ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Επισκόπηση των κατηγοριών και τεχνικών ανίχνευσης Hardware Trojans

Διπλωματική Εργασία

Γεώργιος Δημόπουλος - Μαρινέλης

Επιβλέπων: Γεώργιος Σταμούλης

Ιούνιος 2023

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

A survey on Hardware Trojan taxonomy and detection techniques

Diploma Thesis

Georgios Dimopoulos - Marinelis

Supervisor: Georgios Stamoulis

June 2023

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων	**Γεώργιος Σταμούλης** Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Φώτιος Πλέσσας** Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Αντώνιος Δαδαλίαρης** Επίκουρος Καθηγητής, Τμήμα Πληροφορικής & Τηλεπικοινωνιών, Σχολή Θετικών Επιστημών, Πανεπιστήμιο Θεσσαλίας

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

Γεώργιος Δημόπουλος - Μαρινέλης

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Georgios Dimopoulos - Marinelis

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή Γεώργιο Σταμούλη για την ευκαιρία που μου έδωσε να δουλέψω τη διπλωματική μου εργασία σε ένα θέμα που βρίσκω πολύ ενδιαφέρον.

Επίσης θα ήθελα να ευχαριστήσω τον διδάκτορα Δημήτριο Γαρυφάλλου για την πολύτιμη βοήθεια και καθοδήγηση καθώς και για τη συνεργασία του.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για τη στήριξη και την αγάπη που μου δείξανε κατά τα ακαδημαικά μου χρόνια.

Διπλωματική Εργασία

Επισκόπηση των κατηγοριών και τεχνικών ανίχνευσης Hardware Trojans

Γεώργιος Δημόπουλος - Μαρινέλης

Περίληψη

Στις μέρες μας, λόγω της γρήγορης ανάπτυξης της τεχνολογίας, τα ολοκληρωμένα κυκλώματα έχουν μια εκτενή αλληλεπίδραση με την καθημερηνότητα μας. Ο σχεδιασμός ολοκληρωμένων κυκλωμάτων έχει μια μεγάλη γκάμα περιορισμών από το frontend μέχρι το backend. Εκμεταλλευόμενες αυτούς τους περιορισμούς, κακόβουλες απειλές, όπως τα Hardware Trojans, αλλοιώνουν το σχεδιασμό των κυκλωμάτων και παίζουν ένα πολύ σημαντικό ρόλο στην ασφάλεια υλικού. Αυτή η Διπλωματική Εργασία εστιάζει σε κάθε πτυχή της απειλής των Hardware Trojans. Αρχικά, περιγράφεται συνοπτικά η λογική των Hardware Trojans και ο τρόπος με τον οποίο εισάγονται στις συσκευές. Προσεγγίζεται η ταξινόμηση των κακόβουλων απειλών σύμφωνα με τα χαρακτηριστικά τους και τον τρόπο ενεργοποίησης τους. Ακόμη, περιγράφονται και αναλύονται διεξοδικά οι τεχνικές ανίχνυσης ως αντίμετρα που βοηθούν στην αντιμετώπισης της απειλής των Hardware Trojans.

Λέξεις-κλειδιά: Hardware Trojan, ολοκληρωμένα κυκλώματα, ταξινόμηση, τεχνικές ανίχνευσης

Diploma Thesis

A survey on Hardware Trojan taxonomy and detection techniques

Georgios Dimopoulos - Marinelis

Abstract

Nowadays integrated circuits have a vast interaction with our daily lives since the technology development is rapid. Integrated circuits design has a majority of constraints from frontend to backend. Taking advantage of these constraints, malicious threaths, like Hardware Trojans, modify the design of the circuits and play a crucial role in hardware security. This thesis concentrates on every aspect of the Hardware Trojan threat. The logic of Hardware Trojans is briefly described along with the way they are inserted in the devices.The taxonomy of malicious threats is approached according to the characteristics and the way that Hardware Trojans are triggered. Furthermore, detection techniques are outlined and thoroughly analyzed as countermeasures helping with the threat of Hardware Trojans.

Keywords: Hardware Trojan, integrated circuits, taxonomy, detection techniques

Πίνακας Περιεχομένων

Πίνακας εικόνων

Συντομογραφίες

Διπλωματική Εργασία (ΔΕ)

Ολοκληρωμένο Κύκλωμα (Integrated Circuit -- IC)

Hardware Trojan (HT)

Ολοκληρωμένα Κυκλώματα Ειδικής Εφαρμογής (Application Specific Integrated Circuit -ASIC)

Επεξεργαστές Ψηφιακών Σημάτων (Digital Signal Processors – DSP)

Γλώσσας Περιγραφής Υλικού (Hardware Description Language - HDL)

Επίπεδο Μεταφοράς Καταχωρητή (Register Transfer Level - RTL)

Global Positioning System (GPS)

Χημική Μηχανική Στίλβωση (Chemical Mechanical Polishing – CMP)

Ηλεκτρονικό Μικροσκόπιο Σάρωσης (Scanning Electron Microscope – SEM)

Οπτικό Μικροσκόπιο Σάρωσης (Scanning Optical Microscope - SOM)

Ανάλυση Απεικόνισης σε Πικο–Δεύτερα (PiCosecond Imaging Analysis - PICA)

Απεικόνιση Αντίθετης Τάσης (Voltage Contrast Imaging - VCI)

Μεταβολή Τάσης από Φως (Light Included Voltage Alteration - LIVA)

Μεταβολή Τάσης από Φορτίο (Charge-Included Voltage Alteration – CIVA)

Multiple Excitation of Rare Occurrence (MERO)

Κεφάλαιο 1 Εισαγωγή

Οι επιθέσεις στα ολοκληρωμένα κυκλώματα (Integrated Circuit -- ICs) αποτελούν μια σημαντική απειλή στις μέρες μας, καθώς η τεχνολογία αναπτύσσεται ταχύτερα μέρα με τη μέρα και έχει σημαντικό ρόλο στην καθημερινότητα των ανθρώπων. Οι άνθρωποι πρέπει να νιώθουν ασφαλείς όταν χρησιμοποιούν ηλεκτρονικές συσκευές, και για να γίνει αυτό, περισσότερες απειλές πρέπει να εντοπιστούν και να διαχειριστούν. Η εφαρμογή κακόβουλης λογικής σε ICs είναι μια από αυτές τις απειλές. Μπορούν να οριστούν σε διάφορες μορφές, όπως επιπλέον πύλες μέσα στη λογική ενός τσιπ υπολογιστή ή Hardware Trojans μέσα σε ένα ολοκληρωμένο κύκλωμα, οι οποίες επιτρέπουν στον εισβολέα να πάρει μη θεμιτή πρόσβαση στο σύστημα. Μόλις το λογισμικό προσβληθεί από την απειλή, ο δημιουργός της μπορεί να διαβάσει τα δεδομένα του συστήματος. Η περιγραφόμενη λοιπόν απειλή, οδηγεί στην ολική έλλειψη ασφάλειας, που μπορεί να είναι καταστροφική για το χρήστη ή ακόμα και για τον οργανισμό αν η συσκευή χρησιμοποιείται για εταιρικούς σκοπούς.

1.1 Αντικείμενο της διπλωματικής

Καθώς οι απειλές από την εφαρμογή κακόβουλης λογικής σε ICs είναι ένα πολύ φλέγον ζήτημα, σε αυτή τη διπλωματική θα αναλυθούν οι κύριες έννοιες ασφάλειας υλικού και η συσχέτιση τους με τα σχετικά ερευνητικά θέματα. Επιπλέον, θα εξεταστούν νέα θέματα ασφάλειας υλικού συνυφασμένα με την ύπαρξη Hardware Trojan, στα οποία θα διερευνηθεί το περιθώριο μελλοντικής εξέλιξης του.Το γεγονός αυτό καθιστά την εν λόγω διπλωματική εργασία μια καλή προσπάθεια στις συνολικές προσπάθειες για έρευνα στον συγκεκριμένο κλάδο. Πιο αναλυτικά, η συνεισφορά και ο στόχος της διπλωματικής εργασίας (ΔΕ) αυτής είναι:

- Να διερευνηθούν οι ερευνητικές προσπάθειες που έχουν πραγματοποιηθεί σε αυτόν τον κλάδο.
- Να γίνει μια ολική κατανόηση των προκλήσεων στον κλάδο της ασφάλειας του υλικού.
- Να αναζητηθούν εργαλεία και λύσεις για την διαχείριση των θεμάτων στην ασφάλεια του υλικού.

1.2 Οργάνωση του τόμου

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στο θέμα και τους στόχους της εν λόγω διπλωματικής εργασίας.

Στο δεύτερο κεφάλαιο αναλύεται βιβλιογραφικά ο κλάδος της ασφάλειας υλικού και η απειλή από Hardware Trojans. Επιπλέον γίνεται περιγραφή του τρόπου με τον οποίο αυτά λειτουργούν με την ανάλυση ερευνητικών

αναφορών. Στο τρίτο κεφάλαιο πραγματοποιείταιαναφορά στην κατηγοριοποίηση των απειλών από Hardware Trojans σύμφωνα με τη δομή και τη λογική ενεργοποίησής τους.

Στο τέταρτο κεφάλαιο εξετάζονται οι διαθέσιμες ερευνητικές μέθοδοι για τον εντοπισμό των κακόβουλων απειλών.

Τέλος, στο πέμπτο κεφάλαιο γίνεται μια αναφορά συμπερασμάτων και πιθανών μελλοντικών ερευνητικών κατευθύνσεων στον συγκεκριμένο κλάδο.

Κεφάλαιο 2 Βιβλιογραφικό υπόβαθρο

2.1. Εισαγωγή

Με την ιλιγγιώδη επέκταση της πληροφορικής και το σημαντικό ρόλο που κατέχει στην καθημερινότητα μας, η πιθανότητα εφαρμογής κακόβουλης λογικής σε ICs είναι μεγαλύτερη από ποτέ [1].

Το 2008, ο Adee [2] ανέφερε ότι μια σημαντική αποτυχία σε ένα Σύριο ραντάρ μπορεί να είχε προκληθεί σκόπιμα μέσω της κρυμμένου εμπορικού μικροεπεξεργαστή. Σύμφωνα με Αμερικανικό ανταποκριτή άμυνας που μίλησε υπό τον όρο της ανωνυμίας, ένας 'Ευρωπαϊκός κατασκευαστής chip' κατασκεύασε πρόσφατα τέτοιους μικροεπεξεργαστές με απομακρυσμένους διακόπτες θανάτου για τέτοιους σκοπούς. Δεδομένων των ολέθριων συνεπειών που συνδέονται με τέτοιου είδους αδυναμίες, το αποκαλούμενο θέμα των Hardware Trojans (HT) έχει λάβει σημαντική προσοχή από την ακαδημαϊκή κοινότητα, τη βιομηχανία, και τις κυβερνήσεις κατά την τελευταία δεκαετία [2].

Όπως είναι εμφανές λοιπόν, η διαχείριση της ασφάλειας του υλικού συχνά συνδέεται με την ασφάλεια του κυβερνοχώρου, την κρυπτογραφία και το υλικό της. Η ασφάλεια ενός συστήματος πληροφορικής σχετίζεται άμεσα με την ασφάλεια του λογισμικού ή των δεδομένων που διαχειριζόμαστε. Το συγκεκριμένο υλικό που βοηθάει στη διαδικασία της επεξεργασίας των δεδομένων καταγράφεται ως αξιόπιστο αρχικά. Επικίνδυνες τροποποιήσεις υλικού, όπως οι απειλές Hardware Trojan που θα μελετηθούν, αποτελούν ισχυρές απειλές για το ηλεκτρονικό υλικό και παραβαίνουν την αρχική παραδοχή της εμπιστοσύνης του υλικού [2].

Τα επικοινωνιακά κυκλώματα γίνονται ολοένα και πιο ευάλωτα σε τέτοιου είδους απειλές από κακόβουλες δραστηριότητες και αλλοιώσεις. Η κατάσταση αυτή έχει δημιουργήσει σοβαρές ανησυχίες για πιθανές απειλές σε στρατιωτικά συστήματα, οικονομικές υποδομές και ασφάλεια μεταφορών. Το κακόβουλο υλικό μπορεί να σχεδιαστεί είτε για να απενεργοποιήσει είτε για να καταστρέψει ένα σύστημα μελλοντικά, αλλά και για να αποσπάσει ευάλωτη ή μυστική πληροφορία. Τα HTs μπορούν να εφαρμοστούν ως διαφοροποιήσεις υλικού σε Ολοκληρωμένα Κυκλώματα Ειδικής Εφαρμογής (ASIC), σε μικροεπεξεργαστές, μικροελεγκτές, επεξεργαστές δικτύων και Επεξεργαστές Ψηφιακών Σημάτων (DSP). Μπορούν επιπλέον να εφαρμοστούν ως τροποποιήσεις υλικού σε Συστοιχία Επιτόπια Προγραμματιζόμενων Πυλών (FPGA). Όλες οι παραπάνω ανησυχίες έχουν καταχωρηθεί σε σύγχρονες αναφορές του Αμερικανικού συμβουλίου αμυντικής επιστήμης, της Αμερικανικής γερουσίας και του διεθνούς οργανισμού εξοπλισμού ημιαγωγών και υλικών [3].

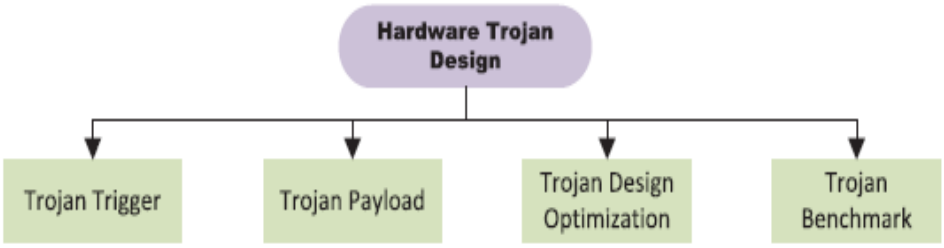
Η διαδικασία κατασκευής ενός IC περιέχει τρία βασικά στάδια: το σχεδιασμό (που περιλαμβάνει μοντέλα, εργαλεία και σχεδιαστές), την κατασκευή (που περιλαμβάνει τη δημιουργία της μάσκας, τη λιθογραφία και τη συσκευασία) και τον έλεγχο της παραγωγής. Στην διαδικασία σχεδιασμού ενός ASIC, το IC είναι σχεδιασμένο έχοντας χρησιμοποιήσει εργαλεία έμπιστων εταιρειών όπως το Synopsys, Cadence, Mentor Graphics κ.α.. Παρόλα αυτά, τα μοντέλα που χρησιμοποιούνται από το δημιουργό κατά τη σχεδίαση και από το χυτήριο στη διαδικασία μετασχεδιασμού, δε θεωρούνται έμπιστα. Το στάδιο της κατασκευής μπορεί επίσης να χαρακτηριστεί ως μη έμπιστο, καθώς ο επιτιθέμενος μπορεί να αντικαταστήσει τα γνήσια IC με ένα HT ή μπορεί να επηρεάσει τη διαδικασία κατασκευής εφαρμόζοντας ένα HT στη μάσκα του IC. Ο έλεγχος της παραγωγής θεωρείται έμπιστος, υπό την προυπόθεση πως πραγματοποιείται στο κέντρο ελέγχου παραγωγής του πελάτη.[3].

Υπάρχουν δύο βασικοί τρόποι για να επιβεβαιωθεί ότι το IC που χρησιμοποιεί ο πελάτης είναι αυθεντικό (δηλαδή πραγματοποιεί μόνο τις λειτουργίες για τις οποίες έχει προγραμματιστεί και τίποτα παραπάνω). Η πρώτη επιλογή είναι να γίνει όλη η διαδικασία κατασκευής με έμπιστες μεθόδους. Αυτή η επιλογή είναι απαγορευτικά ακριβή και σχεδόν αδύνατη με τις σύγχρονες τάσεις στην παγκόσμια διανομή των IC.

Η δεύτερη επιλογή είναι η επαλήθευση της αξιοπιστίας των κατασκευασμένων IC κατά την επιστροφή στον πελάτη. Η επιλογή αυτή προϋποθέτει, κατά τη διαδικασία του ελέγχου μετά την κατασκευή του IC, την επιβεβαίωση ότι πληρεί τις αυθεντικές λειτουργικές προδιαγραφές και τις σωστές προδιαγραφές επιδόσεων. Το τελευταίο βήμα αποκαλείται πιστοποίηση σχεδιασμού silicon [4].

Γενικά, οι τεχνικές ασφάλειας υλικού κάνουν διαφοροποιήσεις στο IC ώστε να αποτρέψουν τις επιθέσεις και να προστατεύσουν τα Intellectual Properties (IP) και τα κρυφά κλειδιά. Παρόλα αυτά, υπάρχουν και είδη απειλών που είναι τελείως διαφορετικά, που στοχεύουν να αλλοιώσουν κακοβούλως το σχεδιασμό πριν ή μετά την κατασκευή. Ο εντοπισμός τέτοιων απειλών είναι δύσκολος για διάφορους λόγους. Αρχικά, λόγω του μεγάλου όγκου μαλακών (Soft), σταθερών (Firm) και σκληρών πυρήνων (Hard) IP που χρησιμοποιούνται, όπως και λόγω της πολυπλοκότητας των IP, είναι δύσκολος ο εντοπισμός των μικρών κακόβουλων αλλοιώσεων. Έπειτα, τα χαρακτηριστικά των IC της κλίμακας μερικών νανομέτρων κάνουν τη φυσική επιθεώρηση πολύ δύσκολη και δαπανηρή. Επιπλέον, η διαδικασία της αντιστροφής καταστροφικής μηχανικής δεν εγγυάται πως τα IC θα απαλλαγούν από τα HT, ειδικά όταν αυτά έχουν εγκατασταθεί σε κάποιο μέρος του του τσιπ [4].

Επιπρόσθετα, τα κυκλώματα HT, από τον σχεδιασμό τους, ενεργοποιούνται κάτω από συγκεκριμένες συνθήκες, γεγονός που κάνει δύσκολη την ενεργοποίησή τους με τυχαίες ή λειτουργικές προσπάθειες. Ακόμη, οι έλεγχοι που γίνονται ώστε να εντοπίσουν τα λάθη της παραγωγής δεν μπορούν να εγγυηθούν την ανίχνευση των HT. Αυτοί οι έλεγχοι γίνονται σε κυκλώματα που δεν έχουν κάποιο κακόβουλο υλικό και κατά συνέπεια δεν μπορούν να εντοπίσουν ή να ενεργοποιήσουν κάποιο HT. Τέλος, καθώς τα φυσικά μεγέθη των χαρακτηριστικών μειώνονται λόγω των βελτιώσεων της λιθογραφίας, οι διαδικασίες και οι περιβαλλοντικές διαφοροποιήσεις έχουν μεγαλύτερη επιρροή στην πολυπλοκότητα των παραμέτρων των ICs. Έτσι, η ανίχνευση των HT με τη χρήση απλών αναλύσεων αυτών των παραμετρικών σημάτων δεν είναι αποτελεσματική [5].

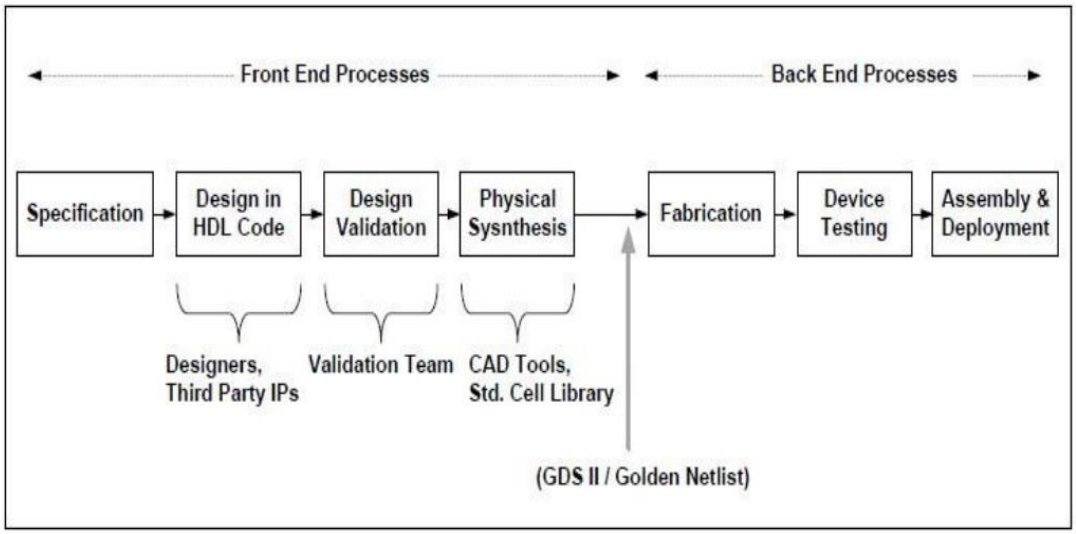


Εικόνα 2.1.: Σχεδιασμός HT [1]

Η υπάρχουσα έρευνα για το σχεδιασμό HT μπορεί να ταξινομηθεί σε τέσσερις κατηγορίες, όπως φαίνεται στην Εικόνα 2.1. Επειδή οι μηχανισμοί ενεργοποίησης και το ωφέλιμο φορτίο ενός HT καθορίζουν τη δυσκολία ενεργοποίησης και ανίχνευσης, αυτό έχει παρακινήσει τους ερευνητές να διερευνήσουν και να αξιολογήσουν νέους ενεργοποιητές και ωφέλιμα φορτία (Triggers and Payloads). Ένα παράδειγμα αποτελεί το γεγονός ότι οι νέοι ενεργοποιητές χρησιμοποιούν καταστάσεις don't-care σε ένα σχεδιασμό ή μηχανισμούς φθοράς του πυριτίου.

