ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

<<ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΞΙΟΠΙΣΤΩΝ ΣΥΣΚΕΥΩΝ>>

ΔΡΑΚΟΠΟΥΛΟΣ ΗΛΙΑΣ

ΕΠΙΒΛΕΠΩΝ : ΚΙΤΣΟΣ ΠΑΡΑΣΚΕΥΑΣ

Πάτρα , 2021

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία /2021

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

Ευχαριστίες:

Θα ήθελα να ευχαριστήσω τον εισηγητή μου καθηγητή κ. Κίτσο Παρασκευά ο οποίος με επόπτευε στην πτυχιακή εργασία μου και την οικογένειά μου για τη συμπαράσταση που μου είχαν σε όλη την πορεία μου μέχρι το τέλος.

Υπεύθυνη Δήλωση:

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία.

Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες.
Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής Αντιρρίου (Πρώην Τμήμα Τηλεπικοινωνιακών Συστημάτων και Δικτύων).

Δομή και στόχοι της διπλωματικής εργασίας:

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Πλέον οι περισσότεροι οργανισμοί βασίζονται στην λειτουργία τους. Επίμαχο σημείο αυτών είναι η ασφάλεια τους. Στη παρούσα εργασία παρουσιάζονται τα βασικά θέματα που αφορούν τις Πολιτικές και τα Μοντέλα Ασφαλείας των Πληροφοριακών Συστημάτων.

Αρχικά, θα γίνει μια μικρή εισαγωγή για να γνωρίσουμε το Πληροφοριακό Σύστημα. Έπειτα, θα αναφερθούν ορισμένες βασικές έννοιες των Πληροφοριακών Συστημάτων όπως οι προϋποθέσεις που χρειάζονται για την ασφάλεια, οι κίνδυνοι που υπάρχουν και τα οφέλη από την ανάλυση της επικινδυνότητας. Στη συνέχεια θα γίνει αναφορά στον όρο trusted computing και σε ορισμένες πολιτικές καθώς και ορισμένα μοντέλα ασφαλείας των Πληροφοριακών Συστημάτων, αλλά και πώς το καθένα προσφέρει ξεχωριστά την έννοια της ασφάλειας σε ένα Πληροφοριακό Σύστημα.

Στόχος της διπλωματικής αυτής εργασίας αποτελεί ο καθορισμός των εννοιών της ασφάλειας και της εμπιστοσύνης σε Συστήματα Συσκευών αλλά και με ποιους τρόπους μπορεί ένα Σύστημα να είναι πάντα ασφαλές και έμπιστο.

Thanks:

I would like to thank my rapporteur, Professor Kitso Paraskeua, who has supervised me in my thesis and my family for the support they have had me all the way to the end.

Statutory Declaration:

I certify that I am the author of this dissertation and that all the assistance I have had for her preparation is fully recognized and refers to the dissertation.

I have also mentioned the sources from which I have used data, ideas or words, whether these are mentioned exactly or paraphrased.

We also assure that this thesis was prepared by us personally especially for the requirements of the curriculum of the Department of Computer Engineering Antirio (former Department of Telecommunication Systems and Networks).

Structure and objectives of the thesis:

The use of Information Systems is constantly increasing. Now most organizations rely on their function. Their point of view is their security. This paper presents the key issues related to Information Systems Security Policies and Models.

Initially, there will be a small introduction to getting to know the Information System. Then, some basic concepts of Information Systems will be mentioned, such as the prerequisites for security, the risks that exist and the benefits of risk analysis. Then we will refer to the term trusted computing and certain policies as well as some security models of the Information Systems, but also how each offers separately the concept of security in an Information System.

In the end there will be a technical piece as an experiment. The aim of this diploma thesis is to define the concepts of security and confidence in Device Systems, but also in what ways a system can always be secure and trustworthy.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

Όλες οι έξυπνες συσκευές, συμπεριλαμβανομένων και των ηλεκτρονικών υπολογιστών, συνδυάζουν όλες αυτές τις δυνατότητες που έχουν οι παραδοσιακές συσκευές, δηλαδή προσφέρουν διασκέδαση, πλατφόρμες γεωγραφικού εντοπισμού όπως το GPS. Ακόμα, μπορούμε να κάνουμε ηλεκτρονικές αγορές και συναλλαγές με εύκολο και γρήγορο τρόπο. Αν και οι δυνατότητες που ανοίγονται μπροστά τους όπως για παράδειγμα οι τραπεζικές συναλλαγές, οι ηλεκτρονικές πληρωμές και η κοινωνική δικτύωση υπάρχουν μερικοί άνθρωποι που χρησιμοποιούν τις συσκευές μόνο για τηλεφωνικές κλήσεις και γραπτά μηνύματα. Πέρα από αυτά, το μεγαλύτερο μέρος του πληθυσμού πραγματοποιεί πλέον πολλές από τις ενέργειες που έκανε με τον παραδοσιακό τρόπο με μια κινητή συσκευή ή και με έναν ηλεκτρονικό υπολογιστή, καθώς αυτά περιέχουν πολλές εφαρμογές όπως η τηλεόραση, η φωτογραφική μηχανή, κ.ά. Επιπλέον, οι έξυπνες συσκευές κατέχουν σημαντικό ρόλο στην καθημερινότητα των ανθρώπων. Πιο συγκεκριμένα, παρέχεται πιο εύκολα η ψυχαγωγία, η επικοινωνία, η δικτύωση, οι συναλλαγές καθώς επίσης και οι αγορές. Τέλος, μπορούμε να πούμε ότι έχουν κερδίσει ακόμα και τον επιχειρηματικό κόσμο, καθώς παρέχονται στους εργαζόμενους περισσότερα εργαλεία ώστε να οργανώνουν καλύτερα την δουλειά τους αλλά και οι ίδιες επιχειρήσεις μέσω των έξυπνων συσκευών να προωθούν πιο εύκολα στους καταναλωτές τα προϊόντα (Juniper, 2011).

Η εξέλιξη που υπάρχει στη κινητή τηλεφωνία μπορούμε να πούμε ότι προχωρά με αλματώδεις ρυθμούς, όπως μπορεί να εξηγηθεί από την τεράστια αύξηση στον αριθμό των εφαρμογών στο Play Store στα κινητά και στους Η/Υ (laptops, notebooks) σε αγορές. Όμως, υπάρχει ένα σημείο στο τομέα της ασφάλειας στον οποίο έχουν παρατηρηθεί ελάχιστα βήματα προόδου. Πιο συγκεκριμένα, οι εφαρμογές αυτές υστερούν σε αυτό το κομμάτι σε αντίθεση με τους υπολογιστές και τα laptops που είναι εδώ και χρόνια εξοπλισμένοι με λογισμικό ασφάλειας, χωρίς αυτό να σημαίνει ότι είναι και απαραβίαστοι. Στη συντριπτική τους πλειοψηφία μένουν χωρίς προστασία, με αποτέλεσμα να είναι ευάλωτοι σε απειλές, όπως υποκλοπές, κακόβουλο λογισμικό, κλπ., και να ελλοχεύουν πολλοί κίνδυνοι.

Γίνονται εύκολα στόχοι επίθεσης καθώς αποθηκεύουν μεγάλο όγκο δεδομένων που έχουν μεγάλη αξία. Οι τρεις πρωταρχικοί στόχοι επίθεσης είναι τα ηλεκτρονικά δεδομένα ενός υπολογιστή ή κινητού, η ταυτότητα του κάτοχου/χρήστη

και η διαθεσιμότητα αυτών. Αυτό έχει σαν αποτέλεσμα να βρίσκουν είσοδο αυτοί που θέλουν να πράξουν με αθέμιτο τρόπο και να προχωρήσουν σε άλλες κακόβουλες ενέργειες, εκμεταλλευόμενοι τις αδυναμίες χρησιμοποιώντας τεχνολογίες όπως για παράδειγμα τα SMS, τα δίκτυα Wi-Fi, κλπ.

Όλα τα παραπάνω οδηγούν σε αρνητικές επιπτώσεις στα χαρακτηριστικά όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών, με αποτέλεσμα να έρχονται σε αντίθεση με την ασφάλεια των συστημάτων. Όταν τα χαρακτηριστικά αυτά δεν μπορούν να ικανοποιηθούν τότε δημιουργείται σοβαρό πρόβλημα καθώς μπορεί να απειληθούν άμεσα ανθρώπινες ζωές αλλά και η ασφάλεια σε τοπικό, εθνικό αλλά και παγκόσμιο επίπεδο. Για αυτό, η ασφάλεια των πληροφοριακών συστημάτων αποτελεί σημαντικό κρίκο για την σύγχρονη κοινωνία.

ΚΕΦΑΛΑΙΟ 2 . ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΜΕΛΕΤΗΣ

Πληροφορία είναι οποιοδήποτε στοιχείο που είναι βασισμένο στη γνώση και έχει προέλθει από επεξεργασία δεδομένων. Η πληροφορία μπορεί να εμφανιστεί σε διάφορες μορφές, όπως τυπωμένη, γραμμένη σε χαρτί ή σε ηλεκτρονική μορφή και να μεταδίδεται είτε με φυσικά μέσα δηλαδή το ταχυδρομείο, είτε με ηλεκτρονικά μέσα όπως τα e-mail. Παρά τα σημαντικά πλεονεκτήματα και δυνατότητες που προσφέρει η χρήση των ολοένα και περισσότερων προχωρημένων τεχνικών και τεχνολογιών, αμβλύνονται τα προβλήματα σχετικά με το πόσο ασφαλείς παραμένουν οι πληροφορίες.

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από αλλοιώσεις και καταστροφές που μπορεί να προκύψουν. Επιπλέον, μπορεί να συσχετιστεί με την ικανότητά του να παρέχει αξιόπιστες πληροφορίες στους χρήστες όταν τις αναζητούν. Αυτό μπορεί να βασιστεί σε μια σειρά από μέτρα τα οποία είναι ικανά να διασφαλίζουν την ακεραιότητα την εμπιστευτικότητα των δεδομένων, καθώς επίσης και την σωστή λειτουργία του συστήματος. Επιπρόσθετα, η ασφάλεια των πληροφοριών αποτελεί γνωστικό πεδίο της πληροφορικής, το οποίο ασχολείται με την προστασία των δικτύων, των υπολογιστών και των δεδομένων, με σκοπό να μην επιτρέπει την πρόσβαση ή χρήση τους από μη εξουσιοδοτημένα άτομα ή κακόβουλους χρήστες.

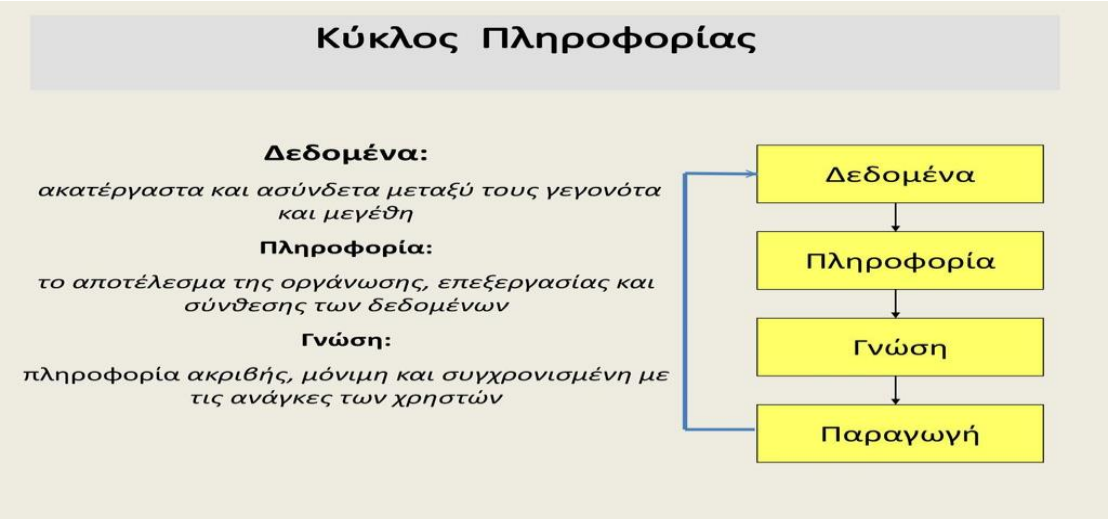
Ειδικότερα, ο σχεδιασμός ασφαλείας στα πληροφοριακά συστήματα, συνδέεται άμεσα τόσο με διαδικασίες και μέτρα όσο και με κοινωνικές αντιλήψεις, προφυλάσσοντας από κάθε είδους απειλή. Αρχικά, για τον σχεδιασμό ασφαλείας μπορεί να οριστεί ως βάση ο εντοπισμός ενός θεωρητικού πλαισίου, στη συνέχεια η αξιολόγησή του και τέλος η διαμόρφωσή του. Βέβαια οι πολιτικές ασφαλείας προϋποθέτουν ότι θα υπάρχουν κάποιες αρχές, οι οποίες να συνδέονται με τους σχεδιαστικούς στόχους των λειτουργικών συστημάτων. Όλα τα αντικείμενα που υπάρχουν στο σύστημα θα πρέπει να αναγνωρίζονται και να παρέχουν εμπιστευτικότητα και αξιοπιστία. Για το λόγο αυτό η αποδοτικότητα των μηχανισμών ασφαλείας θα πρέπει να βασίζεται στην αποτελεσματικότητα του σχεδιασμού και όχι στην άγνοια που έχουν οι χρήστες.

Βασικός στόχος ενός συστήματος ασφαλείας είναι να υπάρχει η εμπιστοσύνη μεταξύ οργανισμού και πελατών έτσι ώστε να περιοριστεί η επικινδυνότητα. Αυτό επιτυγχάνεται με τη λήψη ενός συνόλου μέτρων ασφαλείας προκειμένου να δημιουργηθεί ένα ολοκληρωμένο πλαίσιο. Τρία από τα πιο σημαντικά είδη των πολιτικών ασφαλείας είναι τα τεχνικά συστήματα πληροφοριών, όπως για παράδειγμα τα λειτουργικά συστήματα και τα δίκτυα υπολογιστών, τα οργανωτικά συστήματα και τα ατομικά.

Όταν να εφαρμόζεται μια πολιτική ασφαλείας επιδιώκεται:

- η κάλυψη των συνόλων και λειτουργιών από οδηγίες και μέτρα προστασίας (πληρότητα)
- η ενημέρωση των τρεχουσών τεχνολογικών εξελίξεων (επικαιρότητα)
- η παροχή σαφήνειας, κατανόησης και ανεξαρτησίας από την πολιτική στο πληροφοριακό σύστημα.

Για να μπορεί αυτό να αποτελέσει ένα επιτυχές σύστημα πολιτικής ασφαλείας είναι απαραίτητη μια σειρά πραγμάτων. Πιο συγκεκριμένα, θα πρέπει να είναι ξεκάθαροι και κατάλληλοι οι στόχοι για το περιβάλλον που θα εφαρμοστούν, οι χρήστες να είναι κατάλληλα εκπαιδευμένοι και η πρόσβαση να είναι εύκολη και άμεση στο πληροφοριακό σύστημα.



Εικόνα 1: Βασική Δομή Ασφάλειας και Εμπιστοσύνης

2.1 ΠΡΟΥΠΟΘΕΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η δυνατότητα ενός συστήματος πληροφοριών να μπορεί να αντιστέκεται σε κακοπροαίρετες ενέργειες που θέτουν σε κίνδυνο τη διαθεσιμότητα, την επαλήθευση της ταυτότητας καθώς επίσης την ακεραιότητα και το απόρρητο των δεδομένων, ορίζει το πλαίσιο της ασφάλειας των δικτύων και των πληροφοριών. Στις μέρες μας, η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων συνδέεται με τρεις βασικές έννοιες:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητας Πληροφοριών (Integrity) και
- Διαθεσιμότητα Πληροφοριών (Availability)

2.1.1 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Οι έννοιες της ασφάλειας και της εμπιστευτικότητας τις περισσότερες φορές σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα που η ασφάλεια έχει μεγάλη σημασία στο να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα μπορεί οριστεί ως η πρόληψη μίας μη επιτρεπόμενης αποκάλυψης πληροφοριών από μη εξουσιοδοτημένα άτομα. Επομένως, τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα δεδομένα που μεταφέρονται μεταξύ των υπολογιστών, αποκαλύπτονται μόνο σε άτομα που επιτρέπεται. Αυτό έχει να κάνει όχι μόνο με την προστασία από μία μη επιτρεπτή αποκάλυψη, αλλά ακόμη και με το γεγονός ότι τα δεδομένα αυτά απλώς υπάρχουν. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, όπως με την κλοπή φορητών υπολογιστών. Υπάρχουν βέβαια και άλλες διατυπώσεις της εμπιστευτικότητας όπως είναι η ιδιωτικότητα δηλαδή η προστασία δεδομένων προσωπικού χαρακτήρα που αφορούν συγκεκριμένα πρόσωπα και η μυστικότητα, δηλαδή η προστασία των δεδομένων που ανήκουν σε κάποιον οργανισμό.

2.1.2 ΑΚΕΡΑΙΟΤΗΤΑ

Η ακεραιότητα είναι η πρόληψη μίας μη επιτρεπόμενης μεταβολής πληροφοριών, αλλά και της μη επιτρεπόμενης δημιουργίας δεδομένων, με σκοπό οι πληροφορίες και τα δεδομένα να παραμένουν όπως είναι. Επομένως, ενέργειες όπως η μετατροπή, η διαγραφή, η δημιουργία αλλά και όποιες άλλες συμβούν στα δεδομένα ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέλη. Ορισμένα παραδείγματα υπηρεσιών συναφή με την ακεραιότητα είναι:

•Η Ακεραιότητα Σύνδεσης με αποκατάσταση (Connection Integrity Service With Recovery) : Εξασφαλίζει την ακεραιότητα των δεδομένων και παράλληλα παρέχει τη δυνατότητα ανάκτησης αυτών.

•Η Ακεραιότητα Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery): Παρέχει μόνο ακεραιότητα δεδομένων.

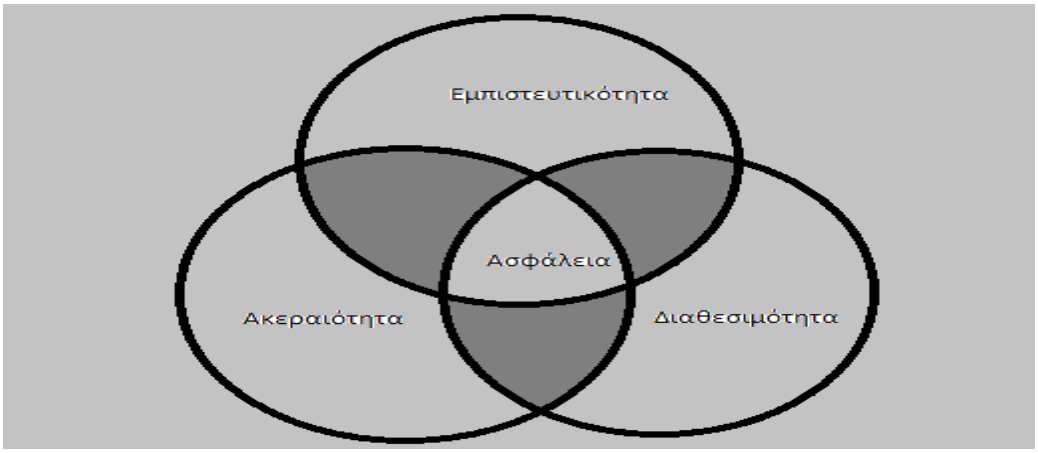
•Η Ακεραιότητα Σύνδεσης Επιλεγμένου Πεδίου (Selected Field Connection Integrity Service): Παρέχει ακεραιότητα μεμονωμένων πεδίων δεδομένων.

•Η Ακεραιότητα Άνευ Εγκατάστασης Σύνδεσης (Connectionless Integrity Service): Παρέχει ακεραιότητα μεμονωμένων τμημάτων δεδομένων.
•Η Ακεραιότητα Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (Selected Field Connectionless Integrity Service): Παρέχει ακεραιότητα συγκεκριμένων πεδίων σε μεμονωμένα τμήματα δεδομένων.

2.1.3 ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Η διαθεσιμότητα είναι η ιδιότητα του να είναι οποιαδήποτε στιγμή προσβάσιμες και χωρίς καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν χρειάζονται. Σε αυτή την περίπτωση, οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης και μπορούν να έχουν πρόσβαση όταν το επιθυμούν. Η διαθεσιμότητα καλύπτει περιοχές πέρα από το φυσικό σκοπό της ασφάλειας, δηλαδή ένα μεγάλο μέρος της τεχνολογίας που απαιτείται για τη διασφάλιση της διαθεσιμότητας προέρχεται από άλλες περιοχές. Όσον αφορά την ασφάλεια, δίνεται ένα ιδιαίτερο βάρος στις κακόβουλες επιθέσεις που εμποδίζουν την είσοδο των εξουσιοδοτημένων χρηστών

στο σύστημα. Αυτές οι επιθέσεις φέρουν το όνομα επιθέσεις άρνησης παροχής υπηρεσιών, που παρεμποδίζουν την επιτρεπόμενη πρόσβαση στις πληροφορίες και στη δημιουργία καθυστέρησης των λειτουργιών. Στόχος εδώ είναι η εξάλειψη σκόπιμης απώλειας της διαθεσιμότητας.



Εικόνα 2:Βασικές Προϋποθέσεις Ασφαλείας

2.2 ΔΕΥΤΕΡΕΥΟΥΣΕΣ ΕΝΝΟΙΕΣ

Εκτός από τις βασικές τρεις θεμελιώδεις έννοιες που περιγράφθηκαν νωρίτερα, υπάρχουν μερικές ακόμη δευτερεύουσες έννοιες της ασφάλειας που αξίζει να σημειωθούν. Ειδικότερα:

- **Εξουσιοδοτημένη χρήση (authorized use):**

Τα περισσότερα σύγχρονα λειτουργικά συστήματα βασίζονται στην εξουσιοδότηση. Η εξουσιοδότηση αποτελεί μια λειτουργία κατά την οποία καθορίζονται τα δικαιώματα πρόσβασης σε πόρους που σχετίζονται με την ασφάλεια των πληροφοριών αλλά και των υπολογιστών δίνοντας έμφαση στον έλεγχο της πρόσβασης. Το σύστημα χρησιμοποιεί τους κανόνες ελέγχου πρόσβασης για να αποφασίσει εάν τα αιτήματα για την πρόσβαση στο σύστημα θα εγκριθούν ή θα απορριφθούν. Οι πόροι περιλαμβάνουν ξεχωριστά αρχεία ή δεδομένα, προγράμματα

υπολογιστή και την λειτουργικότητα που παρέχεται από εφαρμογές ηλεκτρονικών υπολογιστών.

Όταν ένας καταναλωτής προσπαθεί να αποκτήσει πρόσβαση σε έναν πόρο, ενεργοποιείται μια διαδικασία όπου ελέγχει αν του επιτρέπεται να χρησιμοποιεί αυτόν τον πόρο, διότι μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν το υπολογιστικό σύστημα. Η πρόσβαση επιτρέπεται σε ορισμένους τύπους εφαρμογών. Εφόσον αποκτήσουν την επιτρεπόμενη άδεια πρόσβασης, εισέρχονται σε ό, τι χρειάζονται και συνήθως είναι εξουσιοδοτημένοι για απεριόριστη πρόσβαση σε διάφορους πόρους ενός συστήματος.

Βέβαια μπορεί να εντοπιστεί και το ενδεχόμενο της "Μερικής εμπιστοσύνης". Σύμφωνα με αυτό, οι επισκέπτες συχνά θα έχουν περιορισμένη εξουσιοδότηση ώστε να προστατεύοντα οι πόροι από ακατάλληλη πρόσβαση και χρήση. Η πολιτική πρόσβασης γενικά παρέχει σε όλους τους καταναλωτές πλήρη πρόσβαση, αλλά κάποιοι άλλοι επιμένουν ότι μόνο ο διαχειριστής μπορεί να εξουσιοδοτεί αυτός αποκλειστικά έναν καταναλωτή να χρησιμοποιεί κάθε πόρο. Για αυτό πολλές φορές είναι απαραίτητη η αλλαγή ή κατάργηση της εξουσιοδότησης ενός χρήστη και αυτό επιτυγχάνεται με την αλλαγή ή τη διαγραφή των κανόνων πρόσβασης στο σύστημα για καθένα πόρο ξεχωριστά.

- **Αυθεντικοποίηση μηνυμάτων (message authentication):**

Στόχος εδώ είναι να γνωρίζουμε με βέβαιο τρόπο ότι κατά την ενέργεια ενός χρήστη μέσω δικτύου, ότι το άτομο που το σύστημα επιβεβαιώνει, ότι πράγματι είναι αυτός.

