ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΑΧΕΙΡΙΣΗ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΔΕΔΟΜΕΝΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Απομακρυσμένη Επιβεβαίωση (Attestation) Λογισμικού μέσω TPM

Χρήστος Χ. Αυλωνίτης

Επιβλέπων: **Ευστάθιος Χατζηευθυμιάδης,** Αναπληρωτής Καθηγητής ΕΚΠΑ

ΑΘΗΝΑ

ΔΕΚΕΜΒΡΙΟΣ 2017

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Απομακρυσμένη Επιβεβαίωση (Attestation) Λογισμικού μέσω TPM

Χρήστος Χ. Αυλωνίτης
Α.Μ.: Μ1429

ΕΠΙΒΛΕΠΩΝ: **Ευστάθιος Χατζηευθυμιάδης ,** Αναπληρωτής Καθηγητής ΕΚΠΑ

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: **Ευστάθιος Χατζηευθυμιάδης,** Αναπληρωτής Καθηγητής ΕΚΠΑ
Αθανασία Αλωνιστιώτη, Επίκουρη Καθηγήτρια ΕΚΠΑ

ΔΕΚΕΜΒΡΙΟΣ 2017

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία ασχολείται με τη μελέτη του Trusted Platform Module(TPM) ενός coprocessor που μπορεί να εκτελεί λειτουργίες όπως hash functions, asymmetric encryption και decryption, asymmetric signing και signature verification, symmetric encryption και decryption, symmetric signing (HMAC) και signature verification, και key generation. Επίσης μπορεί να αποθηκεύσει με ασφάλεια κωδικούς πρόσβασης, πιστοποιητικά και κλειδιά κρυπτογράφησης. Το TPM μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση μετρήσεων πλατφόρμας που βοηθούν να διασφαλιστεί ότι η πλατφόρμα παραμένει αξιόπιστη. Έγινε μελέτη των σχετιζόμενων πρότυπων του Trusted Computing Group(TCG), ενός οργανισμού που ασχολείται με τη δημιουργία προδιαγραφών ασφάλειας για υπολογιστές. Επίσης η εργασία ασχολείται με τη μελέτη ενός παραδείγματος remote attestation μέσω 2 υπολογιστών (attestation client και attestation server) σύμφωνα με το οποίο, μετά το πέρας της διαδικασίας, ο attestation server μπορεί να βεβαιωθεί για το σωστό status λειτουργίας του attestation client.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια συστημάτων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: TPM, Trusted Platform Module, επιβεβαίωση, TCG

ABSTRACT

This thesis deals with the study of a coprocessor Trusted Platform Module (TPM) that can perform functions such as hash functions, asymmetric encryption and decryption, symmetric signing and signature verification, symmetric signing (HMAC), and signature verification, and key generation. It can also safely store passwords, certificates and encryption keys. The TPM can also be used to store platform metrics to help ensure that the platform remains reliable. A related study of the Trusted Computing Group (TCG), an organization that is involved in creating security standards for computers, has been studied. Also, this thesis deals with the study of a remote attestation through attestation client and attestation server, where attestation server can verify attestation client at the end of the process.

SUBJECT AREA: Security systems

KEYWORDS: TPM, Trusted Platform Module, attestation, TCG

Θα ήθελα να αφιερώσω αυτή την εργασία στην αγαπημένη μου οικογένεια.

Στη Γεωργία, στο Γιάννη και στη Μαρία.

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ θερμά τον κ. Χατζηευθυμιάδη που μου πρότεινε το συγκεκριμένο θέμα και μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον αντικείμενο όπως επίσης και για την καθοδήγηση που μου παρείχε σε όλα τα στάδια αυτής της εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

1.1 Trusted Platform Module

Το TPM (Trusted Platform Module) είναι ένα τσιπ υπολογιστή (μικροελεγκτής) που μπορεί να αποθηκεύσει με ασφάλεια αντικείμενα που χρησιμοποιούνται για τον έλεγχο ταυτότητας της πλατφόρμας (του υπολογιστή ή του φορητού υπολογιστή). Αυτά τα αντικείμενα μπορεί να περιλαμβάνουν κωδικούς πρόσβασης, πιστοποιητικά ή κλειδιά κρυπτογράφησης. Ένα TPM μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση μετρήσεων πλατφόρμας που βοηθούν να διασφαλιστεί ότι η πλατφόρμα παραμένει αξιόπιστη. Το TPM σχεδιάστηκε για να ασφαλίζει το υλικό, ενσωματώνοντας κρυπτογραφικά κλειδιά σε συσκευές. Η τεχνική προδιαγραφή του TPM γράφτηκε από μια κοινοπραξία βιομηχανίας ηλεκτρονικών υπολογιστών με την ονομασία Trusted Computing Group (TCG).

Εικόνα 1:TPM Chip

Ο Trusted Computing Group είναι ένας διεθνής οργανισμός που περιλαμβάνει περίπου 120 εταιρείες που ασχολούνται με τη δημιουργία προδιαγραφών ασφάλειας για υπολογιστές για αξιόπιστες λειτουργικές μονάδες και άλλες συσκευές και πρωτόκολλα απαραίτητα για τη λειτουργία ενός αξιόπιστου περιβάλλοντος. Ο Διεθνής Οργανισμός Τυποποίησης (ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) τυποποίησαν τις προδιαγραφές ως ISO / IEC 11889 το 2009. [3]

Ο έλεγχος ταυτότητας (εξασφάλιση ότι η πλατφόρμα μπορεί να αποδείξει ότι είναι αυτό που ισχυρίζεται ότι είναι) και η επιβεβαίωση (μια διαδικασία που βοηθά να αποδειχθεί ότι μια πλατφόρμα είναι αξιόπιστη και δεν έχει παραβιαστεί) είναι απαραίτητα βήματα για την εξασφάλιση ασφαλέστερου υπολογισμού σε όλα τα περιβάλλοντα. Όλα τα παραπάνω μπορούν να χρησιμοποιηθούν εκτός των υπολογιστών, και σε κινητά τηλέφωνα ή σε εξοπλισμό δικτύου. Η φύση της κρυπτογραφίας με βάση το υλικό διασφαλίζει ότι οι πληροφορίες που αποθηκεύονται στο υλικό προστατεύονται καλύτερα

από εξωτερικές επιθέσεις λογισμικού. Αυτές οι εφαρμογές που αποθηκεύουν μυστικά σε ένα TPM καθιστούν πολύ πιο δύσκολη την πρόσβαση σε πληροφορίες σχετικά με υπολογιστικές συσκευές χωρίς κατάλληλη εξουσιοδότηση (π.χ., αν η συσκευή κλαπεί).

Εάν η διαμόρφωση της πλατφόρμας έχει αλλάξει ως αποτέλεσμα μη εξουσιοδοτημένων δραστηριοτήτων, η πρόσβαση σε δεδομένα και μυστικά μπορεί να απαγορευτεί και να σφραγιστεί με τη χρήση αυτών των εφαρμογών. Ωστόσο, είναι σημαντικό να κατανοήσουμε ότι το TPM δεν μπορεί να ελέγξει το λογισμικό που εκτελείται σε έναν υπολογιστή. Το TPM μπορεί να αποθηκεύσει παραμέτρους ρύθμισης χρόνου πριν από την εκτέλεση, αλλά άλλες είναι οι εφαρμογές καθορίζουν και εφαρμόζουν πολιτικές που σχετίζονται με αυτές τις πληροφορίες. Οι διαδικασίες που χρειάζονται για την εξασφάλιση μυστικών, όπως η ψηφιακή υπογραφή, μπορούν να γίνουν πιο ασφαλείς με το TPM. Και οι εφαρμογές κρίσιμης σημασίας που απαιτούν μεγαλύτερη ασφάλεια, όπως ασφαλές ηλεκτρονικό ταχυδρομείο ή ασφαλής διαχείριση εγγράφων, μπορούν να προσφέρουν ένα υψηλότερο επίπεδο προστασίας με τη χρήση ενός TPM.

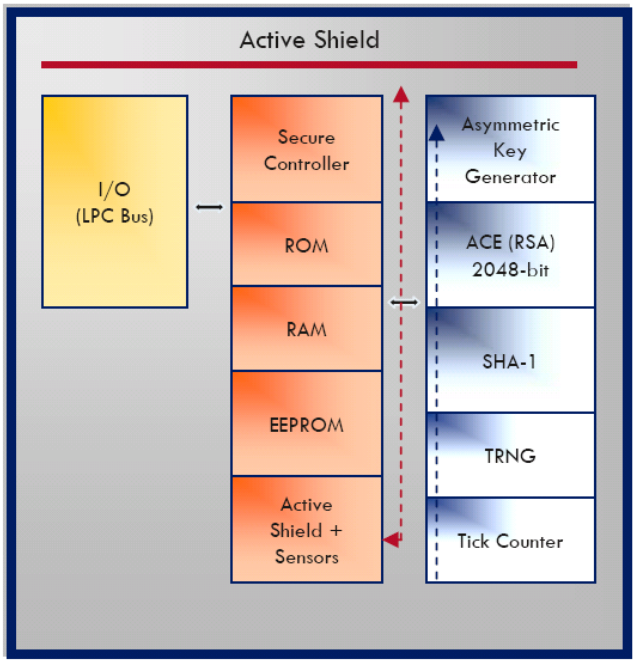
Για παράδειγμα, αν κατά την εκκίνηση διαπιστωθεί ότι ένας υπολογιστής δεν είναι αξιόπιστος λόγω μη αναμενόμενων αλλαγών στη διαμόρφωση, η πρόσβαση σε εφαρμογές υψηλής ασφάλειας μπορεί να αποκλειστεί μέχρι να διορθωθεί το πρόβλημα (εάν έχει ρυθμιστεί μια πολιτική που απαιτεί τέτοια ενέργεια).

Με ένα TPM, κάποιος μπορεί να είναι πιο σίγουρος ότι τα αντικείμενα που είναι απαραίτητα για την υπογραφή ασφαλών μηνυμάτων ηλεκτρονικού ταχυδρομείου δεν έχουν επηρεαστεί από επιθέσεις λογισμικού και με τη χρήση απομακρυσμένης επιβεβαίωσης, άλλες πλατφόρμες στο αξιόπιστο δίκτυο μπορούν να προσδιορίσουν, σε ποιο βαθμό μπορούν να εμπιστευτούν πληροφορίες από άλλο υπολογιστή. Η επιβεβαίωση ή οποιαδήποτε άλλη λειτουργία του TPM δεν μεταδίδει προσωπικές πληροφορίες του χρήστη της πλατφόρμας.

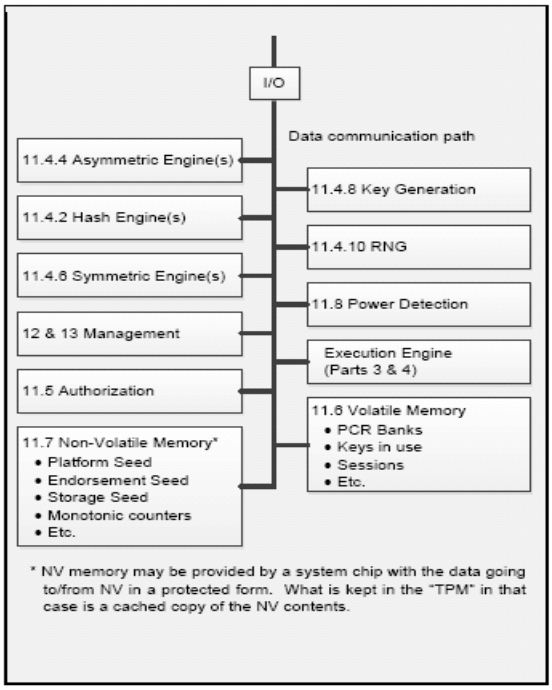
Αυτές οι δυνατότητες μπορούν να βελτιώσουν την ασφάλεια σε πολλούς τομείς της πληροφορικής, όπως το ηλεκτρονικό εμπόριο, τις εφαρμογές πολιτών-κυβερνήσεων, τις ηλεκτρονικές τραπεζικές υπηρεσίες, τις εμπιστευτικές κυβερνητικές επικοινωνίες και σε πολλούς άλλους τομείς όπου απαιτείται μεγαλύτερη ασφάλεια. Η ασφάλεια που βασίζεται στο υλικό μπορεί να βελτιώσει την προστασία στο VPN, στα ασύρματα δίκτυα, στην κρυπτογράφηση αρχείων (όπως στο BitLocker της Microsoft) και τη διαχείριση κωδικού πρόσβασης / PIN / διαπιστευτηρίων. Η προδιαγραφή TPM είναι OS-agnostic και υπάρχει στοίβα λογισμικού για διάφορα Λειτουργικά Συστήματα. Σύμφωνα με αναφορές έρευνας αγοράς, το 2007 πωλήθηκαν περισσότεροι από 100 εκατομμύρια επώνυμοι υπολογιστές και φορητοί υπολογιστές με TPM.

1.1.1 Συστατικά του TPM

Παρακάτω ακολουθούν εικόνες με τα συστατικά των 2 εκδόσεων TPM [7]. Την έκδοση TPM 1.2 και TPM 2.



Εικόνα 2: Συστατικά του TPM 1.2 [7]



Εικόνα 3: Συστατικά του TPM 2 [13]

I/O

Η μονάδα I/O έχει τα παρακάτω χαρακτηριστικά:

- Διαχειρίζεται τη ροή πληροφοριών μέσω του διαύλου επικοινωνίας.
- Συνήθως είναι LPC - Low Pin Count Bus.

Cryptography Subsystem

Το υποσύστημα κρυπτογράφησης υλοποιεί τις κρυπτογραφικές λειτουργίες του TPM. Μπορεί να καλείται από τη λειτουργική μονάδα ανίχνευσης εντολών, το υποσύστημα εξουσιοδότησης ή από το υποσύστημα εκτέλεσης εντολών.

Το TPM χρησιμοποιεί συμβατικές κρυπτογραφικές λειτουργίες με συμβατικούς τρόπους. Αυτές οι λειτουργίες περιλαμβάνουν:

- hash functions,
- asymmetric encryption και decryption,
- asymmetric signing και signature verification,
- symmetric encryption και decryption,
- symmetric signing (HMAC) και signature verification, και
- key generation.

Hash functions

Οι λειτουργίες Hash μπορούν να χρησιμοποιηθούν απευθείας από εξωτερικό λογισμικό ή από λειτουργίες του TPM. Το TPM χρησιμοποιεί κατακερματισμό για να παρέχει έλεγχο ακεραιότητας και έλεγχο ταυτότητας, καθώς και λειτουργίες μονής κατεύθυνσης, όπου απαιτείται (KDF).

HMAC Algorithm

Το TPM εφαρμόζει τον Hash Message Authentication Code (HMAC) που περιγράφεται στο ISO / IEC 9797-2. Ένα HMAC είναι μια μορφή συμμετρικής υπογραφής σε ορισμένα δεδομένα. Παρέχει τη διαβεβαίωση ότι τα προστατευμένα δεδομένα δεν τροποποιήθηκαν και ότι προέρχονταν από μια οντότητα με πρόσβαση σε μια βασική τιμή. Για να έχει χρησιμότητα στην προστασία δεδομένων, το κλειδί πρέπει να είναι μυστικό ή κοινό απόρρητο.

Asymmetric Operations

Ένα TPM χρησιμοποιεί ασύμμετρους αλγορίθμους για τη βεβαίωση(attestation), την ταυτοποίηση και τη ανταλλαγή μυστικών. Ένα TPM μπορεί να υποστηρίζει οποιονδήποτε ασύμμετρο αλγόριθμο στον οποίο ο TCG έχει εκχωρήσει ένα αναγνωριστικό. Ένα ασύμμετρο αναγνωριστικό αλγορίθμου θα υποδείξει μια οικογένεια αλγορίθμων και μεθόδων που χρησιμοποιούνται με αυτόν τον αλγόριθμο.

Signature Operations

Signing

Το TPM μπορεί να υπογράψει χρησιμοποιώντας είτε έναν ασύμμετρο είτε έναν συμμετρικό αλγόριθμο. Η μέθοδος υπογραφής εξαρτάται από τον τύπο του κλειδιού. Για έναν ασύμμετρο αλγόριθμο, οι μέθοδοι υπογραφής εξαρτώνται από τον αλγόριθμο (RSA ή ECC). Για συμμετρικές υπογραφές, μόνο το σύστημα υπογραφής HMAC ορίζεται αυτή τη στιγμή. Εάν ένα κλειδί μπορεί να χρησιμοποιηθεί για την υπογραφή, τότε θα έχει την ιδιότητα sign.

Επαλήθευση υπογραφής

Η εντολή TPM2_VerifySignature() επικυρώνει μια υπογραφή. Η εντολή παίρνει ένα handle ενός δημόσιου κλειδιού, ένα digest, και ένα μπλοκ που περιέχει την υπογραφή πάνω στο digest. Το TPM επικυρώνει ότι το σχήμα υπογραφής είναι συμβατό με το

επιλεγμένο κλειδί. Οποιοσδήποτε συνδυασμός hashes και μη ανώνυμων σχημάτων υπογραφής που υποστηρίζει ένα TPM για υπογραφή υποστηρίζεται επίσης για επαλήθευση υπογραφής. Εάν η υπογραφή είναι έγκυρη, το TPM θα παράγει ένα ticket.
Το TPM χρησιμοποιεί tickets για δύο σκοπούς:

- εκ νέου υπογραφή των δεδομένων. Αφού ελέγξει μια ασύμμετρη υπογραφή, το TPM ξαναυπογράφει το digest χρησιμοποιώντας ένα συμμετρικό κλειδί TPM. Το TPM μπορεί αργότερα να επαληθεύσει μια υπογραφή χωρίς να χρειάζεται να φορτώσει το ασύμμετρο κλειδί.
- επέκταση της κρατικής-state μνήμης. Κατά το hashing ενός εξωτερικού μηνύματος, το TPM έχει κάποια κατάσταση που υποδεικνύει ότι το μήνυμα δεν ξεκίνησε με TPM_GENERATED_VALUE. Αυτές οι πληροφορίες κατάστασης δεν μπορούν να διατηρηθούν επ 'αόριστον στο TPM. Ένα ticket επιτρέπει την αποθήκευση αυτής της κατάστασης από το TPM κατά τρόπο που είναι εύκολο για την επικύρωση του TPM. Όταν παρουσιάζεται αργότερα ένα digest στο TPM που πρόκειται να υπογραφεί, παρέχεται το ticket επιτρέποντας στο TPM να επιβεβαιώσει ότι το digest που θα υπογραφεί είναι ασφαλές για να το υπογράψει.

Συμμετρική κρυπτογράφηση
Το TPM χρησιμοποιεί συμμετρική κρυπτογράφηση για την κρυπτογράφηση ορισμένων παραμέτρων εντολών (τυπικά, πληροφορίες ελέγχου ταυτότητας) και για την κρυπτογράφηση προστατευμένων αντικειμένων που είναι αποθηκευμένα εκτός αυτού.
Η λειτουργία ανάκτησης κρυπτογραφίας Cipher Feedback mode(CFB) είναι ο μόνος τρόπος κρυπτογράφησης μπλοκ που απαιτείται από αυτήν την προδιαγραφή.
Οποιοσδήποτε συμμετρικός block cipher που υποστηρίζεται από ένα TPM μπορεί να χρησιμοποιηθεί για κρυπτογράφηση παραμέτρων. Ωστόσο, δεν επιτρέπεται η χρήση αδύναμων κλειδιών. Επιπλέον, ένα TPM θα πρέπει να υποστηρίζει την κρυπτογράφηση XOR, η οποία είναι hash-based stream cipher.XOR obfuscation μπορεί να χρησιμοποιηθεί μόνο για το πέρασμα εμπιστευτικών παραμέτρων. Όταν συνδυάζεται με ένα ασύμμετρο κλειδί - όπως σε ένα κλειδί αποκρυπτογράφησης ECC - ένα συμμετρικό κλειδί απαιτείται για να έχει τόσα bits security strength ασφαλείας όσα το ασύμμετρο κλειδί με το οποίο είναι συνδεδεμένο.
Όταν χρησιμοποιείται ένα συμμετρικό κλειδί για κρυπτογράφηση δεδομένων, τα κρυπτογραφημένα δεδομένα έχουν HMAC. Αυτό το HMAC ελέγχεται πριν από την αποκρυπτογράφηση των δεδομένων. Η επαλήθευση ότι τα αποκρυπτογραφημένα δεδομένα συνδέονται σωστά με το συμμετρικό κλειδί αποσκοπεί στο να καταστήσει πιο δύσκολη την εκτέλεση ανάλυσης ισχύος από τη πλευρά του επιτιθέμενου.

Secure Controller(1.2)

- Επαλήθευση εντολών.
- Εκτελεί τον κατάλληλο κώδικα εντολής.
- Ελέγχει την εσωτερική ροή εκτέλεσης TPM.

ROM

- TCG firmware.

EEPROM

- Δεδομένα χρήστη.
- Κλειδιά χρήστη [π.χ. Κλειδί επικύρωσης (EK) και Ριζικό κλειδί αποθήκευσης(SRK). και μυστικό του ιδιοκτήτη.

- Πιστοποιητικό κλειδιού επικύρωσης.

Asymmetric key generation (RSA, αποθήκευση και κλειδί μέγεθος> = 2048)

- Υποστήριξη κλειδιών 1024, 2048 bit.
- Προτείνεται η χρήση 2048.
- Για χρήση κλειδιού RSA πρέπει να φορτώθεί στο TPM.
- Το TPM μπορεί να κρυπτογραφήσει και να αποκρυπτογραφήσει χρησιμοποιώντας τα κλειδιά RSA.
- Χρήση των κλειδιών για υπογραφή ή χρήση κρυπτογράφησης.

Advanced Crypto Engine (ACE)

- Ασύμμετρες λειτουργίες κλειδιών(μήκος κλειδιού έως 2048-bit).

SHA-1 engine (160 bit)

- SHA-1 για Hashing (μέτρηση της ακεραιότητας).
- Χρησιμοποιείται κυρίως από το TPM ως αξιόπιστος hash αλγόριθμος.
- Χρήση κατά τη διαδικασία εκκίνησης.
- Το TPM δεν είναι crypto accelerator.

Random Noise Generator (RNG)

Το RNG είναι η πηγή τυχαιότητας στο TPM. Το TPM χρησιμοποιεί τυχαίες τιμές για nonces, για δημιουργία κλειδιών και για τυχαιότητα στις υπογραφές.
Ο RNG είναι προστατευμένη δυνατότητα χωρίς έλεγχο πρόσβασης. Αποτελείται από:

- μια πηγή εντροπίας και συλλέκτη,
- καταχωρητή κατάστασης, και
- μια λειτουργία ανάμειξης (τυπικά μια εγκεκριμένη λειτουργία κατακερματισμού).

Ο συλλέκτης εντροπίας συλλέγει την εντροπία από τις πηγές εντροπίας και απομακρύνει την προκατάληψη (bias). Η εντροπία που συλλέγεται στη συνέχεια χρησιμοποιείται για την ενημέρωση του καταχωρητή κατάστασης παρέχοντας είσοδο στη λειτουργία ανάμειξης για την παραγωγή τυχαίων αριθμών. Η λειτουργία ανάμιξης μπορεί να υλοποιηθεί με μια γεννήτρια ψευδοτυχαίων αριθμών (PRNG). Ένα PRNG μπορεί να παράγει αριθμούς που είναι προφανώς τυχαίοι από μια μη τυχαία είσοδο (όπως ένας μετρητής). Ο συνδυασμός ενός εγκεκριμένου PRNG με μια είσοδο που έχει πολύ μεγαλύτερη εντροπία από έναν μετρητή αποδίδει ένα RNG με ιδιότητες όχι χειρότερες από το υποκείμενο PRNG και ενδεχομένως πολύ βελτιωμένες.

Tick counter

- Καταγράφει τις εντολές TPM.

1.1.2 Τι μπορεί να κάνει ένα TPM

- Δημιουργία κωδικών[6].
- Αποθήκευση ψηφιακών διαπιστευτηρίων, όπως κωδικοί πρόσβασης σε υλικό.
- Διαχείριση κλειδιών.
- Παρέχει αυξημένη ασφάλεια στις έξυπνες κάρτες, στους αναγνώστες δακτυλικών αποτυπωμάτων και usb tokens για τον έλεγχο ταυτότητας πολλαπλών παραγόντων.

- Κρυπτογράφηση αρχείων και φακέλων για έλεγχο της πρόσβασης.
- Δημιουργία πληροφοριών κατάστασης για να ενεργοποίηση ακεραιότητας τελικού σημείου.
- Πληροφορίες κατάστασης hash πριν από τη διακοπή του σκληρού δίσκου για ακεραιότητα τελικού σημείου.
- Παρέχει αυξημένη ασφάλεια σε VPN, απομακρυσμένη και ασύρματη πρόσβαση.
- Χρήση σε συνδυασμό με κρυπτογράφηση πλήρους δίσκου για περιορισμό πρόσβασης σε ευαίσθητα δεδομένα.

1.1.3 Έναρξη χρήσης TPM

- Ενεργοποίηση του TPM από το BIOS[6].
- Φόρτωση του διαθέσιμου λογισμικού βοηθητικού προγράμματος TPM. Η Dell, η HP, η Lenovo και άλλες εταιρίες περιλαμβάνουν εφαρμογές λογισμικού για τη χρήση του TPM στα προϊόντα desktop και notebook για επιχειρήσεις.
- Ενεργοποίηση του TPM και ανάληψη ιδιοκτησίας. Αυτός είναι ο κωδικός πρόσβασης που χρησιμοποιείται για την αποδοχή άλλων λειτουργιών, όπως δημιουργία κλειδιών.
- Χρήση του TPM για δημιουργία κλειδιών για μια συγκεκριμένη ανάγκη, όπως η λήψη ενός πιστοποιητικού εικονικού ιδιωτικού δικτύου (VPN) χρησιμοποιώντας την Αρχή Πιστοποίησης της Microsoft (CA). Για να αξιοποιηθεί το TPM, πρέπει να ενημερώθεί η Αρχή Πιστοποίησης της Microsoft για το ποιος φορέας παροχής κρυπτογραφικών υπηρεσιών (CSP) θα χρησιμοποιηθεί. (Ο πάροχος κρυπτογραφικών υπηρεσιών (CSP) είναι μια βιβλιοθήκη λογισμικού που υλοποιεί το Microsoft CryptoAPI (CAPI). Οι CSPs εφαρμόζουν λειτουργίες κωδικοποίησης και αποκωδικοποίησης, τις οποίες τα προγράμματα εφαρμογών ηλεκτρονικών υπολογιστών μπορούν να χρησιμοποιήσουν, για παράδειγμα, για να εφαρμόσουν ισχυρό έλεγχο ταυτότητας χρήστη ή για ασφαλή ηλεκτρονική αλληλογραφία.[17]) Στη συνέχεια ο CSP επιλογής θα προκαλέσει την παραγωγή του ζεύγους κλειδιών χρησιμοποιώντας το TPM.

1.1.4 Βασικές έννοιες ασφάλειας

- Μήνυμα: Μια σειρά από bytes που στέλνονται μεταξύ δύο συμβαλλομένων[1].
- Μυστικότητα: Μέσο αποτροπής ενός μη εξουσιοδοτημένου παρατηρητή ενός μηνύματος από τον προσδιορισμό του περιεχομένου του.
- Κοινόχρηστο μυστικό: Μια τιμή που είναι γνωστή σε δύο μέρη. Το μυστικό μπορεί να είναι τόσο απλό όσο ένας κωδικός πρόσβασης, ή μπορεί να είναι και ένα κλειδί κρυπτογράφησης που γνωρίζουν και τα 2 μέρη.
- Ακεραιότητα: Μια ένδειξη ότι ένα μήνυμα δεν έχει αλλάξει κατά την αποθήκευση ή τη μετάδοση.
- Έλεγχος ταυτότητας: Ένας τρόπος υποδείξεως ότι ένα μήνυμα μπορεί να συνδεθεί στον δημιουργό, οπότε ο παραλήπτης μπορεί να επιβεβαιώσει ότι μόνο ο δημιουργός θα μπορούσε να έχει στείλει το μήνυμα.
- Εξουσιοδότηση: Η απόδειξη ότι ο χρήστης μπορεί να εκτελέσει μια λειτουργία.
- Anti-replay: Ένας τρόπος να εμποδιστεί ένας εισβολέας να επαναχρησιμοποιήσει ένα έγκυρο μήνυμα.

- Nonrepudiation: Ένα μέσο για την αποτροπή του αποστολέα ενός μηνύματος από την αξίωση ότι δεν έστειλε το μήνυμα.
- HMAC authorization: Χρησιμοποιεί (HMAC) για εξουσιοδότηση.Το κλειδί HMAC προκύπτει χρησιμοποιώντας ένα κοινό μυστικό.
- Policy ή enhanced authorization (EA): Εδώ γίνεται χρήση κάποιας πολιτικής που πρέπει να ικανοποιηθεί ώστε να δωθεί εξουσιοδότηση σε ένα αντικείμενο.
- Session: Τα sessions χρησιμοποιούνται για εξουσιοδήτηση και για λειτουργίες ανά εντολή.(κρυπτογράφηση, αποκρυπτογράφηση, audit και άλλες). Σε περίπτωση των HMAC policy Sessions τα sessions δημιουργούνται και χρησιμοποιούνται από πολλές εντολές.
- Handle: Ένα αναγνωριστικό που προσδιορίζει με μοναδικό τρόπο έναν πόρο του TPM που καταλαμβάνει τη μνήμη του TPM.
- Ρεύμα byte: Σε μια εντολή, τα πραγματικά bytes που αποστέλλονται στο TPM. Σε μια απόκριση, τα πραγματικά bytes που ελήφθησαν από το TPM.
- Κανονικοποιημένα δεδομένα: Τα σχήματα των εντολών που περιγράφονται στο μέρος 3 του προτύπου και περιγράφουν τις εισόδους και τις εξόδους από τη μονάδα TPM με δομές C. Αυτές οι δομές είναι συχνά πολύ μεγαλύτερες από τα δεδομένα που αποστέλλονται στο TPM. Ορισμένες δομές περιέχουν unions που αποτελούνται από στοιχεία με πολύ διαφορετικά μεγέθη. Για μια συγκεκριμένη περίπτωση ενός από αυτά τα union, μόνο τα δεδομένα που απαιτούνται από το συγκεκριμένο στοιχείο σύνδεσης είναι που χρησιμοποιείται κατά την αποστολή της εντολής αποστέλλεται στο TPM. Επιπλέον, όλα τα δεδομένα που αποστέλλονται και λαμβάνονται από το TPM είναι σε big-endian byte.
- Unmarshalled data: Δεδομένα της δομής σε γλώσσα C.
- Δεδομένα που έχουν ταξινομηθεί με σήματα: Τα δεδομένα στην κανονικοποιημένη μορφή του - δηλαδή, με τη μορφή αποστέλλονται ή λαμβάνονται από το TPM.

2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ TPM

2.1 Basic Trusted Platform Features

Μια αξιόπιστη πλατφόρμα παρέχει τις τρεις ρίζες της εμπιστοσύνης που περιγράφηκαν προηγουμένως. Και οι τρεις ρίζες χρησιμοποιούν πιστοποίηση και βεβαίωση (attestation) για να αποδείξουν την ακρίβεια των πληροφοριών. Μια αξιόπιστη πλατφόρμα θα προσφέρει επίσης προστατευμένες τοποθεσίες για τα κλειδιά και τα αντικείμενα δεδομένων που της έχουν ανατεθεί. Τέλος, μια αξιόπιστη πλατφόρμα μπορεί να παρέχει μέτρηση ακεραιότητας για να εξασφαλίσει την αξιοπιστία μιας πλατφόρμας από καταγραφή των αλλαγών στην κατάσταση της πλατφόρμας. Αυτό γίνεται με την καταγραφή καταγεγραμένων καταχωρήσεων σε PCR για μεταγενέστερη επικύρωση.

2.1.1 Ανάληψη ιδιοκτησίας TPM

Η ανάληψη ιδιοκτησίας ενός TPM είναι η διαδικασία εισαγωγής ενός κοινού μυστικού σε μια μη προσβάσιμη θέση του TPM. Κάθε οντότητα που γνωρίζει το κοινό μυστικό είναι ιδιοκτήτης του TPM. Απόδειξη ιδιοκτησίας συμβαίνει όταν μια οντότητα, ανταποκρινόμενη σε μια πρόκληση, αποδεικνύει τη γνώση του κοινού μυστικού. Ορισμένες λειτουργίες στο TPM απαιτούν έλεγχο ταυτότητας από έναν κάτοχο TPM. Ο ιδιοκτήτης του TPM έχει τον απόλυτο έλεγχο του TPM. Ο ιδιοκτήτης του TPM μπορεί να ενεργοποιήσει ή να απενεργοποιήσει το TPM, να δημιουργήσει AIK και να ορίσει πολιτικές για το TPM.

2.1.2 Platform Configuration Register (PCR)

Τα PCR (Platform Configuration Registers) είναι καταχωρητές 160 bit που βρίσκονται σε απρόσιτες τοποθεσίες και χρησιμοποιούνται στην ακεραιότητα μετρήσεων για την επικύρωση του περιεχομένου ενός αρχείου καταγραφής μετρήσεων. Η συμπεριφορά μιας αξιόπιστης πλατφόρμας είναι να διατηρεί ένα αρχείο καταγραφής των γεγονότων που επηρεάζουν την κατάσταση ασφαλείας της πλατφόρμας. Όταν πραγματοποιούνται προσθήκες στο αρχείο καταγραφής, το TPM λαμβάνει ένα αντίγραφο του αρχείου ή μιας σύνοψης των δεδομένων που περιγράφονται από το αρχείο καταγραφής. Τα δεδομένα που αποστέλλονται στο TPM περιλαμβάνονται σε συσσωρευμένο κατακερματισμό σε PCR. Το TPM μπορεί στη συνέχεια να παρέχει μια βεβαίωση της τιμής των PCR, η οποία, με τη σειρά της, επαληθεύει το περιεχόμενο του αρχείου καταγραφής. Η μέτρηση ακεραιότητας των εκτελέσιμων αρχείων αποθηκεύεται σωρευτικά στα PCR.

PCR [i] = SHA-1 (PCR [i] || newMeasurement)

Η επέκταση PCR δεν είναι αντιμεταθετική (δηλαδή η μέτρηση του A και μετά του B δεν έχει ίδια τιμή PCR με τη μέτρηση του B και μετά του A). Τα PCR μπορούν να αποθηκεύσουν απεριόριστο αριθμό μετρήσεων. Κάθε καταχωρητής περιέχει συγκεκριμένες τιμές:

- BIOS, ROM, Memory Block Register [καταχωρητής PCR 0-4]
- OS loaders [καταχωρητής PCR 5-7]
- Λειτουργικό σύστημα (OS) [καταχωρητής PCR 8-15]
- Debug [καταχωρητής PCR 16]
- Localities, Trusted OS[καταχωρητής PCR 17-22]

- Applications specific [καταχωρητής 23]

2.1.3 Root of Trust

- Root of Trust for Measurement (RTM)

  Υλοποιείται στο BIOS, εκκινεί διεργασία καταγραφής του λογισμικού που εκτελείται.

