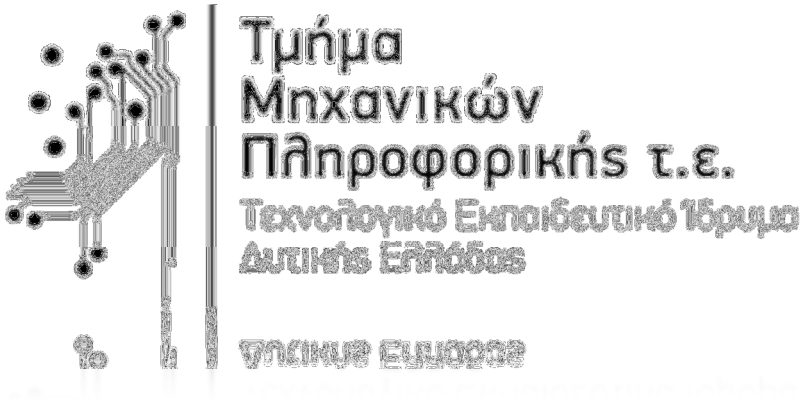


Πτυχιακη

ΕΠΙΣΚΟΠΗΣΗ ΜΕΘΟΔΩΝ ΑΝΙΧΝΕΥΣΗΣ ΙΟΜΟΡΦΟΥ ΥΛΙΣΜΙΚΟΥ (HARDWARE TROJAN DETECTION)

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΧΡΙΣΤΙΝΑ ΖΑΦΕΙΡΗ

ΑΜ:0970

ΕΠΙΒΛΕΠΩΝ: ΠΑΡΑΣΚΕΥΑΣ ΚΙΤΣΟΣ

ΑΝΤΙΡΡΙΟ 2017

Περιεχόμενα

Εισαγωγή

1.1 Ανασκόπηση στο ηλεκτρονικό έγκλημα

Η διείσδυση του διαδικτύου στην ανθρώπινη καθημερινότητα αποτελεί πλέον γεγονός ενώ τείνει να αυξάνεται σε καθημερινή βάση καθώς εξελίσσεται και βελτιώνεται η τεχνολογία. Πλέον, οι άνθρωποι επικοινωνούν, εργάζονται αλλά και μαθαίνουν διαμέσου του διαδικτύου το οποίο μπορεί να περιγραφεί ως ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, που έχει τη δυνατότητα να διασυνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων.

Στα μεγαλύτερα πλεονεκτήματα του διαδικτύου συγκαταλέγονται τόσο η ταχύτητα όσο και η ευκολία στη χρήση καθώς τα πάντα γύρω από αυτό μπορούν να πραγματοποιηθούν με τη χρήση και μόνο μερικών κουμπιών. Η ορθή του χρήση οδηγεί σε αναβάθμιση του μορφωτικού επιπέδου ενώ παράλληλα οι ηλεκτρονικοί υπολογιστές οι οποίοι αποτελούν και την επέκταση αυτού, αποτελούν πλέον αναπόσπαστα μέρη της καθημερινότητας είστε ως είτε ως μέσα ψυχαγωγίας και ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων.

Ως γνωστόν, το διαδίκτυο αποτελεί το μεγαλύτερο διασυνδεδεμένο δίκτυο υπολογιστών το οποίο λόγω της ανοικτής δομής και της απεριόριστης εξάπλωσής του συνδέει εκατοντάδες εκατομμύρια χρήστες σε όλο τον κόσμο. Οι υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο, συνεργάζονται με τρόπο τέτοιο αλλά και επικοινωνούν ώστε να μεταφέρουν την πληροφορία ε όλα τα μήκη και πλάτη της γης.

Ακριβώς επειδή το διαδίκτυο παρέχει μία πλήρη και καθολική σύνδεση όλων των υπολογιστών μεταξύ τους ελλοχεύει σειρά κινδύνων ανάμεσα στους οποίους συγκαταλέγεται και το ηλεκτρονικό έγκλημα. Οι δυνατότητες που παρέχονται στο χρήστη διαμέσου του διαδικτύου, ενός είναι ασύλληπτες, αφετέρου όμως εισάγουν σειρά παραβατικών συμπεριφορών που οδηγούν σε αξιόποινες πράξεις οι οποίες όπως συνίσταται μόνο με τη χρήση Η/Υ και του ιντερνέτ, όπως η διασπορά κακόβουλου λογισμικού σε Η/Υ και η παραβίαση ηλεκτρονικών αρχείων.

Λόγω της ιδιαίτερης πολυπλοκότητας του διαδικτύου κυριαρχεί ένα ιδιαίτερο καθεστώς στο οποίο οι δράστες μπορούν να παραμένουν ανώνυμοι ενώ οι διωκτικές αρχές να συναντήσουν

ιδιαίτερη δυσκολία προκειμένου να οδηγηθούν σε συλλήψεις. Ακόμη και σήμερα όπου η εξέλιξη της τεχνολογίας είναι ραγδαία και τα μέσα που παρέχονται στις διωκτικές αρχές όλο και πιο σύγχρονα, η διαλεύκανση της ηλεκτρονικής εγκληματικότητας παραμένει μία δύσκολη υπόθεση.

Οι ορισμοί που δόθηκαν κατά καιρούς γύρω από το ηλεκτρονικό έγκλημα είναι πάρα πολλοί και ποικίλουν ως προς τον τρόπο έκφρασης. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης, χαρακτήρισε ως ηλεκτρονικό έγκλημα την κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων. Επιπρόσθετα, και με βάση τα όσα υποστηρίζει ο Shinder, βασικό στοιχείο για την τέλεση κάθε ηλεκτρονικού εγκλήματος είναι η ύπαρξη ενός υπολογιστή ο οποίος διαδραματίζει τους παρακάτω ρόλους :

- Μπορεί να αποτελεί το στόχο κάποιας επίθεσης, και άρα ο Η/Υ να είναι το «θύμα» της επίθεσης.
- Δύναται να αποτελεί μέσο για τη διάπραξη κάποιας επίθεσης. Εδώ είναι το εργαλείο που χρησιμοποιείται από το δράστη για την πραγματοποίηση εγκληματικού σκοπού.
- Υπάρχει και η περίπτωση που ο Η/Υ αποτελεί βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Στην ευρύτερη κατηγορία του ηλεκτρονικού εγκλήματος συγκαταλέγεται το διαδικτυακό έγκλημα το οποίο σύμφωνα με τον Parker είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, καθώς για την τέλεση του ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο.

Στο σύνολό τους ως ηλεκτρονικά εγκλήματα χαρακτηρίζονται τα παρακάτω :

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.
- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσεται η διασπορά κακόβουλου λογισμικού.

Ο ερευνητής Pipkin και οι συνεργάτες του διαχωρίζουν τα ηλεκτρονικά εγκλήματα στις παρακάτω κατηγορίες :

- Εγκλήματα τα οποία τελούνται με χρήση Η/Υ όπως η απάτη, η κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και η κλοπή της ηλεκτρονικής ταυτότητας.
- Ειδικά εγκλήματα των Η/Υ όπως η επίθεση της άρνησης παροχής υπηρεσίων , η άρνηση πρόσβασης σε πληροφόριες και η διασπορά καταστρεπτικών ιών.
- Αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί
- Εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

Μία άλλη κατηγοριοποίηση, σχετική πάντα με το ηλεκτρονικό έγκλημα δόθηκε από την Εξεταστική Επιτροπή του Ηνωμένου Βασιλείου στη δεκαετία του 1980 και πρότεινε τον παρακάτω διαχωρισμό :

- **Απάτη**: Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή /συμπίεση/ ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς)
- **Κλοπή:** των δεδομένων, του λογισμικού
- **Χρήση** λογισμικού χωρίς άδεια: χρήση παράνομων αντιγράφων λογισμικού
- **Ιδιωτική εργασία**: μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκοδιμή κέρδους ή για ίδιον όφελος
- **Χάκινγκ:** :ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας
- **Σαμποτάζ:** η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό
- **Εισαγωγή:** πορνογραφικού υλικού
- **Ιοι:** διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής.

Τέλος, τα βασικά χαρακτηριστικά των ηλεκτρονικών εγκλημάτων συνοψίζονται στα παρακάτω :

- Το διαδικτυακό έγκλημα διαπράττεται σε χρόνο ελάχιστων δευτερολέπτων.
- Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα. Η εισβολή σε ένα υπολογιστικό σύστημα διευκολύνεται από το ίδιο το

διαδίκτυο και αυτό γιατί διατίθεται σε αυτό ελεύθερα εφαρμογές λογισμικού με τις οποίες οι χάκερς μπορούν να εισβάλλουν εύκολα σε δίκτυα και υπολογιστικά συστήματα και να πραγματοποιήσουν πλήθος ηλεκτρονικών επιθέσεων.

- Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (του κράτους στο οποίο γίνεται αντιληπτή η διάπραξη του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία).
- Για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής τεχνολογίας και διαδικτύου καθώς και συνεχή εκπαίδευση όσων είναι αρμόδιοι για τη δίωξή του (αστυνομικές και δικαστικές αρχές).
- Το ηλεκτρονικό έγκλημα έχει εισάγει νέους περιορισμούς:
    - Πολλές φορές είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου ηλεκτρονικού υπολογιστή ο εγκληματίας μμπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου
    - Ο ακριβής χρόνος τέλεσης του εγκλήματος και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημιά που προκλήθηκαν πολύ αργότερα από το χρόνο που πραγματοποιηθήκαν.

1.2 Οι κυριότερες απειλές στο διαδίκτυο

Όπως προναφέρθηκε, το διαδίκτυο αποτελεί μία αστείρευτη πηγή πληροφοριών που φέρνει το χρήστη όλο και κοντύτερα στη γνώση άμεσα και χωρίς να απαιτείται ιδιαίτερη τεχνογνωσία. Πρόκειται για μία κοινωνία τεραστίου μεγέθους, η οποία, όπως και κάθε άλλης μορφής κοινωνία ελλοχεύει μία σειρά κινδύνων που χρήζουν σειράς ενεργειών ώστε να αντιμετωπιστούν.

Παρακάτω θα γίνει μία προσπάθεια αναφοράς των σημαντικότερων από αυτούς ώστε να γίνει κατανοητή η φύση τους αλλά και ο τρόπος λειτουργίας τους.

- ***Ευπάθειες***

Πρόκειται για μία εγγενή αδυναμία στο σύστημα η οποία δίνει τη δυνατότητα στον επίδοξο επιτιθέμενο ώστε να παρέμβει στην ασφάλεια του συστήματος και να μειώσει τα επίπεδά της.

Κάθε ευπάθεια αποτελεί την τομή των παρακάτω στοιχείων !

1. Της ευαισθησίας και του ελαττώματος του συστήματος
2. Της πρόσβασης του επιτιθέμενου στο ελάττωμα
3. Της ικανότητας του επιτιθέμενου να εκμεταλλευτεί το ελάττωμα

Για να θεωρηθεί ένα σύστημα ευάλωτο, θα πρέπει ο επιτιθέμενος να χρησιμοποιεί είτε κάποια συγκεκριμένη τεχνική είτε το κατάλληλο εργαλείο το οποίο θα μειώσει τα επίπεδα ασφαλείας του συστήματος. Η χρήση της ευπάθειας με την ίδια σημασία του κίνδυνου μπορεί να οδηγήσει σε σύγχυση. Έπειτα υπάρχουν ευπάθειες χωρίς κίνδυνο: για παράδειγμα, όταν το πληγέν στοιχείο δεν έχει καμία αξία. Η ευπάθεια ξεκινάει από τη στιγμή που εμφανίζεται το κενό ασφαλείας μέχρι ότου η πρόσβαση της απενεργοποιηθεί ή ο επιτιθέμενος αποκοπεί.

- ***Κακόβουλα Λογισμικά***

Στα κακόβουλα λογισμικά συγκαταλέγονται όλα εκείνα τα προγράμματα τα οποία έχουν γραφεί με στόχο να επιτεθούν στην εμπιστευτικότητα και την ακεραιότητα των συστημάτων. Συνήθως, απαιτείται εγκατάστασή τους στον υπολογιστή και άρα η συμβολή της ανθρώπινης παρέμβασης ώστε να αυτά να μπορούν να λειτουργήσουν αποτελεσματικά.

Τα κακόβουλα λογισμικά, στην πλειοψηφία τους επιφέρουν μία σειρά αρνητικών παρενεργειών στον υπολογιστή πέραν τούτου όμως, πολλές φορές συμπεριλαμβάνεται σε αυτά κώδικας που έχει ως στόχο :

- Την αναπαραγωγή του: Εξάπλωση του στο σύστημα που προσβάλλει («μόλυνση» από πρόγραμμα σε πρόγραμμα).
- Τη μετάδοση του: Εξάπλωση του από το σύστημα που μολύνθηκε σε άλλο/άλλα συστήματα (π.χ. από Η/Υ σε Η/Υ)

- ***Μολυσματικά Κακόβουλα Λογισμικά***
  - *Ιοί*

Κάθε ιός υπολογιστή, αποτελεί ένα πρόγραμμα, το οποίο έχει την ικανότητα να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Πέραν των παραπάνω, ο ιός έχει τη δυνατότητα, δεδομένης της ύπαρξης δικτύου, να μεταδοθεί από έναν υπολογιστή σε έναν άλλο.

Κάποιοι από τους ιούς έχουν ως βασικό στόχο την πρόκληση της ζημίας στον υπολογιστή στον οποίο έχουν εγκατασταθεί. Μάλιστα, η φθορά που μπορεί να επέλθει από το σκληρό δίσκο λόγω της ύπαρξης αυτών ενδέχεται να είναι καταστροφική και να μην υπάρχει η δυνατότητα ανάκτησης του περιεχομένου. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων. Ακόμη και αυτοί δημιουργούν πρόβλημα στον υπολογιστή καθώς καταλαμβάνουν χώρο στη μνήμη και προκαλούν αστάθεια του συστήματος.

Τέλος, όπως είναι γνωστό, πολλοί από τους ιούς δεν έχουν ως αντικειμενικό στόχο την πρόκληση σφαλμάτων αλλά έχουν την υποκλοπή πολλών και σημαντικών προσωπικών δεδομένων ή την έντονη παρενόχληση του χρήστη.

- *Μηνύματα Απατηλού Περιεχομένου (Hoaxes)*

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

- **«Προειδοποιητικά»:** είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα .
- **«Συμπαράστασης»:** παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.
- **«Εκφοβισμού» :** οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο κίνδυνος που προκύπτει από τα μηνύματα αυτά δεν έχει καμία σχέση με αυτόν που επιφέρουν οι ιοί. Ουσιαστικά αφορά μονάχα στην κατάληψη χώρου και στην επιβάρυνση των λογαριασμών των χρηστών. Τέτοιου είδους μηνύματα συνοδεύονται πάντα από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know").

Ως αποστολείς εμφανίζονται συνήθως ιδιαίτερα γνωστές εταιρίες έτσι ώστε να ξεγελαστεί ο χρήστης και να προβεί στις ενέργειες που του ζητά το μήνυμα. Αυτό το οποίο συνίσταται στο χρήστη να κάνει είναι φυσικά να προβεί σε διαγραφή αυτών ή να κάνει χρήση του προγράμματος καταστολής ιών που έχει στον υπολογιστή του.

- *Σκουλήκια*

Το «σκουλήκι» (worm) μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host). Έχει παρόμοια μορφή με τους ιούς με τη διαφορά ότι αυτά δε χρειάζονται εκτελέσιμα αρχεία παρά μόνο τη χρήση του διαδικτύου. Έτσι, ένα σκουλήκι δεν απαιτεί από τον χρήστη να ανοίξει οποιοδήποτε αρχείο για την εκτέλεσή του, καθώς μπορεί να λειτουργήσει χωρίς την παρέμβαση του χρήστη.

Η δράση τους δεν είναι τόσο καταστροφική καθώς δεν προβαίνουν σε διαγραφή αρχείων. Ουσιαστικά καθυστερούν τη σύνδεση με το διαδίκτυο επειδή στέλνουν τα αντίγραφα τους σε άλλους Η/Υ. Επίσης κάνουν το σύστημα του Η/Υ πιο αργό χρησιμοποιώντας πολλή μνήμη με το να αντιγράφουν τον εαυτό τους πολλές φορές και γεμίζοντας τον ελεύθερο χώρο του σκληρού δίσκου (rabbits). Υπάρχουν όμως και ορισμένα σκουλήκια που έχουν ταυτόχρονα ιδιότητες ιών, πράγμα που τα καθιστά πιο επικίνδυνα από τα συνηθισμένα σκουλήκια.

- **Μεταμφιεσμένα Κακόβουλα Λογισμικά**
  - *Δούρειοι Ίπποι*

Πρόκειται για το κακόβουλο εκείνο λογισμικό το οποίο παρουσιάζεται να εκτελεί κάποια χρήσιμη λειτουργία ενώ στην ουσία εγκαθιστά στον υπολογιστή άλλα κακόβουλα προγράμματα τα οποία κρύβουν μέσα τους κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Η ζημία που προκαλείται στον υπολογιστή από το πρόγραμμα αυτό είναι ιδιαίτερα σοβαρή. Κάθε Δούρειος Ίππος ή Trojan Horse, αποστέλλεται στο χρήστη διαμέσου ή μέσω κάποιου προγράμματος που λαμβάνει αρχεία και πληροφορίες από το διαδίκτυο και μπορεί να φθάσει υπό μορφή προγράμματος αστείου ή λογισμικού κάποιου είδους.

Η λειτουργία τους ξεκινά με την ενεργοποίηση κάποιου προγράμματος ενώ στα αποτελέσματα της μόλυνσης που επέρχεται από αυτούς συγκαταλέγεται η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου.

  - *Rootkits*

Κάθε Rootkit είναι ένα πρόγραμμα σχεδιασμένο με τρόπο τέτοιο ώστε να καταλαμβάνει τον έλεγχο του λειτουργικού συστήματος, ή μιας ομάδας ηλεκτρονικών υπολογιστών, χωρίς τη σχετική έγκριση από το διαχειριστή του συστήματος. Συνήθως, υπάρχει ενσωμάτωση των Rootkits σε κάποιο από τα βασικά αρχεία του λειτουργικού συστήματος γεγονός που τους δίνει πλήρη πρόσβαση στον έλεγχο όλου του συστήματος και συνεπαγωγικά και οποιουδήποτε λογισμικού καταστολής ιών.

  - *Backdoor Ioί*

Οι ιοί αυτής της μορφής έχουν τη μοναδική ικανότητα ώστε να παρακάμπτουν τις συνήθεις διαδικασίες ελέγχου ταυτότητας. Μπορούν να εγκατασταθούν πριν το κακόβουλο λογισμικό ώστε να επιτρέψουν την είσοδο σε επίδοξους εισβολείς και έτσι να υπάρξει απώλεια κωδικό αλλά και προσβολής του υπολογιστή από Δούρειους Ίππους.