Σε πολλά συστήματα η ταυτότητα του χρήστη βεβαιώνεται με ένα συνθηματικό στην αρχή κάθε ακολουθίας. Αυτό γίνεται διότι το σύστημα ελέγχει και αποδεικνύει την πραγματική ταυτότητα των εξυπηρετητών και εκείνων που εξυπηρετούν, μέσω κρυπτογράφησης, έτσι ώστε να παρέχεται ασφάλεια κατά την χρήση.

- **Μη απάρνηση (non repudiation):**

Γενικά, η μη απάρνηση δηλώνει με βεβαιότητα εάν ένας χρήστης παρέλαβε ένα μήνυμα που στάλθηκε ή εκτέλεσε κάποια ενέργεια, προκειμένου να μην μπορεί να απαρνηθεί κάτι. Για παράδειγμα, ο μοναδικός κάτοχος του λογαριασμού ενός υπολογιστή δεν πρέπει να επιτρέπει σε άλλους να τον χρησιμοποιούν δίνοντας τον κωδικό πρόσβασής του. Αυτό εμποδίζει τον κάτοχο του λογαριασμού να αρνηθεί τις ενέργειες που εκτελούνται από το λογαριασμό. Σε συσχετισμό με την ασφάλεια, πραγματοποιείται μια υπηρεσία που αποδεικνύει την ακεραιότητα, την προέλευση των δεδομένων και τον έλεγχο της ταυτότητας.

- **Απόδοση ευθυνών (accountability):**

Στην πραγματικότητα δεν είναι εφικτό να αντιλαμβάνονται και να εμποδίζονται όλες οι ακατάλληλες ενέργειες, αφού ακόμη και οι κατάλληλες ενέργειες μπορεί να προκαλέσουν προβλήματα ασφάλειας. Καθημερινά γίνονται ευρέως γνωστές νέες απειλές στην ασφάλεια των συστημάτων. Για την αντιμετώπιση αυτών, πρέπει οι χρήστες να είναι υπόλογοι για τις πράξεις τους. Αυτό γίνεται με τη διατήρηση εγγραφών ελέγχου ασφαλείας, όπου αυτές θα χρησιμοποιηθούν για την επίλυση του προβλήματος και την ανακάλυψη του εισβολέα και την απόδοση ευθυνών.

2.3 ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Εάν μελετήσουμε πρώτα τη λειτουργία ενός συστήματος για την παροχή πληροφοριών, εμφανίζονται οι μορφές των απειλών που έρχεται αντιμέτωπη η ασφάλεια ενός υπολογιστικού συστήματος. Γενικά, υπάρχει ροή πληροφοριών από μια πηγή σε κάποιο προορισμό, δηλαδή σε ένα άλλο αρχείο ή έναν χρήστη. Ακόμα, πληροφορία μπορεί να αποτελέσει και ένα κακόβουλο πρόγραμμα το οποίο μπορεί να εξαπλωθεί μέσω διαφόρων φορέων, όπως μέσω SMS που περιέχει μια μολυσμένη ιστοσελίδα, μέσω ασύρματων μολυσμένων δικτύων στα οποία συνδέονται οι συσκευές, μέσω της τεχνολογίας κινητών ηλεκτρονικών πληρωμών NFC (Near Field Communication), καθώς και μέσω μολυσμένου περιεχομένου που λαμβάνεται μέσα από το Διαδίκτυο ή μέσω της τεχνολογίας Bluetooth (Georgiadis et al., 2014).

Για την επεξήγηση της έννοιας της απειλής παραθέτουμε ορισμένα παραδείγματα επιθέσεων, όπως είναι η αποστολή ενός κακόβουλου μηνύματος που έχει σαν αποτέλεσμα την επανεκκίνηση της λειτουργίας μίας συσκευής και να οδηγήσει σε επιθέσεις άρνησης παροχής υπηρεσίας. Επιπλέον, μια ακόμα πιθανή επίθεση θα μπορούσε να ξεκινήσει με ένα τηλέφωνο που στέλνει ένα SMS/MMS σε άλλα τηλέφωνα, το οποίο περιλαμβάνει ένα αρχείο, που είναι μολυσμένο με ιό. Ανοίγοντάς το ο χρήστης, η συσκευή έχει μολυνθεί και ο ιός μεταφέρεται σε όλες τις επαφές που είναι αποθηκευμένες.

Μια ακόμα εισβολή, πέραν των SMS/MMS, μπορεί να επιχειρηθεί μέσω της παρακολούθησης των συνδέσεων μιας συσκευής μέσω του Wi-Fi. Έτσι μπορεί να αποκτήσει πρόσβαση στη συσκευή αλλά και να στείλει κάποιο κακόβουλο πρόγραμμα χρησιμοποιώντας το ίδιο κανάλι επικοινωνίας. Οι έξυπνες συσκευές είναι αρκετά ευάλωτες σε τέτοιες επιθέσεις, καθώς πολύ συχνά το Wi-Fi είναι ο μόνος τρόπος με τον οποίο μπορούν οι χρήστες να αποκτήσουν πρόσβαση στο Διαδίκτυο. Οι χρήστες μπορούν να ανακατευθυνθούν βέβαια σε ιστοσελίδες κακόβουλου περιεχομένου με μολυσμένες εφαρμογές δελεάζοντας τον χρήστη να τις χρησιμοποιήσει. Για αυτό, το πρόγραμμα περιήγησης που υπάρχει στις συσκευές αποτελεί τον ιδανικότερο φορέα επίθεσης.

Ένα ακόμα παράδειγμα, μπορεί να αποτελέσει η ασύρματη τεχνολογία NFC που διευκολύνει την αποστολή πληροφοριών και την πραγματοποίηση πληρωμών. Μέσω της διευκόλυνσης αυτής, υπάρχει ο κίνδυνος της επίθεσης από κακόβουλο κώδικα που λαμβάνουν οι συσκευές NFC. Ο κώδικας αυτός υποκλέπτει πληροφορίες από τη συσκευή NFC και τις στέλνει στον εισβολέα, ο οποίος στη συνέχεια μπορεί να αποκτήσει πρόσβαση στη συγκεκριμένη συσκευή, με αποτέλεσμα να μεταποιήσει ή να καταστρέψει τα δεδομένα.

Μία άλλη μορφή επιθέσεων μπορεί να αποτελέσει η τεχνολογία Bluetooth, η οποία υπάρχει σε όλες τις συσκευές και χρησιμοποιείται συνεχώς από τους χρήστες για μεταφορά δεδομένων και αρχείων. Η τεχνολογία αυτή επιτρέπει σε ορισμένα worms[1] να εξαπλωθούν μεταξύ των συνδεδεμένων συσκευών. Έτσι, με την πρώτη σύνδεση των συσκευών, εκείνα αλληλεπιδρούν ανενόχλητα μεταξύ των συσκευών.

[1]Worms: είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού.

2.3.1 ΕΙΔΗ ΑΠΕΙΛΩΝ

Η ασφάλεια αποτελείται από διαδικασίες και μέτρα που έχουν σχεδιαστεί και εφαρμοστεί για την προστασία συστημάτων, δικτύων και δεδομένων από το έγκλημα στον ηλεκτρονικό χώρο. Η αποτελεσματική ασφάλεια μειώνει τον κίνδυνο των επιθέσεων και προστατεύει οργανισμούς και ιδιώτες από τη σκόπιμη εκμετάλλευση συστημάτων, δικτύων και τεχνολογιών.

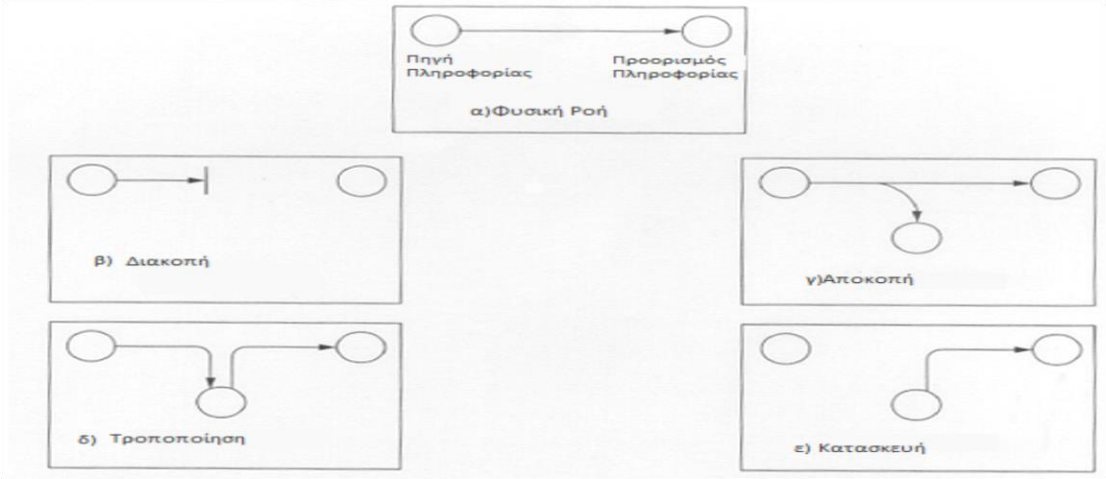
Ο όρος ασφάλεια αποσκοπεί σε πολλά πράγματα που κυμαίνονται από μπλοκ υλικού έως μονάδες λογισμικού. Ένας πιο αποτελεσματικός τρόπος να εξετάσουμε την έννοια της ασφάλειας, είναι από την πλευρά της επίθεσης που πρόκειται να διασφαλιστεί. Κάποιες από τις απειλές που χρειάζεται να διασφαλιστούν είναι οι παρακάτω:

•**Διακοπή:** ένας πόρος του συστήματος καταστρέφεται ή δεν είναι διαθέσιμος ή δεν μπορεί να χρησιμοποιηθεί. Αυτό αποτελεί απειλή κατά της διαθεσιμότητας. Για παράδειγμα η κατάργηση μιας γραμμής επικοινωνίας ή η αχρήστευση του συστήματος διαχείρισης.

•**Αποκοπή:** Ένας μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση στο σύστημα. Αυτό αποτελεί απειλή κατά του απόρρητου του συστήματος. Για παράδειγμα η κλοπή δεδομένων από το δίκτυο.

•**Τροποποίηση**: Ένας μη εξουσιοδοτημένος χρήστης, όχι μόνο αποκτά πρόσβαση στο σύστημα αλλά επιδρά αρνητικά στη λειτουργία του. Αυτό αποτελεί απειλή κατά της ακεραιότητας.

•**Κατασκευή (Πλαστογράφηση):** Ένας μη εξουσιοδοτημένος χρήστης εισάγει πλαστά αντικείμενα στο σύστημα. Και αυτό αποτελεί σαν μία απειλή κατά της ακεραιότητας. Για παράδειγμα η εισαγωγή πλαστών μηνυμάτων ή η προσθήκη εγγραφών σε ένα αρχείο.



Εικόνα 3: Κύριες κατηγορίες Απειλών

Οι πόροι ενός υπολογιστικού συστήματος που είναι πιο εύκολο να απειληθούν είναι το υλικό, το λογισμικό, τα δεδομένα, οι γραμμές επικοινωνίας και το δίκτυο.

2.3.1.1 ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΟΥ ΥΛΙΚΟΥ

Μια συσκευή αλλάζει τα χέρια πολλές φορές καθώς πηγαίνει από το εργοστάσιο στο χρήστη και στο τέλος της ζωής. Πρέπει να προστατευτεί με κάποιο τρόπο η ακεραιότητα της συσκευής καθώς περνάει από αυτόν τον κύκλο.

Η πιο σημαντική απειλή κατά του υπολογιστικού συστήματος είναι στο τομέα του υλικού. Το υλικό και η διαθεσιμότητά του είναι το πιο εύκολο τμήμα σε επιθέσεις και το δυσκολότερο στη χρήση ελέγχου. Η καταστροφή των μηχανημάτων ή και η κλοπή τους ακόμα επέρχονται τυχαία ή εσκεμμένα. Η συνεχόμενη αύξηση των προσωπικών υπολογιστών καθώς και της χρήσης των τοπικών δικτύων αυξάνουν την πιθανότητα μιας επερχόμενης βλάβης.

Οι ισχυρές άμυνες εξαρτώνται από υλικολογισμικούς και αξιόπιστους διακομιστές, οι οποίοι με τη σειρά τους βασίζονται σε ένα βασικό σύνολο χαρακτηριστικών υλικού.

2.3.1.2 ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ

Σαν απειλή κατά του υπολογιστικού συστήματος είναι και η επίθεση λογισμικού. Αυτές είναι οι πιο κοινές επιθέσεις όπου κάποιος βρίσκει τρόπο να χρησιμοποιήσει τον υπάρχοντα κώδικα για να αποκτήσει πρόσβαση σε περιορισμένους πόρους. Θα μπορούσε να οφείλεται σε σφάλμα λογισμικού ή σε

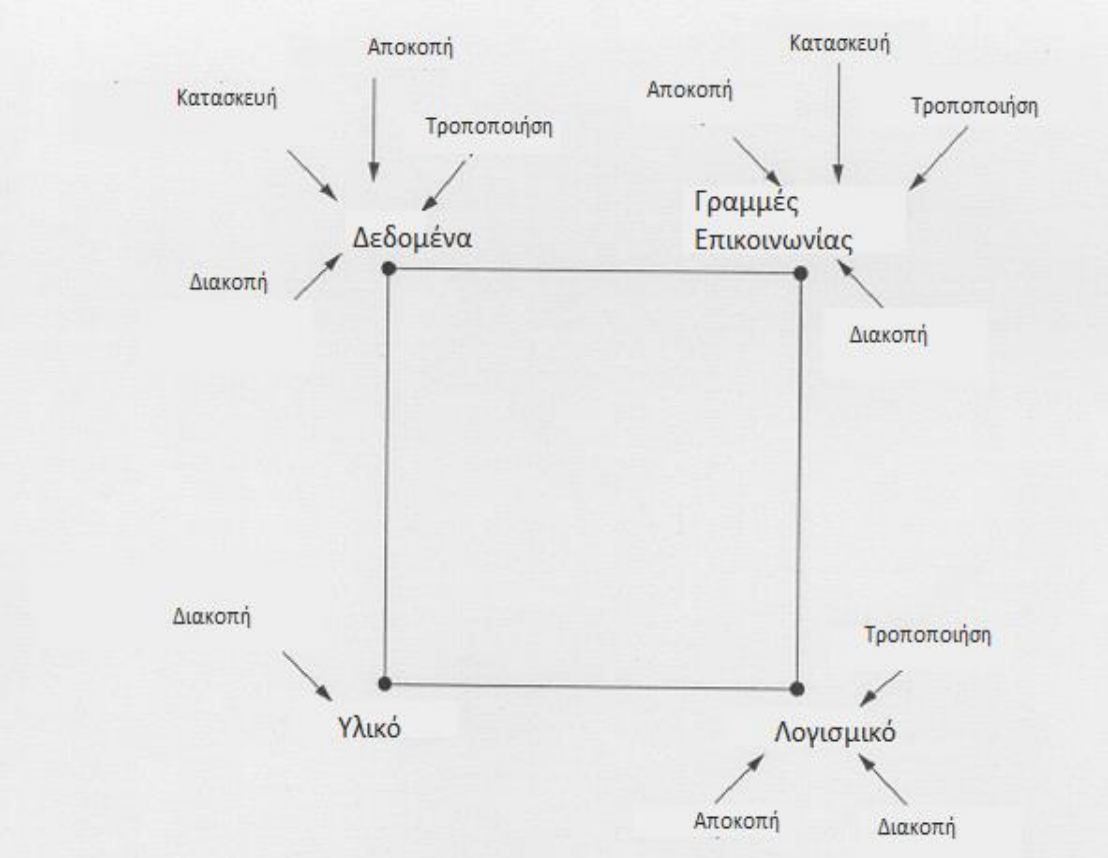
απροσδόκητες ακολουθίες κλήσεων. Ειδικότερα, το λογισμικό αλλά και τα προγράμματα εφαρμογών μπορούν είτε να σβηστούν είτε να τροποποιηθούν ή ακόμα και να καταστραφούν, έτσι ώστε να μη μπορούν να χρησιμοποιηθούν ξανά. Η δημιουργία αρχείων back-up της τελευταίας έκδοσης του λογισμικού, μπορεί να διαφυλάξει τη διαθεσιμότητα του λογισμικού. Στην περίπτωση της τροποποίησης λογισμικού, όπου το αποτέλεσμα είναι ένα πρόγραμμα που εξακολουθεί να λειτουργεί, αντιμετωπίζεται πιο δύσκολα και συμπεριφέρεται διαφορετικά από πριν.

2.3.1.3 ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Εκτός από την ασφάλεια του υλικού και του λογισμικού, χρειάζεται να επικεντρωθούμε σε ένα πιο ευρέως διαδεδομένο πρόβλημα. Αυτό αφορά τις απειλές κατά των δεδομένων και πως αυτές επηρεάζουν έναν οργανισμό ή μια επιχείρηση. Πιο συγκεκριμένα, όσον αφορά το απόρρητο των δεδομένων, είναι η μη εξουσιοδοτημένη ανάγνωση των αρχείων/δεδομένων και πάνω σε αυτό έχουν διεξαχθεί οι περισσότερες έρευνες ασφαλείας. Από τη άλλη, η ανάλυση των δεδομένων που εμφανίζεται μέσω στατιστικών βάσεων, οι οποίες παρέχουν συνολικές πληροφορίες αποτελούν λιγότερο φανερό πρόβλημα του απόρρητου. Παρόλα αυτά η εκτεταμένη χρήση των στατιστικών βάσεων απειλεί την αποκάλυψη προσωπικών δεδομένων. Στην πραγματικότητα, χαρακτηριστικά από ιδιώτες μπορεί να αναγνωριστούν με προσεκτική ανάλυση.

2.3.1.4 ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΩΝ ΓΡΑΜΜΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΤΟΥ ΔΙΚΤΥΟΥ

Ένας εισβολέας μπορεί να χρησιμοποιήσει πολλαπλά μέσα για να πάρει, να παραβιάσει ή να διαταράξει τα δεδομένα. Οι συσκευές πρέπει για το λόγο αυτό να αναπτύξουν κρυπτογραφικές άμυνες, ώστε να ταιριάζουν με τα στοιχεία που επικοινωνούν. Τα συστήματα επικοινωνίας είναι απαραίτητα ώστε να πραγματοποιηθεί η μετάδοση των δεδομένων. Έτσι το πρόβλημα της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας που σχετίζονται με την ασφάλεια των δεδομένων, απασχολούν εξίσου και την ασφάλεια των δικτύων και των γραμμών επικοινωνίας. Από τα παραπάνω, οι απειλές κατηγοριοποιούνται σε παθητικές και ενεργές.



Σχήμα 1: Η Επιρροή των απειλών ανάλογα με τον μέσο που απειλούν

Οι παθητικές απειλές έχουν να κάνουν με την παρατήρηση των μεταδόσεων σε έναν οργανισμό. Ο στόχος των εισβολέων είναι να κλέψουν πληροφορίες που κυκλοφορούν στο δίκτυο.

Υπάρχουν δύο κατηγορίες παθητικών απειλών. Η πρώτη είναι η κυκλοφορία του περιεχομένου ενός μηνύματος και η δεύτερη είναι η ανάλυση της κυκλοφορίας του δικτύου. Με τον όρο κυκλοφορία του περιεχομένου ενός μηνύματος, εννοείται μία τηλεφωνική συνομιλία, ένα ηλεκτρονικό μήνυμα ή ένα απεσταλμένο αρχείο μπορεί να περιέχει απόρρητες πληροφορίες. Σκοπός είναι ο αποκλεισμός του εισβολέα σε οποιαδήποτε πρόσβαση στις πληροφορίες. Η δεύτερη παθητική απειλή είναι η ανάλυση της κυκλοφορίας του δικτύου η οποία δεν παρουσιάζει τόσο συχνή εφαρμογή.

Η τεχνική που χρησιμοποιείται σήμερα είναι η κρυπτογράφηση. Παρόλα αυτά, ακόμη και αν εφαρμοζόταν αυτή η τεχνική θα μπορούσε να προσδιοριστεί η τοποθεσία και η ταυτότητα του αποστολέα. Αυτή η πληροφορία μπορεί να αποδειχθεί χρήσιμη για να ανακαλυφθεί η φύση της επικοινωνίας.

Οι παθητικές απειλές είναι πολύ δύσκολο να ανακαλυφθούν επειδή δεν περιλαμβάνουν τροποποίηση δεδομένων. Όμως, είναι εφικτό να προληφθούν αυτές οι επιθέσεις. Στόχος εδώ είναι να επιτευχθεί η πρόληψη και όχι η ανακάλυψη.

Η δεύτερη βασική κατηγορία είναι οι ενεργές απειλές. Σε αυτή τη κατηγορία γίνεται λόγος για την δημιουργία μίας σωστής ροής δεδομένων ή μίας λανθασμένης ροής δεδομένων. Για αυτό γίνεται αναφορά σε τρείς υποκατηγορίες. Αρχικά η διακοπή της υπηρεσίας μηνυμάτων, η τροποποίηση της ροής των δεδομένων, η άρνηση υπηρεσίας μηνυμάτων και η πλαστογράφηση.

Η διακοπή της υπηρεσίας μηνυμάτων υποδηλώνει ότι μπορεί να διακοπεί η μετάδοση κάποιου τμήματος του αρχικού μηνύματος ή και ακόμα και ολόκληρου του δικτύου.

Η τροποποίηση της ροής των δεδομένων δηλώνει ότι κάποιο τμήμα του αρχικού μηνύματος έχει υποστεί πλαστογράφηση ή ακόμα και ότι τα μηνύματα καθυστερούν. Η πλαστογράφηση συμβαίνει όταν μια ολόκληρη οντότητα υποδηλώνει ότι είναι κάποια άλλη. Η πλαστογράφηση συνήθως περιλαμβάνει μια από τις άλλες δύο μορφές ενεργών απειλών.

Η άρνηση υπηρεσίας μηνυμάτων εμποδίζει την μετάδοση των μηνυμάτων προς μια κατεύθυνση ή μπορεί να προκαλέσει υπερφόρτωση του δικτύου με μηνύματα με αποτέλεσμα να μειωθεί η απόδοση του.

Οι ενεργές απειλές παρουσιάζουν τα αντίθετα χαρακτηριστικά από τις παθητικές. Ενώ για τις παθητικές απειλές είναι δύσκολο να προληφθούν μέτρα για την αντιμετώπισή τους, παρόλα αυτά είναι ευρέως διαθέσιμα. Αντίθετα όμως, οι ενεργές απειλές δύσκολα αντιμετωπίζονται, καθώς αυτό θα απαιτούσε την προστασία μέσω κάποιου φυσικού τρόπου. Σε αυτή τη κατηγορία σκοπός είναι η ανακάλυψη αυτών των επιθέσεων και η επαναφορά του συστήματος στην ομαλή του λειτουργία.

2.3.1.5 ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΔΙΚΤΥΟΥ

Το σύστημα διαχείρισης ενός δικτύου αποτελείται από εφαρμογές και βάσεις δεδομένων που ασχολούνται με την διαμόρφωση και τη δομή του δικτύου. Όλες οι απειλές που συζητήθηκαν παραπάνω στο κεφάλαιο μπορούν να θεωρηθούν και σαν απειλές του συστήματος διαχείρισης. Σαν απειλή μπορεί να θεωρηθεί η προσπάθεια ενός χρήστη, που δεν έχει εξουσιοδότηση, να αποκτήσει πρόσβαση σε εφαρμογές και πληροφορίες με σκοπό να αποκτήσει την διαχείριση του συστήματος. Επιπλέον, ένα υπολογιστικό σύστημα μπορεί να προσποιηθεί ότι είναι εκείνο ο κεντρικός σταθμός διαχείρισης ολόκληρου του δικτύου. Ακόμα, μία ακόμα απειλή μπορεί να αποτελέσει το πρωτόκολλο κυκλοφορίας, το οποίο μπορεί να γίνει στόχος, με σκοπό ο εισβολέας να αποκτήσει πρόσβαση σε προσωπικά δεδομένα. Τέλος, πιο καταστροφικό θα ήταν η τροποποίηση της κυκλοφορίας με σκοπό τη διακοπή λειτουργίας του ή ακόμα και των πόρων που το σύστημα διαχειρίζεται .

