ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Βιβλιογραφική έρευνα τεχνικών ανίχνευσης κακόβουλων τροποποιήσεων υλικού

Διπλωματική Εργασία

Τσαβδαρίδης Παύλος

Επιβλέπων Καθηγητής:

Σταμούλης Γεώργιος, Καθηγητής Π.Θ

Βόλος, 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Βιβλιογραφική έρευνα τεχνικών ανίχνευσης κακόβουλων τροποποιήσεων υλικού

Διπλωματική Εργασία

Τσαβδαρίδης Παύλος

Επιβλέπων Καθηγητής:

Σταμούλης Γεώργιος, Καθηγητής Π.Θ

Βόλος, 2019

UNIVERSITY OF THESALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

A survey on hardware Trojan detection techniques

Diploma Thesis

Tsavdaridis Pavlos

Supervisor:

Stamoylis Georgios, Professor U.TH

Volos, 2019

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή αυτής της διπλωματικής εργασίας, κ. Σταμούλη Γεώργιο, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου το εν λόγω θέμα, καθώς και για την πολύτιμη βοήθεια και καθοδήγησή του κατά τη διάρκεια εκπόνησης.

Επίσης, ευχαριστώ τους φίλους και συμφοιτητές μου για την υποστήριξη και την συνεργασία κατά τη διάρκεια των σπουδών. Τέλος, θα ήθελα να πω ένα μεγάλο ευχαριστώ και πόσο ευγνώμων είμαι, στη γυναίκα μου, στους γονείς μου, στις αδερφές μου και στη γιαγιά μου, για την αμέριστη και ανιδιοτελή βοήθεια και αγάπη τους όλα αυτά τα χρόνια.

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, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει 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. 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/Η Δηλών/ούσα

(Υπογραφή)

Τσαβδαρίδης Παύλος

03/07/2019

ΠΕΡΙΛΗΨΗ

Η εργασία σχετίζεται με τις τεχνικές ανίχνευσης κακόβουλων τροποποιήσεων υλικού. Σκοπός της εργασίας είναι η αναζήτηση τέτοιων μεθόδων στη βιβλιογραφία και η καταγραφή τους. Ωστόσο, επειδή οι μέθοδοι και οι τεχνικές ανίχνευσης κακόβουλων τροποποιήσεων υλικού είναι πολλές, η εργασία αυτή εστιάζει κυρίως σε έναν τύπο ανίχνευσης κακόβουλων τροποποιήσεων υλικού, αυτόν της ανάλυσης πλευρικών καναλιών. Αρχικά, γίνεται μια εισαγωγή στις κακόβουλες τροποποιήσεις υλικού και σε ταξινομίες που έχει προτείνει η επιστημονική κοινότητα. Έπειτα, αναλύονται οι τεχνικές ανίχνευσης κακόβουλων τροποποιήσεων υλικού που βασίζονται στην ισχύ, το χρόνο, την ενεργοποίηση, την αρχιτεκτονική της κακόβουλης τροποποίησης υλικού. Τέλος, αναλύονται πιο σύγχρονες προσεγγίσεις όπως αυτές που χρησιμοποιούν τα μέσα της μηχανικής μάθησης για να εντοπίσουν μια κακόβουλη τροποποίηση υλικού.

ABSTRACT

This thesis is related to hardware Trojan detection techniques. The aim of the thesis is to search for such methods in the scientific work of scientific community and to record them. However, because the methods and techniques for detecting malicious hardware Trojans are many, this work focuses primarily on one type of hardware Trojan detection techniques, that of side-channel analysis. Initially, there is an introduction to hardware Trojans and taxonomies proposed by the scientific community. Next, hardware Trojan detection techniques based on power, time, and activation are analyzed. Finally, more modern approaches such as those using machine learning tools to detect hardware Trojans are analyzed.

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη της βιομηχανίας κυκλωμάτων θεωρείται εκθετική πλέον. Αποτέλεσμα αυτού είναι και η ταχεία παγκοσμιοποίηση της αλυσίδας εφοδιασμού της. Επειδή ένα πολύπλοκο κύκλωμα συχνά περιλαμβάνει πολλούς προμηθευτές, χυτήρια κατασκευών και εγκαταστάσεις ελέγχων που εκτείνονται σε πολλές ηπείρους, είναι εξαιρετικά δύσκολο, αν όχι εντελώς αδύνατο, να εντοπιστεί η πηγή κάθε εξαρτήματος και να εξασφαλιστεί η ασφάλεια και η ακεραιότητα ολόκληρης της αλυσίδας εφοδιασμού.

Η πολυπλοκότητα και η εξέλιξη παράλληλα που χαρακτηρίζει τη σημερινή διαδικασίας ανάπτυξης κυκλωμάτων προκαλεί ολοένα και περισσότερες απειλές που βασίζονται στις κακόβουλες τροποποιήσεις υλικού. Από την πρώτη εμφάνιση και παράλληλα εντοπισμού τους από τους Agrawal et al. (2007), το πεδίο της έρευνας κακόβουλων τροποποιήσεων υλικού έχει σημειώσει αξιοσημείωτη ανάπτυξη και έχουν αξιοποιηθεί, επιδειχθεί και βελτιωθεί διάφοροι μηχανισμοί επίθεσης κακόβουλων τροποποιήσεων υλικού και άμυνας κατά αυτών.

Μέχρι πρόσφατα, οι περισσότερες κακόβουλες τροποποιήσεις υλικού αναπτύσσονταν ως ψηφιακά κυκλώματα και οι όποιες τεχνικές ανίχνευσής τους ακολουθούσαν την ίδια υπόθεση. Ωστόσο, καθώς τα κυκλώματα και οι τεχνολογίες, γύρω από αυτά εξελίσσονται συνεχώς, οι επιθέσεις μέσω κακόβουλων τροποποιήσεων υλικού εξελίσσονται και αυτές και λαμβάνουν υπόψη τα νέα δεδομένα.

Τί είναι όμως μια κακόβουλη τροποποίηση υλικού; Είναι μια κακόβουλη τροποποίηση στο υλικό ενός κυκλώματος που προκαλεί σε ένα τσιπ να εκτελέσει ανεπιθύμητες λειτουργίες. Στην ιδανική περίπτωση, αυτές οι τροποποιήσεις που γίνονται σε ένα κύκλωμα θα πρέπει να ανιχνεύονται κατά τη διάρκεια οποιασδήποτε φάσης ελέγχου.

Προκειμένου να αποφύγει ένα τέτοιο λειτουργικό έλεγχο, κάποιος που θέλει να επέμβει σε ένα κύκλωμα συνήθως σχεδιάζει την κακόβουλη τροποποίηση υλικού έτσι ώστε αυτή να ενεργοποιηθεί μόνο κάτω από ορισμένες σπάνιες συνθήκες και να παραμείνει μη ανιχνεύσιμη κατά τη διάρκεια των ελέγχων (Nowroz, Hu, Koushanfar & Reda, 2014).

Για παράδειγμα, μπορεί μια κακόβουλη τροποποίηση υλικού να χρησιμοποιεί έναν πυκνωτή και ένα μετρητή που τον αυξάνει κάθε φορά που εκτελείται μια εντολή. Μετά από

λίγους κύκλους, ο πυκνωτής φορτίζει και επιβεβαιώνει ένα σήμα το οποίο χρησιμοποιείται για την αναστροφή κάποιων συγκεκριμένων κομματιών λογικής ελέγχου και μπορεί να δώσει πρόσβαση σε αυτόν που κατευθύνει την κακόβουλη τροποποίηση σε αρχεία του συστήματος και σε αρχεία που κανονικά δεν έχει πρόσβαση.

Οι συνέπειες που μια κακόβουλη τροποποίηση υλικού μπορεί να προκαλέσει είναι σίγουρα πολλές και σίγουρα σημαντικές γι' αυτόν που δέχεται την επίθεση. Για παράδειγμα, μπορεί να επέμβει στα αρχεία μητρώου (Register Files) τα οποία αποθηκεύουν κρίσιμες πληροφορίες ασφάλειας και μια παραβίαση σε αυτά, μπορεί τελικά να οδηγήσει σε διαρροή ευαίσθητων δεδομένων.

Πιο συγκεκριμένα, ένα τμήμα κώδικα ενός αρχείου μητρώου μπορεί περιέχει ένα πεδίο που καθορίζει τα δικαιώματα πρόσβασης (Current Privilege Level) και δείχνει αν η κεντρική μονάδα επεξεργασίας εκτελείται αυτή τη στιγμή σε κατάσταση λειτουργίας χρήστη (user mode) ή πυρήνα (kernel mode). Οι διαδικασίες λειτουργίας χρήστη δεν επιτρέπεται να έχουν πρόσβαση στα δεδομένα από τον χώρο του πυρήνα βάσει του αρχείου με τα δικαιώματα πρόσβασης που έχει οριστεί στο τμήμα κώδικα ενός αρχείου μητρώου. Αυτός που θέλει να βλάψει το κύκλωμα όμως, μπορεί να πάρει τον έλεγχο της λειτουργίας του πυρήνα χειριζόμενος την καταχώρηση στα αρχεία μητρώου που αποθηκεύει τη λειτουργία εκτέλεσης και να εκτελέσει μη εξουσιοδοτημένες ενέργειες (Chakraborty, Narasimhan & Bhunia, 2010).

Από την ταξινομία των κακόβουλων τροποποιήσεων υλικού μπορεί να καταλάβει κανείς εύκολα πως οι μορφές και οι τρόποι που μπορεί να υφίσταται μια κακόβουλη τροποποίηση υλικού και αντίστοιχα να ενεργεί, ποικίλουν. Για παράδειγμα, μια κακόβουλη τροποποίηση μπορεί να είναι απενεργοποιημένη και να ενεργοποιείται κάτω από συγκεκριμένες σπάνιες συνθήκες (όπως αυτή που αναφέρεται πιο πάνω). Μπορεί, επίσης, να είναι μόνιμα ενεργοποιημένη επιφέροντας μικρές αλλαγές στο κύκλωμα, γεγονός που τελικά οδηγεί στο ότι το τσιπ θα συμπεριφερθεί όπως θα συμπεριφέρονταν και χωρίς την κακόβουλη τροποποίηση και άρα η ανίχνευσή του είναι δύσκολη.

Αντίστοιχα, υπάρχουν πολλές κατηγορίες ανίχνευσης κακόβουλων τροποποιήσεων υλικού. Η εργασία αυτή θα επικεντρωθεί στην ανάλυση πλευρικών καναλιών για την ανίχνευση κακόβουλων τροποποιήσεων υλικού και θα αναλυθούν οι τεχνικές ανίχνευσης κακόβουλων τροποποιήσεων υλικού που βασίζονται στην ισχύ, το χρόνο, την ενεργοποίηση και την αρχιτεκτονική της κακόβουλης τροποποίησης υλικού. Τέλος, θα αναλυθούν πιο σύγχρονες προσεγγίσεις όπως αυτές που χρησιμοποιούν τα μέσα της μηχανικής μάθησης για να εντοπίσουν μια κακόβουλη τροποποίηση υλικού (Tehranipoor & Koushanfar, 2010).

Έτσι, στο επόμενο κεφάλαιο (Κεφάλαιο 2) γίνεται μια εισαγωγή στις κακόβουλες τροποποιήσεις υλικού και αναλύονται δύο βασικές ταξινομίες με βάση συγκεκριμένα χαρακτηριστικά του. Η εισαγωγή αυτή είναι απαραίτητη για να γίνει ξεκάθαρη η λειτουργία και η δομή των κακόβουλων τροποποιήσεων υλικού, στοιχεία που θα οδηγήσουν στην καλύτερα κατανόηση των μεθόδων ανίχνευσής τους.

Έπειτα από το Κεφάλαιο 2, λοιπόν, ακολουθεί το Κεφάλαιο 3 που αποτελεί την έρευνα για τις μεθόδους ανίχνευσης κακόβουλων τροποποιήσεων υλικού. Στο κεφάλαιο αυτό αναλύονται οι μέθοδοι που βασίζονται στην ανάλυση πλευρικών καναλιών, μιας και οι μέθοδοι ανίχνευσης είναι πολλοί στη βιβλιογραφία. Αναλυτικότερα, αναπτύσσονται μέθοδοι που βασίζονται στην ισχύ, το χρόνο, την ενεργοποίηση και την αρχιτεκτονική της κακόβουλης τροποποίησης υλικού. Η τελευταία παράγραφος του κεφαλαίου είναι αφιερωμένη σε σύγχρονες προσεγγίσεις που φέρνουν ένα βήμα μπροστά τις μεθόδους ανίχνευσης και βασίζονται σε σύγχρονες εξελίξεις όπως είναι η μηχανική μάθηση.

ΚΕΦΑΛΑΙΟ 2

ΚΑΚΟΒΟΥΛΕΣ ΤΡΟΠΟΙΗΣΕΙΣ ΥΛΙΚΟΥ

Μια κακόβουλη τροποποίηση υλικού είναι μια κακόβουλη τροποποίηση του κυκλώματος ενός ολοκληρωμένου τσιπ. Η κακόβουλη τροποποίηση υλικού χαρακτηρίζεται τόσο από την εμφάνισή της (από πλευράς υλικού) όσο και από τη συμπεριφορά της (από πλευράς υλικού). Ο φόρτος (payload) μιας κακόβουλης τροποποίησης υλικού είναι ολόκληρη η δραστηριότητα την οποία εκτελεί ο δούρειος ίππος όταν ενεργοποιείται. Σε γενικές γραμμές, οι κακόβουλες τροποποιήσεις υλικού προσπαθούν να παρακάμψουν ή να απενεργοποιήσουν τα όρια που θέτει η ασφάλεια ενός συστήματος.

Μέσω της παράκαμψης της ασφάλειας ή μέσω της απενεργοποίησής της, οι κακόβουλες τροποποιήσεις υλικού μπορούν να προβούν σε μια σειρά από κακόβουλες ενέργειες. Ένα παράδειγμα κακόβουλης ενέργειας είναι ακόμα και η διαρροή προσωπικών πληροφοριών που βρίσκονται στο σύστημα μέσω της εκπομπής τους εκτός του τσιπ μέσω ειδικών συχνοτήτων. Οι τροποποιήσεις, επίσης, έχουν τη δυνατότητα να σταματήσουν τη λειτουργία, να διαταράξουν τις διεργασίες ή ακόμα και να καταστρέψουν ολόκληρο το τσιπ ή τα μέρη από το οποίο αποτελείται.

Οι κακόβουλες τροποποιήσεις υλικού μπορούν να εισαχθούν ως κρυμμένα στοιχεία (καμουφλαρισμένα θα έλεγε κάποιος) που εισάγονται «μη επίσημα» κατά τη διαδικασία σχεδιασμού ενός τσιπ υπολογιστή, χρησιμοποιώντας ένα κύκλωμα που, όπως είναι αναμενόμενο προέρχεται από μια μη αξιόπιστη πηγή ή βρήκε το δρόμο του στη διαδικασία αυτή μέσω ενός υπαλλήλου (ανήθικου θα μπορούσε να πει κάποιος). Τα συγκεκριμένα, τροποποιημένα, κυκλώματα χρησιμοποιούνται πολύ συχνά για ομάδες ειδικών συμφερόντων, όπως π.χ. οι κυβερνήσεις και χρηματοδοτούνται μέχρι και από επιχειρήσεις. Μάλιστα, πολλές φορές ο σκοπός τους σχετίζεται με χαρακτηριστικά κατασκοπείας (Chakraborty, Narasimhan & Bhunia, 2009).

Οι «επιθέσεις» μέσω κακόβουλων τροποποιήσεων υλικού σε κυβερνητικά τμήματα πληροφορικής υψίστης ασφαλείας, είναι ένα πολύ γνωστό πρόβλημα και αποτελεί τροχοπέδη στη διαδικασία αγοράς περιφερειακών συσκευών όπως ποντίκια, πληκτρολόγια, κάρτες γραφικών και κάρτες δικτύου. Ειδικά οι αγορές από μη αξιόπιστες πηγές, μπορεί να οδηγήσουν σε υλικό (hardware) το οποίο έχει υποστεί κακόβουλη τροποποίηση και έτσι υπάρχει μεγάλη πιθανότητα και κίνδυνος να διαρρεύσουν κωδικοί πρόσβασης που

εισάγονται μέσω του πληκτρολογίου, ή να δοθεί η δυνατότητα απομακρυσμένης πρόσβασης σε άλλα άτομα χωρίς την απαραίτητη εξουσιοδότηση από το σύστημα (Hagelin, 2006).

2.1 Ταξινομία τροποποιήσεων υλικού

Το πρόβλημα των τροποποιήσεων με κακόβουλους σκοπούς βασίζεται στην οικονομική κατάσταση που επικρατεί στον κόσμο τα τελευταία χρόνια. Λόγω των παγκόσμιων οικονομικών πιέσεων, τα εργοστάσια παραγωγής των τσιπ και των συσκευών γενικότερα, έχουν εξαπλωθεί σε όλο τον κόσμο και όπως είναι αναμενόμενο, η εξάπλωση οδηγεί σε χώρες και περιοχές που τα κόστη κατασκευής, μπορούν να είναι φθηνότερα, παρά ακριβότερα. Πολλά από τα εργοστάσια παραγωγής τσιπ και συσκευών, ωστόσο, απειλούνται από κακόβουλες «επιθέσεις» και πολλοί κακόβουλοι παράγοντες μπορούν να προσπεράσουν τα μέτρα ασφαλείας των εργοστασίων και ως αποτέλεσμα να εισάγουν τροποποιημένο υλικό στη διαδικασία σχεδιασμού και παραγωγής των τσιπ (Bhasin et al., 2013).

2.2 Ταξινομία με βάση τα χαρακτηριστικά ενεργοποίησης

Μιλώντας για κακόβουλες τροποποιήσεις θεωρείται σημαντικό να γίνει μια αναφορά στους τύπους και τα είδη των κακόβουλων τροποποιήσεων υλικού. Για τον λόγο αυτό, θεωρήθηκε απαραίτητη η ανάλυση δύο βασικών ταξινομιών που θα βοηθήσει τον αναγνώστη της εργασίας να καταλάβει, εκτός από τη σημασία των κακόβουλων τροποποιήσεων υλικού, τα είδη και τους τύπους τους.

Οι Jin, Kupp, & Makris (2009), παρουσιάζουν τρείς (3) ομάδες χαρακτηριστικών των κακόβουλων τροποποιήσεων υλικού με βάση τα χαρακτηριστικά ενεργοποίησής τους. Κάθε ομάδα χαρακτηριστικών, σχετίζεται με τις μεθόδους στις οποίες βασίζεται μια κακόβουλη τροποποίηση υλικού για να δράσει και κάθε ομάδα περιλαμβάνει ένα σύνολο μεθόδων μέσω των οποίων επιτυγχάνονται οι κακόβουλες ενέργειες. Οι τρείς (3) ομάδες χαρακτηριστικών είναι ο φόρτος (payload), τα εναύσματα (triggers) και η βελτιστοποίηση κώδικα (code optimization).

2.2.1 Φόρτος (payload)

Για να είναι χρήσιμη μια κακόβουλη τροποποίηση στους δημιουργούς της, θα πρέπει σίγουρα να περιλαμβάνει ένα φόρτο. Να περιλαμβάνει δηλαδή τα απαραίτητα δεδομένα για να εκτελέσει οποιαδήποτε κακόβουλη πράξη. Ουσιαστικά, πρόκειται για μια προσπάθεια

σύνδεσης της ενεργοποίησης της κακόβουλης τροποποίησης με κάποιο ντετερμινιστικό γεγονός που είναι σίγουρα ευνοϊκό για τον εισβολέα – αυτόν που θέλει να βλάψει ουσιαστικά το σύστημα. Ανάλογα με το φόρτο της κάθε κακόβουλης τροποποίησης, μπορούν να διακριθούν κάποιες ομάδες κακόβουλων τροποποιήσεων (Lin et al., 2009).

Για παράδειγμα, μια κακόβουλη τροποποίηση μπορεί να μεταδώσει στον εισβολέα μέσω εσωτερικών σημάτων πληροφορίες σχετικά με ευαίσθητα δεδομένα του συστήματος. Θα μπορούσε για παράδειγμα να μεταδώσει τον κωδικό πρόσβασης ενός χρήστη. Αυτό θα έδινε τη δυνατότητα πρόσβασης σε αρχεία του χρήστη χωρίς την έγκρισή του, με καταστροφικές συνέπειες γι' αυτόν. Μάλιστα, δεν επιχειρείται στην εργασία να γίνει αναφορά στις συνέπειες που μπορεί να έχει μια τέτοια κακόβουλη ενέργεια μέσω μιας κακόβουλης τροποποίησης υλικού σε κυβερνητικό επίπεδο.

Βέβαια, σαφώς, για έναν εισβολέα, που θέλει να επηρεάσει μια συσκευή η οποία είναι και κρυπτογραφημένη, η πιο πολύτιμη πληροφορία γι' αυτόν είναι το κλειδί κρυπτογράφησης. Μέσω, λοιπόν, των εσωτερικών σημάτων μπορεί να μεταδοθεί η πληροφορία αυτή. Πιο συγκεκριμένα, όταν ενεργοποιηθεί η τροποποίηση, το κλειδί θα μεταδοθεί μαζί με το κείμενο κρυπτογράφησης. Αυτός που έχει τοποθετήσει την τροποποίηση (ή αυτός που κρύβεται γενικότερα πίσω από την ενέργεια), ακούγοντας κατάλληλα το κανάλι μετάδοσης, μπορεί να καταγράψει το κλειδί και να εισέλθει ανενόχλητος το σύστημα.

Επίσης, μια κακόβουλη τροποποίηση μπορεί να επέμβει σε άλλα κυκλώματα και να επηρεάσει τη λειτουργία τους. Η τροποποίηση, δηλαδή, επεμβαίνει στη λειτουργία των κυκλωμάτων μέσω των αντίστοιχων αρχείων και αλλάζει τις όποιες ρυθμισμένες λειτουργίες, με άλλες. Οι λειτουργίες στις οποίες γίνεται αναφορά, πρέπει να σημειωθεί ότι βασίζονται σε αρχεία απλού κειμένου (plain text) (Lin et al., 2009).

Όταν, λοιπόν, ενεργοποιείται μια τέτοια κακόβουλη τροποποίηση που επηρεάζει τη λειτουργία άλλων κυκλωμάτων, ο δέκτης που προορίζεται να λάβει κανονικά το σήμα, θα το λάβει αλλά τροποποιημένο ανάλογα με το ποια εντολή έχει δοθεί από την κακόβουλη τροποποίηση να μεταδοθεί. Για παράδειγμα, μπορεί μέσω της τροποποίησης μια λέξη να αντικαθίσταται με μια άλλη. Έτσι, μπορεί ένα κείμενο που αρχικά δίνεται εντολή να μεταδοθεί να είναι το «κατέθεσε 100 ευρώ στο λογαριασμό» και τελικά να μεταδίδεται το «κατέθεσε 10000 ευρώ στο λογαριασμό». Μια τέτοια τροποποίηση μπορεί να προκαλέσει τεράστιες συνέπειες τόσο γι' αυτόν που εκπέμπει το μήνυμα όσο και γι' αυτόν που το λαμβάνει.

Τέλος, σε κάποιες περιπτώσεις, περισσότερο ακραίες μπορεί η τροποποίηση να επέμβει με τέτοιο τρόπο στα κυκλώματα ώστε να αλλάξει τη λειτουργία τους και τελικά να οδηγήσει στην καταστροφή ολόκληρου του τσιπ.

Αυτή η προσέγγιση έχει το πλεονέκτημα ότι είναι πολύ δύσκολο να εντοπιστεί κατά τη διάρκεια της φάσης ελέγχου, αφού ο χρόνος που τίθεται στην τροποποίηση να μείνει ανενεργή είναι συνήθως μεγαλύτερος από τον χρόνο που απαιτεί η φάση ελέγχου. Έτσι, στη φάση του ελέγχου, οι κακόβουλες τροποποιήσεις αδρανοποιούνται, μένουν ανενεργές και τελικά δε βλάπτουν τα τσιπ. Ωστόσο, αργότερα αν δεν εντοπιστούν στη φάση ελέγχου και τελειώσει ο χρόνος για τον οποίο έχουν ρυθμιστεί να είναι ανενεργές, προκαλούν την καταστροφή του τσιπ (Kutzner, Poschmann & Stöttinger, 2013).

2.2.2 Εναύσματα (triggers)

Όπως με το χαρακτηριστικό του φόρτου, έτσι και στο κομμάτι αυτό, οι κακόβουλες τροποποιήσεις υλικού μπορούν να διαχωριστούν ανάλογα με το έναυσμα που τα ενεργοποιεί. Το κάθε έναυσμα για κάθε κακόβουλη τροποποίηση λογισμικού έχει σχεδιαστεί για να αποφεύγει τη φάση του ελέγχου του τσιπ είτε με βάση εντολές – εναύσματα που χρησιμοποιούνται σπάνια (π.χ. αδιευκρίνιστες ακολουθίες εισόδου), είτε με τη χρήση κάποιου μετρητή (counter) που οδηγεί στην ενεργοποίηση της τροποποίησης μετά από μεγάλο χρονικό διάστημα.

Ένα παράδειγμα τροποποίησης που βασίζεται σε έναυσμα, σύμφωνα με τους Beaumont, Hopkins & Newby (2011) είναι όταν ο άνθρωπος που θέλει να βλάψει μια συσκευή έχει κανονικά πρόσβαση σε αυτή (την έχει στα χέρια του δηλαδή, σαν υλική οντότητα) και μπορεί να δώσει μια ειδική εντολή εισόδου η οποία με τη σειρά της ενεργοποιεί την κακόβουλη τροποποίηση υλικού άμεσα.

Στην κατηγορία αυτή, οι μέθοδοι εναύσματος μπορούν να είναι αρκετά αχανείς και δύσκολο να ανιχνευθούν κατά τη διάρκεια φάσης του ελέγχου. Το πιο συμπαγές αλλά χρήσιμο έναυσμα μπορεί να είναι ο επαναπροσδιορισμός ενός σπανίως χρησιμοποιούμενου πλήκτρου στο πληκτρολόγιο το οποίο δίνει την εντολή της ενεργοποίησης της κακόβουλης τροποποίησης. Η φυσική παρουσία του ανθρώπου που θέλει να βλάψει τη συσκευή βέβαια είναι βασική αλλά αυτή είναι και η κατηγορία εναυσμάτων η οποία αναλύεται στην παράγραφο αυτή.

Μια εναλλακτική προσέγγιση είναι η χρήση μιας ειδικά διαμορφωμένης συμβολοσειράς ως εντολή εισόδου. Η χρήση μιας ειδικής συμβολοσειράς ως έναυσμα έχεις πολλές

πιθανότητες να ξεφύγει από τη φάση του ελέγχου, καθώς ο αριθμός των συνδυασμών εντολών εισόδου είναι πολύ μεγάλος και αυτή η ειδική συμβολοσειρά είναι αβέβαιο για το αν θα πληκτρολογηθεί τυχαία. Είναι σαφές, ωστόσο, ότι ένα έναυσμα που βασίζεται στη φυσική παρουσία αυτού που θέλει να βλάψει μια συσκευή έχει περιορισμένες εφαρμογές (Beaumont, Hopkins & Newby, 2011).