- **Λογισμικά με στόχο το κέρδος και την παρέμβαση σε προσωπικά δεδομένα**

  - ***Spyware***

Πρόκειται για την κατηγορία εκείνη των προγραμμάτων που εγκαθίσταται στον υπολογιστή με άκρως ύπουλο τρόπο και έχει ως στόχο την παρακολούθηση και την καταγραφή των κινήσεων του χρήστη στο διαδίκτυο. Τα Spyware εκτελούνται στο παρασκήνιο και δεν παρεμβαίνουν στη συμπεριφορά του χρήστη. Η εγκατάστασή τους γίνεται με τους παρακάτω τρόπους :

Με την εγκατάσταση προγραμμάτων: Μερικά προγράμματα , συνήθως προγράμματα που μοιράζουν αρχεία (peer-to-peer file sharing client) εγκαθιστούν spyware μαζί με την εγκατάσταση τους, παρόλο που ισχυρίζονται το αντίθετο. Το πιο γνωστό σε αυτή την κατηγορία είναι το Kazaa.

Με την επίσκεψη σε δικτυακούς τόπους: Μερικοί δικτυακοί τόποι προσπαθούν να κατεβάσουν και να εγκαταστήσουν αυτόματα στον υπολογιστή του χρήστη κάποιο spyware. Αν οι ρυθμίσεις ασφαλείας του φυλλομετρητή είναι σωστές, μπορεί να εμφανιστεί ένα προειδοποιητικό μήνυμα που ενημερώνει ότι ένα πρόγραμμα θα πρέπει να εγκατασταθεί, και μας ζητάει να το εγκρίνουμε ή όχι. Τις περισσότερες φορές όμως αυτό το μήνυμα δεν εμφανίζετε.

Με την εγκατάσταση Add-ons: Τα Add-ons είναι προγράμματα που ενισχύουν το φυλλομετρητή (browser). Μπορεί να είναι γραμμές εργαλείων, κουμπιά αναζήτησης, κινούμενες εικόνες κλπ. Αυτό τα προγράμματα κάνουν αυτό που λένε αλλά μεταφέρουν μαζί τους και spyware.

Τα βασικότερα χαρακτηριστικά τους είναι :

- ✓ Τα Spyware ξεκινάνε μαζί με τον υπολογιστή κατά την εκκίνηση του και πιάνουν μνήμη και υπολογιστική ισχύ.
- ✓ Εμφανίζουν συνεχώς παράθυρα με ανεπιθύμητες διαφημίσεις.
- ✓ Αλλάζουν την αρχική σελίδα του φυλλομετρητή.
- ✓ Αλλάζουν τα αποτελέσματα αναζητήσεων και εμφανίζουν άλλα, κάνοντας με αυτό τον τρόπο τις μηχανές αναζήτησης δύσχρηστες.

- ✓ Μερικά Spyware αλλάζουν τις ρυθμίσεις του φυλλομετρητή έτσι ώστε αν συνδέεστε με dial-up σύνδεση στο διαδίκτυο το modem καλεί πανάκριβούς αριθμούς φουσκώνοντας το τηλεφωνικό λογαριασμό.
- ✓ Μερικά Spyware αλλάζουν τις ρυθμίσεις του τοίχους προστασίας (firewall) επιτρέποντας την εισβολή άλλων Spyware προγραμμάτων.
- ✓ Μερικά Spyware είναι αρκετά έξυπνα ,καταλαβαίνουν αν ο χρήστης προσπαθήσει να τα απεγκαταστήσει από το Windows registry και εγκαθιστούνται ξανά αυτόματα.

- *Botnets*

Ως Botnet χαρακτηρίζεται το δίκτυο εκείνο των υπολογιστών το οποίο ελέγχεται εξ αποστάσεως από τον botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται ζόμπι. Κάθε botmaster έχει τη δυνατότητα να χρησιμοποιεί τα ζόμπι ώστε να ικανοποιήσει κακόβουλους στόχους καθώς μπορεί να παρέμβει απομακρυσμένα σε αυτούς ως ένας χρήστης με πλήρη δικαιώματα. Πέραν λοιπόν της υποκλοπής δεδομένων από τα ζόμπι, παρέχεται και η δυνατότητα της πλήρους απόκρυψης της ταυτότητας του χρήστη καθώς καθώς ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος. Ανάλογα με το μέγεθος του Botnet, ο δράστης μπορεί να αλλάζει σε ορισμένες εξαιρετικές περιπτώσεις τη διεύθυνση IP του ακόμη και ανά δευτερόλεπτο, ώστε να μπορεί να προβαίνει σε παράνομες ενέργειες μέσω των συνδέσεων των θυμάτων του. Επιπλέον, ο εξ αποστάσεως έλεγχος των υπολογιστών εξυπηρετεί ιδανικά τη μετάδοση του κακόβουλου κώδικα Bot ή τη μαζική αποστολή spam.

- *Keystroke logger*

Το ιδιαίτερα επικίνδυνο αυτό πρόγραμμα έχει τη δυνατότητα υποκλοπής του κάθε χαρακτήρα που πληκτρολογεί ο χρήστης στον προσωπικό του υπολογιστή. Μία keylogger συσκευή είναι μία ιδιαίτερα μικρού μεγέθους συσκευή που συχνά δεν γίνεται αντιληπτή εάν αυτή τοποθετηθεί σε ένα υπολογιστή. Ο χρήστης ανυποψίαστος πληκτρολογεί το κείμενο που επιθυμεί το οποίο όμως με τη σειρά του αποθηκεύεται ως κείμενο στο δικό του μικροσκοπικό σκληρό δίσκο .

Από την άλλη, ένα keylogger πρόγραμμα δεν απαιτεί φυσική πρόσβαση στον υπολογιστή παρά μονάχα την εγκατάσταση του ώστε να είναι σε θέση να παρακολουθήσει τη δραστηριότητα του χρήστη. Ένα keylogger πρόγραμμα συνήθως αποτελείται από δύο αρχεία τα οποία είναι εγκατεστημένα στον ίδιο φάκελο: ένα αρχείο DLL(το οποίο κάνει την καταγραφή) και ένα αρχείο EXE το οποίο εγκαθιστά το DLL αρχείο και το ενεργοποιεί για να ξεκινήσει την καταγραφή.

- *Adware*

Το λογισμικό αυτής της μορφής είναι ιδιαίτερα ενοχλητικό καθώς κατορθώνει με αυτοματοποιημένο τρόπο να επιδεικνύει, ή να λαμβάνει διαφημιστικό υλικό μέσω Internet. Η εκτέλεση αυτού του λογισμικού μπορεί να γίνεται νόμιμα, στα πλαίσια μιας εφαρμογής που το ορίζει ρητώς στους Όρους Χρήσης της, ή με τρόπο μη φανερό.

Στις παρενέργειες του λογισμικού αυτού συγκαταλέγονται :

- ✓ Η εμφάνιση ανεπιθύμητων μηνυμάτων στον browser, ή στην επιφάνεια εργασίας
- ✓ Η αλλαγή της αρχικής σελίδας του browser
- ✓ Η αλλαγή της αρχικής σελίδας αναζήτησης στο Web,
- ✓ Η αναδρομολόγηση σε λανθασμένο (πλαστό) δικτυακό τόπο (web spoofing)

- *Crimeware*

Σχεδιασμένο με στόχο την υποκλοπή ταυτότητας το λογισμικό αυτό καταφέρνει να παρέχει στους επίδοξους εισβολής πρόσβαση σε online λογαριασμούς του χρήστη σε εταιρείες παροχής χρηματοοικονομικών υπηρεσιών και online εμπόρους λιανικής πώλησης, με σκοπό τη λήψη κεφαλαίων από τους λογαριασμούς αυτούς ή συμπληρώνοντας μη εγκεκριμένες συναλλαγές που εμπλουτίζουν την δυνατότητα του κλέφτη στον έλεγχο του Crimeware. Στους στόχους του συγκαταλέγεται επίσης η εξαγωγή των εμπιστευτικών πληροφοριών με στόχο των εκβιασμό του χρήστη.

- *Scareware*

Τα ψεύτικα αυτά πακέτα καταστολής λογισμικού ιών προειδοποιούν εσφαλμένα τους χρήστες για την ύπαρξη κακόβουλου λογισμικού στον υπολογιστή τους και τους παρασύρουν

σε αγορές λογισμικών που δεν επιτελούν καμία απολύτως λειτουργία. Η προσέγγιση βασίζεται στον εκφοβισμό των χρηστών για να αγοράσουν άχρηστα προϊόντα και όχι στην αντιμετώπιση πραγματικών προβλημάτων.

- *Πειρατεία Λογισμικού*

Ως πειρατεία λογισμικού ορίζεται η μη εξουσιοδοτημένη αντιγραφή ή διανομή λογισμικού, η οποία πραγματοποιείται με την λήψη, αντιγραφή, κοινή χρήση, πώληση ή εγκατάσταση πολλαπλών αντιγράφων σε προσωπικούς ή εταιρικούς υπολογιστές. Αυτό που οι περισσότεροι δεν κατανοούν όταν αγοράζουν λογισμικό, είναι ότι στην πραγματικότητα αγοράζουν την άδεια χρήσης του και όχι το ίδιο το λογισμικό. Η άδεια θα πρέπει να διαβάζεται πολύ προσεκτικά γιατί καθορίζει σε πόσους υπολογιστές επιτρέπεται η εγκατάσταση του λογισμικού. Επομένως, η δημιουργία περισσοτέρων αντιγράφων από όσα ορίζει η άδεια αποτελεί πειρατεία.

1.3 Ενδεδειγμένη προστασία από ιούς

Με στόχο την προστασία από τους ιούς συνίστανται στον κάθε χρήστη τα παρακάτω

- Τήρηση αντιγράφων ασφαλείας.
- Συχνή ανανέωση (update) του προγράμματος καταστολής ιών.
- Συχνή ανανέωση (update) του προγράμματος πλοήγησης στο internet.
- Συχνή ανανέωση (update) του προγράμματος ανάγνωσης των email.
- Συχνή ανανέωση (update) του προγράμματος Adobe Acrobat Reader.
- Συχνή ανανέωση (update) των προγραμμάτων Microsoft Office και OpenOffice .
- Ανίχνευση κάθε νέου αρχείου που «κατεβάζει» ο χρήστης από το Internet.
- Αποφυγή εισαγωγής αγνώστων USB sticks στον υπολογιστή .
- Ενεργοποίηση της εφαρμογής πλήρους εμφάνισης των τύπων αρχείων στον Η/Υ.
- Χρήση κάποιου προγράμματος firewall
- Συχνό update στο λειτουργικό σύστημα του Η/Υ, ώστε να καλύπτονται τα όποια κενά ασφαλείας έχουν εντοπιστεί.

Κεφάλαιο 1

1.1 Trojan Horses - Δούρειοι Ίπποι

Ο όρος «Δούρειος ίππος» προέρχεται από τον πολύ γνωστό Δούρειο Ίππο που χρησιμοποιήθηκε στον Τρωικό πόλεμο ως δώρο από τον Οδυσσέα προς τους Τρώες με σκοπό αυτοί να εξαπατηθούν και να μπορέσουν οι Αχαιοί στρατιώτες να εισέλθουν στην πόλη της Τροίας.

Παρόμοια είναι η λειτουργία των Δούρειων Ίππων και στον κόσμο των υπολογιστών. Η λειτουργία τους έχει ως σκοπό την εξαπάτηση των χρηστών. Εκ πρώτης όψεως φαίνονται ως κανονικά και χρήσιμα προγράμματα, στην πραγματικότητα όμως, πίσω από αυτά κρύβεται ένας βλαβερός κώδικας που ενεργοποιείται όταν το πρόγραμμα εκτελεστεί.

Ο όρος «Δούρειος ίππος» χρησιμοποιήθηκε για πρώτη φορά από τον Ken Thompson το 1983 κατά τη διάλεξή του στην τελετή απονομής βραβείων Turing. Ο Thompson ονόμασε «Δούρειο ίππο» τη δυνατότητα προσθήκης κώδικα κακόβουλου τύπου στην εντολή login του Unix με στόχο την υποκλοπή κωδικών πρόσβασης. Επιπρόσθετα, διαπίστωσε ότι οποιοσδήποτε μεταγλωττιστής C μπορεί να μετατραπεί κατάλληλα ώστε να προσθέτει αυτόματα κώδικα κακόβουλου τύπου στα προγράμματα που δημιουργεί, γεγονός που καθιστά δύσκολο τον εντοπισμό του κακόβουλου κώδικα.

Στις πλέον σύνηθεις λειτουργίες των Δούρειων Ίππων περιλαμβάνονται η καταστροφή των δεδομένων, η τροποποίηση αυτών, η προσπάθεια υποκλοπής στοιχείων και η αλλοίωση των δεδομένων κατά την εκκίνηση του προγράμματος. Χρησιμοποιούνται εν γένει για να πραγματοποιήσουν έμμεσα λειτουργίες που ο μη εξουσιοδοτημένος χρήστης δεν μπορεί άμεσα να εκτελέσει.

Κάθε Δούρειος Ίππος, συμπεριλαμβάνεται μέσα στα κατά τα άλλα αθώα προγράμματα και επιχειρεί να εκτελέσει μια λειτουργία διαφορετική από αυτή που θα επιχειρούσε ο χρήστης. Το σημαντικότερο πρόβλημα το οποίο εντοπίζεται στην ύπαρξη των Δούρειων Ίππων, είναι ότι αυτοί είναι ιδιαίτερα δύσκολο να εντοπιστούν και αυτό οφείλεται σε δύο πολύ βασικούς λόγους. Ο πρώτος είναι ότι συχνά παίρνουν τη μορφή ιδιαίτερα συνηθισμένων εργαλείων ή εργαλείων που απαιτούν την χειροκίνητη εγκατάσταση τους από το χρήστη. Ο δεύτερος λόγος για τον οποίο είναι δύσκολο να εντοπιστούν είναι ότι υπάρχουν σε

κάποιο υπολογιστή με τη μορφή ενός μεταφρασμένου προγράμματος το οποίο είναι δύσκολο να ελεγχθεί τι ακριβώς κάνει.

Ένας Δούρειος Ίππος αποτελείται από δύο βασικά μέρη, το server και τον client. Έτσι, για να μπορέσει αυτός να λειτουργήσει, θα πρέπει να εγκατασταθεί στον υπολογιστή, και αμέσως επόμενα να λειτουργήσει το μέρος server. Στη συνέχεια, το μέρος client, εκτελείται στον υπολογιστή του επιτιθέμενου και διαμέσου της IP του υπολογιστή καθίσταται πλέον δυνατός ο έλεγχος του υπολογιστή - θύμα. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή καλούνται droppers.

Η επικοινωνία των Δούρειων Ίππων γίνεται με τους clients διαμέσου των διαφόρων ports, οι οποίες απενεργοποιούνται με τη χρήση των firewall. Στην πλειοψηφία των περιπτώσεων, η ύπαρξη των Δούρειων Ίππων στους υπολογιστές δημιουργεί κερκόπορτες, τις οποίες χρησιμοποιεί ο επιτιθέμενος ώστε να συνδεθεί με το σύστημα. Ως κερκόπορτα, καλείται ένα μυστικό σημείο εισόδου σε ένα πρόγραμμα, το οποίο επιτρέπει στον επιτιθέμενο να αποκτήσει δικαιώματα προσπέλασης στο σύστημα παρακάμπτοντας τις συνήθεις διαδικασίες προσπέλασης.

1.2 Physically Unclonable Function - PUF

Η λειτουργία όλων των συστημάτων ασφάλειας ενός υπολογιστικού συστήματος βασίζεται στην ύπαρξη αλγορίθμων κρυπτογράφησης και κατακερματισμού. Οι αλγόριθμοι αυτοί, απαιτούν την ύπαρξη ενός κλειδιού το οποίο είναι γνωστό στο λογισμικό και στα εξουσιοδοτημένα συστήματα.

Κρίσιμο ζήτημα για την ασφάλεια των ευφυών συστημάτων και των επικοινωνιών τους με τα συστήματα του Smart Grid αποτελεί το κατά πόσο τα κλειδιά κρυπτογράφησης μπορούν να παραμείνουν κρυφά. Πολλές μέθοδοι έχουν προταθεί με πλέον υποσχόμενη τη χρήση ειδικών κυκλωμάτων που ονομάζονται PUF (Physically Unclonable Function).

Κύριο χαρακτηριστικό των κυκλωμάτων αυτών είναι το γεγονός ότι παράγουν δεδομένα με τη μέθοδο της τυχαιότητας ώστε να μην είναι δυνατή η πρόβλεψη της εξόδου τους. Ακόμη, η τυχαιότητα προκύπτει από κατασκευαστικά χαρακτηριστικά ώστε σε περίπτωση απόπειρας

παραβίασης του κυκλώματος να αλλοιώνεται η διαδικασία παραγωγής δεδομένων με αποτέλεσμα να μην αποκτά την πληροφορία ο επιτιθέμενος.

Τα κυκλώματα PUF, χωρίζονται σε δύο μεγάλες κατηγορίες, τα ασθενή PUF (Weak PUF) και τα ισχυρά PUF (Strong PUF). Η διαφορά τους έγκειται στο πλήθος των τυχαίων δεδομένων που παράγουν με τα ασθενή να παράγουν συγκεκριμένα δεδομένα σε κάθε έξοδό τους και τα ισχυρά να παράγουν δεδομένα εξόδου με βάση την είσοδο που λαμβάνουν.

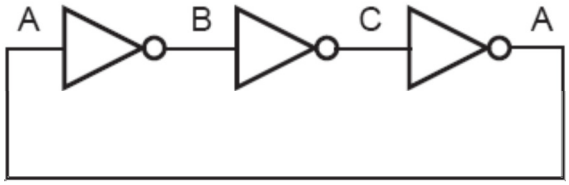
Στα ευφυή συστήματα χρησιμοποιούνται κυρίως τα ασθενή PUF και μία υποκατηγορία των ασθενών που καλούνται ελεγχόμενα. Τα ελεγχόμενα PUF περιλαμβάνουν μία διεπαφή διαμέσου της οποίας δέχονται ερωτήματα. Στην περίπτωση της χρήσης ενός ασθενούς PUF τα δεδομένα που παράγονται από το PUF χρησιμοποιούνται για την παραγωγή των κλειδιών κρυπτογράφησης.

Έτσι λοιπόν, με τη χρήση των PUF, αποφεύγεται η χρήση της μη πτητικής μνήμης για την αποθήκευση των κλειδιών γεγονός που θα εγκυμονούσε πολύ σοβαρούς κινδύνους. Ακόμη, εξ' ορισμού τους τα PUF δεν μπορούν να προβλεφθούν από κάποιον επιτιθέμενο. Τέλος, υφίστανται PUF τα οποία σε περίπτωση φυσικής παραβίασης αλλοιώνεται το χαρακτηριστικό που προσδίδει την τυχαιότητα, ουσιαστικά καταστρέφοντας τα κλειδιά κρυπτογράφησης πριν αυτά υποκλαπούν από τον επιτιθέμενο. Τα ανωτέρω πλεονεκτήματα τα καθιστούν ιδανική λύση για τη φύλαξη κλειδιών κρυπτογράφησης στους ευφυείς μετρητές.

