Transport Layer Security (TLS) Implementation for Secured MN-HA Communication in Mobile IPv6

Sunguk Lee

Research Institute of Industrial Science and Technology
Pohang, Korea
sunguk@rist.re.kr

Abstract

Mobile IPv6 usually use the IPsec/IKEv2 to secure Mobile Node (MN) and Home Agent (HA) communication. The implementation of IPsec/IKEv2 with MIPv6 is complex because it requires a tight coupling between MIPv6 protocol part and the IPsec/IKEv2 part of the IP stack. This paper proposes a security mechanism which uses Transport Layer Security (TLS) for establishing Keying Material and other bootstrapping parameters required to protect Mobile IPv6 signaling and data traffic between Mobile Node and Home Agent. This mechanism also supports Dual-Stack Mobile IPv6 which IPsec/IKEv2 finds it difficult to implement. TLS based establishment of Mobile IPv6 security associations compared to IKEv2 is the ease of implementation while providing an equivalent level of security.

Keyword: *TLS, Mobile IPv6, IKEv2, IPsec, AAA*

1. Introduction

The base specification of Mobile IPv6 [4] mandates IPsec support between MN and HA for authentication. Also, return routability messages passing via the HA (HoT/HoTi) and mobile prefix discovery messages must be protected using IPsec.

Even though IPsec may offer strong protection, use of IPsec may not be feasible in all cases where MIPv6 may be used. Use of IPsec may be too taxing for battery and processor for small handheld devices. Also depending on the model of the home agent (home agent may deploy by enterprise or service provider), MN may have to VPN back into the enterprise (which may impose dual IPsec requirement on MN) [5].

IPsec/IKEv (2) based MIPv6 over public wireless carrier's networks may pose serious capacity and scalability challenge. The multiple round trips to perform ISAKMP/IKE to establish IPsec SA is too taxing on the wireless link, it increase setup latency during initial access and handoffs. The use of manual [5] IPsec SA in these large public network deployments suffers from scalability issue and involves provisioning nightmare [5].

Also, having an authentication mechanism tied to the Mobile's home IP address does not permit the mobility entity to derive or acquire a dynamic home address based on the configured prefix.

In this mechanism, the MN is not tied with the mobility entities home IP address and therefore does not mandate SA relationship with an IP address.

Another important motivation for this proposed mechanism is the use of the bootstrapping. All information needed by the Mobile Node is provided by the HAC. This includes the Home

Agent Address, Mobile IPv6 Service Port Number, Home Address, Home Link Prefix and DNS server address. This will provide dynamic configuration and need not to undergo protocol to protocol communication between MN and HA, that in a way reduces time.

The content of the paper are as follows: Section 2, the Background, here we discussed the related information about the AAA, TLS and MIPv6 with IPSec/IKEv2 implementation. In Section 3, the proposed secure MN and HA Communication and Section 4 is the conclusion.

2. Background

2.1 AAA

The AAA protocol means Authentication, Authorization, and Accounting protocol. With the increasing popularity of mobile devices, a need has been generated to allow users to attach to any domain convenient to their current location. The need service from a foreign domain requires Authorization, which leads directly to Authentication, and of course Accounting. An agent in a foreign domain, being called on to provide access to a resource by a mobile user, is likely to request or require the client to provide credentials which can be authenticated before access to resources is permitted. Once authenticated, the mobile user may be authorized to access services within the foreign domain. An accounting of the actual resources may then be assembled [6].

The current Mobile IPv6 design relies on use of IPsec for authentication of protocol signaling between the MN and the HA. The associated IPsec SA is created by running IKE between the two. The initial authentication and authorization of MN and HA should be performed during the IKE execution. This is where HA must consult the AAA infrastructure. The authorization at this stage is for establishing an IPsec SA for Mobile IPv6 service. Authorization parameters for the subsequent Mobile IPv6 binding updates may also be delivered to the HA at this stage. Upon successful IPsec SA establishment for Mobile IPv6 service, MN can send binding updates to the HA. By the help of IPsec SA, the HA can authenticate the MN without AAA server help. Furthermore, the HA can also authorize the binding update if it already has the authorization parameters from its earlier interaction with the AAA server. Otherwise, the HA must contact the AAA server again to perform binding update authorization [7].

