ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΚΑΙ ΑΝΑΛΥΣΗ ΕΠΙΘΕΣΕΩΝ ΜΕ HARDWARE TROJANS ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:
ΚΩΝΣΤΑΝΤΙΝΟΣ ΘΕΟΔΩΡΑΚΟΠΟΥΛΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΦΩΤΙΟΣ ΒΑΡΤΖΙΩΤΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΚΑΙ ΑΝΑΛΥΣΗ ΕΠΙΘΕΣΕΩΝ ΜΕ HARDWARE TROJANS ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΦΩΤΙΟΣ ΒΑΡΤΖΙΩΤΗΣ

Άρτα, Δεκέμβριος 2021

STUDY AND ANALYSIS OF ATTACKS WITH HARDWARE TROJANS AND TACKLING STRATEGIES

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

Επιβλέπων καθηγητής: Φώτιος Βαρτζίωτης

Μέλος επιτροπής: Νικόλαος Γιαννακέας

Μέλος επιτροπής: Γρηγόριος Δουμένης

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον Καθηγητή μου για την ανάθεση αυτού του θέματος καθώς και την σωστή καθοδήγησή του προκειμένου να ολοκληρωθεί με ευτυχία η πτυχιακή μου εργασία για το θέμα των κακόβουλων επιθέσεων Hardware Trojan σε ένα υλικό.

ΠΕΡΙΛΗΨΗ

Στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας πραγματοποιήθηκε έρευνα όσον αφορά στο κλάδο των κακόβουλων επιθέσεων στο υλικό. Τέτοιου είδους επιθέσεις είναι ευρέως διαδεδομένες και ως Hardware Trojans. Τα τελευταία δέκα χρόνια έχουν παρατηρηθεί ολοένα και περισσότερες κακόβουλες επιθέσεις στη διαδικασία ανάπτυξης ενός ολοκληρωμένου κυκλώματος.

Καθώς η τεχνολογία συνεχώς εξελίσσεται, οι επιθέσεις Hardware Trojan προσπαθούν να προσαρμοστούν στις νέες συνθήκες. Με τη συγκεκριμένη εξέλιξη, εξελίχθηκαν επίσης και οι κακόβουλες τροποποιήσεις στα ολοκληρωμένα κυκλώματα, γεγονός που μπορεί να δημιουργήσει δυσάρεστες και καταστροφικές συνέπειες. Μια επίθεση υλικού Trojan τοποθετείται από αντιπάλους, χωρίς να το γνωρίζουν οι σχεδιαστές του αντίστοιχου υλικού. Οι επιθέσεις αυτές στοχεύουν στην παραβίαση και κατ' επέκταση στη μείωση της εμπιστοσύνης όσον αφορά το υλικό που δέχεται την επίθεση.

Οι επιθέσεις Hardware Trojan μπορούν να εμφανίζονται σε οποιοδήποτε στάδιο της σχεδίασης και κατασκευής του υλικού. Αυτό έχει ως αποτέλεσμα να γεννιούνται ολοένα και περισσότερες ανησυχίες σχετικά με την ασφάλεια στην κατασκευή και τη βιομηχανία των αντίστοιχων ηλεκτρονικών προϊόντων. Οι επιθέσεις Hardware Trojan, γενικότερα προκαλούν καταστροφικές συνέπειες στο υλικό που υφίσταται τις επιθέσεις αυτές.

Για να αποφύγουν οι εταιρίες σχεδιασμού των ολοκληρωμένων κυκλωμάτων τις αρνητικές αυτές συνέπειες που έχει οποιοδήποτε είδος επίθεση υλικού Trojan, αναζητούν συνεχώς μεθόδους ανίχνευσής τους. Στόχος τους είναι η όσο το δυνατόν πιο γρήγορη ανίχνευση μιας επίθεσης στο προς ανάπτυξη υλικό.

Λέξεις-κλειδιά:

Επιθέσεις υλικού, Hardware Trojans, Ανίχνευση επιθέσεων, ολοκληρωμένα κυκλώματα, Επιθέσεις λογισμικού, Φάση εισαγωγής, επίπεδο αφαίρεσης, Μηχανισμός ενεργοποίησης, ωφέλιμο φορτίο, απόκριση Hardware trojan, Μοντέλα Hardware Trojan, Τρόποι πρόβλεψης HT.

ABSTRACT

In the context of this dissertation, research was conducted regarding the field of malicious material attacks. Such attacks are also common as Hardware Trojans. In the last ten years there have been more and more malicious attacks in the process of developing an integrated circuit.

From time to time various types of Hardware Trojans hardware attacks have been observed. In the last decade more and more attacks against the material have been noticed by experts

As technology evolves, Hardware Trojan attacks try to adapt to new conditions. However, all these new technologies, as already observed, can have unpleasant consequences. A Hardware Trojan attack is placed by opponents, without the designers of the respective hardware knowing it. These attacks are aimed at violating and consequently reducing trust in the material.

Hardware Trojan attacks can occur at any stage of the hardware development. As a result, there are growing concerns about the safety in the manufacture and industry of the corresponding electronic products. Hardware Trojan attacks generally cause catastrophic consequences for the hardware that undergoes these attacks.

To avoid the negative consequences of any kind of Trojan hardware attack, integrated circuit design companies are constantly looking for methods to detect them. Its goal is to detect an attack on the material to be developed as quickly as possible.

Keywords:

Hardware Trojans, Attack detection, integrated circuits, Software Trojan, Insertion Phase, Abstraction Level, Trigger, Payload, Model of Hardware Trojan, Ways of forecasting HT.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ ΚΑΙ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια έχει αναπτυχθεί ένας τομέας στον επιστημονικό χώρο, ο οποίος διαταράσσει συνεχώς τους επιστήμονες σε ολόκληρο τον κόσμο. Ο συγκεκριμένος κλάδος που αναφέραμε ασχολείται με τις κακόβουλες επιθέσεις στο υλικό. Ο όρος αυτός είναι ευρέως γνωστός ως Hardware Trojans. Ο λόγος που απασχολεί ολοένα και περισσότερους επιστήμονες και ερευνητές του κλάδου είναι διότι η ασφάλεια τόσο του υλικού όσο και του λογισμικού είναι από τα πλέον σημαντικά ζητήματα του επιστημονικού κόσμου. Πρέπει να σημειωθεί ότι οι κακόβουλες επιθέσεις μπορούν να συμβούν είτε στο υλικό – hardware, είτε στο λογισμικό – software. Οι επιθέσεις υλικού όπως έχει προκύψει ύστερα από μελέτες έχουν αυξηθεί σε πολύ μεγάλο βαθμό τα τελευταία δέκα χρόνια. Πρέπει να αναφέρουμε ότι δεν υπάρχει μόνο ένας τύπος Hardware Trojan. Ύστερα από τις μελέτες του επιστημονικού κλάδου, οι επιστήμονες έφτασαν στο συμπέρασμα ότι οι επιθέσεις Hardware Trojan μπορούν να έχουν πολλούς και διαφορετικούς τύπους. Πρόκειται, συγκεκριμένα για επιθέσεις σε κάθε είδους ηλεκτρονικό υλικό. Οι επιθέσεις αυτές στοχεύουν στην παραβίαση και κατ' επέκταση στην μείωση της εμπιστοσύνης όσον αφορά το υλικό. [1]

Ένα επίσης σημαντικό ζήτημα που απασχολεί τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων στις μέρες μας και τις βιομηχανίες είναι το γεγονός ότι οι κακόβουλες επιθέσεις Hardware Trojan μπορούν να εμφανίζονται σε οποιοδήποτε στάδιο της διαδικασίας ανάπτυξης του εκάστοτε υλικού. Οι κακόβουλες αυτές επιθέσεις μπορούν να λάβουν χώρα σε διάφορες συσκευές είτε αυτές ανήκουν στο υπολογιστικό σύστημα όπως είναι λόγου χάριν οι μνήμες καθώς και οι επεξεργαστές είτε ανήκουν σε συσκευές εκτός υπολογιστικού συστήματος όπως είναι παραδείγματος χάριν το Ίντερνετ των πραγμάτων – Internet of Things. [2]

Στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας θα μελετηθεί ο κλάδος των Hardware Trojan. Πρόκειται για μια απειλή όσον αφορά τόσο την ασφάλεια όσο και την αξιοπιστία των υπολογιστικών συστημάτων. Σημαντικό κομμάτι της έρευνας για τους μελετητές του κλάδου αποτελεί ο προσδιορισμός της ύπαρξης ή μη ενός Hardware Trojan στο αντίστοιχο υλικό.

Από πολλούς ερευνητές έχει ειπωθεί ότι το υλικό – hardware αποτελεί πολύ αξιόπιστο στοιχείο για μια ηλεκτρονική συσκευή. Στο γεγονός αυτό βασίστηκαν και οι δημιουργοί των κακόβουλων επιθέσεων Trojan. Αυτοί που δημιουργούν και τοποθετούν ένα κακόβουλο Trojan στο προς ανάπτυξη υλικό χαρακτηρίζονται ως αντίπαλοι. Ο κύριος στόχος των αντιπάλων του εκάστοτε υλικού είναι να προκαλέσουν βλάβες στη λειτουργικότητα του προς επίθεση υλικού. Επίσης η τοποθέτηση ενός hardware Trojan από έναν εισβολέα θα μπορούσε να έχει ως κίνητρο την διείσδυση στο δίκτυο. [3]Τέτοιου είδους επιθέσεις υλικού συνήθως κατασκευάζονται και τοποθετούνται από αντιπάλους, προκειμένου να δημιουργηθεί οποιαδήποτε βλάβη στη λειτουργία του εκάστοτε υλικού. Μια καταστροφική συνέπεια που μπορεί επίσης να προκαλέσει η είσοδος ενός Hardware Trojan στο υλικό και που προσπαθούν συνεχώς οι σχεδιαστές να αποτρέψουν είναι η πλήρης και ολοκληρωτική καταστροφή του.

Όλα τα διαφορετικά είδη Hardware Trojan είναι κακόβουλες τροποποιήσεις που επηρεάζουν είτε σε μικρό είτε σε πολύ μεγάλο βαθμό τη λειτουργία ενός ολοκληρωμένου κυκλώματος . Τέτοιου είδους τροποποιήσεις υλικού όπως είναι λογικό είναι ανεπιθύμητες για τον κατασκευαστή και σχεδιαστή του εκάστοτε υλικού. Κανένας σχεδιαστής υλικού δεν γνωρίζει εκ τον προτέρων για τις παραβιάσεις στο υλικό, που μπορεί να έχουν τρομερές επιπτώσεις σε όλο το σύστημα.

1.1 Ορισμός

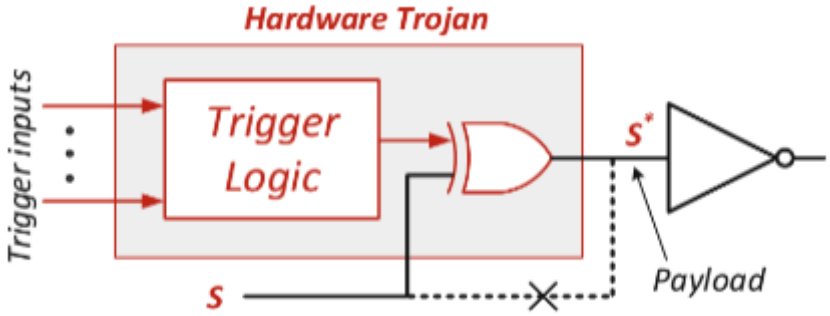
Στο σημείο αυτό είναι σκόπιμο να αναφερθούμε στον ορισμό που υπάρχει για τις επιθέσεις Hardware Trojan, προκειμένου να γίνει περισσότερο κατανοητή η λειτουργία τους και ο λόγος ύπαρξής τους. Ονομάζουμε Hardware Trojan οποιαδήποτε τροποποίηση μπορεί να πραγματοποιηθεί σε ένα ήδη υπάρχον ολοκληρωμένο κύκλωμα, με τη δυσάρεστη συνέπεια να διαταραχθεί και να αλλάξει η λειτουργία του. [4]

1.2 Λειτουργία

Κατά καιρούς έχουν παρατηρηθεί διάφοροι τύποι επιθέσεων υλικού Hardware Trojans. Την τελευταία δεκαετία ολοένα και περισσότερες επιθέσεις εναντίον του υλικού έχουν γίνει αντιληπτές από τους ειδικούς. Καθώς η τεχνολογία συνεχώς εξελίσσεται, διαμορφώνονται αναλόγως και οι επιθέσεις Trojans ώστε να μην είναι εύκολη η ανίχνευση τους. Η πιο απλή μορφή που θα μπορούσε να έχει ένα Trojan είναι η προσθήκη ενός

μπλοκ κυκλώματος. Με τη συγκεκριμένη προσθήκη μπορεί να προσκληθεί τόσο ανώμαλη λειτουργία του ολοκληρωμένου κυκλώματος όσο και τροποποίηση στην αρχική συμπεριφορά του σχεδίου. Τα συγκεκριμένα μπλοκ κυκλώματος έχουν τη δυνατότητα να εφαρμόζουν μια συνάρτηση σε μορφή Boolean. Η τιμή αυτή προκαλεί την ενεργοποίηση του Trojan, μόνο όταν ορισμένοι κόμβοι του κυκλώματος φτάσουν σε μια συγκεκριμένη κατάσταση.

Στην εικόνα που ακολουθεί μπορεί κανείς να δει την αναπαράσταση της δομής ενός Hardware Trojan. Παρατηρώντας κανείς την εικόνα που ακολουθεί μπορεί να δει την δυσλειτουργία που προκαλείται λόγω του Hardware Trojan, αναστρέφοντας το σήμα S, όταν η συνθήκη είναι αληθής. [1]



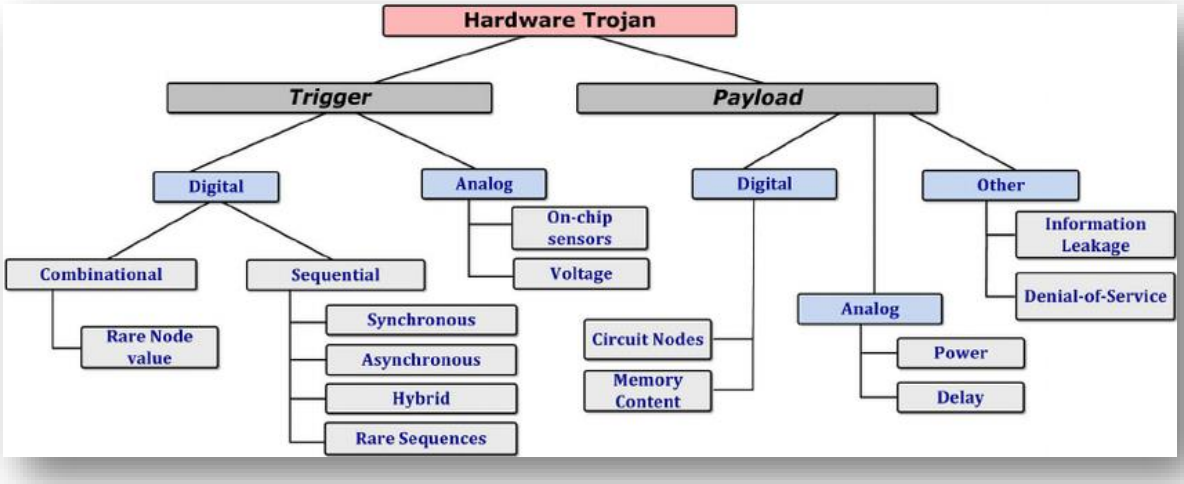
Εικόνα 1 - Δομή ενός Hardware Trojan [1]

Ο μοναδικός σκοπός όλων των Hardware Trojan είναι ακριβώς ο ίδιος σε όλες τις περιπτώσεις. Πιο συγκεκριμένα, δημιουργούνται για να θέσουν σε κίνδυνο την εμπιστοσύνη και την ακεραιότητα του υλικού που υφίσταται την επίθεση. Σε ορισμένα υλικά, μια επίθεση Trojan μπορεί να σημαίνει μείωση του αναμενομένου χρόνου ζωής του, παραδείγματος χάριν από τα 20 χρόνια αναμενόμενου χρόνου ζωής στα 5 χρόνια. Εν αντιθέσει, με άλλες περιπτώσεις επιθέσεων Trojan όπου υπάρχει πλήρης αποτυχία του εκάστοτε συστήματος όταν αυτό ενεργοποιηθεί [4]. Οι επιθέσεις υλικού Hardware Trojan έχουν αναπαρασταθεί με διάφορες μορφές. Ο λόγος που συμβαίνει αυτό είναι διότι ο κλάδος των Hardware Trojan είναι ένας συνεχώς εξελισσόμενος κλάδος. Αυτό σημαίνει ότι συνεχώς ανακαλύπτονται και μελετιούνται καινούργιες μορφές και τύποι επιθέσεων Trojan. [5]

Είναι σημαντικό να σημειωθεί ότι το Hardware Trojan δεν είναι ένα ελάττωμα ούτε στην κατασκευή ούτε στην σχεδίαση του υλικού. Το Trojan σε οποιαδήποτε μορφή και αν βρίσκεται έχει εισαχθεί από κάποιον αντίπαλο και ο εκάστοτε σχεδιαστής του υλικού δεν γνωρίζει τη θέση ενεργοποίησή του. Η ενεργοποίηση ενός Hardware Trojan πραγματοποιείται μέσω ενός ειδικού μηχανισμού. Τον συγκεκριμένο μηχανισμό μπορεί κανείς να τον συναντήσει με τον όρο «Trigger». Επίσης, προσφέρουν μια συγκεκριμένη λειτουργία, την οποία έχουν ονομάσει «Payload». Ένα Trojan μπορεί να είναι είτε μικρού είτε μεγάλου μεγέθους ανεξάρτητα από το μέγεθος που έχει το υπόλοιπο κύκλωμα. Μπορεί να αποτελείται από λίγα μόλις τρανζίστορ μέχρι και πολλών εκατομμυρίων τρανζίστορ. [1]

Τα Hardware Trojan μπορούν να εμφανιστούν σε πολλές μορφές σε ένα κύκλωμα. Η ενεργοποίηση τους πραγματοποιείται είτε από ένα ακολουθιακό είτε από ένα συνδυαστικό ψηφιακό κύκλωμα. Μπορεί επίσης να πραγματοποιηθεί η ενεργοποίηση του ακόμα και από ένα υβριδικό συνδυασμό των δύο. Ένας επιπλέον τρόπος ενεργοποίησής του είναι από αναλογικά ερεθίσματα [4]. Από την άλλη μεριά, η απόκριση ενός Hardware Trojan μπορεί να είναι είτε αναλογική είτε ψηφιακή. Και στις δυο περιπτώσεις πρέπει να είναι σχεδιασμένα με τέτοιο τρόπο ώστε να προκύπτουν κακόβουλες συνέπειες όταν πραγματοποιηθεί η ενεργοποίηση. [6]

Στην Εικόνα που ακολουθεί μπορεί κανείς να παρατηρήσει τις ταξινομήσεις του Hardware Trojan που βασίζεται σε μηχανισμούς ενεργοποίησης – trigger καθώς και σε μηχανισμούς του ωφέλιμου φορτίου – Payload. Το ωφέλιμο φορτίο μπορείς κανείς να το συναντήσει και με τον όρο απόκριση του Hardware Trojan – HT.



Εικόνα 2 - Ταξινόμηση του Hardware Trojan [7]

Σύμφωνα με την πρώτη παραλλαγή του μηχανισμού ενεργοποίησης – Trigger, τα Hardware Trojan έχουν τη δυνατότητα να ταξινομηθούν σε αναλογικά και σε ψηφιακά Trojan. Ο τρόπος ενεργοποίησης τους σε κάθε περίπτωση διαφέρει. Πιο συγκεκριμένα, στα αναλογικά Trojan η ενεργοποίηση πραγματοποιείται από αναλογικές συνθήκες, όπως είναι λόγου χάριν η θερμοκρασία. Εν αντιθέσει με τα ψηφιακά Trojan, τα οποία ενεργοποιούνται με βάση μια λογική συνάρτηση Boolean. [8]

Σε συνέχεια της ταξινόμησης των Trojan, είναι χρήσιμο να αναφερθούμε στην περαιτέρω ταξινόμηση των ψηφιακών ενεργοποιημένων Trojan. Πιο συγκεκριμένα, αυτός ο τύπος Trojan μπορεί να ταξινομηθεί σε ακολουθιακούς και σε συνδυαστικούς τύπους. [8] Τα αναλογικά Trojan προκαλούν επιθέσεις που μπορεί να βλάψουν όλα ή επιλεγμένα υποσυστήματα των κυκλωμάτων. Τέτοιου είδους Trojan αναφέρονται και ως reliability Trojans από ορισμένους ερευνητές του συγκεκριμένου κλάδου. Τα reliability Trojan μπορεί να προκαλέσουν τη γήρανση των συσκευών. [1]

Για την κατηγοριοποίηση όσον αφορά το ωφέλιμο φορτίο – Payload, τα Trojan είναι υπεύθυνα για την λειτουργική δυσλειτουργία κατά τη διαδικασία ενεργοποίησης, με αποτέλεσμα να προκληθεί θέρμανση ή ακόμα και διαρροή πληροφοριών. Με βάση την παραλλαγή του ωφέλιμου φορτίου τα Hardware Trojan μπορούν να ταξινομηθούν σε αναλογικά, ψηφιακά και σε άλλη μορφή.