  Το RTM αποστέλλει πληροφορίες σχετικά με την ακεραιότητα (μετρήσεις) στο RTS. Συνήθως, το RTM είναι η CPU που ελέγχεται από το Core Root of Trust for Measurement (CRTM). Το CRTM είναι το πρώτο σύνολο εντολών που εκτελούνται όταν δημιουργείται μια νέα αλυσίδα εμπιστοσύνης. Όταν επαναφέρεται ένα σύστημα, η CPU ξεκινά την εκτέλεση του CRTM. Στη συνέχεια, το CRTM στέλνει τιμές που υποδεικνύουν την ταυτότητά του στο RTS. Αυτό καθιερώνει το σημείο εκκίνησης για μια αλυσίδα εμπιστοσύνης.

- Root of Trust for Storage (RTS)

  Υλοποιείται στο TPM. Η μνήμη TPM προστατεύεται από πρόσβαση από οποιαδήποτε οντότητα εκτός του TPM. Επειδή το TPM μπορεί να είναι αξιόπιστο για να αποτρέψει την ακατάλληλη πρόσβαση στη μνήμη του, το TPM μπορεί να λειτουργήσει ως RTS.

- Root of Trust for Reporting (RTR)

  Το RTR αναφέρει τα περιεχόμενα του RTS. Μια αναφορά RTR είναι συνήθως μια ψηφιακά υπογεγγραμένη σύνοψη του περιεχομένου επιλεγμένων τιμών μέσα σε ένα TPM.

  Οι συνηθισμένες τιμές αναφορών του RTR είναι:

  1. απόδειξη της διαμόρφωσης πλατφόρμας σε PCR (όπως TPM2_Quote ()),
  2. αρχεία καταγραφής ελέγχου (όπως TPM2_GetCommandAuditDI ()) και
  3. ιδιότητες κλειδιού (όπως TPM2_Certify ()).

2.1.4 Certification

Η κύρια μέθοδος δημιουργίας εμπιστοσύνης σε ένα κλειδί είναι με πιστοποιητικό που υποδεικνύει ότι οι διαδικασίες που χρησιμοποιούνται για τη δημιουργία και την προστασία του κλειδιού πληροί τα απαραίτητα κριτήρια ασφαλείας. Ένα πιστοποιητικό μπορεί να παρέχεται με την αποστολή του TPM με ένα ενσωματωμένο κλειδί (δηλαδή ένα κλειδί έγκρισης-Endorsement Key) μαζί με ένα πιστοποιητικό γνησιότητας για το κλειδί έγκρισης.

Το κλειδί έγκρισης και το πιστοποιητικό του μπορούν να χρησιμοποιηθούν για τη συσχέτιση διαπιστευτηρίων (πιστοποιητικών) με άλλα κλειδιά TPM. Όταν ένα πιστοποιημένο κλειδί έχει ιδιότητες που του επιτρέπουν να υπογράψει δεδομένα που έχουν δημιουργηθεί από το TPM, μπορεί να βεβαιώσει την εγγραφή των χαρακτηριστικών της πλατφόρμας του TPM που επηρεάζουν την ακεραιότητα (αξιοπιστία) μιας πλατφόρμας.

2.1.5 Κλειδιά επιβεβαίωσης

Όταν το TPM δημιουργεί ένα μήνυμα και το υπογράφει (όπως στο TPM2_Quote ()), χρησιμοποιεί μια ειδική τιμή (TPM_GENERATED_VALUE) ως κεφαλίδα μηνύματος. Ένα μήνυμα που δημιουργείται από το TPM αρχίζει πάντα με αυτήν την τιμή. Όταν το TPM λάβει ένα εξωτερικά παρεχόμενο μήνυμα, ελέγχει τις πρώτες οκτάδες του μηνύματος για να βεβαιωθεί ότι δεν έχουν την ίδια τιμή με το TPM_GENERATED_VALUE. Όταν ολοκληρωθεί η επεξεργασία, το TPM παράγει ένα εισιτήριο που υποδεικνύει ότι το μήνυμα δεν ξεκινάει με TPM_GENERATED_VALUE. Όταν ένα AK χρησιμοποιείται για την υπογραφή του digest, ο καλών παρέχει το εισιτήριο έτσι ώστε το TPM να μπορεί να καθορίσει ότι το μήνυμα που χρησιμοποιείται για τη δημιουργία του digest δεν ήταν πιθανή πλαστογράφηση των δεδομένων πιστοποίησης TPM. Το digest στο εισιτήριο πρέπει να ταιριάζει με το digest που παρουσιάζεται στο AK για υπογραφή. Εάν ένας εισβολέας δημιούργησε ένα μπλοκ μηνύματος το οποίο ήταν πανομοιότυπο με ένα quote που δημιουργήθηκε από το TPM, το μπλοκ μηνύματος θα ξεκινούσε με TPM_GENERATED_VALUE για να υποδείξει ότι είναι ένα σωστό TPM quote. Όταν το TPM εκτελεί ένα digest αυτού του μπλοκ, ελέγχει ότι οι πρώτες οκτάδες είναι ίδιες με τις TPM_GENERATED_VALUE. Δεν θα δημιουργήσει το εισιτήριο που να δείχνει ότι το μήνυμα είναι ασφαλές να υπογράψει, οπότε ένα AK δεν μπορεί να χρησιμοποιηθεί για να υπογράψει αυτό το digest. Ομοίως, μια οντότητα που ελέγχει μια βεβαίωση από ένα AK πρέπει να επαληθεύσει ότι το μήνυμα που έχει υπογραφεί αρχίζει με TPM_GENERATED_VALUE προκειμένου να επαληθευτεί ότι το μήνυμα είναι πράγματι ένα quote που έχει παραχθεί από το TPM.

Οι τιμές που υπογράφονται από ένα AK μπορούν να διασφαλιστούν ώστε να αντικατοπτρίζουν την κατάσταση TPM, αλλά τα AKs μπορούν επίσης να χρησιμοποιηθούν για γενικούς σκοπούς υπογραφής. Ένα AK δεν έχει μεγάλη αξία σε έναν απομακρυσμένο αμφισβητία εάν το AK δεν μπορεί να συνδεθεί με την πλατφόρμα που αντιπροσωπεύει. Αυτή η συσχέτιση γίνεται χρησιμοποιώντας τη διαδικασία πιστοποίησης ταυτότητας.

2.1.6 Πιστοποίηση ταυτότητας κλειδιού βεβαίωσης

Οποιοσδήποτε χρήστης TPM που μπορεί να δημιουργήσει ένα κλειδί σε ένα TPM μπορεί να δημιουργήσει ένα κλειδί υπογραφής περιορισμένης χρήσης. Στη συνέχεια, ο δημιουργός κλειδιών μπορεί να ζητήσει από ένα τρίτο μέρος, όπως μια Αρχή Πιστοποίησης (CA) βεβαίωσης, να παράσχει πιστοποιητικό γι 'αυτό. Η ΑΠ βεβαίωσης μπορεί να ζητήσει από τον καλούντα να δώσει κάποια στοιχεία ότι το κλειδί που πιστοποιείται είναι ένα κλειδί TPM. Η απόδειξη της συσχέτισης με το TPM μπορεί να παρασχεθεί χρησιμοποιώντας πιστοποιητικό που δημιουργήθηκε προηγουμένως για ένα άλλο κλειδί στο ίδιο TPM. Ένα πιστοποιητικό EK μπορεί να παράσχει τα εν λόγω αποδεικτικά στοιχεία. Δεν υπάρχει προϋπόθεση ότι τα πιστοποιητικά προέρχονται μόνο από αρχή πιστοποίησης βεβαίωσης. Η μέθοδος που περιγράφεται παραπάνω είναι ένα παράδειγμα ενός σχεδίου που μπορεί να χρησιμοποιηθεί όταν απαιτείται ιδιωτικότητα. Εάν ένα πιστοποιημένο κλειδί μπορεί να υπογράψει, μπορεί να χρησιμοποιηθεί για να πιστοποιήσει ότι κάποιο άλλο αντικείμενο κατοικεί στο ίδιο TPM. Αυτό επιτρέπει στο νέο AK να συνδεθεί με ένα πιστοποιημένο κλειδί. Μια Αρχή Πιστοποίησης μπορεί να χρησιμοποιήσει την πιστοποίηση από το TPM για να παράγει ένα παραδοσιακό πιστοποιητικό για το νέο κλειδί. Εάν το πιστοποιημένο κλειδί είναι ένα κλειδί αποκρυπτογράφησης που δεν μπορεί να υπογράψει, τότε χρησιμοποιείται μια

εναλλακτική μέθοδος για να επιτρέπεται η αξιόπιστη πιστοποίηση του νέου αντικειμένου κλειδιού ή δεδομένων. Για αυτή την εναλλακτική πιστοποίηση, παρέχεται στην Αρχή Πιστοποίησης η ταυτότητα του αντικειμένου που πρόκειται να πιστοποιηθεί και ένα πιστοποιητικό για το κλειδί αποκρυπτογράφησης (όπως ένα EK). Από το πιστοποιητικό, η Αρχή Πιστοποίησης καθορίζει το δημόσιο κλειδί για το κλειδί αποκρυπτογράφησης. Στη συνέχεια, η Αρχή Πιστοποίησης παράγει ένα υπό όρους πιστοποιητικό για το αντικείμενο που πρόκειται να πιστοποιηθεί. Το πιστοποιητικό εξαρτάται από την εκτέλεση κάποιας ενέργειας στην πιστοποίηση (όπως κρυπτογράφηση συμμετρικά) με μια τιμή που απαιτείται να γίνει γνωστή πριν από τη χρήση της πιστοποίησης. Αυτή η διαδικασία παράγει έναν προσδιοριστή πιστοποίησης που δίνεται στο TPM που περιέχει και το πιστοποιημένο κλειδί αποκρυπτογράφησης και το κλειδί που πρέπει να πιστοποιηθεί. Ένας κοινός προσδιοριστής διαπιστευτηρίων θα ήταν ένα συμμετρικό κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των διαπιστευτηρίων.

Μια άλλη επιλογή για τον προσδιοριστή διαπιστευτηρίων θα μπορούσε να είναι το σύνολο ή μέρος της υπογραφής του πιστοποιητικού. Άλλες επιλογές είναι δυνατές. Ο προσδιοριστής διαπιστευτηρίων προστατεύεται με μεθόδους που εξαρτώνται από τον τύπο του πιστοποιημένου κλειδιού αποκρυπτογράφησης. Υπάρχουν πρόσθετες μέθοδοι κατάλληλες για τα κλειδιά RSA και πρόσθετες μέθοδοι που είναι κατάλληλες για το κλειδί ECC. Η διαδικασία προστασίας παράγει ένα κρυπτογραφημένο blob, ένα HMAC πάνω από το blob και μια μυστική τιμή που μπορεί να ανακτηθεί μόνο από το πιστοποιημένο κλειδί αποκρυπτογράφησης. Το TPM2_ActivateCredential() χρησιμοποιείται για την πρόσβαση στον προσδιοριστή πιστοποίησης. Το TPM ανακτά τη μυστική τιμή και τη χρησιμοποιεί για να παράγει τα απαραίτητα κλειδιά για την αποκρυπτογράφηση και την επικύρωση του HMAC και του κρυπτογραφημένου blob. Εάν ο προσδιοριστής πιστοποιήσεων ανακτάται με επιτυχία και το κλειδί που πιστοποιείται με πιστοποίηση που φορτώνεται στο TPM, τότε τα περιεχόμενα του προσδιοριστή διαπιστευτηρίων επιστρέφονται στον καλούντα. Μπορούν στη συνέχεια να χρησιμοποιήσουν αυτήν την τιμή για να ολοκληρώσουν την πιστοποίηση κλειδιών. Η διαδικασία προστασίας που χρησιμοποιείται για τους προσδιοριστές πιστοποίησης είναι σχεδόν ίδια με τη διαδικασία που χρησιμοποιείται για την εισαγωγή κλειδιών. Προκειμένου να διασφαλιστεί ότι δεν υπάρχει κακή χρήση των κρυπτογραφημένων δομών, χρησιμοποιείται μια συγκεκριμένη τιμή για τη διαδικασία ανάκτησης κλειδιών. Στην περίπτωση ενός προσδιοριστή πιστοποίησης, η ετικέτα "TAYTOTHTA" χρησιμοποιείται στο KDF που δημιουργεί τα κλειδιά (συμμετρική και HMAC) από την τιμή του σπόρου. Το TPM2_ActivateCredential() συσχετίζει μια πιστοποίηση με οποιοδήποτε αντικείμενο. Η επιλογή των χαρακτηριστικών για ένα αντικείμενο προς πιστοποίηση είναι στη διακριτική ευχέρεια της Αρχής Πιστοποίησης. Επειδή ένα μοναδικό αναγνωριστικό για το αντικείμενο περιλαμβάνεται στο hash ακεραιότητας, το TPM επιβάλλει την προσβασιμότητα του διαπιστευτηρίου μόνο αν το αντικείμενο ταιριάζει με τα κριτήρια που καθορίζει η αρχή πιστοποίησης όπως εκφράζεται στο αναγνωριστικό αντικειμένου.

2.1.7 Προστατευμένη τοποθεσία-Protected Location

Όταν το ευαίσθητο τμήμα ενός αντικειμένου δεν κρατιέται σε απρόσιτη θέση στο TPM, είναι κρυπτογραφημένο. Όταν κρυπτογραφείται, αλλά όχι στο TPM, δεν προστατεύεται από τη διαγραφή, αλλά προστατεύεται από την αποκάλυψη των ευαίσθητων τμημάτων του[13]. Οπουδήποτε αποθηκεύεται, βρίσκεται σε προστατευμένη τοποθεσία. Τα αντικείμενα που βρίσκονται σε προστατευμένο αποθήκευτικό χώρο πρέπει να

φορτωθούν στο TPM για χρήση. Η εφαρμογή που δημιούργησε τα αντικείμενα διαχειρίζεται την κίνηση τους από το χώρο αποθήκευσης στο TPM. Επειδή ένα TPM έχει περιορισμένη μνήμη, μπορεί να μην είναι δυνατή η ταυτόχρονη φύλαξη όλων των αντικειμένων που απαιτούνται από όλες τις εφαρμογές. Το TPM υποστηρίζει την εναλλαγή των αντικειμένων από έναν διαχειριστή πόρων TPM (TPM Resource Manager-TRM), έτσι ώστε το TPM να μπορεί να εξυπηρετήσει αυτές τις πολλαπλές εφαρμογές. Τα αντικείμενα κρυπτογραφούνται πριν επιστραφούν στο TRM από το TPM. Εάν το αντικείμενο απαιτείται αργότερα, το TRM μπορεί να φορτώσει εκ νέου το αντικείμενο στο TPM παρέχοντας μια συμπεριφορά παρόμοια με την κρυφή μνήμη. Η κρυπτογράφηση προστατευμένων τοποθεσιών χρησιμοποιεί πολλαπλούς σπόρους και κλειδιά που παραμένουν πάντα στο TPM. Ένα από αυτά είναι το Context κλειδί. Πρόκειται για ένα συμμετρικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση δεδομένων όταν μετατοπίζονται προσωρινά από το TPM έτσι ώστε να μπορεί να φορτωθεί διαφορετικό σύνολο αντικειμένων εργασίας. Άλλες ευαίσθητες τιμές που δεν αφήνουν ποτέ το TPM είναι οι πρωτογενείς σπόροι(Primary Seeds). Αυτοί οι σπόροι είναι η ρίζα των ιεραρχιών αποθήκευσης που προστατεύουν αντικείμενα που διατηρούνται από εφαρμογές. Ένας πρωτεύων σπόρος είναι ένας τυχαίος αριθμός που χρησιμοποιείται για τη δημιουργία κλειδιών προστασίας για άλλα αντικείμενα. Αυτά τα αντικείμενα ενδέχεται να είναι κλειδιά αποθήκευσης που περιέχουν κλειδιά προστασίας που στη συνέχεια χρησιμοποιούνται για την προστασία ακόμα περισσότερων αντικειμένων. Οι πρωτογενείς σπόροι μπορούν να αλλάξουν, και όταν αλλάξουν, τα αντικείμενα που προστατεύονται δεν θα είναι πλέον χρησιμοποιήσιμα. Για παράδειγμα, ο Storage Primary Seed (SPS) δημιουργεί την ιεραρχία αποθήκευσης για δεδομένα σχετικά με τον ιδιοκτήτη και ο σπόρος αλλάζει όταν αλλάζει ο κάτοχος.

2.1.8 Μέτρηση ακεραιότητας και αναφορά-Integrity Measurement and Reporting

Η βασική ρίζα εμπιστοσύνης για μέτρηση (CRTM) είναι το σημείο εκκίνησης της μέτρησης. Αυτή η διαδικασία καθιστά τις αρχικές μετρήσεις της πλατφόρμας που εκτείνονται σε PCR στο TPM. Προκειμένου οι μετρήσεις να έχουν νόημα, ο κώδικας εκτέλεσης πρέπει να ελέγχει το περιβάλλον στο οποίο εκτελείται, έτσι ώστε οι τιμές που καταγράφονται στο TPM να είναι αντιπροσωπευτικές της αρχικής κατάστασης εμπιστοσύνης της πλατφόρμας. Ένα reset δημιουργεί ένα περιβάλλον στο οποίο η πλατφόρμα βρίσκεται σε μια γνωστή αρχική κατάσταση, με τον κύριο κώδικα λειτουργίας CPU να προέρχεται από κάποια καλά καθορισμένη αρχική τοποθεσία. Δεδομένου ότι ο κώδικας αυτός έχει αποκλειστικό έλεγχο της πλατφόρμας εκείνη τη στιγμή, μπορεί να κάνει μετρήσεις της πλατφόρμας από το firmware. Από αυτές τις αρχικές μετρήσεις μπορεί να δημιουργηθεί μια αλυσίδα εμπιστοσύνης. Επειδή αυτή η αλυσίδα εμπιστοσύνης δημιουργείται μία φορά μετά το reset της πλατφόρμας, δεν είναι δυνατή η αλλαγή της αρχικής κατάστασης εμπιστοσύνης, επομένως ονομάζεται στατικό RTM (S-RTM).

Μια εναλλακτική μέθοδος για την αρχικοποίηση της πλατφόρμας είναι διαθέσιμη σε ορισμένες αρχιτεκτονικές επεξεργαστών. Αφήνει την CPU να λειτουργεί ως CRTM και εφαρμόζει προστασία σε τμήματα μνήμης που μετρά. Αυτή η διαδικασία επιτρέπει σε μια νέα αλυσίδα εμπιστοσύνης να ξεκινήσει χωρίς να γίνει επανεκκίνηση της πλατφόρμας. Επειδή το RTM μπορεί να αποκατασταθεί δυναμικά, αυτή η μέθοδος ονομάζεται δυναμική RTM (D-RTM).

Τόσο το S-RTM όσο και το D-RTM μπορούν να πάρουν ένα σύστημα σε άγνωστη κατάσταση και να το επιστρέψουν σε μια γνωστή κατάσταση. Το D-RTM έχει το πλεονέκτημα ότι δεν απαιτεί επανεκκίνηση του συστήματος. Μια μέτρηση ακεραιότητας είναι μια τιμή που αντιπροσωπεύει πιθανή αλλαγή στην κατάσταση εμπιστοσύνης της πλατφόρμας.Το μετρημένο αντικείμενο είναι συνήθως:

- μια τιμή δεδομένων,
- το hash του κώδικα ή των δεδομένων, ή
- ένδειξη του υπογράφοντος κάποιου κώδικα ή δεδομένων.

Το RTM (συνήθως, ο κώδικας που τρέχει στη CPU) κάνει αυτές τις μετρήσεις και τις καταγράφει σε RTS χρησιμοποιώντας το Extend. Η διαδικασία επέκτασης επιτρέπει στο TPM να συσσωρεύει έναν απεριόριστο αριθμό μετρήσεων σε σχετικά μικρή ποσότητα μνήμης. Η σύνοψη μιας αυθαίρετης σειράς μετρήσεων ακεραιότητας είναι στατιστικά μοναδική και ένας αξιολογητής μπορεί να γνωρίζει τις τιμές που αντιπροσωπεύουν συγκεκριμένες ακολουθίες μετρήσεων. Για την αντιμετώπιση περιπτώσεων όπου οι τιμές PCR δεν είναι πολύ γνωστές, το RTM διατηρεί ένα ημερολόγιο μεμονωμένων μετρήσεων. Οι τιμές PCR μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της ακρίβειας του ημερολογίου και οι καταχωρίσεις του ημερολογίου μπορούν να αξιολογηθούν μεμονωμένα για να προσδιοριστεί εάν η αλλαγή στην κατάσταση συστήματος που υποδεικνύεται από το συμβάν είναι αποδεκτή. Οι εκτελεστές (Implementers) παίζουν ένα ρόλο στον καθορισμό του τρόπου κατανομής των συμβάντων των δεδομένων. Οι προδιαγραφές της πλατφόρμας TCG παρέχουν πρόσθετη εικόνα για τον καθορισμό της διαμόρφωσης και της αναπαράστασης της πλατφόρμας καθώς και για τους αναμενόμενους αποδέκτες των δεδομένων μέτρησης. Η αναφορά ακεραιότητας είναι η διαδικασία πιστοποίησης μετρήσεων ακεραιότητας που καταγράφονται σε PCR. Η φιλοσοφία πίσω από τη μέτρηση της ακεραιότητας, την καταγραφή και την αναφορά είναι ότι μια πλατφόρμα μπορεί να εισέλθει σε οποιαδήποτε κατάσταση - συμπεριλαμβανομένων ανεπιθύμητων ή ανασφαλών καταστάσεων - αλλά υποχρεούται να αναφέρει με ακρίβεια τις καταστάσεις αυτές. Μια ανεξάρτητη διαδικασία μπορεί να αξιολογήσει τις καταστάσεις ακεραιότητας και να καθορίσει μια κατάλληλη απάντηση.

2.1.9 Authentication and attestation

Το attestation είναι η παρουσίαση αξιόπιστων στοιχείων σχετικά με μια συσκευή σε μια απομακρυσμένη οντότητα. Στο πλαίσιο του TPM, τα αποδεικτικά στοιχεία γενικά σημαίνουν PCRs. Ο Verifier, αυτός που επαληθεύει, μπορεί να επιθεωρήσει τα PCRs, και να επαληθεύσει την αλυσίδα εμπιστοσύνης. Το κύριο εργαλείο είναι το Quote δηλαδή υπογεγραμμένη αναφορά των τρεχουσών τιμών των PCR[4].

Είδη Attestation

Οι αξιόπιστες πλατφόρμες χρησιμοποιούν μια ιεραρχία βεβαιώσεων:

1) Μια εξωτερική οντότητα διαβεβαιώνει-πιστοποιεί ένα TPM προκειμένου να εγγυηθεί ότι το TPM είναι γνήσιο και συμμορφώνεται με αυτήν την προδιαγραφή TPM. Αυτή η βεβαίωση λαμβάνει τη μορφή ενός ασύμμετρου κλειδιού που είναι ενσωματωμένο σε ένα γνήσιο TPM, καθώς και μια πιστοποίηση που εγγυάται το δημόσιο κλειδί αυτού του ζεύγους. Μια πιστοποίηση που χρησιμοποιείται για να εγγυηθεί για το ενσωματωμένο

ασύμμετρο κλειδί ονομάζεται συνήθως "Πιστοποιητικό έγκρισης(Endorsement Certificate)".

2) Μια εξωτερική οντότητα βεβαιώνει σε μια πλατφόρμα για να εγγυηθεί ότι η πλατφόρμα περιέχει ένα Root-of-Trust-for-Measurement, ένα πραγματικό TPM, καθώς και μια αξιόπιστη διαδρομή μεταξύ του RTM και του TPM. Αυτή η βεβαίωση λαμβάνει τη μορφή μιας πιστοποίησης που εγγυάται πληροφορίες, συμπεριλαμβανομένου του δημόσιου κλειδιού του ασύμμετρου ζεύγους κλειδιών στο TPM. Μια πιστοποίηση που χρησιμοποιείται για την πιστοποίηση της πλατφόρμας ονομάζεται συνήθως "Πιστοποιητικό πλατφόρμας".

3) Μια εξωτερική οντότητα που ονομάζεται "CA Certification" βεβαιώνει ένα ασύμμετρο ζεύγος κλειδιών σε ένα TPM, προκειμένου να εγγυηθεί ότι ένα κλειδί προστατεύεται από ένα μη αναγνωρισμένο αλλά γνήσιο TPM και έχει συγκεκριμένες ιδιότητες. Αυτή η βεβαίωση λαμβάνει τη μορφή μιας πιστοποίησης που εγγυάται πληροφορίες, συμπεριλαμβανομένου του δημόσιου κλειδιού του ζεύγους κλειδιών. Μια Attestation CA βασικά βασίζεται σε βεβαιώσεις τύπου 1 και 2 προκειμένου να παράγει βεβαίωση τύπου 3. Οι διαπιστεύσεις που δημιουργούνται από την αρχή πιστοποίησης καλούνται συνήθως "Πιστοποιητικό κλειδιού πιστοποίησης-Attestation Key Certificate".

4) Μια αξιόπιστη πλατφόρμα βεβαιώνει ένα ασύμμετρο ζεύγος κλειδιών για να εγγυηθεί ότι ένα ζευγάρι κλειδιών προστατεύεται από ένα γνήσιο αλλά μη αναγνωρισμένο TPM με συγκεκριμένες ιδιότητες. Αυτή η βεβαίωση λαμβάνει τη μορφή υπογραφής που υπογράφεται από το TPM της πλατφόρμας πάνω σε πληροφορίες που περιγράφουν το ζευγάρι κλειδιών, χρησιμοποιώντας ένα κλειδί βεβαίωσης που προστατεύεται από το TPM, καθώς και βεβαίωση τύπου 3 που εγγυάται το κλειδί βεβαίωσης. Αυτός ο τύπος βεβαίωσης γίνεται χρησιμοποιώντας την εντολή TPM2_Certify ().

5) Μια αξιόπιστη πλατφόρμα πιστοποιεί μια μέτρηση προκειμένου να επιβεβαιώσει ότι υπάρχει μια συγκεκριμένη κατάσταση software/firmware σε μια πλατφόρμα. Αυτή η βεβαίωση λαμβάνει τη μορφή υπογραφής μέσω μέτρησης software/firmware σε PCR χρησιμοποιώντας κλειδί βεβαίωσης που προστατεύεται από το TPM, συν τη βεβαίωση τύπου 3 ή 4 για το εν λόγω κλειδί βεβαίωσης. Αυτός είναι ο τύπος της βεβαίωσης που κοινώς αποκαλείται "quote" και γίνεται με την εντολή TPM2_Quote ().

6) Μια εξωτερική οντότητα πιστοποιεί μια μέτρηση software/firmware προκειμένου να εγγυηθεί για συγκεκριμένο software/firmware. Αυτή η βεβαίωση λαμβάνει τη μορφή ενός πιστοποιητικού που εγγυάται πληροφορίες, συμπεριλαμβανομένης της τιμής μιας μέτρησης και της κατάστασης που αντιπροσωπεύει. Αυτό ονομάζεται συνήθως "πιστοποίηση τρίτου μέρους".

Η βεβαίωση των τύπων 3 και 4 συνεπάγεται τη χρήση κλειδιού για την υπογραφή των περιεχομένων απρόσιτων τοποθεσιών. Ένα κλειδί βεβαίωσης (AK) είναι ένας ιδιαίτερος τύπος κλειδιού υπογραφής που έχει περιορισμό στη χρήση του, προκειμένου να αποφευχθεί η πλαστογράφηση (η υπογραφή εξωτερικών δεδομένων που έχει την ίδια μορφή με τα γνήσια δεδομένα βεβαίωσης). Ο περιορισμός είναι ότι ένα AK μπορεί να χρησιμοποιηθεί μόνο για να υπογράψει ένα digest που έχει δημιουργήσει το TPM. Εάν ένα AK είναι γνωστό ότι προστατεύεται από ένα TPM (δυνάμει βεβαίωσης τύπου 3 ή 4), μπορεί να βασιστεί σε αναφορά με ακρίβεια στο περιεχόμενο απρόσιτης τοποθεσίας και να μην υπογράψει εξωτερικά δεδομένα που φαίνεται να είναι έγκυρα και που έχουν παραχθεί από το TPM, αλλά δεν είναι.

2.1.10 Secure Boot vs Measured Boot

Υπάρχουν γενικά δύο προσεγγίσεις για να διασφαλιστεί ότι ο κώδικας που εκτελείται σε μια συσκευή δικτύου είναι εγκεκριμένος και δεν έχει υποβληθεί σε παράνομη τροποποίηση.

Ασφαλής εκκίνηση (**Secure Boot**) [8]
Γνωστή και ως Verified Boot είναι μια διαδικασία με την οποία σε κάθε στάδιο της εκκίνησης ελέγχεται μια κρυπτογραφική υπογραφή του επόμενου σταδίου πριν αυτό εκτελεστεί. Σε ένα τυπικό σύστημα, μπορεί να υπάρχει ένα BIOS που κάνει έλεγχο της υπογραφής του Loader του λειτουργικού συστήματος ο οποίος με τη σειρά του θα να ελέγξει τον πυρήνα του λειτουργικού συστήματος πριν το εκκινήσει.

Μετρημένη εκκίνηση(**Measured Boot**)
Γνωστή και ως δοκιμαστική ή αυθεντική εκκίνηση είναι μια διαδικασία η οποία σε κάθε στάδιο "μετράει" ή υπολογίζει και αποθηκεύει το hash των components του επόμενου σταδίου πριν αυτό εκτελεστεί.

Τα Secure and Measured Boot μπορούν να επεκταθούν στο λογισμικό χρόνου εκτέλεσης μέσω μηχανισμών όπως το Linux Integrity Measurement Architecture [IMA]. Το Secure Boot είναι ένα υποσύνολο μιας γενικής αρχιτεκτονικής Secure Computing, που υπαγορεύει τη συμπεριφορά της πλατφόρμας, σε αντίθεση με το Trusted Computing, το οποίο επιτρέπει στον Administrator να συμπεραίνει τη συμπεριφορά μιας πλατφόρμας. Ενώ οι εφαρμογές ασφαλούς εκκίνησης είναι σχετικά συχνές, πλήρη περιβάλλοντα Secure Computing ή Trusted Computing είναι ακόμα δύσκολο να σχεδιαστούν και εφαρμογή. Τα Secure Boot και Measured Boot έχουν ομοιότητες και μερικές διαφορές:

Ενώ το Measured Boot εξαρτάται από το TPM για την ασφαλή αποθήκευση των μετρήσεων, το Secure Boot μπορεί να υλοποιηθεί χωρίς τη χρήση της τεχνολογίας TPM. Και οι δύο τεχνικές βασίζονται σε μια ρίζα της εμπιστοσύνης στο αρχικό BIOS, αν και θα μπορούσε να γίνει η ασφαλής εκκίνηση χρησιμοποιώντας τη ρίζα της εμπιστοσύνης που παρέχεται από το Trusted Computing. Ενώ το Measured Boot δεν θα σταματήσει ένα κατεστραμμένο σύστημα από την εκκίνηση, είναι σε θέση να επαληθεύσει η κατάσταση μιας ευρύτερης περιοχής εξαρτημάτων στη διαδρομή εκκίνησης (π.χ. αρχεία διαμόρφωσης που ενδέχεται να επηρεάσουν την ασφάλεια του συστήματος, εκτός από τα εκτελέσιμα). Η ασφαλής εκκίνηση και η μέτρηση της εκκίνησης έχουν διαφορετικά προφίλ κινδύνου. Η ασφαλής εκκίνηση μπορεί να μετατρέψει ένα αθώο λάθος, όπως μια βασική αναντιστοιχία σε μια διακοπή του δικτύου με την άρνηση εκκίνησης, ενώ η μέτρηση εκκίνησης μπορεί να επιτρέψει τη συνέχιση ενός κατεστραμμένου συστατικού δικτύου ρισκάροντας για περαιτέρω ζημιές.

2.2 Οντότητες

Μία οντότητα στο TPM 2.0 είναι ένα αντικείμενο στο TPM που μπορεί άμεσα να συσχετιστεί με ένα handle. Μία μόνιμη οντότητα είναι αυτή της οποίας ο χειριστής(handle) έχει οριστεί από το TPM πρότυπο και δεν μπορεί να δημιουργηθεί η να διαγραφεί.

Το TPM 2.0 έχει 3 μόνιμες ιεραρχίες (platform, storage, and endorsement), κάθε μία από τις οποίες αναφέρεται από ένα μόνιμο χειριστή: TPM_RH_PLATFORM

(0x4000000C), TPM_RH_OWNER (0x40000001), and TPM_RH_ENDORSEMENT (x4000000B). Τα Permissions σε αυτές τις ιεραρχίες δίνονται μέσω authorizations, έτσι κάθε μία έχει και ένα authorization value και ένα policy.

2.3 Ιεραρχίες

Η ιεραρχία είναι μια συλογή από οντότητες που σχετίζονται και διαχειρίζονται ως group. Αυτές οι οντότητες είναι permanent objects (hierarchy handles), primary objects στη ρίζα του δέντρου και άλλα αντικείμενα όπως κλειδιά στο δέντρο.

Οι 3 ιεραρχίες του TPM 2 επιτρέπουν τα παρακάτω:

- Τη χρήση του TPM ως ένας cryptographic coprocessor.
- Ενεργοποίηση ή απενεργοποίηση διαφόρων συστατικών του TPM.
- Διαχωρισμό ευαίσθητων από μη ευαίσθητες εφαρμογές όσον αφορά τη μυστικότητα.

Οι 3 ιεραρχίες έχουν τα παρακάτω κοινά:

- Κάθε μια έχει μια τιμή εξουσιοδότησης και μια πολιτική.
- Κάθε μία έχει ένα flag ενεργοποίησης.
- Κάθε μια έχει ένα σπόρο από τον οποίο παράγονται κλειδιά και data objects.
- Κάθε μια μπορεί να έχει ιδιωτικά κλειδιά από τα οποία μπορούν να δημιουργηθούν απόγονοι.

2.3.1 Ιεραρχία πλατφόρμας

Η ιεραρχία της πλατφόρμας προορίζεται να βρίσκεται υπό τον έλεγχο του κατασκευαστή της πλατφόρμας, που αντιπροσωπεύεται από τον κωδικό πρώτης εκκίνησης(early boot code shipped) που αποστέλλεται με την πλατφόρμα.

2.3.2 Ιεραρχία αποθήκευσης

Η ιεραρχία αποθήκευσης προορίζεται να χρησιμοποιηθεί από τον ιδιοκτήτη της πλατφόρμας: είτε στην επιχείρηση από το τμήμα πληροφορικής ή από τον τελικό χρήστη. Η ιεραρχία αποθήκευσης είναι ισοδύναμη με την ιεραρχία αποθήκευσης του TPM 1.2. Έχει μια πολιτική του ιδιοκτητη και μια τιμή εξουσιοδότησης, όπου και οι δύο παραμένουν αμετάβλητες μέσω των επανεκκινήσεων. Η πρόθεση είναι να ρυθμιστούν και σπάνια να αλλάξουν. Η ιεραρχία μπορεί να απενεργοποιηθεί από τον ιδιοκτήτη χωρίς να επηρεάζεται η ιεραρχία πλατφόρμας. Αυτό επιτρέπει στο λογισμικό της πλατφόρμας να χρησιμοποιεί το TPM ακόμα και αν ο ιδιοκτήτης απενεργοποιήσει την ιεραρχία του. Η ιεραρχία αποθήκευσης προορίζεται για λειτουργίες που δεν επηρεάζουν την ιδιωτικότητα, ενώ η ιεραρχία εγκρίσεων, με ξεχωριστούς ελέγχους, ρυθμίζει την ιδιωτικότητα.