Σχήμα 2 :Ο Διαχωρισμός των απειλών

2.4 ΟΦΕΛΗ ΑΝΑΛΥΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Κάθε επιχείρηση είναι απαραίτητο να οργανώνει ένα πλάνο ανάλυσης και αντιμετώπισης ενδεχόμενων κινδύνων που μπορεί να προκύψουν. Αυτό το πλάνο αποσκοπεί σε τρία βασικά στοιχεία. Αρχικά στην αποφυγή κινδύνων, έπειτα στην προστασία από λάθος αποφάσεις και τέλος στη μείωση των απωλειών από απρόσμενα γεγονότα. Με την διαδικασία της ανάλυσης των κινδύνων, προκύπτουν τα εξής οφέλη:

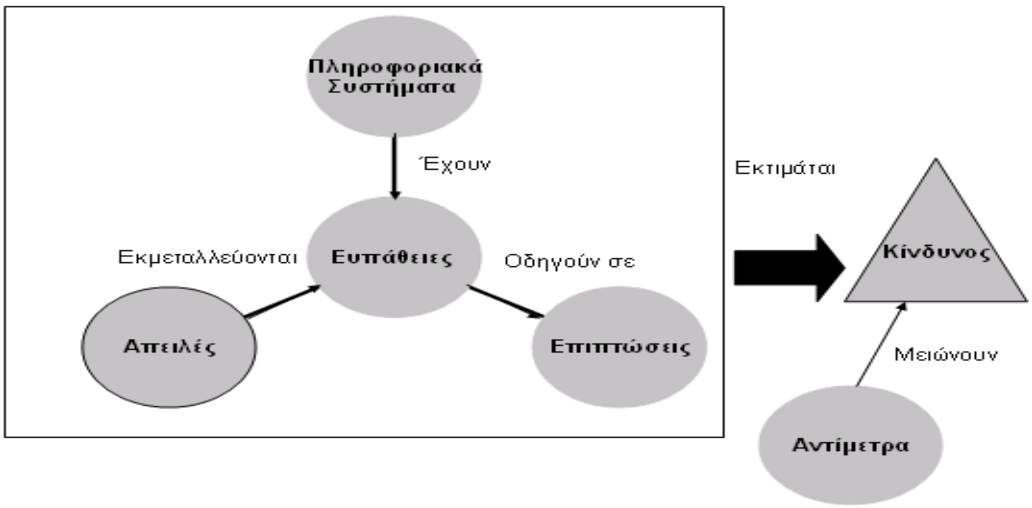
- Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος
- Βελτίωση της κατανόησης των αναγκών του συστήματος
- Κατανόηση της αναγκαιότητας της ασφάλειας και
- Δικαιολόγηση των δαπανών για την ασφάλεια

Πλέον, υπάρχουν πολλές και διαφορετικές τεχνικές για την ανάλυση της επικινδυνότητας ώστε να επιτευχθεί η αξιολόγηση της ασφάλειας των πληροφοριακών συστημάτων. Στην συγκεκριμένη περίπτωση, τα αποτελέσματα της ανάλυσης επικινδυνότητας είναι αυτά που καθορίζουν τη διαμόρφωση της πολιτικής ασφάλειας.

Από αυτή την ανάλυση προκύπτει το πλεονέκτημα ότι η πολιτική ασφαλείας ανταποκρίνεται στις ολοένα αυξανόμενες ανάγκες που έχει ένας οργανισμός. Για τον οργανισμό αυτό έχει μελετηθεί η επικινδυνότητα και ότι το επίπεδο της ασφάλειας ανταποκρίνεται στους κινδύνους που τα πληροφοριακά συστήματα αντιμετωπίζουν.

Βέβαια από την ανάλυση απορρέει και το μειονέκτημα ότι οι μέθοδοι ανάλυσης επικινδυνότητας δεν ανταποκρίνονται τόσο αντικειμενικά όσο θα περίμενε κάποιος, αλλά υποκειμενικά. Άρα τα αποτελέσματα εξαρτώνται σε μεγάλο βαθμό από την εμπειρία και τις γνώσεις του αναλυτή και κατά πόσο είναι είναι σε θέση να αντιμετωπίσει τις απειλές, ώστε να έχει όσο λιγότερες επιπτώσεις γίνεται. Όμως επειδή δεν υπάρχει το τέλειο πληροφοριακό σύστημα, ο αναλυτής χρειάζεται να δει τους κινδύνους και ανάλογα με την εκτίμηση που θα κάνει να δημιουργήσει και να εφαρμόσει τα κατάλληλα αντίμετρα, ώστε να επανέλθει η αρμονική λειτουργία του πληροφοριακού συστήματος. Με τον όρο αντίμετρα δηλώνεται οποιοσδήποτε

μηχανισμός ή διαδικασία ο οποίος μπορεί να συμβάλει στον περιορισμό ή στην εξάλειψη των επιπτώσεων μιας απειλής.



Εικόνα 4: Οφέλη Ανάλυσης Επικινδυνότητας

Η επίτευξη της ασφάλειας των συστημάτων επιτυγχάνεται μέσω ενός χάρτη πορείας για την αντιμετώπιση των κινδύνων. Οι απειλές στα πληροφοριακά συστήματα είναι πολλές όπως αναφέραμε και αποσκοπούν να κάνουν το σύστημα να λειτουργεί με δυσκολία καθιστώντας το ευπαθές. Πιο συγκεκριμένα το πλάνο διαχείρισης και αντιμετώπισης κινδύνων των πληροφοριακών συστημάτων προϋποθέτει τα παρακάτω:

- Την αναγνώριση των απειλών που επιδρούν σε ένα πληροφοριακό σύστημα
- Την αναγνώριση των επιμέρους ευπαθειών
- Την αναγνώριση των πιθανών απωλειών όπου εκμεταλλεύονται ορισμένες από τις ευπάθειες
- Την πιθανότητα όπου μπορεί να συμβεί μια απώλεια
- Τον προσδιορισμό των απαραίτητων αντίμετρων για την αντιμετώπιση των κινδύνων
- Την διαμόρφωση και υλοποίηση ενός αποτελεσματικού συστήματος ασφαλείας.

ΚΕΦΑΛΑΙΟ 3: ΕΜΠΙΣΤΗ ΕΠΕΞΕΡΓΑΣΙΑ

Ο όρος Έμπιστη Επεξεργασία, “Trusted computing”, αναφέρεται στις βελτιώσεις του υλικού και στις τροποποιήσεις του λογισμικού για να επιλύουν προβλήματα ασφάλειας υπολογιστών. Το Trusted Computing είναι μια τεχνολογία που δημιουργήθηκε από την Ομάδα Trusted Computing Group. Ο όρος εξάγεται από τα αξιόπιστα συστήματα και έχει εξειδικευμένο νόημα, όπου ο υπολογιστής συμπεριφέρεται με αναμενόμενους τρόπους και συμπεριφορές που θα αναληφθούν από το υλικό και το λογισμικό του υπολογιστή.

Αρκετοί υποστηρικτές αυτών των αξιόπιστων υπολογιστών όπως για παράδειγμα, όπως η International Data Corporation, η Ομάδα στρατηγικής για τις επιχειρήσεις και η Endpoint Technologies Associates, μπορούν να ισχυριστούν ότι η τεχνολογία θα προχωρήσει με αλματώδεις και αποτελεσματικούς τρόπους προκειμένου να μπορεί να κάνει τους υπολογιστές ασφαλείς και αξιόπιστες πηγές χωρίς κακόβουλα λογισμικά και ιούς.

Επιπλέον, το Trusted Computing θα επιτρέπει στους υπολογιστές και τους διακομιστές να παρέχουν ένα πιο αποτελεσματικό πλαίσιο το οποίο θα εξασφαλίζει την ασφάλεια στους υπολογιστές σε αντίθεση με αυτήν που ήδη είναι διαθέσιμη. Από την άλλη πλευρά, υπάρχουν και αυτοί που υποστηρίζουν ότι αυτή τεχνολογία δεν εστιάζει τόσο στην αύξηση της ασφάλειας του υπολογιστή, όσο στην επίτευξη πολιτικών σκοπών και στη διαχείριση των ψηφιακών δικαιωμάτων. Λόγω του ότι οι υποστηρικτές του Trusting Computing ισχυρίζονται, ότι το υλικό δεν είναι απλά ασφαλές για τον ιδιοκτήτη του, αλλά και ασφαλισμένο έναντι του κατόχου του, ανέπτυξε μια διαμάχη. Ακόμα και όταν κάποια επιστημονικά άρθρα άρχισαν να δημοσιεύουν αποσπάσματα σχετικά με "αξιόπιστους υπολογιστές" , οι αντίπαλοι αναφέρονται σε αυτό ως επικίνδυνο computing.

Αρκετοί σημαντικοί κατασκευαστές υλικού και πωλητές λογισμικού, γνωστοί ως Trusted Computing Group (TCG), συνεργάζονται σε αυτό το εγχείρημα και έχουν καταλήξει σε συγκεκριμένα σχέδια. Ορίζουν μία αξιόπιστη υπολογιστική τεχνολογία την οποία χωρίζουν σε τέσσερις τεχνολογίες, που απαιτούν τη χρήση νέου ή βελτιωμένου υλικού στο επίπεδο των προσωπικών υπολογιστών (PC):

- **Κλειδί έγκρισης:** αυτό το κλειδί χρησιμοποιείται για να επιτρέψει την εκτέλεση ασφαλών συναλλαγών
- **Κάλυψη μνήμης**: όπου αποτρέπει την ακατάλληλη ανάγνωση ή ανάγνωση από τα προγράμματα από τη μνήμη άλλου υπολογιστή.
- **Ασφαλής είσοδος / έξοδος (I / O)**: όπου αντιμετωπίζει τις απειλές από το spyware[2], όπως τα keyloggers[3] και τα προγράμματα που καταγράφουν το περιεχόμενο μιας οθόνης.
- **Σφραγισμένη αποθήκευση:** όπου επιτρέπει στους υπολογιστές να αποθηκεύουν με ασφάλεια κλειδιά κρυπτογράφησης και άλλα κρίσιμα δεδομένα.
- **Απομακρυσμένη βεβαίωση:** όπου ανιχνεύει παράνομες αλλαγές στο λογισμικό δημιουργώντας κρυπτογραφημένα πιστοποιητικά για όλες τις εφαρμογές σε έναν υπολογιστή.
- **Αξιόπιστο τρίτο μέρος:** είναι μια οντότητα που διευκολύνει τις αλληλεπιδράσεις μεταξύ δύο μερών που και οι δύο εμπιστεύονται το τρίτο μέρος, το οποίο εξετάζει όλες τις κρίσιμες επικοινωνίες μεταξύ των μερών.

Για να είναι αποτελεσματικά τα μέτρα αυτά πρέπει να διέπονται από προόδους και βελτιώσεις στο λογισμικό καθώς επίσης και τα λειτουργικά συστήματα που χρησιμοποιούν οι υπολογιστές.

Μπορούμε να πούμε πως η αξιόπιστη πληροφορική έχει σκοπό να εξασφαλίσει όσο πιο δυνατόν έγκυρα τα αποτελέσματα των υπολογιστών καθώς περιλαμβάνει οποιοδήποτε είδος υλικού, λογισμικού, αλγορίθμου ή οτιδήποτε άλλο. Προτάθηκε μια ιδέα, η οποία υποστήριζε ότι από τη στιγμή που θα υπάρξουν αποτελεσματικοί μηχανισμοί στο υλικό, αυτόματα δεν θα ήταν αναγκαίος ο συνεχής έλεγχος της ασφάλειας των υπολογιστών από τους χρήστες και τους διαχειριστές των δικτύων. Παρόλα αυτά, παρουσιάστηκαν προβλήματα όσον αφορά την σωστή

[2]spyware ή τον ελληνικό λογισμικό κατασκοπίας, αναφερόμαστε σε ένα είδος κακόβουλου λογισμικού το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη.

[3] Keyloggers: χρησιμοποιούνται για την καταγραφή πληκτρολογίου , μια μέθοδος καταγραφής και καταγραφής πληκτρολογήσεων χρηστών υπολογιστών, συμπεριλαμβανομένων ευαίσθητων κωδικών πρόσβασης.

λειτουργία της ιδιωτικής ζωής των χρηστών, αλλά και ανησυχίες πως οι ζωές θα ήταν άμεσα συνυφασμένες από αυτό.

Το ευρύτερο πεδίο της βάσης αξιόπιστων υπολογιστών περιλαμβάνει ένα υπολογιστικό σύστημα που παρέχει ένα ασφαλές περιβάλλον. Αποτελείται από το λειτουργικό σύστημα και τους μηχανισμούς ασφαλείας, καθώς και το υλικό του υπολογιστή, τους πόρους του δικτύου και τις ανάλογες διαδικασίες. Στόχος των βιομηχανιών είναι να παράγουν ηλεκτρονικούς υπολογιστές και συσκευές στοχεύοντας στη διατήρηση ενός ασφαλούς πλαισίου γύρω από τα μηχανήματα και τις περιφερειακές τους συσκευές.

Εφόσον ένας υπολογιστής είναι εφοδιασμένος με την τεχνολογία Trusted Computing, είναι σε θέση να πιστοποιεί τη δική του ταυτότητα. Απαιτεί από όλους τους προμηθευτές λογισμικού και υλικού να ακολουθήσουν όλες τις προδιαγραφές που έκανες ευρέως γνωστές η ομάδα αξιόπιστων υπολογιστών, προκειμένου να υπάρχει αλληλεπίδραση και λειτουργικότητα μεταξύ τους. Όμως, παρά τις απαιτήσεις συνεχίζουν να υπάρχουν προβλήματα στη λειτουργικότητα, τα οποία αφορούν την σωστή επιλογή λογισμικού. Με την απελευθέρωσή του ως λογισμικό ανοιχτού κώδικα, συντέλεσε στο να διατίθεται ο πηγαίος κώδικας σε τρίτον για να τον εξετάσει. Αυτό βέβαια δεν σημαίνει απαραιτήτως ότι το λογισμικό είναι δωρεάν, αλλά δίνει τη δυνατότητα σε κάθε χρήστη να χρησιμοποιήσει τις δυνατότητες που προσφέρει ο παρεχόμενος κώδικας. Στην πράξη, όμως τα περισσότερα προγράμματα ανοιχτού κώδικα είναι δωρεάν και χαρακτηρίζονται ελεύθερα.

Το Trusted Computing θα επιτρέπει στις εταιρείες να δημιουργήσουν ένα σύστημα διαχείρισης ψηφιακών δικαιωμάτων (DRM) το οποίο δεν θα μπορεί να παρακαμφθεί, αλλά δεν θα είναι και αδύνατο. Ένα παράδειγμα είναι η λήψη ενός αρχείου. Η σφραγισμένη αποθήκευση θα μπορούσε να χρησιμοποιηθεί για να εμποδίσει τον χρήστη από το άνοιγμα του αρχείου με μία μη εξουσιοδοτημένη συσκευή.

Τα νέα επιχειρηματικά μοντέλα για χρήση λογισμικού (υπηρεσιών) μέσω Διαδικτύου ενδέχεται να ενισχυθούν από την τεχνολογία. Με την ενίσχυση του συστήματος διαχείρισης των ψηφιακών δικαιωμάτων DRM, κάποιος θα μπορούσε να βασίσει ένα επιχειρηματικό μοντέλο πάνω σε αυτή το σύστημα.

Το Trusted Computing θα μπορούσε να χρησιμοποιηθεί για την αντιμετώπιση της εξαπάτησης στα διαδικτυακά παιχνίδια . Μερικοί παίκτες επεμβαίνουν στο αντίγραφο του παιχνιδιού τροποποιώντας το για να αποκτήσουν με άδικο τρόπο

πλεονεκτήματα στο παιχνίδι. Η απομακρυσμένη βεβαίωση, η ασφαλής είσοδος / έξοδος και η αποθήκευση μνήμης είναι ορισμένες υπηρεσίες οι οποίες θα μπορούσαν να χρησιμοποιηθούν προκειμένου να καθοριστεί η εκτέλεση ενός μη τροποποιημένου αντιγράφου του λογισμικού, από όλες τις συσκευές αναπαραγωγής που είναι συνδεδεμένες σε έναν διακομιστή.

Το Trusted Computing θα μπορούσε να χρησιμοποιηθεί για να εγγυηθεί ότι οι συμμετέχοντες σε ένα σύστημα υπολογιστών, επιστρέφουν τα αποτελέσματα των υπολογισμών όπως είναι στη πραγματικότητα χωρίς να τα μεταποιούν. Αυτό θα επιτρέπει την εκτέλεση προσομοιώσεων μεγάλης κλίμακας χωρίς περιττούς υπολογισμούς, προκειμένου να εγγυηθεί ότι κακόβουλοι κεντρικοί υπολογιστές δεν υπονομεύουν τα αποτελέσματα για να επιτύχουν το συμπέρασμα που θέλουν.

ΚΕΦΑΛΑΙΟ 4: ΤΕΧΝΟΛΟΓΙΕΣ ΠΑΡΟΧΗΣ ΑΣΦΑΛΕΙΑΣ

Σε αυτό το κεφάλαιο θα ασχοληθούμε με ορισμένες τεχνολογίες και πιο συγκεκριμένα με τρείς τεχνολογίες τις οποίες θα αναλύσουμε πως η κάθε μία παρέχει ασφάλεια σε ένα σύστημα.

4.1: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ARM ΤΕΧΝΟΛΟΓΙΑ

Η ARM (Advanced RISC Machine) είναι μια αρχιτεκτονική συνόλου εντολών RISC των 32-bit, η οποία έχει αναπτυχθεί από την ARM Holdings η οποία παλαιότερα ονομαζόταν Μηχανή RISC Acorn (Acorn RISC Machine). Η αρχιτεκτονική ARM εμφανίζεται πιο συχνά όσον αφορά τους επεξεργαστές της, διότι είναι σχετικά απλοί, κάτι που τους κάνει κατάλληλους για εφαρμογές χαμηλής ισχύος. Αυτό έχει ως αποτέλεσμα να έχουν υπερισχύσει στις αγορές των κινητών και των ενσωματωμένων συστημάτων, σαν μικροί και σχετικά χαμηλού κόστους μικροεπεξεργαστές. Για να διατηρηθεί η σχεδίαση απλή και γρήγορη, η αρχική υλοποίηση της ARM είχε κατασκευαστεί όπως ο απλούστερος επεξεργαστής 6502 των 8-bit που χρησιμοποιούνταν πριν στους μικροϋπολογιστές Acorn.

Η αρχιτεκτονική ARM περιλαμβάνει τα εξής RISC χαρακτηριστικά:

•Αρχιτεκτονική φόρτωσης/αποθήκευσης.

•Δεν υποστηρίζει μη-ευθυγραμμισμένη πρόσβαση στη μνήμη.

•Ομοιόμορφο αρχείο καταχωρητών 16 × 32-bit.

•Σταθερό εύρος εντολών 32-bit για εύκολη αποκωδικοποίηση,
με μειονέκτημα την μικρότερη πυκνότητα κώδικα. Συνήθως η εκτέλεση
γίνεται σε έναν κύκλο.

Η απλή σχεδίαση, βελτιώθηκε με προσθήκη των εξής χαρακτηριστικών:

•Εκτέλεση υπό συνθήκη των περισσότερων εντολών, που μειώνει τις όποιες επιβαρύνσεις και αντιμετωπίζει την έλλειψη μηχανισμού πρόβλεψης διακλάδωσης.
•Οι αριθμητικές εντολές αλλάζουν τον κώδικα μόνο όταν χρειάζεται.

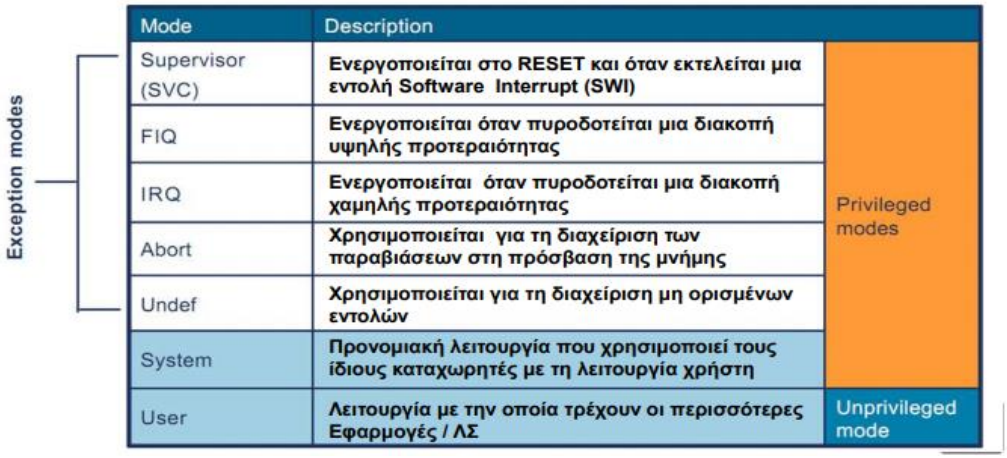
•Ισχυροί τρόποι σχηματισμού διευθύνσεων με δείκτες.

•Ένας καταχωρητής συνδέσμου για γρήγορες κλήσεις συναρτήσεων-φύλλων (leaf function calls).

•Απλό αλλά γρήγορο υποσύστημα διακοπών 2 επιπέδων προτεραιοτήτων.

Από το 2005, πάνω από ένα δισεκατομμύριο κινητά τηλέφωνα πωλούνται κάθε χρόνο και έχουν ενσωματωμένο έναν επεξεργαστή ARM. Οι πυρήνες ARM χρησιμοποιούνται σε αρκετά προϊόντα, όπως τα έξυπνα τηλέφωνα (smartphones), στον φορητό αναπαραγωγέα πολυμέσων iPod της Apple, στην ψηφιακή μηχανή PowerShot A470 της Cannon, στη φορητή κονσόλα βιντεοπαιχνιδιών Nintendo DS. Το 2009 οι επεξεργαστές ARM εγκαταστάθηκαν σε πολλούς ενσωματωμένους επεξεργαστές και σε πολλά ηλεκτρονικά προϊόντα.
Η αρχιτεκτονική ARM είναι διαθέσιμη προκειμένου να τη χρησιμοποιήσει όποιος τη χρειάζεται. Κάποιες από τις εταιρείες που την έχουν ή την είχαν αγοράσει είναι η Alcatel, η Apple, η Intel , η LG και άλλες πολλές μεγάλες πολυεθνικές εταιρίες.

Αρχιτεκτονική	Οικογένεια
ARMv1	ARM1
ARMv2	ARM2, ARM3
ARMv3	ARM6, ARM7
ARMv4	Strong ARM, ARM7TDMI, ARM9TDMI
ARMv5	ARM7EJ, ARM9E, ARM10E, X-Scale
ARMv6	ARM11
ARMv7	Cortex
ARMv8	Cortex-A35 , Cortex-A53, CortexA-57 CortexA-72



Σχήμα 3: Οι 7 Βασικές Λειτουργίες του πυρήνα της ARM

4.1.1: TRUSTZONE ΚΑΙ ΠΛΑΙΣΙΟ ΠΑΡΟΧΗ ΑΣΦΑΛΕΙΑΣ

Η τεχνολογία Arm TrustZone είναι μια προσέγγιση συστήματος για το Chip (SoC) και για την ασφάλεια του CPU σε όλο το σύστημα. Το TrustZone αποτελεί ασφάλεια που βασίζεται στο υλικό που ενσωματώνεται σε SoC’s από σχεδιαστές chip ημιαγωγών με σκοπό να παρέχουν ασφαλή τελικούς προορισμούς και μια βάση εμπιστοσύνης στη συσκευή.

Η αρχιτεκτονική υλικού του TrustZone στοχεύει στο να παρέχει ένα πλαίσιο ασφαλείας αντιμετωπίζοντας πολλές από τις απειλές που θα συναντήσει. Η τεχνολογία TrustZone αντί να παρέχει μια σταθερή λύση ασφάλειας για όλους, επιλέγει να παρέχει κάποια πρώτα στάδια υποδομής δίνοντας στους σχεδιαστές SoC την επιλογή μιας σειράς από αυτά, ώστε να μπορούν να εκπληρώσουν συγκεκριμένες λειτουργίες εντός του περιβάλλοντος ασφαλείας.

Βασικός στόχος της αρχιτεκτονικής για την ασφάλεια, είναι η κατασκευή ενός προγραμματιζόμενου περιβάλλοντος το οποίο θα στοχεύει στην εμπιστευτικότητα αλλά και ακεραιότητα μεταξύ όλων των περιουσιακών στοιχείων, με σκοπό να αποτρέπονται συγκεκριμένες επιθέσεις.