Οι ερευνητές μελετούν και αναλύουν περισσότερο τα ψηφιακά Trigger σε ένα Hardware Trojan. Ο κυριότερος λόγος που συμβαίνει αυτό είναι διότι απαρτίζεται τόσο από συνδυαστικά όσο και από ακολουθιακά κυκλώματα. Όσον αφορά στα συνδυαστικά Trojan triggers είναι απαραίτητο να αναφέρουμε ότι δεν διαθέτουν οποιαδήποτε είδους στοιχείο το οποίο με τη σειρά του θα φανέρωνε την κατάσταση στην οποία βρίσκετε το εκάστοτε κύκλωμα. Ως παράδειγμα τέτοιου είδους στοιχείων μπορούμε να αναφέρουμε την ύπαρξη των flip – flops μέσα σε ένα ολοκληρωμένο κύκλωμα. Ένα επίσης σημαντικό χαρακτηριστικό για τα συνδυαστικά Triggers είναι ότι στηρίζονται σε μια συγκεκριμένη συνθήκη. Η συνθήκη αυτή μπορεί να πραγματοποιηθεί σε ένα συγκεκριμένο πλήθος κόμβων ενός ολοκληρωμένου κυκλώματος που δεν χρησιμοποιούνται συχνά. Από την άλλη μεριά, τα ακολουθιακά κυκλώματα Hardware Trojans στηρίζονται σε μια αλληλουχία καταστάσεων. Για τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων, η διαδικασία ανίχνευσης ενός Trojan που ανήκει στην κατηγορία των ακολουθιακών είναι πιο δύσκολη συγκριτικά με την ανίχνευση των Trojans που ανήκουν στην δεύτερη κατηγορία, η οποία είναι τα συνδυαστικά Trojan triggers. Ο λόγος που συμβαίνει αυτό είναι διότι πρέπει να πραγματοποιηθεί συγκεκριμένη ακολουθία συνθηκών πριν τη διαδικασία ενεργοποίησή τους, όπως έχουμε ήδη αναφέρει προηγουμένως. Η ανίχνευση των ακουλουθιακών Trojan Trigger δεν είναι εφικτή όταν χρησιμοποιούνται συμβατικές μέθοδοι για τις απαραίτητες δοκιμές στο σχεδιασμό και στην κατασκευή των ολοκληρωμένων κυκλωμάτων. [9]

Για να γίνει πλήρως κατανοητή η κατηγοριοποίηση του μηχανισμού ενεργοποίησης ενός Hardware Trojan είναι απαραίτητο να αναφερθούμε και να περιγράψουμε περαιτέρω και την επόμενη κατηγορία τους που είναι τα αναλογικά Trojans. Η συγκεκριμένη κατηγορία στηρίζεται σε φυσικά φαινόμενα προκειμένου να πραγματοποιηθεί η ενεργοποίηση των αντίστοιχων Hardware Trojans. Ως παραδείγματα τέτοιου είδους φυσικών φαινόμενων που μπορούν να συμβάλλουν στην ενεργοποίηση ενός Hardware Trojan μπορούμε να αναφέρουμε τη θερμοκρασία, τη χωρητικότητα μιας πύλης του ολοκληρωμένου κυκλώματος καθώς και την ακτινοβολία RF.

Το κυριότερο χαρακτηριστικό που διακρίνει όλα τα είδη των Trojan είναι ότι πρέπει να σχεδιαστούν και να τοποθετηθούν με τέτοιο τρόπο ώστε να είναι όσο γίνετε πιο δύσκολη η ανίχνευσή τους κατά τις δοκιμές που πρέπει να περνάνε όλα τα ολοκληρωμένα κυκλώματα τόσο στην διαδικασία σχεδιασμού όσο και στη διαδικασία της κατασκευής τους. Αυτό

μπορεί να επιτευχθεί εάν ο αντίπαλος επιλέξει να τοποθετήσει το αντίστοιχο Trojan σε τέτοιο σημείο στο οποίο είναι σχεδόν αδύνατον να ενεργοποιηθεί το Trojan όταν πραγματοποιηθούν οι αντίστοιχες δοκιμές από τους σχεδιαστές του υλικού.

1.3 Κύρια Χαρακτηριστικά των Hardware Trojans

Για την καλύτερη κατανόηση των επιθέσεων υλικού Trojan είναι σκόπιμο να αναφερθούμε λεπτομερώς στα κυριότερα χαρακτηριστικά τους. Αρχικά, πρέπει να αναφερθούμε στο μέγεθος τους. Πρόκειται για μικρά σε μέγεθος αν τα συγκρίνει κάνεις με το προς επίθεση σχέδιο. Το γεγονός αυτό δυσκολεύει την ανίχνευση των Hardware Trojans, διότι οι ιδιότητες του ολοκληρωμένου κυκλώματος στο οποίο υφίσταται κάποιου είδους επίθεση Trojan με τις ιδιότητες ενός ολοκληρωμένου κυκλώματος χωρίς την ύπαρξη Trojan είναι πανομοιότυπες. Ένα δεύτερο μα εξίσου σημαντικό χαρακτηριστικό των Hardware Trojans είναι ότι έχουν τη δυνατότητα να παραμένουν σε κατάσταση εκτός λειτουργίας κατά τη φυσιολογική λειτουργία του προς επίθεση ολοκληρωμένου κυκλώματος και να ενεργοποιούνται όταν προκύπτει μια συγκεκριμένη συνθήκη. Ένα τρίτο και τελευταίο χαρακτηριστικό που θα αναφέρουμε για τα Hardware Trojan είναι η συμπεριφορά τους. Πιο συγκεκριμένα, η συμπεριφορά κάθε Hardware Trojan είναι άγνωστη στον εκάστοτε σχεδιαστή του αντίστοιχου υλικού προς κατασκευή. Για το λόγο αυτό δεν θα μπορούσε να υπάρξει μια τεχνική για την ανίχνευση Trojan, η οποία να απευθυνόταν σε όλους τους διαφορετικούς τύπους Trojans που υπάρχουν και συνεχώς εξελίσσονται με την πάροδο του χρόνου. [10]

1.4 Διαφορά του HT με το ST

Διακρίνεται μια βασική διαφορά των επιθέσεων Hardware Trojan HT με τις επιθέσεις Software Trojan- ST. Είναι ιδιαίτερα σημαντικό να αναφερθούμε και να αναλύσουμε περαιτέρω τη διαφοροποίησή τους.

Οι επιθέσεις στο υλικό Hardware Trojan ανιχνεύονται πολύ δυσκολότερα σε σύγκριση με τις επιθέσεις στο λογισμικό. Εάν μια επίθεση HT ανιχνευθεί μετά από τη διαδικασία παραγωγής του υλικού, δεν μπορεί να απομακρυνθεί. Το γεγονός αυτό συμβάλλει ώστε οι περισσότερες κακόβουλες επιθέσεις να πραγματοποιούνται στο υλικό – hardware. [4]

Στο σημείο αυτό προκειμένου να γίνει πλήρως κατανοητές οι δυο έννοιες και η διαφοροποίησή τους, και ο άμεσος τρόπος που μπορούν να επηρεάσουν τα διάφορα Trojan τους χρήστες, είναι σκόπιμο να αναφερθούμε σε ένα χαρακτηριστικό παράδειγμα. Πιο συγκεκριμένα, αξίζει να αναφερθούμε στους ειδικούς της Kaspersky Lab, οι οποίοι παρατήρησαν ένα ασυνήθιστο καινούργιο Trojan. Το συγκεκριμένο Trojan διανέμεται στις συσκευές μέσα από το Google Play Store που διαθέτουν όλες οι Android συσκευές. Το Trojan Dvmap είχε τη δυνατότητα να αποκτά δικαιώματα απόλυτης πρόσβασης σε συσκευές Android. Μια ακόμα ανεπιθύμητη συνέπεια από το συγκεκριμένο Trojan είναι η δυνατότητα του να ελέγχει τη συσκευή με τη χρήση κακόβουλου κώδικα στη βιβλιοθήκη του εκάστοτε συστήματος. Αξιοσημείωτο είναι το γεγονός ότι το Μάρτιο του 2017 το συγκεκριμένο Trojan έχει κατέβει από το Google Play πάνω από 50 χιλιάδες φορές. Η εταιρία Kaspersky Lab με τη σειρά της ανέφερε την ύπαρξη του συγκεκριμένου Trojan στην Google, η οποία το αφαίρεσε εν συνεχεία από το κατάστημα. Το Trojan αυτό ονομαζόταν Dvmap και παρουσιαζόταν ως παιχνίδι που θα μπορούσαν οι χρήστες του Google play store να κατεβάσουν τοπικά στις ηλεκτρονικές τους συσκευές. Προκειμένου να μην αντιληφθεί η google την ύπαρξη κακόβουλης απειλής μέσω του συγκεκριμένου παιχνιδιού οι σχεδιαστές του ανέβασαν στο google play store μια καθαρή εφαρμογή περίπου στα τέλη Μάρτη του 2017. Μετά από ένα σύντομο χρονικό διάστημα ανανέωσαν την καθαρή εφαρμογή με το κακόβουλο λογισμικό. Το κακόβουλο αυτό λογισμικό αντικαταστάθηκε πολύ σύντομα από την αρχική καθαρή εφαρμογή. Η αλλαγή αυτή από την καθαρή εφαρμογή και το κακόβουλο λογισμικό πραγματοποιήθηκε περισσότερες από πέντε φορές στο μικρό διάστημα των τεσσάρων εβδομάδων. [11]

Το λεγόμενο Trojan Dvmap είχε δύο φάσης όσον αφορά την είσοδο του στην εκάστοτε ηλεκτρονική συσκευή. Σύμφωνα με το αρχικό στάδιο εγκατάστασης του συγκεκριμένου Trojan ήταν η προσπάθειά του να αποκτήσει πλήρη πρόσβαση και δικαιώματα της εκάστοτε συσκευής. Εάν η διαδικασία αυτή στεφθεί με απόλυτη επιτυχία, ξεκινάει η διαδικασία εγκατάστασης πρόσθετων εργαλείων. Εν συνεχεία πραγματοποιείται η αντικατάσταση του καθαρού κώδικα της συσκευής με αυτή του κακόβουλου κώδικα. Η μετατροπή αυτή θα μπορούσε να επιφέρει καταστροφικές συνέπειες στη συσκευή μέχρι και την πλήρη καταστροφή της. [11]

1.5 Ομοιότητα του Hardware Trojan με το Software Trojan

Πέρα από τη διαφορά που υπάρχει ανάμεσα στο Hardware Trojan με τα Software Trojan που αναφέρθηκαν στην προηγούμενη υπό ενότητα, διακρίνονται επίσης και ορισμένες ομοιότητες που θα ήταν ιδιαίτερα σημαντικό να αναφέρουμε. Οι επιθέσεις Trojan είτε αναφερόμαστε σε υλικό είτε αναφερόμαστε σε λογισμικό διαθέτει τα ίδια βασικά χαρακτηριστικά. Πιο συγκεκριμένα, αναφερόμαστε στα τρία κύρια χαρακτηριστικά τα οποία είναι, η κακόβουλη πρόθεση, η αποφυγή εντοπισμού καθώς και η σπανιότητα όσον αφορά την ενεργοποίησή του. Μια δεύτερη ομοιότητα μεταξύ των δυο είναι η ύπαρξη και στις δύο περιπτώσεις του μηχανισμού ενεργοποίησης- trigger και του ωφέλιμου φορτίου - payload. [1]

1.6 Κύκλος ανάπτυξης ενός ολοκληρωμένου κυκλώματος IC

Η διαδικασία ανάπτυξης και κατασκευής ενός ολοκληρωμένου κυκλώματος απαρτίζεται από πολλά και διαφορετικά τμήματα. Προκειμένου να είναι πλήρως αξιόπιστο ένα ολοκληρωμένο κύκλωμα μετά το πέρας της κατασκευής του θα πρέπει όλα τα επιμέρους τμήματα στον κύκλο ανάπτυξης του να είναι εξίσου αξιόπιστα. Για να γίνει πλήρως κατανοητός ο τρόπος με τον οποίο μπορεί να επηρεαστεί η αξιοπιστία των επιμέρους τμημάτων και κατ’ επέκταση η αξιοπιστία του τελικού υλικού θα πρέπει να αναφερθούμε και να αναλύσουμε περαιτέρω τον κύκλο ανάπτυξης των ολοκληρωμένων κυκλωμάτων.

Αρχικά είναι σκόπιμο να αναφέρουμε ότι ο κύκλος ανάπτυξης ενός ολοκληρωμένου κυκλώματος ταξινομείται σε δύο υποκατηγορίες. Οι υποκατηγορίες αυτές είναι αρχικά ο σχεδιασμός και εν συνεχεία η κατασκευή του IC. Οι επιστήμονες ονόμασαν τη διαδικασία του σχεδιασμού ενός ολοκληρωμένου κυκλώματος ως φάση front- end. Η συγκεκριμένη διαδικασία δίνει πληροφορίες ως προς το τι θα είναι ικανό να κάνει το προς εξέλιξη υλικό. Όπως έχουμε ήδη αναφέρει, η δεύτερη φάση στη διαδικασία ανάπτυξης των ICs είναι η φάση της κατασκευής. Τη συγκεκριμένη φάση, οι επιστήμονες την ονόμασαν ως φάση back end. Πρόκειται για το στάδιο εκείνο όπου δημιουργείται το τελικό, φυσικό προϊόν. [12] Στη συνέχεια της συγκεκριμένης ενότητας θα αναφερθούμε και θα αναλύσουμε περαιτέρω τις δυο υποκατηγορίες όσον αφορά τη φάση ανάπτυξης των ολοκληρωμένων κυκλωμάτων.

Ξεκινώντας από τη φάση σχεδιασμού - front end, θα μπορούσαμε να αναφέρουμε ότι πραγματοποιείται η μετατροπή της υψηλού επιπέδου περιγραφής σε επίπεδο πυλών. Πιο συγκεκριμένα, στη φάση της προδιαγραφής καθορίζονται οι προδιαγραφές και οι απαιτήσεις του εκάστοτε συστήματος. Η αρχιτεκτονική του προς εξέλιξη υλικού σχεδιάζεται με τέτοιο τρόπο ώστε να ικανοποιεί τις αρχικές απαιτήσεις και προδιαγραφές. Στη συνέχεια ακολουθεί η διαδικασία του σχεδιασμού. Στο συγκεκριμένο στάδιο πραγματοποιείται η υλοποίηση της αρχιτεκτονικής του σε κώδικα. Η μετατροπή αυτή απαιτεί την ύπαρξη μιας γλώσσας περιγραφής υλικού γνωστή και ως HDL. Οι πιο συνηθισμένα χρησιμοποιούμενες γλώσσες HDL είναι είτε η VHDL είτε η γλώσσα Verilog. Στο σημείο αυτό πρέπει να αναφέρουμε ότι υπάρχει μια εσωτερική ομάδα σχεδιασμού μέσα στην εκάστοτε εταιρία που έχει αναλάβει την ανάπτυξη του ολοκληρωμένου κυκλώματος, η οποία αναλαμβάνει την μετατροπή του σχεδιασμού σε κώδικα HDL. Από την άλλη μεριά υπάρχουν εταιρείες ανάπτυξης ολοκληρωμένων κυκλωμάτων, οι οποίες δεν αναλαμβάνουν το τμήμα της μετατροπής του σχεδιασμού σε κώδικα, αναθέτοντας τη διαδικασία σε τρίτους προμηθευτές. [13]

Μετά τη διαδικασία σχεδιασμού ακολουθεί η λεγόμενη διαδικασία επικύρωσης. Όπως είναι λογικό ο σχεδιασμός του υλικού που βρίσκεται πλέον κωδικοποιημένος σε γλώσσα περιγραφής υλικού θα πρέπει να περάσει από δοκιμές με τη χρήση προσομοιωτών. Ο λόγος που συμβαίνει αυτό είναι για να σιγουρευτούν οι σχεδιαστές για την ορθότητα του εκάστοτε υλικού που βρίσκεται προς σχεδίαση. Οι αρμόδιοι πραγματοποιούν πολλαπλές και άκρως αυστηρές δοκιμές στη διαδικασία επικύρωσης. Ο λόγος είναι ότι θα πρέπει να ανιχνευθούν όλα τα τυχόν σφάλματα που μπορεί να προκύψουν στον εκάστοτε σχεδιασμό ενός υλικού. Εάν τα σφάλματα που μπορεί να έχει ένας σχεδιασμός δεν εντοπιστούν έγκαιρα δηλαδή στη φάση της επικύρωσης και γίνουν αντιληπτά μετά τη διαδικασία της κατασκευής του, τότε το κόστος των σφαλμάτων θα ήταν καταστροφικό. Είναι εξαιρετικά χρήσιμο να αναφέρουμε ότι οι δυο διαδικασίες που μόλις περιεγράφηκαν, δηλαδή η διαδικασία του σχεδιασμού και η διαδικασία της επικύρωσης είναι διαδικασίες που εκτελούνται σχεδόν παράλληλα, ακολουθώντας βήματα εμπρός και πίσω, με σκοπό να ανιχνεύονται και κατά επέκταση να διορθώνονται τα λάθη που προκύπτουν. [13]

Μετά από τη διαδικασία της επικύρωσης, ακολουθεί η διαδικασία της «χρυσής διάταξης». Ο επικυρωμένος πλέον, χωρίς σφάλματα σχεδιασμός είναι σε θέση να τροποποιηθεί σε πύλες και κατάλληλες συνδέσεις. Για τη συγκεκριμένη μετατροπή είναι απαραίτητη η

χρήση κατάλληλων εργαλείων λογισμικού αυτοματοποιημένου σχεδιασμού, γνωστά ευρέως ως CAD. [13]

Μετά την λεπτομερή περιγραφή της φάσης του σχεδιασμού Frond end, σειρά έχει η περιγραφή για τη φάση της κατασκευής Back end. Πιο συγκεκριμένα, το τελικό μοντέλο που προκύπτει από τη φάση του σχεδιασμού του υλικού παραδίνεται στο αντίστοιχο εργοστάσιο που αναλαμβάνει να κατασκευάσει ένα φυσικό τσιπ. Κατά κύριο λόγο οι εταιρείες που αναλαμβάνουν το σχεδιασμό των υλικών, δεν έχουν τις προδιαγραφές ώστε να αναλάβουν και την διαδικασία της κατασκευής των αντίστοιχων υλικών. Αυτό έχει ως αποτέλεσμα τα σχέδια που δημιουργούν οι ίδιες οι εταιρίες να κατασκευάζονται σε άλλες εταιρίες που διαθέτουν τις κατάλληλες προδιαγραφές ώστε να φέρουν εις πέρας τη διαδικασία της κατασκευής του εκάστοτε υλικού με επιτυχία.

Ύστερα και από την επιτυχημένη ολοκλήρωση της διαδικασίας κατασκευής που περιεγράφηκε προηγουμένως, ακολουθεί η διαδικασία της εξέτασης. Στο σημείο αυτό, είναι απαραίτητο να ακολουθήσει ο έλεγχος και οι τελικές δοκιμές σε όλον τον επιμέρους εξοπλισμό που απαρτίζει το προς κατασκευή υλικό. Οι συγκεκριμένες δοκιμές μπορούν να πραγματοποιηθούν με τη χρήση αυτόματου εξοπλισμού δοκιμών, γνωστό επίσης και με τη συντομογραφία ATE (Automatic Test Equipment). Ο κύριος στόχος της χρήσης τέτοιου είδους αυτόματου εξοπλισμού δοκιμών είναι η εύρεση τυχών κατασκευαστικών βλαβών και δυσλειτουργιών στη διαδικασία κατασκευής. Ο έλεγχος αυτός καθιστάτε απαραίτητος για την ανίχνευση και τον έλεγχο της απόδοσης. Είναι απαραίτητο στο σημείο αυτό να αναφέρουμε ότι οι δοκιμαστικές αυτές καταστάσεις θα πρέπει να πραγματοποιούνται τόσο σε οποιαδήποτε πύλη υπάρχει στο προς κατασκευή τσιπ όσο και σε οποιαδήποτε σύνδεση έχει χρησιμοποιηθεί για την κατασκευή του. [3]

Η τελευταία διαδικασία που υπάρχει στη φάση της κατασκευής ενός υλικού είναι η διαδικασία της συναρμολόγησης. Πρόκειται για την ολοκλήρωση της πλακέτας, στην οποία θα ξεκινήσει η τοποθέτηση των κατάλληλων εξαρτημάτων. Πιο συγκεκριμένα, τα εξαρτήματα που είναι απαραίτητα για την ολοκλήρωση της κατασκευής του υλικού είναι τα κατάλληλα τσιπ, τόσο τα μηχανικά όσο και τα ηλεκτρονικά εξαρτήματα. Ως παραδείγματα ηλεκτρονικών εξαρτημάτων μπορούμε να αναφέρουμε τόσο τις αντιστάσεις που είναι απαραίτητες να χρησιμοποιηθούν όσο και τους πυκνωτές. [9]

Ως αξιόπιστους παράγοντες στην διαδικασία ανάπτυξης ενός ολοκληρωμένου κυκλώματος τόσο στη φάση του σχεδιασμού όσο και στη φάση της κατασκευής θεωρείται η εκάστοτε εταιρία σχεδιασμού. Όπως έχουμε ήδη αναφέρει οποιαδήποτε εταιρία σχεδιασμού αναλαμβάνει ένα πλήθος λειτουργιών και ενεργειών για να ολοκληρωθεί η διαδικασία ανάπτυξης του IC. Ως παραδείγματα αυτών των ενεργειών μπορούμε να αναφέρουμε τα εξής, σχεδιασμό προδιαγραφών, RTL σχεδιασμός της τελικής διάταξης καθώς και τη σχεδίαση της netlist. [1]

Εκτός από τους αξιόπιστους παράγοντες που όπως έχουμε αναφέρει είναι η εταιρίες σχεδιασμού, υπάρχουν επίσης και αναξιόπιστοι παράγοντες κατά τη διαδικασία ανάπτυξης των ολοκληρωμένων κυκλωμάτων. Τέτοιου είδους αναξιόπιστοι παράγοντες είναι λόγου χάριν τα εργοστάσια τρίτων προμηθευτών. Τα συγκεκριμένα εργοστάσια αναλαμβάνουν με τη σειρά τους διάφορες ενέργειες για την επιτυχημένη ολοκλήρωση των ICs. Ως παράδειγμα μπορούμε να αναφερθούμε τόσο στην κατασκευή, όσο και στην συναρμολόγηση και τον τελικό έλεγχο της πλακέτας. Συνήθως τις ενέργειες αυτές τις αναλαμβάνουν τα συγκεκριμένα εργοστάσια διότι δεν είναι σε θέση οι εταιρίες σχεδιασμού να τις εκτελέσουν με απόλυτη επιτυχία.