1.3 Ταλαντωτές Δακτυλίου - Ring Oscillators

Οι ταλαντωτές δακτυλίου αποτελούνται από μια σειρά ενισχυτικών σταδίων μέσα σε βρόχο. Η πιο συνηθισμένη τοπολογία φαίνεται στο σχήμα όπου ο ταλαντωτής αποτελείται από έναν περιττό αριθμό (≥3) αναστροφέων με συνολική dc στροφή φάσης 180º τοποθετημένων σε ένα βρόχο ανάδρασης. Με βάση τα κριτήρια ταλάντωσης του Barkhausen, η ταλάντωση θα προκύψει σε εκείνη τη συχνότητα στην οποία η συνολική στροφή φάσης θα ισούται με μηδέν και το κέρδος του κλειστού βρόχου ίσο με τη μονάδα. Μπορεί εύκολα να αποδειχτεί ότι αν έχουμε M αναστροφείς με καθυστέρηση T_d για το κάθε στάδιο, τότε η συχνότητα ταλάντωσης είναι:

$$f_0 = \frac{1}{2MT_d}$$



Οι ταλαντωτές δακτυλίου είναι πολύ εύκολο να υλοποιηθούν ως ολοκληρωμένα κυκλώματα. Παρουσιάζουν όμως υψηλό θόρυβο φάσης και γι' αυτό σπάνια χρησιμοποιούνται σε RF κυκλώματα. Χρησιμοποιούνται όμως συχνά σε ψηφιακά κυκλώματα υψηλής ταχύτητας.

Οι ταλαντωτές δακτυλίου, χαρακτηρίζονται από ευκολία στην σχεδίαση και την ολοκλήρωση, πολλαπλούς τρόπους ελέγχου της συχνότητας, ταυτόχρονη παράγωγή πολλαπλών φάσεων του σήματος εξόδου και σχετικά μεγάλο εύρος συχνοτήτων συντονισμού. Το κύριο μειονέκτημα τους είναι το υψηλό phase noise και η ευαισθησία στις παρεμβολές λόγω του υψηλού τους κέρδους.

Κεφάλαιο 2

2.1 Ταλαντωτές δακτυλίου για τους Δούρειους Ίππους (Trojan Horses)

2.1.1 Εφαρμοσμένες μέθοδοι για την ανίχνευση Δουρείων Ίππων στο υλικό

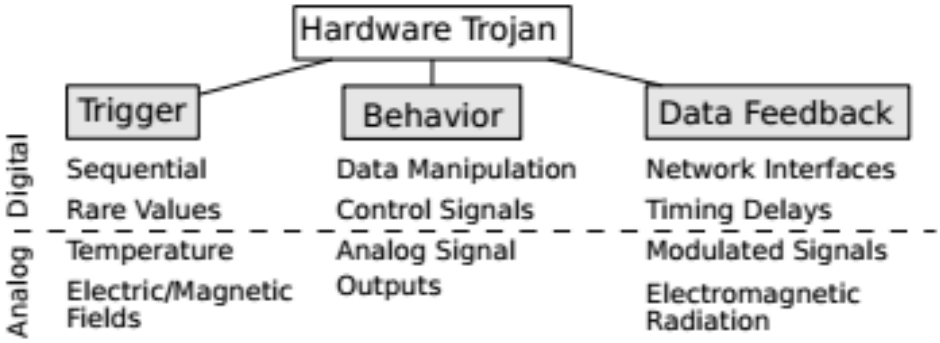
Οι τεχνολογικές εξελίξεις στον τομέα των εφαρμοσμένων συστημάτων εγείρουν σοβαρούς προβληματισμούς σε θέματα ασφάλειας τόσο των ίδιων των συστημάτων όσο και των ενσωμάτων σε αυτά σχεδιασμών κυκλωμάτων. Στους πλέον σύνηθεις σχεδιασμούς, παρουσιάζονται πολλά σημεία από στα οποία μπορεί να εμφανιστεί μία κακόβουλη λειτουργία, όπως αυτή των Δούρειων Ίππων. Η εμφάνιση αυτή μπορεί και να οφείλεται σε κάποιον "αξιόπιστο" σχεδιαστή συστήματα, σε κάποια εισβολή που μπορεί να γίνει από την IP ή ακόμη και στην εισβολή κακόβουλων λειτουργιών κατά την παραγωγική φάση του συστήματος.

Ως Δούρειος Ίππος υλικού χαρακτηρίζεται μία αλλοίωση στο τσιπ σιλικόνης η οποία τελικά επηρεάζει τη συνολική λειτουργία του. Στα πλαίσια της αναγνώρισης της ύπαρξης αλλά και της αντιμετώπισης των αλλοιώσεων αυτών, έχουν αρχίσει να αναπτύσσονται μεθοδολογίες ανίχνευσης που αφορούν στους σχεδιασμούς των ψηφιακών αλλά και των μικτών σημάτων. Βέβαια, μέχρι σήμερα, καμία από αυτές δε μπορεί να εγγυηθεί την πλήρη καταπολέμηση των δούρειων ίππων, μπορεί όμως να αυξήσει τα επίπεδα προστασίας έναντι αυτών.

Μάλιστα, δεν είναι λίγοι οι ερευνητές εκείνοι, οι οποίοι έχουν προτείνει διάφορες ταξινομήσεις και διαχωρισμούς των Δούρειων Ίππων ανάλογα με της τεχνικές που ενεργοποιούνται, τη λειτουργικότητά τους αλλά και τα έως τώρα γνωστά χαρακτηριστικά τους. Οι Δούρειοι Ίπποι βρίσκονται εμφωλευμένοι μέσα σε κάποιο λογισμικό το οποίο πρέπει να εγκατασταθεί στον υπολογιστή ώστε να εκκινήσει η λειτουργία τους. Το μονοπάτι που ακολουθεί συνήθως ένας κακόβουλος επιτιθέμενος είναι αυτό το οποίο έχεις ως στόχο τη διαρροή των πληροφοριών διαμέσου αποστολής πακέτων ή σημάτων.

Πέραν των γνωστών αναλύσεων και στρατηγικών που υπάρχουν έως σήμερα, προτείνονται διάφορες μέθοδοι ανίχνευσης Δούρειων Ίππων που βασίζονται στην αντίστροφη μηχανική ή στην εξέταση τυχαίων δειγμάτων των κυκλωμάτων κατά τη διαδικασία της παραγωγής τους. Ένας Δούρειος Ίππος ο οποίος εντοπίζεται σε ένα τσιπ σιλικόνης μπορεί να διαχωριστεί στον ενεργοποιητή, στην χειραγώγηση των δεδομένων και στην ανατροφοδότηση. Κάθε ένα από τα στοιχεία αυτά, μπορεί να λειτουργήσει ανεξάρτητα, θα πρέπει όμως να συνενωθεί με τα υπόλοιπα ώστε να αποκτήσει κακόβουλο χαρακτήρα και να λειτουργήσει εναντίον του συστήματος.

Οι ενεργοποιητές συνήθως, συνήθως εξετάζουν τις τιμές εισόδου ή τους αστερισμούς των σημάτων ώστε να προβούν στην ενεργοποίηση των Δούρειων Ίππων. Έτσι, είναι συνήθως δύσκολο να εντοπιστούν κατά τη διάρκεια της διαδικασίας παραγωγής. Η μονάδα χειραγώγησης των δεδομένων, επηρεάζει άμεσα τις εσωτερικές λειτουργίες του τσιπ και έτσι δεν μπορεί σε καμία περίπτωση να διασφαλιστεί η ασφαλής λειτουργία του κυκλώματος. Κύριος στόχος ενός Δούρειου Ίππου δεν είναι η διαρροή των πληροφοριών αλλά η καταστροφή μίας συγκεκριμένης λειτουργίας. Η ανατροφοδότηση των πληροφοριών προς έναν επιτιθέμενο γίνεται διαμέσου των στοιχείων που συμμετέχουν στην επικοινωνία ή άμεσα εάν έχουν πειραχθεί τα pins του τσιπ. Η μεταφορά των δεδομένων όμως, μπορεί να μην επηρεάσει τη λειτουργία του συστήματος στην οποία ενδεχόμενα να στοχεύει ο επιτιθέμενος, παρόλα αυτά του δίνει πληροφορίες για τον και πότε αυτός μπορεί να έχει πρόσβαση στην πληροφορία.



Εικόνα 1 : Διαχωρισμός των μερών από τα οποία αποτελείται ένας Δούρειος Ίππος

Όπως φαίνεται και στην παραπάνω εικόνα, τα μέρη από τα οποία αποτελείται ένας Δούρειος Ίππος δε στοχεύουν μόνο στην ψηφιακή λειτουργία του κυκλώματος αλλά αναφέρονται και στην αναλογική λειτουργία αυτών καθώς στοχεύουν στα μεικτά σήματα.

Περνώντας λοιπόν στην ανίχνευση των Δούρειων Ίππων, αυτή μπορεί να χαρακτηριστεί ως η αξιολόγηση της λειτουργίας του κυκλώματος, της δομής και των λειτουργικών αλληλεπιδράσεων που συντελούνται στα διάφορα επίπεδα αφαίρεσης του κυκλώματος.

Οι Michael Rathmair, Florian Schupfer και Christian Krieg (2014) πρότειναν διάφορες μεθόδους ανίχνευσης των Δούρειων Ίππων συζητώντας τα πλεονεκτήματα και τα μειονεκτήματα κάθε μίας από αυτές. Οι μέθοδοι αυτοί, αξιολογούνται με βάση τα επίπεδα ασφάλειας έναντι των Δούρειων Ίππων και είναι οι παρακάτω :

- **Έλεγχος Ιδιοκτησίας** : Οι αλγόριθμοι ελέγχου του μοντέλου λειτουργούν με βάση έναν αριθμό πεπερασμένων παραστάσεων (M) σε μία συνάρτηση του συστήματος και ελέγχουν εάν μία ιδιότητα (p) ακολουθεί τα πρότυπα του μοντέλου. Οι ιδιότητες διαμορφώνονται μέσα προτασιακές χρονικές λογικές (PTL) και περιλαμβάνουν όλους τους ελέγχους που διεξάγονται κατά μήκος του μονοπατιού που ακολουθεί το μοντέλο ή σε μία και μόνο κατάσταση. Αρχικά, επιλέγεται ένα πεδίο το οποίο αντιπροσωπεύει μία σειρά αφηρημένων ιδιοτήτων *Pabstract, n* οι οποίες καθορίζονται με μία φυσική γλώσσα. Στη συνέχεια, και με βάση τη συνάρτηση $P_{abstract,1} = \{p_1, p_2, p_3, \ldots\}$ όλες οι αφηρημένες συναρτήσεις μετατρέπονται σε ένα σύνολο από PTL οι οποίες υιοθετούνται κατά τη διάρκεια του σχεδιασμού. Τέλος, οι ήδη εντοπισμένες κακόβουλες συναρτήσεις, αναστρέφονται και διακομίζονται προς το ανάλογο εργαλείο ελέγχου. Για να αναγνωριστεί μία κακόβουλη ιδιότητα φ_t θα πρέπει να ικανοποιηθεί η συνθήκη *pk* στο μοντέλο.
  Η μέθοδος αυτή, εξαρτάται από το βαθμό στον οποίο έχουν καταγραφεί τα χαρακτηριστικά των κακόβουλων συναρτήσεων. Εάν μία κακόβουλη ιδιότητα δεν ταυτοποιηθεί, τότε ένας Δούρειος Ίππος ενδεχόμενα να παραμένει κρυμμένος μέσα στο μοντέλο. Ένα ακόμη μειονέκτημα της μεθόδου αυτής είναι η αδυναμία στην κλιμάκωση τη στιγμή κατά την οποία η πολυπλοκότητα στο σχεδιασμό των συστημάτων και των μερών που λαμβάνουν χώρα σε αυτά αυξάνεται εκθετικά.
- **Ανάλυση προσβασιμότητας** : Η ανάλυση αυτή αξιολογεί τις καταστάσεις ενός μοντέλου πεπερασμένων καταστάσεων οι οποίες είναι προσβάσιμες από συναρτήσεις ενεργοποίησης μεταβάσεων. Η ενεργοποίηση ενός δούρειου ίππου μέσα στο σύστημα ενδέχεται να οδηγήσει σε καταστάσεις στις οποίες το σύστημα πλέον δε θα έχει πρόσβαση. Έτσι, οι καταστάσεις αυτές, μπορεί να οδηγήσουν σε διαρροή πληροφορίας αλλά και σε χειραγώγηση της συμπεριφοράς του συστήματος.

Σε ότι αφορά στην ανίχνευση των Δούρειων Ίππων η μέθοδος αυτή παρουσιάζει περιορισμούς και ιδιαίτερα στην περίπτωση όπου ο Ίππος δε θα προσθέσει επιπλέον καταστάσεις στο σύστημα. Επιπλέον, η μέθοδος απαιτεί λεπτομερή γνώση της δομής και της συμπεριφοράς του κυκλώματος αλλά και των καταστάσεων του συστήματος. Έτσι, δεν είναι η πλέον ιδανική για την περίπτωση των Δούρειων Ίππων.

- **Έλεγχος Ισοτιμίας** : Στον έλεγχο ισοτιμίας τα σχέδια αλλά και τα χαρακτηριστικά του συστήματος ενδέχεται να μετατραπούν σε ένα διάγραμμα ROBDD (Reduced Ordered Binary Decision Diagram) το οποίο καταλήγει σε μία κανονικοποιημένη μορφή που αποτελεί μοναδική αναπαράσταση της ψηφιακής λογική και συμπεριφοράς του συστήματος.

  Σε ότι αφορά την ανίχνευση των Δούρειων Ίππων σε επίπεδο υλικού, η μέθοδος αυτή παρουσιάζεται να είναι ιδιαίτερα υποσχόμενη και μάλιστα σε διάφορα επίπεδα αφαιρετότητας του συστήματος. Η μέθοδος βασίζεται στη συνάρτηση

  $$f_n \equiv f_m \text{ iff } i_n \equiv i_m \wedge o_n \equiv o_m \wedge \varphi_n \equiv \varphi_m$$

- **Έλεγχος δομικού σχεδιασμού** : Οι έλεγχοι της μορφής αυτής βασίζονται στις διασυνδέσεις μεταξύ των κανονικοποιημένων μοντέλων συστημάτων. Απαραίτητη προϋπόθεση ώστε να διεξαχθούν οι έλεγχοι αυτοί είναι η πλήρης γνώση της υλοποίησης του συστήματος. Το παραπάνω σημαίνει ότι τα κελιά και οι διασυνδέσεις θα πρέπει να συνδέονται άμεσα με ένα λειτουργικό μπλοκ του σχεδιασμού. Παρόμοια με τον έλεγχο του δομικού σχεδιασμού είναι και η δομική ανάλυση η οποία εστιάζει όμως στον εντοπισμό των Δούρειων Ίππων σε επίπεδο υλικού.

2.1.2 Εμφάνιση των Δούρειων Ίππων σε επίπεδο Υλικού - Τρέχουσες τάσεις και προσεγγίσεις

Όπως αναφέρθηκε και στην προηγούμενη ενότητα, οι σχεδιασμοί των ολοκληρωμένων κυκλωμάτων τείνουν να γίνονται όλο και πιο σύνθετοι καθιστώντας τις εταιρίες παραγωγής ημιαγωγών όχι ικανές στο να παράγουν πάντα τον ιδιαίτερα μικρού μεγέθους εξοπλισμό που απαιτείται. Το παραπάνω, οδηγεί σε outsourcing της παραγωγής σε άλλες εταιρίες σε πολλά και διαφορετικά μέρη του κόσμου. Αυτό, οδηγεί πολλές φορές σε κακόβουλη αλλοίωση του σχεδιασμού των ηλεκτρονικών κυκλωμάτων χωρίς να το γνωρίζει η εταιρία παραγωγής των ημιαγωγών.

Οι διαφορετικοί τύποι χειραγώγησης των ολοκληρωμένων κυκλωμάτων είναι και αυτοί που εξασθενούν την άμυνα του συστήματος ενώ την ίδια στιγμή παρέχουν μη εξουσιοτημένη πρόσβαση στο σύστημα και στις διάφορες λειτουργίες του. Η χειραγώγηση αυτή του συστήματος και διαγραφή ή η τροποποίηση του αρχικού σχεδιασμού είναι γνωστή και ως Δούρειο Ίππος υλικού.

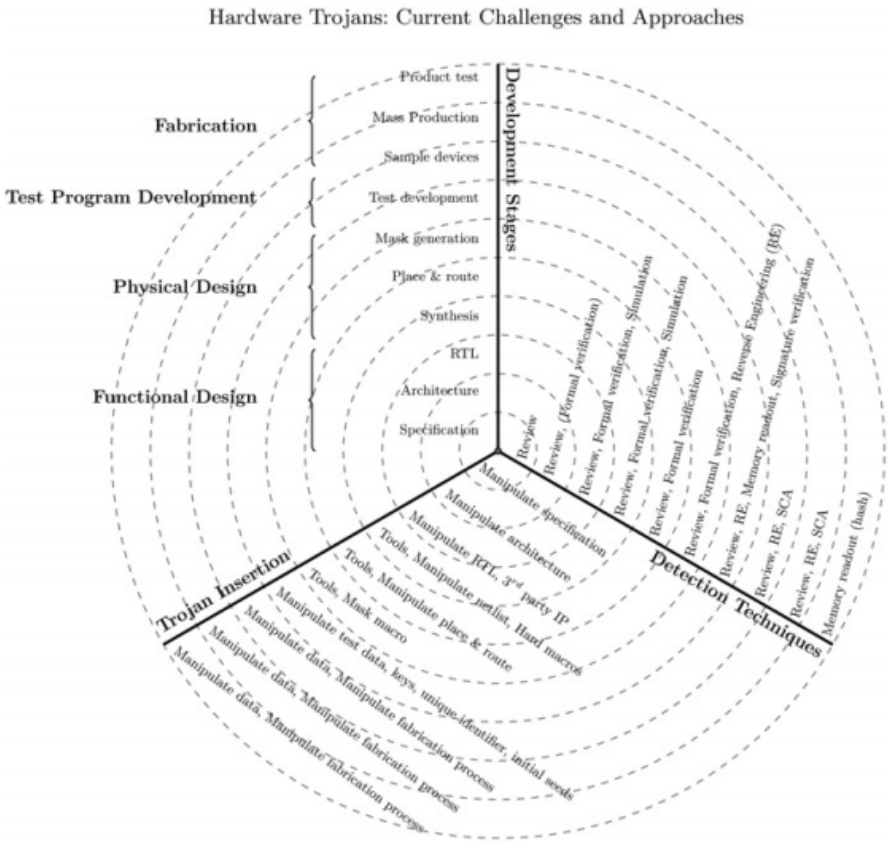
Οι Δούρειοι Ίπποι, αποτελούν απειλή όχι μόνο για τις ευαίσθητες συσκευές που χρησιμοποιούνται σε στρατιωτικά ή οικονομικά συστήματα, αλλά και για τις ίδιες τις οικιακές συσκευές. Το βασικό πλεονέκτημά τους έγκειται στο γεγονός ότι μπορούν να έχουν πρόσβαση σε ολόκληρη τη γραμμή παραγωγής των τσιπ καθώς παρεμβαίνουν στο σχεδιασμό ή τη διαδικασία παραγωγής τους. Κάποια από τα βασικά χαρακτηριστικά των Δούρειων Ίππων είναι :

1. Δεν αλλάζουν τη φυσική μορφή και των αριθμό των εισόδων και των εξόδων του ολοκληρωμένου κυκλώματος
2. Είναι μικρότεροι κατά τουλάχιστον 3-4 τάξεις μεγέθους του πλάτους του αρχικού κυκλώματος
3. Παραμένουν μη αναγνωρίσιμοι κατά τη διάρκεια των φάσεων δοκιμών
4. Λειτουργούν συγκεκαλυμμένα κατά την κανονική λειτουργία του ολοκληρωμένου κυκλώματος

Η ανάπτυξη των ημιαγωγών ακόμη και σήμερα αποτελεί μία ιδιαίτερα πολύπλοκη διαδικασία και έτσι η τόσο η εισαγωγή των Δούρειων Ίππων στα ολοκληρωμένα κυκλώματα

όσο και η προσπάθεια προστασίας από αυτούς αποτελεί μία ιδιαίτερα δύσκολη και δυσνόητη διαδικασία.

