulnerable to attack through its routing protocols and, despite all its good qualities, BGP is no exception. Faulty, misconfigured, or deliberately malicious sources can disrupt overall Internet behavior by injecting bogus routing information into the BGP-distributed routing database (by modifying, forging, or replaying BGP packets). The same methods can also be used to disrupt local and overall network behavior by breaking the distributed communication of information between BGP peers. The sources of bogus information can be either outsiders or true BGP peers.
As a TCP/IP protocol, BGP is subject to all TCP/IP attacks, e.g., IP spoofing, session stealing, etc; any outsider can inject believable BGP messages into the communication between BGP peers, and thereby inject bogus routing information or break the peer-peer connection. Any break in the peer-peer communication has a ripple effect on routing that can be widespread; furthermore, outsider sources can also disrupt communications between BGP peers by breaking their TCP connection with spoofed packets. Outsider sources of bogus BGP information can reside anywhere in the world. BGP speakers themselves can inject bogus routing information, either by masquerading as any other legitimate BGP speaker, or by distributing unauthorized routing information as themselves. Historically, misconfigured and faulty routers have been responsible for widespread disruptions in the Internet. The legitimate BGP peers have the context and information to produce believable, yet bogus, routing information, and therefore have the opportunity to cause great damage. The cryptographic protections of TCPMD5 and operational protections cannot exclude the bogus information arising from a legitimate peer. The risk of disruptions caused by legitimate BGP speakers is real and cannot be ignored.
Bogus routing information can have many different effects on routing behavior. If the bogus information removes routing information for a particular network, that network can become unreachable for the portion of the Internet that accepts the bogus information. If the bogus information changes the route to a network, then packets destined for that network may be forwarded by a sub-optimal path, or by a path that does not follow the expected policy, or by a path that will not forward the traffic. Consequently, traffic to that network could be delayed by a path that is longer than necessary for that reason the network could become unreachable from areas where the bogus information is accepted. Traffic might also be forwarded along a path that permits some adversary to view or modify the data. If the bogus information makes it appear that an autonomous system originates a network when it does not, then packets for that network may not be deliverable for the portion of the Internet that accepts the bogus information. A false announcement that an autonomous systems originates a network may also fragment aggregated address blocks in other parts of the Internet and cause routing problems for other networks.

What could possibly go wrong?

The damages that might result from these attacks include:

- Starvation: Data traffic destined for a node is forwarded to a part of the network that cannot deliver it.

- Network congestion: More data traffic is forwarded through some portion of the network than would otherwise need to carry the traffic.
- Black hole: Large amounts of traffic are directed to be forwarded through one router that cannot handle the increased level of traffic and drops many/most/all packets.
- Delay: Data traffic destined for a node is forwarded along a path that is in some way inferior to the path it would otherwise take.
- Looping: Data traffic is forwarded along a path that loops, so that the data is never delivered.
- Eavesdrop: Data traffic is forwarded through some router or network that would otherwise not see the traffic, affording an opportunity to see the data.
- Partition: Some portion of the network believes that it is partitioned from the rest of the network, when, in fact, it is not.
- Cut: Some portion of the network believes that it has no route to some network to which it is, in fact, connected.
- Churn: The forwarding in the network changes at a rapid pace, resulting in large variations in the data delivery patterns (and adversely affecting congestion control techniques).
- Instability: BGP becomes unstable in such a way that convergence on a global forwarding state is not achieved.
- Overload: The BGP messages themselves become a significant portion of the traffic the network carries.
- Resource exhaustion: The BGP messages themselves cause exhaustion of critical router resources, such as table space.
- Address-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.
- Confidentiality violations: The routing data carried in BGP is carried in cleartext, so eavesdropping is a possible attack against routing data confidentiality. (Routing data confidentiality is not a common requirement.)
- Message manipulation: BGP does not provide protection against insertion, deletion and modification of messages.
- Man-in-the-middle: 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.
- BGP route manipulation: A malicious device alters the content of the BGP table, preventing traffic from reaching the intended destination. For example routing to endpoints in malicious networks or creating of route instabilities.
- BGP route hijacking: A rogue device maliciously announces a victim’s prefixes to reroute traffic to or through itself, which otherwise would not happen. Rerouting traffic can cause instability in some networks with a sudden load increase. This allows attackers to access potentially unencrypted traffic to which they would otherwise not have access or use hijacked BGP to launch spam campaigns, bypassing IP blacklist mitigation.
- Sniffing. This requires control of a device along the path of the victim's communications. The attacker can achieve this by using BGP to detour traffic through a malicious network.
- Revelation of network topologies. Every BGP-enabled router possesses all the routing information of the Internet, knowledge useful for criminal operations and waging cyberwar. In theory, BGP keeps the policies underlying these interconnections private. However, most relationships among ASs are as peers (which exchange traffic at no charge to each other), customers, or providers. With patience, an attacker can use the routing table to unmask these relationships.
- Denial of service. An attacker can black-hole portions of the Internet either by creating false routes or by killing valid ones.

