March 2022

TRUSTWORTHY ENABLER FOR EOGRE, GRE AND EOIP PROTOCOLS USED ACROSS HETEROGENOUS TECHNOLOGIES

NIRANJAN M M

TRUSTWORTHY ENABLER FOR EOGRE, GRE AND EOIP PROTOCOLS USED ACROSS HETEROGENOUS TECHNOLOGIES

AUTHOR:
NIRANJAN M M

ABSTRACT

The EoGRE tunnelling protocol is used as an aggregation method for aggregating data flows of different users with similar service requirements in the same tunnel. EoGRE tunnels are used in the SP Wi-Fi deployments and 5G deployments. In 5G deployments, especially in the context of network slicing, EoGRE is used between CPE and Tunnel Gateway (TGW) to reduce the signalling traffic. In Wi-Fi deployments, Wireless LAN Controllers (WLCs) or Access Points (APs) establishes the EoGRE tunnel with the Tunnel Gateway (TGW). Tunnel end points TGW and CPE of EoGRE need to know whether the peer device is trustworthy or not before sending data over tunnel. If any one of the devices is compromised i.e., it is no longer a trusted entity, which could create harm to the network (in-turn to the user data traffic) by allowing "malicious CPE to connect to the valid TGW" or "valid CPE connecting to malicious TGW". Currently EoGRE does not include any capabilities to exchange trust and integrity measurement information between TGW and CPE to prove the peer was not tampered. The techniques presented herein applies exchanging trust and integrity measurement information between TGW and CPE in EoGRE messages to provide Proof of Integrity and trust to the EoGRE tunnel. This holds good even for GRE and EoIP protocols. Additionally, this method applicable for other tunnelling protocols such as PPTP, PPPoE and L2TP as well.

DETAILED DESCRIPTION

The EoGRE tunnelling protocol is used as an aggregation method for aggregating data flows of different users with similar service requirements in the same tunnel. In this method, Customer Premises Equipment's (CPEs) bridges the ethernet traffic coming from an end host/client and encapsulate the traffic in EoGRE tunnel. When the EoGRE tunnels are terminated on a service provider broadband network gateway, the traffic from end host/client is also terminated and subscriber sessions are initiated for the end host/client. EoGRE tunnels are used in the SP Wi-Fi deployments, 5G deployments etc., In 5G deployments, especially in the context of network slicing, EoGRE is used between CPE and Tunnel Gateway (TGW) to reduce the signalling traffic. In Wi-Fi deployments, Wireless LAN Controllers (WLCs) or Access Points (APs) establishes the EoGRE tunnel with the Tunnel Gateway (TGW). WLC/AP aggregates the Wi-Fi traffic from wireless clients (hotspots) and send it to the TGW. AP/WLC acts as Customer Premises Equipment (CPE) used in 5G/4G deployments.

In general, EoGRE, GRE and EoIP are used as tunnelling protocol for sending ethernet packet over the tunnels to send/receive data over heterogeneous technologies. For simplicity, let us consider EoGRE tunnel and same is applicable to GRE and EoIP tunnels. Consider EoGRE tunnel endpoints as below:

- TGW (Tunnel Gateway) from the broadband service provider device at the EPC (Evolved Packet Core). This could be PGW (Packet Data Network Gateway) as well.
- Customer Premises Equipment (CPE) from the access network. It would be WLC or AP or Base Station (BS).

With this background, tunnel end points TGW and CPE of EoGRE need to know whether the peer device is trustworthy or not before sending data over tunnel. If any one of the

devices is compromised i.e., it is no longer a trusted entity, which could create harm to the network (in-turn to the user data traffic) by allowing "malicious CPE to connect to the valid TGW" or "valid CPE connecting to malicious TGW". Currently EoGRE does not include any capabilities to exchange trust and integrity measurement information between TGW and CPE to prove the peer was not tampered.

There are techniques based on TCG guidance for Securing Network Equipment's (https://trustedcomputinggroup.org/tcg-guidance-securing-network-equipment/) to provide trustworthiness to the platforms/devices and protocols. But there are no methods to provide trustworthiness to EoGRE protocols used for packet data over heterogeneous devices across 5G/4G/3G/Wi-Fi technologies.