Έτσι λοιπόν, και σύμφωνα με τα όσα υποστηρίζουν οι Nisha et al (2014) στην έρευνά τους, η διαδικασία παραγωγή των ολοκληρωμένων κυκλωμάτων μπορεί να διαχωριστεί σε τέσσερις διαφορετικές φάσεις όπως αυτές παρουσιάζονται στην εικόνα που ακολουθεί. Όπως μπορεί κανείς να παρατηρήσει, η πιθανότητα εισαγωγής ενός Δούρειου Ίππου εμφανίζεται σε πολλά σημεία και έχει διαφορετικές επιπτώσεις στο σύστημα. Στο κάτω και δεξιά άκρο μπορεί κανείς να παρατηρήσει τις τεχνικές ανίχνευση και εντοπισμού των Δούρειων Ίππων με βάση πάντα τις τεχνικές που μπορούν να χρησιμοποιηθούν.



Εικόνα 2 : Φασης παραγωγής και σχεδιασμού ολοκληρωμένων κυκλωμάτων

Οι σχεδιασμοί των Δούρειων Ίππων υλικού μπορούν να περιγραφούν με βάση τις φυσικές ιδιότητές τους, τη μέθοδο ενεργοποίησης που χρησιμοποιούν αλλά και τα χαρακτηριστικά δράσης τους. Επιπλέον, μπορούν να χαρακτηριστούν με βάση τις παρακάτω ιδιότητες :

- Τύπος : Περιγράφει εάν υπάρχει κάποια αλλοίωση ή διαγραφή των πυλών ή κάποια τροποποίηση των καλωδίων.
- Μέγεθος : Ο αριθμός των στοιχείων που περιλαμβάνεται σε ένα κύκλωμα Δούρειου Ίππου
- Δομή : Αναφέρεται στο εάν έχουν γίνει ή όχι τροποποιήσεις στο αρχικό σχέδιο
- Διανομή : Περιγράφει εάν το κύκλωμα ενεργοποιητής και το κύκλωμα payload έχουν τοποθετηθεί ή όχι μαζί
- Χαρακτηριστικά ενεργοποίησης : Περιγράφει τα χαρακτηριστικά ενεργοποίησης του σήματος :
    - Εξωτερικό σήμα : Με τον τρόπο αυτό οι επιτιθέμενοι μπορούν να ενεργοποιήσουν το Δούρειο Ίππο τη στιγμή που αυτοί επιθυμούν
    - Εσωτερικό Σήματα : Αναφέρεται στους Ίππους που είναι πάντα ενεργοί ή ενεργοποιούνται από κάποια τιμή που θα λάβει ο αισθητήρας
- Χαρακτηριστικά ενεργοποίησης : Περιγράφουν τα χαρακτηριστικά του Payload :
    - Λειτουργία τροποποίησης : Αναφέρεται στους Δούρειους Ίππους στου αλλοιώνουν την λειτουργία για την οποία έχει σχεδιαστεί το ολοκληρωμένο κύκλωμα
    - Μετάδοση πληροφορίας : Δούρειοι Ίπποι που διαρρέουν πληροφορία
    - Άρνηση της υπηρεσίας (DoS) : Δούρειοι Ίπποι οι οποίοι είτε περιστασιακά είτε μόνιμα δημιουργούν πρόβλημα στην παροχή υπηρεσιών

Παρακάτω αναλύονται οι τρόποι με τους οποίους οι Δούρειοι Ίπποι μπορούν να εισαχθούν σε ένα ολοκληρωμένο κύκλωμα στις διάφορες φάσεις δημιουργίας και εκμετάλλευσης αυτού. Ειδικότερα :

- **Λειτουργικός σχεδιασμός** : Ένας Δούρειος Ίππος μπορεί να χειραγωγήσει το λειτουργικό σχεδιασμό παρεμβαίνοντας στην αρχιτεκτονική ή στους κανόνες λειτουργίας του ή επιτρέποντας την εισαγωγή άλλων κακόβουλων λογισμικών διαμέσου των IP πυρήνων. Το στάδιο του λειτουργικού σχεδιασμού μπορεί να επηρεαστεί από :
    - *Κάποιον κακόβουλο εντός της εταιρίας παραγωγής του ημιαγωγού* : Πρόκειται για κάποιον που έχει μη εξουσιοδοτημένη πρόσβαση στο λειτουργικό

σχεδιασμό παρόλα αυτά όμως μπορεί να λειτουργήσει με τρόπο τέτοιο ώστε να διευκολύνει την εισβολή των Δούρειων Ίππων στις μετέπειτα φάσεις.

- *Τρίτα μέρη* : Οι τρίτοι (third parties) έχουν πάντα τη δυνατότητα ώστε να πηρεάσουν το σύστημα. Πρόκειται συνήθως για έναν εργολάβο που παράγει και επεξεργάζεται συγκεκριμένα μέρη του συστήματος και έτσι μπορεί να συμπεριλάβει σε αυτά κακόβουλα στοιχεία.

- **Φυσικός σχεδιασμός** : Και στη φάση αυτή σχεδιασμού μπορούν να υπάρξουν αλλοιώσεις από τους διαφορετικούς τύπους Δούρειων Ίππων που μπορούν να εισέλθουν στο σύστημα. Έτσι το σύστημα μπορεί να επηρεαστεί από :
  - *Κάποιον κακόβουλο εντός της εταιρίας παραγωγής του ημιαγωγού* : Κάποιος κακόβουλος εντός της εταιρίας παραγωγής ενδέχεται να τροποποιήσει τα αρχεία σχεδιασμού και να εισάγει μακροεντολές, κατά τη διάρκεια τη σύνθεσης. Επιπλέον, μπορεί να "πειράζει" ακόμη και τα ίδια τα εργαλεία σχεδιασμού
  - *Τρίτα μέρη* : Οι πάροχοι των IP ενδεχόμενα να μην προβαίνουν σε επαρκείς ελέγχους εισβολών και να παρουσιάζουν κενά ασφάλειας στα συστήματά τους. Επιπρόσθετα, οι εταιρίες παραγωγής ημιαγωγών χρησιμοποιούν εργαλεία αυτόματου ηλεκτρονικού σχεδιασμού σε πολλά στάδια του σχεδιασμού. Μια κακόβουλη εισβολή στα εργαλεία αυτά μπορεί να επηρεάσει το σχεδιασμό του υλικού για πολλές εταιρίες.
- **Ανάπτυξη του προγράμματος ελέγχου** : Τα προγράμματα ελέγχου μπορούν και αυτά με τη σειρά τους να παραβιαστούν είτε από κάποιον κακόβουλο εντός της εταιρίας είτε από τρίτα μέρη.
  - *Κακόβουλος εντός της εταιρίας παραγωγής του ημιαγωγού* : Ο κακόβουλος εντός της εταιρίας μπορεί να τροποποιήσει τα κλειδιά ή να προσθέσει επιπλέον κλειδιά κατά τη διάρκεια ανάπτυξης των τεστ. Ακόμη, μπορεί να εισάγει αλλοιώσεις στον boot loader της συσκευής.
  - *Τρίτα μέρη* : Και στην περίπτωση αυτή, το κακόβουλο λογισμικό μπορεί να εισχωρήσει από τους παρόχους των IP.
- **Κατασκευή** : Οι διάφορες κακόβουλες χειραγωγήσεις μπορούν επίσης να γίνουν και κατά το χρόνο παραγωγής καθώς το κακόβουλο προσωπικό ή τα τρίτα μέρη μπορούν να επηρεάσουν τη διαδικασία αυτή.
  - *Κακόβουλο προσωπικό εντός του χυτηρίου* : Το προσωπικό έχει συνήθως πρόσβαση τόσο στη διαδικασία παραγωγής όσο και στα εργαλεία. Έτσι

λοιπόν, μπορούν να εισχωρήσουν ένα Δούρειο Ίππο στο ολοκληρωμένο κύκλωμα με πολλούς και διαφορετικούς τρόπους.

- *Τρίτα μέρη* : Τη διαδικασία της παραγωγής μπορούν να επηρεάσουν τα εργαλεία που προέρχονται από συνεργάτες και χρησιμοποιούνται στα χυτήρια

Παρακάτω αναλύονται όλοι οι πιθανοί τρόποι με τους οποίους θα μπορούσε δυνητικά να γίνει ανίχνευση των Δούρειων Ίππων στα διαφορετικά στάδια παραγωγής των ολοκληρωμένων κυκλωμάτων.

- **Λειτουργικός Σχεδιασμός** : Οποιαδήποτε κακόβουλη εισβολή στο στάδιο αυτό μπορεί να εντοπιστεί στο πλαίσιο του λεπτομερούς επανέλεγχου. Επιπρόσθετα, δυνατότητα εντοπισμού υπάρχει αρχιτεκτονικής αρκεί να ακολουθηθεί τυπική επαλήθευση η οποία μπορεί να υπάρξει μόνο και εάν οι οποιεσδήποτε ιδιότητες έχουν καθοριστεί επίσημα.
- **Φυσικός σχεδιασμός** : Στο στάδιο αυτό, ως τεχνικές ανίχνευσης Δούρειων Ίππων μπορούν να χρησιμοποιηθούν ο επανέλεγχος, η τυπική επαλήθευση και η λειτουργική ανάλυση του σχεδιασμού. Οι τεχνικές τυπικής επαλήθευσης μπορούν να χρησιμοποιηθούν ώστε να επιβεβαιώσουν τα αποτελέσματα που ακολουθούν της σύνθεσης. Μετά τη διαδικασία παραγωγής μάσκας. ο σχεδιασμός θα πρέπει να εξαχθεί έτσι ώστε να διασφαλιστεί ότι δεν υπάρχει κάποιο κακόβουλο στοιχείο μέσα σε αυτόν ή ότι δεν έχει γίνει κάποια αλλοίωση.
- **Ανάπτυξη προγράμματος ελέγχου** : Το επόμενο στάδιο στην ανάπτυξη των ολοκληρωμένων κυκλωμάτων είναι αυτό του ελέγχου του προτύπου ανάπτυξης. Στο στάδιο αυτό μπορούν να διεξαχθούν διάφοροι έλεγχοι αυθεντικότητας και ακεραιότητας μέσα σε ένα τσιπ όταν θα έχουν περαστεί σε αυτό όλα τα προγράμματα τα οποία καλείται να χρησιμοποιήσει. Βέβαια, αυτό απαιτεί κρυπτογραφημένα μέρη τα οποία να παρίστανται στο τσιπ. Όλα τα στοιχεία της μνήμης που έχουν χρησιμοποιηθεί στο πρόγραμμα ελέγχου μπορούν να αναγνωστούν σε ανάλογες συσκευές ελέγχου αρκεί μόνο το τσιπ να μη βρίσκεται σε κατάσταση λειτουργίας όπου δεν είναι αναγνώσιμη η μνήμη του.
- **Παραγωγή** : Οι διάφορες μέθοδοι ανίχνευσης Δούρειων Ίππων που χρησιμοποιούνται κατά τη διαδικασία παραγωγής είναι η οπτική εξέταση, η λειτουργική ανάλυση, η ανάλυση πλευρικού καναλιού και η ανάγνωση της μνήμης.
    - *Οπτική εξέταση* : Κάθε επίπεδο του ολοκληρωμένου κυκλώματος φωτογραφίζεται και εξετάζεται λεπτομερώς για οποιαδήποτε προσθήκη,

διαγραφή ή αλλοίωση στο σχεδιασμό. Η τεχνική αυτή έχει ένα υψηλό επίπεδο ασφάλειας και είναι αποδοτική ακόμη και για αλλαγές απειροελάχιστου μεγέθους. Σημαντικό μειονέκτημά της είναι το κόστος που εισάγει καθώς απαιτεί εξειδικευμένο εξοπλισμό.

- *Λειτουργική ανάλυση* : Η μέθοδος αυτή αποτελεί ένα εργαλείο ελέγχου που συντελείται καθώς τελειώσει η διαδικασία παραγωγής. Έχει χαμηλό κόστος αλλά οι έλεγχοι αφορούν αποκλειστικά την καλή λειτουργία του ολοκληρωμένου κυκλώματος. Οι Δούρειοι Ίπποι είναι σχεδιασμένοι έτσι ώστε να μην είναι αντιληπτοί σε αυτοί τη φάση γεγονός που καθιστά τα εργαλεία αυτά αναποτελεσματικά.
- *Ανάλυση πλευρικού καναλιού (Side Channel Analysis - SCA)* : Πρόκειται για τη μέθοδο που προσμετρά φυσικές ιδιότητες όπως είναι η ισχύς, η τάση και η καθυστέρηση με κάποιες στατιστικές μεθόδους. Έχει χαμηλό κόστος και είναι ιδιαίτερα αποτελεσματική. Η κύρια πρόκληση που καλείται να αντιμετωπίσει η τεχνική αυτή είναι ο θόρυβος που προκαλείται από το περιβάλλον. Στην περίπτωση των Δούρειων Ίππων παραμένει ενεργό συνεχόμενα μονάχα το κύκλωμα ενεργοποίησης το οποίο είναι πολύ μικρό και αποτελείται από μερικές πύλες που πολλές φορές μπορεί να μην αντιληπτές από την SCA λόγω των υψηλών επιπέδων θορύβου. Έτσι λοιπών, ο εντοπισμός των Δούρειων Ίππων γίνεται μόνο στην περίπτωση όπου το κύκλωμα ενεργοποιητής δεν είναι μικρότερο από 3-4 τάξεις μεγέθους από το αρχικό κύκλωμα.

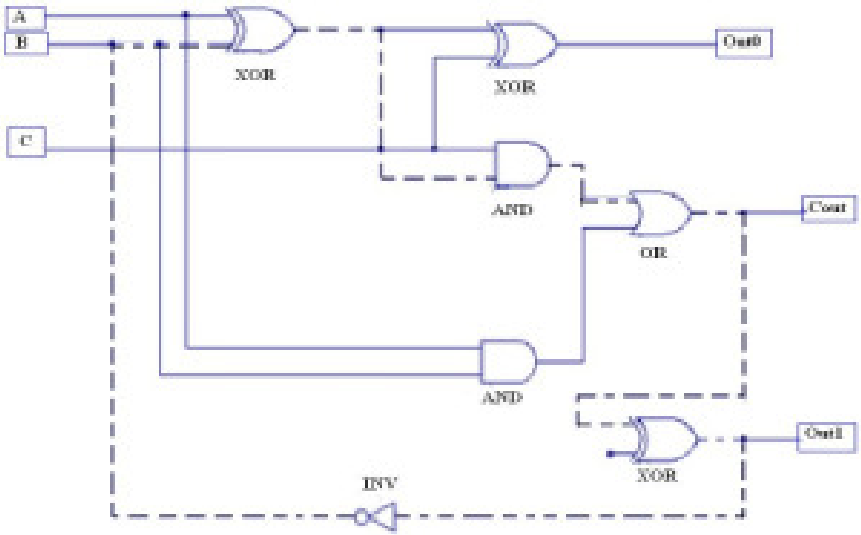
- **Τροποποίηση Δομής** : Η τροποποίηση της δομής αναφέρεται στις αλλαγές στο αρχικό κύκλωμα κατά το χρόνο σχεδιασμού που συντελούνται όταν εισάγοντα καινούρια κυκλωματικά στοιχεία ή αναδιανέμονται τα παλιά. Το παραπάνω γίνεται με στόχο να ενισχυθεί η ανίχνευση των Δούρειων Ίππων σε συνεργασία πάντα με άλλες τεχνικές ανίχνευσης όπως είναι η καθυστέρηση ή οι λογικοί έλεγχοι.
- **Ανάγνωση μνήμης** : Από τη στιγμή που τεχνικές όπως η οπτική εξέταση ή η SCA μπορεί να μην είναι αποτελεσματικές, θα μπορούσε να γίνεται ανάγνωση της μνήμης του κάθε ολοκληρωμένου κυκλώματος μετά τη μαζική παραγωγή του.

Τόσο το κόστος, όσο και η προσπάθεια εισαγωγής των Δούρειων Ίππων στα ολοκληρωμένα κυκλώματα αυξάνονται σε κάθε βήμα σχεδιασμού. Το ίδιο ισχύει και για τις τεχνικές εντοπισμού τους σε κάθε φάση ανάπτυξης. Καθώς αυξάνονται τα στάδια, αυξάνεται και η

πολυπλοκότητα αλλά και ο χρόνο που απαιτείται ώστε να γίνει ο εντοπισμός των Δούρειων Ίππων.

2.1.3 Υλοποιήσεις κυκλωμάτων που περιλαμβάνουν Ταλαντωτές Δακτυλίων

Οι Ameya Nayak, Kang Yen, και Jeffrey Fan (2014) προέβησαν στο σχεδιασμό ενός Δούρειου Ίππου που θα προβαίνει σε κακή λειτουργία του κυκλώματος και θα δίνει λανθασμένες εξόδους όταν ενεργοποιείται. Το κύκλωμα που έχει σχεδιαστεί περιλαμβάνει ένα RO (Ring Oscillator) το οποίο όμως δεν εμφανίζεται στο σχήμα που ακολουθεί. Ο Δούρειος Ίππος εισάγεται στη φάση του σχεδιασμού και θα ενεργοποιηθεί εξωτερικά με την είσοδο του χρήστη. Το payload, συνδέεται με το αρχικό κύκλωμα και κρατά το μέγεθος του Δούρειου Ίππου μικρό ενώ την ίδια στιγμή τον τοποθετεί έξω από το RO και μπροστά από το δίκτυο εξόδου. Η έξοδος του μετρητή αποστέλλεται στην πύλη OR ενώ η δεύτερη είσοδος έρχεται από τον Αθροιστή. Έτσι, η έξοδος του κυκλώματος θα είναι 1111 για πολλαπλούς συνδυασμούς εισόδου.



