Ethernet-Traffic Flow Security

Don Fedyk, LabN Consulting LLC

This paper introduces the high-level problem statement, requirements and proposed solution for Ethernet - Traffic Flow Security (E-TFS) for MACsec IEEE 802.1AE [1]. The goal of this paper is to initiate work to standardize E-TFS for interoperable implementations. Ethernet - Traffic Flow Security is the term for the complete security – data confidentiality, frame data integrity, data origin authenticity offered by MACsec with the addition of traffic flow confidentiality mechanisms described in this a paper.

1 Problem Statement

In recent years concern for Privacy in networking has increased. IEEE has standardized encryption of user data in Ethernet Frames and while this protects explicit information in the Ethernet Payload Data Units from external snooping it leaves unprotected information implicit in the communication. It is well known that some personally identifiable information can still be derived from a MACsec packet flow. Within MACsec deployments today, user identity may be exposed in packets or frames where the ultimate or end user source and destination is not hidden. Substantial additional information regarding the content and purpose of the communication can be obtained from analysis of the sizes and time intervals of the frames, particularly where the behavior of the traffic follows known patterns – for example see Shuster et al [2]. Privacy exposures have also been documented in IEEE 802.1 in several places. The white paper Privacy considerations in bridged networks [4] provides an overview, and section Y.5 highlights privacy exposure that is applicable here. This paper proposes a method of hiding end user addresses and provides mechanisms for obscuring observable traffic flow characteristics which can correlate to user identity, content or applications.

This problem is not unique to Ethernet, for example in the Internet Engineering Task Force (IETF) in the Internet Protocol Security (IPsec) group the document IP Encapsulating Security Payload (ESP) [5] describes the problem for IPSec as "The traffic flow confidentiality (TFC) service generally is effective only if ESP is employed in a fashion that conceals the ultimate source and destination addresses of correspondents, e.g., in tunnel mode between security gateways, and only if sufficient traffic flows between IPsec peers (either naturally or as a result of generation of masking traffic) to conceal the characteristics of specific, individual subscriber traffic flows." In other words, the solution in IPsec is to use tunnel mode and anonymizing the packets as much as possible. A parallel activity is being started in the IETF titled IP Traffic Flow Security [6] to improve confidentiality in IPsec.

2 High Level Requirements:

- The solution must not limit EDE/802.1AE functionality, notably mapping of VLANs and priorities and support for multiple SecYs, e.g., EDE-CCs.
- Red-side addresses must not be exposed on the black-side network port.
- The solution must not significantly impact network bandwidth availability or network latency.
- The solution should allow for different implementation/deployment choices related to a specific deployment, including fixed frame size and/or transmission data rate.
- Solution should minimize required configuration, in particular, the receiver configuration.