Κεφάλαιο 2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Οι κακόβουλες επιθέσεις υλικού γνωστές ως Hardware Trojan υπάρχουν εδώ και μερικά χρόνια. Προβληματίζουν ιδιαίτερα τους ερευνητές του συγκεκριμένου κλάδου και τους σχεδιαστές του υλικού. Για το λόγο αυτό, τα τελευταία χρόνια οι επιθέσεις Hardware Trojan έχουν μελετηθεί εκτενώς από τους επιστήμονες. Σκοπός της συγκεκριμένης παρατεταμένης μελέτης είναι να αποφευχθούν όσο το δυνατόν περισσότερο οι κακόβουλες συνέπειες που έχει σε ένα υλικό καθώς και στη φήμη της εταιρίας που δέχεται μια επίθεση Hardware Trojan. Κατανοώντας πλήρως και μελετώντας τον συγκεκριμένο κλάδο από την αρχή της εμφάνισής τους μέχρι και σήμερα, οι επιστήμονες προσπαθούν να ελαττώσουν στο έπακρο τις επιθέσεις.

2.1 Ιστορική εξέλιξη Hardware Trojan

Είναι ιδιαίτερα σημαντικό να αναφερθούμε στην ιστορική εξέλιξη των επιθέσεων υλικού Trojan καθώς και πότε οι συγκεκριμένες κακόβουλες επιθέσεις έφτασαν στο προσκήνιο. Την τελευταία δεκαετία οι βιομηχανίες ολοκληρωμένων κυκλωμάτων έχουν θορυβηθεί ιδιαίτερα από την εμφάνιση των κακόβουλων επιθέσεων στο λογισμικό. Αποτέλεσε για τους ίδιους ένα συνεχώς αναδυόμενο πρόβλημα που αφορά την ασφάλεια. Τα περιστατικά που έχουν καταγραφεί τα τελευταία χρόνια από επιθέσεις υλικού, έρχονται στο φως για να επιβεβαιώσουν τις αρνητικές επιπτώσεις για τις οποίες ανησυχούν δικαίως οι επιστήμονες.

Η πρώτη έρευνα που δημοσιεύθηκε γύρω από το πολυσυζητημένο στις μέρες μας θέμα των επιθέσεων Hardware Trojan ήταν το χρονική περίοδο του 2007 από τον Agrawal. [4]. Από αυτή την πρώτη έρευνα έως και σήμερα τα Hardware Trojan έχουν αναπτυχθεί σε πολύ μεγάλο βαθμό. Μέσα σε αυτό το χρονικό διάστημα έχουν διεξαχθεί πάρα πολλές σε αριθμό έρευνες γύρω από αυτό το θέμα και ιδιαίτερα στον τρόπο με τον οποίο μπορεί να ανιχνευθεί μια τέτοιου είδους επίθεση υλικού – Hardware Trojan HT. Οι κακόβουλες επιθέσεις Hardware Trojan εκτός από τον κλάδο της βιομηχανίας υλικού απασχόλησε επίσης τον στρατό, την εκπαίδευση και πολλούς ακόμα τομείς από την εμφάνισή τους μέχρι και σήμερα.

Κατά καιρούς έχουν καταγραφεί ορισμένες προσπάθειες αποφυγής των επιθέσεων υλικού HT, οι οποίες στόχευαν είτε στον έλεγχο μιας συσκευής είτε στην απόκτηση προσωπικών

πληροφοριών είτε ακόμα και στην ολοκληρωτική καταστροφή ενός ολοκληρωμένου συστήματος.

Τον Σεπτέμβριο του 2007, πραγματοποιήθηκε με επιτυχία μια αεροπορική επίθεση εναντίον του πυρηνικού αντιδραστήρα της Συρίας. Αξιοσημείωτο ήταν το γεγονός ότι το προηγμένο σύστημα της Συρίας που είναι υπεύθυνο για την αεράμυνα, δεν απάντησε καθόλου σε όλη της διάρκεια της επίθεσης. Την επόμενη χρονιά και συγκεκριμένα το 2008, ο Adee υποστήριξε ότι το προηγμένο σύστημα αεράμυνας δεν απάντησε κατά την επίθεση που υπέστη λόγω της απενεργοποίησης του από έναν ενσωματωμένο διακόπτη. Ο συγκεκριμένος διακόπτης που ήταν υπεύθυνος για την απενεργοποίησή του, ενεργοποιήθηκε από απόσταση. [4]

Την χρονική στιγμή του 2016, ο Yang ανακάλυψε ένα σχετικά μικρό Hardware Trojan. Το συγκεκριμένο κακόβουλο HT ονομάστηκε A2. Το Hardware Trojan A2 εκτελούσε μια επίθεση κλιμάκωσης προνομίων στον επεξεργαστή OR1200. Αυτό συνέβαινε μέσω της εκτέλεσης ενός πλήθους από φαινομενικά ακίνδυνες εντολές. [4]. Τέτοιου είδους επιθέσεις στο υλικό, όπως αυτή που περιγράψαμε προηγουμένως είναι πολύ δύσκολο να εντοπιστούν από τους ειδικούς.

Το 2018, και συγκεκριμένα τον Ιανουάριο της χρονιάς αυτής, το Ίδρυμα Ελεύθερου Λογισμικού – Free Software Foundation, έκανε μια σημαντική ανακάλυψη. Η αποκάλυψη αφορούσε τους υπολογιστές Intel όπου είχαν ένα ενσωματωμένο υποσύστημα, με την ονομασία Intel Management Engine. Το υποσύστημα είναι ικανό να αναλάβει πλήρη έλεγχο του υπολογιστή. Επίσης, μπορεί να έχει πρόσβαση και στην κύρια μνήμη του εκάστοτε υπολογιστή. Η ύπαρξη του συγκεκριμένου υποσυστήματος στους υπολογιστές μπορεί να έχει σοβαρές επιπτώσεις όσον αφορά την ασφάλεια των χρηστών του. Από την άλλη μεριά, ο εκάστοτε χρήστης δεν μπορεί να καταλάβει την ύπαρξή του μέσα στον υπολογιστή, ούτε μπορεί με κάποιο τρόπο να το απενεργοποιήσει. Για κάθε χρήστη των συγκεκριμένων υπολογιστών, κάτι τέτοιο μπορεί να θεωρηθεί και να χαρακτηριστεί ως επίθεση Hardware Trojan. [4]

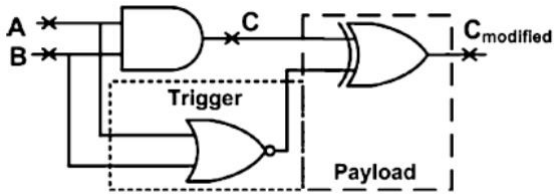
Από την δεκαετία του 2000 έχουν ξεκινήσει μελέτες για την αντιμετώπιση των επιθέσεων υλικού. Όμως στις αρχές του έτους 2014 οι συγκεκριμένες μελέτες έφτασαν στο απόγειο τους. Πιο συγκεκριμένα, στις Ηνωμένες πολιτείες της Αμερικής λήφθηκε η απόφαση από

το συμβούλιο Semiconductor Research Council (SRC) να δημιουργηθεί και να χρηματοδοτηθεί το Trustworthy and Secure Semiconductors and Systems (T3S). Αξιοσημείωτο είναι το ποσό της επένδυσης για την έρευνα των επιθέσεων Trojan που αγγίζει το ποσό των 9 εκατομμυρίων δολαρίων. [14]

Το Μάιο της ίδιας χρονιάς, το συμβούλιο SRC οργάνωσε μια συγκέντρωση, στην οποία συμμετείχε τόσο ο ακαδημαϊκός κόσμος όσο και η βιομηχανικός προκειμένου να ληφθούν απόψεις για την κατεύθυνση που θα πρέπει να ακολουθήσει η έρευνα για τα αντίμετρα των επιθέσεων Hardware Trojan. [14]

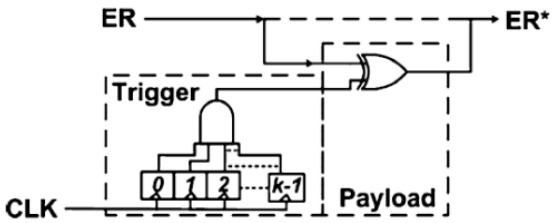
2.2 Παραδείγματα

Προκειμένου να γίνει πλήρως κατανοητή η έννοια των Hardware Trojan, θα ήταν σκόπιμο να αναφερθούμε στη δομή που μπορεί να έχουν μέσα σε ένα ολοκληρωμένο κύκλωμα με τη βοήθεια ορισμένων παραδειγμάτων. Στη συνέχεια της υπό ενότητας αυτής θα περιγράψουμε μερικά χαρακτηριστικά παραδείγματα.



Εικόνα 3 - Χαρακτηριστικό παράδειγμα Hardware Trojan [3]

Στην παραπάνω εικόνα μπορεί κανείς να παρατηρήσει ένα συνδυαστικό Trojan. Το συγκεκριμένο παράδειγμα διαθέτει ως μηχανισμό ενεργοποίησης μια πύλη NOR. Ενώ το ρόλο του ωφέλιμου φορτίου – payload κατέχει η πύλη XOR. Αυτό το Trojan που αναπαριστάνετε στην παραπάνω εικόνα μπορεί να ενεργοποιηθεί μόνο όταν πραγματοποιηθεί μια συγκεκριμένη συνθήκη. Πιο αναλυτικά, η συνθήκη ενεργοποίησης είναι όταν A=0 και B=0. Όταν οι συγκεκριμένες τιμές των A,B εμφανιστούν στην πύλη NOR, ενεργοποιείται το συγκεκριμένο Trojan. Αυτό έχει ως αποτέλεσμα το ωφέλιμο φορτίο payload να προκαλεί αλλοίωση στην έξοδο από C σε Cmodified. [3]



Εικόνα 4 - Δεύτερο χαρακτηριστικό παράδειγμα Hardware Trojan [3]

Στην Εικόνα 4 αναπαριστάνετε το δεύτερο χαρακτηριστικό παράδειγμα ενός Hardware Trojan. Πρόκειται για ένα συγχρονισμένο ακολουθιακό Hardware Trojan. Όπως μπορεί κανείς να παρατηρήσει το συγκεκριμένο Hardware Trojan διαθέτει έναν μετρητή που βοηθάει στην ενεργοποίησή του. Πιο συγκεκριμένα, ως μηχανισμό ενεργοποίησης trigger διαθέτει έναν μετρητή αποτελούμενο από k bit καθώς και μια πύλη AND. Από την άλλη μεριά, όπως μπορεί κανείς να παρατηρήσει στην εικόνα υπάρχει μια πύλη XOR, η οποία έχει το ρόλο του ωφέλιμου φορτίου – Payload. Η ενεργοποίηση του συγκεκριμένου Trojan που αναπαριστάνετε στην παραπάνω εικόνα πραγματοποιείται όταν φτάσει μια προκαθορισμένη τιμή 2k-1. Η ενεργοποίηση αυτού του Hardware Trojan έχει ως αποτέλεσμα να αντιστρέφεται η έξοδος. Η αναμενόμενη έξοδος χωρίς την ύπαρξη του Hardware Trojan θα ήταν η έξοδος ER, εν αντιθέσει με την ύπαρξη και την ενεργοποίηση του Trojan όπου η έξοδος πλέον θα είναι η αντεστραμμένη έξοδος ER*. [3]

2.3 Έρευνες για Hardware Trojan

Από την πρώτη στιγμή που εμφανίστηκε στο προσκήνιο ο όρος Hardware Trojan μέχρι και σήμερα έχουν πραγματοποιηθεί πολλές έρευνες και επιστημονικές μελέτες γύρω από το θέμα των κακόβουλων επιθέσεων στο υλικό και στους τρόπους με τους οποίους μπορούν να αυτές να ανιχνευθούν. Οι τρόποι με τους οποίους ανιχνεύονται και αντιμετωπίζονται τέτοιου είδους επιθέσεις θα αναφερθεί και θα αναλυθεί περαιτέρω σε επόμενα κεφάλαια.

Ο Swarup Bhunia πραγματοποίησε μελέτη και περαιτέρω ανάλυση για τα μοντέλα και τις ταξινομήσεις που υπάρχουν για τις επιθέσεις Hardware Trojan. Επίσης, ανέλυσε τις προσεγγίσεις όσον αφορά την προστασία του υλικού από τέτοιου είδους επιθέσεις. Οι Tehranipoor και Koushanfar πραγματοποίησαν έρευνες για τις τεχνικές ανίχνευσης επιθέσεων υλικού Trojan. Πιο συγκεκριμένα, ανέλυσαν μηχανισμούς ανίχνευσης που ήδη

υπάρχουν καθώς και μεθοδολογίες DFS. Ο Chakraborty μελέτησε τις τεχνικές ανίχνευσης Hardware Trojan τελευταίας τεχνολογίας. [1]

Οι έρευνες που αναφέρθηκαν προηγουμένως έχουν πραγματοποιηθεί χρονικά πριν το 2014. Υπάρχουν επίσης πολλές έρευνες που έχουν λάβει χώρα τα τελευταία έξι χρόνια σχετικά με τις κακόβουλες επιθέσεις υλικού. Από την άλλη πλευρά, υπάρχουν πολλοί ερευνητές που στηρίζουν τις έρευνες και τις μελέτες τους στην κατανάλωση της ενέργειας. Με τον τρόπο αυτό είναι εφικτή η κατασκευή των λεγόμενων αποτυπωμάτων των ολοκληρωμένων κυκλωμάτων. Η έννοια αυτή είναι ευρέως γνωστή επίσης με τον όρο fingerprints. Η αποτύπωση αυτή βασίζεται στις παραμέτρους των side – channel. Σύμφωνα με τις έρευνες που έχουν πραγματοποιηθεί γύρω από το θέμα των αποτυπωμάτων των ολοκληρωμένων κυκλωμάτων, οι ερευνητές συμπέραναν ότι η συγκεκριμένη μέθοδος είναι από τις πλέον διαδεδομένες και πολύ χρησιμοποιούμενες μεθόδους αξιολόγησης. Ο λόγος που κατατάσσετε στις καλύτερες μεθόδους αξιολόγησης είναι διότι έχει τη δυνατότητα να αποφανθεί εάν ένα ολοκληρωμένο κύκλωμα περιέχει μια επίθεση Trojan. Δεν ήταν λίγοι οι ερευνητές που βασίστηκαν στην παραπάνω ιδέα και προσπάθησαν να την εξελίξουν με διάφορους τρόπους, χρησιμοποιώντας μετρήσεις side -channel. Ως παράδειγμα μπορούμε να αναφέρουμε τα σήματα μετάβασης παροχής ενέργειας, τη θερμοκρασία καθώς και τα ρεύματα διαρροής. Πολλοί ήταν οι ερευνητές που στηρίχθηκαν σε μετρήσεις απόδοσης ενέργειας καθώς και σε τυχόν διαφορές στατιστικών ανάμεσα στο πρώτο και στο τροποποιημένο σύστημα. [4]

Κεφάλαιο 3 ΑΝΑΛΥΣΗ ΜΕΘΟΔΩΝ ΕΠΙΘΕΣΕΩΝ

Όπως έχουμε ήδη αναφέρει σε προηγούμενα κεφάλαια, οι επιθέσεις Hardware Trojan είναι κακόβουλες τροποποιήσεις, οι οποίες υφίστανται στο υλικό ενός κυκλώματος. Οι τροποποιήσεις αυτές τοποθετούνται από ανταγωνιστές κυρίως με σκοπό να βλάψουν τη λειτουργία του εκάστοτε υλικού και κατ' επέκταση τη φήμη της εταιρίας. Τέτοιου είδους επιθέσεις στο υλικό είναι ανεπιθύμητες από τον εκάστοτε σχεδιαστή του. Ένα Trojan μπορεί να έχει οποιαδήποτε μορφή και αποτελεί μια σκόπιμη εισαγωγή κυρίως από έναν αντίπαλο. Για το λόγο αυτό, η θέση ενεργοποίησης του εκάστοτε trojan δεν είναι γνωστή από τον σχεδιαστή του υλικού.

Έχει παρατηρηθεί ότι τα διάφορα είδη των Hardware Trojan έχουν τρία κοινά χαρακτηριστικά. Πιο συγκεκριμένα όλα τα είδη Trojan χαρακτηρίζονται από κακόβουλη πρόθεση. Τα διάφορα Trojans έχουν πάντα ως σκοπό να προκαλέσουν κακόβουλες τροποποιήσεις στο εκάστοτε υλικό στο οποίο τοποθετούνται. Ένα δεύτερο χαρακτηριστικό που έχουν όλες οι επιθέσεις Trojan είναι η δυνατότητα τους ως προς την αποφυγή εντοπισμού. Πιο συγκεκριμένα, κάθε επιτυχημένο Hardware Trojan θα πρέπει να έχει σχεδιαστεί με τέτοιο τρόπο ώστε να μην είναι δυνατή η ανίχνευσή του από τους σχεδιαστές του προς επίθεση υλικού. Ένα τρίτο και τελευταίο χαρακτηριστικό που διακρίνει όλες τις επιθέσεις υλικού είναι η σπανιότητα ενεργοποίησης. Ο στόχος των επιθέσεων είναι να μην ενεργοποιούνται κατά τη διάρκεια της διαδικασίας των δοκιμών που εκτελούνται από τους σχεδιαστές του εκάστοτε υλικού. Οι δημιουργοί των Trojan επιθυμούν να μην ενεργοποιείται στις δοκιμές που πραγματοποιούνται αλλά όποτε το κρίνουν οι ίδιοι. Σκοπός τους είναι να μην ανιχνεύεται το Trojan από τους σχεδιαστές.

Τα Trojan έχουν τη δυνατότητα να εισαχθούν από τους αντιπάλους σε ολοκληρωμένα κυκλώματα - Integrated Circuit, IC, όπως είναι λόγου χάριν τα ολοκληρωμένα κυκλώματα ελέγχου, οι αισθητήρες, οι μονάδες μνήμης καθώς και προγράμματα εισόδου – εξόδου. Ένας ακόμα τρόπος εισαγωγής των επιθέσεων υλικού Trojan είναι να εισαχθούν σε ενσωματωμένα συστήματα, όπως είναι οι επεξεργαστές. Επιπλέον, θα μπορούσαν να εισαχθούν μέσω κρυπτογραφικών μηχανών σε Systems on a Chip- SoCs.

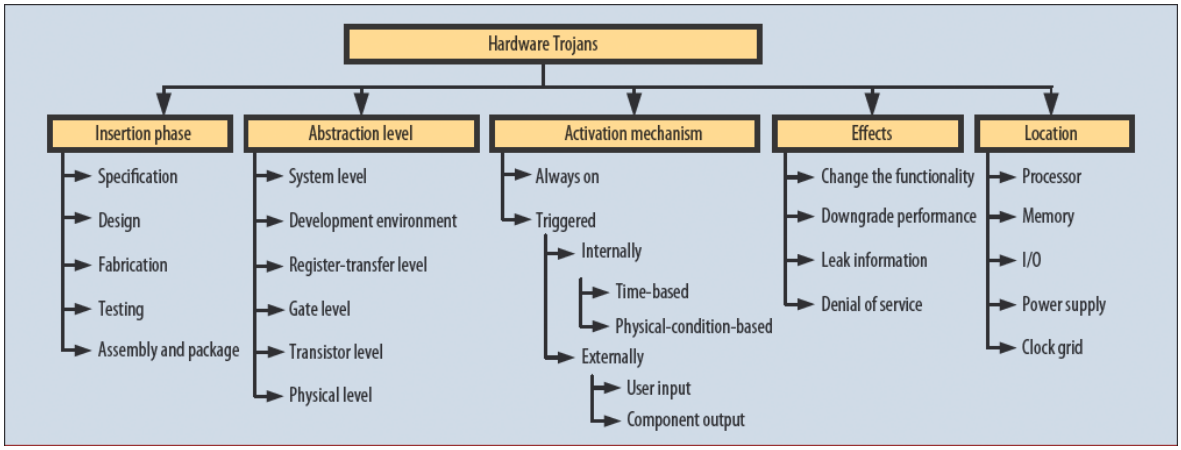
Με οποιονδήποτε τρόπο και να πραγματοποιηθεί η εισαγωγή του Trojan στο υλικό, ο σκοπός παραμένει ο ίδιος. Ο σκοπός του αντιπάλου είναι να αποδυναμώσει ή να

απενεργοποιήσει τα στοιχεία που αφορούν την ασφάλεια του συστήματος που δέχεται την επίθεση. Με τον όρο αντίπαλος αναφερόμαστε σε κάθε οντότητα που πιθανόν να εμπλέκεται στη διαδικασία σχεδιασμού, κατασκευής και δοκιμής ενός ολοκληρωμένου κυκλώματος. Με τον συγκεκριμένο όρο δεν αναφερόμαστε αποκλειστικά σε ανθρώπινη οντότητα. Αντίπαλος θα μπορούσε να χαρακτηριστεί και ο χώρος σχεδιασμού, ο ηλεκτρονικός σχεδιασμός με τη βοήθεια του υπολογιστή – EDA καθώς και τα εργαλεία υποβοηθούμενης σχεδίασης CAD. [1]. Διακρίνονται διάφοροι τύποι και μοντέλα επιθέσεων Hardware Trojan. Στο συγκεκριμένο κεφάλαιο θα πραγματοποιηθεί περαιτέρω μελέτη και ανάλυση των μεθόδων επιθέσεων Trojan.

