Πανεπιστήμιο Δυτικής Αττικής

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

ΠΜΣ "Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων"

Διπλωματική εργασία

Μηχανισμοί Ασφάλειας σε Επίπεδο Υλικού με Χρήση της Θεωρίας Παιγνίων

ΔΕΣΠΟΤΑΚΗΣ ΓΕΩΡΓΙΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Δρ. Εμμανουήλ Μιχαηλίδης

05/09/2023

Η παρούσα διπλωματική εργασία παρουσιάστηκε

από τον

Γεώργιο Δεσποτάκη

ΑΜ: 21004

Εισηγητής: Εμμανουήλ Μιχαηλίδης

ΕΠΙΤΡΟΠΗ ΕΞΕΤΑΣΗΣ

Α/Α	**ΟΝΟΜΑ ΕΠΩΝΥΜΟ**	**ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ/ΤΜΗΜΑ**	**ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ**
1	**Εμμανουήλ Μιχαηλίδης**	**Ακαδημαϊκός Υπότροφος**	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2023.09.07 16:36:24 +03'00'
2	**Ιωάννης Βογιατζής**	**Καθηγητής**	Ioannis Voyiatzis Digitally signed by Ioannis Voyiatzis Date: 2023.09.15 13:46:21 +03'00'
3	**Παναγιώτης Γιαννακόπουλος**	**Καθηγητής**	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.09.07 23:07:51 +03'00'

Δήλωση συγγραφέα μεταπτυχιακής εργασίας

Ο κάτωθι υπογράφων Γεώργιος Δεσποτάκης μεταπτυχιακός φοιτητής του προγράμματος σπουδών «Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής δηλώνω ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποίαν είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης οι πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών η λέξεων είτε ακριβώς είτε παραφρασμένες αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, στον εκδοτικό οίκο ή το περιοδικό συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο δηλών

ΕΥΧΑΡΙΣΤΙΕΣ

Από τη θέση αυτή θα ήθελα να απευθύνω τις ευχαριστίες μου προς τους καθηγητές μου, κυριότερα στον κ. Δρ. Εμμανουήλ Μιχαηλίδης για την όλη υποστήριξη κατά την συγγραφή της διπλωματικής μου, καθώς και τους συνεπιμορφούμενους του μεταπτυχιακού προγράμματος στις Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων, για όλο αυτό το ταξίδι της γνώσης που περάσαμε παρέα, όλο αυτό το διάστημα. Ανταλλάξαμε αρκετές χρήσιμες απόψεις/πληροφορίες που σίγουρα θα τις χρησιμοποιήσω στο μέλλον. Θα ήθελα επίσης να ευχαριστήσω την οικογένεια μου για την αμέριστη συμπαράσταση, όλους αυτούς τους μήνες, την κατανόηση και την υπομονή που έδειξαν για το χρόνο που αφιέρωσα για την διεκπεραίωση του μεταπτυχιακού προγράμματος στις Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Τα τελευταία χρόνια έχει γίνει σημαντική πρόοδος στον τομέα της ασφάλειας των υπολογιστικών συστημάτων. Παράλληλα, όμως, εξελίσσονται και γίνονται πιο επικίνδυνες οι επιθέσεις από κακόβουλους χρήστες. Αν και το υλικό (hardware) των συστημάτων αυτών θεωρείται εγγενώς ασφαλές και βάση εμπιστοσύνης («root-of-trust), η ασφάλεια υλικού αποτελεί πρόκληση. Πρόσφατα, έχουν προταθεί διάφορες μέθοδοι για προστασίας του υλικού από πιθανές επιθέσεις. Ωστόσο, οι συμβατικοί μηχανισμοί ασφαλείας δεν επαρκούν πάντα για να προστατέψουν το υλικό. Οπότε, απαιτούνται νέες προσεγγίσεις ασφάλειας. Στην κατεύθυνση αυτή, η εργασία μελετά πολυεπίπεδα την εφαρμογή της θεωρίας παιγνίων για την ασφάλεια υλικού απέναντι σε κακόβουλες επιθέσεις και διερευνά τις αλληλεπιδράσεις μεταξύ ενός κακόβουλου κατασκευαστή και του τελικού χρήστη. Αρχικά, η εργασία παρέχει πληροφορίες για υλικό, τους τύπους του υλικού, τα θέματα ασφάλειας και αξιοπιστίας του υλικού, τα τρωτά σημεία, τις απειλές και τα αντίμετρα απέναντι στις επιθέσεις. Στη συνέχεια, η εργασία ερευνά τη χρήση της θεωρίας παιγνίων, θεωρεί την ασφάλεια ως ένα μη συνεργάσιμο, μηδενικό, επαναλαμβανόμενο παιχνίδι και αποτυπώνει τη λογική των διαφορετικών τύπων ασφάλειας υπό αβεβαιότητα. Με δεδομένο ότι κακόβουλοι χρήστες επιτίθενται στο υλικό για να προκαλέσουν φθορά ή να συλλέξουν δεδομένα, το παίγνιο διαχωρίζεται σε ένα στάδιο μάθησης, στο οποίο ο αμυνόμενος μαθαίνει για τις τάσεις του επιτιθέμενου, καθώς και σε ένα στάδιο πραγματικού παιγνίου, όπου χρησιμοποιείται αυτή η μάθηση. Η εργασία παρουσιάζει τα πρόσφατα ερευνητικά αποτελέσματα εφαρμογής της θεωρίας παιγνίων για την ασφάλεια υλικού, συμπεριλαμβανομένων των αποτελεσμάτων ανίχνευσης Δούρειων Ίππων Υλικού (Hardware Trojans – HTs) στα ολοκληρωμένα κυκλώματα.

ABSTRACT

In recent years, significant progress has been made in the field of computer security. At the same time, however, attacks by malicious users are evolving and becoming more dangerous. Although the hardware of these systems is considered inherently secure and a basis of trust ("root-of-trust"), hardware security is a challenge. Recently, various methods have been proposed to protect the hardware from potential attacks. However, conventional security mechanisms are not always sufficient to protect hardware. Thus, new security approaches are required. In this direction, the paper studies the application of game theory for hardware security against malicious attacks in multi-level manner and explores the interactions between a malicious manufacturer and the end user. First, the paper provides information on hardware, hardware types, hardware security and reliability issues, vulnerabilities, threats, and countermeasures against attacks. The paper then explores the use of game theory, considers security as a non-cooperative, zero-sum, repeated game, and captures the logic of different types of security under uncertainty. Given that malicious users attack the hardware to cause damage or collect data, the game is separated into a learning stage, in which the defender learns about the attacker's tendencies, and an actual game stage, where this learning is used. The paper presents the recent research results of applying game theory to hardware security, including the detection results of Hardware Trojans (HTs) in integrated circuits.

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΣΥΜΒΟΛΙΣΜΟΙ

HSM: Hardware Security Modules

PUFs: Physical Unclonable Functions

CPU: Central Processing Unit

PCBs: Printed Circuit Boards

COTS: Commercial Off the Shelf

ASICs: Application Specific Integrated Circuits

IC: Integrated Circuit

IP: Internet Protocol

HTs: Hardware trojans

IoT: Internet of Things

RSA: Rivest-Shamir-Adleman

SPA: Simple power analysis

DPA: Differential power analysis

ML: Machine Learning

EMA: Ανάλυση ηλεκτρομαγνητικής ισχύος

CAD: Computer-aided design

MAC: Message Authentication Code

XbarPUF: memristive Crossbar PUF

WTMPUF: Write-Time Memristive PUF

AES: Advanced Encryption Standard

PKI: Public key infrastructure

CMOS: Complementary metal-oxide semiconductor

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή στο υλικό

Το υλικό αποτελεί έναν πολύ σημαντικό κρίκο στην αλυσίδα της λειτουργικότητας ενός συστήματος, για την γρήγορη κι επιτυχή απόδοση των υπηρεσιών που υπηρετεί ως προς την καθημερινότητα των ανθρώπων. Όμως η δυσκολία ως προς την ασφάλεια των υλικών είναι ένα πολύ σύνθετο και πολύπλοκο ζήτημα, καθώς και οι διάφορες τεχνικές και μηχανισμοί προστασίας που έχουν δημιουργηθεί τα τελευταία χρονιά, έρχονται να προσθέσουν ακόμα περισσότερη πολυπλοκότητα. Σε αυτήν τη εισαγωγική ενότητα θα αναφέρουμε κάποιες βασικές έννοιες κι ορισμούς που αφορούν στο υλικό, με σκοπό να διευκολύνουμε την ανάπτυξη των κεφαλαίων της διπλωματικής που αναφέρονται παρακάτω.

Εικόνα 1 Διάφοροι τύποι υλικού

Ως είθισται γενικότερα, έτσι και στην ορολογία του υλικού χρησιμοποιούνται αρκετοί αγγλικοί όροι. Αν κάποιος προσπαθήσει να ανατρέξει να βρει τον όρο υλικό στην βιβλιογραφία, θα συναντήσει την αγγλική λέξη hardware. Το υλικό είναι μια ηλεκτρονική διάταξη, που αποσκοπεί στο να συμμετέχει ενεργά σε ένα λειτουργικό σύστημα που εμπεριέχεται, αποτελώντας σημαντικό μέρος του μαζί και με άλλες συσκευές, με στόχο την επιτυχή κι ασφαλή λειτουργία του οποιαδήποτε συστήματος εξυπηρετεί, λειτουργώντας μαζί και με τα υπόλοιπα μέρη, όπως είναι και το λογισμικό (software). Επίσης το υλικό θέτει ως μέγιστο στόχο την παροχή ασφαλών πληροφοριών στους εξουσιοδοτημένους χρήστες του, όταν αυτοί τις χρειάζονται.

Υλικό μπορεί να είναι ένα οποιοδήποτε φυσικό μέρος ή συσκευή που μπορούμε να την δούμε και να την αγγίξουμε. Η κάθε συσκευή έχει την δική της αυτόνομη λειτουργία, αλλά παράλληλα συνεργάζεται και με τα υπόλοιπα μέρη ενός συστήματος που απαρτίζεται (υλικό και λογισμικό). Οι διάφοροι τύποι υλικών που μπορεί να

συναντήσουμε σε ένα λειτουργικό σύστημα είναι μια οθόνη, μια μητρική πλακέτα, μια μονάδα ισχύος, καθώς και διάφορες μικρότερες περιφερειακές συσκευές όπως το ποντίκι ή το πληκτρολόγιο. Οι διάφοροι τύποι συσκευών αλληλοεπιδρούν μεταξύ τους και συνεργάζονται με στόχο την πλήρη λειτουργικότητα του συστήματος. Το υλικό είναι αυτό που μεταφέρει το λογισμικό.

Πίνακας 1 Οι σημαντικότεροι τύποι υλικού

	Οι σημαντικότεροι τύποι υλικού
1	CPU ή μικροεπεξεργαστής
2	Μνήμη
3	Μητρική πλακέτα
4	Σκληρός δίσκος
5	Συσκευές εισόδου
6	Προσαρμογέας δικτύου

1.2 Ασφάλεια και αξιοπιστία του υλικού

Η ασφάλεια του υλικού αποτελεί για την σημερινή εποχή ένα μέιζον θέμα ως προς την αξιοπιστία και την εγγύτητα της ασφαλής λειτουργίας των ψηφιακών συστημάτων. Τα παλαιότερα χρόνια η ασφάλεια εστιαζόταν γύρω από το λογισμικό (software security), καθώς οι επιθέσεις στόχευαν περισσότερο το λογισμικό κι ως εκ τούτου δινόταν ιδιαίτερη βαρύτητα στην αντιμετώπιση τυχών κακόβουλων επιθέσεων γύρω από αυτόν τον τομέα.

Στο πέρασμα του χρόνου όμως αυτό άλλαξε σημαντικά κι αρχίσαν να γίνονται όλο και περισσότερες επιθέσεις στο υλικό, όπου παραβίαζαν την ασφάλεια του εκάστοτε υλικού, μειώνοντας την αξιοπιστία του. Ανέκαθεν όμως η απαρέγκλιτη λειτουργία του υλικού, ασχέτως με την έκθεση του σε εχθρικά περιβάλλοντα, αποτελούσε κι επιβαλλόταν να ήταν κι είναι μέιζον προτεραιότητας θέμα ως προς την ορθή λειτουργία του και την αξιοπιστία του.

Η ασφάλεια υλικού αποσκοπεί στην διαφύλαξη και την αξιοπιστία των συστημάτων από λάθη, σφάλματα και εγκληματικές πράξεις. Απαιτείτε φυσικά μεγάλη εξειδίκευση και μια πολύ μεγάλη επιστημονική ομάδα, αποτελούμενη από πολλές ειδικότητες, έτσι ώστε να μπορεί η ασφάλεια του υλικού να είναι όσον το δυνατότερο εξειδικευμένη, πολυεπίπεδη και να μπορεί να ανταπεξέλθει στην οικονομία, στους νόμους και στους οργανισμούς. Η ικανότητα ενός συστήματος για να τα καταφέρνει εξίσου καλά στην ανάλυση, στην αξιολόγηση και στον έλεγχο είναι σημαντικές

παράμετροι, αλλά δεν επαρκούν γιατί ασχολούνται μόνο με τα λάθη και τα σφάλματα [16].

Για την ασφάλεια του υλικού απαιτούνται υψηλές προδιάγραφες διασφάλισης έτσι ώστε η λειτουργία του να γίνετε απερίσκεπτα και απρόσκοπτα. Ένα λάθος ή μια αποτυχία στην διασφάλιση μπορεί να θέσει σε κίνδυνο το περιβάλλον, την οικονομία, να ανθίσει την εγκληματικότητα ή κι ακόμα τον ίδιο τον άνθρωπο. Βέβαια η κάθε κατηγορία απαιτεί διαφορετική προσέγγιση προς την αποτελεσματικότητα της ασφάλειας και των συστημάτων που θα προστατεύουν το εκάστοτε υλικό.

Πολλές φορές η αποτυχία ως προς την διασφάλιση της ακεραιότητας του υλικού, οφείλετε στο ότι οι κατασκευαστές τους προστατεύουν το υλικό με λάθος τρόπο. Έτσι πρέπει να γίνει κατανοητό πως πρέπει να γνωρίζουμε καλά τι είναι αυτό που θέλουμε να προστατεύσουμε και με ποιον τρόπο, εξ αρχής. Εξίσου σημαντική είναι επίσης και η ορθή συντήρηση των συστημάτων, για να υπάρχει στο χρόνο καλή ανταπόκριση τους κατά την χρήση τους.

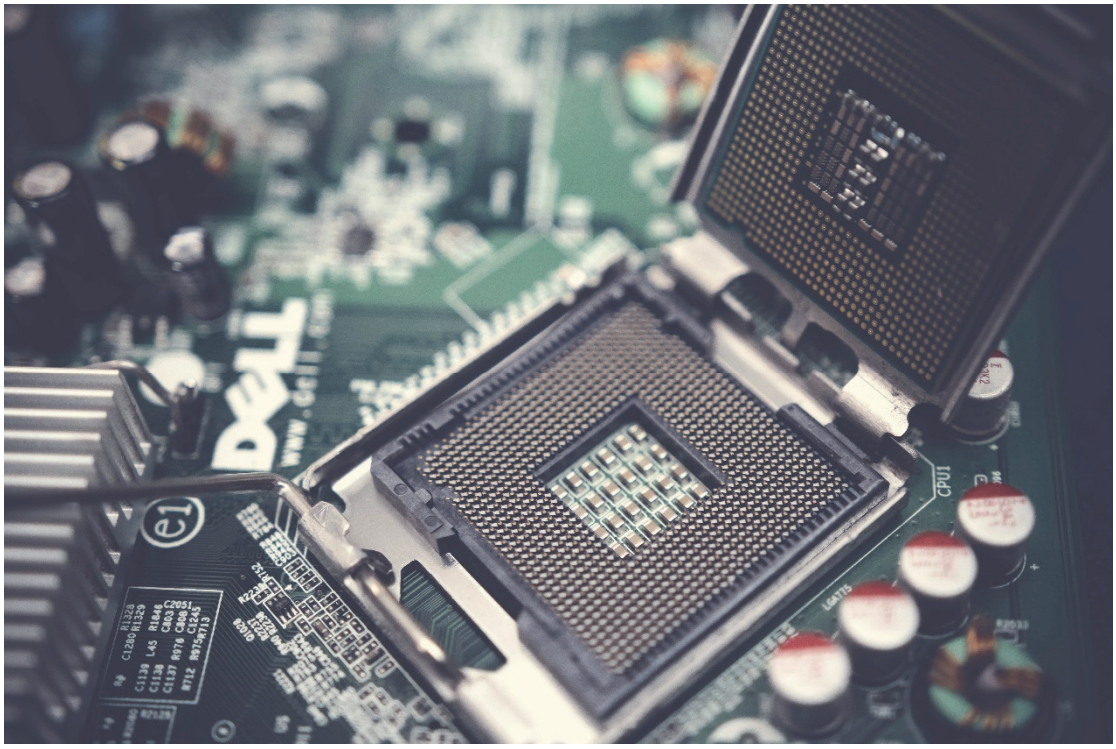
Ορίζοντας ένα γενικό πλαίσιο για το τι μπορεί να θεωρηθεί καλή και σωστή ασφάλεια, θα επικεντρωθούμε σε τέσσερα βασικά πράγματα. Πρώτον στην πολιτική, δεύτερον στον μηχανισμό, τρίτον στην διαβεβαίωση και τέταρτον στο κίνητρο. Είναι πλέον πολύ σημαντικό να γνωρίζουμε τι θέλουμε να πετύχουμε, ορίζοντας την πολιτική μας, την κρυπτογράφηση μας για τον ορθό έλεγχο πρόσβασης, την εμπιστοσύνη που μπορούμε να δείχνουμε στον εκάστοτε μηχανισμό, καθώς και το κίνητρο που υπάρχει ώστε να διαφυλάξουμε το σύστημα ακέραιο.

Τέλος, καλό είναι από την πλευρά των εταιρειών να ανακοινώνονται οι πολιτικές ασφαλείας και ποιοι είναι οι στόχοι τους. Μπορεί αυτό να είναι κουραστικό για τους αγοραστές, όμως οι ξεκάθαροι στόχοι απαιτούν κατασκευές με εξασφαλισμένη ασφάλεια.

1.3 Βήματα κατασκευής υλικού

Για την κατασκευή ενός υλικού (chip) απαιτούνται κάποια βήματα έτσι ώστε να παραχθεί ένα ολοκληρωμένο κύκλωμα. Τα στάδια αυτά είναι η σχεδίαση, η εσωτερική διάταξη, η χάραξη του όπου παράγετε ένα wafer (ένας δίσκος πυριτίου). Από αυτά τα στάδια παράγετε μια παρτίδα chip τα οποία τεμαχίζονται κι αποτελώντας πολλά μικρά κομμάτια, εσωκλείονται σε διάφορα κυκλώματα. Πριν εισαχθούν στα διάφορα κυκλώματα που θα περιέχονται, θα πρέπει απαραιτήτως να ελεγχθούν πρωτίστως για διάφορες αστοχίες. Τέλος, τα διάφορα υλικά (chip) μέσω μεταλλικών

ακίδων που είναι απαραίτητες για την σύνδεση στην πλακέτα, τοποθετούνται σε μια συσκευασία.



Εικόνα 2 Chip

1.4 Αρχιτεκτονική του υλικού

Σημαίνοντα ρόλο στην κατασκευή ενός κυκλώματος παίζει η αρχιτεκτονική του, όπου εκεί αποφασίζετε το πώς οι ακροδέκτες του θα έρχονται σε επαφή με τους εξωτερικούς υποδοχείς, για τις συνδέσεις όπου θα το καθιστούν λειτουργικό. Μέσω της πλακέτας, όπου αποτελεί μέσω των εξαρτημάτων της μια ηλεκτρονική σύνδεση, από τις διαδρομές της οποίας θα επιτευχθούν οι συνδέσεις, η επικοινωνία των εξαρτημάτων και η λειτουργικότητα του υλικού (chip). Αν το υλικό (chip) που παράγετε δεν ελεγχθεί για πιθανές αστοχίες του, τότε υπάρχουν αρκετές πιθανότητες να είναι ευάλωτο ως προς την ασφάλεια του και θέτει σε κίνδυνο το όλο σύστημα που θα περιβάλετε.

1.5 Η σημασία της ασφάλειας υλικού

Η ασφάλεια του υλικού εξαρτάται από μια σύνθετη γκάμα γνωστικών αντικειμένων, που στόχο έχουν την έγκαιρη και έγκυρη ανίχνευση κακόβουλων ενεργειών απέναντι στο υλικό. Το υλικό κατά την διάρκεια μη εξουσιοδοτημένων πράξεων, αποκτά πάρα πολύ σημαντικό ρόλο για την αποφυγή κακόβουλων ενεργειών.

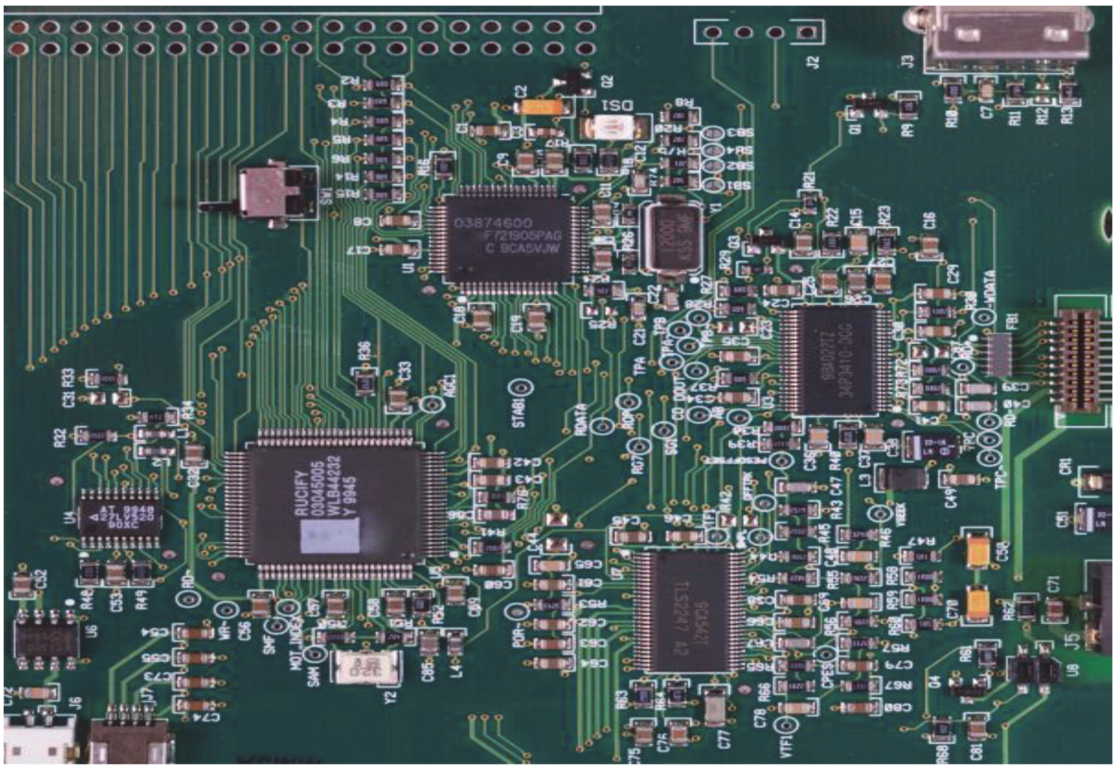
Το υλικό αποτελεί βασικό εξάρτημα για την ομαλή λειτουργία ενός ολοκληρωμένου συστήματος, κι έτσι για αυτόν το λόγο αποτελεί πάντα έναν από τους

στόχους κακόβουλων επιθέσεων και πράξεων με απώτερο στόχο την διακοπή της ομαλής του λειτουργίας του ιδίου, αλλά κι εν γένει του όλου λειτουργικού συστήματος.

Πολλές έννοιες που χρησιμοποιούνται στην ασφάλεια φαίνονται κατανοητοί κι άλλοτε δημιουργούν σύγχυση. Γι' αυτό καλό είναι να ξεκαθαρίσουμε τι είναι και τι εννοούμε με τον όρο υλικό. Είναι μια συσκευή, ένα προϊόν ή ένα υλικό ή κάποια από τα προηγούμενα που αποτελούν ένα σύστημα ή μια υποδομή, ή ακόμα όλα τα προηγούμενα μαζί με κάποιες εφαρμογές, συν το προσωπικό, τους εσωτερικούς και εξωτερικούς χρήστες, την διαχείριση και τους πελάτες.

Ο πλουραλισμός όλων των παραπάνω εννοιών είναι αυτός που προκαλεί σύγχυση σε ένα λειτουργικό σύστημα με αποτέλεσμα να υπάρχουν τρωτά σημεία. Σε όλα αυτά πάντα θα πρέπει να υπολογίζουμε και τον ανθρώπινο παράγοντα που εμπλέκετε πάντα στις διαδικασίες υλοποίησης. Το να μην υπολογιστεί λοιπόν η ανθρώπινη συνιστώσα δημιουργείτε αυτομάτως πρόβλημα ευχρηστίας του υλικού και είναι άμεσα ένας λόγος κι αυτός αποτυχίας ενός συστήματος ασφάλειας.

Στα υλικά μπορούμε να κατατάξουμε όλα εκείνα τα στοιχεία τα οποία αποτελούν ένα ηλεκτρονικό κύκλωμα. Έτσι σε αυτό μπορεί να ενταχθούν ηλεκτρονικά και αναλογικά στοιχεία όπως πυκνωτές, αντιστάσεις, ενισχυτές, τρανζίστορ, τυπωμένες πλάκες (Printed Circuit Boards-PCBs) κι εξαρτήματα όπως application specific integrated circuits-ASICs ή Commercial Off the Shelf-COTS [29].



Εικόνα 3 Ψηφιακό κύκλωμα/μικροεπεξεργαστές

Τα κυκλώματα προσαρμοσμένης λειτουργίας ASICs όπως το αποτυπώνει και η φράση παράγονται και δημιουργούνται για συγκεκριμένο λόγο έπειτα από ζήτηση για να εκπληρώσουν έναν στόχο. Τα κυκλώματα γενικής χρήσης COTS, μπορούν να εξυπηρετήσουν την λειτουργία του εκάστοτε λειτουργικού συστήματος σε μια πιο γενικευμένη εμπορική χρήση.

1.6 Άλλες λύσεις για την ασφάλεια υλικού

Στο πέρασμα των χρόνων, παρατηρείται να έχουμε και μια αυξανόμενη ζήτηση ως προς την μελέτη εκείνων των λύσεων που θα βοηθήσουν ακόμα περισσότερο στην μεγιστοποίηση της ασφάλειας των υλικών. Οι περισσότερες λύσεις, μέχρι και σήμερα, εστιάζουν στην εξασφάλιση της ιδιωτικότητας του υλικού, σε όλες τις εκδόσεις της εφαρμογής του στο υλικό. Πιο συγκεκριμένα, παρατηρείται η διάσταση να προτείνονται διάφορες αρχιτεκτονικές και διαφορετικές τεχνικές ασφαλείας που σκοπό έχουν την διασφάλιση της ιδιωτικότητας των συσκευών, και με τους όσο πιο δυνατόν λιγότερους πόρους.

Ένα ζήτημα που προκαλεί την μη εγγυημένη ασφάλεια στις συσκευές είναι πως χρησιμοποιούν στους επεξεργαστές τους πολύ χαμηλής ποιότητας λειτουργικά συστήματα, έχοντας πολύ μικρή μνήμη και χωρητικότητα, κοντά στις πιο χαμηλότερες προδιάγραφες που απαιτούνται για να τους παραχωρηθεί η άδεια κυκλοφορίας, κάνοντας πολύ περιπλοκή την ασφάλεια και την προστασία τους. Επιπλέον, λύσεις μπορούν να δοθούν μέσα από τα κρυπτογραφικά πρωτόγονα και από τα πρωτόκολλα ελέγχου ταυτότητας που αποτελούν σύγχρονους μηχανισμούς ασφάλειας [24].

1.7 Η θεωρία των παίγνιων ως λύση για την ασφάλεια υλικού

Ένα πολύτιμο εργαλείο στην προστασία και στην ασφάλεια του υλικού, μπορεί να μας προσφέρει η θεωρία των παίγνιων. Οι λύσεις μέσα από τα παίγνια, τις στρατηγικές και τις σημαντικές αποφάσεις που λαμβάνονται μέσω αυτών, αποτρέπει τις κακόβουλες επιθέσεις σε συσκευές, συνεισφέροντας στην μεγιστοποιήσει της ασφάλειας. Η επιστήμη της μηχανικής μάθησης είναι αυτή που ασχολείται με την κατασκευή των υλικών και μέσα από την συνεχιζόμενη ενασχόλησή της, αποκτώντας εμπειρίες και γνώση, μπορεί να βελτιώνει την ασφάλεια στο πέρασμα των χρόνων.

Η θεωρία των παίγνιων ως ένα παρακλάδι των μαθηματικών, αποτελείται από ένα σύνολο ειδικά σχεδιασμένων εργαλείων, με στόχο να μπορούμε να κατανοήσουμε το πώς τα άτομα που λαμβάνουν σημαντικές αποφάσεις αλληλοεπιδρούν κι επηρεάζονται. Οι αποφάσεις που παίρνονται χρήζουν ανάλυσης μέσω της επιστήμης της θεωρίας των παίγνιων, για να μπορέσουμε να προβλέψουμε καταστάσεις από τους

συμμετέχοντες (παίχτες), όπου η κάθε απόφαση τους είναι αλληλεξαρτούμενες από τις στρατηγικές του εκάστοτε παίχτη [31].

Η ασφάλεια του υλικού μπορεί να στηριχθεί στην επιστήμη της θεωρίας των παίγνιων καθώς τα άτομα που επιτίθονται στο υλικό, λαμβάνουν αποφάσεις που στόχος τους είναι μέσα από καθορισμένες στρατηγικές να παρέμβουν σε μια συσκευή, λαμβάνοντας πάντα υπόψιν τους και την γνώση που μπορεί να διαθέτουν τα άτομα που βρίσκονται απέναντι τους. Η δυνατότητα που μας δίνεται να μπορούμε να συλλέξουμε και να κατανοήσουμε τις στρατηγικές αποφάσεις κατά την διάρκεια μιας επίθεσης στο υλικό, είναι αυτή που κάνει την θεωρία των παίγνιων μοναδική στην αντιμετώπιση των επιθέσεων του υλικού. Κάτι το οποίο δεν μπορεί συμβεί από άλλα πιθανά αντίμετρα που χρησιμοποιούνται κατά των επιθέσεων σε συσκευές, για την ασφάλειά τους.

Η συγκεκριμένη θεωρία αναπτύχθηκε για να μελετήσει καταστάσεις συμπεριφορών και στρατηγικών των παιχτών που συμμετέχουν σε ένα παιχνίδι και εξαρτώνται και από τις επιλογές των άλλων. Στο πέρασμα των ετών όμως εξελίχθηκε κι έχει φτάσει στο σημείο πλέον, να μπορεί να διαχειρίζεται μια πολύ μεγάλη γκάμα αλληλεπιδράσεων. Πλέον, μπορεί να προσφέρει λύσεις σε διάφορους τομείς της κοινωνικής μας ζωής μέσα από διάφορες αποφάσεις στρατηγικής σημασίας καθώς και να διαχειρίζεται τα αποτελέσματα των αποφάσεων αυτών. Αυτό συμβαίνει και με την ασφάλεια υλικού, όπου μπορεί να αναλύει αποφάσεις και αποτελέσματα των διαφόρων τύπων επιθέσεων που μπορούν να συμβούν κατά την διάρκεια της παρέμβασης σε μια συσκευή.

