TPM Quick Reference

Ariel Segall

October 23, 2012

1 Cryptographic Terms

Nonce A freshly generated random value used to prove recency

Symmetric Key A key used for cryptographic algorithms based on shared secrets. Good for cases where speed matters, but both parties must possess the secret. *The TPM does not provide symmetric encryption functionality.*

Asymmetric Key A key (technically, a key **pair**) used for cryptographic algorithms where only one party possesses a secret. Excellent security properties, but relatively slow. Also known as “public key pair”, since the algorithms are often referred to as “public key cryptography”. In TPM contexts, these are almost always RSA keys.

Public Key The half of an asymmetric key pair that can be freely provided to other people. Used for encryption and verification of signatures.

Private Key The half of an asymmetric key pair that must be kept secret. Used for decryption and signing.

CA (Certificate Authority) Trusted entity which issues certificates for keys. Usually run by an enterprise.

Hash A function that turns arbitrary data into a short, constant-length chunk of output data (also known as a hash). The critical features of hashes are that they are **one-way** (it is computationally infeasible to calculate the original data from the hash) and **collision resistant** (it is extremely difficult to find two pieces of source data that hash to the same result).

Denial of Service (DoS) A general term for an attack or system failure which causes a particular service to be unavailable. Impossible to completely prevent; do not imply a loss of future security.

Man in the Middle An attack where an adversary forwards messages between two honest parties resulting in false security assumptions; usually, the adversary can masquerade as one of the parties.

2 Trusted Computing Terms

AIK (Identity Key, Attestation Identity Key) A key which can be used to sign reports from the TPM, including quotes and CertifyKey certificates. A TPM can have many identities; only the TPM owner and owner-approved parties can create identities.

AR Access Requestor: TNC term for client machine seeking network access

Attestation The act of providing verifiable evidence (usually about a machine or its software state) to a remote party. In *mutual attestation*, two or more parties provide evidence to each other. Attestation is usually the first step in more complex transactions, used to establish trust.

Attester The participant providing evidence during an attestation.

Bind An operation which encrypts data using a TPM binding key. Bound data does not have PCR constraints, although binding keys can for similar effect. Bound data can be created locally or remotely.

DRTM (Dynamic Root of Trust for Measurement) A RTM that is part of the CPU or its firmware; called dynamic because, unlike a BIOS, it measures and launches whatever is provided to it, and can be run more than once per boot.

EK (Endorsement Key) The key that acts as the RTR for the TPM. An asymmetric key used only to certify AIKs.

Extend The only operation which adds data to a PCR. The current value is hashed with the additional data; the result is the new value of the PCR.

Late Launch A term used to describe systems which use the DRTM to avoid trusting the BIOS, boot loader, and other standard early system components. The "late launch" here refers to the launch of trusted software, such as an OS or hypervisor, via the DRTM.

Migratable Migratable keys can be "migrated" off of a given TPM by encrypting them with another key, usually (but not always) a key belonging to a different TPM.

Non-Migratable Non-migratable keys will always be locked to a given TPM, and will only exist in the clear within that TPM's internal memory.

NVRAM Non-Volatile RAM (memory); the TPM's long-term internal storage. Very limited in size.

PCR (Platform Configuration Register) A 20-byte register (region of memory) inside the TPM that always starts each boot at a known value, and which can be *extended* and in some cases *reset*. Used to store system measurements, among other things.

PDP Policy Decision Point: TNC term for a machine which evaluates a network access request and decides whether or not to grant it, ideally based on attestation evidence.

PEP Policy Enforcement Point: TNC term for gateway machine allowing or denying network access

Quote A signed report of PCR contents in a special TPM format, using a nonce for freshness.

Reset The operation which returns a PCR to a known value. Most PCRs are only reset when the system boots; some can be reset by software or hardware operations.

Root of Trust A component that is assumed to be correct, and which can be used to establish trust in other components.

RTM (Root of Trust for Measurement) The component which takes the first measurements of the system; see DRTM, SRTM.

RTR (Root of Trust for Reporting) In the TPM context, the EK: the key which is responsible for providing the lowest-level identification of the platform. The EK is not directly used for system reporting, but "reports" on the identity keys, which are.

