Assessing the security of Internet paths: A case study of Dutch critical infrastructures

AUTHORS:
SHYAM KRISHNA KHADKA (s.k.khadka@utwente.nl), University of Twente

SUZAN BAYHAN (s.bayhan@ utwente.nl), University of Twente

RALPH HOLZ (r.holz@ utwente.nl), University of Twente

CRISTIAN HESSELMAN (cristian.hesselman@sidn.nl), SIDN Labs

EXECUTIVE SUMMARY

Critical Infrastructures (CIs) such as banks and telecom operators increasingly rely on cloud-based email services from Microsoft or Google. However, CIs often have limited insight into the security status of the paths their network traffic might follow, across the Internet, to reach these cloud providers, which we consider a supply chain risk. We therefore developed a generic method that finds plausible Internet paths to clouds and other hosts on the Internet, and identifies to what extent the transit networks, the so-called "Autonomous Systems (ASes)", on a path support a routing-security feature known as "Route Origin Validation (ROV)". We used our method in a case study to find secure paths from four CIs in the Netherlands to Microsoft's cloud-based email service.

THE PROBLEM: LIMITED INSIGHT INTO THE SECURITY OF PATHS TOWARD THE CLOUD

CIs typically have limited insight into the security status of the paths that their traffic might follow across the Internet to reach the email infrastructure of their cloud provider. For example, a CI might not know their traffic passes through networks (ASes) that do not implement Route Origin Validation (ROV). As a result, the CI's traffic is vulnerable to prefix hijacks, which is the situation where someone tricks the wider Internet into sending data to the wrong place, which can cause outages or let attackers see or even modify the data. Even if a single AS on a path does not deploy ROV, it can remain vulnerable to such attacks, known as "collateral damage".

Ultimately, these attacks constitute a possible form of supply chain vulnerability for CIs. The risk is real: prefix hijacks are common incidents on the Internet and are well-known to have been used for malicious purposes, for instance, to attack payment systems, steal cryptocurrency, disrupt traffic, and stage Distributed Denial-of-Service (DDoS) attacks. Our question, therefore, was what it would take to enable CIs to get more insight into the security status of each Autonomous System on a path towards their cloud provider or other destination.

OUR APPROACH: CALCULATE THE ROV SCORE OF VALID INTERNET PATHS

We combine routing data collected from public route collectors (RouteViews and RIPE RIS) to find Internet paths and then use ROV scores to assess the security of those paths. We use our method of calculating the ROV score of paths for four CIs (two banks, one water supply company and one energy company) in the Netherlands. We observed a higher number of ROV-unprotected paths compared to ROV-protected ones. For instance, one bank in our study had 40 ROV-unprotected paths and only 20 ROV-protected paths across path lengths of one to three AS hops, totaling 20 paths for a maximum length of three hops. These findings enabled us to propose practical recommendations for improving path security for such CIs.

RECOMMENDATION: COALITION OF ASes TO FORWARD CI TRAFFIC

- A coalition of ASes that are ROV-protected would increase the number of ROV-protected paths to forward traffic between each other.
- We envision that ASes could also offer such concepts as a value-added service to customers who need more insight into the (ROV-based) security of ASes that handle their traffic (for example, through visualizations), as well as more control over which path will be chosen.
- Key project partners have expressed an interest in following up on possible business models.

CONCLUSION

Although we used our method to calculate the ROV scores of Internet paths from CIs to Microsoft’s mail service in the Netherlands, it can also be used to assess the ROV security of paths from any source AS to any destination AS, with or without a particular destination IP prefix. Our case study shows that multiple paths are 100% ROV-protected and multiple others with considerably less or even entirely without ROV protection. However, our analysis also reveals that implementing ROV fully on the side of the upstream providers of CIs will increase the number of fully ROV-protected paths toward the Microsoft mail service by 72.5% on average. We hence are optimistic that our method provides a useful metric to improve overall network security in the Netherlands.

Blog post: https://blog.apnic.net/2024/07/12/assessing-the-security-of-internet-paths/

Paper:https://www.sidnlabs.nl/downloads/6yyoRiOIxGs9EZNPVsdRVn/4a635100c204fef25caf07382ef28682/ANRW-path-security-final.pdf