3.1 Ταξινόμηση Hardware Trojan

Προκειμένου να γίνει πλήρως κατανοητή η διαδικασία μιας επίθεσης υλικού Hardware Trojan, είναι σκόπιμο να αναφερθούμε και να κατανοήσουμε σε βάθος τους διαφορετικούς τύπους Trojan που έχουν μελετηθεί από τους ειδικούς του κλάδου. Η ταξινόμηση των Trojan βασίζεται στα επιμέρους χαρακτηριστικά που διαθέτουν. Είναι ιδιαίτερα σημαντικό να κατανοηθούν, διότι αποτελούν τη βάση για την περαιτέρω αξιολόγηση και αποτελεσματικότητα των μηχανισμών που στοχεύουν στην ανίχνευση των Trojans.

Η πρώτη δημοσιευμένη ταξινόμηση των Hardware Trojan πραγματοποιήθηκε το 2008. Η συγκεκριμένη ταξινόμηση αποτελούνταν από έξι βασικά χαρακτηριστικά. Μεταξύ άλλων υπήρχαν τα φυσικά χαρακτηριστικά καθώς και η ενεργοποίηση. Με την πάροδο των χρόνων και καθώς οι τεχνολογίες συνεχώς εξελίσσονται με ραγδαίους ρυθμούς τα Hardware Trojans γίνονται όλο και πιο περίπλοκα. [8, ch.2] Για το λόγο αυτό η ταξινόμηση εξελίχθηκε με αποτέλεσμα να υπάρχουν πλέον εννέα χαρακτηριστικά για τρείς κατηγορίες έναντι των έξι χαρακτηριστικών που προϋπήρχαν. Από τη χρονική στιγμή του 2007 μέχρι και σήμερα, υπήρξαν πολλές μελέτες και έρευνες που στόχευαν στην ιδανική και πλέον αποτελεσματική κατηγοριοποίηση των Hardware Trojans. Η πιο ολοκληρωμένη ταξινόμηση βασίζεται σε δύο βασικά κριτήρια και αποτελείται από πέντε βασικές κατηγορίες.



Εικόνα 5 - Πέντε ολοκληρωμένες κατηγορίες ταξινόμησης Hardware Trojan [15]

Στην Εικόνα 5 που φαίνεται προηγουμένως, μπορεί κανείς να παρατηρήσει τις πέντε ολοκληρωμένες κατηγορίες ταξινόμησης των Hardware Trojans. Είναι σημαντικό να αναφερθούμε και να αναλύσουμε περαιτέρω τις πέντε ολοκληρωμένες αυτές κατηγορίες. Αυτή η ανάλυση βρίσκεται στις επόμενες υπό ενότητες που υπάρχουν στη συνέχεια.

3.1.1 Φάση εισαγωγής – Insertion Phase

Όπως μπορεί κανείς να δει από την Εικόνα 7, η πρώτη κατηγορία είναι αυτή της εισαγωγής – Insertion phase. Στην κατηγορία αυτή, το υλικό είναι ιδιαίτερα ευαίσθητό και κατ' επέκταση ευάλωτο σε κακόβουλες τροποποιήσεις. Στη φάση της εισαγωγής συμπεριλαμβάνονται τα στάδια του σχεδιασμού και της κατασκευής των υλικών – hardware. Πιο συγκεκριμένα, καθορίζονται τα χαρακτηριστικά και οι προδιαγραφές όσον αφορά τον σχεδιασμό μέχρι και την διαδικασία συναρμολόγησης του υλικού στην εκάστοτε πλακέτα του κυκλώματος. [8, ch.2] Στη συνέχεια παρουσιάζονται οι επιμέρους ευπάθειες στη διαδικασία εισαγωγής ενός Trojan.

- **Προδιαγραφές – Specification**. Ο εκάστοτε αντίπαλος έχει τη δυνατότητα να αλλάζει προδιαγραφές για το σύστημα. Αυτές οι αδύναμες προδιαγραφές κατασκευάζονται σκόπιμα από την πλευρά των αντιπάλων. Το γεγονός αυτό, έχει ως συνέχεια, να κλονίζεται η αξιοπιστία της διαδικασίας σχεδιασμού, θέτοντας τη συσκευή ευάλωτη όσον αφορά τη διακίνηση προσωπικών και ευαίσθητων δεδομένων. [8, ch.2]

- **Σχεδιασμός – Design**. Μπορεί ο σχεδιασμός να πραγματοποιείται σε εσωτερικό επίπεδο, παρ' όλα αυτά μπορούν επίσης να επηρεάσουν το ολοκληρωμένο κύκλωμα η χρήση τόσο αναξιόπιστων εργαλείων όσο και μη αξιόπιστων βιβλιοθηκών και IPs τρίτων προμηθευτών. [15]
- **Κατασκευή – Fabrication**. Την αξιοπιστία του ολοκληρωμένου κυκλώματος μπορεί να την επηρεάσει επίσης ένα αναξιόπιστο είτε εργοστάσιο κατασκευής είτε ομάδα προσωπικού. Υπάρχει πιθανότητα να επηρεαστεί τόσο από την αφαίρεση όσο και από την προσθήκη εξαρτημάτων. [8]
- **Τεστ – Testing.** Στη διαδικασία των δοκιμαστικών τεστ, μειώνονται οι πιθανότητες ο κάθε αντίπαλος να καταφέρει να τροποποιήσει τη δομή και τη σύσταση των ολοκληρωμένων κυκλωμάτων. Παρ' όλα αυτά ο αντίπαλος θα μπορούσε να τροποποιήσει τα κυκλώματα δοκιμής ή τα αποτελέσματα, ώστε να καλυφθούν τα Trojan. [8] Τα δοκιμαστικά τεστ αποτελούν το τελευταίο βήμα για τον σχεδιασμό των ολοκληρωμένων κυκλωμάτων. Συμπεραίνουμε λοιπόν ότι αυτό το τελευταίο βήμα αποτελεί και την τελευταία προσπάθεια για τους σχεδιαστές να καταφέρουν να βρουν τυχόν επιθέσεις υλικού Trojan προτού ξεκινήσει η διαδικασία της ανάπτυξης, η οποία αναλύεται στη συνέχεια.
- **Συναρμολόγηση & Συσκευασία - Assembly and Package.** Ένας πιθανός αντίπαλος μπορεί να προκαλέσει τροποποιήσεις στο αυθεντικό σχέδιο προκειμένου να δημιουργήσει δυσλειτουργίες, ακόμα και να δημιουργηθούν διαρροές πληροφοριών. [15]

3.1.2 Επίπεδο αφαίρεσης – Abstraction Level

Η δεύτερη κατηγορία ονομάστηκε Επίπεδο Αφαίρεσης - Abstraction Level. Η συγκεκριμένη κατηγορία απαρτίζεται από τα διαφορετικά στάδια ανάπτυξης του υλικού. Τα στάδια που περιγράφονται στο abstraction level είναι στάδια πριν την τελική κατασκευή του hardware. Εμβαθύνει από τις διαστάσεις και τις τελικές θέσεις των στοιχείων που βρίσκονται στο εσωτερικό τμήμα των κυκλωμάτων μέχρι τις διασυνδέσεις και τα πρωτόκολλα επικοινωνίας που είναι απαραίτητα στη δημιουργία των ολοκληρωμένων κυκλωμάτων – IC. [8] Στη συνέχεια αναλύονται περαιτέρω τα πιθανά σημεία εισαγωγής ενός Hardware Trojan όσον αφορά το επίπεδο αφαίρεσης.

- **Σύστημα – System level.** Ένα Hardware Trojan μπορεί να τοποθετηθεί σε επίπεδο συστήματος. Πιο συγκεκριμένα, όταν ένας αντίπαλος επεμβαίνει με την προσθήκη Trojan στο system level μπορεί να προκαλέσει τροποποιήσεις στις προδιαγραφές της λειτουργίας, τις διεπαφές καθώς και στα πρωτόκολλα του αρχικού σχεδίου του αντίστοιχου προς επίθεση υλικού. [15]
- **Περιβάλλον ανάπτυξης – Development environment.** Χρησιμοποιώντας αναξιόπιστα εργαλεία, αυξάνεται ο κίνδυνος να υπάρξουν μυστικές και άγνωστες λειτουργίες. Αυτό έχει ως αποτέλεσμα οι σχεδιαστές των υλικών να κατασκευάζουν ολοκληρωμένα κυκλώματα που θα έχουν υποστεί κάποιου είδους επίθεση Trojan. [8].
- **Επίπεδο μεταφοράς - Register - transfer level.** Αξιοσημείωτο είναι το γεγονός ότι ένα Hardware Trojan μπορεί να είναι αλλαγές σε ένα από τα αυθεντικά τμήματα του κώδικα σε επίπεδο Register- Transfer -RT. Πιθανές απειλές στο συγκεκριμένο επίπεδο θα μπορούσε να είναι ένας προμηθευτής κώδικα ο οποίος να θεωρείται μη αξιόπιστος, προσθέτοντας στο ολοκληρωμένο κύκλωμα ένα Hardware Trojan.
- **Πύλη – Gate Level.** Στο επίπεδο Πύλης υπάρχει επίσης η πιθανότητα για την εισαγωγή μια απειλής Trojan. Πιο συγκεκριμένα, ως επίθεση Trojan μπορεί να θεωρηθεί είτε η αφαίρεση είτε η εισαγωγή πυλών στην πρωταρχική netlist. Σε αυτό το επίπεδο τόσο οι αντίπαλοι του σχεδιασμού όσο και οι μη αξιόπιστοι προμηθευτές έχουν τη δυνατότητα προσθήκης Trojan στο αντίστοιχο υλικό. Ως παράδειγμα τέτοιου Hardware Trojan μπορούμε να αναφέρουμε ένα συγκριτή ο οποίος αποτελείται από πύλες XOR με σκοπό την παρακολούθηση των σημάτων του ολοκληρωμένου κυκλώματος. [15]
- **Τρανζίστορ - Transistor level.** Με την εισαγωγή των τρανζίστορ στα ολοκληρωμένα κυκλώματα μεγεθύνεται σε πολύ μεγάλο βαθμό η πιθανότητα ύπαρξης διαρροών. Το γεγονός αυτό, ευνοεί τους αντιπάλους διότι είναι πιο εύκολο να αποκτήσουν περισσότερες γνώσεις όσον αφορά την εσωτερική κατάσταση ασφαλείας. Στο συγκεκριμένο επίπεδο, οι πιθανές αιτίες προσθήκης ενός Hardware Trojan μπορούν να προκληθούν τόσο από τους αντίπαλους στη φάση του σχεδιασμού όσο και από αναξιόπιστα εργαλεία.
- **Φυσική Διάταξη – Physical Level.** Οι παράμετροι που παρουσιάζουν τα διάφορα εξαρτήματα που απαρτίζουν ένα ολοκληρωμένο κύκλωμα, είναι ευάλωτες ακόμα

και όταν πραγματοποιηθεί η προβλεπόμενη διάταξη. Πιο συγκεκριμένα, ένας αντίπαλος μπορεί να επέμβει και να τροποποιήσει παραδείγματος χάριν τα μήκη των τρανζίστορ που υπάρχουν στο κύκλωμα, ακόμα και τα πλάτη των καναλιών. Υπάρχει επίσης η πιθανότητα τροποποίησης των καλωδίων από τους αντιπάλους. Αυτό έχει ως αποτέλεσμα να προκληθούν προβλήματα όσον αφορά τη λειτουργία καθώς και σημαντικές διαρροές. [15]

3.1.3 Μηχανισμός ενεργοποίησης - Activation mechanism.

Η τρίτη κατηγοριοποίηση των Hardware Trojan αφορά στο λεγόμενο activation mechanism. Πρόκειται για τον μηχανισμό ενεργοποίησης. Πιο συγκεκριμένα, αποτελείται από τα μέσα με τα οποία ενεργοποιούνται τα Trojans. Στην κατηγορία αυτή, περιλαμβάνονται παραδείγματος χάριν Trojan, τα οποία προκειμένου να ενεργοποιηθούν χρειάζονται συγκεκριμένους κανόνες. [15]

- **Πάντα ενεργοποιημένο - Always on.** Στη συγκεκριμένη κατηγορία το Hardware Trojan που έχει τοποθετηθεί στο υλικό είναι πάντα ενεργοποιημένο. Το γεγονός αυτό έχει ως αποτέλεσμα το αντίστοιχο κύκλωμα που υφίσταται την επίθεση να επηρεάζεται συνεχώς από το αντίστοιχο Trojan. Στην περίπτωση αυτή, το Hardware Trojan απαρτίζεται αποκλειστικά και μόνο από το Payload. [15]
- **Εσωτερική ενεργοποίηση - Triggered Internally.** Στην κατηγορία της εσωτερικής ενεργοποίησης, το Hardware Trojan που έχει εισαχθεί στο υλικό ενεργοποιείται μόνο όταν πραγματοποιηθεί μια καθορισμένη εσωτερική κατάσταση στο ολοκληρωμένο κύκλωμα. Ως παράδειγμα μπορούμε να αναφερθούμε στην ύπαρξη ενός εσωτερικού μετρητή στο κύκλωμα, ο οποίος μπορεί να προκαλέσει την ενεργοποίηση του Hardware trojan όταν και μόνο όταν το ρολόι του μετρητή ξεπεράσει μια συγκεκριμένη, προκαθορισμένη τιμή. [15]
- **Εξωτερική ενεργοποίηση - Triggered Externally.** Ένα Hardware Trojan μπορεί επίσης να ενεργοποιηθεί από έναν εξωτερικό παράγοντα. Πιο συγκεκριμένα, ο αντίπαλος έχοντας γνώση για την ύπαρξη του Trojan στο συγκεκριμένο σύστημα μπορεί να το ενεργοποιήσει από απόσταση. [15]

3.1.4 Επιπτώσεις - Effects

Η τέταρτη κατηγοριοποίηση ονομάστηκε από τους ειδικούς του κλάδου Effects. Πρόκειται για το ανεπιθύμητο αποτέλεσμα που μπορεί να προκύψει από την απόκριση των Hardware Trojans. Στο σημείο αυτό, μπορούν να τοποθετηθούν από αντιπάλους μικρά σφάλματα. Τα σφάλματα αυτά, είναι ιδιαίτερα δύσκολο να εντοπιστούν από τους αρμόδιους. Επίσης, στην κατηγορία αυτή, μπορεί να προκληθεί πλήρης καταστροφή του αντίστοιχου υλικού. [15] Είναι σημαντικό να αναφέρουμε ότι ένα Hardware Trojan μπορεί να προκαλέσει βλάβη στην λειτουργία του υλικού και στην αξιοπιστία του έως και την πλήρως καταστροφή του. [14]

- **Αλλαγή λειτουργίας - Change the functionality.** Με την ενεργοποίηση ενός Hardware Trojan στο προς επίθεση υλικό, παρατηρούνται αλλαγές στις λειτουργίες του. Οι αλλαγές αυτές μπορεί να είναι είτε προσθήκες νέων λειτουργιών που καθορίζονται από το αντίστοιχο Trojan είτε αφαίρεση κάποιας από τις αρχικές λειτουργίες του. [15]
- **Μείωση αξιοπιστίας - Downgrade performance.** Μια ακόμα ανεπιθύμητη επίπτωση που μπορεί να προκαλέσει ένα Hardware Trojan στο υλικό είναι η μείωση της αξιοπιστίας του. Αυτό επιτυγχάνεται υποβαθμίζοντας την απόδοση του ολοκληρωμένου κυκλώματος. [15]
- **Διαρροή δεδομένων - Leak information.** Τα Hardware Trojan έχουν σχεδιαστεί και κατασκευαστεί με τέτοιο τρόπο ώστε να έχουν τη δυνατότητα να προκαλούν διαρροή κλειδιών ή κρυπτογραφημένων κειμένων που αφορούν τα ολοκληρωμένα κυκλώματα. [15]
- **Άρνηση Παροχής υπηρεσιών - Denial of service.** Μια τελευταία αλλά εξίσου σημαντική επίπτωση από την χρήση των Trojan είναι ότι δεν μπορεί το προς επίθεση ολοκληρωμένο κύκλωμα να λειτουργήσει με σωστό τρόπο, όπως προβλέπουν οι σχεδιαστές του. Για να γίνει περισσότερο κατανοητή η δυσλειτουργία που προκαλούν τα Trojan είναι απαραίτητο να αναφέρουμε ένα χαρακτηριστικό παράδειγμα. Ως τέτοιου είδους παράδειγμα μπορούμε να αναφέρουμε ένα στρατιωτικό Radar το οποίο με τη χρήση ενός Hardware Trojan δεν έχει πλέον τη δυνατότητα να εντοπίσει ορισμένες απειλές, τις οποίες υπό άλλες συνθήκες θα ήταν σε θέση να εντοπίσει.

3.1.5 Θέση - Location

Στην πέμπτη και τελευταία κατηγορία βρίσκεται η τοποθεσία – location. Η συγκεκριμένη κατηγορία περιγράφει το σημείο στο οποίο μπορεί να εισαχθεί ένα Hardware Trojan με φυσικό τρόπο. Στην κατηγορία αυτή μπορούν να ενταχθούν Trojans, τα οποία στοχεύουν σε μεμονωμένα στοιχεία του ολοκληρωμένου κυκλώματος μέχρι και σε σύνθετα στοιχεία του όπως είναι λόγου χάριν οι επεξεργαστές. [15] Στη συνέχεια αναλύονται περαιτέρω τα σημεία στα οποία μπορούν να τοποθετηθούν και να επηρεάσουν τα διάφορα Hardware Trojans.

- **Επεξεργαστές – Processor.** Ένα Trojan μπορεί να επηρεάσει τους επεξεργαστές ενός ολοκληρωμένου κυκλώματος. Πιο συγκεκριμένα, έχει τη δυνατότητα είτε να αφαιρέσει είτε να εισάγει οδηγίες των επεξεργαστών. Αυτό έχει ως αποτέλεσμα να εκτελούν διαφορετικές λειτουργίες προκαλώντας γενική δυσλειτουργία του κυκλώματος. [15]
- **Μνήμες – Memory .** Οι αντίπαλοι που εισάγουν ένα Trojan έχουν τη δυνατότητα να ελέγχουν τα διάφορα στοιχεία της μνήμης με αποτέλεσμα να λαμβάνουν πρόσβαση και να διαχειρίζονται ευαίσθητα προσωπικά δεδομένα, τα οποία βρίσκονται αποθηκευμένα στην αντίστοιχη συσκευή. [15]
- **I/O.** Ένα Trojan μπορεί επίσης να επηρεάσει τα Pins, γεγονός που μπορεί να προκαλέσει την τροποποίηση των σημάτων καθώς και την παρακολούθηση από τους αντιπάλους διαφόρων επικοινωνιών
- **Τροφοδοσία ρεύματος - Power supply.** Ένα επιπλέον τμήμα που μπορεί να επηρεάσει η προσθήκη και η ενεργοποίηση ενός Hardware Trojan είναι το δίκτυο τροφοδοσίας. Στην περίπτωση αυτή, ο εκάστοτε αντίπαλος έχει τη δυνατότητα να επηρεάζει την τάση και το ρεύμα της αντίστοιχης συσκευής. Κάτι τέτοιο έχει ως ανεπιθύμητη συνέπεια να μεγαλώνουν οι πιθανότητας διαρροής. Επίσης ανεπιθύμητη επίπτωση μπορεί να είναι και η δημιουργία αστοχιών. [15]
- **Ρολόι - Clock grid.** Με την τοποθέτηση ενός Trojan υπάρχει η πιθανότητα για τροποποίηση της συχνότητας του εκάστοτε ολοκληρωμένου κυκλώματος. Έχουν επίσης παρατηρηθεί αυξήσεις όσον αφορά το θόρυβο τους αντίστοιχου ρολογιού, γεγονός που δημιουργεί πολλές δυσκολίες στη λειτουργικότητα του. [15]

Συγκεκριμένα, μπορεί να πραγματοποιηθεί περαιτέρω μελέτη του θορύβου στο εκάστοτε ολοκληρωμένο κύκλωμα και να εντοπιστεί αναξιόπιστο υλικό Hardware Trojan [3, p. 23].

3.2 Ταξινόμηση με βάση το μηχανισμό ενεργοποίησης

Όπως έχουμε ήδη αναφέρει, τόσο οι τεχνικές όσο και τα Hardware Trojan γενικότερα θα πρέπει να παραμένουν μυστικές και άγνωστες ως προς τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων. Ο κύριος λόγος της μυστικότητας είναι για να γίνει όλο και πιο δύσκολη η ανίχνευσή τους από τους σχεδιαστές τόσο κατά τη διάρκεια των δοκιμών που πραγματοποιούνται κατά την επικύρωση του κώδικα όσο και κατά τη διάρκεια της κατασκευής του αντίστοιχου υλικού.