RTS (Root of Trust for Storage) In the TPM context, the SRK: the key which is responsible for the security (encryption) of other keys or data, including other storage keys.

Seal An operation which encrypts data using a TPM storage key. Sealed data can have PCR constraints on when it can be opened, and records the PCR state when it was created. Only decryptable on the same machine it was encrypted on.

SRK (Storage Root Key) The key that acts as the RTS for the TPM, created when ownership is taken. An asymmetric key used only to encrypt other keys or data.

SRTM (Static Root of Trust for Measurement) A RTM that is part of the standard system boot process; static because what it measures never changes, and it always executes at the same stage of boot. The SRTM is a subset of the BIOS.

TBS (Trusted Base Services) Windows 7's native interface for programming the TPM. Driver level; programmer must actually feed in byte strings according to TPM spec. **Not generally usable today**–modifies commands in unpredictable ways.

TNC (Trusted Network Connect) TCG architecture for network access control that supports attestation and trusted computing.

TPM (Trusted Platform Module) Hardware chip soldered to the motherboard on most modern computers, providing a RTR and RTS as well as cryptographic functioanlity and storage.

TPM Key Shorthand for an asymmetric key created by a TPM and permanently bound to that TPM (non-migratable); its private half will never exist in the clear outside the TPM.

TSS (Trusted Software Stack) TCG-defined interface for developers to use when writing software that uses the TPM. C-level. Fairly solid implementations exist on Linux (TrouSerS) and Windows XP (NTRU TSS). Windows 7 has unreliable ports, and may have hard-to-find commercial implementations from NTRU and/or Wave Systems.

Verifier (Appraiser) The participant evaluating evidence during an attestation

3 Where to Find More Information

Sadly, there are not yet any good, centralized resources for newcomers to trusted computing to use.

http://www.trustedcomputinggroup.org The Trusted Computing Group is the largest organization in this field, and their website has by far the most information on trusted computing topics, including TPMs, TNC, and a wide variety of other technologies. However, the website has a very diverse audience and years' worth of content; many of the documents are aimed more at marketing than at technical information delivery. The "Developer" sections are usually most helpful for implementers or people seeking technical details, and include specifications and some talks and whitepapers about how to use the relevant technologies.

It's also worth noting that many TCG specifications are multi-part, because they're long; you will usually need all of the parts to make complete sense out of what's going on.

Andrew Martin's Ten-Page Introduction to Trusted Computing Andrew Martin is a professor at Oxford who's been doing trusted computing research for years. In response to the lack of introductory material in the field, he put together a ten-page introduction to trusted computing.

www.cs.ox.ac.uk/files/1873/RR-08-11.PDF

Books David Grawrock's *Dynamics of a Trusted Platform* is an extremely detailed book on the design and implementation of Intel's Trusted Execution Technology (TXT). It covers the goals and history of trusted computing, and does a very deep dive into the roots of trust for measurement as well as how the TPM interacts with the platform and CPU. Primarily useful for those planning on using the RTM, but can be useful for anyone wanting a low-level perspective on trusted computing.

3.1 Roots of Trust for Measurement

Flicker Flicker is a project out of CMU which uses the RTM to perform limited, high-trust operations with TPM verification. Open source, with downloadable demonstration code and instructions for both Intel and AMD platforms.

https://sparrow.ece.cmu.edu/group/flicker.html

3.2 Programming for the TPM

Dave Challener's *Practical Guide to Trusted Computing* is the primary reference manual for anyone interested in programming for the TPM using the Trusted Software Stack. Contains demonstration code for a number of basic applications, and an introduction to the concepts and abstractions the TSS uses. Not perfect (some of the code is buggy, and attestation is not a use case that is covered at all) but better than anything else we have.

Dave also taught a short session on TSS programming for the Trusted Infrastructure Workshop, whose slides and handout are publicly available:

http://www.cylab.cmu.edu/tiw/slides/challener-TPM.pdf

http://www.cylab.cmu.edu/tiw/slides/challener-handout.pdf

Unfortunately, there are no guides to programming the TPM directly or via TBS. Some Flicker code uses this approach, and you can refer to that, but the best manual you'll have for this process is the TPM specification itself.