Η εφαρμογή της θεωρίας των παίγνιων στην ασφάλεια του υλικού, προσπαθεί να βρει καταστάσεις ισορροπίας, κατά την διάρκεια της επίθεσης, στην συσκευή που απειλείται από κακόβουλη ενέργεια. Την σημερινή εποχή θα μπορούσαμε να αναφέρουμε ότι η θεωρία των παίγνιων αποτελεί ένα είδος ομπρέλας στην κοινωνική επιστήμη, γιατί έχει την δυνατότητα να προστατεύει τους ανθρώπους και μη, όπως και τις συσκευές που είναι το θέμα μας στην παρούσα διπλωματική εργασία.. Φυσικά και είναι αδύνατον μόνο μια θεωρία να μπορεί να προστατεύει μια τόσο μεγάλη γκάμα παιχνιδιών. Γι' αυτό έχουν προταθεί κι έχουν αναπτυχθεί αρκετές θεωρίες όπου η κάθε μια έχει το δικό της πεδίο εφαρμογής και με τα ανάλογα αποτελέσματα ανά περίπτωση [31].

1.8 Δομή εργασίας

Στην παρούσα εργασία, αρχικά γίνεται εισαγωγή σε γενικές έννοιες πάνω στην ασφάλεια υλικού, συμπεριλαμβανομένων και κάποιων βασικών χαρακτηριστικών του.

Επίσης θα αναφερθούμε και σε θεωρητικά θέματα που αφορούν την θεωρεία των παίγνιων και την πιθανή λύση που μπορεί να προσφέρουν, ενάντια στις επιθέσεις του υλικού. Αυτό το σενάριο αποτυπώνεται χρησιμοποιώντας τη θεωρία των παίγνιων.

Θα αναφερθούμε στο 2ο κεφάλαιο στην ασφάλεια του υλικού γενικότερα, δίνοντας έμφαση σε πιθανούς κίνδυνους που ελλοχεύουν, ποιες είναι οι ευπάθειες που προκύπτουν σε ένα υλικό και χρειάζεται να εξειδικεύσουμε περισσότερο σε θέματα ασφάλειας. Στο 3ο κεφάλαιο θα δούμε κάποιες συμβατικές μεθόδους ασφαλείας υλικού, τι περιορισμοί υπάρχουν και μας οδηγούν στην πρόταση για ασφάλεια μέσω της θεωρίας παίγνιων.

Στο 4ο κεφάλαιο θα αναφερθούμε στην θεωρία των παίγνιων, αναλύοντας κάποιες θεωρητικές έννοιες. Στο 5ο κεφάλαιο θα μιλήσουμε για τις μεθόδους ασφάλειας υλικού που βασίζονται στη θεωρία των παίγνιων. Στο 6ο και τελευταίο κεφάλαιο θα αναφερθούμε σε συμπεράσματα που προκύπτουν μέσα από την ανάπτυξη των κεφαλαίων της διπλωματικής και κάνοντας κάποιες προτάσεις, προς όφελος της ασφάλειας του υλικού [16].

ΚΕΦΑΛΑΙΟ 2: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΥΛΙΚΟΥ

2.1 Γενικά ζητήματα ασφάλειας υλικού

Κατά τα πρώτα χρόνια κατασκευής των διαφόρων υλικών, η ασφάλεια τους δεν αποτελούσε μέιζον θέμα κατά την φάση του σχεδιασμού τους, καθώς προτεραιότητα δινόταν στην ανθεκτικότητα και στην λειτουργικότητά τους. Αυτές οι προτεραιότητες, εκτός των μηχανισμών ασφαλείας, προκάλεσαν μια ελλιπής πολιτική ασφαλείας και διαχείρισης των υλικών. Μέσα από αυτήν την αδυναμία μιας σταθερής πολιτικής ασφαλείας, προκλήθηκαν και αρκετά ζητήματα ασφάλειας των συσκευών που αφορούσαν σε μια σειρά επικίνδυνων επιθέσεων όπως είναι η διασπορά του κακόβουλου λογισμικού στο υλικό (viruses, Trojan horses, worms), η πλαστοπροσωπία (masquerading), η παθητική ή ενεργή παρακολούθηση (passive tapping ή active tapping), η ανάλυση επικοινωνίας (traffic analysis), καθώς και η επανεκπομπή μηνυμάτων (replay).

Η άμυνα και η προστασία του υλικού από τις παραπάνω πιθανές επιθέσεις, αποτελεί μέγιστο στόχο των κατασκευαστών, έτσι ώστε οι τελικοί χρήστες να μπορούν να χρησιμοποιούν τις συσκευές για τις υπηρεσίες που προσφέρουν και παρέχουν, δίχως να κινδυνεύουν από κακόβουλες επιθέσεις, η αξιοπιστία και η ακεραιότητά τους. Αλλιώς σε μια διαφορετική περίπτωση μπορεί να προκληθούν πολλαπλές και διάφορες συνέπειες όπως είναι η αποκάλυψη ή αλλοίωση των πληροφοριών μιας συσκευής, η αδυναμία εξυπηρέτησης από την συσκευή, καθώς και το κόστος αυξάνεται για να διορθωθούν οι δυσλειτουργίες που προκλήθηκαν από τις επιθέσεις. Όλες οι παραπάνω συνέπειες είναι ικανές από μόνες τους να καταδείξουν την σημαντικότητα της ασφάλειας του υλικού.

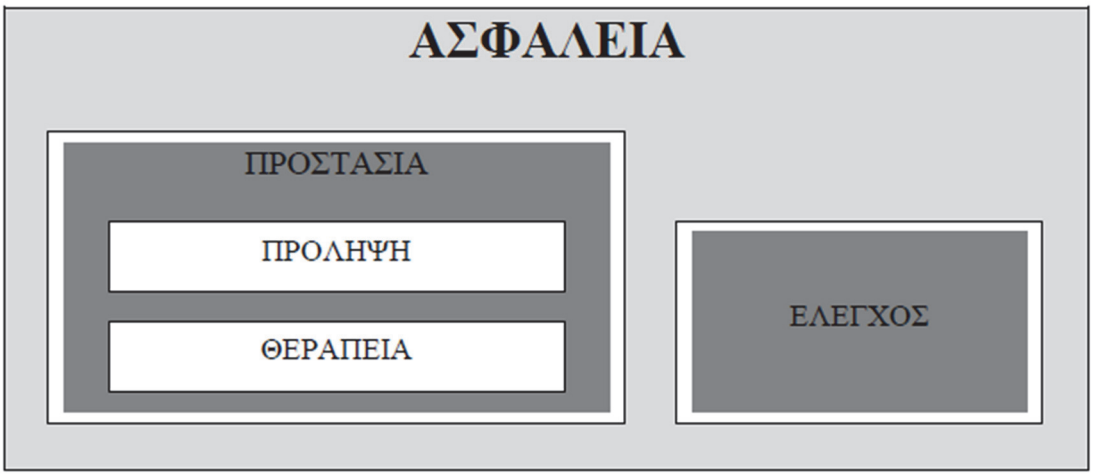
2.2 Γενικά θέματα ασφάλειας

Σε αυτό το κεφάλαιο θα αναφερθούμε στην προστασία του υλικού και στην αναγκαιότητα που υπάρχει για την ασφάλεια του υλικού. Η ασφάλεια σχετίζεται γενικώς με τρεις βασικές παραμέτρους: τον άνθρωπο, το ίδιο το υλικό και την εξέλιξη της τεχνολογίας, της γνώσης και της εκπαίδευσης των ανθρώπων, καθώς και της πολιτικής φιλοσοφίας της χωράς όσον αφορά τα θέματα για την ασφάλεια του υλικού. Το υλικό δημιουργείται από τον άνθρωπο για να εξυπηρετήσει τις ανάγκες και τις απαιτήσεις του ανθρώπου, κι η συμπεριφορά του οποίου δεν μπορεί να προβλεφθεί.

Το υλικό είναι αυτό που γίνετε περιζήτητο λόγο της ποιότητάς του και τα τελευταία χρόνια λόγο των αποκλειστικών δικαιωμάτων του κάθε αγαθού αποκτά μεγάλη αξία, παράλληλα με την προστασία των πληροφοριών που διαδίδει. Επίσης, η

τεχνολογία χαρακτηρίζετε από την ταχύτατη εξέλιξή της κι αυτό δημιουργεί τεράστια περιθώρια βελτίωσης, ανά μικρά τακτά χρονικά διαστήματα, στο κάθε υλικό συγκεκριμένα, αλλά και σε όλη την πληροφορική γενικότερα.

Τέλος σημαντικό είναι να αναφέρουμε ότι τα υλικά πλέον αρχίζουν κι έχουν ένα συγκεκριμένο κύκλο ζωής κι αυτό από μόνο του επιφέρει στην κάθε επιχείρηση να χρειάζεται να επενδύει χρήματα για την ποιότητα του υλικού. Καταλαβαίνουμε λοιπόν, το πόσο σημαντικό είναι να προστατεύονται τα υλικά από διάφορες κακόβουλες επιθέσεις [27].



Εικόνα 4 Η έννοια της ασφάλειας [27]

Στο πέρασμα των χρόνων η εξέλιξη της τεχνολογίας έχει επηρεάσει την εξέλιξη της ασφάλειας μέσα από διάφορα μοντέλα ενός συστήματος, που στόχο έχουν τη δημιουργία νέων μέτρων προστασίας. Μέσω διάφορων τεχνικών και μεθόδων αποσκοπούμε στην καλύτερη ασφάλεια του υλικού. Οι τεχνικές αυτές κι οι νέες μέθοδοι μπορούν να χωριστούν σε δυο κατηγορίες, που είναι κατά περίπτωση είτε σε μια εκτατή ανάγκη, είτε κατά την καθημερινή λειτουργία του υλικού.

Εικόνα 5 Τα στάδια της ασφάλειας

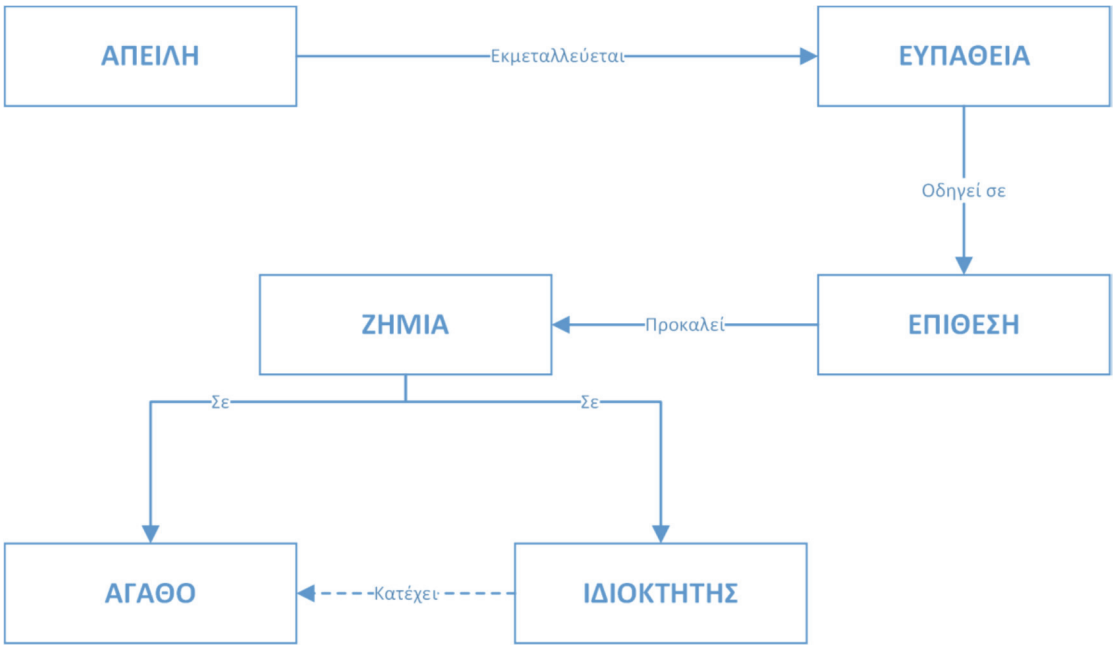
Στην πρώτη περίπτωση κατά την στιγμή μιας ξαφνικής δυσλειτουργίας του, μπορεί να υπάρξει μια ολική καταστροφή ή μια μερική δυσλειτουργία του υλικού, όπου αυτό μπορεί να οφείλετε σε φυσικά αίτια (πχ διακοπή ρεύματος, πυρκαγιά), σε κακή επικοινωνία του υλικού με τον υπόλοιπο εξοπλισμό, αστοχία του ιδίου του υλικού, είτε

ακόμα κι από πτώση του υλικού ή του εξοπλισμού. Ουσιαστικά σε μια τέτοια περίπτωση είναι αδύνατη η ορθή επαναλειτουργία του υλικού. Σε αυτές τις περιπτώσεις πάντα μια καλή λύση είναι να υπάρχει κάποιο υλικό ως εφεδρικό, το οποίο θα έχει όμως ελεγχθεί και δοκιμαστεί και πρωτύτερα ότι μπορεί να ανταποκριθεί στις απαιτήσεις μας, δίχως να προκαλεί δυσλειτουργία και στα υπόλοιπα μέρη του λειτουργικού συστήματος που χρησιμοποιούμε.

Η πρόβλεψη κατά την διάρκεια χρήσης ενός υλικού, ως προς την ασφάλεια του πρέπει να είναι συνεχής και να δίνετε ιδιαίτερο βάρος κατά την καθημερινή του λειτουργία, χωρίς καμία έκπτωση ως προς τη ασφάλεια. Η χρήση ενός υλικού, η πρόσβαση σε αυτό, η συντήρηση του, η επιδιόρθωσή του καθώς και το ποιος έχει την ευθύνη και την εποπτεία της λειτουργικότητάς του, η οποία θα πρέπει να γίνετε από άτομα εξειδικευμένα και έμπιστα [29].

Συνεπώς κατά την χρήση και την λειτουργία ενός υλικού θα πρέπει να έχουμε φυσική και λογική προστασία, για προφυλάξεις από φυσικά αίτια και κακόβουλες πράξεις. Οι κίνδυνοι που διατρέχει ένα υλικό είναι αρκετοί και μέσα από αρκετές συνιστώσες πρέπει να προστατευτεί. Μερικά παραδείγματα μέτρων προστασίας είναι η χρήση του υλικού από εξουσιοδοτημένα άτομα, η καταγραφή των συνήθων τρόπων παραβιάσεων ασφάλειας, η ορθή εποπτεία, η τήρηση βασικών κανόνων ασφαλείας και η όσο τον δυνατόν σωστών χώρων χρήσης των υλικών έτσι ώστε να τηρούνται οι βασικές προδιαγραφές (π.χ. πυρασφάλεια).

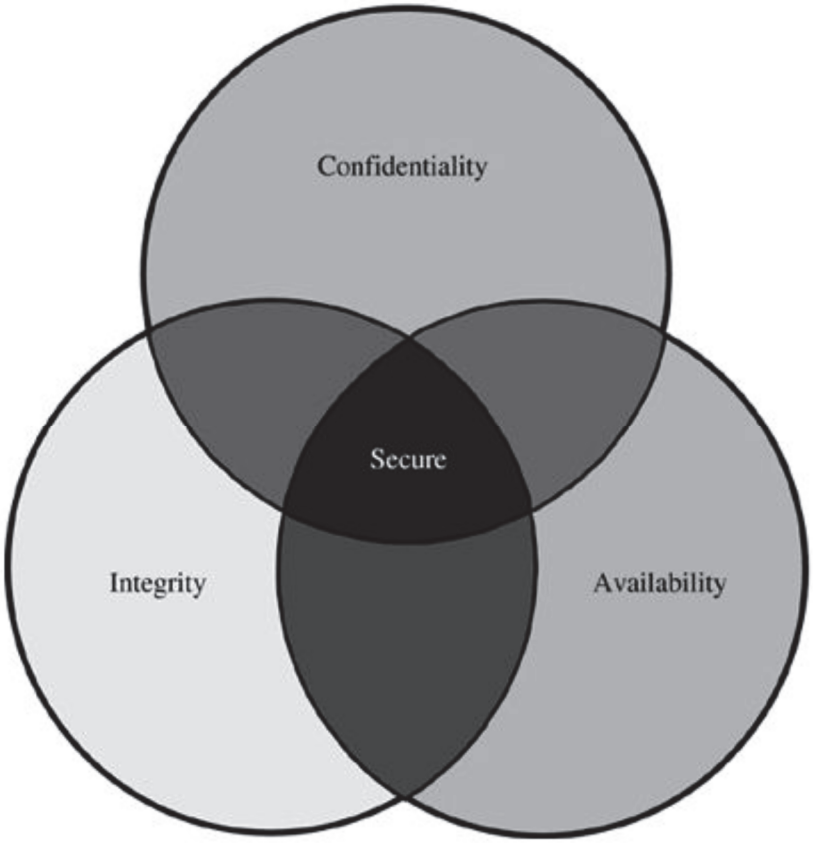
Για την αξιοπιστία της ασφάλειας του υλικού, θα πρέπει να γίνονται κάποια τεστ για να διαπιστωθεί αν το υλικό είναι ευάλωτο από διάφορες επιθέσεις. Επίσης, θα πρέπει διάφορες δοκιμές να πραγματοποιούνται για να διαπιστωθεί εάν το υλικό είναι ευάλωτο σε ξαφνικές και απρόκλητες συμπεριφορές ως προς την λειτουργία του. Σημαντικό είναι οι έλεγχοι να διενεργούνται στην αρχή μιας κατασκευής ενός ολοκληρωμένου συστήματος, γιατί σε μεταγενέστερα στάδια οι δοκιμές ελέγχου απαιτούν περισσότερο κόστος και χρόνο, για την επιδιόρθωσή τους. Γι’ αυτό και οι καλοί έλεγχοι στο υλικό, πριν την χρήση του, είναι πολύ σημαντική παράμετρος για την αξιοπιστία του. Σημαντικό επίσης κατά την διάρκεια των δοκίμων είναι να μπορέσουμε να καταγράψουμε τυχόν γνωστές αστοχίες. Η παρούσα εργασία θα εμβαθύνει σε θέματα ασφάλειας υλικού και προστασίας του από κακόβουλες εξωτερικές επιθέσεις [29].



Εικόνα 6 Συσχέτιση βασικών εννοιών

2.3 Παράγοντες ασφάλειας υλικού

Εξαρχής η ακεραιότητα, η εμπιστευτικότητα, η διαθεσιμότητα και η αξιοπιστία ενός υλικού αποτελούσαν ιδιαιτέρως σημαντικούς παράγοντες για την ασφάλεια ενός συστήματος. Αυτές οι μέθοδοι που θα αναφερθούν στις παρακάτω παραγράφους αποτελούν συμβατές μεθόδους ασφαλείας που χρησιμοποιούνται στις μέρες μας. Όμως έχει παρατηρηθεί πως μόνο με αυτές τις μεθόδους δεν καλύπτετε επαρκώς η ασφάλεια του υλικού και για αυτό το λόγο σε επόμενα κεφάλαια θα αναπτύξουμε και την ασφάλεια του υλικού μέσω της θεωρίας των παίγνιων.



Εικόνα 7 Βασικές αρχές ασφάλειας [27]

Ως προς την ακεραιότητα θέλουμε να εξασφαλίζουμε ότι τα δεδομένα που μεταφέρονται δεν θα κινδυνεύουν από κάποιον εξωτερικό παράγοντα να καταστραφούν μερικώς ή ολικώς. Αυτό μπορεί να επιτευχθεί με την λειτουργία κατακερματισμού (hash functions) με την οποία προσθέτουμε περισσότερη ασφάλεια στα δεδομένα, καθώς και σε οποιαδήποτε προσπάθεια παρέμβασης, η λειτουργία του κατακερματισμού μεταβάλετε (hash value).

Μέσω των κρυπτογραφικών αλγορίθμων μπορούμε ως προς την εμπιστευτικότητα να μειώσουμε τους κινδύνους ώστε τα δεδομένα να μην μπορούν να είναι ευάλωτα από τρίτους μη εξουσιοδοτημένους χρήστες. Το πιο ιδανικό σενάριο θα είναι, πρόσβαση στο εκάστοτε υλικό, που μπορεί ενίοτε να αποτελεί και στόχο κακόβουλων επιθέσεων, να μπορεί να έχουν μόνο οι εξουσιοδοτημένοι χρήστες, χρησιμοποιώντας κάποιο κλειδί κρυπτογράφησης.

Ως προς τη διαθεσιμότητα επιδιώκουμε πως όταν χρειάζονται κι αναζητούνται τα δεδομένα ή κάποιες πληροφορίες από ένα υλικό, αυτά να είναι πάντα διαθέσιμα κατά την λειτουργικότητα του συστήματος.

Τέλος, ως προς την αξιοπιστία του υλικού, νοούμε την ικανότητα του εκάστοτε υλικού να μπορεί να αποκρίνετε ορθά στις λειτουργίες που εκτελεί και για το σκοπό

που προορίζεται, όταν αυτές του ζητούνται. Η διάρκεια του και η λειτουργικότητά του θα πρέπει ιδανικά να είναι έτσι δομημένη ώστε να μπορεί να ανταποκρίνεται σε συγκεκριμένες συνθήκες. Αν το υλικό όμως το αφήσουμε εκτεθειμένο κάτω από αντίξοες περιβαλλοντικές συνθήκες άμεσα το καθιστούμε ευάλωτο σε εχθρικά περιβάλλοντα, και αυτό θα το κάνει μη λειτουργικό ως προς την χρήση για την οποία προορίζετε. Ακόμα ακόμα μπορεί να τεθεί και εντελώς εκτός λειτουργίας [29].

ΑΣΦΑΛΕΣ	ΕΜΠΙΣΤΟ
Είναι ή δεν είναι ασφαλές;	Υπάρχουν διάφορες βαθμίδες εμπιστοσύνης
Ισχυρισμός	Πεποίθηση
Βεβαιώνεται στη βάση χαρακτηριστικών ασφάλειας του προϊόντος	Κρίνεται στη βάση γεγονότων και αναλύσεων
Απόλυτο: χωρίς επιφυλάξεις για το πώς, που, πότε και από ποιόν χρησιμοποιείται	Σχετικό: θεωρείται στο πλαίσιο της χρήσης
Σκοπός	Χαρακτηριστικό

Εικόνα 8 Αντιπαραβολή ασφαλούς και έμπιστου [27]

2.4 Απειλές

Τα άτομα που έχουν στην κατοχή τους ένα υλικό, μια συσκευή και το χρησιμοποιείται σε ένα ολοκληρωμένο σύστημα είναι συνήθως και η μεγαλύτερη απειλή γι' αυτό. Η κακή χρήση ενός νόμιμου υλικού από τους ανθρώπους, κατά την διάρκεια της λειτουργίας του, οφείλετε στην απροσεξία των ατόμων αυτών, στην μη καλή εκπαίδευσή τους κατά την χρήση του, σε δόλο πολλές φορές, σε μια επιπόλαιη κίνηση στα ευαίσθητα σημεία του υλικού, καθώς και σε παραποίηση των συνθηματικών του υλικού. Τέλος, ένας παραπονεμένος χρήστης ή ένας δυσαρεστημένος και κακοπροαίρετος υπάλληλος μιας εταιρείας ή ενός οργανισμού, είναι και αυτός που αποτελεί την μεγαλύτερη απειλή για την ασφάλεια του υλικού.

2.5 Είδη απειλών

Όπως έχουμε αναφέρει και παραπάνω, απειλές σε ένα υλικό είναι οι καταστάσεις αυτές όπου το ενδεχόμενο βλάβης είναι υπαρκτό και η δυσλειτουργία του συστήματος που το περιλαμβάνει, προκαλεί την ζημιά και διακόπτεται η ομαλή ροή του.

Κανονική ροή

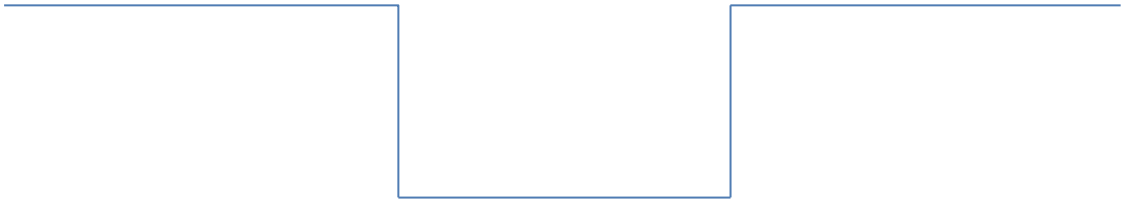
Σε ένα πληροφοριακό σύστημα που είναι άρρηκτα συνδεδεμένο με το υλικό που εσωκλείει για την λειτουργικότητά του, μπορούμε να παραθέσουμε τα παρακάτω είδη απειλών:

1) Η υποκλοπή που γίνετε συνήθως στο υλικό, έχει ως στόχο να πλήξει την εμπιστευτικότητα του συστήματος. Κάποιο μη συμβατό μέρος καταφέρνει σε αυτήν τη περίπτωση να έχει αποκτήσει πρόσβαση σε ένα μέρος του συστήματος, για να δημιουργήσει πρόβλημα μέσω της υποκλοπής. Ως παράδειγμα αναφέρουμε την κλοπή κάποιων αρχείων ή δεδομένων.

Υποκλοπή

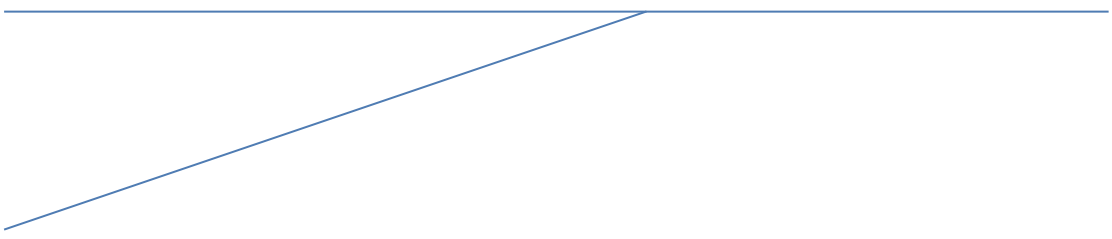
2) Η μεταβολή που γίνετε στο υλικό από ένα μη εξουσιοδοτημένο μέρος, καταφέρνει όχι απλώς να έχει πρόσβαση στα δεδομένα, αλλά να μπορεί να τα τροποποιεί, επηρεάζοντας την λειτουργία του υλικού. Η απειλή αυτή πλήττει την ακεραιότητα του υλικού και κατ' επέκταση του συστήματος. Ως παράδειγμα αναφέρουμε την μεταβολή των τιμών σε μια βάση δεδομένων.

Μεταβολή



3) Η πλαστογραφία είναι μια απειλή που σκοπό έχει την παραποίηση ενός υλικού. Σε αυτήν την περίπτωση έχουμε εισαγωγή δεδομένων που μπορούν να παραποιούν το υλικό, όπως μπορεί να συμβαίνει σε μια προσπάθεια αναπαραγωγής. Η πλαστογραφία μπορεί να προκαλέσει βλάβη στην ακεραιότητα αλλά και στην διαθεσιμότητα του υλικού.

Πλαστογραφία



4) Η διακοπή είναι μια απειλή κατά του υλικού, η οποία μπορεί να επιφέρει πλήρη παύση της λειτουργίας του υλικού, όπου και το καθιστά παντελώς άχρηστο. Μια τέτοια κακοπροαίρετη απειλή μπορεί να πλήξει την διαθεσιμότητα του υλικού, μέσα από την διαδικασία της διαγραφής αρχείων.

Διακοπή

2.6 Κατηγορίες απειλών

Οι απειλές ενάντια στο υλικό μπορούν να καταταγούν σε τρεις κατηγορίες, όπως θα αναφέρουμε παρακάτω:

1) Φυσικές απειλές: Σε αυτήν την κατηγορία δεν είναι πάντα εφικτή η αποφυγή μιας ζημίας, μετά από μια πρόκληση φωτιάς ή ενός εκτατού καιρικού φαινομένου (π.χ. πλημμύρα). Είναι σημαντικό όμως να μπορούμε να διαγνώσουμε έγκαιρα την φυσική απειλή, έτσι ώστε να μπορούμε να αντιδράσουμε γρηγορά και να αποσοβήσουμε την απειλή ή έστω να την περιορίσουμε. Καλό είναι να αποφεύγονται μη επιτρεπτές ενέργειες κατά την χρήση του υλικού (π.χ. κάπνισμα) οι οποίες είναι ικανές να προκαλέσουν από μόνες τους φυσικές απειλές, ενώ καλό είναι πάντα να υπάρχει κι ένα εφεδρικό υλικό, ένα εφεδρικό back-up, για έκτακτες περιπτώσεις.

2) Ακούσιες απειλές: Αυτού του είδους οι καταστροφές μπορεί να προκληθούν από μια απροσεξία ή από μια αστοχία του υλικού, είτε από άγνοια είτε κι από απροσεξία ενός ατόμου. Η μη σωστή εκπαίδευση των ανθρώπων που χρησιμοποιούν τα υλικά, μπορεί να επιφέρει την βλάβη σε ένα υλικό. Συνήθως το ποσοστό των βλαβών από άγνοια και η μη σωστή εκπαίδευση, είναι πολύ μεγαλύτερο από το ποσοστό μιας κακής χρήσης ενός υλικού.

3) Εκούσιες απειλές: Είναι οι απειλές οι οποίες προέρχονται από κακόβουλους χρήστες, οι οποίοι εισβάλουν στα δεδομένα του υλικού και προκαλούν τη δυσλειτουργία του. Αυτές οι απειλές προέρχονται συνήθως από δυσαρεστημένους υπαλλήλους και οι επιτυχία τους εξαρτάται από τον χρόνο που έχουν στην διάθεσή τους καθώς και από τα μέσα που διαθέτουν, για να πραγματοποιήσουν την επίθεσή τους. Πιθανό κέρδος τους μπορεί να είναι η εκδίκηση επειδή είναι δυσαρεστημένοι, καθώς και η πρόκληση κι η δημιουργία δυσάρεστων καταστάσεων στο εργασιακό τους περιβάλλον.

2.7 Γενικά θέματα επιθέσεων υλικού

Οι επιθέσεις στο υλικό είτε στα λειτουργικά συστήματα, όπως έχουμε αναφέρει στην διπλωματική μου, αυξάνονται με ραγδαία ταχύτητα, συνεπώς έχουμε και μια

αύξηση των υλικών και των συσκευών που περικλείονται και χρησιμοποιούνται από τα εκάστοτε συστήματα για να είναι λειτουργικά. Η μεγάλη ανάπτυξη που παρατηρείται στην κατασκευή των υλικών, με την έλλειψη προτύπων ασφαλείας κατά την παραγωγή τους, σε συνάρτηση και με την μεγάλη ζήτηση σε χαμηλό κόστος που υπάρχει στην εποχή μας, μας κάνει να αναμένουμε κι ακόμα μεγαλύτερη αύξηση των επιθέσεων υλικού από κακόβουλους χρήστες. Η αύξηση των κακόβουλων επιθέσεων μας κάνει να ανησυχούμε, γιατί πιθανώς να έχουμε και καταστροφικά αποτελέσματα μέσα από τις αλλοιώσεις των υλικών.

Τα αντίμετρα πρέπει να περιλαμβάνουν όλες εκείνες τις διαδικασίες και τις τεχνικές, που να μπορούν να διαφυλάσσουν τα υλικά και κατ' επέκταση όλο το λειτουργικό σύστημα. Τα μέτρα προστασίας μόνο με τη χρήση ενός λογισμικού, δεν είναι ικανά να προστατεύσουν τα υλικά μέρη, καθώς η πρόσβαση σε πληροφορίες και οι απόκτηση δεδομένων μπορεί να γίνει μέσα από «πόρτες».

Η παραβίαση του υλικού με την μέθοδο της αντίστροφης μηχανικής, οι επιθέσεις μέσω πλευρικού καναλιού καθώς και το ψεύτικο αντίγραφο αποτελούν τις πιο σύνηθες επιθέσεις στο υλικό. Οι επεμβατικές επεμβάσεις απαιτούν γνώση και οικονομικούς πόρους, για να θεωρηθούν επιτυχημένες, με σκοπό την αλλοίωση του υλικού που παραβιάζουν. Οι μη επεμβατικές παρεμβάσεις δεν απαιτούν γνώση, ούτε οικονομικούς πόρους και δεν έχουν στόχο την αλλοίωση του υλικού. Τέλος, οι ημιεπεμβατικές επιθέσεις απαιτούν μερική γνώση και μιας μέσης κατάστασης οικονομικούς πόρους για να επιτευχθούν και να παραβιάσουν μερικώς το υλικό - στόχο.