Ένας άλλος τρόπος χρήσης του εναύσματος πέρα από τη φυσική, ουσιαστικά εκτέλεση, είναι το έναυσμα να δοθεί εσωτερικά αυτή τη φορά, μέσω μιας εντολής εισόδου ειδικά για την ενεργοποίηση της κακόβουλης τροποποίησης ή μέσω μιας αλλαγής σήματος. Στην κατηγορία αυτή η φυσική επαφή του ανθρώπου που θέλει να βλάψει μια συσκευή δεν είναι δεδομένη όπως πριν.

Για το λόγο αυτό, πολλές υλοποιήσεις κακόβουλων τροποποιήσεων χρησιμοποιούν έναν εσωτερικό μετρητή που ουσιαστικά αποτελεί το μηχανισμό για να ενεργοποιηθεί η κακόβουλη τροποποίηση. Έτσι, ένας εσωτερικός μετρητής μπορεί να κρατάει τον αριθμό των χρόνων μετάδοσης σημάτων του τσιπ και μόλις υπερβεί ένα προκαθορισμένο αριθμό, τότε, να δοθεί εντολή στην κακόβουλη τροποποίηση να ενεργοποιηθεί (Liu, Luo & Wang, 2011).

Αντίστοιχα, η εναλλαγή εσωτερικών σημάτων όπως αναφέρθηκε, μπορεί να λειτουργήσει ως έναυσμα. Για παράδειγμα, κάθε φορά που αλλάζει το κλειδί της μεταφοράς των σημάτων τότε ενεργοποιείται αντίστοιχα και το έναυσμα για την ενεργοποίηση της κακόβουλης τροποποίησης.

Ένα ακόμη παράδειγμα χρήσης του εναύσματος είναι να μη χρειάζεται τελικά κάποιο είδος εναύσματος. Αυτό συμβαίνει γιατί δε χρειάζεται να υπάρξει έναυσμα από τη στιγμή που η κακόβουλη τροποποίηση είναι μόνιμα ενεργοποιημένη. Η απουσία του εναύσματος κάνει τις κακόβουλες τροποποιήσεις αυτές, πιο επιθετικές και ρυθμίζει την τροποποίηση έτσι ώστε να είναι πάντα ενεργοποιημένη.

Στην περίπτωση της μη ύπαρξης εναύσματος, πρέπει ο φόρτος της κακόβουλης τροποποίησης να είναι καλά κρυμμένος. Αυτό σημαίνει ότι η οποιαδήποτε μετάδοση πληροφοριών και σημάτων γίνεται με τρόπους που δεν μπορούν να ανιχνευθούν κατά τη φάση του ελέγχου του τσιπ. Ένα μειονέκτημα της περίπτωσης αυτής είναι ότι η κακόβουλη τροποποίηση αναγκάζεται να κάνει χρήση ενέργειας η οποία θα είναι υψηλότερη, και μετρώντας την κατά τη διάρκεια της φάσης του ελέγχου υπάρχει μεγάλη πιθανότητα να προκύψουν οι αντίστοιχες υποψίες (Liu, Luo & Wang, 2011).

2.2.3 Βελτιστοποίηση κώδικα (code optimization)

Η τρίτη ομάδα χαρακτηριστικών είναι η βελτιστοποίηση κώδικα. Σε αυτές τις περιπτώσεις οι μέθοδοι που χρησιμοποιούνται είναι επίσης δύσκολα ανιχνεύσιμες κατά τη φάση του ελέγχου του τσιπ.

Η πρώτη περίπτωση στοχεύει ειδικά στον κώδικα μιας γλώσσας περιγραφής υλικού (Hardware Description Language - HDL). Η γλώσσα αυτή, λοιπόν, είναι μια εξειδικευμένη γλώσσα υπολογιστών που χρησιμοποιείται για να περιγράψει τη δομή και τη συμπεριφορά των ηλεκτρονικών κυκλωμάτων και πιο συχνά τα κυκλώματα ψηφιακής λογικής (Yazdanbakhsh, 2015).

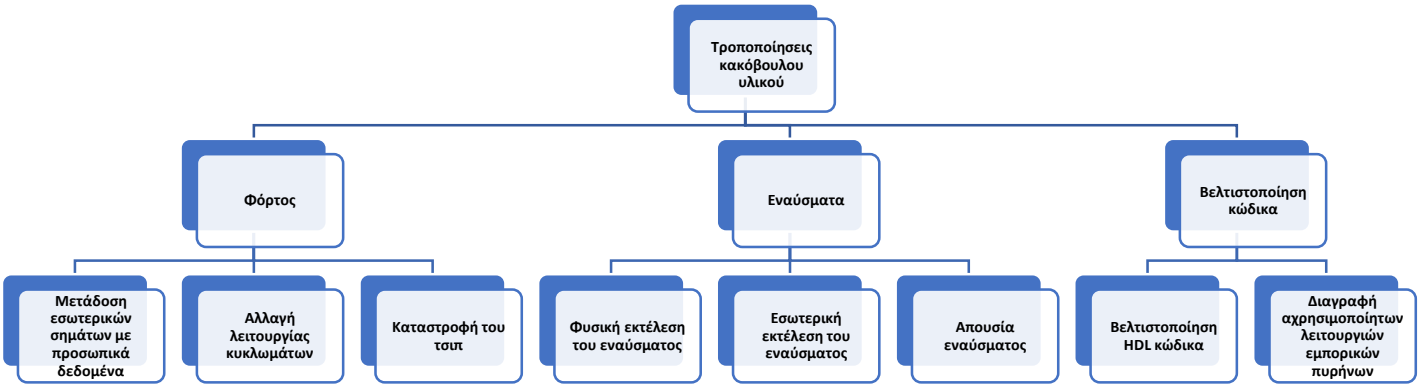
Όταν ο κώδικας αυτός δεν είναι βελτιστοποιημένος, τότε πολλές φορές το αποτέλεσμα περιέχει πολλά σημεία που ο κώδικας μπορεί να αντικατασταθεί με άλλον καλύτερο και περισσότερο βελτιστοποιημένο. Έτσι, αυτός που θέλει να βλάψει μια συσκευή και επιπλέον ξέρει και τις προδιαγραφές του κυκλώματος που θέλει να επηρεάσει, μπορεί να γράψει ξανά τον κώδικα HDL με πιο συμπαγή τρόπο χωρίς να επηρεαστεί η λειτουργία και η λειτουργικότητα του κυκλώματος. Αποτέλεσμα αυτού, είναι οι πόροι του τσιπ που ουσιαστικά ελευθερώνει με τη βελτιστοποίηση ο εισβολέας, να είναι διαθέσιμοι για να χρησιμοποιηθούν από την κακόβουλη τροποποίηση (Jyothi & Rajendran, 2018).

Η δεύτερη περίπτωση, είναι η επίθεση σε εμπορικά διαθέσιμα κυκλώματα και πυρήνες. Οι εμπορικοί πυρήνες χρησιμοποιούνται σήμερα ευρέως τόσο σε ακαδημαϊκά όσο και σε εμπορικά συστήματα για την ελαχιστοποίηση του χρόνου ανάπτυξης.

Ως επαναχρησιμοποιήσιμες μονάδες, οι εμπορικοί πυρήνες σχεδιάζονται συνήθως για να ολοκληρώσουν κάποια γενική φύσεως λειτουργία και έτσι να ανταποκρίνονται εύκολα σε πολλά και διαφορετικά σενάρια χρήσης και εργασιών.

Ωστόσο, στις περισσότερες εφαρμογές, όλες αυτές οι λειτουργίες που έχουν προγραμματιστεί στα κυκλώματα δε θα είναι χρήσιμες. Αυτό οδηγεί σε μη βελτιστοποιημένο κώδικα HDL, ο οποίος μπορεί να βελτιστοποιηθεί τροποποιώντας λειτουργίες που δε χρησιμοποιούνται. Ουσιαστικά, οι λειτουργίες αυτές εξαλείφονται. Και πάλι, λοιπόν, η περιοχή του τσιπ που εξοικονομείται με αυτή την βελτιστοποίηση μέσω της κακόβουλης τροποποίησης υλικού, μπορεί να χρησιμοποιηθεί για την εισαγωγή των κακόβουλων τροποποιήσεων υλικού (Yazdanbakhsh, 2015).

Η παρακάτω εικόνα δείχνει την ταξινομία, σχηματικά, ως προς την προσέγγιση που περιγράφηκε σε αυτή την παράγραφο.



Εικόνα 1: Ταξινομία κακόβουλων τροποποιήσεων υλικού κατά Yin, Kupp & Makris (2009)

2.3 Ταξινομία με βάση τα φυσικά χαρακτηριστικά, την ενεργοποίηση και τα χαρακτηριστικά δράσης

Μια ταξινομία, η οποία σύμφωνα με τους Tehranipoor & Koushanfar (2010), είναι και η πρώτη προσπάθεια ταξινομίας των κακόβουλων τροποποιήσεων υλικού είναι αυτή των Wang et al. (2008). Στην ταξινομία αυτή, οι συγγραφείς στο έργο τους διαχωρίζουν τις κακόβουλες τροποποιήσεις υλικού σε τρείς (3) βασικές κατηγορίες και σύμφωνα με τα φυσικά χαρακτηριστικά, την ενεργοποίηση και τα χαρακτηριστικά δράσης.

Τα φυσικά χαρακτηριστικά (τα απτά δηλαδή) χωρίζονται περαιτέρω σε τέσσερις κατηγορίες. Οι κατηγορίες αυτές είναι ο τύπος, το μέγεθος, η κατανομή και η δομή των κακόβουλων τροποποιήσεων. Η ταξινόμηση που προτείνεται, λοιπόν, περιγράφει τις κακόβουλες τροποποιήσεις χρησιμοποιώντας έξι χαρακτηριστικά συνολικά, που περιλαμβάνουν τέσσερα από την κατηγορία φυσικών χαρακτηριστικών, ένα με βάση τα χαρακτηριστικά ενεργοποίησης και ένα ακόμα με βάση τα χαρακτηριστικά δράσης. Σύμφωνα με τους δημιουργούς της ταξινομίας, υπάρχει και η πιθανότητα κάποιοι τύποι

κακόβουλων τροποποιήσεων, να είναι υβριδικοί με βάση την ταξινομία αυτή. Για παράδειγμα, μπορεί μια κακόβουλη τροποποίηση να διαθέτει περισσότερα από ένα φυσικά χαρακτηριστικά στη συγκεκριμένη κατηγορία.

2.3.1 Ταξινομία με βάση τα φυσικά χαρακτηριστικά

Στην κατηγορία των φυσικών χαρακτηριστικών, όπως αναφέρθηκε ήδη υπάρχουν τέσσερα βασικά χαρακτηριστικά και είναι ο τύπος, το μέγεθος, η κατανομή και η δομή. Προφανώς, και η κατηγορία αυτή αναφέρεται με τη φυσική παρουσία των τροποποιήσεων, το καθαρό υλικό δηλαδή.

Ξεκινώντας από τον τύπο, το χαρακτηριστικό αυτό χωρίζει τις κακόβουλες τροποποιήσεις σε λειτουργικές και παραμετρικές κλάσεις. Η λειτουργική κλάση περιλαμβάνει τις κακόβουλες τροποποιήσεις που επιτυγχάνονται με φυσικό τρόπο (μέσω καθαρά υλικού δηλαδή) και γίνονται με την προσθήκη ή διαγραφή τρανζίστορ ή πυλών. Η παραμετρική κλάση από την άλλη περιλαμβάνει τις κακόβουλες τροποποιήσεις, αυτές που πραγματοποιούνται μέσω του ήδη υφιστάμενου υλικού – δηλαδή των κυκλωμάτων και των πυλών.

Για παράδειγμα, στην παραμετρική κλάση εντάσσονται ενέργειες που αραιώνουν ένα σύρμα σε κύκλωμα. Επίσης, μπορεί να αποδυναμώνουν ένα τρανζίστορ ή γενικότερα να επεμβαίνουν στη φυσική γεωμετρία του σχεδιασμού. Σκοπός φυσικά στις ενέργειες αυτές είναι η υπονόμευση της αξιοπιστίας ή η πρόκληση μιας αποτυχίας σε λειτουργικό και παραγωγικό επίπεδο (Karri, Rajendran, Rosenfeld & Tehranipoor, 2010).

Περνώντας στο μέγεθος, γίνεται αναφορά ουσιαστικά στο μέγεθος της κακόβουλης τροποποίησης υλικού. Δηλαδή, γίνεται αναφορά στον αριθμό των στοιχείων αυτών του τσιπ που έχουν προστεθεί, αφαιρεθεί ή και τροποποιηθεί. Το μέγεθος μιας κακόβουλης τροποποίησης είναι πολύ σημαντικός παράγοντας κατά τη διαδικασία της ενεργοποίησης. Αυτό γιατί μια μικρού μεγέθους κακόβουλη τροποποίηση έχει περισσότερες πιθανότητες να ενεργοποιηθεί από μία που έχει μεγαλύτερο μέγεθος και άρα μεγαλύτερο αριθμό εισόδων (Shakya, 2019).

Στην κατηγορία των φυσικών τροποποιήσεων ανήκει και η κατανομή. Η διαδικασία της κατανομής περιγράφει τη θέση της κακόβουλης τροποποίησης στην φυσική διάταξη και γεωμετρία του τσιπ. Για παράδειγμα, μια συμπαγής κατανομή αναφέρεται σε μια κακόβουλη τροποποίηση υλικού, τα στοιχεία της οποίας είναι τοποθετημένα κοντά μεταξύ τους και σε σχέση με τη συνολική διάταξη του τσιπ. Αντίθετα, μια αραιή κατανομή

αναφέρεται στις τροποποιήσεις εκείνες, των οποίων τα στοιχεία είναι διασκορπισμένα σε όλη τη διάταξη του τσιπ (Salmani, 2018).

Αξίζει να αναφερθεί στο σημείο αυτό πως οι Ng et al. (2015), σημειώνουν πως η κατανομή των κακόβουλων τροποποιήσεων είναι άμεσα εξαρτώμενη από το διαθέσιμο χώρο που μπορεί να προκύψει στη διάταξη του τσιπ. Όπως είναι αναμενόμενο, όταν υπάρχουν διεσπαρμένοι μικροί διαθέσιμοι χώροι στη διάταξη, τότε αυτός που θέλει να βλάψει μια συσκευή θα πρέπει να τοποθετήσει αντίστοιχα πολλά και μικρά κομμάτια της κακόβουλης τροποποίησης σε πολλά και διαφορετικά μικρά μέρη της διάταξης, διεσπαρμένα. Επιπλέον, θεωρείται αυτονόητο ότι όλες αυτές οι παρεμβάσεις του «εισβολέα» στο τσιπ θα πρέπει να μην επηρεάζουν τη φυσική διάταξη και τη γεωμετρία του σχεδίου και του τσιπ .

Τελευταία στην κατηγορία των φυσικών χαρακτηριστικών εντάσσεται η δομή. Αυτό συμβαίνει γιατί ο εισβολέας του τσιπ όταν φτάνει στο σημείο να αναδημιουργεί τη διάταξη του τσιπ για να μπορέσει με τον τρόπο του να εισάγει την κακόβουλη τροποποίηση, ουσιαστικά επεμβαίνει άμεσα στις διαστάσεις του τσιπ, οι οποίες με τη σειρά τους αλλάζουν.

Ωστόσο, οποιαδήποτε αλλαγή που προκαλεί ο εισβολέας έχει ως αποτέλεσμα την ανακατανομή άλλων στοιχείων του τσιπ. Αντίστοιχα, αυτές οι ανακατανομές έχουν ως άμεσο αποτέλεσμα την αλλαγή στοιχείων του τσιπ όπως η καθυστέρηση και η ισχύ – αλλαγές που θα κάνουν την ανίχνευση της κακόβουλης τροποποίησης ευκολότερη στη φάση του ελέγχου.

Για να επιτευχθεί, λοιπόν, το βέλτιστο αποτέλεσμα από την πλευρά του εισβολέα, θα πρέπει να υιοθετηθεί μια στρατηγική τέτοια, που εξασφαλίζει για την κακόβουλη τροποποίηση όσο το δυνατό μικρότερο αποτύπωμα αυτής (Ng et al., 2015).

Για παράδειγμα σε μικρές και συμπαγείς διανομές το μικρότερο δυνατό αποτύπωμα μπορεί εύκολα να επιτευχθεί αφού στις περιπτώσεις αυτές η κακόβουλη τροποποίηση υλικού μπορεί απλά να εισαχθεί μέσω μιας μικρής αλλαγής στη γεωμετρία ενός καλωδίου ή ενός τρανζίστορ. Ωστόσο, για τις λειτουργικές κακόβουλες τροποποιήσεις το μέγεθος αλλά η κατανομή έχουν σημαντικό αντίκτυπο στο φυσικό αποτύπωμά τους.

Το ίδιο ισχύει και για τις διανομές με μεγάλο μέγεθος. Στις περιπτώσεις αυτές οι επιπλοκές είναι περισσότερες αφού από τη μία, η κατανομή της κακόβουλης τροποποίησης σε ολόκληρη τη διάταξη του τσιπ μπορεί να μην οδηγήσει τελικά σε μεγάλο φυσικό αποτύπωμα για την τροποποίηση, επειδή είναι πιο δύσκολη η ανίχνευσή της με βάση μια ανωμαλία σε ισχύ ή σε μια διαρροή. Από την άλλη, όμως, η κατανομή της κακόβουλης

τροποποίησης σε πολλά μέρη της διάταξης του τσιπ μπορεί στην πραγματικότητα να επιδεινώσει το φυσικό αποτύπωμα από άλλες απόψεις. Αυτό συμβαίνει αφού το μήκος των συρμάτων που συνδέουν την κακόβουλη τροποποίηση αυξάνεται σημαντικά.

Το γεγονός αυτό, αλλάζει την κατανομή της χωρητικότητας του τσιπ και αυξάνει τις πιθανότητες τελικά, η κακόβουλη τροποποίηση να επηρεάσει την καθυστέρησή του (Salmani & Tehranipoor, 2016).

Έτσι, λοιπόν, μια συμπαγής κακόβουλη τροποποίηση μπορεί να είναι πιο αποδοτική για έναν εισβολέα, ιδιαίτερα αν οι τεχνικές κάλυψης ισχύος ή και διαρροής, όπως η τροφοδοσία μέσω τρανζίστορ, χρησιμοποιούνται για τη μείωση του αποτυπώματός της.

2.3.2 Ταξινομία με βάση την ενεργοποίηση

Η ενεργοποίηση και τα χαρακτηριστικά ενεργοποίησης αναφέρονται στις μεθόδους που χρησιμοποιούνται και προκαλούν την ενεργοποίηση της κακόβουλης τροποποίησης και την εκκίνηση, ουσιαστικά, των κακόβουλων ενεργειών ως προς το χρήστη-θύμα. Ο εισβολέας ή αλλιώς όποιος τοποθέτησε την κακόβουλη τροποποίηση δε θα πρέπει να επιτρέψει στον κανονικό χρήστη να την ενεργοποιήσει εύκολα, αφού από τη μία ο εισβολέας δε θέλει η τροποποίηση να ενεργοποιηθεί τυχαία αλλά ούτε να ανιχνευθεί σε οποιαδήποτε στάδιο της φάσης ελέγχου. Άρα, η ενεργοποίηση της κακόβουλης τροποποίησης θεωρείται σπάνιο φαινόμενο από στατιστικής πλευράς. Έτσι και αλλιώς, μια φορά αρκεί να ενεργοποιηθεί για να προξενήσει το αντίστοιχο κακό στο χρήστη.

Οι Tehranipoor & Koushanfar (2010) χωρίζουν την ενεργοποίηση σε 2 κατηγορίες. Από τη μία, βρίσκεται η κατηγορία που αναφέρεται σε κακόβουλες τροποποιήσεις υλικού οι οποίες ενεργοποιούνται εξωτερικά και από την άλλη, βρίσκεται η κατηγορία που αναφέρεται σε κακόβουλες τροποποιήσεις υλικού οι οποίες ενεργοποιούνται εσωτερικά.

Στην πρώτη κατηγορία η κακόβουλη τροποποίηση μπορεί να ενεργοποιηθεί εξωτερικά από αυτόν που θέλει να βλάψει μια συσκευή, σε όποια χρονική στιγμή επιθυμεί αυτός. Η διαδικασία αυτή επιτυγχάνεται με την ενσωμάτωση κεραίας ή δέκτη στο τσιπ και έπειτα με τον αντίστοιχο έλεγχο μέσω εξωτερικών σημάτων.

Στη δεύτερη κατηγορία, αυτή των κακόβουλων τροποποιήσεων υλικού που ενεργοποιούνται εσωτερικά, συναντώνται δύο υποκατηγορίες τροποποιήσεων. Αυτές είναι όσες είναι μόνιμα ενεργοποιημένες και όσες ενεργοποιούνται υπό συνθήκες.

Οι μόνιμα ενεργοποιημένες τροποποιήσεις, όπως φαίνεται και από το όνομά τους, δείχνουν ότι η κακόβουλη τροποποίηση είναι πάντα ενεργή και μπορεί να διακόψει τη

λειτουργία του τσιπ οποιαδήποτε στιγμή. Αυτή η κατηγορία αναφέρεται στις κακόβουλες τροποποιήσεις που εφαρμόζονται μέσω αλλαγής της γεωμετρίας του τσιπ έτσι ώστε ορισμένοι κόμβοι ή διαδρομές στο τσιπ να έχουν υψηλότερη πιθανότητα να οδηγήσουν σε κάποια αποτυχία (Bhunia & Tehranipoor, 2018).

Για να ενεργοποιηθεί σε αυτές τις περιπτώσεις η κακόβουλη τροποποίηση, πρέπει ο εισβολέας να την εισάγει οπωσδήποτε σε κόμβους ή μονοπάτια που σπάνια χρησιμοποιούνται. Στην επιστημονική κοινότητα, τέτοιοι κόμβοι και διαδρομές αναφέρονται ως βλάβες που είναι δύσκολο να ανιχνευθούν, επειδή οι συνθήκες κάτω από τις οποίες γίνεται η ανίχνευση σφαλμάτων σε αυτές, είναι δύσκολο να προσδιοριστούν. Επίσης, είναι και στατιστικά σπάνιο να προκύψουν χρησιμοποιώντας τυχαία ερεθίσματα στη φάση του ελέγχου.

Συγκεκριμένα, για τις ενεργοποιημένες υπό συνθήκες κακόβουλες τροποποιήσεις ισχύει ότι αναφέρεται στις τροποποιήσεις αυτές που είναι ανενεργές έως ότου ισχύσει συγκεκριμένη συνθήκη. Η ενεργοποίηση μπορεί να βασιστεί στην έξοδο ενός αισθητήρα που παρακολουθεί τη θερμοκρασία, την τάση κλπ. Επίσης μπορεί να βασίζεται σε μια εσωτερική λογική κατάσταση, ένα συγκεκριμένο μοτίβο εισόδου ή μια τιμή εσωτερικού μετρητή. Η κακόβουλη τροποποίηση σε αυτές τις περιπτώσεις, υλοποιείται με την προσθήκη λογικών πυλών στο τσιπ και ως εκ τούτου εντοπίζεται υπό τη μορφή κυκλώματος (Bhunia & Tehranipoor, 2018).

Μια διαφορά ανάμεσα στις μόνιμα ενεργοποιημένες κακόβουλες τροποποιήσεις υλικού και σε αυτές που ενεργοποιούνται υπό συνθήκες, είναι πως στην περίπτωση των μόνιμα ενεργοποιημένων είναι δύσκολο να ανιχνευθούν ενώ για την περίπτωση αυτών που ενεργοποιούνται υπό συνθήκες η ανίχνευση είναι δυνατή ακόμα και όταν είναι ανενεργές.

Η διαφορά βασίζεται στο ότι στις μόνιμα ενεργοποιημένες κακόβουλες τροποποιήσεις εφαρμόζονται μικρές αλλαγές στην ήδη υπάρχουσα κατανομή συρμάτων και τρανζίστορ, γεγονός που τελικά οδηγεί στο ότι το τσιπ θα συμπεριφερθεί όπως θα συμπεριφέρονταν και χωρίς την κακόβουλη τροποποίηση. Φυσικά, προϋπόθεση είναι ότι οι κόμβοι ή τα μονοπάτια που αλλοιώνονται από την κακόβουλη τροποποίηση δεν χρησιμοποιούνται στη φάση ελέγχου και ως αποτέλεσμα η κακόβουλη τροποποίηση παραμένει ανενεργή (Bhunia & Tehranipoor, 2018).

Αντίθετα, μια κακόβουλη τροποποίηση που θεωρείται ενεργοποιημένη υπό συνθήκες, χρειάζεται αισθητήρες ή λογικά στοιχεία (π.χ. πύλες) για να ελέγχει τις συνθήκες ενεργοποίησης που έχουν οριστεί. Αποτέλεσμα αυτού, είναι η τροποποίηση να καταναλώνει

ισχύ ή ακόμα και να προσθέτει φόρτο στα καλώδια του αρχικού κυκλώματος, πράγμα που με τη σειρά του αλλάζει την καθυστέρηση του τσιπ.

Αυτές οι μικρές αλλαγές στα χαρακτηριστικά του τσιπ συμβαίνουν ακόμα και όταν η κακόβουλη τροποποίηση παραμένει ανενεργή. Αυτό σημαίνει ότι η ανίχνευση μιας τροποποίησης που είναι μόνιμα ενεργοποιημένη θα επιτευχθεί μόνο με την πλήρη ενεργοποίησή της, ενώ ανίχνευση μιας κακόβουλης τροποποίησης υλικού που ενεργοποιείται υπό συνθήκες μπορεί να επιτευχθεί χωρίς να ενεργοποιηθεί πλήρως (Wang, Tehranipoor & Plusquellic, 2008).

2.3.3 Ταξινομία με βάση τα χαρακτηριστικά δράσης

Τα χαρακτηριστικά δράσης αναφέρονται στις κακόβουλες πράξεις που μια τροποποίηση εκτελεί όταν προσβάλλει ένα σύστημα. Οι δράσεις χωρίζονται σε τρεις υποκατηγορίες. Πρώτη είναι αυτή της τροποποίησης λειτουργίας, δεύτερη αυτή της τροποποίησης προδιαγραφών και τρίτη αυτή της μετάδοσης πληροφοριών.

Ο πρώτος τύπος δράσης αναφέρεται σε κακόβουλες τροποποιήσεις που αλλάζουν τη λειτουργία των τσιπ είτε τροποποιώντας τον κώδικα λογικής HDL ή αφαιρώντας τον ή παρακάμπτοντας την υπάρχουσα λογική που έχει δημιουργηθεί από τον νόμιμο κατασκευαστή (Kutzner, Poschmann & Stöttinger, 2013).