Εικόνα 3 : Το κύκλωμα που χρησιμοποιήθηκε

Μία αποδεκτή μέθοδος για την ανίχνευση των Δούρειων Ίππων είναι η συνάρτηση PUF. Ένα RO δίκτυο από την άλλη, είναι ένα στοιχείο το οποίο ενσωματώνεται σε ένα κύκλωμα και έχει λειτουργία ενός ανιχνευτή Δούρειου Ίππου. Ένα RO αποτελείται από πολυπλέκτες και πύλες και έχει δυο μορφές λειτουργίας, τη μορφή ελέγχου και τη λειτουργική μορφή. Το RO αυτό, έχει ως στόχο την ανίχνευση των Δούρειων Ίππων όταν είναι στη μορφή ελέγχου ενώ

απενεργοποιείται τελείως όταν είναι στη λειτουργική κατάσταση ώστε το κύκλωμα να εκτελεί την κανονική του λειτουργία.

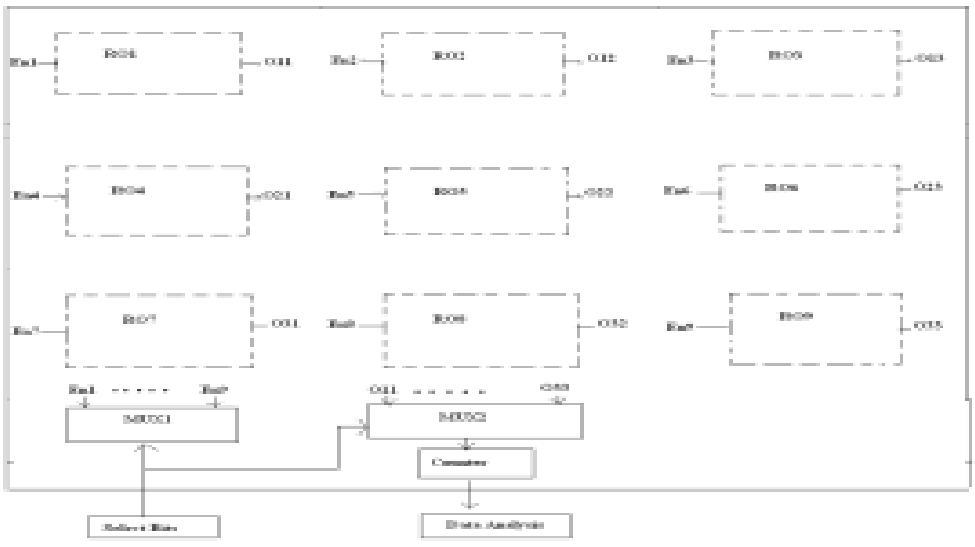
Κάθε φορά λοιπόν που εισάγεται στο δίκτυο ένα διάνυσμα ελέγχου, οι πολυπλέκτες, οι αντιστροφείς και οι πύλες σχηματίζουν έναν βρόγχο που καταλήγει στην ενεργοποίηση του RO και το κάνουν να ταλαντώνεται. Η συχνότητα στο σημείο αυτό υπολογίζεται με τη χρήση του μετρητή.

Από τη στιγμή που εισαγωγή επιπλέον πυλών που εκτελούν κακόβουλες λειτουργίες θα επιφέρουν αλλαγή στη συχνότητα, τα κυκλώματα με και χωρίς Δούρειους Ίππου αναμένονται να είναι διαφορετικά. Εάν η διαφορά αυτή στη συχνότητα βρίσκεται εκτός των σημείων ανοχής τότε επιβεβαιώνεται η ύπαρξη των Δούρειων Ίππων εντός του κυκλώματος.

Το κύκλωμα που σχεδιάστηκε, αποτελείται από 4 πύλες XOR και δύο AND σε συνδυασμό με έναν αναστροφέα. Ο βρόγχος που σημειώνεται με παύλες στο σχήμα ορίζεται ως Ταλαντωτής Δακτυλίου (RO). Η έξοδος από την πύλη XOR προωθείται στον αναστροφέα και γίνεται είσοδος στο σημείο B. Οι συνδυασμοί εισόδου φυσικά και θα μπορούσαν να είναι πολλές αλλά οι έξοδοι από το RO θα παρουσιάσουν την ίδια συχνότητα.

Η ιδέα της υλοποίησης του κυκλώματος αυτού εντοπίζεται στην είσοδο ενός Δούρειου Ίππου στο σημείο στο οποίο δεν καλύπτεται από το RO.

Οι ερευνητές, χρησιμοποίησαν μία αρχιτεκτονική δικτύου RON (Ring Oscillator Network) και προσπάθησαν να εντοπίσουν την ύπαρξη ενός Δούρειου Ίππου από την ένδειξη αλλαγή συχνότητας στο RO. Στην εικόνα που ακολουθεί φαίνεται η αρχιτεκτονική του δικτύου που σχεδιάστηκε.



Εικόνα 4 : Αρχιτεκτονική Δικτύου

Στην αρχιτεκτονική αυτή, ενσωματώνονται διάφορα RO στο σχεδιασμό του κυκλώματος τα οποία θα ενεργοποιηθούν με την εισαγωγή ενός ή και περισσοτέρων bit. Για να μετρηθούν τα αποτελέσματα, χρησιμοποιήθηκαν επίσης πολλαπλές FPGAs. Η διαφορά στις συχνότητες που καταμετρήθηκαν ήταν της τάξεως του 6,6%, οριακά δηλαδή με βάση τους κανόνες που υφίστανται και έτσι ήταν δύσκολο να επιβεβαιωθεί η ύπαρξη ενός Δούρειου Ίππου στο κύκλωμα.

Όταν οι συχνότητες του RO καταμετρήθηκαν σε ένα framework που βασίζεται σε FPGA, παρατηρήθηκαν αλλαγές στη συχνότητα για κάθε Δούρειο Ίππο που εισήχθη εντοπίστηκαν να είναι εντός των πλαισίων ανοχής. Η συνθήκη ενεργοποίησης του Δούρειου Ίππου, αυξάνει το φόρτο σε κάποιος εσωτερικούς κόμβους στο σύστημα αλλά ο φόρτος αυτός δεν είναι αρκετός ώστε να επιβεβαιώσει την ύπαρξη κακόβουλου λογισμικού.

Στη συνέχεια, χρησιμοποιήθηκε ένα διαφορετικό σχήμα το οποίο περιλάμβανε RO σε όλο το μήκος του σχεδιασμού του. Και στην περίπτωση αυτή δεν παρατηρήθηκε καμία σημαντική διαφορά σε ότι αφορά στις τιμές που λήφθηκαν από τις συχνότητες που καταμετρήθηκαν.

Οι Sumanthi et al, (2015), μελέτησαν ένα σενάριο που αφορούσε στην ανίχνευση των Δούρειων Ίππων σε FPGA συσκευές ενώ παράλληλα πρότειναν μια τεχνική ανίσχνευσης αυτών. Το σενάριο αυτό βασίζεται σε DSDPC ή αλλιώς Delay Signatures at Different Process Corners, και βασίζεται στην τεχνικη ανίσχνευσης Δούρειων Ίππων για FPGAs. Για να γίνει λοιπόν ο απαραίτητος έλεγχος με βάση το προφίλ αυτό, θα πρέπει να αποθυκευθεί το προφίλ καθυστέρησης του αρχικού net list. Μετά το τέλος της κάθε χρονικής περιόδου, το προφίλ καθυστέρησης που εξάγεται συγκρίνεται με το αρχικό με στόχο να ελεγχθεί εάν υπάρχει οποιαδήποτε αλλοίωση. Η προτεινόμενη αυτή μέθοδος, βελτιστοποιεί τη διαδικασία ανίχνευσης καθώς πρόκειται για μία μέθοδο μη-καταστροφική και μη-παρεμβατική που δε χρειάζεται επιπλέον κυκλωματικά στοιχεία για την ανίχνευση των Ίππων.

Η αύξηση της χρήσης των FPGA στις κρίσιμες εφαρμογές οδήγησε τους σχεδιαστές κυκλωμάτων να λαμβάνουν σοβαρά υπόψη τους το θέμα της ασφάλειας ακόμη και σε επίπεδο σχεδιασμού. Οι σημαντικότερες παράμετροι που λαμβάνουν χώρα στο σχεδιασμό των ολοκληρωμένων κυκλωμάτων είναι η τάση της παροχής (Vdd), η θερμοκρασία λειτουργίας (T), και η καθυστέρηση του κυκλώματος (D). Η καθυστέρηση λοιπόν, εκφράζεται με βάση τον παρακάτω τύπο :

$$Delay \propto [\ (\ C_{out}\ .\ V_{dd}\ )\ /\ I_{d}\ ]$$

όπου το C_{out}, σηματοδοτεί το φόρτο εξόδου, το Vdd την τάση παροχής και το Id το ρεύμα. Από τη συνάρτηση αυτή καθίσταται ξεκάθαρο ότι το Id μπορεί να εκφραστεί επίσης και ως

$$I_d \propto [\mu(T)(V_{dd} - V_{th}(T))\hat{}\alpha]$$

όπου μ είναι η κινητικότητα, V_{th} το κατώφλι της τάσεως και α η ταχύτητα το ρεύματος. Η θερμοκρασία του ρεύματος εξαρτάται άμεσα από τις δύο παραπάνω συνιστώσες και η εξάρτηση αυτή μπορεί ακόμη να γραφεί και ως

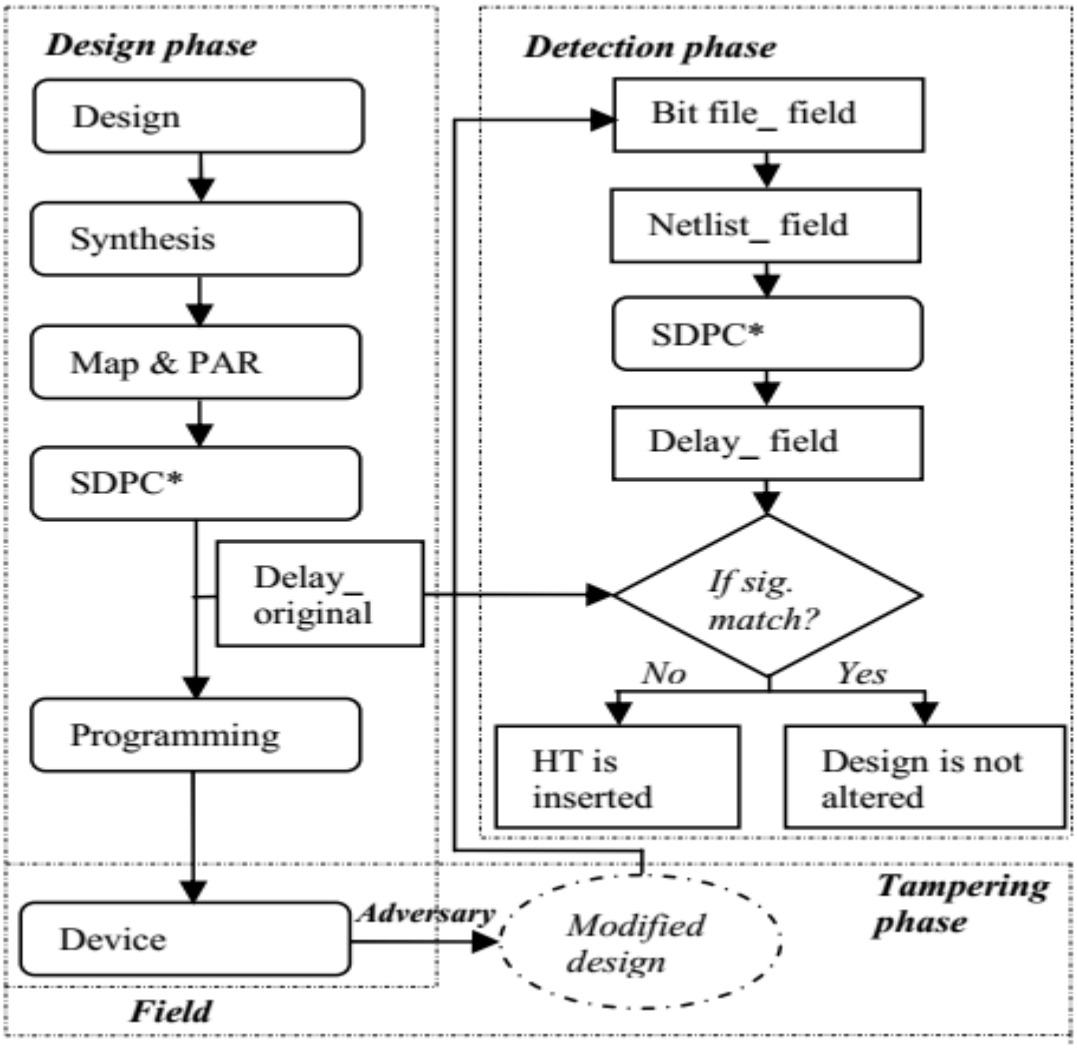
$$\mu(T) = [\mu(T_R)(T_R/T)\hat{}m]$$

$$V_{th}(T) = V_{th}(T_R) - \kappa(T - T_R)$$

Από τις παραπάνω συναρτήσεις, καθίσταται σαφές ότι τόσο η κινητικότητα όσο και η τάση μειώνονται καθώς αυξάνεται η θερμοκρασία. Έτσι λοιπόν, η καθυστέρηση, αυξάνεται ή μειώνεται ανάλογα με την τιμή που θα λάβει το Vdd. Εξ ορισμού, σε ένα τσιπ των 90nm, η τιμές της καθυστέρησης μειώνονται καθώς αυξάνεται η τάση αλλά και η θερμοκρασία λειτουργίας. Ένα ανάλογο τσιπ χρησιμοποίησαν και οι συγγραφείς προσπαθώντας να μελετήσουν την αποτελεσματικότητα της προσομοίωσής τους.

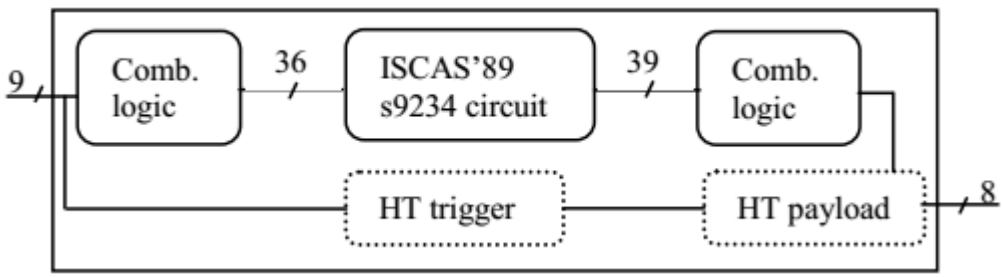
Αυτό λοιπόν το οποίο μελετήθηκε από τους Sumanthi et al, (2015), είναι τα process corners τα οποία δεν αποτελούν τίποτε λιγότερο από τα άκρα των μεταβολών των παραμέτρων μέσα στα οποία ένα κύκλωμα θεωρείται ότι λειτουργεί αποτελεσματικά.

Κάθε FPGA λειτουργεί με βάση έναν κώδικα HDL ο οποίος με στόχο να επαληθεύσει την ορθότητα του σχεδιασμού εκτελεί προσομοιώσεις σε διάφορα επίπεδα. Η εικόνα που ακολουθεί, παρουσιάζει τη ροή των δεδομένων μέσα στο κύκλωμα κατά τη φάση σχεδιασμού, τη φάση αλλοίωσης αλλά και τη φάση ανίχνευσης.



Κάθε φορά που κάποιος προσπαθεί να χειραγωγήσει το σχεδιασμό του κυκλώματος, παράγεται το net list και εισάγεται ο Δούρειος Ίππος.

Οι συγγραφείς έθεσαν ως στόχο την επιβεβαίωση της αποτελεσματικότητας των delay signatures για την ανίχνευση των Δούρειων Ίππων και για το λόγο αυτό χρησιμοποίησαν το κύκλωμα s9234 σε έναν τσίπ 90nm Xilinx Spartan-3s100evq100-4 με χρήση του Xilinx ISE 12.2 (free version). Το κύκλωμα αυτό έχει 36 εισόδους, 39 εξόδους, 211D flip flops, 3570 inverters και 2027 συνολικές πύλες. Με χρήση της απλής συνδυαστικής λογικής το κύκλωμα μειώθηκε σημαντικά όπως φαίνεται στην εικόνα που ακολουθεί.



Παράλληλα, με στόχο να επιδείξουν το αποτέλεσμα της εισαγωγής ενός Δούρειου Ίππου είτε στο bitstream είτε στο netlist, εισήγαγαν δύο διαφορετικούς τύπους Ίππων εκ των οποίων ο πρώτος σχεδιάστηκε με χρήση 5 εισόδων AND και έναν συνδυασμός μιας XOR με ένα inverter, ενώ ο δεύτερος με το ίδιο κύκλωμα αλλά με 2*1 πολυπλέκτες. Τα αποτελέσματα που εξήχθηκαν παρουσιάζονται στους πίνακες που ακολουθούν.

Data path		**Out_0**	**Out_1**	**Out_2**	**Out_3**
Path delay without HT		5169ps	2759ps	2470ps	1525ps
HT1	Path Delay	5667ps	2801ps	2508ps	1598ps
	Increased delay	*498ps*	*42ps*	*38ps*	*73ps*
HT2	Path Delay	5686ps	2792ps	2515ps	1620ps
	Increased delay	*517ps*	*33ps*	*45ps*	*95ps*

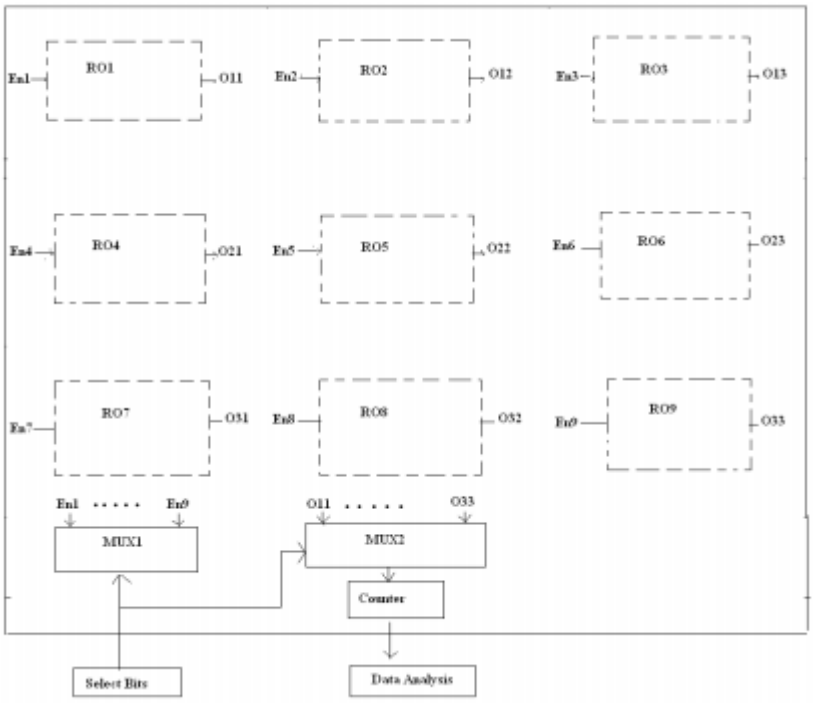
Data path		**Out_0**	**Out_1**	**Out_2**	**Out_3**
Path delay without HT		4833ps	2203ps	2078ps	1495ps
HT1	Path Delay	5387ps	2274ps	2143ps	1624ps
	Increased delay	*554ps*	*71ps*	*65ps*	*129ps*
HT2	Path Delay	5414ps	2272ps	2162ps	1619ps
	Increased delay	*581ps*	*69ps*	*84ps*	*124ps*

Data path		**Out_0**	**Out_1**	**Out_2**	**Out_3**
Path delay without HT		4007ps	1974ps	1966ps	1171ps
HT1	Path Delay	5001ps	2168ps	2068ps	1390ps
	Increased delay	*994ps*	*194ps*	*102ps*	*219ps*
HT2	Path Delay	5073ps	2175ps	2087ps	1513ps
	Increased delay	*1003ps*	*201ps*	*121ps*	*342ps*

Ο πρώτος πίνακας παρουσιάζει τα αποτελέσματα σε ένα slow process corner ενώ ο δεύτερος σε ένα typical process corner. Τέλος, ο τρίτος πίνακας, παρουσιάζει τα αποτελέσματα σε ένα fast process corner.