2.2. Ροή Σχεδίασης IC

Υπάρχει μια πληθώρα διαδικασιών οι οποίες εντάσσονται στον κύκλο της ζωής των σύγχρονων ICs.Για να θεωρηθούν ως ασφαλή τα κυκλώματα αυτά, θα πρέπει όλες αυτές οι διαδικασίες να είναι έμπιστες. Για να γίνουν αντιληπτοί οι τρόποι με τους οποίους μπορεί να αλλοιωθεί το υλικό, πρέπει πρώτα να είναι αντιληπτή η ροή σχεδίασης ενός IC.. Στην Εικόνα 2.2. φαίνονται οι ποικίλες διαδικασίες που εφαρμόζονται σε ένα σύνηθες κύκλο ζωής ολοκληρωμένου κυκλώματος. Δύο είναι τα βασικά στάδια του κύκλου ζωής ενός IC: πρώτα ο σχεδιασμός και έπειτα η κατασκευή. Ο σχεδιασμός (front-end) ορίζει το κύκλωμα και το στόχο του υλικού.. Η κατασκευή (back-end) αποτελεί την δημιουργία ενός προϊόντος βασισμένου στις προδιαγραφές του σχεδιασμού.[8].



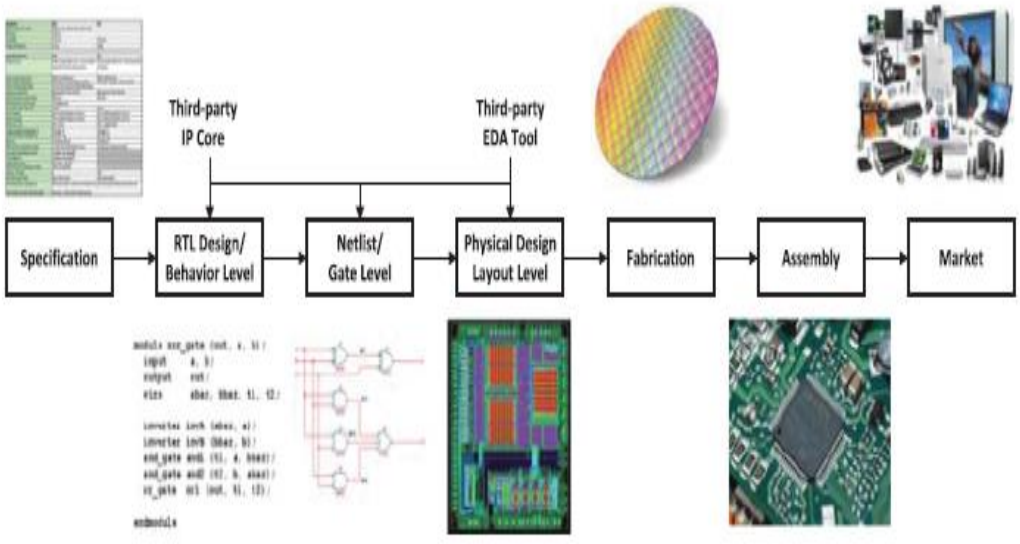
Εικόνα 2.2.: Διαδικασίες κύκλου ζωής IC [7]

Κατά το front-end στάδιο γίνεται μετατροπή της περιγραφής υψηλού επιπέδου σε επίπεδο πυλών. Η πρώτη διαδικασία αυτού του σταδίου είναι η διαδικασία της προδιαγραφής, κατά την οποία καθορίζονται οι απαιτήσεις του συστήματος σε υψηλό επίπεδο και σε δεύτερο χρόνο οι προδιαγραφές και η αρχιτεκτονική του υλικού που μπορεί να ακολουθήσει αυτές τις απαιτήσεις. Η δεύτερη διαδικασία είναι αυτή του σχεδιασμού που αναλαμβάνει να κωδικοποιήσει την αρχιτεκτονική του υλικού με τη βοήθεια της γλώσσας περιγραφής υλικού (HDL), π.χ. VHDL ή Verilog. Η κωδικοποίηση του σχεδιασμού γίνεται είτε από την κατάλληλη ομάδα της εταιρείας είτε αγοράζεται από εξωτερικούς συνεργάτες με πνευματικά δικαιώματα [8].

Η επόμενη διαδικασία είναι αυτή της επικύρωσης του σχεδιασμού. Σκοπός στη διαδικασία αυτή είναι η επαλήθευση της εγκυρότητας του σχεδιασμού του υλικού. Αυτό πραγματοποιείται με προσομοιώσεις, στην HDL πλέον μορφή του σχεδιασμού, οι οποίες χρησιμοποιούν εισόδους δοκιμών. Στη συγκεκριμένη διαδικασία δίνεται ιδιαίτερη προσοχή και οι ομάδες που ασχολούνται με αυτή είναι πιο έμπειρες και πιο μεγάλες, καθώς οι αστοχίες υλικού έχουν μεγάλο κόστος για να διορθωθούν μετά τη διαδικασία κατασκευής. Υπάρχουν περιπτώσεις όπου η επαλήθευση έχει χρήση και όσο ακόμα τρέχει η διαδικασία επικύρωσης, για την επιβεβαίωση της ορθότητας τους σχεδιασμού. Οι διαδικασία της επικύρωσης αλλά και αυτή του σχεδιασμού είναι άμεσα συνδεόμενες και εξαρτώμενες με στόχο να γίνεται αποτελεσματικότερα η επίβλεψη των πιθανών σφαλμάτων [8].

Τέλος, υπάρχει και η διαδικασία της φυσικής σύνθεσης, όπου γίνεται η μετατροπή του επικυρωμένου σχεδιασμού σε λογικές πύλες και συνδέσεις καταλήγοντας σε μια τελική διάταξη. Η τελική μορφή της διάταξης αποκαλείται και ως γραφικό σύστημα βάσεων δεδομένων GDSII stream format (GDS-II) [8].

Το στάδιο του back-end, στοχεύει στη μετατροπή της διάταξης σε σύστημα υλικού. Η πρώτη διαδικασία είναι αυτή της κατασκευής, όπου γίνεται χρήση της διάταξης ή του συστήματος βάσης δεδομένων, έτσι ώστε να δημιουργηθεί ένα τσιπ. Γενικά οι επιχειρήσεις συνηθίζουν να αποφεύγουν να έχουν υποδομές κατασκευής, και προτιμούν τα σχέδια τους να κατασκευάζονται σε εγκαταστάσεις εξωτερικών συνεργατών. Η δεύτερη διαδικασία είναι αυτή της εξέτασης, όπου όλες οι παραγόμενες συνδέσεις δοκιμάζονται με τη βοήθεια αυτόματων εξοπλισμών, έτσι εντοπίζονται πιθανά προβλήματα και βλάβες που προέκυψαν κατά την παραγωγή. Πρόκειται για έναν σημαντικό έλεγχο που είναι απαραίτητος για κάθε κατασκευαστική διαδικασία, καθώς η απόδοση της δεν είναι ποτέ στο 100%. Τέλος, έχουμε τη διαδικασία της συναρμολόγησης, όπου ουσιαστικά τα τσιπ και άλλα ηλεκτρονικά και μηχανικά εξαρτήματα (πυκνωτές, αντιστάτες) υλοποιούνται στην πλακέτα [9].



Εικόνα 2.3.: Εφοδιαστική αλυσίδα συγχρόνων ημιαγωγών [1]

Όπως φαίνεται και στην Εικόνα 2.3., υπάρχει διαθέσιμο ένα σύγχρονο μοντέλο παραγωγής και διανομής ημιαγωγών και κατ' επέκταση σχεδιασμού και δημιουργίας IC. Αρχικά υπάρχει μια επιχείρηση που ασχολείται συνήθως με το σχεδιασμό των προδιαγραφών, το Επίπεδο Μεταφοράς Καταχωρητή (RTL) και τη δημιουργία διάταξης. Στην συνέχεια μια άλλη επιχείρηση, συνήθως εργοστάσιο, ασχολείται με την κατασκευή και την εκτύπωση του ολοκληρωμένου.

Για την κατασκευή ενός ημιαγωγού προηγμένης τεχνολογίας απαιτείται επένδυση σε κάθε στάδιο της διαδικασίας ανάπτυξης ενός IC, η οποία είναι απαγορευτική. Για παράδειγμα, το 2015, το εκτιμώμενο κόστος για την ιδιοκτησία ενός χυτηρίου ήταν 5 δισεκατομμύρια δολάρια [34]. Κατά συνέπεια, οι περισσότερες εταιρείες ημιαγωγών, δεν μπορούν να διατηρήσουν οικονομικά μια τόσο μεγάλη εφοδιαστική αλυσίδα, από το σχεδιασμό μέχρι τη συσκευασία. Έτσι, με στόχο να μειώσουν το κόστος έρευνας και ανάπτυξης και να επιταχύνουν τον κύκλο ανάπτυξης, αναθέτουν την κατασκευή σε εξωτερικούς συνεργάτες – χυτήρια, αγοράζουν τα πνευματικά δικαιώματα των πυρήνων και χρησιμοποιούν εργαλεία αυτοματοποίησης ηλεκτρονικού σχεδιασμού (EDA) εξωτερικών συνεργατών. Η συνεργασία αυτή με εξωτερικούς συνεργάτες αυξάνει τις ανησυχίες για την ασφάλεια και η εφοδιαστική αλυσίδα θεωρείται ως πιο ευάλωτη σε απειλές όπως την εισβολή ενός HT [9].

2.3. Απειλή ενός Hardware Trojan.

Ο κίνδυνος από μια κακόβουλη αλλοίωση λογισμικού μπορεί να είναι συνδεδεμένη με τις κυβερνητικές υπηρεσίες. Η αντιμετώπιση των απειλών σε ότι αφορά την ασφάλεια του υλικού είναι ένας τρόπος αντιμετώπισης των ευάλωτων σημείων των λογισμικών στον ενεργειακό, στρατιωτικό, πολιτικό και οικονομικό κλάδο μια χωράς. Καθώς η εγκατάσταση ολοκληρωμένων κυκλωμάτων σε μη έμπιστα εργοστάσια εμφανίζεται ολοένα και περισσότερο, δημιουργήθηκαν αρκετές μέθοδοι εντοπισμού που ανακαλύπτουν κατά πόσο μια απειλή αποκρύπτει πληροφορίες ή επηρεάζει τη λειτουργία του κυκλώματος [6].

Γύρω στο 1980, τα υλικά που χρησιμοποιούνταν ήταν ασφαλή. Το τοπίο έχει αλλάξει τα τελευταία χρόνια λόγω των ραγδαίων τεχνολογικών αλμάτων, που οδήγησαν στην ανάγκη για αξιόπιστα ολοκληρωμένα κυκλώματα IC. Πολλά είναι τα παραδείγματα

που υποδεικνύουν τις απειλές αυτές – HT, επικεντρώνονται στη σημασία τους και δίνουν προσοχή στις επιπτώσεις τους [6].

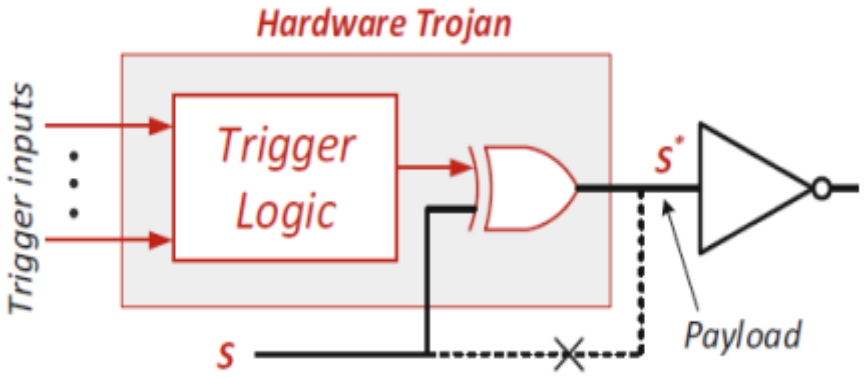
Οι κακόβουλες αυτές αλλαγές εκκινούνται υπό συγκεκριμένες συνθήκες που διαχειρίζονται από τον προγραμματιστή της απειλής, με αποτέλεσμα να είναι αρκετά δύσκολο να ανιχνευτούν. Έχουν τη δυνατότητα να εισχωρήσουν σε μεγάλο αριθμό συσκευών, από υπολογιστές και κινητά τηλέφωνα μέχρι στρατιωτικές και αεροναυπηγικές συσκευές ανίχνευσης. Επιπλέον αποτελούν κίνδυνο για το ευάλωτο διαδίκτυο των πραγμάτων (IoT), με αποτέλεσμα να αποτελούν απειλή και για ασύρματες οικιακές συσκευές [7].

Συγκεκριμένα, στον στρατιωτικό εξοπλισμό που είναι φτιαγμένος με IC, η απειλή από HT μπορεί και να αποβεί μοιραία, καθώς αλλοιώσεις στον κώδικα κατασκευής τους είναι ικανές να οδηγήσουν στο να χαθεί ο έλεγχος πυραύλων, να διαρρεύσουν κρυπτογραφημένα μηνύματα αλλά και να αποτύχουν εξοπλισμοί διάσωσης [7].

Τα ICs που έχουν προσβληθεί από κάποιο HT, έχουν τροποποιήσεις στην λειτουργικότητα ή τις προδιαγραφές τους, μπορεί να διαρρεύσουν ευαίσθητες πληροφορίες, και μπορεί να έχουν αναξιόπιστη συμπεριφορά. Ανά καιρούς η βιβλιογραφία έχει προτείνει ακριβείς κατηγοριοποιήσεις για να καλύψουν το ευρύ φάσμα των πιθανών HT. Για παράδειγμα, μια κατηγοριοποίηση ξεχωρίζει τα HT βάση πέντε διαφορετικών χαρακτηριστικών: φάση εισαγωγής, επίπεδο αφαίρεσης, μηχανισμός ενεργοποίησης, φαινόμενα και θέση. Τα HT είναι σχεδιασμένα ώστε να μην γίνονται αντιληπτά από τα έξυπνα συστήματα ελέγχου, γεγονός που τα διαφοροποιεί από απειλές που είχαν μελετηθεί τις προηγούμενες δεκαετίες. Έτσι, αποτελούν ένα πρόβλημα πιο περίπλοκο από την απλή εμφάνιση κατασκευαστικών προβλημάτων [7].

2.4. Η λογική ενός Hardware Trojan

Όπως έχει αναφερθεί, τα τελευταία χρόνια, έχουν ανιχνευτεί διάφορες δυνατές μορφές απειλών από HT, καθώς οι τεχνολογίες που χρησιμοποιούν και τα μοντέλα τους εξελίσσονται συνεχώς. Ένας απλός τύπος εισβολής από HT, μπορεί να προσβάλει την συμπεριφορά ενός σχεδίου, με την τοποθέτηση ενός μπλοκ κυκλώματος. Ένας απλός τύπος διαγράμματος HT φαίνεται στην Εικόνα 2.4., λειτουργεί, προκαλώντας βλάβη με την ενεργοποίηση – αναστροφή του σήματος S, στην περίπτωση που μια λογική συνθήκη είναι αληθής [7].



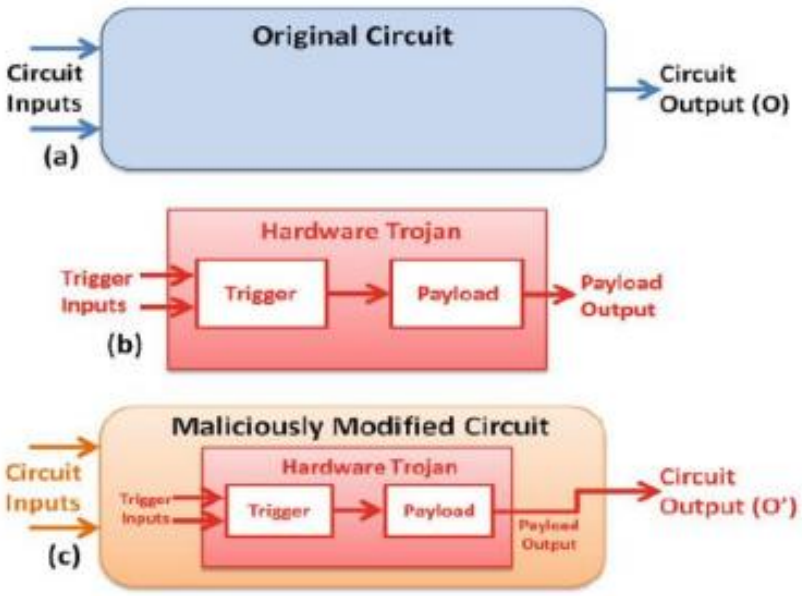
Εικόνα 2.4.: Διάγραμμα υλικού Hardware Trojan [7]

Με την βοήθεια των μπλοκ κυκλωμάτων που εφαρμόζονται, τρέχει μια συνάρτηση τύπου Boolean, κατά την οποία κάποιοι εσωτερικοί κόμβοι έρχονται σε κατάλληλη κατάσταση. Η ενεργοποίηση μπορεί να γίνει με δύο τρόπους, είτε συνδυαστικά είτε ακολουθιακά. Επιπλέον υπάρχουν τύποι HT που είναι συνεχώς σε κατάσταση on και σε αυτές τις περιπτώσεις, η ενεργοποίηση είναι ανεξάρτητη του περιβάλλοντος και του κυκλώματος [7].

Το payload ή αλλιώς κακόβουλο φορτίο, αποτελεί κομμάτι του HT που κατευθύνει τον τρόπο με τον οποίο ο σχεδιασμός θα αποκλίνει από τη καθορισμένη συμπεριφορά του. Έχει την ικανότητα να τροποποιήσει την κατάσταση στο εσωτερικό ενός κυκλώματος με αποτέλεσμα μέχρι και την καταστροφή [7].

Ο τρόπος λειτουργίας και ο στόχος ενός HT είναι πάντα κοινός, χρησιμοποιεί μια μέθοδο ώστε να θέσει σε κίνδυνο την ακεραιότητα, την αξιοπιστία ή την ταυτότητα κάποιου υλικού. Τα HT μπορούν να κατασκευαστούν στοχευμένα με σκοπό να

καταστρέψουν τη φήμη κάποιου brand μιας επιχείρησης, στα πλαίσια του ανταγωνισμού που υπάρχει στου διάφορους επιχειρησιακούς κλάδους [7].



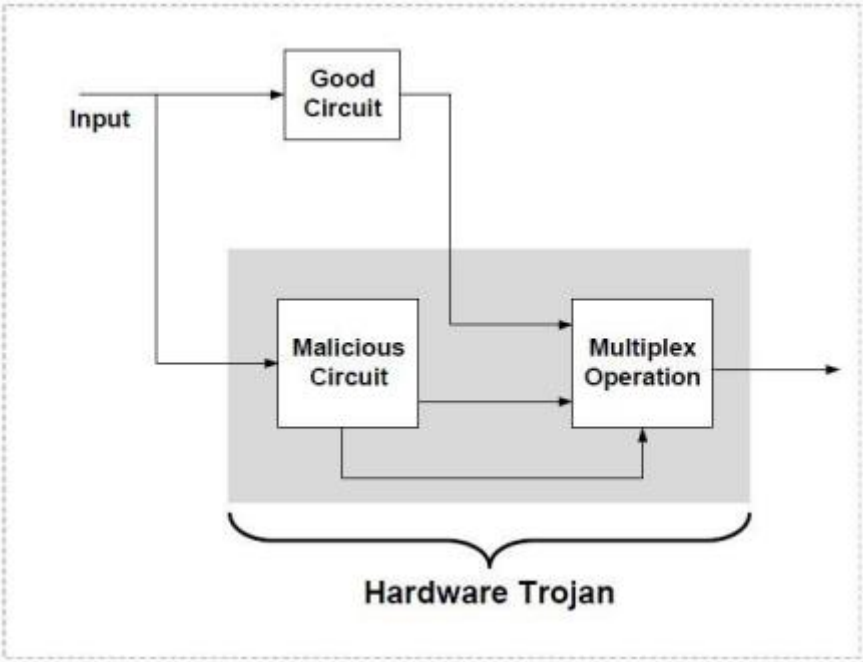
Εικόνα 2.5.: Κύκλωμα προσβεβλημένο από HT [7]

Στην Εικόνα 2.5. φαίνεται ένα κύκλωμα που έχει αλλοιωθεί από ένα HT και πως μετατρέπεται το τελικό αποτέλεσμα σε σχέση με τον αρχικό σχεδιασμό του αυθεντικού κυκλώματος.