Hence, we need to have trustworthiness to EoGRE tunnelling protocol used between TGW and CPE by having trust and integrity measurement information in the tunnelled packets. These tunnels would be based on per-user-group or per-service, per policy etc., as per the requirement. As these are not pre-established tunnels unlike IPSec, TLS etc., we need to send trust and integrity measurement information in the initial packets exchanged between the peers, subsequently exchange the current integrity measurements upon timeout.

The techniques presented herein applies exchanging trust and integrity measurement information between TGW and CPE in EoGRE messages to provide Proof of Integrity and trust to the EoGRE tunnel.

A. Trust, Identity, and Integrity Measurements:

The trust and integrity measurements are of different types:

1. SUDI (Secure Unique Device Identifier): SUDI is programmed into the device's TAM chip (which also provides TPM functionality, stores PCR values, AIK support etc.,) during the manufacturing process. TAM chip is embedded in hardware and hence tamper-proof.

   SUDI consists of three components:

   - An IEEE 802.1AR-compliant X.509v3 certificate which contains the platform's unique Product ID (PID) and Serial Number (SN) pair, and the public portion of a unique RSA or ECC key-pair.
   - The private portion of the key-pair associated with the X.509v3 certificate.
   - The chain of certificates of the SUDI signing Certificate Authorities.

   SUDI provides hardware fingerprint and uniquely mapped to the PID and SN to provide platform identity and trust.
2. PCR (Platform Configuration Register) values: The devices would be having TAM (Trusted Anchor Module) chip (e.g., ACT2), where it maintains PCRs which stores the integrity measurements of the device.

   Integrity measurements would be of signature or hash of the BIOS/micro loader, bootloader, OS etc.,

   The PCR value is calculated as below ("integrity" of "integrity measurement values" of each stage in the device boot-up):

   PCRnew value = hash [PCRexisting value || hash (new measurement)] [Note: PCR values are with SHA256 of 256 bits]

   TCG has defined two operations of retrieving the integrity of the measurements: "PCR Read" and "PCR Quote". "PCR Read" returns the content of the PCR (running hash value that was computed across some number of logged integrity measurements). "PCR Quote" returns the signed content [signed by Attestation Identity Key (AIK), by the TPM] along with signed nonce provided by the requester to protect against replay

attacks. "PCR Quote" provides trust and Integrity of the system (starting from boot, including BIOS/micro loader, bootloader, OS etc.,).

3. Known Good Values (KGV): The KGV is gathered by the manufacturer as part of the software build and regression process. The signed KGV will be published and maintained by the manufacturer in a well-known location. This is used against the measurement information received by the peer device (aka tunnel endpoint).
   KGV provides integrity of the software running, applications, libraries, config/manifest files etc.,

B. Proof of Integrity, Freshness of Proof of Integrity, and Proof of Trust:
EoGRE packets between the peers (i.e., TGW and CPE) are extended with extensions that carry Proof of Integrity, Freshness of proof of Integrity, Proof of Trust with the intent to validate Proof of Integrity and trust.

1. Proof of Integrity:
   TPM functionality is used as root of trust and as proof of Integrity of EoGRE tunnel.
   Both EoGRE end points gather below integrity measurements from the peer device:
   - Hardware Fingerprint - Derived from SUDI or similar
   - Software - micro loader, BIOS, boot load, kernel, operating system (PCR values)
   - Runtime - application binaries, libraries, config/manifest files (KGV)
     These measurements are verified against the device fingerprint (e.g., imprinted in the device identity certificate issued by the manufacturer - SUDI). The result of verification determines the decision to allow EoGRE tunnelled packets between the peers.
2. Freshness of Proof of Integrity:
   Along with Proof of Integrity, Freshness of the Proof of Integrity can also be considered.
   Proof of Integrity can also be accompanied with a signature to prove freshness of the Proof of Integrity i.e., by adding a signature over random data "nonce" presented by the peer. This would help is detecting the replay of old evidence via a "nonce". A "nonce" is a random number provided by the entity making the request. This "nonce" is passed into the TPM/vTPM. Results coming out of the TPM/vTPM include a signature based on the "nonce". The result is the output from the TPM/vTPM which could not have been generated before that "nonce" was provided.
   Example:
   Message from CPE contains random data "nonce"; it is extended to carry intention to validate Proof of Integrity. The subsequent message from TGW to CPE carries an extension to its Proof of Integrity along with a signature (signed by the TPM) over random data "nonce" received earlier from the CPE. Same is applicable in the other direction i.e., from TGW to CPE.
3. Proof of Trust:
   SUDI provides hardware fingerprint and uniquely mapped to the PID and SN to provide platform identity and proof of trust.