2.3.3 Ιεραρχία εγκρίσεων

Η ιεραρχία εγκρίσεων είναι η ιεραρχία που πρέπει να επιλεχθεί όταν ο χρήστης έχει να χειριστεί θέματα ιδιωτικότητας. Οι προμηθευτές της πλατφόρμας και του TPM πιστοποιούν ότι τα πρωτεύοντα κλειδιά σε αυτήν την ιεραρχία περιορίζονται σε ένα

αυθεντικό TPM που συνδέεται με μια αυθεντική πλατφόρμα. Όπως και με το TPM 1.2, ένα πρωτεύον κλειδί μπορεί να είναι ένα κλειδί κρυπτογράφησης. Επίσης μπορούν να δημιουργηθούν πιστοποιητικά χρησιμοποιώντας την εντολή TPM2_ActivateCredential. Σε αντίθεση με το TPM 1.2, ένα πρωτεύον κλειδί μπορεί επίσης να είναι ένα κλειδί υπογραφής. Δημιουργία και πιστοποίηση τέτοιων κλειδιών είναι ευαίσθητη διαδικασία όσον αφορά την προστασία της ιδιωτικότητας, διότι επιτρέπει τη συσχέτιση των κλειδιών πίσω σε ένα ενιαίο TPM.

2.3.4 Ιεραρχία NULL

Η ιεραρχία NULL είναι ανάλογη με τις τρεις ιεραρχίες. Μπορεί να έχει πρωτεύοντα κλειδιά από τα οποία μπορούν να δημιουργηθούν οι απόγονοι. Πολλές ιδιότητες είναι διαφορετικές:

• Η τιμή εξουσιοδότησης είναι κωδικός πρόσβασης μηδενικού μήκους και η πολιτική είναι άδεια (δεν μπορεί να ικανοποιηθεί). Αυτά δεν μπορούν να αλλάξουν.
• Δεν μπορεί να απενεργοποιηθεί.
• Έχει έναν σπόρο από τον οποίο μπορούν να εξαχθούν κλειδιά και αντικείμενα δεδομένων.

2.4 Primitives

2.4.1 Digest Primitives

Το TPM 2.0 προσφέρει δύο πρωτότυπα API κρυπτογράφησης.
Η απλούστερη αλλά λιγότερο ευέλικτη επιλογή είναι η TPM2_Hash. Ο καλών εισάγει το μήνυμα και το TPM επιστρέφει το digest. Το μήκος του μηνύματος περιορίζεται από το μέγεθος του buffer της εισόδου TPM, συνήθως 1 ή 2 KB. Το άλλο API εφαρμόζει το συνηθισμένο πρότυπο εκκίνησης / ενημέρωσης / ολοκλήρωσης χρησιμοποιώντας τις εντολές TPM2_HashSequenceStart, TPM2_SequenceUpdate και TPM2_SequenceComplete.

2.4.2 HMAC Primitives

Το TPM 2.0 υποστηρίζει το HMAC ως πρωταρχικό, ενώ το TPM 1.2 προσφέρει μόνο το υποκείμενο digest API. Το κλειδί HMAC είναι ένα φορτωμένο, κλειδωμένο, κατακερματισμένο TPM αντικείμενο. Για ένα περιορισμένο(restricted) κλειδί, θα πρέπει να χρησιμοποιηθεί ο αλγόριθμος του κλειδιού. Για ένα κλειδί χωρίς περιορισμούς(unrestricted), ο καλών μπορεί να αντικαταστήσει τον αλγόριθμο του κλειδιού. Όπως συμβαίνει με οποιοδήποτε κλειδί, είναι διαθέσιμο το πλήρες πλήθος των μεθόδων εξουσιοδότησης. Όπως και με τα digests, υπάρχουν τόσο απλά όσο και πλήρως ευέλικτα API. Το TPM2_HMAC είναι το πιο απλό API. Με την εισαγωγή ενός ένα handle του κλειδιού, ενός digest αλγόριθμου και ενός μηνύματος και το TPM επιστρέφει το HMAC. Το άλλο API εφαρμόζει και πάλι το συνηθισμένο πρότυπο εκκίνησης / ενημέρωσης / ολοκλήρωσης, χρησιμοποιώντας τις εντολές TPM2_HMAC_Start, TPM2_SequenceUpdate και TPM2_SequenceComplete.

2.4.3 RSA Primitives

Δύο εντολές προσφέρουν τις λειτουργίες RSA: TPM2_RSA_Encrypt και TPM2_RSA_Decrypt. Και οι δύο λειτουργούν με ένα φορτωμένο κλειδί RSA. Και τα δύο επιτρέπουν διάφορα σχήματα padding: PKCS # 1, OAEP, και χωρίς padding. Το φορτωμένο κλειδί δεν μπορεί να αντικατασταθεί. Ο καλών μπορεί, ωστόσο, να καθορίσει ένα σχήμα padding εάν το σχήμα(scheme)του κλειδιού είναι μηδενικό. Το TPM2_RSA_Decrypt είναι λειτουργία ιδιωτικού κλειδιού. Το κλειδί αποκρυπτογράφησης πρέπει να είναι εξουσιοδοτημένο και το padding επικυρώνεται και αφαιρείται πριν το TPM επιστρέψει το απλό κείμενο.Το TPM2_RSA_Encrypt είναι η λειτουργία δημόσιου κλειδιού. Πρέπει το κλειδί και το μήνυμα να είναι προσδιορισμένα αλλά δεν απαιτείται άδεια για αυτήν τη λειτουργία δημόσιου κλειδιού. Το padding προστίθεται πριν από την κρυπτογράφηση.

2.4.4 Symmetric Key Primitives

Το TPM2_EncryptDecrypt επιτρέπει στο TPM να πραγματοποιεί συμμετρική κρυπτογράφηση και αποκρυπτογράφηση. Η λειτουργία είναι κατάλληλη για μικρό αριθμό μπλοκ λόγω του μέγεθος της εισόδου του buffer του TPM. Ωστόσο, το API περιλαμβάνει ένα διάνυσμα αρχικοποίησης (IV) στην είσοδο και μια chaining value στην έξοδο, έτσι ώστε ένας μεγαλύτερος αριθμός μπλοκ να μπορεί να λειτουργήσει σε parts. Όπως και με ένα κλειδί HMAC, ένα restricted κλειδί έχει σταθερή λειτουργία. Ο καλών μπορεί να καθορίσει το mode κατά τη χρήση ενός κλειδιού χωρίς περιορισμούς. Το κλειδί πρέπει να είναι ένα συμμετρικό αντικείμενο κρυπτογράφησης. Πρέπει να είναι authorized και το πλήρες σετ επιλογών εξουσιοδότησης είναι διαθέσιμο. Η κρυπτογράφηση συμμετρικού κλειδιού είναι ένα ευαίσθητο θέμα. Παρόλο που το TPM δεν είναι πολύ γρήγορο, τα δικά του προστατευμένα στο hardware κλειδιά είναι πολύ ασφαλέστερα από τα κλειδιά λογισμικού.

2.5 TPM και κρυπτογραφικά κλειδιά

Σε μια συσκεύη ασφάλειας όπως το TPM, η ικανότητα να χρησιμοποιεί κλειδιά κρατώντας τα ταυτόχρονα ασφαλή στο hardware, είναι το δυνατό σημείο του TPM. Το TPM μπορεί να παράξει και να εισάγει κλειδιά που εχουν δημιουργηθεί εκτός του TPM. Υποστηρίζει συμμετρικά και ασύμετρα κλειδιά. Επίσης το TPM ως συσκευή περιορισμένης μνήμης λειτουργεί ως key cache όπου οι εφαρμογές μπορούν να εναλλάσουν κλειδιά εκτός και εντός του TPM όποτε χρειάζεται. Υπάρχουν 3 ιεραρχίες κλειδιών υπό τον έλεγχο διαφορετικών ρόλων ασφαλείας και κάθε μία από αυτές μπορούν να σχηματίσουν δέντρα κλειδιών τα οποία έχουν σχέση γονέα παιδιού.

2.5.1 Τύποι και ιδιότητες κλειδιών

Κάθε κλειδί έχει ιδιότητες, οι οποίες έχουν οριστεί στη δημιουργία. Περιλαμβάνουν τα εξής:

- Χρήση, όπως υπογραφή ή κρυπτογράφηση.
- Συμμετρικά ή ασύμμετρα, και ο αλγόριθμος.
- Περιορισμοί στην αναπαραγωγή αντιγράφων (duplication).

- Περιορισμοί στη χρήση.

Παρακάτω αναφέρονται τα κλειδιά του TPM.

α) **Endorsement Key (EK).** Το Endorsement Key αποτελεί μοναδική ταυτότητα της πλατφόρμας, το δημιουργεί ο κατασκευαστής σε ασφαλές περιβάλλον είναι non-migratable και είναι αποθηκευμένο μέσα στο τσιπ και δεν μπορεί να αφαιρεθεί.
β) **Storage Root Key (SRK).** Είναι 2048 bit RSA κλειδί και βρίσκεται στη κορυφαία ιεραρχία του TPM. Δημιουργείται κατά τη διάρκεια της ανάληψης ιδιοκτησίας είναι non-migratable, είναι αποθηκευμένο μέσα στο τσιπ, και μπορεί να αφαιρεθεί.

γ) **Storage Keys.** Είναι RSA κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση άλλων στοιχείων στην ιεραρχία των κλειδιών TPM. Δημιουργούνται κατά την αρχικοποίηση του χρήστη.

δ) **Signature Keys.** Είναι κλειδιά RSA που χρησιμοποιούνται για υπογραφές.

2.5.2 Δημιουργία κλειδιών

Το TPM δημιουργεί ζεύγη κλειδιών RSA καθώς και συμμετρικά κλειδιά. Η λειτουργία δημιουργίας είναι προστατευμένη και το ιδιωτικό κλειδί κρατιέται σε απροσπέλαστη θέση. Η παραγωγή κλειδιών παράγει δύο διαφορετικούς τύπους κλειδιών.

Το πρώτο, ένα συνηθισμένο κλειδί, παράγεται με τη χρήση της γεννήτριας τυχαίων αριθμών (RNG) για να παράξει το σπόρο του υπολογισμού. Το αποτέλεσμα του υπολογισμού είναι μια τιμή μυστικού κλειδιού που διατηρείται σε προστατευμένη τοποθεσία.

Ο δεύτερος τύπος, ένα πρωτεύον κλειδί, προέρχεται από μια τιμή σπόρου, όχι από το RNG απευθείας. Το RNG συνήθως δημιουργεί τους σπόρους που αποθηκεύονται μόνιμα στο TPM. Η δημιουργία ενός πρωτεύοντος κλειδιού από έναν σπόρο βασίζεται στη χρήση μιας εγκεκριμένης συνάρτησης εξαγωγής κλειδιών (KDF).

Το KDF που ορίζεται στο SP800-108 χρησιμοποιείται ευρέως σε αυτή την προδιαγραφή.

Αυτή η προδιαγραφή δεν θέτει κανένα ανώτερο όριο στο χρόνο που επιτρέπεται να παράγει ένα κλειδί. Οι προδιαγραφές για την πλατφόρμα ενδέχεται να περιορίζουν τον χρόνο δημιουργίας διαφόρων τύπων κλειδιών.

Ανάλογα με την εφαρμογή, το TPM μπορεί να δημιουργήσει ένα κλειδί είτε

• χρησιμοποιώντας bits από το RNG, ή

• εξαγωγή του κλειδιού από μια άλλη μυστική τιμή.

2.5.3 Εντολές κλειδιών

Εντολές κλειδιών είναι οι παρακάτω:

TPM2_Create και TPM2_CreatePrimary: Δημιουργούν όλους τους τύπους κλειδιών από templates.
TPM2_Load (για wrapped private keys) και **TPM2_LoadExternal** (για δημόσια κλειδιά και πιθανόν ιδιωτικά) Φορτώνουν κλειδιά στο TPM.

TPM2_ContextSave και **TPM2_ContextLoad:** χρησιμοποιούνται για την ανταλλαγή κλειδιών στην TPM key cache.
TPM2_FlushContext: διαγράφει ένα κλειδί από το TPM.
TPM2_EvictControl: μπορεί να κάνει persistent ένα κλειδί που είναι φορτωμένο στο TPM.
Οι εντολές **TPM2_Unseal, TPM2_RSA_Encrypt,** και **TPM2_RSA_Decrypt** χρησιμοποιούν κλειδιά κρυπτογράφησης.
Οι εντολές **TPM2_HMAC, TPM2_HMAC_Start, TPM2_SequenceUpdate,** και **TPM2_SequenceCompete** χρησιμοποιούν συμμετρικά κλειδιά για ψηφιακές υπογραφές και keyed-hash message authentication code (HMAC) αλγόριθμο.
TPM2_Sign: είναι γενικού σκοπού εντολή υπογραφής.
TPM2_VerifySignature: επιβεβαιώνει την ψηφιακή υπογραφή.
TPM2_Certify, TPM2_Quote, TPM2_GetSessionAuditDigest,TPM_GetTime: είναι ειδικές εντολές ψηφιακής υπογραφής που υπογράφουν δομές attestation. Συγκεκριμένα η εντολή TPM2_Certify μπορεί να χρησιμοποιηθεί ώστε το TPM κλειδί να υπογράψει ένα άλλο κλειδί (συγκεκριμένα το όνομα του). Έτσι το TPM μπορεί να χρησιμοποιηθεί ως certificate authority, όπου το issuer key βεβειώνει τις ιδιότητες του subject key.

2.5.4 Εξουσιοδότηση κλειδιού Key Authorization

Αν και η προστασία του υλικού από ιδιωτικά ή συμμετρικά κλειδιά από μόνη της αποτελεί σημαντική βελτίωση σε σχέση με τα κλειδιά που παράγονται από το λογισμικό, το TPM προσφέρει επίσης ισχυρό έλεγχο πρόσβασης. Ένα κλειδί που παράγεται από λογισμικό συχνά χρησιμοποιεί έναν κωδικό πρόσβασης για τον έλεγχο πρόσβασης, για να προστατεύσει το κλειδί. Για παράδειγμα, το μυστικό κλειδί μπορεί να κρυπτογραφηθεί με κωδικό πρόσβασης. Αυτή η προστασία είναι τόσο ισχυρή όσο ο κωδικός πρόσβασης, και το μυστικό κλειδί είναι ευάλωτο σε offline hammering attack. Δηλαδή, αν κάποτε ο επιτιθέμενος αποκτήσει το κρυπτογραφημένο κλειδί, η εξαγωγή του κλειδιού εξαρτάται από το σπάσιμο του κωδικού πρόσβασης. Ο ιδιοκτήτης του κλειδιού δεν μπορεί να αποτρέψει μια επίθεση υψηλής ταχύτητας με απεριόριστο αριθμό κωδικών πρόσβασης.

Αυτή η επίθεση μπορεί να παραλληλισθεί, με πολλούς υπολογιστές να δοκιμάζουν διαφορετικούς κωδικούς πρόσβασης ταυτόχρονα. Το σύννεφο έχει καταστήσει αυτό το είδος της επίθεσης πολύ εφικτό.

Το TPM βελτιώνει τα κλειδιά του λογισμικού από δύο απόψεις. Πρώτον, όταν το κλειδί φεύγει από το TPM είναι περιτυλιγμένο (κρυπτογραφημένο) με ισχυρό γονικό κλειδί (κλειδί κρυπτογράφησης). Ο επιτιθέμενος πρέπει τώρα να σπάσει ένα ισχυρό κλειδί παρά έναν αδύναμο κωδικό πρόσβασης.

Δεύτερον, όταν φορτώνεται ένα κλειδί στο TPM, προστατεύεται από αυτό που αναφέρουν οι προδιαγραφές ως dictionary attack protection logic. Κάθε φορά που ένας εισβολέας δεν καταφέρει να σπάσει το κλειδί , αυτή η λογική καταγράφει την αποτυχία. Μετά από έναν ρυθμιζόμενο αριθμό αποτυχιών, το TPM αποκλείει περαιτέρω προσπάθειες για ένα ρυθμιζόμενο χρονικό διάστημα. Αυτό περιορίζει, ενδεχομένως σοβαρά, την ταχύτητα με την οποία ένας εισβολέας μπορεί να δοκιμάσει κωδικούς πρόσβασης. Ο περιορισμός του ρυθμού μπορεί να κάνει ακόμη και για ένα αδύναμο κωδικός πρόσβαση κλειδιού TPM, πολύ περισσότερο χρόνο για να σπάσει από ένα ισχυρό κλειδί λογισμικού κωδικό πρόσβασης, όπου η επίθεση δεν είναι χρονικά περιορισμένη.

2.5.5 Χαρακτηριστικά συμμετρικών και ασύμμετρων κλειδιών

Το TPM 2.0 υποστηρίζει μια ποικιλία ασύμμετρων αλγορίθμων, σε αντίθεση με το TPM 1.2, το οποίο υποστήριζε μόνο RSA. Το TPM 2.0 εισάγει επίσης ορισμένους εντελώς νέους τύπους κλειδιών.

Ένα κλειδί συμμετρικής υπογραφής μπορεί να χρησιμοποιηθεί στις εντολές TPM HMAC. Το TPM 2.0 μπορεί να κάνει συμμετρική υπογραφή (MAC) με ένα κλειδί που δεν βρίσκεται ποτέ στην εξωτερική πλευρά του TPM.

2.5.6 Χαρακτηριστικά αναπαραγωγή αντιγράφων (Duplication Attributes)

Η αναπαραγωγή αντιγράφων είναι η διαδικασία αντιγραφής ενός κλειδιού από μια θέση σε μια ιεραρχία σε μια άλλη.

Το κλειδί μπορεί να γίνει το παιδί ενός άλλου γονικού κλειδιού. Η ιεραρχία ή ο γονέας μπορεί να είναι στο ίδιο ή σε διαφορετικό TPM. Τα πρωτεύοντα κλειδιά δεν μπορούν να αντιγραφούν, είναι σταθερά στο σύστημα ιεραρχίας σε ένα TPM.

Μια βασική περίπτωση χρήσης για επικάλυψη είναι τα αντίγραφα ασφαλείας. Αν ένα κλειδί ήταν κλειδωμένο για πάντα σε ένα TPM και το TPM ή η μητρική πλακέτα του απέτυχαν, το κλειδί θα χανόταν μόνιμα.

Μια δεύτερη περίπτωση χρήσης είναι η κατανομή των κλειδιών μεταξύ πολλών συσκευών. Για παράδειγμα το κλειδί υπογραφής ενός χρήστη μπορεί να αντιγραφεί μεταξύ ενός φορητού υπολογιστή, ενός tablet και ενός κινητού τηλεφώνου.

Το TPM 1.2 έχει μια παρόμοια διαδικασία που ονομάζεται μετανάστευση. Ο όρος μετανάστευση σημαίνει ότι μετακινείται το κλειδί: δηλαδή ότι θα υπήρχε τώρα στη θέση προορισμού αλλά δεν υπάρχει πια στην πηγή. Αυτή η συνέπεια ήταν λανθασμένη. Μετά τη μετάβαση, το κλειδί θα μπορούσε να υπάρχει και στον προορισμό και στην πηγή. Για το λόγο αυτό, ο όρος TPM 2.0 άλλαξε σε duplication.

Τα κλειδιά TPM 2.0 έχουν δύο χαρακτηριστικά που ελέγχουν την αναπαραγωγή αντιγράφων. Στο ένα άκρο, ένα κλειδί μπορεί να κλειδωθεί σε ένα μόνο γονέα σε ένα TPM και ποτέ να μην αντιγράφει. Το αντίθετο άκρο είναι ένα κλειδί που μπορεί να αναπαράγεται ελεύθερα σε άλλο γονέα στο ίδιο ή άλλο TPM.

Η ενδιάμεση περίπτωση είναι ένα κλειδί περιορισμένο σε έναν γονέα αλλά αυτό να μετακινηθεί σιωπηρά αν ο γονέας μετακινηθεί. Αυτή η περίπτωση προσφέρει τη δυνατότητα αναπαραγωγής ολόκληρου του κλαδιού του δέντρου. Αν ο γονέας αναπαράγεται, όλα τα παιδιά του είναι διαθέσιμα στον προορισμό.

2.5.7 Restricted Signing Key

Ένα άλλο χαρακτηριστικό των κλειδιών υπογραφής είναι το χαρακτηριστικό περιορισμένης χρήσης. Η περίπτωση χρήσης ενός περιορισμένου κλειδιού είναι στις υπογραφές δομών πιστοποίησης TPM. Αυτές οι δομές περιλαμβάνουν Platform Configuration Register (PCR) quotes, ένα πιστοποιημένο αντικείμενο TPM, μια υπογραφή του χρόνου του TPM, ή μια υπογραφή πάνω σε ένα αρχείο ελέγχου. Η υπογραφή, είναι πάνω σε ένα digest αλλά ο επαληθευτής θέλει τη διαβεβαίωση ότι το digest δεν δημιουργήθηκε εκτός TPM πάνω από ψευδείς τιμές και δόθηκε στο TPM για

υπογραφή. Για παράδειγμα, ένα quote είναι υπογραφή πάνω σε ένα σύνολο τιμών PCR, αλλά η πραγματική διαδικασία υπογραφής υπογράφει ένα digest.

Ένας χρήστης θα μπορούσε να δημιουργήσει ένα digest οποιωνδήποτε τιμών PCR και να χρησιμοποιήσει ένα μη περιορισμένο κλειδί για να το υπογράψει.

Ο χρήστης θα μπορούσε τότε να ισχυριστεί ότι η υπογραφή ήταν ένα quote. Ωστόσο, το συμβαλλόμενο μέρος θα παρατηρούσε ότι το κλειδί δεν ήταν περιορισμένο και έτσι δεν θα εμπιστεύοταν τον ισχυρισμό. Ένα περιορισμένο κλειδί παρέχει τη διαβεβαίωση ότι η υπογραφή ήταν πάνω σε ένα digest που δημιουργήθηκε από το TPM.

Ένα περιορισμένο κλειδί υπογραφής μπορεί να υπογράψει μόνο ένα digest που παράγεται από το TPM. Αυτό είναι μια γενίκευση των κλειδιών πληροφόρησης TPM 1.2 και του κλειδιού βεβαίωσης ταυτότητας attestation identity key (AIK), τα οποία θα μπορούσαν να υπογράψουν μόνο μια εσωτερικά δημιουργημένη δομή του TPM. Για εσωτερικά δεδομένα TPM, αυτή η διαβεβαίωση είναι εύκολη, επειδή το TPM δημιουργεί το digest από τα εσωτερικά δεδομένα του κατά το χρόνο υπογραφής.

2.5.8 Restricted Decryption Key

Περιορισμένο κλειδί αποκρυπτογράφησης
Ένα restricted κλειδί αποκρυπτογράφησης είναι στην πραγματικότητα ένα κλειδί αποθήκευσης. Αυτό το κλειδί αποκρυπτογραφεί μόνο τα δεδομένα που έχουν μια συγκεκριμένη μορφή, συμπεριλαμβανομένης μιας τιμής ακεραιότητας σε σχέση με την υπόλοιπη δομή.
Μόνο αυτά τα κλειδιά μπορούν να χρησιμοποιηθούν ως γονείς για τη δημιουργία ή τη φόρτωση αντικειμένων-παιδιών ή την ενεργοποίηση μια πιστοποίησης. Αυτές οι λειτουργίες θέτουν περιορισμούς στο αποτέλεσμα της αποκρυπτογράφησης. Για παράδειγμα, η φόρτωση δεν επιστρέφει το αποτέλεσμα της αποκρυπτογράφησης.
Ένα κλειδί χωρίς περιορισμούς μπορεί να εκτελέσει μια αποκρυπτογράφηση γενικού σκοπού σε όλα τα παρεχόμενα δεδομένα και να επιστρέψει αποτέλεσμα. Εάν επιτρεπόταν να χρησιμοποιηθεί ως κλειδί αποθήκευσης, θα μπορούσε να αποκρυπτογραφήσει και να επιστρέψει το ιδιωτικό κλειδί ενός παιδιού. Εάν θα μπορούσε να χρησιμοποιηθεί σε σφραγισμένα δεδομένα, θα επέστρεφε τα δεδομένα χωρίς να ελέγχεται η εξουσιοδότηση.

2.5.9 Πιστοποίηση

Το TPM μπορεί βεβαίως να ενεργεί ως αρχή πιστοποίησης. Το ιδιωτικό κλειδί υπογραφής προστατεύεται από το υλικό και ένα ευρύ φάσμα επιλογών εξουσιοδότησης, αλλά μπορεί εύκολα να δημιουργηθεί αντίγραφο ασφαλείας. Αυτό προσφέρει πολύ καλύτερη προστασία από ένα κλειδί λογισμικού.
Μια έμπιστη τρίτη οντότητα (αρχή πιστοποίησης) μπορεί επίσης να υπογράψει ένα πιστοποιητικό X.509 για ένα κλειδί TPM.
Για τα κλειδιά αποκρυπτογράφησης, υπάρχει μια επιπλοκή λόγω μιας τυπικής απαίτησης της αρχής πιστοποίησης(CA) για απόδειξη κατοχής.
Ο αιτών του πιστοποιητικού πρέπει να προσκομίσει αποδεικτικά στοιχεία στην αρχή πιστοποίησης ότι κατέχει ιδιωτικό κλειδί. Αυτό γίνεται συνήθως με την αυτόματη υπογραφή της αίτησης υπογραφής πιστοποιητικού certificate signing request (CSR).

Για τα κλειδιά αποκρυπτογράφησης, το TPM δεν μπορεί απλώς να υπογράψει το CSR, επειδή αυτά τα κλειδιά είναι περιορίσμένα μόνο να αποκρυπτογραφούν και δεν μπορούν να υπογράψουν. Το TPM έχει μια λύση αλλά αυτό απαιτεί μια μη τυπική αρχή πιστοποίησης.
Λιγότερο προφανές είναι ότι το TPM μπορεί να πιστοποιεί δεδομένα που βρίσκονται στη συσκευή. Το TPM προσφέρει αρκετές εντολές για να υποστηρίξει αυτό το χαρακτηριστικό. Η εντολή TPM2_Certify δηλώνει ότι ένα αντικείμενο που έχει όνομα είναι φορτωμένο στο TPM. Επειδή το όνομα αντιπροσωπεύει κρυπτογραφικά τον δημόσιο χώρο του αντικειμένου, κάποιος μπορεί να διαβεβαιωθεί ότι το αντικείμενο έχει ένα συσχετιζόμενο ιδιωτικό μέρος. Το όνομα περιλαμβάνει επίσης ιδιότητες του κλειδιού συμπεριλαμβανομένου του εάν είναι περιορισμένο, αν έχει οριστεί σε γονέα ή έχει οριστεί σε TPM και την πολιτική εξουσιοδότησης.

2.6 NV Indexes

Το TPM απαιτεί τη χρήση μη πτητικής μνήμης για δύο γενικές κατηγορίες δεδομένων:

- Δομές δεδομένων που ορίζονται από την αρχιτεκτονική TPM.
- Μη δομημένα δεδομένα που ορίζονται από έναν χρήστη ή από μια συγκεκριμένη πλατφόρμα

Προσδιορισμός
Μία χρήση της μη πτητικής μνήμης TPM είναι για δεδομένα ή πεδία που ορίζονται στην προδιαγραφή βιβλιοθήκης TPM. Αυτό περιλαμβάνει τιμές εξουσιοδότησης ιεραρχίας, τους σπόρους, και τις αποδείξεις και τα ιδιωτικά δεδομένα που το TPM δεν θα αποκαλύψει προς τα έξω(εκτός TPM).
Περιλαμβάνει επίσης μετρητές, ρολόι και άλλα: μη πτητικά δεδομένα που ο καλών μπορεί να διαβάσει.
Η μη πτητική μνήμη μπορεί επίσης να κρατήσει δομημένα δεδομένα που γίνονται επίμονα, όπως ένα κλειδί.
Το TPM 2.0 διαθέτει τέσσερις τύπους ευρετηρίων NV: συνήθεις (μη δομημένα δεδομένα), πεδίο bit, μετρητής,και εκτεταμένους δείκτες δεδομένων. Ένας δείκτης μπορεί να διαβαστεί ή να γραφτεί χρησιμοποιώντας τον κωδικό πρόσβασης και τους ελέγχους πολιτικής του πρότυπου TPM. Οι υβριδικοί δείκτες υπάρχουν συνήθως σε πτητική μνήμη, αλλά ο κανονικός τερματισμός λειτουργίας μπορεί να τα αποθηκεύσει στη μνήμη NV.

2.6.1 NV Ordinary Index

Ένας **συνηθισμένος** δείκτης είναι όπως ο αντίστοιχος δείκτης στο TPM 1.2. Διαθέτει μη δομημένα δεδομένα αυθαίρετου μήκους. Σε αντίθεση με τον μετρητή, το πεδίο bit και τα ευρετήρια επέκτασης, δεν υπάρχει περιορισμός στον τύπο των δεδομένων που μπορούν να γραφτούν.

2.6.2 NV Counter Index

Ένας μετρητής NV είναι μια τιμή 64-bit που μπορεί μόνο να αυξηθεί. Στην αρχή της πρώτης increment εντολής, αρχικοποιείται στην μεγαλύτερη τιμή που έχει ποτέ ο μετρητής στο TPM. Αυτό περιλαμβάνει τα τωρινά ευρετήρια και τους μετρητές που

έχουν οριστεί στο παρελθόν, αλλά δεν βρίσκονται πλέον στο TPM. Έτσι, ένας μετρητής δεν μπορεί ποτέ να γυρίσει πίσω, ακόμα και στην περίπτωση της διαγραφής και της επαναδημιουργίας του ευρετηρίου.

2.6.3 NV Δείκτης πεδίου bit

Ένας δείκτης πεδίου bit περιέχει 64 bits, αρχικοποιείται σε όλα τα bits χωρίς τιμές στην αρχή της πρώτης εγγραφής.

2.6.4 NV Extend Index

Ένας δείκτης επέκτασης ορίζεται με έναν συγκεκριμένο αλγόριθμο κατακερματισμού και είναι σταθερός για τη διάρκεια ζωής του δείκτη. Το μέγεθος δεδομένων του ευρετηρίου βασίζεται στον αλγόριθμο κατακερματισμού του. Αρχικοποιείται σε μηδέν πριν από την πρώτη εγγραφή. Η εγγραφή είναι μια επέκταση, παρόμοια με αυτή που εκτελείται σε ένα PCR.

2.6.5 Υβριδικό ευρετήριο

Όπως και με ένα μη υβριδικό, τα μεταδεδομένα του δείκτη NV (δείκτης χειρισμού του, μέγεθος, χαρακτηριστικά, πολιτική και ο κωδικός πρόσβασης) είναι μη πτητικά.Τα δεδομένα δημιουργούνται σε πτητική μνήμη. Εκτός από τους υβριδικούς μετρητές τα δεδομένα του δείκτη γράφονται μόνο στη μνήμη NV σε περίπτωση κανονικού τερματισμού. Οποιοσδήποτε από τους τέσσερις τύπους ευρετηρίου (συνήθης, μετρητής, πεδίο bit, ή επέκταση) μπορεί να είναι ένας υβριδικός δείκτης.

2.7 Authorizations και sessions

Οι εξουσιοδοτήσεις και οι συνεδρίες είναι από τις πιο σημαντικές έννοιες του TPM 2.0. Οι εξουσιοδοτήσεις ελέγχουν την πρόσβαση σε οντότητες του TPM, παρέχοντας αυξημένη ασφάλεια. Οι συνεδρίες είναι το όχημα για τις εξουσιοδοτήσεις και τη διατήρηση της κατάστασης μεταξύ των επόμενων εντολών. Επιπρόσθετα, οι συνεδρίες καθορίζουν μερικά ανά εντολή χαρακτηριστικά όπως κρυπτογράφηση και αποκρυπτογράφηση παραμέτρων εντολής και απόκρισης.

Υπάρχουν 3 τύποι συνόδων: η σύνοδος με κωδικό πρόσβασης, η σύνοδος HMAC και η σύνοδος πολιτικών.

Και οι τρεις τύποι συνόδων αποτελούν μέσο για την έγκριση ενεργειών και, στην περίπτωση του HMAC και των συνεδριών πολιτικής, διαμορφώνουν τις περιόδους λειτουργίας ανά εντολή.Οι Συνεδρίες κωδικού πρόσβασης είναι ο απλούστερος τύπος εξουσιοδότησης: ένας κωδικός πρόσβασης διαβιβιάζεται στο TPM να εγκρίνει μια ενέργεια. Αυτό έχει προφανή ζητήματα ασφαλείας, εάν η πρόσβαση στο TPM γίνεται απομακρυσμένα. Η χρήση των συνθηκών κωδικού πρόσβασης προορίζεται για τοπική πρόσβαση.

2.7.1 Παραλλαγές δημιουργίας συνόδων

Αυτές ορίζονται κατά το χρόνο δημιουργίας της συνόδου και διαρκούν για όλη τη σύνοδο. Προσδιορίζουν τον τρόπο με τον οποίο τα κλειδιά συνόδου και τα κλειδιά HMAC δημιουργούνται και το πώς παράγεται το HMAC. Υπάρχουν δύο επιλογές εδώ: bound vs. unbound, και salted vs. unsalted. Ο συνδυασμός αυτών των δύο επιλογών έχει ως αποτέλεσμα τέσσερις παραλλαγές της συνεδρίας:

- Οι δεσμευμένες(bound) συνεδρίες ουσιαστικά "δεσμεύουν" την εξουσιοδότηση στην τιμή εξουσιοδότησης της συνεδρίας. Αυτή η δέσμευση γίνεται με τη συμπερίληψη της δεσμευμένης τιμής εξουσιοδότησης της οντότητας στη συνεδρία δημιουργίας κλειδιού.
- Μια μη δεσμευμένη(unbound) συνεδρία δεν χρησιμοποιεί την δεσμευμένη εξουσιοδότηση της οντότητας στη συνεδρία δημιουργίας κλειδιού.
- Μια salted συνεδρία προσθέτει επιπλέον εντροπία, το αλάτι(salt), στη συνεδρία παραγωγής κλειδιών παρόμοια με τις δεσμευμένες συνεδρίες. Αυτό επηρεάζει όλους τους υπολογισμούς που εξαρτώνται από το κλειδί συνόδου. Η επιπλέον εντροπία αποστέλλεται στο TPM σε κρυπτογραφημένη μορφή, η κρυπτογραφημένη παράμετρος του αλατιού που διαβιβάζεται στην εντολή TPM2_StartAuthSession.
- Μια unsalted συνεδρία δεν προσθέτει την εντροπία με αυτόν τον τρόπο.

2.7.2 Τροποποιητές χρήσης συνόδων

Αυτοί τροποποιούν τις ενέργειες της HMAC ή της πολιτικής συνόδου ανά εντολή. Continue, encrypt, decrypt, και audit είναι οι πιο συχνά χρησιμοποιούμενοι τροποποιητές:

- Continue: Εάν δεν έχει οριστεί, η συνεδρία τερματίζεται μετά από μια επιτυχημένη εντολή.
- Decrypt: Υποδεικνύει ότι η πρώτη παράμετρος της εντολής TPM2B αποστέλλεται στο TPM σε κρυπτογραφημένη μορφή.
- Encrypt: προκαλεί την πρώτη παράμετρο απόκρισης TPM2B να επιστραφεί από το TPM σε κρυπτογραφημένη μορφή.
- Audit: Προκαλεί μια εντολή χρησιμοποιώντας τη συνεδρία που πρόκειται να ελεγχθεί.

