Platform Trust Services (PTS) Protocol Binding to TNC IF-M Specification
Frequently Asked Questions
September 2011

Q. What is this specification about?
A. This specification describes the attestation protocol used by a remote challenger to obtain TPM protected attestation evidence as part of a Trusted Network Connect (TNC)-based remote assessment of a platform. The TNC protocol allows for retrieval of posture information (e.g. what anti-virus is installed) about a remote system using the TNC application layer protocol known as IF-M.

By layering the PTS Protocol on top of IF-M, using the extensibility of IF-M, the PTS Protocol allows for remote parties to communicate with the Platform Trust Services (PTS) software on the system being assessed and request TPM rooted "quotes" of information about the platform. These quotes provide TPM signed evidence that could prove the TNC software and its dependencies aren't under the influence of local malware or configured to falsify responses. The combination of traditional TNC assessment and TPM-based integrity evidence can provide higher assurance evaluations of the trustworthiness of a remote platform.

The specification and associated information can be found at http://www.trustedcomputinggroup.org/resources/tcg_attestation_pts_protocol_binding_to_tnc_ifm.

Q. What benefit is there to this new specification?
A. This new specification enables remote challengers to perform a TPM-based assessment of another system prior to sharing private or security sensitive information. The TPM is capable of storing measurements (code and state hashes) of the operational status of a machine and creating a cryptographically signed report of these measurements in such a way that local malware (even rootkits specifically targeting the TNC software) would be unable to hide its existence. Therefore, remote challengers can determine the level of trustworthiness leveraging both the TPM and TNC for performing an assessment without fear of malware intervention or the system attempting to lie about its state.

Q. What is the PTS?
A. The Platform Trust Services is a TCG-standard, trusted software component that performs measurements (hashes) of other system components during the boot and operation of the platform and can store the results in the TPM for protection. The PTS is also capable of creating detailed attestation reports of the current state of the platform optionally backed by TPM signed evidence. The combination of TPM and PTS-backed information allows a remote challenger to gain a more complete understanding of the posture of a platform in order to make a well-informed decision. For example, the PTS reporting could provide evidence that the TNC software and its underlying dependencies are running free of malware allowing the TNC posture messages to be relied upon for the remainder of an assessment.

Q. Why build the PTS Protocol on top of the TNC architecture?
A. The TNC protocols provide a proven base for performing remote assessments of a platform either over 802.1X, IKEv2 or TCP/IP network connections. The remote challenger wishing to perform a TPM-based assessment of a platform is very likely to operate over one of these protocols, and in many cases will wish to perform an integrated TNC and TPM-based

assessment. By building the PTS Protocol on top of the TNC protocol stack, this protocol can be run as part of a TNC assessment, so the remote challenger can see a single assessment view of the system including TPM and TNC assessment information. Another advantage is that developers can leverage existing TNC implementations when creating protocols based upon this specification.

Q. Is a PTS-based assessment different from a TPM quote?
A. The PTS is trusted software that builds upon the capabilities of the TPM. The PTS is capable of measuring processes and files on the platform into the Platform Configuration Registers (PCR) of the TPM. When the PTS is requested to create a report of the state of a portion of the platform, it is able to integrate a TPM quote into the response to show the TPM's registers match the contents of the PTS's report. Therefore, the PTS can offer a more granular reporting of the platform's state describing details of what is included in the TPM's quote. The PTS also is capable of reporting without including a TPM quote in cases where the remote challenger has already established the PTS is trustworthy.

Q. Why were the three schema specifications updated and why is it now 2.0?
A. As part of the definition of the PTS attestation protocol, the TCG Infrastructure Work Group decided to include messages for detecting when the client platform lacked or had older versions of the relevant schemas (particularly Reference Manifests). These messages allowed the remote challenger to push or reference the latest schemas to be used during the assessment. However, the 1.0 version of the schemas lacked the desired fields to make this version detection possible, so the specifications were modified to add both a version and information about the component being described by the schema. The changes required the addition of a few new mandatory fields that were not present in the 1.0 schemas, so the version was incremented for backward compatibility.

These changes plus the PTS Protocol are intended to make dynamic discovery and provisioning of schemas interoperable and much easier for customers.

Q. Who implements/supports this specification?
A. This is a new specification, and there are no public implementations as of yet. However, implementations of the TNC protocols, TPM and PTS do exist so this new specification allows a standard integration of these implementations. Interested developers should download the specification from the URL above to add it to an existing TNC product. Developers interested in more information about the PTS should see: http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_platform_trust_services_interface_specification_ifpts_version_10 and refer to the open source implementation found at: http://www.trustedcomputinggroup.org/resources/open_platform_trust_service.