3 Solution Framework

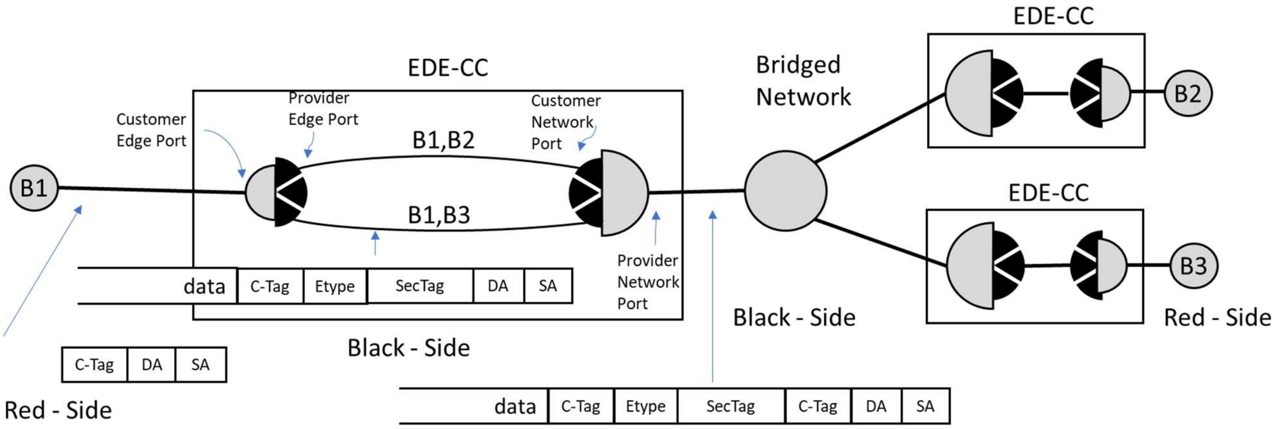

Figure 1 Existing MACsec between Ethernet Encryption devices

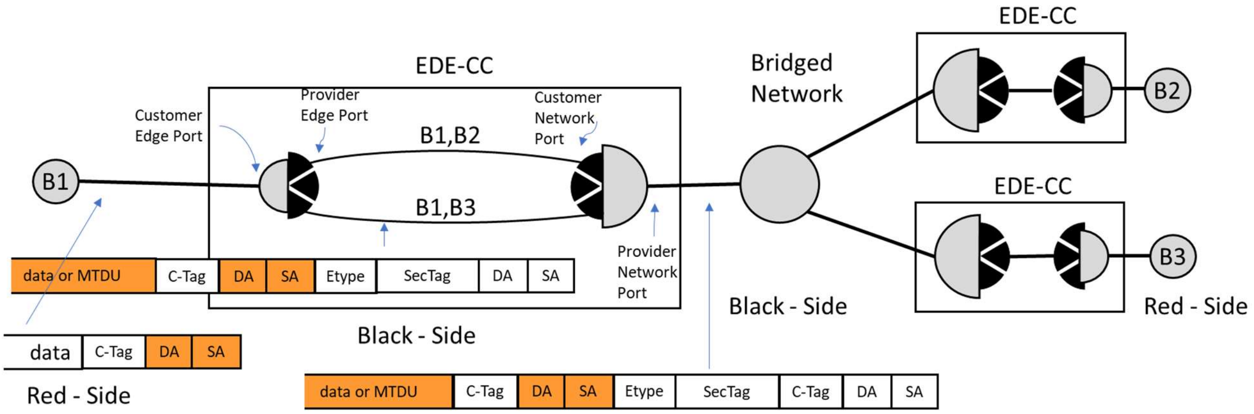

Figure 2 Example Tunnels between Ethernet Encryption devices with E-TFS

E-TFS proposes to use tunneling and frame encoding to enhance MACsec by introducing Ethernet Traffic Tunnels (ETTs) that encapsulate Red network addresses (user address or end point addresses) in the secure data of MACsec. ETTs therefore encapsulate MAC addresses of user frames in a tunnel supporting a fixed priority. Further, ETTs propose an internal frame format to supports both variable and fixed size frames allowing multiple user frames to be aggregated or fragmented within an ETT in order to minimize impact on available user bandwidth.

E-TFS is proposed in this paper in the context of Ethernet Data Encryption (EDE) devices, as defined in IEEE P802.1AE-2018 [1] but, in principle, E-TFS could be used with non-EDE implementations of MACsec. Figure 1 illustrates a typical placement of EDEs with the red network and the black network. ETTs provide traffic flow security between Ethernet stations. In this proposal, ETTs operate over MACsec in order to secure the contents of any communication, and ETTs typical deployment is within EDEs.

As pointed out simply hiding end point addresses by itself is not enough to provide traffic flow confidentiality or prevent traffic analysis by an external observer in the black network. Additional mechanisms that obscure frame sizes and frame transmission timing are also desired. The tradeoff for anonymizing the data is loss of some black-side network bandwidth where the tunnels are used.