Οι εξουσιοδοτήσεις HMAC είναι ένας τρόπος χρήσης ενός απλού κωδικού πρόσβασης με ασφαλέστερο τρόπο.

Μόλις η εφαρμογή και το TPM συμφωνήσουν για τον κωδικό πρόσβασης (τη στιγμή δημιουργίας της οντότητας ή τροποποίησης της τιμής εξουσιοδότησης), δεν υπάρχει ποτέ ανάγκη επανυποβολής του κωδικού πρόσβασης.

Αυτή η εφάπαξ επικοινωνία του κωδικού πρόσβασης στο TPM μπορεί να επιτευχθεί με έναν ασφαλή τρόπο: ο κωδικός πρόσβασης μπορεί να διαβιβαστεί στο TPM σε κρυπτογραφημένη μορφή. Η συνεδρία HMAC επιτυγχάνει αυτό το επιπλέον επίπεδο ασφάλειας χρησιμοποιώντας τον κωδικό πρόσβασης (authValue, όπως ονομάζεται στη προδιαγραφή TPM 2.0) ως μία από τις εισόδους ενός HMAC που υπολογίζεται στις εντολές και στις αποκρίσεις.

Σε μια εντολή, η εφαρμογή κλήσης υπολογίζει το HMAC και το εισάγει στην ροή byte της εντολής. Όταν το TPM λάβει την ροή byte της εντολής, αν το TPM καθορίζει ότι το HMAC έχει υπολογιστεί σωστά, η ενέργεια είναι εγκεκριμένη. Σε μια απόκριση, το TPM υπολογίζει το HMAC της απόκρισης και το εισάγει στο byte stream της απόκρισης.

Ο καλών υπολογίζει το HMAC της απόκρισης και το συγκρίνει με το πεδίο HMAC της ροής byte της απάντησης. Εάν ταιριάζουν, η απόκριση είναι αξιόπιστη. Όλα αυτά λειτουργούν μόνο εάν η εφαρμογή και το TPM γνωρίζουν και συμφωνούν στη τιμή AuthValue.

Οι συνεδρίες HMAC χρησιμοποιούν δύο nonces, ένα από τον καλούντα (nonceCaller) και ένα από το TPM (nonceTPM) για την αποτροπή επιθέσεων επανάληψης. Αυτά τα nonces περιλαμβάνονται στον υπολογισμό του HMAC.

Επειδή το nonceTPM αλλάζει για κάθε εντολή που αποστέλλεται και η καλούσα εφαρμογή μπορεί, εάν το επιθυμεί, να αλλάξει το nonceCaller σε κάθε εντολή, ένας εισβολέας δεν μπορεί να επαναλάβει τις ροές byte της εντολής.

Αναπαραγόμενα ρεύματα byte εντολών που χρησιμοποιούν HMAC εξουσιοδότηση θα αποτύγχάνουν πάντοτε επειδή τα nonces θα είναι διαφορετικά στο replay.

Οι συνεδρίες HMAC διατηρούν την κατάσταση κατά τη διάρκεια της συνεδρίας και μπορούν να χρησιμοποιηθούν για εξουσιοδότηση πολλαπλών ενεργειών σε οντότητες TPM. Μια συνεδρία HMAC ξεκινά χρησιμοποιώντας την TPM2_StartAuthSession εντολή. Όταν ξεκινήσει, μπορούν να διαμορφωθούν οι συνεδρίες HMAC ως bound vs. unbound και salted vs. unsalted συνεδριών. Ο συνδυασμός αυτών των δύο επιλογών έχουν ως αποτέλεσμα τέσσερις παραλλαγές συνεδριών HMAC. Αυτές οι τέσσερις παραλλαγές καθορίζουν το πώς υπολογίζονται το κλειδί συνόδου και τα HMACs.

Ακολουθεί πίνακας με σύγκριση των 3 τύπων συνόδων.

Πίνακας 1: Σύγκριση των 3 τύπων συνόδων

	Password	HMAC	Policy
State/Other Info	No state is maintained between subsequent uses.	State is maintained for the lifetime of the session.	State is maintained for the lifetime of the session. Built on top of HMAC sessions.
Security	The password is in the clear on every command; a snooper could easily grab the password.	Much more secure than a password (especially when sending commands to remote a TPM). Nonces are used to prevent replay attacks.	Enhanced security by allowing complex sequences of commands and internal and external states to authorize. Nonces are used to prevent replay attacks if an HMAC is being used.
Method of Starting	None	`TPM2_StartAuthSession`	`TPM2_StartAuthSession`
Per-Command Session Modifiers	None	Decrypt, encrypt, audit	Decrypt and encrypt

Η ίδια η προδιαγραφή TPM 2.0 συχνά επικαλύπτει τους όρους session και authorization.

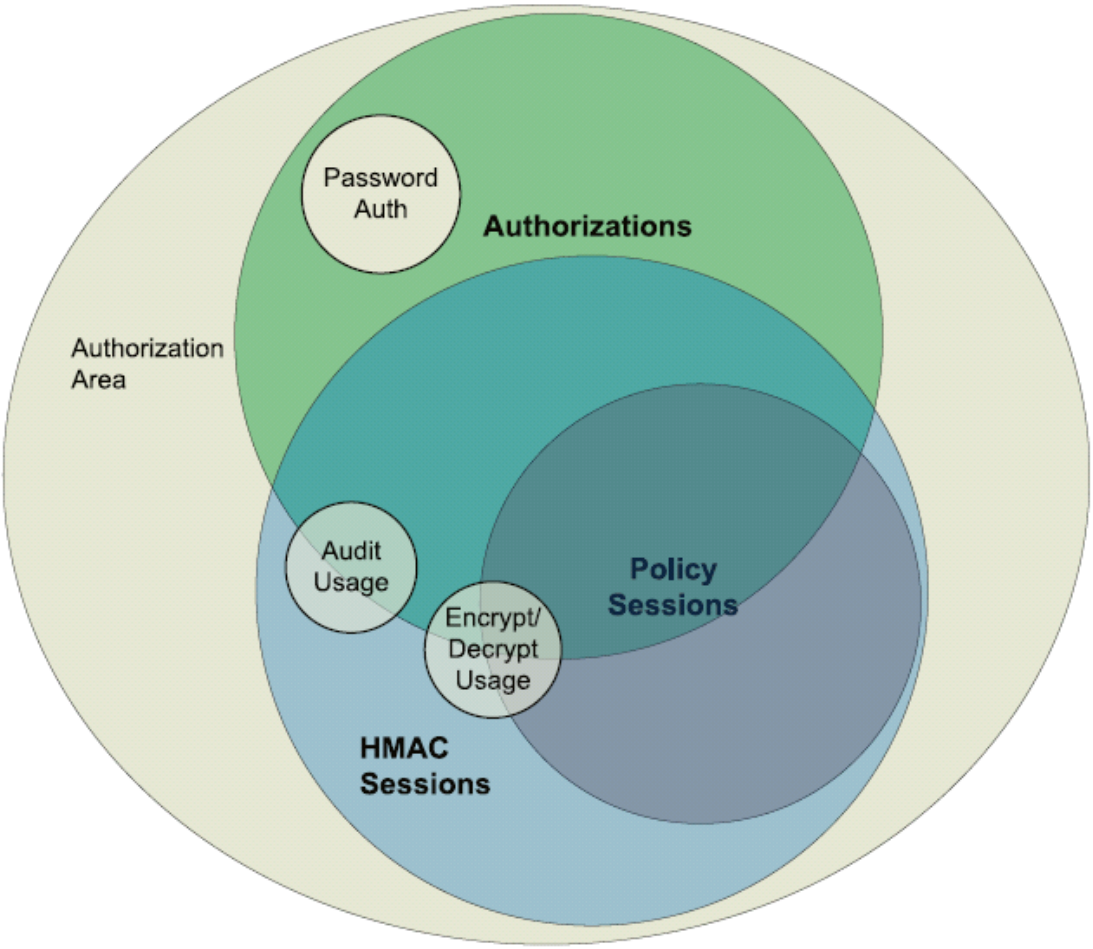
Ακολουθούν μερικά παραδείγματα από την προδιαγραφή:

• Η περιοχή εξουσιοδότησης στις εντολές χρησιμοποιείται και για session και για authorization. Αλλά οι συνεδρίες μπορούν να χρησιμοποιηθούν με τρόπους που δεν έχουν καμία σχέση με την εξουσιοδότηση. Για παράδειγμα, μπορεί να χρησιμοποιηθούν για να ρυθμίσουν την κρυπτογράφηση και την αποκρυπτογράφηση εντολών και των παραμέτρων απόκρισης και να επιτρέπουν το auditing των εντολών. Οι συνεδρίες που δεν έχουν καμία σχέση με την εξουσιοδότηση μπορούν να χρησιμοποιηθούν για τους σκοπούς αυτούς.

• Οι ετικέτες TPM_ST_NO_SESSIONS και TPM_ST_SESSIONS χρησιμοποιούνται για να υποδείξουν εάν υπάρχει περιοχή εξουσιοδότησης σε μια εντολή.

• Οι σύνοδοι ξεκινούν με την εντολή TPM2_StartAuthSession.Το όνομα της εντολής υποδεικνύει ότι αρχίζει η εξουσιοδότηση, αλλά στην πραγματικότητα μια συνεδρία αρχίζει με αυτή την εντολή. Η συνεδρία μπορεί ποτέ να μην χρησιμοποιηθεί για εξουσιοδότηση.

• Μια άλλη περίπτωση είναι οι εξουσιοδοτήσεις κωδικού πρόσβασης. Από τεχνικής άποψης είναι συνεδρίες, αλλά δεν διατηρείται καμία κατάσταση μεταξύ των επόμενων εντολών, και το TPM2_StartAuthSession δεν χρησιμοποιείται για την εκκίνηση της συνεδρίας κωδικού πρόσβασης. Η εξουσιοδότηση κωδικού πρόσβασης είναι one-shot εξουσιοδότηση που ισχύει μόνο για μία εντολή.



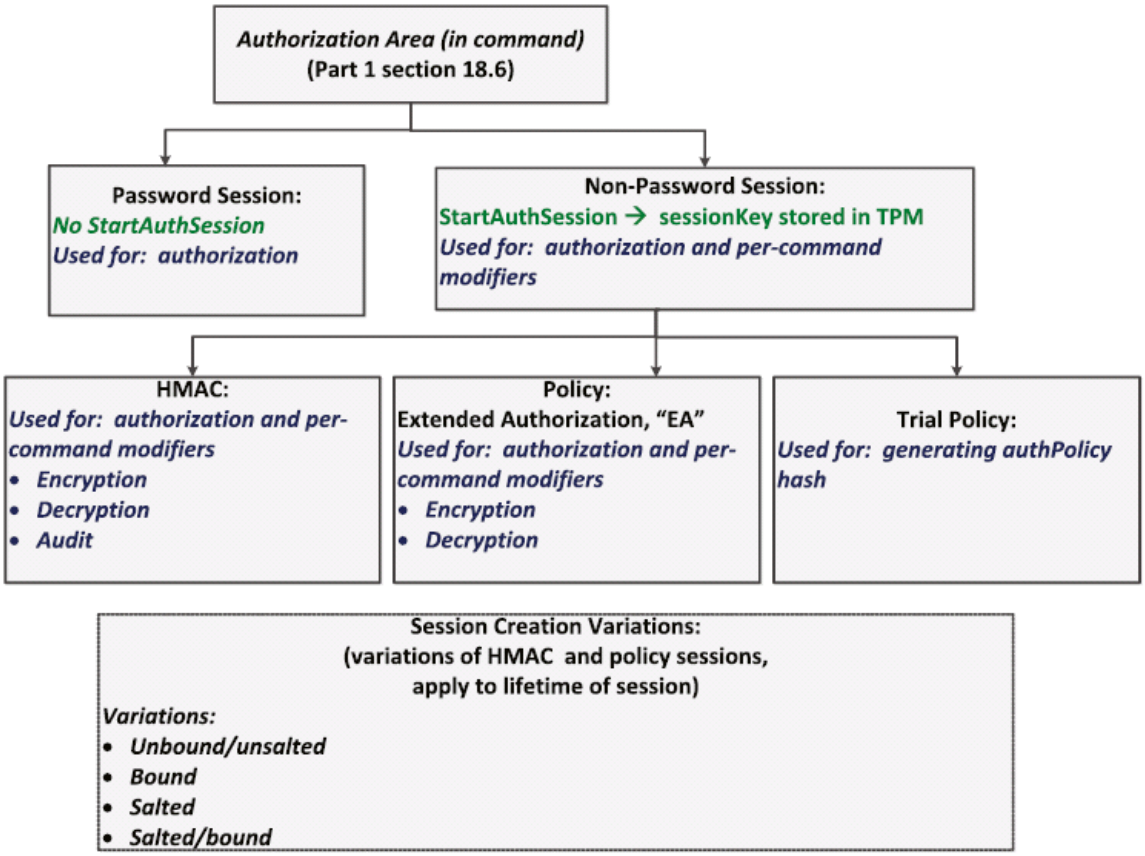
Εικόνα 4: Venn διάγραμμα για Authorizations και sessions

Στο παραπάτω διάγραμμα παρατηρούμε τα εξής:

- Οι εξουσιοδοτήσεις μπορούν να είναι κωδικός πρόσβασης, HMAC ή πολιτική εξουσιοδότησης.
- Οι εξουσιοδοτήσεις κωδικού πρόσβασης δεν μπορούν ποτέ να χρησιμοποιηθούν ως τροποποιητές συνόδων.
- Οι HMAC και συνεδρίες πολιτικών μπορούν να χρησιμοποιηθούν για εξουσιοδοτήσεις αλλά μπορεί επίσης να χρησιμοποιηθούν για να θέσουν τους τροποποιητές χρήσης συνόδου πέρα από οποιαδήποτε εξουσιοδότηση. Αυτός

είναι ο λόγος για τον οποίο οι HMAC και οι συνεδρίες πολιτικών βρίσκονται στο όριο του κύκλου έγκρισης.

- Οι τροποποιητές εντολών μπορούν να χρησιμοποιηθούν στις συνεδρίες που χρησιμοποιούνται για εξουσιοδότηση καθώς και σε συνεδρίες που δεν χρησιμοποιούνται για εξουσιοδότηση, γιαυτό οι κύκλοι audit, encrypt, and decrypt βρίσκονται στο σύνορο του κύκλου εξουσιοδότησης.
- Οι συνεδρίες που δεν χρησιμοποιούνται για εξουσιοδότηση μπορούν επίσης να βρίσκονται στη περιοχή εξουσιοδότησης των ροών byte εντολής και απόκρισης.
- Οι συνεδρίες πολιτικής μπορούν να χρησιμοποιηθούν για κρυπτογράφηση ή αποκρυπτογράφηση, αλλά όχι για έλεγχο.
- Οι συνεδρίες HMAC μπορούν να χρησιμοποιηθούν για κρυπτογράφηση, αποκρυπτογράφηση ή / και έλεγχο.



Εικόνα 5: Διάγραμμα για Authorizations και sessions

Το παραπάνω διάγραμμα απεικονίζει τη σχέση κάπως διαφορετικά:

- Η περιοχή εξουσιοδότησης μπορεί να καθορίσει τις παραμέτρους για τον κωδικό πρόσβασης, HMAC ή συνεδρίες πολιτικής.
- Οι σύνοδοι που άρχισαν με την εντολή TPM2_StartAuthSession μπορεί να είναι συνεδρίες HMAC, πολιτικής ή συνεδρίες δοκιμαστικής πολιτικής.
- Οι συνεδρίες HMAC μπορούν να διαμορφωθούν ανά εντολή και να αφορούν έλεγχο, αποκρυπτογράφηση και / ή κρυπτογράφηση των συνόδων.
- Οι συνεδρίες πολιτικής μπορούν να ρυθμιστούν ανά εντολή για αποκρυπτογράφηση και / ή κρυπτογράφηση συνόδων. Δεν μπορούν να χρησιμοποιηθούν για έλεγχο.
- Οι τέσσερις παραλλαγές της συνόδου μπορούν να εφαρμοστούν σε πολιτικές HMAC ή δοκιμαστικές συνόδους πολιτικής.

2.8 Πολιτικές εκτεταμένης εξουσιοδότησης Extended Authorization (EA)Policies

Όλες οι οντότητες του TPM μπορούν να εξουσιοδοτηθούν με δύο βασικούς τρόπους. Ο πρώτος βασίζεται σε ένα κωδικό που σχετίζεται με την οντότητα όταν δημιουργείται. Ο δεύτερος είναι με μια πολιτική που συσχετίζεται με την οντότητα όταν αυτή δημιουργείται. Μια πολιτική είναι ένας τρόπος εξουσιοδότησης μια εντολής που μπορεί να αποτελείται από σχεδόν οποιαδήποτε προσέγγιση εξουσιοδότησης που μπορεί να σκεφτεί κάποιος.

Με την εκτεταμένη εξουσιοδότηση ο χρήστης μπορεί να περιορίσει μια οντότητα, ώστε να μπορεί να χρησιμοποιηθεί μόνο υπό συγκεκριμένες συνθήκες. Το σύνολο των περιορισμών σε μια οντότητα ονομάζεται πολιτική.

Η εκτεταμένη εξουσιοδότηση στο TPM δημιουργήθηκε για να λύσει το βασικό πρόβλημα της δυνατότητας διαχείρισης της εξουσιοδότησης της οντότητας TPM.

Επιτρέπει επίσης στον χρήστη να καθορίσει εξουσιοδοτήσεις που μπορούν να λύσουν τα ακόλουθα προβλήματα:

- Να επιτρέπονται πολλαπλοί βαθμοί επαλήθευσης ταυτότητας (κωδικοί πρόσβασης, βιομετρικά στοιχεία κ.λπ.).
- Να επιτρέπεται η επαλήθευση πολλών παραγόντων (απαιτούνται περισσότεροι από ένας τύπος αυθεντικοποίησης).
- Να επιτρέπεται η δημιουργία πολιτικών χωρίς τη χρήση TPM. Οι πολιτικές δεν περιέχουν μυστικά, και έτσι μπορούν να δημιουργηθούν εξ ολοκλήρου από λογισμικό.
- Επιτρέπει τη βεβαίωση της πολιτικής που σχετίζεται με μια οντότητα.
- Επιτρέπει σε πολλούς ανθρώπους ή ρόλους να ικανοποιήσουν μια πολιτική.
- Επιτρέπει τον περιορισμό των δυνατοτήτων ενός συγκεκριμένου ρόλου για ένα αντικείμενο συγκεκριμένων ενεργειών ή χρηστών.
- Διορθώνει το πρόβλημα ευθραυστότητας PCR. Στο TPM 1.2, όταν μια οντότητα ήταν κλειδωμένη σε ένα σύνολο PCR εάν οι διαμορφώσεις άλλαζαν, τότε η οντότητα δεν μπορούσε να χρησιμοποιηθούν πλέον.
- Δυνανότητα αλλαγής συμπεριφοράς μιας πολιτικής-ευκαμψία.

2.8.1 Πώς λειτουργεί η εκτεταμένη εξουσιοδότηση

Μια πολιτική είναι ένα hash που αντιπροσωπεύει ένα σύνολο αυθεντικοποιήσεις που όλες μαζί ικανοποιούν μια πολιτική. Όταν δημιουργείται μια οντότητα (για παράδειγμα, ένα κλειδί), μια πολιτική μπορεί να συσχετιστεί με αυτό.

Αυτό γίνεται σε τρία στάδια:

1. Δημιουργείται μια σύνοδος πολιτικής. Όταν η σύνοδος πολιτικής και το TPM εκκινούν, το TPM δημιουργεί μια προσωρινή μνήμη συνόδου πολιτικής για αυτή τη σύνοδο. (Το μέγεθος του buffer συνόδου πολιτικής είναι το μέγεθος του αλγόριθμου κατακερματισμού που επιλέχθηκε όταν ξεκίνησε η συνεδρία και είναι αρχικοποιημένο με μηδενικά.)

2. Ο χρήστης παρέχει μία ή περισσότερες αυθεντικοποιήσεις στο TPM, χρησιμοποιώντας εντολές TPM2_PolicyXXX. Αυτό αλλάζει τη προσωρινή μνήμη πολιτικής συνόδου. Μπορούν επίσης να ορίσουν flags στη συνεδρία που αντιπροσωπεύει τους ελέγχους πρέπει να γίνουν όταν η εντολή εκτελείται.

3. Όταν η οντότητα χρησιμοποιείται σε μια εντολή, το TPM συγκρίνει τη πολιτική που σχετίζεται με την οντότητα με την τιμή στη συνεδρία πολιτικής. Αν δεν είναι οι ίδιες, η εντολή δεν θα είναι εκτελέσει. Οι πολιτικές δεν περιέχουν μυστικά. Ως αποτέλεσμα, όλες οι πολιτικές μπορούν να δημιουργηθούν σε λογισμικό εκτός TPM. Ωστόσο, το TPM πρέπει να είναι σε θέση να αναπαράγει πολιτικές για να τις χρησιμοποιήσει.

2.9 TCG Specifation

Παρακάτω παρουσιάζονται 2 εκδόσεις του TPM. Η έκδοση 1.2 και η έκδοση 2.

2.9.1΄Έκδοση 1.2

Η έκδοση 1.2 αποτελείται από 3 μέρη.

- Μέρος 1: Design Principles
- Μέρος 2: TPM Structures
- Μέρος 3: Commands

Σενάρια χρήσης TPM

Identification

Η χρήση που προβλέπεται για το πρώτο ενσωματωμένο κύκλωμα ασφαλείας είναι η αναγνώριση συσκευής (DeviceID).

Οι έξυπνες κάρτες χρησιμοποιούν τα κλειδιά τους για αυτό το σκοπό. Το ιδιωτικό κλειδί ενσωματωμένο στο τσιπ προσδιορίζει την κάρτα στην οποία υπάρχει, έναν κωδικό επαλήθευσης ή PIN για την αυθεντικοποίηση του ατόμου που κατέχει την κάρτα, όπου μαζί σχηματίζουν "το πράγμα που έχετε" και το" κάτι που γνωρίζετε " για έλεγχο ταυτότητας. Ο έλεγχος ταυτότητας μπορεί να χρησιμοποιηθεί για:

- VPN για αναγνώριση μιας συσκευής πριν από τη πρόσβαση σε δίκτυο: Ένας οργανισμός μπορεί να είναι σίγουρος ότι μόνο οι συσκευές που ανήκουν στην επιχείρηση επιτρέπονται στο δίκτυο της επιχείρησης.

- VPN που αναγνωρίζει έναν χρήστη πριν από την παροχή πρόσβασης σε ένα δίκτυο: Ένας οργανισμός μπορεί να είναι σίγουρος ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στο δίκτυο μιας επιχείρησης.
- Υπογραφή χρήστη ηλεκτρονικού ταχυδρομείου: Ο παραλήπτης του ηλεκτρονικού ταχυδρομείου μπορεί να γνωρίζει με κάποια βεβαιότητα ποιός έστειλε το ηλεκτρονικό μύνημα.

Κρυπτογράφηση

Η δεύτερη περίπτωση χρήσης για ένα ενωσματωμένο τσιπ ασφαλείας είναι η κρυπτογράφηση κλειδιών που χρησιμοποιούνται με τη σειρά τους για την κρυπτογράφηση αρχείων στο σκληρό δίσκο ή για την αποκρυπτογράφηση αρχείων που εισήλθαν από άλλα συστήματα. Παραδείγματα:

- Κρυπτογράφηση αρχείων και φακέλων.
- Πλήρης κρυπτογράφηση δίσκου.
- Κρυπτογράφηση κωδικών πρόσβασης για έναν διαχειριστή κωδικών πρόσβασης.
- Κρυπτογράφηση απομακρυσμένων αρχείων.

Key Storage

- Ευαίσθητες ως προς την ιδιωτικότητα λύσεις που χρησιμοποιούν διαφορετικά κλειδιά για παροχή ελάχιστης πληροφορίας του αιτούντα. Δεν απαιτείται ένα μοναδικό κλειδί το οποίο περιλαμβάνει την ηλικία του χρήστη, το βάρος, την οικογενειακή κατάσταση, τις συνθήκες υγείας, και ούτω καθεξής.
- Διαφορετικά κλειδιά για διαφορετικά επίπεδα ασφαλείας: Προσωπικά, οικονομικά και επιχειρηματικά δεδομένα απαιτούν διαφορετικά επίπεδα εμπιστευτικότητας.
- Διαφορετικά κλειδιά για πολλούς χρήστες του ίδιου υπολογιστή: Μερικές φορές τα άτομα μοιράζονται έναν υπολογιστή. Αν συμβαίνει αυτό, δεν θέλουν να δώσουν αμοιβαία πλήρη πρόσβαση στα αρχεία τους.

Random Number Generator

Υπάρχουν πολλές χρήσεις για ένα RNG:

- Δημιουργία nonces (τυχαίων αριθμών) που χρησιμοποιούνται σε πρωτόκολλα ασφαλείας.
- Δημιουργία εφήμερων κλειδιών για κρυπτογράφηση αρχείων.
- Δημιουργία κλειδιών μακροπρόθεσμης χρήσης (όπως κλειδιά που χρησιμοποιούνται για αποθήκευση).

NVRAM Storage

Η NVRAM παρέχει τα εξής:

- Αποθήκευση ριζικών κλειδιών για αλυσίδες πιστοποιητικών: Αυτά είναι δημόσια κλειδιά στα οποία όλοι πρέπει να έχουν πρόσβαση - αλλά είναι πολύ σημαντικό αυτό να μην αλλάξουν.
- Αποθήκευση κλειδιού επικύρωσης (endorsement key-EK): Ένα EK αποθηκεύεται από το κατασκευαστή και χρησιμοποιείται για την αποκρυπτογράφηση των πιστοποιητικών και την παράδοση κωδικών πρόσβασης στο TPM κατά τη διάρκεια του provisioning.
- Χώρος αποθήκευσης για αναπαράσταση της κατάστασης της μηχανής. Αυτό χρησιμοποιείται από κάποιες εφαρμογές της Intel που χρησιμοποιούν TPM και τεχνολογία Intel Trusted Execution Technology (TXT), όπου ονομάζεται πολιτική ελέγχου εκκίνησης. Όπως το δημόσιο κλειδί ρίζας που χρησιμοποιείται σε εφαρμογές ασφαλούς εκκίνησης όπως το Unified Extensible Firmware Interface (UEFI), αυτό χρησιμοποιείται από τον ιδιοκτήτη του συστήματος για να καθορίσει την κατάσταση του μηχανήματος σε μια ελεγχόμενη εκκίνηση, συνήθως μέσω ενός hypervisor. Το πλεονέκτημα έναντι της μεθόδου ασφαλούς εκκίνησης UEFI είναι ότι με τον TPM ο τελικός χρήστης έχει πλήρη έλεγχο του περιεχομένου του χώρου αποθήκευσης NVRAM.
- Χώρος αποθήκευσης για τα κλειδιά αποκρυπτογράφησης που χρησιμοποιούνται πριν γίνει διαθέσιμος ο σκληρός δίσκος. Για για παράδειγμα, ένα κλειδί που χρησιμοποιείται για μια αυτο-κρυπτογραφημένη μονάδα δίσκου.

2.9.2 Έκδοση 2

Η έκδοση 2 αποτελείται από 4 μέρη.

- Μέρος 1: Architecture

  Περιγράφει τις ιδιότητες, λειτουργίες και μεθόδους ενός TPM. Επίσης περιέχει περιγραφές ορισμένων από τις ρουτίνες χειρισμού δεδομένων που χρησιμοποιούνται από αυτήν την προδιαγραφή.

- Μέρος 2: Structures

  Περιγράφει τις σταθερές, τους τύπους δεδομένων, τις δομές και τα unions της διεπαφής TPM.

- Μέρος 3: Commands

  Περιγράφει τις εντολές, και κώδικα σε γλώσσα C που απεικονίζει τις ενέργειες που εκτελούνται από ένα TPM.

- Μέρος 4: Supporting Routines

  Παρουσιάζει τον κώδικα C που περιγράφει τους αλγορίθμους και τις μεθόδους που χρησιμοποιούνται από τον κώδικα εντολών στο TPM.

Σύγκριση TPM 1.2 με TPM 2

Το TPM 1.2 έχει τα παρακάτω χαρακτηριστικά:

- Ταυτοποίηση συσκευών: Πριν την δημιουργία του TPM οι συσκευές προσδιορίζονταν ως επί το πλείστον από διευθύνσεις MAC ή διευθύνσεις IP.

- Ασφαλής δημιουργία κλειδιών: Μία γεννήτρια τυχαίων αριθμών στο υλικού είναι ένα μεγάλο πλεονέκτημα κατά τη δημιουργία κλειδιών. Ενας αριθμός από εφαρμογών ασφάλειας έχουν αποτύχει εξαιτίας της κακής δημιουργίας κλειδιών.
- Ασφαλής αποθήκευση των κλειδιών: Κρατώντας καλά κλειδιά ασφαλή, ιδιαίτερα από επιθέσεις λογισμικού, είναι ένα μεγάλο πλεονέκτημα για μια συσκευή.
- Έλεγχος ορθής λειτουργίας συσκευής: Πριν την έλευση του TPM, τα IT τμήματα ενός οργανισμού χρησιμοποιούσαν λογισμικό για να πιστοποιήσουν την υγεία του συστήματος. Αλλά αν ένα σύστημα μπορούσε να αναφέρει ότι ήταν υγιής, ακόμη και όταν δεν ήταν.

Το TPM 2 έχει επιπλέον τα παρακάτω χαρακτηριστικά:

- Ευκινησία αλγορίθμου: Οι αλγόριθμοι μπορούν να αλλάξουν εάν αποδειχθούν κρυπτογραφικά πιο αδύναμοι από το αναμενόμενο.
- Ενισχυμένη εξουσιοδότηση: Αυτή η νέα δυνατότητα ενοποιεί τον τρόπο με τον οποίο όλες οι οντότητες σε ένα TPM μπορούν να εξουσιοδοτηθούν, ενώ παράλληλα επιτρέπουν τον πολλαπλό παράγοντα πιστοποίησης πολλών χρηστών.
- Γρήγορη φόρτωση κλειδιών: Η φόρτωση κλειδιών σε ένα TPM απαιτεί σχετικά μεγάλο χρονικό διάστημα. Τώρα μπορούν να φορτωθούν γρήγορα, χρησιμοποιώντας συμμετρική και όχι ασύμμετρη κρυπτογράφηση.
- Πιο αξιόπιστα PCRs: Στο παρελθόν, η αντιστοίχηση κλειδιών με καταστάσεις της συσκευής προκάλεσαν προβλήματα διαχείρισης. Συχνά, όταν έπρεπε να αλλάξει η κατάσταση της συσκευής μέσω μιας εγκεκριμένης αλλαγής, τα κλειδιά έπρεπε να αλλάξουν επίσης. Αυτό δεν συμβαίνει πλέον.
- Ευέλικτη διαχείριση: Μπορούν να υπάρχουν διαφορετικά είδη εξουσιοδότησης χωριστά, επιτρέποντας πολύ πιο ευέλικτη διαχείριση των πόρων του TPM.
- Αναγνώριση πόρων βάσει ονόματος: Έμμεσες αναφορές στο σχεδιασμό του TPM 1.2 οδήγησε σε προκλήσεις ασφάλειας. Αυτά έχουν διορθωθεί με τη χρήση κρυπτογραφικά ασφαλών ονομάτων για όλους τους πόρους TPM.

Πίνακας 2:Σύγκριση προδιαγραφών TPM 1.2 και TPM 2

Specification	TPM 1.2	TPM 2.0
Architecture	The one-size-fits-all specification consists of three parts.	A complete specification consists of a platform-specific specification which references a common four-part TPM 2.0 library.Platform-specific specifications define what parts of the library are mandatory, optional, or banned for that platform; and detail other requirements for that platform.Platform-specific specifications include PC Client,mobile, and Automotive-Thin.

Algorithms	SHA-1 and RSA are required.AES is optional. Triple DES was once an optional algorithm in earlier versions of TPM 1.2 but has been banned in TPM 1.2 version 94.The MGF1 hash-based mask generation function that is defined in PKCS#1 is required.	The PC Client Platform TPM Profile (PTP) Specification requires SHA-1 and SHA-256 for hashes; RSA, ECC using the Barreto-Naehrig 256-bit curve, and ECC using the NIST P-256 curve for public-key cryptography and asymmetric digital signature generation and verification; HMAC for symmetric digital signature generation and verification; 128-bit AES for symmetric-key algorithm; and the MGF1 hash-based mask generation function that is defined in PKCS#1 are required by the TCG PC Client Platform TPM Profile (PTP) Specification.Many other algorithms are also defined but are optional.
Crypto Primitives	A random number generator, a public-key cryptographic algorithm, a cryptographic hash function, a mask generation function, digital signature generation and verification, and Direct Anonymous Attestation are required. Symmetric-key algorithms and exclusive or are optional Key generation is also required.	A random number generator, public-key cryptographic algorithms, cryptographic hash functions, symmetric-key algorithms, digital signature generation and verification, mask generation functions, exclusive or, and ECC-based Direct Anonymous Attestation using the Barreto-Naehrig 256-bit curve are required by the TCG PC Client Platform TPM Profile (PTP) Specification. The TPM 2.0 common library specification also requires key generation and key derivation functions.
Hierarchy	One (storage)	Three (platform, storage and endorsement)
Root Keys	One (SRK RSA-2048)	Multiple keys and algorithms per hierarchy
Authorization	HMAC, PCR, locality, physical presence	Password, HMAC, and policy (which covers HMAC, PCR, locality, and physical presence).
NV RAM	Unstructured data	Unstructured data, Counter, Bitmap, Extend

2.10 Εντολές TPM

2.10.1 Δομή εντολών / αποκρίσεων TPM

Μια εντολή είναι μια προστατευμένη ικανότητα TPM που υποδεικνύει μια ενέργεια που πρέπει να εκτελεστεί από το TPM. Περιέχει από ένα έως πέντε πεδία, με την ακόλουθη σειρά:

1) μια κεφαλίδα εντολής που περιέχει τα παρακάτω:

- tag: Προσδιορίζει εάν η εντολή περιέχει συνόδους - δηλαδή αν περιέχει μια περιοχή εξουσιοδότησης.
- commandSize: Το μέγεθος σε byte της ροής εντολών, συμπεριλαμβανομένων όλων των πεδίων της κεφαλίδας.
- commandCode: Προσδιορίζει την εντολή TPM που πρόκειται να εκτελεστεί.

2) Έναν εξαρτώμενο από την εντολή αριθμό (μηδέν έως τρία) handles που προσδιορίζουν τις προστατευμένες θέσεις στις οποίες λειτουργεί η εντολή (Protected Capability).

3) Μια τιμή 32-bit που υποδεικνύει το μέγεθος της περιοχής εξουσιοδότησης.

4) Περιοχή εξουσιοδότησης που περιέχει μία έως τρεις δομές συνόδων.

5) Μια περιοχή παραμέτρων που εξαρτάται από την εντολή που περιέχει πληροφορίες για την εντολή.

Μια απόκριση περιέχει:

1) Μια κεφαλίδα απόκρισης που περιέχει τα παρακάτω:

- tag: Προσδιορίζει εάν η απάντηση περιέχει συνόδους.
- responseSize: Το μέγεθος σε byte της ροής της απόκρισης, συμπεριλαμβανομένων όλων των πεδίων της κεφαλίδας.
- responseCode: Προσδιορίζει αν η εντολή TPM ήταν επιτυχής και, αν όχι, το συγκεκριμένο σφάλμα

2) Έναν εξαρτώμενο από την εντολή αριθμό (μηδέν ή ένα) των handles που αναγνωρίζουν τις προστατευμένες θέσεις με τις οποίες λειτουργεί η εντολή (Protected Capability).