What is BGP Hijacking?

BGP hijacking is an illicit process of taking control of a group of IP prefixes assigned to a potential victim. Either intentionally or accidentally, it is achieved by changing paths used for forwarding network traffic, exploiting the weaknesses of BGP. BGP exchanges routing and reachability information among AS. Information is

exchanged between BGP speaking routers called BGP peers (neighbors). BGP peers are explicitly defined with the neighbor command and they trust each other. The IP prefix is then installed into the peer routing table and is advertised to the other BGP peers. The prefix is then propagated to other ASs without checking if an origin AS owns the prefixes which it announces. In fact, everyone who has been assigned an AS number or gained access to a BGP speaking router can announce any prefix.

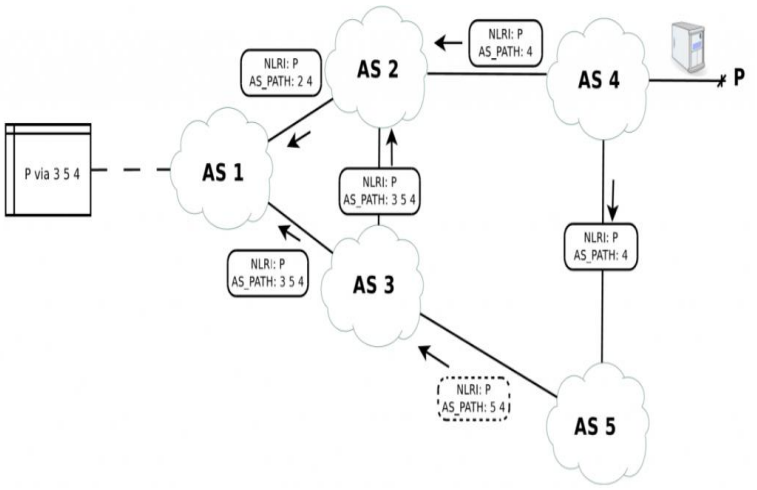
Prefix/Rooting Hijack Attacks: Prefix hijacks are deliberate intentional generation of bogus routing information; the reasons behind them are of a multitude that is difficult to fathom.

The attacker could announce routes to disrupt the services running on top of the IP space covered by the routes, or hijack the traffic to analyze confidential information flowing towards that service: this easily disrupts the Internet by causing cyberattacks, shutting down services, or creating reliability issues. One use of hijacking is to block social media sites. The attacker could also simply announce routes with a crafted AS path to show fake neighboring connections in famous websites or even worse, the attacker could hijack the traffic to manipulate the flowing packets at his/her will, or simply want to exploit unused routes to generate spam.

There are roughly 65,000 AS's that make up the global internet, and little to no oversight for how each AS peering filters must be configured.

Consider now this kind of attack applied to those 65,000 AS's, each with its own filter policy, if any. The consequence is that part of the Internet will redirect its traffic towards the attacker, while the rest will redirect its traffic towards the proper origin. The amount of AS's redirecting their traffic towards the attacker will depend on two factors: the quality of the filters applied by the providers, and the BGP decision process output of each AS.

Route Leaks and Fat Finger Syndrome: Route leaks are unintentional generation of bogus routing information caused by router misconfigurations, such as typos in the filter configuration or mis-origination of someone's else network (fat finger). Even if unintentional, the consequences of a route leak can be the same as the prefix hijacks. Now think again about the 65,000 AS's in the Internet and imagine that AS 4 is a rural service provider with few resources, both technical and economic. This would mean that probably the upstream connection he/she bought from his/her providers is very limited, thus making the two links a *bottleneck* in this route leak scenario. In this case it is possible that AS 5 will not be able to handle the amount of traffic directed to *P,* causing not only an additional delay, but also several packet losses.



How Attackers Can Exploit BGP

Because a nation state can easily control the border routers of many ASs, both overtly and covertly, cyberwar is potentially the most serious scenario for BGP exploitation. However, any individual can get into the act by breaking into a BGP-enabled router. The Internet has many poorly managed edge networks whose border routers are more likely to suffer default passwords or remotely exploitable vulnerabilities, or allow Telnet logins.

Even without control of a border router, an attacker may send it off-path, third-party reset (RST) segments with forged source addresses of victim routers. This makes it appear as if the victim routers have gone offline, removing them from the routing table.

The TCP MD5 Signature protocol, adopted in 1998, was supposed to make it impossible to forge resets. However, discovery of mathematical flaws in MD5 and the power of today's processors mean that it only takes hours for a laptop to find a valid sequence number.

