protection for control plane messages.

Summary

Embodiments described herein provide enhanced protection for NAS messages. A NAS procedure (e.g., registration of a UE) includes a set of Information Elements (IEs) that carry information. The embodiments described below set forth ways of protecting the IEs or a subset of the IEs that are sent in NAS messages. Thus, the information carried in the IEs is less vulnerable to malicious attacks.

In an aspect there is provided a User Equipment (UE) comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processor, cause the UE to initiate a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and a network element of a mobile network,

wherein, in a first phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

constructs a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

sends the first initial NAS message to the network element; and

receives a response from the network element that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE, and

wherein, in a second phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

constructs a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sends the subsequent NAS message to the network element.

In an aspect, there is provided network element of a mobility network comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processor, cause the network element to carry out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and the network element,

wherein, in a first phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

receive, from the UE, a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

construct a response to the first initial NAS message that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE; and

send, to the UE, the response to the first initial NAS message, and

wherein, in a second phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

receive, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs.

In an aspect there is provided a method comprising:

initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and a network element of a mobile network,

wherein, in a first phase of the NAS procedure, said initiating comprises:

constructing a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

sending the first initial NAS message to the network element; and

receiving a response from the network element that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE, and

wherein, in a second phase of the NAS procedure, said initiating comprises:

constructing a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sending the subsequent NAS message to the network element.

In an aspect, there is provided a method comprising:

causing a network element of a mobile network to carry out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and the network element,

wherein, in a first phase of the NAS procedure, said causing comprises:

receiving, from the UE, a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

constructing a response to the first initial NAS message that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE; and

sending, to the UE, the response to the first initial NAS message, and

wherein, in a second phase of the NAS procedure, said causing comprises:

constructing a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sending the subsequent NAS message to the network element.

In an aspect, there is User Equipment (UE) comprising:

at least one processor; and

at least one memory including computer program code; the at least one memory and the computer program code being configured to, with the at least one processor, cause the UE to initiate and perform a Non-Access Stratum (NAS) procedure to establish a NAS communication session between the UE and a network element of a mobile network;

wherein the at least one memory and the computer program code are configured, with the at least one processor, to:

determine that a NAS security context exists for use by the UE;

construct a first initial NAS message, the first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling, the first initial NAS message further including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure, which is different from the first set of NAS protocol IEs; and

send the first initial NAS message to the network element.

One embodiment comprises a network element of a mobile network. The network element includes a processor(s), and memory including computer program code executable by the processor. The processor is configured to cause the network element to perform a NAS procedure in multiple phases to establish a NAS communication session between the network element and a UE. For a first phase of the NAS procedure, the processor is further configured to cause the network element to receive an initial NAS message from the UE, where the initial NAS message is populated with a subset of NAS protocol IEs, from the NAS protocol IEs for the NAS procedure, that are designated for security-related handling. The processor is further configured to cause the network element to process the subset of the NAS protocol IEs to determine that a NAS security context does not exist for the UE, select a NAS security algorithm for the NAS security context, and send a response to the UE that indicates the NAS security algorithm and a security key set identifier of the NAS security context. For a second phase of the NAS procedure, the processor is further configured to cause the network element to receive a subsequent NAS message from the UE having a NAS message container that contains the initial NAS message encrypted based on the NAS security algorithm, and decrypt the NAS message container of the subsequent NAS message, where the initial NAS message contained in the NAS message container of the subsequent NAS message is populated with each of the NAS protocol IEs for the NAS procedure.

In another embodiment, for the first phase, the subset of the NAS protocol IEs are encrypted in the initial NAS message using a public key of a Home Public Land Mobile

Network (HPLMN) for the UE. The processor is further configured to cause the network element to initiate decryption of the subset of the NAS protocol IEs.