Στο φυσικό επίπεδο προσπάθησαν οι (1) να μελετήσουν την ύπαρξη των Δούρειων Ίππων στα ολοκληρωμένα κυκλώματα. Στόχος του Δούρειου Ίππου που δημιούργησαν ήταν λανθασμένη λειτουργία του κυκλώματος και η παραγωγή λανθασμένων εξόδων. Το προτεινόμενο κύκλωμα, περιλάμβανε έναν αθροιστή 4-bit και ένα RO εσωτερικό. Ο Δούρειος Ίππος, εισήχθη στη φάση του σχεδιασμού το Register Transfer Level (RTL), και ενεργοποιείται εξωτερικά με είσοδο που δίνεται από το χρήστη. Το Payload συνδέεται με το αρχικό κύκλωμα κρατώντας το μέγεθος του Ίππου αρκετά χαμηλό και τοποθετώντας των έξω από το RO και πριν την έξοδο. Η έξοδος αποστέλλεται στην πύλη OR και η δεύτερη είσοδος

έρχεται από τον αθροιστή. Έτσι λοιπόν, η έξοδος του κυκλώματος για πολλαπλές εισόδους θα έπρεπε να είναι 1111. Η εικόνα που ακολουθεί παρουσιάζει την αρχιτεκτονική του κυκλώματος που όπως αυτό προτάθηκε από τους ερευνητές.



Συγκεκριμένα bit ενεργοποιούν ένα ή πολλαπλά RO η έξοδος των οποίων παράγεται από τη συχνότητα του κάθε ενός ξεχωριστά. Στόχος του σχεδιασμού αυτού είναι να διασφαλίσει την λειτουργία του κυκλώματος και να εντοπίσει όποιες ανεπιθύμητες αλλαγές και παράλληλα να ανιχνεύσει τις όποιες πτώσεις στην τάση λόγω της εισαγωγής του Δούρειου Ίππου.

Υπάρχουν και διάφοροι παράγοντες όπως ο θόρυβος, οι ποικιλίες στις διαδικασίες αλλά και οι περιβαλλοντικοί που ασκούν σημαντικές επιρροές στις συχνότητες που παράγονται από τα RO. Έτσι, η τιμή ανοχής θα πρέπει να καθοριστεί με τρόπο τέτοιο ώστε να μετράται η συχνότητα του RO σε κάθε βρόγχο. Όπως έχει αποδειχθεί από πολλές μελέτες, δε θα πρέπει να υπάρχει απόκλιση μεγαλύτερη της τάξεως του 6,6%.

Ο Δούρειος Ίππος που χρησιμοποίησαν οι ερευνητές, ήταν εντός του πλαισίου αυτού και άρα ήταν ιδιαίτερα δύσκολο να ανιχνευθεί. Το trigger του Δούρειου Ίππου, εισήγαγε απλά φόρτο σε κάποιους από τους αρχικούς κόμβους του κυκλώματος. Έτσι, ακόμη και εάν όλα τα μονοπάτια του κυκλώματος ή όλες οι πύλες εξοπλίζονταν με RO, οι Δούρειοι Ίπποι θα μπορούσαν και πάλι να εισαχθούν χωρίς να επηρεάζουν σημαντικά την καθυστέρηση. Στον πίνακα που ακολουθεί παρουσιάζονται τα διαφορετικά κυκλώματα που χρησιμοποίησαν οι ερευνητές και τα αποτελέσματα που έλαβαν.

Benchmark	No. of inputs	No. of configurable RO paths	Counter value before Trojan insertion	Counter value after Trojan insertion	% change
c880	60	24	4346	4234	1.12
c2670	233	43	29e3	29b1	3.23
c3540	50	8	3581	3796	2.15
c5315	178	58	546d	542b	4.21
c6288	32	12	8042	8039	0.09
c7550	207	37	4a26	4a53	5.63

Σε αυτά παρουσιάζονται και τα αποτελέσματα που λήφθησαν μετά την εισαγωγή του προτεινόμενου από αυτούς Ίππου. Όπως μπορεί κανείς να παρατηρήσει, οι τιμές παραμένουν σχεδόν οι ίδιες με ελάχιστες διαφοροποιήσεις να παρουσιάζονται.

Οι (2) έκαναν μία ιδιαίτερα σοβαρή προσπάθεια ανίχνευσης των Δούρειων Ίππων σε όλα τα στάδια ανάπτυξης του κυκλώματος. Για να προβούν στην αξιολόγηση αυτή, χρησιμοποίησαν το Hardware Trojan Kit το οποίο επιτρέπει την κατασκευή Ίππων που έχουν τις ιδιότητες ενεργοποίησης, της συγκαλυμμένης επικοινωνίας, του payload και τις ανίχνευσης. Τα στοιχεία που δημιουργήθηκαν, εξετάστηκαν σε διάφορα Xilinx FPGAs, με στόχο να ανιχνευθούν χαρακτηριστικά και ιδιότητες που θα τα χαρακτηρίζουν ως κακόβουλα στο κύκλωμα. Αφού έγινε η εξέταση των χαρακτηριστικών, χρησιμοποιήθηκε ένα RO ώστε να ληφθεί κάποια ανατροφοδότηση από το κύκλωμα. Παράλληλα, εισήχθηκε μία σειρά από κανόνες που είχαν ως στόχο την ελαχιστοποίηση του κινδύνου από τη χρήση του RO.

Οι συγγραφείς έλαβαν ως δεδομένο ότι κάθε Ίππος, αφήνει κάποια στοιχεία της ύπαρξής του στο κύκλωμα. Σύμφωνα με αυτό όμως, και κάθε κανόνας ανίχνευσης έχει μία μόνο πιθανότητα να τον ανιχνεύσει με βάση πάντα κάποια συγκεκριμένη ένδειξη. Έτσι λοιπόν, όσο περισσότερες ενδείξεις υπάρχουν, όσο περισσότεροι κανόνες δηλαδή, τόσο περισσότερες θα είναι και οι πιθανότητες ανίχνευσης. Άρα, με τη θέσπιση των πολλαπλών κανόνων ακόμη και η σπάνια περίπτωση της εισαγωγής πολλαπλών Ίππων υπάρχει έντονη η πιθανότητα ανίχνευσης αυτών.

Φυσικά, το όλο εγχείρημα, παρουσιάζει κάποιους περιορισμούς που στηρίζονται στην ποιότητα της επαλήθευσης αλλά και στους ίδιους τους κανόνες που τίθενται με στόχο την ανίχνευση των Ίππων.

Μία διαφορετική προσέγγιση, που αφορά στη χρήση αισθητήρων χρησιμοποίησαν οι (3). Οι συγγραφείς σχεδίασαν και παρήγαγαν ένα τσιπ 90nm με τεχνολογία IBM στο οποίος εισήγαγαν περισσότερους από 20 Δούρειους Ίππους. Από αυτούς, εντοπίστηκαν μόνο οι 8. Επιπλέον, οι συγγραφείς πρότειναν μία βελτίωση της αρχιτεκτονικής RON ώστε αυτή να παρουσιάζει μεγαλύτερη ευαισθησία στους μικρούς Δούρειους Ίππους. Στη συνέχεια, τα

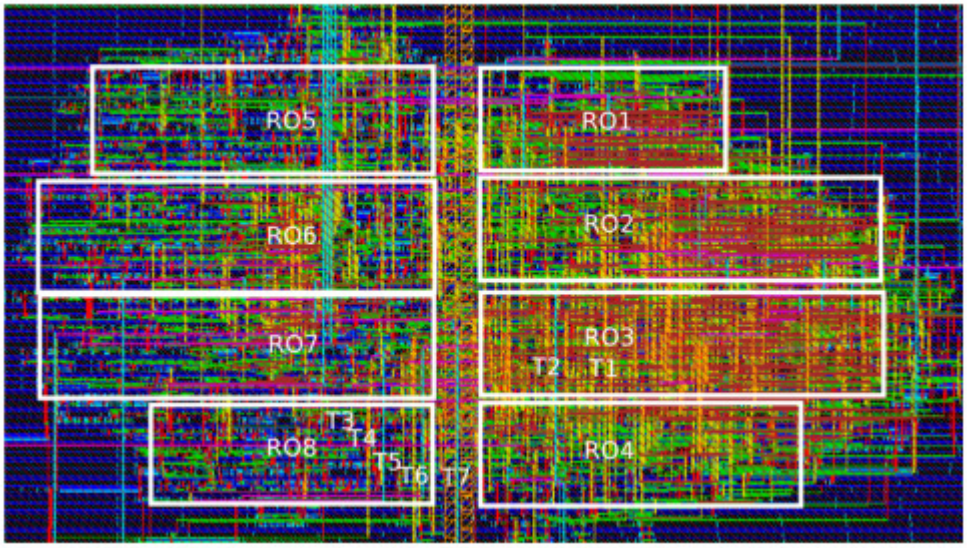
τσιπ, εξετάστηκαν ώστε να καθοριστεί η επιρροή των διαφορετικών Δούρειων Ίππων σε διαφορετικούς ταλαντωτές δακτυλίου.

Οι βελτιώσεις που προτείνονται για την αρχιτεκτονική RON αφορούν κυρίως σε μετρήσεις και είναι οι εξής :

Low Voltage Testing (LVT) : Έχει ως στόχο την αύξηση τόσο της συνολικής όσο και της τοπικής ευαισθησίας του RON τεστάροντας το τσιπ σε χαμηλότερη τάση. Χαμηλώνοντας την τάση αυξάνεται η θερμοκρασία. Ο προφανής περιορισμός στην μέθοδο αυτή είναι ότι το Vc θα πρέπει να είναι υψηλότερο από την τάση κατωφλίου.

Variable Source Resistance Testing (VSRT) : Η μέθοδος αυτή, αυξάνει την ευαισθησία στο RO σε συνολικό επίπεδο. Σημαντικό πλεονέκτημα της μεθόδου είναι ότι με μεγάλους Δούρειους Ίππους, η τάση μπορεί όντως να πέσει κάτω από την τάση κατωφλίου και να προκαλέσει σφάλμα.

Με στόχο λοιπόν να αναλυθεί η αποτελεσματικότητα της RON δομής, δημιουργήθηκαν 40 τσιπ με χρήση της τεχνολογίας IBM των 90 nm. Η RON δομή εισήχθη σε ένα κύκλωμα όπως αυτό παρουσιάζεται στην ακόλουθη εικόνα :



Τα δεδομένα που συλλέχθηκαν για κάθε τσιπ ξεχωριστά ενώ συχνότητα για κάθε RO μετρήθηκε 10 φορές. Έπειτα, καταμετρήθηκε ο θόρυβος για τσιπ και υπολογίστηκε με βάση τη συνάρτηση

$$MN_{jk} = \frac{Max\{f_{Trial1}, \ldots, f_{Trial10}\} - Min\{f_{Trial1}, \ldots, f_{Trial10}\}}{1/10 \sum_{m=1}^{10} f_{Trialm}}$$

ενώ ο υπολογισμός για το σύνολο των τσιπ έγινε με βάση τη συνάρτηση

$$MN = \frac{1}{N_C} \sum_{k=1}^{N_C} \frac{1}{8} \sum_{j=1}^{8} MN_{jk}$$

Το επίπεδο του θορύβου εντοπίστηκε να είναι 0,23% τόσο για τις κανονικές όσο και για τις βέλτιστες συνθήκες. Για να αναλυθεί η επιρροή των Δούρειων Ίππων στη δομή RON εντοπίστηκε ο ταλαντωτής εκείνος δακτυλίου που δέχεται τη σοβαρότερη επιρροή από το Δούρειο Ίππο σε κάθε κύκλωμα. Έτσι, μετά από σειρά ελέγχων, εντοπίστηκαν αυτοί με τη μεγαλύτερη ευαισθησία και εντοπίστηκαν τα τσιπ τα οποία δέχονται τις σοβαρότερες επιρροές.

Οι ερευνητές υποστήριξαν ότι κάθε RON είναι ιδιαίτερα ανθεκτικό στην αφαίρεση, τη μοντελοποίηση την τροποποίηση των απειλών που δέχονται από ένα αντίπαλο. Οι πύλες RON κατανέμονται σε όλο το τσιπ και έτσι είναι σχετικά δύσκολο να αναγνωριστούν. Εάν για κάποιο λόγο αυτό εντοπιστεί, είναι δύσκολο είτε να αφαιρεθεί είναι να αποτραπεί οι λειτουργία τους καθώς αυτό θα γίνει άμεσα αντιληπτό.

Η δομή που αυτοί έχουν προτείνει απαιτεί έλεγχο διαμέσου των μεθόδων LVT & VSRT που περιγράφηκαν παραπάνω και αυξάνουν την ευαισθησία σ όλο το κύκλωμα. Οι μελετητές χρησιμοποίησαν ένα δίκτυο RON με 33 ICs που περιλάμβαναν το κύκλωμα ISCAS'89 s9234 που έκανε χρήση της IBM 90nm διαδικασίας. Αποδείχθηκε ότι, η επιρροή των Δούρειων Ίππων σε έναν ταλαντωτή δακτυλίου αυξάνεται ότι όταν αυξηθεί και η διαδικασία του Switching και ότι οι ταλαντωτές δακτυλίου οι οποίοι δέχθηκαν τη μεγαλύτερη επιρροή ήταν αυτοί οι οποίοι διαμοιράζονταν την ίδια τάση με τους Ίππους.

Αποδείχθηκε ότι οποιαδήποτε μείωση στην τάση και οποιαδήποτε αύξηση στην αντίσταση οδηγεί σε σημαντική βελτίωση του RO απέναντι στην ανίχνευση των Ίππων. Ακόμη αποδείχθηκε ότι, παρουσία θορύβου και άλλον περιβαλλοντικών παραγόντων, τα ολοκληρωμένα κυκλώματα μπορούν επιτυχώς να ανταπεξέλθουν εάν χρησιμοποιήσουν τις κατάλληλες τεχνικές.

Σημαντική προσπάθεια στο κομμάτι της ανίχνευσης των Δούρειων Ίππων κατέβαλλαν και οι (4) οι οποιοι πρότειναν ένα σχήμα ανίχνευσης Δούρειων Ίππων που βασίζεται σε τμηματοποίηση της αλυσίδας ελέγχου και στη χρήση του αλγορίθμου walking ones όπου η διαδικασία του switching επιτρέπεται μονάχα ανάμεσα σε δύο flops και μειώνει το λόγο ισχύος του Δούρειου Ίππου προς το συνολικό κύκλωμα.

Το σχήμα που πρότειναν οι συγγραφεί, περιλαμβάνει διαμοιρασμό της.

Στο σχήμα αυτό, οι αλυσίδες scan διαμοιράζονται σε m τμήματα με διαφορετικά bloc το καθένα όπως φαίνεται στην εικόνα που ακολουθεί ενώ η είσοδος του scan προέρχεται από ακολουθία walking ones που επιτρέπει μέχρι δύο μεταβάσεις.

Στόχος της τμηματοποίησης αυτής είναι η μείωση της εσωτερική ισχύος των flops που κατά συνέπεια μειώνει το λόγο ισχύος του Δούρειου Ίππου στο συνολικό κύκλωμα. Η ανίχνευση όπως αυτή προτείνεται από το σχήμα θα έχει τα παρακάτω βήματα :

1. Επανεκκίνηση όλων των flop μέσα στο κύκλωμα
2. Ενεργοποίηση του πρώτου τμήματος της αλυσίδας και φόρτωση της τιμής 1 σε αυτό. Σε συνέχεια προώθηση της τιμής κατά μήκος του τμήματος και είσοδος της τιμής 0 στο δεύτερο τμήμα.
3. Παρατήρηση για κάθε κύκλο της ισχύος που διανέμεται ή της ενέργειας που εξάγεται.
4. Επανάληψη των βημάτων 2 και 3 για όλα τα τμήματα της αλυσίδας.
5. Εάν εισαχθεί κάποιος Δούρειος Ίππος στη διαδικασία παραγωγής θα καταλήξει σε μία επιπλέον μετάβαση κατά την ανάλυση γεγονός που μπορεί άμεσα να συγκριθεί με τις αρχικές τιμές.

Η μέθοδος αυτή είναι ιδιαίτερα επιτυχής και μάλιστα ανιχνεύει τους Ίππους με ελάχιστες τροποποιήσεις στο σχεδιασμό του κυκλώματος. Ο Δούρειος Ίππος μπορεί επίσης να εντοπιστεί κάνοντας χρήση της πληροφορίας του τμήματος αλλά και του κύκλου ρολογιού.

Το σχήμα που προτάθηκε, εξετάστηκε με ISCAS κυκλώματα τύπου S15850. Ως μηχανισμός εκκίνησης του Δούρειου Ίππου θεωρείται μία κατάσταση που εξαρτάται από το ρολόι. Στη συγκεκριμένη περίπτωση, μία πύλη AND 4-bit θεωρείται το trigger και μία XOR θεωρείται

το payload. Αφού γίνει η εισαγωγή του Δούρειου Ίππου, το flop του πρώτου τμήματος κάνει 6 μεταβάσεις οι οποίες προκαλούνται από τον ίδιο τον Ίππο.

Αυτό το οποίο συμπεραίνεται είναι ότι οι επιπλέον μεταβάσεις επιβεβαιώνουν την ύπαρξη του Δούρειου Ίππου. Η μέθοδος φαίνεται να είναι ιδιαίτερα αποδοτική και αξιόπιστη λόγω του ελάχιστου αριθμού των μεταβάσεων που χρησιμοποιεί.

Μία τελείως διαφορετική προσέγγιση η οποία μάλιστα βασίζεται σε έναν γενετικό αλγόριθμο που αφορά φυσικά στην ανίχνευση των Δούρειων Ίππων με τη βοήθεια ενός RON πρότειναν οι Karimian et al (2015).