3) Μια τιμή 32-bit που υποδεικνύει το μέγεθος της περιοχής παραμέτρων.

4) Μια περιοχή παραμέτρων εξαρτώμενη από την εντολή που περιέχει τις τιμές που παράγονται από το TPM.

5) Περιοχή εξουσιοδότησης που περιέχει μία έως τρεις δομές συνόδων.

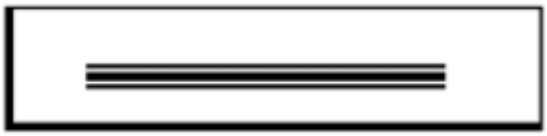
2.10.2 Εντολή χωρίς authorizations(TPM2_Startup)

Πίνακας 3: Εντολή TPM2_Startup (πίνακας 5, μέρος 3 του TPM 2 Πρότυπου)

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Startup {NV}
TPM_SU	startupType	TPM_SU_CLEAR or TPM_SU_STATE

Η στήλη Type του παραπάνω πίνακα παρουσιάζει τον τύπο δεδομένων για κάθε πεδίο της εντολής. Αυτοί οι τύποι ορίζονται στο Μέρος 2 της προδιαγραφής. Η στήλη Name περιέχει το όνομα της παραμέτρου που πρέπει να μεταβιβαστεί προς ή από το TPM. Αυτό είναι και το όνομα της παραμέτρου στον πηγαίο κώδικα του μέρους 3. Η στήλη Description περιγράφει το πεδίο καθώς και ειδικές απαιτήσεις για τον πεδίο. Το TPM2_Startup έχει δύο ειδικές απαιτήσεις για το πεδίο: Η ετικέτα-tag πρέπει να είναι πάντα TPM_ST_NO_SESSIONS επειδή η εντολή δεν περιέχει συνόδους και το commandCode πρέπει να είναι TPM_CC_Startup. Η {NV} είναι μια διακόσμηση-decoration του πίνακα που σημαίνει ότι η εντολή μπορεί να ενημερώσει μη πτητική μνήμη μέσα στοTPM.

Η γραμμή



είναι ένας διαχωριστής που σημαίνει ότι τα πεδία που ακολουθούν ανήκουν στην περιοχή παραμέτρων. Σε αυτήν την περίπτωση, η startupType είναι η μόνη παράμετρος σε αυτήν την περιοχή.

Πίνακας 4: Απόκριση TPM2_Startup(πίνακας 6, μέρος 3 του TPM 2 Πρότυπου)

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

Ακολουθούν εξηγήσεις των πεδίων ανταπόκρισης:

- tag: Υποδεικνύει εάν η απόκριση έχει συνόδους. Επειδη αυτή η εντολή δεν έχει ποτέ περιόδους σύνδεσης, η ετικέτα είναι πάντα TPM_ST_NO_SESSIONS.
- responseSize: Το μέγεθος σε bytes της απόκρισης.

- responseCode: Υποδεικνύει αν η εντολή έχει περάσει ή έχει αποτύχει. Το TPM_RC_SUCCESS υποδεικνύει το πέρασμα. Άλλοι κωδικοί υποδεικνύουν αστοχία. Η εντολή TPM2_Startup δεν έχει παραμέτρους επιστροφής.

2.10.3 Εντολή με authorizations(TPM2_Create)

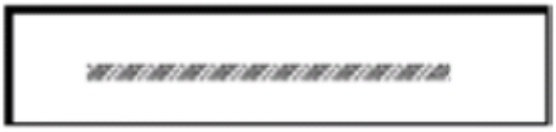
Πίνακας 5: Εντολή TPM2_Create (πίνακας 19, μέρος 3 του TPM 2 Πρότυπου)

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Create
TPMI_DH_OBJECT	@parentHandle	handle of parent for new object Auth Index: 1 Auth Role: USER
TPM2B_SENSITIVE_CREATE	inSensitive	the sensitive data
TPM2B_PUBLIC	inPublic	the public template
TPM2B_DATA	outsideInfo	data that will be included in the creation data for this object to provide permanent, verifiable linkage between this object and some object owner data
TPML_PCR_SELECTION	creationPCR	PCR that will be used in creation data

Ακολουθούν επεξηγήσεις των πεδίων εντολής του παραπάνω πίνακα:

- tag: Σε αυτήν την περίπτωση, το TPM_ST_SESSIONS υποδηλώνει ότι η εντολή πρέπει να έχει συνεδρίες. Μια άλλη ένδειξη είναι το σύμβολο @ μπροστά από το parentHandle. Αυτό σημαίνει ότι απαιτείται μια συνεδρία εξουσιοδότησης με αυτό το handle.
- commandSize: Το μέγεθος σε byte της συνολικής ροής.
- commandCode: Ο κώδικας εντολής για αυτήν την εντολή.

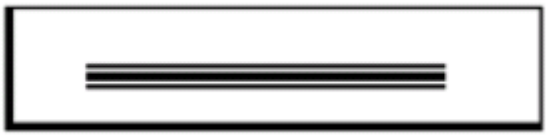
Ο παρακάτω διαχωριστής δεν υπήρχε στην TPM2_Startup εντολή:



Αυτή η γραμμή δείχνει ότι τα πεδία που βρίσκονται κάτω από αυτή, βρίσκονται στην περιοχή χειρισμού(handle area). Τα handles είναι αναφορές 32-bit σε διάφορες οντότητες του TPM. Η parentHandle είναι η μόνη παράμετρος χειρισμού για αυτή την εντολή. Οι εντολές μπορούν να λάβουν έως και 2 handles σε αυτήν την περιοχή. Το κείμενο "Index Auth: 1" στην περιγραφή υποδεικνύει την σειρά της εξουσιοδότησης.

Στην περίπτωση αυτή, η εξουσιοδότηση για το parentHandle πρέπει να είναι η πρώτη εξουσιοδότηση στην ενότητα εξουσιοδότησης. Όλες οι εντολές που λαμβάνουν τις εξουσιοδοτήσεις μπορούν να πάρουν μέχρι τρεις εξουσιοδοτήσεις. Το κείμενο "Auth Role: USER" πρόκειται για περαιτέρω ρόλο σχετικά με την εξουσιοδότηση. Οι ρόλοι Auth είναι ανάλογοι με τα προνομιακά επίπεδα σε ένα λειτουργικό σύστημα. Ελέγχουν ποιος μπορεί να έχει πρόσβαση σε ορισμένες οντότητες.

Ακολουθεί μια γραμμή που δείχνει την αρχή της περιοχής παραμέτρων:



Αλλά σε αυτή την περίπτωση, επειδή η ετικέτα είναι ίση με TPM_ST_SESSIONS, υποδεικνύοντας ότι αυτή η εντολή απαιτεί μια session εξουσιοδότησης, αυτός ο διαχωριστής δείχνει επίσης πού εισάγονται τα δεδομένα εξουσιοδότησης στη ροή byte εντολών. Η περιοχή εξουσιοδότησης αυτής της εντολής μπορεί να έχει μεταξύ ενός και τριών συνεδριών. Αυτή η εντολή παίρνει τέσσερις παραμέτρους: insensitive, inPublic, outsideInfo και creationPCR.

Πίνακας 6: Απόκριση TPM2_Create (πίνακας 20, μέρος 3 του TPM 2 Πρότυπου)

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PRIVATE	outPrivate	the private portion of the object
TPM2B_PUBLIC	outPublic	the public portion of the created object
TPM2B_CREATION_DATA	creationData	contains a TPMS_CREATION_DATA
TPM2B_DIGEST	creationHash	digest of *creationData* using *nameAlg* of *outPublic*
TPMT_TK_CREATION	creationTicket	ticket used by TPM2_CertifyCreation() to validate that the creation data was produced by the TPM

Ακολουθούν εξηγήσεις των πεδίων απόκρισης:

- η ετικέτα, το responseSize και το responseCode είναι όπως περιγράφηκε προηγουμένως, εκτός αν περάσει η εντολή, η ετικέτα είναι TPM_RC_SESSIONS για να υποδείξει τη παρουσία συνεδριών στην απάντηση. Υπάρχουν τρεις περιπτώσεις εδώ:
    - Εάν η εντολή δεν έχει συνεδρίες, η απάντηση δεν θα έχει συνεδρίες. Για αυτήν την εντολή, η ετικέτα είναι πάντα ρυθμισμένη σε TPM_ST_NO_SESSIONS.
    - Εάν η εντολή έχει συνεδρίες και επιστρέφει επιτυχώς, η ετικέτα απόκρισης είναι TPM_ST_SESSIONS, υποδεικνύοντας ότι η απάντηση, επίσης, έχει συνεδρίες.

- Εάν η εντολή έχει συνεδρίες αλλά αποτυγχάνει, η ετικέτα απόκρισης είναι TPM_ST_NO_SESSIONS. Οι αποτυχημένες εντολές δεν έχουν ποτέ συνεδρίες ή τις παραμέτρους απόκρισης στην απάντησή τους.

Αυτή η εντολή επιστρέφει πέντε παραμέτρους απόκρισης: outPrivate, outPublic, creationData, creationHash και creationTicket.

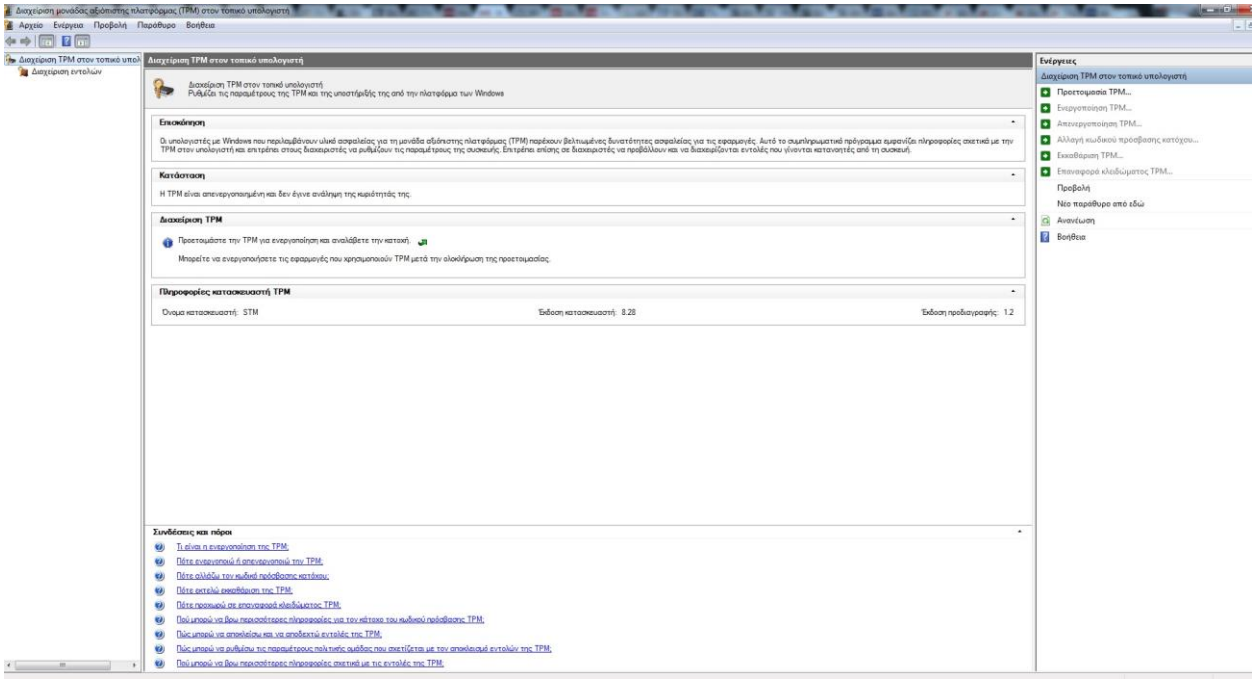
2.11 Έναρξη χρήσης TPM

2.11.1 Ενεργοποίηση του TPM

Η ενεργοποίηση του tpm σε windows 7 γίνεται ακολουθώντας τα παρακάτω βήματα.

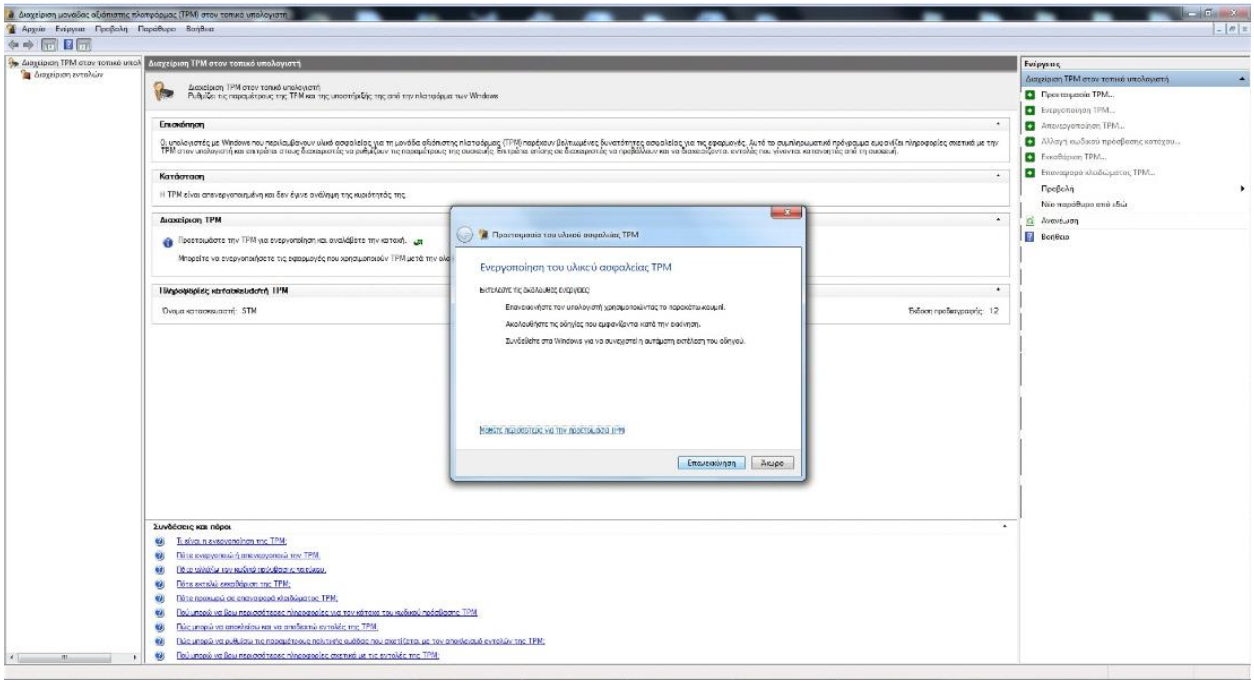
Ενεργοποίηση του TPM στο BIOS, κατά την έναρξη του υπολογιστή πατάμε F2, και στο tab security επιλέγουμε enable tpm.

Μετά την εκκίνηση στο Command line πληκτρολογούμε tmp.msc όπου εμφανίζεται η παρακάτω κονσόλα με τίτλο «Διαχείριση μονάδας αξιόπιστης πλατφόρμας»:



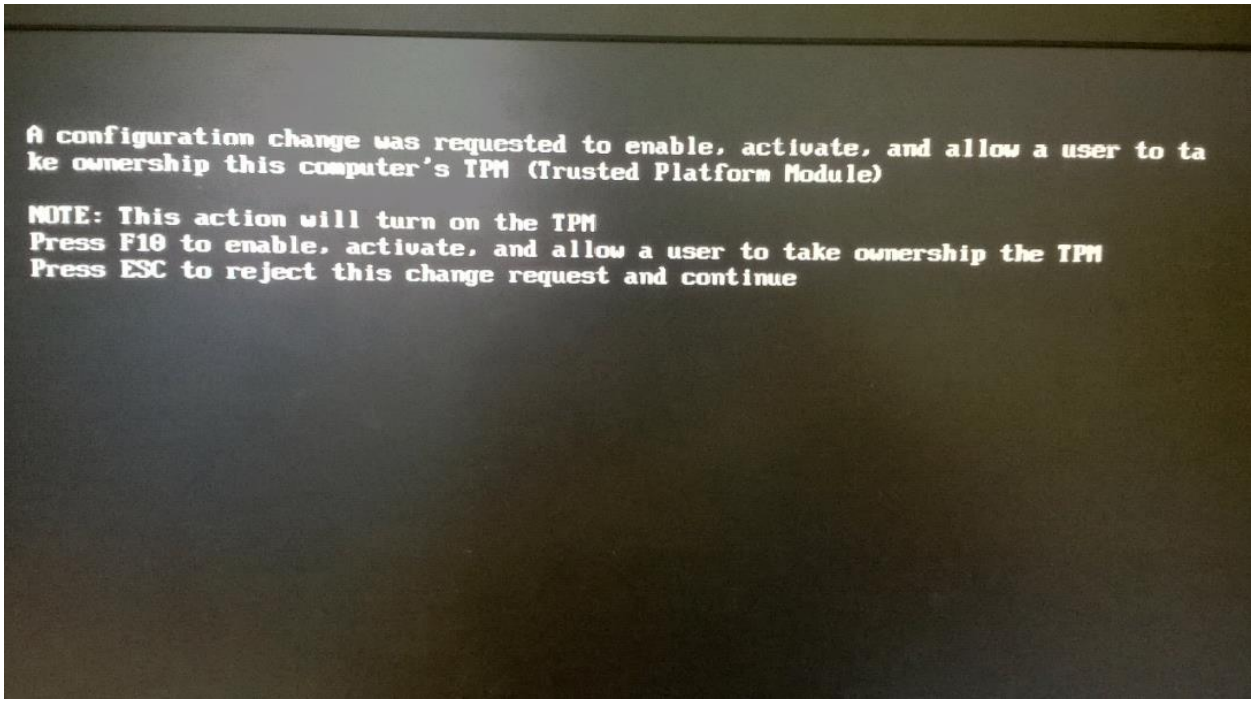
Εικόνα 6: Διαχείριση μονάδας αξιόπιστης πλατφόρμας

Επιλέγουμε προετοιμασία TPM



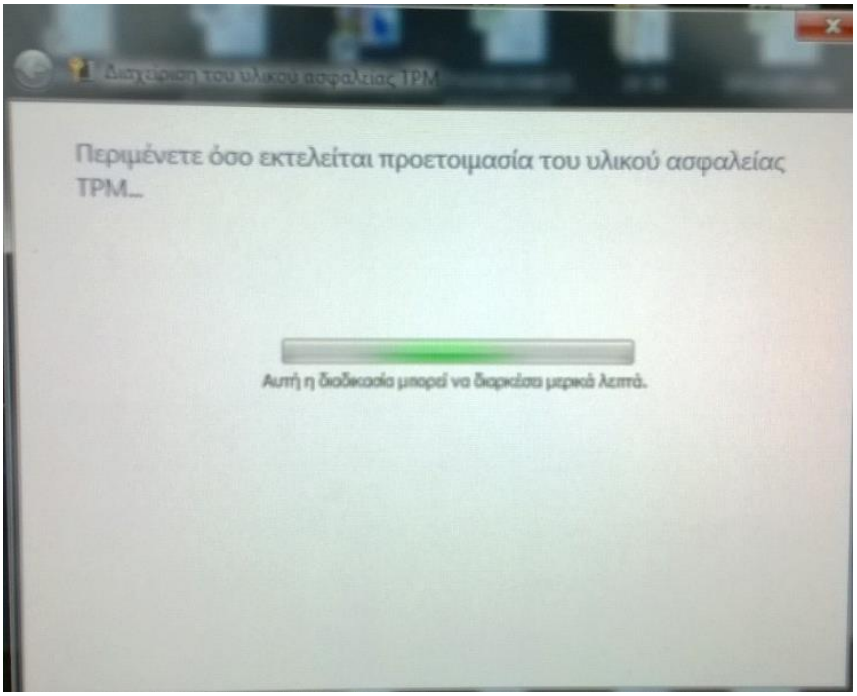
Εικόνα 7: Προετοιμασία TPM

Κάνουμε επανεκκίνηση



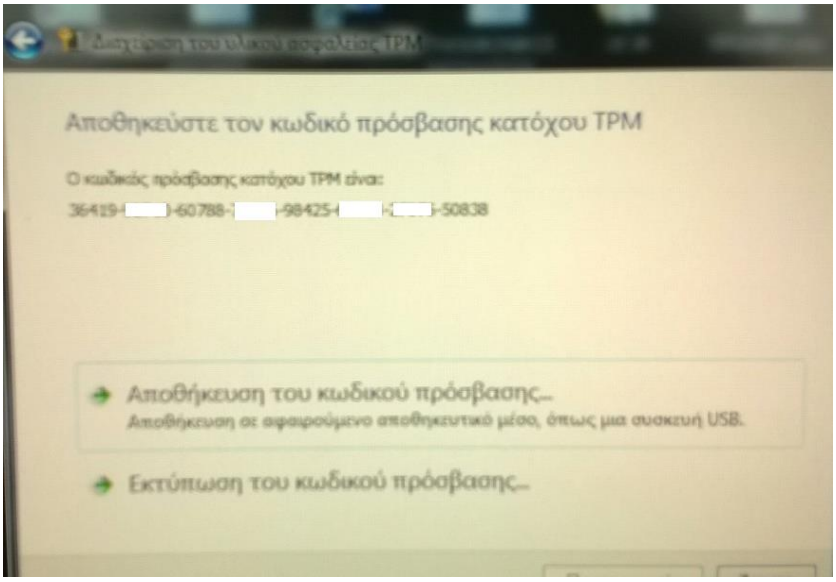
Εικόνα 8: Επανεκκίνηση λόγω προετοιμασίας TPM

Στη κονσόλα με τίτλο «Διαχείριση μονάδας αξιόπιστης πλατφόρμας» επιλέγουμε ενεργοποίηση tpm.



Εικόνα 9:Προετοιμασία υλικού ασφαλείας

Αφού ολοκληρωθεί η διαδικασία εμφανίζεται ο κωδικός πρόσβασης κατόχου TPM.

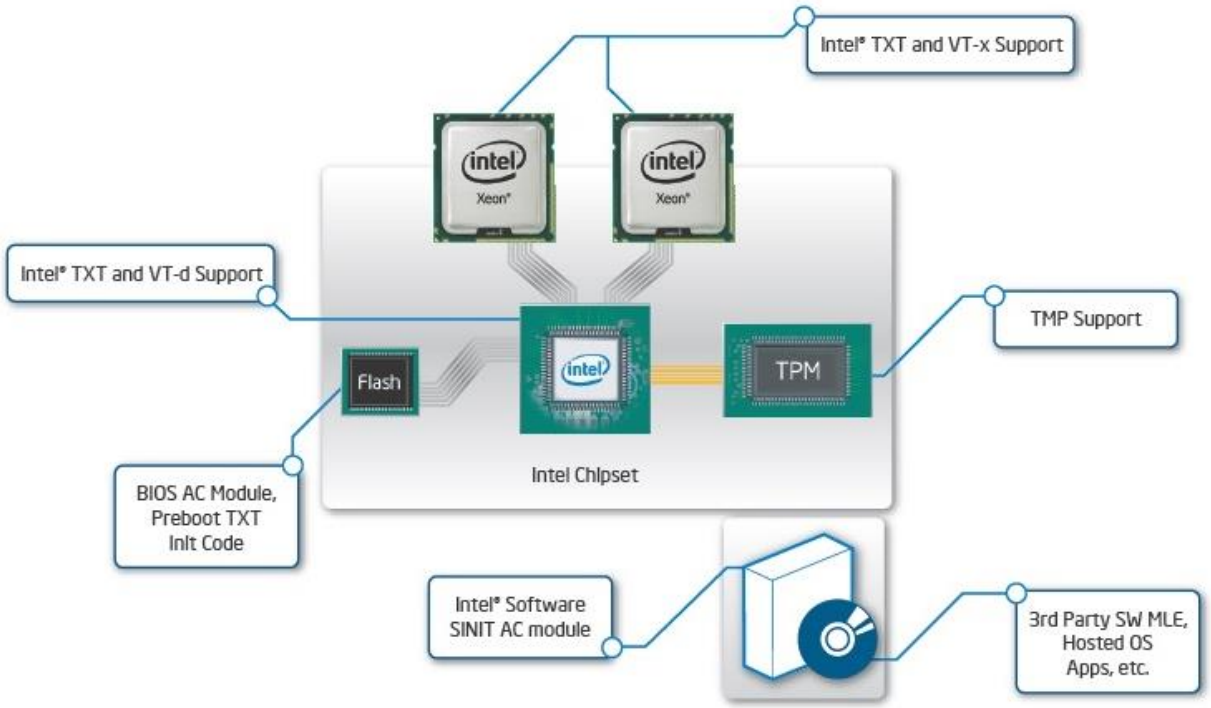


Εικόνα 10: Κωδικός πρόσβασης κατόχου TPM

3. ΕΦΑΡΜΟΓΕΣ TPM

3.1 Intel TXT

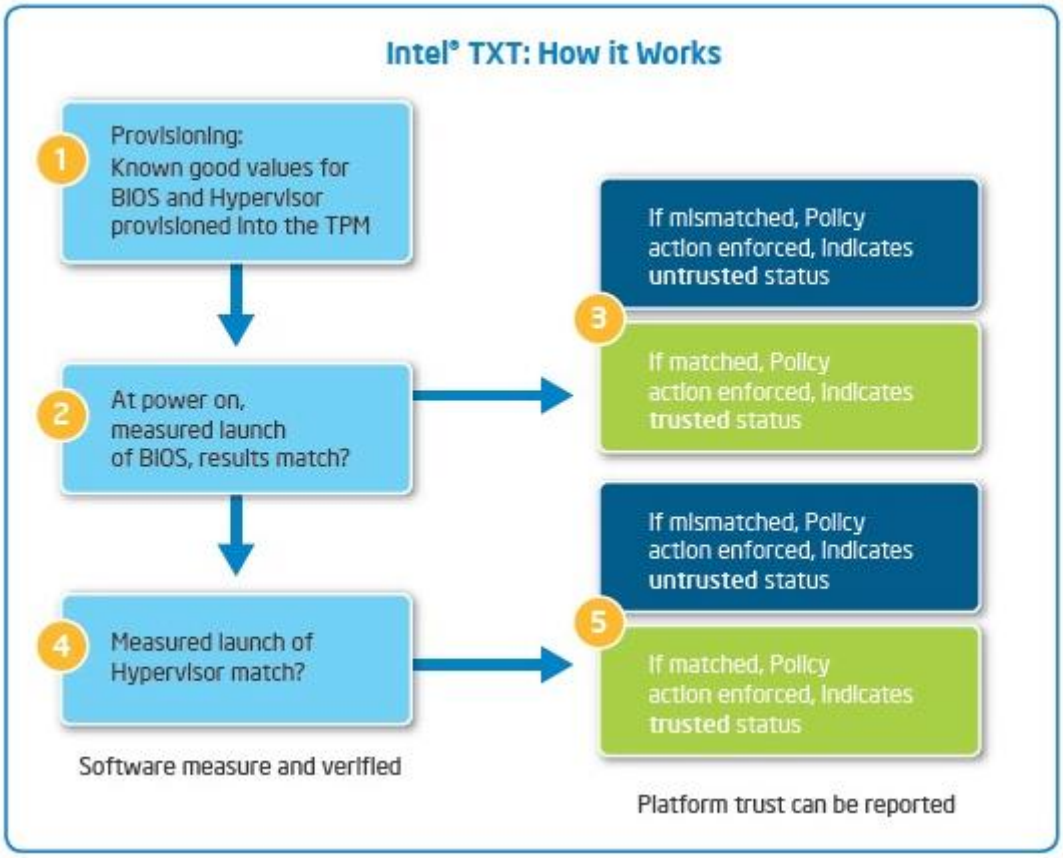
Σχεδιασμένο για να προστατεύει από επιθέσεις με βάση το λογισμικό, η τεχνολογία Trusted Execution της Intel ενσωματώνει νέες λειτουργίες ασφάλειας και δυνατότητες στον επεξεργαστή, το chipset και σε άλλα συστατικά της πλατφόρμας. Η ασφάλεια υλικού δίνει τη δυνατότητα να αυξήσει την εμπιστευτικότητα και την ακεραιότητα των ευαίσθητων πληροφοριών από επιθέσεις με βάση το λογισμικό, προστατεύοντας ευαίσθητες πληροφορίες χωρίς να θέτει σε κίνδυνο τη χρηστικότητα της πλατφόρμας. Τρία μοντέλα χρήσης μπορούν να βοηθήσουν στην τεχνολογία Trusted Execution.



Εικόνα 11: Συστατικά του TXT[12]

Τα μοντέλα χρήσης είναι:

- Τοπική επαλήθευση.
- Επαλήθευση από απόσταση.
- Λειτουργία πολλαπλών επιπέδων.



Εικόνα 12: Λειτουργία του TXT

Τοπική επαλήθευση

Η τοπική επαλήθευση χρησιμοποιεί την ικανότητα μέτρησης της τεχνολογίας Trusted Execution για να επιτρέψει στον τοπικό χρήστη να έχει εμπιστοσύνη ότι η πλατφόρμα εκτελείται σε μια γνωστή κατάσταση. Η εμπιστοσύνη προέρχεται από την ικανότητα υλικού του Trusted Execution Technology να μετράει σωστά τη διαμόρφωση εκκίνησης και να αποθηκεύει τη μέτρηση στην πλατφόρμα Trusted Platform Module (TPM).

Απομακρυσμένη επαλήθευση

Η απομακρυσμένη επαλήθευση λαμβάνει τις μετρήσεις που λαμβάνονται από τη τεχνολογία Trusted Execution και αποθηκεύει στο TPM και χρησιμοποιεί το TPM για ενημέρωση των απομακρυσμένων οντοτοτήτων σχετικά με τη τρέχουσα ρύθμιση της πλατφόρμας. Η ουσία σε αυτό το μοντέλο χρήσης είναι ότι η απομακρυσμένη οντότητα μπορεί να βασιστεί στις ιδιότητες της τεχνολογίας αξιόπιστης εκτέλεσης για την παροχή των εξασφαλίσεων που αναφέρονται παραπάνω.

Κανένα σύστημα υπολογιστή δεν μπορεί να παρέχει απόλυτη ασφάλεια σε όλες τις συνθήκες. Η τεχνολογία Intel Virtualization απαιτεί ένα σύστημα υπολογιστή με ενεργοποιημένο επεξεργαστή Intel®, BIOS, οθόνη εικονικής μηχανής (VMM) και, για κάποιες χρήσεις, ένα συγκεκριμένο λογισμικό πλατφόρμας που είναι ενεργοποιημένο για αυτό το λόγο. Επιπλέον, η τεχνολογία Intel Trusted Execution απαιτεί από το σύστημα να περιέχει ένα TPMv1.2 όπως ορίζεται από την ομάδα Trusted Computing

Group και συγκεκριμένο λογισμικό για ορισμένες χρήσεις. Λειτουργικότητα, επιδόσεις ή άλλα οφέλη θα διαφέρουν ανάλογα με τις ρυθμίσεις παραμέτρων υλικού και λογισμικού και ενδέχεται να απαιτούν ενημέρωση του BIOS. Οι εφαρμογές λογισμικού ενδέχεται να μην είναι συμβατές με όλα τα λειτουργικά συστήματα.

Λειτουργία πολλαπλών επιπέδων

Η λειτουργία πολλαπλών επιπέδων εκμεταλλεύεται τις προστασίες μνήμης που παρέχεται από την Τεχνολογία Trusted Execution για την εκτέλεση δύο ή περισσότερων εφαρμογών ή λειτουργικά συστήματα που απαιτούν αυστηρό διαχωρισμό και διαχειριζόμενη επικοινωνία μεταξύ των οντοτήτων.

3.2 BitLocker™ drive encryption

Το BitLocker ξεκίνησε ως τμήμα της αρχιτεκτονικής Next Generation Secure Computing Base της Microsoft το 2004 ως χαρακτηριστικό με κωδικό όνομα "Cornerstone", και σχεδιάστηκε για την προστασία πληροφοριών σε συσκευές, ειδικά σε περίπτωση απώλειας ή κλοπής μιας συσκευής. Ένα άλλο χαρακτηριστικό, με τίτλο "Κρυπτογράφηση Ακεραιότητας κώδικα", σχεδιάστηκε για να επικυρώνει την ακεραιότητα των αρχείων εκκίνησης και των συστημάτων Microsoft Windows. Όταν χρησιμοποιείται σε συνδυασμό με ένα Trusted Platform Module (TPM), το BitLocker μπορεί να επικυρώσει την ακεραιότητα των αρχείων εκκίνησης και συστήματος πριν αποκρυπτογραφήσει έναν προστατευμένο τόμο. Μια ανεπιτυχής επικύρωση θα απαγορεύσει την πρόσβαση σε προστατευμένο σύστημα.

3.3 Windows Virtual Smart Card

Η τεχνολογία της εικονικής έξυπνης κάρτας[9] από τη Microsoft προσφέρει συγκρίσιμα πλεονεκτήματα ασφάλειας σε σχέση με τις φυσικές έξυπνες κάρτες, χρησιμοποιώντας έλεγχο ταυτότητας δύο παραγόντων. Οι εικονικές έξυπνες κάρτες προσομοιώνουν τη λειτουργικότητα των φυσικών έξυπνων καρτών, αλλά χρησιμοποιούν το τσιπ TPM (Trusted Platform Module) που είναι διαθέσιμο σε υπολογιστές αντί να απαιτεί τη χρήση ξεχωριστής φυσικής έξυπνης κάρτας και αναγνώστη. Οι εικονικές έξυπνες κάρτες δημιουργούνται στο TPM, όπου τα κλειδιά που χρησιμοποιούνται για έλεγχο ταυτότητας αποθηκεύονται σε κρυπτογραφικά ασφαλές υλικό.