Άλλες επιθέσεις που μπορούν να προκαλέσουν αλλοιώσεις στο υλικό, μπορούν να προκληθούν από επιθέσεις χρονισμού, αλυσιδωτής σάρωσης καθώς κι επιθέσεις cache. Οι επιτυχία των επιθέσεων αυτών βασίζετε στην ευπάθεια που μπορεί να έχουν τα σχέδια ενός υλικού. Η απειλή και το διακύβευμα από αυτές τις επιθέσεις είναι τεράστια, αφού η παραβίαση μπορεί να επιφέρει απώλεια χρήματων από κλεμμένα αρχεία ή δεδομένα. Η αμυντική θωράκιση από τέτοιες επιθέσεις εξαρτάται από τα στοιχεία που προστατεύουν την ασφάλεια του υλικού [32].

2.8 Είδη επιθέσεων

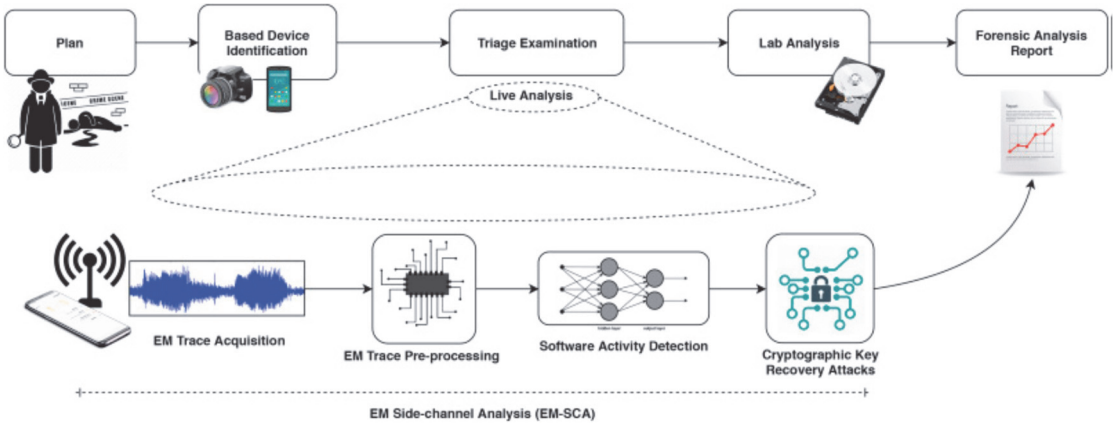
Όταν αναφερόμαστε στην φράση ασφάλεια υλικού, εννοούμε την προστασία εκείνη που διαφυλάσσει την συσκευή και το ίδιο το υλικό από κλοπή - εισβολή - ζημιά. Παρακάτω θα αναφερθούμε σε διάφορες επιθέσεις που μπορούν να γίνουν σε ένα υλικό, σε μια συσκευή.

Α) Ψεύτικο αντίγραφο

Η επίθεση μέσω δημιουργίας ψεύτικου αντιγράφου, έχει στόχο την υποκλοπή των πνευματικών δικαιωμάτων από τον πραγματικό δημιουργό. Ο κακόβουλος χρήστης σε αυτές τις περιπτώσεις χρησιμοποιεί Trojans επηρεάζοντας τις συσκευές.

Β) Επίθεση πλευρικού καναλιού

Είναι μια σύνηθες μορφή επίθεσης που χρησιμοποιούν οι κακόβουλοι χρήστες για να αποκτήσουν πρόσβαση σε πληροφορίες του υλικού. Οι επιτιθέμενοι σε αυτήν τη περίπτωση μέσω των φυσικών λειτουργιών της συσκευής, προσπαθούν να εκμεταλλευτούν την κατανάλωση ενέργειας και διαμέσου του ρεύματος να αποκτήσουν δεδομένα που τους είναι χρήσιμα. Αυτό επιτυγχάνετε με την μέτρηση της ισχύος, των φωτονικών εκπομπών και των ηλεκτρομαγνητικών εκπομπών.



Εικόνα 9 Επίθεση πλευρικού καναλιού [32]

Γ) Παραβίαση πνευματικής ιδιοκτησίας

Η κλοπή των πνευματικών δικαιωμάτων από τον πραγματικό δημιουργό, γίνετε συνήθως κατά τον σχεδιασμό ενός υλικού. Οπού οι κακόβουλοι χρήστες υποκλέπτουν πληροφορίες και σχεδιαστικές πατέντες, κι εν συνεχεία διεκδικούν την ιδιοκτησία τους, κατοχυρώνουν και τα πνευματικά δικαιώματα, τα χρησιμοποιούν σε δικά τους υλικά που δημιουργούν κι όλα αυτά αποτελούν μία πρόκληση για το επίπεδο ασφαλείας.

Αυτή η επίθεση προϋποθέτει την εξειδικευμένη γνώση και τον απαιτούμενο εξοπλισμό από την πλευρά των επιτιθέμενων. Πρόκειται για μια επίθεση που απαιτεί την αναδιαμόρφωση στο Ολοκληρωμένο Κύκλωμα (Integrated Circuit-IC) ή στην Πνευματική Ιδιοκτησία (Internet Protocol-IP) όπου μέσα του να εσωκλείει ένα κακόβουλο κύκλωμα. Ο κακόβουλος χρήστης, σε αυτήν τη περίπτωση, θέλει να αποκτήσει τα δικαιώματα της IC είτε της IP.

Η ενέργεια αυτή περιλαμβάνει αρκετά στάδια. Ενδεικτικά να αναφέρουμε ότι περιλαμβάνει την εξακρίβωση του υλικού που χρησιμοποιείται, την αφαίρεση

κομματιών του σχεδιασμού καθώς κι ενδελεχή παρατήρηση της λειτουργίας του IC ή IP. Εν συνεχεία μέσω της παρατήρησης του κυκλώματος και των εξόδων κι εσοδών όλων των πιθανών συνδυασμών, αξιολογείται η συμπεριφορά του κυκλώματος. Η εισχώρηση κατά τον σχεδιασμό κακόβουλου κυκλώματος μπορεί να αλλοιώσει τα συστήματα και τα υλικά, δίνοντας σημαντικές πληροφορίες και δεδομένα.

Δ) Δούρειοι ίπποι σε επίπεδο υλικού

Οι κακόβουλοι χρήστες σε μια επίθεση υλικού με HTs, προσπαθούν να μεταβάλουν ολόκληρο το σύστημα ή να ενσωματώσουν ένα δικό τους σύστημα στο ήδη υπάρχον κύκλωμα, που να επιφέρει μετατροπές και παραπλάνηση στον έλεγχο καθώς και στην επικοινωνία του υλικού. Με αυτήν τη μέθοδο συλλέγονται κρίσιμες πληροφορίες και δεδομένα, αλλοιώνοντας έτσι την ασφάλεια του υλικού σε επίπεδο εμπιστευτικότητας. Επίσης μπορούν να υποκλέψουν και κρυπτογραφικά κλειδιά λόγω της ζεύξης των υλικών στο internet. Οι δούρειοι ίπποι είναι πολύ δύσκολο να γίνουν αντιληπτοί από τους χρήστες, γιατί εγκαθίστανται είτε χειροκίνητα είτε μεταφρασμένα μέσω κάποιου προγράμματος και είναι αδύνατον να αποτραπεί, όλο αυτό, λόγο της λειτουργικότητάς του.

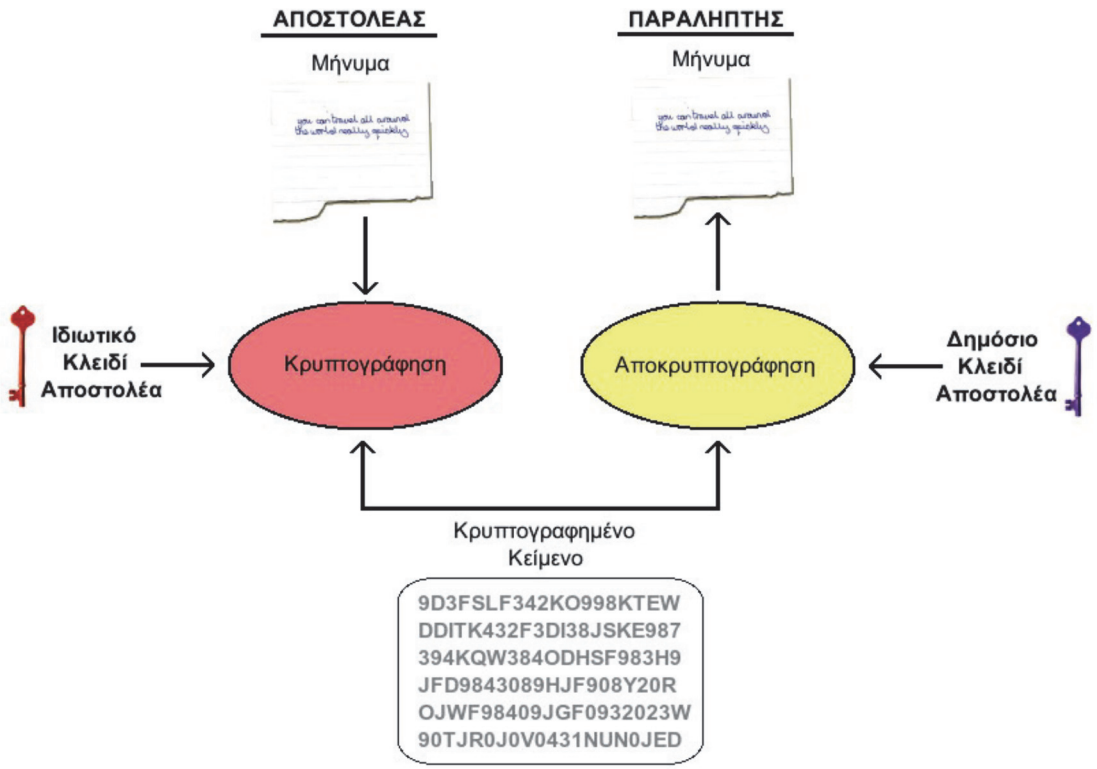
Τα HTs έχουν διαφορετικό βαθμό επιπτώσεων σε ένα ολοκληρωμένο κύκλωμα. Ορισμένα HTs μπορούν να προκαλέσουν την αποδοχή εισόδων που θα έπρεπε να απορριφθούν από τις μονάδες ανίχνευσης σφαλμάτων, ενώ κάποια άλλα μπορούν να υποβαθμίσουν την απόδοση αλλοιώνοντας σκόπιμα τις λειτουργικές παραμέτρους μιας συσκευής. Ορισμένα HTs μπορούν να διαρρεύσουν ευαίσθητα δεδομένα δημιουργώντας μια κερκόπορτα για κακόβουλους χάκερ στο ολοκληρωμένο κύκλωμα.

Επιπροσθέτως κάποια HTs μπορούν επίσης να δημιουργήσουν μια επίθεση άρνησης παροχής υπηρεσιών με tar- geting modules για να εξαντλήσουν τους σπάνιους πόρους όπως το εύρος ζώνης, ο υπολογισμός και η ισχύς της μπαταρίας. Αυτό καθιστά τα HTs υλικού έναν σοβαρό κίνδυνο για την ασφάλεια ενός ολοκληρωμένου κυκλώματος. Επιπλέον, ο αντίκτυπος των HTs επιδεινώνεται όταν τα μολυσμένα ολοκληρωμένα κυκλώματα χρησιμοποιούνται σε κυβερνοφυσικά συστήματα, π.χ. γνωστικά ραδιόφωνα, συστήματα υγείας στο Διαδίκτυο των Πραγμάτων (Internet of Things -IoT), ρομποτική και μη επανδρωμένα αεροσκάφη, καθώς τα HTs μπορούν να διευκολύνουν τις κυβερνο-φυσικές επιθέσεις σε τέτοια συστήματα [37].

Ε) Timing attacks

Ο επιτιθέμενος στις επιθέσεις χρονισμού, επιδιώκει με την βοήθεια της στατιστικής ανάλυσης, την είσοδο του στο υλικό μέσω τυχαίων συσχετισμών. Αυτή η

μέθοδος μπορεί να στεφθεί με επιτυχία μόνο αν το κύκλωμα του υλικού παρουσιάζει την ίδια συμπεριφορά σε κάθε του εκτέλεση. Έτσι, με αυτήν τη μέθοδο ο επιτιθέμενος θέλει να εισβάλει στο υλικό εκμεταλλευόμενος κάποιες μικρές περιστασιακές διαφορές που προκύπτουν στο χρονοδιάγραμμα εμφάνισης των αλγορίθμων, έτσι ώστε να μπορέσουν να παρακολουθήσουν τη λειτουργία της προσωρινής μνήμης του υλικού. Από εκεί μετά θα μπορέσουν να αφ' υπάρξουν δεδομένα που θα αφορούν τα αλγοριθμικά χαρακτηριστικά, που θα τους βοηθήσουν στην ολοκλήρωση της επίθεσης τους.



Εικόνα 10 Ασύμμετρη κρυπτογράφηση [16]

Ο κρυπτό αναλυτής έχει την δυνατότητα να παρακολουθήσει το πώς μεταφέρεται η πληροφορία από και προς την μνήμη, ενώ το υλικό τρέχει τον κρυπτογραφημένο αλγόριθμο. Με αυτόν το τρόπο ο επιτιθέμενος έχει την δυνατότητα να αποκρυπτογραφήσει το κρυφό κλειδί, μέσω της μέτρησης της τιμής του χρόνου που απαιτεί το υλικό μέχρι να τρέξει τις κρυπτογραφικές λειτουργίες του, κι όπου εν συνεχεία και μέσω της σύγκρισης των διαφορών που παρατηρούνται ανάμεσα σε αυτές τις χρονικές μετρήσεις, δίνεται η ευκαιρία στον κακόβουλο χρήστη να βρει τους εκθέτες που χρειάζεται και με παραγοντοποιήσεις των κλειδιών (Rivest-Shamir-Adleman-RSA) να παραβιάσει το κρυπτό σύστημα του υλικού. Αν το υλικό είναι ευάλωτο τότε έχουμε μια απλή επίθεση και απαιτείται μόνο ένα κρυπτογράφημα.

ΣΤ΄) Simple power analysis

Στις (Simple power analysis-SPA) επιθέσεις, ο επιτιθέμενος επιχειρεί ομοίως όπως και στις επιθέσεις χρονισμού, με τη χρήση της στατιστικής ανάλυσης να μπορέσει να βρει τους συσχετισμούς εκείνους μεταξύ των εισόδων κι εξόδων του κυκλώματος του υλικού, που θα του επιτρέψουν την εισβολή σε αυτό. Στόχος του επιτιθέμενου είναι η εμπλοκή του στην ροή των εντολών, όπου εκεί μη αφήνοντας αποδεικτικά στοιχεία από την εισχώρηση του, το θύμα δεν θα μάθει ποτέ ότι έγινε επίθεση στο υλικό του.

Η SPA επίθεση είναι μια μη επεμβατική επίθεση κι ως εκ τούτου δεν χρειάζεται κάποια προετοιμασία για την επίθεση σε κάποιο υλικό. Σε αυτές τις επιθέσεις υπάρχουν μεγάλες αλλαγές στο ρεύμα ή στην ισχύ, που οφείλονται σε έναν αλγόριθμο λόγο της συμπεριφοράς του. Ο κακόβουλος χρήστης μέσα από τον συγκεκριμένο τύπο επίθεσης μπορεί να κλέψει κλειδιά που απαιτούνται κατά την επικοινωνία του υλικού με τα υπόλοιπα μέρη του συστήματος. Αυτός ο τύπος επίθεσης για να είναι αποτελεσματικός, η στατιστική ανάλυση απαιτεί έναν μικρό αριθμό ιχνών αλλά κι έναν μεγάλο αριθμό ακρίβειας.

Ζ) Differential power analysis

Η (Differential power analysis-DPA) επίθεση είναι όμοια με τις επιθέσεις SPA και πλευρικού καναλιού, ανήκει στην κατηγορία των μη επεμβατικών επιθέσεων και η στόχευση αυτής της επίθεσης καθώς και η αποτελεσματικότητά της, είναι άρρηκτα συνδεδεμένη με τα δεδομένα.

Η DPA κατά κύριο λόγο μπορεί να μετρά δυναμική ισχύ, αλλά έχει και την δυνατότητα παράλληλα, όπως και στις επιθέσεις SPA, να παρατηρεί μικρές αλλαγές. Τέλος, και εδώ ο επιτιθέμενος δεν αφήνει πίσω του ίχνη κι έτσι ο κάτοχος του υλικού δεν ξέρει ότι έχει πέσει θύμα παραβίασης. Ο κακόβουλος χρήστης πραγματοποιεί χιλιάδες ίχνη και δημιουργεί ένα εξαρτημένο άθροισμα δεδομένων, με την παραβίαση ενός υλικού, στην συγκεκριμένη περίπτωση, να γίνεται εισχωρώντας τυχαία από την είσοδο του.

Η) Επιθέσεις μηχανικής μάθησης (Machine Learning-ML)

Είναι άλλη μια μη επεμβατική επίθεση, αρκετά συνηθισμένη, που στόχο έχει την παραβίαση του υλικού μέσω της Physical Unclonable Functions-PUF. Εδώ ο επιτιθέμενος παρατηρεί συνεχώς κι ενδελεχώς την είσοδο κι έξοδο της PUF του στοχοποιημένου υλικού, όπου συλλέγοντας πληροφορίες και δεδομένα από ένα σύνολο αποκρίσεων, προσπαθεί να αποκωδικοποιήσει την συμπεριφορά της PUF, με σκοπό να βρει ένα μοντέλο εισόδου στην συσκευή.

Θ) Ανάλυση ηλεκτρομαγνητικής ισχύος (EMA)

Η επίθεση με την μορφή της ανάλυσης της ηλεκτρομαγνητικής ισχύος είναι πανομοιότυπη με τις επιθέσεις DPA και SPA. Μέσω των επιθέσεων που πραγματοποιεί ο επιτιθέμενος, έχει σκοπό να δημιουργήσει πληροφορίες και δεδομένα εξειδικευμένα με στόχο ο κρυπταναλυτής να εξάγει τα κλειδιά [32].

ΚΕΦΑΛΑΙΟ 3: ΣΥΜΒΑΤΙΚΕΣ ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΥΛΙΚΟΥ

3.1 Συμβατικοί περιορισμοί ασφάλειας

Για την ασφάλεια υλικού σημαντικό ρολό παίζει η σχεδίαση του υλικού, η ορθή δοκιμή του υλικού καθώς κι όλα τα στάδια που θα περάσει και θα χρειαστεί μέχρι την τελική του κυκλοφορία. Όσο πιο πιστά γίνονται κι εφαρμόζονται οι έλεγχοι κατά την διάρκεια παραγωγής ενός υλικού τόσο μεγαλύτερη ασφάλεια επιτυγχάνετε. Η μη πρόσβαση στα ακέραια δεδομένα του υλικού, είναι αυτή που καθορίζει την εμπιστευτικότητα του υλικού.

Η διασφάλιση της εμπιστευτικότητας του υλικού είναι βασική αρχή για την ασφάλεια του υλικού και κατ' επέκταση του λειτουργικού συστήματος που θα χρησιμοποιηθεί. Σημαντικό επίσης είναι να αναφέρουμε πως για την εύρυθμη λειτουργία και την αύξηση της ασφάλειας του υλικού ενός συστήματος, παίζει η επικοινωνία μεταξύ του υλικού και του λογισμικού. Η ορθή επικοινωνία των δυο αυτών διευκολύνει την ομαλή λειτουργία, την τήρηση των κανόνων και τον συντονισμό του υλικού.

Τέλος, σημαντικό επίσης είναι να γνωρίζουμε τις πιθανές ευπάθειες ενός υλικού έτσι ώστε να μπορούμε εξαρχής μέσω της ανάλυσης των ευπαθειών του, να μειωθούν οι απειλές απέναντι του. Σίγουρα κατά τα πολλά στάδια παραγωγής ενός υλικού, υπάρχουν αρκετά τρωτά σημεία που ελλοχεύει ο κίνδυνος για κάποια αστοχία ή ευπάθεια στο υλικό. Όπως προανέφερα η μη τυπική μέθοδος ελέγχων, δημιουργεί αρκετές ευπάθειες στο υλικό και που στην συνέχεια οδηγεί σε σφάλματα. Τα σφάλματα αυτά μπορούν να φαίνονται ακόμα και με γυμνό μάτι, μέσω μιας απλής παρατήρησης.

Άλλη μια αιτία που μπορεί να οδηγήσει σε σφάλματα και αστοχία υλικού, είναι ο μη καθορισμός των ρόλων των ατόμων που θα έρθουν σε επαφή με το υλικό κατά την παραγωγή του. Αυτό μπορεί να φέρει σε επαφή με το υλικό ένα μη εξειδικευμένο υπάλληλο, όπου δεν θα πραγματοποιήσει την σωστή εργασία και αυτό να οδηγήσει σε παραγωγή ενός ελλαττωματικού υλικού.

Ένα ακόμα επιπλέον σημαντικό σημείο κατά την παραγωγή ενός υλικού είναι τα μέσα που χρησιμοποιούνται για τα δοκιμαστικά τεστ. Αυτά αν διαρρεύσουν από μέσα προς τα έξω, από τα ίδια τα άτομα που δοκιμάζουν τις τυχόν αστοχίες, θα επιφέρουν τα άκρως αντίθετα αποτελέσματα που αναμένουμε. Η διαρροή θεμάτων και μεθόδων ασφαλείας είναι μια μεγάλη πληγή στην διάδοση ευπαθειών και θεμάτων ασφαλείας [16].

3.2 Κίνδυνοι υλικού

Η ασφάλεια των συσκευών συνεχίζουν να βασίζονται σε λύσεις που δεν μπορούν να αντιμετωπίσουν πλήρως κι αποτελεσματικά τις επιθέσεις, παραμένοντας και καθιστώντας έτσι το κάθε υλικό ευάλωτο απέναντι σε κακόβουλους χρήστες. Τα όποια πρωτόκολλα και συστήματα ασφάλειας υπάρχουν, στηρίζουν την ασφάλεια τους στην προστασία των αρχείων, των δεδομένων και των πληροφοριών κατά την μεταφορά τους στην επικοινωνία.

Η προστασία στηρίζεται σε μαθηματικές προσεγγίσεις, καθώς είναι δύσκολο να επιλυθούν από τους επιτιθέμενους. Η εξαγωγή κλειδιών θα μπορεί να γίνεται σε πιο σύντομο χρονικό διάστημα, μόνο όταν θα γίνουν πραγματικότητα οι κβαντικοί υπολογιστές. Στις περιπτώσεις όπου η προστασία μιας συσκευής βασίζεται σε λύσεις λογισμικού, η συσκευή αυτή καθίσταται άμεσα ευάλωτη κι επιρρεπείς σε μια πιθανή επίθεση, κι αυτό γιατί τα κλειδιά αποθηκεύονται στις μη-πτητικές μνήμες των υλικών.

Συνεπώς, η ασφάλεια που παρέχεται μόνο μέσω λογισμικού σε μια συσκευή, θεωρείται υψηλής επικινδυνότητας και η αποφυγή επιθέσεων καθίσταται δύσκολη έως αδύνατη. Επομένως μια πιο ορθή προσέγγιση και μια πιο σωστή μέθοδος ασφάλειας ενός υλικού, είναι καλυτέρα να βασίζεται σε λύσεις hardware υλικού συνδυαστικά με λύσεις λογισμικού, παρέχοντας την απαιτούμενη προστασία των συσκευών [24].

Τα HT έχουν σχεδιαστεί για να είναι αθόρυβα, δηλαδή να μην μπορούν να εντοπιστούν εύκολα, και ενδέχεται να μην ενεργοποιούνται μέχρι να πληρούνται ορισμένοι παράγοντες χρόνου, ρεύματος, θερμοκρασίας, τάσης ή λογικής. Επομένως, μόλις τα κατασκευασμένα ολοκληρωμένα κυκλώματα επιστρέψουν στον σχεδιαστή, ο έλεγχος αυτών των κυκλωμάτων για πιθανούς κινδύνους ασφαλείας είναι πρωταρχικής σημασίας. Υπάρχουν πολλαπλές στρατηγικές που μπορούν να χρησιμοποιηθούν για τον έλεγχο της επικράτησης των trojans υλικού σε ένα ολοκληρωμένο κύκλωμα.

Μπορούμε να αναφερθούμε σε δύο τύπους τεχνικών ανίχνευσης trojan, τις καταστροφικές και μη καταστροφικές. Στις καταστροφικές τεχνικές, τα ολοκληρωμένα κυκλώματα απομεταλλώνονται για να ελεγχθούν τα εσωτερικά κυκλώματα, πράγμα που είναι ακριβό και χρονοβόρο. Από την άλλη πλευρά, οι μη καταστροφικές τεχνικές περιλαμβάνουν ανάλυση πλευρικών καναλιών και λογικό έλεγχο. Ωστόσο, οι μέθοδοι βασίζονται σε μεγάλο βαθμό στη διαθεσιμότητα επαρκών πόρων για δοκιμές και ενδέχεται να παρεμποδίζονται από την έλλειψη πόρων για αποτελεσματικές δοκιμές. Αυτό εγείρει την ανάγκη για αποτελεσματικές στρατηγικές δοκιμών που μπορούν να ανιχνεύσουν τα περισσότερα trojans με περιορισμένους πόρους.

Προκειμένου να καταπολεμηθούν τα ζητήματα που σχετίζονται με την έλλειψη πόρων δοκιμών, μια πολλά υποσχόμενη προσέγγιση που διερευνάται πρόσφατα είναι η μελέτη των στρατηγικών αλληλεπιδράσεων που μπορεί να λαμβάνουν χώρα μεταξύ ενός κατασκευαστή ολοκληρωμένου κυκλώματος και ενός σχεδιαστή (δοκιμαστή). Αυτό μπορεί να βοηθήσει τον ελεγκτή να χρησιμοποιήσει αποτελεσματικά τους πόρους του για τον εντοπισμό των περισσότερων trojans.

Μια αποτελεσματική μέθοδος για την προσεκτική μελέτη των αλληλεπιδράσεων μεταξύ των παραγόντων, σε μια δεδομένη κατάσταση, είναι η χρήση της θεωρίας παιγνίων. Η θεωρία παιγνίων παρέχει ένα ισχυρό μαθηματικό εργαλείο για τη μελέτη τέτοιων αλληλεπιδράσεων και επιτρέπει σε κάθε παίχτη να επιτύχει το καλύτερο δυνατό αποτέλεσμα υπό το πρίσμα των ενεργειών των αντιπάλων του. [37]

3.3 Προστασία μέσω Hardware Security Modules (HSM)

Η μέθοδος προστασίας (Hardware Security Modules-HSM), που παρέχεται μέσα από λύσεις του hardware υλικού άπτεται αποκλειστικά στην χρήση ολοκληρωμένων κυκλωμάτων, για την αποθήκευση κρυπτογραφικών κλειδιών. Αυτές οι μονάδες ασφαλείας έχουν την δυνατότητα να παρέχουν καλύτερη προστασία έναντι σε κάθε κακόβουλη ενέργεια, μέσω της ικανότητας τους να αποκλείουν την πρόσβαση σε αρχεία και δεδομένα με σκοπό την εγγραφή τους ή την ανάγνωσή τους.

Η ασφάλεια των υλικών που εξαρτάται από τις μονάδες ασφαλείας HSM, έχουν περάσει κι έχουν δοκιμαστεί μια επεξεργασία κρυπτογράφησης, όπου μέσα από διαδικασίες διαχείρισης τα κλειδιά μπορούν να αποθηκευτούν, να αποκρυπτογραφηθούν ή και να κρυπτογραφηθούν. Επίσης, ο συγκεκριμένος τύπος ασφαλείας έχει δοκιμαστεί και χρησιμοποιηθεί μαζί με μηχανισμούς προστασίας μέσω λογισμικού, όπως Προηγμένο πρότυπο κρυπτογράφησης (Advanced Encryption Standard-AES και Υποδομή Δημόσιου Κλειδιού (Public key infrastructure-PKI).

Ένα σημαντικό μειονέκτημα των λύσεων προστασίας μιας συσκευής που στηρίζεται στο hardware υλικό, είναι πως εμφανίζεται πολύ ευάλωτη σε επιθέσεις τύπου Man-In-The-Middle, όπου οι κακόβουλοι χρήστες έχουν την δυνατότητα να κλωνοποιήσουν το υλικό μέσω της πρόσβασης που αποκτούν στην μονάδα HSM. Μια λύση σε αυτό το πρόβλημα προσφέρεται μέσα από την χρησιμοποίηση PUFs [24].

3.4 Προστασία μέσω Physical Unclonable Functions (PUFs)

Σημαντικό μέτρο προστασίας αποτελούν οι PUF όπου μπορούν να αντιμετωπίζουν τους κινδύνους από κακόβουλες επιθέσεις, γιατί έχουν την δυνατότητα να παρέχουν ασφαλή αναγνώριση των αντικειμένων. Η χρησιμοποίηση των φυσικών

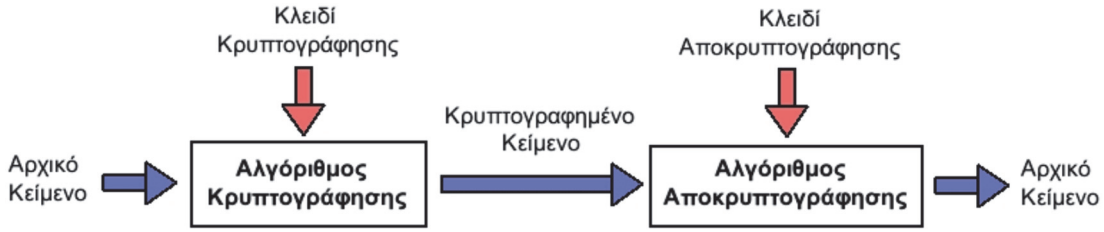
μη κλωνοποιήσιμων συναρτήσεων ήρθαν στο προσκήνιο ως ένα πρόσθετο μέτρο ασφάλειας που υποστηρίζει το hardware υλικό.

$$(Μοναδικότητα) = \frac{1}{\binom{l}{2}} \sum_{l=1}^{l-1} \sum_{j=i+1}^{l} HD(R_i, R_j) * 100\%.$$

$$(Αξιοπιστία) = 100 - \frac{1}{n * (l-1)} \sum_{i=0}^{n} \sum_{n=1}^{n} HD(R_{i,k}, R_{j,k}).$$

Κατά την φάση της κατασκευής ενός υλικού χρησιμοποιούνται πανομοιότυπα υλικά με τα πρωτότυπα, με σκοπό την δημιουργία ενός αποτυπώματος hardware υλικού της συσκευής. Πράγμα το οποίο μας δίνει το πολυπόθητο πλεονέκτημα, μέσα από τις συναρτήσεις PUF, στο να μην μπορούν να κλωνοποιηθούν οι ιδιότητες της συσκευής από κακόβουλους εισβολείς κι επιτιθέμενους.

Οι συναρτήσεις PUF χρησιμοποιούνται σε πολύ μεγάλο βαθμό για την ασφάλεια των υλικών, όπου και την συναντάμε πολύ συχνά στην βιβλιογραφία, ως μια λύση πολύ αποδοτική στην αποφυγή και στην αντιμετώπιση των κακόβουλων επιθέσεων σε συσκευές. Χρησιμοποιείται πολύ συχνά ως πρότυπο ασφάλειας στις συσκευές και ελέγχει την ταυτότητα και την αυθεντικοποίηση τους. Επίσης, είναι μια λύση προστασίας οικονομική ως προς το κόστος της δημιουργίας κρυπτογραφικών κλειδιών από το υλικό.



