Security Evaluation of Network Traffic Mirroring in Public Cloud

Vipul Sharma

Technical Report

RHUL–ISG–2021–4

23 November 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

More and more enterprises are moving their information technology workloads from an on-premise data centre to the public cloud; the network monitoring techniques used in traditional on-premises environment are being tailored to enable these technologies to run in the public cloud. Network traffic mirroring is one of the technique that is being used to detect and prevent attacks, analyse performance issues and carry out network forensics. This is the technology wherein the network traffic is mirrored from one system (mirror source) onto another system (mirror destination) in order to carry out network traffic analysis.

Network traffic mirroring has been carried out for long in an on-premise environment but it is relatively new in the public cloud setup; a security evaluation of the technique in public cloud setup is therefore required to understand the security implications of using this technique in public cloud setup and considerations one must undertake to keep the infrastructure secure. The key focus of the project was to carry out a security evaluation of network traffic mirroring technique across public cloud environments.

After looking at how the technique was implemented in traditional on-premise environment; a comprehensive study was carried out analysing how network traffic mirroring is being implemented in public cloud; specifically in Amazon web services (AWS) and Google cloud platform (GCP). The differences in implementation were studied and security impact was analysed. The differences ranged from the way network traffic mirroring was implemented to how the mirrored traffic packets were mirrored across to the mirror target destination from a mirror source. There were also differences in the type of virtual instances that were supported as a mirror source.

In order to carry out an in-depth security evaluation of the network mirroring technique as implemented in a public cloud environment; a lab environment was setup on both the cloud environments i.e on AWS as well as GCP; the lab consisted of virtual instances to be used as mirror source and mirror destination (target). Security evaluation was carried out for ICMP, HTTP and DNS traffic and the traffic was examined at the mirror source as well as the mirror destination.

Various weaknesses were identified during the experimentation. It was discovered that although the network traffic for HTTP and ICMP get mirrored effectively from the mirror source to the mirror destination; the network

traffic for DNS is not mirrored across. Also the inherent features of public cloud like elasticity and scalability (wherein depending upon pre-defined cpu or memory threshold the computing instance will scale out or scale in automatically if the threshold is breached) results in the network traffic mirroring not to work effectively when mirroring is carried out from one computing instance to another computing instance or when network traffic mirroring is carried out for a specific network card to another mirroring traffic destination.

The massive weakness discovered during this project across both the cloud offering was the inability to mirror the DNS traffic. In order to demonstrate the security implications of this weakness; a further experiment was carried out by registering three domain names and creating a DNS setup. A comprehensive experiment was undertaken wherein data exfiltration was carried out successfully from the mirror source instance to the DNS server; there was no DNS traffic mirrored for this on to the mirror destination instance. The experiment was successful for data exfiltration for both plain text as well as for base64 encoded text. This experimentation showed that the weakness found in the lab setup can be exploited by a malicious user to exfiltrate data from a computing instance without its trace being captured in the network traffic mirroring setup in public cloud environments.

The project paper also provides some details on the countermeasures that could be considered in order to address the weaknesses identified during the experimentation. These measures leverage the public cloud features like serverless applications and appending DNS specifically with the DNS queries, The drawbacks of these countermeasures were also mentioned.

The security evaluation of the network traffic mirroring technique in public cloud does brings out some serious weaknesses in the technique and addressing the same is imperative for enterprises to adapt the technique.