Network Working Group
Internet-Draft
Intended status: Standard Track

L. Yong
Huawei USA
T. Herbert
Google

Expires: April 2015

October 27, 2014

Generic UDP Encapsulation (GUE) for Secure Transport
draft-hy-gue-4-secure-transport-00

Abstract

This document specifies use of generic UDP encapsulation (GUE) [GUE] to provide secure transport over IP networks and Internet, including use of IPSEC with GUE and methods to provide integrity and authentication of the GUE header.

Status of This Document

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 27, 2015.

Table of Contents

1. Introduction

This document specifies use of generic UDP encapsulation (GUE) [GUE] to provide secure transport over IP networks and Internet, including use of IPSEC with GUE and methods to provide integrity and authentication of the GUE header.

Secure transport over IP networks is extremely important for many applications in IP networks. Tunnel mechanisms can be used to provide secure transport for some network protocols over IP networks. For example: IPsec [RFC4301], L2TP [RFC3931].

This draft specifies GUE security capability to tunnel a network protocol/application over IP networks. This security capability also offers option feature to GUE applications such as Network virtualization overlay [GUE4NVO] for secured transport.

The draft allocates two flag bits from GUE undefined flag bits for Security purpose. Security field usage and key management, etc. is expected to be negotiated out of band between two tunnel end points.

2. Terminology

The terms defined in [RFC768] are used in this document.

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Generic UDP Encapsulation (GUE) for Secure Transport

GUE [GUE] defines a generic GUE header that applies any UDP tunnel application. GUE header contains some key fields that a UDP tunnel application needs. These key fields are version, control message indication (c), Header Length (HLen), and Protocol Type (or ctype). It also contains some undefined flags for a UDP tunnel application to specify.

This document proposes to allocate two flag bits from GUE undefined flags for GUE to provide secure transport to a tunneled protocol. This secure transport feature can apply to a GUE application when it is necessary. GUE format with Security Flag is shown in figure 1.

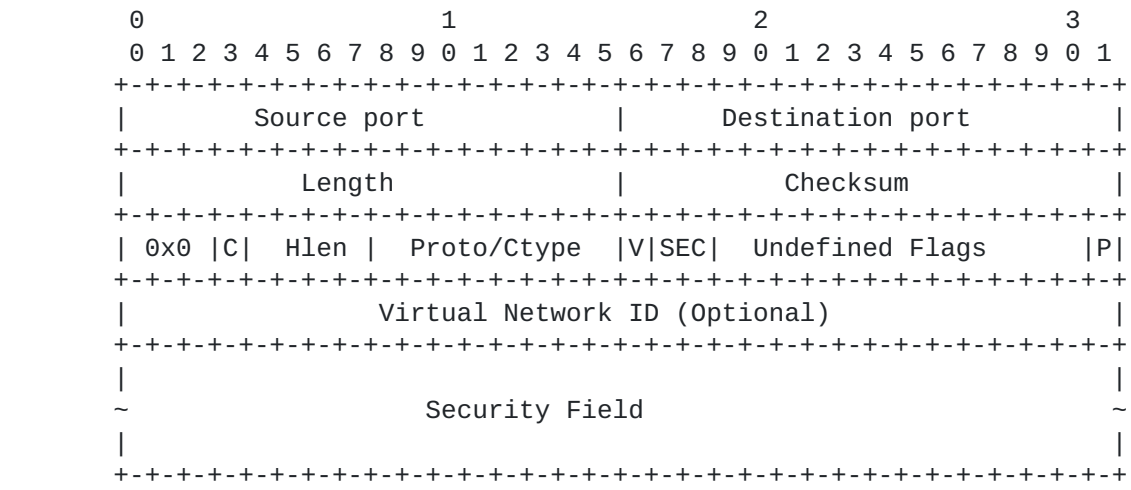


Figure 1 GUE Format with Security Flag

- 'V' Virtualization flag: This flag is designated for network virtualization overlay (NVO). When set, Security field appear after that; when clear, security field appear after GUE header. To tunnel a protocol for secure transport, this flag MUST be clear. NVO may utilize secure transport [GUE4NVO].

- 'SEC' Security flags: Indicates presence of security field. To provide security capability, the flags MUST be set. Different sizes are allowed to allow different methods and extensibility. The use of the security field is expected to be negotiated out of band between two communicating hosts. Potential uses of the security field are discussed in Security Considerations.

    - 00 - No security field
    - 01 - 64 bit security field
    - 10 - 128 bit security field
    - 11 - 256 bit security field

The usage of the key fields in the GUE header [GUE] for secure transport is described as below:

- Type: Set to 0x0 for secure transport.
- Control flag: When it set, control message presents and control processing MUST occur after security validation.
- Hlen: summary of optional fields (byte)/4
- Protocol: Contain the protocol of the encapsulated payload packet, i.e. next header. The next header begins at the offset provided by Hlen.
- CType: N/A
- 'P' Private flag. It is the last bit in the GUE header. For usage of private field see [GUE].