Αρχικά, πρέπει να αναφέρουμε και να περιγράψουμε περαιτέρω το συνδυαστικό μηχανισμό ενεργοποίησης. Στην συγκεκριμένη περίπτωση, το αντίστοιχο trigger του Hardware Trojan δεν απαρτίζεται από κανενός είδους μνήμης. Από την άλλη μεριά, η ενεργοποίηση του Trojan εξαρτάται από την εμφάνιση μιας συγκεκριμένης κατάστασης σε ορισμένους εσωτερικούς κόμβους του κυκλώματος. Οι καταστάσεις αυτές είναι δυαδικές τιμές (bits) που δεν μπορούν να εμφανιστούν υπό κανονικές συνθήκες στους κόμβους του ολοκληρωμένου κυκλώματος χωρίς την ύπαρξη του Hardware Trojan. Στον συνδυαστικό μηχανισμό ενεργοποίησης η διαδικασία ανίχνευσης ενός Hardware trojan στο ολοκληρωμένο κύκλωμα είναι εξαιρετικά δύσκολη, εάν χρησιμοποιείται από τους ελεγκτές η τυχαία μέθοδος επαλήθευσης. [12]

Προκειμένου να γίνει πλήρως κατανοητή η διαδικασία του συνδυαστικού μηχανισμού ενεργοποίησης θα μπορούσαμε να ανατρέξουμε στην εικόνα 4 οπού δείχνει ένα παράδειγμα ενός Trojan που ενεργοποιείται συνδυαστικά , η συνθήκη ενεργοποίησης είναι όταν A=0 και B=0 στους αντίστοιχους κόμβους. Τα A και B αναγκάζουν έναν κόμβο ωφέλιμου φορτίου C να έχει λανθασμένη τιμή Cmodified . Συνήθως, ένας αντίπαλος θα επέλεγε μια εξαιρετικά σπάνια συνθήκη ενεργοποίησης έτσι ώστε να είναι πολύ απίθανο για το Trojan να ενεργοποιηθεί κατά τη διάρκεια συμβατικής δοκιμής. [3]

Μια δεύτερη μορφή μηχανισμού ενεργοποίησης είναι αυτή του ακολουθιακού μηχανισμού trigger. Η συγκεκριμένη κατηγορία μπορεί να ενεργοποιηθεί μόνο όταν συμβεί μια σπάνια

σειρά καταστάσεων σε προκαθορισμένους κόμβους του ολοκληρωμένου κυκλώματος. Συνήθως, στη συγκεκριμένη κατηγορία ο μηχανισμός ενεργοποίησης πραγματοποιείται με τη βοήθεια των state – machines. Βλέποντας την εικόνα 5 μπορούμε να παρατηρήσουμε ένα ακολουθιακό μηχανισμό trigger με την ονομασία timer bomb trojan, δείχνει έναν μετρητή k-bit που ενεργοποιείται όταν το πλήθος φτάνει το 2k−1, τροποποιώντας τον κόμβο ER σε ER*.

Μια τρίτη κατηγορία είναι αυτή του μηχανισμού Trigger always - on. Πιο συγκεκριμένα υπάρχουν Hardware Trojans τα οποία δεν ενεργοποιούνται ούτε απενεργοποιούνται από μια λογική συνθήκη. Τις περισσότερες φορές, τέτοιου είδους επιθέσεις εκτελούν αρνητικές και κακόβουλες λειτουργίες χωρίς την ύπαρξη καμιάς λογικής ενεργοποίησης. Ως παράδειγμα trigger always on μπορούμε να αναφέρουμε τη σκόπιμη αλλαγή όσον αφορά στη φάση της κατασκευής. Αυτό περιλαμβάνει Trojans όπως η αραίωση των συρμάτων τρανζίστορ, αλλάζοντας την ισχύ κίνησης των τρανζίστορ αλλάζοντας το μήκος-πλάτος τους, την αναλογία κ.λπ. Μια συσκευή με τέτοια αλλαγή μπορεί να αρχίσει να λειτουργεί ακριβώς όπως η κανονική συσκευή, αλλά θα αποτυγχάνει όποτε οι εσωτερικές συνθήκες υπερβαίνουν τις φυσικές τιμές που υποστηρίζεται από την κατασκευασμένη συσκευή. Έτσι, η αποτυχία τους δεν μπορεί να προβλεφθεί με ακρίβεια, αλλά μόνο μια στατιστική πιθανότητα εμφάνισης ενός τέτοιου Με τη συγκεκριμένη τροποποίηση επηρεάζονται τόσο οι κόμβοι όσο και οι συνδέσεις στο ολοκληρωμένο κύκλωμα. Αυτό έχει ως αποτέλεσμα να αυξάνεται η πιθανότητα αποτυχία του συγκεκριμένου ολοκληρωμένου κυκλώματος προς ανάπτυξη. [1]

3.3 Ταξινόμηση με βάση το ωφέλιμο φορτίο - payload

Ο κύριος στόχος του ωφέλιμου φορτίου είναι να προκαλέσει τροποποίηση στην ομαλή λειτουργία του ολοκληρωμένου κυκλώματος. Το ωφέλιμο φορτίο μπορεί να κατηγοριοποιηθεί σε δύο επιμέρους υποκατηγορίες. Η κατηγοριοποίηση αυτή πραγματοποιείται ανάλογα με τον τρόπο επιρροής του ωφέλιμου φορτίου ως προς την κανονική λειτουργία του εκάστοτε ολοκληρωμένου κυκλώματος. Η πρώτη κατηγορία που υπάρχει είναι το ωφέλιμο φορτίο, το οποίο μπορεί να προσθέσει καινούργιες λειτουργίες που έχει ορίσει ο εκάστοτε αντίπαλος. Στη συγκεκριμένη περίπτωση το ωφέλιμο φορτίο δεν επηρεάζει την λειτουργικότητα του ολοκληρωμένου κυκλώματος, αλλά προσθέτει νέες λειτουργίες. Αυτή την κατηγορία μπορεί κανείς να τη συναντήσει και με το διεθνή

όρο emitter backdoor. Ο σκοπός της ύπαρξης του συγκεκριμένου ωφέλιμου φορτίου – payload είναι να εκτελούνται ορισμένες νέες λειτουργίες, οι οποίες δεν θα είναι ορατές από τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων. Η δεύτερη υποκατηγορία είναι το ωφέλιμο φορτίο, το οποίο αλλάζει την κανονική λειτουργία του ολοκληρωμένου κυκλώματος. Στην περίπτωση αυτή το payload δεν προσθέτει καινούργιες λειτουργίες στις κανονικές λειτουργίες του κυκλώματος. Ο αντίπαλος στην περίπτωση αυτή οφείλει να γνωρίζει σε πολύ μεγάλο βαθμό το αντίστοιχο προς επίθεση υλικό. Ο κύριος λόγος είναι διότι η αλλαγή που θα προκληθεί μέσω του ωφέλιμου φορτίου δεν πρέπει να καταρρεύσει το σύστημα. Η συγκεκριμένη κατηγορία με βάση του ωφέλιμου φορτίο μπορεί να χωριστεί σε δύο υπό κατηγορίες. Η πρώτη κατηγορία είναι αυτή στην οποία το ωφέλιμο φορτίο να μπορεί να τροποποιήσει τη διασύνδεση δεδομένων. Αυτή η κατηγορία μπορεί επίσης να ονομαστεί ως Backdoor corrupter data. Από την άλλη μεριά υπάρχει η κατηγορία στην οποία το ωφέλιμο φορτίο Payload να μπορεί να αλλάξει τη διεπαφή(interface) ελέγχου της τρέχουσας κατάστασης. [1]

3.4 Μοντέλα Trojan επιθέσεων

Οι επιθέσεις υλικού Hardware Trojan με την πάροδο του χρόνου έχουν εξελιχθεί σε πολύ μεγάλο βαθμό. Η συνεχής εξέλιξή τους αποσκοπεί στο να γίνουν πιο ισχυρές οι επιθέσεις υλικού trojan προκειμένου να εισχωρήσουν στα όλο και πιο αξιόπιστα και ασφαλή κυκλώματα.

Μια επίθεση Trojan θα μπορούσε να εισαχθεί σε οποιοδήποτε στάδιο του σχεδιασμού του υλικού από τον εκάστοτε ανταγωνιστή. Αυτό είχε ως αποτέλεσμα να δημιουργηθεί η ανάγκη για πολύπλοκα μοντέλα επιθέσεων Trojan.

Η διαδικασία της σωστής και ακριβής μοντελοποίησης των Hardware Trojan αποτελεί μια από τις πιο σημαντικές λειτουργίες. Ο κύριος λόγος είναι διότι πραγματοποιείται με τον καλύτερο δυνατό τρόπο η ανάλυση και η μελέτη τόσο των επιθέσεων υλικού Trojan που μπορεί να προκύψουν όσο και των επιπτώσεων που θα προκαλέσει η εκάστοτε επίθεση στο αντίστοιχο υλικό και στη φήμη του.

Πριν ξεκινήσει η διαδικασία της επίθεσης Hardware Trojan, ο εκάστοτε αντίπαλος θα πρέπει να πραγματοποιήσει ορισμένες βασικές ενέργειες. Η πιο σημαντική απόφαση που θα πρέπει να λάβει είναι η επιλογή του πλέον κατάλληλου μοντέλου Trojan που ταιριάζει

για την κάθε περίπτωση. Στο σημείο αυτό, είναι ιδιαίτερα σημαντικό να υπενθυμίσουμε ότι κάθε αντίπαλος έχει τη δυνατότητα να πραγματοποιήσει εισαγωγή του Trojan σε πολλές και διαφορετικές φάσης όσον αφορά τη διαδικασία σχεδιασμού του αντίστοιχου υλικού. Αυτό το γεγονός, οδηγεί στην επιτακτική ανάγκη για τα λεγόμενα μοντέλα πολλαπλών επιθέσεων - Multiple Attack Models.

Στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας πραγματοποιήθηκε έρευνα όσον αφορά επτά ολοκληρωμένα μοντέλα επίθεσης Trojan. Στην εικόνα που ακολουθεί, γίνεται αναφορά στα συγκεκριμένα μοντέλα, τα οποία αναλύονται και περιγράφονται στη συνέχεια. [1]

Model	Description	3PIP Vendor	SoC Developer	Foundry
A	Untrusted 3PIP vendor	Untrusted	Trusted	Trusted
B	Untrusted foundry	Trusted	Trusted	Untrusted
C	Untrusted EDA tool, or rogue employee	Trusted	Untrusted	Trusted
D	Commercial off-the-shelf (COTS component	Untrusted	Untrusted	Untrusted
E	Untrusted design house	Untrusted	Untrusted	Trusted
F	Fabless SoC design house	Untrusted	Trusted	Untrusted
G	Untrusted SoC developer with trusted IPs	Trusted	Untrusted	Untrusted

Εικόνα 6 - Επτά ολοκληρωμένα μοντέλα επίθεσης Trojan [1]

- Μοντέλο Επίθεσης Trojan A

Στο συγκεκριμένο μοντέλο επιθέσεων Trojan περιλαμβάνονται οι μη αξιόπιστοι προμηθευτές 3PIP. Οι σχεδιαστές των System on a chip – SoC τις περισσότερες φορές προκειμένου να ολοκληρώσουν με επιτυχία τα σχέδια τους χρειάστηκε να προμηθευτούν IP από τρίτους κατασκευαστές. Αυτό συμβαίνει για να μειωθεί ο χρόνος κατασκευής και να είναι μικρότερο το κόστος. Επίσης, ένα ακόμα πλεονέκτημα της χρήσης υλικού από τρίτους προμηθευτές είναι η μείωση του φυσικού μεγέθους που θα έχει το προς κατασκευή ολοκληρωμένο κύκλωμα. Εκτός από τα πολλά οφέλη όμως που μπορεί να έχει η προμήθεια αυτή, παρουσιάζεται και ένα σημαντικό μειονέκτημα. Το μειονέκτημα αυτό είναι ότι οι αντίπαλοι σε έναν μη αξιόπιστο προμηθευτή έχουν τη δυνατότητα να εισάγουν

ένα Hardware Trojan στο αντίστοιχο προς κατασκευή υλικό. Η προσθήκη του Trojan στη συγκεκριμένη περίπτωση δεν είναι γνωστή από τον εκάστοτε σχεδιαστή του SoC.

- Μοντέλο Επίθεσης Trojan B

Το συγκεκριμένο μοντέλο επιθέσεων Trojan αναφέρετε στα αναξιόπιστα εργοστάσια. Σε αυτή την περίπτωση οι αντίπαλοι έχουν τη δυνατότητα να εισάγουν οποιοδήποτε Trojan σε οποιοδήποτε σημείο καθώς διαθέτουν πρόσβαση σε όλα τα επίπεδα του σχεδίου.

- Μοντέλο Επίθεσης Trojan C

Στο συγκεκριμένο μοντέλο Trojan περιέχεται ο μη αξιόπιστος προγραμματιστής SoC. Για την σωστή κατασκευή υλικού είναι απαραίτητο να υπάρχουν άριστα εκπαιδευμένοι σχεδιαστές SoC καθώς και τα πλέον κατάλληλα εργαλεία σχεδιασμού. Στο μοντέλο επίθεσης C, αντίπαλοι θεωρούνται οι εσωτερικές απειλές. Τέτοιες απειλές είναι λόγου χάριν η χρήση μη αξιόπιστων εργαλείων λογισμικού EDA καθώς και CAD.

- Μοντέλο Επίθεσης Trojan D

Μη αξιόπιστα εξαρτήματα Commercial off the shelf – COTS. Ένα προϊόν COTS είναι συνήθως ένα προϊόν υλικού ή λογισμικού υπολογιστή προσαρμοσμένο για συγκεκριμένες χρήσεις και διατίθεται στο ευρύ κοινό. Τέτοια προϊόντα έχουν σχεδιαστεί για να είναι άμεσα διαθέσιμα και φιλικά προς τον χρήστη. Πολλές φορές οι σχεδιαστές των ολοκληρωμένων κυκλωμάτων χρησιμοποιούν εξαρτήματα COTS. Τα εξαρτήματα αυτά έχουν εμφανώς χαμηλότερο κόστος συγκριτικά με ένα προσαρμοσμένο προϊόν. Η ενσωμάτωσή τους σε ένα ολοκληρωμένο κύκλωμα δεν απαιτεί εξειδικευμένες τεχνικές ανάπτυξης. Τα εξαρτήματα COTS δημιουργούνται με μη αξιόπιστο τρόπο. Αυτό έχει ως δυσάρεστη συνέπεια να προκύπτουν πολλά ευάλωτα σημεία όσον αφορά τη διαδικασία σχεδίασης των ολοκληρωμένων κυκλωμάτων.

- Μοντέλο Επίθεσης Trojan E

Untrusted Design House. Στο μοντέλο επίθεσης Trojan E αναφερόμαστε σε μη αξιόπιστους οίκους σχεδίασης των ολοκληρωμένων κυκλωμάτων καθώς και σε μη

αξιόπιστους πωλητές των IP. Πρόκειται ουσιαστικά για μια ολόκληρη μη αξιόπιστη διαδικασία εφοδιασμού για την σχεδίαση των ολοκληρωμένων κυκλωμάτων.

- Μοντέλο Επίθεσης Trojan F

Untrusted Outsourcer.

Ο όρος "fabless" σημαίνει ότι η εταιρεία σχεδιάζει και πουλά το υλικό και τα τσιπ ημιαγωγών, αλλά δεν κατασκευάζει τις silicon wafers ή τα τσιπ που χρησιμοποιούνται στα προϊόντα της. Αντίθετα, αναθέτει την κατασκευή σε εργοστάσιο παραγωγής. Το συγκεκριμένο μοντέλων επιθέσεων αποτελεί έναν συνδυασμό δύο επιμέρους μοντέλων. Πιο συγκεκριμένα, αναφερόμαστε στον συνδυασμό του μοντέλου A και του μοντέλου B. Οι σχεδιαστές χρησιμοποιούν τόσο μη αξιόπιστους προμηθευτές 3PIP όσο και μη αξιόπιστα εργοστάσια. Το γεγονός αυτό έχει ως αποτέλεσμα να μην μπορούν με σιγουριά να αποφανθούν ότι το υλικό που σχεδιάστηκε αποτελεί υλικό χωρίς την τοποθέτηση οποιουδήποτε Trojan.

- Μοντέλο Επίθεσης Trojan G

Untrusted Systems Integrator. Στο συγκεκριμένο μοντέλο περιλαμβάνονται οι μη αξιόπιστοι ολοκληρωτές συστήματος. Οι ίδιοι εξυπηρετούν πελάτες, οι οποίοι στοχεύουν στην εύρεση ενός προμηθευτή που θα μπορούσε να αναλάβει τόσο την σχεδίαση όσο και την κατασκευή. Το γεγονός αυτό μπορεί να οδηγήσει σε τρωτά σημεία όσον αφορά την διαδικασία σχεδίασης των ολοκληρωμένων κυκλωμάτων ενός υλικού. [1]

Κεφάλαιο 4 ΑΝΑΛΥΣΗ ΜΕΘΟΔΩΝ ΑΜΥΝΑΣ ΑΠΟ HARDWARE TROJAN

Καθώς η τεχνολογία συνεχώς εξελίσσεται με ραγδαίους ρυθμούς, δίνει διαρκώς περισσότερες δυνατότητες στους χρήστες της. Αυτή η συνεχή εξέλιξη, έχει ως αποτέλεσμα να εξελίσσονται παράλληλα και οι επιθέσεις υλικού Trojans. Οι κατασκευαστές θα πρέπει συνεχώς να αναζητούν λύσεις και μεθόδους άμυνας απέναντι στις εξελισσόμενες επιθέσεις που προσβάλλουν το αντίστοιχο προς σχεδίαση και κατασκευή υλικό – hardware.

Οι ειδικοί του κλάδου είναι υπεύθυνοι στο να μελετούν τις διάφορες επιθέσεις Trojan που υπάρχουν. Όπως έχουμε ήδη αναφέρει, ένα Trojan μπορεί να τοποθετηθεί σε διάφορα στάδια κατά τη διαδικασία της σχεδίασης και κατασκευής των υλικών. Συμπεραίνουμε συνεπώς πως ο ρόλος που έχουν όσοι αναζητούν τρόπους ανίχνευσης τέτοιου είδους επιθέσεων είναι πολύ δύσκολος. Ο λόγος είναι αφενός διότι τα Trojans τοποθετούνται σε διάφορα σημεία όπως έχουμε ήδη αναφέρει και αφετέρου διότι οι αντίπαλοι συνεχώς βελτιώνουν τα Trojan με σκοπό να είναι όσο το δυνατόν πιο δύσκολη η ανίχνευσή τους.

Κατά καιρούς έχουν μελετηθεί και εφαρμοστεί διάφορες τεχνικές που αποσκοπούν στην πρόληψη των επιθέσεων Hardware Trojan. Πιο συγκεκριμένα, έχουν χρησιμοποιηθεί τεχνικές που συνεχώς εξελίσσονται με την πάροδο των χρόνων, οι οποίες λαμβάνουν χώρα μετά από το στάδιο του σχεδιασμού ενός ολοκληρωμένου κυκλώματος – IC, οι οποίες αποσκοπούν στην προστασία του από τα διάφορα Hardware Trojans. Τέτοιου είδους τεχνικές έχουν ως κύριο στόχο τους να μπλοκάρουν την ενεργοποίηση των Trojan που έχουν ήδη τοποθετηθεί σε ένα ολοκληρωμένο κύκλωμα. Υπάρχουν επίσης, τεχνικές για την αποτροπή των Trojans κατά το στάδιο κατασκευής των ολοκληρωμένων κυκλωμάτων. [14]

Όπως έχουμε ήδη αναφέρει, μέχρι σήμερα έχουν πραγματοποιηθεί πολλές έρευνες και μεγάλο πλήθος ερευνητών έχουν ασχοληθεί με το συγκεκριμένο κλάδο. Οι μέθοδοι που έχουν αναπτυχθεί μπορούν να χωριστούν σε δύο κατηγορίες. Στην πρώτη κατηγορία κατατάσσονται οι μέθοδοι ανίχνευσης που εφαρμόζονται πριν την κατασκευή του υλικού. Εν αντιθέσει με την δεύτερη κατηγορία, στην οποία κατατάσσονται οι μέθοδοι ανίχνευσης μετά τη διαδικασία κατασκευής. [16]

Στη συνέχεια του συγκεκριμένου κεφαλαίου θα αναφερθούμε και θα πραγματοποιήσουμε περαιτέρω μελέτη για τις διάφορες τεχνικές πρόληψης και ανίχνευσης των επιθέσεων Hardware Trojans

4.1 Τεχνικές Ανίχνευσης πριν την κατασκευή

Όπως έχουμε ήδη αναφέρει και σε προηγούμενες ενότητες της συγκεκριμένης πτυχιακής εργασίας, ένα Trojan μπορεί να τοποθετηθεί πριν την κατασκευή του υλικού. Για το λόγο αυτό, οι ειδικοί του κλάδου θα πρέπει να αναζητούν συνεχώς τρόπους με τους οποίους θα έχουν τη δυνατότητα να ανιχνεύσουν έγκαιρα τέτοιου είδους επιθέσεις υλικού Trojan. Στο στάδιο αυτό θα πρέπει να πραγματοποιείται με πολύ μεγάλη ακρίβεια το netlist του εκάστοτε σχεδίου προκειμένου να κατασκευαστεί ένα όσο το δυνατόν πιο αξιόπιστο υλικό. Αυτό επιτυγχάνεται εάν στο συγκεκριμένο στάδιο γίνει η πλέον κατάλληλη επιλογή όσον αφορά τα αντίστοιχα τμήματα του σχεδίου.