Τα HT ανεξάρτητα από τον τύπο τους, αποτελούν μια σκόπιμη απειλή που τοποθετείται στο κύκλωμα σε θέση που είναι άγνωστη στον σχεδιαστή. Ένα HT μπορεί να αφαιρεθεί αφού δημιουργηθεί το IC, καθώς το λογισμικό HT μπορεί να καταστραφεί μετά την ανάπτυξή του. Αυτό γίνεται αφενός λόγω των δοκιμών στο υλικό που επικεντρώνεται στην λειτουργία αυτή του κυκλώματος και αφετέρου στον εξονυχιστικό έλεγχο των λειτουργιών που απαιτούν χρόνο και δαπάνες. Καθώς οι HT στοχεύουν να είναι μη ανιχνεύσιμοι τοποθετούνται συνήθως σε εσωτερικούς κόμβους του κυκλώματος και έτσι είναι δύσκολο να ενεργοποιηθούν σε απλές δοκιμές [7].

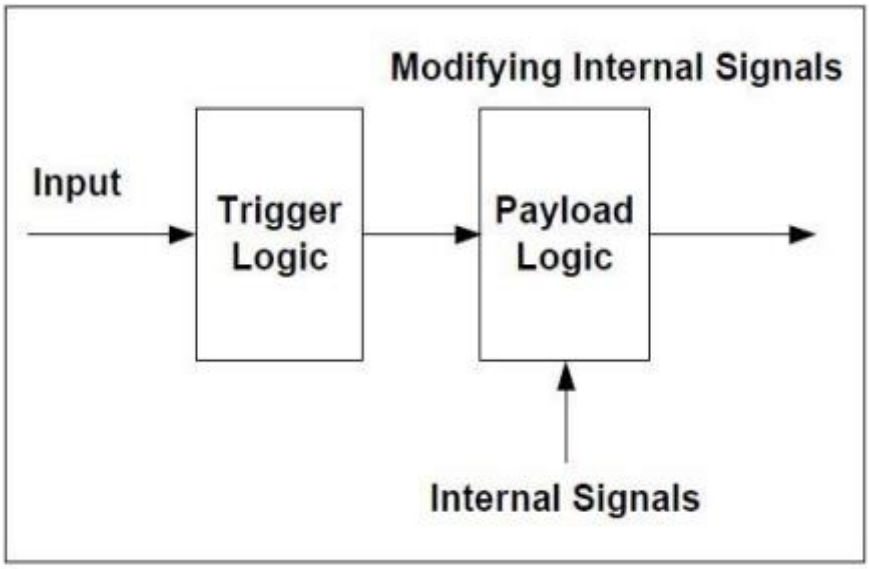
Στην Εικόνα 2.6. φαίνεται ένα σχεδιάγραμμα δομής ενός HT. Και η αυθεντική δομή του κυκλώματος αλλά και η κακόβουλη, φαίνονται μαζί σε ένα σχήμα. Το κύκλωμα βασίζεται στη λογική ενός πολυπλέκτη – multiplex (MUX), όπου με αυτόν

ενεργοποιούνται και οι δύο δομές του κυκλώματος. Η λογική του προσβεβλημένου υλικού επιλέγεται όταν εκκινήσει ο HT.



Εικόνα 2.6.: Σχεδιάγραμμα δομής HT [7]

Η βασική μορφή του HT μπορεί να διακριθεί σε δυο κομμάτια, τη λογική του κακόβουλου φορτίου – payload και της ενεργοποίησης. Στην Εικόνα 2.7. φαίνεται η βασική μορφή του HT σε κάθε σχεδιασμό. Η λογική του φορτίου payload, διαφοροποιεί τα εσωτερικά σήματα του αρχικού κυκλώματος με κάποια μέθοδο αλλοίωσης που χρησιμοποιεί ο εισβολέας. Η ενεργοποίηση είναι η λογική που εκκινεί το payload με στόχο να αλλοιώσει την κανονική συμπεριφορά του κυκλώματος [7].

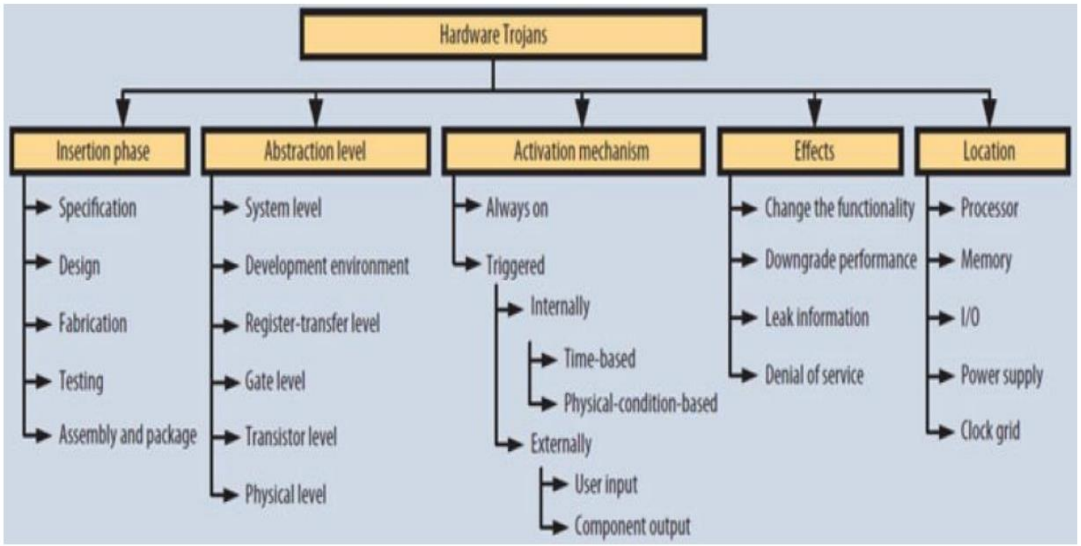


Εικόνα 2.7.: Λογική ενός HT [7]

Κεφάλαιο 3 Κατηγοριοποίηση των Hardware Trojans

3.1. Επίπεδα κατηγοριοποίησης των Hardware Trojans

Η κατηγοριοποίηση των HT διακρίνεται σε 5 διαφορετικά επίπεδα, τη φάση εισαγωγής, το επίπεδο αφαίρεσης, το μηχανισμό ενεργοποίησης, την κατηγορία αποτελεσμάτων και την κατηγορία θέσης. Όπως φαίνεται και στην Εικόνα 3.1., η κάθε κατηγορία έχει επιπλέον και τα δικά της υποεπίπεδα.



Εικόνα 3.1.: Κατηγοριοποίηση των HT [10]

3.1.1. Στάδιο υλοποίησης του κυκλώματος

Ένα τσιπ κατασκευάζεται σε πολλαπλά στάδια ξεκινώντας από τις προδιαγραφές έως και την εφαρμογή του φυσικού IC ή συναρμολόγηση. Τα HT μπορούν να κατηγοριοποιηθούν με βάση τη διαδικασία παραγωγής κατά την οποία και εισάγονται στο τσιπ. Ουσιαστικά, η φάση της εισαγωγής αναλύεται στα στάδια του σχεδιασμού και της παραγωγής, και εκεί είναι όπου το υλικό κινδυνεύει από κακόβουλη αλλοίωση. Πιο αναλυτικά, αποτελείται από την φάση των προδιαγραφών, του σχεδιασμού, της κατασκευής, της συναρμολόγησης και του ελέγχου [10].

Φάση προδιαγραφών: Ένα HT μπορεί να εισαχθεί για να αλλοιώσει τις προδιαγραφές του τσιπ που ορίζουν όλα τα χαρακτηριστικά του. Στην περίπτωση που

τροποποιούνται οι προδιαγραφές, δεν λειτουργούν και οι μηχανισμοί ανίχνευσης. Η προβλεπόμενη λειτουργικότητα και το αναμενόμενο περιβάλλον (π.χ. θερμοκρασία λειτουργίας) μπορούν να τροποποιηθούν για να παρακάμψουν την διαδικασία ανίχνευσης [10].

Φάσης σχεδιασμού: Κατά τη διάρκεια της φάσης αυτής, ο σχεδιασμός αντιστοιχείται με την προβλεπόμενη τεχνολογία. Πολλαπλοί περιορισμοί σχεδιασμού όπως λειτουργικοί, λογικοί, φυσικοί και χρονικοί εξετάζονται κατά τη διάρκεια της φάσης αυτής. Συχνά, οι σχεδιαστές κατά τη φάση αυτή, χρησιμοποιούν μπλοκ και τυποποιημένα κελιά εξωτερικών συνεργατών, έχοντας πάρει τα πνευματικά δικαιώματα με στόχο να επιταχύνουν τη διαδικασία. Αυτή η τάση, αποτελεί μια επιπλέον πηγή απειλής από HT καθώς η επαλήθευση και η προσομοίωση για τέτοιους πυρήνες δεν είναι πάντα διαθέσιμη [11].

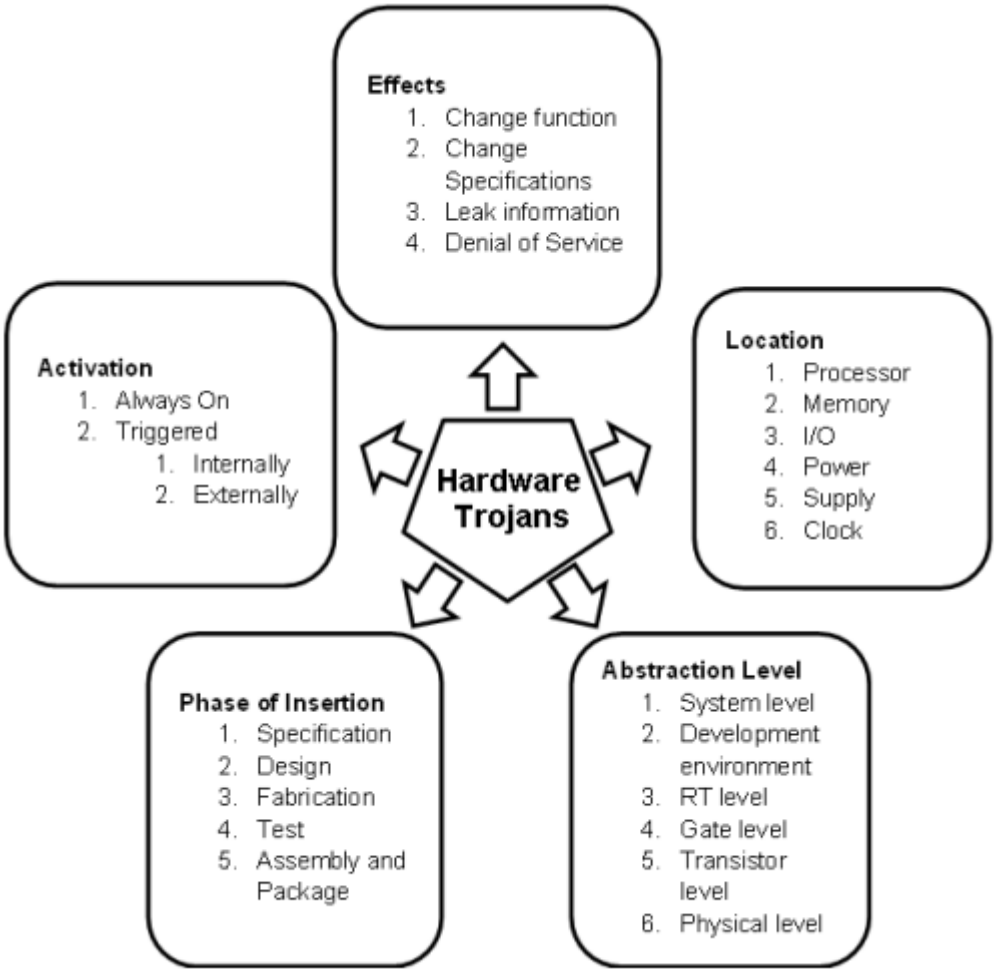
Φάση κατασκευής: Κατά τη διάρκεια της φάσης αυτής παράγονται πλακέτες χρησιμοποιώντας τις οδηγίες της φάσης σχεδιασμού. Μια πολύ μικρή αλλαγή στο σχεδιασμό μπορεί να επιτρέψει την τοποθέτηση κρυφών λειτουργιών. Τέτοιες προσπάθειες δημιουργίας HT έχουν επιχειρηθεί και στο παρελθόν, με την τροποποίηση συγκεκριμένων τμημάτων της ενεργούς περιοχής της πύλης, εφαρμόζοντας διαφορετικές πολικότητες [12].

Φάση συναρμολόγησης: Σε αυτή τη φάση συναρμολογείται μια πλακέτα τυπωμένου κυκλώματος ενώνοντας διάφορα κομμάτια του IC, μπλοκ εισόδου/εξόδου και άλλα ηλεκτρικά και ηλεκτρονικά μέρη. Επιπλέον σε αυτή τη φάση είναι πιθανό να εισαχθούν μη θωρακισμένα καλώδια και να οδηγήσουν στην διαρροή πληροφοριών. Έτσι, παρόλο που θα υπάρχουν αξιόπιστα ICs σε ένα σύστημα, οι κακόβουλη συναρμολόγηση μπορεί να οδηγήσει σε κενά ασφαλείας [10].

Φάση ελέγχου: Η φάση αυτή είναι ευκαιρία για επιβεβαίωση της αξιοπιστίας ενός τσιπ ή ενός συστήματος. Δεν υπάρχει λόγος να εισαχθεί κάποιο HT σε αυτή τη φάση, αλλά μια αναξιόπιστη υποδομή ελέγχου μπορεί να μην ανιχνεύσει τα HT που έχουν είδη εισαχθεί σε προηγούμενες φάσεις [10].

3.1.2. Επίπεδο αφαίρεσης της σχεδίασης

Οι HT μπορούν να εισαχθούν στα διαφορετικά επίπεδα της αφαίρεσης λογισμικού. Σε κάθε διαφορετικό επίπεδο της φάσης αφαίρεσης, εισάγονται και διαφορετικά HT με διαφορετικές λειτουργίες. Το επίπεδο αφαίρεσης αποτελείται από τα διαφορετικά στάδια δημιουργίας του IP υλικού πριν από την κατασκευή. Η φάση αυτή αρχίζει με τη δημιουργία των διασυνδέσεων και των πρωτοκόλλων επικοινωνίας του IC (επίπεδο συστήματος) μέχρι τη δημιουργία των φυσικών θέσεων και διαστάσεων των εσωτερικών συνιστωσών του IC (φυσικό επίπεδο).



Εικόνα 3.2.: Κατηγοριοποίηση των HT με βάση το επίπεδο εισαγωγής [10]

Επίπεδο συστήματος: Αποτελεί το υψηλότερο επίπεδο αφαίρεσης. Σε αυτό το επίπεδο η αρχιτεκτονική του συστήματος είναι χωρισμένη σε διαφορετικά υλικά, μονάδες λογισμικού, πρωτόκολλα επικοινωνιών και δεδομένα. Ένα HT το οποίο εισάγεται στο επίπεδο αυτό μπορεί να ενεργοποιηθεί από ένα μέρος του λογισμικού. Για παράδειγμα τα δεδομένα που εισάγονται από ένα μεταβατικό σύστημα μπορούν να αλλάξουν και μέσα στο ίδιο το σύστημα, πριν εφαρμοστεί η εισαγωγή [10].

Περιβάλλον ανάπτυξης: Ο σχεδιασμός σύγχρονων IC περιλαμβάνει εργαλεία αυτόματου ηλεκτρονικού σχεδιασμού που χρησιμεύουν στη σύνθεση, την προσομοίωση, την επιβεβαίωση και την επαλήθευση των διαφορετικών πρωτοτύπων από εξωτερικούς συνεργάτες. Αν το εργαλείο EDA είναι σχεδιασμένο να κρύψει ορισμένες λειτουργίες του συστήματος κατά τον έλεγχο επιβεβαίωσης, είναι πιθανό να βρεθούν κάποια HT. Έτσι, το περιβάλλον ανάπτυξης έχει ένα πολύ σημαντικό ρόλο στην εισαγωγή των HT [10].

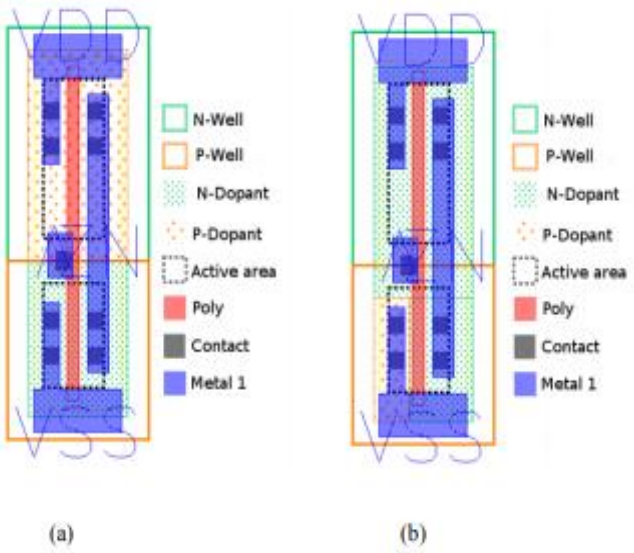
Επίπεδο μεταφοράς καταχωρητών (Register transfer level- RTL): Σε αυτό το επίπεδο το σύστημα περιγράφεται σχετικά με τους καταχωρητές, τα σήματα και τη συνδυαστική λογική. Εάν ο επιτιθέμενος έχει την πρόσβαση να αλλάξει το σχεδιασμό του RTL, μπορεί να προκαλέσει σοβαρή απειλή καθώς αποκτά τον ευρύτερο έλεγχο στο λογισμικό [4].

Επίπεδο πύλης: Η περιγραφή του επιπέδου πύλης ενός IC απεικονίζει το κύκλωμα σχετικά με τις λογικές πύλες και τις συνδέσεις του. Τις περισσότερος φορές η εισαγωγή των HT γίνεται με την αλλοίωση του επιπέδου πύλης καθώς σε σχέση με το RTL είναι ευκολότερο να ελεγχθεί το μέγεθος του HT [10].

Επίπεδο τρανζίστορ: Οι πύλες μπορούν να διαχωριστούν σε τρανζίστορς. Οι HT που εισάγονται σε αυτό το επίπεδο, έχουν μεγαλύτερη ευελιξία καθώς ελέγχουν την κατανάλωση ενέργειας, την καθυστέρηση, και παραμέτρους του τρανζίστορ όπως την τάση του ρεύματος, το μέγεθος του καναλιού και το πάχος του οξειδίου [13].

Φυσικό επίπεδο: Στο επίπεδο αυτό είναι δυνατό να εισαχθεί ένας HT αλλοιώνοντας το μέγεθος των καλωδίων, τις αποστάσεις μεταξύ των στοιχείων του κυκλώματος, και αλλάζοντας τη διανομή του μεταλλικού στρώματος. Προηγουμένως, αναφέρθηκε πως ένας HT μπορεί να εισαχθεί κατά την φάση της κατασκευής, αλλοιώνοντας τη

φυσική διάταξη του κυκλώματος, στην Εικόνα 3.3. φαίνεται ένα τέτοιο παράδειγμα αλλοίωσης που είναι μέρος του φυσικού επιπέδου [12].