Η τεχνολογία TrustZone παρέχει μια βάση για την ασφάλεια του συστήματος με τη δημιουργία μιας αξιόπιστης πλατφόρμας. Οποιοδήποτε τμήμα του συστήματος μπορεί να σχεδιαστεί για να είναι μέρος του ασφαλούς κόσμου,

συμπεριλαμβανομένων τον εντοπισμό σφαλμάτων, των περιφερειακών, των διακοπών και της μνήμης.

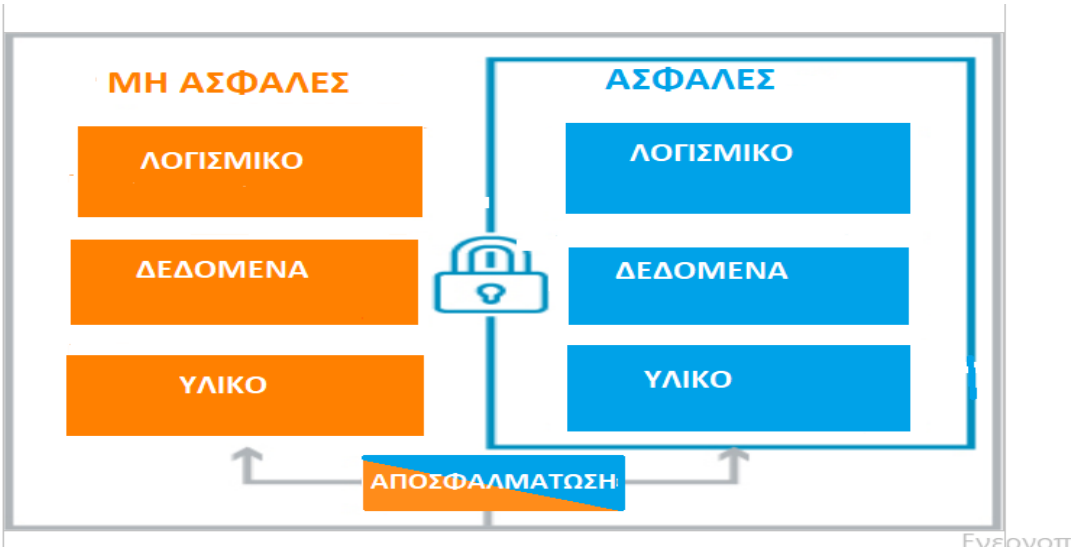
Η λύση είναι να εμπλουτισθεί το λειτουργικό σύστημα με ένα πιο περιοριστικό περιβάλλον προκειμένου να εξαχθούν τα συστατικά ασφαλείας από τις εφαρμογές ή το λειτουργικό σύστημα σε αυτό το περιβάλλον. Τα περιβάλλοντα αξιόπιστης εκτέλεσης παρέχουν ένα τέτοιο λογισμικό. Αυτό το λογισμικό είναι διαθέσιμο και προσφέρει αξιόπιστη εκκίνηση και ασφαλή εκτέλεση χρόνου, η οποία φροντίζει για την εναλλαγή μεταξύ των μη ασφαλών (μη αξιόπιστων) και ασφαλών (αξιόπιστων) κόσμων.

Η δημιουργία ενός TEE (Trusted Execution Environment), αποτελεί μια ασφαλής περιοχή ενός κύριου επεξεργαστή που εξασφαλίζει την προστασία του κωδικού και των δεδομένων που έχουν φορτωθεί στο εσωτερικό του. Ένα TEE ως απομονωμένο περιβάλλον εκτέλεσης παρέχει χαρακτηριστικά ασφαλείας όπως η μεμονωμένη εκτέλεση, η ακεραιότητα των εφαρμογών που εκτελούνται καθώς και η εμπιστευτικότητα των περιουσιακών τους στοιχείων. Το TEE έχει σχεδιαστεί για να προστατεύει από επιθέσεις εφαρμογών λογισμικού, εάν κάποιος έχει κλέψει τη συσκευή κάποιου και από κοινές επιθέσεις υλικού. Το TEE βασίζεται στο TrustZone παρέχοντας έναν "ασφαλή κόσμο", βάζοντας μικρά όρια ασφάλειας ώστε να προσφέρουν πιστοποίηση και αποδεδειγμένη ασφάλεια. Επιπλέον, χρησιμοποιείται για τη διασφάλιση των κρυπτογραφικών κλειδιών, των διαπιστευτηρίων και άλλων ασφαλή περιουσιακών στοιχείων. Το TrustZone παρέχει στον επιβλέποντα χαρακτηριστικά ασφαλείας στο σύστημα που δεν είναι διαθέσιμα, όπως ασφαλή αποσφαλμάτωση, ασφαλείς συναλλαγές και πραγματοποίηση ασφαλών διακοπών απευθείας στον ασφαλή κόσμο. Ενώ παρέχει και ορισμένες επεκτάσεις ασφαλείας στον επεξεργαστή όπως μία πρόσθετη κατάσταση διασφαλίζει τον ασφαλή κωδικό εφαρμογής και τα δεδομένα που πρέπει να απομονωθούν από τις κανονικές λειτουργίες.

Στο επίκεντρο της προσέγγισης TrustZone παρουσιάζεται η έννοια των ασφαλών και μη ασφαλών κόσμων που διαχωρίζονται από το υλικό, εμποδίζοντας το μη ασφαλές λογισμικό από την άμεση πρόσβαση σε ασφαλείς πόρους. Μέσα στον επεξεργαστή, το λογισμικό είτε βρίσκεται στον ασφαλή κόσμο είτε στον μη ασφαλή κόσμο, μπορεί να επιτευχθεί μια εναλλαγή μεταξύ αυτών των δύο κόσμων μέσω

λογισμικού που αναφέρεται ως ασφαλή οθόνη (Cortex-A)[4] ή από την λογική πυρήνα (Cortex-M)[5]. Αυτή η έννοια των ασφαλών και των μη ασφαλών κόσμων επεκτείνεται πέρα από τον επεξεργαστή ώστε να καλύπτει τη μνήμη, το λογισμικό και τα περιφερειακά συστήματα εντός ενός SoC.

Για να κατασκευαστεί ένα γενικό πλαίσιο το οποίο θα λύνει προβλήματα ασφάλειας, που μπορεί να μην παρέχει οικονομικές αποδόσεις όπως οι παραδοσιακές μέθοδοι, χρειάζεται μια πλατφόρμα που να περιέχει αυτά τα χαρακτηριστικά. Για να υπάρχει ασφάλεια στο σύστημα χρειάζεται ο διαχωρισμός όλων των υλικών του SoC και του λογισμικού, σε τουλάχιστον έναν από τους δύο κόσμους. Στην πραγματικότητα, εξασφαλίζεται ότι δεν υπάρχει μόνο ο ασφαλής κόσμος και ότι οι πόροι είναι διαθέσιμοι από τα συνήθη στοιχεία του μη ασφαλούς κόσμου, επιτρέποντας μια ισχυρή ασφάλεια μεταξύ τους. Η εφαρμογή ισχυρού λογισμικού, που εκτελείται στους ασφαλείς πυρήνες του επεξεργαστή, μπορεί να προστατεύσει σχεδόν οποιοδήποτε περιουσιακό στοιχείο από πολλές πιθανές επιθέσεις. Τέτοιες επιθέσεις στην πραγματικότητα είναι δύσκολο να εξασφαλιστούν συμπεριλαμβανομένων των κωδικών πρόσβασης που εισάγονται χρησιμοποιώντας ένα πληκτρολόγιο ή μία οθόνη αφής.



Εικόνα 5: Ασφαλής και Μη Ασφαλής Κόσμος

[4] Cortex-A: είναι μια ομάδα πυρήνων επεξεργαστή RISC ARM 32-bit και 64-bit με άδεια από την Arm Holdings

[5] Cortex-M: είναι μια ομάδα πυρήνων επεξεργαστή RISC ARM 32-bit με άδεια από την Arm Holdings. Χρησιμοποιούνται συνήθως ως αποκλειστικά τσιπ μικροελεγκτή αλλά επίσης και ως ελεγκτές οθόνης αφής.

Η δεύτερη πτυχή της αρχιτεκτονικής TrustZone είναι κάποιες επεκτάσεις που έχουν εφαρμοστεί σε ορισμένους από τους πυρήνες επεξεργαστών της ARM. Αυτές οι επεκτάσεις επιτρέπουν σε έναν μόνο φυσικό επεξεργαστή την αποτελεσματική αλλά και την ασφαλή εκτέλεση κώδικα μεταξύ και των δύο κόσμων, με τρόπο όμως χρονοβόρο. Αυτό βέβαια αναιρεί την ανάγκη να υπάρχει ένας αποκλειστικός επεξεργαστής ασφαλείας, ο οποίος θα υπάρχει σε έναν από τους δύο κόσμους, εξοικονομώντας χώρο και ισχύ, παρέχοντας υψηλής απόδοσης λογισμικό ασφαλείας για να τρέχει παράλληλα με τον κανονικό κόσμο που λειτουργεί στο περιβάλλον.

Η τελική όψη της αρχιτεκτονικής υλικού TrustZone είναι η ασφάλεια υποδομής. Επιτρέπει τον έλεγχο της πρόσβασης στον ασφαλή κόσμο μέσω της αποσφαλμάτωσης , χωρίς να μειώνει την δυνατότητα του εντοπισμού σφαλμάτων του κανονικού κόσμου.

Το Arm TrustZone δημιουργεί έναν απομονωμένο ασφαλή κόσμο, ο οποίος μπορεί να χρησιμοποιηθεί για την παροχή εμπιστευτικότητας και ακεραιότητας στο σύστημα. Χρησιμοποιείται σε δισεκατομμύρια επεξεργαστές εφαρμογών για την προστασία κωδικών και δεδομένων υψηλής αξίας για ποικίλες περιπτώσεις χρήσης, όπως έλεγχος ταυτότητας, πληρωμή, προστασία περιεχομένου και επιχειρήσεις. Στους επεξεργαστές εφαρμογών χρησιμοποιείται συχνά για να παρέχει ένα όριο ασφαλείας. Αντί της παροχής μίας σταθερής λύσης ασφαλείας, η τεχνολογία Arm TrustZone παρέχει τις βάσεις υποδομής, που επιτρέπουν στον σχεδιαστή της SoC να επιλέξει από μια σειρά λειτουργιών που μπορούν να εκπληρώσουν συγκεκριμένες ενέργειε εντός του περιβάλλοντος ασφαλείας.

Εικόνα 6: Δυνατότητες του TrustZone

4.2 ΕΙΣΑΓΩΓΗ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ PSA

Το PSA Certified είναι ένα σύστημα πιστοποίησης ασφάλειας για υλικό, λογισμικό και συσκευές Internet of Things (IoT)[6], το οποίο εξασφαλίζει ένα ψηφιακό μετασχηματισμό σε όλες τις βιομηχανίες. Επιπλέον, αντιμετωπίζει τις προκλήσεις αλλά και τις πιέσεις που σχετίζονται με τον σχεδιασμό και την εφαρμογή της ασφάλειας, προσφέροντας εμπιστοσύνη και χαμηλότερο κόστος. Στοχεύει στην ασφάλεια των συνδεδεμένων συσκευών, από ανάλυση έως αξιολόγηση ασφάλειας και πιστοποίηση. Το πλαίσιο αυτό παρέχει ορισμένους πόρους για να βοηθήσει στην επίλυση του αυξανόμενου κατακερματισμού των απαιτήσεων IoT και να εξασφαλίσει ότι η ασφάλεια δεν αποτελεί πλέον εμπόδιο στην ανάπτυξη των προϊόντων.

Το PSA έχει εξελιχθεί έκτοτε σε πιστοποίηση PSA, που μπορεί να χρησιμοποιηθεί από τους σχεδιαστές IoT για πρακτικές ασφαλείας. Το πλαίσιο περιλαμβάνει τέσσερα διαφορετικά επίπεδα εμπιστοσύνης, με κάθε επίπεδο να διαθέτει διαφορετικό επίπεδο αξιολόγησης.

Το PSA Certified framework δημιουργήθηκε για να εξασφαλίσει ότι η ασφάλεια έχει σχεδιαστεί σε μια συσκευή από την αρχή. Τα τέσσερα πιστοποιημένα στάδια του πλαισίου PSA καθοδηγούν την εφαρμογή ασφαλείας για κάθε περίπτωση χρήσης είναι τα εξής:

- Ανάλυση: Η αξιολόγηση των περιουσιακών στοιχείων και των απειλών που προσδιορίζουν συγκεκριμένες απαιτήσεις ασφάλειας.
- Αρχιτέκτονας: Ο σχεδιασμός καθιερωμένης αρχιτεκτονικής ασφαλείας που βασίζεται σε καθορισμένες απαιτήσεις ασφαλείας.
- Υλοποίηση: Η διαδικασία της ένωσης του υλικού και του υλικολογισμικού, με σκοπό τη δημιουργία μιας εφαρμογής υψηλής ποιότητας, της οποίας οι λειτουργίες ασφαλείας θα είναι προσβάσιμες.
- Πιστοποίηση: Ένα σύστημα πιστοποίησης το οποίο διασφαλίζει ότι τα προϊόντα συμμορφώνονται με τις απαιτήσεις ασφαλείας και τους 10 στόχους ασφαλείας που περιγράφονται από το PSA Certified ως στόχοι αντιμετώπισης.

Το PSA Certified έχει ως στόχο να εξαλείψει τον κατακερματισμό της βιομηχανίας προκειμένου να κατασκευάζει προϊόντα και προγραμματιστές IoT με διάφορους τρόπους.

[6](IoT) περιγράφει το δίκτυο φυσικών αντικειμένων - "πράγματα" - που είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες με σκοπό τη σύνδεση και την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα μέσω του Διαδικτύου

Μέσω κορυφαίων προμηθευτών chip, παρέχει στον κόσμο συστήματα on-chip τα οποία είναι κατασκευασμένα με PSA Root of Trust[7] (PSA-RoT) παρέχοντας ένα παγκοσμίως διαθέσιμο πλαίσιο ασφαλείας, με ενσωματωμένες λειτουργίες, όπου μπορούν όλες οι συσκευές να τις αξιοποιήσουν. Το PSA Root of Trust (PSA-RoT) αναπτύχθηκε και σχεδιάστηκε για να βοηθήσει τους προγραμματιστές προκειμένου να εδραιώσουν αποτελεσματικά την ασφάλεια ακόμη και σε συστήματα χαμηλού κόστους. Παρέχει ένα εύχρηστο στοιχείο ασφαλείας το οποίο εφοδιάζονται οι περισσότεροι από τους κορυφαίους προμηθευτές chip στον κόσμο.

Το PSA-RoT παρέχει ένα υψηλό επίπεδο API το οποίο περιλαμβάνει:

-API κρυπτογραφίας PSA (Επίπεδο 1)

-API πιστοποίησης PSA (Επίπεδο 2)

-API αποθήκευσης PSA (Επίπεδο 3)

(Επίπεδο 1)

Το πρώτο επίπεδο πιστοποίησης ασφαλείας απευθύνεται σε προμηθευτές chip, πλατφόρμες λογισμικού και κατασκευαστές συσκευών. Ορισμένα εργαστήρια πιστοποίησης εκτελούν πιστοποιήσεις, οι οποίες αποτελούνται από ερωτήσεις, ελέγχους εγγράφων και συνεντεύξεις σε ένα από αυτά. Οι συμπληρωμένες απαντήσεις συνοδεύονται από επεξηγηματικές σημειώσεις και ελέγχονται από το εργαστήριο πιστοποίησης, οι οποίες συντονίζονται με άλλες σημαντικές απαιτήσεις, όπως πρότυπα και νόμοι.

(Επίπεδο 2)

Το δεύτερο επίπεδο πιστοποίησης ασφαλείας αποτελείται από δοκιμές που γίνονται σε εργαστήρια, στοχεύοντας στην αναθεώρηση του πηγαίου κώδικα και στην PSA-RoT της εμπιστοσύνης. Αυτό ημερολογιακά λαμβάνεται κατά τη διάρκεια ενός μήνα. Επιπλέον στοχεύει σε καθορισμένες μεθόδους επίθεσης και αξιοποιεί συγκεκριμένες μεθοδολογίες αξιολόγησης, επιτυγχάνοντας ότι το υλικό εναρμονίζεται με τις λειτουργίες του PSA RoT.

[7] Root of Trust (RoT): είναι μια πηγή που μπορεί πάντα να είναι αξιόπιστη μέσα σε ένα κρυπτογραφικό σύστημα.

(Επίπεδο 3)

Το τελικό επίπεδο παρουσιάζεται ως μία επέκταση του επιπέδου 2, διευρύνοντας την πολυπλοκότητα των επιθέσεων μέσω της ανάλυσης της προστασίας από φυσικές και πλευρικές επιθέσεις.

Εικόνα 7: Τα 3 στάδια της PSA

4.2.1 ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΥΠΑΘΕΙΩΝ ΚΑΙ ΚΙΝΔΥΝΩΝ

Επειδή κάθε σύστημα, συσκευή είναι ευάλωτο συνεχώς σε επιθέσεις και απειλές, έτσι ώστε να εκμεταλλευτούν τις αδυναμίες ασφαλείας, είναι σημαντικό να ληφθούν υπόψιν όλες οι απειλές και πώς αυτές ενδεχομένως επηρεάζουν ένα σύστημα. Στο PSA Certified, ανάλογα με το σημείο δράσης, οι τύποι απειλών διαχωρίζονται σε τέσσερις τομείς: στην επικοινωνία , στην φυσική απειλή στον κύκλος ζωής και το λογισμικό .

-Ευπάθειες επικοινωνίας.

Οι εισβολείς μπορούν να χρησιμοποιήσουν πολλούς τρόπους έτσι ώστε να παρακολουθήσουν, να πλαστογραφήσουν ή να επηρεάσουν μηνύματα που

αποστέλλονται μεταξύ συσκευών και διακομιστή . Οι κρυπτογραφικές άμυνες θα πρέπει να αντιστοιχούν στα δεδομένα με την μεγαλύτερη αξία που κοινοποιούνται.

-Φυσικές απειλές.

Συχνά χωρίζονται σε δύο κατηγορίες: τις μη επεμβατικές και τις επεμβατικές. Η μη επεμβατική ή αλλιώς και πλαϊνό κανάλι, χρησιμοποιεί διάφορους τρόπους για να προσπαθήσει να αποκτήσει πρόσβαση στο τσιπ και να αποκτήσει πληροφορίες. Τέτοιες μπορεί να αποτελούν η αλλαγή της τάσης στην τροφοδοσία ή παρεμβολή με ηλεκτρομαγνητικές υπογραφές. Ενώ οι επεμβατικές τεχνικές εστιάζουν από το άνοιγμα του τσιπ για απλή ανίχνευση μέχρι και την τροποποίηση συγκεκριμένου τμήματος ή ακόμα και ολόκληρου του chip.

-Ευπάθειες κύκλου ζωής.

Οι συσκευές αλλάζουν συνεχώς πολλές φορές χέρια από το εργοστάσιο προς τον χρήστη, από μία ενδεχόμενη συντήρηση τους μέχρι και στο τέλος του κύκλου ζωής τους. Θα πρέπει να προστατεύεται η ακεραιότητα της συσκευής σε κάθε περίπτωση. Πιο συγκεκριμένα να γίνεται έλεγχος για το ποιος και πώς την επιδιορθώνει, για το πώς χειρίζεται τα εμπιστευτικά δεδομένα, ακόμα και αν είναι νόμιμες οι αναβαθμίσεις που γίνονται στο υλικό ή στο λογισμικό. Ακόμα θα πρέπει να ελέγχονται απαγορευμένες διαδικασίες, όπως η κλοπή, οι υπερβολικές αλλαγές ή οι αλλαγές Wi-Fi.

-Ευπάθειες λογισμικού.

Αυτές είναι οι πιο συχνές επιθέσεις όπου κάποιος μπορεί να αποκτήσει πρόσβαση σε περιορισμένους πόρους. Θα μπορούσε να οφείλεται σε σφάλμα λογισμικού ή σε απρόσμενες ακολουθίες κλήσεων, όπου είναι ανοιχτές και κατηγοριοποιούνται σε ολόκληρες κατηγορίες εκμεταλλεύσεων.

Για τους λόγους αυτούς, κάθε συσκευή πρέπει να επιτύχει 10 βασικούς στόχους έτσι ώστε να αντιμετωπίσει ορισμένες από τι θεμελιώδεις απειλές, εξασφαλίζοντας ότι υπάρχει μία βάση για την ασφάλεια. Για να επιτευχθεί η ασφάλεια πρέπει να εφαρμοστούν ορισμένα αντίμετρα όπως:

-Μοναδική αναγνώριση.

Για την χρήση μιας συγκεκριμένης συσκευής, θα πρέπει να εκχωρηθεί μια μοναδική ταυτότητα σε αυτή και θα πρέπει να είναι αποδεκτή. Αυτή η ταυτότητα ορίζει την αξιόπιστη αλληλεπίδραση με τη συσκευή, προκειμένου να είναι εφικτή η ανταλλαγή δεδομένων και κυρίως η διαχείριση της συσκευής.

-Κύκλος ζωής ασφαλείας

Κάθε συσκευή ανάλογα τις εκδόσεις που ορίζονται στο λογισμικό, την κατάσταση του χρόνου εκτέλεσης, τη διαμόρφωση του υλικού και τη φάση του κύκλου ζωής της, θα πρέπει να υποστηρίζει τον κύκλο ζωής ασφαλείας. Κάθε μεταβολή στην κατάσταση του κύκλου ζωής ασφαλείας πρέπει να είναι αποδεκτή διότι μπορεί να επηρεάσει την πρόσβαση στη συσκευή.

-Επιβεβαίωση

Η βεβαίωση αποδεικνύεται από την ταυτότητα και την κατάσταση ασφαλείας του κύκλου ζωής της συσκευής. Για να πραγματοποιείται η επαλήθευση της συσκευής απαιτούνται τα δεδομένα αναγνώρισης και πιστοποίησης της συσκευής.

-Ασφαλής εκκίνηση

Μόνο εάν πραγματοποιούνται ασφαλείς εκκινήσεις και ασφαλείς διαδικασίες φόρτωσης διασφαλίζεται ότι μπορεί να εκτελεστεί μόνο ένα εγκεκριμένο λογισμικό σε μια συσκευή. Οποιοδήποτε μη εξουσιοδοτημένο λογισμικό, θα πρέπει να εντοπιστεί και να εμποδιστεί. Μόνο εάν το μη εξουσιοδοτημένο λογισμικό δεν πρόκειται να θέσει σε κίνδυνο τη συσκευή, ενδέχεται να γίνει επιτρεπτό.

-Ασφαλής ενημέρωση

Απαιτούνται ασφαλείς ενημερώσεις για την παροχή ασφάλειας στις συσκευές. Ο έλεγχος ταυτότητας, κατά τη λήψη της ενημέρωσης, ενδέχεται να πραγματοποιηθεί, αλλά η εκτέλεση της θα πρέπει να εγκριθεί μέσω της ασφαλούς εκκίνησης της συσκευής.

-Αντί-επαναφορά

Η επαναφορά σε προηγούμενες εκδόσεις λογισμικού δεν είναι απαραίτητη και θα πρέπει να γίνεται μόνο για λόγους ανάκτησης εφόσον επιτρέπεται και εάν είναι ανάγκη.

-Απομόνωση

Η απομόνωση αποτρέπει τη δράση μιας υπηρεσίας ή διαδικασίας από το να θέσει σε κίνδυνο άλλες υπηρεσίες. Αυτό γίνεται με την απομόνωση των λιγότερο αξιόπιστων υπηρεσιών από τις μη αξιόπιστες υπηρεσίες.

