Attestation Protocols: A Tutortial Introduction

Perry Alexander Brigid Halling

October 7, 2012

Contents

List of Figures

List of Tables

Abstract

This document is intended to provide a tutorial overview of the basic attestation protocols used by a TPM.

1 Introduction

2 Certificate Authority Based Attestation

1. An appraiser sends an attestation request indicating what PCRs are needed along with a nonce.

2. The user software receives the request and requests a fresh AIK key pair from the TPM using the `TPM_MakeIdentity` command. Parameters to the `TPM_MakeIdentity` command describe properties of the desired AIK pair.
3. The TPM responds to the `TPM_MakeIdentity` command by generating a new AIK wrapped key pair and returning the public key, AIK signed by the TPM using AIK^{-1}. The new AIK is installed in the TPM prior to signing it's public part.
4. The user software sends the certified public EK and the signed public AIK to the Privacy CA. The public AIK is signed by the TPM using AIK^{-1}.
5. The Privacy CA checks the certificate on EK and determines if it has been revoked. It then uses AIK to check the signature on itself. Recall that only the TPM with AIK installed could generate that signature. If signature check succeeds, the Privacy CA knows the key is from the right TPM. If both checks are successful, the Privacy CA signs a certificate for the public AIK and encrypts the certificate with a fresh session key. It they encrypts the session key and the public AIK with EK.
6. Both the encrypted certificate and the encrypted session key and AIK are receive by the user software. The user software then uses the `TPM_ActivateIdentity` command to decyrpt the session key. Only the TPM associated with EK can decrypt the session key and will in turn decrypt the certificate. Thus, any recipient of the certificate knows the AIK was generate by the right TPM.
7. The user software decrypts the AIK certificate with the session key that can only be obtained if it has access to the TPM associated with the public EK sent to the CA.
8. The user software requests a quote from the TPM using the `TPM_Quote` command. The resulting quote is signed with the AIK. The certified AIK public key is also signed with the AIK. The user software sends the signed AIK certificate, signed quote, and stored measurement list back to the appraiser.
9. The appraiser analyzes the signed blobs received from the user software as follows: (i) the certified public AIK is used to check it's own signature; (ii) the certified public AIK is used to check the quote signature; (iii) the nonce is checked against the nonce sent with the request; and (iv) PCRs from the quote are compared with expected values.

3 Direct Anonymous Attestation

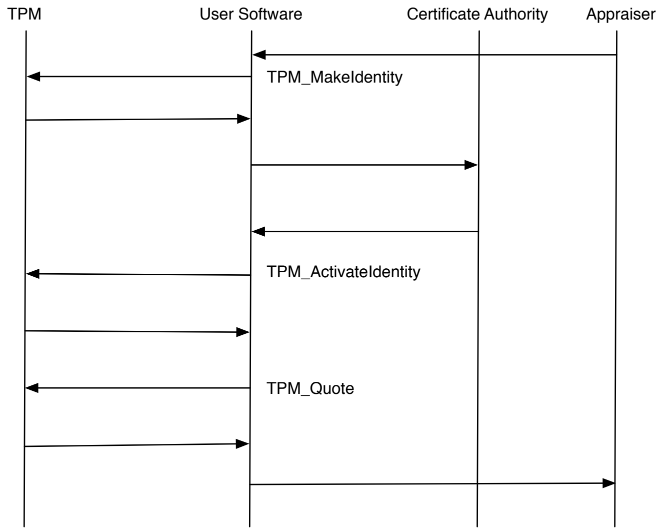

Figure 1: Protocol for Privacy CA remote attestation.