Στο σημείο αυτό είναι σκόπιμο να αναφερθούμε στην τυπική επαλήθευση του σχεδίου. Πρόκειται για μια επαλήθευση του σχεδίου που βασίζεται σε έναν αλγόριθμο. Είναι σκόπιμο να αναφέρουμε ότι το πρόγραμμα δοκιμής (testbench) έχει τη δυνατότητα να διαβάζει το μοντέλο που περιγράφει το πρόγραμμα RTL και εφαρμόζει στις εισόδους του τα διανύσματα δοκιμής του αντίστοιχου αρχείου. Σε κάθε κύκλο, πραγματοποιεί μια σύγκριση μεταξύ της εξόδου του μοντέλου RTL με την αναμενόμενη έξοδο. Εάν μετά τη σύγκριση των δυο εξόδων, αυτές δεν ταιριάζουν τότε το πρόγραμμα εκτυπώνει σφάλμα. Με τη βοήθεια του αλγορίθμου αυτού, επιβεβαιώνεται η εγκυρότητα του εκάστοτε σχεδίου για την μετ' έπειτα κατασκευή του αντίστοιχου υλικού. Προκειμένου να εκτελεστεί η συγκεκριμένη μορφή επαλήθευσης αρκεί να καθοριστούν οι προδιαγραφές του. Εν συνεχεία, θα πρέπει να χαρακτηριστούν και να καταγραφούν ως ιδιότητες το πλήθος των λειτουργιών του. Για την σωστή υλοποίηση της τυπικής επαλήθευσης του σχεδίου θα πρέπει να εκτελεστούν τόσο ο έλεγχος μοντέλου όσο και ο έλεγχος ιδιοτήτων.

Κύριος στόχος της συγκεκριμένης μορφής επαλήθευσης είναι ελέγχοντας τις λειτουργικές ιδιότητες του εκάστοτε σχεδίου να μπορεί να ελεγχθεί κάθε επιμέρους κομμάτι του σχεδιασμού ώστε το υλικό να συνεχίσει στην διαδικασία της κατασκευής χωρίς την υποψία ότι υπάρχει κάποιου είδους επίθεση Trojan.

Στόχος της λογικής επαλήθευσης είναι να αποδείξει ότι ένα κελί εκτελεί σωστά τη λειτουργία που επιθυμούμε σε κάθε ένα από τα παραπάνω επίπεδα. Αυτό επιτυγχάνεται αν προσομοιώσουμε με ένα μοντέλο το κελί, να εφαρμόσουμε ένα σύνολο δυαδικών ακολουθιών στην είσοδό του, το οποίο ονομάζουμαι σύνολο διανυσμάτων δοκιμής, και να ελέγξουμε ότι η έξοδος για κάθε διάνυσμα δοκιμής είναι αυτή που αναμένουμε με βάση τις λειτουργικές προδιαγραφές

Η μέθοδος της τυπικής επαλήθευσης μπορεί να χρησιμοποιηθεί κατά κύριο λόγο σε μικρού μεγέθους σχέδια. Πιο συγκεκριμένα, με τη χρήση της τυπικής επαλήθευσης σε ένα μικρό σχέδιο, μπορεί κανείς να συμπεράνει εάν στο εκάστοτε σχέδιο έχει τοποθετηθεί επίθεση Trojan ή εάν το σχέδιο είναι καθαρό από επιθέσεις. Κάτι αντίστοιχο όμως δεν μπορεί να συμβεί σε μεγάλα σε μέγεθος σχέδια. Ο λόγος είναι διότι η διαδικασία της προδιαγραφής σε τέτοιου είδους σχέδια είναι σχεδόν ανέφικτος και δεν διαθέτουν επίσημο μοντέλο αναφοράς. Η ιδανικότερη λύση για την επαλήθευση σε μεγάλου μεγέθους σχέδια είναι η εξαντλητική επαλήθευση προκειμένου να ανιχνευθούν τυχόν Trojans. [10]

Μια δεύτερη μέθοδος για την ανίχνευση τυχόν Trojans πριν τη διαδικασία της κατασκευής του υλικού είναι η λεγόμενη λειτουργική επαλήθευση. Η συγκεκριμένη μέθοδος επαλήθευσης στηρίζεται στη προσομοίωση, εν αντιθέσει με την τυπική επαλήθευση, η οποία βασίζεται στον αλγόριθμο. Η ομοιότητα των δυο προαναφερθέντων μεθόδων είναι ότι χρησιμοποιούνται για την απόδειξη της ορθότητας του εκάστοτε σχεδίου πριν την κατασκευή του αντίστοιχου υλικού. [12]

Η συγκεκριμένη μέθοδος επαλήθευσης βασίζεται στη κάλυψη του κώδικα καθώς και στην λειτουργική κάλυψη, προκειμένου να ανιχνευθούν τα αντίστοιχα Hardware Trojans. Η λειτουργική επαλήθευση μπορεί να χρησιμοποιηθεί με επιτυχία σε μικρά σχέδια. Η λειτουργική επαλήθευση Συχνά αναφέρεται ως Automatic Test Pattern Generation (ATPG) αυτή η τεχνική είναι πιο συνηθισμένη η οποία χρησιμοποιείται για τον εντοπισμό κατασκευαστικών βλαβών. Έχει αποδειχθεί αποτελεσματική στον εντοπισμό hardware trojans. Το ATPG περιλαμβάνει τις εισόδους των θυρών που ερεθίζονται και στη συνέχεια οι θύρες εξόδου παρακολουθούνται για τυχών παραλλαγές που μπορεί να υποδηλώνει ότι έχει ενεργοποιηθεί ένα trojan υλικού.

Στο σημείο αυτό, είναι ιδιαίτερα σημαντικό να αναφερθούμε στο γεγονός ότι η χρήση διαφόρων τεχνικών και μεθόδων που αποσκοπούν στην εύρεση τυχόν Trojan στο υλικό πριν τη διαδικασία της κατασκευής του, δεν είναι σε θέση να εγγυηθούν ότι δεν θα υπάρξει κανένα είδος Trojan στο αντίστοιχο υλικό.

4.2 Ασφάλιση των ολοκληρωμένων κυκλωμάτων

Όπως έχουμε αναφέρει και σε προηγούμενα κεφάλαια της συγκεκριμένης πτυχιακής εργασίας, η διαδικασία σχεδιασμού των ολοκληρωμένων κυκλωμάτων αποτελείται από πολλά και διαφορετικά στάδια. Αρχικά, θα πρέπει να πραγματοποιηθεί η μετάφραση των προδιαγραφών του σχεδίου για το εκάστοτε ολοκληρωμένο κύκλωμα και εν συνεχεία η μετατροπή του σε κώδικα με βάση μια γλώσσα σχεδιασμού υλικού. Το επόμενο βήμα είναι η σύνθεση, δηλαδή η παραγωγή μιας netlist. Ακολουθεί η διαδικασία της τοποθέτησης και εν συνεχεία η διαδικασία της δρομολόγησης. Τα ψηφιακά αρχεία που προκύπτουν είναι πλέον έτοιμα να παραδοθούν για κατασκευή. Όταν το εργοστάσιο δημιουργήσει τα κυκλώματα, ακολουθεί το βήμα της δοκιμής. Το βήμα αυτό είναι ιδιαίτερα σημαντικό καθώς εξασφαλίζει τη σωστή λειτουργία του κυκλώματος και ελέγχει εάν στο κύκλωμα έχει τοποθετηθεί οποιουδήποτε είδους επίθεση Hardware Trojan, το οποίο θα είχε αρνητικές μέχρι και καταστροφικές συνέπειες για το εκάστοτε κύκλωμα. Εάν ολοκληρωθεί η διαδικασία των δοκιμών με επιτυχία, τότε και μόνο τότε ακολουθεί η φάση της συναρμολόγησης και συσκευασίας. [17]

Πολλές φορές για να πραγματοποιηθεί με επιτυχία η διαδικασία σχεδιασμού ορισμένων πιο σύνθετων συσκευών είναι απαραίτητο να ενσωματωθούν τμήματα του εκάστοτε υλικού από τρίτους προμηθευτές, οι οποίοι μπορεί να βρίσκονται σε διάφορα σημεία ανά τον κόσμο. Το γεγονός αυτό, ναι μεν βοηθάει στην εξοικονόμηση τόσο πόρων όσο και χρόνου για τις εταιρίες σχεδιασμού, αλλά αυξάνει τον κίνδυνο όσον αφορά την ασφάλεια του εκάστοτε υλικού. [18]

Η επιλογή της πλέον κατάλληλης επίθεσης βασίζεται πάρα πολύ στους πόρους καθώς και στον προσδιορισμό του αντιπάλου. Στα αρχικά βήματα της διαδικασία σχεδιασμού ενός ολοκληρωμένου κυκλώματος, είναι πιο εύκολο να υπάρξει τροποποίηση των σχεδίων. Παρ’ όλα αυτά μπορούν να χρησιμοποιηθούν με πολύ αποτελεσματικό τρόπο εργαλεία που στοχεύουν στον εντοπισμό τυχόν επιθέσεων Hardware Trojans. Ο εντοπισμός μιας

επίθεσης Hardware Trojan στα πρώτα στάδια της διαδικασίας σχεδιασμού ενός ολοκληρωμένου κυκλώματος αποτελεί μεν πρόβλημα όμως είναι πιο εύκολα διαχειρίσιμο και πιο οικονομικό συγκριτικά με τον εντοπισμό μιας επίθεσης στη διαδικασία κατασκευής του. Για το λόγο αυτό, η διαδικασία της κατασκευής ενός ολοκληρωμένου κυκλώματος θεωρείται το πιο κρίσιμο σημείο για την τοποθέτηση των επιθέσεων Hardware Trojans. Όταν εντοπιστεί ένα Hardware Trojan ενώ έχει ήδη ξεκινήσει η διαδικασία κατασκευής τότε η διαδικασία απομάκρυνσης του από το ολοκληρωμένο κύκλωμα θεωρείται αδύνατη. Επίσης, στο σημείο αυτό η οικονομική συνέπεια είναι τεράστια για την εταιρία ανάπτυξης του ολοκληρωμένου κυκλώματος. [10]

4.3 Τεχνικές ανίχνευσης Trojan

Η διαδικασία της ανίχνευσης μιας επίθεσης Hardware Trojan είναι μια εξαιρετικά δύσκολη όσο και πολύπλοκη διαδικασία για τους σχεδιαστές και κατασκευαστές των ολοκληρωμένων κυκλωμάτων. Όσο ο χρόνος περνάει και η τεχνολογία αναπτύσσεται, εξελίσσονται και τα ολοκληρωμένα κυκλώματα. Αυτή η εξέλιξη συνεπάγεται την χρήση μεγαλύτερου αριθμού πυλών κατά την κατασκευή τους. Αυτό συνεπάγεται ότι η διαδικασία ανίχνευσης κακόβουλου υλικού στα ολοκληρωμένα κυκλώματα γίνεται ολοένα και πιο δύσκολη διαδικασία. Ο λόγος που συμβαίνει αυτό είναι διότι στις μέρες μας τα κυκλώματα απαρτίζεται από ολοένα και πιο πολύπλοκη εσωτερική σύνθεση. [19]

Ένας επιπλέον λόγος για τον οποίο η διαδικασία της ανίχνευσης των Hardware Trojan είναι μια δύσκολη διαδικασία είναι διότι δεν είναι λίγες οι ευκαιρίες που έχουν οι αντίπαλοι να πραγματοποιήσουν με επιτυχία την εισαγωγή του εκάστοτε Trojan στα πολλά και διαφορετικά τμήματα της διαδικασίας ανάπτυξης τους. Στις μέρες μας τα εργοστάσια που αναλαμβάνουν την κατασκευή τμημάτων κατά την διαδικασία κατασκευής των ολοκληρωμένων κυκλωμάτων χρησιμοποιούν ιδιαίτερα σύγχρονες τεχνολογίες και εγκαταστάσεις. Είναι λοιπόν σε θέση να κατασκευάζουν, να τοποθετούν και να κρύβουν όσο το δυνατόν καλύτερα και με απόλυτη στρατηγική οποιουδήποτε είδους κακόβουλη επίθεση. Οι επιθέσεις στο υλικό είναι ένα φαινόμενο που παρατηρείται ολοένα και περισσότερο στις μέρες μας και προβληματίζει ιδιαίτερα τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων.

Για τους λόγους που αναφέρθηκαν προηγουμένως και για πολλούς ακόμα λόγους, οι επιστήμονες του συγκεκριμένου κλάδου στρέφονται συνεχώς στην διαδικασία ανίχνευσης των κακόβουλων τροποποιήσεων Hardware Trojans. Τα τελευταία δέκα χρόνια έχουν αναπτυχθεί και συνεχίζουν να εφαρμόζονται στις μέρες μας πολλές και διαφορετικές μέθοδοι που αποσκοπούν στην ανίχνευση κακόβουλων τροποποιήσεων στο υλικό.

Σύμφωνα με τους επιστήμονες Tehranipoor και Koushanfar, οι οποίοι πραγματοποίησαν έρευνα το 2010 γύρω από το θέμα που προβληματίζει ολόκληρη την επιστημονική κοινότητα που είναι τα Hardware Trojan, αναφέρουν ότι υπάρχουν δύο βασικές κατηγορίες όσον αφορά τις μεθόδους ανίχνευσης των Hardware Trojans μέσα στα ολοκληρωμένα κυκλώματα. Πιο συγκεκριμένα, αναφέρθηκαν στην πρώτη κατηγορία, η οποία ονομάζεται ανάλυση πλευρικών καναλιών. Η κατηγορία αυτή είναι επίσης γνωστή και με τον διεθνή όρο side – channel analysis. Από την άλλη μεριά, η δεύτερη κατηγορία μεθόδων ανίχνευσης των Hardware Trojans είναι η λεγόμενη ενεργοποίηση κακόβουλων τροποποιήσεων όσον αφορά το υλικό. Η συγκεκριμένη κατηγορία είναι επίσης γνωστή ως Trojan activation. Και οι δυο αυτές κατηγορίες έχουν σχέση με την αποτελεσματική αντιμετώπιση και στοχεύουν στην εξάλειψη του φαινομένου των κακόβουλων τροποποιήσεων. Το κύριο χαρακτηριστικό που παρατηρείται ότι διαθέτουν και οι δύο κατηγορίες για την ανίχνευση των Trojan που αναφέρθηκαν προηγουμένως είναι ότι η δράση τους εστιάζεται κατά κύριο λόγο στο επίπεδων των τσιπ και της αρχιτεκτονικής. Στο σημείο αυτό, είναι ιδιαίτερα σημαντικό να αναλύσουμε περισσότερο τις δύο αυτές κατηγορίες ανίχνευσης κακόβουλης τροποποίησης υλικού. Η πρώτη κατηγορία των πλευρικών καναλιών – side channel στηρίζεται στη λογική ότι οι επιθέσεις Trojan κάποιες φορές προσπαθούν να τροποποιήσουν ορισμένα από τα χαρακτηριστικά που διαθέτει το προς επίθεση τσιπ. Τέτοιου είδους αλλαγές όπως είναι λογικό έχουν την τάση να επηρεάζουν σε μεγάλο βαθμό και τα αντίστοιχα χαρακτηριστικά του ολοκληρωμένου κυκλώματος, όπως είναι λόγου χάριν η ισχύς και η καθυστέρηση τόσο της καλωδίωσης όσο και των πυλών που υπάρχουν στο εκάστοτε τσιπ. Είναι εξίσου σημαντικό να αναφέρουμε ότι τα σήματα πλευρικών καναλιών, τα οποία βασίζονται στην ισχύ, έχουν τη δυνατότητα να πληροφορούν για την εσωτερική δομή του εκάστοτε κυκλώματος καθώς και για τις λειτουργίες και δραστηριότητες που συμβαίνουν μέσα σε αυτό. Με τον τρόπο αυτό, η ανίχνευση κακόβουλων τροποποιήσεων μπορεί να πραγματοποιηθεί χωρίς να χρειαστεί η πλήρης ενεργοποίηση του εκάστοτε Hardware Trojan που έχει τοποθετηθεί

μέσα σε αυτό. [9]. Από την άλλη πλευρά, υπάρχουν επίσης σήματα πλευρικών καναλιών, τα οποία στηρίζονται στο χρόνο. Στη συγκεκριμένη περίπτωση υπάρχει η δυνατότητα να ανιχνευθεί μια κακόβουλη τροποποίηση από ένα Hardware Trojan μέσα σε ένα ολοκληρωμένο κύκλωμα εάν το τσιπ στη διαδικασία δοκιμών έχει χρησιμοποιήσει ελέγχους ευαίσθητους σε πολύ μικρές τροποποιήσεις στην καθυστέρηση. Πιο αναλυτικά, θα πρέπει οι έλεγχοι να πραγματοποιούνται στα συγκεκριμένα μονοπάτια, τα οποία έχουν επηρεαστεί σε μικρό ή μεγάλο βαθμό από την επίθεση του εκάστοτε Hardware Trojan. [9].

Λίγο αργότερα ο Tehranipoor ισχυρίστηκε ότι υπάρχουν τρείς κατηγορίες όσον αφορά στην ανίχνευση ενός Trojan μέσα στο υλικό. Πιο συγκεκριμένα, αναφέρει ότι οι τρείς αυτές κατηγορίες ανίχνευσης βασίζονται αντίστοιχα στην ισχύ, το χρόνο καθώς και την ενεργοποίηση. Στο σημείο αυτό είναι ιδιαίτερα σημαντικό να αναλύσουμε περισσότερο τις τεχνικές ανίχνευσης των κακόβουλων τροποποιήσεων του υλικού. [17]

4.3.1 Ανάλυση βασισμένη στην ισχύ

Ο πρώτος που ανακάλυψε τεχνικές και μεθόδους εντοπισμού των Hardware Trojans που στηρίζονται στην ανάλυση των πλευρικών καναλιών – side – channel analysis ήταν ο Agrawal, το 2007. Οι συγκεκριμένες μέθοδοι στηρίζονται στις πληροφορίες που παρέχουν τα πλευρικά κανάλια προκειμένου να εντοπίζουν πιθανές κακόβουλες τροποποιήσεις στην ισχύ του εκάστοτε ολοκληρωμένου κυκλώματος. Η διαδικασία που ακολουθείτε αρχικά ξεκινάει με δειγματοληπτικούς ελέγχους που επιλέγονται με τυχαίο τρόπο. Σύμφωνα με τους συγκεκριμένους ελέγχους πραγματοποιείται μέτρηση τις ισχύς ορισμένων διαδρομών. Τα δεδομένα που προκύπτουν από τους συγκεκριμένους ελέγχους αποτελούνται από διάφορα και σημαντικά στοιχεία. Ένα στοιχείο ανάλυσης που προκύπτει είναι αυτό της κατανάλωσης ισχύος του εκάστοτε κυκλώματος. Το συγκεκριμένο στοιχείο προκύπτει ύστερα από την τοποθέτηση εισόδου. Η μέτρηση του θορύβου είναι το δεύτερο στοιχείο μέτρησης που προκύπτει από τους δειγματοληπτικούς ελέγχους. Το στοιχείο αυτό υπάρχει η δυνατότητα σε ορισμένες μετρήσεις να μην υπάρχει. Οι ίδιες οι μετρήσεις αποτελούν ένα επόμενο αλλά εξίσου σημαντικό στοιχείο και όπως γίνεται αντιληπτό δεν μπορούν να λείπουν. Οι μετρήσεις μπορεί να έχουν διάφορες παραλλαγές, οι οποίες στηρίζονται στο

γεγονός των τυχαίων δειγμάτων. Το τελευταίο αλλά εξίσου σημαντικό στοιχείο είναι η μέτρηση της κατανάλωσης της ενέργειας. Η μέτρηση αυτή στηρίζεται στην ύπαρξη μιας τυχόν κακόβουλης τροποποίησης από ένα Hardware Trojan. Από αυτούς τους πρώτους ελέγχους δημιουργείται η πρώτη υπογραφή, όπου αυτή ορίζεται ως αναφορά για τους ελέγχους που προκύπτουν στη συνέχεια. Ύστερα πραγματοποιούνται οι ίδιοι έλεγχοι και στο κύκλωμα υπό εξέταση. Εάν η υπογραφή που θα προκύψει είναι ίδια με την υπογραφή που προέκυψε από τους πρώτους ελέγχους τότε το κύκλωμα δεν διατρέχει κάποιου είδους κίνδυνο και κακόβουλη τροποποίηση. Αντίθετα, εάν η υπογραφή που προκύψει από το κύκλωμα ταυτοποίησης είναι διαφορετική από την υπογραφή των πρώτων ελέγχων τότε το εκάστοτε κύκλωμα χαρακτηρίζεται ως ύποπτο και είναι αυξημένη η πιθανότητα να υπάρχει στο εσωτερικό του κάποιου είδους Hardware Trojan. Με τη χρήση τέτοιου είδους ελέγχων όπως αυτοί που περιεγράφηκαν προηγουμένως έχουν τη δυνατότητα να ανιχνεύουν διάφορα είδη Hardware Trojan ανεξάρτητα από το μέγεθός τους. Ο λόγος είναι διότι οι έλεγχοι που εκτελούνται, πραγματοποιούνται με τυχαίο τρόπο. Αξιοσημείωτο είναι το γεγονός ότι το 2008 ο Wang αποφάνθηκε ότι κάθε Hardware Trojan προκειμένου να λειτουργήσει έχει ως απαραίτητη προϋπόθεση την ύπαρξη τροφοδοσίας ρεύματος. Όπως έχουμε ήδη αναφέρει τα Hardware Trojan μπορούν να έχουν πολλούς και διαφορετικούς τύπους καθώς και μεγέθη. Για το λόγο αυτό η επίδραση που έχει κάθε Trojan στα χαρακτηριστικά ισχύος κυκλώματος μπορεί επίσης να διαφέρει. [10]

Οι Rad, Wang Tehranipoor και Plusquellic στο έργο τους το 2008 παρουσίασαν μια διαφορετική προσέγγιση όσον αφορά την ανάλυση η οποία βασίζεται στην ισχύ. Ισχυρίσθηκαν ότι μπορεί να πραγματοποιηθεί μια μέθοδος ανίχνευσης, η οποία να μπορεί να στηριχθεί σε συγκεκριμένα τμήματα του προς επίθεση κυκλώματος. Στα συγκεκριμένα σημεία του εκάστοτε κυκλώματος πραγματοποιείται η εφαρμογή μεγάλης ισχύς από μια θύρα ισχύος. Η διαδικασία αυτή λαμβάνει χώρα σε περισσότερα τμήματα την ίδια χρονική στιγμή και λαμβάνονται μεμονωμένες μετρήσεις σύμφωνα με τυχαίους συνδυασμούς. Μαζί με τη διαδικασία μετρήσεων που αναφέραμε προηγουμένως, εκτελείται επίσης την ίδια χρονική στιγμή και ένας αλγόριθμος καταγραφής της ισχύς. [20] Ο συγκεκριμένος αλγόριθμος στηρίζεται στην ανάλυση των κυματομορφών που λαμβάνει από τις θύρες ισχύος, όσο η διαδικασία το μετρήσεων συνεχίζεται. Στη συνέχεια, με βάση τις μετρήσεις αυτές δημιουργείται ένα διάγραμμα. Στο διάγραμμα αυτό απεικονίζεται κάθε μέτρηση που λάβαμε, η οποία έχει καταταχθεί είτε σε φυσιολογική είτε σε μη φυσιολογική. Οι

μετρήσεις που έχουν καταταχθεί σε μη φυσιολογικές τιμές σημαίνει ότι πιθανόν να υπάρχει κακόβουλη τροποποίηση Hardware Trojan στη συγκεκριμένη περιοχή του εκάστοτε κυκλώματος.