Χρησιμοποιώντας συσκευές TPM που παρέχουν τις ίδιες κρυπτογραφικές δυνατότητες με τις φυσικές έξυπνες κάρτες, οι εικονικές έξυπνες κάρτες ολοκληρώνουν τις τρεις βασικές ιδιότητες που είναι επιθυμητές για τις έξυπνες κάρτες:

- Μη εξαγωγιμότητα (**Non-exportability)**

  Επειδή όλες οι ιδιωτικές πληροφορίες στην εικονική έξυπνη κάρτα κρυπτογραφούνται χρησιμοποιώντας το TPM στον κεντρικό υπολογιστή, δεν μπορούν να χρησιμοποιηθούν σε διαφορετικό υπολογιστή με διαφορετικό TPM. Επιπλέον, τα TPM σχεδιάζονται ώστε να είναι ανθεκτικά στις παραβιάσεις και να μην μπορούν να εξαχθούν, οπότε ένας κακόβουλος χρήστης δεν μπορεί να αναστρέψει την κατασκευή ενός ίδιου TPM ή να εγκαταστήσει το ίδιο TPM σε διαφορετικό υπολογιστή

- Απομονωμένη κρυπτογραφία(**Isolated cryptography**)

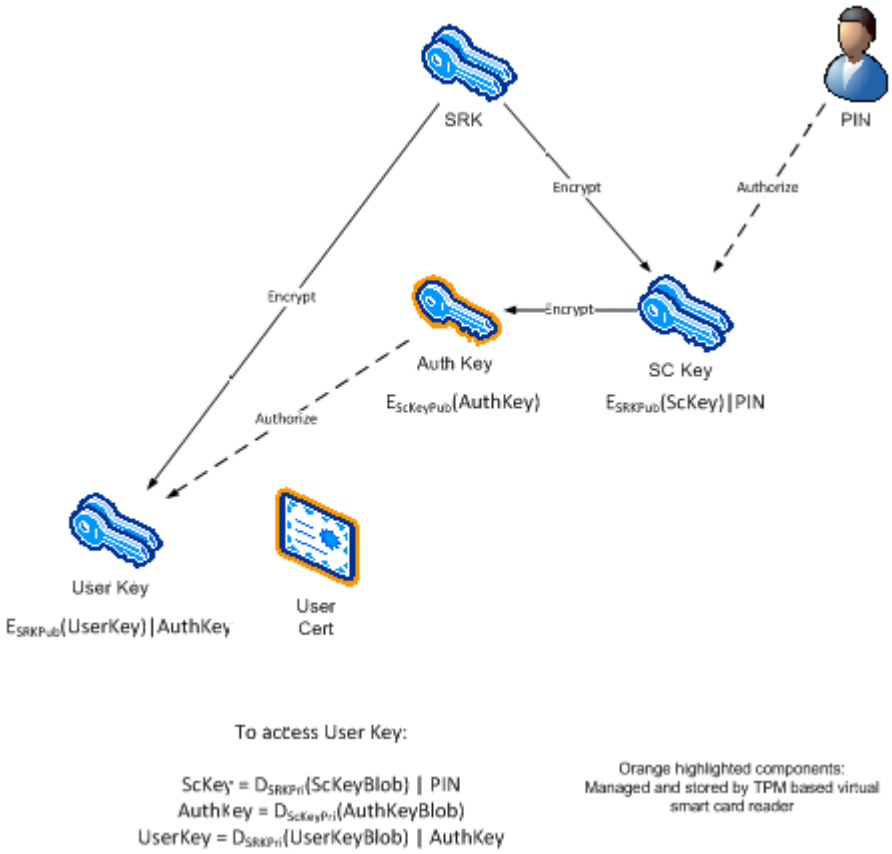
Τα TPM παρέχουν τις ίδιες ιδιότητες της απομονωμένης κρυπτογράφησης που προσφέρονται από φυσικές έξυπνες κάρτες. Τα μη κρυπτογραφημένα αντίγραφα των ιδιωτικών κλειδιών φορτώνονται μόνο μέσα στο TPM και ποτέ στη μνήμη που είναι προσβάσιμη από το λειτουργικό σύστημα. Όλες οι κρυπτογραφικές λειτουργίες με αυτά τα ιδιωτικά κλειδιά εμφανίζονται μέσα στο TPM.

- Αντι-σφυρηλάτηση(**Anti-hammering**)

  Εάν ένας χρήστης εισάγει εσφαλμένα έναν κωδικό PIN, η εικονική έξυπνη κάρτα αποκρίνεται χρησιμοποιώντας τη λογική αντι-σφυρηλάτησης του TPM, η οποία απορρίπτει περαιτέρω προσπάθειες για κάποιο χρονικό διάστημα. Αυτό είναι επίσης γνωστό ως lockout.

Ένα βασικό χαρακτηριστικό των εικονικών έξυπνων καρτών TPM [10] είναι η ικανότητά τους να αποθηκεύουν και να χρησιμοποιούν με ασφάλεια τα μυστικά δεδομένα. Τα δεδομένα μπορούν να προσεγγιστούν και να χρησιμοποιηθούν εντός του συστήματος εικονικών έξυπνων καρτών, αλλά δεν έχουν νόημα εκτός του προβλεπόμενου περιβάλλοντος. Στις εικονικές έξυπνες κάρτες TPM, η ασφάλεια εξασφαλίζεται με μια ασφαλή βασική ιεραρχία, η οποία περιλαμβάνει αρκετές αλυσίδες κρυπτογράφησης. Αυτό προέρχεται από το ριζικό κλειδί αποθήκευσης του TPM, το οποίο παράγεται και αποθηκεύεται μέσα στο TPM και δεν εκτίθεται ποτέ έξω από το τσιπ. Η ιεραρχία των κλειδιών του TPM έχει σχεδιαστεί για να επιτρέπει την κρυπτογράφηση των δεδομένων χρήστη με το ριζικό κλειδί αποθήκευσης, αλλά επιτρέπει την αποκρυπτογράφηση με το PIN χρήστη κατά τέτοιο τρόπο ώστε η αλλαγή του PIN να μην απαιτεί την επανακρυπτογράφηση των δεδομένων.

Το παρακάτω διάγραμμα απεικονίζει την ασφαλή ιεραρχία κλειδιών και τη διαδικασία πρόσβασης στο κλειδί χρήστη.



Εικόνα 13: Διαδικασία πρόσβασης στο κλειδί χρήστη

Τα ακόλουθα κλειδιά αποθηκεύονται στον σκληρό δίσκο:

- Κλειδί του χρήστη
- Το κλειδί της έξυπνης κάρτας, το οποίο κρυπτογραφείται από το βασικό κλειδί αποθήκευσης
- Κλειδί Εξουσιοδότησης για την αποκρυπτογράφηση κλειδιού χρήστη, το οποίο κρυπτογραφείται από το δημόσιο τμήμα του κλειδιού έξυπνης κάρτας

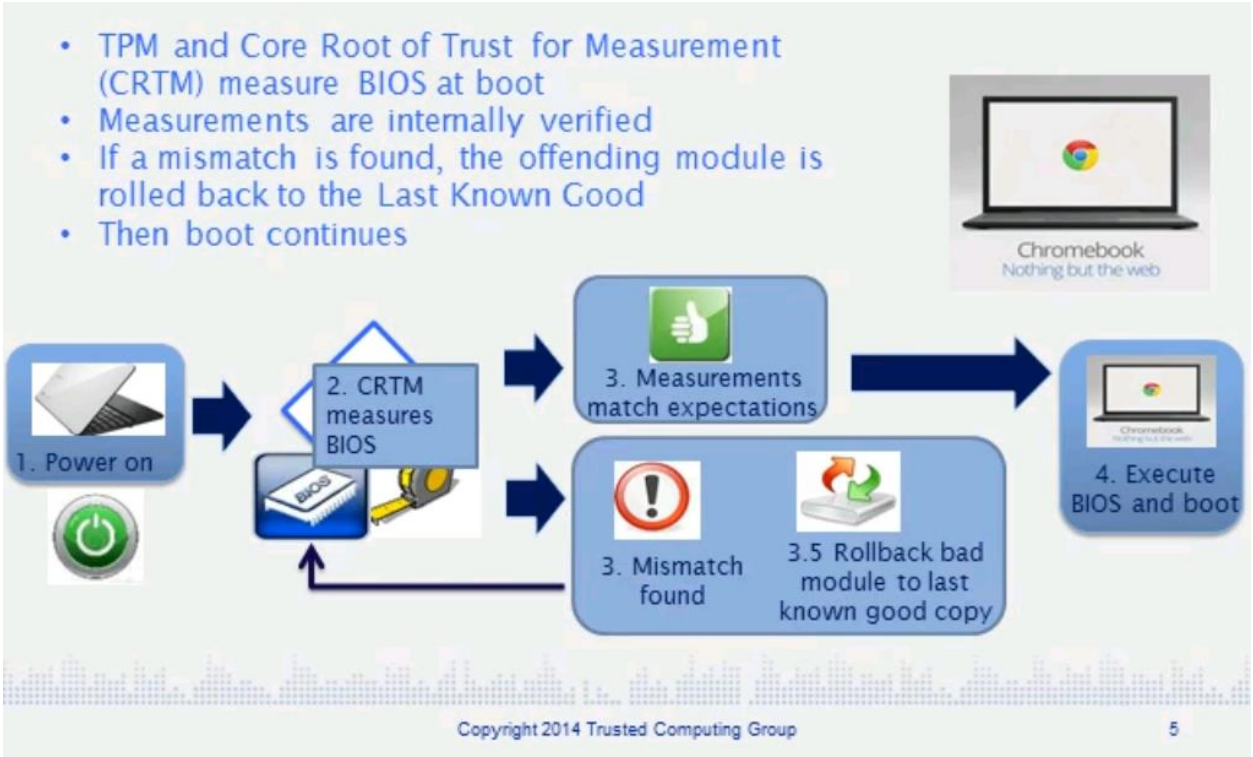
Όταν ο χρήστης εισάγει ένα PIN, επιτρέπεται η χρήση του αποκρυπτογραφημένου κλειδιού έξυπνης κάρτας με αυτόν τον κωδικό PIN. Εάν αυτή η εξουσιοδότηση επιτύχει, το αποκρυπτογραφημένο κλειδί έξυπνης κάρτας χρησιμοποιείται για την αποκρυπτογράφηση του κλειδιού auth. Στη συνέχεια, το κλειδί auth παρέχεται στο TPM για να επιτρέψει την αποκρυπτογράφηση και τη χρήση του κλειδιού του χρήστη που είναι αποθηκευμένο στην εικονική έξυπνη κάρτα.

Το κλειδί auth είναι το μόνο ευαίσθητο δεδομένο που χρησιμοποιείται υπό τη μορφή κειμένου εκτός του TPM, αλλά η παρουσία του στη μνήμη προστατεύεται από το Microsoft Data Protection API (DPAPI), έτσι ώστε πριν αποθηκευτεί με οποιονδήποτε τρόπο, να είναι κρυπτογραφημένο. Όλα τα δεδομένα πλην του κλειδιού auth επεξεργάζονται μόνο ως απλό κείμενο μέσα στο TPM, το οποίο είναι απομονωμένο από εξωτερική πρόσβαση.

3.4 Chrome OS

Το Chrome OS [11], χρησιμοποιεί το TPM για τις παρακάτω εργασίες:

- Αποτροπή της επαναφοράς της έκδοσης λογισμικού και του firmware.
- Διατήρηση πληροφοριών για την ανίχνευση μεταβάσεων μεταξύ κανονικών και προγραμματιστικών λειτουργιών.
- Προστασία των κλειδιών κρυπτογράφησης δεδομένων χρήστη.
- Προστασία ορισμένων κλειδιών RSA χρήστη (πιστοποιητικά που υποστηρίζονται από hardware).
- Παροχή αποδεικτικών παραβιάσεων για χαρακτηριστικά εγκατάστασης.
- Προστασία των κρυπτογραφημένων κλειδιών διαμερίσματος.
- Βεβαίωση κλειδιών με προστασία TPM.
- Δοκιμή λειτουργίας συσκευής.
- Το TPM δεν είναι άμεσα διαθέσιμο εκτός του Chrome OS για οποιονδήποτε σκοπό. Δηλαδή, κανένας απομακρυσμένος υπολογιστής δεν έχει πρόσβαση στο TPM.



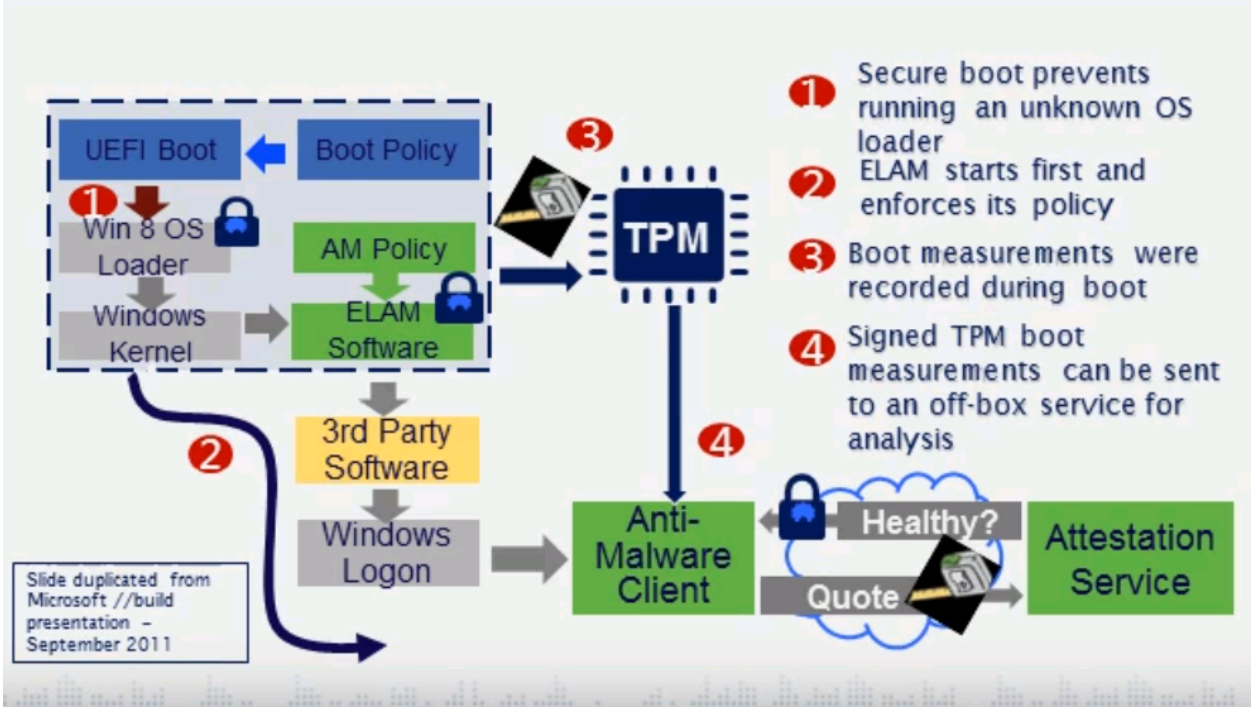
Εικόνα 14: Chrome OS[15]

Μετά το power on χρησιμοποιεί κώδικα που λέγεται CRTM και κάνει μετρήσεις στο BIOS και αποθηκεύει τις μετρήσεις στο TPM. Κατόπιν εξετάζει τις τιμές και τις συγκρίνει με τις αναμενόμενες τιμές. Αν βρεθούν ίδιες τότε το pc εκκινεί. Αν προκύψει διαφορά τότε το chrome book διαγράφει το mismatched module και εγκαθιστά τη σωστή έκδοση αυτού του module. Μετά κάνει reset το σύστημα και μετράει ξανά. Αν οι τιμές είναι ίδιες με τις αναμενόμενες τότε εκκινεί κανονικά.

Το Chrome OS δεν χρησιμοποιεί το TPM για τα εξής:

- Αξιόπιστη εκκίνηση - το TPM δεν χρησιμοποιείται ως μέρος της λύσης εκκίνησης που έχει πιστοποιηθεί από το Chrome OS.
- Υποβολή αναφοράς διαμόρφωσης πλατφόρμας υλικού.
- Κρυπτογράφηση ολόκληρου του δίσκου. Συγκεκριμένα, το TPM δεν χρησιμοποιείται για την ανάπτυξη(unwrap) ενός κλειδιού κρυπτογράφησης κατά τη διάρκεια της διαδικασίας εκκίνησης.

3.5 Windows 8



Εικόνα 15: Windows 8[15]

Τα Windows 8 για την αντιμετώπιση των rootkits (περίπλοκος και επικίνδυνος τύπος κακόβουλου λογισμικού που εκτελείται σε λειτουργία πυρήνα, χρησιμοποιώντας τα ίδια προνόμια με το λειτουργικό σύστημα), υποστηρίζουν τέσσερις λειτουργίες για την αποτροπή της φόρτωσης των rootkits και των bootkits κατά τη διάρκεια της διαδικασίας εκκίνησης:

Secure Boot. Οι υπολογιστές με firmware UEFI και μια μονάδα Trusted Platform Module (TPM) μπορούν να ρυθμιστούν ώστε να φορτώνουν μόνο αξιόπιστους bootloaders του λειτουργικού συστήματος.

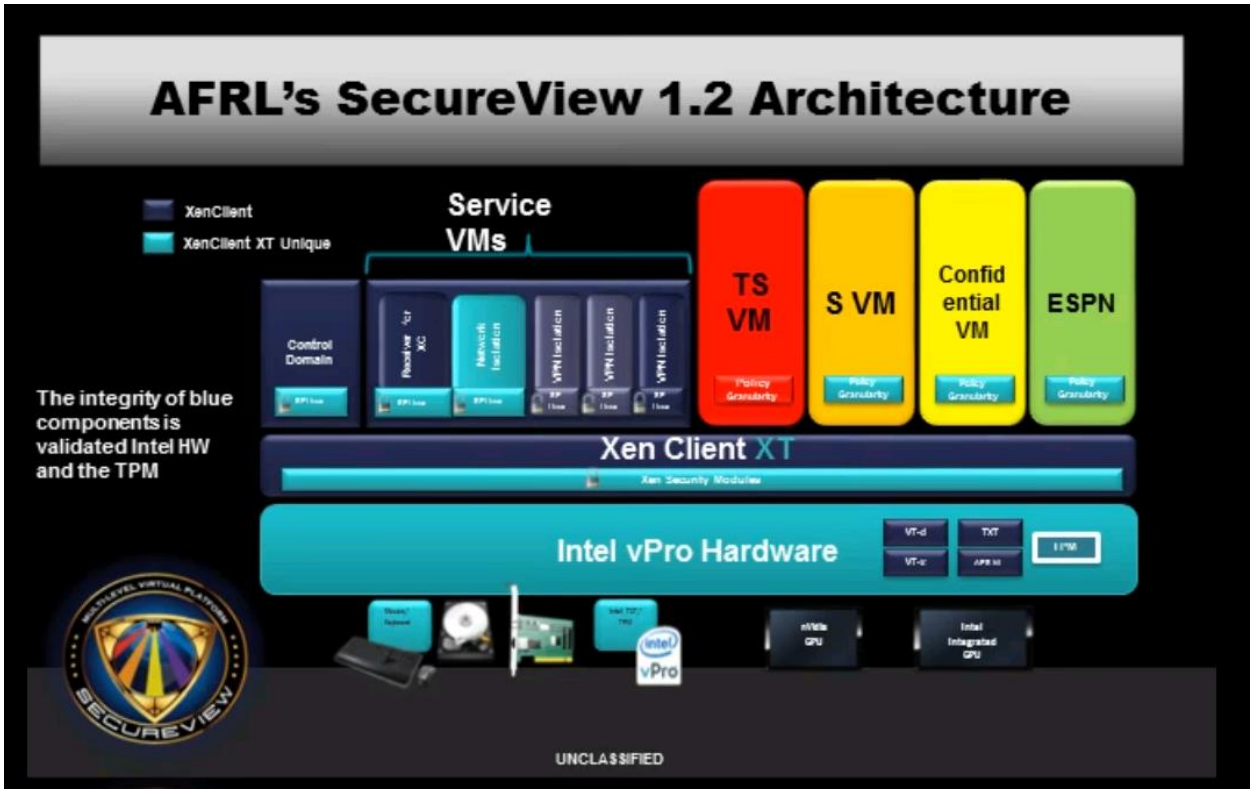
Trusted Boot. Τα Windows ελέγχουν την ακεραιότητα κάθε στοιχείου της διαδικασίας εκκίνησης πριν τη φόρτωσή της.

Early Launch Anti-Malware (ELAM)-Πρόωρη εκκίνηση κατά του κακόβουλου λογισμικού (ELAM). Το ELAM ελέγχει όλους τους οδηγούς πριν φορτώσουν και αποτρέπει τη φόρτωση των μη εγκεκριμένων οδηγών.

Measured Boot. Το firmware του υπολογιστή καταγράφει τη διαδικασία εκκίνησης και τα Windows μπορούν να το στείλουν σε έναν αξιόπιστο διακομιστή που μπορεί να εκτιμήσει αντικειμενικά την κατάσταση του υπολογιστή.

3.6 Secure View(Air Force Research Laboratory)

Το SecureView [16], είναι μια λύση που παρέχει στους χρήστες την δυνατότητα πρόσβασης σε πολλαπλά ανεξάρτητα επίπεδα ασφαλείας-Multiple Independent Levels of Security(MILS) από ένα μόνο σταθμό εργασίας. Ένας υπολογιστής φιλοξενεί πολλαπλές εικονικές μηχανές επισκεπτών (VM) που εκτελούνται σε διαφορετικά classification levels. Η ασφάλεια και η αλυσίδα εμπιστοσύνης δημιουργούνται στον επεξεργαστή και το chipset του υπολογιστή. Αυτές οι δυνατότητες υποστηρίζονται από την Τεχνολογία Virtualization Intel® (Intel® VT) και παρέχει διασφαλίσεις, μέσω της τεχνολογίας Intel® Trusted Execution Technology (Intel® TXT) και προστατεύουν κάθε εικονικό περιβάλλον από μόλυνση κακόβουλων προγραμμάτων.



Εικόνα 16: Αρχιτεκτονική Secure view [15]

Το SecureView παρέχει έμπιστη εκκίνηση με υποστήριξη υλικού, διατηρεί απομόνωση μεταξύ πολλαπλών ανεξάρτητων εικονικών μηχανών και επαληθεύει την ακεραιότητα του πελάτη κατά την εκκίνησή του. Γίνονται μετρήσεις της κατάστασης του υπολογιστή, οι οποίες κρυπτογραφούνται και αποθηκεύονται κατά την εγκατάσταση. Κατά την επόμενη εκκίνηση του συστήματος, επαναλαμβάνονται οι μετρήσεις και τα κλειδιά κρυπτογράφησης αποσφραγίζονται μόνο εάν ταιριάζουν με την κατάλληλη κρυπτογραφική απόκριση από την αξιόπιστη πλατφόρμα (TPM).

Εικόνα 17: Secure view [17]

3.7 Άλλες Χρήσεις

Παρακάτω παρουσιάζονται διάφορες εφαρμογές που κάνουν χρήση του TPM.

Πίνακας 7: Εφαρμογές και SDKs που χρησιμοποιούν TPM

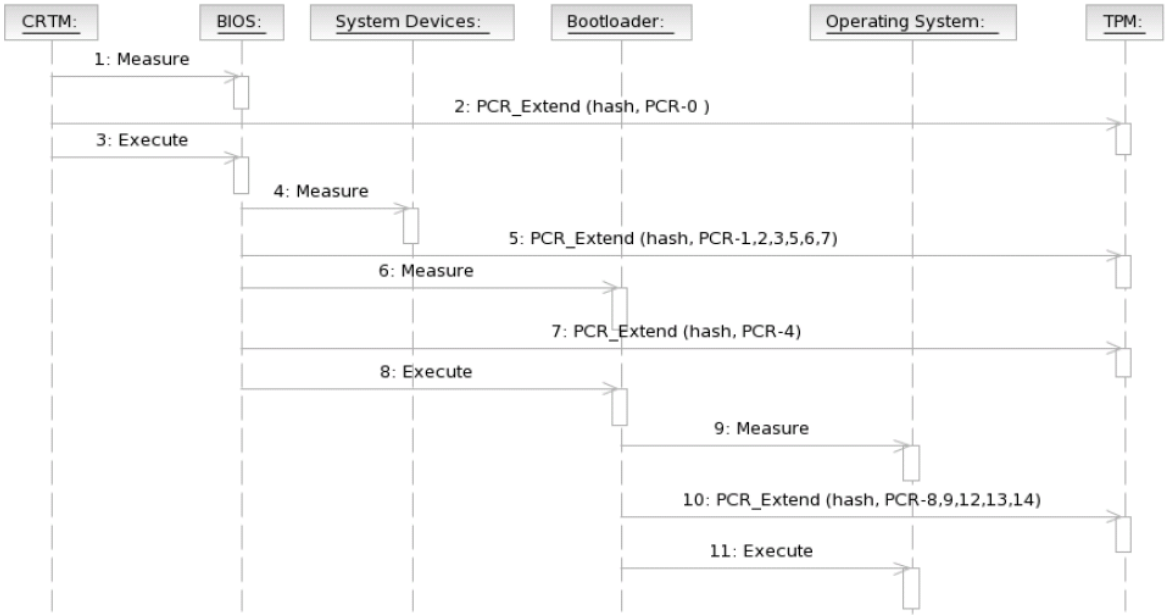
Application Type	Application Name	Interface	OS
VPN	StrongSwan clients (used in Linux, BSD, Solaris, and so on)	TrouSerS (1.2)	Linux
	Cisco client VPNs.	Wave Systems (MS CAPI) Charismathics (1.2)	Windows
	Microsoft embedded VPN or DirectAccess can directly use either TPM 1.2 or TPM 2.0 in Windows 8.	Microsoft TBS TPM Base Services (1.2 or 2.0)	Windows
	Checkpoint Firewall VPN can use the TPM.	(1.2)	
	TypeSafe (TPM-backed TLS).	jTSS (1.2)	Linux
Attestation	Wave Systems Embassy client/ERAS server package.	TrouSerS (1.2)	Windows
	Wave Systems Endpoint Monitor	TrouSerS (1.2)	Windows
	Strong Swan TNC solution hooked to the TPM with PTS.	(1.2)	Linux
	NCP's Secure VPN GovNet Box (a separate box interposed between a computer and the network that establishes a secure VPN). The software is tested using TPM attestation.	(1.2)	Unknown
	AnyConnect	(1.2)	
	JW Secure has written an application that is Kerberos-like for Windows.	Microsoft TBS TPM Base Services (2.0)	Windows
	Integrity Measurement Architecture.	TrouSerS (1.2)	Linux, Unix-like OSs

Application Type	Application Name	Interface	OS
	TPM Quote tools (SourceForge)	TrouSerS (1.2)	Linux, Windows
	TrustedGRUB	Direct (1.2)	Linux
	TVE	Trousers(1.2)	Linux
	Tboot	Direct(1.2)	Windows, Linux
	Flicker	Direct / Trousers (1.2)	Windows
Full disk encryption	Microsoft BitLocker	Microsoft TBS TPM Base Services (1.2, 2.0)	Windows
	dm-crypt	Direct (1.2)	Linux, Android
	SecureDoc		
File and folder encryption	Pretty Good Privacy (PGP)	PKCS #11 (1.2)	Windows
	OpenPGP	PKCS #11(1.2)	Linux
E-mail	Thunderbird for encrypted e-mail and signed e-mail	PKCS #11(1.2)	Windows, Linux
	Outlook	MS CAPI(1.2, 2.0)	Windows
Web browsers	Internet Explorer	MS CAPI(1.2, 2.0)	Windows
	Firefox	PKCS #11(1.2)	Windows Linux
	Chrome	PKCS #11(1.2)	Windows Linux
TPM Manager	TPM Manager (SourceForge)	microTSS (1.2)	Linux

4. ATTESTATION

4.1 Bootloader

Παρακάτω περιγράφεται η αλυσίδα εμπιστοσύνης κατά τη διαδικασία εκκίνησης ενός συστήματος με TPM.



Εικόνα 18: Η αλυσίδα εμπιστοσύνης με ένα TCG-enabled Bootloader[18]

1.CRTM (Core Root of Trust for Measurement): Το CRTM μετράει το BIOS και επεκτείνει τα αποτελέσματα στο TPM.

2.BIOS: Το BIOS μετρά όλο το firmware πριν από την εκτέλεση καθώς και το bootloader (αποθηκευμένο στο MBR του μέσου εκκίνησης) και επεκτείνει τα αποτελέσματα στα PCRs του TPM.

3.Bootloader: Ο bootloader συνεχίζει την αλυσίδα εμπιστοσύνης, μετρώντας όλα τα αρχεία του λειτουργικού συστήματος που έχουν φορτωθεί και επεκτείνοντας τα αποτελέσματα στο TPM.

4.Ο πυρήνας του OS: Σε αυτό το σημείο της αλυσίδας εμπιστοσύνης, το λειτουργικό σύστημα πρέπει να διασφαλίσει ότι η αλυσίδα συνεχίζεται για να διατηρηθεί η διαμόρφωση της πλατφόρμας, ακόμα και αν το σύστημα αλλάξει κατά την εκτέλεση. Μετά την εκκίνηση του bootstrapping, το λειτουργικό σύστημα θα έπρεπε να έχει φορτωθεί, όλοι οι κώδικες που εκτελέστηκαν θα μετρηθούν και θα επεκταθούν στο TPM.

Η διαμόρφωση της πλατφόρμας αντικατοπτρίζεται πλέον από τις τιμές των PCRs εντός του TPM και είναι έτοιμη να επιβεβαιώσει την ακεραιότητά του ή να την πιστοποιήσει σε μια εξωτερική οντότητα.

Δεδομένου ότι ο ορισμός TCG του TrustedBoot τελειώνει αμέσως μετά τη διαδικασία εκκίνησης, είναι ευθύνη του τρέχοντος λειτουργικού συστήματος να συνεχίσει την αλυσίδα εμπιστοσύνης. Πολλές προσεγγίσεις βρίσκονται επί του παρόντος υπό έρευνα και / ή εφαρμογή. Η IBM, για παράδειγμα, έχει εφαρμόσει την εν λόγω επέκταση IMA για Linux.

4.2 IMA

Η IMA είναι ένα open source trusted computing στοιχείο. Η IMA διατηρεί μια λίστα μέτρησης χρόνου εκτέλεσης και, εάν αποθηκεύεται σε μια μονάδα Trusted Platform Module (TPM), μια συνολική τιμή ακεραιότητας αυτής της λίστας. Το πλεονέκτημα της αποθήκευσης της συνολικής τιμής ακεραιότητας στο TPM είναι ότι η λίστα μετρήσεων δεν μπορεί να υπονομευθεί από οποιαδήποτε επίθεση λογισμικού, χωρίς να είναι ανιχνεύσιμη. Ως εκ τούτου, σε ένα αξιόπιστο σύστημα εκκίνησης, η IMA μπορεί να χρησιμοποιηθεί για να πιστοποιήσει την ακεραιότητα του χρόνου εκτέλεσης του συστήματος.

Οι παρακάτω ενότητες παρέχουν διάφορες λειτουργίες ακεραιότητας:

- Συλλογή - μέτρηση ενός αρχείου πριν από την πρόσβαση σε αυτό.
- Αποθήκευση - προσθέτει τη μέτρηση σε μια λίστα του πυρήνα και, αν υπάρχει Trusted Platform Module (TPM) ,επεκτείνει το IMA PCR.
- Βεβαίωση - αν υπάρχει, χρησιμοποιεί το TPM για να υπογράψει την τιμή IMA PCR, ώστε να επιτρέψει την απομακρυσμένη επικύρωση της λίστας μετρήσεων.
- Εκτίμηση - επιβολή τοπικής επικύρωσης μιας μέτρησης έναντι μιας καλής αποθηκευμένης τιμής.
- Προστασία - προστατεύει τα χαρακτηριστικά επέκτασης ασφαλείας ενός αρχείου (συμπεριλαμβανομένου του hash εκτίμησης) από off-line attack.

Οι στόχοι του υποσυστήματος ακεραιότητας του πυρήνα είναι να ανιχνεύσουν αν τα αρχεία έχουν αλλοιωθεί με τυχαίο η κακόβουλο τρόπο, τόσο εξ αποστάσεως όσο και τοπικά, να εκτιμήσουν τη μέτρηση ενός αρχείου έναντι μιας σωστής τιμής που αποθηκεύεται ως εκτεταμένο χαρακτηριστικό και την επιβολή της ακεραιότητας τοπικών αρχείων. Αυτοί οι στόχοι είναι συμπληρωματικοί ως προς τις Προστασίες Υποχρεωτικού Ελέγχου Πρόσβασης (MAC) που παρέχονται από τις μονάδες LSM, όπως το SElinux και το Smack, οι οποίοι, ανάλογα με την πολιτική, μπορούν να επιχειρήσουν να προστατεύσουν την ακεραιότητα των αρχείων.[19]

5. ΠΑΡΑΔΕΙΓΜΑ ATTESTATION

Το παράδειγμα[21] περιλαμβάνει 5 βασικά κομμάτια:

1. Ένα διακομιστή βεβαίωσης(attestation server)
2. Ένα πελάτη βεβαίωσης που ωθεί τιμές στο διακομιστή(attestation client)
3. Ένα πελάτη εγγραφής που εγγράφει ένα κλειδί υπογραφής με το διακομιστή
4. Ένα βοηθητικό πρόγραμμα για την παροχή πιστοποιητικού EK στο SW TPM για δοκιμές
5. Demo κώδικας php για την εμφάνιση των αποτελεσμάτων

Ο κώδικας είναι σε γλώσσα C, με μορφοποίηση json στη διεπαφή πελάτη / διακομιστή. Η MySQL χρησιμοποιείται για αποθήκευση δεδομένων. Το web UI απαιτεί ένα web server, php και τη διεπαφή php στη βάση δεδομένων mysql. Περιλαμβάνει τις βεβαιώσεις BIOS και IMA (Integrity Measurement Architecture), συμπεριλαμβανομένης της επικύρωσης των event logs και της επαλήθευσης της υπογραφής IMA.

5.1 Εντολές TPM

Μεταξύ των εντολών είναι:

- Δημιουργία ενός EK από ένα πρότυπο χρησιμοποιώντας την εντολή TPM2_CreatePrimary.
- Επικύρωση πιστοποιητικών EK με τα πιστοποιητικά ρίζας του προμηθευτή TPM.
- Δημιουργία, φόρτωση και χρήση κλειδιού υπογραφής βεβαίωσης.
- Οι διαδικασίες Make Credential και Activate Credential, συμπεριλαμβανομένης της δημιουργίας, κρυπτογράφησης και αποκρυπτογράφησης της πρόκλησης.
- Χρήση του TPM2_Quote για την υπογραφή των PCRs.
- Parsing του αρχείου συμβάντων TPM 2.0.
- Parsing του αρχείου IMA μορφής TPM 1.2.
- Παραδείγματα RSA και ελλειπτικών καμπυλών για τα κλειδιά επικύρωσης και βεβαιώσεων.

Εγγραφή και ροή βεβαίωσης.

Αυτές οι ροές ακολουθούν τα πρότυπα πρωτόκολλα TCG.

Κωδικός βάσης δεδομένων

Η πρόσβαση στη βάση δεδομένων είναι ενσωματωμένη στον κώδικα.

Σχήμα βάσης δεδομένων

Ενώ το σχήμα αντιπροσωπεύει τυπική αποθήκευση, ορισμένα πεδία, όπως ο κατασκευαστής TPM, είναι αποκλειστικά για το demo.

Κρυπτογραφική εφαρμογή

Παρόμοια με τη βάση δεδομένων, ο κωδικός κρυπτογράφησης χρησιμοποιεί το OpenSSL.

Privacy CA

Σε μια εφαρμογή παραγωγής δεν πρέπει να υπάρχει η privacy CA στο διακομιστή βεβαίωσης. Θα πρέπει να βρίσκεται σε ξεχωριστή πλατφόρμα με απομόνωση για ασφάλεια. Το πιστοποιητικό X.509 του κλειδιού πιστοποίησης είναι ένας ελάχιστος φορέας για το δημόσιο κλειδί του πελάτη.

Μορφή αρχείου καταγραφής IMA

Ο IMA log parser είναι hard coded στη μορφή TPM 1.2 SHA-1.

Κλειδιά επαλήθευσης IMA

Ο διακομιστής χρησιμοποιεί 1 κλειδί για επικύρωση υπογραφών IMA.

Μορφή ανταλλαγής δεδομένων διακομιστή πελάτη

Τα δεδομένα αποστέλλονται σε json, με δυαδικούς πίνακες που στέλνονται ως hex ascii. Το json υποστηρίζεται καλά από τις βιβλιοθήκες δημιουργίας και ανάλυσης και η μορφή κειμένου διευκολύνει την αποσφαλμάτωση.