Εικόνα 3.3.: (a) Μη τροποποιημένη πύλη αντιστροφέα - inverter(b) τροποποιημένη πύλη αντιστροφέα- inverter σε φυσικό επίπεδο [10]

3.1.3. Μηχανισμός ενεργοποίησης

Οι ΗΤ μπορούν να κατηγοριοποιηθούν σε σχέση με το μηχανισμό ενεργοποίησης τους. Κάποιοι ΗΤ ενεργοποιούνται μόνο κάτω από συγκεκριμένες συνθήκες. Για παράδειγμα υπάρχουν περιπτώσεις ΗΤ που ενεργοποιούνται από πολλαπλούς μηχανισμούς ενεργοποίησης με κόμβους χαμηλών πιθανοτήτων. Οι εσωτερικοί τρόποι ενεργοποίησης ενός ΗΤ μπορούν να διακριθούν και σε υποκατηγορίες όπως τη χρονική ενεργοποίηση (με τη χρήση χρονομέτρου) και την ενεργοποίηση με βάση τις φυσικές συνθήκες (υγρασία, υψόμετρο, ατμοσφαιρική πίεση κλπ). Οι ΗΤ που ενεργοποιούνται από εξωτερικό διακόπτη ή εξωτερική εισροή δεδομένων, υπάγονται στην κατηγορία εξωτερικής ενεργοποίησης. Τέλος κάποια άλλοι ΗΤ είναι σχεδιασμένοι να είναι πάντα ενεργοί [14].

3.1.4. Βάση αποτελεσμάτων

Ο εισβολέας εισάγει τον HT με στόχο να δημιουργήσει ένα μη επιθυμητό αποτέλεσμα. Με βάση λοιπόν το αποτέλεσμα οι HT διακρίνονται στις παρακάτω κατηγορίες [10]:

1) Αλλαγή στη λειτουργία: Ο HT μπορεί να οδηγήσει σε λειτουργία η οποία δεν συμπεριλαμβάνεται στις προδιαγραφές της συσκευής. Για παράδειγμα ένας HT που έχει τοποθετηθεί σε μια συσκευή GPS (global positioning system) μπορεί να αλλοιώσει τα δεδομένα τοποθεσίας που αυτός παράγει.
2) Μείωση αξιοπιστίας: Οι HT που υπάγονται σε αυτή την κατηγορία μειώνουν την απόδοση της συσκευής. Για παράδειγμα η τοποθέτηση ενός υψηλά παρασιτικού πυκνωτή μαζί με ένα κόμβο υψηλής πιθανότητας μετάβασης, μπορεί να οδηγήσει σε σημαντική κατανάλωση ενέργειας και να απορροφήσει την μπαταρία ενός κινητού.
3) Απώλεια πληροφορίας: Όπως έχει ήδη αναφερθεί υπάρχει πιθανότητα απώλειας κάποιας ευαίσθητης πληροφορίας από κακόβουλη εισβολή στην πλακέτα του κυκλώματος. Οι υπολογιστές έχουν ενσωματωμένους θερμικούς αισθητήρες για να εντοπίζουν τις διακυμάνσεις στη θερμοκρασία. Ο αισθητήρας στέλνει σήμα στον εσωτερικό ανεμιστήρα ώστε να ψύξει το σύστημα και να αποφύγει πιθανή βλάβη στημητρική. Έχει αποδειχθεί ότι αν ένας υπολογιστής έχει εκτεθεί σε κάποια απειλή τότε με την χρήση αυτού του αισθητήρα θερμοκρασίας είναι πιθανό να μεταδώσει οκτώ bits δεδομένων σε ένα άλλο υπολογιστή που είναι υπό τον έλεγχο του εισβολέα, χρησιμοποιώντας την εκπομπή θερμότητας.
4) Άρνηση υπηρεσίας: Αυτού του είδους οι επιθέσεις γίνονται με στόχο να κάνουν ένα σύστημα μη διαθέσιμο στον προοριζόμενο χρήστη.

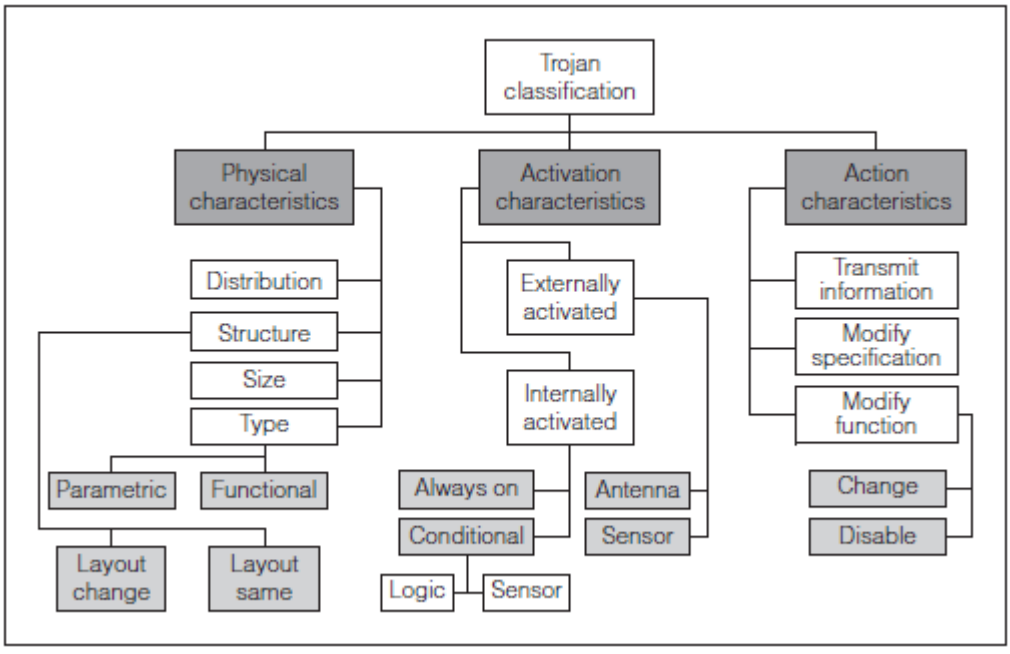
3.1.5. Βάση θέσης

Σε αυτή την κατηγορία γίνεται περιγραφή του υλικού στο οποίο μπορεί ένας HT να εισαχθεί. Συμπεριλαμβάνει τις περιπτώσεις HT που αποσκοπούν σε μονό στοιχείο του IC και δημιουργούν επιθέσεις fault injection, και τις περιπτώσεις HT που επικεντρώνονται σε πολλαπλά στοιχεία σαν τους επεξεργαστές και αλλοιώνουν την αλληλουχία εκτέλεσης των εντολών [7].

3.2. Ταξινόμηση των Hardware Trojans

3.2.1. Η πρώτη αναλυτική ταξινόμηση των HT

Ο Wang και οι συνεργάτες του ανέπτυξαν την πρώτη αναλυτική ταξινόμηση των HT [15]. Η αναλυτική αυτή ταξινόμηση επιτρέπει στους ερευνητές να εξετάσουν τις μεθόδους τους εναντίον των διαφορετικών τύπων HT. Επειδή οι κακόβουλες αλλοιώσεις στη δομή και τη λειτουργία ενός τσιπ μπορούν να έχουν διαφορετικές μορφές, ο Wang και οι συνεργάτες του διαχώρισαν την ταξινόμηση των HT σε τρεις βασικές κατηγορίες, σύμφωνα με τα φυσικά τους χαρακτηριστικά, τα χαρακτηριστικά της ενεργοποίησης τους και τα χαρακτηριστικά δράσης τους. Παρόλου που οι HT μπορούν να ανήκουν σε περισσότερες από μια εκ των κατηγοριών αυτών, η ταξινόμηση αυτή, καλύπτει τα βασικά χαρακτηριστικά των HT και είναι σημαντική για να οριστούν και να αξιολογηθούν οι δυνατότητες αρκετών μεθόδων ανίχνευσης.



Εικόνα 3.4.: Ταξινόμηση HT κατά Wang [3]

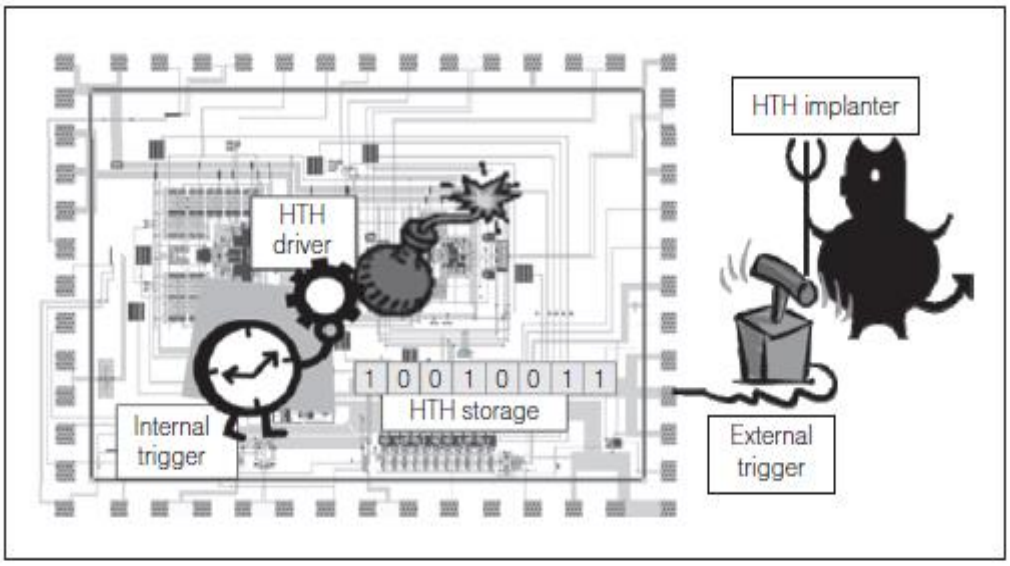
Η κατηγορία των φυσικών χαρακτηριστικών περιγράφει τις διάφορες μορφές του υλικού των HT. Η κατηγορία του τύπου διαχωρίζει τα HT σε λειτουργικά και παραμετρικά. Τα λειτουργικά HT είναι αυτά που γίνονται αντιληπτά με την πρόσθεση ή διαγραφή τρανζίστορ ή πυλών, ενώ τα παραμετρικά HT είναι αυτά που γίνονται αντιληπτά με αλλοιώσεις στα υπάρχοντα καλώδια ή λογική. Η κατηγορία μεγέθους σχετίζεται με τον αριθμό των κομματιών του τσιπ που έχουν προστεθεί, αφαιρεθεί ή διαφοροποιηθεί. Η κατηγορία της διανομής, περιγράφει την θέση του HT στην φυσική δομή του τσιπ. Η κατηγορία της δομής αναφέρεται στην περίπτωση που ο δημιουργός αναγκάζεται να αναδημιουργήσει τη διάταξη για να εισάγει έναν HT ο οποίος μπορεί να αλλάξει τη φυσική μορφή του τσιπ. Τέτοιες αλλαγές μπορούν να οδηγήσουν σε διαφορετική τοποθέτηση για ορισμένα ή όλα τα στοιχεία του σχεδιασμού. Οποιαδήποτε κακόβουλη αλλαγή στη φυσική δομή που θα μπορούσε να αλλάξει τα χαρακτηριστικά ανταπόκρισης και ενέργειας του τσιπ διευκολύνει την ανίχνευση του HT. Ο Wang και οι συνεργάτες του εντόπισαν τις δυνατότητες των δημιουργών των HT για ελαχιστοποίηση των πιθανοτήτων ανίχνευσης [15].

Τα χαρακτηριστικά ενεργοποίησης αναφέρονται στα κριτήρια που προκαλούν τον HT να πυροδοτηθεί και να εφαρμόσει την καταστροφική του λειτουργία. Τα χαρακτηριστικά πυροδότησης, διακρίνονται σε δύο υποκατηγορίες, τα εξωτερικά ενεργοποιημένα (μέσω μιας κεραίας ή ενός αισθητήρα που μπορεί να αλληλοεπιδρά με το εξωτερικό περιβάλλον) και τα εσωτερικά ενεργοποιημένα (που κατηγοριοποιούνται επιπλέον σε always – on, συνεχώς ενεργά και condition based , βασισμένα σε συνθήκη). Το always – on σημαίνει ότι ο HT είναι συνεχώς ενεργός και μπορεί ανά πάσα στιγμή να επηρεάσει τη λειτουργία της συσκευής. Η υποκατηγορία αυτή, περιλαμβάνει τα HT που εφαρμόζονται αλλοιώνοντας τη γεωμετρία της συσκευής έτσι ώστε συγκεκριμένοι κόμβοι ή διαδρομές να έχουν μεγαλύτερη ευαισθησία στην αποτυχία. Ο δημιουργός του HT μπορεί να τα εισάγει σε κόμβους ή διαδρομές που χρησιμοποιούνται σπάνια. Η υποκατηγορία HT που βασίζονται σε συνθήκη, περιλαμβάνει τα HT που είναι ανενεργά μέχρι κάποια συγκεκριμένη συνθήκη να πληρείται. Η συνθήκη ενεργοποίησης, μπορεί να βασίζεται στο αποτέλεσμα ενός αισθητήρα, που ελέγχει τη θερμοκρασία, την τάση, ή και

οποιαδήποτε άλλη εξωτερική περιβαλλοντική συνθήκη (π.χ., υγρασία, υψόμετρο, ηλεκτρομαγνητική παρεμβολή). Εναλλακτικά, αυτή η συνθήκη μπορεί να βασίζεται και σε μια εσωτερική λογική κατάσταση, ένα συγκεκριμένο μοτίβο εισόδου ή μια εσωτερική τιμή μετρητή. Ο HT σε αυτές τις περιπτώσεις εφαρμόζεται προσθέτοντας λογικές πύλες ή flip – flops στη συσκευή, και έτσι παρουσιάζεται ως συνδυαστικό ή διαδοχικό κύκλωμα [15].

Τα χαρακτηριστικά δράσης, εντοπίζουν τους τύπους διασπαστικών συμπεριφορών που εισάγονται από τους HT. Το σχήμα κατηγοριοποίησης που δείχνει η Εικόνα 3.4. διακρίνει τις δράσεις των HT σε τρεις υποκατηγορίες, τροποποίηση λειτουργίας, τροποποίηση προδιαγραφών και μετάδοση πληροφοριών. Η τροποποίηση λειτουργίας αναφέρεται σε HT που αλλοιώνουν τη λειτουργία της συσκευής προσθέτοντας κάποια λογική ή αφαιρώντας - διαφοροποιώντας κάποια υπάρχουσα λογική. Η τροποποίηση προδιαγραφών αναφέρεται σε HT που στοχεύουν με την επίθεση τους στην αλλαγή των παραμετρικών ρυθμίσεων της συσκευής, όπως την καθυστέρηση, όταν αλλοιώνονται τα καλώδια και η γεωμετρία του τρανζίστορ. Τέλος, η υποκατηγορία μεταφοράς πληροφοριών, περιλαμβάνει HT που μεταφέρουν σημαντικές πληροφορίες στον δημιουργό τους [16].

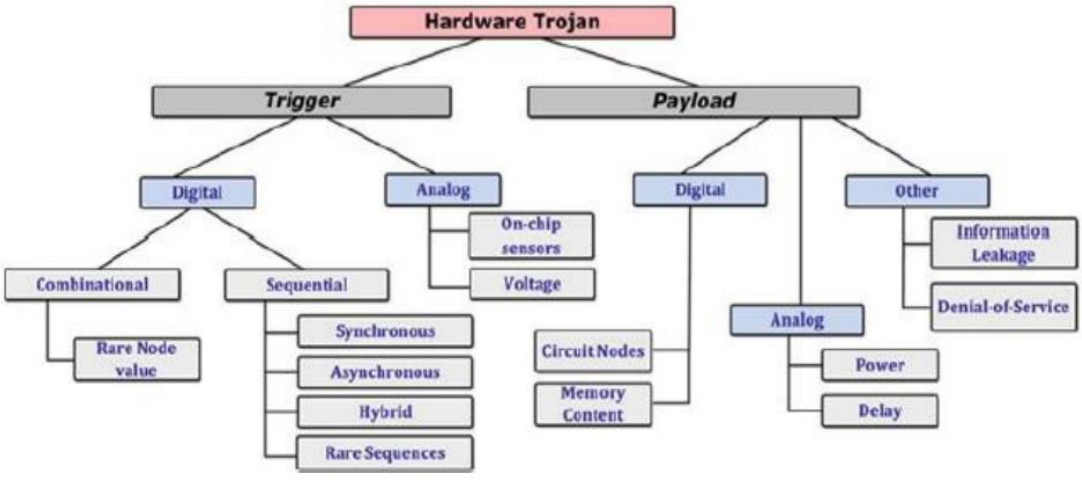
Οι ερευνητές έχουν σχεδιάσει πολλά είδη HT για να αξιολογήσουν τις μεθόδους ανίχνευσης τους. Για να προσομοιώσουν μια εισβολή HT, ο Alkabani και οι συνεργάτες του [17], κατηγοριοποίησαν τα υλικά που χρειάζονται για ένα HT σε τρείς κατηγορίες, triggers – μηχανισμούς ενεργοποίησης, αποθήκευσης, και οδηγούς, όπως φαίνεται στην Εικόνα 3.5. Ο μηχανισμός ενεργοποίησης εκκινεί τον προγραμματισμένο HT, έπειτα, η λειτουργία του μπορεί να αποθηκευτεί στην μνήμη ή σε ένα διαδοχικό κύκλωμα. Τέλος, ο οδηγός υλοποιεί την λειτουργία που προκαλείται από το μηχανισμό ενεργοποίησης.



Εικόνα 3.5.: Τρία μέρη του HT [3]

3.2.2. Περιγραφή ταξινόμησης HT σύμφωνα με τα βασικά τους χαρακτηριστικά

Τα δύο βασικά χαρακτηριστικά των HT με τα οποία γίνεται και η κύρια ταξινόμηση τους είναι η πυροδότηση (trigger) και το φορτίο payload. Ο τρόπος κατηγοριοποίησης τους φαίνεται στην Εικόνα 3.6..



Εικόνα 3.6.: Ταξινόμηση κύριων χαρακτηριστικών HT [7]

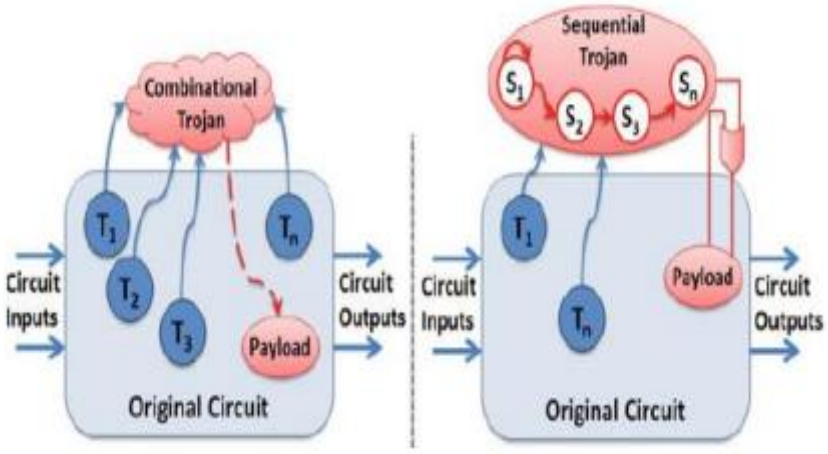
Η πυροδότηση λειτουργεί με τη συνεχή παρακολούθηση ορισμένων σημάτων του κυκλώματος και ξεκινάει με την έναρξη του κατάλληλου συμβάντος, το οποίο τις περισσότερες φορές είναι μέρος του αρχικού κυκλώματος. Το payload φορτίο με τη σειρά του είναι αυτό που μετά την πυροδότηση, ξεκινάει και δημιουργεί την

αλλοίωση στο κύκλωμα. Υπάρχουν περιπτώσεις όπου οι HT παραμένουν σε ανενεργή κατάσταση για μεγάλο χρονικό διάστημα και περιμένουν να εντοπίσουν ορισμένα περιστατικά για να ξεκινήσουν την πυροδότηση και να δημιουργήσουν το κακόβουλο φορτίο στο κύκλωμα [7].

Τα triggers αποτελούνται από δύο τύπους, τα ψηφιακά και τα αναλογικά. Πιο κοινή περίπτωση HT είναι η ψηφιακή διότι περιέχει συνδυαστικά και διαδοχικά κυκλώματα.

Τα συνδυαστικά triggers δεν αποτελούνται από χαρακτηριστικά που εμφανίζουν την κατάσταση του κυκλώματος (flip-flops) και βασίζονται σε ορισμένη συνθήκη που τρέχει σε ορισμένους κόμβους του κυκλώματος. Οι διαδοχικοί triggers ακολουθούν μια συγκεκριμένη ροή καταστάσεων που τρέχει πριν την ενεργοποίηση (μετρητές, μηχανές πεπερασμένων συνθηκών). Λόγω των συγκεκριμένων συνθηκών που πρέπει να ακολουθούνται πριν την ενεργοποίηση, είναι και δυσκολότερο να ανιχνευτούν οι διαδοχικοί HT [6].