Εικόνα 11 Βασικές έννοιες κρυπτογραφίας [16]

Μέσα από το πέρασμα των ετών η χρήση των συναρτήσεων PUF άρχισε να χρησιμοποιείται περισσότερο κι εμφανίστηκε στο προσκήνιο και η χρήση ψηφιακών φυσικών μη κλωνοποιημένων συναρτήσεων, με στόχο την βέλτιστη απόδοση και σχεδίαση συσκευών (Computer-aided design CAD). Αυτό προκλήθηκε από την αναγκαιότητα διότι ήταν πολύ δύσκολο οι ψηφιακές PUF να συμπεριλαμβάνουν και τις αναλογικές, και μέσα λοιπόν από αυτήν την εξέλιξη οδηγηθήκαμε στην μόνιμη χρήση των ψηφιακών συναρτήσεων της PUF.

Μέσα από την εξέλιξη της τεχνολογίας στο πέρασμα των χρόνων και την πρόοδο των μεθόδων ασφαλείας που στηρίζονται στο hardware υλικό, θα υπάρξει και

μια βελτίωση της σχεδίασης CAD, με συνέπεια την βελτιστοποίηση της απόδοσης στην ασφάλεια των υλικών, από κακόβουλες επιθέσεις πλευρικών καναλιών ή φυσικών επιθέσεων. Μέσα από το ίδιο πνεύμα της περαιτέρω εξέλιξης της ασφάλειας υλικών, μπορούμε να αναφέρουμε ότι οι PUF μέσω των συναρτήσεων τους, του ελέγχου ταυτότητας και χωρίς την απαίτηση αποθήκευσης κρυφών κλειδιών, κι αξιοποιώντας ιδανικά τα πρότυπα και πρωτότυπα χαρακτηριστικά τους, αύξησαν την ασφάλεια των υλικών στο μέγιστο βαθμό.

Ο έλεγχος ταυτότητας μπορεί να γίνεται μέσα από τέσσερα βήματα, όπου το καθ' ένα βήμα αποτελείται από τρία μηνύματα. Αναλύοντας λίγο περισσότερο αυτά τα βήματα θα δούμε ότι στο πρώτο βήμα η εκάστοτε συσκευή αρχίζει τον έλεγχο ταυτότητας αποστέλλοντας το αναγνωριστικό της για επαλήθευση. Η επαλήθευση πραγματοποιείται από τον διακομιστή μέσω ενός αναγνωριστικού μηνύματος και με την βοήθεια ενός Κωδικού Αυθεντικοποίησης Μηνύματος (Message Authentication Code-MAC). Για να είναι ο έλεγχος επιτυχής θα πρέπει το μήνυμα 3 από το MAC να επαληθευθεί από τον διακομιστή και μόνο τότε ο έλεγχος ταυτοποίησης είναι έγκυρος.

Στην περίπτωση όμως που η επαλήθευση του MAC δεν στεφθεί με επιτυχία σε κανένα βήμα, έχουμε απόρριψη του ελέγχου ταυτότητας. Αυτή η μέθοδος προσδίδει μεγάλη ασφάλεια κι αποτρέπει αρκετούς τύπους επιθέσεων έναντι των συσκευών που προστατεύονται από το συγκεκριμένο πρωτόκολλο. Ενδεικτικά αναφέρουμε κάποιες από αυτές τις επιθέσεις που αποτρέπονται, όπως η πλαστοπροσωπία, η υποκλοπή κι η κλωνοποίηση [24].

3.5 Προστασία μέσω νανοηλεκτρικού υλικού

Μια επόμενη λύση στην ασφάλεια των υλικών είναι η προστασία μέσω του νανοηλεκτρικού hardware υλικού. Εδώ σε μια τέτοια περίπτωση η παρεχόμενη ασφάλεια δημιουργείται μέσω των metal oxide memristors, εφαρμόζοντας πρότυπα πρωτοκόλλα ασφαλείας στο υλικό, όπου τα πρότυπα ασφάλειας νανοκλίμακας, παρέχουν υψηλή προστασία, αλλά συνάμα έχουν και μικρή κατανάλωση ενέργειας.

3.6 Προστασία μέσω XbarPUF

Άλλη λύση που θα μπορούσε να χρησιμοποιηθεί είναι το XbarPUF (memristive Crossbar PUF), όπου η αποδοτικότητά του κυμαίνεται στα ίδια επίπεδα με το WTMPUF (Write-Time Memristive PUF), βασίζεται στην τεχνολογία complementary metal-oxide semiconductor-CMOS και τα πλεονεκτήματά του είναι ότι δεν επηρεάζεται από την ελαχιστοποίηση του αριθμού των τρανζίστορ και δεν εξαρτάται ούτε επηρεάζεται επίσης, από τον ακριβή χρόνο εγγραφής. Τέλος, το XbarPUF

καταναλώνει πολύ μικρότερη ισχύ, απ' ότι καταναλώνουν ποσότητα ισχύος τα WTMPUF και APUF.

3.7 Τυπικές λύσεις

Συνεχίζοντας τις αναφορές μας ως προς τις τυπικές λύσεις προστασίας που διαφυλάσσουν την ασφάλεια του υλικού, οι συσκευές που χρειάζονται πολύ χαμηλή ισχύ για να λειτουργήσουν, χρήζουν βελτιώσεις και υποστήριξη ώστε να μπορούν να αντισταθμίσουν την χαμηλή ισχύ, με το κόστος και την ασφάλειά τους. Σε συγκρίσεις που έχουν γίνει και που αφορούν τον έλεγχο της ταυτότητας ενός υλικού, μεταξύ εκείνων που βασίζονται στην κρυπτογραφία και μεταξύ εκείνων που βασίζονται στις συναρτήσεις PUF, βρέθηκε να χρειάζεται να υποστηριχθούν περισσότερο τα μπλοκ hardware υλικού. Αυτή η ανάγκη υποστήριξης είναι που θα δώσει καλύτερο έλεγχο ταυτότητας και ασφάλειας των υλικών.

Συνεχώς όμως οι απαιτήσεις και τα ζητήματα θα αυξάνονται και θα απαιτούνται συνεχώς νέες κατευθύνσεις στα θέματα ασφάλειας των υλικών. Θα πρέπει να υπάρχει και να γίνει ένας καθορισμός πρωτοκόλλων που θα άπτονται των θεμάτων ασφαλείας και θα χρησιμοποιούνται ανά περίπτωση στις συσκευές. Τα προβλήματα όσον αφορά την προστασία των υλικών πάντα θα υπάρχουν, όμως μέσα από μηχανισμούς που σχετίζονται με την προστασία και την ασφάλεια μέσω των κρυπτογραφικών αλγορίθμων, έχουν δώσει λύσεις ως προς την αποτροπή της πρόσβασης και του ελέγχου των κλειδιών, από κακόβουλους χρήστες [24].

3.8 Ευπάθειες ασφάλειας υλικών

Πρώτο μας μέλημα λοιπόν, είναι να ανακαλύψουμε πιθανά κενά ασφαλείας στο υλικό κατά την φάση της κατασκευής του κι εν συνεχεία να προσαρμόσουμε την συμπεριφορά μας στους θεσμοθετημένους κανόνες για να μπορέσουμε να καταστρώσουμε την στρατηγική της άμυνας μας στο παίγνιο. Εφόσον δημιουργήσουμε ένα πρότυπο μοντέλο, μετέπειτα μπορούμε να δούμε ποιοι άνθρωποι είναι ικανοί να προσαρμοστούν στο μοντέλο μας.

Σε αυτόν το τρόπο σκέψης έχει βασιστεί και η ισορροπία Nash. Στην οποία σ' ένα παιχνίδι μη συνεργάσιμου τύπου, ο κάθε παίχτης δρα ως προς το δικό του συμφέρον και σκοπός του είναι να μεγιστοποιήσει τα δικά του οφέλη. Αν για παράδειγμα, σε ένα τέτοιο παίγνιο καταφέρουμε να προβλέψουμε τις αποφάσεις και τις στρατηγικές των παιχτών, τότε η πρόβλεψη αυτή θεωρείται ισορροπία Nash [21].

Η ισορροπία κατά Nash αφορά την ισορροπία παιγνίων που είναι μη μηδενικού αθροίσματος (δηλαδή στα παίγνια που δεν ισχύει ότι το κέρδος του ενός παίκτη είναι

απαραίτητα ζημιά του άλλου όπως στα παίγνια μηδενικού αθροίσματος). Επίσης ονομάστηκε έτσι χάρη στο όνομα του μαθηματικού John Nash που βρήκε την ισορροπία των συγκεκριμένων παιγνίων.

3.9 Θεωρία παίγνιων και η σύνδεσή της με την ασφάλεια υλικού

Τα υλικά μέρη ενός λειτουργικού συστήματος που συμμετέχουν μαζί και με τα λογισμικά μέρη στην εύρυθμη λειτουργία του ενός οποιουδήποτε συστήματος, η ασφάλεια του κάθε υλικού μπορεί μέσα από την επιστήμη της θεωρία των παίγνιων να προστατευτεί. Η θεωρία των παίγνιων διασφαλίζει το υλικό μέρος ενός συστήματος από κάθε φυσικό ή μη φυσικό κίνδυνο καθώς και πιστοποιεί την ασφάλεια και την συμβατότητα των συσκευών.

Σιγουρά η πιστοποίηση του κάθε υλικού αποτελεί κι ευθύνη του εκάστοτε κατασκευαστή, όμως και ο τελικός χρήστης είναι εκείνος που έχει την τελική ευθύνη και πρέπει να δείχνει το ενδιαφέρον του για την ασφάλεια των υλικών του. Καλό είναι να ιεραρχούνται οι ρόλοι στην ασφάλεια του υλικού κι η θεωρία των παίγνιων έχει σημαίνοντα ρόλο σε αυτό, παρέχοντας σημαντική ασφάλεια σε επίπεδο συσκευών. Οι τελικοί χρήστες, όπως προαναφέραμε παραπάνω, προστατεύονται και δεν αφήνουν το υλικό τους εκτιθείτε σε πιθανούς κινδύνους, έχοντας πάντα τον έλεγχο πρόσβασης στην συσκευή τους και στους κωδικούς πρόσβασης με διάφορες δυνατότητες όπως η κρυπτογράφηση, η εναλλαγή κι απόκρυψη των κωδικών.

3.10 Η θεωρία των παίγνιων ως αντίμετρο στις επιθέσεις

Όταν υπάρχουν δύο ή περισσότερες ορθολογικές οντότητες που αντιμετωπίζουν αλληλεξαρτώμενες επιλογές, μπορούμε να χρησιμοποιήσουμε τη θεωρία παιγνίων για να μοντελοποιήσουμε τη συμπεριφορά τους και να κατανοήσουμε καλύτερα το συνολικό σημείο λειτουργίας του συστήματος. Η κύρια συνεισφορά της διπλωματικής, είναι να προτείνει τη χρήση της θεωρίας παιγνίων για τις αλληλεπιδράσεις μεταξύ ευφυών επιτιθέμενων και αμυνόμενων. Η εργασία διαπραγματεύεται την πρώτη εφαρμογή μιας θεωρητικής προσέγγισης παιγνίων στον τομέα της ανίχνευσης Trojan υλικού. Η θεωρία των παίγνιων βοηθά στον εντοπισμό των βέλτιστων συνόλων δοκιμών που αυξάνουν την πιθανότητα αποκάλυψης Trojans υλικού. Επιτρέπει επίσης την εύρεση των βέλτιστων συνθηκών δοκιμής που μπορούν να χρησιμοποιηθούν για να αναγκάσουν έναν επιτιθέμενο να μην εισάγει κανένα Trojan, ώστε να αποφευχθούν σοβαρές κυρώσεις [38].

Με τη χρήση της θεωρίας των παιγνίων, προτείνονται λύσεις σε στρατηγικές καταστάσεις ασφάλειας στον κυβερνοχώρο, στις οποίες η επιτυχία ενός ατόμου να

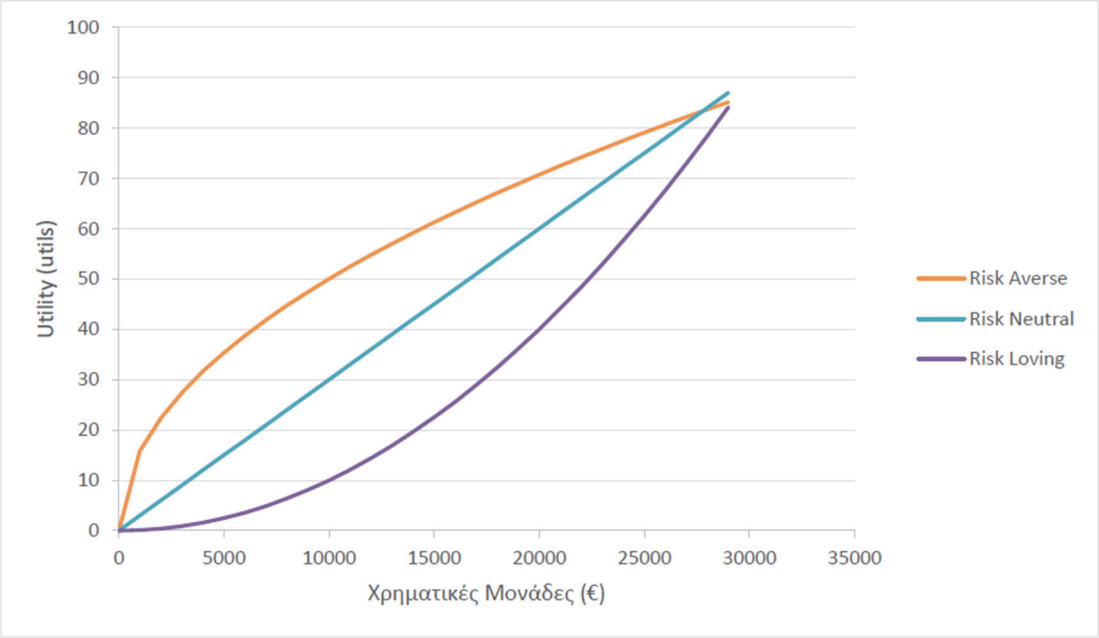
διασφαλίσει το περιουσιακό του στοιχείο εξαρτάται από την εμπιστοσύνη των άλλων να διασφαλίσουν επίσης το περιουσιακό τους στοιχείο. Σε ορισμένα σενάρια, το παίγνιο ασφάλειας είναι στατικό, αλλά σε άλλα, το μοντέλο του παιγνίου είναι επαναλαμβανόμενο ή γενικότερα στοχαστικό. Ένα στοχαστικό παίγνιο είναι μια γενίκευση ενός επαναλαμβανόμενου παίγνιου. Σε ένα επαναλαμβανόμενο παίγνιο, οι παίκτες παίζουν το ίδιο παίγνιο σε όλες τις περιόδους, ενώ σε ένα στοχαστικό παίγνιο, το παίγνιο μπορεί να αλλάξει τυχαία από τη μια περίοδο στην άλλη.

ΚΕΦΑΛΑΙΟ 4: ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ

4.1 Γενικές αρχές της θεωρίας των παίγνιων

Η γνώση για την ασφάλεια του υλικού στηρίζετε είτε μεμονωμένα, είτε συνδυαστικά σε γνωστικά αντικείμενα όπως η πληροφορική, η κρυπτογραφία κ.α. Απαραίτητη κρίνετε η γνώση προγραμματισμού για την αποφυγή των hackers, crackers κ.λπ., οι οποίοι εκμεταλλεύονται διάφορες ευπάθειες των υλικών για την πρόσβαση τους στο υλικό, με στόχο την διαχείριση του υλικού. Η θεωρία των παίγνιων χρησιμοποιώντας πληροφορίες θεωρίας, μαθηματικά μοντέλα και αριθμούς στοχεύει στην προστασία των υλικών μέσω της εμπιστευτικότητας και της ακεραιότητας. Στην διπλωματική μου εργασία θα ασχοληθούμε εκτενέστερα με την θεωρία των παίγνιων ως ένα μικρό παρακλάδι της ασφάλειας υλικού των λειτουργικών συστημάτων.

Στην θεωρία των παίγνιων εμπλέκονται τουλάχιστον δυο ή περισσότερα αντιμαχόμενα στρατόπεδα, όπου ο καθένας από την πλευρά του (χρήστης και επιτιθέμενος) προσπαθεί να επιβληθεί στον άλλον, μέσω στρατηγικών αποφάσεων ή διαφόρων στρατηγικών κινήσεων, προς όφελος του. Ο καθένας προσπαθεί μέσω επιρροών για τα συμφέροντά του να καθορίζει με τις επιλογές του τις αποφάσεις. Συνεπώς, με την θεωρία των παίγνιων δημιουργείτε μια κατάσταση ανταγωνισμού και αντιπαλότητας μεταξύ των υποομάδων που απαρτίζουν τα αντίπαλα στρατόπεδα.



Εικόνα 12 Συναρτήσεις ωφέλειας διαφόρων παιχτών [31]

4.2 Ιστορικές αναφορές

Αναφέροντας κάποια ιστορικά δεδομένα για την θεωρία των παίγνιων, η οποία αποδίδετε στον John von Neumann που αρχικώς ασχολήθηκε με την συγκεκριμένη

θεωρία. Μετέπειτα αναπτύχθηκε από τον George B. Dantzig η θεωρία Simplex που έδωσε πολύτιμη βοήθεια στο να επιλυθούν αρκετές δυσλειτουργίες μέσω του γραμμικού προγραμματισμού.

Εικόνα 13 John von Neumann

Εικόνα 14 John Nash

Ακόμα περισσότερο εξελίχθηκε η θεωρία των παίγνιων από τον Nash, έναν Αμερικανό μαθηματικό κι οποίος πήγε ένα βήμα παραπέρα, ως προς την εξέλιξη της θεωρίας, το αντικείμενο των παίγνιων μέσω του γραμμικού προγραμματισμού και γι' αυτό άλλωστε τιμήθηκε και με το βραβείο Nobel οικονομίας. Μια ξεχωριστή περίπτωση για την εξέλιξη της θεωρίας των παίγνιων αποτέλεσε στο πέρασμα των χρόνων κι ο Shapley, με πολύτιμη συνεισφορά. Τέλος, ο Lemke έκανε το τεράστιο βήμα στην ανάπτυξη της θεωρίας των παίγνιων μέσω της ανακάλυψης του αλγορίθμου, όπου και χρησιμοποιήθηκε για την επίλυση των παίγνιων.

Η θεωρία των παίγνιων μπορεί να μας προδικάζει από μονή της ως ορολογία, για κάποιο παιχνίδι και δη επιτραπέζιο. Μοιάζει σαν ένα παιχνίδι σκάκι που σε μια παρτίδα μπορεί να παίρνονται σοβαρές αποφάσεις σε κάθε κίνηση, έτσι και στην θεωρία των παίγνιων λαμβάνοντες αποφάσεις που μπορούν να επηρεάσουν οικονομικά, πολιτικά και στρατιωτικά ζητήματα. Οι αποφάσεις αυτές συνήθως λαμβάνονται από έναν ή περισσότερους παίχτες που αποφασίζουν εκείνη τη δεδομένη χρονική στιγμή προς όφελος τους.

Εμβαθύνοντας λίγο περισσότερο, ο κάθε παίχτης αποτελεί κι έναν αντίπαλο σε κάθε παίγνιο. Ο κάθε παίχτης καταστρώνει την στρατηγική του, σε πραγματικό χρόνο, μέσα από τα διαφορά όπλα/επιλογές που διαθέτει. Τα κέρδη ή οι απώλειες του κάθε παίχτη, είναι αυτές που διαμορφώνουν τα αποτελέσματα και καθορίζουν και τις περαιτέρω αποφάσεις ή τις επόμενες επιλογές και των άλλων παιχτών.

4.3 Κανόνες της θεωρίας των παίγνιων

Κάθε παίγνιο διέπετε από κανόνες που είναι ξεκάθαροι εξ αρχής και τους γνωρίζουν όλοι οι παίχτες άπαντες. Έτσι, ο κάθε παίχτης ξέρει τι μπορεί και τι επιτρέπετε να κάνει βάσει κανόνων. Αυτοί οι κανόνες είναι που καθορίζουν τα κέρδη ή τις απώλειες, αναλόγως πάντα με τις κινήσεις του εκάστου παίχτη και τις επιλογές που έκανε. Ο παίχτης σε κάθε σημείο του παίγνιου απαιτείτε να κάνει μια κίνηση κάθε φορά, κι ανάλογα τις διαθέσιμες κινήσεις που έχει στην διάθεση του, σε συνάρτηση πάντα και με τις κινήσεις του αντιπάλου του. Ο κάθε παίχτης σε κάθε παίγνιο μπορεί να καταστρώνει μια στρατηγική παιξίματος και μέσα από τις αποφάσεις που λαμβάνει να ξετυλίγει το σενάριο της στρατηγικής του που ακολουθεί.

4.4 Ταξινόμηση των παίγνιων με βάση τα κριτήρια και τους κανόνες

Αναλόγως με τα κριτήρια που υπάρχουν σε ένα παίγνιο, μπορούμε να ταξινομήσουμε τα παίγνια σε διάφορες κατηγορίες. Πρωτίστως ένα κριτήριο που μας δίνει την δυνατότητα να ταξινομήσουμε ένα παίγνιο είναι ο αριθμός των παιχτών. Αν υπάρχουν δυο παίχτες τα παίγνια λέγονται «παίγνια δυο παιχτών», ενώ αν υπάρχουν περισσότεροι παίχτες, μπορούμε να πούμε πως έχουμε τα «παίγνια παιχτών». Είναι ευκόλως κατανοητό πως για να υπάρξει παίγνιο, πρέπει να έχουμε την παρουσία τουλάχιστον δυο παιχτών.

Πίνακας 2 Μηδενικό παιχνίδι

Στρατηγική σειρών	Στρατηγική στηλών			
	Στήλη 1	στήλη 2	…	στήλη n
Σειρά 1	a11	a12	…	a1n
Σειρά 2	a21	a22	…	a2n
:	:	:	…	:
Σειρά m	am1	am2	…	amn

Η παρουσία πιο πολλών παιχτών δίνει την δυνατότητα στους παίχτες για περισσότερες συνεργασίες, συνασπισμούς και μεγαλύτερη ανταγωνιστικότητα. Κάποιοι παίχτες μπορούν να ενώσουν τις δυνάμεις τους, να δημιουργήσουν τους λεγόμενους συνασπισμούς δυνάμεων, προς όφελος τους. Έτσι, μπορούμε να ταξινομήσουμε και τα παίγνια σε «παίγνια συνεργασίας» και σε «παίγνια μη συνεργασίας».

Ακόμα τα παίγνια αναλόγως με ποια σειρά παίρνονται οι αποφάσεις, μπορούμε να τα ταξινομήσουμε σε «δυναμικά παίγνια» και σε «στατικά παίγνια». Στα μεν δυναμικά παίγνια παίζει σημαντικό ρόλο με ποια σειρά παίρνονται οι αποφάσεις, ενώ

στα δε στατικά παίγνια δεν παίζει κανένα ρόλο με ποια σειρά παίρνονται οι αποφάσεις από τους παίχτες.

Ο αριθμός των στρατηγικών που ακολουθεί ο κάθε παίχτης, είναι αυτός που μπορεί να μας δώσει την δυνατότητα για μια ακόμη κατηγορία και να ταξινομούν τα παίγνια σε «πεπερασμένα», σε «μη πεπερασμένα» ή σε «απειροπαίγνια». Τα κέρδη ή οι απώλειες των παιχτών με πεπερασμένο αριθμό κινήσεων και στρατηγικών, μπορούν να καταγράφονται σε πίνακες, κι αυτά τα παίγνια μπορούν να ονομάζονται και «πινακοπαίγνια».

Μια άλλη ταξινόμηση των παίγνιων μπορεί να υπάρξει από τα χαρακτηριστικά των κερδών και των απωλειών των παιχτών. Στα παίγνια που συμμετέχουν δυο παίχτες όπου ο ένας παίχτης κερδίζει την απώλεια του άλλου παίχτη, οι συνεργασίες σε αυτό το παίγνιο είναι ανέφικτες και το παίγνιο σε αυτή την περίπτωση ονομάζεται «παίγνιο μηδενικού αθροίσματος», γιατί το άθροισμα των κερδών είναι μηδέν. Σε αυτήν την περίπτωση έχουμε το εξής οξύμωρο, ότι μπορεί να έχουμε και συνεργασία μεταξύ των παιχτών, αλλά και φαινόμενα ανταγωνισμού. Όταν οι παίχτες βρίσκονται στην φάση του ανταγωνισμού τα κέρδη του ενός, είναι απώλειες για τον άλλον. Ενώ στα παίγνια σταθερής διαφοράς, η συνεργασία είναι αυτή που θα οδηγήσει τους παίχτες στο κέρδος είτε στην απώλεια.

Τελευταία κατηγορία που μπορούμε να ταξινομήσουμε τα παίγνια είναι οι στρατηγικές που αποφασίζουν να ακολουθούν οι παίχτες κατά την διάρκεια του παίγνιου. Αν ο παίχτης διαλέγει μια ξεκάθαρη στρατηγική να ακολουθήσει, λέμε ότι παίζει με «ξεκάθαρη στρατηγική», ενώ όταν ακολουθεί πολλαπλές στρατηγικές λέμε ότι παίζει με «μικτή στρατηγική».

4.5 Ανάλυση των παίγνιων

Περισσότεροι από ένας τρόποι υπάρχουν για να αναλύσουμε και να περιγράψουμε τα παίγνια. Τα παίγνια όταν αναφέρετε ότι βρίσκονται σε μια εκτεταμένη μορφή, οι κανόνες που τα καθορίζουν αναλύονται με την μορφή ενός δέντρου και μέσω των διακλαδώσεών του δημιουργείτε το επονομαζόμενο δένδρο του παίγνιου. Στο δένδρο του παίγνιου οι εκάστοτε κινήσεις των παιχτών ονομάζονται ως κλάδοι και ο κάθε παίχτης κάνοντας μια κίνηση όταν έρθει η σειρά του, αυτό δηλώνετε ως κόμβος. Επίσης, είναι από την αρχή ξεκάθαρο το ποιες θα είναι οι αμοιβές ή οι ζημίες των παιχτών τελειώνοντας το παιχνίδι, όπως κι οι πληροφορίες κι οι επιλογές που έχουν στην διάθεσή τους οι παίχτες. Όλα αυτά είναι ξεκάθαρα από την αρχή και οι παίχτες γνωρίζουν τους κανόνες που διέπουν το παίγνιο.

Το παίγνιο χαρακτηρίζετε τέλειας πληροφόρησης, όταν όλοι οι παίχτες γνωρίζουν τις κινήσεις των άλλων παιχτών, ακόμα κι αν αυτές γίνονται τυχαία, επειδή αυτές οι κινήσεις δεν γίνονται ταυτόχρονα από όλους τους παίχτες κι ο κάθε παίχτης γνωρίζει ακριβώς ποια κίνηση έκαναν οι προηγούμενοι παίχτες από αυτόν. Ως παράδειγμα αξίζει να αναφέρουμε πως ένα παιγνίδι τέλειας πληροφόρησης είναι το σκάκι, με το πόκερ εν αντίθεση που δεν είναι γιατί οι αντίπαλοι παίχτες δεν γνωρίζουν επακριβώς τις κινήσεις του κάθε παίχτη που συμμετέχει. Η τέλεια πληροφόρηση στην εκτεταμένη της μορφή είναι πολύ βοηθητική και χρησιμοποιείτε σε υπολογιστές για την δημιουργία των παιχνιδιών όπως το σκάκι κ.α.

Ένας άλλος τρόπος χαρακτηρισμού των παίγνιων, εξαρτάται κι απαιτεί την γνώση όλων εκείνων των επιλογών και των δυνατοτήτων του κάθε παίχτη κι αυτό καθίσταται δυνατόν μόνο μέσω της ακριβής δήλωσης των κερδών και των ζημίων από τους παίχτες, όπου τα αποτελέσματα εξαρτώνται άμεσα από όλες τις πιθανές και συνδυαστικές επιλογές στρατηγικών που κάνουν οι παίχτες. Τα παίγνια αυτά των παιχτών, αν πούμε ότι είναι πεπερασμένα, ονομάζονται διπινακοπαίγνια κι αναπαρίστανται με την χρήση δυο πινάκων. Μέσω τον πινάκων αναπαρίστανται τα κέρδη ή οι ζημιές των παιχτών ανά ζεύγος στρατηγικών, όπου οι κινήσεις και οι στρατηγικές του κάθε παίχτη καταγράφονται. Η καταγραφή αυτή διεκπεραιώνεται με το να σημειώνονται οι κινήσεις/στρατηγικές του ενός παίχτη στις στήλες του πίνακα και οι κινήσεις/στρατηγικές του άλλου παίχτη στις γραμμές του πίνακα.

Δεν είναι πανάκια να αναφέρουμε πως ένα παίγνιο πάντα διενεργείται με την βοήθεια μητρών. Αν για παράδειγμα ο αριθμός των στρατηγικών κινήσεων κι επιλογών ενός παίχτη δεν είναι πεπερασμένος, τότε μπορούν να αναφερθούν ως στοιχεία ενός συνόλου αυτές οι στρατηγικές. Τα κέρδη ή οι ζημιές θα μπορούν να καταγραφούν ως πραγματικές συναρτήσεις ενός συνόλου στρατηγικών. Όταν λοιπόν αναφερόμαστε σε ένα τέτοιο παίγνιο, μπορούμε να πούμε πως το παίγνιο βρίσκεται σε κανονική μορφή. Στην κανονική μορφή η δυναμική των παίγνιων μπορούμε να πούμε πως χαμηλώνει και υπολείπεται, γιατί σε αυτή τη μορφή των παίγνιων, οι παίχτες ενεργούν μια φορά και το παίξιμο τους δεν εξαρτάται από μια σειρά αποφάσεων.

Έτσι, με απλά λόγια μπορούμε να πούμε ότι τα παίγνια σε αυτή τη μορφή λέγονται στατικά. Με την κανονική μορφή των παίγνιων, μας δίνεται οι δυνατότητα να αναλύσουμε, να περιγράψουμε και να αναφερόμαστε σε απτές εφαρμογές της καθημερινότητάς μας, της ζωής μας, της αγοράς και της οικονομίας. Επίσης, στην περίπτωση που ο αριθμός των στρατηγικών δεν είναι πεπερασμένος, όπως

προαναφέραμε, δίνεται η δυνατότητα μέσω των κατάλληλων μεθόδων για μια περαιτέρω και πιο θεωρητική και αλγοριθμική μελέτη.

4.6 Θεωρία φυλακισμένου

Το δίλημμα του φυλακισμένου είναι ένα κλασικό παράδειγμα που μας δείχνει ότι η συνεργασία μας συμφέρει. Ο κάθε αντίπαλος πιθανώς να ομολογήσει 8/10 φορές και ακόμα χειρότερα, πιστεύει πως και ο αντιμαχόμενος του θα ομολογήσει 8/10 φορές και αυτό αλλάζει τα πράματα εντελώς. Το αν οι άνθρωποι περισσότερο συνεργάζονται ή ανταγωνίζονται μεταξύ τους είναι μια συζήτηση που δεν σταματάει τουλάχιστον μεταξύ των προσεγγίσεων των διεθνών σχέσεων.

Εικόνα 15 Το δίλημμα του φυλακισμένου

Αυτό που κάνει εντύπωση στο παραπάνω δίλημμα είναι ότι πηγαίνοντας με την ανθρώπινη λογική (ορθολογισμός) ο φυλακισμένος επιλέγει να καρφώσει τον σύντροφό του επειδή αυτό πιστεύει ότι είναι προς το συμφέρον του, το ίδιο κάνει και ο άλλος και καταλήγουν και οι δύο να εκτίσουν μεγάλη ποινή.

Αλλά αν υποθέσουμε ότι ο καθένας από τους κρατούμενους κοιτάξει ποιο είναι το συμφέρον του άλλου και όχι το δικό του τότε χωρίς να το περιμένουν βγαίνουν τελικά και οι δύο κερδισμένοι. Αυτή είναι η κατά Θεόν Λογική και συνήθως υπερβαίνει, ξεπερνά την ανθρώπινη λογική (ορθολογισμός). Αρκεί επίσης κάποιος να κοιτάξει την Ελλάδα σήμερα για να δει που μας οδήγησε η λογική του ΕΓΩ αντί του ΕΜΕΙΣ.

