Technical Disclosure Commons

Defensive Publications Series

July 03, 2019

VEHICLE-TO-EVERYTHING THREAT PROTECTION USING SECURITY INTELLIGENCE ENGINE AND MULTI-ACCESS EDGE COMPUTING

Manish Jhanji

Satish Kumar Mandavilly

Rakesh Mishra

Amitesh Shukla

VEHICLE-TO-EVERYTHING THREAT PROTECTION USING SECURITY INTELLIGENCE ENGINE AND MULTI-ACCESS EDGE COMPUTING

AUTHORS:
Manish Jhanji
Satish Kumar Mandavilly
Rakesh Mishra
Amitesh Shukla

ABSTRACT

Techniques are described herein for a threat protection mechanism for Vehicle-to-Everything (V2X) communication channels. This includes shared intelligence at the Multi-access Edge Computing (MEC) function, Security Intelligence Engine (SIE), Original Equipment Manufacturer (OEM) vendors, application providers, and external device vendors. It is capable of securing Vehicle User Entities (V-UEs) simultaneously in real time.

DETAILED DESCRIPTION

One of the key requirements of 5G infrastructure for Vehicle-to-Everything (V2X) communication is threat protection. The International Mobile Subscriber Identity (IMSI) of a Vehicle User Entity (V-UE) only provides network authentication but does not protect data from an external threat. Thus, V2X communication can be vulnerable to attacks.

Accordingly, techniques are described herein for a Multi-access Edge Computing (MEC) based solution to protect vehicle data from threats and secure V2X communication. The solution maintains a database of threat related information (e.g., threat signatures) and synchronizes the policy information during vehicle on-boarding and other critical events. The solution may adapt to new threats and take appropriate actions based on 3rd Generation Partnership Project (3GPP) standards, for example.

Some of the critical vehicle data/commands which need to be protected include the vehicle On Board Diagnostic (OBD), infotainment Link Interconnect Network (LIN) information, Engine Control Unit (ECU) firmware upgrades, powertrain/battery information, body electronic module, vehicle telemetry (e.g., location), Diagnostic Trouble Codes (DTCs), V2X metadata, etc.

As per 3GPP standards, a V-UE may support eight different slices with a common Access Mobility Function (AMF) for all the slices and a Session Management Function (SMF) per slice. The network slice(s) use Ultra-Reliable Low Latency Communication (URLLC) application(s) for V2X communication. The User Plane Function (UPF) is connected to the Mobile Edge Host (MEH).

Figure 1 below illustrates an example solution for V2X threat protection.

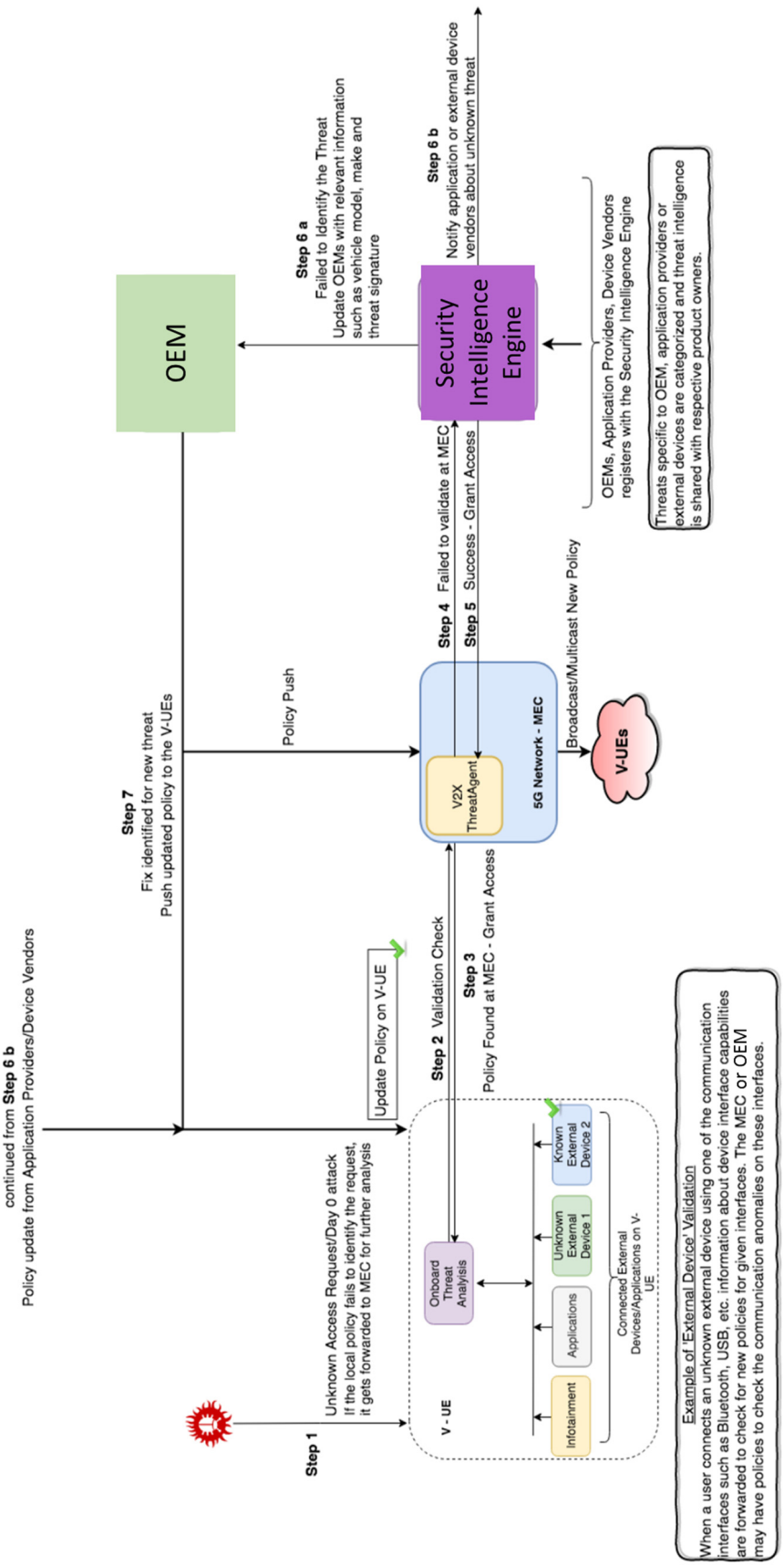

Figure 1

The Security Intelligence Engine (SIE) handles unknown requests from the MEC function and provides an interface for the OEMs / application providers / device vendors for registration and policy enforcement. This module also forwards unknown events that could not be resolved by the V-UE, MEC function, or SIE to respective vendors for further analysis and policy generation. It also classifies the threat based on applications, external devices, or OEMs, and identifies the owner of the entity under threat and shares the threat signature with the respective vendors.

The MEC function deploys a V2X threat agent that handles requests from the V-UE, forwards the request to the SIE (if the SIE previously failed to identify the threat), and broadcasts/multicasts any new policy identified by OEM/vendors.

The Onboard Threat Analysis module performs local decision/policy enforcement and handles updates from the MEC function.

Figures 2a and 2b below collectively illustrate an example Message Sequence Chart (MSC) between the V-UE and the 5G network. The message represented by the dark green arrows are new to V2X communications.

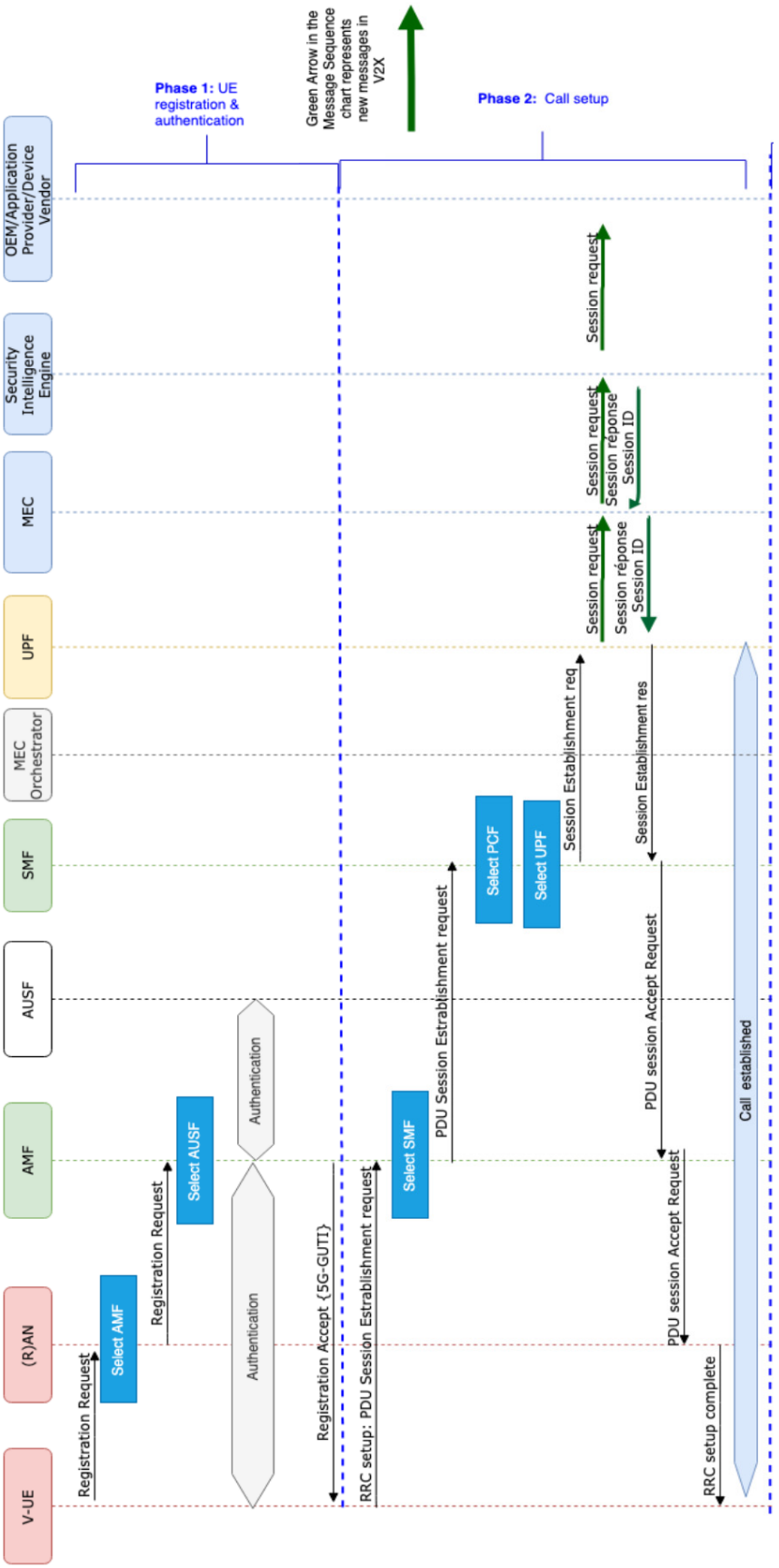

Figure 2a

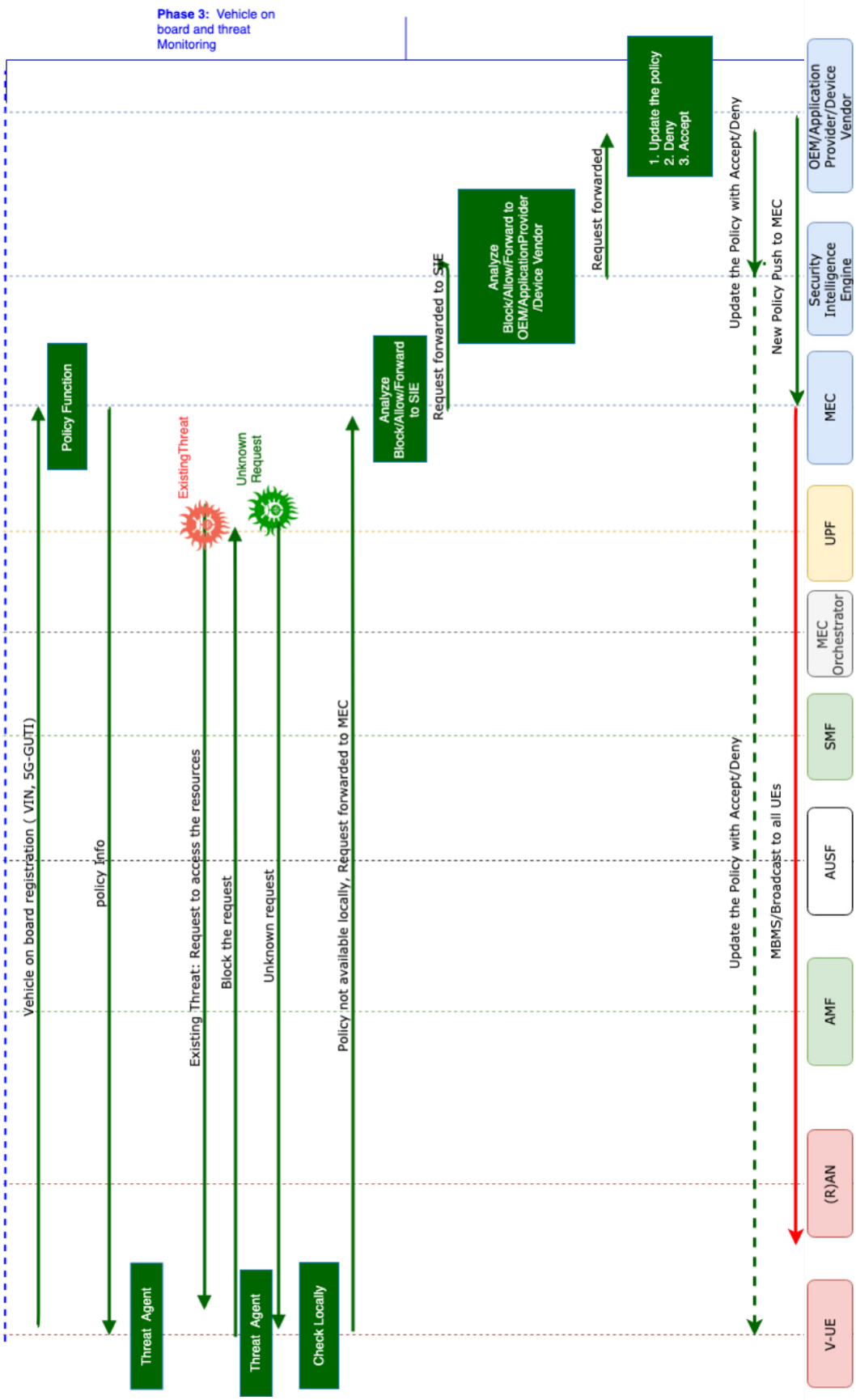
Phase 3: Vehicle on board and threat Monitoring
Vehicle on board registration (VIN, 5G-GUTI)
policy info
Existing Threat: Request to access the resources
Block the request
Unknown request
Policy not available locally, Request forwarded to MEC
Update the Policy with Accept/Deny
MBMS/Broadcast to all UEs
Update the Policy with Accept/Deny
New Policy Push to MEC
Request forwarded to SIE
Request forwarded
Policy Function
ExistingThreat
Unknown Request
Analyze Block/Allow/Forward to SIE
Analyze Block/Allow/Forward to OEM/ApplicationProvider /Device Vendor
1. Update the policy
2. Deny
3. Accept
Threat Agent
Threat Agent
Check Locally
V-UE
(R)AN
AMF
AUSF
SMF
MEC Orchestrator
UPF
MEC
Security Intelligence Engine
OEM/Application Provider/Device Vendor

Figure 2b

The MSC has three phases with respect to the V-UE and 5G communications. The first phase involves V-UE registration and authentication. In this phase, the V-UE registers its presence in the 5G network and obtains a Globally Unique Temporary Identifier (GUTI) number.

The second phase involves call setup. In this phase, the V-UE initiates the call as per 5G standards. During call establishment, the MEC function sends a session request to the SIE. The SIE may create a V-UE contest and send the response with a session identifier.

The third phase involves vehicle onboarding and threat monitoring. In this phase, the V-UE sends its Vehicle Identification Number (VIN), RAN_ID, RAN_TYPE and GUTI to the MEC function. Based on the VIN, the MEC function identifies the vehicle type, model, and year, and sends the appropriate policy information to the V-UE.

When there is an unauthorized/unknown request to access a vehicle resource, the following sequence of events may occur. Initially, the OEM/application providers/device vendors register with the SIE and push all known policies. Next, the V-UE obtains the request and checks the request locally based on the policy information. If the V-UE fails to identify the request, it sends a validation message to the MEC function to validate the request.

The MEC function obtains the request from the V-UE and checks the corresponding policy. The MEC function responds to the UE with a grant indicating whether the request is accepted or denied. If the corresponding policy is not present on the MEC function, it sends a request to the SIE controller to validate the request.

The SIE validates the request locally and sends the response back to the MEC function. If the SIE controller fails to identify the threat, it sends the notification to the OEM, application provider, or device vendor with the threat signature and additional information about the V-UE. Once the threat message from the SIE controller is received, the OEM/application provider/device vendor analyzes the request and takes appropriate action. For example, it may decide to accept/deny the request or push a new policy to the MEC function / V-UE or broadcast to all corresponding V-UEs.

Figure 3 below illustrates a high-level handover scenario between a 5G network, other networks, and out of network coverage areas. This diagram represents an aerial view of V2X handover.

Figure 3

The following sequence of events is for an autonomous car (V-UE) moving from location 1 to location 5. Initially, the car starts from location 1, and has access to a 5G network. If the car is powered on for the first time, the car registers its presence in the network. The car then obtains the threat policy from the MEC function.

If the car proceeds to location 2, V-UE handoff from 5G to 4G occurs in accordance with standard handoff processes. Since the car has moved to a new RAN, the V-UE may repeat the three phases as discussed above in connection with Figure 2. At the first phase, it sends its VIN, Temporary IMSI (T-IMSI), new RAN_TYPE (4G), RAN_ID, and Primary Cell Identifier (PCI). At the third phase, the V-UE obtains the new policy.

When the car moves to location 3, the car is out of the network coverage area. Based on the existing policy, the UE continuously monitors events occurring in the system. It rejects the request if the UE identifies the request as a threat. The car maintains an audit log for all allowed and denied events.

When the car reaches location 4 (a new RAN 3G network), it pushes the audit log events to the MEC function after repeating the three phases. The MEC function evaluates

all the events and based on the new threat intelligence may push modified policies to all registered vehicles of same make/model.

Some example of policies which may be pushed by the OEM / device vendors include:

mec_policy_1 = {**Event**:Firmware_upgrade: **Condition**: RPM = 0 **and** Authorized Wi-Fi AP: {**Action**: Grant_Access} Else {**Action**: Access_Denied}; Notify_User, Audit_Event_log, etc.}

mec_policy_2 = {**Event**:Web_Browser_Access_CAN_BUS: **Condition**: Any_Source : {**Action**: Access_Denied}; Notify_User, Audit_Event_log, etc.}

...etc.

At the MEC level, security policies of newly identified threats are automatically pushed across vendors. The MEC function has an intelligence to broadcast/multicast to all affected V-UEs. The SIE has the intelligence to redirect the threat signature to respective vendors. Infotainment/external peripheral vendors may enforce in real time the security polices which are pushed as the V-UE hands over across MEC functions. Policies may be pushed based on the capabilities of the cell area (e.g., 5G, Long Term Evolution (LTE), 3G, etc.).

In summary, techniques are described herein for a threat protection mechanism for V2X communication channels. A shared intelligence at the MEC function, SIE, OEM vendors, application providers, and external device vendors may improve the safety and security of multiple V-UEs simultaneously in real time. These techniques may thereby protect vehicles, drivers, and passengers from external attacks.