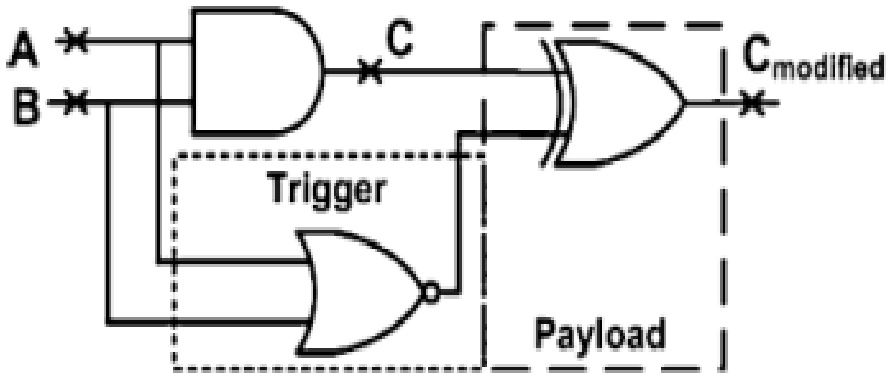
Από την άλλη, οι αναλογικοί triggers χρησιμοποιούν φυσικά φαινόμενα για να πυροδοτηθούν (ακτινοβολία, θερμοκρασία, χωρητικότητα πύλης). Υπάρχουν και οι περιπτώσεις υβριδικών HT οι οποίοι είναι μια μίξη των ψηφιακών και των αναλογικών. Στην Εικόνα 3.7. φαίνονται δυο παραδείγματα HT, ένας αναλογικός και ένας διαδοχικός.



Εικόνα 3.7.: Γενικά μοντέλα HT [7]

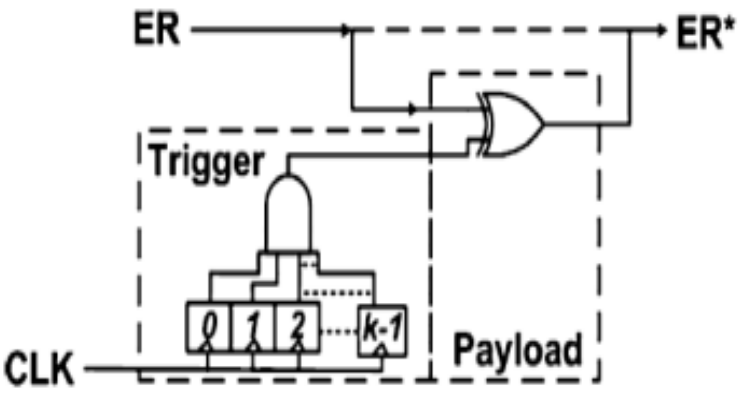
Ως προαπαιτούμενο υπάρχει το γεγονός ότι οι HT πρέπει να είναι κρυφοί και να πυροδοτούνται σε συγκεκριμένες περιπτώσεις. Κατά συνέπεια, ο χρήστης που δημιουργεί τους HT διαλέγει τους κόμβους που δεν πυροδοτούνται κατά τις απλές διαδικασίες δοκιμής. Αφού ενεργοποιηθεί ο HT, τότε πυροδοτείται και το payload, το οποίο μπορεί να διακριθεί σε αναλογικό (αλλοιώνει την απόδοση), ψηφιακό (αλλοιώνει τις λογικές τιμές) ή και άλλα (διαρροή δεδομένων, πληροφοριών). Αποτελεί το σημαντικό κομμάτι ενός HT διότι είναι αυτό που επηρεάζει τη συμπεριφορά του κυκλώματος [6].

Θα ακολουθήσουν κάποια παραδείγματα αρχιτεκτονικής HT όπου θα δείχνουν καλύτερα το τρόπο ενεργοποίησης τους. Στην Εικόνα 3.8. φαίνεται ένας HT συνδυασμού που διαθέτει μια πύλη NOR για την εκκίνηση και αντίστοιχα μια πύλη τύπου XOR για payload φορτίο. Το συγκεκριμένο παράδειγμα HT πυροδοτείται όταν στους κόμβους της πύλης NOR πληρείται η συνθήκη A = 0 και B = 0, τότε το payload καταλήγει σε ανεστραμμένη έξοδο Cmodified.



Εικόνα 3.8.: Παράδειγμα συνδυαστικού HT [7]

Στην Εικόνα 3.9. φαίνεται ένας HT με διαδοχικό μηχανισμό ενεργοποίησης, που διαθέτει και μετρητή πυροδότησης. Ο trigger διαθέτει ένα μετρητή kilobit όπως και μια λογική πύλη AND ενώ το φορτίο διαθέτει μια λογική πύλη XOR. Υπάρχει μία προκαθορισμένη τιμή 2k – 1 μετά από την οποία εκκινείται ο HT, που καταλήγει στην ανεστραμμένη έξοδο ER*.

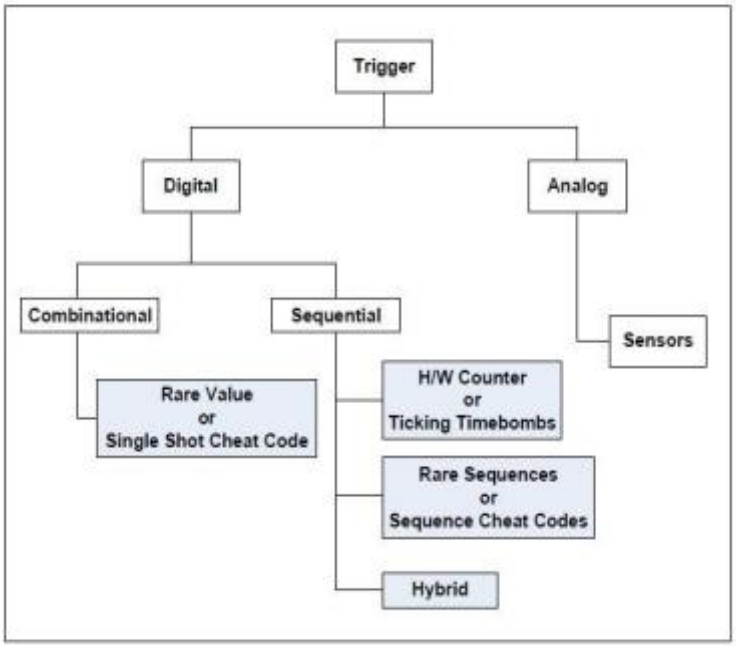


Εικόνα 3.9.: Παράδειγμα διαδοχικού HT [7]

3.3. Ταξινόμηση σύμφωνα με την πυροδότηση

Όπως έχει εξηγηθεί και σε προηγούμενα κεφάλαια, οι τακτικές των HT είναι κρυφές από τη φύση τους. Αυτό οφείλεται στο γεγονός ότι ο trigger εκκινείται σε συγκεκριμένες ειδικές συνθήκες του κυκλώματος. Τέτοιοι τύποι HT είναι σε ανενεργή κατάσταση και πραγματοποιούν τις αλλοιώσεις όταν εκκινούν. Με την ανενεργή αυτή κατάσταση αποτρέπουν την ανίχνευσή τους κατά τους ελέγχους επικύρωσης του κώδικα HDL και του ελέγχου της συσκευής μετά την κατασκευής της [18].

Στην Εικόνα 3.10. φαίνεται η κατηγοριοποίηση των HT σε σχέση με το μηχανισμό πυροδότησης. Οι μηχανισμοί εκκίνησης των HT, όπως έχει προαναφερθεί διαχωρίζονται σε ψηφιακούς και αναλογικούς. Η πρώτη κατηγορία, αυτή των ψηφιακών HT εφαρμόζει δύο μεθόδους για την ενεργοποίηση, που σχετίζονται με τα δεδομένα εισόδου και το πέρασμα του χρόνου ή τον συνδυασμό και των δύο. Οι ψηφιακοί HT διαχωρίζονται σε συνδυαστικούς και διαδοχικούς [18].

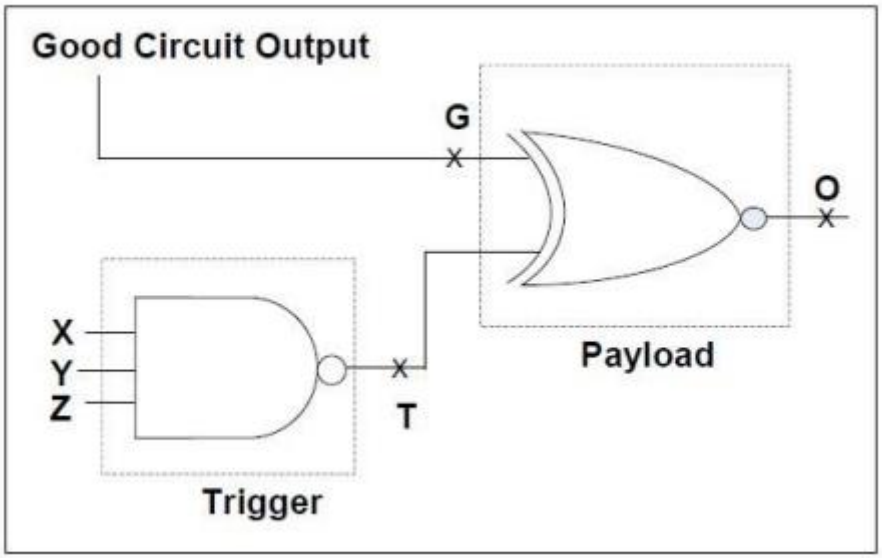


Εικόνα 3.10.: Κατηγοριοποίηση HT σε σχέση με την πυροδότηση [7]

3.3.1. Συνδυαστικός μηχανισμός πυροδότησης

Η λογική του συνδυαστικού μηχανισμού πυροδότησης βασίζεται στο γεγονός ότι δεν περιέχει πληροφορίες μνήμης όπως μανδαλωτή ή flip-flop. Οι HT αυτοί ξεκινάνε όταν στους κόμβους εσωτερικά του κυκλώματος εμφανίζονται ορισμένα σύνολα τιμών. Οι τιμές αυτές αποτελούν ακολουθία ασυνήθιστων ή σπάνιων δυαδικών ψηφίων (bits), που δεν βρίσκονται την ίδια χρονική στιγμή στους κόμβους του κυκλώματος όσο η συσκευή λειτουργεί [19].

Σε αυτή την περίπτωση μηχανισμού πυροδότησης, ο δημιουργός του HT έχει τον έλεγχο σε μεγάλο βαθμό. Πρακτικά, αυτός ο μηχανισμός ενεργοποίησης εφαρμόζει μια αρκετά ιδιαίτερη κατάσταση στη συσκευή, καθώς μεγάλο μέρος των εσωτερικών κόμβων φτάνει σε ένα ορισμένο αριθμό bits έως την πυροδότηση. Οι τιμές αυτές είναι πολύ δύσκολο να ανιχνευθούν με κάποια απλή και τυχαία μέθοδο ανίχνευσης [19].



Εικόνα 3.11.: Συνδυαστικός HT [7]

Στην Εικόνα 3.11. φαίνεται ένα παράδειγμα ενός μοντέλου συνδυαστικού HT. Στην περίπτωση που ο μηχανισμός ενεργοποίησης είναι ανενεργός, στον κόμβο T παρατηρείται η τιμή 1, με αποτέλεσμα ο κόμβος O να έχει την ίδια τιμή με τον κόμβο G που προέρχεται από το αρχικό κύκλωμα. Στην περίπτωση που ο μηχανισμός ενεργοποιηθεί, απαιτείται ο συνδυασμός τιμών X,Y,Z = 1, τότε ο κόμβος T έχει τιμή 0 με αποτέλεσμα ο κόμβος να έχει τιμή που θα είναι συμπληρωματική αυτής του κόμβου G.

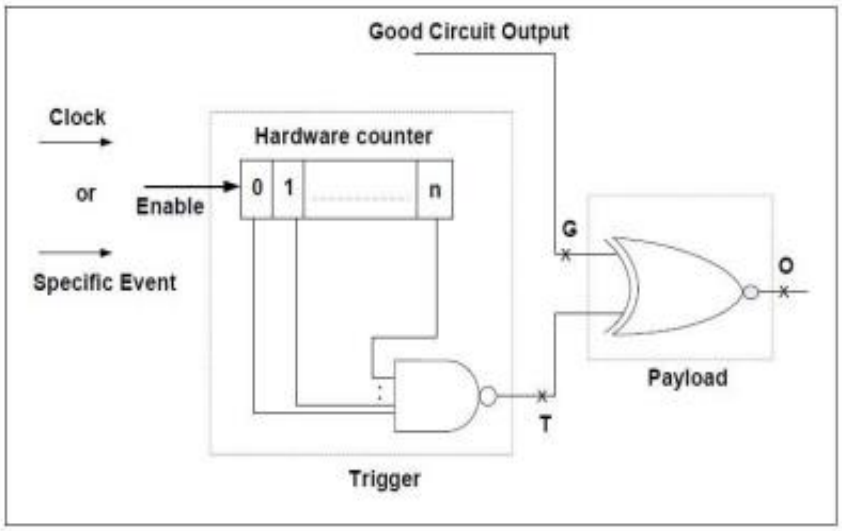
3.3.2. Πυροδότηση μηχανισμού ακολουθίας

Και στη συγκεκριμένη μέθοδο ενεργοποίησης ενός HT απαιτείται ορισμένη ακολουθία γεγονότων σε ορισμένους κόμβους του κυκλώματος ώστε να πυροδοτηθεί. Ένα από τα πιθανά γεγονότα αποτελεί η χρήση state-machines. Ο δημιουργός του διαδοχικού HT βρίσκει έναν state χώρο για την εφαρμογή του. Οι συγκεκριμένες ακολουθίες bit είναι εξαιρετικά δύσκολο να γίνουν αντιληπτές στις φάσεις του σχεδιασμού και του ελέγχου του αρχικού κυκλώματος [19].

Μια κοινή περίπτωση ακολουθιακού μηχανισμού πυροδότησης αποτελεί ένας μετρητής, που πολλές φορές αποκαλείται και σαν (ticking time bombs) ωρολογιακές βόμβες. Όταν ο μετρητής πιάσει ορισμένα όρια τιμών, μετά την πυροδότηση της

συσκευής, τότε ξεκινάει και η λογική του συγκεκριμένου μηχανισμού πυροδότησης. Σε μια απλή περίπτωση timebomb η τιμή του μετρητή εφαρμόζει ευκολότερα στο υλικό καθώς, ανεβαίνει μια φορά στον κύκλο του ρολογιού. Ο συγκεκριμένος μηχανισμός πυροδότησης είναι ανεξάρτητος από τα δεδομένα εισόδου και κατά συνέπεια δεν χρειάζεται λογισμικό για την πυροδότηση του HT. Ο δημιουργός του HT θέτει μια τιμή ενεργοποίησης στο μετρητή, με την οποία η timebomb γίνεται δύσκολα ανιχνεύσιμη στις διαδικασίες επαλήθευσης του σχεδιασμού και της δοκιμής των συσκευών. Αυτό το καταφέρνει διότι γνωρίζει πολύ καλά τον αριθμό των κύκλων ρολογιών και των διαδικασιών επαλήθευσης. Σε πιο σύνθετες διαδικασίες, η τιμή του μετρητή έχει διαφορετική λογική καθώς αυξάνεται από το ρολόι [19].

Η Εικόνα 3.12. παρουσιάζει ένα παράδειγμα HT διαδοχικής μεθόδου πυροδότησης με μετρητή. Στην είσοδο του μηχανισμού υπάρχει είτε ρολόι είτε η εκκίνηση ενός συγκεκριμένου γεγονότος. Ο μηχανισμός ξεκινάει μόνο όταν τα bits του μετρητή έχουν τιμή 1, που συνεπάγεται σε τιμή 0 στον κόμβο T και η τιμή της εξόδου O αποτελεί συμπλήρωμα του κόμβου G του κανονικού κυκλώματος.

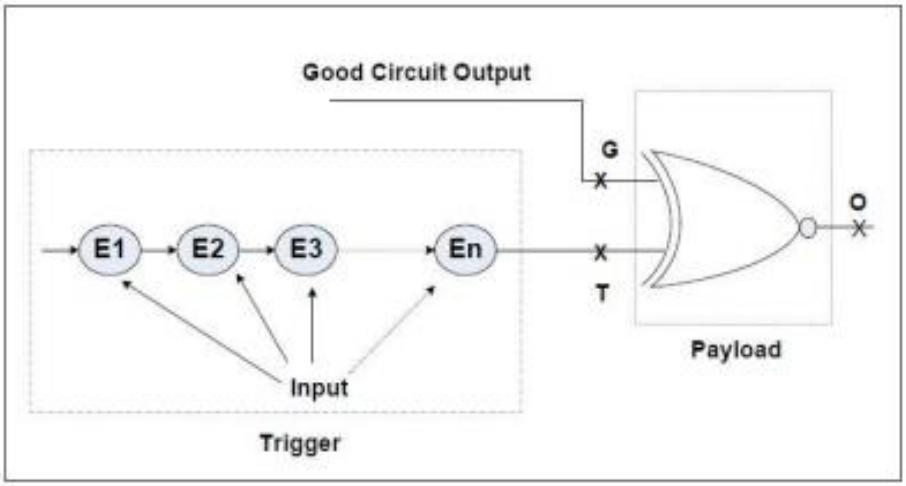


Εικόνα 3.12.: Διαδοχικός HT [7]

Μια άλλη περίπτωση διαδοχικού μηχανισμού αποτελεί η εφαρμογή διαδοχικών σπάνιων συμβάντων που ονομάζεται και ‘κώδικας εξαπατήσεως σειράς’ (sequence cheat code). Τα γεγονότα αυτά μπορεί να μην συμβαίνουν σε διαδοχικούς κύκλους και η μέθοδος πυροδότησης λειτουργεί εντοπίζοντας τα. Ο συγκεκριμένος

μηχανισμός πυροδότησης αποτελεί ένα πολύπλοκο παράδειγμα σχετικά με την υλοποίηση του [19].

Αναφορικά, οι ακολουθίες γεγονότων είναι εφικτό να αποτελούν συνδυασμό διαδικασιών ανάγνωσης και εγγραφής στη μνήμη με διαφορετικά συμβάντα στο δίαυλο δεδομένων και το δίαυλο διευθύνσεων. Η Εικόνα 3.13. παρουσιάζει ένα παράδειγμα μηχανισμού διαδοχικής μεθόδου πυροδότησης που είναι βασισμένο σε σπάνια γεγονότα.



Εικόνα 3.13.: Διαδοχικός HT σπάνιων γεγονότων [7]

3.3.3. Πυροδότηση μηχανισμού always-on

Οι HT αυτού του είδους είναι πάντα σε ενεργή κατάσταση και δεν επηρεάζονται από τις διάφορες λογικές συνθήκες που υπάρχουν. Επιπλέον, ενεργούν με την εκτέλεση κακόβουλων ενεργειών οπότε και δεν χρειάζονται συγκεκριμένη λογική πυροδότησης. Ένα παράδειγμα αποτελεί η αλλαγή της διαδικασίας κατασκευής, που συνεπάγεται στην αλλαγή κάποιων κόμβων η διαδρομών και στην μεγαλύτερη πιθανότητα αποτυχίας. Στη συγκεκριμένη περίπτωση ο μηχανισμός φθείρει κάποιες διαδρομές της συσκευής. Αυτή η περίπτωση HT που οδηγεί στη γρηγορότερη αποτυχία της συσκευής, στηρίζεται στην αξιοπιστία [6].