Ο δεύτερος τύπος δράσης αναφέρεται σε κακόβουλες τροποποιήσεις που εστιάζουν την επίθεσή τους στην αλλαγή των παραμετρικών ιδιοτήτων του τσιπ. Για παράδειγμα ένας τέτοιος τύπος δράσης μπορεί να επέμβει στις προδιαγραφές του τσιπ και να αλλάξει τα στοιχεία που συνδέονται με την καθυστέρησή του. Αυτός ο τύπος δράσης αναφέρεται σε κακόβουλες τροποποιήσεις που επεμβαίνουν στη φυσική παρουσία των καλωδίων και των τρανζίστορ.

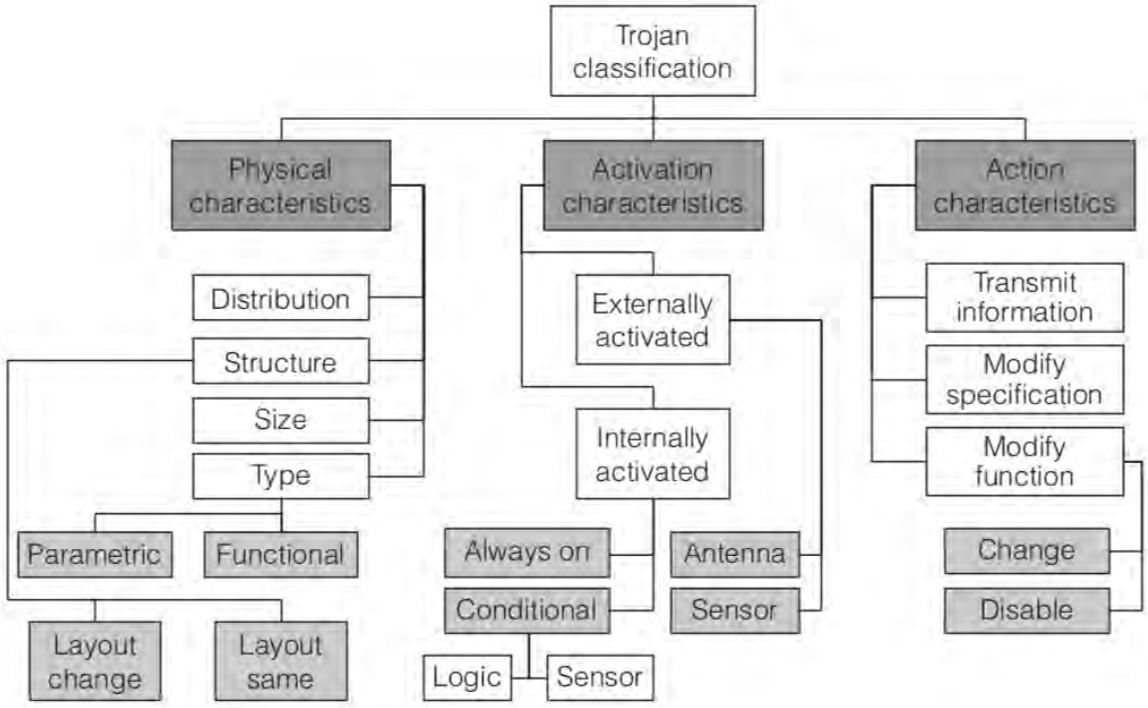
Ο τρίτος τύπος δράσης αναφέρεται σε κακόβουλες τροποποιήσεις που μεταδίδουν βασικές πληροφορίες εσωτερικά του τσιπ προς αυτόν που θέλει να το βλάψει, τον εισβολέα (Kutzner, Poschmann & Stöttinger, 2013).

Ένα χαρακτηριστικό που διαφέρει σημαντικά μεταξύ των τύπων τροποποίησης λειτουργίας και τροποποίησης προδιαγραφών αφορά τις δυνατότητές τους. Από τη μία, η φύση των πρώτων κακόβουλων τροποποιήσεων περιορίζει τις καταστροφικές τους ικανότητες σε δράσεις που οδηγούν στην αποτυχία του συστήματος. Αυτό ισχύει, επειδή στους τύπους τροποποίησης λειτουργίας οι κακόβουλες τροποποιήσεις εφαρμόζονται ως

αλλαγές στα υπάρχοντα καλώδια και τα τρανζίστορ. Επομένως, δεν υποστηρίζονται νέες δυνατότητες.

Αντίθετα, οι τύποι τροποποίησης λειτουργίας έχουν απεριόριστες δυνατότητες ουσιαστικά. Αυτό συμβαίνει γιατί οι τύποι τροποποίησης λειτουργίας, αφού ενεργοποιηθούν, μπορούν να αλλάξουν οποιοδήποτε χαρακτηριστικό του τσιπ ή να εισαγάγουν νέες λειτουργίες (Tehranipoor & Sunar, 2010).

Για να γίνει σχηματικά η αναπαράσταση της ταξινομίας που πρότειναν οι Wang et al. (2008) ακολουθεί η επόμενη εικόνα, που παρουσιάζει οπτικά όλη την ταξινομία.



Εικόνα 2: Ταξινομία κακόβουλων τροποποιήσεων υλικού κατά τους Wang et al. (2008)

ΚΕΦΑΛΑΙΟ 3

ΑΝΙΧΝΕΥΣΗ ΚΑΚΟΒΟΥΛΩΝ ΤΡΟΠΟΠΟΙΗΣΕΩΝ ΥΛΙΚΟΥ

Η συνεχής εξέλιξη στις τεχνολογίες των κυκλωμάτων απαιτεί δαπανηρές αναβαθμίσεις των τεχνολογιών και διαδικασιών παραγωγής. Λόγω αυτού του υψηλού κόστους, στις εταιρίες που παρέχουν επεξεργαστές σήμερα, οι σχεδιαστές κυκλωμάτων και τα χυτήρια είναι ξεχωριστές εταιρείες που βρίσκονται συχνά σε διαφορετικά μέρη του κόσμου. Μία, λοιπόν, από τις πιθανές απειλές αυτού του επιχειρησιακού μοντέλου είναι και η τοποθέτηση κακόβουλων τροποποιήσεων υλικού στα κυκλώματα προς κατασκευή και κατ' επέκταση στα τσιπ και τους επεξεργαστές.

Μια κακόβουλη τροποποίηση υλικού μπορεί να εισαχθεί στο κύκλωμα για να επιτρέψει σε αυτόν που θέλει να το βλάψει να παρακολουθεί, να ελέγχει ή να κλέβει πληροφορίες από το τσιπ. Μάλιστα μπορεί μέχρι και να ενεργοποιήσει ή να απενεργοποιήσει εξ ολοκλήρου όλα ή τμήματα του τσιπ (Zhao et al., 2019).

Η εδραίωση της εμπιστοσύνης των κυκλωμάτων εν όψει μη αξιόπιστων κατασκευών είναι ένα δύσκολο και σημαντικό πρόβλημα, ιδίως επειδή τα κυκλώματα πλέον είναι οι πυλώνες των επιχειρήσεων, των κυβερνήσεων και της άμυνας στα νέα δεδομένα της σύγχρονης εποχής.

Η ανίχνευση κακόβουλων τροποποιήσεων υλικού είναι μια πολύπλοκη και δύσκολη διαδικασία. Λαμβάνοντας υπόψη το γεγονός πως ο αριθμός των πυλών στα κυκλώματα αυξάνεται σημαντικά, η ανίχνευση γίνεται ακόμα πιο μεγάλη πρόκληση. Έτσι, υπάρχει περιορισμένη δυνατότητα ελέγχου και μιας καλής οπτικής στα ολοένα και πιο σύνθετα εσωτερικά μέρη των κυκλωμάτων (Jyothi & Rajendran, 2018).

Επιπλέον, υπάρχουν πολλές ευκαιρίες για εισαγωγή κακόβουλων τροποποιήσεων υλικού στα διάφορα στάδια κατασκευής. Δεδομένου ότι τα χυτήρια είναι εξοπλισμένα με προηγμένες τεχνολογίες, διαδικασίες και υπερσύγχρονες εγκαταστάσεις, είναι σε θέση να σχεδιάζουν και να κρύβουν στρατηγικά τις όποιες κακόβουλες τροποποιήσεις λογισμικού.

Σα να μη φτάνει αυτό, οι διακυμάνσεις των διεργασιών στα τσιπ και το εύρος αυτών συνεχώς αυξάνεται και το γεγονός αυτό από μόνο του εισάγει μια αβεβαιότητα στα χαρακτηριστικά που μπορούν να μετρηθούν και να ελεγχθούν, περιπλέκοντας περαιτέρω τη διαδικασία ανίχνευσης κακόβουλων τροποποιήσεων (Alkabani & Koushanfar, 2009).

Έτσι, η ανίχνευση κακόβουλων τροποποιήσεων υλικού έχει απασχολήσει ιδιαίτερα την επιστημονική κοινότητα τελευταία. Για την αντιμετώπιση του φαινομένου, του οποίου οι διαστάσεις μεγεθύνονται, έχουν αναπτυχθεί αρκετές μεθοδολογίες ανίχνευσης κακόβουλων τροποποιήσεων τα τελευταία χρόνια. Οι Tehranipoor & Koushanfar (2010) αναφέρουν πως οι μεθοδολογίες ανίχνευσης κακόβουλων τροποποιήσεων μπορούν να χωριστούν σε δύο βασικές κατηγορίες. Η πρώτη ονομάζεται ανάλυση πλευρικών καναλιών (side-channel analysis) και η δεύτερη ενεργοποίηση κακόβουλων τροποποιήσεων υλικού (Trojan activation). Τόσο η μία όσο και η άλλη κατηγορία, αφορούν προσεγγίσεις στην αντιμετώπιση του φαινομένου, με εστίαση σε δράσεις στο επίπεδο του τσιπ και στο αρχιτεκτονικό επίπεδο της κακόβουλης τροποποίησης.

Η πρώτη κατηγορία ανίχνευσης κακόβουλων τροποποιήσεων υλικού που αναπτύσσεται στα πλαίσια της εργασίας είναι αυτή της ανάλυσης πλευρικών καναλιών. Τα σήματα πλευρικών καναλιών, όπως αυτά π.χ. που αναφέρονται στο συγχρονισμό και την ισχύ, μπορούν να χρησιμοποιηθούν για την ανίχνευση κακόβουλων τροποποιήσεων υλικού. Η κατηγορία αυτή και κατ' επέκταση μια ενδεχόμενη ανίχνευση κακόβουλης τροποποίησης υλικού, βασίζεται στο γεγονός πως οι κακόβουλες τροποποιήσεις υλικού πολλές φορές αλλάζουν κάποια παραμετρικά χαρακτηριστικά του τσιπ. Οι αλλαγές, ή ακόμα και οι τροποποιήσεις αφορούν, για παράδειγμα, ενέργειες που έχουν ως σκοπό την υποβάθμιση του τσιπ, την αλλαγή της ισχύος του αλλά και πρόκληση ζητημάτων αξιοπιστίας σε αυτό. Οι αλλαγές, ωστόσο, που εκτελούνται στο τσιπ επηρεάζουν άμεσα τα χαρακτηριστικά του, όπως η ισχύς και η καθυστέρηση των καλωδίων και των λογικών πυλών του κυκλώματος.

Τα σήματα πλευρικών καναλιών που βασίζονται στην ισχύ, παρέχουν στον ενδιαφερόμενο μια πλήρη εικόνα για την εσωτερική δομή του κυκλώματος και των δραστηριοτήτων που λαμβάνουν χώρα εντός αυτού. Έτσι, επιτρέπεται η ανίχνευση των κακόβουλων τροποποιήσεων υλικού χωρίς την πλήρη ενεργοποίησή τους (Nagata, Danger & Miura, 2018).

Τα σήματα πλευρικών καναλιών που βασίζονται στο χρόνο, μπορούν να ανιχνεύσουν την παρουσία μια κακόβουλης τροποποίησης υλικού αν το τσιπ έχει δοκιμαστεί χρησιμοποιώντας ελέγχους οι οποίοι είναι ευαίσθητοι σε μικρές αλλαγές της καθυστέρησης του τσιπ και συγκεκριμένα στις διαδρομές αυτές που έχουν επηρεαστεί από την κακόβουλη τροποποίηση. Επίσης, οι εν λόγω έλεγχοι θα πρέπει επίσης να είναι σε θέση να ξεχωρίσουν αποτελεσματικά τις κακόβουλες τροποποιήσεις από πιθανές δυσλειτουργίες του κυκλώματος.

Επιπλέον, οι Tehranipoor et al. (2010) αναφέρουν πως οι τεχνικές ανίχνευσης βασίζονται στην ισχύ, το χρόνο και την ενεργοποίηση, οπότε εδώ εντοπίζονται τρεις κατηγορίες.

Στην πρώτη κατηγορία οι προσεγγίσεις ανίχνευσης εκμεταλλεύονται την ισχύ στα κυκλώματα και τη χρησιμοποιούν για την ανίχνευση των κακόβουλων τροποποιήσεων υλικού. Οι περισσότερες κακόβουλες τροποποιήσεις υλικού πρέπει να συνδεθούν με την τροφοδοσία του κυκλώματος για να λειτουργήσουν, και οποιαδήποτε δραστηριότητα σε μια κακόβουλη τροποποίηση υλικού θα αντλήσει ρεύμα από το δίκτυο διανομής ενέργειας, μια δραστηριότητα όπου μπορεί να μετρηθεί εξωτερικά. Τέτοιες δραστηριότητες, ωστόσο, καλύπτονται πολλές φορές από τις άλλες δραστηριότητες των διεργασιών του κυκλώματος.

Για την ανίχνευση κακόβουλων τροποποιήσεων υλικού χρησιμοποιώντας ανάλυση σήματος βασισμένη στην ισχύ, οι κατασκευαστές εντοπίζουν πρώτα ένα πρωτότυπο κύκλωμα χωρίς κάποια κακόβουλη τροποποίηση υλικού με τη διεξαγωγή μιας σειράς δοκιμών σε μεγάλο αριθμό κυκλωμάτων. Η υπογραφή ισχύος του πρωτότυπου κυκλώματος αποκτάται με την εφαρμογή τυχαίων ελέγχων. Η ισχύς που μετράται τελικά περιλαμβάνει: α) την ισχύ που καταναλώνεται από το κύκλωμα, β) το θόρυβο, που μπορεί να αφαιρεθεί με επαναλαμβανόμενες μετρήσεις. και γ) τυχαίες παραλλαγές της διαδικασίας, οι οποίες δεν μπορούν να αφαιρέσουν. Οποιαδήποτε πρόσθετη ενέργεια θεωρείται ότι προέρχεται από μια κακόβουλη τροποποίηση υλικού (Tehranipoor et al., 2010).

Μετά την απόκτηση της υπογραφής του πρωτότυπου κυκλώματος, οι μηχανικοί που ελέγχουν το κύκλωμα εφαρμόζουν τα ίδια μοτίβα ελέγχου στο κύκλωμα υπό έλεγχο. Εάν η υπογραφή ισχύος του κυκλώματος υπό έλεγχο είναι διαφορετική από την υπογραφή του πρωτότυπου κυκλώματος, τότε οι ερευνητές θέτουν το κύκλωμα υπό έλεγχο ως πιθανό να φέρει κάποια κακόβουλη τροποποίηση υλικού.

Ωστόσο, η ανάλυση σήματος βασισμένη σε ισχύ παρουσιάζει δύο μεγάλες προκλήσεις. Πρώτον, εξαιτίας των μεταβολών της διαδικασίας στις παραμέτρους του κυκλώματος, δεν μπορούν να υπάρξουν δύο ίδια κυκλώματα, έτσι η ισχύς που μετράται για το ίδιο σύνολο ελέγχων θα είναι διαφορετική. Δεύτερον, τα τυχαία πρότυπα ελέγχων δεν εγγυώνται ότι θα δημιουργήσουν δραστηριότητα σε κακόβουλες τροποποιήσεις υλικού. Όπως έχει αναφερθεί νωρίτερα στην εργασία, μια κακόβουλη τροποποίηση υλικού μπορεί να αποδειχθεί ανθεκτική σε τέτοια μοτίβα και τελικά να καμουφλάρεται (Nowroz, Hu, Koushanfar & Reda, 2014).

Στη δεύτερη κατηγορία, αυτή των αναλύσεων βασισμένων στο χρόνο, συναντώνται οι προσεγγίσεις που βασίζονται στην επιρροή των κακόβουλων τροποποιήσεων υλικού στα χαρακτηριστικά χρονισμού ενός κυκλώματος. Η επιρροή βασίζεται στο ότι μια κακόβουλη

τροποποίηση υλικού προσθέτει πρόσθετο φόρτο στις διαδρομές ενός κυκλώματος, άρα επηρεάζει τα χαρακτηριστικά χρονισμού του.

Ακόμα κι αν η επιρροή είναι μικρή, οι εξελιγμένες μέθοδοι ελέγχου της καθυστέρησης θα μπορούσαν να την καταγράψουν, ειδικά εάν η κακόβουλη τροποποίηση υλικού επηρεάζει την καθυστέρηση των βασικών διαδρομών (Bhunia, Hsiao, Banga & Narasimhan, 2014).

Η ανίχνευση κακόβουλων τροποποιήσεων υλικού με βάση την ανάλυση σήματος βασισμένη στο χρόνο παρουσιάζει επίσης διάφορες προκλήσεις. Πρώτον, η διαφοροποίηση των κακόβουλων τροποποιήσεων υλικού από τις παραλλαγές της διαδικασίας είναι δύσκολη, διότι και οι δύο μπορούν να επηρεάσουν την καθυστέρηση του κυκλώματος.

Δεύτερον, είναι εξαιρετικά δύσκολο να εντοπιστεί μια κακόβουλη τροποποίηση υλικού που έχει εισαχθεί σε μικρές διαδρομές στο κύκλωμα, καθώς απαιτούνται σήματα υψηλής συχνότητας για να δοκιμαστούν αυτές οι διαδρομές. Τα μοτίβα ελέγχων που εφαρμόζονται σε υψηλότερη από τη λειτουργική συχνότητα επηρεάζονται από τους θορύβους του κυκλώματος (όπως θόρυβος τροφοδοσίας), καθιστώντας την ανίχνευση ανακριβή.

Τρίτον, οι μέθοδοι ανάλυσης και ανίχνευσης που βασίζονται στο χρόνο, προϋποθέτουν την ύπαρξη ενός πρωτότυπου κυκλώματος. Αυτή η υπόθεση δεν είναι έγκυρη αν υποθέσει κάποιος πως οι κακόβουλες τροποποιήσεις υλικού εισάγονται σε όλα τα κυκλώματα – και γιατί όχι – ακόμα και στα πρωτότυπα (Wei, Li, Koushanfar & Potkonjak, 2012).

Τέλος, η τρίτη κατηγορία είναι αυτή των αναλύσεων με βάση την ενεργοποίηση των κακόβουλων τροποποιήσεων υλικού. Οι αναλύσεις με βάση την ενεργοποίηση της κακόβουλης τροποποίησης υλικού μπορούν να επιταχύνουν τη διαδικασία ανίχνευσης της τροποποίησης και σε μερικές περιπτώσεις έχουν συνδυαστεί με την ανάλυση βασισμένη στην ισχύ. Εάν ένα τμήμα της κακόβουλης τροποποίησης υλικού είναι ενεργοποιημένο, θα καταναλώσει περισσότερη ισχύ και έτσι θα διευκολύνει τη διαφοροποίηση της υπογραφής ενός κυκλώματος με κακόβουλη τροποποίηση υλικού από ένα χωρίς τροποποίηση.

Οι προσεγγίσεις που βασίζονται στην ενεργοποίηση της κακόβουλης τροποποίησης υλικού μπορούν να χωριστούν σε αυτές που σχετίζονται με την περιοχή που εισάγεται η τροποποίηση και σε αυτές που δεν σχετίζονται. Στις περιπτώσεις που οι αναλύσεις δε σχετίζονται με την περιοχή που έχει εισαχθεί η κακόβουλη τροποποίηση υλικού εφαρμόζονται τυχαίοι έλεγχοι.

Αντίθετα, στις προσεγγίσεις που σχετίζονται με την περιοχή που έχει εισαχθεί η κακόβουλη τροποποίηση υλικού, συγκρίνεται η διαφορά ανάμεσα στην ισχύ του κυκλώματος υπό έλεγχο και την ισχύ του πρωτότυπου κυκλώματος. Έτσι, εντοπίζονται οι

περιοχές που η διαφορά στην ισχύ ανάμεσα στα δύο κυκλώματα είναι σημαντική και κατ' επέκταση εντοπίζονται οι περιοχές που υπάρχει μεγαλύτερη πιθανότητα να έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού (Bhunia et al., 2013).

3.1 Ανάλυση βασισμένη στην ισχύ

Οι Agrawal et al. (2007) ήταν οι πρώτοι που ανέπτυξαν τεχνικές ανίχνευσης κακόβουλων τροποποιήσεων υλικού χρησιμοποιώντας την ανάλυση πλευρικών καναλιών. Οι συγκεκριμένοι χρησιμοποιούσαν τις πληροφορίες των πλευρικών καναλιών για να ανιχνεύσουν πιθανές επιρροές κακόβουλων τροποποιήσεων υλικού στην κατανάλωση ισχύος του κυκλώματος. Κατά τη διαδικασία ανίχνευσης και για να οδηγηθεί τελικά ο έλεγχος σε ένα καθαρό κύκλωμα ή όχι, γίνονταν τυχαίοι δειγματοληπτικοί έλεγχοι σε όλο το κύκλωμα, οι οποίοι μετρούσαν την ισχύ συγκεκριμένων μονοπατιών. Τα δεδομένα που συλλέγονταν σε κάθε μέτρηση ισχύος περιέχουν διάφορα στοιχεία.

Ένα στοιχείο ανάλυσης είναι της κατανάλωσης ισχύος του κυκλώματος, μετά την εφαρμογή εισόδων οι οποίες είναι ίδιες σε όλα τα κανονικά κυκλώματα χωρίς να έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Ένα ακόμα στοιχείο ανάλυσης είναι η μέτρηση του θορύβου αλλά μπορεί και να αφαιρεθεί από κάποιες μετρήσεις. Επόμενο στοιχείο είναι ίδιες οι μετρήσεις οι οποίες μπορεί να χαρακτηρίζονται από πολλές παραλλαγές που βασίζονται στην τυχαιότητα και δεν είναι δυνατή η αφαίρεσή τους. Τελευταίο στοιχείο είναι η μέτρηση της κατανάλωσης της ενέργειας που προέρχεται από κάποια ενδεχόμενη κακόβουλη τροποποίηση υλικού. Όταν τελειώσουν οι τυχαίοι έλεγχοι υπάρχει και η πιθανότητα κάποια κυκλώματα να είναι αντίστροφα σχεδιασμένα (reverse engineered) για να εξασφαλίσουν πως δεν έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού.

Από τους ελέγχους των Agrawal et al. (2007) τελικά προκύπτει μια πρώτη υπογραφή και χρησιμοποιείται ως αναφορά στους επόμενους ελέγχους. Μετά, λοιπόν, το πέρας των ελέγχων και την πρώτη υπογραφή οι ίδιοι έλεγχοι εκτελούνται και στο αντίστοιχο κύκλωμα προς ταυτοποίηση. Αν το κύκλωμα προς ταυτοποίηση οδηγηθεί σε διαφορετική υπογραφή από αυτή που παράχθηκε πρώτα τότε το κύκλωμα θεωρείται ύποπτο και υπάρχει μεγάλη πιθανότητα να περιέχει μια κακόβουλη τροποποίηση υλικού.

Μέσω των ελέγχων αυτών μπορούν να ανιχνευθούν πολλά και διαφορετικά μεγέθη κακόβουλων τροποποιήσεων υλικού αφού οι έλεγχοι που εκτελούνται είναι τυχαίοι και οι διαδικασίες που εφαρμόζονται χαρακτηρίζονται από μεγάλη ποικιλία. Αν, για παράδειγμα,

τα μεγέθη της κακόβουλης τροποποίησης και του κυκλώματος στο οποίο έχει εισαχθεί είναι συγκρίσιμα, τότε μπορεί εύκολα η κακόβουλη τροποποίηση να ανιχνευθεί αφού αυτή θα έχει φανερή επίπτωση στην ισχύ του κυκλώματος.

Από την άλλη, όμως, αν το μέγεθος της κακόβουλης τροποποίησης είναι μικρό, υπάρχει περίπτωση οι διαδικασίες που είναι ποικίλες να καλύψουν την επίπτωση της κακόβουλης τροποποίησης και τελικά να μην ανιχνευθεί.

Οι Wang et al. (2008) αναφέρουν επί αυτού ότι σε κάθε περίπτωση οι κακόβουλες τροποποιήσεις υλικού που εισάγονται στα τσιπ και τα κυκλώματα απαιτούν τροφοδοσία ρεύματος για να λειτουργήσουν. Παρόλα αυτά, είναι γεγονός πως οι κακόβουλες τροποποιήσεις υλικού μπορούν να είναι διαφορετικών τύπων και μεγεθών και η επίδρασή τους στα χαρακτηριστικά ισχύος κυκλώματος μπορεί να είναι πολύ μεγάλη ή πολύ μικρή.

Στη προσέγγισή τους, οι συγγραφείς προτείνουν τη μέτρηση της ισχύος από διάφορες θύρες ισχύος ή ελεγχόμενες συνδέσεις και την εφαρμογή τυχαίων ελέγχων για να αυξήσουν τις διεργασίες στο κύκλωμα. Η ποσότητα ρεύματος που μπορεί να τραβήξει μια κακόβουλη τροποποίηση υλικού μπορεί να είναι τόσο μικρή ώστε να μπορεί να ανιχνευθεί από κάποιο συμβατικό εξοπλισμό μέτρησης. Ωστόσο, η δυνατότητα ανίχνευσης κακόβουλων τροποποιήσεων υλικού μπορεί να ενισχυθεί σημαντικά με τη μέτρηση της ισχύος τοπικά και από πολλαπλές θύρες ή ελεγχόμενες συνδέσεις. Αν προκύψουν ίδια αποτελέσματα σε όλες τις μετρήσεις που θα γίνουν σε όλες τις θύρες ισχύος ή τις ελεγχόμενες συνδέσεις τότε μπορεί να ειπωθεί το συμπέρασμα πως η περιοχή υπό έλεγχο είναι ελεύθερη από κάποια κακόβουλη τροποποίηση υλικού.

Μια εναλλακτική προσέγγιση στην κατηγορία της ανάλυσης με βάση την ισχύ παρουσίασαν στο έργο τους οι Rad, Wang, Tehranipoor & Plusquellic (2008). Η πρόταση περιλαμβάνει μια μέθοδο ανάλυσης της ισχύος η οποία βασίζεται σε συγκεκριμένες περιοχές του κυκλώματος. Στις περιοχές αυτές εφαρμόζεται μεγάλη ισχύ από μια θύρα ισχύος. Η διαδικασία γίνεται σε πολλές περιοχές παράλληλα και πραγματοποιούνται μεμονωμένες μετρήσεις σε κάθε θύρα ισχύος και με βάση τυχαίους αλλά προκαθορισμένους συνδυασμούς.