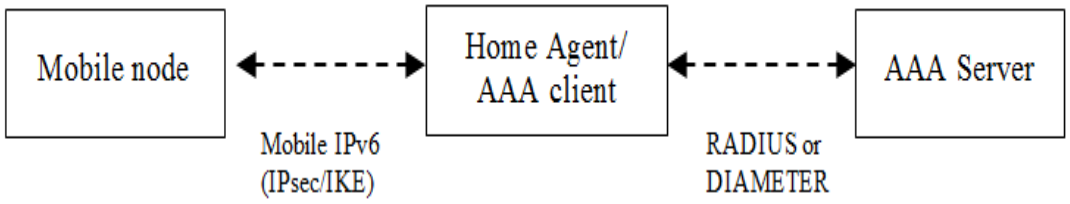

Figure 1. MIP6-AAA Framework

Figure 1 illustrates the Mobile IPv6 using AAA server. The Mobile IPv6 protocol is executed between the MN and the HA, as it normally would. Unlike a HA that relies on the preconfigured information, the AAA-enabled communicates with a AAA server in order to authenticate and authorize the MN before starting the Mobile IPv6 service, and later for making the accounting information available [7].

AAA backend protocols, such as RADIUS [8] and Diameter [9], enable centralized management of authentication, authorization, and accounting (AAA) for a limited type of services network access.

2.2 Transport Layer Security Solution

TLS is an IETF standards track protocol, last updated in RFC 5246, and is based on the earlier SSL specifications developed by Netscape Communications. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

Mobile IPv6 signaling between a mobile node and its home agent is secured using IPsec. The security association between a mobile node and the home agent is established using IKEv1 or IKEv2. The security model specified for Mobile IPv6, which relies on IKE/IPsec, requires interaction between the Mobile IPv6 protocol components and the IKE/ IPsec module of the IP stack [10]. One group of Internet Engineering Task Force (IETF) proposed a an alternate security framework for Mobile IPv6 and Dual-Stack Mobile IPv6, which relies on Transport Layer Security for establishing keying material and other bootstrapping parameters required to protect Mobile IPv6 signaling and data traffic between the mobile node and home agent [10].

The TLS connection is only used between the MN and the HAC during the MN authentication and bootstrapping phase.

2.3 MIPv6 Security Mechanisms with IPsec/IKEv2 Protocol with AAA

Dynamic Home Agent (HA) reassignment reduces both the signaling traffic and the data traffic to the home network. Simultaneous bindings with two or more HAs are supported in our model to provide seamless HA handover. Furthermore, the whole dynamic Home Agent/home address reassignment procedure is completed in a single registration signaling cycle. Hence it minimizes the delay of the Foreign Agent (FA) handoff.