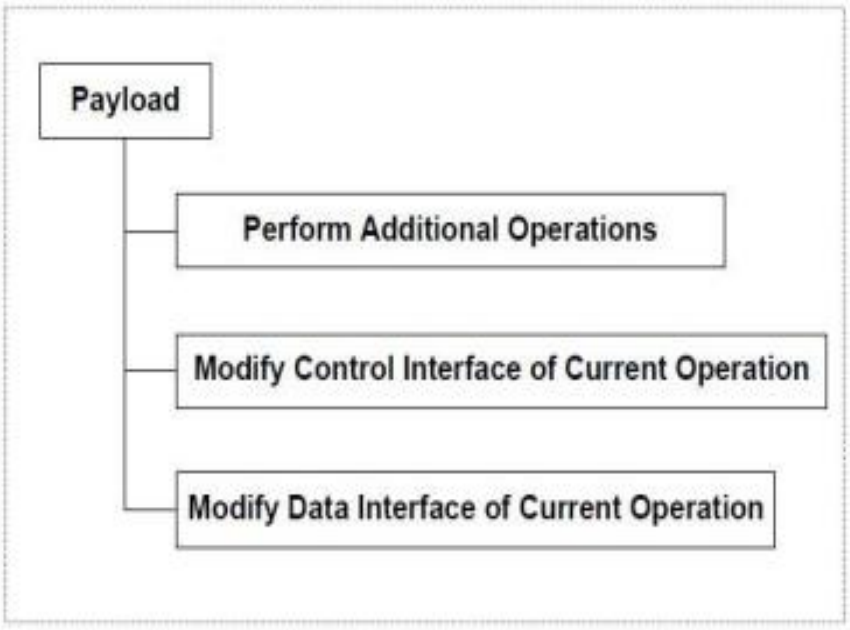
Ο μηχανισμός σκανδαλισμού μπορεί να έχει αναλογικά φυσικά χαρακτηριστικά, καθώς αισθητήρες on-chip εφαρμόζονται για να δημιουργήσουν αλλοίωση. Οι συγκεκριμένοι αισθητήρες έχουν τη δυνατότητα να καταγράφουν τις εξωτερικές

συνθήκες, υγρασία, θερμοκρασία, υψόμετρο και τάσεις. Οι διακυμάνσεις στη θερμοκρασία μπορούν να πυροδοτήσουν έναν ΗΤ υλικού, για παράδειγμα η χρήση ενός ταλαντωτή με βάση τον μετατροπέα, αυξάνει τη μεταγωγή σε κάποιο πρότυπο εισόδου και κατά επέκταση την θερμοκρασία της συσκευής. Έτσι πυροδοτείτε ένας ΗΤ [6].

3.4. Ταξινόμηση σύμφωνα με τη λογική του payload φορτίου

Αποτελεί την ταξινόμηση η οποία ευθύνεται για την αλλαγή της προκαθορισμένης λειτουργίας της συσκευής, το στόχο δηλαδή που θέτει ο δημιουργός του ΗΤ. Διακρίνεται σε δύο βασικές κατηγορίες, σε σχέση με τον τρόπου που το payload φορτίο αλλοιώνει την προκαθορισμένη λειτουργία μια συσκευής. Η πρώτη κατηγορία δεν αλλοιώνει την προκαθορισμένη λειτουργία μια συσκευής, στοχεύει στο να δημιουργήσει καινούργιες λειτουργίες που διαχειρίζεται ο δημιουργός του ΗΤ. Ονομάζεται emitter backdoor και προσπαθεί να εφαρμόσει μια λειτουργία που είναι κρυφή [18].

Η επόμενη κατηγορία payload φορτίου αλλάζει την υπάρχουσα λειτουργία χωρίς να εκτελέσει επιπλέον λειτουργίες. Σε αυτή την περίπτωση είναι βασικό ο δημιουργός του φορτίου να έχει γνώση στο συγκεκριμένο πρόγραμμα, ώστε η αλλαγή που θα εφαρμόσει να μην διαλύσει το σύστημα. Η κατηγορία αυτή μπορεί να διακριθεί σε δύο επιμέρους μέρη. Το payload που αλλάζει την αλληλεπίδραση δεδομένων της παρούσας λειτουργίας, που λέγεται ‘backdoor corrupter data’ και το payload που αλλάζει τη διεπαφή ελέγχου της παρούσας λειτουργίας. Στην Εικόνα 3.14. φαίνεται η ταξινόμηση του ΗΤ με βάση τα διάφορα φορτία payload [18].



Εικόνα 3.14.: Κατηγορίες φορτίου payload [7]

Επιπλέον με το payload υπάρχει δυνατότητα εκτέλεσης καινούργιων λειτουργιών, κρυφά, που γίνονται από τον δημιουργό του HT χωρίς να αλλάζουν την κανονική λειτουργία της συσκευής. Η τακτική αυτή εφαρμόζεται για διαρροή κρυφών πληροφοριών και την λεγόμενη “side channel attack” [7].

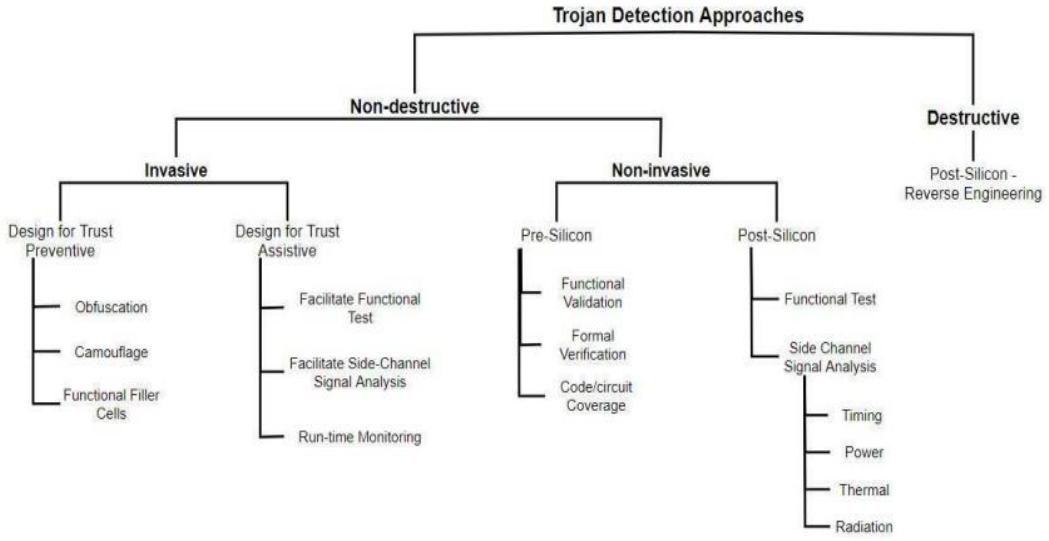
Το κύκλωμα του payload φορτίου αλλάζει τις πληροφορίες ενός σχεδίου ώστε να αλλοιώσει τις υπάρχουσες λειτουργίες. Για το σχεδιασμό που σχετίζεται με μικροεπεξεργαστή, αυτή η απειλή μπορεί [7]:

- να αλλοιώσει τα δεδομένα των μεθόδων εισόδου στη μνήμη
- να διαφοροποιήσει τη διεύθυνση των λειτουργιών εισόδου στη μνήμη
- να διαφοροποιήσει τα δεδομένα εισόδου του καταχωρητή
- να αλλάξει τη διεύθυνση που χρησιμοποιείται για την είσοδο στο αρχείο μητρώου
- να χρησιμοποιηθεί για να αλλοιώσει τη διαδοχικότητα των εντολών που τρέχουν για ένα πρόγραμμα, διαλύοντας την τιμή του καταχωρητή.

Κεφάλαιο 4 Τεχνικές ανίχνευσης των Hardware Trojans

4.1. Η λογική ανίχνευσης των Hardware Trojans

Σε αυτήν την ενότητα περιγράφεται η λογική των τεχνικών ανίχνευσης των HT και αρχικά για να εξηγηθούν καλύτερα κατηγοριοποιούνται σύμφωνα με το πως ανιχνεύουν την κακόβουλη λογική. Στην Εικόνα 4.1. φαίνεται η σχετική κατηγοριοποίηση. Η πλειοψηφία αυτών των τεχνικών αναφέρονται στην ανίχνευση των HT σε κατασκευασμένα IC.



Εικόνα 4.1.: Κατηγορίες μεθόδων ανίχνευσης [7]

Τα δύο βασικά είδη κατηγοριών στα οποία μπορούν να διακριθούν οι μέθοδοι ανίχνευσης HT είναι οι καταστροφικοί (destructive) και οι μη καταστροφικοί (non-destructive). Οι καταστροφικές τεχνικές αντίστροφης μηχανικής χρησιμοποιούνται σε ένα δείγμα του κατασκευασμένου IC με στόχο να το ελέγξουν με τεχνικές όπως χημική μηχανική στίλβωση (Chemical mechanical polishing – CMP), έπειτα με τη χρήση ηλεκτρονικού μικροσκοπίου σάρωσης (Scanning electron microscope – SEM), ανακατασκευή εικόνας και ανάλυση, και στη συνέχεια με την απόκτηση ενός τσιπ χωρίς HT γνωστό και σαν golden chip. Παρόλα αυτά, αυτές οι τεχνικές είναι πολύ ακριβές, χρονοβόρες και τα αποτελέσματα δεν μπορούν να γενικευτούν σε όλα τα κατασκευασμένα ICs. Επιπλέον, ο έλεγχος μόνο σε συγκεκριμένο κομμάτι του τσιπ

είναι αναποτελεσματικός καθώς ο HT μπορεί να επηρεάσει μόνο ένα μικρό ποσοστό αυτών. Οι μη καταστροφικές τεχνικές μπορούν να κατηγοριοποιηθούν σε δύο βασικές υποκατηγορίες, τις επεμβατικές και τις μη επεμβατικές. Οι επεμβατικές τεχνικές μεταβάλλουν το σχεδιασμό προκειμένου να ενσωματώσουν χαρακτηριστικά για την ανίχνευση του HT, ενώ οι μη επεμβατικές τεχνικές αφήνουν το σχεδιασμό ανεπηρέαστο [20].

4.1.1. Καταστροφικές

Σε ότι αφορά τις καταστροφικές τεχνικές, μια από τις μεθόδους που χρησιμοποιούνται είναι να εφαρμοστούν εξελιγμένες τεχνικές ανάλυσης της αστοχίας. Μερικές από αυτές τις τεχνικές αναφέρθηκαν και προηγουμένως, οπτικό μικροσκόπιο σάρωσης (Scanning optical microscope - SOM), ηλεκτρονικό μικροσκόπιο σάρωσης (SEM), ανάλυση απεικόνισης σε πικο – δεύτερα (picosecond imaging analysis - PICA), απεικόνιση αντίθετης τάσης (voltage contrast imaging - VCI), μεταβολή τάσης από φως (light included voltage alteration - LIVA), μεταβολή τάσης από φορτίο(charge included voltage alteration – CIVA). Παρόλο που οι παραπάνω μέθοδοι μπορούν να είναι αποτελεσματικές για λόγους αυθεντικοποίησης, είναι εξαιρετικά χρονοβόρες και ακριβές [15].

Έτσι, μπορεί να γίνει αντιληπτό ότι οι παραπάνω μέθοδοι δεν είναι εύχρηστοι σε εφαρμογές όπου όλα τα τσιπ πρέπει να επαληθευτούν. Ένα ακόμα μειονέκτημα είναι ότι πολλές από αυτές τις τεχνικές είναι μη αποτελεσματικές για τεχνολογίες του νανομέτρου. Επιπλέον, ο δημιουργός του HT μπορεί να τους εισάγει τυχαία στο τσιπ, με αποτέλεσμα ο χρόνος που θα χρειαστεί για την επαλήθευση του κάθε τσιπ να είναι ιδιαίτερα κοστοβόρος. Όπως γίνεται αντιληπτό, χρειάστηκαν νέες, πιο αποτελεσματικές μέθοδοι ανίχνευσης των HT, με μεγαλύτερο επίπεδο εμπιστοσύνης και λιγότερο απαιτούμενο χρόνο επαλήθευσης [15].

4.1.2. Μη καταστροφικές – επεμβατικές

Ένας αρκετά πιο αποτελεσματικός τρόπος να ανιχνευθούν οι HT είναι μέσω των συγκεκριμένων μεθόδων που ασχολούνται με τη διαδικασία ανίχνευσης από το στάδιο του σχεδιασμού. Οι επεμβατικές τεχνικές διακρίνονται επιπλέον σε βοηθητικές και προληπτικές. Οι βοηθητικές τεχνικές διευκολύνουν στην ανίχνευση

των HT χρησιμοποιώντας μετακατασκευαστικούς ελέγχους, ενώ οι προληπτικές τεχνικές εμποδίζουν την εισαγωγή των HT κατά τον σχεδιασμό ή την κατασκευή του IC. Οι βοηθητικές τεχνικές διακρίνονται σε τρία είδη σύμφωνα με το αντικείμενο τους [20]:

- Λειτουργικός έλεγχος: Επικεντρώνεται στην ενεργοποίηση του HT από τα δεδομένα εισόδου και την παρακολούθησή του από τα δεδομένα εξόδου, μια γενικά δύσκολη διαδικασία, καθώς οι HT είναι κρυφοί από τη φύση τους.
- Ανάλυση σήματος πλευρικού καναλιού (side - channel signal analysis): Οι μέθοδοι αυτού του σχεδιασμού μπορούν να ανιχνεύσουν λειτουργικά HT χωρίς να τα ενεργοποιήσουν αλλά μετρώντας τα δευτερεύοντα χαρακτηριστικά τους.
- Παρακολούθηση εκτέλεσης (Runtime monitoring): Η παρακολούθηση της εκτέλεσης κρίσιμων υπολογισμών μπορεί να αυξήσει αισθητά το επίπεδο εμπιστοσύνης από τις επιθέσεις των HT. Οι συγκεκριμένες μέθοδοι χρησιμοποιούν υπάρχουσες ή συμπληρωματικές δομές του τσιπ για να παρακολουθήσουν τη συμπεριφορά του τσιπ σε λειτουργικές συνθήκες όπως τη θερμοκρασία και την παροδική ισχύ.

Οι προληπτικές τεχνικές, κατατάσσονται και αυτές με την σειρά τους σε τρεις επιμέρους κατηγορίες [20]:

- Απόκρυψη λογικής (Logic obfuscation): Στοχεύει στο να κρύψει την πρακτική λειτουργία και εφαρμογή του σχεδιασμού εισάγοντας ενσωματωμένους μηχανισμούς ασφάλισης στον αρχικό σχεδιασμό.
- Καμουφλαρισμά (Camouflaging): Στοχεύει στο να εμποδίσει τους δημιουργούς του HT να εξάγουν τη σωστή λίστα δικτύων του επιπέδου πυλών ενός κυκλώματος με την απεικόνιση διαφορετικών στρωμάτων, έτσι ο κανονικός σχεδιασμός προστατεύεται από την εισαγωγή του HT.
- Μέθοδος πλήρωσης λειτουργικών κελιών: Στοχεύει να γεμίσει όλα τα κενά κατά τη διάρκεια του σχεδιασμού, βασιζόμενη στην ενσωματωμένη προσέγγιση επαλήθευσης.

4.1.3. Μη καταστρεπτικές - μη επεμβατικές

Μια διαφορετική προσέγγιση για την ανίχνευση των HT είναι η σύγκριση του ελέγχου του IC με ένα λειτουργικό μοντέλο του IC. Αυτές οι τεχνικές κατηγοριοποιούνται σε δύο κύριες κατηγορίες: χρόνου εκτέλεσης και χρόνου ελέγχου. Οι τεχνικές χρόνου εκτέλεσης χρησιμοποιούν ένα διαδικτυακό σύστημα παρακολούθησης το οποίο προσπαθεί να ανιχνεύσει ύποπτες δραστηριότητες κατά τη διάρκεια των λειτουργιών πεδίου. Οι τεχνικές χρόνου ελέγχου στοχεύουν να ανιχνεύσουν τις συσκευές που είναι προσβεβλημένες από HT πριν την ανάπτυξη [21].

- Χρόνου εκτέλεσης: Πολλοί ερευνητές προτείνουν διαφορετικές προσεγγίσεις σχετικά με τις τεχνικές αυτές. Μια από τις μεθόδους περιλαμβάνει την προσθήκη αναδιαμορφώσιμου σχεδιασμού ώστε να ενεργοποιηθεί η λογική άμυνας
- Χρόνου ελέγχου: Οι τεχνικές αυτές διακρίνονται σε δυο κατηγορίες, τις τεχνικές λογικού ελέγχου χρόνου και τις τεχνικές μέτρησης παραμέτρων πλευρικού καναλιού, όπως η τάση, η καθυστέρηση, η θερμοκρασία και η ακτινοβολία.

  Οι τεχνικές λογικού ελέγχου χρόνου αντιμετωπίζουν μια σοβαρή δυσκολία, την εξαιρετικά μεγάλη χωρητικότητα του HT, η οποία καθιστά υπολογιστικά αδύνατη τη δημιουργία ενός εκτεταμένου συνόλου διανυσμάτων δοκιμής ως είσοδο στο IC/τσιπ για την ανίχνευση. Έτσι, μια στατιστική ανάλυση θα ήταν κατάλληλη για την παραγωγή των διανυσμάτων δοκιμής.

  Οι τεχνικές που βασίζονται στη λογική του πλευρικού καναλιού, στοχεύουν στο να παρατηρούν το αντίκτυπο της εισαγωγής ενός HT σε μια φυσική παράμετρο του κυκλώματος, όπως το μεταβατικό ρεύμα, την κατανάλωση ενέργειας ή την καθυστέρηση της διαδρομής. Το πλεονέκτημα αυτής της τεχνικής κρύβεται στο γεγονός ότι παρόλο που το κύκλωμα που είναι προσβεβλημένο από έναν HT δεν προκαλεί εμφανής δυσλειτουργία κατά την διαδικασία του ελέγχου, η παρουσία του μπορεί να γίνει εμφανής στις παραμέτρους πλευρικού καναλιού. Στην Εικόνα 4.2. φαίνονται τα πλεονεκτήματα και τα μειονεκτήματα των δυο αυτών μεθόδων. Ο πίνακας αυτός δείχνει ότι οι δύο αυτές προσεγγίσεις έχουν συμπληρωματικό πεδίο

εφαρμογής όσον αφορά την ικανότητα ανίχνευσης HT. Έτσι, οι προσεγγίσεις που συνδυάζουν τα καλύτερα στοιχεία και των δύο κόσμων μπορούν να θεωρηθούν ως οι πλέον υποσχόμενες.

	Logic Testing Approach	Side-channel Approach
Advantages	• Effective for small Trojans • Robust under process noise	• Effective for large Trojans • Test generation is easy
Disadvantages	• Test generation is complex • Large Trojan detection_ challenging	• Vulnerable to process noise • Small Trojan detection challenging

Εικόνα 4.2.: Πλεονεκτήματα/μειονεκτήματα μεθόδων χρόνου ελέγχου [21]

4.2. Η μέθοδος ασφάλισης κυκλώματος IC

Ο κύκλος σχεδιασμού ενός ολοκληρωμένου κυκλώματος αποτελείται από διαφορετικά βήματα. Το αρχικό βήμα είναι η εξήγηση του τεύχους προδιαγραφών στην αρχιτεκτονική και στη συνέχεια η σύνταξη σε μια γλώσσα περιγραφής υλικού. Το επόμενο κομμάτι είναι η σύνθεση, όπου παράγεται μια λίστα σε επίπεδο πυλών – netlist. Η netlist παίρνει μια πραγματοποιήσιμη μορφή κατά τη διάρκεια της τοποθέτησης. Έπειτα τα τελικά ψηφιακά αρχεία καταλήγουν στην κατασκευή. Αφού το εργοστάσιο κατασκευάσει τα τελικά κυκλώματα, το στάδιο της δοκιμής επαληθεύει τη σωστή λειτουργία τους και αφού τελειώσουν τα στάδια της συναρμολόγησης και της συσκευασίας, τα κυκλώματα οδηγούνται για ανάπτυξη [22].

Για να σχεδιαστούν πιο πολύπλοκες συσκευές χρειάζεται η προσθήκη στοιχείων λογισμικού και υλικών που αγοράζονται από διαφορετικούς προμηθευτές και πωλητές. Το γεγονός αυτό επιστεί την προσοχή στο χρόνο αλλά και στους πόρους που απαιτούνται για την διατήρηση της ποιότητας, όπως και των δοκιμών ασφαλείας, και αναπτύσσει τις ανησυχίες για την ασφάλεια διότι οι σχεδιασμοί και τα τσιπ διέρχονται μέσα από εξαιρετικά μεγάλες αλυσίδες εφοδιασμού [22].