Στις μετρήσεις που εκτελούνται, εκτελείται παράλληλα και ένας αλγόριθμος ανίχνευσης της ισχύος, ο οποίος βασίζεται στη στατιστική ανάλυση των κυματομορφών που παράγονται στις θύρες ισχύος κατά τη διάρκεια της όλης διαδικασίας. Στη συνέχεια, οι μετρήσεις διαμορφώνουν ένα διάγραμμα σκέδασης μέσω του οποίου η κάθε μέτρηση αντιστοιχείται σε φυσιολογική ή και σε κάποια που προέρχεται από κάποια κακόβουλη τροποποίηση υλικού. Ο διαχωρισμός των μετρήσεων, γίνεται από πολλά μοντέλα που

διακρίνουν μετρήσεις ισχύος και προέρχονται από κυκλώματα που δεν έχουν υποστεί κακόβουλες τροποποιήσεις υλικού.

Παρόλα αυτά, η ανάλυση που βασίζεται στις συγκεκριμένες περιοχές, δεν είναι επαρκής για να ανιχνευθούν όλες οι πιθανές παραλλαγές των μετρήσεων της ισχύος και για το λόγο αυτό εφαρμόζεται μια διαδικασία βαθμονόμησης (calibration) των σημάτων. Η βαθμονόμηση των σημάτων σχετίζεται με την εξάλειψη των μεταβολών στα σήματα και τις μετρήσεις, ούτως ώστε η προσέγγιση των συγγραφέων, η οποία βασίζεται στην ανάλυση ισχύος συγκεκριμένων περιοχών, να αξιοποιηθεί πλήρως (Rad et al., 2008).

Η βαθμονόμηση λαμβάνει χώρα σε κάθε θύρα ισχύος και για κάθε τσιπ ξεχωριστά και μετρά την απόκριση κάθε θύρας ισχύος σε ένα παλμό. Η απόκριση κάθε θύρας ισχύος κανονικοποιείται από το άθροισμα του ρεύματος που αντλείται από τις θύρες ισχύος στην ίδια σειρά με τη θύρα αυτή. Έτσι, προκύπτει ένας πίνακας με τις κανονικοποιημένες τιμές όλων των θυρών ισχύος. Έπειτα, λοιπόν, αφού εφαρμοστεί η τεχνική της εφαρμογής μεγάλης ισχύς σε κάθε θύρα ισχύος, βαθμονομούνται όλες οι αποκρίσεις μέσω του πίνακα που παράχθηκε.

Η διαδικασία της βαθμονόμησης, έτσι, σύμφωνα με τους Rad et al., (2008) οδηγεί στον περαιτέρω διαχωρισμό των μετρήσεων ισχύος ανάμεσα σε κυκλώματα που δεν έχουν υποστεί κακόβουλη τροποποίηση και σε κυκλώματα που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Αυτό δηλαδή σημαίνει ότι αν στο διάγραμμα διασποράς οι μετρήσεις είχαν μια απόσταση α, έπειτα από τη βαθμονόμηση αποκτούν μια απόσταση β, μεγαλύτερη από την α, άρα διαχωρίζονται ευκολότερα.

Οι Alkabani & Koshanfar (2008) πρότειναν προσεγγίσεις πάνω στο συγχρονισμό και το χαρακτηρισμό της ισχύος μέσω μετρήσεων χωρίς απώλειες σε επίπεδο πύλης. Κάθε μέτρηση αντιστοιχείται σε μία εξίσωση. Αφού δημιουργηθεί ένας γραμμικός αριθμός μετρήσεων, σχηματίζεται ένα σύστημα εξισώσεων για τη χαρτογράφηση των χαρακτηριστικών που μετρούνται στο επίπεδο πύλης πάντα.

Οι συγγραφείς χρησιμοποίησαν μεθόδους στατιστικής σύγκλισης στο επίπεδο της πύλης για να μετρήσουν την ακεραιότητα του σήματος και τελικά να εντοπίσουν την όποια ενδεχόμενη κακόβουλη τροποποίηση υλικού. Στο έργο και τα πειράματα, διαπίστωσαν αποδοτικές και αξιόπιστες προσεγγίσεις για τις καταναλώσεις ισχύος σε επίπεδο πύλης και εντοπίστηκαν κακόβουλες παρεμβολές με τη χρήση πολλαπλών ελέγχων συνέπειας.

Οι Potkonjak et al (2009) χρησιμοποίησαν την παραπάνω προσέγγιση για την ανίχνευση κακόβουλων τροποποιήσεων υλικού. Οι ερευνητές συνδυάζουν μετρήσεις τόσο συγχρονισμού όσο και στατικής ισχύος σε επίπεδο πύλης και η ανίχνευση οποιασδήποτε

κακόβουλης τροποποίησης επιτυγχάνεται μέσω του χειρισμού των εξισώσεων. Αυτή η μέθοδος συγκρίνει όλες τις μετρήσεις και ανιχνεύει τις πύλες που έχουν διαφορετικά χαρακτηριστικά, σε σχέση με αυτά που κανονικά έχουν προκαθοριστεί να έχουν.

Για την εκτίμηση των ορίων των φυσιολογικών τιμών στις οποίες πρέπει να κινούνται οι μετρήσεις χρησιμοποιούνται τεχνικές στατιστικής επικύρωσης με βάση πραγματικά δεδομένα από τους κατασκευαστές. Η μέθοδος των ερευνητών είναι σε θέση να ξεχωρίσει τις μετρήσεις και να εντοπίσει «λάθη» που προκαλούνται από μη επεμβατικές ενέργειες αλλά όχι σε μεταβολές που μπορούν να προκύψουν από την εκτέλεση της μεθόδου.

Τα αποτελέσματα τελικά, της μεθόδου, είναι ελπιδοφόρα επειδή η χαρτογράφηση σε επίπεδο πύλης μπορεί να επιτευχθεί και μάλιστα με μεγάλη ακρίβεια. Οι μέθοδοι που χρησιμοποιούνται σε επίπεδο πύλης μπορούν να εντοπίσουν αποτελεσματικά τα χαρακτηριστικά των πυλών που ελέγχουν και η απόδοσή τους στη μέτρηση της στατικής ισχύος θεωρείται υψηλή.

Μια επιπλέον προσέγγιση δημοσίευσαν στο έργο τους οι Narasimhan et al. (2012). Εκεί προτείνεται μια νέα μη επεμβατική προσέγγιση που ανιχνεύει τις κακόβουλες τροποποιήσεις υλικού μέσω ανάλυσης πλευρικών καναλιών πολλαπλών παραμέτρων. Χρησιμοποιείται η εγγενής σχέση μεταξύ δυναμικού ρεύματος και μέγιστης συχνότητας λειτουργίας ενός κυκλώματος για να απομονωθεί αντίστοιχα η επίδραση ενός κυκλώματος που έχει υποστεί κακόβουλη τροποποίηση υλικού από τον θόρυβο της διαδικασίας. Επίσης, προτείνεται μια προσέγγιση δημιουργίας ελέγχων και πολλών τεχνικών ελέγχου για να βελτιωθεί η ευαισθησία ανίχνευσης των κακόβουλων τροποποιήσεων υλικού.

Για να χρησιμοποιηθεί η ανάλυση πλευρικών καναλιών στην ανίχνευση των κακόβουλων τροποποιήσεων υλικού, πρέπει να γίνει διάκριση της συμβολής της κακόβουλης τροποποίησης υλικού από θόρυβο των διεργασιών ανάμεσα στα κυκλώματα που είναι ανέγγιχτα και σε αυτά που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Κάτι τέτοιο επιτυγχάνεται από τη σύγκριση των πληροφοριών των πλευρικών καναλιών ανάμεσα στους δύο τύπους αυτούς των κυκλωμάτων.

Ωστόσο, η επίδραση ενός κυκλώματος που έχει υποστεί κακόβουλη τροποποίηση υλικού στη μέγιστη συχνότητα λειτουργίας αλλά και στο παροδικό ρεύμα τροφοδοσίας του τσιπ μπορεί να καλυφθεί. Γι’ αυτό και η επίδραση μιας συνδυαστικής τροποποίησης υλικού παρατηρείται μόνο στην ισχύ. Η επίδραση αυτή δεν επηρεάζει την μέγιστη συχνότητα λειτουργίας του τσιπ αφού η κακόβουλη τροποποίηση δεν συνηθίζεται να τοποθετείται στην κρίσιμη διαδρομή του κυκλώματος. Το πρόβλημα γίνεται ακόμα πιο έντονο όταν το μέγεθος των κακόβουλων τροποποιήσεων μικραίνει (Narasimhan et al., 2012).

Για να ξεπεραστεί αυτό το ζήτημα, η σχέση μεταξύ παροδικού ρεύματος τροφοδοσίας και μέγιστης συχνότητας λειτουργίας μπορεί να χρησιμοποιηθεί για να γίνει διάκριση μεταξύ των αρχικών και των παραποιημένων εκδόσεων των κυκλωμάτων. Αν βέβαια, ληφθεί υπόψη μόνο μια παράμετρος στην ανάλυση πλευρικών καναλιών δεν θα είναι δυνατή η διάκριση. Αυτό γιατί δύο τσιπ μπορούν να έχουν το ίδιο παροδικό ρεύμα τροφοδοσίας – το ένα γιατί έχει υποστεί κακόβουλη τροποποίηση υλικού και το άλλο γιατί επηρεάζεται από το θόρυβο των διεργασιών.

Παρόλα αυτά, οι Narasimhan et al. (2012) αναφέρουν ότι μπορεί να χρησιμοποιηθεί η συσχέτιση μεταξύ παροδικού ρεύματος τροφοδοσίας και μέγιστης συχνότητας λειτουργίας για τη διάκριση κακόβουλων τροποποιήσεων υλικού σε ένα κύκλωμα ακόμα και υπό το θόρυβο των διεργασιών. Η παρουσία μιας κακόβουλης τροποποίησης υλικού θα προκαλέσει το τσιπ να αποκλίνει από τη γραμμική συσχέτιση παροδικού ρεύματος τροφοδοσίας και μέγιστης συχνότητας λειτουργίας.

Στην πράξη, η καθυστέρηση οποιασδήποτε διαδρομής στο κύκλωμα μπορεί να χρησιμοποιηθεί για το σκοπό αυτό. Ως εκ τούτου, γίνεται δύσκολο γι’ αυτόν που θέλει να επέμβει με κακόβουλο σκοπό στο κύκλωμα τσιπ, να γνωρίζει εκ των προτέρων ποια διαδρομή και κατ’ επέκταση ποια καθυστέρηση θα χρησιμοποιηθεί για τη βαθμονόμηση του θορύβου των διεργασιών.

Έτσι οι Narasimhan et al. (2012), καταλήγουν στο ότι δεδομένου πως ένας τυπικός σχεδιασμός θα έχει μεγάλο αριθμό διαδρομών, δεν θα είναι εφικτό για έναν εισβολέα να διαχειριστεί όλες τις διαδρομές στο τσιπ για να μπορέσει να καμουφλάρει την επιρροή της κακόβουλης τροποποίησης υλικού. Ακόμη και στην περίπτωση, βέβαια, που αυτός που θέλει να επέμβει με κακόβουλο σκοπό στο κύκλωμα μαντέψει τη διαδρομή που θα ελεγχθεί, μια κακόβουλη τροποποίηση υλικού, όπως έχει ήδη αναφερθεί, είναι πιθανό να αυξήσει τόσο την καθυστέρηση όσο και τη δραστηριότητα της διαδρομής στην οποία εισάγεται.

Ως εκ τούτου, ένα τσιπ που περιέχει μια κακόβουλη τροποποίηση υλικού θα αποκλίνει από την αναμενόμενη γραμμική συσχέτιση παροδικού ρεύματος τροφοδοσίας και μέγιστης συχνότητας λειτουργίας, όπου τόσο η μία όσο και η άλλη αυξάνονται ή μειώνονται ταυτόχρονα. Τέλος, για να αλλάξει η μέγιστη συχνότητα λειτουργίας, έτσι ώστε η κακόβουλη τροποποίηση υλικού να καταφέρει να «κοροϊδέψει» την προσέγγιση των συγγραφέων, αυτός που θέλει να επέμβει με κακόβουλο σκοπό στο κύκλωμα πρέπει να γνωρίζει το ακριβές μέγεθος της διακύμανσης των διεργασιών για κάθε διαδρομή του κάθε τσιπ κάτι που είναι δύσκολο να εκτιμηθεί πριν από την διαδικασία της κατασκευής (Narasimhan et al., 2012).

Η προσέγγιση, έτσι, απέδειξε πως η χρήση συνδυασμένης ανάλυσης πλευρικών καναλιών και ανάλυσης λογικής παρέχει υψηλή συνολική κάλυψη ανίχνευσης για κυκλώματα που έχουν υποστεί κακόβουλη τροποποίηση υλικού για διαφορετικούς τύπους και μεγέθη.

Μια ακόμα προσέγγιση παρουσιάζουν στο έργο τους οι Alkabani & Koushanfar (2009) η οποία βασίζεται στην εκτίμηση της διαρροής μιας πύλης. Στην προσέγγιση αυτή, αρχικά το πρώτο βήμα είναι ο έλεγχος των εισόδων και η παραγωγή των αντίστοιχων ελέγχων εισόδου που αντικατοπτρίζουν τις μετρήσεις του ρεύματος που διαρρέει από την πύλη. Για κάθε τσιπ υπό έλεγχο, το ζητούμενο του σταδίου αυτού είναι για κάθε τσιπ που υπόκειται σε έλεγχο να εκτιμηθεί η διαρροή ρεύματος σε κάθε πύλη μέσω διαφορετικών εισόδων. Για να επιτευχθεί αυτό, μετράται το συνολικό ρεύμα στην έξοδο του κυκλώματος το οποίο διαμορφώνεται από το άθροισμα των διαρροών των πυλών. Υποθέτοντας, όμως, ότι η τιμή διαρροής κάθε πύλης για κάθε συνδυασμό εισόδων είναι γνωστή από τις προσομοιώσεις, τότε ο στόχος μπορεί να αλλάξει και να βρεί τις αποκλίσεις στις διαρροές στις πύλες του κυκλώματος υπό εξέταση σε σχέση με τις διαρροές στις πύλες του πρωτότυπου κυκλώματος.

Το επόμενο βήμα στην προσέγγιση των Alkabani & Koushanfar (2009) είναι η εφαρμογή των ελέγχων και η χαρτογράφηση των τιμών που μετρήθηκαν στις διαρροές των πυλών. Δεδομένου ότι η διαρροή που μετράται είναι μια συνάρτηση πολλών στοιχείων των κυκλωμάτων και η κακόβουλη τροποποίηση υλικού δεν έχει καταστεί ακόμα γνωστή στα μοντέλα προσομοίωσης, ο αντίκτυπος μιας κακόβουλης τροποποίησης υλικού θα αλλάξει τις εκτιμήσεις των συνολικών διαρροών πύλης. Αυτό το γεγονός, παίζει σημαντικό ρόλο στην τελική ανίχνευση της κακόβουλης τροποποίησης υλικού.

Για το αν τελικά οι μετρήσεις που παρατηρούνται είναι φυσιολογικές ή προέρχονται εξαιτίας μια κακόβουλης τροποποίησης υλικού εκτελείται μια σύγκριση των τιμών της προσομοίωσης με αυτές που κανονικά το κύκλωμα θα έπρεπε να έχει. Μια πύλη, λοιπόν, χαρακτηρίζεται από μη κανονικές μετρήσεις όταν οι μετρήσεις έχουν μεγάλη απόκλιση στα εκτιμώμενα χαρακτηριστικά διαρροής σε σύγκριση με την τιμή που θα έπρεπε να είχε με βάση τις τιμές των προσομοιώσεων. Για να ποσοτικοποιηθεί αυτή η απόκλιση, γίνεται χρήση της ευκλείδειας απόστασης μεταξύ της τιμής της διαρροής πύλης και της κανονικής της τιμής.

Τέλος, εισάγεται επιπλέον αλγόριθμος ανίχνευσης κακόβουλων τροποποιήσεων υλικού που οι συγγραφείς υιοθετούν στη διαδικασία. Ο αλγόριθμος αυτός βασίζεται στη

συνεκτικότητα και χρησιμοποιεί ιδιότητες όπως αυτή της βελτιστοποίησης και χρήσης εκτιμήσεων διαρροής πύλης, της ανάλυσης ευαισθησίας αλλά και της βαθμονόμησης.

Από την πειραματική αξιολόγηση της προσέγγισης προέκυψε η επιβεβαίωση ότι η προσέγγιση είναι αποτελεσματική στην ανίχνευση των κακόβουλων τροποποιήσεων υλικού όπως επίσης ότι αυτή είναι και ανθεκτική στην επιρροή από το θόρυβο και τη μεταβολή των διεργασιών (Alkabani & Koushanfar, 2009).

Μια πιο σύγχρονη προσέγγιση, χρονολογικά, είναι αυτή των Huang, Bhunia & Mishra (2016). Στο έργο τους, επισημαίνουν πως η ανάλυση πλευρικών καναλιών – μια κατηγορία ανίχνευσης που αφορά και την προσέγγισή τους, μπορεί να πετύχει σημαντικά υψηλότερη κάλυψη ανίχνευσης για κακόβουλες τροποποιήσεις υλικού όλων των τύπων αλλά και μεγεθών, καθώς δεν απαιτεί την ενεργοποίηση ή διάδοση της άγνωστης τροποποίησης υλικού. Ωστόσο, οι αναλύσεις πλευρικών καναλιών έχουν συχνά περιορισμένη αποτελεσματικότητα λόγω της χαμηλής ευαισθησίας ανίχνευσης κάτω από μεγάλες παραλλαγές διεργασιών και του μικρού αποτυπώματος της κακόβουλης τροποποίησης υλικού στην υπογραφή των πλευρικών καναλιών ενός κυκλώματος.

Το κενό αυτό καλύπτουν, βέβαια, οι συγγραφείς με μια προσέγγιση δημιουργίας ελέγχων που λαμβάνει υπόψη τα δεδομένα των πλευρικών καναλιών. Η προσέγγιση βασίζεται σε μια ειδική τεχνική που προτείνουν οι συγγραφείς και μπορεί να αυξήσει σημαντικά την ευαισθησία ανίχνευσης τροποποιήσεων υλικού (Huang, Bhunia & Mishra, 2016).

Η προσέγγιση βασίζεται στην έννοια της στατιστικής μεγιστοποίησης της δραστηριότητας σε όλους τους σπάνια ενεργοποιημένους κόμβους ενός κυκλώματος. Η αποτελεσματικότητα ενός προτύπου ελέγχου για ανάλυση πλευρικών καναλιών μετράται με δύο τρόπους: 1) την ικανότητα να δημιουργεί το μεγαλύτερο μέρος της δραστηριότητας μέσα σε μια κακόβουλη τροποποίηση υλικού ή να ενεργοποιήσει αντίστοιχα μια κακόβουλη τροποποίηση υλικού και 2) την ικανότητα να δημιουργήσει υψηλή δραστηριότητα από την κακόβουλη τροποποίηση υλικού προς το κύκλωμα.

Έπειτα, τίθενται κάποια μέτρα που βοηθούν στην ανίχνευση της κακόβουλης τροποποίησης υλικού. Το πρώτο μέτρο των Huang, Bhunia & Mishra (2016) είναι αυτό που κρατάει τη διαφορά της δραστηριότητας μεταξύ του κυκλώματος προς έλεγχο και του πρωτότυπου κυκλώματος. Το δεύτερο είναι το πηλίκο του πρώτου μέτρου προς τη συνολική δραστηριότητα στο πρωτότυπο κύκλωμα. Έτσι, μπορεί να δημιουργηθεί ένας αποτελεσματικός έλεγχος τόσο βασιζόμενος στα δεδομένα του πρώτου αλλά και του δεύτερου μέτρου, γεγονός που βοηθάει στην ανάλυση της ευαισθησίας των πλευρικών καναλιών.

Παρόλα αυτά, οι κύριες προκλήσεις που αφορούν τη δημιουργία ελέγχων είναι ότι δεν είναι γνωστή η θέση μιας κακόβουλης τροποποίησης υλικού μέσα σε ένα κύκλωμα – που είναι και βασικό πρόβλημα. Επίσης, η κακόβουλη τροποποίηση υλικού είναι καλά κρυμμένη και καμουφλαρισμένη και στις περισσότερες περιπτώσεις παρουσιάζει χαμηλά επίπεδα δραστηριότητας όταν δεν είναι στην φάση ενεργοποίησης. Οι δύο αυτές προκλήσεις έχουν αποτέλεσμα οι τυχαίοι έλεγχοι να μην είναι αποτελεσματικοί στο να ανιχνεύουν τα σήματα των πλευρικών καναλιών που προέρχονται από κάποια κακόβουλη τροποποίηση υλικού.

Αντίθετα, η προσέγγιση των Huang, Bhunia & Mishra (2016), βασίζεται στη δημιουργία ενός συνόλου ελέγχων για κάθε υποψήφιο «σπάνιο» κόμβο που μπορεί να έχει υποστεί κακόβουλη τροποποίηση, ώστε να δημιουργείται δραστηριότητα που θα μπορεί να οδηγήσει τελικά στην ανίχνευση κακόβουλων τροποποιήσεων υλικού. Έτσι, γίνονται επαναλαμβανόμενοι έλεγχοι που αυξάνουν τη δραστηριότητα για να αυξηθεί η πιθανότητα μιας πλήρους ή μερικής ενεργοποίησης μιας κακόβουλης τροποποίησης υλικού.

Στην προσέγγιση των Huang, Bhunia & Mishra (2016) δημιουργείται ένα σύνολο ελέγχων για όλους τους σπάνια χρησιμοποιούμενους κόμβους και εκτελούνται έλεγχοι σε κάθε κόμβο ξεχωριστά. Ο αριθμός των ελέγχων είναι προκαθορισμένος κάθε φορά, ανάλογα με τον αριθμό που έχει θέσει ο ρυθμιστής της όλης διαδικασίας. Έτσι, αν ο αριθμός των ελέγχων που τεθούν είναι μεγάλος, τότε υπάρχει και μεγαλύτερη πιθανότητα να δημιουργηθεί περισσότερη δραστηριότητα στους κόμβους του κυκλώματος και τους κόμβους που επηρεάζει μια κακόβουλη τροποποίηση υλικού. Αποτέλεσμα, είναι ακόμα και η τροποποίηση υλικού που χρησιμοποιεί κάποια συνθήκη ή έναυσμα για να ενεργοποιηθεί, να φανερώνει υψηλή δραστηριότητα ακόμα και αν δεν είναι πλήρως ενεργοποιημένη.

Στα αποτελέσματα αποδείχθηκε ότι η προσέγγιση των συγγραφέων θα ήταν γενικότερα αποτελεσματική για όλες τις περιπτώσεις ανάλυσης πλευρικών καναλιών που βασίζονται στη δραστηριότητα μέσα στις κακόβουλες τροποποιήσεις υλικού. Επιπλέον, αποδείχθηκε πως η προσέγγιση ήταν αποτελεσματική και σε διαφορετικές μορφές και μεγέθη κακόβουλων τροποποιήσεων υλικού εφόσον, φυσικά, η κακόβουλη τροποποίηση υλικού είχε εισαχθεί μέσω αλλαγών στη δομή ενός κυκλώματος που είναι και ο κυρίαρχος τρόπος χρήσης των κακόβουλων τροποποιήσεων υλικού.

Στην προσομοίωση από ένα σύνολο κυκλωμάτων που δέχθηκαν την προσέγγιση των συγγραφέων και τους αντίστοιχους ελέγχους, αποδείχθηκε ότι η προτεινόμενη προσέγγιση μπορεί να βελτιώσει την ευαισθησία της ανάλυσης πλευρικών καναλιών κατά περισσότερο από 96,61%, σε σύγκριση με τυχαίες δοκιμές για ένα μεγάλο σύνολο αυθαίρετων

κακόβουλων τροποποιήσεων υλικού. Αυτό δείχνει ότι μια μεγάλη παραγωγή στατιστικών ελέγχων, όπως η προσέγγιση μπορεί να χρησιμεύσει ως βασικό συστατικό σε μια προσέγγιση ανίχνευσης κακόβουλων τροποποιήσεων υλικού βασισμένη στα δεδομένα των πλευρικών καναλιών (Huang, Bhunia & Mishra, 2016).

3.2 Ανάλυση βασισμένη στο χρόνο

Οι Li & Lach (2008) πρότειναν μια φυσική μη κλωνοποιήσιμη συνάρτηση (Physical Unclonable Function - PUF) για την ανίχνευση κακόβουλων τροποποιήσεων υλικού. Η προσέγγιση των συγγραφέων χρησιμοποιεί τη μέτρηση επιλεγμένων καθυστερήσεων σε συγκεκριμένα μονοπάτια μέσα στο κύκλωμα. Η ανίχνευση των κακόβουλων τροποποιήσεων υλικού επιτυγχάνεται όταν μία ή περισσότερες καθυστερήσεις σε μία διαδρομή εκτείνεται ή αντίστοιχα εκτείνονται, πέρα από ένα προκαθορισμένο όριο.

Παρόλα αυτά, η τεχνική μπορεί εύκολα να επηρεαστεί από τη θερμοκρασία και δεν είναι εύκολο να εφαρμοστεί στα σημερινά κυκλώματα και τσιπ που αποτελούνται από εκατομμύρια διαδρομές. Ωστόσο, οι συγγραφείς έχουν προβλέψει και έχουν εισάγει στην πρότασή τους, ειδική συσκευή που ελέγχει τη θερμοκρασία και μπορεί να ξεπεράσει το πρόβλημα της καθυστέρησης εξαιτίας της θερμοκρασίας. Αυτό γιατί η θερμοκρασία μπορεί να προκαλέσει και αυτή καθυστέρηση αλλά στην προκειμένη περίπτωση ζητείται ο εντοπισμός των καθυστερήσεων που οφείλονται σε κακόβουλες τροποποιήσεις υλικού και όχι στη θερμοκρασία.

Οι Jin και Makris (2008) πρότειναν μια νέα μέθοδο δημιουργίας αποτυπωμάτων, χρησιμοποιώντας πληροφορίες καθυστέρησης, δεδομένα και μετρήσεις ολόκληρου του τσιπ. Η λογική της μεθόδου αυτής σύμφωνα με τους συγγραφείς βασίζεται στο ότι ένα τσιπ έχει πολλές διαδρομές με καθυστέρηση, και κάθε καθυστέρηση αντίστοιχα αντιπροσωπεύει ένα μέρος της καθυστέρησης ολόκληρου του τσιπ. Εδώ, η ανάλυση με βάση το χρόνο μπορεί να δημιουργήσει μια σειρά αποτυπωμάτων με βάση την καθυστέρηση κάθε διαδρομής.