Οι γενετικοί αλγόριθμοι ανήκουν στην κατηγορία εκείνει τον αλγορίθμων που λειτουργούν με βάση τα παραδείγματα που έχουν από την ίδια τη φύση. Για παράδειγμα, ένας γενετικός αλγόριθμος μπορεί να παράξει από μία ομάδα χρωμοσωμάτων σε μία νεά ομαδα αυτών λαμβάνοντας υπόψη του παραμέτρους όπως η σίγαση ή ο διπλασιασμός. Κάθε χρωμόσωμα αντιπαρίσταται με ένα binary string ενώ αυτά που καταφέρνουν να "επιβιώσουν" τελικά είναι αυτά που είναι και τα πλέον κατάλληλα.

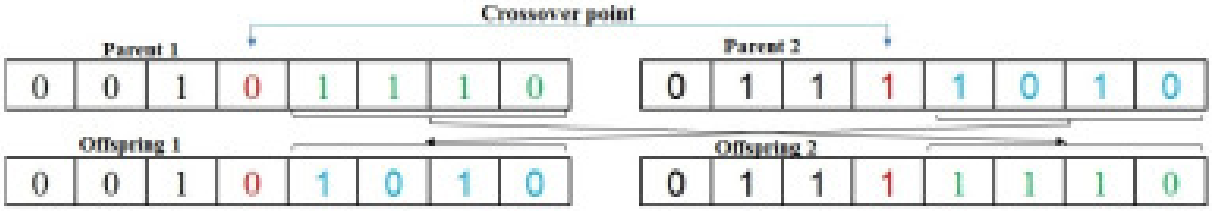
Η παραπάνω λογική μπορεί να εφαρμοστεί και σε περιπτώσεις όπου εμφανίζονται προβλήματα ταξινόμησης και ο σκοπός τους είναι να βρεθεί το σετ εκείνο των τιμών που δίνει τη βέλτιστη ακρίβεια.

Ένας κλασικός γενετικός αλγόριθμος είναι αυτός ο οποίος ξεκινά με ένα τυχαίο δείγμα και κάνει επαναλήψεις εως ότου να παράξει τις επόμενες γενιές. Η καταλληλότητα της κάθε γενιάς αξιολογείται με βάση την καταλληλότητα μας ομάδας χαρακτηριστών. Έπειτα, οι διαφορετικές ομάδες χαρακτηριστικών, εξάγονται από τον πληθυσμό και τροποιούνται με τρόπο τέτοιο ώστε να αρμόζουν στο νέο πληθυσμό που θα παραχθεί. Ο πληθυσμός που παράγεται από αυτό χρησιμοποιείται στην επόμενη επανάληψη του αλγορίθμου και αυτό συνεχίζεται έως ότου τερματιστεί ο αλγόριθμος.

Στην παραπάνω εικόνα, εμφανίζονται 8 διαφορετικά γονίδια σε ένα χρωμόσωμα. Η παρουσία του 0 δείχνει ότι το χαρακτηριστικό θα αγνοηθεί ενώ του 1 ότι θα χρησιμοποιηθεί από την ταξινόμηση του αλγορίθμου. Για να παραχθεί νέος πληθυσμός ο αλγόριθμος χρησιμοποιεί τελεστές μετάλλαξης και μίξης. Όπως μπορεί κανείς να διακρίνει και στην εικόνα, δύο τυχαία γονίδια από το χρωμόσωμα επιλέγονται και μετά τη μετάλλαξή τους παίρνουν τιμή 0 ή 1 αντίστοιχα. Ο μηχανισμός μίξης από την άλλη προβαίνει σε μίξη γονιδίων από ήδη υπάρχουσες λύσεις.

Δύο ήδη υπάρχοντα μέλη του πληθυσμού έχουν επιλεγεί τυχαία για να διαδραματίσουν το ρόλο των γονιών παράλληλα έχει οριστεί και ένα τυχαίο σημείο μίξης. Το κάθε παιδί, παράγεται από τη μίξη των γονιδίων των δύο γονιών. Τα παιδιά από τον πρώτο γονέα αντιγράφονται στη μία μεριά του σημείου μίξης ενώ τα υπόλοιπά ακολουθούν τον άλλο γονιό στην άλλη μεριά του σημείου μίξης.

Η εικόνα που ακολουθεί παρουσιάζει το συγκεκριμένο παράδειγμα με ένα και μόνο σημείο μίξης. Φυσικά, οι παράμετροι που θα μπορούσε να ορίσει ο κάθε χρήστης είναι διαφορετικοί και έχουν διαφορετικές επιρροές στην λύση που θα παρουσιαστεί.



Το χαρακτηριστικό πλεονέκτημα της μορφής αυτής των αλγορίθμων είναι ότι είναι ιδιαίτερα απλοί. Από την άλλη όμως, δυστυχώς πολλές φορές απαιτούν ιδιαίτερα υψηλές δυνατότητες επεξεργασίας.

Η λύση που πρότειναν οι (5), αφορά στο διαχωρισμό των κυκλωμάτων σε αυτά που περιέχουν Δούρειους Ίππους και σε αυτά που δεν περιέχουν κανέναν Ίππο. Οι συγγραφείς λαμβάνουν ένα σετ δεδομένων από ένα ολοκληρωμένο κύκλωμα χωρίς Δούρειο Ίππο και το χρησιμοποιούν με στόχο να εκπαιδεύσουν έναν ταξινομητή. Στόχος τους είναι να επιλέξουν τα χαρακτηριστικά εκείνα που θα κάνουν το βέλτιστο διαχωρισμό ανάμεσα στα κυκλώματα αλλά και θα δημιουργήσουν τον καλύτερο δυνατό κανόνα. Επίσης, σημαντικό για αυτούς είναι να επιλέξουν τον ελάχιστο αριθμό χαρακτηριστικών που χρειάζεται για τη διαδικασία της ταξινόμησης. Το παραπάνω, οφείλεται στο γεγονός ότι οι ταξινομητές είναι ιδιαίτερα ευαίσθητοι στην επιλογή των χαρακτηριστικών και πολλά από αυτά μάλιστα ενδεχόμενα να παράγουν θόρυβο.

Οι συγγραφείς, επέλεξαν έναν αλγόριθμο που βασίζεται σε ένα ήδη υπάρχοντα γενετικό και μία SVM (Support Vector Machine) η οποία θα θέτει τα όρια των αποφάσεων. Ο αλγόριθμος ακολουθεί τα παρακάτω βήματα :

Input: Golden model (Trojan free) IC data S_{TR} and algorithm parameters for GA and SVM
Generate the first chromosome population P randomly
while Number of iterations or desired classification accuracy is not satisfied **do**
  for $i = 1$ **to** P **do**
    $S_{pop} \Leftarrow S_{TR}/2$ {Randomly}
    $S_{fit} \Leftarrow S_{TR}/2$ {Randomly}
    Determine hypersphere via SVM for S_{pop} and all chromosomes (feature sets) in P
    Calculate fitness function using SVM output **and** S_{fit}
    $FF_i = EER(P_i)$ {Compute the fitness FF for each chromosome (feature set) in P}
  end for
  Select N_c parents for crossover based on fitness of P and randomly select crossover points
  Select N_m parents for mutation based on fitness of P and randomly select features to mutate
  $Offspring = N_c + N_m$ {Generate offspring}
  Determine hypersphere via SVM for S_{pop} and all chromosomes (feature sets) in $Offspring$
  Calculate fitness function using SVM output **and** S_{fit}
  $FF_i = EER(P_i)$ {Compute the fitness FF for each chromosome (feature set) in $Offspring$}
  Sort all the chromosomes based on the fitness function for P and $Offspring$ and select the new population P to pass to the next iteration
end while
$Output = optimal features$ {Select the best chromosomes from the last generation of population based on fitness function}

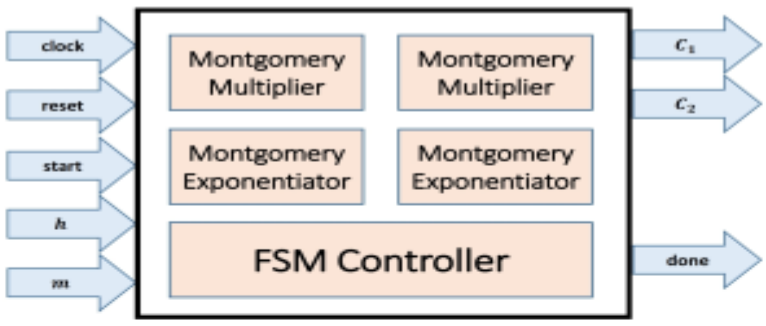
Για να εξεταστεί η αποτελεσματικότητα του αλγορίθμου, χρησιμοποιήθηκαν 33 τεστ chips τεχνολογίας IBM 90nm. Το RON που δημιουργήθηκε, αποτελείται από 8 ROs σε κάθε τσιπ το οποίο επίσης περιλαμβάνει και 15 διαφορετικούς Δούρειους Ίππους που είτε ενεργοποιούνται είτε απενεργοποιούνται κατά τη συλλογή των αποτελεσμάτων.

Κατά τη διεξαγωγή των πειραμάτων χρησιμοποιήθηκαν τρεις διαφορετικοί αλγόριθμοι τα αποτελέσματα των οποίων παρουσιάζονται στον πίνακα που ακολουθεί :

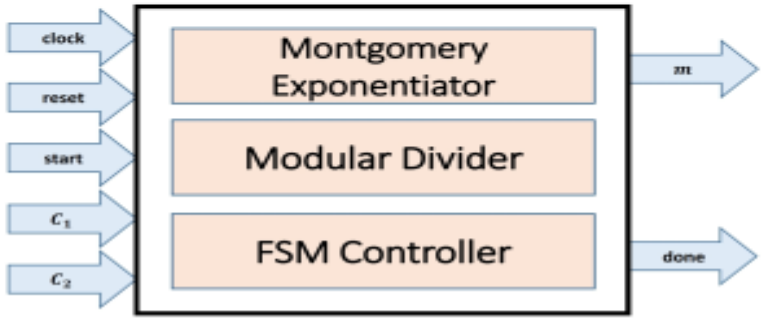
	PCA		SVM		GA+SVM	
N_g	Accuracy	EER	Accuracy	EER	Accuracy	EER
8	66.5%	37.1%	92.7%	10.1%	96.9%	7.4%
16	70.1%	33.4%	94.6%	9.2%	97.8%	6.9%
24	6.8%	28.8%	95.5%	7.7%	99.6%	0.8%

Ακόμη μία πρόταση σχετική πάντα με την αντιμετώπιση των Δούρειων Ίππων στα ολοκληρωμένα κυκλώματα έγινε από τους Ziab et (2015) οι οποίοι ασχολήθηκαν με την ομομορφική κρυπτογράφηση και πρότεινα δύο διαφορετικούς ομομορφικούς σχεδιασμούς. Η ομομορφική κρυπτογράφηση αποτελεί τη μορφή εκείνη της κρυπτογράφησης που επιτρέψει συγκεκριμένες διαδικασίες μέσα σε ένα ciphertext και παράγει ένα κρυπτογραφημένο αποτέλεσμα το οποίο όταν αποκρυπτογραφηθεί ταιριάζει απόλυτα με τις διεργασίες που έχουν γίνει στο κανονικό κείμενο. Ο αλγόριθμος που χρησιμοποιήθηκε από τους συγγραφείς είναι ο αλγόριθμος El Gamal ο οποίος αφορά στην κρυπτογράφηση του δημόσιου κλειδιού και ταυτόχρονα θεωρείται ένας από τους πλέον αποδοτικούς καθώς παρέχει υψηλά επίπεδα ασφάλειας.

Η πρόταση των συγγραφεών αφορά σε δύο διαφορετικές σχήματα ομομορφικής κωδικοποίησης τα οποία στη συνέχεια ενώνονται και κάνουν κοινή χρήση των λειτουργιών τους. Η πρώτη υλοποίηση αφορά στη χρήση του σχήματος κωδικοποίησης El Gamal που αποτελείται από δύο πολλαπλιασιαστές Montgomery, δύο εκθετές Montgomery και έναν ελεγκτή πεπερασμένων καταστάσεων που είναι υπεύθυνος για το συγχρονισμό των εισόδων και των εξόδων στο σχήμα. Στην αποκρυπτογράφηση, χρησιμοιούνται δυο Montgmomery εκθέτες, ένας διαρέτης και ένασ FSM ελεγκτής που είναι επίσης υπεύθυνος για το συγχρονισμό των εισόδων και τον εξόδων των άλλων μερών του κυκλώματος. Στην εικόνα που ακολουθεί φαίνονται αναλυτικά οι διαδικασίες που ακολουθεί το σχήμα αυτό.

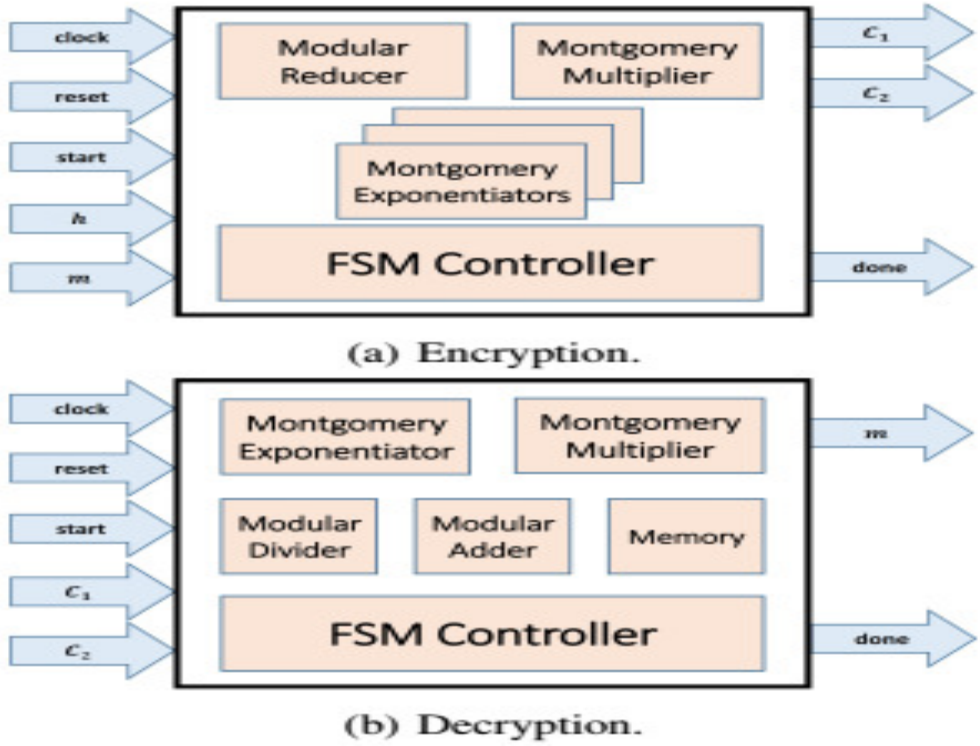


(a) Encryption.



(b) Decryption.

Η δεύτερη υλοποίηση, αφορά στη χρήση ενός CEG (CRT - based ELGamal) σχήματος. Το σχήμα αυτό είναι διαφορετικό από το προηγούμενο καθώς η διαδικασία της κωδικοποίηση απαιτεί πολλαπλούς Montgomery εκθέτες για να γίνει. Οι διαδικασίες που ακολουθούνται φαίνονται στο παρακάτω σχήμα.



(a) Encryption.

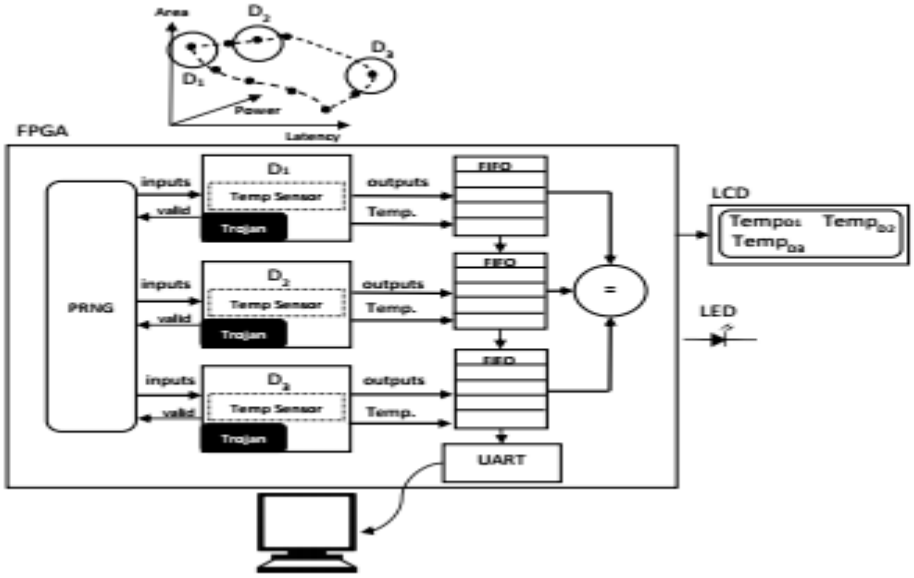
(b) Decryption.

Παράλληλα, οι (6) προέβησαν και στην υλοποίηση ενός διπλού κυκλώματος με στόχο την ικανοποίηση των μερών εκείνων που απαιτούν περισσότερες της μίας λειτουργίες.

Μετά από σειρά προσομοιώσεων που έκαναν οι ερευνητές, διαπίστωσαν ότι η τρίτη υλοποίηση, αυτή δηλαδή που αφορούσε στο σχεδιασμό ενός διπλού κυκλώματος και στο συνδυασμό των αλγορίθμων σε αυτό βελτίωσε σημαντικά τη χρήση των πηγών στο υλικό. Η υλοποίηση αυτή παρουσιάστηκε ιδιαίτερα αποτελεσματική και στη συνολική κατανάλωση ισχύος καθώς μειώνει σημαντικά την ισχύ που καταναλώνεται από τα διπλότυπα. Μάλιστα, η εξοικονόμηση ισχύος έφτασε τα 20,44% για την κωδικοποίηση και το 12,26% για την αποκωδικοποίηση.

Οι (7) πρότειναν και αυτοί με τη σειρά τους μία μέθοδο ανίχνευσης Δούρειων Ίππων οι οποίοι ενεργοποιούνται από τη θερμότητα. Η λύση που προτείνουν οι συγγραφείς γίνεται σε δύο φάσεις. Στην πρώτη φάση, ένας εξερευνητής σχεδιασμού χώρου παράγει μικρό αρχιτεκτονικές με διαφορετικά trade off area vs ισχύ ενώ στη δεύτερη οι μικρό αρχιτεκτονικές αυτές χαρτογραφούνται με διαφορετικά προφίλ με στόχο να δημιουργήσουν

έναν σύστημα 3way redundant. Το σύστημα αυτό χρησιμοποιείται για την ανίχνευση των Δούρειο Ίππων σε συνδυασμό πάντα με ένα σχήμα ψήφων. Τα διαφορετικά προφίλ που εμφανίζονται σε αυτό, σημαίνουν ταυτόχρονα και διαφορετική θερμική συμπεριφορά της κάθε μικρό αρχιτεκτονικής και άρα θερμική ενεργοποίηση του Δούρειου Ίππου σε διαφορετικές χρονικές περιόδους. Η δομή του συστήματος παρουσιάζεται στην εικόνα που ακολουθεί.