-Αλληλεπίδραση

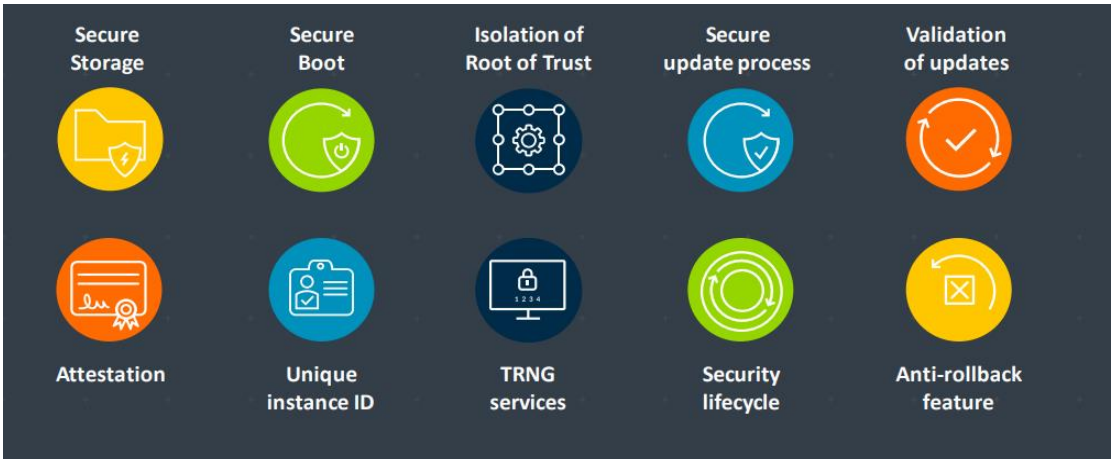
Οι συσκευές πρέπει να επιτρέπουν στις απομονωμένες υπηρεσίες να είναι λειτουργικές. Αυτό δεν σημαίνει απαραίτητα ότι στρέφουν σε κίνδυνο το σύστημα. Ενδέχεται παρόλα αυτά να απαιτείται η τήρηση κάποιων εμπιστευτικών δεδομένων. Σημαντικό είναι να λαμβάνεται υπόψη η αλληλεπίδραση τόσο εντός της συσκευής όσο και μεταξύ της συσκευής και του εξωτερικού κόσμου.

-Ασφαλής αποθήκευση

Προκειμένου να αποφευχθεί η αντιγραφή ή η αποκάλυψη ή η τροποποίηση ιδιωτικών δεδομένων εκτός της συσκευής, πρέπει να δεσμεύεται αποκλειστικά με αυτά. Η εμπιστευτικότητα και η ακεραιότητα αυτών των δεδομένων επιτυγχάνεται χρησιμοποιώντας κλειδιά, τα οποία πρέπει να συνδέονται με τη συσκευή.

-Κρυπτογραφικές / αξιόπιστες υπηρεσίες

Ένα μικρό σύνολο από αξιόπιστες υπηρεσίες και κρυπτογραφικές λειτουργίες αποτελεί υπαρξιακά στοιχεία μιας αξιόπιστης συσκευής. Για αυτό ως κρίσιμες λειτουργίες ορίστηκαν, ο κύκλος ζωής ασφαλείας, η απομόνωση, η ασφαλή αποθήκευση, η βεβαίωση, η ασφαλή εκκίνηση, η ασφαλή φόρτωση και η δέσμευση των δεδομένων.



Εικόνα 8: Τα 10 αντίμετρα της PSA

4.3 ΕΙΣΑΓΩΓΗ ΣΤΗ TPM ΒΑΣΗ

Η βάση αξιόπιστων υπολογιστών (TCB) συνδυάζει υλικό, λογισμικό και έλεγχο που λειτουργούν από κοινού με σκοπό να αποτελέσουν βάση για να επιβάλλουν πολιτική ασφαλείας.

Η Ομάδα Trusted Computing (TCG) θεωρεί πως τα ανοικτά, διαλειτουργικά και διεθνώς ελεγμένα πρότυπα είναι αυτά που καθορίζουν την αξιοπιστία των υπολογιστών και πως η ολοκληρωμένη προσέγγιση για να δημιουργηθούν αυτά τα πρότυπα είναι πιο αποτελεσματική. Το TCG εργάζεται στο πλαίσιο των διεθνών προτύπων και έχει σχέσεις συνεργασίας και ομάδας εργασίας με την IETF και τη μεικτή επιτροπή JTC1 του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC).

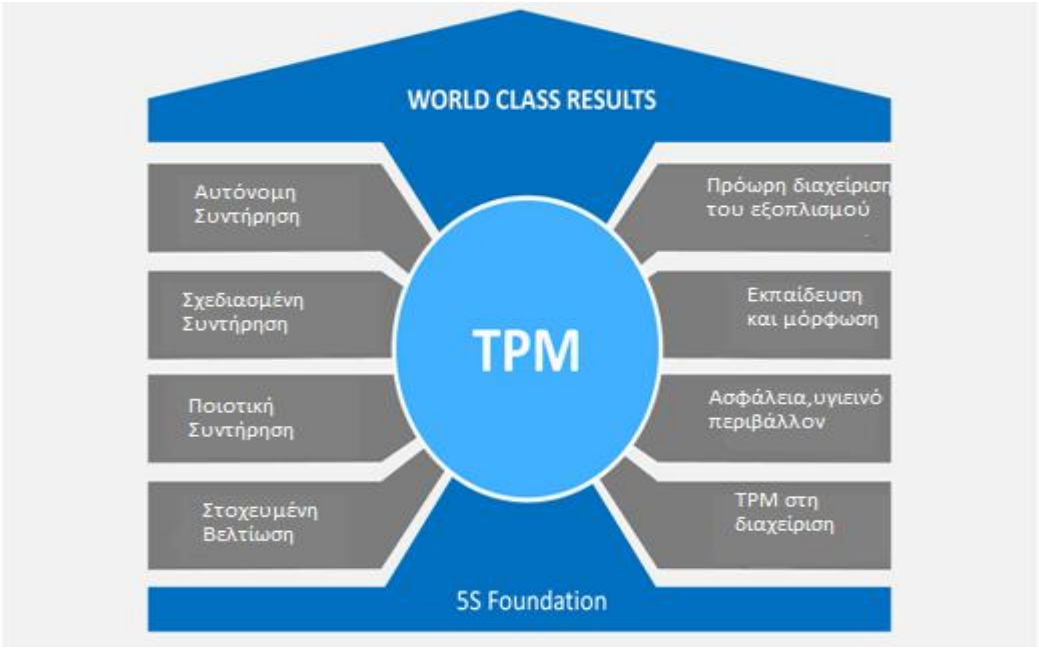
Ενώ, τα κλειστά πρότυπα εμποδίζουν τόσο τις υπάρχουσες όσο και τις αναδυόμενες αγορές. Επίσης, έχουν επιπτώσεις στην ασφάλεια της παγκόσμιας υποδομής ΤΠΕ και αποτελεί εμπόδιο στην τεχνολογική καινοτομία και την ανάπτυξη της βιομηχανίας.

Η TCG αναγνωρίζει τα διεθνή πρότυπα όπως αυτά έχουν καθοριστεί στον τομέα της ασφάλειας ΤΠ ως καταλληλότερη μέθοδο για να εξασφαλίσει την αποτελεσματικότητα, την λειτουργικότητα, τη υιοθέτηση και την αποδοχή από τους χρήστες. Επιπλέον, λαμβάνει υπόψη τις απαιτήσεις που καταγράφονται στην διεθνή αγορά και επικροτεί τη συμμετοχή της βιομηχανίας, του ακαδημαϊκού κόσμου και των κυβερνήσεων σε μια κοινή παγκόσμια διαδικασία ανάπτυξης προτύπων Trusted Computing.

Βασικός στόχος της TCG ήταν η ανάπτυξη μιας μονάδας Trusted Platform Module (TPM), ενός πυρήνα δηλαδή πνευματικής ιδιοκτησίας ή ενός ολοκληρωμένου κυκλώματος. Είναι αναγκαίο ακόμα να συμφωνεί με τις προδιαγραφές που υπέβαλε η Trusted Computing Group και η οποία επιτρέπει αξιόπιστες υπολογιστικές υπηρεσίες και χαρακτηριστικά. Επιπλέον, πρόσφατα κυκλοφόρησε την πρώτη έκδοση βάσει των προδιαγραφών πρωτοκόλλου της Trusted Network Connect για να εξουσιοδοτήσει τους πελάτες δικτύου με βάση τη διαμόρφωση υλικού, το BIOS, την έκδοση του πυρήνα αλλά και τις ενημερώσεις που έχουν εφαρμοστεί στο λειτουργικό σύστημα και το λογισμικό προστασίας από ιούς, κ.λπ. Το Πρόγραμμα Πιστοποίησης TCG αξιοποιεί τα πιστοποιημένα και αναγνωρισμένα πρότυπα αξιολόγησης της ασφάλειας και βασίζεται στην πιστοποίηση από εργαστήρια που λειτουργούν και εποπτεύονται από τα μέλη των εθνικών προγραμμάτων.

Ένας χρήστης συστήματος που έχει δυνατότητα TPM αποκτά πλήρη έλεγχο του λογισμικού και δεν εκτελείται στο σύστημα του ιδιοκτήτη. Σε κάποιες περιπτώσεις, ο χρήστης είτε μπορεί να επιλέξει να δώσει άδεια στον ιδιοκτήτη να διαμορφώσει το υλικό που έχει αγοράσει νόμιμα, είτε να περιορίσει τον ιδιοκτήτη από την πλήρη χρήση της ιδιοκτησίας του. Για αυτό αναπτύχθηκε η δυνατότητα ενός λειτουργικού συστήματος, το οποίο είτε να το έχει επιλέξει ο χρήστης, είτε να έχει προεγκατασταθεί στο υλικό πριν από την αγορά. Το λειτουργικό αυτό παρότι θα εμποδίζει τη φόρτωση μη υπογεγραμμένου ή χωρίς άδεια λογισμικού, θα πρέπει όλοι οι περιορισμοί αυτοί να ενισχυθούν από το λειτουργικό σύστημα και όχι από την τεχνολογία TCG. Το TPM, στην περίπτωση αυτή, παρέχει στο λειτουργικό σύστημα τη δυνατότητα να διασφαλίζει στο λογισμικό συγκεκριμένες διαμορφώσεις, κάτι το οποίο σημαίνει ότι οι "πειρατικές" εκδόσεις που έχουν σχεδιαστεί, για να παρακάμψουν αυτούς τους περιορισμούς, δεν θα λειτουργήσουν.

Το TPM σε συνδυασμό με τον φορτωτή εκκίνησης μπορεί να χρησιμοποιηθεί για να εξασφαλιστεί η λειτουργία μόνο εγκεκριμένων, από τον προμηθευτή, λειτουργικά συστήματα. Αυτό θα μπορούσε να αποτελέσει μία λύση, προκειμένου να περιοριστεί η εκτέλεση εναλλακτικών λειτουργικών συστημάτων.



Εικόνα 9:Τα συστατικά μέρη του TPM

Η αρχιτεκτονική TPM και η μορφή δεδομένων έχουν σχεδιαστεί για να επιτύχει την επιθυμητή λειτουργικότητα. Βασίζεται στην υψηλή ποιοτική συντήρηση, παράλληλα με υψηλή την αποδοτικότητα ως προς το κόστος, ώστε να είναι κατάλληλη για ενσωμάτωση σε εκατομμύρια υπολογιστές με ελάχιστο κόστος. Ακόμα, παρέχει βελτίωση μέσω της άμεσης διαχείρισης που γίνεται στον εξοπλισμό, έτσι ώστε να παρέχεται η λειτουργικότητα που επιθυμούν σε ένα υγιές και ασφαλές περιβάλλον. Αυτή η απόφαση για εξοικονόμηση κόστους, προκειμένου να μπορεί να διαχειριστεί όλες τις αποθηκευμένες πληροφορίες, δίνει την άδεια να χρησιμοποιεί μια ολοκληρωμένη ασύμμετρη κρυπτογράφηση. Επομένως, χρειάζεται να περιέχει μόνο έναν αλγόριθμο ασύμμετρης κρυπτογράφησης, χωρίς αυτό σημαίνει ότι το TPM δεν μπορεί να αποθηκεύσει τέτοια κλειδιά. Απλώς δεν εκτελεί κρυπτογραφία χρησιμοποιώντας αυτά.

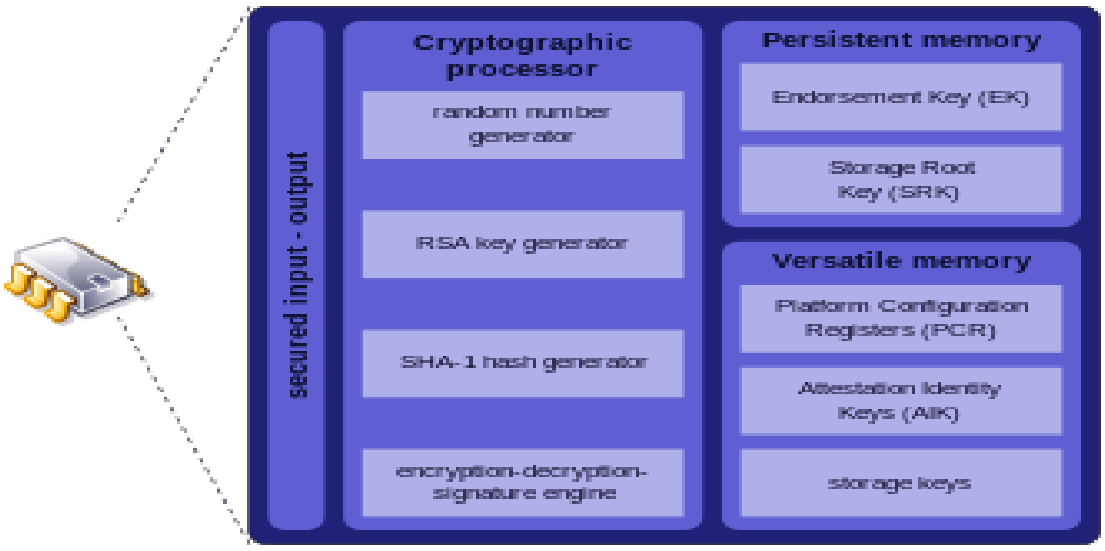
Παρόλο που συμβαίνει ένας συμμετρικός αλγόριθμος κρυπτογράφησης ενδείκνυται να είναι πιο κατάλληλος, διότι τα συμμετρικά κλειδιά σφραγίζονται και κυκλοφορούν προκειμένου να υπάρξει ένα αξιόπιστο λειτουργικό σύστημα. Υπάρχει βέβαια και το ενδεχόμενο της εισαγωγής ψευδών κλειδιών που ενώ μπορεί να φαίνεται άσχετο, τελικά είναι κρίσιμο, καθώς χωρίς αυτό, θα ήταν δυνατό να δημιουργηθεί ένα κλειδί που, ενώ δεν θα είχε την δυνατότητα να κυκλοφορεί σε

ολόκληρο το λειτουργικό σύστημα όπως τα συμμετρικά κλειδιά, αλλά θα είχε μια τιμή γνωστή στον εισβολέα. Οποιαδήποτε προσπάθεια ενός παρόχου να εκδώσει περιεχόμενο μέσω αυτού του ψευδούς κλειδιού, θα σημειωθεί ως παραβίαση.

Το TPM επιλύει αυτό το πρόβλημα μέσω μίας απόδειξης γνωστή ως "TPM Proof" , η οποίο εισάγεται σε κάθε δομή δεδομένων κρυπτογραφημένη και ελέγχεται για αντιστοίχιση με το πρωτότυπο αντίγραφο της απόδειξης TPM. Αυτό διασφαλίζει ότι τα ψευδή κλειδιά δεν μπορούν να εισαχθούν στο λειτουργικό σύστημα χωρίς έγκριση. Ουσιαστικά, αυτό συντελεί στη μετατροπή του ασύμμετρου κρυπτοσυστήματος σε συμμετρικό.

Ωστόσο, το TPM είναι εφοδιασμένο με μία γεννήτρια τυχαίων αριθμών όπου παράγει τυχαία δεδομένα και χρησιμοποιώντας επανειλημμένα διαδικασίες του κρυπτογραφικού κατακερματισμού, πιο συγκεκριμένα του αλγόριθμου κατακερματισμού SHA-1.

Βασικός του στόχος είναι η ανίχνευση και η πρόληψη οποιασδήποτε τροποποίησης συμβεί στα δεδομένα, η αναγνώριση των κλειδιών και η βελτίωση της αποτελεσματικότητας της διαδικασίας των εντολών. Το λογισμικό είναι υπεύθυνο για τον εντοπισμό των δεδομένων, το οποίο συνεπάγεται ότι υπάρχει και ένα τρίτο μέρος όπου επαληθεύει ότι το λογισμικό δεν έχει αλλάξει.



Εικόνα 10:Συστατικάμέρη TPM και η συσχέτιση με τη version 1.2

Τα προγράμματα υπολογιστών μπορούν να χρησιμοποιήσουν ένα TPM για τον έλεγχο ταυτότητας συσκευών υλικού, αφού κάθε τσιπ TPM έχει ένα μοναδικό και μυστικό κλειδί RSA το οποίο καταστρέφεται καθώς παράγεται. Η προσέγγιση της ασφάλειας προς το επίπεδο υλικού παρέχει μεγαλύτερη προστασία από μια λύση μόνο για το λογισμικό.

Το TPM μπορεί να παρακολουθεί και να αποκτά πρόσβαση στον κύριο δίαυλο του υπολογιστή. Κάτι τέτοιο, του επιτρέπει να παρακολουθεί αλλά και να αναφέρει την πορεία της κατάστασης διαμόρφωσης ολόκληρου του υπολογιστή. Πιο συγκεκριμένα, μπορεί να αναφέρει την πορεία από τη στιγμή της ενεργοποίησης μέχρι και ενδεχομένως την εκτέλεση των εφαρμογών σε ένα σύγχρονο λειτουργικό σύστημα. Όμως, η παρακολούθηση από μόνη της έχει περιορισμένες χρήσεις.

Επιπλέον, το TPM μπορεί να επιβεβαιώσει τη διαμόρφωση του υπολογιστή σε εξωτερικούς χρήστες. Είτε είναι ο ιδιοκτήτης μιας συσκευής που επιθυμεί να το διαχειριστεί εξ αποστάσεως, είτε είναι ο κατασκευαστής συσκευής που αφήνει μια συσκευή στα χέρια ενός χρήστη που ενδεχομένως να μην είναι αξιόπιστης. Τέλος, προκειμένου να υποστηρίξει τις απαιτήσεις διαθεσιμότητας και να αποφύγει την αποτυχία του εξοπλισμού, το TPM περιλαμβάνει υποδομή και πρωτόκολλα εντολών για τη μετακίνηση δεδομένων μεταξύ αξιόπιστων συσκευών και για χρήση τρίτων ως μεσάζοντες.

Κατά τη διάρκεια της δημιουργίας, τα δεδομένα μπορούν να χαρακτηριστούν είτε μεταναστευτικά είτε μη μεταναστευτικά, ανάλογα με το απαιτούμενο μοντέλο προστασίας.

Με λίγα λόγια, το TPM παρέχει τα εργαλεία στους σχεδιαστές του λειτουργικού συστήματος, ώστε να μπορούν προστατευθούν από τους εισβολείς με λογική πρόσβαση σε τμήματα χαμηλού επιπέδου του υπολογιστή, όπως για παράδειγμα εισβολείς που μπορούν να ανταλλάξουν σκληρό δίσκο.

4.3.1 TRUSTED COMPUTING ΚΑΙ ΠΑΡΟΧΗ ΑΣΦΑΛΕΙΑΣ

Το Trusted Computing είναι ένα σύνολο προτάσεων και ιδεών για μια αρχιτεκτονική PC που προσφέρει εγγυήσεις σχετικά με το λογισμικό εφαρμογών που εκτελεί και επιτρέπει στις εφαρμογές να επικοινωνούν με ασφάλεια με άλλες εφαρμογές και με διακομιστές. Τα μονοπάτια μεταξύ του υπολογιστή και των

περιφερειακών όπως το πληκτρολόγιο, το ποντίκι και η οθόνη είναι κρυπτογραφημένα. Τα κλειδιά κρυπτογράφησης είναι ενσωματωμένα στο υλικό και δεν είναι διαθέσιμα στον κάτοχο του υπολογιστή. Ο υπολογιστής τρέχει μόνο το λειτουργικό σύστημα αφού πρώτα επαληθεύσει την ταυτότητα και την ακεραιότητά του. Έπειτα το λειτουργικό σύστημα επικοινωνεί με τους απομακρυσμένους διακομιστές προκειμένου να παρέχει εγγυήσεις σχετικά με την ταυτότητα και την ακεραιότητα του λογισμικού εφαρμογών πριν το εκτελέσει.

Το TC απαιτεί υποστήριξη υλικού, για την ενεργοποίηση των κλειδιών κρυπτογράφησης υλικού, για την ασφαλή εκτέλεση και για να αποφύγει τυχόν παραβιάσεις. Κατά την εκκίνηση του ελέγχου, επαληθεύεται η τιμή κατακερματισμού του κώδικα του λειτουργικού συστήματος πριν από τη φόρτωση και τη λειτουργία του. Αυτό εξασφαλίζει τη κατάσταση του λειτουργικού συστήματος όπως αναμένεται. Αυτό με τη σειρά του μπορεί να ελέγξει το hash των προγραμμάτων εφαρμογής, για να ελέγξει την αξιοπιστία τους πριν τα εκτελέσει.

Τα κρυπτογραφικά κλειδιά με βάση το υλικό χρησιμοποιούνται για την εκτέλεση ασφαλών λειτουργιών. Κατά το χρόνο κατασκευής, δημιουργείται ένα ριζικό κρυπτογραφικό κλειδί και αποθηκεύεται μέσα στο υλικό. Αυτό το κλειδί δεν μεταβιβάζεται σε κανένα άλλο στοιχείο και το υλικό έχει σχεδιαστεί με τέτοιο τρόπο ώστε είναι εξαιρετικά δύσκολο να ανακτήσει το αποθηκευμένο κλειδί με οποιαδήποτε μέθοδο, ακόμη και από τον ιδιοκτήτη. Οι εφαρμογές μπορούν να μεταβιβάζουν δεδομένα κρυπτογραφημένα με αυτό το κλειδί για να αποκρυπτογραφηθούν από το υλικό, αλλά θα το κάνουν μόνο υπό ορισμένες αυστηρές συνθήκες. Αντιθέτως, τα αποκρυπτογραφημένα δεδομένα θα μεταβιβαστούν μόνο σε επικυρωμένες εφαρμογές και θα αποθηκευτούν στην ήδη υπάρχουσα μνήμη, καθιστώντας τα μη προσπελάσιμα σε άλλες εφαρμογές και λειτουργικά συστήματα.

Στην διαδικασία κρυπτογράφησης του δημόσιου κλειδιού που χρησιμοποιείται ευρέως, η δημιουργία των κλειδιών μπορεί να γίνει στον τοπικό υπολογιστή και ο δημιουργός έχει τον πλήρη έλεγχο του ποιος έχει πρόσβαση σε αυτήν. Πολλές φορές κάποιες μάρκες κρυπτογράφησης-αποκρυπτογράφησης, διαθέτουν ένα ιδιωτικό / δημόσιο κλειδί το οποίο όταν κατασκευάζεται ενσωματώνεται μόνιμα στο υλικό και οι κατασκευαστές υλικού με αυτό τον τρόπο έχουν την ευκαιρία να καταγράψουν το κλειδί χωρίς όμως να αφήνουν στοιχεία. Με αυτόν τον τρόπο, το κλειδί παρέχει πρόσβαση σε κρυπτογραφημένα δεδομένα και επαληθεύει την ταυτότητάς του.

Το υλικό που έχει τη δυνατότητα TC χρειάζεται κατά την κατασκευή του να υπάρχει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού, που ονομάζεται κλειδί επικύρωσης (EK). Το ιδιωτικό κλειδί συγκρατείται με ασφάλεια από το τσιπ και δεν απελευθερώνεται. Σε μια ιδανική περίπτωση, κατά την παραγωγική διαδικασία καταστρέφονται όλα τα αρχεία του ιδιωτικού κλειδιού. Το τσιπ είναι ανθεκτικό στις παραβιάσεις και η μνήμη αποτρέπει κάποιο άλλο λογισμικό το οποίο επιθυμεί ή τείνει να πάρει το ιδιωτικό κλειδί.

Οι αιτήσεις διασφαλίζονται σε ένα διακομιστή , αποστέλλοντάς του το δημόσιο κλειδί μαζί με το ψηφιακό αποτύπωμα της εφαρμογής. Οι διακομιστές θα πρέπει να γνωρίζουν το σύνολο των έγκυρων δημόσιων κλειδιών. Επίσης, ελέγχει ότι εμπιστεύονται τόσο το υλικό όσο και την εφαρμογή, πριν από την αποστολή του περιεχομένου.

Είναι επίσης σημαντικό οι κατασκευαστές υλικού και οι προγραμματιστές λογισμικού να είναι έμπιστα άτομα και ότι εφαρμόζουν σωστά τα αξιόπιστα πρότυπα των υπολογιστών. Η εσφαλμένη εφαρμογή τους , θα μπορούσε αφενός να αποκρύπτεται από τους χρήστες, με αποτέλεσμα την υπονόμευση της ακεραιότητας ολόκληρου του συστήματος, χωρίς οι χρήστες να γνωρίζουν το ελάττωμα.