Χωρίς να έχει σημασία το μέγεθος της κακόβουλης τροποποίησης υλικού, ακόμα και αν είναι μικρό, σε επίπεδο τσιπ, δε συμβαίνει το ίδιο σε επίπεδο διαδρομής. Στο επίπεδο αυτό ακόμα και μια πολύ μικρή κακόβουλη τροποποίηση υλικού μπορεί να ανιχνευθεί. Η μέθοδος ελέγχου και ανίχνευσης κακόβουλων τροποποιήσεων υλικού γίνεται σύμφωνα με τους Li & Lach (2008) σε τρία βήματα:

1. Πρώτο βήμα είναι η καταγραφή των καθυστερήσεων των διαδρομών του τσιπ υπό εξέταση. Αξίζει να σημειωθεί ότι επιλέγονται διαφορετικά τσιπ από πολλά και διαφορετικά σχέδια. Στα τσιπ που συμμετέχουν στη διαδικασία ελέγχου, στη συνέχεια τρέχουν έλεγχοι σύμφωνα με προκαθορισμένα πρότυπα και συλλέγονται λεπτομερείς πληροφορίες για τις καθυστερήσεις των διαδρομών. Στη συνέχεια, γίνεται έλεγχος των τσιπ με μεθόδους αντίστροφης μηχανικής για να εξασφαλιστεί η γνησιότητα των κυκλωμάτων και κατ' επέκταση του τσιπ.
2. Στο δεύτερο βήμα εκτελείται η δημιουργία αποτυπωμάτων. Παράγονται δηλαδή και χαρτογραφούνται όλα τα αποτυπώματα των καθυστερήσεων, σύμφωνα με τα δεδομένα που εξήχθησαν από τις καθυστερήσεις των μονοπατιών.
3. Στο τρίτο βήμα εκτελείται η ανίχνευση των κακόβουλων τροποποιήσεων υλικού. Στη διαδικασία αυτή όλα τα τσιπ ελέγχονται σύμφωνα με τα ίδια πρότυπα ελέγχου. Έτσι, οι πληροφορίες που σχετίζονται με τις καθυστερήσεις συγκρίνονται τελικά, με τα αποτυπώματα των καθυστερήσεων.

Αυτή η μέθοδος χρησιμοποιεί στατιστική ανάλυση για να αντιμετωπίσει τις διακυμάνσεις των μετρήσεων κατά διαδικασία. Επειδή τα σημερινά κυκλώματα περιλαμβάνουν εκατομμύρια διαδρομές, μετρώντας όλα τα μονοπάτια, ειδικά τα σύντομα, δεν είναι πρακτικό, οπότε η στατιστική ανάλυση φαίνεται να αποδίδει στη συγκεκριμένη περίπτωση.

Μια ακόμα προσέγγιση, με βάση το χρόνο προτείνουν οι Narasimhan et al. (2011) στο έργο τους. Εκεί αναφέρουν πως οι προσεγγίσεις μέσω των λογικών ελέγχων δεν είναι πολύ αποτελεσματικές για την ανίχνευση μεγάλων κακόβουλων τροποποιήσεων υλικού που απαιτούν πολλαπλές αλλαγές κατάστασης οι οποίες συχνά προκαλούνται από σπάνια γεγονότα στο κύκλωμα, προκειμένου να ενεργοποιηθούν και να προκληθούν δυσλειτουργίες. Από την άλλη, ωστόσο, η ανάλυση πλευρικών καναλιών προέκυψε ως μια αποτελεσματική προσέγγιση για την ανίχνευση τέτοιων μεγάλων κακόβουλων τροποποιήσεων υλικού.

Παρ'όλα αυτά, οι συγγραφείς σημειώνουν πως οι προσεγγίσεις ανάλυσης πλευρικών καναλιών αντιμετωπίζουν σημαντικά προβλήματα από τη μεγάλη μείωση της ευαισθησίας ανίχνευσης με αυξανόμενες παραλλαγές της διαδικασίας ή της μείωσης του μεγέθους της κακόβουλης τροποποίησης υλικού.

Γι' αυτό το λόγο οι Narasimhan et al. (2011) πρότειναν την προσέγγιση TeSR, μια προσέγγιση χρονικής αυτοαναφοράς που συγκρίνει την τρέχουσα υπογραφή ενός τσιπ σε δύο διαφορετικές χρονικές στιγμές για να εξαλείψει τελείως την επίδραση του θορύβου της

διαδικασίας, παρέχοντας έτσι υψηλή ευαισθησία ανίχνευσης για κακόβουλες τροποποιήσεις υλικού ανεξάρτητα από το μέγεθος. Επιπλέον, και σε αντίθεση με τις τότε υπάρχουσες προσεγγίσεις, δεν απαιτεί τη χρήση του πρωτότυπου τσιπ ως αναφορά.

Η προσέγγιση των Narasimhan et al. (2011) περιλαμβάνει δύο βήματα. Το πρώτο είναι η παραγωγή του ελέγχου. Το βήμα αυτό για την παραγωγή του ελέγχου ενσωματώνει τόσο λειτουργικές δοκιμές όσο και αναλύσεις πλευρικών καναλιών για να ικανοποιηθούν ακόμα και οι συνθήκες ενεργοποίησης κακόβουλων τροποποιήσεων υλικού που προκαλούνται από τις τιμές των σπάνιων κόμβων προκαλώντας ταυτόχρονα τη μέγιστη δραστηριότητα στην κακόβουλη τροποποίηση υλικού.

Το κύκλωμα που ελέγχεται αρχικά αποσυντίθεται σε μη επικαλυπτόμενα λειτουργικά τμήματα ή μονάδες για να μειωθεί η πολυπλοκότητα της δημιουργίας των ελέγχων ενώ αυξάνεται η ευαισθησία ανίχνευσης των παραμέτρων των πλευρικών καναλιών. Για κάθε τμήμα η μονάδα χρησιμοποιεί μια προσέγγιση που βασίζεται σε στατιστικά πρότυπα παραγωγής ελέγχων.

Έτσι, αρχικά στήνεται μια λίστα με σπάνια ενεργοποιημένους εσωτερικούς κόμβους στο κύκλωμα, μέσω προσομοιώσεων με μεγάλο αριθμό τυχαίων ελέγχων, αλλά και μαζί με τις αντίστοιχες σπάνιες τιμές τους. Έπειτα, δημιουργείται μια σύντομη λίστα ελέγχων που ενεργοποιεί κάθε σπάνιο κόμβο με βάση τη σπάνια τιμή που έχει προκύψει, μια τεχνική που έχει ανώτερη κάλυψη στο έναυσμα των κακόβουλων τροποποιήσεων υλικού σε σύγκριση με τα τυχαία πρότυπα δοκιμών.

Από τους ελέγχους αυτούς, οι Narasimhan et al. (2011) καθορίζουν ένα υποσύνολο ελέγχων που εξασφαλίζει ότι το κύκλωμα φτάνει στην κατάλληλη κατάσταση για να ξεκινήσει ο χαρακτηρισμός για μια συγκεκριμένη περιοχή του ανάλογα με την υπογραφή του. Μόλις το κύκλωμα βρεθεί στην επιθυμητή κατάσταση εκκίνησης ελέγχων, το σετ ελέγχων εφαρμόζεται και θέτει το κύκλωμα σε ένα σταθερό σύνολο μεταβάσεων κατάστασης για να αποτυπωθεί τελικά το τρέχων αποτύπωμα.

Στη συνέχεια, έρχεται το δεύτερο βήμα, αυτό του χαρακτηρισμού του κυκλώματος. Οι συγγραφείς αναφέρουν πως είναι επιθυμητό να υπάρχουν διαθέσιμα διαφορετικά μονοπάτια που οδηγούν στην κατάσταση αυτή. Διαφορετικά, μια κακόβουλη τροποποίηση υλικού μπορεί να συγχρονιστεί με το σήμα ελέγχου. Για να καλυφθούν διαφορετικές πιθανές συνθήκες ενεργοποίησης μιας κακόβουλης τροποποίησης υλικού σε μια περιοχή, οι υπογραφές πρέπει να συγκριθούν με πολλαπλούς διαδοχικούς ελέγχους.

Η διαφορά από τη σύγκριση της τρέχουσας υπογραφής δύο χρονικών στιγμών ορίζεται ως η ευκλείδεια απόσταση μεταξύ των τρεχουσών υπογραφών στις δύο χρονικές στιγμές.

Εάν μία ή περισσότερες από τις τρέχουσες υπογραφές διαφέρουν από το μέσο όρο υπογραφών σε πολλαπλές χρονικές στιγμές με ένα προκαθορισμένο όριο θορύβου, τότε το κύκλωμα είναι πιθανό να έχει υποστεί κάποια κακόβουλη τροποποίηση υλικού.

Τα αποτελέσματα προσομοίωσης της προσέγγισης των Narasimhan et al. (2011) για τρία πολύπλοκα σχέδια και τρία αντιπροσωπευτικά διαδοχικά κυκλώματα που είχαν υποστεί κακόβουλη τροποποίηση υλικού έδειξαν την αποτελεσματικότητα της προσέγγισης κάτω από μεγάλες παραλλαγές διεργασίας.

Μια ακόμα προσέγγιση, αυτή τη φορά πιο σύγχρονη, παρουσίασαν στο έργο τους οι Bao, Forte & Srivastava (2015). Εκεί αναφέρουν πως προηγούμενες προσεγγίσεις χρησιμοποιούν την αντίστροφη μηχανική (reverse engineering) για να εντοπίσουν τις κακόβουλες τροποποιήσεις υλικού σε σύγκριση με το πρωτότυπο τσιπ. Ωστόσο, δεν αναφέρεται το πως κάτι τέτοιο γίνεται αποτελεσματικά. Στην πραγματικότητα, η αντίστροφη μηχανική είναι μια πολύ δαπανηρή διαδικασία που απαιτεί πολύ χρόνο και εντατική χειρωνακτική προσπάθεια. Είναι επίσης πολύ επιρρεπής σε σφάλματα.

Για τους λόγους αυτούς οι συγγραφείς πρότειναν μια καινοτόμα και αξιόπιστη προσέγγιση αντίστροφης μηχανικής για τον εντοπισμό των κακόβουλων τροποποιήσεων υλικού. Πιο συγκεκριμένα, το πρόβλημα της ανίχνευσης κακόβουλων τροποποιήσεων υλικού μετατρέπεται σε πρόβλημα ομαδοποίησης K μέσων όρων κατά συστάδες (K-mean clustering), μια ευρέως χρησιμοποιούμενη μέθοδο μηχανικής μάθησης.

Οι αλγόριθμοι ομαδοποίησης χρησιμοποιούνται για την ταξινόμηση των δεδομένων χωρίς κάποιο χαρακτηρισμό ή ετικέτα (unlabeled) σε διαφορετικές συστάδες ως εξής. Τα δεδομένα που ανήκουν σε διαφορετικές συστάδες πρέπει να είναι όσο το δυνατόν πιο διαφορετικά, ενώ τα δεδομένα της ίδιας συστάδας θα πρέπει να είναι όσο το δυνατόν πιο κοντά. Στη μέθοδο που προτείνεται, γίνεται ομαδοποίηση κάθε πλέγματος του κυκλώματος βάσει των τύπων παρεμβολών που έχει (χωρίς τροποποιήσεις, κακόβουλη προσθήκη τροποποίησης υλικού, κακόβουλη διαγραφή κλπ.) (Bao, Forte & Srivastava, 2015).

Ο στόχος είναι η δημιουργία μιας μηχανής ομαδοποίησης σε συστάδες που να μπορεί να ομαδοποιεί σωστά τα πλέγματα χωρίς τροποποιήσεις σε μια συστάδα και τα πλέγματα που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού σε άλλες διαφορετικές συστάδες. Μετά την ομαδοποίηση, τέλος, γίνεται η τελική ταξινόμηση για κάθε τσιπ.

Η τελική ταξινόμηση για κάθε τσιπ αποφασίζεται εξετάζοντας τον αριθμό των πλεγμάτων που έχουν τοποθετηθεί στις συστάδες με πλέγματα που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού και την τοποθεσία τους. Παρ’όλα αυτά, ένα τσιπ δε χαρακτηρίζεται ως φερόμενο κακόβουλης τροποποίησης υλικού αν έχει μόνο λίγα αραιά

πλέγματα που θεωρούνται πως έχουν υποστεί με τη σειρά τους κάποια κακόβουλη τροποποίηση υλικού. Αντίθετα, προκειμένου να χαρακτηριστεί ένα τσιπ ως φερόμενο κακόβουλης τροποποίησης υλικού, πρέπει να υπάρχει τουλάχιστον ένας προκαθορισμένος αριθμός γειτονικών πλεγμάτων που έχουν υποστεί με τη σειρά τους κάποια κακόβουλη τροποποίηση υλικού στο τσιπ.

Έπειτα, στην προσέγγιση των Bao, Forte & Srivastava (2015) τα γειτονικά πλέγματα στο ίδιο επίπεδο ορίζονται ως οριζόντια γειτονικά πλέγματα και τα γειτονικά πλέγματα μεταξύ γειτονικών επιπέδων στο κύκλωμα ορίζονται ως κατακόρυφα γειτονικά πλέγματα. Αυτό βασίζεται σε δύο βασικούς λόγους. Πρώτον, λόγω του μεγέθους των πλεγμάτων που επιλέγονται, πιθανότατα, οι κακόβουλες τροποποιήσεις υλικού δεν θα χωρέσουν σε ένα πλέγμα. Έτσι, θα επηρεαστούν δύο ή περισσότερα πλέγματα. Δεύτερον, οι κακόβουλες τροποποιήσεις τείνουν να είναι συνεχείς. Συνδέονται με κάποιο τρόπο σε ένα επίπεδο ή συνδέονται με κάποιες άλλες κακόβουλες τροποποιήσεις μέσω γειτονικών επιπέδων.

Ο μέγιστος αριθμός λοιπόν, συνδεδεμένων πλεγμάτων που έχουν υποστεί κάποια τροποποίηση υλικού δίνει μια ιδέα για το πόσο μεγάλες αποκλίσεις από το πρωτότυπο τσιπ υπάρχουν στο υπό εξέταση τσιπ.

Είναι σημαντικό να σημειωθεί ότι ακόμα και αν αυτός που θέλει να προκαλέσει κακό στο τσιπ γνωρίζει ένα τέτοιο σύστημα ανίχνευσης, δεν μπορεί να κρύψει τις κακόβουλες τροποποιήσεις υλικού. Αυτό γιατί για να αποφευχθεί η ανίχνευση, αυτός που θέλει να προκαλέσει κακό στο τσιπ πρέπει να κάνει ασυνεχή τη διασύνδεση της τροποποίησης. Ωστόσο, αυτά τα μη φυσιολογικά πρότυπα θα επισημαίνονται εύκολα ύποπτα από έναν έλεγχο βασισμένο σε κανόνες. Ο κανόνας μπορεί να είναι απλά να ελέγξει εάν υπάρχει μια διασύνδεση πλέγματος που αλλάζει από επίπεδο σε επίπεδο. Αν υπάρχει μια τέτοια σύνδεση, τότε αυτή γίνεται ύποπτη και αν η περιοχή στην οποία συνδέεται είναι και αυτή ύποπτη τότε το τσιπ χαρακτηρίζεται ως φερόμενο κακόβουλης τροποποίησης υλικού.

Τα αποτελέσματα προσομοίωσης των Bao, Forte & Srivastava (2015) βασίζονται στη χρήση εργαλείων τελευταίας τεχνολογίας σε διάφορα ελεύθερα κυκλώματα (δηλαδή διαθέσιμα προς όλους) και δείχνουν ότι η προτεινόμενη προσέγγιση των συγγραφέων μπορεί να ανιχνεύσει τις κακόβουλες τροποποιήσεις υλικού με υψηλό ποσοστό ακρίβειας.

3.3 Ανάλυση βασισμένη στην ενεργοποίηση της κακόβουλης τροποποίησης υλικού

Οι μέθοδοι ανίχνευσης αυτές, δεν βασίζονται στην περιοχή, αλλά βασίζονται σε μια τυχαία ή στοχευμένη ενεργοποίηση των κακόβουλων τροποποιήσεων υλικού.

Ένα παράδειγμα τέτοιας ανάλυσης είναι η μέθοδος που προτείνουν στο έργο τους οι Jha & Jha (2008), βασισμένη στις πιθανότητες της τυχαίας ενεργοποίησης των κακόβουλων τροποποιήσεων για την ανίχνευσή τους. Στο έργο τους έδειξαν ότι είναι δυνατόν να κατασκευαστεί μια μοναδική υπογραφή ενός κυκλώματος με βάση μια συγκεκριμένη πιθανότητα για τα πρότυπα ελέγχων που εφαρμόζονται στις εισόδους του.

Οι Jha & Jha (2008) εφαρμόζουν στο κύκλωμα κώδικες εισόδου βάσει μιας συγκεκριμένης πιθανότητας και συγκρίνουν τις εξόδους του με το αρχικό κύκλωμα. Εάν υπάρχουν διαφορές στις εξόδους, τότε αποδεικνύεται πως υπάρχει στο κύκλωμα τοποθετημένη κακόβουλη τροποποίηση υλικού. Για την ανίχνευση κακόβουλων τροποποιήσεων υλικού σε ένα κύκλωμα, βέβαια, τα πρότυπα μπορούν να εφαρμοστούν μόνο με βάση μια τέτοια πιθανότητα ούτως ώστε να επιτευχθεί ένα επίπεδο εμπιστοσύνης σχετικά με το αν ο αρχικός σχεδιασμός και το κατασκευασμένο τσιπ είναι το ίδιο.

Μια ακόμα μέθοδος ανήκει στην πρόταση των Wolff, Papachristou, Brunia & Chakraborty (2008), η οποία βασίζεται στη σπανιότητα των συνδυασμών στις υλοποιήσεις κυκλωμάτων και τσιπ. Οι σπάνιες, λοιπόν υλοποιήσεις και κατ΄επέκταση και τα σπάνια κυκλώματα και τσιπ που έχουν σχεδιαστεί χρησιμοποιούνται ως εναύσματα ως προς τις κακόβουλες τροποποιήσεις υλικού. Οι συγγραφείς, δημιούργησαν ένα σύνολο συνδυασμών από τέτοιες υλοποιήσεις που οδηγούν τελικά στην ενεργοποίηση κακόβουλων τροποποιήσεων υλικού. Τέλος, σαν πρόταση τίθεται ο συνδυασμός τέτοιων υλοποιήσεων με πιο παραδοσιακές τεχνικές ελέγχου για να ενεργοποιήσουν μια ενδεχόμενη κακόβουλη τροποποίηση υλικού και να κάνουν τον αντίκτυπό της στο υπό έλεγχο κύκλωμα φανερό και να γίνει επιτυχώς η ανίχνευση αυτής.

Οι ίδιοι συγγραφείς, ένα χρόνο αργότερα εξέλιξαν την προσέγγιση αυτή και εισήγαγαν μια τεχνική που παρήγαγε ελέγχους με βάση την πολλαπλή διέγερση σπάνιων λογικών συνθηκών σε εσωτερικούς κόμβους. Μια τέτοια στατιστική προσέγγιση μεγιστοποιεί την πιθανότητα, σύμφωνα με τα λόγια τους, να ενεργοποιηθεί τελικά η κακόβουλη τροποποίηση υλικού και να ανιχνευθεί από τη διαδικασία ελέγχου (Chakraborty, Wolff, Paul, Papachristou & Bhunia, 2009).

Επιπλέον, η προτεινόμενη προσέγγιση παραγωγής ελέγχων με βάση την πολλαπλή διέγερση σπάνιων λογικών συνθηκών σε εσωτερικούς κόμβους μπορεί να είναι αποτελεσματική για την αύξηση της ευαισθησίας της ανίχνευσης κακόβουλων τροποποιήσεων υλικού στις ήδη υπάρχουσες προσεγγίσεις των πλευρικών καναλιών που παρακολουθούν την επίδραση ενός κυκλώματος που έχει υποστεί κακόβουλη τροποποίηση με βάση την ισχύ ή την υπογραφή του κυκλώματος.

Ο κύριος στόχος της προτεινόμενης μεθοδολογίας των Chakraborty et al., (2009) ήταν να παραχθεί ένα σύνολο προτύπων ελέγχου που είναι σύντομο και περιεκτικό (ελαχιστοποιώντας το χρόνο ελέγχου και κατ' επέκταση το κόστος), μεγιστοποιώντας την πιθανότητα ανίχνευσης μεγάλης ποικιλίας κακόβουλων τροποποιήσεων υλικού.

Η βασική ιδέα βασίστηκε στο να ανιχνευθούν σπάνιες διεργασίες με χαμηλές πιθανότητες να εκτελεστούν στους εσωτερικούς κόμβους, να επιλεγούν υποψήφιες ή πιθανές κακόβουλες τροποποιήσεις υλικού που ενεργοποιούνται από ένα υποσύνολο αυτών των σπάνιων διεργασιών και στη συνέχεια να προκύψει ένα βέλτιστο σύνολο ελέγχων. Οι έλεγχοι αυτοί θα πρέπει έπειτα να μπορούν να ενεργοποιήσουν κάθε μία από τις επιλεγμένες διεργασίες (χαμηλής πιθανότητας) μεμονωμένα, με βάση τις σπάνιες λογικές τους τιμές πολλές φορές. Το πόσες φορές θα γίνει κάθε έλεγχος εξαρτάται από την παράμετρο η οποία δίνεται από αυτόν που είναι και υπεύθυνος για τον έλεγχο. Η τακτική αυτή αυξάνει την πιθανότητα ανίχνευσης μιας κακόβουλης τροποποίησης υλικού που έχει ένα υποσύνολο αυτών των διεργασιών στη λίστα με τις διεργασίες και κατ' επέκταση τους κόμβους που επηρεάζει.

Ωστόσο, οι Chakraborty et al., (2009) αναφέρουν ότι η ανίχνευση κακόβουλων τροποποιήσεων υλικού μέσω της τεχνικής αυτής, είναι επιτυχής σε ψηφιακές μορφές κακόβουλης τροποποίησης υλικού που μπορούν να εισαχθούν σε ένα σχέδιο είτε κατά τη διαδικασία του σχεδιασμού (π.χ. μέσω εργαλείου CAD) είτε στο στάδιο παραγωγής. Έτσι, περιπτώσεις κακόβουλων τροποποιήσεων υλικού που βασίζονται σε αναλογικούς μηχανισμούς ενεργοποίησης (π.χ. μέσω θερμότητας) δε λαμβάνονται υπόψη.

Δεδομένου ότι η προτεινόμενη προσέγγιση ανίχνευσης βασίζεται στη λειτουργική επικύρωση του τσιπ χρησιμοποιώντας λογικές τιμές, είναι ισχυρή με βάση με τις παραλλαγές των παραμέτρων και μπορεί να εντοπίσει αξιόπιστα τα μικρά μεγέθη κακόβουλων τροποποιήσεων υλικού, όπως για παράδειγμα όταν αυτές βασίζονται μόνο σε λίγες λογικές πύλες.

Έτσι, η τεχνική μπορεί να χρησιμοποιηθεί για να αυξήσει την ευαισθησία ανίχνευσης πολλών τεχνικών ανίχνευσης κακόβουλων τροποποιήσεων υλικού, όπως αυτές που

παρακολουθούν την ισχύ του κυκλώματος, αυξάνοντας τη δραστηριότητα σε περιοχές που χαρακτηρίζονται από κάποια κακόβουλη τροποποίηση υλικού (Chakraborty et al., 2009).

Τα αποτελέσματα προσομοίωσης που εκτελέστηκαν για την προσέγγιση των συγγραφέων έδειξαν ότι αυτή μπορεί να είναι εξαιρετικά αποτελεσματική για την ανίχνευση αυθαίρετων περιπτώσεων κακόβουλων τροποποιήσεων υλικού μικρού μεγέθους, τόσο συνδυαστικών όσο και διαδοχικών. Επίσης, αποδείχθηκε ότι η προσέγγιση των συγγραφέων μπορεί να επιτύχει συγκρίσιμη ή καλύτερη κάλυψη ανίχνευσης κακόβουλων τροποποιήσεων υλικού με περίπου 85% μείωση στη διάρκεια της διαδικασίας ελέγχου κατά μέσο όρο σε σχέση με τυχαία πρότυπα.

Μια διαφορετική προσέγγιση, έδωσαν στο έργο τους οι Banga & Hsiao (2009) με δύο βασικά στάδια που εντοπίζει τη διαφορά στις κυματομορφές ισχύος ανάμεσα στο κύκλωμα που εξετάζεται και στο κύκλωμα που αντιστοιχεί ουσιαστικά στην αρχική σχεδίαση.

Στο πρώτο στάδιο που ονομάζεται διαίρεση κυκλώματος, γίνεται χρήση ενός προτύπου που αντιλαμβάνεται τις πιθανές περιοχές που υπάρχει πιθανότητα να έχει τοποθετηθεί κάποια κακόβουλη τροποποίηση υλικού. Για την ανίχνευση, λοιπόν, μιας ενδεχόμενης κακόβουλης τροποποίησης υλικού αυξάνεται η δραστηριότητα στα τμήματα του κυκλώματος που έχουν θεωρηθεί ως υποψήφια ως προς το να έχει τοποθετηθεί σε αυτά μια κακόβουλη τροποποίηση υλικού. Παράλληλα ελαχιστοποιείται η δραστηριότητα σε όλα τα υπόλοιπα τμήματα του κυκλώματος.

Στο δεύτερο στάδιο, που ονομάζεται μεγέθυνση δραστηριότητας, γίνεται εφαρμογή ελέγχων σύμφωνα με διαφορετικά πρότυπα στις ίδιες περιοχές που έχουν ανιχνευθεί κατά το πρώτο στάδιο ως πιθανές περιοχές με κακόβουλες τροποποιήσεις υλικού. Σκοπός στη διαδικασία αυτή είναι να μεγεθυνθεί όποια διαφορά εντοπίζεται ανάμεσα στα πρωτότυπα κυκλώματα και τα κυκλώματα που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού (Banga & Hsiao, 2009).

Οι περιοχές, λοιπόν, που παρουσιάζουν αυξημένη δραστηριότητα αναγνωρίζονται χρησιμοποιώντας τα δεδομένα που δημιουργήθηκαν στο πρώτο στάδιο και έτσι γίνεται η σύγκριση για σχετικές διαφορές μεταξύ των προφίλ ισχύος των πρωτότυπων κυκλωμάτων και των κυκλωμάτων που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού.

Στη συνέχεια, κάθε πύλη στο κύκλωμα χαρακτηρίζεται από δύο μετρητές. Ο ένας μετρητής αφορά τη συχνότητα που μια περιοχή φαίνεται να έχει υποστεί μια κακόβουλη τροποποίηση υλικού και ο άλλος τη συχνότητα που μια περιοχή φαίνεται καθαρή όπως στο πρωτότυπο σχέδιο. Κάθε φορά που μια πύλη στέλνει δεδομένα εξόδου και ξεπερνάει ένα καθορισμένο επιτρεπτό όριο, τότε ο πρώτος μετρητής αυξάνεται (ισχύει και το αντίστροφο).

Ο λόγος των δύο μετρητών στο τέλος με όνομα βάρος πύλης, χαρακτηρίζει τελικά τη δραστηριότητα μιας πύλης. Έτσι, πύλες στις οποίες ο λόγος των δύο μετρητών είναι υψηλός, αποτελεί ένδειξη ότι η πύλη επηρεάζεται από μια κακόβουλη τροποποίηση υλικού αφού εντοπίζεται μια διαφορά ισχύος η οποία είναι μεγάλη και δε δικαιολογείται στο πρωτότυπο σχέδιο.