Διεπαφή δικτύου διακομιστή πελάτη

Αυτή τη στιγμή δεν υπάρχει έλεγχος ταυτότητας υπολογιστή-πελάτη ή διακομιστή και τα δεδομένα αποστέλλονται σε ορατή μορφή. Ο έλεγχος ταυτότητας διακομιστή και η κρυπτογράφηση ενδέχεται να απαιτούνται για εξασφάλιση ιδιωτικότητας.

5.2 Διαδικασία Provisioning

Παρακάτω περιγράφεται η διαδικασία provisioning για το attestation key ανάμεσα στο μηχάνημα που εκτελεί το attestation (πελάτης) και στο μηχάνημα που επαληθεύει το attestation(διακομιστής).

Η διαδικασία αποτελείται από τέσσερα βήματα:

- client request
- server challenge
- client response
- server acknowledge

5.2.1 Αίτημα πελάτη

1. Ο πελάτης δημιουργεί το κλειδί SRK αν δεν υπάρχει ήδη. Η εντολή TPM2_CreatePrimary() παράγει ένα επαναλαμβανόμενο ζεύγος κλειδιών όταν χρησιμοποιείται το ίδιο πρότυπο.
2. Ο πελάτης δημιουργεί ένα κλειδί υπογραφής βεβαίωσης κάτω από το SRK.
3. Ο πελάτης διαβάζει το πιστοποιητικό EK από το χώρο TPM NV.
4. Ο πελάτης στέλνει το αίτημα εγγραφής στον διακομιστή. Η αίτηση αποτελείται από:

- command - enrollrequest
- hostname - client hostname
- ekcert - EK certificate (X.509 DER format)
- public - attestation key public part (TPMT_PUBLIC structure)

5.2.2 Server Challenge

Ο διακομιστής λαμβάνει την αίτηση εγγραφής, με ένα όνομα κεντρικού υπολογιστή, πιστοποιητικό EK και δημόσιο κλειδί βεβαίωσης. Ο πελάτης ισχυρίζεται ότι το πιστοποιητικό προέρχεται από ένα αυθεντικό TPM. Ο διακομιστής δεν εμπιστεύεται την αξίωση.

1. Ο διακομιστής ελέγχει αν το hostname του υπολογιστεί δεν έχει εγγραφεί προηγουμένως.

2. Ο διακομιστής επικυρώνει το πιστοποιητικό EK συγκρίνοντάς το με λίστα πιστοποιητικών ρίζας του προμηθευτή TPM. Εάν το πιστοποιητικό είναι έγκυρο, ο διακομιστής εμπιστεύεται ότι το πιστοποιητικό προέρχεται από ένα αυθεντικό TPM, αλλά δεν εμπιστέυεατι ότι αυτό προέρχεται από το TPM του πελάτη.

3. Ο διακομιστής εξάγει το δημόσιο κλειδί EK από το πιστοποιητικό EK.

4. Ο διακομιστής επικυρώνει τις ιδιότητες δημόσιου κλειδιού βεβαίωσης: fixedTPM, fixedParent, sensitiveDataOrigin, sign, restricted, not decrypt, RSASSA algorithm, SHA-256 και RSA 2048-bit . Αυτές είναι οι απαιτούμενες ιδιότητες ενός κλειδιού βεβαίωσης. Έχει παραχθεί από ένα TPM, δεν μπορεί να αντιγραφεί έξω από το TPM, και είναι περιορισμένο να υπογράφει μόνο δεδομένα του TPM όπως το quote. Ο διακομιστής δεν εμπιστεύεται ότι το κλειδί προέκυψε από το TPM του πελάτη, καθώς έχει λάβει μόνο το δημόσιο μέρος.

5. Ο διακομιστής παράγει το πιστοποιητικό X.509 για το δημόσιο κλειδί βεβαίωσης και το υπογράφει με το ιδιωτικό κλειδί της CA. Χρησιμοποιεί το όνομα υπολογιστή-πελάτη ως αντικείμενο CN(κοινό όνομα).

6. Ο διακομιστής παράγει ένα τυχαίο κλειδί AES-256.

7. Ο διακομιστής κρυπτογραφεί το κλειδί πιστοποίησης X.509 με αυτό το κλειδί AES.

8. Ο διακομιστής φορτώνει (TPM2_LoadExternal) το δημόσιο κλειδί βεβαίωσης, χρησιμοποιώντας το TPM του για να υπολογίσει το όνομα. Το όνομα είναι ένα hash του δημόσιου μέρους.

9. Ο διακομιστής φορτώνει το δημόσιο κλειδί EK του πελάτη, το οποίο εξάγεται από το πιστοποιητικό EK.

10. Ο διακομιστής εκτελεί την εντολή TPM2_MakeCredential(), παρέχοντας το EK handle, το κλειδί AES και το όνομα του κλειδιού βεβαίωσης. Η εντολή TPM2_MakeCredential() συνδέει το κλειδί AES και το όνομα, και στη συνέχεια κρυπτογραφεί το αποτέλεσμα με το δημόσιο κλειδί EK. Αυτό γίνεται η πρόκληση του διακομιστή στον πελάτη.

11. Ο διακομιστής αποθηκεύει το όνομα κεντρικού υπολογιστή και το πιστοποιητικό στον πίνακα "machines" της βάσης δεδομένων. Εντούτοις, ορίζει ότι η σειρά είναι

άκυρη, καθώς ο διακομιστής εξακολουθεί να μην γνωρίζει αν το πιστοποιητικό EK ή το κλειδί βεβαίωσης προέρχονται από το TPM του πελάτη.

12. Ο διακομιστής στέλνει την απάντηση στην αίτηση εγγραφής:

- Απάντηση - αίτημα εγγραφής
- Enccert- κρυπτογραφημένο πιστοποιητικό κλειδιού βεβαίωσης
- Credentialblob – η έξοδος της εντολής TPM2_MakeCredential()
- Μυστικό - κλειδί AES κρυπτογραφημένο με το δημόσιο κλειδί EK του πελάτη.

5.2.3 Client Response

Ο πελάτης λαμβάνει την πρόκληση, την απάντηση του διακομιστή στο αίτημα εγγραφής.

1. Ο πελάτης ξαναδημιουργεί το EK χρησιμοποιώντας είτε το προεπιλεγμένο πρότυπο είτε το πρότυπο και το nonce από τη TPM NV.

2. Ο πελάτης φορτώνει το κλειδί βεβαίωσης που αποθηκεύτηκε προηγουμένως.

3. Ο πελάτης εκτελεί την εντολή TPM2_ActivateCredential(), καθορίζοντας το credentialBlob, το κρυπτογραφημένο μυστικό, το EK handle και το handle του κλειδιού πιστοποίησης. Η χρήση του EK απαιτεί μια σύνοδο πολιτικής με μυστικό πολιτικής εναντίον της εξουσιοδότησης επικύρωσης.

4. Το TPM πελάτη επικυρώνει την εξουσιοδότηση: την πολιτική EK για το EK και έναν κενό κωδικό πρόσβασης για το κλειδί πιστοποίησης.

5. Ο πελάτης TPM επικυρώνει την ακεραιότητα του credentialblob έναντι του EK.

6. Το TPM πελάτη επικυρώνει ότι το όνομα του φορτωμένου κλειδιού βεβαίωσης ταιριάζει με αυτό στο credentialBlob. Αυτός ο έλεγχος εμποδίζει τον πελάτη από το να στείλει ένα κλειδί βεβαίωσης στον εξυπηρετητή διαφορετικό από αυτό που παράχθηκε από το TPM.

7. Στη συνέχεια, το TPM του πελάτη αποκρυπτογραφεί το μυστικό χρησιμοποιώντας το EK ιδιωτικό κλειδί για να ανακτήσει το κλειδί AES. Αυτό το βήμα αποδεικνύει ότι ο πελάτης χρησιμοποιεί ένα αυθεντικό TPM για να δημιουργήσει το κλειδί βεβαίωσης.

8. Ο πελάτης χρησιμοποιεί το κλειδί AES για να αποκρυπτογραφήσει το πιστοποιητικό X.509.

9. Ο πελάτης αποστέλλει εντολή στο διακομιστή ζητώντας την εγγραφή του πιστοποιητικού.

• εντολή - enrollcert

• hostname - όνομα κεντρικού υπολογιστή πελάτη

• akcert - το πιστοποιητικό X.509 του κλειδιού βεβαίωσης.

5.2.4 Server Acknowledge

1. Ο διακομιστής ανακτά το μη έγκυρο ακόμα πιστοποιητικό από τη βάση δεδομένων του μηχανήματος, με βάση το hostname.

2. Ο διακομιστής ταιριάζει με το πιστοποιητικό πελάτη στο πιστοποιητικό που δημιουργεί ο διακομιστής. Αυτό αποδεικνύει ότι ο πελάτης θα μπορούσε να αποκρυπτογραφήσει το κλειδί AES (πρόκληση) και στη συνέχεια το πιστοποιητικό. Ο πελάτης θα μπορούσε να το κάνει μόνο αν είχε το ιδιωτικό κλειδί EK (γνωστό από το αυθεντικό TPM) και ένα κλειδί βεβαίωσης με τις ιδιότητες που επικυρώθηκαν από το διακομιστή (επειδή το TPM ταιριάζει το όνομα). Η αντιστοίχιση πιστοποιητικών είναι σημαντική. Δεν αρκεί η διαπίστωση ότι το πιστοποιητικό X.509 είναι έγκυρο, δεδομένου ότι ο πελάτης θα μπορούσε να προσπαθήσει να εγκαταστήσει ένα πλαστό. Πρέπει να είναι το πιστοποιητικό που δημιούργησε ο διακομιστής.

3. Ο διακομιστής επισημαίνει το πιστοποιητικό ως έγκυρο στη βάση δεδομένων.

4. Ο διακομιστής στέλνει μια τελική επιβεβαίωση στον πελάτη.

- response - enrollcert

Μετά το acknowledge του διακομιστή, ο πελάτης αποθηκεύει το δημόσιο και ιδιωτικό μέρος του κλειδιού βεβαίωσης στο σύστημα αρχείων για μελλοντική χρήση κατά την υπογραφή quotes.

5.3 Διαδικασία Quote

Η διαδικασία αποτελείται από έξι βήματα:

- Ο πελάτης ζητά ένα nonce
- Ο διακομιστής παρέχει το nonce και μια επιλογή για το PCR
- Ο πελάτης επιστρέφει τα δεδομένα του quote
- Άιτηση διακομιστή για αρχείο καταγραφής συμβάντων
- Ο πελάτης επιστρέφει το αρχείο καταγραφής συμβάντων
- Αποδοχή διακομιστή

5.3.1 Αίτημα πελάτη για το nonce

1. Ο πελάτης στέλνει το αίτημα για το nonce στο διακομιστή. Η αίτηση αποτελείται από:

- command - nonce
- hostname - όνομα υπολογιστή-πελάτη
- User ID - ο λογαριασμός πελάτη που δημιούργησε το αίτημα (μη αξιόπιστο, για αναφορά)

5.3.2 Ο διακομιστής παρέχει το nonce και την επιλογή PCR

1. Ο διακομιστής αποκρίνεται με ένα nonce και ένα bitmap από PCRs που ο πελάτης θα πρέπει να παραθέσει. Η επιλογή PCR είναι επί του παρόντος σκληρά κωδικοποιημένη

σε "όλα τα PCR". Υπάρχει ελάχιστο όφελος σε θέμα απόδοσης στην αναφορά λιγότερων PCRs. Ο διακομιστής μπορεί να αγνοήσει τα PCR που δεν τον ενδιαφέρουν.

- response - nonce
- nonce - ένα 32 byte nonce
- pcrselect - όλες οι PCR

5.3.3 Ο πελάτης επιστρέφει τα quote δεδομένα

1. Ο πελάτης εκτελεί την εντολή TPM2_Load για να φορτώσει το κλειδί βεβαίωσης.

2. Ο πελάτης εκτελεί την εντολή TPM2_Quote, παρέχοντας τις επιλογές nonce και PCR και υπογράφει με το φορτωμένο κλειδί βεβαίωσης.

3. Ο πελάτης εκτελεί την εντολή TPM2_PCR_Read πολλές φορές για να διαβάσει τα επιλεγμένα PCR.

4. Ο πελάτης αποστέλλει το quote στο διακομιστή.

- command - quote
- hostname - όνομα κεντρικού υπολογιστή πελάτη
- pcr0 - pcr23
- quote δεδομένα
- υπογραφή quote
- ώρα εκκίνησης πελάτη

5.3.4 Αίτηση διακομιστή για αρχείο καταγραφής συμβάντων

Ο διακομιστής επικυρώνει το quote και στη συνέχεια ζητά το αρχείο καταγραφής συμβάντων.

1. Ο διακομιστής ανακτά το πιστοποιητικό κλειδιού βεβαίωσης πελάτη.

2. Αυτό το πιστοποιητικό χρησιμοποιείται για την επαλήθευση της υπογραφής στα δεδομένα του quote.

3. Ο διακομιστής ανασυνθέτει τη σύνοψη quote των δεδομένων των PCR από τα PCRs. Ταιριάζει με το αποτέλεσμα με αυτό που έλαβε από τον πελάτη. Ο διακομιστής τώρα εμπιστεύεται ότι οι τιμές PCR που αποστέλλονται από τον πελάτη είναι αυθεντικές.

4. Ο διακομιστής ταιριάζει το δικό του αντίγραφο nonce με εκείνο στα δεδομένα quote.

Ο διακομιστής εμπιστεύεται τώρα ότι το quote είναι πρόσφατο και όχι μια επανάληψη προηγούμενου quote.

5. Ο διακομιστής στέλνει μια απάντηση στον πελάτη:

• response – quote

5.3.5 Ο πελάτης επιστρέφει το αρχείο καταγραφής συμβάντων

Ο πελάτης λαμβάνει την απόκριση quote, υποδεικνύοντας ότι το quote ήταν έγκυρο. Ο πελάτης στη συνέχεια στέλνει το αρχείο καταγραφής συμβάντων.

1. Ο πελάτης αποστέλλει εντολή στον εξυπηρετητή ζητώντας την επεξεργασία του αρχείου καταγραφής συμβάντων.

- command - biosentry
- hostname - όνομα κεντρικού υπολογιστή πελάτη
- nonce – το nonce του πελάτη
- eventn - οι καταχωρήσεις του αρχείου καταγραφής συμβάντων

5.3.6 Αποδοχή διακομιστή

Ο διακομιστής επεξεργάζεται το αρχείο καταγραφής συμβάντων.

1. Ο διακομιστής ταιριάζει το nonce με το nonce του πελάτη που χρησιμοποιήθηκε για το quote.

Ο διακομιστής χρησιμοποιεί το nonce σαν ένα είδος one time password. Ο πελάτης αντηχεί το quote nonce με το αρχείο καταγραφής συμβάντων και ο διακομιστής ελέγχει για μια αντιστοίχιση. Αυτό εμποδίζει έναν κακόβουλο που παριστάνει το πελάτη, από το να στείλει ένα λανθασμένο αρχείο καταγραφής συμβάντων. Υποθέτει ότι το nonce είναι μια τυχαία τιμή που δεν μπορεί να μαντέψει ο κακόβουλος.

Αυτό είναι περιττό εάν ο υπολογιστής-πελάτης διατηρεί μια σταθερή σύνδεση με τον διακομιστή μέσω της διαδικασίας ή εάν ο υπολογιστής-πελάτης χρησιμοποιεί μια επαληθευμένη σύνδεση.

2. Ο διακομιστής επεξεργάζεται το αρχείο καταγραφής συμβάντων, ανακατασκευάζοντας τις τιμές PCR. Σε κάθε βήμα, ελέγχει για PCR που ταιριάζουν. Όταν ταιριάζουν όλα τα PCR, ο διακομιστής ολοκληρώνει την επεξεργασία.

Ενδέχεται να υπάρχουν περισσότερες καταχωρίσεις στο αρχείο καταγραφής συμβάντων από αυτές που χρησιμοποιήθηκαν για το quote. Ο διακομιστής αγνοεί τις καταχωρίσεις.

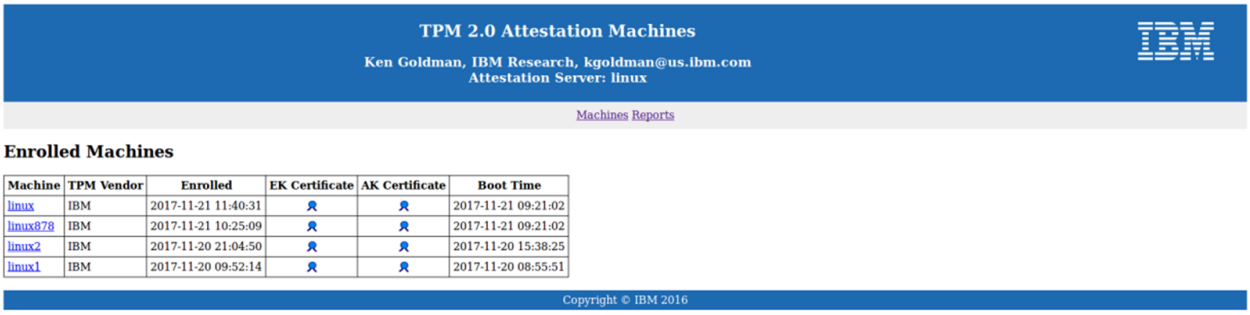
3. Ο διακομιστής στέλνει μια τελική επιβεβαίωση στον πελάτη.

- response - biosentry

5.4 Εφαρμογή

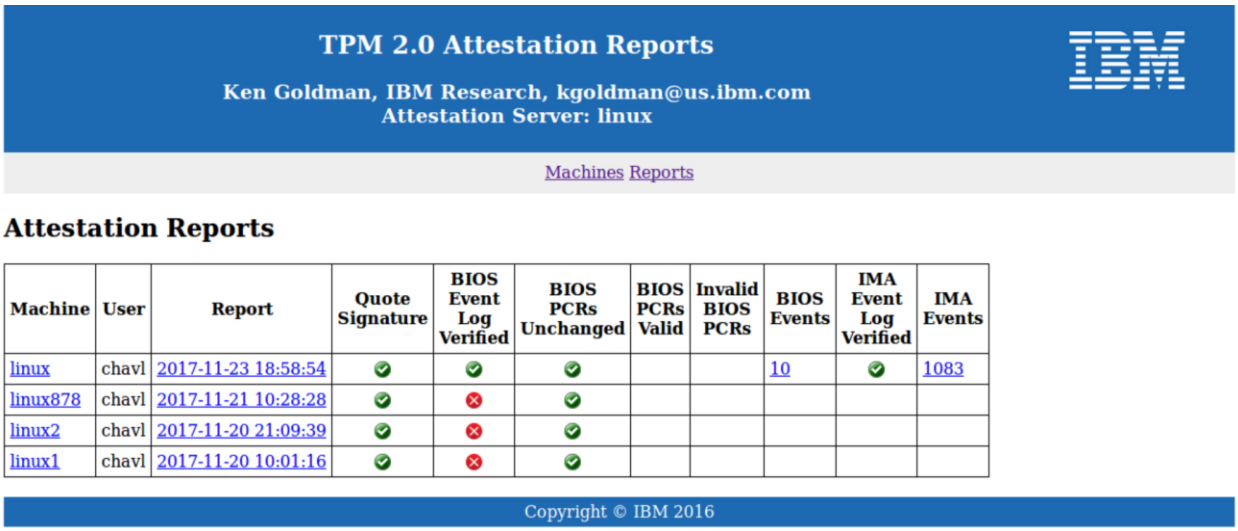
Για την εφαρμογή χρησιμοποιήθηκε λογισμικό της IBM. Συγκεκριμένα έγινε χρήση του software TPM [22], του λογισμικού IBMTSS [23] καθώς και του λογισμικού IBMACS [21]. Παρακάτω ακολουθούν μερικά screenshots από την εφαρμογή:

Παρακάτω φαίνονται οι εγγεγραμένοι υπολογιστές.



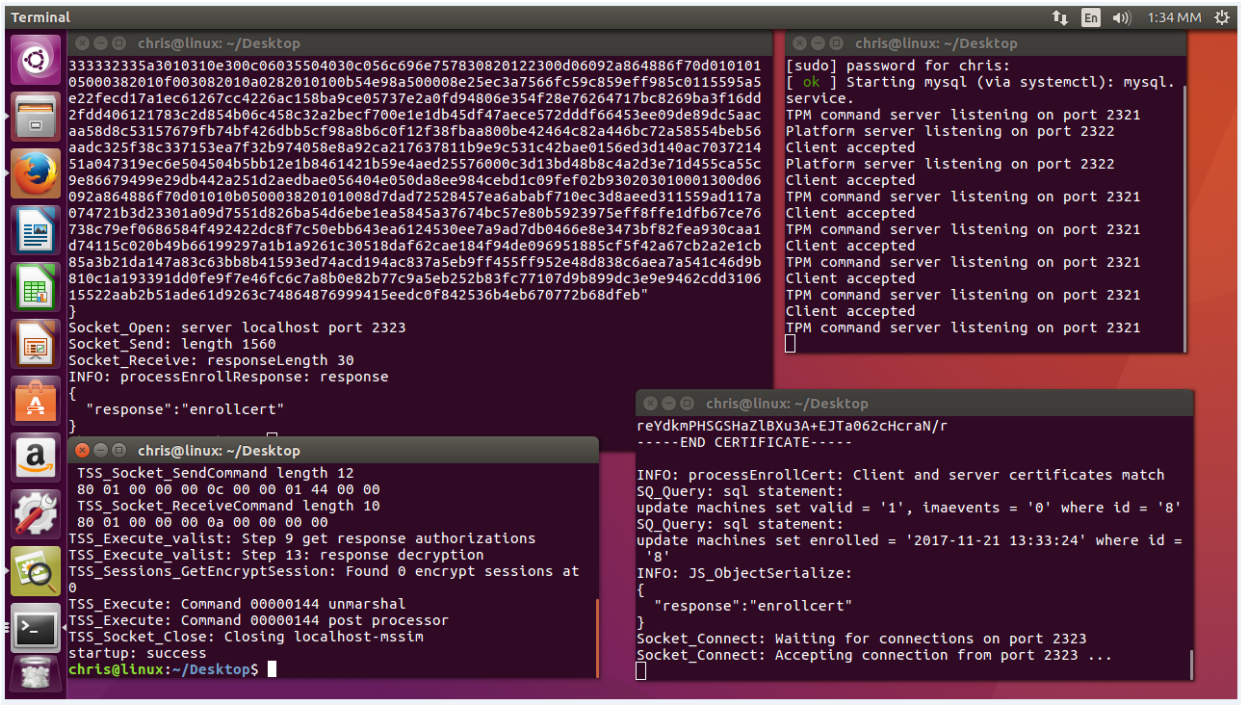
Εικόνα 19:Εγγεγραμένοι υπολογιστές

Τα attestation reports.



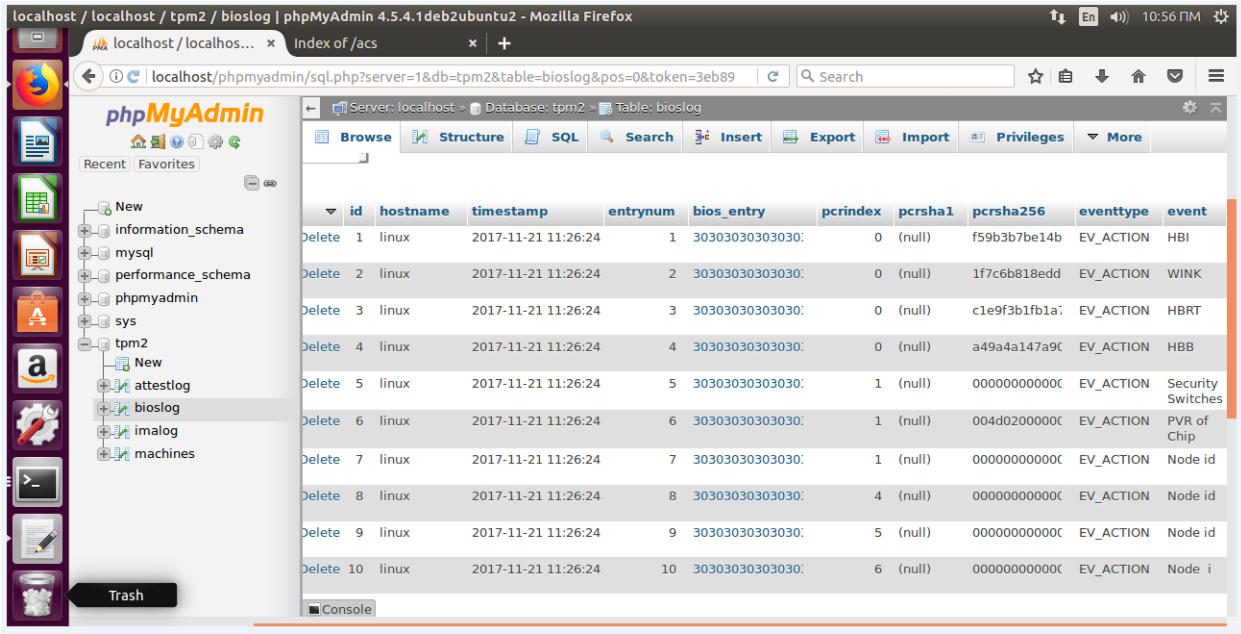
Εικόνα 20:Attestation Reports

Terminals:



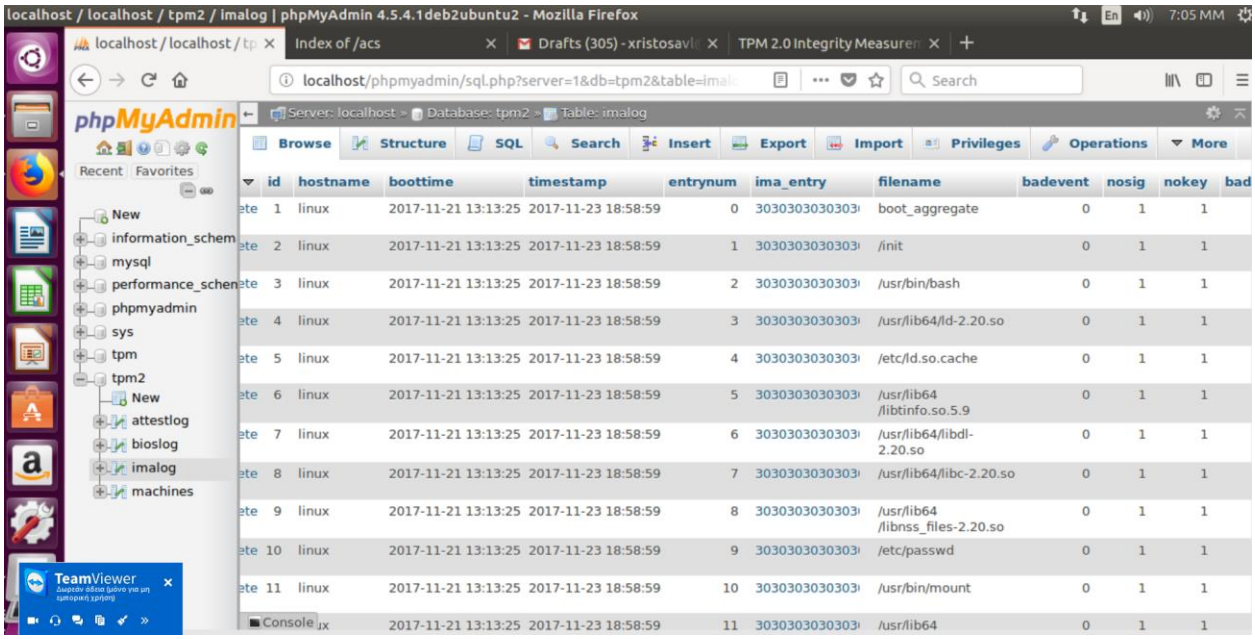
Εικόνα 21: Terminals

Πίνακας bioslog από τη βάση δεδομένων.



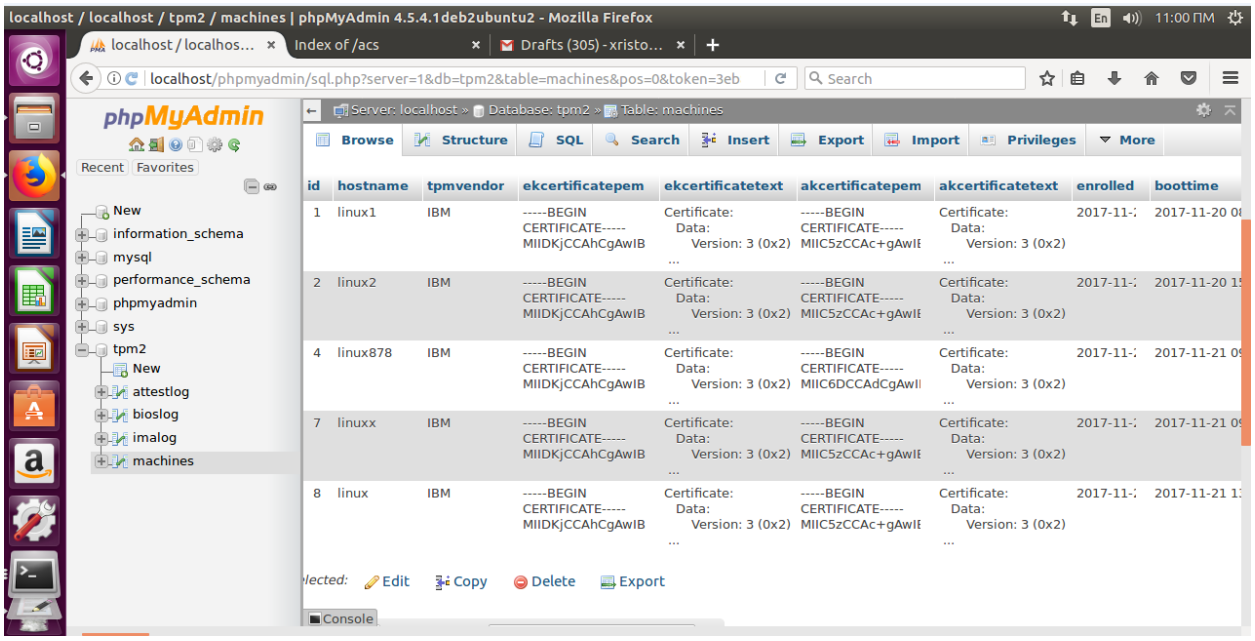
Εικόνα 22: Πίνακας bioslog

Πίνακας imalog από τη βάση δεδομένων.



Εικόνα 23:Πίνακας imalog

Πίνακας machines από τη βάση δεδομένων.



Εικόνα 24: Πίνακας machines

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το πρότυπο TPM ορίζει μια ρίζα εμπιστοσύνης υλικού (hardware root of trust) ευρέως αποδεκτή ως ασφαλέστερη από τη λύση λογισμικού η οποία μπορεί να παραβιαστεί ευκολότερα από τους εισβολείς. Τα οφέλη της ασφάλειας που προσφέρει το TPM χρησιμοποιούνται από διάφορες συσκεύες όπως υπολογιστές, εξοπλισμό δικτύου και ενσωματωμένα συστήματα με επιτυχία.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Attestation Key	Κλειδί βεβαίωσης
Certificate Authority	Αρχή Πιστοποίησης
Core Root of Trust for Measurement	Βασική ρίζα εμπιστοσύνης για μέτρηση
Counter mode	Λειτουργία μετρητή
Dynamic RTM	Δυναμικό RTM
Dictionary attack	Επίθεση λεξικού
Denial of Service	Άρνηση παροχής υπηρεσίας
Digital Signature Algorithm	Αλγόριθμος Ψηφιακής Υπογραφής
Enhanced Authorization	Ενισχυμένη εξουσιοδότηση
Endorsement Key	Κλειδί επικύρωσης
Endorsement Primary Seed	Επικύρωση πρωτογενούς σπόρου
Hash Message Authentication Code	Κωδικός ελέγχου εξακρίβωσης μηνυμάτων Hash
Initialization Vector	Διάνυσμα αρχικοποίησης
Key derivation function	Συνάρτηση εξαγωγής κλειδιών
Physical Presence	Φυσική παρουσία
Platform Primary Seed	Πρωτογενής σπόρος πλατφόρμας
Pseudo-random function	Ψευδοτυχαία συνάρτηση
Pseudo-random number generator	Ψευδοτυχαία γεννήτρια αριθμών
Random number generator	Γεννήτρια τυχαίων αριθμών
Root of Trust for Measurement	Ρίζα εμπιστοσύνης για μέτρηση
Root of Trust for Reporting	Ρίζα της εμπιστοσύνης για αναφορά
Root of Trust for Storage	Ρίζα της εμπιστοσύνης για αποθήκευση
Static RTM	Στατικό RTM
Secure Hash Algorithm	Ασφαλής Αλγόριθμος Hash

Storage Primary Seed	Πρωτογενής σπόρος αποθήκευσης
Storage Root Key	Ριζικό κλειδί αποθήκευσης
Trusted building block	Αξιόπιστο δομικό στοιχείο
Trusted computing base	Αξιόπιστη βάση υπολογισμού
Trusted Computing Group	Ομάδα αξιόπιστων υπολογιστών
Trusted Platform Module	Αξιόπιστη μονάδα πλατφόρμας
Attestation Key	Κλειδί βεβαίωσης
Certificate Authority	Αρχή Πιστοποίησης
Core Root of Trust for Measurement	Βασική ρίζα εμπιστοσύνης για μέτρηση
Counter mode	Λειτουργία μετρητή
Dynamic RTM	Δυναμικό RTM

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

AK	Attestation Key
BIOS	Basic Input/Output System
CA	Certificate Authority
CFB	Cipher Feedback mode
CPU	Central Processing Unit
CRTM	Core Root of Trust for Measurement
CTR	Counter mode
D-RTM	dynamic RTM
DA	dictionary attack
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EA	Enhanced Authorization
EAL	evaluated assurance level
ECDAA	ECC-based Direct Anonymous Attestation
ECDH	Elliptic Curve Diffie-Hellman
EK	Endorsement Key
EPS	Endorsement Primary Seed
FIPS	Federal Information Processing Standard
FUM	Field Upgrade mode
GPIO	General Purpose I/O
HMAC	Hash Message Authentication Code
I/O	Input/Output
KDF	key derivation function
LPC	Low Pin Count

LSb	Least Significant bit
LSO	Least Significant Octet
MSb	Most Significant bit
POST	Power on Self-Test
PP	Physical Presence
PPS	Platform Primary Seed
PRF	pseudo-random function
PRNG	pseudo-random number generator
RNG	random number generator
RSA	Rivest, Shamir and Adleman
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
S-RTM	static RTM
SHA	Secure Hash Algorithm
SRK	Storage Root Key
TBB	trusted building block
TCB	trusted computing base
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSS	TCG Software Stack

ΠΑΡΑΡΤΗΜΑ Ι

Παρακάτω περιγράφονται οι εντολές που υπάρχουν στην κονσόλα διαχείρισης μονάδας αξιόπιστης πλατφόρμας σε υπολογιστή windows 7 και TPM 1.2.