UDP header usage for secure transport: UDP dst port SHOULD be filled with GUE port [GUE]; UDP src port MAY be filled with entropy or a random value. The checksum and length implementation MUST be compliant with GUE implementation [GUE].

4. Encapsulation/Decapsualtion Operation

GUE secure transport applies to both IPv4 and IPv6 underlay networks.
The outer IP address MUST be tunnel egress IP address (dst) and tunnel ingress IP address (src). To tunnel a protocol for secure transport, tunnel ingress and egress MUST compliant GUE header process precedence specified in [GUE]. At tunnel egress, the payload processing MUST be done after security validation

For a GUE application, secure transport is an option feature. When it is used, the flag MUST be set and the security field is placed in the optional fields. The GUE application MUST specify use of this option.

See Section 5 for Security field encoding.

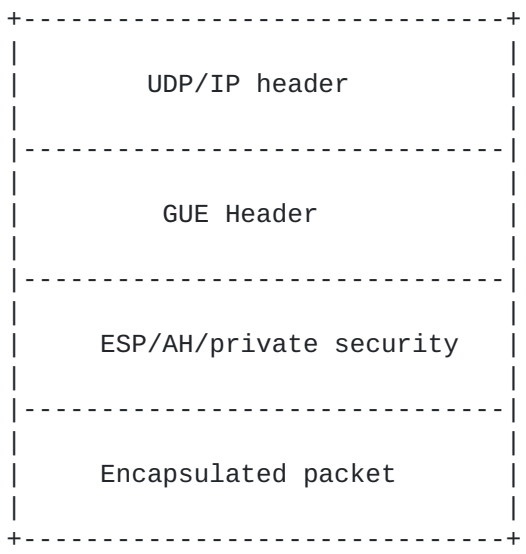
5. Security Considerations

Encapsulation of IP protocols within GUE should not increase security risk, nor provide additional security in itself. As suggested in section 3 the source port for of UDP packets in GUE should be randomly seeded to mitigate some possible denial service attacks.

GUE is most useful when it is in the outermost header of a packet which allows for flow hash calculation as well as making GUE data (such as virtual network identifier) visible to switches and middleboxes. GUE must be amenable to encapsulating (and being encapsulated) within IPsec. Also, we allow provisions to secure the GUE header itself without external protocol.

5.1. GUE and IPsec

GUE may be used to encapsulate IPsec packets. This allows the benefits of deriving a flow hash for the inner, potentially encrypted, packet. In this case the protocol stack may be:



Note that the security does not cover the GUE header (does not authenticate it for instance). The GUE security field may be used to provide authentication or integrity of the GUE header.

5.2. GUE security field use

The GUE security field should be used to provide integrity and authentication of the GUE header. Security negotiation (interpretation of security field, key management, etc.) is expected to be negotiated out of band between two communicating hosts. Two possible uses for this field are outlined below, a more precise specification is deferred to other documents.

5.2.1. Cookies

The security field may be used as a cookie. This would be similar to cookie mechanism described in L2TP [RFC3931], and the general properties should be the same. The cookie may be used to validate the encapsulation. The cookie is a shared value between an encapsulator and decapsulator which should be chosen randomly and may be changed periodically. Different cookies may used for logical flows between the encapsulator and decapsulator, for instance packets sent with different VNIs in network virtualization might have different cookies.

5.2.2. Secure hash

Strong authentication of the GUE header can be provided using a secure hash. This may follow the model of the TCP authentication option [RFC5925]. In this case the security field holds a message digest for the GUE header (e.g. 16 bytes from MD5). The digest might be done over static fields in IP and UDP headers per negotiation (addresses, ports, and protocols). In order to provide enough entropy, a random salt value in each packet might be added, for instance the security field could be a 256 bit value which contains 128 bits of salt value, and a 128 bit digest value. The use of secure hashes requires shared keys which are presumably negotiated and rotated as needed out of band.

6. IANA Considerations

The document does not require any IANA action.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC2119, March 1997.

[RFC3931] Lau, J., Townsley, W., et al, "Layer Tow Tunneling Protocol - Version 3 (L2TPv3)", RFC3931, 1999

[RFC4301] Kent, S., Seo, K., "Security Architecture for the Internet Protocol", RFC4301, December 2005

[RFC5925] Touch, J., et al, " The TCP Authentication Option", RFC5925, June 2010

[GUE] Herbert, T., and Yong, L., "Generic UNP Encapsulation", draft-herbert-gue-01, work in progress.

7.2. Informative References

[GUE4NVO] Yong, L., and Herbert T., "Generic UNP Encapsulation for NVO", draft-hy-nov3-gue-4-nvo-00, work in progress.

8. Authors' Addresses

Lucy Yong
Huawei USA
5340 Legacy Dr.
Plano, TX 75024
US

Email: lucy.yong@huawei.com

Tom Herbert
Google
1600 Amphitheatre Parkway
Mountain View, CA
US

Email: therbert@google.com