Μια ακόμα προσέγγιση, εισήγαγαν οι Banga & Hsiao (2010) στο έργο τους που αφορά τα πρώτα στάδια παραγωγής ενός τσιπ. Το έργο περιλαμβάνει τέσσερα στάδια στην ανίχνευση κακόβουλων τροποποιήσεων υλικού σε κυκλώματα και τσιπ. Η προσέγγιση, λοιπόν, ξεκινά με το πρώτο στάδιο που περιλαμβάνει την αφαίρεση των σημάτων των οποίων η ανίχνευση και η διάδοση είναι εύκολη. Τα σήματα που μένουν υποβάλλονται σε ένα ειδικό εργαλείο ανίχνευσης σημάτων που συμβάλει στον εντοπισμό εκείνων των σημάτων που είναι δύσκολο να ενεργοποιηθούν ή να διαδοθούν.

Αντίθετα όμως με την αναγνώριση των σημάτων που είναι δύσκολο να ενεργοποιηθούν ή να διαδοθούν, πρέπει να ληφθεί υπόψη η συμπεριφορά που προκαλείται από τις κακόβουλες τροποποιήσεις υλικού για να περιοριστούν οι θέσεις που μπορούν αυτές να εισαχθούν στο κύκλωμα.

Έτσι, εισάγεται το τρίτο στάδιο, γίνεται έλεγχος των ύποπτων σημάτων και ορίζεται τελικά αν το σήμα είναι κανονικό ή προέρχεται από κάποια κακόβουλη τροποποίηση υλικού. Τέλος, εφαρμόζεται μια προσέγγιση που απομονώνει περιοχές του τσιπ, μέσω των φιλτραρισμένων σημάτων, που περιλαμβάνουν στα όριά τους κυκλώματα που έχουν υποστεί κακόβουλες τροποποιήσεις υλικού.

Στα αποτελέσματα, οι Banga & Hsiao (2010) απέδειξαν πως η προσέγγισή τους ήταν σε θέση να επιστρέψει ένα πολύ μικρό αριθμό περιοχών όπου θα μπορούσε να εισαχθεί μια κακόβουλη τροποποίηση υλικού.

3.4 Ανάλυση βασισμένη στην αρχιτεκτονική

Οι Verbauwhede & Schaumont (2007) πρότειναν την εξέταση θεμάτων εμπιστοσύνης σε διάφορα επίπεδα αφαιρετικής αρχιτεκτονικής (πρωτόκολλα, λογισμικό, μικροαρχιτεκτονική και κυκλώματα).

Σε πιο αφαιρετικά επίπεδα σχεδίασης, αυτός που θέλει να εισβάλει σε ένα κύκλωμα και να τοποθετήσει μια κακόβουλη τροποποίηση υλικού μπορεί να έχει πρόσβαση στον διερμηνέα του κυκλώματος και να επηρεάσει ή να παραμετροποιήσει το λογισμικό. Οι πληροφορίες πλευρικών καναλιών μπορούν να χρησιμοποιηθούν στο επίπεδο

αρχιτεκτονικής λογισμικού. Στο επίπεδο μικροαρχιτεκτονικής και κυκλωμάτων, αυτός που θέλει να εισβάλει σε ένα κύκλωμα και να τοποθετήσει μια κακόβουλη τροποποίηση υλικού λαμβάνει υπόψη την κατανάλωση ενέργειας ή την ηλεκτρομαγνητική ενέργεια. Ως εκ τούτου, οι συγγραφείς πρότειναν ένα συστηματικό αντίμετρο για την προστασία της εμπιστοσύνης σε διαφορετικούς αφαιρετικούς σχεδιασμούς.

Στο φυσικό επίπεδο παράλληλα, μπορούν να χρησιμοποιηθούν τεχνικές, όπως η τοποθέτηση εξαρτημάτων ασφαλείας σε ειδική θήκη με αισθητήρες φωτός, θερμοκρασίας, διαρροής ή κίνησης και οι οποίες μπορούν να παρέχουν την αντίστοιχη προστασία στο κύκλωμα. Ωστόσο, πληροφορίες πλευρικών καναλιών, όπως η κατανάλωση ενέργειας, θα πρέπει να διαχωρίζονται από τα δεδομένα που υπόκεινται επεξεργασία ή από το χρόνο εκτέλεσης για να παρέχεται η καλύτερη δυνατή προστασία σε επίπεδο κυκλώματος. Για την αντιμετώπιση της διακύμανσης της ισχύος, θα πρέπει να χρησιμοποιηθούν διαφορετικές τεχνολογίες, όπως η δυναμική και η διαφορική λογική.

Σε πειράματα που διεξήχθησαν από τους Verbauwhede & Schaumont (2007), τα προηγμένα πρότυπα κρυπτογράφησης που χρησιμοποιούν δυναμική και διαφορική λογική κυματομορφών ισχύος παρέμειναν ασφαλή. Για να αντιμετωπιστούν οι επιθέσεις πλάγιων καναλιών στο επίπεδο της μικροαρχιτεκτονικής, οι συγγραφείς πρότειναν να εξισορροπηθούν εντολές – if and else – για να χρησιμοποιείται η ίδια ποσότητα χρόνου και ισχύος κατά την εκτέλεση. Η δομή των μικροεπεξεργαστών που παρέχουν πιθανές πληροφορίες πλευρικών καναλιών θα πρέπει να λαμβάνονται σοβαρά υπόψη. Οι συγγραφείς πρότειναν επίσης να χρησιμοποιηθούν ασφαλείς τεχνικές αλγορίθμων για να αντιμετωπίζονται επιθέσεις πλαϊνών καναλιών σε χαμηλότερα επίπεδα αφαιρετικής σχεδίασης.

Οι Deng, Chan & Suh (2009) πρότειναν μια μέθοδο για τον έλεγχο του υλικού ελέγχοντας απευθείας όλες τις λεπτομέρειες της εφαρμογής του κυκλώματος σε χαμηλό επίπεδο. Τα χαρακτηριστικά μικροαρχιτεκτονικής ενός ασφαλούς μικροεπεξεργαστή υψηλού επιπέδου είναι πολύπλοκα και μοναδικά για κάθε μοντέλο. Έτσι, ένας ασφαλής επεξεργαστής επικυρώνεται από το αποτέλεσμα που θα φέρει σε έναν συγκεκριμένο έλεγχο και μέσα σε ένα προκαθορισμένο χρονικό περιθώριο. Η μοναδική και σωστή απάντηση στον κάθε έλεγχο βασίζεται αποκλειστικά στις δραστηριότητες του συγκεκριμένου εσωτερικού μικροαρχιτεκτονικού μηχανισμού του επεξεργαστή.

Οι Deng, Chan & Suh (2009) υπογραμμίζουν πως δεν υφίσταται το ενδεχόμενο της παραβίασης του απορρήτου και των προσωπικών δεδομένων, αφού το αποτέλεσμα που θα φέρει σε έναν συγκεκριμένο έλεγχο και μέσα σε ένα προκαθορισμένο χρονικό περιθώριο το

κύκλωμα εξαρτάται από το μοντέλο που κατασκευάστηκε από τον επεξεργαστή και όχι από τον συγκεκριμένο επεξεργαστή υπό έλεγχο.

Επιπλέον, οι Deng, Chan & Suh (2009) έδειξαν ότι οι μικρές διαφορές στην μικροαρχιτεκτονική οδηγούν σε σημαντικές αποκλίσεις στο αποτέλεσμα που θα φέρει τελικά το κύκλωμα στη διαδικασία ελέγχου. Η δουλειά τους βασίζεται κυρίως στα πλεονεκτήματα που αφορούν την ταχύτητα του πραγματικού επεξεργαστή και όχι σε προσομοιώσεις που επιχειρούν να παραπλανήσουν τον επεξεργαστή. Επιπροσθέτως, το χρονικό όριο που τίθεται για να παραχθεί το αποτέλεσμα του κυκλώματος που τίθεται υπό έλεγχο εξασφαλίζει και την ανθεκτικότητα, ένα στοιχείο που δεν εξασφαλίζεται στις προσεγγίσεις με μοντέλα προσομοίωσης, σύμφωνα με τα λόγια των συγγραφέων.

Η προσέγγιση των Bloom, Narahari & Simha (2009) εισήγαγε έναν μηχανισμό ανίχνευσης δραστηριότητας που προέρχεται από κακόβουλες τροποποιήσεις υλικού. Η προσέγγιση αυτή, έκανε χρήση τόσο ένα κύκλωμα παρακολούθησης και ελέγχου του υλικού όσο και μια εφαρμογή κανονικού λειτουργικού συστήματος.

Οι επιθέσεις που βασίζονται σε κακόβουλες τροποποιήσεις υλικού μπορούν είτε να ενεργοποιηθούν εσωτερικά, είτε εξωτερικά και μπορεί να προκαλέσουν μια σειρά από αρνητικά αποτελέσματα για το σύστημα και το χρήστη. Παραδείγματα τέτοιων αποτελεσμάτων είναι η άρνηση εξυπηρέτησης, η κλιμάκωση των δικαιωμάτων από διεργασίες που κανονικά δε θα εκτελούνταν ή ακόμα και η διαρροή ευαίσθητων πληροφοριών.

Με βάση τα χαρακτηριστικά αυτά οι κακόβουλες τροποποιήσεις υλικού μπορούν να ανιχνευθούν με ανάλυση αποτυχιών και έλεγχο υλικού ή ανάλυση πλευρικών καναλιών. Οι Bloom, Narahari & Simha (2009) επικεντρώθηκαν σε επιθέσεις που έχουν ως αποτέλεσμα την άρνηση εξυπηρέτησης και την κλιμάκωση των δικαιωμάτων από διεργασίες.

Στην προσέγγισή τους, χρησιμοποίησαν όπως αναφέρθηκε πιο πάνω δύο μέσα:

1. Ένα κύκλωμα παρακολούθησης και ελέγχου υλικού για την αποτελεσματική εκτέλεση των ελέγχων
2. Ένα κανονικό λειτουργικό σύστημα το οποίο ήταν υπεύθυνο για την παραγωγή των ελέγχων.

Η υλοποίηση που εισήγαγαν στο έργο τους οι Bloom, Narahari & Simha (2009) αποτελούνταν από ένα κύκλωμα το οποίο περιελάμβανε έναν χρονοδιακόπτη, μια μνήμη RAM, έναν απλό επεξεργαστή και μια διευθυνσιοδοτούμενη μνήμη.

Στο κύκλωμα αυτό, λοιπόν, εκτελούνταν δύο έλεγχοι με τον πρώτο έλεγχο να είναι ο έλεγχος δραστηριότητας και ο δεύτερος να είναι ο έλεγχος προστασίας μνήμης. Παρακάτω περιγράφονται οι δύο έλεγχοι.

1. Έλεγχος δραστηριότητας. Οι έλεγχοι δραστηριότητας είναι ψευδοτυχαίες μη κρυπτογραφημένες προσπελάσεις στη μνήμη που εμποδίζουν επιθέσεις ή αλλιώς τροποποιήσεις που βασίζονται σε στοιχεία προβλέψεων, καθυστέρησης και επαναλήψεις.
2. Έλεγχος προστασίας μνήμης. Στον έλεγχο αυτό προτάθηκαν δύο λύσεις για την προστασία της μνήμης: μια απλή λύση και μια λύση που χρησιμοποιεί ένα λειτουργικό σύστημα που εκτελείται σε πραγματικό χρόνο. Η απλή λύση προγραμματίζει περιοδικά μια διαδικασία που προσπαθεί συνεχώς να διαβάζει τη μνήμη του πυρήνα. Ωστόσο, η διαδικασία είναι χρονοβόρα για το σύστημα. Από την άλλη η λύση που χρησιμοποιεί ένα λειτουργικό σύστημα που εκτελείται σε πραγματικό χρόνο είναι απαραίτητη για τον έλεγχο της χρονικής διάρκειας που εκτελείται η διαδικασία ελέγχου, η οποία δημιουργείται ως εργασία πραγματικού χρόνου (real-time task), η οποία απαιτείται συχνά αλλά είναι λιγότερο χρονοβόρα.

Μια ακόμα προσέγγιση με βάση την αρχιτεκτονική είναι αυτή που πρότειναν οι McIntyre et al. (2009) στην οποία χρησιμοποίησαν πολυπύρηνα συστήματα. Μέσω των πολυπύρηνων συστημάτων, δίνεται η δυνατότητα ταυτόχρονης εκτέλεσης της ίδιας διαδικασίας ελέγχου σε συνδυασμό με τη διαδικασία επαλήθευσης. Οι συγγραφείς εκμεταλλεύονται το ότι τα πολυπύρηνα συστήματα είναι από τη φύση τους περιττά. Έτσι, καθώς μέσω των ελέγχων αποκαλύπτεται η εμπιστοσύνη μεταξύ των πολλαπλών πυρήνων, θα μπορούσε να αξιοποιηθεί κατανεμημένος προγραμματισμός σε επίπεδο λογισμικού για να αποφευχθεί η χρήση των πυρήνων χαμηλής εμπιστοσύνης.

Αξίζει να γίνει και μια αναφορά στο έργο των Argawal et al. (2007) το οποίο εντοπίζεται ανάμεσα στα πρώτα που βασίζονται στην ιδέα της διαφοροποίησης των τσιπ που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού με τη σύγκριση του αποτυπώματος από την ανάλυση πλευρικών καναλιών.

Στο έργο τους, οι Argawal et al. (2007) αναλύουν τα κοινά στοιχεία που αφορούν τη συμπεριφορά διάφορων κακόβουλων τροποποιήσεων υλικού και καταδεικνύει τη σκοπιμότητα δημιουργίας λειτουργικών αποτυπωμάτων για μια οικογένεια κυκλωμάτων και τσιπ για την ανίχνευση κυκλωμάτων και τσιπ που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού.

Για να επιτευχθεί αυτό, οι συγγραφείς χρησιμοποίησαν ένα μοντέλο θορύβου που ήταν υπεύθυνο για την κατασκευή του αποτυπώματος για μια οικογένεια κυκλωμάτων αλλά και μια επέκταση που ήταν ουσιαστικά ένα υπολογιστικό εργαλείο για τον διαχωρισμό της τυχαιότητας και της χρονικής μεταβολής μιας τυχαίας διεργασίας.

Η προσέγγισή των Argawal et al. (2007) ήταν ιδιαίτερα χρήσιμη στην ανίχνευση κακόβουλων τροποποιήσεων υλικού όταν το κύκλωμα που είχε υποστεί κάποια τροποποίηση υλικού ήταν αρκετά μεγάλο σε σύγκριση με ολόκληρη την περιοχή του τσιπ και η διακύμανση των διεργασιών χαμηλή. Επίσης, εξασφαλίστηκε ότι η κακόβουλη τροποποίηση υλικού θα ανιχνευόταν γρήγορα ακόμα και όταν το μέγεθος της τροποποίησης ήταν μικρό σε σχέση με το τσιπ και υπήρχε μεγάλη διακύμανση διεργασιών.

3.5 Σύγχρονες αναλύσεις

Ο λόγος ύπαρξης της ενότητας αυτής έγκειται στο γεγονός πως τα τελευταία χρόνια εντοπίζονται νέες τεχνικές που προτείνουν νέες προσεγγίσεις στις ήδη υπάρχουσες που αφορούν την ανίχνευση μιας κακόβουλης τροποποίησης υλικού.

Πρώτη προσέγγιση που παρουσιάζεται είναι αυτή των Kulkarni, Pino & Mohsenin (2016). Στο έργο τους οι συγγραφείς υπογραμμίζουν πως οι επιστήμονες που ασχολούνται με το φαινόμενο της κακόβουλης τροποποίησης υλικού αντιμετωπίζουν προκλήσεις. Μια πρόκληση είναι η επιβάρυνση του υλικού από τα όλο και αυξανόμενα μέτρα ασφαλείας. Επίσης, πρόκληση είναι και η εξασφάλιση ατόφιων σχεδίων τσιπ μέσω της αποφυγής επιθέσεων κατά το σχεδιασμό, οι οποίες μάλιστα επιθέσεις συμβαίνουν και σε πραγματικό χρόνο.

Για την αντιμετώπιση, λοιπόν της δεύτερης πρόκλησης, οι συγγραφείς προτείνουν μια διαδικτυακή προσέγγιση που βασίζεται σε πραγματικό χρόνο για την ασφάλεια πολυπύρηνων σχεδίων.

Προκειμένου να αποφευχθούν απροσδόκητες επιθέσεις, στην προσέγγιση των Kulkarni, Pino & Mohsenin (2016) οι πολλαπλοί πυρήνες παρέχουν ανατροφοδότηση σε ηλεκτρονικό αλγόριθμο εκμάθησης με βάση τις βασικές πληροφορίες των πυρήνων καθώς και τη συμπεριφορά τους σε εισερχόμενα πακέτα δεδομένων. Η προσέγγιση χαρακτηρίζεται ως εκμάθησης γιατί χρησιμοποιεί τα δεδομένα των πυρήνων για να μάθει τη συμπεριφορά τους. Ο αλγόριθμος εκμάθησης που τρέχει ανανεώνεται σε πραγματικό χρόνο ανάλογα με τη μεταφορά των δεδομένων από τους πυρήνες.

Για να μειωθεί η πολυπλοκότητα του υλικού, ο αλγόριθμος εκπαιδεύεται εκτός σύνδεσης χρησιμοποιώντας ένα σύνολο δεδομένων προερχόμενο από το πρωτότυπο σχέδιο του τσιπ υπό έλεγχο. Τα δεδομένα προκύπτουν από τυχαία τοποθέτηση κακόβουλων τροποποιήσεων σε πακέτα. Οι τροποποιήσεις βασίζονται σε επιθέσεις παραβιάσεων πυρήνων και διαδρομών και ο χαρακτηρισμός τους βασίζεται στη συμπεριφορά του υλικού.

Το σύνολο δεδομένων που προέρχεται από το πρωτότυπο σχέδιο του τσιπ υπό έλεγχο διαθέτει χιλιάδες εγγραφές από τα αποτελέσματα ελέγχων στο πρωτότυπο τσιπ. Επίσης, αποτελείται από τρία λογικά μπλοκ, δηλαδή τη λογικό μπλοκ πρόβλεψης, το λογικό μπλοκ ελέγχου ανατροφοδότησης και το λογικό μπλοκ ανανέωσης του μοντέλου (Kulkarni, Pino & Mohsenin, 2016).

Το λογικό μπλοκ πρόβλεψης χρησιμοποιείται για την πρόβλεψη του αποτελέσματος ελέγχου, η οποία πρόβλεψη υπολογίζει το αποτέλεσμα με βάση θετικά και αρνητικά μοντέλα αλλά και μια παράμετρο που ορίζει τα όρια των θετικών και αρνητικών μοντέλων.

Το λογικό μπλοκ ελέγχου ανατροφοδότησης ουσιαστικά είναι υπεύθυνο για την απόφαση σχετικά με την ενημέρωση του μοντέλου. Αποτελείται από τρία στοιχεία, τα οποία συγκρίνουν ταυτόχρονα την είσοδο ανατροφοδότησης στους πυρήνες με την προβλεπόμενη έξοδο. Σε περίπτωση λανθασμένης πρόβλεψης, το λογικό μπλοκ ελέγχου ανατροφοδότησης καλεί το λογικό μπλοκ ανανέωσης του μοντέλου. Το μπλοκ αυτό είναι υπεύθυνο για την αλλαγή του βάρους των ελέγχων που εκτελούνται.

Επίσης, στην προσέγγιση των Kulkarni, Pino & Mohsenin (2016) ο αλγόριθμος εκμάθησης είναι ήδη ενημερωμένος και εκπαιδευμένος να ανιχνεύει δύο βασικές κακόβουλες τροποποιήσεις υλικού. Ο έλεγχος της απόδοσης γινόταν με την αποστολή πακέτων δεδομένων χωρίς κάποια κακόβουλη τροποποίηση υλικού και έπειτα γινόταν απρόσμενα μια αποστολή με κάποια κακόβουλη τροποποίηση υλικού και όσο ο αλγόριθμος εκμάθησης βρισκόταν σε λειτουργία.

Τα αποτελέσματα των προσομοιώσεων των Kulkarni, Pino & Mohsenin (2016) έδειξαν πως ο αλγόριθμος εκμάθησης που πρότειναν έχει 8% υψηλότερη συνολική ακρίβεια ανίχνευσης κακόβουλων τροποποιήσεων και κατά μέσο όρο 3% υψηλότερη ακρίβεια για απροσδόκητες επιθέσεις σε σύνολο 1000 ελέγχων σε σχέση με αλγόριθμους εποπτικής μηχανικής μάθησης (Supervised Machine Learning). Για το προτεινόμενο πλαίσιο ανίχνευσης κακόβουλων τροποποιήσεων υλικού που βασίζεται στην ανατροφοδότηση των πυρήνων χρησιμοποιώντας μια προσαρμοσμένη αρχιτεκτονική πολλών πυρήνων που είναι ενσωματωμένη στον αλγόριθμο ηλεκτρονικής μάθησης χρησιμοποιήθηκε ειδικός αλγόριθμος που εκτελείται σε πολυπύρηνα σχέδια. Τα αποτελέσματα της εφαρμογής των

δρομολογίων έδειξαν ότι για την ασφάλεια της αρχιτεκτονικής των πολυπύρηνων σχεδίων απαιτούνται 4 επιπλέον κύκλοι για την ολοκλήρωση της μεταφοράς των δεδομένων. Τέλος, παρατηρήθηκε και μείωση της επιφάνειας αλλά και μείωση της καθυστέρησης.

Μια δεύτερη προσέγγιση προτείνουν οι Kulkarni, Pino & Mohsenin (2016) που αναφέρεται και πάλι σε ανίχνευση κακόβουλων τροποποιήσεων λογισμικού σε πραγματικό χρόνο. Σε αυτή την προσέγγιση οι συγγραφείς πρότειναν μια αρχιτεκτονική ανίχνευσης κακόβουλων τροποποιήσεων υλικού για ένα κατά παραγγελία πολυπύρηνο τσιπ. Η προσέγγιση της ανίχνευσης βασίστηκε σε τεχνικές και ειδικούς αλγορίθμους μηχανικής μάθησης.

Το σύνολο δεδομένων που χρησιμοποιούνται στη διαδικασία ελέγχου δημιουργείται με βάση τη συμπεριφορά του τσιπ με πολυπύρηνα κυκλώματα κάτω από κανονικές ρυθμίσεις αλλά και κάτω από συνθήκες που υποδηλώνουν πως το τσιπ έχει υποστεί κάποια κακόβουλη τροποποίηση υλικού. Οι έλεγχοι, επίσης, δίνουν βάρος στην ανίχνευση κακόβουλων τροποποιήσεων υλικού που βασίζονται στην επικοινωνία.

Όπως είναι αναμενόμενο, το να συλλεχθούν όσο πιο σχετικά δεδομένα με βάση την ανάλυση συμπεριφοράς του υλικού είναι το πρώτο και σημαντικότερο βήμα αυτής της έρευνας. Οι συγγραφείς επιμένουν πως ένα καλό σύνολο δεδομένο πρέπει να συμβάλει στην κλάση. Δηλαδή να υπάρχει υψηλή συσχέτιση μεταξύ χαρακτηριστικού και κλάσης και όχι μεταξύ χαρακτηριστικού και χαρακτηριστικού. Η σωστή επιλογή των χαρακτηριστικών θα βοηθήσει και στην αύξηση της ακρίβειας ανίχνευσης κακόβουλων τροποποιήσεων υλικού αλλά και στην υλοποίηση του υλικού.

Η διαγραφή άσχετων χαρακτηριστικών στην προσέγγιση των Kulkarni, Pino & Mohsenin (2016) μειώνει το σύνολο των δεδομένων μειώνοντας έτσι την πολυπλοκότητα του υλικού και τη χρήση της μνήμης. Έτσι, τα χαρακτηριστικά που επιλέχθηκαν για την ανίχνευση των κακόβουλων τροποποιήσεων υλικού ήταν ο αριθμός της πηγής του πυρήνα, ο αριθμός του προορισμού του πυρήνα, η διαδρομή μεταφοράς πακέτων και η απόσταση.

Ο αλγόριθμος μηχανικής μάθησης που χρησιμοποιήθηκε στην προσέγγιση των Kulkarni, Pino & Mohsenin (2016) είναι αποτελεσματικός και παρέχει καλή απόδοση κατά τη χρήση του τόσο για εργασίες ταξινόμησης όσο και παλινδρόμησης. Ο αλγόριθμος προσαρμόζει τα δεδομένα που του παρέχονται (το σύνολο δεδομένων δηλαδή που οι συγγραφείς αναφέρουν) τα οποία περιέχουν ένα σύνολο χαρακτηριστικών και στη συνέχεια δημιουργεί ένα μοντέλο ελέγχου που προβλέπει τα αποτελέσματα με βάση τα αρχικά δεδομένα.

Η διαδικασία που εκτελεί ο αλγόριθμος μηχανικής μάθησης αποτελείται από δύο στάδια.

1. Πρώτο στάδιο είναι η φάση της μάθησης όπου ουσιαστικά θέτει τα όρια στα οποία θα κινηθεί με βάση τα χαρακτηριστικά που του δίνονται και έπειτα ξεχωρίζει με βέλτιστο τρόπο τις κλάσεις.
2. Δεύτερο στάδιο είναι και το ζουμί της υπόθεσης που όπως λέει και το όνομά του (στάδιο πρόβλεψης) χρησιμοποιούνται τα δεδομένα από την πρώτη φάση για να προβλεφθεί η κλάση του τσιπ που εξετάζεται.

Στα αποτελέσματα, βρέθηκε πως ο αλγόριθμος μηχανικής μάθησης που χρησιμοποιήθηκε έχει ακρίβεια ανίχνευσης από 94% έως 97%. Οι έλεγχοι έγιναν με πλαίσιο πολυπύρηνης αρχιτεκτονικής και ενεργοποίησης των κακόβουλων τροποποιήσεων υλικού με βάση δύο διαφορετικές συνθήκες.

Συνεχίζοντας, αξίζει να γίνει μια αναφορά στην προσέγγιση των Reshma, Priyatharishini & Devi (2019) η οποία βασίζεται όπως και άλλες που έχουν αναφερθεί στη μηχανική μάθηση. Αναλυτικότερα, η προσέγγισή τους συνεισφέρει στην ανίχνευση μιας κακόβουλης τροποποίησης υλικού σε επίπεδο πύλης και μέσω αλγορίθμων μηχανικής μάθησης. Σύμφωνα με τα λόγια των συγγραφέων, στην προσέγγιση μπορούν εύκολα να εντοπιστούν μη κακόβουλα τροποποιημένοι κόμβοι και κόμβοι που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού με βάση την πιθανότητα ελέγχου (controllability probability) και την πιθανότητα μετάβασης (transition probability) ενός κυκλώματος που έχει υποστεί κάποια τροποποίηση υλικού. Τα χαρακτηριστικά των δύο αυτών πιθανοτήτων (των τιμών τους στην ουσία) που αφορούν σε κόμβους που έχουν υποστεί κακόβουλη τροποποίηση υλικού εμφανίζουν μεγάλη απόσταση μεταξύ των συστάδων από τους κόμβους που δεν έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Έτσι, είναι εύκολο να διαχωριστούν οι κόμβοι ως κόμβοι που έχουν υποστεί κακόβουλη τροποποίηση υλικού και μη.