Πάντα υπάρχουν καταστάσεις όπου εκ των πραγμάτων δεν υπάρχει δυνατότητα συνεργασίας για τους εμπλεκόμενους. Δεν λύνονται όλα τα προβλήματα με την

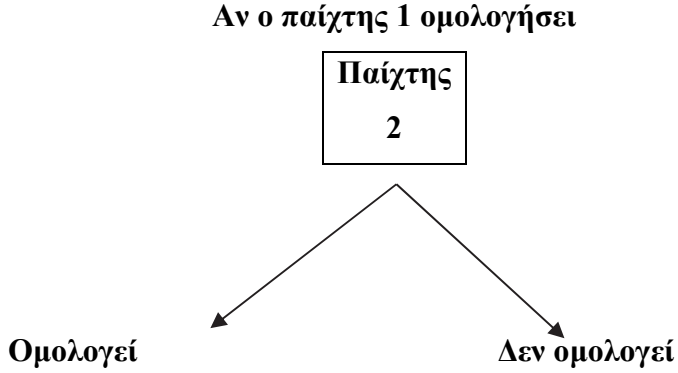
συνεργασία - γιατί ορισμένες φορές το πρόβλημα είναι ακριβώς ο ανταγωνισμός και η αντιπαλότητα. Δεν είναι δυνατόν να καταργηθούν διά παντός οι συγκρούσεις των ανθρώπων, διότι πάντοτε θα υπάρχουν αγαθά που θα φτάνουν για λίγους, αλλά πολλοί θα τα επιθυμούν. Σπάνια αγαθά τα οποία θεωρούνται βασικά μπαίνουν στην κατηγορία του δημόσιου αγαθού και το κράτος αναλαμβάνει να τα παράγει ή να επιχορηγήσει εταιρίες ώστε να έχουν πιο πολλοί άνθρωποι δυνατότητα να τα αγοράσουν.

Τέτοια παραδείγματα συναντά κανείς τόσο στην ασφάλεια των υλικών όσο και στο διαπροσωπικό επίπεδο. Π.χ. δύο αγόρια είναι ερωτευμένα με την ίδια κοπέλα, ή δύο αντιμαχόμενοι διεκδικούν μια συσκευή για τα αρχεία της. Ο μόνος τρόπος να λυθούν τέτοιες διαφορές είναι είτε μέσω σύγκρουσης, είτε διά της παραίτησης. Όσο ο άνθρωπος θα είναι εγωιστής τόσο θα υπάρχουν αναπόφευκτα και συγκρούσεις, γιατί αργά ή γρήγορα οι ακόρεστες επιθυμίες των ανθρώπων στρέφονται προς πράγματα που φτάνουν μόνο για λίγους.

Πίνακας 3 Ανταμοιβή στο δίλημμα του φυλακισμένου

ΠΑΙΧΤΗΣ 1			
		Ομολογεί	**Δεν ομολογεί**
ΠΑΙΧΤΗΣ 2	**Ομολογεί**	**4 χρόνια φυλάκιση**	**1 χρόνο φυλάκιση για τον παίχτη 2 και 8 για τον παίχτη 1**
	Δεν ομολογεί	**8 χρόνια φυλάκιση για τον παίχτη 2 και 1 για τον παίχτη 1**	**3 χρόνια φυλάκιση**

Πίνακας 3 Ανταμοιβή στο δίλημμα του φυλακισμένου



4 χρόνια φυλάκιση	8 χρόνια φυλάκιση

Δεν ξέρω αν αυτά φαίνονται "αρνητικά", αλλά πάντως έτσι έχουν τα πράγματα είτε μας αρέσει είτε όχι. Εγώ δεν συνηθίζω να αξιολογώ τα ανθρώπινα χαρακτηριστικά. Όμως όλοι μας σίγουρα θα γνωρίζουμε ότι υπάρχουν καταστάσεις όπου δύο ή περισσότερα στρατόπεδα αγωνίζονται για ένα αγαθό (στην προκείμενη περίπτωση για ένα υλικό) που είναι απαραίτητο για την επιβίωσή τους ή την καλοπέρασή τους, αλλά φτάνει μόνο για έναν. Σε τέτοιες περιπτώσεις η συνεργασία όχι απλώς δεν συμφέρει, αλλά είναι de facto αδύνατη, και η σύγκρουση αναπόφευκτη.

Βεβαίως, η συνεργασία συμφέρει όταν . . . συμφέρει, αλλά αυτό είναι απλώς μια ταυτολογία. Όπως και να 'χει, οι άνθρωποι επιλέγουν την στρατηγική τους με βάση τα συμφέροντά τους και την κατάσταση στην οποία βρίσκονται, υποκινούμενοι από τον εγωισμό τους και μόνο. Ακόμη κι όταν κάποιος π.χ. δίνει λεφτά σ' έναν ζητιάνο, το κάνει αυτό είτε επειδή θέλει να απολαύσει το συναίσθημα ότι βοήθησε κάποιον άλλον (και αυτή η απόλαυση βασίζεται εν μέρει στην συνειδητοποίηση ότι είναι πιο ισχυρός και πιο τυχερός σε σχέση με τον άλλον), είτε επειδή θέλει να αποφύγει τα δυσάρεστα συναισθήματα των τύψεων (αν είναι πολύ ευαίσθητος).

Σε κάθε περίπτωση, ο καθένας κοιτά πάντοτε το άτομό του και την απόλαυσή του - και αυτό ακριβώς είναι που οδηγεί ενίοτε στον αλτρουισμό και την συνεργασία, και ενίοτε στην θανάσιμη σύγκρουση και τον πόλεμο. Το τι θα συμβεί δεν εξαρτάται μόνο απ' τα υποκείμενα, τον χαρακτήρα και την ιδεολογία τους, αλλά και από την κατάσταση στην οποία βρίσκονται, η οποία πολλές φορές τους οδηγεί αναπόφευκτα σε αντιπαλότητα ή σε επιλογές που τελικά δεν συμφέρουν κανέναν (βλ. π.χ. την τραγωδία των κοινών - η οποία λέγεται "τραγωδία" ακριβώς επειδή είναι αναπόφευκτη).

"Η ζωή μοιάζει με ένα επαναλαμβανόμενο δίλημμα του φυλακισμένου, όπου οι άνθρωποι, συνήθως, συμπεριφέρονται με τον τρόπο, με τον οποίο τους συμπεριφέρθηκε ο συμπαίκτης τους την προηγούμενη φορά, στην λογική του "μία σου και μία μου" και του "ότι μου κάνουν θα τους κάνω". Ταυτόχρονα υπεισέρχονται και άλλοι παράγοντες, όπως η εικόνα, που θέλει ένας άνθρωπος να έχουν οι άλλοι για αυτόν".

ΚΕΦΑΛΑΙΟ 5: ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΥΛΙΚΟΥ ΒΑΣΙΣΜΕΝΟΙ ΣΤΗ ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ

5.1 Μέθοδοι θεωρίας παίγνιων

5.1.1 Θεωρία των παίγνιων και στρατηγική

Η θεωρία των παίγνιων και η σύνδεση με την ασφάλεια του υλικού εξαρτάται από την στρατηγική ικανότητα του κάθε παίχτη, καθώς κι από την αβεβαιότητα που χαρακτηρίζει την κάθε στρατηγική που καταστρώνει ο εκάστοτε παίχτης. Η ικανότητα αυτή και η δυνατότητα του να ξέρουμε τι μπορεί να μας συμβεί στην πορεία της ζωής μας, είναι πολύ σημαντική παράμετρος. Σε αυτήν τη περίπτωση, αυτός που δέχεται την επίθεση (το θύμα), είναι προετοιμασμένος γι' αυτό που πρόκειται να του συμβεί και θα πρέπει να αντιμετωπίσει είτε είναι στην εργασία του είτε είναι στην οικογένειά του.

Η θεωρία των παίγνιων είναι αυτή που μπορεί να μας βοηθάει να βλέπουμε μπροστά και να προβλέπουμε τι πρόκειται να μας συμβεί και με την βοήθειά της να μπορούμε, στην προκείμενη περίπτωση, να παρέχουμε μεγαλύτερη ασφάλεια στο υλικό. Σίγουρα δεν μπορεί να μας παρέχει πλήρη πρόγνωση στο απολυτό, γι' αυτό που θα προκύψει, όμως μπορεί σε έναν μεγάλο βαθμό να εξαλείψει κινδύνους όταν αυτοί εμφανιστούν. Όπως έχουμε αναφέρει και σε προηγούμενο κεφάλαιο, όταν παίζουμε ένα παιχνίδι σκάκι, πρέπει να ενεργούμαι και να σκεφτόμαστε σύμφωνα με την θεωρία των παίγνιων, προβλέποντας «σαν θεωρητική» την εξέλιξη του παιχνιδιού.

Κοιτάμε συνεχώς μπροστά και το ποια θα είναι η επόμενη κίνηση του επιτιθέμενου, έτσι ώστε να έχουμε καλύτερες πιθανότητες να αντιμετωπίσουμε μια πιθανή επίθεση σε ένα υλικό και με αυτό τον τρόπο να αυξήσουμε τις πιθανότητες της νίκης. Πάντα έχουμε στο μυαλό μας όμως ότι κι ο επιτιθέμενος σκέφτεται και πράττει με την ίδια θεωρία, πως και αυτός σκέφτεται με τον ίδιο τρόπο με εμάς, έχοντας κι αυτός έναν ορθολογικό τρόπο σκέψης βασισμένο στην θεωρία των παίγνιων, όπου εμείς θα πρέπει να είμαστε σε θέση να αντιμετωπίσουμε [21].

Συνεπώς με την θεωρία των παίγνιων κι όσον αφορά την μέθοδο που πρέπει να ακολουθείται για την ασφάλεια του υλικού, αναλύουμε το παρόν και το πώς γίνετε η επίθεση, αλλά ταυτόχρονα προβλέπουμε και το μέλλον για το πώς θα εξελιχθεί η επίθεση και το μέχρι που μπορεί να φτάσει ο επιτιθέμενος για την επίτευξη του στόχου του. Και κάθε απόφαση μας έχει συνέπειες (είτε θετικές, είτε αρνητικές) και πάντα σε συνάρτηση και με τις κινήσεις και τις αποφάσεις του αντιπάλου παίχτη καταστρώνονται και οι επόμενες κινήσεις, δράσεις, στρατηγικές και προσδοκίες για το αποτέλεσμα, αλλά και για το μέλλον.

5.1.2 Η σημαντικότητα μιας απόφασης

Στην ασφάλεια του υλικού τα πράγματα δεν είναι τόσο απλά στις αποφάσεις, όπως π.χ. είναι το να αποφασίσουμε μια κίνηση στο πόκερ. Οι αποφάσεις για την ασφάλεια του υλικού είναι πιο περίπλοκες καθώς και οι κίνδυνοι είναι περισσότεροι και τα προβλήματα που μπορεί να προκύψουν, να οδηγήσουν σε απρόβλεπτα αποτελέσματα. Οι αποφάσεις εμπεριέχουν πολλά ρίσκα με πολλαπλές συνεχιζόμενες συνέπειες (θετικές κι αρνητικές) με την διακύβευση του θετικού αποτελέσματος ως προς την ασφάλεια του υλικού να διακατέχεται από αβεβαιότητα. Επίσης, όταν εμπλέκονται πολλοί άνθρωποι στην τελική απόφαση, τα πράγματα γίνονται ακόμα πιο σύνθετα, κι αυτό γιατί όλοι προσπαθούν, μέσα από τις κινήσεις τους, τις στρατηγικές τους και τις γνώμες τους, να καταφέρουν το αποτέλεσμα που επιθυμούν.

Το τι θέλει να πετύχει η κάθε πλευρά που συμμετέχει σε ένα παίγνιο, από το τι νομίζει πραγματικά ότι θα πετύχει η κάθε πλευρά και το τι πετυχαίνει στο τέλος, είναι κάτι που μπορούμε να εκμεταλλευτούμε, μέσω της θεωρίας των παίγνιων, για να επηρεάσουμε την εξέλιξη του παίγνιου και έκβαση του τελικού αποτελέσματος. Η αβεβαιότητα είναι αυτή που θέλουμε να ξεπεράσουμε είτε να παρακάμψουμε στην θεωρία των παίγνιων, κάτι που πρακτικά αυτό είναι ανέφικτο να συμβεί και δεν μπορεί να γίνει σιγουρά, γιατί η αβεβαιότητα είναι μέρος της ζωής και της φύσης μας γενικότερα [21].

5.1.3 Η μπλόφα ως μέρος της στρατηγικής

Η μπλόφα είτε γίνετε στο πόκερ είτε στην διάρκεια μιας επίθεσης εναντίον ενός υλικού, έχει στόχο να πλήξει τον αμυνόμενο μέσω της αβεβαιότητας. Όλοι γνωρίζουν ότι κατά την διάρκεια μιας επίθεσης με στόχο να πλήξει την ασφάλεια ενός υλικού, ελλοχεύει πάντα η περίπτωση της μπλόφας και από τις δυο αντιμαχόμενες πλευρές (αυτή του επιτιθέμενου ή αυτή του αμυνομένου) και το κίνητρο συνεχώς θα είναι να αναγνωριστεί εγκαίρως και να καταπολεμηθεί η μπλόφα άμεσα κι έγκαιρα με την βοήθεια της επιστήμης της θεωρίας των παίγνιων.

Η μπλόφα καθώς και η συχνότητά της κατά την διάρκεια μιας επίθεσης ενάντια ενός υλικού, θα πρέπει να αναλυθεί διεξοδικά γιατί είναι συνυφασμένη με τις εκάστοτε στρατηγικές που ακολουθούν οι αντίπαλοι και εξαρτάται κι από τις αντιμαχόμενες πλευρές, για το ποιοι συμμετέχουν στην σύνθεση των ομάδων, κι αν έχουν την τάση να μπλοφάρουν κι αυτοί ή παίζουν αληθινά. Η μπλόφα στο πόκερ από την μπλόφα στην ασφάλεια του υλικού δεν διαφέρει και πολύ. Όταν ο επιτιθέμενος κατά την διάρκεια της επίθεσης δηλώνει ότι έχει καταφέρει να επέμβει (χακάρει) στο υλικό, αυτό μπορεί

να είναι αληθές, μπορεί όμως να είναι και μπλόφα με στόχο να φέρει σε δύσκολη θέση τον αμυνόμενο και να δυσχεραίνει τις επόμενες κινήσεις του, ακόμα και να καταφύγει σε λάθος στρατηγικές στην εξέλιξη της επίθεσης.

Καταλαβαίνουμε λοιπόν ότι μια εν εξελίξει προσπάθεια παραβίασης ενός υλικού μπορεί να είναι μια αληθινή επίθεση στο υλικό με πραγματικά δεδομένα, μπορεί όμως να είναι και μια μπλόφα, με εικονικά ή παραποιημένα δεδομένα, για να αποκτήσει ο επιτιθέμενος κάποια πλεονεκτήματα έναντι του αμυνομένου. Η άμυνα ενός παίχτη ή μιας ομάδας αποτελούμενης από πολλούς ανθρώπους, σε μια επιθετική ενέργεια που εμπεριέχει το στοιχείο της μπλόφας/παραπλάνησης, είναι μια επίπονη διαδικασία που όμως αν στεφθεί από επιτυχία, προσδίδει μια αξιοπιστία στον αμυνόμενο. Αυτή η αξιοπιστία είναι πολύ σημαντική προκειμένου να διασφαλίσει το υλικό του από μια κακόβουλη ενέργεια.

5.1.4 Αντίμετρα απέναντι σε επιθέσεις στο υλικό

Επιπλέον η αντιμετώπιση της επίθεσης είναι διαφορετική αν πίσω από αυτήν κρύβονται οικονομικά κίνητρα ή απλά είναι μια κακόβουλη επίθεση από έναν κακόβουλο χρήστη που στόχο έχει να πλήξει το υλικό για προσωπική του ικανοποίηση. Στην δεύτερη περίπτωση απλώς θα μιλάμε για απατεώνες που θα πρέπει να αντιμετωπιστούν/εκδιωχθούν μέσω της θεωρίας των παίγνιων, χρησιμοποιώντας την ικανότητα, του να μπορούμε σκεφτόμαστε και να διαμορφώνουμε καταστάσεις μέσω της συγκεκριμένης επιστήμης της θεωρίας των παίγνιων. Στην περίπτωση όμως που τα κίνητρα είναι οικονομικά απαιτούνται πιθανόν προϋπολογισμοί αρκετά μεγάλοι και βοήθεια από εξωτερικούς παράγοντες [21].

Όλες οι μεγάλες εταιρείες που κατασκευάζουν υλικά, φροντίζουν πρωτίστως για το δικό τους μεγαλύτερο κέρδος και ενδιαφέρονται για τα συμφέροντα τους. Αυτό όμως τους κάνει να είναι ιδιαιτέρως προβλέψιμοι ως προς την κατασκευή και τις δικλείδες ασφαλείας που εκπονούν πάνω στην ασφάλεια του υλικού. Και αυτό είναι που μας δίνει την δυνατότητα μέσω της θεωρίας των παίγνιων, χρησιμοποιώντας την λογική, να υποθέσουμε πιθανές μελλοντικές ενέργειες και να δώσουμε την ευκαιρία για μια καλύτερη κατευθυντική εξέλιξη πάνω στην ασφάλεια του υλικού.

Αν για παράδειγμα ένας υπεύθυνος ενός εργοστασίου κατασκευής υλικών, επενδύει πολύ περισσότερα στην μεγιστοποίηση της ασφάλειας των υλικών, από αυτό που μπορεί να καλύψει η εταιρεία, αυτό θα οδηγήσει στο κλείσιμο της εταιρείας. Σε αυτήν την περίπτωση ο υπεύθυνος κοιτάει το άμεσο συμφέρον, που είναι η παροδική αύξηση της ασφαλείας του υλικού, κι όχι αυτό που θα συμβεί μακροπρόθεσμα, δηλαδή

στο κλείσιμο της εταιρείας. Το ίδιο και οι αγοραστές, κοιτούν την εφήμερη χαρά και το πρόσκαιρη εξασφάλιση, αποκτώντας ένα υλικό με μεγάλη ασφάλεια, αλλά που σε λίγο καιρό δεν θα υπάρχει, γιατί το εργοστάσιο θα χρεοκοπήσει και το υλικό θα πάψει να παράγεται, με συνέπεια να μην μπορεί ούτε να επισκευαστεί κι ούτε να αλλαχθεί.

Με αυτές τις λογικές που ακολουθούνται όμως με το πρόβλημα να μεταφέρεται στον επόμενο για να το λύσει, όλοι κοιτούν κοντόφθαλμα για μια γρήγορη επιτυχημένη αγορά ενός υλικού που μόνο ιδιοτελή συμφέροντα επιφέρει. Σε όλους μας ή στους περισσοτέρους για να το πούμε καλύτερα, αρέσει να καταναλώνουμε εις βάρος των άλλων. Το καλύτερο που έχουμε να κάνουμε για τον εαυτό μας είναι να μη μας ενδιαφέρει μόνο ο εαυτός μας. Σίγουρα αυτό θα ήταν το καλύτερο πράγμα που θα μπορούσε να γίνει.

Πραγματικά βάζουμε πιο πάνω τον ατομικισμό και το συμφέρον μας νομίζοντας ότι θα κερδίσουμε περισσότερα χωρίς να καταλαβαίνουμε ότι στο σύνολό και στην γενική εικόνα θα τα χάσουμε όλα. Το περίεργο είναι ότι οι νόμοι είναι για όλους τους άλλους εκτός από αυτούς που τους σκέφτηκαν. Όσο για την ασφάλεια των υλικών, αυτοί που καίγονται για το μέλλον της εξέλιξης της τεχνολογίας, όλος τυχαίος είναι αυτοί που βγάζουν όλο και περισσότερα χρήματα, μέσα από αυτόν τον ατομικισμό, ενώ παράλληλα έχουν και συμφέρον από τις καταστροφές που συντελούνται και που προέρχονται από τις επιθέσεις που γίνονται σε υλικά.

5.1.5 Οι λύσεις μέσα από την θεωρία των παίγνιων

Πάντα μέσα από υγιή ανταγωνισμό πρέπει να βελτιωνόμαστε και να προσπαθούμε να πείσουμε τους συνάνθρωπούς μας, πως η πιο ωφελιμιστική στάση ζωής είναι ο αλτρουισμός και η συνείδηση πως εξ ορισμού η ευτυχία μας περνά μέσα από τον διπλανό μας. Οτιδήποτε άλλο είναι επίπλαστο ή πρόσκαιρο ή ψευδαίσθηση. Δεν μπορεί αρχικά να υπάρξει ατομική επιτυχία κι ευτυχία υπό την έννοια ότι δεν μπορεί να μοιραστεί ως κοινό συναίσθημα και στη συνέχεια, γιατί η δυστυχία μέχρι και του ενός, δεν περιφράζεται ως κάτι που νομοτελειακά πρέπει να λυθεί, γιατί όσο υπάρχει δημιουργεί συλλογικές παθογένειες. Ότι ισχύει για το ατομικό, ισχύει και για υποσύνολα. Κοινωνικό κτήμα γίνεται το κτήμα που φτάνει στον αριθμό του συνόλου.

Εδώ λοιπόν, έρχεται η επιστήμη της θεωρίας των παίγνιων για να μας λύσει ένα μέρος από το πρόβλημα του ατομικισμού που διακατέχει την εποχή μας, και να μας κάνει να αντιληφθούμε το γιατί η ασφάλεια του υλικού πρωτίστως απαιτεί πολιτικές θεωρήσεις, απαιτεί διαφορετική προσέγγιση με αλλαγή νοοτροπίας, φιλοσοφίας και παιδείας. Ευτυχώς που μπορούμε μέσω της χρήσης της θεωρίας των παίγνιων να

προβλέπουμε τέτοιες καταστάσεις και να αντιδρούμε δυναμικά για να υπολογίζουμε τις συνέπειες, σε διάφορα τέτοια πολύπλοκα μοντέλα [21].

Το μυαλό είναι ένας παράδεισος που όσο ποιο πολύ εμβαθύνει τόσο ποιο πολύ περιπλέκεται χάνεται η σταθερότητα και επαναλαμβάνεται η ίδια μεταβλητή θεμάτων με κάθε φορά καλύτερο αποτέλεσμα. Με λίγα λόγια το να ψάχνεσαι χωρίς όρια, ο κόσμος είναι απίστευτα συναρπαστικός και μέσα σε αυτό το σκίνο επιφανειακών καταστάσεων υπάρχει ένας ολόκληρος κόσμος που δεν τον έχεις δει ή συναντήσει πουθενά πάλι και κάπου εκεί υπάρχουν χιλιάδες μικρά και μεγάλα μυστικά κρυμμένα για να ανακαλύψεις και να συνυπάρξεις μαζί τους.

5.1.6 Διαβάθμιση κι ανάλυση των αποφάσεων

Σημαντικό επίσης θεωρώ είναι το να βάζεις μια διαβάθμιση, και να ξεχωρίζεις την ιδιάζουσα βαρύτητα της κάθε απόφασης, καθώς είναι δύσκολο κάθε επιλογή να έχει την ίδια πιθανότητα επιτυχίας. Δεν μπορείς να περιμένεις από τον άλλον να κάνει το σωστό απλά επειδή είναι σωστό από μαθηματικής άποψης. Πιστεύω πως η χρυσή τομή είναι να βρεις αυτές τις παραμέτρους και να τις συμπεριλάβεις ώστε να καταλήξεις σε σωστά αποτελέσματα. Αυτό προϋποθέτει να καταλάβουμε πως όλοι οι συμμετέχοντες παίχτες σκέφτονται και πράττουν ορθολογικά με απώτερο στόχο το δικό τους κέρδος, εξετάζοντας διεξοδικά την θέση αλλά και την κάθε απόφαση του εκάστοτε παίχτη.

Αναλύουμε πολύ προσεχτικά όλες τις αποφάσεις του ενίοτε παίχτη στο κατά πόσο και πόση μεγάλη βαρύτητα έχει η κάθε του απόφαση, στο κατά πόσο ευέλικτος είναι στις αποφάσεις του και στο κατά πόσο μπορεί και είναι ικανός να επηρεάζει και τους άλλους παίχτες (αντιπάλους και μη) στις αποφάσεις τους. Όλοι οι παίχτες που επιτίθονται (π.χ. σε ένα υλικό στην προκειμένη περίπτωση), σκέφτονται ποιος είναι ο καλύτερος τρόπος για την επιτυχία. Όπου ο καλύτερος τρόπος για τους επιτιθέμενους/παραβάτες είναι μια επίθεση στο υλικό, με το μικρότερο κόστος, σε σύντομο χρονικό διάστημα και με το μέγιστο κέρδος γι' αυτούς χωρίς να έχουν καταναλώσει μεγάλη ενέργεια, και να προχωρήσουν στο επόμενο θύμα τους στη συνέχεια.

Γι' αυτό λέμε ότι όλοι οι συμμετέχοντες είναι μέρος του παιχνιδιού με σκοπό την προώθηση των συμφερόντων τους με απώτερο στόχο την επιτυχία και το κέρδος. Όμως μέσω της θεωρίας των παίγνιων βλέπουμε ότι οι άνθρωποι, όσο πλησιάζουν την επιτυχία, είναι περισσότερο προβλέψιμοι ως προς τις αποφάσεις τους για την επίτευξη των στόχων τους. Για να ακριβολογούμε, μπορούμε να αναφέρουμε πως όλες οι

στρατηγικές αλληλεπιδράσεις όλων των εμπλεκόμενων παιχτών είναι μέρος των παίγνιων κι εντάσσονται στην επιστήμη της θεωρίας των παίγνιων [21].

5.1.7 Ο ατομικισμός

Καλό εδώ θα ήταν να αναφερθούμε στον ατομικισμό των παιχτών που για δικό τους όφελος δρουν ενάντια στο κοινωνικό συμφέρον. Αυτό φυσικά σε βάθος χρόνου θα επιφέρει αρνητικά αποτελέσματα στην κοινωνία και στους ίδιους. Μερικά παραδείγματα του ατομικισμού είναι:

Η αγορά πειρατικών δίσκων, που εν αρχή μας δίνετε η δυνατότητα για μια φθηνή αγορά μιας ταινίας ή τραγουδιών, αλλά που σε βάθος χρόνου ένα μεγάλο κινηματογραφικό στούντιο ή μια δισκογραφική εταιρεία δεν θα έχει μελλοντικά την οικονομική δυνατότητα για μια καινούρια παραγωγή ταινιών ή τραγουδιών αντίστοιχα, λόγο έλλειψης πόρων, γιατί όλοι καταλαβαίνουμε ότι τα χρήματα από μια πειρατική αγορά καταλήγουν σε επιτήδειους απατεώνες κι όχι στους πραγματικούς δημιουργούς.

Θέλω να σταθώ στο θέμα της πειρατείας, το οποίο έχει απήχηση και σε άλλες παρόμοιες καταστάσεις, όπως η ασφάλεια υλικού. Ισχύει ότι αν όλοι αγοράζαμε τις συσκευές, οι παραγωγοί τους θα έριχναν και τις τιμές για να τις κάνουν πιο προσιτές και θα έβγαζαν και αυτοί χρήματα και καλύτερης ποιότητας υλικά. Το πρόβλημα εδώ όμως είναι πως μπορεί εγώ σε ατομικό επίπεδο να το κάνω αυτό, και η απάντηση είναι πως δε μπορώ. Το να αποκτήσω ξαφνικά εγώ συνείδηση και να μην ξανακατεβάσω πειρατικά υλικά, δε σημαίνει ότι θα το κάνουν όλοι. Δεν έχω επιρροή σε κανέναν με το να το κάνω αυτό, οπότε το ότι έχω εγώ συνείδηση δε σημαίνει ότι θα αποκτήσουν όλοι και θα το κάνουν.

Το μόνο που μπορώ να κάνω σε ατομικό επίπεδο είναι η δική μου ατομική συνεισφορά και να το διαδώσω σε φίλους προκειμένου, με ελάχιστες πιθανότητες, να το κάνουν και οι ίδιοι. Μέχρι εκεί. Αν λοιπόν δε βγει κάποια "παγκόσμια ανακοίνωση" που να γνωστοποιήσει σε όλους και να τους κάνει όλους να έχουν συνείδηση, τότε το να το κάνει ο κάθε ένας ατομικά δεν οδηγεί πουθενά.

Αντίστοιχα παραδείγματα είναι με το να μην πηγαίνουμε στις εθνικές εκλογές. Με το να απέχω εγώ, δε σημαίνει ότι επηρεάζω τον υπόλοιπο κόσμο να απέχει, και αντίστοιχα με το να πηγαίνω δε σημαίνει ότι θα πάει κι ο άλλος κόσμος. Η διαφορά αυτών των καταστάσεων με το πρώτο παράδειγμα του είναι ότι εγώ αναφέρομαι σε καταστάσεις που η άποψη μου και η σφαίρα επίδρασής μου αφορά ένα πάρα πολύ μικρό ποσοστό, ενώ στην θεωρία των παίγνιων όπου υπάρχουν 2 αντιμαχόμενες

πλευρές και οι ενέργειες του ενός επιδρούν στον άλλον, αλλά παράλληλα απηχούν και σε όλο το φάσμα της κοινωνίας, μπορεί να επηρεάσει θετικά την παγκόσμια κοινότητα.

Το παράνομο παρκάρισμα ή το παρκάρισμα σε βολικά σημεία εξυπηρέτησης προς εμάς είναι ένα σημάδι ατομικισμού, το οποίο όμως είναι ενάντια στο κοινωνικό συμφέρον και δημιουργεί κυκλοφοριακό κομφούζιο εις βάρος των πολλών καθώς και μια οδηγική αναρχία.

Το κτίσιμο σε αυθαίρετα οικόπεδα ωφελεί ατομικά αυτόν που το πράττει, αλλά στο υπόλοιπο κοινωνικό σύνολο, επιφέρει καταστάσεις δυσανάλογες ως προς το περιβάλλον και μας κάνει να ζούμε σε μια άναρχη χώρα και σε μη ανθρώπινες συνθήκες.

Πίνακας 4 Απολαβές παιχτών

Παιχτης1/Παίχτης 2	Εγωισμός	Αλτρουισμός
Εγωισμός	(-19, -19)	(-10, -10)
Αλτρουισμός	(-10, -10)	(-1, -1)

Όλα τα παραπάνω μας δημιουργούν μικρές εφήμερες χαρές, ως προς το ατομικό μας συμφέρον, που όμως δεν βοηθούν το κοινωνικό συμφέρον και δεν αφήνουν πολλά περιθώρια εξέλιξης και προόδου σε κανέναν από εμάς. Αντιθέτως, αν ακολουθήσουμε όλοι μας λογικές πεποιθήσεις θα δημιουργηθούν καλύτεροι οιωνοί και ανοίξουν νέοι ορίζοντες με απώτερο σκοπό το κοινό καλό του τόπου μας [21].

Πάντα προσπαθούσα και προσπαθώ να πείσω πως η πιο ωφελιμιστική στάση ζωής είναι ο αλτρουισμός και η συνείδηση και πως εξ ορισμού η ευτυχία μας περνά μέσα από τον δίπλα μας. Ότι άλλο, είναι επίπλαστο ή πρόσκαιρο ή ψευδαίσθηση. Δεν μπορεί να υπάρξει ατομική ευτυχία, αρχικά υπό την έννοια ότι δεν μπορεί να μοιραστεί ως κοινό συναίσθημα, και στη συνέχεια γιατί η δυστυχία μέχρι και του ενός, δεν περιφράζεται ως κάτι που νομοτελειακά πρέπει να λυθεί, γιατί όσο υπάρχει δημιουργεί συλλογικές παθογένειες. Ότι ισχύει για το ατομικό ισχύει και για τα υποσύνολα. Κοινωνικό κτήμα γίνεται το κτήμα που φτάνει στον αριθμό του συνόλου.