Για να υπάρχει εμπιστοσύνη σε οτιδήποτε έχει εγκριθεί ή κρυπτογραφηθεί από μία πλατφόρμα TPM, ο τελικός χρήστης πρέπει να εμπιστευτεί την εταιρεία που σχεδίασε το τσιπ, τις εταιρείες που επιτρέπεται να δημιουργούν λογισμικό για το τσιπ και την ικανότητα αυτών να μην υπονομεύσουν την όλη διαδικασία.

4.4 ΕΙΣΑΓΩΓΗ ΣΤΗΝ KNOX ΤΕΧΝΟΛΟΓΙΑ

Το KNOX αποτελεί μια πλατφόρμα που παρέχει ασφάλεια σε εταιρείες και προστατεύει τις ιδιωτικές πληροφορίες τους από υποκλοπές. Μια νέα λύση βασισμένη σε Android είναι το Samsung KNOX το οποίο σχεδιάστηκε με κύριο μέλημα την ασφάλεια και την αντιμετώπιση της αντίληψης που έχει η πλατφόρμα ανοικτού κώδικα Android.

Υποστηρίζει ένα καινούριο πρόγραμμα που λέγεται BYOD (Bring Your Own Device). Δίνει τη δυνατότητα στους υπαλλήλους της εταιρείας να φέρνουν τις δικές του συσκευές στο χώρο της δουλειάς χωρίς φόβο και κίνδυνο. Προσφέρει μια εκτεταμένη λύση ασφάλειας που βασίζεται κατά κύριο λόγο σε συσκευές δεν

επιτρέπουν να γίνουν τροποποιήσεις μέσω του λειτουργικού και έχει ήδη εγκριθεί για χρήση στα δίκτυα του Υπουργείου Άμυνας των ΗΠΑ. Η πλειοψηφία των εταιρειών δεν έχει ακόμα τη δομή τέτοιων προγραμμάτων, αλλά καθώς η Samsung ήθελε να πρωτοπορήσει, προ εγκαθιστά το KNOX στις καινούριες συσκευές της και προωθεί τη χρήση του.

Η Samsung KNOX διατηρεί την πλήρη συμβατότητά της με το Android και το οικοσύστημα της Google, ενώ ταυτόχρονα βελτιώνει την ασφάλεια και την διαχείριση. Εκτός από την εξασφάλιση της πλατφόρμας, περιέχει το Samsung KNOX Container το οποίο παρέχει ένα ξεχωριστό περιβάλλον Android μέσα στην κινητή συσκευή, δομημένο με δική του αρχική οθόνη, εφαρμογές και λειτουργίες. Οι εφαρμογές και τα δεδομένα μέσα στο δοχείο είναι διαχωρισμένες από τις εφαρμογές εκτός του κοντέινερ, δηλαδή οι εφαρμογές που είναι εκτός του κοντέινερ δεν μπορούν να χρησιμοποιήσουν την επικοινωνία μέσω διαδικτύου Android (IPC). Ως IPC ορίζεται η επικοινωνία μεταξύ διαφόρων διαδικασιών και περιγράφει τον τρόπο με τον οποίο επικοινωνούν οι διάφοροι τύποι εξαρτημάτων ή τις μεθόδους όπου γίνεται η ανταλλαγή δεδομένων με εφαρμογές μέσα στο δοχείο.

Εικόνα 11: Samsung Knox

Οι εισβολείς δεν μπορούν να «κλέψουν» δεδομένα διότι το κιβώτιο KNOX είναι σχεδιασμένο με τέτοιο τρόπο ώστε να τα διαχωρίζει, να τα αποκρυπτογραφεί

και να τα προστατεύει. Αυτό αποτελεί λύση για τις επιχειρήσεις καθώς τους προσφέρει και άλλα εργαλεία για να διαχειρίζονται τις διάφορες ανάγκες ασφαλείας.

Το Samsung KNOX έχει ενσωματωμένες βασικές τεχνολογίες, αξιοποιώντας δυνατότητες σε επίπεδο υλικού, παρέχει βελτιωμένη ασφάλεια και προστασία στο λειτουργικό σύστημα και στις εφαρμογές. Επιπλέον, πέρα από τη δομή της ασφάλειας που αυτή παρέχει στις συσκευές, η Samsung KNOX λαμβάνει υπόψη τις ανάγκες και απαιτήσεις της κυβέρνησης των ΗΠΑ και του Υπουργείου Άμυνας, για τη συμμόρφωση με πρωτοβουλίες και πρότυπα για την ασφάλεια των φορητών συσκευών, για να μπορεί να χρησιμοποιηθεί σε κυβερνητικά και άλλα περιβάλλοντα επιχειρήσεων υψηλής σημασίας.

Επίσης, η Samsung KNOX διαθέτει μία από τις πιο ολοκληρωμένες δυνατότητες διαχείρισης συσκευών κινητής τηλεφωνίας . Η KNOX, σε συνδυασμό με τη μοναδική εξέλιξη της τεχνολογίας επιτρέπει στις επιχειρήσεις να υποστηρίζουν μοντέλα BYOD και Εταιρικής-Ευθύνης χωρίς να θέτουν σε κίνδυνο την εταιρική ασφάλεια ή την ιδιωτική ζωή των εργαζομένων. Από το κουτί, η Samsung KNOX παρέχεται με ένα σύνολο αρχείων ρυθμίσεων πολιτικής ασφαλείας σχεδιασμένα να ενισχύουν την βασική πλατφόρμα Android και να ικανοποιούν τις γενικές ανάγκες των επιχειρήσεων. Το KNOX προσφέρει διαχειριστικά API που επιτρέπουν την αντικατάσταση των προεπιλεγμένων SE για τα αρχεία πολιτικής Android με αυστηρότερα αρχεία πολιτικής ή συγκεκριμένα για την επιχείρηση. Αυτά τα νέα αρχεία πολιτικής μπορούν να ωθηθούν στη συσκευή.

Βασικά χαρακτηριστικά του KNOX περιλαμβάνουν Secure Boot, Trusted Boot, TrustZone με έδρα την αρχιτεκτονική μέτρησης ακεραιότητας Tima που ενσωματώνει λειτουργίες απορρήτου και ασφαλείας σε επίπεδο ενσωματωμένων συστημάτων, το οποίο λειτουργεί ως buffer (ρυθμιστής) μεταξύ του Kernel του Android OS και του υλικού επεξεργαστή του κινητού.

Το Secure Boot αποτρέπει τη φόρτωση μη εγκεκριμένων φορτωτών εκκίνησης και λειτουργικών συστημάτων κατά την εκκίνηση. Υλοποιείται από κάθε bootloader κρυπτογραφικά επαληθεύοντας την υπογραφή του επόμενου bootloader διαδοχικά, με τη χρήση μια αλυσίδα πιστοποιητικών με το root-of-trust να υπάρχει στο υλικό. Σε περίπτωση που η επαλήθευση αποτύχει σε κάποια βήμα της, η διαδικασία εκκίνησης τερματίζεται.

Ενώ η ασφαλής εκκίνηση είναι αποτελεσματική στην αποτροπή μη εξουσιοδοτημένων εκφορτωτών εκκίνησης, δεν είναι σε θέση να κάνει διάκριση

μεταξύ διαφορετικών εγκεκριμένων δυαδικών εκδόσεων. Για παράδειγμα, το Secure Boot δεν μπορεί να κάνει διάκριση μεταξύ ενός bootloader με γνωστή ευπάθεια σε αντίθεση με μια μεταγενέστερη ενημερωμένη έκδοση, καθώς και οι δύο εκδόσεις έχουν έγκυρες υπογραφές. Ωστόσο, το Trusted Boot εισήχθη για την επαλήθευση του ίδιου bootloader, του πυρήνα και της πλατφόρμας.

Το Trusted Boot αποτελεί δυνατότητα Knox Platform που αντιπροσωπεύει την κορυφαία προστασία εκκίνησης κινητών συσκευών της Samsung. Η αξιόπιστη εκκίνηση αναγνωρίζει και διακρίνει τους μη εξουσιοδοτημένους και τους ξεπερασμένους φορτωτές εκκίνησης πριν να θέσει σε κίνδυνο την κινητή συσκευή σας. Εάν πραγματοποιηθεί φόρτωση μη εξουσιοδοτημένων στοιχείων εκκίνησης, μια επιχείρηση μπορεί να εμπιστευτεί ότι φορτώνονται μόνο επικυρωμένα και τρέχοντα στοιχεία αφού ο Trusted Boot διαχωρίσει εξουσιοδοτημένους από μη εξουσιοδοτημένους φορτωτές εκκίνησης.

Οι μετρήσεις του bootloader καταγράφονται κατά την εκκίνηση της συσκευής σε ασφαλή μνήμη TrustZone. Κατά την εκτέλεση, οι εφαρμογές που λειτουργούν στο ασφαλές TrustZone μπορούν να χρησιμοποιήσουν τις μετρήσεις αυτές για να λάβουν κρίσιμες αποφάσεις για την ασφάλεια

Σε περίπτωση εντοπισμού μη εξουσιοδοτημένης ή μη ενημερωμένης έκδοση εξαρτήματος, έχει ρυθμιστεί μια ασφάλεια παραβίασης. Όταν ρυθμιστεί η ασφάλεια, οι ευαίσθητες εφαρμογές και τα δεδομένα εργασίας στο κοντέινερ Work κρυπτογραφούνται μόνιμα και δεν είναι προσβάσιμα, καθώς η ακεραιότητα της συσκευής δεν είναι πλέον εγγυημένη ή επικυρωμένη.

Ο χρήστης της συσκευής εξακολουθεί να μπορεί να εκκινήσει τη συσκευή και να ξεκινήσει προσωπικές εφαρμογές. Αυτή η δυνατότητα προάγει μια καλή ισορροπία μεταξύ των λειτουργιών των καταναλωτών, όπως κλήσεις smartphone και προσωπικές εφαρμογές και την απαίτηση προστασίας των εταιρικών δεδομένων.

Όλα αυτά τα πλεονεκτήματα καθιστούν την KNOX την ιδανική επιλογή για ρυθμισμένα και γενικά επιχειρηματικά περιβάλλοντα.

4.4.1 ΠΑΡΟΧΗ ΑΣΦΑΛΕΙΑΣ

Το KNOX αντιμετωπίζει την ασφάλεια χρησιμοποιώντας ένα ολοκληρωμένο περιβάλλον, που περιλαμβάνει τα υλικά Root of Trust , Secure Boot και Trusted Boot. Αποτελείται από ενισχύσεις ασφαλείας για Android (SE για Android), αρχιτεκτονική

μέτρησης ακεραιότητας με βάση TrustZone (Tima) και άλλες διάφορες υπηρεσίες που θα αναφερθούν παρακάτω. Η ανάλυση θα γίνει σύμφωνα με τη δομή της πλατφόρμας όπως παρουσιάζεται στην εικόνα παρακάτω.

- **ΔΟΜΗ ANDROID**

Η δομή ξεκινάει με ένα Workspace, ένα λογισμικό που απομονώνει τις επαγγελματικές εφαρμογές από τις αντίστοιχες προσωπικές και παρέχει βελτιωμένους ελέγχους πάνω από τα χαρακτηριστικά της συσκευής για την επιχείρησή από τους διαχειριστές IT.

SE for Android: Διαμοιράζει το λειτουργικό σύστημα σε τομείς ασφαλείας. Σε κάθε τομέα, οι εφαρμογές έχουν τα ελάχιστα δικαιώματα που χρειάζονται για να λειτουργήσουν. Αυτό περιλαμβάνει τη ζημιά που μπορεί να προκληθεί από κακόβουλες ή χρονοβόρες εφαρμογές, καθώς τα προβλήματα σε έναν τομέα δεν εξαπλώνονται σε άλλα. Όταν το SE για το Android ανιχνεύσει μη εξουσιοδοτημένη πρόσβαση, εμφανίζει ένα μήνυμα ειδοποίησης.

- **ΠΥΡΗΝΑΣ**

Η επαληθευμένη εφαρμογή εκκίνησης του Android βασίζεται στον στόχο ελέγχου της ακεραιότητας του στοιχείου DM-verity (Αρχή χαρτογράφησης Συσκευής). Device-mapper είναι ένα πλαίσιο πυρήνα το οποίο για την υλοποίηση εικονικών συσκευών μπλοκ. Ο DM-verity στοχεύει στον έλεγχο της ακεραιότητας του μπλοκ και στο να εγγυηθεί ότι ένας τόμος της συσκευής διατηρείται ακέραιος ενάντια στη διαφθορά ή τις κακόβουλες επιθέσεις.

Η πλατφόρμα KNOX ενισχύει περαιτέρω την ικανότητα κρυπτογράφησης της συσκευής που μέχρι τώρα πρόσφερε η πλατφόρμα Android. Εκτός από τον έλεγχο ταυτότητας μέσω κωδικού πρόσβασης, η ακεραιότητα του συστήματος όπως καθορίζεται από το Trusted Boot, επαληθεύεται επίσης πριν από την αποκρυπτογράφηση των δεδομένων. Αυτό προστατεύει όλα τα δεδομένα της συσκευής από μία απίθανη περίπτωση που το λειτουργικό σύστημα θα παραβιαστεί.

SE for Linux: Είναι μία μονάδα ασφαλείας που υποστηρίζει τις πολιτικές ασφαλείας του ελέγχου πρόσβασης. Το SE Linux είναι ένα σύνολο τροποποιήσεων που υπάρχουν στον πυρήνα και έχουν προστεθεί σε διάφορες διανομές. Η αρχιτεκτονική αυτή προσπαθεί να διαχωρίσει την επιβολή των αποφάσεων ασφαλείας από την ίδια την πολιτική ασφάλειας. Ένας πυρήνας Linux που ενσωματώνει το SE Linux

επιβάλλει πολιτικές ελέγχου πρόσβασης οι οποίες, εκτός από το να περιορίζουν προγράμματα χρηστών και διακομιστές συστημάτων, εμποδίζουν και την πρόσβαση σε αρχεία και πόρους του δικτύου. Ένα πρόβλημα σε οποιαδήποτε από αυτές τις περιοχές μπορεί να επιτρέψει σε ολόκληρο το σύστημα να συμβιβαστεί με αθέμιτες ενέργειες και λειτουργίες, με μοναδικό αποτέλεσμα τη ρήξη του συστήματος. Αντίθετα, η ασφάλεια ενός "τροποποιημένου" συστήματος, εκείνο δηλαδή που είναι βασισμένο σε έναν πυρήνα SE Linux εξαρτάται κυρίως από την ορθότητα του πυρήνα και την διαμόρφωσης της πολιτικής ασφαλείας που θα εφαρμοστεί.

- **HYPERVISOR (Συσκευή Παρακολούθησης)**

Προστασία πυρήνα σε πραγματικό χρόνο: Το RKP εκτελεί συνεχή, στοχευμένη παρακολούθηση του λειτουργικού συστήματος σε πραγματικό χρόνο, προκειμένου να αποφευχθεί η παραβίαση του πυρήνα. Το RKP παρακολουθεί τα κρίσιμα συμβάντα που συμβαίνουν στον πυρήνα, τα οποία στη συνέχεια επιθεωρούνται στο TrustZone. Εάν ένα συμβάν επηρεάζει την ακεραιότητα του πυρήνα του λειτουργικού συστήματος, το RKP είτε καταγράφει μια ειδοποίηση ότι υπάρχει υποψία παραβίασης είτε διακόπτει το συμβάν.

- **TRUSTZONE**

Η απομακρυσμένη βεβαίωση βασίζεται στην αξιόπιστη εκκίνηση και αποσκοπεί στην επαλήθευση της ακεραιότητας της πλατφόρμας. Η απομακρυσμένη βεβαίωση πραγματοποιείται από το σύστημα διαχείρισης της κινητής συσκευής (MDM) της επιχείρησης, συνήθως πριν από τη δημιουργία του χώρου εργασίας KNOX. Όταν ζητηθεί, η βεβαίωση ελέγχει τα δεδομένα που έχουν συγκεντρώσει, τα αξιόπιστα πακέτα και τα επιστρέφει πίσω εφόσον η διαδικασία ολοκληρωθεί.

Η προστασία του συστήματος που προσφέρει η SE για το Android βασίζεται στην διασφάλιση της ακεραιότητας του πυρήνα του λειτουργικού συστήματος . Αν ο ίδιος ο πυρήνας υποστεί βλάβη, ακόμα και από μια ίσως άγνωστη μελλοντική ευπάθεια, ο SE για τους μηχανισμούς ασφαλείας του Android είναι πιθανόν να απενεργοποιηθεί διότι δεν είναι πλέον αποτελεσματικός. Η αρχιτεκτονική μέτρησης της ακεραιότητας με βάση την TrustZone της Samsung (TIMA) αναπτύχθηκε για να λύσει αυτό το θέμα. Το TIMA KeyStore είναι μια υπηρεσία ασφάλειας που βασίζεται στην TrustZone και λειτουργεί με βάση το Trusted Boot. Το KeyStore παρέχει υπηρεσίες για τη δημιουργία και διατήρηση κρυπτογραφικών κλειδιών. Τα κλειδιά

κρυπτογραφούνται περαιτέρω μέσω ενός κλειδιού υλικού, μοναδικό για κάθε συσκευή, το οποίο μπορεί μόνο να αποκρυπτογραφηθεί από το υλικό μέσα από το TrustZone.

Όλες οι κρυπτογραφικές λειτουργίες εκτελούνται μόνο εντός του TrustZone και όταν υποστεί παραβίαση τότε απενεργοποιείται. Ένα βασικό χαρακτηριστικό του TIMA είναι ότι αν οι μετρήσεις Trusted Boot δεν αντιστοιχούν σε εξουσιοδοτημένες τιμές, η λειτουργία τερματίζεται, διασφαλίζοντας την προσωρινή προστασία των επιχειρησιακών δεδομένων.

Το TIMA επιτρέπει την αποθήκευση και ανάκτηση ψηφιακών πιστοποιητικών, καθώς και άλλες λειτουργίες που χρησιμοποιούν αυτά τα πιστοποιητικά, όπως κρυπτογράφηση, αποκρυπτογράφηση, υπογραφή, επαλήθευση με τρόπο παρόμοιο που συμβαίνει και με τις λειτουργίες μιας κάρτας SmartCard. Το TIMA αξιοποιεί τις λειτουργίες υλικού, συγκεκριμένα το TrustZone, για να διασφαλίσει ότι δεν μπορεί να προληφθεί ή να απενεργοποιηθεί από κακόβουλο λογισμικό. Το TIMA εκτελεί συνεχή παρακολούθηση του πυρήνα για να ανιχνεύσει εάν ο νόμιμος κώδικας πυρήνα και τα δεδομένα έχουν υποστεί τροποποίηση. Επιπλέον, η TIMA παρακολουθεί επίσης και το κλειδί SE, για να ανιχνεύει κακόβουλες επιθέσεις.

Μία λειτουργία με την οποία είναι εφοδιασμένο είναι το TIMA Client Certificate Manager. Είναι ένας τύπος ψηφιακού πιστοποιητικού που βασίζεται στην TrustZone και είναι κατασκευασμένη με βάση την αξιόπιστη εκκίνηση. Ένα βασικό χαρακτηριστικό και του TIMA CCM είναι ότι αν οι μετρήσεις Trusted Boot δεν ταιριάζουν με τις εξουσιοδοτημένες τιμές ολόκληρη η λειτουργία TIMA CCM τερματίζεται, διασφαλίζοντας την προστασία των δεδομένων.

- **BOOTLOADER**

Το Secure Boot είναι μια διαδικασία που έχει στόχο να μην επιτρέπει τη φόρτωση "μη εξουσιοδοτημένων" λειτουργικών συστημάτων και λογισμικού κατά την διαδικασία εκκίνησης. Τα λειτουργικά συστήματα και άλλα στοιχεία του συστήματος που έχουν εγκριθεί, θεωρούνται ως "εξουσιοδοτημένο" υλικολογισμικό.

Το Secure Boot είναι η πρώτη γραμμή άμυνας κατά των κακόβουλων επιθέσεων στις κινητές συσκευές KNOX και απαιτεί τον φορτωτή εκκίνησης της συσκευής, τον πυρήνα και το λογισμικό του συστήματος να υπογράφονται κρυπτογραφικά με ένα κλειδί που επαληθεύεται από το υλικό. Το κλειδί

χρησιμοποιείται για την υπογραφή των αρχείων εκκίνησης που εκτελούνται. Το δημόσιο μέρος του κλειδιού αποθηκεύεται στο υλικό κατά τη στιγμή της κατασκευής του και χρησιμοποιείται για να επαληθεύσει εάν έχει εγκριθεί κάθε στοιχείο εκκίνησης. Το Secure Boot υλοποιείται από κάθε bootloader ο οποίος ελέγχει και την υπογραφή του επόμενου bootloader στην ακολουθία, χρησιμοποιώντας μια αλυσίδα πιστοποιητικών. Η διαδικασία εκκίνησης τερματίζεται εάν παρατηρηθεί κάποιο πρόβλημα στην επαλήθευση σε οποιοδήποτε βήμα.

Εάν ο τελικός bootloader δεν καταφέρει να επαληθεύσει τον πυρήνα του Android, εκείνη την στιγμή υποδεικνύεται μία ύποπτη παραβίαση. Ακόμα κι αν ο πυρήνας του Android έχει επανέλθει στην αρχική του εργοστασιακή κατάσταση, η παραβίαση παραμένει. Ωστόσο, η διαδικασία εκκίνησης δεν σταματάει και ο τελικός bootloader συνεχίζει να εκκινεί τον πυρήνα του Android. Αυτή η διαδικασία διασφαλίζει ότι δεν έχει επηρεαστεί η κανονική λειτουργία της συσκευής. Το Secure Boot είναι αποτελεσματικό για την αποτροπή μη εξουσιοδοτημένων προγραμμάτων εκκίνησης.

Παρόλα αυτά, δεν είναι σε θέση να κάνει διάκριση μεταξύ ορισμένων διαφορετικών εκδόσεων εξουσιοδοτημένων αρχείων.

Η Samsung έχει επίσης δημιουργήσει ένα αξιόπιστο σύστημα επικύρωσης που μπορεί να ανιχνεύσει όταν επιχειρούνται απαγορευμένες ενέργειες σε συσκευές Samsung. Αυτά τα δεδομένα μας δίνουν ορατότητα στον τρόπο με τον οποίο χρησιμοποιούνται οι συσκευές μας και μπορούν να μας ειδοποιήσουν για νέες απειλές. Ο καθορισμός των μοντέλων χρήσης μας βοηθά να βελτιώσουμε τις πολιτικές ασφαλείας μας για την καλύτερη ασφάλεια και απόδοση.

Οι βελτιώσεις ασφαλείας για την υπηρεσία διαχείρισης Android παρέχουν έλεγχο επιπέδου διεπαφής προγραμματισμού εφαρμογών (API) του μηχανισμού πολιτικών SE για Android. Επιτρέπουν την προσαρμογή της προστασίας λογισμικού για κάθε οργανισμό επιτρέποντας τη δημιουργία δοχείων ασφαλείας για την απομόνωση των εφαρμογών και των δεδομένων τους.

Η πλατφόρμα KNOX ενισχύει ακόμα περισσότερο την ικανότητα κρυπτογράφησης που προσφέρει η πλατφόρμα Android. Εκτός από τον έλεγχο ταυτότητας με κωδικό πρόσβασης, η ακεραιότητα του συστήματος, όπως καθορίζεται από το Trusted Boot, επαληθεύεται επίσης πριν από την αποκρυπτογράφηση των δεδομένων.

Αυτή η δυνατότητα είναι διαθέσιμη μόνο εάν ο διαχειριστής της επιχείρησης ενεργοποιήσει την κρυπτογράφηση μέσω του MDM. Αυτό διασφαλίζει ότι όλα τα δεδομένα της συσκευής προστατεύονται σε μία αναπάντεχη παραβίαση του λειτουργικού συστήματος.