Από το κύκλωμα υπό εξέταση, εξάγονται οι τιμές των πιθανοτήτων ελέγχου και μετάβασης ως χαρακτηριστικά κακόβουλης τροποποίησης υλικού με τη χρήση ενός αλγορίθμου βαθιάς μάθησης (deep learning algorithm) και χωρίζονται σε συστάδες μέσω της μεθόδου k – μέσων όρων που έχει αναφερθεί και νωρίτερα. Επίσης, δε χρειάζεται στη διαδικασία να γίνει χρήση κάποιου άλλου κυκλώματος προτύπου όπως σε άλλες προσεγγίσεις που έχουν αναφερθεί (Reshma, Priyatharishini & Devi, 2019).

Η πιθανότητα ελέγχου και οι τιμές της μπορούν να χρησιμοποιηθούν για να διακριθούν οι κόμβοι που δεν είναι εύκολο να εξεταστούν. Για παράδειγμα ένα σήμα που έχει χαμηλή δραστηριότητα μπορεί να έχει υψηλή δυνατότητα ελέγχου. Οι τιμές της πιθανότητας ελέγχου κυμαίνονται από το 1 έως το άπειρο και προκύπτουν από τις τιμές εισόδου προς τις τιμές εξόδου.

Οι κόμβοι με υψηλή τιμή πιθανότητας ελέγχου είναι πιο κατάλληλοι για την εισαγωγή μια κακόβουλης τροποποίησης υλικού σε αυτούς επειδή η πιθανότητα ανίχνευσης ενός τέτοιου κόμβου είναι πολύ χαμηλή και είναι πολύ δύσκολο να ελεγχθούν εκείνοι οι συγκεκριμένοι κόμβοι.

Η πιθανότητα μετάβασης παίζει επίσης σημαντικό ρόλο στην εισαγωγή μιας κακόβουλης τροποποίησης υλικού σε ένα κόμβο. Οι κόμβοι με χαμηλή πιθανότητα μετάβασης είναι ευαίσθητοι για την ενεργοποίηση τόσο της κακόβουλης τροποποίησης υλικού αλλά και του φόρτου της. Χαμηλές τιμές στην πιθανότητα μετάβασης υποδεικνύουν ότι σπάνια ενεργοποιούνται και όπως είναι αναμενόμενο οι κακόβουλες τροποποιήσεις υλικού είναι συχνά τοποθετημένες σε κόμβους που δεν χρησιμοποιούνται ή ενεργοποιούνται συχνά (Reshma, Priyatharishini & Devi, 2019).

Ο αλγόριθμος βαθιάς μάθησης, διαμορφώνεται για την εξαγωγή των χαρακτηριστικών των κακόβουλων τροποποιήσεων υλικού. Οι έξοδοι και οι τιμές των πιθανοτήτων ελέγχου και μετάβασης λαμβάνονται ως είσοδος στον αλγόριθμο βαθιάς μάθησης. Έπειτα, ο αλγόριθμος παράγει ελέγχους για το κύκλωμα ελαχιστοποιώντας την τιμή σφάλματος

Οι τιμές της πιθανότητας ελέγχου όλων των κόμβων σε ένα κύκλωμα λαμβάνονται ως είσοδος σε έναν αυτόματο κωδικοποιητή του αλγορίθμου και έτσι παράγουν ομαλοποιημένες τιμές που αντιστοιχούν στον έλεγχο εισόδου που έχει παράγει ο αλγόριθμος. Στη συνέχεια, τα δεδομένα χωρίζονται σε συστάδες με τη χρήση k - μέσων όρων και η τιμή k μπορεί να πάρει 2 τιμές. Η τιμή 1 αναπαριστά κόμβους με υψηλές τιμές ελέγχου οι οποίοι έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Η τιμή 2 αναπαριστά κόμβους με χαμηλές τιμές ελέγχου οι οποίοι δεν έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού. Τέλος, ο αλγόριθμος υπολογίζει την απόσταση μεταξύ των αρχικών δεδομένων και των δεδομένων έπειτα από το διαχωρισμό σε συστάδες. Έτσι προκύπτουν, τελικά, οι κόμβοι που έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού και οι κόμβοι που δεν έχουν υποστεί κάποια κακόβουλη τροποποίηση υλικού (Reshma, Priyatharishini & Devi, 2019).

Ως προς τα αποτελέσματα, αποδείχθηκε πως η προτεινόμενη μέθοδος μπορεί να εντοπίσει όλους τους κόμβους που έχουν μολυνθεί από μια κακόβουλη τροποποίηση υλικού σε λιγότερο από 6 δευτερόλεπτα με απόλυτη ακρίβεια ανίχνευσης. Πρέπει ωστόσο, να σημειωθεί πως παρόλο που οι συγγραφείς δεν το κάνουν ιδιαίτερα φανερό, η ανίχνευση αφορά κακόβουλες τροποποιήσεις υλικού οι οποίες εντάσσονται στην κατηγορία αυτών που είναι μόνιμα ενεργοποιημένες.

Μια επιπλέον προσέγγιση πρόσθεσαν στο έργο τους οι Chen, Guo, Wang, Li & Lu (2019) το οποίο δεν είναι ακόμα επίσημα δημοσιευμένο στο επιστημονικό περιοδικό «IEEE Internet of Things Journal» αλλά είναι σε κατάσταση αποδοχής από το περιοδικό και αναμένεται η δημοσίευση του.

Η προσέγγιση αφορά συγκεκριμένα κυκλώματα, που ονομάζονται ως επιτόπια συστοιχία προγραμματιζόμενων πυλών (Field Programmable Gate Array - FPGA) και θα γίνει πρώτα μια μικρή αναφορά σε αυτά για να εξοικειωθεί ο αναγνώστης. Το κύκλωμα λοιπόν, αυτό, ένα ολοκληρωμένο κύκλωμα σχεδιασμένο για να διαμορφώνεται από έναν πελάτη ή έναν σχεδιαστή μετά την κατασκευή του – γι' αυτό και ο όρος Field Programmable. Ο προγραμματισμός του κυκλώματος βασίζεται σε γλώσσες HDL που έχουν αναφερθεί πιο πάνω. Τέλος, τα κυκλώματα αυτά περιέχουν μια σειρά προγραμματιζόμενων πυλών που μπορούν να διαμορφωθούν έτσι ώστε να εκτελούν πολύπλοκες συνδυαστικές λειτουργίες ή και πιο απλές (Sadrozinski & Wu, 2016).

Η προσέγγιση, λοιπόν των Chen et al., (2019), εστιάζει ιδιαίτερα στον τύπο αυτό των κυκλωμάτων γιατί χρησιμοποιείται με μεγάλη συχνότητα στο σχεδιασμό και τη χρήση των σημερινών έξυπνων συσκευών και όπως και όλα τα κυκλώματα, έτσι και αυτά απειλούνται από τον κίνδυνο της κακόβουλης τροποποίησης υλικού. Γι' αυτό, οι συγγραφείς θεωρούν άμεση την ανάγκη ανίχνευσης FPGA κυκλωμάτων με κακόβουλες τροποποιήσεις υλικού για να βελτιωθούν τα επίπεδα ασφάλειάς τους.

Για να επιτευχθεί αυτός ο στόχος, η προσέγγιση βασίζεται σε κάποια βήματα. Πρώτο βήμα είναι η παρουσίαση ενός πειραματικού πλαισίου που βοηθά να συλλεχθεί η ηλεκτρομαγνητική ακτινοβολία που εκπέμπεται από το FPGA κύκλωμα.

Στο βήμα αυτό, πρώτα σαρώνεται η επιφάνεια ενός μη προγραμματισμένου FPGA κυκλώματος που είναι ενεργοποιημένο, χρησιμοποιώντας έναν αισθητήρα ηλεκτρομαγνητισμού υψηλής ευαισθησίας. Με αυτόν τον τρόπο, διαμορφώνεται ένα αναλυτικό προφίλ ηλεκτρομαγνητισμού που αφορά όλο το FPGA κύκλωμα. Στη συνέχεια το προφίλ αυτό χρησιμοποιείται για τον έλεγχο του FPGA κυκλώματος αλλά αυτή τη φορά με είσοδο το 0. Έπειτα, εκτελείται μια ακόμα σάρωση του κυκλώματος. Έπειτα, το βήμα αυτό επαναλαμβάνεται για να δημιουργηθεί ένα δείγμα από σαρώσεις (Chen et al., 2019).

Στη συνέχεια, προτείνεται το βήμα που αναγνωρίζει την όποια κακόβουλη τροποποίηση υλικού μέσω των χαρακτηριστικών που εξάγονται από τα ληφθέντα ηλεκτρομαγνητικά ίχνη. Στο βήμα αυτό, διακρίνονται αυτόματα τα FPGA κυκλώματα που έχουν υποστεί κάποια τροποποίηση υλικού και αυτά που δεν έχουν υποστεί κάποια τροποποίηση υλικού. Η διάκριση γίνεται μέσω ειδικού νευρωνικού δικτύου και βασίζεται στο δείγμα των

σαρώσεων που έχει δημιουργηθεί στο προηγούμενο βήμα. Επίσης, χρησιμοποιούνται στατιστικές μέθοδοι για τη βελτίωση της ανίχνευσης κακόβουλων τροποποιήσεων υλικού.

Τα αποτελέσματα, των ελέγχων των Chen et al., (2019) απέδειξαν πως ότι η προσέγγισή είναι έγκυρη στην ανίχνευση των κακόβουλων τροποποιήσεων υλικού στα FPGA κυκλώματα. Συγκεκριμένα, τα ποσοστά επιτυχίας στην ανίχνευση κακόβουλων τροποποιήσεων υλικού που είναι μόνιμα ενεργοποιημένες έφτασαν το 100%, ενώ ταυτόχρονα το αντίστοιχο ποσοστό για τις κακόβουλες τροποποιήσεις που ενεργοποιούνται μέσω ενός εναύσματος έφτασαν το 92%. Επίσης, ο ρυθμός ανίχνευσης για τις διαδοχικές τροποποιήσεις υλικού έφτασε το 88%. Αυτό οφείλεται στο γεγονός ότι οι διαδοχικές τροποποιήσεις υλικού όχι μόνο τροποποιούν τη κατανομή του κυκλώματος, αλλά και απαιτούν περισσότερα σύρματα για να ελέγξουν επιπλέον πύλες. Ως εκ τούτου, οι διαδοχικές τροποποιήσεις υλικού προκαλούν περισσότερες αλλαγές στο προφίλ του ηλεκτρομαγνητισμού, οδηγώντας σε μεγαλύτερη πιθανότητα ανίχνευσης.

Με βάση τη μηχανική μάθηση, οι Han, Wang & Liu (2019) προτείνουν μια ακόμα σύγχρονη προσέγγιση στην ανίχνευση κακόβουλων τροποποιήσεων υλικού. Η προσέγγιση των συγγραφέων αναφέρεται στο επίπεδο μεταφοράς καταχωρητών (Register Transfer Level - RTL) κατά τη διαδικασία του σχεδιασμού.

Στο σχεδιασμό ψηφιακών κυκλωμάτων, το επίπεδο μεταφοράς καταχωρητών (RTL) είναι ένας αφαιρετικός σχεδιασμός ο οποίος μοντελοποιεί ένα σύγχρονο ψηφιακό κύκλωμα από την άποψη της ροής των ψηφιακών σημάτων (δεδομένων) μεταξύ των καταχωρητών και των λογικών λειτουργιών που εκτελούνται σε αυτά τα σήματα. Η αφαιρετικότητα σε επίπεδο μεταφοράς καταχωρητών χρησιμοποιείται σε γλώσσες (HDL) για τη δημιουργία παραστάσεων υψηλού επιπέδου για ένα κύκλωμα, από το οποίο μπορούν να προκύψουν αναπαραστάσεις χαμηλότερου επιπέδου και τελικά πραγματικές καλωδιώσεις. Ο σχεδιασμός σε επίπεδο μεταφοράς καταχωρητών είναι τυπική πρακτική στον σύγχρονο ψηφιακό σχεδιασμό (Biswal & Biswas, 2017).

Για να ανιχνευθεί, λοιπόν, με ακρίβεια κάποια κακόβουλη τροποποίηση υλικού κατά τη διαδικασία σχεδιασμού ενός κυκλώματος, η προσέγγιση των συγγραφέων χρησιμοποιεί μια μέθοδο ανίχνευσης με βάση τη μηχανική μάθηση στο επίπεδο μεταφοράς καταχωρητών.

Σε αυτή τη μέθοδο, τα χαρακτηριστικά του κυκλώματος εξάγονται από τους πηγαίους κώδικες του επιπέδου μεταφοράς καταχωρητών και κατασκευάζεται μια βάση δεδομένων χρησιμοποιώντας κυκλώματα σε μια βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού. Η βάση έχει σημαντική αξία αφού χρησιμοποιείται για να «εκπαιδεύσει» μέσω της μηχανικής

μάθησης ένα αποδοτικό μοντέλο ανίχνευσης με βάση έναν αλγόριθμο ανίχνευσης κακόβουλων τροποποιήσεων υλικού (Han, Wang & Liu, 2019).

Προκειμένου να επεκταθεί η βιβλιοθήκη των κακόβουλων τροποποιήσεων υλικού για την ανίχνευση νέων τύπων κακόβουλων τροποποιήσεων υλικού και την ενημέρωση του μοντέλου ανίχνευσης εγκαίρως, χρησιμοποιείται ένας μηχανισμός διακομιστή-πελάτη.

Έτσι, κατασκευάζεται ένας διακομιστής για την εκπαίδευση του μοντέλου ανίχνευσης βασισμένο σε μια βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού και έναν πελάτη για να γίνει η διαδικασία ανίχνευσης. Στον διακομιστή, τα χαρακτηριστικά του κυκλώματος εξάγονται από τους πηγαίους κώδικες του επιπέδου μεταφοράς καταχωρητών των κυκλωμάτων στη βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού. Στη συνέχεια, κατασκευάζονται 11 κυκλώματα με βάση του πηγαίους κώδικες τόσο από την οπτική της μονάδας όσο και του σήματος.

Έπειτα, όλες αυτές οι πληροφορίες χρησιμοποιούνται για την κατασκευή της βάσης δεδομένων εκπαίδευσης, έτσι ώστε ένα μοντέλο ανίχνευσης κακόβουλων τροποποιήσεων υλικού να εκπαιδεύεται με βάση τον αντίστοιχο αλγόριθμο ανίχνευσης τροποποιήσεων υλικού. Το μοντέλο χρησιμοποιείται στον πελάτη - κύκλωμα για την πρόβλεψη των κακόβουλων τροποποιήσεων υλικού. Τα χαρακτηριστικά που εξάγονται από τη διαδικασία, εισάγονται στο μοντέλο ανίχνευσης και η έξοδος εμφανίζει ύποπτα σήματα. Όταν ανακαλυφθεί ένας νέος τύπος κακόβουλης τροποποίησης υλικού, η βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού θα επεκταθεί και το μοντέλο ανίχνευσης θα επανεκκινηθεί στο διακομιστή και θα ενημερωθεί στον πελάτη – κύκλωμα (Han, Wang & Liu, 2019).

Από τις προσομοιώσεις προέκυψε πως η μέθοδος έφτασε το 100% σε ποσοστό επιτυχίας ανίχνευσης κακόβουλων τροποποιήσεων υλικού και γενικότερα η έρευνα έδειξε πως η ανίχνευση κακόβουλων τροποποιήσεων υλικού είναι ιδιαίτερα αποτελεσματική όταν χρησιμοποιεί τεχνικές μηχανικής μάθησης.

Μια παρόμοια προσέγγιση η οποία βασίστηκε και αυτή στη διαδικασία του σχεδιασμού και στο επίπεδο μεταφοράς καταχωρητών ήταν του Salmani (2018) όπου μοιράζεται πολλές ομοιότητες στη λογική σε σχέση με αυτή των Han, Wang & Liu (2019). Από τη μία και οι δύο προσεγγίσεις χρησιμοποιούν μια βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού για την ανίχνευση νέων τύπων κακόβουλων τροποποιήσεων υλικού και έναν αλγόριθμο ανίχνευσης κακόβουλων τροποποιήσεων υλικού.

Η όλη διαδικασία, από την άλλη, στην προσέγγιση του Salmani (2018), δε χρησιμοποιεί μηχανική μάθηση για να ανανεώσει τα δεδομένα που προκύπτουν από την ανίχνευση

κακόβουλων τροποποιήσεων υλικού, αλλά μένει στα δεδομένα που υπάρχουν ήδη στη βιβλιοθήκη κακόβουλων τροποποιήσεων υλικού που χρησιμοποιεί. Αντίθετα, στην προσέγγιση των Han, Wang & Liu (2019) χρησιμοποιείται και η λογική της μηχανικής μάθησης μέσω ενός εξυπηρετητή μέσω του οποίου επιτυγχάνεται η ανανέωση των δεδομένων που σχετίζονται με την ανίχνευση νέων κακόβουλων τροποποιήσεων υλικού.

Μια διαφορετική προσέγγιση με βάση την παρακολούθηση της θερμοκρασίας προτείνουν στο έργο τους οι Έλληνες Pyrgas, Pirpilidis, Panayiotarou & Kitsos (2017). Εκεί λοιπόν, παρουσιάζουν μια αποτελεσματική τεχνική για την ανίχνευση κακόβουλων τροποποιήσεων υλικού, με βάση τους αισθητήρες θερμότητας. Κάθε αισθητήρας αποτελείται από έναν ταλαντωτή δακτυλίων (Ring Oscillator) με τρεις μετατροπείς, έναν πολυπλέκτη ελέγχου (Control Multiplexer) και έναν μετρητή δακτυλίων. Εξαιτίας της χρήσης μεγάλου αριθμού αισθητήρων πάνω στο τσιπ ήταν απαραίτητη μια πολύ συμπαγής σχεδίαση αισθητήρων για να αποφευχθεί ένας μεγάλος αριθμός πρόσθετων πόρων υλικού. Έτσι, οι αισθητήρες τοποθετήθηκαν σε μια δομή 6x5 σε ίση απόσταση μεταξύ τους, προκειμένου να καλύψουν ολόκληρη την περιοχή της υλοποίησης προκαλώντας συνολική επιβάρυνση μόνο 1,9%.

Κάθε ταλαντωτής δακτυλίων ήταν συμπαγής για να κρατήσει την επιβάρυνση των αισθητήρων σε όσο το δυνατό χαμηλότερα επίπεδα. Επίσης, ήταν ευαίσθητος ιδιαίτερα στην ανίχνευση μεταβολών της θερμοκρασίας.

Οι αισθητήρες είχαν δύο βασικές λειτουργίες. Η μία λειτουργία καταγράφει τον αριθμό των ταλαντώσεων και στη συνέχεια μεταδίδει τη μέτρηση του αριθμού αυτού. Όταν ο ταλαντωτής δακτυλίων είναι ενεργοποιημένος το κύκλωμα ταλαντώνεται και η έξοδος του ταλαντωτή δακτυλίων τροφοδοτεί την είσοδο του μετρητή. Στη συνέχεια, ο μετρητής καταγράφει τον αριθμό των ταλαντώσεων (Pyrgas et al., 2017).

Έπειτα, υπολογίστηκαν οι μέσες τιμές μέτρησης για κάθε αισθητήρα, για αδρανείς και ενεργές κακόβουλες τροποποιήσεις υλικού, όπως και η διαφορά τους αλλά και η διαφορά θερμοκρασίας. Όταν ο αισθητήρας είναι πολύ μακριά από μια κακόβουλη τροποποίηση υλικού τότε ο αισθητής δεν είναι ευαίσθητος είτε η κακόβουλη τροποποίηση υλικού είναι ενεργή είτε αδρανής. Όταν όμως η κακόβουλη τροποποίηση υλικού βρίσκεται κοντά στον αισθητήρα, η τιμή μέτρησης όταν η κακόβουλη τροποποίηση υλικού είναι ενεργή είναι πολύ διαφορετική σε σύγκριση με την τιμή μέτρησης όταν η κακόβουλη τροποποίηση υλικού είναι αδρανής.

Έτσι, στην προσέγγιση των Pyrgas et al., (2017) απεικονίζονται σχηματικά με κλιμακούμενους χρωματισμούς οι διαφορές αυτές και μια κακόβουλη τροποποίηση υλικού

που προκαλεί μεγάλη διαφορά στις μετρήσεις παρουσιάζεται με διαφορετικό χρώμα. Ενδεικτικά, αναφέρεται πως στους πειραματισμούς οι μικρές διαφορές αντιστοιχούνταν σε μπλε χρώματα και όσο οι διαφορές στη θερμοκρασία μεγάλωναν τα χρώματα κινούνταν προς το κίτρινο και το κόκκινο. Έτσι, οι κακόβουλες τροποποιήσεις υλικού ξεχώριζαν αφού αντιστοιχούνταν σε κίτρινο χρώμα.

Τα αποτελέσματα από τα πειράματα έδειξαν πως η προτεινόμενη προσέγγιση των συγγραφέων απέδωσε καρπούς και αποδείχθηκε αποτελεσματική. Σύμφωνα με τα λόγια των συγγραφέων, μάλιστα, ήταν οι πρώτοι που είχαν χρησιμοποιήσει τέτοιου είδους αισθητήρες για την ανίχνευση κακόβουλων τροποποιήσεων υλικού.

Αξίζει, στο σημείο αυτό να γίνει μια αναφορά στην προσέγγιση των Zhao et al. (2018) η οποία βασίζεται στη θεωρία του χάους. Ενώ οι ερευνητές εργάζονται για την ενίσχυση των παραδοσιακών ελέγχων στα κυκλώματα και την ανάπτυξη νέων μεθόδων για την ανίχνευση κακόβουλων τροποποιήσεων υλικού, εξακολουθεί να υπάρχει η πιθανότητα μια κακόβουλη τροποποίηση υλικού να αποφύγει την ανίχνευση κατά τη διάρκεια του ελέγχου και να ενεργοποιηθεί μόλις χρησιμοποιηθεί το τσιπ.

Ένα σύστημα ανίχνευσης κακόβουλων τροποποιήσεων υλικού που λειτουργεί κατά το χρόνο εκτέλεσης. (runtime) θα μπορούσε να παρακολουθεί ένα κύκλωμα κατά τη διάρκεια που το ίδιο λειτουργεί και εκτελεί διεργασίες και έτσι να παρέχεται μια τελευταία γραμμή άμυνας. Ωστόσο, οι περισσότερες προσεγγίσεις που λειτουργούν κατά το χρόνο εκτέλεσης δεν είναι αποδοτικές λόγω της γενικής επιβάρυνσης που εισάγεται από το πρόσθετο υλικό ή από την υπολογιστική πολυπλοκότητα.

Στο γεγονός αυτό βασίστηκαν οι Zhao et al. (2018) και πρότειναν ένα μοντέλο ανίχνευσης που βασίζεται στο χρόνο εκτέλεσης και ξεπερνά τους προαναφερθέντες περιορισμούς. Εφαρμόζει τη θεωρία του χάους, η οποία έχει αποδειχθεί ότι είναι αποτελεσματική σε αρκετούς άλλους τομείς, για να χαρακτηρίσει δυναμικά δεδομένα και έτσι δίνεται η δυνατότητα να αναλυθούν και να ερμηνευθούν δεδομένα κατανάλωσης ισχύος είτε αυτά είναι χαοτικά είτε όχι.

Η προσέγγιση των Zhao et al. (2018) βασίζεται στο χάος, και δεν κάνει καμία παραδοχή σχετικά με τη στατιστική κατανομή της κατανάλωσης ρεύματος, γεγονός που καθιστά το μοντέλο εφαρμόσιμο στο χρόνο εκτέλεσης, δεδομένου ότι η κατανάλωση ενέργειας είναι πολύ δυναμική, καθώς εξαρτάται σε μεγάλο βαθμό από την εφαρμογή και τα δεδομένα. Η επιβάρυνση από το πρόσθετο υλικό, που είναι και η κύρια πρόκληση για τις προσεγγίσεις κατά τη διάρκεια του χρόνου εκτέλεσης, μειώνεται, αξιοποιώντας τους διαθέσιμους θερμικούς αισθητήρες που υπάρχουν στα περισσότερα σύγχρονα κυκλώματα.

Στη διαδικασία της προσέγγισης χρησιμοποιούνται πληροφορίες για την κατανάλωση ισχύος του συστήματος, που συλλέγονται από αισθητήρες θερμοκρασίας στο τσιπ, για την κατασκευή των μοντέλων ελέγχου. Επίσης, χρησιμοποιείται και μια ειδική μονάδα ακύρωσης ή μείωσης θορύβου που βοηθάει στο φιλτράρισμα των συλλεγόμενων δεδομένων ισχύος για να βελτιωθεί η ακρίβεια των μοντέλων ελέγχου. Η μονάδα ανίχνευσης παρακολουθεί τα δεδομένα κατανάλωσης ρεύματος με ειδικές λειτουργίες που βασίζονται στο χάος και συγκρίνει τα δεδομένα με τα όρια που παράγονται από τα μοντέλα ελέγχου για να ελέγξει εάν το σύστημα έχει οποιαδήποτε ανώμαλη συμπεριφορά.

Τα αποτελέσματα της προσέγγισης των Zhao et al. (2018) για την ανίχνευση κακόβουλων τροποποιήσεων απέδειξαν ότι το προτεινόμενο μοντέλο ξεπερνά τις τρέχουσες προσεγγίσεις κατά το χρόνο εκτέλεσης για την ανίχνευση κακόβουλων τροποποιήσεων υλικού, από την άποψη τόσο του ποσοστού ανίχνευσης, όσο και της υπολογιστικής πολυπλοκότητας.

Μια ακόμα προσέγγιση που αφορά αυτή τη φορά την αντίστροφη μηχανική είναι αυτή των Fyrbiak et al. (2018). Η προσέγγιση αφορά ένα συνδυασμό προτάσεων των συγγραφέων για την ανίχνευση κακόβουλων τροποποιήσεων υλικού.

Αρχικά, προτείνεται το HAL, ένα ολοκληρωμένο πλαίσιο αντίστροφης μηχανικής σε επίπεδο πύλης. Το πλαίσιο αυτό επιτρέπει την αυτοματοποίηση της αμυντικής σχεδίασης των κυκλωμάτων σε επίπεδο πύλης. Είναι εμπνευσμένο από τα σύγχρονα πρότυπα σχεδιασμού λογισμικού και αρχιτεκτονικής για να επιτευχθεί ένα καλό επίπεδο συντήρησης και επεκτασιμότητας. Αποτελείται από διάφορα χωριστά δομικά στοιχεία, το καθένα από τα οποία εστιάζει σε ένα σύνολο λογικών χαρακτηριστικών (Fyrbiak et al., 2018).