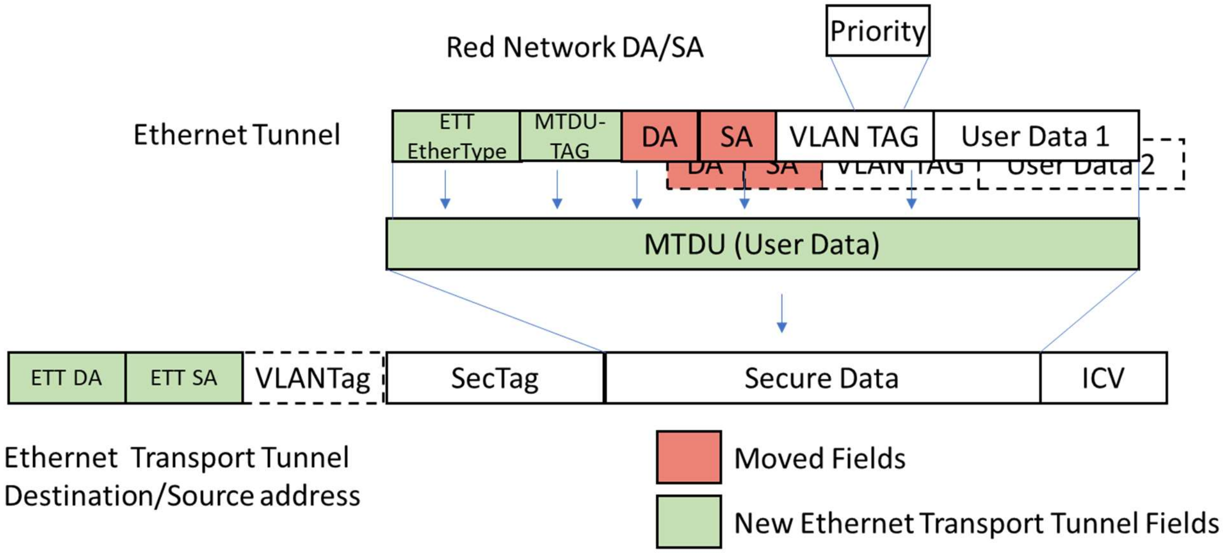

Figure 3: Proposed Ethernet Traffic Tunnel Functional Diagram

Figure *3* illustrates the proposed functional diagram with a new Ethernet type (to be assigned by this work) defines a service interface for E-TFS. A proposed format for an internal data structure (Figure 4) that allows one or more user frames to be concatenated in a single tunnel frame. The user MAC addresses are moved into the secure data area and the MACsec service uses a Source and Destination MAC address for the tunnel. This MAC Tunnel Data Unit (MTDU) enables both fixed sized or variable sized tunnel frames. This format is also intended to allow the existing MACsec format to coexist with ETT frames in a MACsec service. The MTDU allows fragmenting, aggregating or padding of the original Ethernet frames to be carried in the ETT, resulting in fixed size frames. The flexibility of this arrangement allows the fixed size frame rate to be adjusted to meet the user and network needs. This offers EDEs varying levels of privacy by trading off tunnel and network efficiency for better privacy.

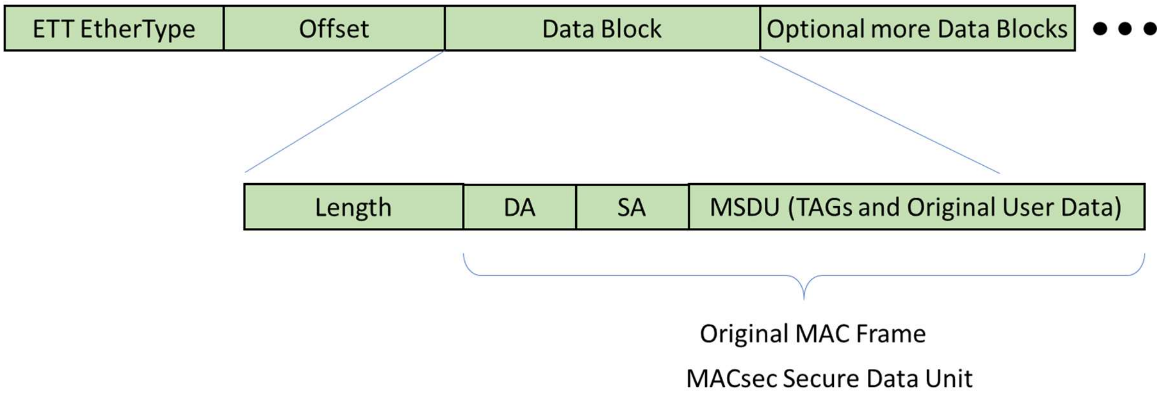

Figure 4 Proposed Logical format of MAC Tunnel Data Unit (MTDU)