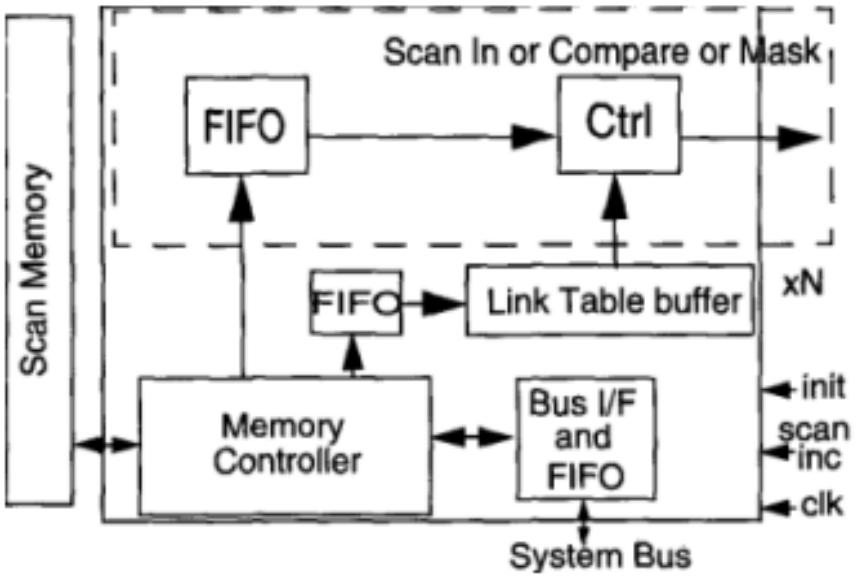
Η επιλογή ενός στόχου για την ολοκλήρωση της επίθεσης είναι συνυφασμένη με τους διαθέσιμους πόρους και την εύρεση του εισβολέα. Στα αρχικά και πιο γενικά στάδια της διαδικασίας σχεδιασμού, τα ψηφιακά σχέδια αλλάζουν με μεγαλύτερη ευκολία. Ωστόσο, είναι ευκολότερο να εφαρμόζονται αυτοματοποιημένα εργαλεία για εύρεση των αλλαγών και λιγότερο κοστοβόρο ώστε να λυθεί ένα ζήτημα που εντοπίστηκε. Το

σημαντικότερο στάδιο για την εισαγωγή της κακόβουλης απειλής είναι η κατασκευή. Αφού ξεκινήσει η κατασκευή των κυκλωμάτων, η εύρεση και καταστροφή των HT είναι εξαιρετικά δυσκολότερη και το οικονομικό βάρος μεγαλύτερο [22].

4.3. Οι μέθοδοι ανίχνευσης

4.3.1. Λογική ανάλυση

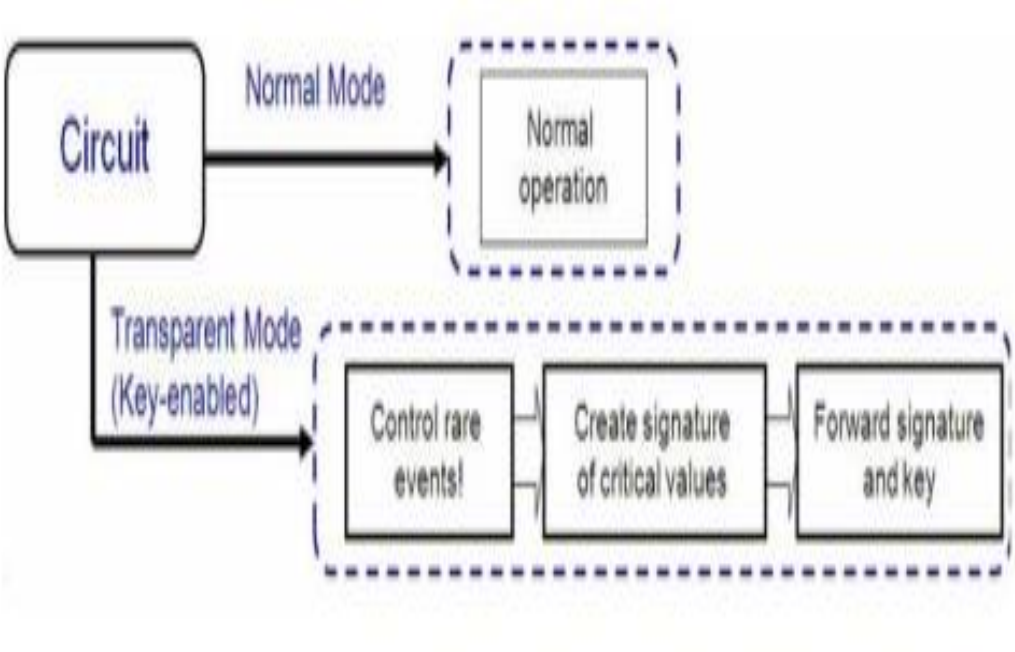
Μια αρχική δοκιμή για μια αυτοματοποιημένη τεχνική ανίχνευσης του ενδεχομένου ύπαρξης HT σε ένα κύκλωμα κατά την διαδικασία του σχεδιασμού αποτελεί ο διορθωτικός έλεγχος (Structural checking). Δημιουργείται μια αμφίδρομη δομή ενωμένου καταλόγου όλου του ASIC. Η λίστα ελέγχεται στο μπροστινό μέρος από τις εισόδους για την εύρεση της εσωτερικής απειλής και στο πίσω μέρος από τις εξόδους για την εύρεση εξωτερικών προσπαθειών αλλοίωσης δεδομένων ή απειλών διαρροής πληροφοριών. Το εργαλείο με το οποίο εκτελείται αυτή η τεχνική παράγει μια αναφορά της τοποθεσίας και των ειδών ύποπτης λογικής και έπειτα απαιτεί από τον σχεδιαστή επιπλέον έρευνα αυτής. Στην περίπτωση που θα επαληθευτεί ότι κάποια λογική έχει στόχο την αλλοίωση κάποια λειτουργίας, τότε αφαιρείται αυτόματα από το σχεδιασμό [23].



Εικόνα 4.3.: Μέθοδος διορθωτικού ελέγχου [7]

Η επόμενη τεχνική που θα περιγράφει είναι η διαφάνεια κατά παραγγελία (On demand transparency). Σε αυτήν την τεχνική ουσιαστικά δημιουργείται μια

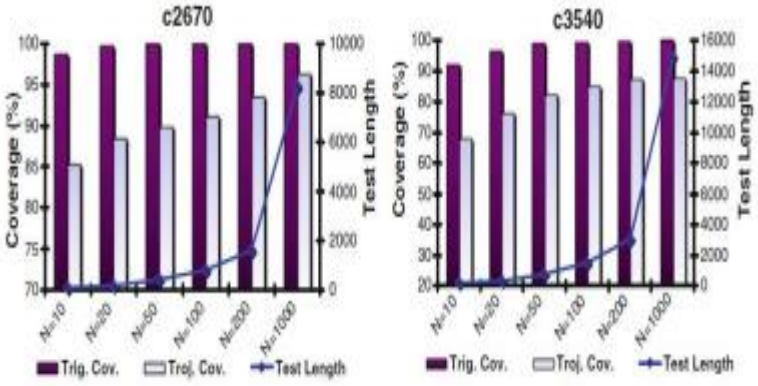
συγκεκριμένη μορφή λειτουργίας (διαφάνεια) του συστήματος. Με αυτή τη μορφή, δημιουργείται μια υπογραφή στην έξοδο του συστήματος, η οποία διαθέτει ένα συγκεκριμένο κλειδί που διαχειρίζεται ο χρήστης στην αρχή του συστήματος. Η είσοδος μιας κακόβουλης απειλής, δημιουργεί υπογραφή διαφορετική από την προκαθορισμένη και έτσι εντοπίζεται η παρουσία του [23].



Εικόνα 4.4.: Μέθοδος on demand transparency [7]

Η τεχνική που ονομάζεται αφαίρεση με βάση το κλειδί (key - based obfuscation), αποτελεί μια γενίκευση της προηγούμενης τεχνικής. Η τεχνική αυτή είναι μια αρκετά χρήσιμη μέθοδος που διαμορφώνει ένα σχεδιασμό σε ένα λειτουργικά ισοδύναμο του, αλλά εμφανώς πιο ανθεκτικό στο να αντιστραφεί μηχανικά (reverse-engineering). Το κύκλωμα τρέχει σε δυο διαφορετικές λειτουργίες, την κανονική και την αλλοιωμένη, που έχουν παρόμοια συμπεριφορά. Η αλλαγή αυτή υπονομεύει την αδράνεια των κόμβων του εσωτερικού κυκλώματος, καθιστώντας δύσκολο για τον δημιουργό της απειλής να τοποθετήσει ένα δύσκολα ανιχνεύσιμο HT. Ακόμη, έχει την ικανότητα να αφοπλίσει κάποιους εισαγόμενους HT, αφήνοντας την ενεργοποίηση μόνο σε ασφαλή λειτουργία με εύκολη ανίχνευση [23].

Μια άλλη μέθοδος που λέγεται πολλαπλή διέγερση σπάνιας εμφάνισης Multiple Excitation of Rare Occurrence (MERO) δημιουργεί ένα συμπαγές σύνολο μοτίβων δοκιμής που ελαχιστοποιεί το χρόνο εκτέλεσης και το κόστος αλλά μεγιστοποιεί την κάλυψη του HT στην ανίχνευση. Με τον εντοπισμό συνθηκών μικρής πιθανότητας στους εσωτερικούς κόμβους, δημιουργούνται βέλτιστα σύνολα διανυσμάτων που μπορούν να ενεργοποιήσουν πολλαπλές φορές τους επιλεγμένους κόμβους μικρής πιθανότητας ξεχωριστά, με τις δικές τους σπάνιες τιμές. Η ενεργοποίηση τέτοιων σπάνιων κόμβων δεν είναι δυνατή με τυχαία μοτίβα. Έτσι, μεγαλώνει η πιθανότητα να ενεργοποιηθεί ένας HT . Η Εικόνα 4.5. δείχνει ότι η κάλυψη για την ανίχνευση ενός HT αυξάνεται για τις μεγαλύτερες τιμές του N [14].



5

Εικόνα 4.5.: Μέθοδος MERO [14]

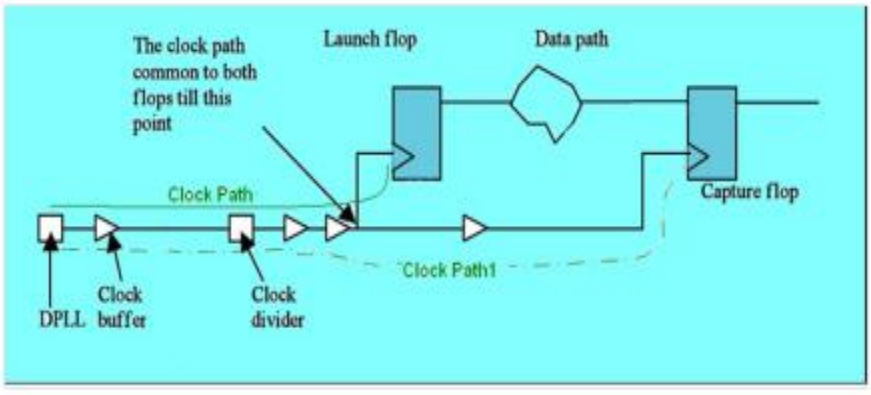
4.3.2. Ανάλυση καθυστέρησης μονοπατιού – Path delay analysis

Μια ευρέως γνωστή και χρησιμοποιούμενη τεχνική ονομάζεται fingerprint-generating, αποτελεί τεχνική δημιουργίας. Σε αυτή την μέθοδο γίνεται η συλλογή των καθυστερήσεων των διαδρομών από το κύκλωμα που δεν είναι προσβεβλημένο από κάποια κακόβουλη απειλή (ασφαλές κύκλωμα), με στόχο να δημιουργηθεί μια σειρά από αποδεικτικά, τα οποία αποτελούν κομμάτια των συνολικών χαρακτηριστικών του γνησίου σχεδιασμού. Για τον υπολογισμό των καθυστερήσεων μπορούν να χρησιμοποιούνται σύγχρονες τεχνικές ανάλυσης χρονισμού, όπως οι [24] [25] [26] [27] [28] [29]. Τα κυκλώματα επαληθεύονται με την σύγκριση των παραμέτρων καθυστέρησης και των αποδεικτικών που προαναφέρθηκαν. Η τεχνική αυτή είναι πολύ αποτελεσματική στην εύρεση μικρών HT καθώς εκμεταλλεύεται τις

καθυστερήσεις διαδρομών του συστήματος αντί του συνολικού αποτυπώματος ισχύος [30].

Μια πανομοιότυπη με τη λογική σχεδιασμού τεχνική σε σχέση με τον χαρακτηρισμό καθυστέρησης, μπορεί να λειτουργήσει σε ένα μεγάλο νούμερο εσωτερικών συνδυαστικών διαδρομών ώστε να παρθούν οι ακριβείς πληροφορίες που σχετίζονται με τις καθυστερήσεις μονοπατιού. Επίσης, γίνεται να λειτουργήσει στις διαδρομές του συστήματος πυρήνα χωρίς να μεταβάλει το χρονισμό και τη λειτουργικότητα. Η πραγματική εφαρμογή των μετρήσεων καθυστέρησης είναι η κατασκευή συγκεκριμένων και μακρόβιων υπογραφών, που θα εκτελούν την επαλήθευση της γνησιότητας σε σχέση με τις διάφορες παραλλαγές. Τα αποτελέσματα μπορούν να μετρηθούν και να βρεθούν σε λειτουργικά μέρη του κυκλώματος. Ακόμη, οι παρατηρήσεις των καθυστερήσεων μπορούν να φανούν χρήσιμες στην εύρεση αλλοιώσεων σχεδιασμού και αλλαγών σε χρόνο δοκιμής και χρόνο εκτέλεσης [30].

Μια ακόμη τεχνική που χρησιμοποιείται για τον υπολογισμό των καθυστερήσεων διαδρομής και θα αναλυθεί είναι η τεχνική σάρωσης του ρολογιού. Μέθοδοι στις οποίες ακολουθείται αυτή η τεχνική, είναι το σφάλμα καθυστέρησης και η καθυστέρηση διαδρομής με στόχο την ολοκληρωμένη κάλυψη σε κόμβους σημαντικών και μη σημαντικών διαδρομών. Σκοπό αποτελεί η δημιουργία υπογραφών καθυστέρησης σε όλες τις διαδρομές. Υλοποιείται μια τεχνική με διάφορες συχνότητες ρολογιού, ξεκινώντας από μικρές ταχύτητες. Με αυτή την τεχνική υπολογισμού της συχνότητας του ρολογιού, σε δεύτερο στάδιο υπολογίζονται και οι καθυστερήσεις από τις διαδρομές [30].



Εικόνα 4.6.: Τεχνική σάρωσης ρολογιού (clock path) [31]

Αν και η συγκεκριμένη μέθοδος με την εύρεση της καθυστέρησης διαδρομής αποτελεί μια αρκετά αποτελεσματική μέθοδο, παρουσιάζει δυσκολίες σε περιπτώσεις περίπλοκων κυκλωμάτων. Η διαδικασία έρευνας των διαδρομών και υπολογισμού των καθυστερήσεών τους σε ολόκληρο το κύκλωμα απαιτεί αρκετό χρόνο και είναι αρκετά περίπλοκη. Ακόμη, από τα αποτελέσματα της προσομοίωσης φαίνεται ότι οι δημιουργοί των HT μπορούν με ευκολία να ελαχιστοποιήσουν την επιρροή τους στην καθυστέρηση κοντά στο μηδέν [30].

4.3.3. Ανάλυση ρεύματος – current analysis

Στην αρχή δημιουργείται μια στατιστική ανάλυση των φορέων δοκιμής με στόχο να ελαχιστοποιηθούν τα ψευδώς θετικά και τα ψευδώς αρνητικά σήματα σε ένα μηχανισμό εντοπισμού υλικού HT, σχετική με την ανάλυση πλευρικών καναλιών (side channel analysis). Παρέχεται ένα νούμερο συσκευών δοκιμής που αποτελούν το IUT (Integrated circuit under tests). Η τεχνική αυτή διαθέτει τρία στάδια [32]:

- Αρχικά, εκτελείται μια δοκιμαστική περίοδος για όλες τις συσκευές ελέγχου και καταγράφονται τα ευρήματα για κάθε συσκευή. Έτσι λοιπόν σε κάθε συσκευή, η διάταξη περνάει από αρκετές επιμέρους δοκιμές. Σε κάθε επιμέρους δοκιμή, γίνεται η καταγραφή κάποιων τιμών όπως η ιδανική κατανάλωση ισχύος και η εμπειρική κατανάλωση ισχύος. Η παρατήρηση τους είναι σημαντική στις συνθήκες που οδηγούνται οι συσκευές κατά τις δοκιμές.
- Έπειτα, καταγράφεται η κατάσταση παρουσίας του HT στη συσκευή, είτε θετικά – True είτε αρνητικά – False και συγκρίνονται με τις αντίστοιχες παρατηρήσεις σε προηγούμενες εργασίες.
- Τελικά, παράγεται ένα στατιστικό αποτέλεσμα που δείχνει κατά πόσο η διάταξη είναι προσβεβλημένη από HT ή όχι. Μετά το πέρας των δοκιμών μιας συσκευής σε πολλές δοκιμαστικές, καταγράφεται η όχι το ενδεχόμενο ύπαρξης του HT, σύμφωνα με το αποτέλεσμα.

Μια διαφορετική έκδοση αυτής της τεχνικής εντοπίζει τα HT σε σχέση με την υπάρχουσα ανάλυση. Γίνεται υπολογισμός του τοπικού παροδικού ρεύματος σε διάφορες εισόδους τροφοδοσίας και καταγράφεται σε σχέση με μια μέθοδο βαθμονόμησης ώστε να διαφοροποιήσει και να ομαλοποιήσει τις υπάρχουσες τιμές. Δημιουργούνται δέκα επί μέρους διατάξεις του αρχικού IC. Η αρχική είναι απαλλαγμένη από HT. Οι υπόλοιπες εννιά διατάξεις έχουν εισάγει διάφορους τύπους HT. Μετά το πέρας της ανάλυσης κατασκευάζεται ένα διάγραμμα που εντοπίζει αν επηρεάστηκε το IC ή όχι. Η τεχνική αυτή διαθέτει δύο βασικές φάσεις [17].

Στην πρώτη φάση εξακριβώνονται οι προδιαγραφές του διαγράμματος, ενώ στην δεύτερη γίνεται ανάλυση των δοκιμών ώστε να εντοπιστούν οι ενεργές απειλές. Εκτελούνται σχετικές προσομοιώσεις ώστε να καταγραφούν τα αποτελέσματα της ανίχνευσης. Η τεχνική αυτή εντοπίζει τα έμπιστα HT που διαθέτουν τέσσερις ή και πάνω τυποποιημένες πύλες που διακρίνονται σε όλο το κύκλωμα. Στην περίπτωση που ο HT δεν είναι μεγάλος η τεχνική αυτή δεν θεωρείται και πολύ αποτελεσματική [17].

Μια επιπλέον μέθοδος εντοπισμού που είναι αρκετά διαδεδομένη σχετίζεται με μη παρεμβατικές εξωτερικές μετρήσεις ρεύματος, όταν το κύκλωμα βρίσκεται σε ηρεμία. Ένας νέος τύπος μέτρησης που καλείται συνεκτικότητα παρουσιάζεται και σχετικά με την τιμή της και τα ορίσματα της συνάρτησης, δημιουργείται μια δυνατή μέθοδος εντοπισμού που βρίσκει τις ιδιότητες της πύλης και εντοπίζει τα HT [17].

Στο πρώτο μέρος της τεχνικής, χρησιμοποιούνται ορισμένα διανύσματα εισόδου για την ολοκλήρωση των υπολογισμών της διαρροής ρεύματος.

Έπειτα, υλοποιούνται οι φορείς υπολογισμού και καταγράφουν τα νούμερα των μετρήσεων στις διαρροές πύλης.

Τελικά, εντοπίζονται οι αλλοιώσεις με σύγκριση μεταξύ των τιμών προσομοίωσης χωρίς HT με την τιμή της ευαισθησίας μεταβολής θορύβου.

Μια άλλη τεχνική που σχετίζεται με τη διαχείριση των ρευμάτων σταθερών καταστάσεων του IC, ονομάζεται steady state current, που υπολογίζονται παράλληλα από διαφορετικά μέρη στην επιφάνεια της διάταξης. Η τεχνική εφαρμόζει μια

διαδικασία για να απαλλαγεί από τις επιπτώσεις των αλλοιώσεων και του περιβάλλοντος των δοκιμών, που λειτουργούν για να ελαττώσουν την ευαισθησία εντοπισμού των κλασσικών τεχνικών ελέγχου. Μια γκάμα από κελιά επιτρέπει στην κακόβουλη απειλή να περάσει από διάφορα μέρη του κυκλώματος. Στο στάδιο του σχεδιασμού, καταγράφεται η ακριβής τοποθεσία και η ισχύς του ρεύματος του κακόβουλου υλικού, όπως και οι προδιαγραφές μεγεθών και διανομής ολόκληρου του ρεύματος που διέρχεται. Οι διάφορες αναλύσεις που έχουν γίνει από ερευνητές αναδεικνύουν ότι η ευαισθησία του εντοπισμού είναι συνυφασμένη με [7]:

- Τα χαρακτηριστικά του υπό εξέταση HT
- Το πρότυπο και τη διακύμανση στο ρεύμα που διέρχεται σε όλη τη συσκευή
- Το μέρος του ηλεκτρικού δικτύου όπου το κακόβουλο υλικό απορροφά το ρεύμα

Οι ερευνητές έχουν κάνει αρκετές προσπάθειες για προτάσεις σχεδιασμών οι οποίες θα επαληθεύουν την ασφάλεια των συσκευών έναντι των κακόβουλων απειλών και βασίζονται στη λογική των αισθητήρων ρεύματος στα ολοκληρωμένα κυκλώματα. Οι προσπάθειες αυτές βασίζονται στην ανάλυση ρεύματος δυναμικού εφοδιασμού με στόχο την ανίχνευση του HT. Όταν μιλάμε για ένα αληθινό παράδειγμα, μια σωστή δομή τοποθετημένων αισθητήρων, μπορεί να επισπεύσει τη διαδικασία ανίχνευσης λόγω της καλύτερης ευαισθησίας, σε σχέση με τους εξωτερικούς υπολογισμούς που προέρχονται από την τεχνική της ανάλυση πλευρικών καναλιών (side channel analysis).