Το πλαίσιο λειτουργεί ως εξής:

α) Καλείται το πλαίσιο από το χρήστη στο επίπεδο πύλης

β) Το πλαίσιο χρησιμοποιεί έναν από τους συντακτικούς αναλυτές (parsers) για να μετατρέψει τους ελέγχους στην είσοδο των πυλών σε γραφική παράσταση

γ) Χρησιμοποιούνται διεργασίες για να αναλύσουν αυτόματα και ενδεχομένως για να χειριστούν τους ελέγχους στις εισόδους των πυλών

δ) Όλες οι αλλαγές στο γράφημα σε όλες τις λειτουργίες των διεργασιών συμπεριλαμβανομένων των μετα-δεδομένων που προστίθενται από τις διεργασίες ή τον χρήστη συγχρονίζονται με μια τοπική βάση δεδομένων

ε) Για την περαιτέρω υποστήριξη του χρήστη, όλη η ροή εργασίας είναι επίσης προσβάσιμη μέσω μιας διαδραστικής διεπαφής

στ) Όταν έχουν επεξεργαστεί επιτυχώς όλα τα πρόσθετα ζητούμενα και οι εργασίες, το γράφημα μπορεί να δημιουργηθεί από την αρχή για να συνθεθούν εκ νέου ανανεωμένες διεργασίες ελέγχου σε γλώσσα HDL.

Επίσης προτείνεται η τεχνική ανίχνευσης κακόβουλων τροποποιήσεων υλικού που ονομάζουν οι Fyrbiak et al. (2018) «ANGEL» η οποία είναι ικανή να ανιχνεύει αυτόματα κακόβουλες τροποποιήσεις υλικού. Η τεχνική αυτή βασίζεται σε προηγούμενες τελευταίες τεχνολογικές εξελίξεις στην ανίχνευση κακόβουλων τροποποιήσεων υλικού. Η τεχνική επικεντρώνεται στην ανίχνευση εισόδων που έχουν επηρεαστεί ελαφρώς για να εισαχθούν στο κύκλωμα κακόβουλες τροποποιήσεις υλικού και επιπλέον στη γειτνίαση των συνδυαστικών πυλών για κάθε πύλη.

Έτσι, αρχικά σκιαγραφούνται οι ελαφρώς επηρεασμένες είσοδοι και στη συνέχεια το γράφημα των εισόδων ενσωματώνεται στο γράφημα που προέκυψε από τη γειτνίαση των συνδυαστικών πυλών για κάθε πύλη. Έτσι, δεν υπάρχει η ανάγκη πρωτότυπου κυκλώματος ή τσιπ για σύγκριση των δεδομένων, γεγονός που είναι ευνοϊκό στην πράξη.

Επιπλέον, παρουσιάζονται αλγόριθμοι αντίστροφης μηχανικής για να αποτραπούν τυχόν προσπάθειες διαρροής των κρυπτογραφικών κλειδιών του κάθε τσιπ χωρίς να υπάρχει πρότερη γνώση για την εσωτερική λειτουργία του σχεδίου του τσιπ.

Στα αποτελέσματα της προσέγγισης των Fyrbiak et al. (2018) αποδείχθηκε πως αυτή επιτρέπει την ανάπτυξη προσαρμοσμένων εργαλείων για την αυτοματοποίηση της αντίστροφης μηχανικής, μιας διαδικασίας που είναι τόσο χρονοβόρα όσο και πολύπλοκη. Το πιο σημαντικό ήταν πως αποδείχθηκε ότι η ανάπτυξη αυτοματοποιημένων και προσαρμοσμένων εργαλείων για την αντίστροφη μηχανική και την ανίχνευση κακόβουλων τροποποιήσεων υλικού δεν είναι τόσο δύσκολη και απαιτητική όσο νομίζει κανείς. Αναλυτικότερα, ο χρόνος που απαιτείται για να αναστραφεί ο μηχανισμός και να αποδυναμωθεί κρυφά ένας σχεδιασμός κακόβουλης τροποποίησης υλικού είναι μόνο μερικές ώρες με τη βοήθεια της προσέγγισης και του πλαισίου HAL.

Οι προσεγγίσεις της επιστημονικής κοινότητας στην ανίχνευση κακόβουλων τροποποιήσεων υλικού είναι πολυπληθείς και συνεχώς παρουσιάζονται νέες και πιο σύγχρονες. Παράδειγμα είναι η προσέγγιση των Alsaiari & Gebali (2019) όπου στηρίζεται σε μια νέα τεχνική σχεδιασμού κυκλωμάτων και τσιπ μέσω αναπροσαρμόσιμων ελέγχων ισχυρισμών (Reconfigurable Assertions Checkers - RACs).

Ο σχεδιασμός με την τεχνική αυτή είναι ένα ισχυρό νέο παράδειγμα που διευκολύνει τη βελτίωση της ποιότητας του ηλεκτρονικού σχεδιασμού. Οι ισχυρισμοί είναι δηλώσεις που χρησιμοποιούνται για να περιγράψουν τις ιδιότητες του σχεδιασμού που μπορούν να

χρησιμοποιηθούν για να ελέγχουν ενεργά την ορθότητα καθ' όλη τη διάρκεια του κύκλου σχεδιασμού αλλά ακόμη και καθ' όλη τη διάρκεια του κύκλου ζωής του προϊόντος. Με την εμφάνιση δύο νέων γλωσσών, (PSL και SVA), οι ισχυρισμοί έχουν ήδη αρχίσει να βελτιώνουν την ποιότητα και την παραγωγικότητα της επαλήθευσης του ψηφιακού σχεδιασμού των κυκλωμάτων και των τσιπ (Chabot, Mazet & Pierre, 2015).

Με την εισαγωγή, όμως, των ισχυρισμών στη διαδικασία του σχεδιασμού των τσιπ, έχουν βρει τρόπο και οι κακόβουλες τροποποιήσεις υλικού να εισέλθουν στην όλη διαδικασία. Έτσι, οι Alsaiari & Gebali (2019) εισάγουν τους αναπροσαρμόσιμους ελέγχους ισχυρισμών για την ανίχνευση κακόβουλων τροποποιήσεων υλικού σε ένα σύστημα σε τσιπ (System on Chip - SoC). Στο έργο τους προτείνεται μια ροή σχεδιασμού ενός τροποποιημένου κυκλώματος για την ενσωμάτωση αναπροσαρμόσιμων ελέγχων ισχυρισμών (RAC) σε ένα σύστημα σε τσιπ (SoC). Αναπτύσσεται επίσης μια ευέλικτη αρχιτεκτονική αναπροσαρμόσιμων ελέγχων ισχυρισμών για την εφαρμογή διαφορετικών τύπων ισχυρισμών.

Στο τσιπ υπό έλεγχο η προσέγγιση των συγγραφέων υποστηρίζει οποιαδήποτε Boolean έκφραση (άλλωστε οι εκφράσεις αυτές είναι που χρησιμοποιούνται και στους ελέγχους ισχυρισμών) αφού εξαρτάται από τις απαιτήσεις των ελέγχων ισχυρισμών που απαιτούνται για την ανίχνευση μιας κακόβουλης τροποποίησης υλικού.

Ανάλογα με το κάθε σύστημα σε τσιπ (SoC) και αν γίνεται έλεγχος για άρνηση εξυπηρέτησης (DoS) που προκαλείται από μια κακόβουλη τροποποίηση υλικού, ο ισχυρισμός ελέγχει εάν υπάρχει έγκυρη επιβεβαίωση για μια αίτηση διαύλου στο σύστημα. Αν γίνεται έλεγχος για διαρροή πληροφοριών ο ισχυρισμός επαληθεύει ότι μια αίτηση εγγραφής δεν αλλάζει στην αίτηση ανάγνωσης.

Οι Alsaiari & Gebali (2019) σημειώνουν πως εξετάζονται μόνο οι εντολές "always", "never", "eventually", "until", και "next". Η εντολή "before" δεν υποστηρίζεται και η εντολή "abort" χρησιμοποιείται μόνο εάν το σήμα της "abort" εντολής πρόκειται να αντιμετωπιστεί ως ένας τελεστής, διαφορετικά θα μπορούσε να αποκρύψει την ύπαρξη μιας κακόβουλης τροποποίησης υλικού.

Η χρήση αναπροσαρμόσιμων ελέγχων ισχυρισμών για την ανίχνευση των κακόβουλων τροποποιήσεων υλικού έγινε σε δύο μελέτες περίπτωσης προηγμένης αρχιτεκτονικής μικροελεγκτών. Η μία αφορούσε μια κακόβουλη τροποποίηση υλικού που οδηγούσε σε άρνηση εξυπηρέτησης (Denial of Service) και η άλλη αφορούσε μια κακόβουλη τροποποίηση υλικού που οδηγούσε σε διαρροή πληροφοριών. Και στις δύο περιπτώσεις, οι αναπροσαρμόσιμοι έλεγχοι ισχυρισμών ήταν σε θέση να ανιχνεύσουν την κακόβουλη

τροποποίηση υλικού με την ενεργοποίησή της. Μάλιστα, η επιβάρυνση σε χώρο και ισχύ ήταν μόλις 3% και 1% αντίστοιχα.

Τέλος, στις σύγχρονες προσεγγίσεις υπάρχει αυτή των Liu, Zhao & Chen (2019), στην οποία προτείνεται μια μέθοδος ανίχνευσης κακόβουλων τροποποιήσεων υλικού με ανάλυση των συνδυασμένων δομικών χαρακτηριστικών των κακόβουλων τροποποιήσεων υλικού και των κυκλωμάτων που προσβάλλουν.

Τα δομικά χαρακτηριστικά των συνδυαστικών και διαδοχικών κακόβουλων τροποποιήσεων υλικού εξάγονται και σχηματίζουν μια βάση δεδομένων με τα χαρακτηριστικά των κακόβουλων τροποποιήσεων υλικού. Έπειτα, προτείνεται μια αποδοτική προσέγγιση κβαντισμού για την αντιστοίχιση χαρακτηριστικών με σκοπό την αναζήτηση των χαρακτηριστικών από τα σχέδια των κυκλωμάτων.

Η προτεινόμενη προσέγγιση των Liu, Zhao & Chen (2019) προσδιορίζει ύποπτα κυκλώματα από ένα σχέδιο κυκλώματος αναζητώντας μικρά κομμάτια κυκλωμάτων που έχουν τα χαρακτηριστικά που αντιστοιχούνται στη βάση δεδομένων που έχει δημιουργηθεί με τα χαρακτηριστικά των κακόβουλων τροποποιήσεων υλικού. Έπειτα, προτείνονται αλγόριθμοι αντιστοίχισης χαρακτηριστικών για την δομική ανάλυση χαρακτηριστικών τόσο των συνδυαστικών, όσο και των διαδοχικών κακόβουλων τροποποιήσεων υλικού, αντίστοιχα. Ο βαθμός αντιστοίχισης ποσοτικοποιείται ως ακέραιες τιμές (integers) που αντιστοιχούν σε σπάνιες τιμές κακόβουλων τροποποιήσεων υλικού. Όσο μεγαλύτερος είναι ο βαθμός αντιστοίχισης, τόσο μεγαλύτερη είναι και η σπάνια τιμή της κακόβουλης τροποποίησης υλικού.

Τα πειράματα που διεξήχθησαν έδειξαν ότι η προτεινόμενη μέθοδος μπορεί να ανιχνεύσει με επιτυχία όλες τις κακόβουλες τροποποιήσεις υλικού με διάρκεια εκτέλεσης 72 δευτερολέπτων και με χαμηλά ποσοστά αποτυχίας.

ΚΕΦΑΛΑΙΟ 4

ΣΥΜΠΕΡΑΣΜΑΤΑ - ΠΡΟΤΑΣΕΙΣ

Είναι γεγονός πως τα σύγχρονα κυκλώματα αντιμετωπίζουν τον κίνδυνο που επιφέρουν οι κακόβουλες τροποποιήσεις υλικού. Όσοι θέλουν να προσβάλλουν τα κυκλώματα μπορούν εύκολα, πλέον, να το κάνουν αφού πολλά και διαφορετικά μέρη των κυκλωμάτων παράγονται και διατίθενται από πολλές και διαφορετικές πηγές από όλα τα μήκη και πλάτη του κόσμου.

Όπως, παρουσιάστηκε και στο κύριο μέρος της παρούσας εργασίας η δομή και οι μορφές των κακόβουλων τροποποιήσεων υλικού ποικίλουν, όπως ποικίλουν και οι τρόποι με τους οποίους μπορούν να ενεργοποιηθούν και να προξενήσουν το κακό για το οποίο έχουν δημιουργηθεί.

Οι συνέπειες, επίσης, των κακόβουλων τροποποιήσεων υλικού ποικίλουν. Μπορούν απλώς να μεταβάλλουν μικρά στοιχεία του κυκλώματος για να αλλοιώσουν κάποια μεταδιδόμενα σήματα μέχρι και να μεταδώσουν οι ίδιες οι τροποποιήσεις ευαίσθητα προσωπικά δεδομένα (κωδικούς, αριθμούς πιστωτικών καρτών) σε αυτόν που οργανώνει την επίθεση στο κύκλωμα. Μπορούν επίσης μέχρι και να καταστρέψουν εντελώς το κύκλωμα.

Όπως είναι φυσικό, η επιστημονική κοινότητα δε μπορεί να μείνει αμέτοχη σε αυτή την κακόβουλη επίθεση και αναπτύσσει συνεχώς μεθόδους ανίχνευσης κακόβουλων τροποποιήσεων υλικού. Οι μέθοδοι μπορούν να βασιστούν σε πολλά στοιχεία του κυκλώματος και της κακόβουλης τροποποίησης υλικού για να προβούν σε μια ανίχνευση. Ωστόσο, από την έρευνα στην ανάλυση πλευρικών καναλιών αποδεικνύεται πως τα ποσοστά επιτυχίας είναι ιδιαίτερα υψηλά καθιστώντας τις σχετικές μεθόδους ανίχνευσης ικανοποιητικά αποδοτικές.

Οι σύγχρονες προσεγγίσεις στην ανίχνευση κακόβουλων τροποποιήσεων υλικού, βέβαια, είναι πολλά υποσχόμενες αφού μπορούν να ανανεώνονται ανάλογα με τα δεδομένα που τους δίνονται και δρουν, αντίστοιχα, δυναμικά στις διαδικασίες ανίχνευσης και αποτελούν σημαντική απειλή για τις σύγχρονες κακόβουλες τροποποιήσεις.

Μια πρόταση για μελλοντική ανάπτυξη της παρούσας εργασίας σε βαθύτερο επίπεδο είναι η χαρτογράφηση ακόμα περισσότερων μεθόδων ανίχνευσης κακόβουλων τροποποιήσεων υλικού για να δοθεί μια πιο ολοκληρωμένη εικόνα. Ωστόσο, η έκταση αυτής

της δουλειάς εκτείνεται πέραν μιας διπλωματικής εργασίας και φτάνει σε ομαδικό επίπεδο ή ακόμα και σε επίπεδο διδακτορικής διατριβής.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Agrawal D., Baktir S., Karakoyunlu D., Rohatgi P., and Sunar, B., "Trojan detection using IC fingerprinting." in 2007 IEEE Symposium on Security and Privacy (SP'07), IEEE, pp. 296-310, May 2007.

Alkabani Y., & Koushanfar F., "Consistency-based characterization for IC Trojan detection." in Proceedings of the 2009 International Conference on Computer-Aided Design, ACM, pp. 123-127, Nov 2009.

Alkabani Y., and Koushanfar F., "Extended Abstract: Designer's Hardware Trojan Horse." in Proc. 0f IEEE International Workshop on Hardware—oriented Security and Trust. Anaheim, USA, IEEE Press, pp. 1-4, 2008

Alsaiari U., & Gebali F., (in press) "Hardware Trojan Detection Using Reconfigurable Assertion Checkers." in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, IEEE, 2019.

Banga M., and Hsiao M. S., "A novel sustained vector technique for the detection of hardware Trojans." in 2009 22nd international conference on VLSI design, pp. 327-332, Jan 2009.

Banga M., and Hsiao M. S., "Trusted RTL: Trojan detection methodology in pre-silicon designs." in 2010 IEEE international symposium on hardware-oriented security and trust (HOST), IEEE, pp. 56-59, Jun 2010.

Bao C., Forte D., and Srivastava, A., "On reverse engineering-based hardware Trojan detection." in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. *35*, no. 1, pp. 49-57, 2015.

Beaumont M., Hopkins B., and Newby T., "Hardware trojans-prevention, detection, countermeasures (a literature review)." In Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Div, pp. 1-38, 2011.

Bhasin S., Danger J. L., Guilley S., Ngo, X. T. and Sauvage, L., "Hardware Trojan horses in cryptographic IP cores." In 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography , IEEE, pp. 15-29, Aug 2013.

Bhunia S., Abramovici M., Agrawal D., Bradley P., Hsiao M. S., Plusquellic J., and Tehranipoor, M., (2013). "Protection against hardware trojan attacks: Towards a comprehensive solution." In IEEE Design & Test, vol. 30, no. 3, pp. 6-17, 2013.

Bhunia S., and Tehranipoor M., The Hardware Trojan War, Springer, Cham, 2018.

Bhunia S., Hsiao M. S., Banga M., and Narasimhan S., (2014). “Hardware Trojan attacks: threat analysis and countermeasures.” In Proceedings of the IEEE, vol. 102, no. 8, pp. 1229-1247, 2014.

Bloom G., Narahari B., and Simha R., “OS support for detecting Trojan circuit attacks.” in 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, pp. 100-103, Jul 2009.

Chabot, M., Mazet, K., & Pierre, L., “Automatic and configurable instrumentation of C programs with temporal assertion checkers.” In 2015 ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE), IEEE, pp. 208-217, Sep 2015.

Chakraborty R. S., Narasimhan S., and Bhunia S., “Hardware Trojan: Threats and emerging solutions.” in 2009 IEEE International high level design validation and test workshop , IEEE, pp. 166-17, Nov 2009.

Chakraborty R. S., Wolff F., Paul S., Papachristou C., and Bhunia S., “MERO: A statistical approach for hardware Trojan detection.” in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, pp. 396-410, Sep 2009.

Chen Z., Guo S., Wang J., Li Y., & Lu Z., (in press) “Towards FPGA security in IoT: A new detection technique for hardware trojans.”, in IEEE Internet of Things Journal, IEEE, 2019.

Deng D. Y., Chan A. H., and Suh G. E., “Hardware authentication leveraging performance limits in detailed simulations and emulations.” in Proceedings of the 46th Annual Design Automation Conference, ACM, pp. 682-687, Jul 2009.

Fyrbiak M., Wallat S., Swierczynski P., Hoffmann M., Hoppach S., Wilhelm M., ... & Paar C., “HAL-the missing piece of the puzzle for hardware reverse engineering, trojan detection and insertion.” In IEEE Transactions on Dependable and Secure Computing, IEEE, vol. 16, no.3, pp. 498-510, 2018.

Hagelin B., “Hardware Politics,“Hard Politics” or “Where, Politics?”: Nordic Defence Equipment Co-operation in the EU Context.” in The Nordic Countries and the European Security and Defence Policy, pp. 167-184, 2006.

Han T., Wang Y., & Liu P., “Hardware Trojans Detection at Register Transfer Level Based on Machine Learning.” in 2019 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, pp. 1-5, May 2019.

Huang Y., Bhunia S., and Mishra P., “MERS: statistical test generation for side-channel analysis based Trojan detection.” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 130-141, Oct 2016.

Jha S., and Jha S. K., “Randomization based probabilistic approach to detect trojan circuits.” in 2008 11th IEEE High Assurance Systems Engineering Symposium, IEEE, pp. 117-124, Dec 2008.

Jin Y., and Makris Y., “Hardware Trojan detection using path delay fingerprint.” in 2008 IEEE International workshop on hardware-oriented security and trust, IEEE, pp. 51-57, Jun 2008.

Jin, Y., Nathan K., and Makris Y., “Experiences in hardware Trojan design and implementation.” in 2009 IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE, 2009, pp. 50-57.

Jyothi V., and Rajendran J. J., “Hardware Trojan Attacks in FPGA and Protection Approaches.” in The Hardware Trojan War, Springer, Cham, pp. 345-368, 2018.

Karri R., Rajendran J., Rosenfeld K., & Tehranipoor M., “Trustworthy hardware: Identifying and classifying hardware trojans.” in Computer, vol. 43, no. 10, pp. 39-46, 2010.

Kulkarni A., Pino Y., and Mohsenin T., “Adaptive real-time trojan detection framework through machine learning.” in 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), IEEE, pp. 120-123, May 2016.

Kulkarni A., Pino Y., and Mohsenin T., “SVM-based real-time hardware Trojan detection for many-core platform.” in 2016 17th International Symposium on Quality Electronic Design (ISQED), IEEE, pp. 362-367, Mar 2016.

Kutzner S., Poschmann A. Y., and Stöttinger M., “Hardware trojan design and detection: a practical evaluation.” in Proceedings of the Workshop on Embedded Systems Security, ACM, pp. 1-16, 2013.

Li J., and Lach J., “At-speed delay characterization for IC authentication and Trojan horse detection.” in 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, pp. 8-14, Jun 2008.

Lin L., Kasper M., Güneysu T., Paar C., and Burleson W., “Trojan side-channels: lightweight hardware trojans through side-channel engineering.” in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg, pp. 382-395, Sep 2009.

Liu H., Luo H., & Wang L., “Design of hardware trojan horse based on counter.” in 2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, IEEE, pp. 1007-1009, Jun 2011.

Liu Q., Zhao P., & Chen F., “A Hardware Trojan Detection Method Based on Structural Features of Trojan and Host Circuits.” In IEEE Access, vol. 7, pp. 44632-44644, 2019.

McIntyre D., Wolff F., Papachristou C., Bhunia S., and Weyer D., (2009, July). “Dynamic evaluation of hardware trust.” in 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, pp. 108-111, Jul, 2009.

Nagata M., Danger J. L., and Miura N., “Creating a safe and robust digitally-connected world” in Impact pub, vol. 11, pp. 22-25, 2018.

Narasimhan S., Du D., Chakraborty R. S., Paul S., Wolff F. G., Papachristou C. A., ... and Bhunia, S., “Hardware Trojan detection by multiple-parameter side-channel analysis.” In IEEE Transactions on computers, vol. 62, no. 11, pp. 2183-219, 2012.

Narasimhan S., Wang X., Du D., Chakraborty R. S., and Bhunia, S., “TeSR: A robust temporal self-referencing approach for hardware Trojan detection.” in 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, IEEE, pp. 71-74, Jun 2011.

Ng X. T., Naj Z., Bhasin S., Roy D. B., Danger J. L., and Guilley, S., “Integrated sensor: A backdoor for hardware Trojan insertions?.” in 2015 Euromicro Conference on Digital System Design, IEEE, pp. 415-422, Aug 2015.

Nowroz A. N., Hu K., Koushanfar F., and Reda S., “Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps.” In IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 12, pp. 1792-1805, 2014.

Potkonjak M., Nahapetian A., Nelson M., and Massey, T., “Hardware Trojan horse detection using gate-level characterization.” in Proceedings of the 46th Annual Design Automation Conference, ACM, pp. 688-693, Jul 2009.

Pyrgas L., Pirpilidis F., Panayiotarou A., & Kitsos P.. Thermal sensor based hardware Trojan detection in FPGAs. In *2017 Euromicro Conference on Digital System Design (DSD)* (pp. 268-273). IEEE.

Rad R. M., Wang X., Tehranipoor M., and Plusquellic J., “Power supply signal calibration techniques for improving detection resolution to hardware Trojans.” in Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design IEEE Press, pp. 632-639, Nov 2008.

Reshma K., Priyatharishini M., and Devi M. N., “Hardware Trojan Detection Using Deep Learning Technique.” in Soft Computing and Signal Processing, Springer, Singapore, pp. 671-680, 2019.

Sadrozinski H. F. W., and Wu, J., Applications of field-programmable gate arrays in scientific research, Florida, CRC Press, 2016.

Salmani H., “Design Techniques for Hardware Trojans Prevention and Detection at the Register-Transfer Level.” in Trusted Digital Circuits, Springer, Cham, pp. 31-38, 2018.

Salmani H., and Tehranipoor M. M., “Vulnerability analysis of a circuit layout to hardware Trojan insertion.” in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1214-1225, 2016.

Salmani H., Trusted Digital Circuits: Hardware Trojan Vulnerabilities, Prevention and Detection, Berlin: Springer, 2017.

Shakya B., He T., Salmani H., Forte D., Bhunia S., and Tehranipoor M., “Benchmarking of hardware trojans and maliciously affected circuits.” In Journal of Hardware and Systems Security, vol. *1*, no. 1, pp. 85-102, 2017.

Tehranipoor M and Koushanfar F., “A survey of hardware trojan taxonomy and detection.” in IEEE design & test of computers, vol. 27, no.1 pp. 10-25, 2010.

Tehranipoor M., and Sunar B., “Hardware trojan horses.” in Towards Hardware-Intrinsic Security, Springer, Berlin, Heidelberg pp. 167-187, 2010

Tehranipoor M., Salmani H., Zhang X., Wang M., Karri R., Rajendran J., & Rosenfeld K., “Trustworthy hardware: Trojan detection and design-for-trust challenges.” in Computer, IEEE, vol. 44, no. 7, pp. 66-74, 2010.

Verbauwhede I., & Schaumont P., “Design methods for security and trust.” in Proceedings of the conference on Design, automation and test in Europe, EDA Consortium, pp. 672-677, Apr 2007.

Wang X., Salmani H., Tehranipoor M., and Plusquellic, J. “Hardware Trojan detection and isolation using current integration and localized current analysis.” in 2008 IEEE international symposium on defect and fault tolerance of VLSI systems, IEEE, pp. 87-95, Oct 2008.

Wang X., Tehranipoor M., and Plusquellic J. “Detecting malicious inclusions in secure hardware: Challenges and solutions.” in 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, pp. 15-19, Jun 2008.

Wang X., Tehranipoor M., and Plusquellic J., “Detecting malicious inclusions in secure hardware: Challenges and solutions. in 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, pp. 15-19, Jun 2008.

Wei S., Li K., Koushanfar F., & Potkonjak M., “Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry.” in Proceedings of the 49th Annual Design Automation Conference, ACM, pp. 90-95, Jun 2012.

Wolff F., Papachristou C., Bhunia S., and Chakraborty R. S., “Towards Trojan-free trusted ICs: Problem analysis and detection scheme.” in Proceedings of the conference on Design, automation and test in Europe, ACM, pp. 1362-1365, Mar 2008.

Yazdanbakhsh A., Mahajan D., Thwaites B., Park J., Nagendrakumar A., Sethuraman S., ... and Esmaeilzadeh H., “Axilog: Language support for approximate hardware design.” in Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, EDA Consortium, pp. 812-817, Mar 2015.

Zhao H., Kwiat L., Kwiat K. A., Kamhoua C. A., & Njilla L., (in press) “Applying Chaos Theory for Runtime Hardware Trojan Monitoring and Detection.” IEEE Transactions on Dependable and Secure Computing, IEEE.