Security Considerations for Tenant ID, Etc.

draft-eastlake-secdispatch-tenantid-consid-03

Donald Eastlake 3rd (Futurewei Technologies) <d3e3e3@gmail.com>
Nancy Cam-Winget (Cisco Systems), Mohammed Umair (IPinfusion)
Scenario

• Inside a network domain, source / ingress information is included in a packet’s header based on information available at ingress and is removed at the egress node(s). What are the Security Considerations?
Scenario

- Inside a network domain, source / ingress information (meta data) is included in a packet’s header based on information available at ingress and is removed at the egress node(s). What are the Security Considerations?
Scenario

• Added Information might be based on:

  • Information only available at ingress node such as
    • Input port ID
    • VLAN Tag

  • Information that would be forwarded anyway but would not be easily accessible due to
    • Encryption
    • Depth in packet
Threats

• These are the primary threats due to the addition of such information to packets:
  • Privacy due to surveillance of added information
    • Link Surveillance
    • Surveillance from within transit/egress nodes
  • Modification/Forgery
    • On a link
    • Within a transit/egress node
• Other threats like packet deletion or replay need to be considered but are only weakly related to the addition of information.
Example

• For example, if VXLAN [RFC7348] is in use, the combination of
  • the outer IP header source and destination IP addresses, which identify VXLAN Tunnel End Points (VTEPs), and
  • the inner original header IP addresses,
• normally enable one to precisely identify a host/VM/Tenant.
Security Considerations

• Surveillance Oriented Considerations
  • Minimization
  • Encryption
  • Obfuscation

• Other Security Considerations
  • Integrity and Authentication Considerations
  • Covert Channel Considerations
Security Considerations

Surveillance Oriented Considerations:

Minimization > Encryption > Obfuscation

• MUST minimize the inclusion of such added information with packets. Information that is not present does not cause security problems for the threats being considered.
Security Considerations

Encryption:

• With good algorithms and key management, this secures plaintext so it cannot be recovered without the key.

• If additional information is needed in packets, consider:
  • Hop-by-hop link encryption and
  • Edge-to-edge encryption.
    • Fields needed to route the packet and control packet handling need to be readable.
  • If some information cannot be encrypted, consider securing it with AEAD.
  • Some information, like number and size of packets, is hard to efficiently conceal.
Security Considerations

Obfuscation, if encryption impractical:

• Weak type security to protect from
  • inadvertent disclosure (such as accidentally viewing a packet as ASCII while debugging a network) and
  • easily guessable valid identifiers (see [RFC9416]).

• Relatively easy, for example
  • XOR some nonzero fixed bytes with a field and
  • assign new identifier values in a non-sequential manner.
Security Considerations

- Other Security Considerations
  - Integrity and Authentication Considerations
    - Integrity and Authentication of additional information is important.
    - When encrypting, authenticated encryption / AEAD should normally be used.
  - Covert Channel Considerations
    - Additional fields or encrypted parts of a packet may provide places that can be used as covert channels to downstream nodes.
Example Fields

- Service Function Chaining (SFC) Network Service Header (NSH) Context Headers (see RFC 9263 in particular).
- VXLAN Network Identifier and NVGRE Virtual Subnet ID.
- Geneve Variable Length Options.
- Outer IP Fields in the case of tunneling.
- IPv6 options.
Next Steps

• Soliciting comments
  • draft-eastlake-secdispatch-tenantid-consider-03

• RTGWG adoption call?
END