REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

THREAT ASSESSMENT[1] *June 2020*

Risks and mitigation options of the Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) used to manage data on the Internet is insecure in nature and has caused tens of thousands of incidents, many of them with global implications. One of the latest examples comes from the 9th of June, when BGP hijacking caused IBM Cloud outage that lasted for hours. There are solutions, the use of which makes the BGP much safer, but unfortunately, Estonia is among the last in the European Union to implement them.

BGP – what is it and how does it work?

BGP is a routing protocol used to exchange routing information between different autonomous systems. Autonomous systems, in turn, contain information about one or more IP prefixes, or IP networks. It depends on the BGP whether our data is securely transferred from one autonomous system to another.

The BGP is like an Internet roadmap, but it can also be compared with the postal service when explaining its role and need. After the sender has put the envelope in the mailbox, the postal company selects the way to use to deliver the letter to the addressee on the basis of the address indicated on it and the information available to the postal company.

If someone wants to transfer data from an IP network device in one autonomous system to an IP network device in another autonomous system, then, like a postal company, they first need information about the possible routes by which this information can be delivered. BGP is designed to exchange such information between different autonomous systems. Based on the information received, a so-called road map is prepared analogously to a postal company and a suitable route is selected for the delivery.

Because the Internet is a network of tens of thousands of smaller networks, data usually flows between different autonomous systems. Each such system must have at least one router that communicates with the routers of the other autonomous systems under the BGP protocol. Autonomous systems are not always connected to a single system; there are also Internet nodes

[1] Section 12 of the Cybersecurity Act:
(2) For the purpose of ensuring cybersecurity, the Estonian Information System Authority observes domains in the Estonian Internet protocol address space and related to the Estonian country code, analyses risks posed to the security of systems, and the impact thereof on the state, society, and the security of systems.
(3) For the purpose of preventing and resolving a cyber incident, the Estonian Information System Authority sends people alerts enabling them to take measures avoiding or reducing the impact of the cyber incident.

where one autonomous system can exchange information with several other autonomous systems at the same time.

The nodes of autonomous systems connected to the Internet are located all over the world. Thanks to such nodes, the multiplicity of possible paths is guaranteed, and if one path is interrupted, it is always possible to choose the next one to deliver the data. As long as all participants share truthful information, the data will reach its desired destination. Problems start when one router sends incorrect information to another.

Security risks of the BGP

BGP was created more than 25 years ago and its authors focused on simplicity, reliability, and ease of use. Security was not one of the priorities at the time, so BGP was initially vulnerable to configuration errors and attacks.

One of the most common problems is BGP hijacking. During it, one node provides false information about data transmission paths to nodes that are directly connected to it through the routing table, or claims to own IP addresses that actually belong to others. Without security protocols, such misinformation can spread around the world in minutes, moving from one autonomous system to another. When this happens, the misled devices try to route data along incorrect or non-existent paths. This can result in service interruptions, fraud, or data theft.

Figure 1: This is what a query that successfully reaches its destination looks like.