C. Message Extensions:
For EoGRE and GRE: This can be achieved by extending GRE (https://tools.ietf.org/html/rfc2784) with a new extension and by adding these trust and integrity measurement information in explicit messages as defined in GRE extensions https://tools.ietf.org/html/rfc2890

For EoIP: EoIP (httpsn://tools.ietf.org/html/rfc3378) can also be extended with a new extension and by adding these trust and integrity measurement information as defined in https://tools.ietf.org/html/rfc3378.

The techniques presented herein adds trust and integrity measurement information to the EoGRE packets as an extension that embeds:

- hardware fingerprint (derived from SUDI or similar) (Platform identity and Trust)
- PCR values (Platform Integrity and Trust)
- KGV (Software Integrity)

TGW and CPE will use this information against the device fingerprint, to verify whether the peer is trustworthy or not.
Depending on the outcome of the verification, the TGW and CPE can decide, whether connectivity to the remote device should be considered or not. That is, if the verification is successful, then only EoGRE tunnelled packets are accepted/processed. CPE can use level of trustworthiness to decide which TGW (if more than one TGW is configured/available) to connect using integrity and trust-based selection criteria (want more secure/trust, least loaded TGW etc., based on configuration/requirement).

In short, trust and integrity measurement information would include hardware fingerprint which is derived from SUDI certificate stored securely in TAM/ACT2 chip, software information (aka KGV) and platform information (aka PCR values). TGW and CPE will use this information to verify the peer is trustworthy or not before processing EoGRE tunnelled packets.

The techniques presented herein provides trustworthiness to EoGRE tunnelling protocol used for packet data transfer across 5G/4G/3G/Wi-Fi technologies. Moreover, this method holds good for GRE and EoIP protocols. Additionally, this method applicable for other tunnelling protocols such as PPTP, PPPoE and L2TP.

Appendix

The main service of mobile networks is to transport user data packets between the user devices and external packet data networks. This is done by using transport tunnels, based on the GPRS Tunnelling Protocol User Plane (GTP-U) or the Generic Routing Encapsulation (GRE) protocol. These user plane tunnels are denoted as "thin pipes" as they carry only the data of a single user data flow. The tunnels must be setup each time when a UE enters the active mode or starts a session with new service requirements. This is very inefficient especially when a UE transmits small amounts of data only sporadically which is the case e.g., for Machine Type Communication.

In contrast to these thin pipes, "fat pipes" using Ethernet over GRE (EoGRE) tunnelling can carry the data flows of different users with similar service requirements in the same tunnel. The advantage is that with "fat pipes", the amount of control signalling is strongly reduced because the setup and maintenance of user specific tunnels (thin pipes) is avoided. As a second advantage, the Ethernet layer natively supports the transport of IP-as well as of non-IP data.

Tunnelling helps in multiple ways:

- Clients can maintain IP address and policy across heterogeneous access networks with different technologies and/or vendors.
- Bypasses MAC address scaling limitation of the L2 switch connecting to the WLC.
- Lawful Intercept (LI).
- Reduces network congestion by reducing OpEx and increasing network efficiency by offloading 5G/4G/3G traffic.

- Provides access to 5G/4G/3G core in spite of a lack of weak cell signal, leading to subscriber retention.
- Lowers CapEx on per user basis or bandwidth basis in dense metro environments.
- Provides Wi-Fi security and subscriber control.
- Delivers scalable, manageable, and secure wireless connectivity.
- Enables new revenue-sharing business models.
- Delivers a Wi-Fi platform that offers new location-based services.
- Provides enhanced quality of experience to the subscribers on Wi-Fi networks.
- Provides unified billing across access networks.
- Provides mobility across radio access technologies-5G or 4G or 3G to Wi-Fi and Wi-Fi to Wi-Fi.
- Provides multiple options within the Wi-Fi platform, thereby enabling location-based services.