Αξιοσημείωτο είναι το γεγονός ότι όταν πραγματοποιείται ανάλυση σε προκαθορισμένα τμήματα ενός κυκλώματος, δεν είναι απόλυτα αξιόπιστο το αποτέλεσμα όσον αφορά την ανίχνευση των Hardware Trojans. Ο λόγος είναι διότι δεν εντοπίζονται όλες οι πιθανές παραλλαγές στις μετρήσεις της αντίστοιχης ισχύς. Αυτό το πρόβλημα, εξομαλύνεται με την χρήση της διαδικασίας που ονομάζεται βαθμονόμηση των σημάτων. [21] Μπορεί κανείς να συναντήσει τη συγκεκριμένη διαδικασία και με τον διεθνή της όρο, ο οποίος είναι Calibration. Η βαθμονόμηση πραγματοποιείται για κάθε θύρα ισχύος καθώς και για κάθε τσιπ. Ο λόγος ύπαρξης της βαθμονόμησης είναι για να καταγράφει την απόκριση στις θύρες ισχύος σε ένα παλμό. Στη συνέχεια κανονικοποιούνται οι αποκρίσεις κάθε θύρας ισχύος και προκύπτει ένας πίνακας. Μετά εφαρμόζεται μεγάλη ισχύ σε κάθε θύρα ξεχωριστά και βαθμονομούνται όλες οι αποκρίσεις. Πραγματοποιείται ο διαχωρισμός των μετρήσεων της ισχύς. [12] Ο διαχωρισμός αυτός περιλαμβάνει τα κυκλώματα εκείνα στα οποία δεν έχουν παρατηρηθεί τροποποιήσεις Hardware Trojan καθώς και στα κυκλώματα εκείνα που υπάρχει οποιουδήποτε είδους κακόβουλη τροποποίηση υλικού.

Οι επιστήμονες συνδυάζοντας τις μετρήσεις του συγχρονισμού και της ισχύος, έχουν τη δυνατότητα να ανιχνεύουν την ύπαρξη έναν Hardware Trojan στο εκάστοτε υλικό. Αυτό επιτυγχάνεται με τη βοήθεια των χειρισμών εξισώσεων. Πιο συγκεκριμένα, με τη μέθοδο αυτή για ανίχνευση οποιασδήποτε κακόβουλης τροποποίησης υλικού πραγματοποιείται η σύγκριση σε όλες τις επιμέρους μετρήσεις και εν συνεχεία εντοπίζονται οι πύλες αυτές του κυκλώματος, οι οποίες διαθέτουν διαφορετικά χαρακτηριστικά από τα προκαθορισμένα.

4.3.2 Ανάλυση που στηρίζεται στο χρόνο

Μια επιπλέον κατηγορία όσον αφορά την ανίχνευση των κακόβουλων τροποποιήσεων του υλικού είναι η ανάλυση η οποία στηρίζεται στο χρόνο. Οι προσεγγίσεις αυτές αναφέρονται στο γεγονός ότι ένα Hardware Trojan, το οποίο θα εισαχθεί σε οποιοδήποτε στάδιο ανάπτυξης ενός υλικού επηρεάζει τα χαρακτηριστικά χρονισμού του. Ο λόγος που συμβαίνει αυτό είναι διότι κάθε Hardware Trojan με την εισαγωγή του προσθέτει επιπλέον

φόρτο στα μονοπάτια του εκάστοτε κυκλώματος. Μερικά Hardware Trojan έχουν μικρή επιρροή εν αντιθέσει με τα υπόλοιπα, τα οποία έχουν μεγάλη επιρροή στο χρονισμό του εκάστοτε κυκλώματος. Ακόμα και η μικρή επιρροή μπορεί να γίνει αντιληπτή από τους ειδικούς. [20]. Ο εντοπισμός ενός Trojan στο κύκλωμα μπορεί να γίνει μια εύκολη διαδικασία εάν αυτό επηρεάζει την καθυστέρηση στα βασικότερα μονοπάτια του εκάστοτε κυκλώματος.

Ένα μειονέκτημα της ανάλυσης σήματος που βασίζεται στο χρόνο είναι το γεγονός ότι δυσκολεύεται να ανιχνεύσει ένα Hardware Trojan το οποίο έχει τοποθετηθεί σε ένα από τα μικρότερα μονοπάτια που υπάρχουν στο εκάστοτε κύκλωμα. Ο λόγος είναι διότι είναι απαραίτητο να χρησιμοποιηθούν υψηλής συχνότητας σήματα προκειμένου να ελεγχθούν και τα συγκεκριμένα μονοπάτια. Στο σημείο αυτό είναι απαραίτητο να αναφέρουμε ότι οι έλεγχοι με χρήση υψηλότερης συχνότητας επηρεάζονται από το θόρυβο, με αποτέλεσμα να μην καταλήγουμε σε σωστά αποτελέσματα όσον αφορά τον εντοπισμό ή μη ενός Hardware Trojan μέσα στο κύκλωμα.

Το 2008, οι επιστήμονες Li και Lach πρότειναν μια προσέγγιση για την ανίχνευση κακόβουλων τροποποιήσεων όσον αφορά την ανάλυση με βάση τον χρόνο. Πρόκειται για τη χρήση μιας φυσικής μη κλωνοποιήσιμης συνάρτησης. Η συνάρτηση αυτή σύμφωνα με του Li και Lach χρησιμοποιεί μετρήσεις συγκεκριμένων καθυστερήσεων σε συγκεκριμένες διαδρομές. Στη μέθοδο αυτή μπορούμε να αποφανθούμε εάν υπάρχει ή όχι κακόβουλη τροποποίηση στο συγκεκριμένο κύκλωμα όταν προκύπτουν μια ή και περισσότερες καθυστερήσεις ενός μονοπατιού.

4.3.3 Ανάλυση που στηρίζεται στην ενεργοποίηση

Μια τρίτη κατηγορία ανίχνευσης ενός Hardware Trojan σε ένα ολοκληρωμένο κύκλωμα είναι η ανάλυση σημάτων που σχετίζονται με την ενεργοποίησή του. Είναι απαραίτητο να αναφέρουμε ότι η συγκεκριμένη κατηγορία μπορεί να χωριστεί σε δυο επιμέρους κατηγορίες. Η πρώτη υπό κατηγορία είναι αυτές που σχετίζονται με το σημείο στο οποίο έχει τοποθετηθεί μια κακόβουλη τροποποίηση Hardware Trojan. Εν αντιθέσει με τη δεύτερη υποκατηγορία στην οποία ανήκουν αυτές οι προσεγγίσεις στις οποίες δεν

σχετίζεται η περιοχή στην οποία τοποθετείται κάθε φορά ένα Trojan στο προς επίθεση υλικό.

Αναλύοντας την δεύτερη υπό κατηγορία όσον αφορά την ανάλυση που στηρίζεται στην ενεργοποίηση των Hardware Trojan παρατηρούμε ότι οι έλεγχοι που πραγματοποιούνται, εφαρμόζονται με τυχαίο τρόπο. Αντίθετα, στην πρώτη υπό κατηγορία που έχει σημασία το σημείο στο οποίο είναι τοποθετημένο ένα Hardware Trojan εντοπίζετε αρχικά η ισχύς του κυκλώματος υπό έλεγχο και εν συνεχεία η ισχύς του πρωτότυπου κυκλώματος. Στη συνέχεια, πραγματοποιείται η σύγκριση στη διαφορά αυτών των δυο τιμών. Με τον τρόπο αυτόν, έχουμε τη δυνατότητα να βρούμε τις περιοχές όπου η παραπάνω διαφορά στην ισχύ είναι σημαντική. Έτσι φτάνουμε στο συμπέρασμα ότι οι περιοχές αυτές έχουν αυξημένα ποσοστά να έχουν υποστεί οποιουδήποτε είδους επίθεση από ένα Hardware Trojan. [3]

4.4 Σύγχρονες αναλύσεις

Είναι πλέον σημαντικό να αναφέρουμε στο σημείο αυτό και τις σύγχρονες αναλύσεις που υπάρχουν. Ο λόγος είναι διότι τα τελευταία χρόνια επειδή η τεχνολογία έχει εξελιχθεί ραγδαία έχουν προκύψει καινούργιες τεχνικές, οι οποίες βασίζονται στις υπάρχουσες μεθόδους που αποσκοπούν στον εντοπισμό οποιουδήποτε Hardware Trojan έχει τοποθετηθεί στο εκάστοτε ολοκληρωμένο κύκλωμα. [1]

Μια από τις σημαντικότερες έρευνες που θα αναφέρουμε όσον αφορά τις σύγχρονες αναλύσεις πραγματοποιήθηκε το 2016. Οι συγγραφείς της συγκεκριμένης έρευνας ήταν οι Kulkarni, Pino και Mohsenin. Συγκεκριμένα, αναφέρονται στο έργο τους στην επιβάρυνση του υλικού όσον αφορά την συνεχώς αυξανόμενη ασφάλεια του. Αναφέρονται επίσης στην εξασφάλιση ακέραιων σχεδίων όσον αφορά στα τσιπ.

Η έρευνα των Kulkarni, Pino και Mohsenin βασίστηκε Στον τρόπο ανίχνευσης Trojan σε χρόνο εκτέλεσης για έναν προσαρμοσμένο πολυπύρηνο που βασίζεται στη μηχανική μάθηση(Machine Learning), προσπαθώντας να Αξιοποιήσουν τη μηχανή διανυσμάτων υποστήριξης (SVM). Το σύνολο δεδομένων δημιουργείται με βάση την συμπεριφορά πολλών πυρήνων υπό κανονικές συνθήκες και υπό συνθήκες που προκαλούνται από Hardware Trojans. Η μελέτη τους στόχευσε σε διάφορες επιθέσεις επικοινωνίας που προκαλούνται από HT, δηλαδή την αλλοίωση διεύθυνσης πυρήνα, την κυκλοφοριακή εκτροπή της κυκλοφορίας και την επίθεση βρόχου διαδρομής. Υλοποίησαν ένα πλαίσιο

για αρχιτεκτονική πολλών πυρήνων με SVM kernel(SVM kernel είναι μια συνάρτηση που χρησιμοποιείται στο SVM για να βοηθήσει στην επίλυση προβλημάτων. Παρέχουν συντομεύσεις για την αποφυγή περίπλοκων υπολογισμών), ενώ η ενεργοποίηση των Trojans βασίζεται σε δύο διαφορετικές συνθήκες. Αξιοσημείωτο είναι ότι η Μηχανή διανυσμάτων υποστήριξης (SVM) είχε ακρίβεια ανίχνευσης της τάξης του 94% έως 97%. Πρέπει να αναφέρουμε οτι για την απόδειξη της απόδοσης του προτεινόμενου πλαισίου ασφαλείας, υλοποίησαν μια εφαρμογή ανίχνευσης Βιοχαρτικών επιληπτικών κρίσεων ως μελέτη. Το HT υλοποιείται στη φάση σχεδιασμού και ενεργοποιείται εσωτερικά. Υπάρχουν δύο διαφορετικοί τρόποι ενεργοποίησης στην εργασία αυτή οι οποίοι είναι: Always-on και Condition-based. Καθώς όπως κα τα ονόματα υποδηλώνουν , οι Always-on HT είναι πάντα ενεργοί και μπορούν να περιλαμβάνουν κακόβουλη δραστηριότητα ανά πάσα στιγμή, ενώ τα βασισμένα σε συνθήκες Trojans ενεργοποιούνται υπό συγκεκριμένες συνθήκες. Στην εργασία των Kulkarni, Pino, Mohsenin, η ενεργοποίηση Trojan βάσει συνθηκών υλοποιείται σε εσωτερικές καταστάσεις της λογικής μετά από συγκεκριμένο αριθμό μεταφορών από πυρήνα σε πυρήνα ή κύκλων ρολογιού. Στο πλαίσιο αυτής της επίθεσης, ο δρομολογητής επιλέγει έναν τυχαίο πυρήνα για τη μεταφορά των δεδομένων. Η επίθεση αυτή επηρεάζει την προθεσμία για τους άλλους πυρήνες, οι οποίοι εξαρτώνται από το επιτιθέμενο πακέτο μεταφοράς. Οι επιθέσεις σε δρομολογητή πολλών πυρήνων μπορούν να επηρεάσουν τα πακέτα δικτύου ρυθμού μεταφοράς, τη διαθεσιμότητα του πυρήνα επεξεργασίας και τη διακοπή στην επικοινωνία του πυρήνα. Ο δρομολογητής μπορεί να δεχθεί εξωτερική επίθεση μέσω της μνήμης αρχιτεκτονικής διεπαφής, συγκεκριμένα την διεπαφή του πυρήνα ή εσωτερικά με αλλοίωση του πίνακα δρομολόγησης που περιλαμβάνει διάφορες επιθέσεις, όπως εκτροπές κυκλοφορίας, βρόχοι δρομολόγησης, επιθέσεις παραποίησης πυρήνα. Όλες οι και οι τρεις επιθέσεις ονομάζονται επίσης επίθεση άρνησης παροχής υπηρεσιών (DoS), όπου ένας συγκεκριμένος πυρήνας που δέχεται επίθεση καθίσταται μη διαθέσιμος.

Εδώ να αναφέρουμε πως η Επίθεση εκτροπής της κυκλοφορίας Είναι μια πολύ κοινή επίθεση στην αρχιτεκτονική δρομολογητών πολλών πυρήνων. Στο πλαίσιο αυτής της επίθεσης, ο δρομολογητής επιλέγει έναν τυχαίο πυρήνα για τη μεταφορά των δεδομένων. Αυτή η επίθεση επηρεάζει την προθεσμία για τους άλλους πυρήνες, οι οποίοι εξαρτώνται από το επιτιθέμενο πακέτο μεταφοράς [28]

Σε αυτό το σημείο πρέπει να αναφερθεί πως το Support Vector Machine (SVM) η αλλιώς Μηχάνημα Διανυσματικής Υποστήριξης κάνει την αντιστοίχιση των δεδομένων σε έναν χώρο χαρακτηριστικών υψηλής διάστασης, έτσι ώστε τα σημεία των δεδομένων να μπορούν να κατηγοριοποιηθούν, ακόμη και όταν τα δεδομένα δεν είναι διαφορετικά γραμμικά διαχωρίσιμα. υπάρχει ένας διαχωριστής μεταξύ των κατηγοριών, που στη συνέχεια τα δεδομένα μετασχηματίζονται με τέτοιο τρόπο ώστε ο διαχωριστής να μπορεί να σχεδιαστεί ως υπερεπίπεδο. Κατόπιν αυτού, τα χαρακτηριστικά των νέων δεδομένων μπορούν να χρησιμοποιηθούν για την πρόβλεψη της ομάδας στην οποία θα πρέπει να ανήκει μια νέα εγγραφή.

Κεφάλαιο 5 ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Συμπεράσματα

Ύστερα από τη μελέτη που πραγματοποιήθηκε στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας καταλήγουμε στο συμπέρασμα ότι από τη ραγδαία εξέλιξη της τεχνολογίας, πέρα από τα πολλά οφέλη που επιφέρει στους χρήστες της, μπορεί να προκύψουν και ορισμένες δυσάρεστες καταστάσεις. Οι περισσότεροι άνθρωποι στις μέρες μας χρησιμοποιούν τις ασύρματες επικοινωνίες στην καθημερινότητά τους. Όμως δεν είναι σε θέση να γνωρίζουν πόσο ασφαλείς είναι οι συσκευές που χρησιμοποιούν ολοένα και περισσότερο στην καθημερινή τους ζωή καθώς και οι εταιρίες που τις παράγουν. Όπως έχουμε ήδη αναφέρει σε προηγούμενα κεφάλαια της συγκεκριμένης πτυχιακής εργασίας τα Hardware Trojan αποτελούν μια σχετικά καινούργια τάση της εποχής που ζούμε. Πρόκειται για κακόβουλες επιθέσεις, οι οποίες έχουν τη δυνατότητα να προκαλέσουν σοβαρά προβλήματα στα ολοκληρωμένα κυκλώματα. Οι επιθέσεις υλικού Hardware Trojan και γενικότερα ο κλάδος των Hardware Trojans προβληματίζει τους επιστήμονες ιδιαίτερα την τελευταία δεκαετία.

Δεν υπάρχει πλέον καμία αμφιβολία ότι τα σύγχρονα ολοκληρωμένα κυκλώματα, τα οποία αναπτύσσονται και κατασκευάζονται στις μέρες μας έχουν τον κίνδυνο να υποστούν κάποιου είδους κακόβουλη τροποποίηση στο υλικό. Όπως έχουμε ήδη αναφέρει μια κακόβουλη προσπάθεια αλλαγή σε ένα ολοκληρωμένο κύκλωμα μπορεί να πραγματοποιηθεί σε πολλά και διαφορετικά τμήματα τόσο κατά τη διαδικασία σχεδιασμού όσο και κατά τη διαδικασία κατασκευής του. Συμπεραίνουμε ότι, οι αντίπαλοι που επιθυμούν να τοποθετήσουν ένα Trojan υλικού στο προς ανάπτυξη ολοκληρωμένο κύκλωμα δεν δυσκολεύονται να το πράξουν. Ο λόγος που συμβαίνει αυτό, είναι διότι οι εταιρίες ανάπτυξης ολοκληρωμένων κυκλωμάτων αναθέτουν σε άλλες εταιρίες από όλα τα μήκη και πλάτη του πλανήτη να αναλάβουν πολλά και διαφορετικά τμήματα για την ολοκλήρωσή τους.

Ύστερα από τη μελέτη που πραγματοποιήθηκε στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας συμπεραίνουμε ότι υπάρχουν πολλά και διαφορετικά είδη επιθέσεων Trojan που μπορούν να βλάψουν ένα ολοκληρωμένο κύκλωμα με ποικίλους τρόπους. Επίσης, αξιοσημείωτο είναι το γεγονός ότι οι διάφορες επιθέσεις Trojan που έχουν παρατηρηθεί

από την αρχή της εμφάνισής τους έως και σήμερα έχουν διαφορετικούς τρόπους με τους οποίους μπορούν να ενεργοποιηθούν όταν είναι ήδη τοποθετημένα μέσα στο αντίστοιχο ολοκληρωμένο κύκλωμα.

Υπάρχει όμως ορισμένα κοινά σημεία όσον αφορά όλες τις επιθέσεις Trojan. Αρχικά, σε όλες τις περιπτώσεις, οι σχεδιαστές των αντίστοιχων ολοκληρωμένων κυκλωμάτων δεν έχουν καμία ιδέα για την τοποθέτηση των αντίστοιχων επιθέσεων Trojan στο εσωτερικό τους. Ένα δεύτερο κοινό στοιχείο που παρατηρείται σε όλες τις κακόβουλες επιθέσεις υλικού Trojan είναι ο στόχος της τοποθέτησης τους. Πιο συγκεκριμένα, ο κύριος στόχος τους είναι να προξενήσουν κακό στο προς επίθεση ολοκληρωμένο κύκλωμα και κατ' επέκταση στη φήμη της αντίστοιχης εταιρίας.

Ένα ακόμα χαρακτηριστικό στον τομέα των επιθέσεων Trojan, το οποίο ποικίλει ανά περίπτωση είναι οι συνέπειες που προκαλούν με την ενεργοποίησή τους. Πιο αναλυτικά, μια επίθεση υλικού Trojan θα μπορούσε να προκαλέσει από μια μικρή τροποποίηση σε συγκεκριμένα τμήματα του ολοκληρωμένου κυκλώματος, με σκοπό να αλλάξουν τα προς μετάδοση σήματα. Από την άλλη μεριά, υπάρχουν επιθέσεις υλικού Hardware Trojan, οι οποίες μπορούν να προκαλέσουν τροποποιήσεις μέσω των οποίων να διαρρεύσουν προς τον επιτιθέμενο προσωπικά δεδομένα όπως είναι λόγου χάριν οι προσωπικοί κωδικοί καθώς και οι τραπεζικές κάρτες. Τέλος, μια πλέον καταστροφική συνέπεια από μια επίθεση Trojan σε ένα ολοκληρωμένο κύκλωμα είναι να προκαλέσει τη πλήρη καταστροφή του.

