Remote Attestation for vNSFs

draft-pastor-i2nsf-vnsf-attestation

Antonio Pastor
Diego R. López
Adrian Shaw

I2NSF Meeting
Yokohama, 3rd November 2015
Why Attestation

- Virtualization applied to the NSF environment (vNSF) implies several additional concerns in security

- User impersonation can become especially serious due to the additional flexibility provided by the virtualization platform
  - Especially when privileges are granted by the virtualization platform

- Altered virtualized elements can try to take control of a vNSF or the virtualization platform
  - Or alter the traffic patterns through the vNSFs

- Physical access to the virtualization platform can further translate into modifying the components or attempting

- These threats can be addressed to an acceptable level of risk by
  - Mutual authentication
  - Attestation of the virtualization platform and the vNSFs

- The Security Controller constitutes the natural focal point for the attestation procedures
  - Mutual authentication with a well-known point
  - Orchestration of the attestation
The Attestation Principles

- The virtualization platform runs a TPM
  - Collecting measurements of the platform, the Security Controller, and the vNSFs

- Users and the Security Controller mutually authenticate
  - Establishing a desired level of assurance

- Trusted connection with the Security Controller
  - Or an endpoint designated by it
  - Through which all traffic to and from the virtualized NSF environment will flow

- The Security Controller makes the attestation measurements available to the user
  - Directly or through a trusted third party
  - The mechanisms for this are under evaluation
    - Results from WGs such as NEA and SACM to be considered
The Attestation Procedures

1. **Create a trusted channel with the Security Controller**
   - The establishment of the trusted channel is completed after the next step
   - The usage of a TPM and the requirements on the attestation measurements allow for the use of self-signed certificates for this

2. **Security Controller attestation**
   - The Security Controller retrieves the measurements and asks the TPM to sign the PCRs with an Attestation Identity Key (AIK)
   - The Security Controller shares the measurements with the user
   - As part of the verification, the application also checks that the digest of the certificate, received during the trusted channel handshake, is present among measurements, so the channel is completely established
   - A TTP can be used as intermediary for the verification

3. **Platform attestation**
   - The Security Controller makes the vNSFs measurements available for verification
   - Similar steps to the ones described for (2) above
   - This step can be applied periodically if the level of assurance requires it
Current Status and Next Steps

• Initial -00 derived from a deliverable of the SECURED project on virtual security environments
  – Too detailed on TCG procedures
  – No specification of the remote attestation procedures
  – Lack of details on the trusted channel between user and the Security Controller

• Make -01 evolve the document to align it better with this presentation
  – And include more context on secure instantiation and management of vNSFs

• And, for sure, address any comments this mostly respected community may have