5.1.8 Τρόποι αντιμετώπισης

Προτείνοντας μερικούς τρόπους αντιμετώπισης ως προς την ασφάλεια του υλικού, καλό θα είναι να αναφέρουμε και να πούμε ότι ο κάθε χρήστης ενός υλικού, θα πρέπει να προμηθεύεται γνήσια υλικά και να τα προστατεύει με γνήσια αντιβιοτικά, για την πλήρη και ορθή τους λειτουργία. Αν ο κάθε χρήστης του εκάστοτε υλικού, αγοράζει παραποιημένα, μεταχειρισμένα υλικά είτε απομιμήσεις υλικών, με αυτήν τη κίνηση του αποσκοπεί στο πρόσκαιρο όφελος που είναι η αγορά σε χαμηλή τιμή ενός

προϊόντος αλλά μακροπρόθεσμα μπορεί να γίνει εύκολος στόχος κακόβουλων επιθέσεων και να κινδυνεύσει χάνοντας σημαίνοντα πράγματα γι' αυτόν, μέσα από την επίθεση υλικού που πιθανόν να δεχτεί.

Μια καλή στρατηγική λοιπόν είναι να αγοράζουμε γνήσια προϊόντα από επίσημους προμηθευτές, έτσι ώστε να μειώνονται οι πιθανότητες το κάθε υλικό να γίνει στόχος κακόβουλων επιθέσεων. Μια δεύτερη καλή στρατηγική κίνηση είναι να ασφαλίζουμε τα υλικά μας με γνήσια αντιβιοτικά, όπως προ είπαμε, για την υψηλότερη προστασία από εξωτερικές επιθέσεις που θα γίνουν, αν γίνουν μελλοντικά. Μια τρίτη επιλογή είναι ανά τακτά χρονικά διαστήματα να γίνονται οι απαιτούμενοι έλεγχοι για πιθανές δυσλειτουργίες και για πιθανές αναβαθμίσεις που μπορεί να έχουν προκύψει από τον επίσημο προμηθευτή και θα πρέπει να γίνονται για να είναι το υλικό ενημερωμένο με τις τελευταίες του αναβαθμίσεις.

Είναι πολύ σημαντικό λοιπόν, να γίνονται όλες αυτές οι εύκολες και φυσιολογικές κινήσεις από τους χρήστες, για την ασφάλεια ενός υλικού και να αποφεύγονται όλα τα πιθανά παράδοξα που γίνονται κατά καιρούς. Όπου παράδοξα αναφέροντας, νοούμε τα υλικά να παραμένουν χωρίς ενημερώσεις κι αναβαθμίσεις, για πολύ μεγάλο χρονικό διάστημα, από την μέρα που αγοράστηκαν μέχρι να φθαρούν κι εκεί μετά ως χρήστες να αρχίσουμε να ανησυχούμε, ενώ θα πρέπει να φροντίζουμε εμείς προληπτικά για την συντήρηση τους.

Όλα τα παραπάνω που αναφέρθηκαν μας δίνουν μια αρμονική λειτουργία ενός συστήματος και που μέρος του είναι και το υλικό. Όλες αυτές οι μικρές ταχτικές κινήσεις είναι ικανές να μειώσουν είτε κι ακόμα να αποτρέψουν από μόνες τους πολλές πιθανότητες για εξωτερικές επιθέσεις από κακόβουλους χρήστες που θέλουν να πλήξουν για δικά τα τους συμφέροντα το υλικό. Μια συμπεριφορά αντικοινωνική από την μεριά των χρηστών ενός υλικού για το πρόσκαιρο κέρδος μπορεί να πλήξει την συνοχή του συστήματος και των υλικών του. Ο εξ ορθολογισμός του τρόπου σκέψης, η αλλαγή συμπεριφοράς και η αλλαγή προτύπων, είναι αυτά που μπορούν να ξεπεράσουν ακόμα και τους ίδιους τους ανθρώπους μαζί με τα ανιδιοτελή μικροσυμφέροντά τους.

5.1.9 Ανάλυση συμπεριφορών των παιχτών

Ζούμε σε μια κοινωνία που ευημερούν και έχουν οικονομικές απολαβές διάφοροι επιτήδειοι, εκμεταλλευόμενοι πρόσκαιρες ευκαιρίες που παρουσιάζονται εις βάρος των άλλων. Καλό θα είναι να γίνει κατανοητό και για την ασφάλεια υλικού αλλά και γενικότερα σε όλα τα αγαθά, πως αναλύοντας τις συμπεριφορές των παιχτών

μπορούμε να παρατηρήσουμε τις στρατηγικές των επιθέσεων στο υλικό. Έχει σημασία να κατανοήσουμε το πόσο σημαίνοντα ρόλο διαδραματίζει η θεωρία των παίγνιων στην ασφάλεια του υλικού, συνεκτιμώντας τις ορθολογικές στρατηγικές αποφάσεις και κινήσεις για την επίλυση των προβλημάτων που δημιουργούνται από τις επιθέσεις στο υλικό [21].

Μια ανάλυση μιας ορθολογικής ανθρώπινης συμπεριφοράς θα είναι πάντα ατελής, καθώς πάντα θα υπάρχουν απρόοπτες αποφάσεις κι ασυνεπείς συμπεριφορές από την πλευρά των παιχτών που θα είναι αντιφατικές με τις ορθολογικές αναλύσεις που έχουν πραγματοποιηθεί. Πιθανόν σε οποιαδήποτε ανάλυση μιας κατάστασης θα υπάρχει μια ακατανόητη απόφαση που θα πρέπει να συνυπολογίσουμε την ώρα του παιγνίου. Θα πρέπει μέσα μας να αναρωτιόμαστε συνεχώς αν η ορθολογικότητα είναι τόσο αποδοτική για την ασφάλεια του υλικού. Παρακάτω θα προσπαθήσουμε να δώσουμε κάποιες πιθανές απαντήσεις, ως προς την λύση των απρόβλεπτων αποφάσεων.

Πιθανόν να μην έχει δημιουργηθεί ακόμα κάποια θεωρία που να συμπεριλαμβάνει τις ακατανόητες αποφάσεις των παιχτών γιατί τα κατάλληλα κι αναλυτικά μας μοντέλα να αποτελούνται ακόμα από τον σωστό τρόπο σκέψης, ελλείψει κιόλας κάποιας καλύτερης και νεότερης θεωρίας.

Μια άλλη εκδοχή είναι πως όταν το διακύβευα είναι μεγάλο κι η εξέλιξη του αποτελέσματος θα επηρεάσει αρκετά πράγματα στο κοινωνικό σύνολο, αναμένουμε ότι σε βάθος χρόνου οι παίχτες θα σκεφτούν περισσότερο ορθολογικά, κι αναμένουμε μια συμπεριφορά προς την τέλεια ορθολογικότητα στην λήψη των αποφάσεων, παρά μια ακατανόητη απόφαση που συνήθως παραπέμπει σε εργαστηριακό πείραμα.

Μια τρίτη απάντηση μπορεί να δοθεί μέσα από το πως ο στόχος μιας επίθεσης υλικού δεν είναι μόνο να δούμε και να αναλύσουμε μια συμπεριφορά ενός παίχτη, αλλά να δούμε σε βάθος χρόνου το πως θα επηρεαστεί το κοινωνικό σύνολο από αυτό. Εν συνεχεία μέσα από μια τέτοια διαδικασία μπορεί να γίνουν αναλύσεις καθώς και να αξιολογηθούν νέες προτάσεις για την ασφάλεια του υλικού που θα προκύψουν μέσα από μελέτες [21].

5.1.10 Λύσεις ζητημάτων ασφαλείας υλικών μέσω της θεωρίας των παίγνιων

Στόχος της εργασίας μας είναι να θέσουμε ζητήματα ασφάλειας υλικού μέσα από την θεωρία των παίγνιων. Όμως ξεκινώντας καλό είναι να δούμε αν το ίδιο το υλικό που θέλουμε να προστατεύσουμε είναι πρώτα από όλα σε καλή κατάσταση, πλήρως λειτουργικό ή είναι ελλαττωματικό. Αν για παράδειγμα διαπιστώσουμε πως

ένα συγκεκριμένο υλικό είναι ελλαττωματικό σε αρκετές παρτίδες του, δεν μπορούμε να μιλάμε για την ασφάλεια του από κακόβουλες επιθέσεις γιατί δεν θα υπάρχει το επιθυμητό αποτέλεσμα. Για να αντιμετωπίσουμε κάθε είδους απειλή στο υλικό, καλό θα είναι να διαμορφώνεται ένα μοντέλο προστασίας από τους δημιουργούς του υλικού, με κανόνες που εκεί θα περιγράφεται και θα αναλύεται κάθε πιθανή συμπεριφορά που μπορεί να προκαλέσει φθορά.

Οι δημιουργοί και οι κατασκευαστές των υλικών θα πρέπει να παράγουν τα υλικά με τέτοιο τρόπο ώστε από μόνα του να βελτιστοποιούν την ασφάλεια τους μέσα από μοντέλα και προδιαγραφές προκαθορισμένες και παίρνοντας ως δεδομένο ότι αυτές είναι συνυφασμένες μέσα από τις τελευταίες τεχνολογικές εξελίξεις. Μέσα από αυτήν τη λογική, το κάθε υλικό για να παραβιαστεί από τον επιτιθέμενο θα πρέπει ο θύτης συνεχώς να προσαρμόζει το μοντέλο του και τις στρατηγικές του με βάση πάντα τις καινούριες τεχνολογικές μεθόδους ασφαλείας που θα διακατέχεται το υλικό από την κατασκευή του [21].

5.2 Τεχνικές που βασίζονται στην θεωρία παίγνιων για την ασφάλεια υλικού

5.2.1 Περίπτωση αμιγούς στρατηγικής minimax maximin

Μέσα από τις αναφορές μου στην διπλωματική μου, έχω αναφερθεί πολλές φορές σε διάφορες κατηγορίες και σε διάφορους τύπους παίγνιων. Οι πιο δημοφιλής κατηγορίες παίγνιων που διαβάζουμε στην βιβλιογραφία αναφέρονται στα παίγνια μηδενικού (και μη μηδενικού) αθροίσματος.

Πίνακας 5 Μήτρα ενός παίγνιου μηδενικού αθροίσματος

	ΠΑΙΧΤΗΣ 2		
ΠΑΙΧΤΗΣ 1	2Α	2Β	2Γ
1Α	-3	-2	3
1Β	1	0	1
1Γ	2	-2	-3

Ο παραπάνω πίνακας 5 μας φανερώνει το κέρδος που μπορεί να αποκομίσει ο παίχτης 1, απέναντι στο παίχτη 2. Αν ο πρώτος παίχτης αποφασίσει να ακολουθήσει την επιλογή 1Α και ο δεύτερος παίχτης αποφασίσει να ακολουθήσει την δική του στρατηγική 2Α τότε ο πρώτος παίχτης θα έχει απώλεια -3 και ο δεύτερος παίχτης θα έχει όφελος 3. Φαίνεται ξεκάθαρα λοιπόν πως σε μια τέτοια περίπτωση ο ένας παίχτης επωφελήθηκε το κέρδος του άλλου παίχτη.

Με τη χρήση του κριτηρίου minimax, θα προσπαθήσουμε να επιλύσουμε το συγκεκριμένο παίγνιο. Ο παίχτης 1 επιλέγει μέσα από έναν συγκεκριμένο πίνακα

αμοιβών, την στρατηγική κίνηση που θα ακολουθήσει και θα του επιφέρει το περισσότερο από τα ελάχιστα (maximin τιμή), καθώς ο παίχτης 2 αποφασίζει εκείνη την στρατηγική του απόφαση που θα του επιφέρει το μικρότερο από τα μεγαλύτερα οφέλη (minimax τιμή). Κατώτερη τιμή λέγεται αυτή η maximin τιμή και η υψηλότερη τιμή του παίγνιου λέγεται minimax. Όταν προκύπτει ταυτίσει αυτών των δυο τιμών, τότε λέμε πως το παίγνιο έχει λύση με αμιγές στρατηγικές και αυτή η λύση χαρακτηρίζεται σταθερή (stable), γιατί στο παίγνιο προκύπτει και παρουσιάζεται ένα σημείο ισορροπίας που επιφέρει και δίνει μια μοναδική τιμή (value of the game) [34].

Πίνακας 6 Ο τροποποιημένος πίνακας 5

	Παίκτης 2			
Παίκτης 1	2Α	2Β	2Γ	**Min γραμμών**
1Α	-3	-2	3	-3
1Β	1	0	1	**0**
1Γ	2	-2	-3	-3
Max στηλών	2	**0**	3	**V=0**

Σε αυτήν τη περίπτωση η λύση του παίγνιου αποτελείται από την στρατηγική 1Β του παίκτη 1 και την στρατηγική απόφαση 2Β του παίκτη 2, αντίστοιχα. Μόνο μέσα από την επιλογή των συγκεκριμένων στρατηγικών κινήσεων και των δυο παικτών το κέρδος και των δυο θα είναι μηδέν (V=0). Σε κάθε άλλη περίπτωση κάποιος παίκτης θα είναι κερδισμένος έναντι του άλλου.

Τέλος, για να μετατρέπει το συγκεκριμένο παίγνιο, σε παίγνιο σταθερού αθροίσματος, απαιτείται μόνο ένα σταθερό ποσό που να διεκδικείται από τους παίχτες και να είναι ίσο με την τιμή c (c>0). Τότε, ο παίκτης 1 θα έχει όφελος τις τιμές που αναφέρονται στον πίνακα 5, και ο παίκτης 2 θα έχει όφελος όποια τιμή θα προκύπτει από την διαφορά της σταθερής τιμής c κι αναλόγως την στρατηγική 1i2j που θα ακολουθείται από τους παίκτες. Σε περίπτωση που η σταθερά c ήταν αρνητική (c<0), τότε οι δύο παίκτες θα αγωνιζόντουσαν για το ποιος θα επιτύχει την μικρότερη δυνατή τιμή, καθώς σε αυτή την περίπτωση επρόκειτο για μέγεθος ζημίας [34].

5.2.2 Ισορροπία Nash

Η ισορροπία κατά Nash αφορά την ισορροπία παιγνίων που είναι μη μηδενικού αθροίσματος. Αυτό πρακτικά συναντάται στα παίγνια που δεν ισχύει ότι το κέρδος του ενός παίκτη είναι απαραίτητα ζημιά του άλλου, όπως στα παίγνια μηδενικού αθροίσματος. Ονομάστηκε έτσι χάρη στο όνομα του μαθηματικού John Nash που

βρήκε την ισορροπία των συγκεκριμένων παιγνίων. Επίσης, είναι μια γενική κι ευρέως αποδεκτή στρατηγική, καθώς προσδίδει καθορισμένη ισορροπία στα παίγνια.

Ο κάθε παίχτης ακολουθεί την στρατηγική του, όπου ακόμα κι αν αλλάξει θέση και στρατηγική δεν βελτιώνει τα κέρδη του, γιατί και οι υπόλοιποι παίχτες αναμένεται να αλλάξουν την θέση τους και θα τον ακολουθήσουν. Η στρατηγική που ακολουθείται στηρίζεται στον ορθολογισμό του εκάστου παίχτη, κι όπως προαναφέραμε, αναμένεται όλοι οι παίχτες να συντάσσονται με την εκάστοτε στρατηγική. Έτσι, καθορίζεται κάθε φορά μια στρατηγική θέση κι αναμένοντας τα αποτελέσματα της κάθε κίνησης, καταλήγουμε στο τέλος στο ποια στρατηγική ήταν η καλύτερη έναντι των άλλων παιχτών [34].

Η ισορροπία κατά Nash δεν προσδίδει πάντα τα καλύτερα κέρδη στους συμμετέχοντες παίχτες και δεν μπορεί να χαρακτηριστεί μια τέτοια συνθήκη, βέλτιστη κατά Pareto. Για να χαρακτηριστεί ένα ζεύγος κινήσεων βέλτιστο κατά Pareto, θα πρέπει στο παίγνιο να μην υπάρξει άλλο ζεύγος στρατηγικών με περισσότερο κέρδος για κάποιον συμμετέχοντα παίχτη. Έτσι, είναι ευκόλως κατανοητό πως για να μπορέσει να ικανοποιηθεί μια τέτοια βελτιστοποίηση, θα πρέπει όλοι οι συμμετέχοντες να μπορέσουν να συμφωνήσουν σε ένα σύνολο θέσεων, κινήσεων και στρατηγικών ξεχωριστών από αυτών που επιφέρουν την ισορροπία κατά Nash.

Ένα τέτοιο παράδειγμα μέσω των παίγνιων μπορεί να βρει εφαρμογή στην ασφάλεια υλικού, όπου οι μεγάλοι κατασκευαστές υλικών που πουλούν το υλικό και οι διάφοροι κακόβουλοι κι επιτιθέμενοι χρήστες συσκευών, που επιτίθονται σε συσκευές αλλοιώνοντας και υποκλέπτοντας τα χαρακτηριστικά τους και τις λειτουργίες τους, να έρθουν σε συμφωνίες με σκοπό την αύξηση των κερδών τους μέσω της βελτιστοποίησης κατά Pareto.

5.2.3 Παράδειγμα με την ισορροπία Nash στην ασφάλεια υλικού

Στο παράδειγμά μας θα ορίσουμε τον παίχτη 1 ως έναν κατασκευαστή υλικών και τον παίχτη 2 ως έναν πιθανό χρήστη. Θα πρέπει να θεωρηθεί δεδομένο η μεταξύ τους σύμβαση για την αγορά του υλικού και για ένα χρονικό διάστημα. Ο κατασκευαστής (παίχτης 1) έχει την δυνατότητα να αποφασίσει για την εταιρεία του και προς όφελός του, αν το υλικό που θα παράγει θα είναι υψηλής ή χαμηλής ποιότητας. Εξυπακούεται πως η κατασκευή υλικού υψηλής ποιότητας απαιτεί και μεγαλύτερο κόστος, το οποίο και είναι ανεξάρτητο από το εάν έχει συναφθεί σύμβαση μεταξύ των δυο παιχτών.

Το αν η κατασκευή του υλικού είναι υψηλής ποιότητας ή είναι χαμηλής ποιότητας, αυτό δεν αναφέρεται ρητά στην σύναψη της σύμβασης, πράγμα το οποίο δίνει την ευχέρεια στον παίχτη 1 να αποφασίσει χωρίς κάποιο κόστος γι' αυτόν το ποια ποιότητα θα επιλέξει. Επίσης, είναι ευκόλως αντιληπτό πως το υλικό υψηλής ποιότητας διαφέρει κατά πολύ στην ασφάλεια του από το υλικό που κατασκευάζεται από χαμηλής ποιότητας υλικά. Σε αυτήν την περίπτωση ο παίχτης 2 δεν είναι σε θέση να γνωρίζει την ποιότητα του υλικού που είναι φτιαγμένο ένα υλικό, ως προς την μεγιστοποίηση της ασφάλειάς του, γιατί αν γνώριζε θα αποφάσιζε να μην προμηθευτεί ποτέ ένα τέτοιο υλικό που είναι φτιαγμένο από χαμηλής ποιότητας υλικά και επηρεάζει την ασφάλεια του προς το χειρότερο [34].

Συνεπώς, οι αποφάσεις που πρέπει να λάβει ο παίχτης 2, είναι αν θα αγοράσει ή αν δεν θα αγοράσει το υλικό. Στο παρακάτω πίνακα απεικονίζεται η μήτρα των αποτελεσμάτων για το παράδειγμα επιλογής ποιότητας «ασφάλειας υλικού». Οι αριθμοί μας δείχνουν τα πιθανά κέρδη του κάθε παίχτη (πχ μηνιαίως) κι είναι εκφρασμένα σε δεκάδες δολάρια.

Πίνακας 7 Μήτρα αποτελεσμάτων

	Παίχτης 2	
Παίχτης 1	Αγοράζει	Δεν αγοράζει
Υψηλή ποιότητα ασφαλείας	2, 2	0, 3
Χαμηλή ποιότητα ασφαλείας	3, 0	1, 1

Στον παραπάνω πίνακα, βλέπουμε τις ανταμοιβές σε μια κατάσταση σαν αυτή που περιγράψαμε στην προηγούμενη παράγραφο. Όπως φαίνεται σε αυτήν την απεικόνιση ο παίχτης 1 προτιμάει να πουλάει χαμηλή ποιότητα ασφάλειας. Αυτό το καταλαβαίνουμε κατευθείαν από το συμβάν πως αν ο παίχτης 2 αποφασίσει να αγοράσει, το κέρδος του παίχτη 1, αυτομάτως από την στρατηγική του κίνηση να κατασκευάζει και να πουλάει χαμηλής ποιότητας υλικά (όφελος 3), είναι περισσότερο από το αντίστοιχο της υψηλής ποιότητας υλικό (όφελος 2), που παρέχει και μεγαλύτερη ασφάλεια.

Το ίδιο συμβαίνει και στην στρατηγική κίνηση του παίχτη 2, «δεν αγοράζει». Αυτό εξηγείται από την απόφαση του παίχτη 1 που είναι και πάλι να κατασκευάσει υλικό με χαμηλή ποιότητα ασφάλειας (1>0). Έτσι, συμπεραίνουμε ότι η στρατηγική απόφαση του παίχτη 1 να κατασκευάζει και να πουλάει υλικά χαμηλής ποιότητας

ασφαλείας, κυριαρχεί έναντι των υλικών υψηλής ποιοτικής κατασκευαστικής ασφάλειας. Συνεπώς, η κυριαρχική στρατηγική του παίχτη 1 είναι να πουλάει χαμηλή ποιότητα.

Από την άλλη πλευρά, όντας ο παίχτης 1 ως ορθολογιστής, ο παίχτης 2 γνωρίζει πως πάντα θα πουλάει ο παίχτης 1 χαμηλής ποιότητας ασφάλεια στο υλικό του, κι έτσι καταλαβαίνει πως από τον συγκεκριμένο κατασκευαστή η προσφερόμενη ασφάλεια υλικού θα είναι χαμηλή. Γνωρίζοντας λοιπόν αυτό, ο παίχτης 2 δεν θα αγοράζει από τον παίχτη 1, γιατί αν πράττει κάτι τέτοιο δεν θα έχει κανένα κέρδος, έναντι της αμοιβής 1 που είναι το κέρδος του όταν δεν αγοράζει από τον παίχτη 1. Επομένως, μέσω της ορθολογικής στρατηγικής απόφασης και σκέψης των παιχτών καταλήγουμε στο συμπέρασμα ότι παίχτης 1 θα παράγει χαμηλής ποιότητας ασφάλεια στο υλικό του, οπότε δεν θα υπογραφεί καμία σύμβαση μεταξύ τους στο τέλος.

Αν αποφασίζαμε να αυξήσουμε την χρησιμότητα της επιλογής από τον παίχτη 2 ως προς την υψηλή ποιότητα ασφάλειας, αυτό δεν θα μας έδινε καμία αντίδραση στο παίγνιο. Όμως αν ο κατασκευαστής του υλικού είχε ως κίνητρο την βελτιστοποίηση της ποιότητας του υλικού ως προς την ασφάλεια, μόνο τότε θα μπορούσε να υπάρξει κάποιας μορφής αντίδραση. Σε αυτές τις περιπτώσεις όμως είναι που μπορούμε να συναντήσουμε τις λεγόμενες ρήτρες απαλλαγής από την πλευρά των κατασκευαστών, προς την πλευρά των τελικών χρηστών, όπου ο πελάτης θα μπορεί να διακόψει την χρήση του υλικού λόγο χαμηλής ποιότητας και ελλιπής παροχής ασφάλειας στην εκάστοτε συσκευή (ρήτρα opt-out) [34].

Στον παρακάτω πίνακα απεικονίζεται το πρόβλημα που προέρχεται από τις ρήτρες απαλλαγής λόγο χαμηλής αξιοπιστίας του υλικού από την πλημμελή ασφάλεια του.

Πίνακας 8 Αποτελέσματα στο πρόβλημα επιλογής ποιότητας με ρήτρα απαλλαγής

	Παίχτης 2	
Παίχτης 1	Αγοράζει	Δεν αγοράζει
Υψηλή ποιότητα ασφαλείας	2, 2	0, 1
Χαμηλή ποιότητα ασφαλείας	1, 0	1, 1

Αυτή η αλλαγή που βλέπουμε στο παραπάνω πίνακα, είναι η απεικόνιση του παίγνιου που προκύπτει μέσα από την εναλλαγή των ποιοτήτων ασφάλειας με την ρήτρα opt-out, προς όφελος του χρήστη. Σε μια τέτοια διαδικασία βλέπουμε πως η

πώληση ενός υλικού χαμηλής ποιότητας ασφαλείας, ακόμα κι αν αποφασίσει ο πελάτης να το αγοράσει, δίνει το ίδιο όφελος στον κατασκευαστή όπως και στον χρήστη όταν δεν υπογράψει τη σύμβαση στην πρώτη θέση (ανταμοιβή 1), αφού θα έχει την δυνατότητα να αποφασίσει μεταγενέστερα.

Πάρα ταύτα παρατηρούμε πως ο τελικός αγοραστής επιθυμεί να αγοράσει το υλικό χαμηλής ποιότητας σε ασφάλεια, λόγο του ότι προτιμά την χαμηλή τιμή αγοράς. Αυτό μπορούμε να πούμε πως οφείλεται στο ότι ο χρήστης δεν θέλει να εμπλακεί σε θέματα που επιφέρουν περαιτέρω ταλαιπωρία κατά την σύναψη και την υπογραφή της σύμβασης. Προτιμά την απεμπλοκή του από αυτές τις διαδικασίες, για να μην ταλαιπωρείτε από γραφειοκρατικές πράξεις.

Επεξηγώντας το παραπάνω παίγνιο, καταλαβαίνουμε ότι δεν έχει και για τους δυο παίχτες κυριαρχούμενη στρατηγική. Ο κάθε παίχτης στο συγκεκριμένο παίγνιο διαλέγει την τακτική του ντετερμινιστικά, καθώς το παίγνιο έχει δυο ισορροπίες κατά Nash. Στην πρώτη απόφαση έχουμε την επιλογή της στρατηγικής «χαμηλή ποιότητα ασφαλείας» - «δεν αγοράζει», ενώ στην δεύτερη την επιλογή της συνδυαστικής στρατηγικής που παρουσιάζεται ως «υψηλή ποιότητα ασφαλείας» - «αγοράζει». Και στις δυο αυτές στρατηγικές περιπτώσεις έχουμε ισορροπίες, αφενός γιατί ο κατασκευαστής (παίχτης 1) πουλάει υψηλής ποιότητας ασφάλεια στο υλικό όταν αγοράζει ο χρήστης, κι αφετέρου αντίστροφα όταν ο χρήστης (παίχτης 2) δείχνει την επιθυμία να αγοράζει όταν του παρέχεται υλικό με υψηλή ποιότητα ασφάλειας.

Καταλαβαίνουμε λοιπόν, μέσα από το παράδειγμα μας, πως μια ισορροπία κατά Nash είναι μοναδική. Και στις δυο περιπτώσεις βέβαια έχουμε ξεκάθαρους κανόνες προς τους παίχτες για το πώς θα εξελιχθεί και θα παιχθεί το παίγνιο, καθώς οι ισορροπίες αποτελούν νόμιμες συστάσεις. Όταν οι δυο παίχτες έχουν αποφασίσει κι έχουν καταστρώσει την στρατηγική τους που επιφέρει ισορροπία κατά Nash, τότε κάνεις από του παίχτες δεν βρίσκει το κίνητρο να παρεκκλίνει της στρατηγικής του [34].

Τώρα στην περίπτωση που κάποιος από τους δυο παίχτες αποφασίσει να παρεκκλίνει της στρατηγικής του, τότε αυτομάτως αυτός ο παίχτης μειώνει το όφελος του. Οπότε οι παίχτες οφείλουν να παραμένουν πιστοί στις ορθολογικές τους στρατηγικές αποφάσεις, καθώς η ισορροπία κατά Nash προσφέρει μια αξιόπιστη και ακριβής λύση στα παίγνια. Αντιθέτως, από την άλλη πλευρά, μια συνδυαστική στρατηγική απόφαση που δεν αποτελεί και δεν επιφέρει ισορροπία κατά Nash, δεν μπορεί να θεωρηθεί και να είναι μια αξιόπιστη λύση.

Επομένως, τέτοιες στρατηγικές αποφάσεις στο παίγνιο δεν προτείνονται, δεδομένου πως ένας παίχτης τουλάχιστον θα παρακάμψει πιθανόν τις συμβουλές και θα αποφασίσει να παίξει με τέτοιο τρόπο που θα του επιφέρει μεγαλύτερο όφελος για τον ίδιο.

Τέλος, επειδή ποτέ δεν θα γίνεται να υπάρχει μια ισορροπία σε μια κυριαρχούμενη στρατηγική, καθώς αυτός που την επιλέγει την κυρίαρχη στρατηγική, πάντα θα βρίσκεται σε υψηλότερη θέση και με μεγαλύτερο όφελος. Έτσι, κατά αυτόν το τρόπο συμπεραίνουμε πως για να οδηγηθούμε σε μια ισορροπία κατά Nash, πρέπει να μην υπάρχουν κυριαρχούμενες στρατηγικές, που θα επιφέρουν το παίγνιο σε ένα στρατηγικό συνδυασμό «μοναδικό».

5.2.4 Επαναλαμβανόμενα παίγνια

Σε προηγούμενη ενότητα αναλύσαμε περισσότερο εμπεριστατωμένα το δίλλημα του φυλακισμένου κι αναδείξαμε πως η μεγιστοποίηση του ατομικού κέρδους δεν μεγιστοποιεί και δεν ωφελεί απαραιτήτως και το κέρδος μιας ομάδας και μιας συλλογικής προσπάθειας. Το παιχνίδι όταν παίζεται με την στρατηγική του διλλήματος του φυλακισμένου είναι ένα παίγνιο αποτελούμενο από κινήσεις ταυτόχρονες. Όμως όταν το παίγνιο παίζεται πολλές φορές, λέμε πως οδεύει στο άπειρο, και τα πράγματα περιπλέκονται περισσότερο.

Οι παίχτες αποκτούν επικοινωνία μεταξύ τους κι έτσι δύναται η επικοινωνία αυτή να επιφέρει και διαφορετικές αποφάσεις και στρατηγικές κινήσεις, που εξαρτώνται από προηγούμενες αποφάσεις/κινήσεις που έκανε ο κάθε παίχτης, κατά την διάρκεια του συγκεκριμένου παίγνιου. Έτσι, μεγαλώνει το πλήθος των αποφάσεων που μπορεί να πάρει ο κάθε παίχτης, με αποτέλεσμα αυτό να είναι ικανό από μόνο του να διαφοροποιεί και να τροποποιεί την έκβαση του αποτελέσματος του παίγνιου.

Αναλύοντας λίγο περισσότερο και για να καταλάβουμε σε ένα επαναλαμβανόμενο παίγνιο, πως επέρχεται το τελικό αποτέλεσμα, στο δίλλημα του φυλακισμένου ορίζουμε τον παρακάτω πίνακα 9 αποδόσεων.