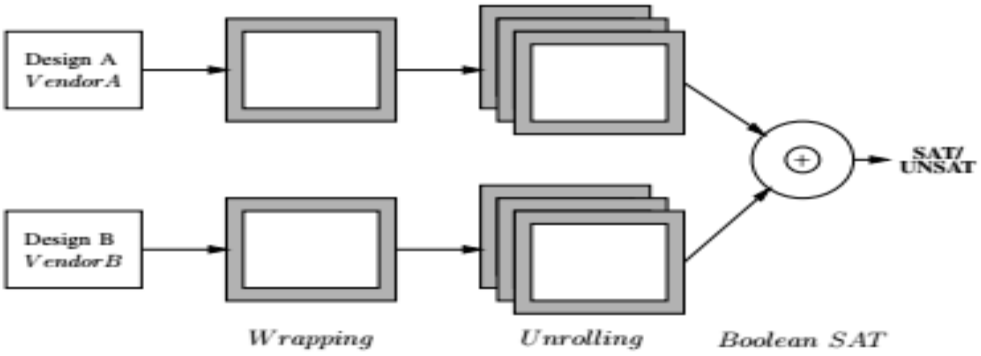


Για να εξεταστεί το παραπάνω προτεινόμενο σχήμα, χρησιμοποιείται ο σχεδιασμός adaptive differential pulse code modulation (ADPCM) της SystemC Synthesizable Benchmark suite (S2CBench). Η IP μορφοποιείται με τρόπο τέτοιο ώστε να περιλαμβάνει μια μονάδα θερμικής διαχείρισης η οποία απενεργοποιεί το ρολόι όταν αυτό φτάσει σε μία συγκεκριμένη θερμοκρασία. Ο Δούρειος Ίππος έχει προγραμματιστεί με τρόπο τέτοιο ώστε να εμφανίζεται όταν η θερμοκρασία φτάσει τους 45oC.

Τα αποτελέσματα της υλοποίησης έδειξαν ότι ο σχεδιασμός αυτός μπορεί να χρησιμοποιηθεί με μεγαλύτερες συμπεριφορικές IPs καθώς το overhead που εισάγεται είναι πολύ μικρό. Η μέθοδος ανιχνεύει ιδιαίτερα αποτελεσματικά τους Δούρειους Ίππους που ενεργοποιούνται από τη θερμοκρασία και μπορεί να αυτοματοποιηθεί πλήρως ώστε να ενσωματωθεί σε όλα τα ολοκληρωμένα κυκλώματα.

Τη χρήση των μη αξιόπιστων μονάδων επέλεξαν οι (8) με στόχο να προβούν στην ανίχνευση των Δούρειων Ίππων εντός των ολοκληρωμένων κυκλωμάτων. Οι συγγραφείς θεώρησαν βέλτιστη τη χρήση πολλαπλών τεχνικών που θα είναι σε θέση να αντιμετωπίσουν

πολλαπλούς τύπους Δούρειων Ίππων. Σημαντικός στόχος της μελέτης τους είναι ο εντοπισμός Ίππων που χρησιμοποιούν payloads που βασίζονται σε λογικούς σχεδιασμούς διαμέσου της χρήσης της σύγκρισης του σχεδιασμού. Βασικό στοιχείο της τεχνικής αυτής είναι η σύγκριση δύο μη αξιόπιστων σχεδιασμών υλικού με παρόμοιες λειτουργίες ώστε να εξεταστεί η έξοδός τους και να εντοπιστεί οποιαδήποτε αλλοίωση κατά το σχεδιασμό.



Η διαδικασία της σύγκρισης γίνεται με τα εξής παρακάτω βήματα :

1. Επιλογή των δύο σχεδιασμών
2. Αποκάλυψη της λογικής κατάστασης μέσα σε κάθε σχεδιασμό
3. Σύγκριση των δύο κυκλωμάτων με βάση τη Boolean ικανοποίηση

Ένα από τα πλέον σημαντικά στοιχεία στην τεχνική αυτή είναι η λήψη της απόφασης σχετικά με το τι προκαλεί τα λάθη και άρα τα false positives και τα false negatives. Αυτό το οποίο λοιπόν μπορεί να ισχύει για τα false positives είναι ότι ναι μεν μπορεί να ανιχνευθεί μία ύποπτη συμπεριφορά χωρίς αυτή να είναι στην πραγματικότητα Δούρειος ενώ για τα false negatives ότι αυτά αφορούν συνήθως σε ένα καθυστερημένο Payload ή σε ένα μη - λογικό Ίππο.

Για να ολοκληρώσουν την έρευνά τους οι (8) χρησιμοποίησαν την Cadence σουίτα εργαλείων. Οι δοκιμές όλες γίναν σε ένα Dell PowerEdge T105 με επεξεργαστή Intel(R) Xeon(R) 2.8 GHz CPU και 16 GB RAM. Στην έρευνα αυτή, αντιμετωπίστηκαν σοβαροί περιορισμοί που αφορούσαν κυρίως στα εργαλεία, στη διακύμανση SAT και στο βάθος εκτύλιξης. Τα αποτελέσματα παρόλα αυτά έδειξαν ότι η μέθοδος αυτή εντοπίζει άμεσα οποιαδήποτε κακόβουλη αλλοίωση του κυκλώματος ενώ παράλληλα βοηθούνται σημαντικά οι σχεδιαστές κυκλωμάτων ώστε να ελέγχουν σε βάθος τα κυκλώματά τους ώστε να λάβουν το μέγεθος της ασφάλειας που επιθυμούν.

Σε μία ανάλογη υλοποίηση που αφορούσε στη χρήση μιας πύλης NAND και ενός κυκλώματος RO προέβησαν και οι Hoque et al (9). Οι ερευνητές παρατήρησαν ότι, προηγούμενες υλοποιήσεις αφενός ήταν ευαίσθητες στην εισαγωγή Δούρειων Ίππων και αφετέρου δεν ήταν παντελώς αξιόπιστες σε ότι αφορά στα λαμβανόμενα αποτελέσματα. Επιπρόσθετα, υλοποιήσεις οι οποίες βασίζονταν στην ανάλυση ισχύος με στόχο να ανακαλύψουν την ύπαρξη Δούρειων Ίππων εισήγαγαν θόρυβο τέτοιο που να είναι μεγαλύτερος από την ίδια την ύπαρξη των Ίππων και παράλληλα απαιτούσαν ιδιαίτερα ακριβό αναλογικό εξοπλισμό.

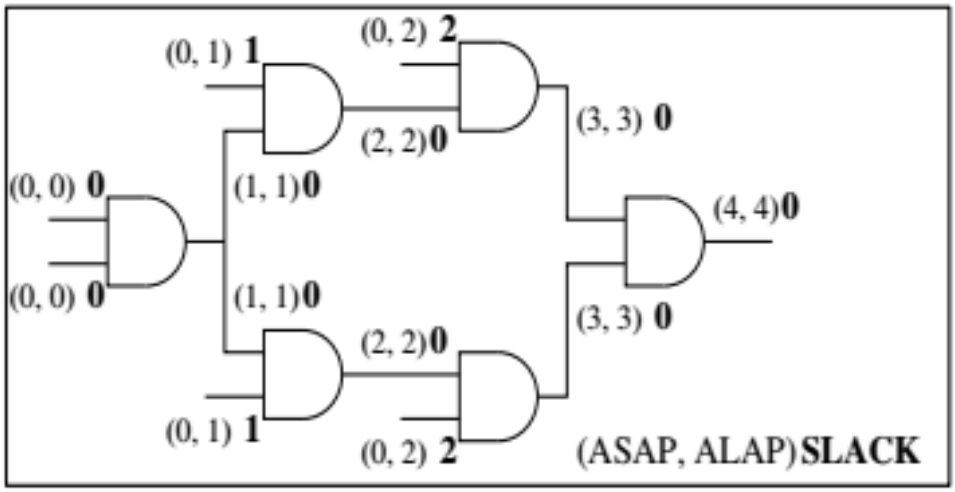
Αντιλαμβανόμενοι λοιπόν τόσο αυτές όσο και πολλές άλλες αδυναμίες, οι συγγραφείς προέβησαν στην υλοποίηση ενός RON που θα είχε φυσικά ως στόχο την ανίχνευση των Δούρειων Ίππων στα ενσωματωμένα κυκλώματα. Η συχνότητα του κάθε RO είναι ιδιαίτερα ευαίσθητη στις διακυμάνσεις που προκαλούνται τόσο από την ίδια τη λειτουργία του κυκλώματος όσο και στις διακυμάνσεις που προκαλούνται από την εμφάνιση των Δούρειων Ίππων. Σε ένα RON, οι διάφοροι ταλαντωτές δακτυλίου, ανιχνεύουν την αύξηση της κατανάλωση ενέργειας που εισάγεται από του Ίππους στις διάφορες περιοχές του κυκλώματος. Ο προτεινόμενος σχεδιασμός αφορούσε στην εξέταση ενός τσιπ των 90nm τις IBM το οποίο περιλάμβανε πάνω από 20 Δούρειους Ίππους.

Τα αποτελέσματα έδειξαν ότι η μέθοδος είναι ιδιαίτερα αποτελεσματική και όσο κοντύτερα τοποθετείται το RO στο Δούρειο Ίππο τόσο ευκολότερο είναι να αποσοβηθεί ο κίνδυνος.

2.1.4 Υλοποιήσεις κυκλωμάτων που περιλαμβάνουν Physical Unclonable Functions

Σειρά ερευνητών προέβη στη χρήση των PUF (Physical Unclonable Function) με στόχο να αντιμετωπίσει την ύπαρξη των Δούρειων Ίππων στα ολοκληρωμένα κυκλώματα. Οι Dupuis et al, (2014) στην έρευνά τους πρότειναν μία νέα τεχνική βασισμένη στην κρυπτογράφηση που αποσκοπεί σε επίλυση του προβλήματων των Δούρειων Ίππων. Η λογική κρυπτογράφηση η οποια πρότειναν οι συγγραφείς χωρίζεται σε δύο διαφορετικούς τύπους. Ο πρώτος αφορά στη συυνδυαστική κρυπτογράφηση και ο δεύτερος στην ακολουθιακή. Στη συνδυαστική, προστίθενται επιπλέον λογικές πύλες στο κύκλωμα ώστε να αντιμετωπίζουν οποιοδήποτε πρόβλημα ενώ στη δεύτερη, η μετάβαση από τη μία κατάσταση στην άλλη, τροποποιείται και έτσι ο σχεδιασμός φτάνει στο επιθυμητό αποτέλεσμα μόνο έαν ακολουθήσει τη σωστή σειρά εισόδων.

Η τεχνική κρυπτογράφησης που προτείνουν οι Dupuis et al, (2014) είναι συνδυαστική και κάνει χρήση ενός εξωτερικού κλειδιού το οποίο προστίθεται στο κύκλωμα και το κάνει να λειτουργεί σωστά εάν και μόνο εισαχθεί η κατάλληλη τιμή για το κλειδί. Στόχος της ερευνητικής ομάδας ήταν να μειώσουν τις τυχαίες τιμές και την οποιαδήποτε αλλοίωση στα σήματα. Πρώτο τους βήμα, ήταν ο εντοπισμός των σημάτων χαμηλού ελέγχου μέσα στο κύκλωμα. Στη συνέχεια, έλεγξαν το αποτέλεσμα που θα είχαν τα σήματα αυτά εάν λειτουργούσαν κανονικά μέσα στο κύκλωμα αλλά και η επιρροή η οποία θα ασκούσαν. Το κύκλωμα που υλοποιησαν παρουσιάζεται στην παρακάτω εικόνα.



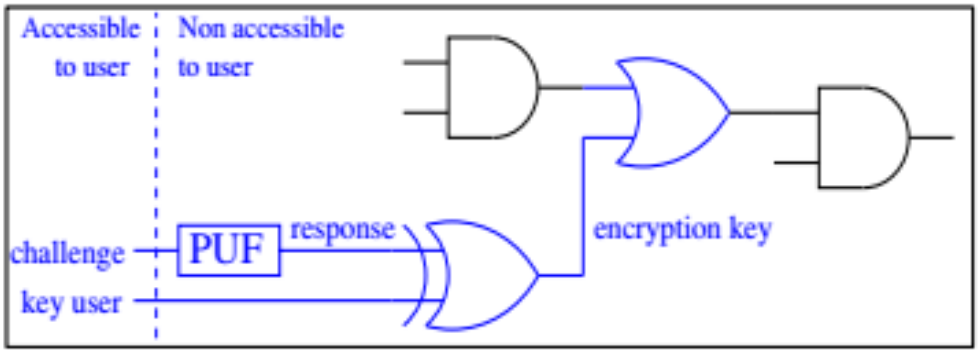
Ο αλγόριθμος κρυπτογράφησης υλοποιείται με την εισαγωγή πυλών IN/OR στο σχεδιασμό. Τα βήματα του αλγορίθμου είναι :

Η πιθανότητα να ληφθεί 0/1 υπολογίζεται για κάθε σήμα

Υποψήφια για κρυπτογράφηση σήματα είναι τα σήματα τα οποία παρουσιάζουν μη ισορροπημένη πιθανότητα

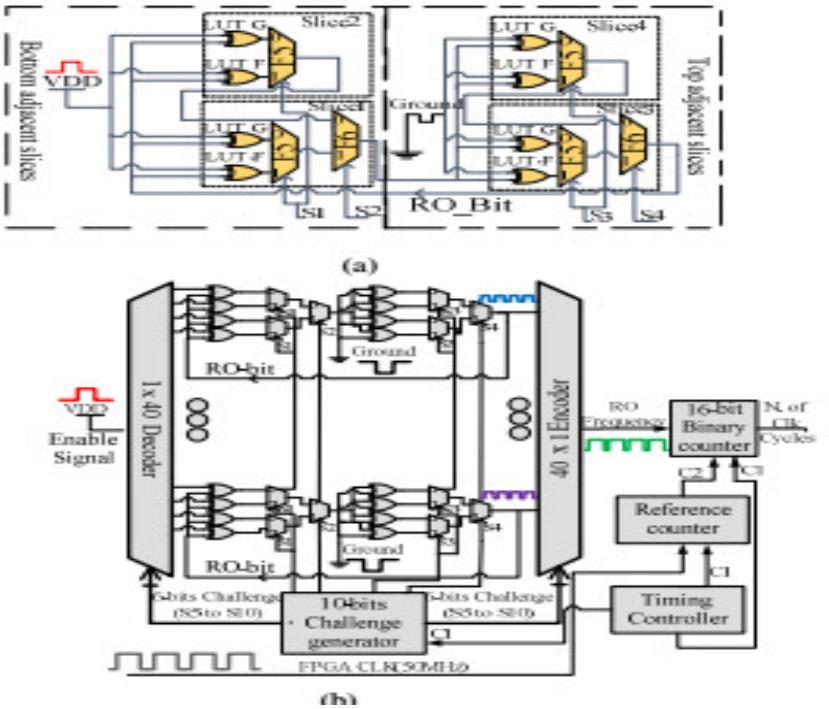
- Υπολογίζονται οι slack χρόνοι για κάθε υποψήφιο σήμα
- Οι εναπομείναντες υποψήφιοι είναι αυτοί οι οποίοι θα έχουν θετικό slack χρόνο
- Επιλέγεται το σήμα το οποίο θα έχει την πιο αβέβαιη πιθανότητα
- Επιλέγεται η πύλη που θα χρησιμοποιηθεί
    - Εάν η πιθανότητα είναι κοντά στο 0 συμπεριλαμβάνεται μία OR πύλη και το κλειδί είναι 0
    - Εάν η πιθανότητα είναι κοντά στο 1 χρησιμοποιείται μία πύλη AND και η τιμή του κλειδιού είναι 1

Στον παραπάνω αλγόριθμο μπορεί να εισαχθεί και μία συνάρτηση PUF ακριβώς όπως και στην παρακάτω εικόνα.



Τα αποτελέσματα των διαφόρων προσομοιώσεων έδειξαν ότι η μέθοδος αυτή είναι ιδιαίτερα αξιόπιστη και ότι με χρήση του αλγορίθμου υπάρχει ελάχιστη ασάφεια στις πιθανότητες. Τα σήματα χαμηλής πιθανότητας είναι και οι στόχοι των Δούρειων Ίππων και ακριβώς επειδή η πιθανότητες αυτές εξαλείφονται λόγω του αλγορίθμου μειώνεται αισθητά και ο κίνδυνος.

Σε μια υλοποίηση η οποία αποτελεί συνδυασμό RO & PUF και ελέγχεται από προγραμματιζόμενες XOR πύλες προέβησαν οι (10). Ο σχεδιασμός που πρότειναν οι συγγραφείς βασίζεται στη χρήση πυλών PXOR όπως φαίνεται στην παρακάτω εικόνα.



Τα αποτελέσματα των πολλαπλών εξομοιώσεων που έκαναν οι συγγραφείς έδειξαν ότι ο σχεδιασμός αυτός λειτουργεί ιδιαίτερα αποτελεσματικά ενώ ο αλγόριθμος που συνοδεύει το κύκλωμα βελτιώνει κατά πολύ την απόδοσή του.

Βιβλιογραφία

1. **Nayak, Ameya, Yen, Kang και Fan, Jeffrey.** Breaching of Ring Oscillator Based Trojan Detection and Prevention in Physical Layer. *Recent Trends in Engineering and Technology.* 2014, Τόμ. 10, 1.

2. **Dabrowski, Adrian, και συν., και συν.** Towards a Hardware Trojan Detection Cycle. 2014.

3. **Shane, Kelly, και συν., και συν.** Detecting Hardware Trojans using On-chip Sensors in an ASIC Design. *J Electron Test.* 2015.

4. **Ritesh, M, και συν., και συν.** Detection and analysis of hardware trojan using scan chain method. 2015.

5. **Karimian, Nima, και συν., και συν.** Genetic Algorithm for Hardware Trojan Detection Genetic Algorithm for Hardware Trojan Detection. 2015.

6. **Ziab, Tarek Ibn, και συν., και συν.** Homomorphic Data Isolation for Hardware Trojan Protection. 2015.

7. **Li, Xiaotong και Schafer, Carrion.** Temperature-triggered Behavioral IPs HW Trojan Detection Method with FPGAs. 2015.

8. **Reece, Trey και Robinson, William.** Detection of Hardware Trojans in Third-Party Intellectual Property using Untrusted Modules. 2015.

9. **Hoque, Tamzidul, και συν., και συν.** Assessment of NAND Based Ring Oscillator for Hardware Trojan Detection. 2015.

10. **Amsaad, Fathi, Hoque, Tamdzidul και Niamat, Mohammed.** Analyzing the Performance of a Configurable ROPUF Design Controlled by Programmable XOR Gates. 2015.

11. *DSDPC: Delay Signatures at Different Process Corners based Hardware Trojan Detection Technique for FPGAs.* **Sumanthi, G., και συν., και συν.** Chennai, India : s.n., 2015. International Conference on Robotics, Automation, Control and Embedded Systems – RACE 2015.

12. **Dupuis, Sophie, και συν., και συν.** A Novel Hardware Logic Encryption Technique for thwarting Illegal Overproduction and Hardware Trojans. *20th IEEE International On-Line Testing Symposium, Platja d'Aro : France.* 2014.