The MTDU consists of an EtherType Identifying an ETT tunnel. The offset field is used to indicate the continuation of a fragmented frame. When there is no previous frame fragmentation the offset field is zero. Each data block in the frame has a length of frame for that MACsec Secure data unit (MSDU). In the case of a fixed size ETT frame additional data blocks or padding will complete the frame. The entire MTDU is encrypted.

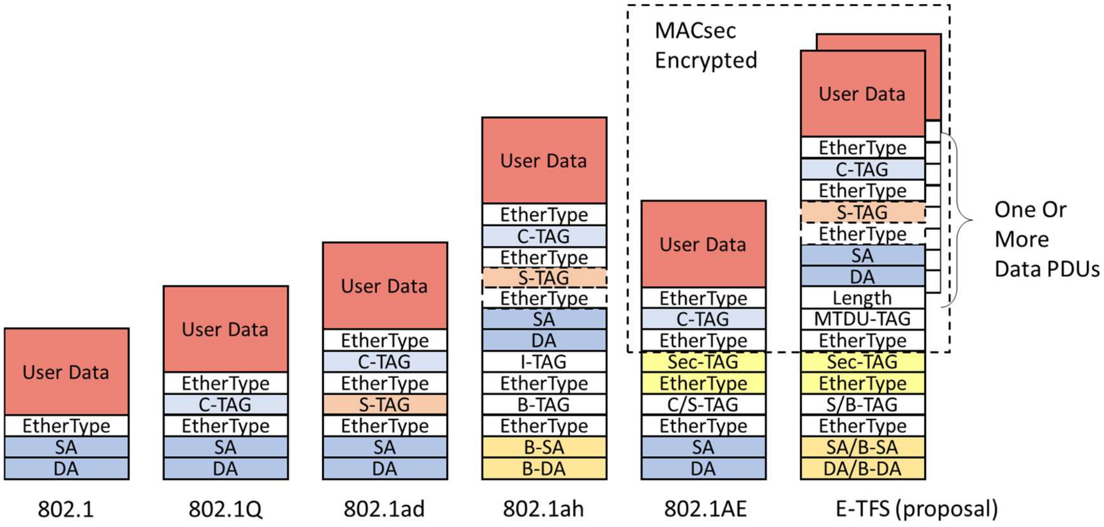

Figure 5 Summary of Ethernet Headers

Are we blending Provider Backbone Bridging (PBB) defined in [7] with MACsec? Figure 5 illustrates the various 802.1 frame headers. When MACsec is applied all data behind (logically above) the MACsec tag is cryptographically protected. What we propose looks like a mix of MACsec 802.1AE and PBB minus the I-SID in the I-TAG. The proposed new MTDU TAG is similar in concept the I-TAG in that MAC addresses are carried. In PBB the B-Component and the I-Component were logically and sometimes physically separated. However, the functions occurring on an EDE device in the network don't need to be exposed. In E-TFS we envision the whole operation of building a subframe and encrypting occurring much as it does today in MACsec EDEs.

4 Detailed Solution Requirements

ETTs are proposed to support both fixed and variable size tunnel frames each providing different tradeoffs in efficiency, delay and traffic flow confidentiality.

Variable sized frames are very similar to current EDE behavior, except that received source and destination MAC addresses are encapsulated.

Fixed sized frames utilize aggregation, fragmentation and padding of ethernet frames as needed to ensure that all transmitted frames are the same size. In addition to this, frames can be provided at a fixed rate (and thus at a fixed interval). This supports a higher degree of traffic flow confidentiality.