Πίνακας 9 Μήτρα ενός παίγνιου μηδενικού αθροίσματος

	ΠΑΙΧΤΗΣ 2		
ΠΑΙΧΤΗΣ 1	B1	B2	B3
A1	-3	-2	3
A2	1	0	1
A3	2	-2	-3

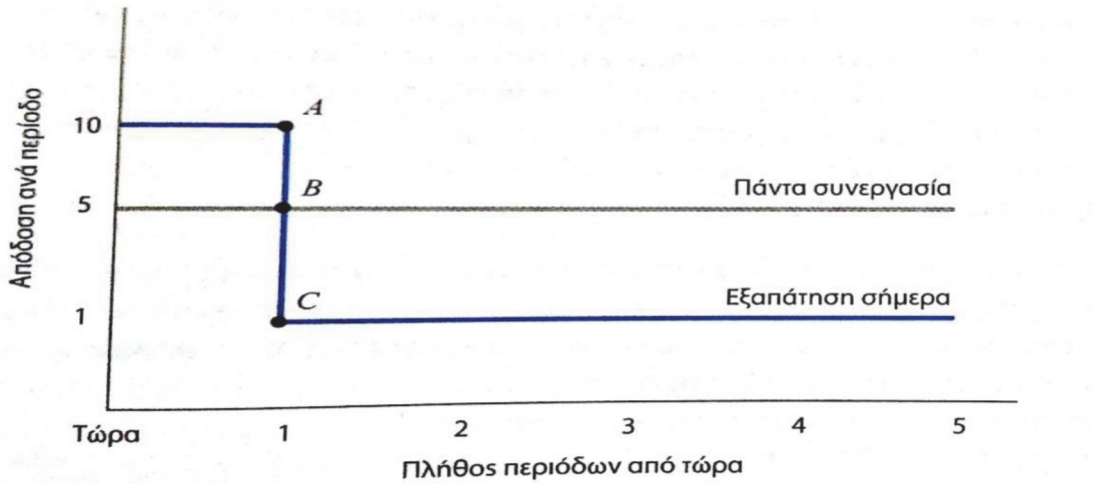
Η κυρίαρχη στρατηγική του κάθε παίχτη είναι να αποκαλύψει το λάθος του, όμως το μεγαλύτερο κέρδος των παιχτών έρχεται μέσα από την συμφωνία να συνεργαστούν και να ομολογήσουν το έγκλημά τους. Γι' αυτό όταν οι παίχτες αποφασίσουν να ομολογήσουν το έγκλημά τους σε ένα παιχνίδι ταυτόχρονης κίνησης, τότε προκύπτει η ισορροπία κατά Nash.

Αν τώρα εμβαθύνουμε λίγο περισσότερο και μπούμε στην διαδικασία να θεωρήσουμε ότι το παιχνίδι επαναλαμβάνεται συνεχώς, τότε ξεκινάει να φαίνεται και μια νέα επιλογή στις αποφάσεις των παιχτών, αυτή της «συνεργασίας» ανάμεσα στους παίχτες που συμμετέχουν, χωρίς φυσικά να μπορεί να αποφευχθεί να υπάρξει και το σενάριο της προδοσίας όπως είπαμε και παραπάνω.

Αναλύοντας περισσότερο το λόγο που συμβαίνει αυτό αρκεί να αναφέρουμε ότι ο παίχτης 1 νομίζει ή θέλει να πιστεύει ότι ο παίχτης 2 θα ακολουθήσει την στρατηγική, όπως αναλύεται παρακάτω:

Ξεκινώντας αποφασίζει την στρατηγική της «ομολογίας» και την ακολουθεί την απόφασή του αυτή, πιστεύοντας πως και ο παίχτης 2 θα επιλέξει την στρατηγική της «ομολογίας». Όταν όμως ο παίχτης 1 ανακαλύψει, την στιγμή που ο παίχτης 2 για πρώτη φορά εγκαταλείπει την στρατηγική της «ομολογίας», τότε και ο παίχτης 1 θα αποφασίσει όταν έρθει η σειρά του να μην ακολουθήσει κι αυτός την στρατηγική απόφαση της «ομολογίας», και για την συγκεκριμένη στιγμή που θα το καταλάβει, αλλά και για όλες τις επόμενες αποφάσεις του που θα ακολουθήσουν.

Η απόφαση αυτή του παίχτη 1 μπορεί να ονομαστεί και ως στρατηγική πυροδότησης της μη συνεργασίας, καθώς όταν ο απέναντι παίχτης αποφασίζει να αλλάξει την απόφασή του για συνεργασία, αυτό συνήθως προκαλεί την διάλυση της «συνεργασίας» μεταξύ των παιχτών, για όλη την περαιτέρω εξέλιξη του παίγνιου.



Εικόνα 16 Στρατηγική πυροδότησης της συνεργασίας [36]

Στην παραπάνω εικόνα φαίνεται το τι συμβαίνει όταν ο παίχτης 2 αλλάξει την στρατηγική της «ομολογίας», επιδεχόμενος αποδόσεις όπως αποτυπώνονται με την ανοιχτόχρωμη γραμμή. Αν όμως ακολουθήσει πιστά την στρατηγική της «ομολογίας», επιδέχεται μια ομαλή ροή αποδόσεων όπως αυτή αποτυπώνεται στην παραπάνω εικόνα. Το εφάπαξ κέρδος του παίχτη που εξαπάτησε, αποτυπώνεται από την απόσταση μεταξύ Α και Β. Η απόσταση μεταξύ των γραμμών Β και C, αποδεικνύει την μείωση του παίχτη που εξαπάτησε, και σε κάθε κέρδος που προκύπτει από τις μελλοντικές αποδόσεις, γιατί κι ο εξαπατημένος παίχτης αντίκειται και εξαπατάει κι αυτός απέναντι στην αδικία που νιώθει.

Προσπαθώντας τώρα, να απαντήσουμε στο ερώτημα ποια στρατηγική είναι αποδοτικότερη, χωρίς περαιτέρω πληροφορίες για το πώς αξιολογεί ο εκάστοτε παίχτης τα κέρδη και τις αποδόσεις, δεν μπορεί αυτό το ερώτημα να απαντηθεί με σιγουριά και βεβαιότητα. Εξαρτάται καθαρά από το που μπορεί να δίνει προτεραιότητα ο κάθε παίχτης, όσον αφορά τα οφέλη του. Αν π.χ. πούμε ότι ο παίχτης 1 ενδιαφέρεται περισσότερο για τις μελλοντικές αποδόσεις παρά για τις τρέχουσες, θα έδινε μεγαλύτερη βαρύτητα στην συνεργασία παρά στην εξαπάτηση.

Η στρατηγική του να κρατήσει κάποιος παίχτης το στόμα του κλειστό την πρώτη φορά που θα παίξει, είναι η καλύτερη απόφαση όσον αφορά την «συνεργασία», γιατί με αυτήν τη τακτική μας δίνετε η δυνατότητα να μπορούμε να επαναλαμβάνουμε την κίνηση του αντίπαλου σε κάθε επόμενη φορά. Συνεπώς, αυτή η τακτική κίνηση είναι καλύτερη ακόμα και από την απόφαση πυροδότησης του παίγνιου. Στόχος μιας

τέτοιας στρατηγικής απόφασης όπως η παραπάνω είναι να τιμωρείται η εξαπάτηση και να πριμοδοτείτε η «συνεργασία». Αυτό που φαίνεται στην εικόνα 16, πέραν της αρχικής μείωσης του κέρδους (απόσταση μεταξύ των γραμμών B και C), είναι και το κίνητρο που δίνεται στον παίχτη να συνεχίσει να συνεργάζεται.

Μέσα από την παραπάνω ανάλυση, μας δίνεται η δυνατότητα να μπορούμε να αναφέρουμε και να προτείνουμε κάποιες συμπεριφορές και στρατηγικές κινήσεις που προάγουν την «συνεργασία» σε ένα επαναλαμβανόμενο παίγνιο διλλήματος. Έτσι, καταλήγουμε στο ότι είναι καλό οι παίχτες να είναι υπομονετικοί, να επικοινωνούν μεταξύ τους, η εξαπάτηση να γίνεται γρήγορα αντιληπτή, καθώς κι ότι το εφάπαξ κέρδος της εξαπάτησης είναι ελάχιστο μπροστά στην ευημερία και τα οφέλη της «συνεργασίας» [34].

5.2.5 Μεικτές στρατηγικές

Οι μεικτές στρατηγικές είναι μια συνέχεια των αμιγώς καθαρών στρατηγικών, των παραπάνω παίγνιων που αναλύσαμε, καθώς τα επίπεδα ασφαλείας εμπεριέχουν και μια αποδεκτή απώλεια κατά την διάρκεια του παιχνιδιού για τους παίχτες. Αν προσπαθήσουμε να ορίσουμε έναν πίνακα απωλειών [A,B] στο παίγνιο, με αυτόν το τρόπο θέτουμε ($1^{ον}$) το επίπεδο ασφαλείας ή ($2^{ον}$) την υψηλότερη απώλεια ή ($3^{ον}$) την χαμηλότερη απώλεια, για τον παίχτη 1, όπου αυτό ορίζεται ακολούθως:

$$\bar{a}^* = \min_{x \epsilon X} \left\{ \max_{y \epsilon Y} a\ (x, y) \right\}.$$

Ενώ το αναμενόμενο επίπεδο ασφαλείας για τον παίχτη 2 ορίζεται ακολούθως:

$$\bar{\beta}^* = \min_{y \epsilon Y} \left\{ \max_{x \in X} \beta\ (x, y) \right\}.$$

Οι στρατηγικές αποφάσεις που λαμβάνονται κι οι οποίες επιφέρουν το επιθυμητό αποτέλεσμα, λέγονται στρατηγικές ασφαλείας των παιχτών και ορίζονται ως εξής:

$$\bar{a}^* = \left\{ \max_{y \in Y} a(\bar{x}, y) \right\}.$$

Και

$$\bar{\beta}^* = \left\{ \max_{x \in X} \beta(x, \bar{y} \right\}.$$

Επιδιώκοντας να βρούμε και να δούμε την υψηλότερη ασφάλεια υλικού του παίχτη 1 σε μικτές στρατηγικές, αναζητούμε την τιμή:

$$\min_{x\epsilon X}\left\{\max_{y\epsilon Y} a\,(x,y)\right\}.$$

Και πιο συγκεκριμένα για το παράδειγμά μας:

$$a(x,y) = (-5x_1 + 1)y_1 + x_1 - 1.$$

Καθώς είναι γραμμικό ως προς το y1, και με δεδομένο το εσωτερικό πρόβλημα μεγιστοποίησης το x1, γίνεται:

$$x_1 - 1 + \max_{0\le y_1\le 1}(-5x_1 + 1)\,y_1.$$

Όπου έχουμε δυο περιπτώσεις να ασχοληθούμε και να αναλύσουμε:

- $(-5x_1 + 1) \ge 0, \text{ή } \chi_1 \le 1/5$

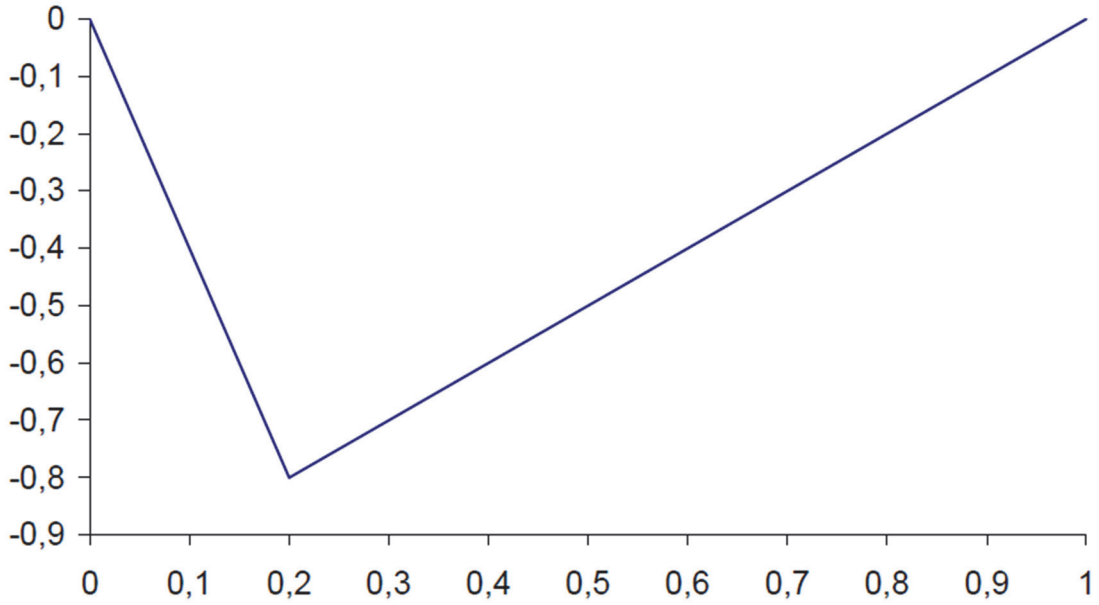
Και

- $(-5x_1 + 1) \le 0, \text{ή } x_1 \ge 1/5$

Στην πρώτη περίπτωση φαίνεται πως έχουμε υψηλότερο επίπεδο ασφάλειας για τιμή y1=1, ενώ για την δεύτερη περίπτωση έχουμε τιμή y1=0 για το y1. Κάνοντας χρήση λοιπόν, αυτών των τιμών, το εσωτερικό πρόβλημα παραλείπεται και παραμένει μόνο το εξωτερικό πρόβλημα, παίρνοντας την μορφή της παρακάτω συνάρτησης:

$$min\begin{cases} -4\chi_1, \alpha\nu\ 0\ \le \chi_1 \le \dfrac{1}{5} \\ x_1 - 1, \alpha\nu\ \dfrac{1}{5} \le \chi_1 \le 1 \end{cases}$$

Στην παρακάτω εικόνα φαίνεται η συνάρτηση όπου στο σημείο χ1=1/5 μειώνεται η τιμή και τα επίπεδα ασφαλείας είναι χ2= -4/5 και χ2=4/5.



Εικόνα 17 Επίπεδα ασφαλείας παίκτη 1

Ομοίως υπολογίζεται και για τον δεύτερο παίχτη το επίπεδο ασφάλειας. Οι μικτές στρατηγικές και του δεύτερου παίχτη είναι οι y1 = 4/5 και y2 = 1/5 και το επίπεδο ασφαλείας της είναι –4/5. Βλέπουμε λοιπόν, πως τα επίπεδα ασφαλείας (4/5, 4/5) είναι ένα αποτέλεσμα παρεμφερές με το αποτέλεσμα που προέρχεται από την ισορροπία κατά Nash σε μικτές στρατηγικές. Αν τελικώς οι στρατηγικές Nash χρησιμοποιηθούν, θα μας δώσουν αποτελέσματα ίσα με αυτά που είδαμε παραπάνω. Όμως το ότι μπορεί να έχουμε τα ίδια επίπεδα ασφαλείας και να μας δίνουν συγχρόνως και τις ίδιες απώλειες, χρησιμοποιώντας τις στρατηγικές Nash, αυτό δεν μπορεί να συμβαίνει πάντα.

Οι παίχτες που λαμβάνουν μέρος στα παίγνια με πίνακες απώλειας, τα επίπεδα ασφαλείας δεν είναι τόσο αισιόδοξα, γιατί αν οι συμμετέχοντες αποφασίσουν να παίξουν με στρατηγικές ασφαλείας και οδηγούνται σε απώλειες που είναι μη αναμενόμενες και πολύ χαμηλότερες από αυτό που αναμένουν για τα επίπεδα ασφάλειας τους. Ένα τέτοιο φαινόμενο μπορεί να χαρακτηριστεί ως παράδοξο, κι αυτό ωφελείται στην μέθοδο των διμητρικών παιχνιδιών.

Αυτό αναλυτικότερα εξηγείται από το ότι ο παίχτης 1 υπολογίζει περισσότερο την ασφάλεια, σκεπτόμενος τον παίχτη 2 κι ότι αυτός θα θέλει να του μεγιστοποιήσει την απώλεια, κάτι το οποίο γίνεται σε ένα παίγνιο μηδενικού αθροίσματος, αλλά δεν ισχύει στην προκείμενη περίπτωση των διμητρικών παιχνιδιών. Στην συγκεκριμένη περίπτωση των διμητρικών παιχνιδιών ο παίχτης 2 έχει ως βασική του προϋπόθεση να ελαχιστοποιήσει την απώλεια του κι όχι την απώλεια του παίχτη 1.

5.3 Ανίχνευση hardware trojans μέσω της θεωρίας παίγνιων

5.3.1 Επιθέσεις στο υλικό μέσω HTs

Η απειλή των HTs υλικού έχει γίνει πιο έντονη λόγω της μαζικής εξωτερικής ανάθεσης των διαδικασιών κατασκευής ολοκληρωμένων κυκλωμάτων (μοντέλο χωρίς εργοστάσιο), καθώς και λόγω της αυξημένης εξάρτησης από εξαρτήματα υλικού COTS. Ένα καλό παράδειγμα του τελευταίου είναι τα παλαιά στρατιωτικά συστήματα, συμπεριλαμβανομένων των αεροδιαστημικών και αμυντικών πλατφόρμων, τα οποία αντιμετωπίζουν την απαξίωση λόγω της παρατεταμένης διάρκειας ζωής τους (π.χ., συχνά λόγω δημοσιονομικών αποφάσεων) και τα οποία βασίζονται στη χρήση COTS για τη συντήρηση και την αντικατάσταση των ηλεκτρονικών τους.

Οι περισσότεροι σχεδιαστές τσιπ έχουν πλέον εγκαταλείψει το εργοστάσιό τους, αναθέτοντας την κατασκευή τους σε εξωχώρια χυτήρια. Με τον τρόπο αυτό, αποφεύγουν το τεράστιο κόστος της κατασκευής ενός υπερσύγχρονου εργοστασίου. Η κατασκευή των υλικών συχνά δίνεται σε χυτήρια στο εξωτερικό. Αυτό δίνει πολλές δυνατότητες σε πιθανούς επιτιθέμενους να τροποποιήσουν κακόβουλα το κύκλωμα του ολοκληρωμένου κυκλώματος και να εισάγουν δούρειους ίππους υλικού.

Οι δούρειοι ίπποι υλικού έχουν σχεδιαστεί για να είναι αθόρυβοι. Μπορούν να είναι πολύ μικρά (π.χ. να αποτελούνται από λίγα μόνο τρανζίστορ), ώστε να αποφεύγουν τις φυσικές επιθεωρήσεις και τις αναλύσεις πλευρικών καναλιών των τσιπ. Επιπλέον, ενεργοποιούνται συνήθως από σπάνιες συνθήκες, ώστε να περνούν τις δοκιμές λειτουργίας. Ακόμα και αν ένα Trojan είναι φυσικά πολύ μικρό, μπορεί να έχει σοβαρές επιπτώσεις, από την απενεργοποίηση ή την καταστροφή του τσιπ μέχρι την ενεργοποίηση κερκόπορτας ή τη μετάδοση εμπιστευτικών πληροφοριών [38].

5.3.2 Κύριες τεχνικές για την ανίχνευση δούρειων ίππων υλικού

Οι κύριες τεχνικές που χρησιμοποιούνται για την ανίχνευση δούρειων ίππων υλικού είναι η φυσική επιθεώρηση, η πλευρική ανάλυση καναλιών, οι μηχανισμοί χρόνου εκτέλεσης και ο έλεγχος λογικής.

Η φυσική επιθεώρηση (που αποκαλείται επίσης καταστροφική αντίστροφη μηχανική ή οπτική αντίστροφη μηχανική) συνίσταται στην ανάλυση του κατασκευασμένου τσιπ με αντίστροφη μηχανική (αποσυσκευασία, απομετάλλωση, μικροφωτογραφία).

Η ανάλυση πλευρικού καναλιού αποσκοπεί στη μέτρηση και ανάλυση των παραμέτρων πλευρικού καναλιού μιας διάταξης, όπως το ρεύμα τροφοδοσίας ή η

καθυστέρηση διαδρομής, ώστε να αποκαλυφθούν ακούσιες τροποποιήσεις στο κύκλωμα.

Οι μηχανισμοί χρόνου εκτέλεσης αποσκοπούν στην ανίχνευση δούρειων ίππων υλικού κατά την εκτέλεση, ενώ το σύστημα βρίσκεται σε λειτουργία, χρησιμοποιώντας συνήθως τεχνικές που βασίζονται στην online παρακολούθηση κρίσιμων λειτουργιών.

Ο έλεγχος λογικής (όπως εφαρμόζεται στην ανίχνευση Trojan) αποσκοπεί στην ανάπτυξη μοτίβων ελέγχου που μπορούν να ενεργοποιήσουν Trojans και να μεταδώσουν τα αποτελέσματά τους στην έξοδο του κυκλώματος. Η τιμή μιας εξόδου συγκρίνεται συνήθως με τη σωστή τιμή, όπως ορίζεται από τις λειτουργικές προδιαγραφές του κυκλώματος, έτσι ώστε να προκύψει ανίχνευση Trojan αν οι δύο τιμές διαφέρουν. Η δοκιμή ενός κυκλώματος με αυτόν τον τρόπο είναι επομένως μια μορφή λειτουργικής δοκιμής [38].

5.3.3 Διαμόρφωση παιχνιδιού ως ένα στατικό μη συνεργατικό παίγνιο

Σε αυτό το παιχνίδι, κάθε παίκτης θέλει να παίξει την καλύτερη δυνατή στρατηγική του ανάλογα με την αντίληψή του για την πιθανή στρατηγική του αντιπάλου του. Οι στρατηγικές που χρησιμοποιούνται και από τους δύο παίκτες καταλήγουν είτε να διαφθείρουν το IC είτε να επιβάλλουν πρόστιμο στον επιτιθέμενο. Εδώ, το παίγνιο θα μοντελοποιηθεί ως ένα στατικό μη συνεργατικό παίγνιο.

Θεωρούμε δύο παίκτες: τον επιτιθέμενο a και τον αμυνόμενο d σε ένα σύνολο N_P τέτοιο ώστε N_P:= {a, d}. Έστω το σύνολο S που αντιπροσωπεύει τους χώρους στρατηγικής S_d και S_a του αμυνόμενου και του επιτιθέμενου, αντίστοιχα. Αυτοί οι χώροι στρατηγικής αντιπροσωπεύουν όλες τις πιθανές ενέργειες των παικτών. Έστω το σύνολο U που αναπαριστά τις συναρτήσεις χρησιμότητας των παικτών U_d και U_a, για τον αμυνόμενο και τον επιτιθέμενο, αντίστοιχα. Τέλος, έστω το παίγνιο $G = \{N_P$, S, U$\}$.

Για τον επιτιθέμενο, ο χώρος στρατηγικών αποτελείται από όλα τα πιθανά είδη τροϊκανών που μπορούν να παιχτούν σε αυτό το παίγνιο, δηλαδή, S_a= T . Εδώ, κάθε στρατηγική στο χώρο στρατηγικών του επιτιθέμενου $s_a \in S_a$αναφέρεται σε ένα αντίστοιχο είδος trojan t ∈ T . Από την άλλη πλευρά, ο αμυνόμενος θα επιλέξει ένα υποσύνολο τύπων trojan. Έστω ότι ο αριθμός των trojans που μπορεί να ελέγξει ο αμυντικός ταυτόχρονα είναι K τύποι. Ο χώρος στρατηγικής του αμυνόμενου μπορεί τότε να είναι S_d που ορίζονται ως όλα τα πιθανά υποσύνολα του T με μέγεθος K, όπου $S_d=\binom{T}{K}$. Εδώ όπου στο χώρο στρατηγικής του αμυνόμενου $s_d \in S_d$.

Οι χρησιμότητες των παικτών μπορούν να προσδιοριστούν χρησιμοποιώντας την επιλογή στρατηγικής για s_a του επιτιθέμενου και την αντίστοιχη επιλογή στρατηγικής για s_d του αμυνόμενου, έτσι ώστε:

$$U_a(s_a, s_d) = \begin{cases} -Fs_a \ \alpha\nu \ s_a \in s_d \\ Vs_a \ \alpha\lambda\lambda\iota\acute{\omega}\varsigma: \end{cases}$$

Όπου V_{s_a} είναι η ανταμοιβή του επιτιθέμενου για το παίξιμο μιας συγκεκριμένης στρατηγικής s_a που δεν εντοπίστηκε από τη στρατηγική s_d του αμυνόμενου. -F_{s_a} είναι το πρόστιμο του επιτιθέμενου για το παίξιμο μιας συγκεκριμένης στρατηγικής που ανιχνεύθηκε. Το μέγεθος του V_{s_a} αντικατοπτρίζει το κέρδος της χρηματικής ανταμοιβής του επιτιθέμενου, το οποίο αντιστοιχεί επίσης στο είδος της ζημίας που μπορεί να προκαλέσει το trojan. Παρατηρούμε ότι το αποτέλεσμα του παιγνίου θα είναι είτε ένα πρόστιμο F_{s_a} που χρεώνεται από τον επιτιθέμενο και καταβάλλεται στον αμυνόμενο, είτε το κέρδος V_{s_a} του επιτιθέμενου που είναι η απώλεια του αμυνόμενου. Έτσι, το παίγνιο θα έχει χαρακτηριστικό μηδενικού αθροίσματος και η χρησιμότητα του αμυνόμενου μπορεί να δοθεί ως εξής:

$$U_d(S_a, S_d) = -U_a(S_a, S_d).$$

Τέλος, έστω P = $\{p_a, p_d\}$, που αντιπροσωπεύει την αντικειμενική κατανομή πιθανοτήτων μικτής στρατηγικής για τον επιτιθέμενο και τον αμυνόμενο αντίστοιχα, επί των ενεργειών τους.

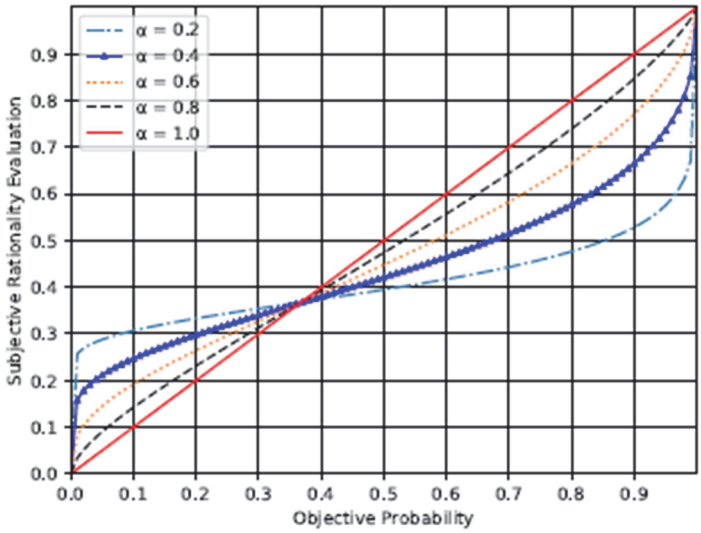
Στη συνέχεια, μελετάμε την επίδραση της θεωρίας προοπτικών (PT) στις χρησιμότητες των παικτών. Σύμφωνα με την PT, οι παίκτες παρεκκλίνουν από τις πιο ορθολογικές στρατηγικές τους όταν αντιμετωπίζουν αβεβαιότητες σχετικά με τις στρατηγικές ή αν υπάρχουν περιορισμοί στην άσκηση μιας συγκεκριμένης στρατηγικής που δεν λαμβάνονται υπόψη κατά τη διάρκεια του παιχνιδιού. Σύμφωνα με την PT, οι παίκτες έχουν μια υποκειμενική ορθολογικότητα των στρατηγικών του αντιπάλου και, ως εκ τούτου, αλλάζουν τις αναμενόμενες χρησιμότητες από αντικειμενικές σε υποκειμενικές.

Στο παίγνιο μας, και οι δύο παίκτες αντιμετωπίζουν αβεβαιότητα όσον αφορά τις στρατηγικές του αντιπάλου. Για τον επιτιθέμενο, δεν είναι απολύτως σίγουρος για τη στρατηγική δοκιμής που θα εφαρμόσει ο αμυνόμενος. Ως εκ τούτου, μπορεί να τείνει να υποτιμά ή να υπερτιμά μια συγκεκριμένη στρατηγική του αντιπάλου του. Η ίδια υπόθεση μπορεί να γίνει και για τον αμυνόμενο. Επίσης, δεδομένου ότι και οι δύο παίκτες είναι άνθρωποι, θα μπορούσαν να υπάρχουν πολλαπλοί λόγοι για την

υποκειμενικότητα: κανονισμοί της εταιρείας, απαίτηση περισσότερων πόρων για την αναπαραγωγή ενός συγκεκριμένου trojan, μη επαρκείς πόροι για τη δοκιμή ορισμένων trojan κ.λπ.

Προκειμένου να καταγραφεί η απόκλιση από τη βέλτιστη στρατηγική για κάθε παίκτη, ενσωματώνεται μια επίδραση στάθμισης w. Σύμφωνα με αυτό το αποτέλεσμα στάθμισης w, οι παίκτες δίνουν υποκειμενική βαρύτητα στις στρατηγικές του αντιπάλου τους για μεγαλύτερη συνάφεια. Η επίδραση στάθμισης εξαρτάται από την παράμετρο ορθολογικότητας α(0, 1], η οποία κρίνει την υποκειμενική αντίληψη ενός παίκτη με βάση την αντικειμενική πιθανότητα. Μια ορθολογικότητα 1 σημαίνει ότι οι παίκτες παίζουν με πλήρη ορθολογισμό, δηλαδή με πλήρη αντικειμενικότητα. Το αποτέλεσμα στάθμισης ορίζεται χρησιμοποιώντας τη συνάρτηση Prelec, ως εξής:

$$w_i(p_i, a_i) = \exp\left(-(-\ln p_i)^{a_i}\right), 0 < a_i \leq 1$$



Εικόνα 18 Αντικειμενική πιθανότητα των παικτών σε σχέση με την υποκειμενική ορθολογική αξιολόγηση μιας στρατηγικής [37]

Σημειώστε ότι, η συνάρτηση Prelec χρησιμοποιείται ευρέως για τη μοντελοποίηση της υποεπιλεκτικότητας κατά τη μελέτη του ορθολογισμού. Η εικόνα 18 δείχνει την επίδραση του αi στην απόκλιση ενός παίκτη μεταξύ της αντικειμενικής πιθανότητας και της αντίστοιχης υποκειμενικής αξιολόγησης. Χρησιμοποιώντας τη συνάρτηση Prelec, η χρησιμότητα για κάθε παίκτη μπορεί στη συνέχεια να ενημερωθεί σε σχέση με την αντιλαμβανόμενη ορθολογικότητά του σχετικά με τις πιθανότητες του αντιπάλου του ως εξής:

$$U_i^{PT}(p_i, p_j a_i a_j) = \sum_{s=S_i} \left(p_i(s_i) w_i(p_j(s_j) | a_j, a_i)\right) u_i(s_i, s_j).$$

Το όπου τα i και j αντιστοιχούν σε έναν παίκτη σε αυτό το σενάριο.

Για να βελτιστοποιήσουν τις χρησιμότητές τους, οι παίκτες πρέπει να λάβουν υπόψη τους τόσο τις ενέργειές τους όσο και τις ενέργειες των αντιπάλων τους. Η λύση σε αυτή την περίπτωση, δίνεται από τη θεωρία παιγνίων ως το σημείο ισορροπίας. Οι λύσεις ισορροπίας, στη θεωρία παιγνίων, αποκαλούνται ως ισορροπία Nash, οι οποίες εμφανίζονται όταν κανένας παίκτης δεν μπορεί να βελτιώσει τη χρησιμότητά του αλλάζοντας μονομερώς τις ενέργειές του. Η ισορροπία Nash μπορεί να είναι είτε καθαρή ισορροπία Nash, όταν κάθε παίκτης επιλέγει μόνο μία ενέργεια, είτε ισορροπία Nash μεικτής στρατηγικής, η οποία είναι μια κατανομή πιθανότητας πάνω στο σύνολο των ενεργειών του παίκτη. Εδώ, εστιάζουμε στην ισορροπία Nash μικτής στρατηγικής και μελετάμε αυτή τη λύση ισορροπίας [37].

5.3.4 Διαμόρφωση παιχνιδιού για ένα επαναλαμβανόμενο παιχνίδι

Εδώ, εξετάζουμε την περίπτωση κατά την οποία ο κατασκευαστής επιστρέφει τα ολοκληρωμένα κυκλώματα στον σχεδιαστή σε πολλαπλές παρτίδες. Κάθε παρτίδα αποτελείται από πολλαπλά πανομοιότυπα ολοκληρωμένα κυκλώματα. Ο έλεγχος όλων των ολοκληρωμένων κυκλωμάτων σε μια παρτίδα, για όλους τους τύπους HT, είναι μια ανέφικτη διαδικασία για τον αμυνόμενο.