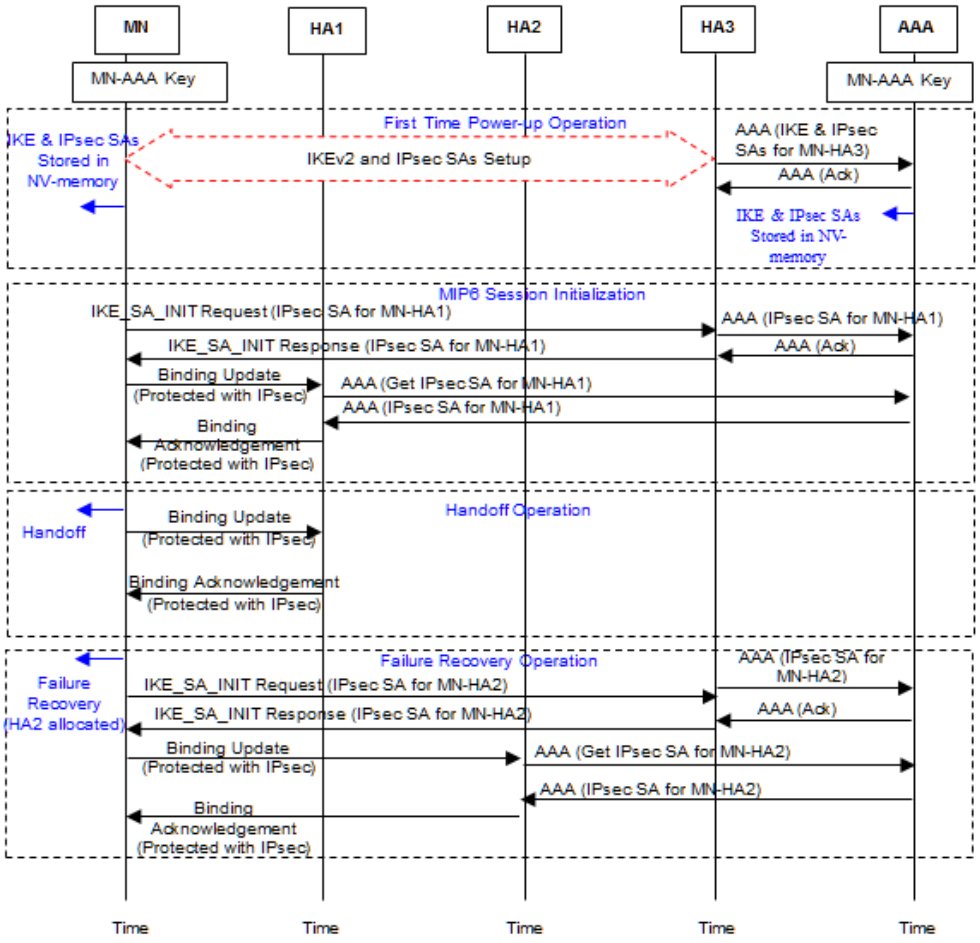

Figure 3. Optimized IKEv2-based Operation for HA in Visited Domain

The figure above is a security mechanism is an Optimized IKEv2-based Operation for HA in Visited Domain. This set-up is applicable if MN wants to initiate a MIP6 session and obtains a dynamic HA (HA1) in the visited domain. MN establishes an IPsec SA with HA3 that uploads the IPsec SA to the home AAA server. This requires only a single round trip of create child SA exchange. MN uses this IPsec SA to protect BU sent to HA1. No need for full IKEv2/EAP exchange between MN and HA1, because HA1 fetches the IPsec SA from the home AAA. Subsequent BUs (after the first one) doesn't need this AAA interaction. The IPsec SA is unique to the MN, HA pair Optimal when a visited domain allocates HA to the MN

As you can see in this mechanism there are too much processes takes place when authenticating the communication between MN and HA in visited domain.

3. Proposed Secure MN and HA Communication

The proposed mechanism used Transport Layer Security (TLS) to secure the communication between Mobile Node and Home Agent. The security model specified for Mobile IPv6, which relies on IKE/IPsec, requires interaction between the Mobile IPv6 protocol component and the IKE/IPsec module of the IP stack. Also this security model

requires a tight coupling between the Mobile IPv6 protocol part and the IKEv2/ IPsec part of the IP stack. Client implementation experience has shown that the use of IKE (v2)/IPsec with Mobile IPv6 is fairly complex. It should be noted that Mobile IPv4 for example, does not use IPsec for security and instead has specified its own security solution. If TLS is used, there will be an ease of securing IPv4 and interoperability between the MIPv6 and IPv4.