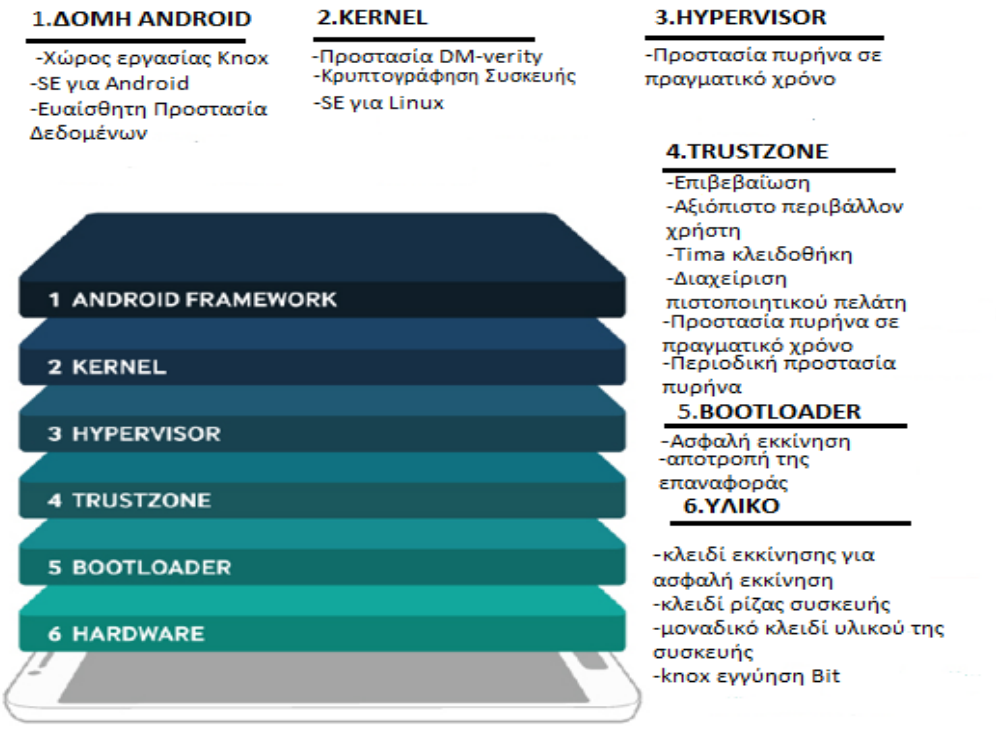
- **ΥΛΙΚΟ**

Τρία στοιχεία υλικού είναι τα θεμέλια του έμπιστου περιβάλλοντος της KNOX. Το βασικό κλειδί συσκευής είναι ένα ασύμμετρο κλειδί μοναδικό για τη συσκευή, το οποίο υπογράφεται από τη Samsung.

Αυτό το πιστοποιητικό βεβαιώνει ότι το βασικό κλειδί συσκευής είναι μοναδικό δημιούργημα της Samsung. Το KNOX χρησιμοποιεί επίσης και άλλα κλειδιά, τα οποία έχουν είσοδο μόνο στο TrustZone Secure World.

Ξεκινάει με το κλειδί ασφαλής εκκίνησης το οποίο ελέγχει ότι τα στοιχεία εκκίνησης στη συσκευή είναι εγκεκριμένα. Ακολουθεί το κλειδί υλικού της συσκευής που είναι ένα κρυπτογραφικό κλειδί το οποίο και αυτό είναι μοναδικό για κάθε συσκευή. Το συγκεκριμένο κλειδί μπορεί και κρυπτογραφεί και αποκρυπτογραφεί δεδομένα αλλά και να κρυπτογραφεί άλλα κρυπτογραφικά κλειδιά της συσκευής.

Επίσης υπάρχει και το κλειδί της ρίζας συσκευής όπου είναι και αυτός ένας άλλος τύπος κρυπτογραφικού κλειδιού, μοναδικό και αυτό για κάθε συσκευή. Αναγνωρίζει τη συσκευή και αποδεικνύει ότι είναι κατασκευασμένη από τη Samsung.



Εικόνα 12: Τα επίπεδα της πλατφόρμας του Knox

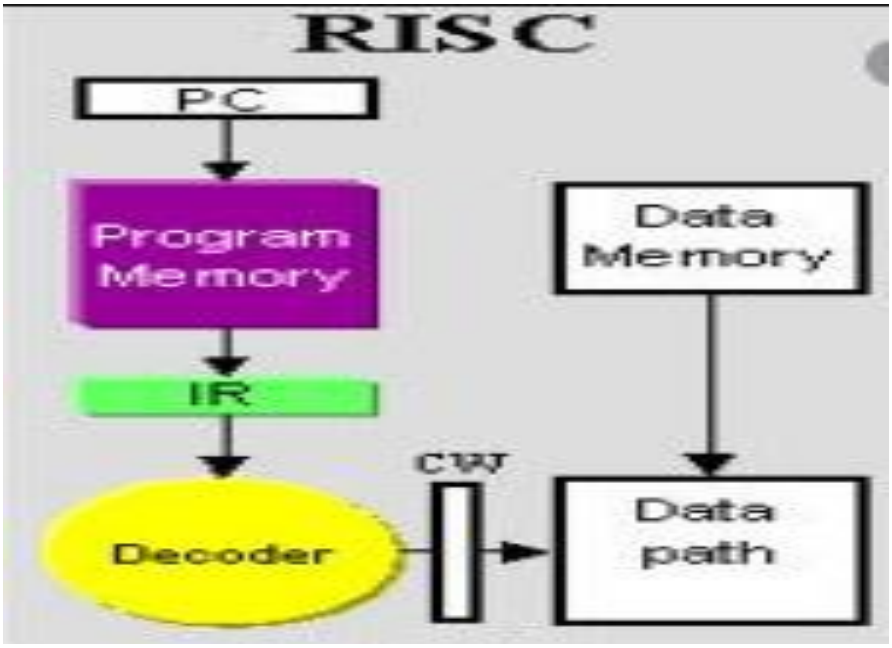
4.5 ΕΙΣΑΓΩΓΗ ΣΤΗ RISC-V ΤΕΝΟΛΟΓΙΑ

Ο επεξεργαστής RISC (Reduced Instruction Set Computer) αποτελεί μία μονάδα αριθμητικής-λογικής υπολογιστή που χρησιμοποιεί περιορισμένο σύνολο εντολών. Τονίζει τις οδηγίες που χρειάζονται πιο συχνά να ληφθούν υπόψη και τις βελτιώνει με σκοπό την ταχύτερη δυνατή εκτέλεση. Το λογισμικό που χρησιμοποιούν οι επεξεργαστές RISC έχει περισσότερες λειτουργίες να διαχειριστεί σε σύγκριση με τους παραδοσιακούς επεξεργαστές CISC (Complex Instruction Set Computer). Όμως, έχουν βασικά πλεονεκτήματα σε εφαρμογές, όπως η ταχύτερη εκτέλεση εντολών, η δημιουργία σταθμών εργασίας γραφικών, η παράλληλη επεξεργασία συστημάτων και είναι λιγότερο δαπανηρές για το σχεδιασμό, τη δοκιμή και την κατασκευή. Τέλος, άρχισαν να χρησιμοποιούνται σε προσωπικούς υπολογιστές σε σχέση με τους επεξεργαστές CISC που είχαν χρησιμοποιηθεί από την εισαγωγή του μικροεπεξεργαστή.

Το RISC-V είναι ένα πρότυπο ISA[8] ανοιχτού κώδικα και χωρίς δικαιώματα που βασίζεται στην αρχτεκτονική του RISC. Όμως, χρειάζονται περισσότερες

[8] ISA: είναι ένας παρωχημένος τύπος διαύλου ηλεκτρονικών υπολογιστών για την προσθήκη καρτών επέκτασης.

οδηγίες ανά πρόγραμμα υπολογιστή, για αυτό υπάρχουν ήδη μερικοί κατασκευαστές που εφαρμόζουν το ISA στους επεξεργαστές τους. Υπάρχουν πολλές ποικιλίες προσιτών πινάκων ανάπτυξης όπου χρησιμοποιούν έναν τέτοιο επεξεργαστή.



Εικόνα 13: Η Δομή του RISC-V

Κύρια χαρακτηριστικά του RISC-V αποδεικνύουν τόσο τη λειτουργικότητα όσο και την αποτελεσματικότητα σε σχέση με άλλους συμβατούς επεξεργαστές.

- **Περιορισμένο σύνολο απλών οδηγιών**.

Στόχος είναι να δημιουργηθεί ένα σύνολο εντολών με οδηγίες, ώστε να εκτελούνται γρήγορα και οι περισσότερες από τις οδηγίες RISC εκτελούνται σε ένα μόνο κύκλο.

-Αρχιτεκτονική φόρτωσης και αποθήκευσης.

Μόνο οι οδηγίες LOAD και STORE αναφέρουν δεδομένα στη μνήμη ενώ όλες οι άλλες λειτουργούν μόνο με καταχωρητές. Χρειάζονται μόνο λίγες οδηγίες για να αποκτηθεί πρόσβαση στη μνήμη και περισσότεροι από έναν κύκλους για την εκτέλεση.

-Οδηγίες με λίγους τρόπους αντιμετώπισης.

Συνήθως οι πιο εύχρηστοι τρόποι είναι η άμεση ή έμμεση εγγραφή και η μετατόπιση.

-Οδηγίες με σταθερό μήκος και ομοιόμορφη μορφή.

Αυτό καθιστά τη φόρτωση και την αποκωδικοποίηση των οδηγιών απλή και γρήγορη. Δεν χρειάζεται να είναι γνωστή η διάρκεια μιας εντολής για να ξεκινήσει η αποκωδικοποίηση του ακόλουθου ενώ τα πεδία των διευθύνσεων βρίσκονται στην ίδια θέση για όλες τις οδηγίες.

-Διατίθεται μεγάλος αριθμός μητρώων.

Οι μεταβλητές και τα αποτελέσματα μπορούν να αποθηκευτούν σε καταχωρητές. Όπως και δεν χρειάζονται επαναλαμβανόμενα φορτία και αποθήκες από και προς τη μνήμη. Όλες οι μεταβλητές των διαδικασιών και οι παράμετροι που έχουν οριστεί, να αποθηκεύονται σε μητρώα.

-Παρέχει ένα νέο επίπεδο ελευθερίας λογισμικού και υλικού στην αρχιτεκτονική με έναν ανοιχτό επεκτάσιμο τρόπο.

-Το Open ISA παρέχει ευκολότερη υποστήριξη από ένα ευρύ φάσμα λειτουργικών συστημάτων, προμηθευτών λογισμικού και προγραμματιστών εργαλείων.

-Η ανοιχτή πηγή υλικού, το RISC-V δεν βασίζεται σε έναν μόνο προμηθευτή - προσφέρει πολλούς προμηθευτές, επομένως, υποστηρίζει απεριόριστες δυνατότητες για μελλοντική ανάπτυξη.

-Κανένα άλλο ISA δεν αρχειοθετείται όπως το RISC-V ISA, επιτρέποντας την επέκταση της αρχιτεκτονικής από τους χρήστες χωρίς να σπάσει τις υπάρχουσες επεκτάσεις ή να προκαλέσει κατακερματισμό λογισμικού.

Οι αρχιτεκτονικές RISC έχουν πολλά πλεονεκτήματα. Ωστόσο, δεν υπάρχει μια οριστική απάντηση, για το αν είναι ο καταλληλότερος επεξεργαστής. Έχουν πραγματοποιηθεί πολλές συγκρίσεις όσον αφορά την απόδοση και έχουν δείξει ότι τα προγράμματα αναφοράς τρέχουν πιο γρήγορα και τα αποτελέσματα είναι πιο εμφανή σε επεξεργαστές RISC παρά σε επεξεργαστές CISC. Βέβαια είναι δύσκολο να προσδιοριστεί ποια είναι η προϋπόθεση εκείνη που έχει συντελέσει ώστε ο επεξεργαστή να εμφανίζει υψηλότερη απόδοση. Δεν σταμάτησαν ωστόσο να υπάρχουν και αρνητές σε αυτό το εγχείρημα. Οι υποστηρικτές της CISC θεωρούν ότι η υψηλότερη ταχύτητα δεν είναι αποτέλεσμα τόσο των τυπικών χαρακτηριστικών που είναι εφοδιασμένο το πρότυπο RISC-V, αλλά όσο της τεχνολογίας που διαθέτει και της χρήσης μεταγλωττιστών. Για να επιτευχθεί αυτό χρειάστηκαν επεξεργαστές με μεγαλύτερη απαίτηση μνήμης σε σύγκριση με τα παρόμοιους επεξεργαστές που χρειάστηκαν για μια αρχιτεκτονική CISC. Ωστόσο, όσο λειτουργικό και αν

παρουσιάζεται αυτό το πρότυπο της RISC-V, παρακάτω φαίνονται τόσο τα πλεονεκτήματα όσο και τα μειονεκτήματα αυτού του προτύπου.

Πλεονεκτήματα:

- Μεγαλύτερη απόδοση εξαιτίας του απλοποιημένου συνόλου οδηγιών που εμφανίζει.
- Εύκολος σχεδιασμός σε σύγκριση με το CISC.
- Είναι λιγότερο ακριβό.

Μειονεκτήματα:

-Η απόδοση του επεξεργαστή θα εξαρτηθεί από τον κώδικα που θα εκτελεστεί.
-Οι επεξεργαστές RISC απαιτούν πολύ γρήγορα συστήματα μνήμης για την τροφοδοσία διαφορετικών οδηγιών. Αυτό απαιτεί μια μεγάλη μνήμη cache.

4.5.1 ΠΑΡΟΧΗ ΑΣΦΑΛΕΙΑΣ

Σύμφωνα με τα δεδομένα από προβλέψεις που έχουν γίνει στην, θα υπάρχουν περισσότερα από 22 δισεκατομμύρια συνδεδεμένες συσκευές Internet of Things (IoT) στον κόσμο έως το 2024. Όμως, λόγω της ραγδαίας ανάπτυξης και εξέλιξης του IoT έχουν προκληθεί ζητήματα γύρω από κινδύνους για την ασφάλεια. Η ολοκλήρωση της ασφάλειας του συστήματος IoT έχει γίνει όλο και πιο περίπλοκη και η ασφάλεια έχει γίνει ένα σοβαρό ζήτημα που απασχολεί όλες τις βιομηχανίες. Για τις έξυπνες συσκευές, παρόλο που έχουν σχεδιαστεί και χρησιμοποιηθεί γενικά μέτρα για την ασφάλεια, τα οποία βασίζονται στον μηχανισμό απομόνωσης, συνεχίζουν να υφίστανται στον έλεγχο ταυτότητας της ασφάλειας. Βασικό συστατικό των συσκευών IoT, αποτελεί η ασφάλεια του μικροεπεξεργαστή, η οποία είναι ιδιαίτερα σημαντική.

Γι’ αυτό, οι παράγοντες ασφαλείας που πρέπει να ληφθούν υπόψη κατά τη διαδικασία της σχεδίαση ενός chip, είναι τα τέσσερα στοιχεία ασφαλείας της πλατφόρμας SoC:

- Το Αξιόπιστο περιβάλλον εκτέλεσης (TEE): Αναγκαστική απομόνωση κώδικα, δεδομένων και αποθηκευμένων πληροφοριών μέσω υλικού.

- Το Root of Trust : αποτελεί μοναδικό αναγνωριστικό και πιστοποιητικό καθώς επίσης παρέχει μια ασφαλή αποθήκευση ιδιωτικών κλειδιών.

- Η Ασφαλής εκκίνηση: δεν επιτρέπει την εκκίνηση σε κάποιο μη εξουσιοδοτημένο κώδικα να κάνει έλεγχο ταυτότητας.

- Τα Εργαλεία: χρειάζονται οι μηχανικοί να έχουν εργαλεία και διαδικασίες που να είναι διαθέσιμα και εύκολα στην ενσωμάτωση.

Το σύστημα ή το λογισμικό είναι αυτά που καθορίζουν τις ευπάθειες ασφαλείας στα ηλεκτρονικά συστήματα. Τόσο οι αρχιτεκτονικές Arm όσο και RISC-V βασίζονται στο μηχανισμό απομόνωσης. Όταν η Arm πραγματοποιεί ασφάλεια υλικού, οι δύο τομείς είναι κωδικοποιημένοι στο υλικό, ενώ το RISC-V είναι ένας τομέας που καθορίζεται από το λογισμικό. Όσον αφορά το λογισμικό, το Armv8-A χρησιμοποιεί το μοντέλο λογισμικού OP-TEE. Το Armv8-M χρησιμοποιεί το μοντέλο λογισμικού PSA, ενώ το RISC-V χρησιμοποιεί το μοντέλο λογισμικού ασφαλείας RISC-V MultiZone το οποίο είναι μικρό και επομένως ταχύτερο.

Αυτή η έκθεση ανάλυσης χωρίζει τα τσιπ RISC-V σε τέσσερις κατηγορίες: τα υψηλής απόδοσης SoC’s, τα οικονομικά αποδοτικά SoC’s, τα βασικά SoC’s και τα FPGA’s. Μεταξύ αυτών, η περισσότερο αναπτυσσόμενη κατηγορία είναι η βασική SoC. Κάποιες από τις μεγαλύτερες αποστολές εφαρμογών IoT είναι οι έξυπνες συσκευές δικτύου, όπως οι έξυπνοι μετρητές, οι μετρητές νερού και οι μετρητές αερίου, οι οποίες είναι και μερικές από τις κύριες αγορές.

Οι υλοποιήσεις του επεξεργαστή περιλαμβάνουν λειτουργίες που στοχεύουν στην βελτιστοποίηση της απόδοσης και της ισχύος. Η πολυπλοκότητα όμως αυξάνει τον κίνδυνο απώλειας όχι μόνο των λειτουργικών σφαλμάτων αλλά και των ευπαθειών ασφαλείας.

Παρόλο που κύριος στόχος είναι η διατήρηση της ασφάλειας, οι εισβολείς γίνονται πιο καταστροφικοί, με αποτέλεσμα να δημιουργούνται τεράστιες προκλήσεις στην ασφάλεια του δικτύου. Ανεξάρτητα από τις ευπάθειες και τους κινδύνους που έχουν αναλυθεί παραπάνω, έχουν ανακαλυφθεί πολλές ακόμη ευπάθειες τόσο σε επεξεργαστές προηγμένης εξέλιξης όσο και σε επεξεργαστές χαμηλού επιπέδου. Οι επιθέσεις ενδέχεται να παραβιάσουν ασφαλή τμήματα και να επιτρέψουν σε κακόβουλες εφαρμογές να αποκτήσουν πρόσβαση σε εμπιστευτικά δεδομένα ή ακόμη και να αναλάβουν τον έλεγχο του συστήματος. Αξίζει να σημειωθεί ότι σε αντίθεση με το λογισμικό, τα προβλήματα του υλικού δεν επιλύονται εύκολα μόνο με ενημερώσεις. Για να αντιμετωπιστεί ένα πρόβλημα που μπορεί να υπάρχει στο υλικό, ενδέχεται να προκαλέσει την υποβάθμιση της απόδοσής του.

Ένας λιγότερο πιθανός κίνδυνος, αλλά με πολύ μεγαλύτερη σημασία είναι η παρουσία κακόβουλου λογισμικού στον πυρήνα RISC-V. Κακόβουλο λογισμικό μπορεί να θεωρηθεί ένα υλικό Trojan, που αποτελεί μια λογική συνάρτηση η οποία έχει σχεδιαστεί σκόπιμα και ενεργοποιείται σε πολύ σπάνιες περιπτώσεις. Οι SoC που χρησιμοποιούν πυρήνες RISC-V ανοιχτού κώδικα ή τρίτου μέρους δεν θα πρέπει πλέον να αγνοούν αυτόν τον κίνδυνο. Η εισβολή αυτού του κακόβουλου λογισμικού θα έχει τεράστιο αντίκτυπο στη βιομηχανική παραγωγή αλλά και στην καθημερινή ζωή των ανθρώπων.

Γι' αυτό, η ασφάλεια έγινε ένα σημαντικό θέμα στην κοινότητα RISC-V και έχουν οριστεί ορισμένοι μηχανισμοί προκειμένου να γίνονται οι απαραίτητοι έλεγχοι, όπως:

-Ασφαλής εκκίνηση

Η ασφαλής εκκίνηση είναι ένας τρόπος για να επαληθεύσουν την ακεραιότητα των λειτουργιών και των ελέγχων ακεραιότητας κάθε σταδίου της διαδικασίας εκκίνησης. Σε στάδιο της χρειάζεται να επαναλάβει την ακεραιότητα του επόμενου σταδίου. Η ασφαλής εκκίνηση περιγράφεται ως προδιαγραφή Unieded Extensible Firmware Interface (UEFI) από την έκδοση 2. Επιβεβαιώνει την ακεραιότητα κάθε σταδίου της διαδικασίας εκκίνησης με τον υπολογισμό ενός κατακερματισμού και τη σύγκριση του αποτελέσματος με κρυπτογραφική υπογραφή. Κατά τη διάρκεια της εκκίνησης απαιτείται μια προσβάσιμη βάση δεδομένων αξιόπιστων δημόσιων κλειδιών, έτσι ώστε η υπογραφή να μπορεί να επαληθευτεί. Κατά τη διαδικασία αυτή, εάν αποτύχει ο έλεγχος της ακεραιότητας, η εκκίνηση ακυρώνεται. Εάν επιτευχθεί, το σύστημα αναμένεται να εκτελείται σε αξιόπιστη κατάσταση. Στην κοινότητα ασφαλείας, αυτός ο προσδιορισμός της ασφαλούς εκκίνησης, είναι γενικότερα αποδεκτός.

-Έλεγχος ταυτότητας της ψηφιακής υπογραφής

Ο έλεγχος ταυτότητας βάσει ψηφιακής υπογραφής αποτελεί πλέον γνωστή τεχνική, που προκύπτει από την κρυπτογράφηση δημόσιου κλειδιού. Χρησιμοποιείται στα περισσότερα προγράμματα περιήγησης ιστού (για SSL)[9]. Επειδή μαθηματικά προβλήματα είναι δύσκολο να επιλυθούν από χρήστες χωρίς γνώση, αποτελούν βάση

[9]SSL (Secure Sockets Layer): πρωτόκολλο που αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο.

για την προστασία δημόσιων κρυπτογραφικών συστημάτων. Το πιο δημοφιλές πρόγραμμα υπογραφής που χρησιμοποιεί ελλειπτικές καμπύλες ονομάζεται Αλγόριθμος Ελλειπτικής Καμπύλης Ψηφιακή Υπογραφή (ECDSA), το πιο δημοφιλές σχήμα κρυπτογράφησης ονομάζεται Σχέδιο Ολοκληρωμένης Κρυπτογράφησης Ελλειπτικής Καμπύλης (ECIES) και η πιο δημοφιλής μέθοδος βασικής συμφωνίας ονομάζεται Ελλειπτική καμπύλη Diffie-Hellman (ECDH).

-Φυσική ανεξάρτητη λειτουργία (PUF)

Οι Φυσικές Ανεξάρτητες Λειτουργίες εξάγουν μυστικά κλειδιά μόνο όταν είναι ενεργοποιημένο το chip, μέσω κάποιων παραλλαγών στους ημιαγωγούς. Η πρώτη αποδεδειγμένη χρήση των κλειδιών που δημιουργήθηκαν από PUF ήταν στον επεξεργαστή AEGIS. Το PUF χρησιμοποιήθηκε για τη δημιουργία ενός συμμετρικού κλειδιού που μοιράστηκε με τον χρήστη μέσω ενός κρυπτογραφικού πρωτοκόλλου. Για αλγόριθμους δημοσίου κλειδιού, το PUF μπορεί να χρησιμοποιηθεί για τη δημιουργία μίας τυχαίας γεννήτριας δημοσίων ή ιδιωτικών κλειδιών μέσα σε έναν ασφαλή επεξεργαστή.

Το ασφαλές SoC βασίζεται στο lowRISC ως βασικό επεξεργαστή. Το LowRISC είναι ένας επεξεργαστής ανοιχτού κώδικα που εφαρμόζει το ανοιχτό RISC-V Instruction Set Architecture (ISA). Αυτό είναι εξοπλισμένο με λειτουργίες ασφαλείας, όπως η ασφαλής εκκίνηση, η κρυπτογράφηση, ο έλεγχος ταυτότητας της μνήμης και η διαχείριση κλειδιών. Στην πράξη, ένα ασφαλές SoC πρέπει να είναι ανθεκτικό έναντι σε επιθέσεις τόσο στο υλικό όσο και στο λογισμικό. Επομένως, το ανεπτυγμένο ασφαλές RISC-V SoC εφαρμόζει διάφορες δυνατότητες για την προστασία από γνωστές επιθέσεις τόσο στο υλικό όσο και στο λογισμικό του υπολογιστικού συστήματος. Οι δυνατότητες περιλαμβάνουν:
•Key Management Unit, δημιουργία και διανομή των κλειδιών στα διάφορα μπλοκ ασφαλείας, όπως Code Authentication Unit (CAU), Secure Debug και Memory Protection Unit.

