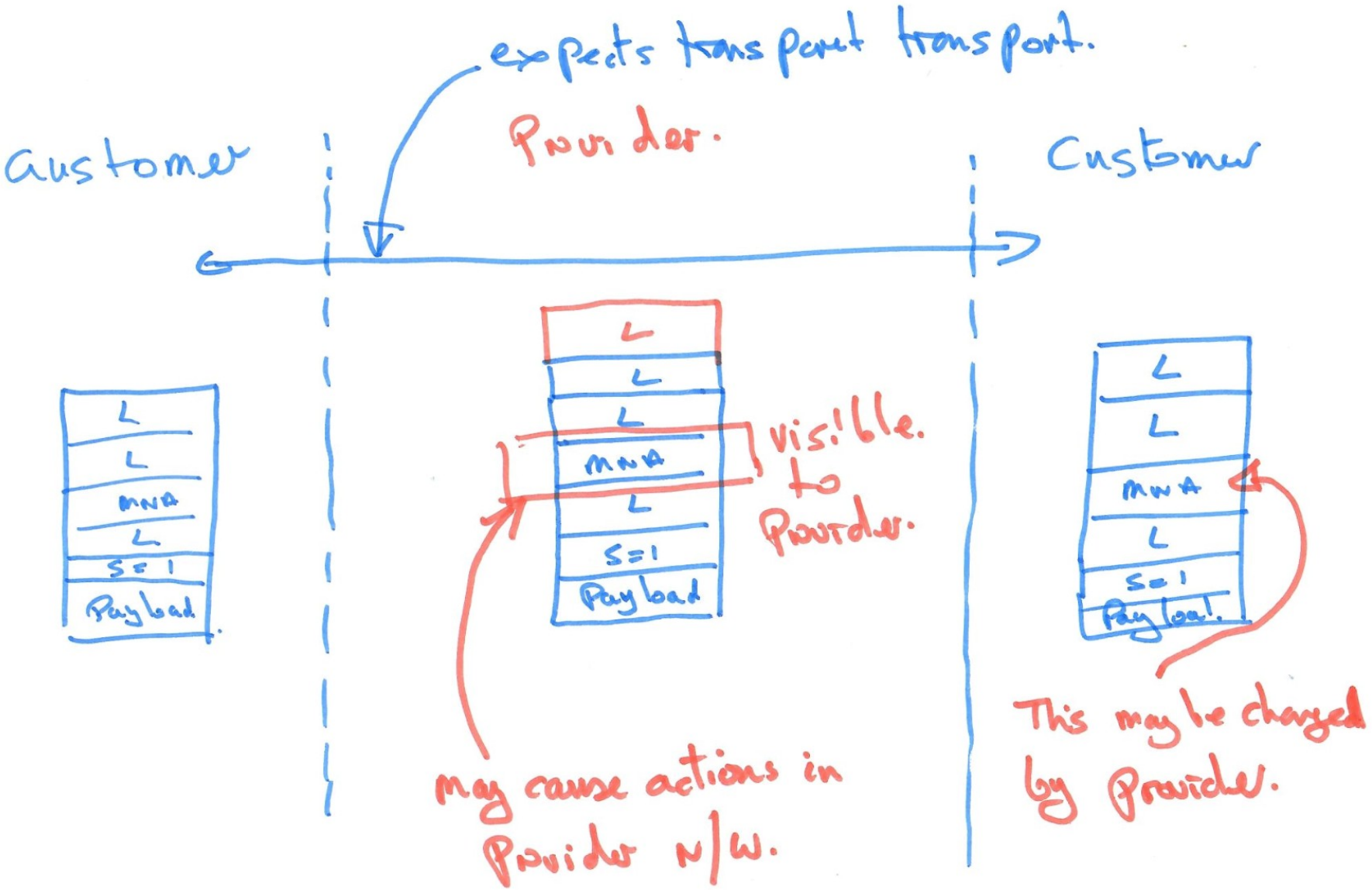
A Security Issue with MNA ISD

Stewart Bryant 19 Oct 2023

The Issue

- When updating the security section of draft-ietf-mpls-mna-fwk I noted an interesting vulnerability.
- Normally carrying MPLS over MPLS is entirely benign - the MPLS LS that is being carried is transparently carried.
- The customer stack may be explored for ECMP purposes but for no other purpose.
- However, if the customer packet contains an MNA header with actions there may be an interaction.


expects transparent transport.
Provider.
Customer
Customer
L
L
MNA
L
S=1
Payload
L
L
L
MNA
L
S=1
Payload
visible to Provider.
may cause actions in Provider N/W.
L
L
MNA
L
S=1
Payload
This may be changed by Provider.

Mitigations

- Reject all inbound packets containing MNA unless the customer is trusted AND there is a processing agreement.
- Fully encapsulate inbound traffic so that MNA Hdr not visible in provider network
- Include MNA Hdr in provider network (may need one per scope)
- Have MNA Hdr state whether provider should process.

Afterthought

- When thinking about this I was concerned about transparency and interactions inside provider network.
- However an attack on the provider network could be used to inject MNA into the customer network as an attack.