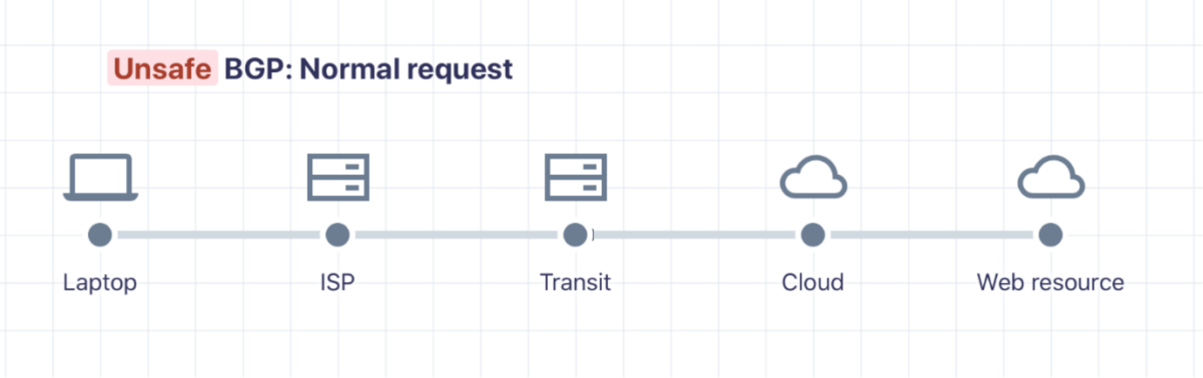
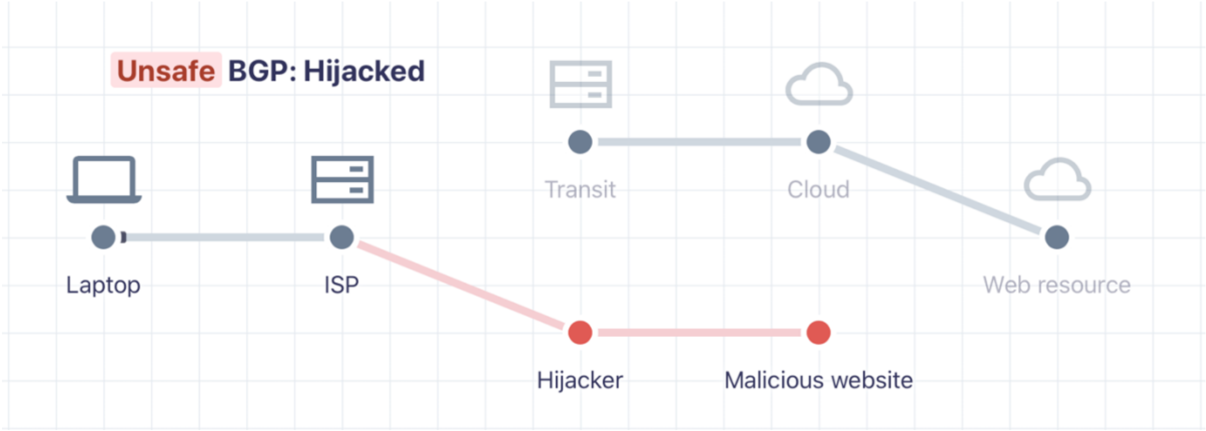


Figure 2: This is the movement of a query that was hijacked halfway due to a BGP vulnerability: the user reaches the hijacker’s page instead of the desired page.



BGP is based on trust: routers publish information about possible data paths, and other routers usually trust the received information blindly and distribute it without checking. In general, the routing information obtained is correct, but errors with high impact and cost also occur. There are mostly due to configuration and human errors, but there have also been more serious malicious hijackings aimed at cryptocurrency or data theft.

Major incidents

Much of Europe's mobile data was routed through a Chinese telecommunications company. On 6 June 2019, the internal routing table of the Switzerland-based data center colocation company Safe Host leaked. Instead of ignoring the leaked routing information, China Telecom, a Chinese Internet service provider, announced Safe Host's routes as its own using unsecured BGP. As a result, much of Europe's mobile data was routed through China Telecom's infrastructure, which meant that the data of many European mobile operators' customers moved through China. During this time, customers experienced slower-than-usual traffic, but a bigger problem was the possible data collection that the Chinese telecom company was able to do during the incident. While routing incidents usually last only a few minutes, this incident lasted more than two hours.

Part of the intra-US Internet traffic went through China. In July 2018, it was discovered that China Telecom had been directing some of its intra-US Internet traffic through China for 2.5 years based on incorrect routing information. For example, data sent from Los Angeles first moved to Hangzhou and only then to Washington.

Criminals hijacked traffic to a cryptocurrency page. In April 2018, criminals took advantage of the BGP's vulnerability to redirect those who wanted to go to myetherwallet.com, a cryptocurrency page, to a similar fraudulent page. When users entered their usernames and passwords, criminals transferred the cryptocurrency in the victims' account to an account under their control.

To Google and Facebook through the Russian Federation. In December 2017, as a result of a BGP hijacking, more than 200 well-known websites (including Google, Facebook, Microsoft, and Apple) were routed through the autonomous system of the Russian Federation, which had not been used for years before the incident. The incident lasted about an hour and raised suspicions that the company that caused the incident stored the data obtained by redirecting the data stream.

Turkey became an Internet node. On the morning of Christmas Eve 2004, the Turkish internet service provider TTNet sent routing information via BGP, which essentially claimed that TTNet was the best route for almost anything on the Internet. As the other service providers did not verify this information, but passed it on to subsequent service providers, most of the global Internet traffic was routed through Turkey for several hours. TTNet's infrastructure was not ready for the increased traffic, so a large proportion of Internet users could not access the desired pages for several hours.

Pakistani telecom took down YouTube. In February 2008, the Pakistani government ordered a national telecom company to block access to YouTube on Pakistani territory. The telecom company changed the routing information so that anyone who wanted to visit the popular video platform was redirected to a page that said YouTube was blocked. Unfortunately, the Pakistani telecom network equipment sent updated routing information via BGP to other Internet service providers, which did not check it but passed it on to the next telecoms. The result: YouTube was offline worldwide for two hours.