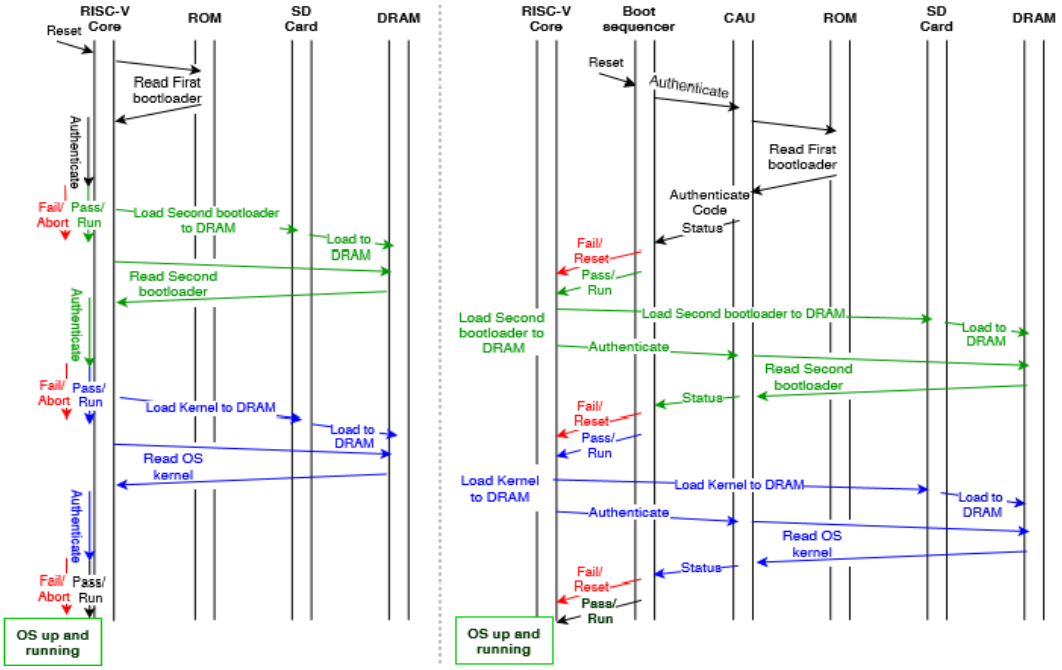
•Μονάδα ελέγχου της ταυτότητας του κώδικα για την προστασία από επιθέσεις, όπως η επίθεση εισβολής εικόνας. Η ασφαλής εκκίνηση υλοποιείται χρησιμοποιώντας το Code Authentication Unit (CAU).

•Ασφαλής εντοπισμός σφαλμάτων για προστασία από διάφορες απειλές υλικού, όπως η εξαγωγή κλειδιού, ο παράνομος εντοπισμός σφαλμάτων και η διερεύνηση και επιθέσεις καναλιού (SCA).

•Το αξιόπιστο περιβάλλον εκτέλεσης (TEE), το οποίο εγγυάται ένα απομονωμένο περιβάλλον εκτέλεσης για την αξιόπιστη εφαρμογή. Αυτή η δυνατότητα είναι απαραίτητη για την προστασία από επιθέσεις όπως η εκμετάλλευση λογισμικού και η κλιμάκωση των προνομίων.

•Η αξιόπιστη μνήμη Off-Chip η οποία αποτελεί βασικό χαρακτηριστικό που προστατεύει από τις επιθέσεις "πλάγιου καναλιού"(SCA) και την ανίχνευση και την εξαγωγή κλειδιών από την κύρια μνήμη. Επιπλέον, χρησιμοποιείται από το TEE με σκοπό να φορτώνει και να εκτελεί αξιόπιστες εφαρμογές, προστατεύοντας έτσι τον κώδικα και τα δεδομένα των εφαρμογών που εκτελούνται.

Έχει παρουσιαστεί ένα ασφαλές πλαίσιο εκκίνησης με εφαρμογή στο ελαφρύ SoC RISC-V. Το πλαίσιο χρησιμοποιεί βελτιστοποιημένο αλγόριθμο ελλειπτικής καμπύλης ψηφιακής υπογραφής (ECDSA), αλγόριθμο κατακερματισμού Secure Hash Algorithm 3 (SHA3) και την λειτουργία Physically Unclonable Function (PUF) Παρουσιάζεται λεπτομερής ανάλυση της απόδοσης και της ασφάλειας για την πλατφόρμα.



Εικόνα 14: Η Ασφαλής εκκίνηση του επεξεργαστή RISC-V

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια και η εμπιστοσύνη σε περιβάλλοντα κινητού αλλά και υπολογιστικά περιβάλλοντα, είναι κρίσιμοι παράμετροι για την υιοθέτηση διαδικασιών από τους χρήστες κινητών και υπολογιστικών συσκευών με σκοπό την εξάλειψη οποιονδήποτε απειλών. Οι απειλές είναι ένα σύνθετο θέμα που έρχονται συχνά αντιμέτωπα όλα τα κινητά και υπολογιστικά περιβάλλοντα όπως για παράδειγμα, το κακόβουλο και ανεπιθύμητο λογισμικό, το οποίο μπορεί να θέσει σε κίνδυνο την εμπιστευτικότητα αλλά και την ακεραιότητα διάφορων ευαίσθητων προσωπικών δεδομένων ή κρίσιμων πληροφοριών που διατηρεί ένας χρήστης. Η ευαισθητοποίηση σε ζητήματα ασφάλειας των συμμετεχόντων και η ανάλυση της επικινδυνότητας όλων των προβλεπόμενων διαδικασιών σε συνδυασμό με την ορθή χρήση τους, αποτελούν ουσιαστική προϋπόθεση στην αποτροπή οποιασδήποτε προσπάθειας παραβίασης των προβλεπόμενων λειτουργιών.

Όσον αφορά το Trusted Computing και σύμφωνα με αυτά που αναφέρθηκαν παραπάνω, κυριότερος στόχος των αξιόπιστων υπολογιστών είναι η παροχή στοιχείων που μπορεί να χρησιμοποιηθούν για την παροχή εγγυήσεων σε χρήστες επιτραπέζιων υπολογιστών αλλά και κινητών, σχετικά με την ακεραιότητα των λειτουργικών τους περιβαλλόντων. Αυτό μπορεί να επιτευχθεί με την παροχή επιπλέον δυνατοτήτων για το τοπικό λειτουργικό σύστημα, αλλά και παροχή εφαρμογών προκειμένου να ελεγχθεί εάν εκτελούνται με το προγραμματισμένο τρόπο που έχει θεσπίσει η Trusted Computing Base. Η ιδέα μιας τέτοιας πλατφόρμας υπολογιστών ως μια «αξιόπιστη βάση υπολογιστών» και τα υπόλοιπα δεν είναι κάτι καινούριο. Πλέον, υπάρχουν αυξανόμενες αποδείξεις ότι είναι πιο αναγκαίο, όχι μόνο στους υψηλούς τομείς διασφάλισης όπου η ιδέα του TCB ήταν διαδεδομένη, αλλά και σε καθημερινά συστήματα που απασχολούνται συνεχώς οι χρήστες.

Ανησυχίες για την ασφάλεια και προσπάθεια δημιουργίας αξιόπιστων περιβαλλόντων εκτέλεσης έχουν κεντρίσει το ενδιαφέρον για σχεδιασμό διαφόρων αρχιτεκτονικών. Μπορεί ακόμη να μην έχει σχεδιαστεί μία ισχυρή αρχιτεκτονική, αλλά αξιόπιστες αρχιτεκτονικές μπορούν να βοηθήσουν, συμβάλλοντας η καθεμία ξεχωριστά, προκειμένου να βοηθήσουν όπου αυτό απαιτείται.

Αρχικά αναλύθηκε η αρχιτεκτονική ARM. Οι επεξεργαστές ARM είναι σχετικά απλοί, κάτι που τους κάνει κατάλληλους για εφαρμογές χαμηλής ισχύος. Είναι μια εναλλακτική λύση χαμηλού κόστους σε σχέση με την προσθήκη ενός επιπλέον εξειδικευμένου πυρήνα σε ένα SoC, δημιουργώντας δύο εικονικούς

επεξεργαστές που υποστηρίζονται από έλεγχο πρόσβασης σε επίπεδο υλικού. Αυτό επιτρέπει στον πυρήνα της εφαρμογής να αλλάζει μεταξύ δύο καταστάσεων, οι οποίες ονομάζονται κόσμοι (worlds), για να μην ξεφεύγει η πληροφορία από τον πιο ασφαλή κόσμο προς τον λιγότερο ασφαλή κόσμο. Η εναλλαγή μεταξύ αυτών των κόσμων συνήθως δεν αλληλεπιδρά με τις άλλες δυνατότητες του επεξεργαστή. και μπορούν να χρησιμοποιήσουν τον πυρήνα, για να ελέγξουν την πρόσβαση σε μυστικές πληροφορίες και τον κώδικα της συσκευής.

Μια κλασική εφαρμογή της τεχνολογίας TrustZone είναι η εκτέλεση ενός πλούσιου λειτουργικού συστήματος στον λιγότερο ασφαλή κόσμο, και ενός μικρότερου και πιο εξειδικευμένου κώδικα στον πιο ασφαλή κόσμο.

Στην πράξη, επειδή οι λεπτομέρειες της υλοποίησης της τεχνολογίας TrustZone δεν έχουν δημοσιευτεί και αναλυθεί, δεν είναι ξεκάθαρο πόση ακριβώς ασφάλεια παρέχει αυτή η αρχιτεκτονική.

Το 2017, η Arm Holdings δημιούργησε το Platform Security Architecture (PSA), ένα πρότυπο για την ασφάλεια IoT. Το πρότυπο δημιουργεί εμπιστοσύνη μεταξύ των υπηρεσιών και των συσκευών Internet of Things. Περιλαμβάνει μια σειρά προδιαγραφών όπως μοντέλα απειλών, αναλύσεις ασφαλείας, προδιαγραφές αρχιτεκτονικής υλικού και υλικολογισμικού. Στόχος του είναι να γίνει ένα στοιχείο ασφαλείας, με ενσωματωμένες λειτουργίες ασφαλείας τόσο για κατασκευαστές λογισμικού όσο και για συσκευές.

Το PSA έχει εξελιχθεί έκτοτε σε πιστοποίηση PSA, ένα πλαίσιο τεσσάρων σταδίων που μπορεί να χρησιμοποιηθεί από τους σχεδιαστές IoT για πρακτικές ασφαλείας. Το πλαίσιο περιλαμβάνει διαφορετικά επίπεδα εμπιστοσύνης, με κάθε επίπεδο να περιλαμβάνει διαφορετικό επίπεδο αξιολόγησης, με προοδευτικά αυξανόμενες εγγυήσεις ασφάλειας.

Η ρίζα εμπιστοσύνης της Trusted Computing Group, το Trusted Platform Module (TPM), αποτελεί αναπόσπαστο μέρος σχεδόν κάθε υπολογιστή, σε επίπεδο επιχείρησης, που πωλείται μέχρι και σήμερα. Το TPM, είναι ένα ασφαλές κρυπτογραφικό ολοκληρωμένο κύκλωμα το οποίο παρέχει μια προσέγγιση βασισμένη σε υλικό για τη διαχείριση του ελέγχου ταυτότητας του χρήστη, της πρόσβασης στο δίκτυο, της προστασίας των δεδομένων και πολλών άλλων που μεταφέρουν την ασφάλεια σε υψηλότερο επίπεδο από την ασφάλεια που βασίζεται σε λογισμικό.

Βέβαια, το πιθανό πρόσθετο κόστος και η πολυπλοκότητα είναι δύο από τους λόγους που οι περισσότεροι ενδιαφερόμενοι πιο συχνά δεν επιλέγουν τη χρήση του

TPM. Αυτό συμβαίνει παρόλο που το TPM διατίθεται ως βασικός εξοπλισμός με πολύ μικρό ή καθόλου επιπρόσθετο κόστος.

Σύμφωνα με την κορυφαία εταιρία ερευνών, η Samsung Knox αξιολογείται ως ισχυρή αλλά και η μοναδική συμμετοχή που κατάφερε να αποσπάσει αυτή τη διάκριση σε όλες τις ενότητες θεμάτων εταιρικής ασφάλειας.

Η Samsung Knox, είναι μία πλατφόρμα ασφαλείας η οποία έχει λάβει τις περισσότερες πιστοποιήσεις ασφαλείας διεθνώς από κάθε άλλη λύση κινητής. Αποτελείται από μια σειρά μηχανισμών άμυνας και ασφάλειας που παρέχουν προστασία από εισβολείς, κακόβουλα λογισμικά και άλλες απειλές. Η ασφάλεια της πλατφόρμας ξεκινά με την υλοποίηση ενός περιβάλλοντος ασφαλείας, που βασίζεται στο hardware. Στη συνέχεια, κατά την εκκίνηση, πραγματοποιούνται αυστηροί έλεγχοι ασφαλείας που παρακολουθούν συνεχώς την αξιοπιστία της συσκευής κατά τη λειτουργία της.

Βασιζόμενη σε αυτή τη θεμελιώδη αρχιτεκτονική ασφαλείας, που ωφελεί καταναλωτές και επιχειρήσεις, αναπτύσσονται ολοκληρωμένες λύσεις για εταιρικές κινητές, παρέχοντας ασφάλεια. Η Πλατφόρμα Knox βρίσκει εφαρμογή σε πολυάριθμα περιβάλλοντα και έχει λάβει τις περισσότερες πιστοποιήσεις ασφαλείας παγκοσμίως από κάθε άλλη λύση κινητής.

Όσον αφορά την RISC-V, πρόκειται για μια ανοιχτή τυπική αρχιτεκτονική συνόλου εντολών (ISA) που βασίζεται σε καθιερωμένες αρχές υπολογιστών, μειωμένων οδηγιών. Σε σύγκριση με ιδιόκτητα ISA όπως αυτά της Arm, η φύση ανοιχτού κώδικα του RISC-V φέρνει πιθανά οφέλη όσον αφορά τη σταθερότητα, την επεκτασιμότητα και την ασφάλεια. Ενώ το RISC-V έχει σημειώσει μεγάλη πρόοδο στην ανάπτυξη και την αρχική υιοθεσία, είναι ακόμα πρώτες μέρες για την τεχνολογία. Ως αποτέλεσμα, υπάρχουν άγνωστα και κάποια επίπεδα κινδύνου.

Μια βασική πρόκληση για μια ευρύτερη υιοθέτηση του RISC-V είναι η έλλειψη ενός καλά ανεπτυγμένου οικοσυστήματος λογισμικού.
Και σε αντίθεση με τα ιδιόκτητα ISA, το RISC-V ISA παρέχεται με άδειες ανοιχτού κώδικα που δεν απαιτούν χρεώσεις για χρήση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

•Arthur, W., Challener, D., Goldman, K., (2015), A Practical Guide to TPM 2.0, Apress Open.

•Marchese, S., (2020), Security vulnerabilities and hardware Trojans in RISC V processors, Electronics world

•Whitepaper: Samsung KnoxTM Security Solution, Samsung Research America

Samsung Electronics Co., Ltd., online, May, 2017.

•Whitepaper : An Overview of Samsung KNOX™, Enterprise Mobility Solutions

•Samsung Electronics Co., Ltd, online, June 2013.

•Γεωργιάδης, Χ. (2015), ΑΣΦΑΛΕΙΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΚΙΝΗΤΟΥ ΕΜΠΟΡΙΟΥ [eBook version], διαθέσιμο σε: http://repfiles.kallipos.gr/html_books/9536/Chapter%207/Chapter07.html

• Δρ. Δασυγένης, Μ., Ενσωματωμένα Συστήματα Ενότητα 6: Η αρχιτεκτονική του ARM. Πανεπιστημιακές παραδόσεις, διαθέσιμο σε:http://arch.icte.uowm.gr/courses/embedded/06ES_oc.pdf

• Ευθυμίου, Α. (2014), Αρχιτεκτονική Υπολογιστών Αρχιτεκτονικό σύνολο εντολών, διαθέσιμο σε: file:///C:/Users/admin/Downloads/l09_ARMx86%20(3).pdf

• Καμπουράκης, Γ. Εισαγωγή στην ασφάλεια Πληροφοριακών και

Επικοινωνιακών Συστημάτων Επικοινωνιακών Σύστημα, Πανεπιστημιακές σημειώσεις, διαθέσιμο σε: http://www.icsd.aegean.gr/website_files/proptyxiako/525297129.pdf

• Καρύδα, Μ. Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, [eBook version], διαθέσιμο σε: https://docplayer.gr/10307682-Politikes-asfaleias-pliroforiakon-systimaton.html

• Λέρα, Μ. (2012), ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝΣΥΣΤΗΜΑΤΩΝ, Κοζάνη, Πανεπιστήμιο Δυτικής Μακεδονίας, Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών (Αδημοσίευτη Διπλωματική Εργασία).

• Μαυρίδης, Ι. & Πάγκαλος, Γ. (2002), Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Θεσσαλονίκη.

• Μήλιου, Α., Ο έλεγχος του δικτύου [eBook version], διαθέσιμο σε: http://agent.csd.auth.gr/Lessons/management/k3.doc

• Οικονομίδης, Κ., (2019), Open Source λογισμικό Διαθέσιμο σε: https://www.dwrean.net/2019/05/open-source.html

• Παναγόπουλος, Αιμ. Χ., (2014), ΘΕΜΑΤΑ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΠΡΟΤΥΠΩΝ ΠΟΙΟΤΗΤΑΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ: Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ, Πάτρα, Πανεπιστήμιο Πατρών, Τμήμα Μηχανικών Η/Υ και Πληροφορικής (Αδημοσίευτη Διπλωματική Εργασία).

• Παπαφράγκου, Κ., (2013), ΑΝΑΠΑΡΑΣΤΑΣΗ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ ΣΥΝΘΕΤΩΝ ΔΙΚΤΥΩΝ ΓΙΑ ΑΝΑΛΥΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ, Πάτρα, Πανεπιστήμιο Πατρών, Τμήμα Ηλεκτρολόγων μηχανικών και τεχνολογίας υπολογιστών (Αδημοσίευτη Διπλωματική Εργασία).

• Παπουτσή, Αικ., (2013), Προσδιορισμός κινδύνων έργων πληροφοριακών συστημάτων: θεωρία και μελέτη περίπτωσης, Πειραιάς, Πανεπιστήμιο Πειραιά, Τμήμα Ψηφιακών Συστημάτων (Αδημοσίευτη Διπλωματική Εργασία).

• Σμυρναίος, Α., (2006), Μελέτη, ανάλυση και προτάσεις βελτίωσης της λειτουργίας, ασφάλειας και διαχείρισης του δικτύου του Τ.Ε.Ι. Δυτικής Μακεδονίας, Κοζάνη, Πανεπιστήμιο Μακεδονίας, Τμήμα Εφαρμοσμένης Πληροφορικής-Συστήματα Υπολογιστών (Αδημοσίευτη Διπλωματική Εργασία).

Ηλεκτρονικές πηγές:

• https://en.wikipedia.org/wiki/Non-repudiation

• https://en.wikipedia.org/wiki/Authorization

• https://el.wikipedia.org/wiki/DNSSEC

• https://en.wikipedia.org/wiki/Trusted_Computing

• https://eneikipedia.orgwiki/Trusted_third_party

• https://en.wikipedia.org/wiki/Hardware_keylogger

• https://el.wikipedia.org/wiki/Spyware

• https://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%B9%CF%84%CE%B5%CE%BA%CF%84%CE%BF%CE%BD%CE%B9%CE%BA%CE%AE_ARM

• https://en.wikipedia.org/wiki/Trusted_execution_environment

• https://en.wikipedia.org/wiki/ARM_Cortex-M

• https://en.wikipedia.org/wiki/ARM_Cortex-A

• https://www.arm.com/solutions/security

• https://en.wikipedia.org/wiki/PSA_Certified

• https://www.psacertified.org/blog/program-overview-digital-whitepaper

https://www.psacertified.org/app/uploads/2020/02/PSA_Certified_10_Security_Goals_PDF.pdf

• https://en.wikipedia.org/wiki/Internet_of_things

• https://cpl.thalesgroup.com/faq/hardware-security-modules/what-root-trust

• https://en.wikipedia.org/wiki/Trusted_Computing

• https://searchsecurity.techtarget.com/definition/trusted-computing

• https://en.wikipedia.org/wiki/Samsung_Knox

- https://www.samsung.com/gr/business/mobile-solutions/knox-solutions/
- https://developer.samsung.com/build
- https://docs.samsungknox.com/admin/whitepaper/kpe/trusted-boot.htm
- https://www.allaboutcircuits.com/industry-articles/how-risc-vs-security-development-of-processor-computer-architecture/
- https://el.wikipedia.org/wiki/ISA
- https://el.wikipedia.org/wiki/SSL
- https://riscv.org/risc-v-isa/
- https://en.wikipedia.org/wiki/RISC-V• https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
- https://riscv.org/blog/2020/03/risc-v-an-open-approach-to-system-security/

Εικόνες

Εικόνα 1: Βασική Δομή Ασφάλειας και Εμπιστοσύνης

(Πηγή :https://slideplayer.gr/slide/11835928/)

Εικόνα 2: Βασικές Προϋποθέσεις Ασφαλείας,

(Πηγή:http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/3186/LOG%20%CE%93%CE%9F%CE%A5%CE%9D%CE%91%CE%A1%CE%97%CE%A3%20-%20%CE%9C%CE%A0%CE%99%CE%9B%CE%91%CE%9B%CE%97%CE%A3%20-%20%CE%A0%CE%95%CE%A0%CE%95%CE%9B%CE%91%CE%A3%CE%97%CE%A3.pdf?sequence=3&isAllowed=y)

Εικόνα 3: Κύριες Κατηγορίες Απειλών ,

(Πηγή: Ασφάλεια Πληροφοριακών Συστημάτων

Αρχιτεκτονική Ασφάλεια, Τμήμα Μηχανικών Πληροφορικής

ΤΕΙ Κρήτης)

Εικόνα 4: Οφέλη Ανάλυσης Επικινδυνότητας,
(Πηγή:http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/3186/LOG%20%CE%93%CE%9F%CE%A5%CE%9D%CE%91%CE%A1%CE%97%CE%A3%20-%20%CE%9C%CE%A0%CE%99%CE%9B%CE%91%CE%9B%CE%97%CE%A3%20-%20%CE%A0%CE%95%CE%A0%CE%95%CE%9B%CE%91%CE%A3%CE%97%CE%A3.pdf?sequence=3&isAllowed=y)

Εικόνα 5: Ασφαλής και Μη Ασφαλής Κόσμος

(Πηγή ιστοσελίδα: https://www.microcontrollertips.com/embedded-security-brief-arm-trustzone-explained/)

Εικόνα 6: Δυνατότητες του TrustZone,

(Πηγή ιστοσελίδα: https://www.vpnmentor.com/reviews/trust-zone/)

Εικόνα 7: Τα 3 στάδια της PSA,

(Πηγή :Ethan Zhang, (2019), PSA building trust in IoT)

Εικόνα 8: Τα 10 αντίμετρα της PSA,

(Πηγή : Ethan Zhang, (2019), PSA building trust in IoT)

Εικόνα 9: Τα συστατικά μέρη του TPM,

(Πηγή :https://www.blockdit.com/posts/5eb0ce51344f963b0d2a7af2)

Εικόνα 10: Τα συστατικά μέρη του TPM και η συσχέτιση με τη version 1.2,

(Πηγή: https://en.Wikipedia.org/wiki/Trusted_Platform_Module)

Εικόνα 11:Samsung Knox,

(Πηγή: https://newtravelers.ru/en/tenda/knox-samsung-chto-eto-takoe-chto-iz-sebya-predstavlyaet-samsung-knox-zachem.html)

Εικόνα 12: Τα Επίπεδα Πλατφόρμας Knox,

(Πηγή: https://kp-cdn.samsungknox.com/b9821c47b3ef1cce894325a61a6fcdac.pdf)

Εικόνα 13: Η Δομή του RISC-V,

(Πηγή: https://www.google.com/search?q=risc+-v&rlz=1C1GCEA_enGR935GR935&sxsrf=ALeKk03WxUSE17sJs29PMMPdh64EzB8zKQ:1612559256784&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjRybet09PuAhX6A2MBHe7WCDYQ_AUoAXoECAQQAw&biw=1152&bih=753#imgrc=Kc75yYhlpJ79_M)

Εικόνα 14: Η ασφαλής εκκίνηση του επεξεργαστή RISC-V,

(Πηγή:https://www.researchgate.net/publication/332677369_Lightweight_Secure-Boot_Architecture_for_RISC-V_System-on-Chip)

Σχήμα 2: Ο Διαχωρισμός των απειλών

(Πηγή: Ασφάλεια Πληροφοριακών Συστημάτων

Αρχιτεκτονική Ασφάλεια, Τμήμα Μηχανικών Πληροφορικής

ΤΕΙ Κρήτης)

Σχήμα 3: Οι 7 Βασικές Λειτουργίες της ARM,

(Πηγή: http://arch.icte.uowm.gr/courses/embedded/06ES_oc.pdf)