Σε ένα σχέδιο που στοχεύει στη μικρή λειτουργία ισχύος, ο αισθητήρας εκμεταλλεύεται τα υπάρχοντα τρανζίστορ τροφοδοσίας.

Η χρήση των τρανζίστορ τροφοδοσίας γίνεται για την απενεργοποίηση των κομματιών του κυκλώματος στις ανέπαφες καταστάσεις, για να ελαχιστοποιηθεί το ρεύμα που διαρρέει.

Τα κυκλώματα που χαρακτηρίζονται από τρέχουσα μνήμη, εκμεταλλεύονται τα τρανζίστορ για τον υπολογισμό του ρεύματος τροφοδοσίας.

Τα δεδομένα διάφορων αισθητήρων συλλέγονται από το κύκλωμα και στέλνονται με τη βοήθεια των ακροδεκτών εξόδου του ολοκληρωμένου κυκλώματος.

Μια κλιμακούμενη τεχνική εντοπισμού και εύρεσης που εκμεταλλεύεται την κατανομή και την κατάσταση του επιπέδου πύλης , gate level characterization (GLC), παρατηρείται ως πιο έμπιστη από την προηγούμενη. Σε όλα τα διαφορετικά διανύσματα εισόδου, εφαρμόζεται το σύνολο του ρεύματος που διαρρέει.

- Η βασική ιδέα είναι να διακριθεί το αρχικό κύκλωμα σε άλλα μικρότερα κυκλώματα που χρησιμοποιούν διανύσματα εισαγωγής, αυτό γίνεται ώστε να αποκτήσουν τα υπό - κυκλώματα τις επιθυμητές ιδιότητες και να είναι πιο ακριβή στον εντοπισμό των απειλών.
- Αφού τελειώσει η τμηματοποίηση, τοποθετούνται τμήματα δοκιμής σε περίπτωση που υπάρχουν εναπομείναντα μεγάλα τμήματα. Ξεκινώντας από την κατανομή και ανιχνεύοντας τη διαρροή της πύλης, γίνεται λήψη των ακριβών αποτελεσμάτων από το GLC και αποφασίζεται αν υπάρχει ο HT.

Η εγκυρότητα των μεθόδων έχει να κάνει κατά βάση με την ποιότητα της διαδικασίας που δημιουργεί τα πρότυπα της δοκιμής.

4.3.4. Ανάλυση ισχύος – Power analysis

Η βασική ιδέα είναι η υιοθέτηση μιας στατιστικής ανάλυσης που βοηθάει στον εντοπισμό του HT αναλύοντας τα μεταβατικά σήματα παροχής ηλεκτρικού ρεύματος – power supply transient signals. Η τεχνική αυτή, αποτελεί μια μέθοδο ανάλυσης της παροδικής παροχής ενέργειας, που είναι ανθεκτική στο αντίκτυπο που έχει η αλλαγή της διαδικασίας και του περιβάλλοντος [33].

Το πρώτο βήμα είναι η συλλογή των δεδομένων από τις πύλες ισχύος του κυκλώματος. Δημιουργείται ένα διάγραμμα εκμεταλλευόμενο τις περιοχές που προκύπτουν για κάθε ζευγάρι πυλών ισχύος, από προσομοιώσεις μοντέλου που δεν είναι προσβεβλημένο από HT και από ένα που είναι. Κάτω από τις πύλες τροφοδοσίας των ολοκληρωμένων κυκλωμάτων, υπάρχουν τα ειδικά κυκλώματα βαθμονόμησης, που ενώνονται σαν αλυσίδες και συμβάλλουν στην ολοκλήρωση της

διαδικασίας βαθμονόμησης. Τα κυκλώματα αυτά, λειτουργούν ώστε να δημιουργούν ένα απλό ερέθισμα στο δίκτυο ηλεκτρικής ενέργειας [33].

Η ολοκλήρωση μιας μετάβασης σε ένα δίκτυο, απαιτεί έναν αριθμό κύκλων του ρολογιού, σε σχέση με τους οποίους προκύπτει και η πιθανότητα της εκάστοτε μετάβασης. Υπάρχουν δίκτυα στα οποία, η πιθανότητα μετάβασης είναι μικρότερη από ένα ορισμένο όριο και σε αυτά τα δίκτυα πρέπει να γίνουν δράσεις ώστε να αυξηθεί η πιθανότητα μετάβασης. Για να επιτευχθεί αυτός ο στόχος, η προτεινόμενη διαδικασία, είναι η εισαγωγή ενός εικονικού flip – flop το οποίο δεν θα αλλάζει την λειτουργία του IC [33].

Η μέθοδος της περιφερειακής ενεργοποίησης , regional activation, όπου οι μεταβάσεις συμβαίνουν μόνο σε ένα μέρος του ολοκληρωμένου κυκλώματος και τα υπόλοιπα μέρη διατηρούνται σταθερά, αποτελεί μια αποτελεσματική λύση για την αύξηση της κατανάλωσης ρεύματος από HT σε ένα κύκλωμα. Η κατανάλωση ρεύματος που απαιτεί ένας HT θεωρείται μικρή σε σχέση με αυτή του κυκλώματος, στη λογική ότι και ο HT είναι μικρός σε σχέση με το κύκλωμα. Έτσι, για να διευκολυνθεί η διαδικασία εντοπισμού, πρέπει και να αυξηθεί η κατανάλωση ρεύματος από τον HT στο κύκλωμα [33].

Όταν μειώνεται η κατανάλωση ενέργειας στο κύκλωμα, αυξάνεται και η κατανάλωση ρεύματος από τον HT στο κύκλωμα. Η κατάσταση αυτή επιτυγχάνεται με την εφαρμογή μεταβάσεων σε μέρος του κυκλώματος και διατήρηση άλλων περιοχών σε κατάσταση αδράνειας.

Η ερευνητική κοινότητα προτείνει μία καινούργια μέθοδο, που λέγεται αναδιάταξη κυψελών σάρωσης – layout aware scan-cell reordering, η οποία χρησιμοποιεί τη διάταξη για την ανίχνευση του σχεδιασμού σε κάποιο μέρος του κυκλώματος. Η τεχνική αυτή δημιουργεί τις αλυσίδες σάρωσης έχοντας υπόψη τις φυσικές προδιαγραφές των κυψελών σάρωσης. Όταν απαιτούνται αλλαγές στα μέρη του προορισμού που είναι σχετικές με την παρακολούθηση της κατανάλωσης ενέργειας, γίνονται με την χρήση τυχαίων μοτίβων. Μια αρκετά αποτελεσματική μέθοδος εντοπισμού HT από άποψη χρόνου εκτέλεσης και κόστους, αποτελεί η καταγραφή της θερμοκρασίας. Πέρα από την αλλοίωση στη σχέση ισχύος και θερμοκρασίας, οι

ΗΤ αλλοιώνουν και την κατανάλωση ισχύος της συσκευής. Παρακάτω θα περιγραφεί μια διαδικασία καταγραφής της θερμοκρασίας. Η διαδικασία αυτή περιέχει φάση σχεδιασμού και φάση δοκιμής χρόνου και εκτέλεσης [33].

Στην φάση του σχεδιασμού, κάποια στατιστικά δεδομένα από τη λειτουργία της μεταγωγής, την κατανάλωση ενέργειας και τη θερμική δυναμική καταγράφονται και έπειτα εφαρμόζονται θερμικοί αισθητήρες. Η φάση του χρόνου δοκιμής είναι σχετική με τη βαθμονόμηση της συσκευής που οφείλεται στη διακύμανση και η φάση χρόνου εκτέλεσης συγκεντρώνει και διαχειρίζεται δεδομένα από τους θερμικούς αισθητήρες της φάσης σχεδιασμού για να εντοπιστεί η πυροδότηση του ΗΤ [33].

4.3.5. Υβριδική ανάλυση

Η μέθοδος segmentation & GLC διαφοροποιείται για να ενσωματώσει τη θερμική επεξεργασία. Αυτή η διαφοροποίηση προσφέρει λύση στο πρόβλημα της συσχέτισης και αυξάνει την αποτελεσματικότητα του εντοπισμού στις αλλαγές της διαρροής ισχύος.

Εκμεταλλευόμενη αυτήν την προσέγγιση, αναπτύσσεται και μια νέα κλιμακούμενη ιδέα side channel, που λέγεται αυτοαναφορά – self-referencing, η οποία λειτουργεί σε συνεργασία με τον αλγόριθμο παραγωγής διανυσμάτων και στοχεύει στην αύξηση της ευαισθησίας εντοπισμού του ΗΤ σε έντονες διακυμάνσεις της διαδικασίας [7].

Η τεχνική αυτή κάνει σύγκριση του παροδικού ρεύματος μιας περιοχής του IC με μια περιοχή ενός άλλου, και εκμεταλλευόμενη τη χωρική συσχέτιση των διάφορών κομματιών του IC, απαλείφει το θόρυβο που υπάρχει στην διαδικασία. Για να γίνει αντιληπτή η παρουσία του ΗΤ στο ρεύμα τροφοδοσίας, εφαρμόζεται μια διαδικασία δημιουργίας διανυσμάτων που διαχωρίζει το κύκλωμα σε διάφορα κομμάτια. Σε κάθε κομμάτι εντοπίζει τα διανύσματα δοκιμής που οδηγούν στη μέγιστη δραστηριότητα στην εκάστοτε περιοχή, και την μικραίνουν αντίστοιχα σε άλλα κομμάτια [7].

4.3.6. Διάφορες λοιπές μέθοδοι

Η τεχνική probabilistically compare the functionality, συγκρίνει τις πιθανότητες της λειτουργίας του IC. Λειτουργεί, δημιουργώντας μια μοναδική υπογραφή πιθανοτήτων του IC όπως και μια κατανομή πιθανοτήτων στις πύλες με στόχο η κατανομή της εξόδου να είναι μοναδική σε όλα τα κυκλώματα. Για έξοδο χρησιμοποιείται ή κάποιο μοτίβο εισόδου που διαχωρίζει τη λειτουργικότητα του κυκλώματος από το σχεδιασμό ή ένα επίπεδο εμπιστοσύνης που αποδεικνύει ότι το κύκλωμα δεν είναι προσβεβλημένο από HT. Το επίπεδο αυτό μπορεί να γίνει αποτελεσματικότερο με εφαρμογή της μεθόδου ανάλυσης για περισσότερο χρόνο [7].

Το τελευταίο μέσο αντίδρασης είναι ο εντοπισμός των ενεργών HT, αυτό συμβαίνει στην περίπτωση που ο HT δεν γίνει αντιληπτός από τις αρχικές μεθόδους ανίχνευσης. Μια τέτοια τεχνική ονομάζεται SHADE (Secure heartbeat and dual encryption). Δύο είναι τα κύρια στοιχεία της μεθόδου αυτής, η αρχιτεκτονική και ο ειδικά προσαρμοσμένος μεταγλωττιστής [7].

Η αρχιτεκτονική διαθέτει δύο χαρακτηριστικά επεξεργασίας που ελέγχουν την ορθότητα και την ανταπόκριση, χρησιμοποιώντας ένα περιβάλλον λειτουργίας το οποίο παρά την ύπαρξη μη έμπιστου υλικού είναι ασφαλές. Ο μεταγλωττιστής ευθύνεται για τη διαχείριση των εφαρμογών που δρουν κάτω από την αρχιτεκτονική [7].

Μια επιπλέον μέθοδος εντοπισμού που εκμεταλλεύεται την επεξεργασία εικόνας, κάνει μια σύγκριση μεταξύ των μικρών οπτικών εικόνων από πυρίτιο και των αξιόπιστων μοντέλων δηλαδή των αυθεντικών εικόνων των στρώσεων του κυκλώματος. Με την εξακρίβωση των εικόνων εντοπίζεται ο HT που έχει τοποθετηθεί στην εφαρμογή κρυπτογράφησης [7].

Κεφάλαιο 5 Συμπεράσματα

Τα κακόβουλα υλικά είναι μια συνεχώς αναδυόμενη απειλή καθώς η ύπαρξη σχεδιασμένων υλικών σε εφαρμογές οικιακών εφαρμογών, οικονομικών και στρατιωτικών συστημάτων συνεχίζει να αυξάνεται. Σε αυτή την διπλωματική, παρουσιάστηκε μια κατανοητή ανάλυση των κακόβουλων υλικών HT. Μετά από μια μικρή εισαγωγή στο θέμα, παρουσιαστήκαν μέθοδοι για την κατηγοριοποίηση των κακόβουλων υλικών. Οι απειλές αυτές κατηγοριοποιήθηκαν συμφώνα με τα εξαρτήματα τους, τις προδιαγραφές τους και τα χαρακτηριστικά της συμπεριφοράς τους. Επιπλέον κατηγοριοποιήθηκαν και σύμφωνα με την ευπάθεια του υλικού τους. Ακόμη, παρουσιάστηκαν οι μεθοδολογίες για την ανίχνευση των HT, όπως ο λογικός έλεγχος (logic testing) και η ανάλυση πλαϊνού καναλιού (side channel analysis). Η διερεύνηση των μεθόδων εντοπισμού, φανερώνει την πληθώρα διαθέσιμων τεχνικών που καλύπτουν τις διάφορες πτυχές της λειτουργίας των IC. Αποφάνθηκε πως ένα κύκλωμα που δεν προσβάλλεται από HT είναι πολλές φορές δυσκολότερο να επαληθευτεί καθώς η πολυπλοκότητα του αυξάνεται αισθητά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S. and Tehranipoor, M., 2016. Hardware trojans: Lessons learned after one decade of research. ACM Transactions on Design Automation of Electronic Systems (TODAES), 22(1), pp.1-23.

[2] S. Adee. 2008. The hunt for the kill switch. IEEE Spectrum 45, 5 (May 2008), 34–39. DOI:http://dx.doi.org/10.1109/MSPEC.2008.4505310

[3] Tehranipoor, M. and Koushanfar, F., 2016. A survey of hardware trojan taxonomy and detection. IEEE Design & Test of Computers, (01), pp.1-1.

[4] Jin, Y., Kupp, N. and Makris, Y., 2009, July. Experiences in hardware Trojan design and implementation. In 2009 IEEE International Workshop on Hardware-Oriented Security and Trust (pp. 50-57). IEEE.

[5] Tehranipoor, M. and Wang, C. eds., 2011. Introduction to hardware security and trust. Springer Science & Business Media.

[6] Li, H., Liu, Q. and Zhang, J., 2016. A survey of hardware Trojan threat and defense. Integration, 55, pp.426-437.

[7] Tompatsidis, N., 2020. HARDWARE TROJAN.

[8] Prashanth, Reddy G., 2017. DESING AND DETECTION OF HARDWARE TROAJNS.

[9] Bhunia, S., Hsiao, M.S., Banga, M. and Narasimhan, S., 2014. Hardware Trojan attacks: Threat analysis and countermeasures. Proceedings of the IEEE, 102(8), pp.1229-1247.

[10] Hoque, T., 2015. Ring oscillator-based hardware trojan detection. The University of Toledo.

[11] Chakraborty, Rajat Subhra, Seetharam Narasimhan, and Swarup Bhunia. "Hardware Trojan: Threats and emerging solutions." High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International. IEEE, 2009.

[12] Becker, Georg T., et al. "Stealthy dopant-level hardware trojans." Cryptographic Hardware and Embedded Systems-CHES 2013. Springer Berlin Heidelberg, 2013. 197-214.

[13] A. Ferraiuolo, X. Zhang, and M. Tehranipoor. "Experimental analysis of a ring oscillator network for hardware Trojan detection in a 90nm asic." Computer-Aided Design (ICCAD), 2012 IEEE/ACM International Conference on , vol., no., pp.37,42, 5-8 Nov. 2012.

[14] Chakraborty, Rajat Subhra, et al. "MERO: A statistical approach for hardware Trojan detection." Cryptographic Hardware and Embedded Systems-CHES 2009. Springer Berlin Heidelberg, 2009. 396-410.

[15] X. Wang, M. Tehranipoor, and J. Plusquellic, ‘‘Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions,’’ Proc. IEEE Int’l Workshop Hardware Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 15-19.

[16] Y. Alkabani and F. Koushanfar, ‘‘Extended Abstract: Designer’s Hardware Trojan Horse,’’ Proc. IEEE Int’l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 82-83.

[17] X. Wang et al., ‘‘Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis,’’ Proc. IEEE Int’l Symp. Defect and Fault Tolerance of VLSI Systems (DFT 08), IEEE CS Press, 2008, pp. 87-95.

[18] Sklavos, N., Chaves, R., Di Natale, G. and Regazzoni, F., 2017. Hardware security and trust. Cham, Switzerland: Springer.

[19] Salmani, H. and Tehranipoor, M., 2013, October. Analyzing circuit vulnerability to hardware Trojan insertion at the behavioral level. In 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS) (pp. 190-195). IEEE.

[20] Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S. and Tehranipoor, M., 2016. Hardware trojans: Lessons learned after one decade of research. ACM Transactions on Design Automation of Electronic Systems (TODAES), 22(1), pp.1-23.

[21] Katerina, N., 2022. Malicious Hardware (Doctoral dissertation, University of Piraeus (Greece)).

[22] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, “Trojan detection using IC fingerprinting,” IEEE Symp. on Security and Privacy, pp. 296–310, 2007.

[23] Adam Waksman, Matthew Suozzo, Simha Sethumadhavan “FANCI: Identification of Stealthy Malicious Logic Using Boolean Functional Analysis”, ACM.CCS’13.

[24] D. Garyfallou, I. Tsiokanos, N. Evmorfopoulos, G. Stamoulis, and G. Karakonstantis, “Accurate Estimation of Dynamic Timing Slacks using Event-Driven Simulation,” in Proc. of the 21st International Symposium on Quality Electronic Design (ISQED), pp. 225 230, 2020.

[25] D. Garyfallou, A. Vagenas, C. Antoniadis, Y. Massoud, and G. I. Stamoulis, “Leveraging Machine Learning for Gate-level Timing Estimation Using Current Source Models and Effective Capacitance,” in Proc. Of the 22nd Great Lakes Symposium on VLSI (GLSVLSI), pp. 77–83, 2022.

[26] D. Garyfallou, C. Antoniadis, N. Evmorfopoulos, and G. Stamoulis, “A Sparsity-Aware MOR Methodology for Fast and Accurate Timing Analysis of VLSI Interconnects,” in Proc. of the 16th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), pp. 89–92, 2019.

[27] D. Garyfallou et al., “Gate Delay Estimation With Library Compatible Current Source Models and Effective Capacitance,” IEEE Trans. on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 5, pp. 962–972, 2021.

[28] C. Antoniadis, D. Garyfallou, N. Evmorfopoulos, and G. Stamoulis, “EVT-based worst case delay estimation under process variation,” in Proc. of the Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1333–1338, 2018.

[29] D. Garyfallou, Ph.D. thesis, “Novel techniques for timing analysis of VLSI circuits in advanced technology nodes”, 2021.

[30] Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor. 2010. Trustworthy hardware: Identify-ing and classifying hardware Trojans.Computer43, 10 (Oct. 2010), 39–46.

[31] Govind, P.R., 2018. Design and detection of Hardware Trojans (Doctoral dissertation, Masarykova univerzita, Fakulta informatiky).

[32] Banga, M., Chandrasekar, M., Fang, L. and Hsiao, M.S., 2008, May. Guided test generation for isolation and detection of embedded Trojans in ICs. In Proceedings of the 18th ACM Great Lakes symposium on VLSI (pp. 363-366).

[33] T. Tuan and B. Lai, “Leakage power analysis of a 90nm FPGA,” in IEEE 2003 Custom Integrated Circuits Conference. Proceedings, 2003, pp. 57–60. 10, 12

[34] DIGITIMES, 2012. Trends in the global IC design service market. Retrieved from http://www.digitimes.com/news/a20120313RS400.html?chid=2.