Για τους λόγους και τις συνέπειες από τις κακόβουλες τροποποιήσεις Hardware Trojan που αναφέραμε προηγουμένως και αναλύσαμε περαιτέρω στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας, οι επιστήμονες δεν θα μπορούσαν να μείνουν αδρανής. Η επιστημονική κοινότητα, λοιπόν συνεχώς αναζητά και αναπτύσσει καινούργιες μεθόδους ανίχνευσης των κακόβουλων αυτών επιθέσεων προς το υλικό. Οι διάφοροι μέθοδοι που έχουν χρησιμοποιηθεί κατά καιρούς έχουν στηριχθεί σε διάφορα στοιχεία που υπάρχουν μέσα σε ένα ολοκληρωμένο κύκλωμα και της τροποποίησης υλικού, με σκοπό να ανιχνευθούν οι κακόβουλες προσθήκες μέσα στο εκάστοτε ολοκληρωμένο κύκλωμα. Ωστόσο μετά από έρευνες γύρω από το θέμα των επιθέσεων υλικού Hardware Trojan και των τρόπων ανίχνευσης τους, έχουν παρατηρηθεί ότι σε πολλές περιπτώσεις το ποσοστό σωστής ανίχνευσης των Trojan στο υλικό είναι ιδιαίτερα υψηλό. Αυτό το γεγονός είναι

ιδιαίτερα ενθαρρυντικό και σημαντικό για τους σχεδιαστές των ολοκληρωμένων κυκλωμάτων, διότι οι τεχνικές ανίχνευσης των επιθέσεων στο υλικό αποδεικνύονται ικανοποιητικά αποδοτικές και έχουν τη δυνατότητα να αποφύγουν τις καταστροφικές συνέπειες από την ενεργοποίηση τους.

Οι πιο πρόσφατες και σύγχρονες μελέτες όσον αφορά την ανίχνευση των κακόβουλων επιθέσεων υλικού Hardware Trojan είναι πολλά υποσχόμενες. Οι συγκεκριμένες προσεγγίσεις έχουν τη δυνατότητα να ανανεώνονται με βάση τις πληροφορίες και τα δεδομένα τα οποία λαμβάνουν, με αποτέλεσμα να αντιμετωπίζουν με δυναμικό τρόπο τις διαδικασίες ανίχνευσης των κακόβουλων επιθέσεων όσον αφορά τα Hardware Trojan. [22] Στις μέρες μας, οι συγκεκριμένες συνεχώς εξελισσόμενες μεθόδους ανίχνευσης αποτελούν πλέον σημαντική απειλή για τους αντιπάλους που δημιουργούν και ενσωματώνουν οποιουδήποτε είδους επίθεση Hardware Trojan στο προς ανάπτυξη ολοκληρωμένο κύκλωμα.

5.2 Μελλοντικές εξελίξεις

Όπως έχουμε ήδη αναφέρει η τεχνολογία και οι υπηρεσίες που αυτή προσφέρει συνεχώς στους χρήστες της αναπτύσσονται με ραγδαίους ρυθμούς. Αυτό έχει ως αποτέλεσμα οι αντίπαλοι να επωφελούνται συνεχώς από την συγκεκριμένη ραγδαία ανάπτυξη. Δημιουργούν λοιπόν, με σύμμαχο τους την εξελισσόμενη τεχνολογία, Hardware Trojan με περισσότερες δυνατότητες. Με την πάροδο των χρόνων, οι αντίπαλοι θα δημιουργούν πιο ισχυρά Hardware Trojan, προκειμένου να επιτύχουν τον σκοπό τους, ο οποίος δεν είναι άλλος από το να προκαλούν καταστροφικές συνέπειες στο προς επίθεση ολοκληρωμένο κύκλωμα και κατ’ επέκταση στη φήμη της εταιρίας που το κατασκευάζει.

Ένας επιπλέον μελλοντικός στόχος που έχουν οι αντίπαλοι που δημιουργούν τις αντίστοιχες επιθέσεις υλικού Hardware Trojans είναι να κατασκευάζουν Trojans τα οποία θα είναι όσο τον δυνατόν λιγότερο ανιχνεύσιμα από τους κατασκευαστές των ολοκληρωμένων κυκλωμάτων. Και στο σημείο αυτό, επίσης βοηθάει σε πολύ μεγάλο βαθμό η μελλοντική εξέλιξη της τεχνολογίας, καθώς με την πάροδο του χρόνου τα Hardware Trojans γίνονται συνεχώς ισχυρότερα.

Από την άλλη μεριά, οι εταιρίες σχεδιασμού ολοκληρωμένων κυκλωμάτων προσπαθούν συνεχώς να προσαρμόζονται στις καινούργιες αλλαγές και στα συνεχώς ανανεωμένα

Hardware Trojan. Έχοντας πλήρη επίγνωση για την εξέλιξη της τεχνολογία και κατά συνέπεια την εξέλιξη των επιθέσεων στα ολοκληρωμένα κυκλώματα που θα πραγματοποιηθεί σε πολύ μεγάλο βαθμό μελλοντικά στα επόμενα χρόνια, δεν θα πρέπει να μένουν αδρανής. Έχουν τη δυνατότητα οι εταιρίες σχεδιασμού των ολοκληρωμένων κυκλωμάτων να εντοπίσουν και να σταματήσουν τις πολύ αρνητικές και καταστροφικές συνέπειες που θα δημιουργηθούν στο προς επίθεση υλικό με την ενεργοποίηση των αντίστοιχων Hardware Trojan.

Θα πρέπει επομένως όλες οι εταιρίες σχεδιασμού και κατασκευής των ολοκληρωμένων κυκλωμάτων να προσαρμόζονται στις μελλοντικές εξελίξεις της τεχνολογίας και κατ' επέκταση στις μελλοντικές εξελίξεις των επιθέσεων υλικού – Hardware Trojan. Στόχος των εταιριών ανάπτυξης των ολοκληρωμένων κυκλωμάτων όπως έχουμε ήδη αναφέρει είναι η έγκυρη ανίχνευση των επιθέσεων Trojan. Με την έννοια έγκυρη ανίχνευση των Hardware Trojans αναφερόμαστε στην ανίχνευσή τους πριν πραγματοποιηθεί η ενεργοποίησή τους, και επιβαρυνθούν από τις καταστροφικές συνέπειες που επιφέρουν. Υπάρχουν ήδη πολύ σημαντικές και εξίσου αποτελεσματικές μέθοδοι για την ανίχνευση τους. Είναι όμως ιδιαίτερα σημαντικό όσο τα χρόνια περνούν και μελετιούνται σε βάθος τα Hardware Trojan, να αναπτυχθούν καινούργιες πιο εξελιγμένες αλλά εξίσου αποτελεσματικές μέθοδοι που αποσκοπούν στην ανίχνευση των αντίστοιχων Hardware Trojan μέσα σε ένα ολοκληρωμένο κύκλωμα.

Πέρα από την μελέτη και την έρευνα που πραγματοποιήθηκε στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας, υπάρχουν επίσης μελλοντικές κατευθύνσεις και μονοπάτια όσον αφορά τον τομέα των Hardware Trojan. Στο σημείο αυτό, θεωρούμε σκόπιμο να αναφέρουμε ορισμένα μελλοντικά ερευνητικά θέματα που θα απασχολήσουν τους επιστήμονες στο μέλλον.

Πιο πολύπλοκες επιθέσεις Hardware Trojan. Ένας ερευνητικός προβληματισμός που θα παραμείνει και μελλοντικά ως σημείο εκτεταμένης έρευνας και μελέτης από τους επιστήμονες είναι η τοποθέτηση πιο σύνθετων και εξίσου ισχυρών επιθέσεων σε ένα ολοκληρωμένο κύκλωμα, η οποία θα λαμβάνει χώρα με την ενεργοποίηση του αντίστοιχου Trojan. Θα πρέπει να πραγματοποιηθεί μελέτη για τη σωστή αντιμετώπιση των επιθέσεων και να αναπτυχθούν τα κατάλληλα αντίμετρα για την έγκυρη αντιμετώπισή τους. Ο λόγος που θα πρέπει να βρεθούν αποτελεσματικοί τρόποι για την ανίχνευση και την

αντιμετώπιση τέτοιου είδους επιθέσεων είναι διότι όταν το Trojan ενεργοποιηθεί και ελέγχεται πλέον από τον αντίπαλο που το έχει τοποθετήσει στο αντίστοιχο υλικό μπορεί να υπάρξει ανεπιθύμητη διαρροή μυστικών και προσωπικών δεδομένων καθώς και η καταστροφική συνέπεια της δυσλειτουργίας του εκάστοτε προς επίθεση υλικού. Οι τροποποιήσεις στο εκάστοτε υλικό μπορεί να διαφέρουν ανάλογα το αντίστοιχο Trojan και το λόγο για τον οποίο δημιουργήθηκε. Όπως έχουμε ήδη αναφέρει υπάρχουν πολλά και διαφορετικά είδη επιθέσεων υλικού Hardware Trojans. Επομένως θα ήταν σκόπιμο μελλοντικά να μελετάτε και η αποτελεσματικότητά τους ως προς το ποσοστό ανίχνευσής τους κατά τη διαδικασία των δοκιμών.

Αυτοματοποιημένη ανάλυση αδύναμων σημείων. Στις μέρες μας δημιουργείται ολοένα και περισσότερο η ανάγκη για την ύπαρξη εργαλείων CAD, τα οποία αποσκοπούν στην αυτοματοποιημένη ανάλυση ενός σχεδίου. Η συγκεκριμένη ανάλυση αφορά τόσο την αξιοπιστία του εκάστοτε σχεδίου όσο και την ευαισθησία του στις κακόβουλες τροποποιήσεις που μπορεί να προκληθούν από τα διάφορα είδη Hardware Trojans. Μελλοντικά οι ερευνητές θα πρέπει να αναζητούν τέτοιου είδους εργαλεία προκειμένου να αξιολογείται κατά πόσο είναι αξιόπιστο ένα IP, το οποίο έχει ενσωματωθεί σε ένα ολοκληρωμένο κύκλωμα. Ο σκοπός της ύπαρξης τέτοιων εργαλείων είναι προκειμένου να βοηθήσουν να καταλάβουμε μια πιθανή κακόβουλη συμπεριφορά σε ένα IP, πριν αυτό χρησιμοποιηθεί από έναν σχεδιαστή SoC. Επίσης, το εργαλείο που θα πρέπει να αναπτυχθεί θα πρέπει να είναι ικανό να αναλύει κατά πόσο ένα σχέδιο υλικό είναι ευαίσθητο και διαθέτει ευάλωτα σημεία σε μια πιθανή επίθεση.

Μετρήσεις και σημεία αναφοράς. Ένα επιπλέον σημείο μελλοντικής μελέτης από τους ερευνητές του κλάδου είναι για τα εργαλεία CAD. Πιο αναλυτικά αναφερόμαστε στην ανάπτυξη συγκεκριμένων μετρήσεων καθώς και σημεία αναφοράς για τα διάφορα επίπεδα που υφίστανται κατά τη διαδικασία ανάπτυξης του εκάστοτε υλικού. Είναι σκόπιμο λοιπόν να βρεθούν εργαλεία τα οποία να αποσκοπούν στη διαδικασία πραγματοποίησης τέτοιου είδους μετρήσεων. Με δεδομένο ότι μπορούν να λαμβάνουν διαφορετικές πτυχές της αξιολόγησης και καταλήγοντας σε μια συνολική αναφορά όσον αφορά την εμπιστοσύνη και την αξιοπιστία.

Επαλήθευση εμπιστοσύνης. Η αξιοπιστία και η ανοχή σφαλμάτων εξετάζει τον τρόπο κατασκευής συστημάτων έτσι ώστε να μην συμβαίνει η φυσική αστοχία μεμονωμένων

εξαρτημάτων και να καταρρίψει όλο το σύστημα.. Όπως έχουμε ήδη αναφέρει δεν υπάρχει συγκεκριμένη λύση, η οποία να έχει τη δυνατότητα να παρέχει προστασία με αποτελεσματικό τρόπο για όλες τις επιθέσεις Hardware Trojan όλων των διαφορετικών τύπων που έχουν παρατηρηθεί κατά καιρούς. Αυτό έχει χαρακτηριστεί από τους επιστήμονες του κλάδου ως μια εξαιρετικά δύσκολη διαδικασία. Φτάνουμε λοιπόν στο συμπέρασμα ότι ένα ενεργό θέμα που θα απασχολήσει τους επιστήμονες και μελλοντικά όσον αφορά τον κλάδο των Hardware Trojan είναι η αποτελεσματική επαλήθευση εμπιστοσύνης και αξιοπιστίας. Όπως είναι ήδη γνωστό από μελέτες που έχουν ήδη πραγματοποιηθεί η επαλήθευση της αξιοπιστίας επιτυγχάνεται μέσω λογικών δοκιμών και ανάλυσης πλευρικών καναλιών. Αυτές οι μέθοδοι παρ' όλα αυτά είναι τις περισσότερες φορές αποτελεσματικές όταν πρόκειται είτε για υποθετικές καταστάσεις είτε για συγκεκριμένους τύπους Hardware Trojans. Προκύπτει λοιπόν η επιτακτική ανάγκη για περαιτέρω έρευνα στο μέλλον από τους ερευνητές ως προς το πρόβλημα της επαλήθευσης εμπιστοσύνης στον τομέα των επιθέσεων Hardware Trojans.

Προσεγγίσεις Design-for-Security (DfS). Οι λύσεις που ήδη αναφέρθηκαν και αναλύθηκαν στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας όσον αφορά την επαλήθευση αξιοπιστίας αποτελούν ιδιαίτερα ελκυστικές λύσεις. Ο λόγος είναι διότι αφενός δεν επιβαρύνουν ούτε το υλικό αφετέρου δεν αλλοιώνουν τη διαδικασία σχεδιασμού του αντίστοιχου υλικού. Όμως δεν προσφέρουν πλήρης διασφάλιση όσον αφορά την ιδιότητα της εμπιστοσύνης. Θα μπορούσαν να προσφέρουν μεγαλύτερη εμπιστοσύνη, συνδυάζοντας κατάλληλα τις λύσεις επαλήθευσης αξιοπιστίας με τις πλέον σωστές σχεδιαστικές λύσεις. Κάθε υλικό που σχεδιάζεται θα πρέπει να βασίζεται στο γεγονός της αποτελεσματικότητας ώστε να κάνουν ένα Hardware Trojan να μπορεί να ενεργοποιείται εύκολα στις δοκιμές που πραγματοποιούνται είτε να είναι εύκολη να το παρατηρήσουν οι σχεδιαστές του εκάστοτε υλικού. Επομένως, τα επόμενα χρόνια σίγουρα οι επιστήμονες του συγκεκριμένου κλάδου θα στρέψουν τις έρευνές τους στις αποτελεσματικές λύσεις σχεδιασμού χαμηλών εξόδων προκειμένου να αυξηθούν τα επίπεδα εμπιστοσύνης και αξιοπιστίας του υλικού.

Επιθέσεις Trojan σε συσκευές Nanoscale. Η συνεχώς αναπτυσσόμενη τεχνολογία στις μέρες μας έχει δημιουργήσει καινούργιες συσκευές νανοκλίμακας, οι οποίες διαθέτουν σημαντικές και ενδιαφέρουσες ιδιότητες. Πρόκειται για συσκευές που θα απασχολήσουν μελλοντικά, καθώς χαρακτηρίζονται από την πολλά υποσχόμενη συμπεριφορά τους.

Αξιοσημείωτο είναι το γεγονός ότι τέτοιου είδους συσκευές νανοκλίμακας πρόκειται να αλλάξουν σε πολύ μεγάλο βαθμό τις έννοιες και τις λειτουργίες των Hardware Trojan που γνωρίζουμε μέχρι σήμερα. Είναι σημαντικό λοιπόν να αναφέρουμε ότι οι επιστήμονες θα επικεντρωθούν μελλοντικά στις επιθέσεις υλικού Hardware Trojan που αφορούν συσκευές Νανοκλίμακας καθώς και σε προσεγγίσεις σχεδιασμού τέτοιου είδους συσκευών, οι οποίες να είναι ανθεκτικές σε κακόβουλες επιθέσεις Trojan.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] S. B. ·. M. M. Tehranipoor, The Hardware Trojan War, Attacks, Myths and Defenses, Springer, 2018.

[2] Chen Dong; Guorong He; Ximeng Liu; Yang Yang; Wenzhong Guo, "A Multi-Layer Hardware Trojan Protection Framework for IoT Chips," 05 February 2019. [Online].

[3] Rajat Subhra Chakraborty, Seetharam Narasimhan and Swarup Bhunia, "Hardware Trojan: Threats and Emerging Solutions," 2018. [Online].

[4] Mingfu Xue,Chongyan Gu,Weiqiang Liu,Shichao Yu,Máire O'Neill, "Ten years of hardware Trojans: a survey from the attacker's perspective," 30 September 2020. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-cdt.2020.0041.

[5] Secureic, "https://www.secure-ic.com/blogpost/hardware-trojans/," 8 July 2021. [Online].

[6] Samer Moein; Thomas Aaron Gulliver; Fayez Gebali; Abdulrahman Alkandari, "A New Characterization of Hardware Trojans," 01 June 2016. [Online].

[7] Swarup Bhunia; Michael S. Hsiao; Mainak Banga; Seetharam Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," 15 July 2014. [Online].

[8] K. Alexios, "Hardware Trojan Threat Taxonomies (2017-2020)," 2020. [Online]. Available: https://www.grin.com/document/1138728.

[9] Nagata M., Danger J. L., and Miura N., "Creating a safe and robust digitally-connected," 25 July 2018. [Online].

[10] W. Y. &. L. P. Han T., "Hardware Trojans Detection at Register Transfer Level Based on Machine Learing," IEEE International Symposium on Circuits and Systems, 2019, pp. 1 - 5.

[11] Techpress, "https://www.techpress.gr/index.php/archives/124082," 25 Ιουλίου 2017. [Online].

[12] Catherine Rooney, Amar Seeam, Xavier Bellekens, "Creation and Detection of Hardware Trojans Using Non-Invasive Off-The-Shelf Technologies," 22 July 2018. [Online].

[13] "Laboratory of Digital Systems and Computer Architecture," [Online]. Available: http://arch.icte.uowm.gr/mdasyg/book/embedded/chapter04.pdf.

[14] Angela_Raucher, "Hardware trojan attacks and countermeasures," 11 2015. [Online]. Available: https://www.techdesignforums.com/practice/guides/hardware-trojan-security-countermeasures/.

[15] Ramesh Karri and Jeyavijayan Rajendran, Kurt Rosenfeld, Mohammad Tehranipoor,, "TRUSTWORTHY HARDWARE: IDENTIFYING AND CLASSIFYING HARDWARE TROJAN," October 2010. [Online]. Available: https://static.googleusercontent.com/media/research.google.com/el//pubs/archive/37398.pdf.

[16] Chen Dong; Yulin Liu; Jinghui Chen; Ximeng Liu; Wenzhong Guo; Yuzhong Chen, "An Unsupervised Detection Approach for Hardware Trojans d," 13 July 2020. [Online].

[17] Wei S., Li K., Koushanfar F., & Potkonjak M., "Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry," 2012, pp. 90 - 95.

[18] Triskelelabs, "What are the possibilities of hardware Trojans in 2021?," 2020. [Online]. Available: https://www.triskelelabs.com/blog/what-are-the-possibilities-of-hardware-trojans-in-2021.

[19] N. Das, M. Saha and B. K. Sikdar, "Hard to Detect Combinational Hardware Trojans," 15 December 2018. [Online].

[20] Bhunia S., Hsiao M. S., Banga M., and Narasimhan S, "Hardware Trojan attacks: threat analysis and countermeasures.," 2014, pp. 1229 - 1247.

[21] Roshni Shende; Dayanand D. Ambawade, "A side channel based power analysis technique for hardware trojan detection using statistical learning approach," 21 July 2016. [Online].

[22] ZhiQiang Zhao; GaiGai Yang; Lei Li; Zhen Li; Jia Li, "A novel technique for defending hardware Trojan circuit," 19 March 2015. [Online].

[23] Geensforgeens, "Hardware Trojan," 7 May 2021. [Online]. Available:

https://www.geeksforgeeks.org/hardware-trojan/.

[24] Chen Dong, Yi Xu,Ximeng Liu, Fan Zhang, Guorong He and Yuzhong Chen, "Hardware Trojans in Chips: A Survey for Detection and Prevention," 2020 September 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7570641/.

[25] Lin Ni; Shaoqing Li; Jihua Chen; Pei Wei; Zhixun Zhao, " THE INFLUENCE ON SENSITIVITY OF HARDWARE TROJANS DETECTION BY TEST VECTOR," 22 May 2017. [Online].

[26] Lin Ni; Shaoqing Li; Jihua Chen; Pei Wei; Zhixun Zhao, "The influence on sensitivity of hardware Trojans detection by test vector," 24 May 2014. [Online].

[27] Bhunia Swarup, Michael S. Hsiao, Mainak Banga, & Seetharam Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," August 2014. [Online]. Available: https://www.researchgate.net/publication/264124590_Hardware_Trojan_Attacks_Threat_Analysis_and_Countermeasures.

[28] Amey Kulkarni, Youngok Pino, and Tinoosh Mohsenin, "SVM-based Real-Time Hardware Trojan Detection for Many-Core Platform," 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7479228.