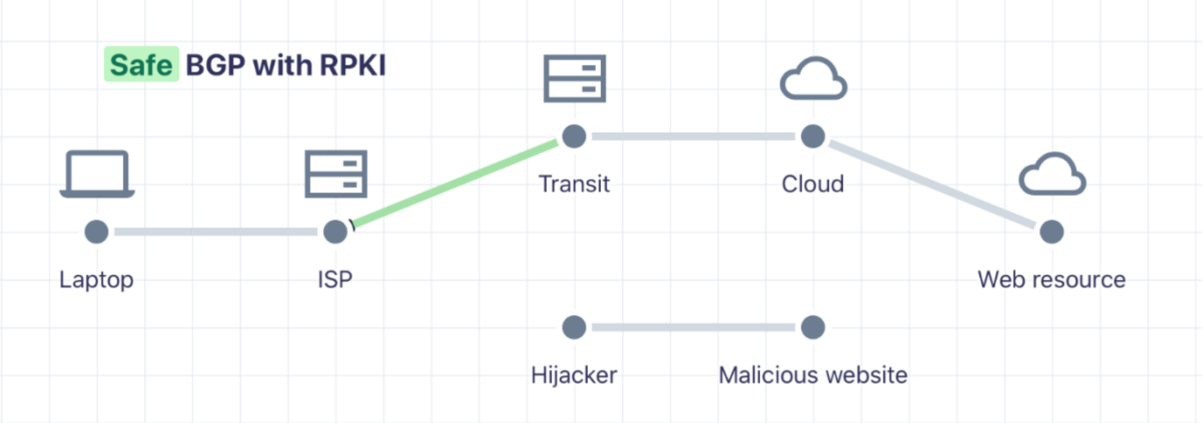
RIA's recommendations: how to make the BGP more secure

As these cases confirm, the BGP is not secure by default. Monitoring network traffic, looking for anomalies, sharing your routing practices with partners, and filtering prefixes help increase security, but the validation of BGP routes is crucial here.

One of the most recognised and common routing information validation solutions is RPKI (Resource Public Key Infrastructure), which we recommend to implement for all Estonian companies that have an autonomous system.

With the RPKI, the owner of the autonomous system can express the connection between their autonomous system and their prefix by means of an ROA record (Route Originate Authorisation) and confirm it with a digital signature. This, in turn, allows routers configured to check routing information using RPKI to filter out the incorrect routings.

Figure 3: BGP hijacking attempt after RPKI implementation.



What to do to sign ROA records?

As the Regional Internet Registry (RIR) in our region is RIPE, we use their chain of trust. The signing takes place through the RIPE LIR portal and takes a few minutes.

- Go to lirportal.ripe.net
- Log in to your RIPE NCC account.
- In the page header, select Manage IP-S and ASN > LIR portal > Resources > RPKI Dashboard.
- Follow the instructions on the screen.
- When answering whether you want to use your own or the RIPE certificate authority (CA), we recommend that you choose the latter. As the certificates are maintained by RIPE anyway, the use of your own certificate does not add significantly in terms of opportunities or risks.
- The window that opens has a column of Autonomous System (AS) numbers and prefixes. Select all prefixes and click the 'Create ROA for selected BGP Announcements' button.
- Confirm your selections.
- This is followed by a RIPE inspection and test. If no problems occur during this process, a digitally signed ROA record is made after two days, after which the other autonomous systems can validate the routing pointing to your autonomous system.

What can I do to get my routers to validate routings as well?

We recommend using the RIPE validation solution rpki-validator.ripe.net to validate the routings.
The installation guide is available at https://labs.ripe.net/Members/tashi_phuntsho_3/how-to-install-an-rpki-validator.
Examples of router settings can be found at: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration

If you have any questions, you can also contact CERT-EE: cert@cert.ee

Risks associated with the implementation of RPKI

There are no significant risks associated with the implementation of RPKI. Configuring the system so that incoming routings are accepted if the validation solution is interrupted does not run the risk of availability. If the validation solution is interrupted, all routings are accepted, i.e. the situation before the implementation of RPKI is maintained.

Summary

RPKI is not a new technology, but unfortunately, it is not used as widely as it could be to secure BGP. According to the information received by CERT-EE, the IP addresses of Estonian internet service providers have also been announced from the wrong networks, but despite this, we are still among the last in the implementation of RPKI in Europe and this makes us very vulnerable to BGP hijackings. Continuing in the same way, Estonia may become more and more likely to be hit by an incident due to the weakness of the BGP.