Όνομα εντολής	Περιγραφή
TPM_Init	Αυτή είναι η πρώτη εντολή που αποστέλλει ο υπολογιστής. Κατά τη διεργασία εκκίνησης, αυτή η εντολή αποστέλλεται στην TPM. Η εκτέλεση αυτής της εντολής δεν είναι δυνατή από το λογισμικό.
TPM_SaveState	Αυτή η εντολή προειδοποιεί την TPM να αποθηκεύσει την κατάσταση πριν την μετάβαση σε κατάσταση αναστολής λειτουργίας.
TPM_Startup	Αυτή η εντολή πρέπει να ακολουθεί την εντολή TPM_Init. Μεταδίδει πρόσθετες πληροφορίες για τον υπολογιστή στην TPM σχετικά με τον τύπο της επαναρύθμισης που συμβαίνει κατά τη διάρκεια της κλήσης.
TPM_SelfTestFull	Αυτή η εντολή δοκιμάζει όλες τις εσωτερικές συναρτήσεις της TPM. Σε περίπτωση αποτυχίας, η TPM μεταβαίνει σε κατάσταση λειτουργίας αποτυχίας.
TPM_ContinueSelfTest	Αυτή η εντολή ενημερώνει την TPM όταν δεν μπορεί να ολοκληρώσει την εσωτερική δοκιμή όλων των συναρτήσεων TPM που δεν δοκιμάστηκαν κατά τον έλεγχο στην εκκίνηση.
TPM_GetTestResult	Αυτή η εντολή παρέχει πληροφορίες για τον κατασκευαστή και διαγνωστικές πληροφορίες για τα αποτελέσματα της εσωτερικής δοκιμής.
TPM_OwnerSetDisable	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να ενεργοποιεί ή να απενεργοποιεί την TPM. Ανατρέξτε στις περιγραφές για τις εντολές TPM_PhysicalEnable και TPM_PhysicalDisable για περισσότερες πληροφορίες.

TPM_PhysicalEnable	Αυτή η εντολή ενεργοποιεί την TPM. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα. Η ενεργοποίηση της TPM περιλαμβάνει την ενεργοποίηση της TPM (με την εντολή TPM_PhysicalSetDeactivated).
TPM_PhysicalDisable	Αυτή η εντολή απενεργοποιεί την TPM. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα. Η απενεργοποίηση της TPM περιλαμβάνει την απενεργοποίηση της TPM (με την εντολή TPM_PhysicalSetDeactivated).
TPM_SetOwnerInstall	Αυτή η εντολή επιτρέπει ή δεν επιτρέπει τη δυνατότητα ορισμού κατόχου. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα.
TPM_PhysicalSetDeactivated	Αυτή η εντολή ενεργοποιεί ή απενεργοποιεί την TPM. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα. Δεν συνιστάται ο αποκλεισμός αυτής της εντολής.
TPM_SetTempDeactivated	Αυτή η εντολή επιτρέπει στο χειριστή του υπολογιστή να απενεργοποιήσει την TPM μέχρι την επόμενη επανεκκίνηση του υπολογιστή. Ο χειριστής πρέπει να έχει φυσική παρουσία στον υπολογιστή ή να δώσει την τιμή εξουσιοδότησης χειριστή που ορίστηκε με την εντολή TPM_SetOperatorAuth.
TPM_SetOperatorAuth	Αυτή η εντολή ορίζει την τιμή εξουσιοδότησης χειριστή. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα.

TSC_PhysicalPresence	Αυτή η εντολή απαιτεί τη φυσική παρουσία στον υπολογιστή. Η εκτέλεση αυτής της εντολής δεν είναι δυνατή από το λειτουργικό σύστημα.
TSC_ResetEstablishmentBit	Αυτή η εντολή δεν χρησιμοποιείται στην τρέχουσα έκδοση του BitLocker.
TPM_TakeOwnership	Αυτή η εντολή λαμβάνει την κυριότητας της TPM με νέα τιμή εξουσιοδότησης κατόχου, που προέρχεται από τον κωδικό πρόσβασης κατόχου. Μεταξύ των άλλων συνθηκών που πρέπει να πληρούνται πριν να είναι δυνατή η εκτέλεση της εντολής, η TPM πρέπει να ενεργοποιηθεί και να απενεργοποιηθεί.
TPM_OwnerClear	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να εκκαθαρίσει την TPM. Αυτό σημαίνει ότι το μόνο κλειδί που παραμένει στην TPM είναι το κλειδί έγκρισης.
TPM_DisableOwnerClear	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να απενεργοποιήσει μόνιμα την εντολή TPM_OwnerClear. Όταν χρησιμοποιείται, ο κάτοχος πρέπει να εκτελέσει την εντολή TPM_ForceClear για εκκαθάριση της TPM.
TPM_ForceClear	Αυτή η εντολή εκκαθαρίζει την TPM. Για αυτή την εντολή απαιτείται η φυσική παρουσία στον υπολογιστή και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα.
TPM_DisableForceClear	Αυτή η εντολή απενεργοποιεί την εντολή TPM_ForceClear μέχρι την επανεκκίνηση του υπολογιστή.
TPM_SetCapability	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να ορίζει τιμές για την TPM.
TPM_GetCapability	Αυτή η εντολή επιστρέφει πληροφορίες για την TPM.
TPM_GetAuditDigest	Αυτή η εντολή επιστρέψει τη σύνοψη ελέγχων για την TPM.
TPM_GetAuditDigestSigned	Αυτή η εντολή επιστρέφει μια υπογεγραμμένη σύνοψη ελέγχων για την TPM και μια λίστα με τις εντολές που ελέγχονται.

TPM_SetOrdinalAuditStatus	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να καθορίσει μια σημαία ελέγχου για έναν δεδομένο αριθμό εντολής. Όταν είναι ενεργοποιημένη η σημαία, η εντολή επιστρέφει έναν έλεγχο στη σύνοψη ελέγχων και η εντολή προστίθεται στη λίστα με τις εντολές που ελέγχονται.
TPM_ResetLockValue	Αυτή η εντολή επαναρυθμίζει τους μηχανισμούς που χρησιμοποιούνται για προστασία από επιθέσεις στις τιμές εξουσιοδότησης της TPM.
TPM_SetRedirection	Αυτή η εντολή επιτρέπει στην TPM να επικοινωνεί απευθείας με ένα συνδεδεμένο επεξεργαστή ασφαλείας, πραγματοποιώντας ανακατεύθυνση της εξόδου.
TPM_FieldUpgrade	Αυτή η εντολή επιτρέπει στον κατασκευαστή να αναβαθμίσει τις λειτουργίες της TPM. Αυτή η εντολή είναι συγκεκριμένη για τον κατασκευαστή της TPM.
TPM_Seal	Αυτή η εντολή επιτρέπει στην TPM να σφραγίζει τους μυστικούς κωδικούς μέχρι να γίνουν με επιτυχία οι έλεγχοι ακεραιότητας, ρυθμίσεων παραμέτρων υπολογιστή και εξουσιοδότησης.
TPM_Unseal	Αυτή η εντολή δημοσιεύει μυστικούς κωδικούς που είχαν σφραγιστεί προηγουμένως από την TPM αν είναι επιτυχείς οι έλεγχοι για την ακεραιότητα, τη διαμόρφωση πλατφόρμας και την εξουσιοδότηση.
TPM_Unbind	Αυτή η εντολή αποκρυπτογραφεί δεδομένα που είχαν κρυπτογραφηθεί προηγουμένως με το δημόσιο τμήμα ενός κλειδιού που έχει δεσμευθεί στην TPM.
TPM_CreateWrapKey	Αυτή η εντολή παράγει και δημιουργεί ένα ασφαλές ασυμμετρικό κλειδί.
TPM_GetPubKey	Αυτή η εντολή επιτρέπει σε έναν κάτοχο ενός φορτωμένου κλειδιού να αποκτήσει την τιμή του δημόσιου κλειδιού για το συγκεκριμένο κλειδί. Το φορτωμένο κλειδί δημιουργείται χρησιμοποιώντας την εντολή TPM_LoadKey2.

TPM_Sealx	Αυτή η εντολή επιτρέπει στο λογισμικό να προστατεύει μυστικούς κωδικούς ώστε να δημοσιεύονται μόνο όταν έχουν επικυρωθεί οι συγκεκριμένες ρυθμίσεις παραμέτρων του υπολογιστή. Ο μυστικός κωδικός πρέπει να είναι κρυπτογραφημένος.
TPM_LoadKey2	Αυτή η εντολή φορτώνει ένα κλειδί στην TPM ώστε ο κάτοχος να μπορεί να ορίσει και άλλες ενέργειες σε αυτή. Αυτές οι ενέργειες περιλαμβάνουν την αναδίπλωση, την κατάργηση αναδίπλωσης, τη δέσμευση, την αποδέσμευση, τη σφράγιση, την αποσφράγιση και την υπογραφή.
TPM_CMK_CreateTicket	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργήσει ένα δελτίο επαλήθευσης υπογραφής, χρησιμοποιώντας ένα παρεχόμενο δημόσιο κλειδί. Αυτό το δελτίο χρησιμοποιείται με ένα κλειδί μετεγκατάστασης με δυνατότητα πιστοποιητικού (όπως δημιουργείται με την εντολή TPM_CMK_CreateKey) για τη δημιουργία ενός αντικειμένου BLOB μετεγκατάστασης που χρειάζεται για τη μετακίνηση του κλειδιού σε νέο υπολογιστή ή σε γονικό κλειδί.
TPM_CMK_CreateKey	Αυτή η εντολή δημιουργεί ένα ασφαλές ασύμμετρο κλειδί μετεγκατάστασης με δυνατότητα πιστοποιητικού, χρησιμοποιώντας ένα δελτίο εξουσιοδότησης για μία ή περισσότερες αρχές μετεγκατάστασης (όπως δημιουργήθηκε με την εντολή TPM_CMK_ApproveMA).
TPM_CMK_CreateBlob	Αυτή η εντολή επιτρέπει σε μια οντότητα με γνώση του δελτίου εξουσιοδότησης μετεγκατάστασης (όπως δημιουργήθηκε με την εντολή TPM_CMK_CreateTicket) ενός κλειδιού μετεγκατάστασης με δυνατότητα πιστοποίησης (όπως δημιουργήθηκε με την εντολή TPM_CMK_CreateKey) να

	δημιουργήσει ένα αντικείμενο BLOB μετεγκατάστασης που είναι απαραίτητο για τη μετακίνηση του κλειδιού σε νέο υπολογιστή ή γονικό κλειδί.
TPM_CMK_SetRestrictions	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να καθορίσει τη χρήση ενός κλειδιού μετεγκατάστασης με δυνατότητα πιστοποιητικού (όπως δημιουργείται με την εντολή TPM_CMK_CreateKey).
TPM_CMK_ApproveMA	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργήσει ένα δελτίο εξουσιοδότησης για μία ή περισσότερες αρχές μετεγκατάστασης ώστε οι χρήστες να μπορούν να δημιουργούν κλειδιά μετεγκατάστασης με δυνατότητα πιστοποιητικού (με την εντολή TPM_CMK_CreateKey) χωρίς την παρέμβαση του κάτοχο της TPM.
TPM_CMK_ConvertMigration	Αυτή η εντολή δημιουργεί ένα αντικείμενο BLOB κλειδιού μετεγκατάστασης με δυνατότητα πιστοποιητικού που μπορεί να φορτωθεί σε άλλο υπολογιστή χρησιμοποιώντας την εντολή TPM_LoadKey2. Σε αυτή την εντολή δίδεται ένας τυχαίος αριθμός και το αντικείμενο BLOB μετεγκατάστασης του κλειδιού μετεγκατάστασης με δυνατότητα πιστοποιητικού (όπως δημιουργείται με την εντολή TPM_CMK_CreateBlob).
TPM_MigrateKey	Αυτή η εντολή επιτρέπει στην TPM να μετεγκαταστήσει ένα αντικείμενο BLOB (όπως δημιουργείται από το TPM_CreateMigrationBlob ή το TPM_CMK_CreateBlob) σε έναν προορισμό με εκ νέου κρυπτογράφηση χρησιμοποιώντας δεδομένο δημόσιο κλειδί.

TPM_CreateMigrationBlob	Αυτή η εντολή επιτρέπει σε μια οντότητα με γνώση του δελτίου εξουσιοδότησης μετεγκατάστασης ενός κλειδιού (όπως δημιουργήθηκε με την εντολή TPM_CMK_CreateTicket) να δημιουργήσει ένα αντικείμενο BLOB μετεγκατάστασης που είναι απαραίτητο για τη μετακίνηση ενός κλειδιού μετεγκατάστασης σε νέο υπολογιστή ή γονικό κλειδί.
TPM_ConvertMigrationBlob	Αυτή η εντολή δημιουργεί ένα αντικείμενο BLOB κλειδιού που μπορεί να φορτωθεί σε άλλο υπολογιστή χρησιμοποιώντας την εντολή TPM_LoadKey2. Σε αυτή την εντολή δίδεται ένας τυχαίος αριθμός και το αντικείμενο BLOB μετεγκατάστασης του κλειδιού (όπως δημιουργείται με την εντολή TPM_CreateMigrationBlob).
TPM_AuthorizeMigrationKey	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργήσει ένα δελτίο εξουσιοδότησης μετεγκατάστασης ώστε οι χρήστες να μπορούν να μετακινούν κλειδιά χωρίς την παρέμβαση του κάτοχο της TPM.
TPM_CreateMaintenanceArchive	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργήσει ένα αρχείο συντήρησης το οποίο επιτρέπει την μετεγκατάσταση των δεδομένων που περιλαμβάνονται στην TPM. Αυτά τα δεδομένα περιλαμβάνουν το ριζικό κλειδί αποθήκευσης (SRK) και την εξουσιοδότηση του κατόχου της TPM.
TPM_LoadMaintenanceArchive	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να φορτώσει ένα αρχείο συντήρησης (που δημιουργείται με την εντολή TPM_CreateMaintenanceArchive). Όταν φορτωθεί, η τιμή εξουσιοδότησης για το ριζικό κλειδί αποθήκευσης (SRK) ορίζεται στο κλειδί για την εξουσιοδότηση του κατόχου της TPM.

TPM_KillMaintenanceFeature	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να αποτρέψει τη δημιουργία ενός αρχείου συντήρησης χρησιμοποιώντας την εντολή TPM_CreateMaintenanceArchive. Η ενέργεια είναι έγκυρη μέχρι να οριστεί νέος κάτοχος της TPM χρησιμοποιώντας την εντολή TPM_TakeOwnership.
TPM_LoadManuMaintPub	Αυτή η εντολή φορτώνει το δημόσιο κλειδί του κατασκευαστή του υπολογιστή στην TPM για χρήση κατά τη συντήρηση. Αυτή η εντολή μπορεί να εκτελεστεί μόνο μία φορά και πρέπει να εκτελεστεί πριν από την αποστολή του υπολογιστή.
TPM_ReadManuMaintPub	Αυτή η εντολή επιστρέφει τη σύνοψη του δημόσιου κλειδιού συντήρησης του κατασκευαστή του υπολογιστή (φορτώνεται με την εντολή TPM_LoadManuMaintPub).
TPM_CertifyKey	Αυτή η εντολή πιστοποιεί ένα φορτωμένο κλειδί (δημιουργείται με την εντολή TPM_LoadKey2) με το δημόσιο τμήμα άλλου κλειδιού. Ένα κλειδί ταυτότητας TPM μπορεί να πιστοποιηθεί μόνο για κλειδιά που δεν μπορούν να μετεγκατασταθούν. Τα κλειδιά υπογραφής και τα προηγούμενο κλειδιά μπορούν να πιστοποιήσουν όλα τα κλειδιά.
TPM_CertifyKey2	Αυτή η εντολή βασίζεται στην TPM_CertifyKey, αλλά περιλαμβάνει επιπλέον παραμέτρους για πιστοποίηση ενός CMK (Certifiable Migration Key).
TPM_Sign	Αυτή η εντολή υπογράφει δεδομένα με ένα φορτωμένο κλειδί υπογραφής και επιστρέφει την προκύπτουσα ψηφιακή υπογραφή.
TPM_GetRandom	Αυτή η εντολή επιστρέφει τυχαία δεδομένα καθορισμένου μήκους από το πρόγραμμα δημιουργίας τυχαίων αριθμών της TPM.
TPM_StirRandom	Αυτή η εντολή προσθέτει εντροπία στην κατάσταση του προγράμματος δημιουργίας τυχαίων αριθμών της TPM.

TPM_SHA1Start	Αυτή η εντολή εκκινεί τη διεργασία υπολογισμού μιας σύνοψης SHA-1. Αυτή η εντολή πρέπει να ακολουθείται από την εκτέλεση της εντολής TPM_SHA1Update διαφορετικά η διεργασία SHA-1 ακυρώνεται.
TPM_SHA1Update	Αυτή η εντολή εισάγει πλήρη μπλοκ δεδομένων σε μια σύνοψη SHA-1 που βρίσκεται σε εκκρεμότητα (εκκινείται με την εντολή TPM_SHA1Start).
TPM_SHA1Complete	Αυτή η εντολή ολοκληρώνει μια διεργασία σύνοψης SHA-1 που βρίσκεται σε εκκρεμότητα και επιστρέφει το αποτέλεσμα κατακερματισμού SHA-1 που προκύπτει.
TPM_SHA1CompleteExtend	Αυτή η εντολή ολοκληρώνει μια διεργασία σύνοψης SHA-1 που βρίσκεται σε εκκρεμότητα, επιστρέφει το αποτέλεσμα κατακερματισμού SHA-1 και περιλαμβάνει τον κατακερματισμό σε έναν καταχωρητή διαμόρφωσης πλατφόρμας (PCR).
TPM_CreateEndorsementKeyPair	Αυτή η εντολή δημιουργεί το κλειδί έγκρισης (EK) της TPM αν δεν υπάρχει ήδη αυτό το κλειδί.
TPM_ReadPubek	Αυτή η εντολή επιστρέφει το δημόσιο τμήμα του κλειδιού έγκρισης της TPM. Αυτή η εντολή απενεργοποιείται όταν γίνεται ανάληψη της κυριότητας της TPM χρησιμοποιώντας την εντολή TPM_TakeOwnership.
TPM_CreateRevocableEK	Αυτή η εντολή δημιουργεί το κλειδί έγκρισης (EK) για την TPM. Ο χρήστης μπορεί επίσης να καθορίσει να θα είναι δυνατή η επαναρύθμιση του EK και μπορεί να καθορίσει την τιμή εξουσιοδότησης που είναι απαραίτητη για την επαναφορά αυτού του κλειδιού (αν αυτή η τιμή δεν πρόκειται να δημιουργηθεί από την TPM). Πρόκειται για προαιρετική εντολή που μπορεί να μην υποστηρίζεται από τον κατασκευαστή του υπολογιστή.

TPM_RevokeTrust	Αυτή η εντολή απαλείφει κλειδί έγκρισης TPM με δυνατότητα ανάκλησης (δημιουργείται με την εντολή TPM_CreateRevocableEK) και επαναρυθμίζει την TPM να βρει τη σωστή τιμή εξουσιοδότησης για αυτή την επαναρύθμιση. Για αυτή την εντολή απαιτείται η φυσική παρουσία στην πλατφόρμα και δεν είναι δυνατή η εκτέλεσή της από το λειτουργικό σύστημα.
TPM_OwnerReadInternalPub	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να επιστρέψει το δημόσιο τμήμα του κλειδιού έγκρισης (EK) για την TPM ή το ριζικό κλειδί αποθήκευσης (SRK).
TPM_MakeIdentity	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργεί ένα κλειδί επιβεβαίωσης ταυτότητας (Attestation Identity Key, AIK) που μπορεί να χρησιμοποιηθεί για την υπογραφή πληροφοριών που δημιουργούνται εσωτερικά από την TPM.
TPM_ActivateIdentity	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να ξεδιπλώνει το κλειδί περιόδου λειτουργίας που επιτρέπει την αποκρυπτογράφηση του διαπιστευτηρίου για κλειδί επιβεβαίωσης ταυτότητας (AIK), αποκτώντας συνεπώς τη διαβεβαίωση ότι τα διαπιστευτήρια είναι έγκυρα για την TPM.
TPM_Extend	Αυτή η εντολή προσθέτει μια νέα σύνοψη σε καθορισμένο καταχωρητή διαμόρφωσης πλατφόρμας (PCR) και επιστρέφει αυτή την εκτεταμένη σύνοψη.
TPM_PCRRead	Η εντολή επιστρέφει τα περιεχόμενα ενός καθορισμένου καταχωρητή διαμόρφωσης πλατφόρμας (PCR).
TPM_Quote	Αυτή η εντολή επιστρέφει μια υπογεγραμμένη σύνοψη που είναι συνδυασμός των περιεχομένων ενός καθορισμένου καταχωρητή διαμόρφωσης πλατφόρμας (PCR) και ορισμένων καθορισμένων εξωτερικών δεδομένων. Η σύνοψη υπογράφεται με ένα φορτωμένο

	κλειδί.
TPM_Quote2	Αυτή η εντολή είναι παρόμοια με την εντολή TPM_Quote, αλλά περιλαμβάνει πληροφορίες τοπικότητας ώστε να παρέχει πιο ολοκληρωμένη εικόνα των τρεχουσών ρυθμίσεων παραμέτρων του υπολογιστή.
TPM_PCR_Reset	Με αυτή την εντολή γίνεται επαναρύθμιση του καθορισμένου καταχωρητή διαμόρφωσης πλατφόρμας (PCR) στην προεπιλεγμένη κατάσταση.
TPM_ChangeAuth	Αυτή η εντολή επιτρέπει στον κάτοχο μιας οντότητας (όπως ένα κλειδί TPM) να αλλάζει την τιμή εξουσιοδότησης για τη συγκεκριμένη οντότητα.
TPM_ChangeAuthOwner	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να αλλάζει την τιμή εξουσιοδότησης του κατόχου της TPM ή την τιμή εξουσιοδότησης για το ριζικό κλειδί αποθήκευσης (SRK).
TPM_OIAP	Αυτή η εντολή δημιουργεί ένα δείκτη χειρισμού για περίοδο λειτουργίας εξουσιοδότησης για το πρωτόκολλο OIAP (Object-Independent Authorization Protocol) που χρησιμοποιείται για την ασφαλή διαβίβαση δεδομένων εξουσιοδότησης στην TPM, καθώς και πληροφορίες που χρειάζεται η TPM για την παρακολούθηση αυτού του δείκτη περιόδου λειτουργίας εξουσιοδότησης.
TPM_OSAP	Αυτή η εντολή δημιουργεί ένα δείκτη χειρισμού για περίοδο λειτουργίας εξουσιοδότησης για το πρωτόκολλο OSAP (Object-Specific Authorization Protocol) που χρησιμοποιείται για την ασφαλή διαβίβαση δεδομένων εξουσιοδότησης στην TPM, καθώς και πληροφορίες που χρειάζεται η TPM για την παρακολούθηση αυτού του δείκτη περιόδου λειτουργίας

	εξουσιοδότησης.
TPM_DSAP	Αυτή η εντολή δημιουργεί ένα δείκτη χειρισμού για περίοδο λειτουργίας εξουσιοδότησης για το πρωτόκολλο DSAP (Delegate-Specific Authorization Protocol) που χρησιμοποιείται για την ασφαλή διαβίβαση δεδομένων αντιπροσώπευσης εξουσιοδότησης στην TPM, καθώς και πληροφορίες που χρειάζεται η TPM για την παρακολούθηση αυτού του δείκτη περιόδου λειτουργίας εξουσιοδότησης.
TPM_SetOwnerPointer	Αυτή η εντολή καθορίζει την αναφορά στην εξουσιοδότηση χρήστη που χρησιμοποιεί η TPM κατά την εκτέλεση περιόδου λειτουργίας OIAP ή OSAP. Χρησιμοποιήστε αυτή την εντολή μόνο όταν χρειάζεστε να παρέχετε λειτουργίες ανάθεσης κατόχου για παλιότερο κώδικα που δεν υποστηρίζει DSAP.
TPM_Delegate_UpdateVerification	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να ενημερώσει μια οντότητα ανάθεσης ώστε να συνεχίζει να είναι αποδεκτή από την TPM.
TPM_Delegate_Manage	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να διαχειριστεί πίνακες οικογενειών αναθέσεων. Εκτελέστε αυτή την εντολή τουλάχιστον μία φορά πριν εκτελέσετε εντολές ανάθεση για τον πίνακα οικογενειών.
TPM_Delegate_CreateKeyDelegation	Αυτή η εντολή επιτρέπει στον κάτοχο ενός κλειδιού να αναθέτει το δικαίωμα χρήσης για το συγκεκριμένο κλειδί.
TPM_Delegate_CreateOwnerDelegation	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να αναθέτει το δικαίωμα εκτέλεσης εντολών που συνήθως

	απαιτούν την εξουσιοδότηση του κατόχου.
TPM_Delegate_VerifyDelegation	Αυτή η εντολή ερμηνεύει το αντικείμενο BLOB ανάθεσης και επιστρέφει αν το αντικείμενο BLOB είναι έγκυρο.
TPM_Delegate_LoadOwnerDelegation	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να φορτώνει μια σειρά πινάκων ανάθεσης στη μόνιμη αποθήκευση της TPM. Αυτή η εντολή δεν μπορεί να χρησιμοποιηθεί για τη φόρτωση αντικειμένων BLOB ανάθεσης κλειδιών στην TPM.
TPM_Delegate_ReadTable	Με αυτή την εντολή πραγματοποιείται ανάγνωση δημόσιων περιεχομένων της οικογένειας και των πινάκων ανάθεσης που έχουν αποθηκευτεί στην TPM.
TPM_NV_DefineSpace	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να καθορίσει χώρο για μια περιοχή μόνιμης αποθήκευσης στην TPM. Ο ορισμός περιλαμβάνει τις απαιτήσεις πρόσβασης για την εγγραφή και την ανάγνωση στην περιοχή.
TPM_NV_WriteValue	Αυτή η εντολή εγγράφει μια συγκεκριμένη τιμή σε μια καθορισμένη περιοχή μόνιμης αποθήκευσης (δημιουργείται με την εντολή TPM_NV_DefineSpace).
TPM_NV_WriteValueAuth	Αυτή η εντολή εγγράφει μια συγκεκριμένη τιμή σε μια καθορισμένη περιοχή μόνιμης αποθήκευσης αν βρει την απαιτούμενη εξουσιοδότηση για τη συγκεκριμένη περιοχή.
TPM_NV_ReadValue	Με αυτή την εντολή είναι δυνατή η ανάγνωση από ορισμένη περιοχή μόνιμης αποθήκευσης.
TPM_NV_ReadValueAuth	Με αυτή την εντολή είναι δυνατή η ανάγνωση από ορισμένη περιοχή μόνιμης αποθήκευσης αν βρει την απαιτούμενη εξουσιοδότηση για τη συγκεκριμένη περιοχή.

TPM_KeyControlOwner	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να καθορίζει ορισμένα χαρακτηριστικά, όπως αν το κλειδί μπορεί να καταργηθεί από άλλον πέραν του κατόχου.
TPM_SaveContext	Αυτή η εντολή αποθηκεύει έναν φορτωμένο πόρο εκτός της TPM. Μετά την επιτυχή εκτέλεση αυτής της εντολής, η TPM δημοσιεύει αυτόματα την εσωτερική μνήμη για περιόδους λειτουργίας, ωστόσο αφήνει στη θέση τους τα κλειδιά.
TPM_LoadContext	Αυτή η εντολή φορτώνει ένα περιβάλλον που αποθηκεύτηκε προηγουμένως στην TPM.
TPM_FlushSpecific	Αυτή η εντολή εκκαθαρίζει έναν καθορισμένο δείκτη πόρων από την TPM.
TPM_GetTicks	Αυτή η εντολή επιστρέφει το τρέχον πλήθος υποδιαιρέσεων χρονομέτρησης της TPM.
TPM_TickStampBlob	Αυτή η εντολή υπογράφει μια συγκεκριμένη σύνοψη με το τρέχον πλήθος υποδιαιρέσεων χρονομέτρησης της TPM, χρησιμοποιώντας ένα φορτωμένο κλειδί υπογραφής.
TPM_EstablishTransport	Αυτή η εντολή καθορίσει μια περίοδο λειτουργίας μεταφοράς που μπορεί να χρησιμοποιηθεί για την εμπιστευτική μεταφορά κοινόχρηστων μυστικών κωδικών, κλειδιών κρυπτογράφησης και αρχείων καταγραφής περιόδων λειτουργίας προς την TPM (χρησιμοποιώντας την εντολή TPM_ExecuteTransport).
TPM_ExecuteTransport	Αυτή η εντολή παραδίδει μια αναδιπλωμένη εντολή TPM προς την TPM εντός μιας περιόδου λειτουργίας μεταφοράς. Η TPM ξεδιπλώνει την εντολή και στη συνέχεια την εκτελεί.
TPM_ReleaseTransportSigned	Αυτή η εντολή ολοκληρώνει την περίοδο λειτουργίας μεταφοράς. Αν έχει ενεργοποιηθεί η καταγραφή, αυτή η εντολή επιστρέφει ένα κατακερματισμό όλων των λειτουργιών που εκτελέστηκαν κατά

	τη διάρκεια της περιόδου λειτουργίας, καθώς και την ψηφιακή υπογραφή του κατακερματισμού.
TPM_CreateCounter	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημιουργήσει έναν μονοτονικό μετρητή, να αντιστοιχίσει μια τιμή εξουσιοδότησης στο μετρητή, να προσαυξήσει την τιμή του εσωτερικού μετρητή της TPM κατά ένα και να ορίσει την τιμή έναρξης του νέου μετρητή ώστε να είναι η ενημερωμένη εσωτερική τιμή.
TPM_IncrementCounter	Αυτή η εντολή επιτρέπει στον κάτοχο του μονοτονικού μετρητή να προσαυξήσει το μετρητή κατά ένα και να επιστρέψει αυτή την ενημερωμένη τιμή.
TPM_ReadCounter	Αυτή η εντολή επιστρέφει την τιμή του καθορισμένου μονοτονικού μετρητή.
TPM_ReleaseCounter	Αυτή η εντολή επιτρέπει στον κάτοχο του μετρητή να δημοσιεύει τον καθορισμένο μετρητή. Αυτή η εντολή διακόπτει όλες τις συνεπακόλουθες αναγνώσεις ή προσαυξήσεις του μετρητή.
TPM_ReleaseCounterOwner	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να δημοσιεύει τον καθορισμένο μετρητή. Διακόπτει όλες τις συνεπακόλουθες αναγνώσεις ή προσαυξήσεις του μετρητή.
TPM_DAA_Join	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να καθιερώσει τις παραμέτρους DAA (Direct Anonymous Attestation) στην TPM για μια συγκεκριμένη αρχή που εκδίδει DAA.
TPM_DAA_Sign	Αυτή η εντολή επιτρέπει στον κάτοχο της TPM να υπογράψει δεδομένα χρησιμοποιώντας την DAA (Direct Anonymous Attestation).
TPM_ChangeAuthAsymStart	Αυτή η εντολή αντικαθιστάται με τον ορισμό μια περιόδου λειτουργίας μεταφοράς με την TPM και εκτελώντας την εντολή

	TPM_ChangeAuth.
TPM_ChangeAuthAsymFinish	Αυτή η εντολή αντικαθιστάται με τον ορισμό μια περιόδου λειτουργίας μεταφοράς με την TPM και εκτελώντας την εντολή TPM_ChangeAuth.
TPM_DirWriteAuth	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_NV_WriteValue και TPM_NV_WriteValueAuth.
TPM_DirRead	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_NV_ReadValue και TPM_NV_ReadValueAuth.
TPM_LoadKey	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_LoadKey2.
TPM_EvictKey	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_FlushSpecific.
TPM_CertifySelfTest	Αυτή η εντολή εκτελεί πλήρη εσωτερική δοκιμή και επιστρέφει την ελεγμένη τιμή αν η δοκιμή είναι επιτυχής. Αυτή η εντολή δεν αναβαθμίζεται για την έκδοση 1.2 της TPM.
TPM_Reset	Αυτή η εντολή δημοσιεύει όλους τους πόρους που συσχετίζονται με υπάρχουσες περιόδους λειτουργίας ελέγχου ταυτότητας. Αυτή η εντολή δεν αναβαθμίζεται για την έκδοση 1.2 της TPM.
TPM_OwnerReadPubek	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_OwnerReadInternalPub.
TPM_DisablePubekRead	Αυτή η εντολή αντικαθίσταται καθώς η εντολή TPM_TakeOwnership απενεργοποιεί αυτόματα την ανάγνωση του δημόσιου τμήματος του κλειδιού έγκρισης (EK) χρησιμοποιώντας την εντολή TPM_ReadPubek.
TPM_Terminate_Handle	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_FlushSpecific.
TPM_SaveKeyContext	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_SaveContext.
TPM_LoadKeyContext	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_LoadContext.

TPM_LoadAuthContext	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_LoadContext.
TPM_SaveAuthContext	Αυτή η εντολή αντικαθίσταται από την εντολή TPM_SaveContext.
TPM_GetCapabilitySigned	Αυτή η εντολή διαγράφηκε λόγω προβληματισμών σχετικά με την ασφάλεια.
TPM_GetCapabilityOwner	Αυτή η εντολή διαγράφηκε λόγω προβληματισμών σχετικά με την ασφάλεια.
TPM_GetAuditEvent	Αυτή η εντολή διαγράφηκε λόγω προβληματισμών σχετικά με την ασφάλεια.
TPM_GetAuditEventSigned	Αυτή η εντολή διαγράφηκε λόγω προβληματισμών σχετικά με την ασφάλεια.
TPM_GetOrdinalAuditStatus	Αυτή η εντολή διαγράφηκε λόγω προβληματισμών σχετικά με την ασφάλεια.

ΑΝΑΦΟΡΕΣ

[1] Will Arthur, David Challener, Kenneth Goldman, A Practical Guide to TPM 2.0, Using the New Trusted Platform Module in the New Age of Security.
[2] Bryan Parno,Jonathan M. McCune, Adrian Perrig, Bootstrapping Trust in Modern Computers, Springer,2011
[3] https://en.wikipedia.org/wiki/Trusted_Platform_Module
[4] http://opensecuritytraining.info/IntroToTrustedComputing.html
[5] https://trustedcomputinggroup.org/trusted-platform-module-tpm-summary/
[6] https://trustedcomputinggroup.org/use-tpm-guide-hardware-based-endpoint-security/
[7] http://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf
[8] https://trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_NetEq_1_0r26b_Public-Review.pdf
[9] https://docs.microsoft.com/en-us/windows/access-protection/virtual-smart-cards/virtual-smart-card-overview
[10] https://docs.microsoft.com/en-us/windows/access-protection/virtual-smart-cards/virtual-smart-card-evaluate-security
[11] https://www.chromium.org/developers/design-documents/tpm-usage
[12] https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html
[13] Trusted Platform Module Library Part 1: Architecture, Family “2.0”, Level 00 Revision 01.38 September 29, 2016
[14] https://www.youtube.com/watch?v=e94KJbic5wE
[15] https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/secureview-government-industry-collaboration-delivers-improbved-levels-of-security-performance-and-cost-saving-for-mission-critical-applications.pdf
[16] https://www.yumpu.com/en/document/view/57790332/secureview-overview/4
[17] https://en.wikipedia.org/wiki/Cryptographic_Service_Provider
[18] http://www.selhorst.net/data/TSS-Study_en.pdf
[19] https://sourceforge.net/p/linux-ima/wiki/Home/
[20] http://apple.wikia.com/wiki/TPM
[21] https://sourceforge.net/projects/ibmtpm20acs/
[22] https://sourceforge.net/projects/ibmswtpm2/
[23] https://sourceforge.net/projects/ibmtpm20tss/