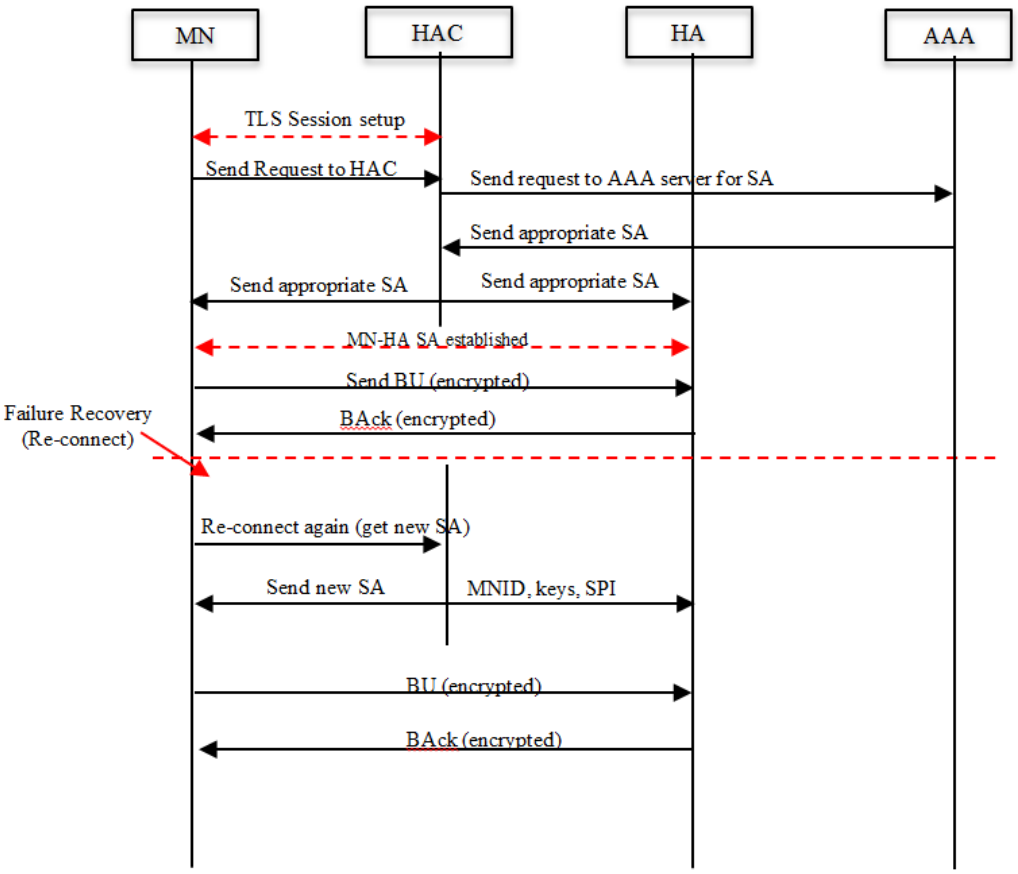

Figure 4. Proposed Secure Communication

The TLS connection is only used between the MN and the HAC during the MN authentication and bootstrapping phase. During the Mobile IPv6 bootstrapping, the MN and the HAC negotiate a single ciphersuite for protecting the traffic between the MN and the HA. The allowed ciphersuites for this specification are a subset of those in TLS version.

Another introduced new entity is HAC [11]. HAC is a functional entity and can be co-located with the HA, AAA or as a separate element. Security for the MN-HA signaling and optionally user traffic is via the SA bootstrapped by the HAC. The Authentication and MN-HA SA establishment executed between the MN and the HAC (PSK or EAP-based) through a TLS tunnel.

The Authentication and MN-HA SA establishment executed between the MN and the HAC (PSK- or EAP-based) through a TLS tunnel.

Mobile IPv6 specification requires that Mobile Nodes (MNs) are provisioned with a set of configuration parameters namely, the Home Address and the Home Agent Address, in order

to accomplish a home registration. The integration of the Authentication, Authorization, and Accounting (AAA) infrastructure will enable dynamic Mobile IPv6 bootstrapping. In this case, the AAA infrastructure can be exploited to offload the end host's authentication to the AAA server as well as to deliver the necessary configuration parameters to the visited network [12]. As shown in figure 4, we have designed separate HAC and AAA server. This two could be in the same location or as separate entities. Noticed that in the Failure Recovery scenario, HAC don't have to request AAA server for security information because the previous security association was already saved in Non-volatile memory of the HAC, HAC will have change the Security Parameter Index and re-connect again to MN.