Επομένως, μια πολλά υποσχόμενη προσέγγιση για τον αμυνόμενο είναι να μάθει για τις στρατηγικές του επιτιθέμενου ελέγχοντας κάθε ένα ολοκληρωμένο κύκλωμα, για κάθε πιθανό HT, σε ένα αρχικό σύνολο παρτίδων για να καταλάβει τις πιθανολογικές προτιμήσεις του επιτιθέμενου. Στη συνέχεια, αυτή η γνώση θα χρησιμοποιηθεί για τον έλεγχο των HT σε επόμενες παρτίδες. Αυτό το σενάριο αντιπροσωπεύει ένα επαναλαμβανόμενο παίγνιο, το οποίο προτείνουμε να χωριστεί σε δύο ξεχωριστά στάδια: στάδιο εκμάθησης και στάδιο πραγματικού παιγνίου.

Στο πλαίσιο αυτού του σεναρίου, οι παίκτες θα αναλάβουν δράση στην αρχή κάθε σταδίου. Αυτές οι ενέργειες θα επηρεάσουν τα αποτελέσματά τους από όλες τις επόμενες παρτίδες. Έστω N το σύνολο των παρτίδων στο παιχνίδι. Για κάθε παρτίδα ο αμυντικός θα ελέγξει όλα τα ολοκληρωμένα κυκλώματα ανά παρτίδα, κι αυτό συμβολίζεται με C_L. Στο στάδιο του παιχνιδιού, ο αμυνόμενος θα επιλέξει τυχαία μερικά ICs ανά παρτίδα για δοκιμή, τα οποία συμβολίζονται με C_A έτσι ώστε $C_A < C_L$. Σε κάθε IC, κατά τη φάση του παιχνιδιού, ο αμυνόμενος θα αναζητήσει τον ίδιο αριθμό XTs, που δίνεται από το K. Ο αμυνόμενος θα επιλέξει N_L ως αριθμό παρτίδων

εκμάθησης και N_A ως αριθμό παρτίδων στη φάση του παιχνιδιού, όπου N_A= N - N_L. Η χρησιμότητα στο στάδιο μάθησης U_L θα υπολογιστεί από:

$$U_{L_i} = C_L U_i^{PT}(p_i, p_j, a_i, a_i).$$

Ομοίως, η χρησιμότητα στο πραγματικό στάδιο του παιχνιδιού θα δίνεται από:

$$U_{A_i} = C_A U_i^{PT}(p_i, p_j, a_i, a_j).$$

Η συνολική χρησιμότητα UT i ολόκληρου του παιγνίου θα δίνεται από:

$$U_{T_i} = U_{L_i} + U_{A_i},$$

όπου το i συμβολίζει έναν παίκτη σε αυτό το παίγνιο [37].

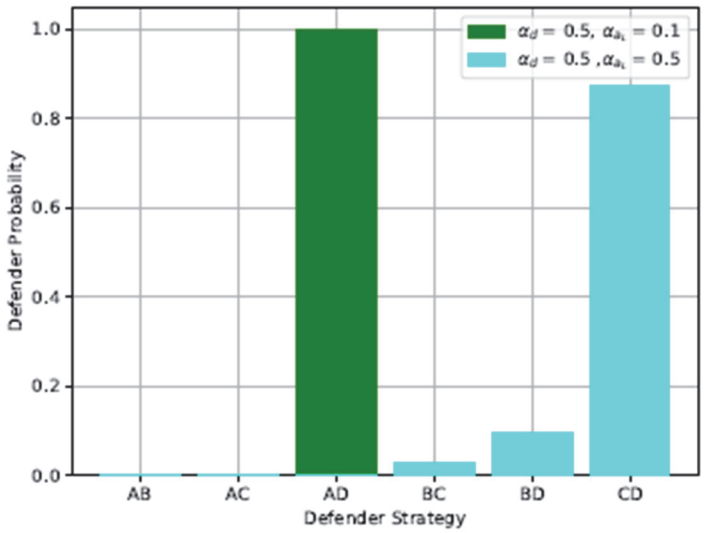
5.3.5 Αποτελέσματα προσομοίωσης και ανάλυση

Για τις προσομοιώσεις μας, υποθέτουμε ότι ο επιτιθέμενος έχει πρόσβαση σε 4 είδη trojans, έτσι ώστε ο χώρος στρατηγικής του επιτιθέμενου είναι S_A= T = {A,B,C,D}. Το κέρδος από κάθε trojan θεωρείται να είναι: V_A= 1, V_B= 2, V_C= 4, V_D= 12, που αντιστοιχεί σε στο μέγεθος της ζημίας που μπορεί να γίνει με το συγκεκριμένο trojan. Για τον αμυνόμενο, αφήνουμε K = 2, το οποίο συνήθως εξαρτάται από το τους πόρους που διαθέτει ο αμυνόμενος. Με βάση την τιμή του K, ο χώρος στρατηγικής S_D του αμυνόμενου θα αποτελείται από $\binom{4}{2}$= 6 με πιθανές στρατηγικές δοκιμής, δηλαδή {AB, AC, AD, BC, BD, CD}. Τέλος, το πρόστιμο του επιτιθέμενου F = [8,6,2,4] υποδηλώνει την ποινή για τον επιτιθέμενο σε περίπτωση επιτυχούς ανίχνευσης.

Ο πίνακας 10 δείχνει στρατηγικές και για τους δύο παίκτες και τις αντίστοιχες χρησιμότητές τους, στο στατικό παίγνιο. Δεδομένου ότι τα αποτελέσματα εναλλάσσονται μεταξύ θετικών και αρνητικών για κάθε παίκτη, δεν υπάρχει κυρίαρχη στρατηγική για κανέναν παίκτη. Η ισορροπία μεικτής στρατηγικής μπορεί στη συνέχεια να επιτευχθεί με την εκτέλεση του αλγορίθμου εικονικού παιχνιδιού. Αυτό απαιτεί την αρχικοποίηση των στρατηγικών πιθανοτήτων. Εδώ, χρησιμοποιούμε τις ίδιες αρχικές πιθανότητες. Για τον επιτιθέμενο, το αρχικό στρατηγικό προφίλ p_a= [0,2083, 0,1667, 0,3333, 0,2917] και για τον αμυνόμενο, το αρχικό στρατηγικό προφίλ p_d= [0,2051, 0.2564, 0.2564, 0.0513, 0.0513, 0.1795].

Πίνακας 10 Στρατηγικές σε στατικό παίγνιο

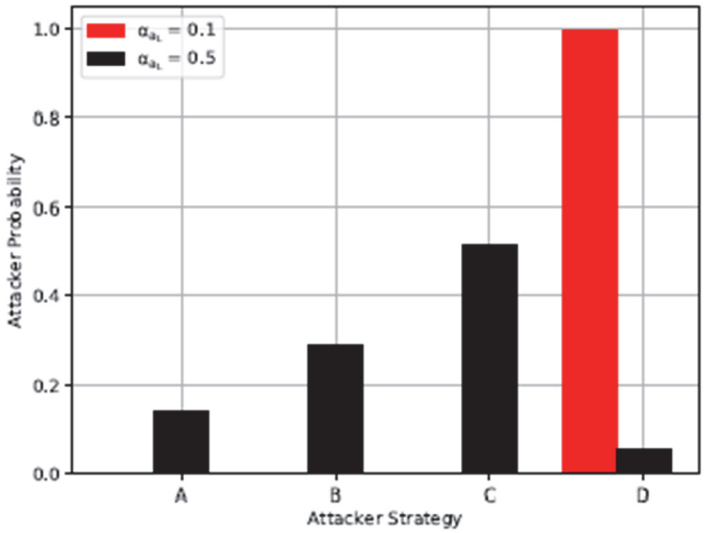
	Αμυνόμενος						
Επιτιθέμενος		AB	AC	AD	BC	BD	CD
	A	-8,8	-8,8	-8,8	1,-1	1,-1	1,-1
	B	-6,6	2,-2	2,-2	-6,6	-6,6	2,-2
	C	4,-4	-2,2	4,-4	-2,2	4,-4	-2,2
	D	12,-12	12,-12	-4,4	12,-12	-4,4	-4,4



Εικόνα 19 Στρατηγικές αμυνόμενου [37]

Για τον επιτιθέμενο, αφήνουμε την πραγματική ορθολογικότητά του a_{a_A} να είναι 0,5. Στη συνέχεια, εφαρμόζουμε το πρόβλημα εξαπάτησης για να υπολογίσουμε την ορθολογικότητα εξαπάτησης, δηλαδή την ορθολογικότητα που θα χρησιμοποιήσει ο επιτιθέμενος στο πραγματικό παίγνιο. Η βέλτιστη ορθολογικότητα εξαπάτησης του επιτιθέμενου υπολογίστηκε ότι είναι a_{a_L}= 0,1. Επομένως, ο επιτιθέμενος θα θέσει a_{a_L}= 0,1. Στη συνέχεια, εκτελούμε τον αλγόριθμο εικονικού παιχνιδιού όταν a_d= 0,5 και όταν a_{a_L} ισούται τόσο με 0,1 όσο και με 0,5. Η εικόνα 19 δείχνει το στρατηγικό προφίλ του αμυνόμενου, στην ισορροπία, και για τις δύο ορθολογικότητες του επιτιθέμενου. Από την εικόνα 19, βλέπουμε ότι όταν a_{a_L}= 0,1, ο αμυνόμενος θα επιλέξει τη στρατηγική AD με μεγάλη πιθανότητα. Ωστόσο, αυτό αλλάζει όταν η ορθολογικότητα του επιτιθέμενου αλλάξει σε a_{a_L}= 0,5, καθώς ο αμυνόμενος θα έχει μια πιο ευρεία κατανομή πιθανοτήτων [37].

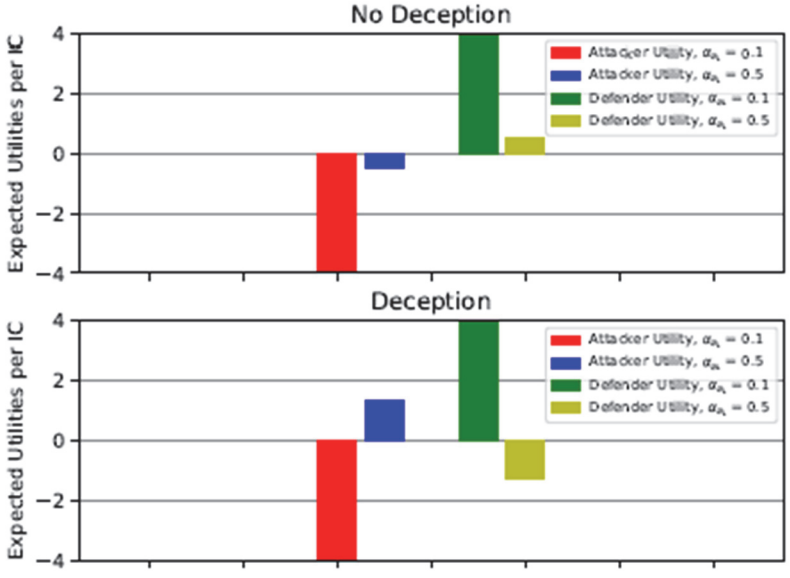
Ομοίως, η εικόνα 20 δείχνει το στρατηγικό προφίλ του επιτιθέμενου όταν a_d= 0,5 και όταν a_{a_L} είναι ίσο με 0,1 και 0,5. Βλέπουμε ότι για a_{a_L}= 0,1, ο επιτιθέμενος επιλέγει τη στρατηγική D.



Εικόνα 20 Στρατηγικές επιτιθέμενου [37]

Ομοίως, όταν a_{a_L}= 0,5, ο επιτιθέμενος έχει μια πιο κατανεμημένη πιθανότητα σε όλες τις στρατηγικές τους.

Στη συνέχεια μελετάμε τις χρησιμότητες των παικτών που υπολογίζονται με βάση τις στρατηγικές ισορροπίας στις εικόνες 19 και 20. Στην εικόνα 21 παρουσιάζονται οι χρησιμότητες των παικτών, για μία μόνο παρτίδα, σε δύο διαφορετικές συνθήκες: χωρίς εξαπάτηση και εξαπάτηση. Κατά τη διάρκεια της περίπτωσης χωρίς εξαπάτηση, το άνω μέρος της εικόνας 21, βλέπουμε ότι όταν ο επιτιθέμενος έχει ορθολογισμό a_{a_L}= 0,1, τόσο στο στάδιο της μάθησης όσο και στο στάδιο του πραγματικού παιχνιδιού, και ο αμυνόμενος έχει ορθολογισμό a_d= 0,5, ο επιτιθέμενος υφίσταται πλήγμα χρησιμότητας -3,9614854 ανά IC. Εν τω μεταξύ, ο αμυνόμενος λαμβάνει χρησιμότητα 3,9614854 ανά IC.

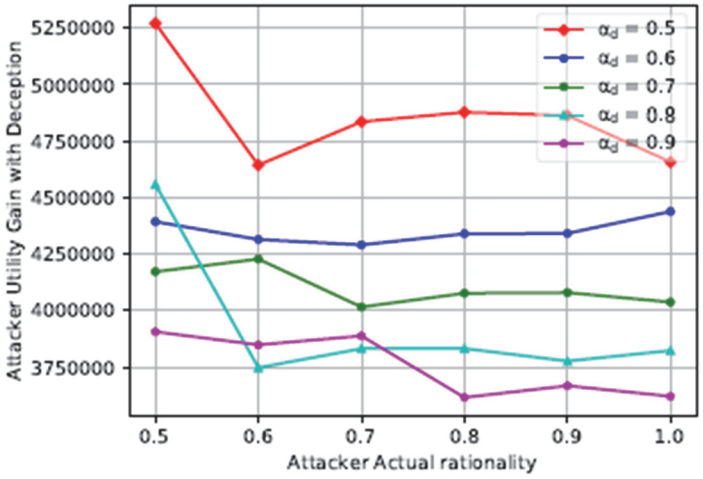


Εικόνα 21 Οι χρησιμότητες των παιχτών με εξαπάτηση και χωρίς εξαπάτηση [37]

Ομοίως, όταν ο επιτιθέμενος έχει ορθολογισμό a_{a_L}= 0,5, και στα δύο στάδια, ο επιτιθέμενος λαμβάνει ένα χτύπημα χρησιμότητας -0,4984252 ανά IC και ο αμυνόμενος λαμβάνει χρησιμότητα 0,4984252 ανά IC. Αυτό δείχνει ότι ο επιτιθέμενος θα υποστεί αρνητικό αποτέλεσμα όταν παίζει με τον ίδιο ορθολογισμό και στα δύο στάδια του παιχνιδιού, ανεξάρτητα από το αν έπαιζε υψηλή ή χαμηλή ορθολογικότητα. Αυτό οφείλεται στο γεγονός ότι, ο αμυντικός τυχαιοποιεί τις ενέργειές του και θα είναι σε θέση να ανιχνεύσει τα HTs με υψηλή πιθανότητα.

Από την άλλη πλευρά, σε περίπτωση εξαπάτησης, ο επιτιθέμενος παίζει χαμηλότερο επίπεδο ορθολογισμού a_{a_L} κατά τη διάρκεια του σταδίου εκμάθησης. Ο αμυνόμενος θα λάβει τις στρατηγικές του επιτιθέμενου που αντιστοιχούν σε a_{a_L}= 0,1 και έτσι θα παίξει το αντίστοιχο προφίλ. Ωστόσο, στο στάδιο του πραγματικού παιγνίου, ο επιτιθέμενος θα αλλάξει τη στρατηγική του στην πραγματική ορθολογικότητά του a_{a_A}= 0,5. Η περίπτωση αυτή παρουσιάζεται στο κάτω μέρος της εικόνας 21. Σε αυτή την περίπτωση, ο αμυνόμενος θα λάβει χτύπημα χρησιμότητας -1,3090019 ανά IC, ενώ ο επιτιθέμενος λαμβάνει κέρδος χρησιμότητας 1,3090019 ανά IC, το οποίο αντιπροσωπεύει την επιτυχία του επιτιθέμενου να εξαπατήσει τον αμυνόμενο [37].

Η συσσωρευμένη χρησιμότητα του επιτιθέμενου από το μοντέλο υπερπαιχνιδιού, παρουσιάζεται στην εικόνα 22. Αυτή η χρησιμότητα αντιπροσωπεύει το αποτέλεσμα του επιτιθέμενου όταν παίζει ορθολογικά.



Εικόνα 22 Επιτιθέμενος με συσσωρευμένη χρησιμότητα [37]

Δεδομένου ότι αυτή η χρησιμότητα εξαρτάται τόσο από την ορθολογικότητα του επιτιθέμενου όσο και από την ορθολογικότητα του αμυνόμενου, στην εικόνα 22 μελετάμε διαφορετικά σενάρια για την ορθολογικότητα των παικτών και πώς

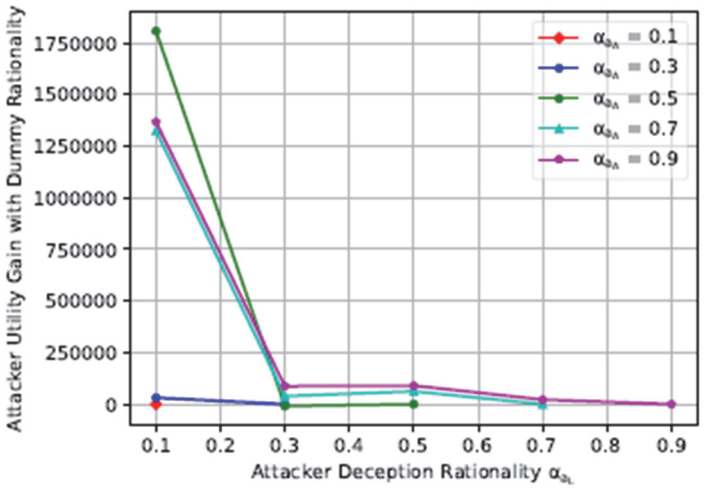
επηρεάζουν τη συσσωρευμένη χρησιμότητα του επιτιθέμενου. Από την εικόνα 22, βλέπουμε ότι το κέρδος χρησιμότητας του επιτιθέμενου θα είναι πάντα υψηλότερο όταν αντιμετωπίζει έναν αμυνόμενο με χαμηλότερη ή ίση ορθολογικότητα.

Για παράδειγμα, ένας επιτιθέμενος με πραγματική ορθολογικότητα 0,5 θα κερδίσει την υψηλότερη χρησιμότητα απέναντι σε έναν αμυνόμενο με ορθολογισμό 0,5. Το ίδιο παρατηρείται και για έναν επιτιθέμενο με πραγματική ορθολογικότητα 0,6 έναντι αμυνόμενων με ορθολογικότητες 0,5 και 0,6. Είναι ενδιαφέρον ότι, αν η ορθολογικότητα του αμυνόμενου είναι υψηλότερη από 0,6, ο επιτιθέμενος εξακολουθεί να επιτυγχάνει θετικό κέρδος χρησιμότητας, αλλά γίνεται η λιγότερο προβλέψιμη.

Για παράδειγμα, ένας επιτιθέμενος με πραγματικό ορθολογισμό 0,5 θα επιτύχει υψηλότερη χρησιμότητα έναντι του υπερασπιστή του ορθολογισμού του 0,8 παρά 0,6. Το ίδιο συμβαίνει και για τις ορθολογικότητες του επιτιθέμενου 0,6 και 0,7, καθώς ο επιτιθέμενος θα επιτύχει μεγαλύτερη χρησιμότητα όταν ο αμυνόμενος έχει ορθολογισμό 0,9 σε σύγκριση με 0,8.

Μια άλλη ενδιαφέρουσα διαπίστωση στην εικόνα 22 είναι ότι ένας επιτιθέμενος με μεγαλύτερη πραγματική ορθολογικότητα δεν επιτυγχάνει, κατ' ανάγκη, μεγαλύτερη χρησιμότητα από έναν επιτιθέμενο με μικρότερη ορθολογικότητα. Για το παράδειγμα, ένας επιτιθέμενος με πραγματικό ορθολογισμό 0,6 τα καταφέρνει καλύτερα όταν αντιμετωπίζει έναν αμυνόμενο με ορθολογισμό 0,7. Αυτό επιβεβαιώνει τη σημασία του μοντέλου υπερπαιχνιδιών για να μπορέσει ο επιτιθέμενος επιτυγχάνοντας τη μέγιστη χρησιμότητά του με τον υπολογισμό της ορθολογικότητας εξαπάτησης, η οποία μπορεί να διαφέρει για κάθε πραγματική ορθολογικότητα.

Τέλος, η εικόνα 23 μελετά τη χρησιμότητα διαφορετικών τύπων επιτιθέμενων, διαφορετικών ως προς τις πραγματικές ορθολογικότητες a_{a_A}, για την επιλογή των ορθολογικών εξαπάτησης a_{a_L}. Κάθε καμπύλη αντιπροσωπεύει έναν τύπο επιτιθέμενου και εκτείνεται από τη χαμηλότερη δυνατή ορθολογικότητα μέχρι την πραγματική ορθολογικότητα του επιτιθέμενου. Βλέπουμε ότι η ορθολογικότητα εξαπάτησης a_{a_L}= 0,1 επιτυγχάνει την υψηλότερη χρησιμότητα κέρδος οποιουδήποτε επιτιθέμενου με πραγματική ορθολογικότητα μεγαλύτερη από 0,3.



Εικόνα 23 Η χρησιμότητα κι η ικανότητα του επιτιθέμενου [37]

Μια άλλη σημαντική διαπίστωση από την εικόνα 23 είναι ότι ένας επιτιθέμενος με χαμηλότερη πραγματική ορθολογικότητα, π.χ. 0,3, δεν θα επωφεληθεί πολύ από την εξαπάτηση. Παρομοίως, ένας επιτιθέμενος με υψηλή ορθολογικότητα θα μεγιστοποιήσει τη χρησιμότητά του εάν παίζει μια ορθολογικότητα εξαπάτησης χαμηλότερη ή ίση με 0,3. Αυτό επιβεβαιώνει τα ευρήματα της εικόνας 18 σχετικά με το σημείο καμπής 0,37 και την επίδρασή του στην αλλαγή της σειράς των στρατηγικών ενός παίκτη. Σημειώστε ότι, στην εικόνα 23, η βέλτιστη ορθολογικότητα εξαπάτησης για όλους τους παίκτες είναι 0,1. Ωστόσο, αυτή δεν είναι μια γενική περίπτωση στα σενάρια εξαπάτησης, αλλά μάλλον η λύση της, η οποία εξαρτάται και από τις άλλες παραμέτρους του παιγνίου [37].

ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

6.1 Σύνοψη και συμπεράσματα

Ολοκληρώνοντας την διπλωματική εργασία, κάποια συμπεράσματα μέσα από την θεωρία των παίγνιων που μπορούν να εξαχθούν, είναι πως η ασφάλεια του υλικού μέσω της θεωρίας αποτελεί μια από τις μεγαλύτερες προόδους της επιστήμης. Είναι ένα μεγάλο επίτευγμα $20^{ου}$ αιώνα η ανακάλυψη της επιστήμης της θεωρίας των παίγνιων για την ασφάλεια ενός υλικού, οπού με τη χρήση των μαθηματικών φτάνουμε κοντά στα όρια της ασφάλειας του υλικού. Η ασφάλεια του υλικού είναι χρήσιμη για όλους τους ενδιαφερόμενους και μέσω των θεσμικών οργάνων αποτελεί ένα μέρος μιας πολιτισμένης κοινωνίας.

Όπως εξετάσαμε στην διπλωματική εργασία, μόνο χρήσιμα και ασφαλή συμπεράσματα μπορούμε να εξάγουμε μέσα από την χρήση της επιστήμης της θεωρίας των παίγνιων και να δούμε πως με μια παραβίαση ενός υλικού μπορεί να έχουμε μόνο πρόσκαιρα κέρδη και πολλά αναπόφευκτα καταστροφικά αποτελέσματα στην όλη ιστορία, μιας κακόβουλης και παράνομης πράξης. Θα πρέπει να αλλάξουμε φιλοσοφία και τρόπο προσέγγισης του κέρδους και της ευημερίας μας, και να γίνουμε ικανοί για να μπορέσουμε να πατάξουμε κάθε παράνομη πράξη, ως προς την ασφάλεια του υλικού, χωρίς κανέναν ατομικισμό και πέρα από κάθε μικρό προσωπικό συμφέρον του πολίτη.

Η θεωρία των παίγνιων σε σχέση με την ασφάλεια υλικού και με βάση την μεθοδολογία που αναλύσαμε, προκύπτει πως μας προσφέρει μια πολύ δυνατή, αναλυτική κι εμπεριστατωμένη λύση στην προστασία των συσκευών. Αναλύει το πρόβλημα κάθε φορά που παρουσιάζεται, λαμβάνοντας υπόψη διαφορετικές προσεγγίσεις, τροποποιήσεις και περιορισμούς που προκύπτουν κάθε φορά, χωρίς να διαφοροποιείται και να μειώνεται η ασφάλεια που προσφέρει. Επιπλέον, μπορεί να διαχειριστεί περισσότερες από μια περιπτώσεις απειλών, επιλύοντας προβλήματα δίχως να πραγματοποιεί ουσιαστικές αλλαγές στο υλικό.

Κατά την διάρκεια μιας επίθεσης στο υλικό, λόγο των πολλών παραμέτρων, ένας μη εξοικειωμένος χρήστης σίγουρα θα δυσκολευτεί να χρησιμοποιήσει την θεωρία των παίγνιων σωστά για να επιλύσει ένα ζήτημα. Είναι δύσκολο ένας χρήστης που δεν είναι εκπαιδευμένος καλά, να ξέρει σωστά την χρησιμότητα της κάθε κίνησής του σε ένα περίπλοκο ζήτημα, εκτός κι αν απειλείται από μια απλή επίθεση, που μπορεί απλά να αποφασίσει μόνος του, δίνοντας μια τυπική λύση. Όταν η επίθεση είναι περίπλοκη, η θεωρία των παίγνιων μπορεί να δώσει λύσεις, όμως οι απαντήσεις που

δίνονται χρειάζονται προσοχή λόγο των πολλών παραμέτρων που θα υπάρχουν σε μια συνθέτη απειλή, καθώς θα ξεπροβάλλουν νέες μεταβλητές που θα απαιτούν τεκμηριωμένες απαντήσεις.

Στην παρούσα εργασία, προτείναμε ένα νέο πλαίσιο για την αποκάλυψη σε συστήματα ανίχνευσης trojan υλικού. Χρησιμοποιήθηκε η θεωρία προοπτικών για τη μοντελοποίηση των βασικών ωφελειών των παικτών, χωρίς de- ception, προκειμένου να ληφθούν υπόψη οι διαφορετικές ορθολογικότητες των παικτών. Στη συνέχεια διατυπώσαμε ένα επαναλαμβανόμενο παίγνιο στο οποίο ο αμυνόμενος μαθαίνει για τις στρατηγικές του επιτιθέμενου στο στάδιο της εκμάθησης και στη συνέχεια εφαρμόζει αυτή τη γνώση εκμάθησης στο επόμενο στάδιο του πραγματικού παιγνίου. Το κίνητρο πίσω από την εξαπάτηση συζητήθηκε προσεκτικά, το οποίο βασίζεται στην παραδοχή της επίδρασης της συνάρτησης Prelec στην αντιστροφή της σειράς αξιολόγησης μεταξύ χαμηλών και υψηλών πιθανοτήτων.

6.2 Προτάσεις και ιδέες για μελλοντική έρευνα

Ιδιαιτέρως ενδιαφέρον θέματα προς συζήτηση και περαιτέρω ανάλυση γεννιούνται με το πέρας της διπλωματικής μου, όπως η συνεχιζόμενη βελτιστοποίηση της ασφάλειας των υλικών που περιλαμβάνονται σε ένα σύστημα. Η θεωρία των παίγνιων μέσα από την μεθοδολογία που ακολουθεί και με την χρήση υπολογιστικών μαθηματικών μοντέλων, μπορεί να μας δώσει ακόμα μεγαλύτερη ασφάλεια στις συσκευές των χρηστών κατά την λειτουργία τους.

Η θεωρία παίγνιων βασίζεται σε μία προϋπόθεση, η οποία θεωρεί πως όλοι οι παίκτες, που συμμετέχουν σε ένα παίγνιο, είναι ορθολογικοί (μη αντιφατικοί) κι έχουν έναν ορθό και συμβατικό τρόπο σκέψης. Όταν ένας τουλάχιστον παίκτης διαθέτει αντιφατικό σύστημα σκέψης, τότε η θεωρία των παιγνίων δεν εφαρμόζεται ή αν εφαρμοστεί πιθανόν να οδηγήσει σε λάθη (πχ Πολιτική, Οικονομία, Διεθνείς Σχέσεις κτλ.). Βέβαια οι εχθροί των κοινωνιών θέλουν να τους θεωρούμε ορθολογικούς (μη αντιφατικούς), ώστε να χρησιμοποιούμε λάθος μεθόδους για να τους αντιμετωπίσουμε.

Η θεωρία των παίγνιων αν καταφέρει να λειτουργεί σε μικρότερους χρόνους εξετάζοντας όλες τις πιθανές λύσεις, θα είναι μια σημαντική πρόοδος γιατί με αυτό τον τρόπο θα καταφέρει να χρησιμοποιεί και λιγότερη ισχύ απόδοσης. Επίσης, η ανάλυση όλων των πιθανών λύσεων σε μια παρεμβατική επίθεση, εξετάζοντας όλο τον χώρο της συσκευής, δημιουργεί και συνοδά προβλήματα μνήμης.

Τέλος, δοκιμάσαμε το προτεινόμενο πλαίσιο χρησιμοποιώντας προσομοιώσεις και τα αποτελέσματα έδειξαν ότι ο επιτιθέμενος μπορεί να εισάγει επιτυχώς trojans

υλικού χωρίς να γίνεται αντιληπτός. Τα αποτελέσματα έδειξαν επίσης το κέρδος του επιτιθέμενου σε χρησιμότητα κάτω από διαφορετικούς συνδυασμούς του επιτιθέμενου και του αμυνόμενου.

Μελλοντικά, θα επικεντρωθούμε στην κατασκευή πιο αυστηρών μηχανισμών άμυνας χρησιμοποιώντας την άμυνα κινούμενου στόχου και υψηλότερα επίπεδα θεωρίας υπερπαιγνίων. Μια πιθανή προγραμματιστική αλλαγή να μπορεί να μας δώσει πολύ καλύτερα αποτελέσματα σε πραγματικό χρόνο, επιλύοντας προβλήματα ακόμα κι από πολύπλοκες επιθέσεις, πρόταση η οποία μένει να αποδειχθεί και να διαπραγματευτεί σε μελλοντική εργασία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Bazerman M.H., Samuelson W.F., 1983, I won the auction but don't want the prize, Journal of Conflict Resolution, 27, pp. 618-634.

[2] Binmore, Ken (1991), Fun and Games: A Text on Game Theory. D. C. Heath, Lexington, MA.

[3] Dixit, Avinash K., and Nalebuff, Barry J. (1991), Thinking Strategically: The Competitive Edge in Business, Politics, and Everyday Life. Norton, New York.

[4] Fudenberg, Drew and Tirole, Jean (1991), Game Theory. MIT Press, Cambridge, MA.

[5] Gibbons, Robert (1992), Game Theory for Applied Economists. Princeton University Press, Princeton, NJ.

[6] Harrington S., Danzon P., 1994, Cutting in liability insurance markets, Journal of Business, 67(4), pp. 511-538.

[7] John Kay, 2007, Η αλήθεια για τις αγορές, εκδόσεις Κριτική.

[8] John Lipczynski, John O.S Wilson, John Goddard(2012): Βιομηχανική Οργάνωση Ανταγωνισμός, Στρατηγική, Πολιτική. Εκδόσεις Π.Χ Πασχαλίδης

[9] Klemperer P., 2004, Auctions: Theory and Practice, Princeton University Press.

[10] Martin J. Osborne Ariel Rubinstein (1990), Bargaining and Markets

[11] Martin J. Osborne Ariel Rubinstein (1994), A Course in Game Theory.

[12] Myerson, Roger B. (1991), Game Theory: Analysis of Conflict. Harvard University Press, Cambridge, MA.

[13] R. Gibbons, Εισαγωγή στη Θεωρία Παιγνίων, εκδ. Γ. & Κ. Δαρδανός, Αθήνα 2009.Κωδικός Βιβλίου στον ΕΥΔΟΞΟ: 31325.

[14] