March 2022

ATTESTED PMIPV6 PROTOCOL FOR SEAMLESS HANDOVER IN 5G/LTE/Wi-Fi DEPLOYMENTS

NIRANJAN M M

ATTESTED PMIPV6 PROTOCOL FOR SEAMLESS HANDOVER IN 5G/LTE/Wi-Fi DEPLOYMENTS

AUTHOR:
NIRANJAN M M

ABSTRACT

To have seamless client handover/roaming across different radio access technologies and even across different vendors, PMIPv6 tunnelling protocol is used, for example, between Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) in 5G/LTE/Wi-Fi deployments. In other words, PMIPv6 is the standardised way of integrating trusted non-3GPP access networks with a standardised 3GPP Evolved Packet Core (EPC). PMIPv6 tunnel end points i.e., MAG and LMA need to know whether the peer device is trustworthy or not before establishing tunnel. If the MAG or LMA is compromised i.e., it is no longer a trusted entity, which could create harm to the network by allowing "malicious MAG to connect to the valid LMA" or "valid MAG connecting to malicious LMA". Currently PMIPv6 does not include any capabilities to exchange trust information between MAG and LMA to prove the peer was not tampered. The techniques presented herein define attestation method to PMIPv6 messages exchanged between MAG and LMA to provide Proof of Integrity for PMIPv6 tunnels.

DETAILED DESCRIPTION

PMIPv6 enables IP mobility for a client/host without requiring its participation in any mobility-related signalling. The network is responsible for managing IP mobility on behalf of the client/host. The mobility entities in the network are responsible for tracking the movements of the client/host and initiating the required mobility signalling on its behalf. With the extensions to the PMIPv6 protocol, MAG can register with more than one proxy Care-of Address (pCoA) with the LMA and simultaneously establish multiple IP tunnel with the LMA. This allows the MAG to utilize all the available access networks to route the mobile node's IP traffic. PMIPv6 facilities IP mobility by keeping below mobility parameters constant throughout the PMIPv6 domain, i.e., MN's IP address, MN's Gateway IP address, MN's Gateway MAC, DHCP Server address etc.,

In short, to have seamless client handover/roaming across different radio access technologies and even across different vendors, PMIPv6 tunnelling protocol is used.

- PMIPv6 tunnelling protocol is used between Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) in 5G/LTE deployments.
- PMIPv6 tunnelling protocol is used between WLC (act as MAG) and LMA in Wi-Fi deployments.
- To overcome the limitations of centralised mobility management, Distributed Mobility Management (DMM) concepts are used to bring the mobility anchor closed to the MN (Mobile Node), called as anchor and access routers as "Mobility Anchor and Access Router (MAAR)". PMIPv6 is also used between Serving MAAR (S-MAAR) acts as MAG and Anchor MAAR (A-MAAR) acts as LMA (A-MAAR is the MAAR that advertises the prefix used in the communication/flow. S-MAAR is the MAAR where MN (Mobile Node) is attached to it for communication/flow).

In short, PMIPv6 is the standardised way of integrating trusted non-3GPP access networks with a standardised 3GPP Evolved Packet Core (EPC). PMIPv6 tunnel end points i.e., MAG and LMA need to know whether the peer device is trustworthy or not before establishing tunnel. If the MAG or LMA is compromised i.e., it is no longer a trusted entity, which could create harm to the network by allowing "malicious MAG to connect to the valid LMA" or "valid MAG connecting to malicious LMA". Currently PMIPv6 does not include any capabilities to exchange trust information between MAG and LMA to prove the peer was not tampered.

In any of the above scenarios, PMIPv6 tunnel end points, i.e., MAG and LMA need to know whether the peer device is trustworthy or not before establishing tunnel. Hence, we need to have trustworthiness to PMIPv6 tunnelling protocol used between MAG and LMA by having attestation information in all tunnel establishments messages such as Proxy Binding Update (PBU), Proxy Binding Acknowledgement (PBA) exchanged during Mobile Node (MN) attachment and detachment flows.

The techniques presented herein define attestation method to PMIPv6 messages exchanged between MAG and LMA to provide Proof of Integrity for PMIPv6 tunnels. PMIPv6 messages between the peers (i.e., MAG and LMA) are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

A. Proof of Integrity:
TPM functionality is used as root of trust and as Proof of Integrity of PMIPv6 tunnel.
Both PMIPv6 end points gather below integrity measurements from the peer device:

- Hardware
- Software - micro loaded, BIOS, boot load, kernel, operating system
- Runtime - application binaries, libraries, config/manifest files

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 PMIPv6 tunnel establishment between the peers.

B. Freshness of the Proof of Integrity:
With Proof of Integrity, Freshness of the Proof of Integrity can also be considered.

As PMIPv6 is a request (Binding Update) and response (Binding Acknowledgement) type of protocol where each request is followed by a response, 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: Binding Update/Ack is the PMIPv6 message to establish PMIPv6 tunnel between MAG and LMA. The operation consists of the Proxy Binding Update and Proxy Binding Acknowledgement. Proxy Binding Request (PBU) from MAG contains random data "nonce", it is extended to carry intention to validate Proof of Integrity. Proxy Binding Acknowledgement (PBA) from LMA carries an extension to its Proof of Integrity along with a signature over random data "nonce" received in Proxy Binding Request.

For PMIPv6 (Proxy Mobile IPv6): This can be achieved by extending PMIPv6 with a new extension https://tools.ietf.org/html/rfc5213#page-69 (section 8.1) and by adding these attestation information in explicit Proxy Binding Update and Proxy Binding Acknowledgement for bi-directional tunnel management as defined in https://tools.ietf.org/html/rfc5213#page-37 (section 5.6.1)

For MIPv6 (Mobile IPv6): MIPv6 can also be extended with a new extension https://tools.ietf.org/html/rfc3775#page-161 and by adding these attestation information in Binding Refresh Request message etc., as defined in https://tools.ietf.org/html/rfc3775#page-31 (section 6.1).

In summary, this method adds attestation information to the PMIPv6 messages as an extension that embeds:

- a hardware fingerprint (derived from SUDI or similar)
- platform information includes PCR, counters, time-ticks etc.,

MAG and LMA will use this information against the device fingerprint, to verify whether the peer is trustworthy or not.
Integrity information can be added to the following PMIPv6 messages:

Proxy Binding Update
Proxy Binding Acknowledgement

Depending on the outcome of the verification, the MAG and LMA can decide, whether connectivity to the remote device should be considered or not. That is, if the verification is successful, then only PMIPv6 tunnel is established.
MAG can use level of trustworthiness to decide which LMA (if more than one LMA is configured/available) to connect using attestation-based selection criteria (want more secure/trust, least loaded LMA etc., based on configuration/requirement).
In short, attestation information would include hardware fingerprint which is derived from SUDI certificate stored securely in ACT2 chip, software information (version, OS, BIOS, kernel, application binaries/libraries etc.,) and platform information (counter, time-ticks, signature etc.,). MAG and LMA will use this information to verify the peer is trustworthy or not, before PMIPv6 tunnel is established.

The techniques presented herein provides trustworthiness to PMIPv6 tunnelling protocol used in seamless client handover/roaming across 5G/4G/3G/WiMAX/Wi-Fi technologies. Moreover, this method provides trustworthiness between MAG and LMA in both centralized and distributed mobility management (DMM) scenarios. Additionally, this method applicable for Mobile IP (MIP) and Mobile IPv6 (MIPv6) as well.