USE CASES

of Path Validation Technique

I. SERVICE FUNCTION CHAINING (SFC) PATH ATTESTATION AND VALIDATION

Customers can select atomic security functions and attest as a security package (SFC path), subsequently the service provider can provide sequential evidence of processing of these functions for the traffic.

II. HIGH SECURITY TRAFFIC PATH

No data leak from the path

Some customers have high data security demands for their sensitive traffic, e.g., VOIP calls or video conferences for VIP clients, a bank's financial data. This requires assurance that their data only travels on top of their selected secure path.

III. ROUTING COMPLIANCE

a) **Data Sovereignty/Geofencing: Ensuring No Data Leakage**

- For legal or business compliance reasons, customer privacy data must remain within defined geolocations, such as their campus or native country.
- Also, some devices are behind their security updates, still generating cryptographically vulnerable traffic. Path validation can monitor and keep these data from “escaping” a limited domain.

b) **Geo-detour: Avoidance of Certain Geolocations**

Certain domains or geolocations could be undermined by natural disasters or negative human activities, avoiding which can prevent potential performance loss.

IV. PREFERENCED ROUTING PATH SELECTION

a) **Trusted path selection**

- To provide high-security VPN services for VIP customers, the operator needs to prove that the VPN connection utilizes a path composed of high-security level network devices.
- “High security” can be defined by a set of trust metrics such as remote attestation results, ciphersuites in use, software supply-chain statements, previous event reports, etc.
- Once the path is chosen, path validation outcomes can also be a trust metric in reverse.

b) **Level of Trust**

Progressively, clients can calculate a level of trust (LoT) on a VPN service based on the above “trust metrics”. Conversely, customers can request particular LoT from service providers, to be enforced by this service provider and verified by an independent third party for audit purposes. (relates to the Trust-Enhanced Networking topic discussed in the ALTO WG)

V. SUPPORTING SECURE TELEMETRY SUCH AS IOAM, IFIT, SRV6 PATH TRACING

One of the goals of secure telemetry is to accurately log a packet’s transit path. A cryptographically verifiable secure proof of transit can enhance the credibility of these recorded transit paths.

VI. INGRESS FILTERING

- uRPF filters address-spoofing packets by performing a reverse path lookup in FIB table, all the way to the source IP address. Packets without a valid path are dropped.
- Path validation can 1. augment the uRPF check by executing an actual path traversal, ensuring that the stored path is not only existent but also current, potentially lowering the false negative rate. 2. It can also immediately discard packets that do not have a valid transit proof.

VII. MISSING ANYTHING?

Put it down, let us know!

Path Validation Side Meeting @ IETF 118

Location: Karlin 4

Date: Nov 7 2023, Tuesday

Time: 6:30PM – 8:00PM

Organized by: Huawei

Contact: liuchunchi@huawei.com