4.1 Core Requirements

1. An E-TFS solution shall ensure that source and destination MAC addressing information received on a user (red) port are not directly exposed on a SecY (black side network port).

2. An E-TFS solution should support the selection of a transmit SecY (an internal port) based on user (red side) destination MAC address, frame priority or VID or a combination of those fields. Note: one or more MAC addresses or VIDs may be mapped to a single SecY.

3. An E-TFS solution shall use a single priority for all transmitted frames transmitted for a particular ETT.

4. An E-TFS solution shall use a single VID for all transmitted frames transmitted for a particular ETT.

5. An E-TFS solution shall use the same destination address used for all frames sent to a particular ETT. This address can be Unicast or Multicast.

6. An E-TFS solution shall use a common ETT data unit format for all frames and receive processing for any properly decrypted ETT frame should be independent of the frame being fixed or variable.

4.2 Requirements – Variable sized frames

E-TFS using variable sized frames provides addressing hiding by encryption. (As described above, address hiding is a byproduct of using ETTs.) The requirements in this section apply to any E-TFS frame.

7. An E-TFS solution shall generate an ETT frame for every received user (red side) frame that matches an ETT configured in the mode proposed in this section.

4.3 Requirements –Fixed sized frames

E-TFS supports fixed frame sizes by using aggregation, fragmentation and padding. The requirements in this section apply to any E-TFS implementation that uses these mechanisms to achieve a fixed size frame and all requirements should be interpreted with this caveat.

8. An E-TFS solution shall recover from the loss of ETT frames losing the minimal amount of users' frames.

9. An E-TFS solution shall process ETT frames received out of order. The maximum number of frames that may be processed out of order is an implementation decision.

10. An E-TFS solution shall generate a fixed size ETT frame for received user (red side) based on configuration.

11. An E-TFS solution shall support aggregation and fragmentation/reassembly to provide a bandwidth efficient fixed size ETT frame format.

12. An E-TFS solution shall allow the use of a configured maximum latency a user frame may experience, during fixed generation frame processing, before being transmitted OR shall allow the configuration of fixed sized ETT frames at a fixed ETT-specific transmission rate based on per-ETT configuration information.

5 References

[1] IEEE Std 802.1AE-2018, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

[2] R. Schuster, V. Shmatikov, and E. Tromer, "Beauty and the Burst: Remote Identification of Encrypted Video Streams" 26th USENIX Security Symposium, August 16–18, 2017, Vancouver, BC, Canada

[3] https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-schuster.pdf. in Proceedings of 26th USENIX Security Symposium 2017

[4] Mick Seaman, Privacy considerations in bridged networks, White Paper http://www.ieee802.org/1/files/public/docs2018/e-seaman-privacy-in-bridged-networks-1018-v01.pdf

[5] Stephen Kent, "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[6] Chris Hopps, "IP Traffic Flow Security", draft-chopps-ipsecme-iptfs-00, Feb 2019.

[7] IEEE Std 802.1Q-2014, IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks.

Appendix A. Abbreviations and Acronyms

Abbreviation / Acronyms	Definition
C-TAG	Customer VLAN tag
EDE	Ethernet Data Encryption device
EDE-CC	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of C-TAGs
EDE-CS	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of S-TAGs
EDE-M	VLAN-unaware Ethernet Data Encryption device operating as a Customer Bridge
EDE-SS	Ethernet Data Encryption device with red-side recognition of S-TAGs and black-side addition and removal of S-TAGs
E-TFS	Ethernet Traffic Flow Security
ETT	Ethernet Traffic Tunnel
I-SID	Backbone Service Instance
I-TAG	Backbone Service Instance tag
IETF	Internet Engineering Task Force
LAN	IEEE 802 Local Area Network
MAC	Media Access Control
MSDU	MACsec Secure Data Unit
MTDU	MAC Tunnel Data Unit
MTDU-TAG	MAC Tunnel Data Unit TAG (Proposed New TAG).
PBB	Provider Backbone Bridge
SecY	MAC Security Entity
S-TAG	Service VLAN tag
VLAN	Virtual Local Area Network
VID	VLAN Identifier