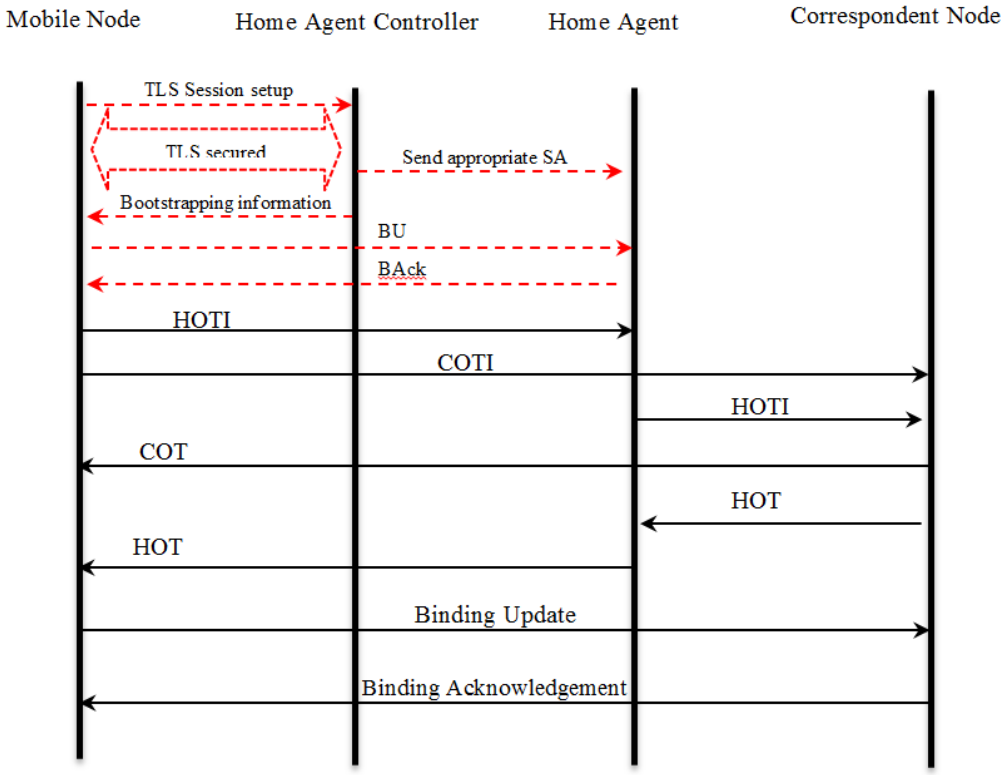

Figure 5. Return Routability Procedure

The Return Routability is not change, the process as it was. MN and HA communication is secured by TLS not the IPsec.

The red dotted arrow line indicates the exchanges of the request and response message between the MN and HAC to authenticate the communication and obtain the TLS secured tunnel. The SA established between MN and HAC contained at least of the following information, Mobility SPI, MN-HA keys for ciphering, MN-HA shared key for integrity protection, Security association validity time, Security association scope, and Selected ciphersuite. After the exchanges of the assigned SA, MN and HA already have the knowledge of each other. When the MN contacts the HAC to distribute the security-related information, the HAC may also provision the MN with various MIPv6- related bootstrapping information. It is then followed by the execution of Return Routability Procedure.

4. Conclusion

In the previous section, we have illustrated the security mechanism using IPsec and IKEv2 with AAA infrastructure, Optimized IKEv2-based Operation for HA in Visited Domain. This mechanisms use an IPsec/IKE2 to secure the communication between Mobile Node and Home Agent. Instead of using IKEv2 to establish security associations, the security framework proposed is based on TLS-protected messages to exchange keys and bootstrapping parameters between the MN and HAC. The use of TLS and HAC can offer advantages over IPsec and IKEv2 in implementation plus it support Dual-Stack Mobile IPv6, which when implemented using IPsec/IKEv2 needs different security configuration. TLS based establishment of Mobile IPv6 security associations compared to IKEv2 is the ease of implementation while providing an equivalent level of security.

References

[1] C. Perkins, D. Johnson and J. Arkko, "Mobility Support in IPv6", RFC 6275, **(2011)** July.
[2] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, **(2005)** December.
[3] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, **(2008)** August.
[4] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, **(2004)** June.
[5] A. Patel, K. Leung, M. Khalil, H. Akhtar and K. Chowdhury, "Authentication Protocol for Mobile IPv6", Internet Draft, **(2004)** July 2.
[6] R. I. Chen, R. -C. Wang and H. -C. Chao, "Mobile IPv6 and AAA Architecture Based on WLAN", Proceedings, SAINTW'04, **(2004)**.
[7] A. Yegin, "AAA Mobile IPv6 Application Framework", Internet-Draft, **(2005)** February 18.
[8] C. Rigney, S. Willens, A. Rubens and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, **(2000)** June.
[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, "Diameter Base Protocol", RFC 3588, **(2003)** September.
[10] Korhonen, et. al., "Transport Layer Security-based Mobile IPv6 Security Framework for Mobile Node to Home Agent Communication", Internet-Draft, **(2012)** February 15.
[11] J. Korhonen, et. al., "Mobile IPv6 Security Framework Using Transport Layer Security for Communication between the Mobile Node and Home Agent", RFC 6618, **(2012)** May.
[12] G. Giaretta, et. al., "Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6", RFC 5637, **(2009)** September.
[13] B. Aboba, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, **(2008)** August.