Real attack examples

- Routing to endpoints in malicious networks. On October 3, 2002, the UUNet segment of WorldCom's backbone suffered major outages. Later, analysts concluded that this was simply an episode of the unintentional routing instabilities that plague the Internet. Because the causes remain poorly understood, they may blow back upon the attacker. This may deter cyberwarriors from triggering instabilities. But what if script kiddies ever popularize this means of having fun?
- A partial BGP hijacking occurs when two origin Autonomous Systems announce an identical IP prefix with the same prefix length. The BGP best path selection rules, such as preferring the shortest AS path, determine which path is the best.
  An example of Partial BGP Hijacking a route leak which falls perfectly in this scenario is the infamous hijack of YouTube prefixes by Pakistan Telecom on Sunday, February 24th, 2008. The Pakistan ISP (AS17557) configured a static route 208.65.153.0/24 pointing to null in order to block YouTube access for AS17557 customers. However, the ISP started to announce the prefix 208.65.153.0/24 towards its upstream provider PCCW Global (AS 3491) which didn't apply proper filters and caused a domino effect, propagating the announcement to its peers. In an hour and twenty minutes, YouTube (AS36561) that had been announcing prefix 208.65.152.0/22 (208.65.152.0/24, 208.65.153.0/24, 208.65.154.0/24, 208.65.155.0/24) so far, started to fight back. YouTube began to announce more specific prefix 208.65.153.0/24. They kept announcing 208.65.152.0/24 for another 11 minutes, however the service would still not be available for a large part of YouTube users. Those were the users whose traffic took a path towards Pakistan Telecom AS17557, thus it could not reach YouTube. The traffic was being backhauled by a static route configured on Pakistan AS17557 edge router causing about 3 hours of service disruption to YouTube.
- The complete BGP hijacking occurs when an attacker announces de-aggregated thus a more specific IP prefix than the actual owner of the prefix. This tactic, however, was put to good use by YouTube in the incident described above, to bring the hijacked prefix 208.65.153.0/24 back. YouTube started to announce this prefix as two sub-prefixes 208.65.153.0/25 and 208.65.153.128/25. They knew that the longest prefix match rule prefers more specific route. Paths toward these prefixes were preferred so the YouTube service could be reachable again. After the PCCW Global (AS3491) withdrew all prefixes originated by AS 17557 (Pakistan Telecom), YouTube could announce the aggregate route 208.65.152.0/22 again instead of the more specific prefixes.
- April 8 2010, for 18 minutes, a significant portion of Internet traffic, including that of U.S. government and military sites, was misrouted to China. Early estimates indicated 15 percent of all traffic was sent in the wrong direction, but that figure was misreported from the source document; rather, traffic from 15 percent of Internet sites was affected, which doesn't correlate to 15 percent of all Net traffic. Whether it was 15 or only 1 percent of all traffic that was misrouted, the incident lays bare a huge Internet security vulnerability in BGP (Border Gateway Protocol), a routing protocol used by ISPs to direct backbone traffic around the Internet. BGP routing tables are used in a nearly fully meshed network among all ISPs in the world. It's not hyperbole to say this is the way the Internet works.
- According to The Washington Post, Internet monitoring company Renesys says man-in-the-middle attacks began surfacing in 2013. In February 2013, traffic from major financial institutions, governments, and network service providers was diverted from its usual paths and went through Belarus before it was sent back through to the normal destinations.
- In another case, all traffic between Europe and North America was rerouted through a service provider in Iceland. The culprits probably carefully crafted this so that the additional delays created little to no performance degradation. The victims of man-in-the-middle attacks may never realize that their traffic was diverted.
- More worrisome still is that malicious attacks are becoming more widespread. A 2014 study by Andrei Robachevsky of the Internet Society found that at least 10% of routing incidents are real threats. There are a few malicious attacks every month.
- BGP route hijack attack with a man-in-the-middle attack. In this type of attack, traffic is diverted, giving criminals access to it before it goes to its final destination. In 2015, researchers at Dell SecureWorks uncovered multiple man-in-the-middle BGP attacks used to steal bitcoins. The thief earned about $83,000 in profits in more than four months, compromising 51 networks from 19 different ISPs.

Conclusion

So as we understand BGP (in particular BGP3 that is the one we discussed about) is spread worldwide and due to all the mentioned vulnerabilities this is a very big problem to face as a possible attack could have far-reaching catastrophic consequences. As we anticipated a possible solution to face this problem could be to adopt BGP4 protocol. In fact this new version of BGP (released in 2006) try to solve most of the known problems: it correct errors, clarify ambiguities and update the specification with common industry practices. Unfortunately even if a solution is already present, the problem is still not completely solved, because the transition from BGP3 to BGP4 is difficult due to the incompatibility between the two protocols, so the most of ASs don't want to invest (also because there are not advantage in performances).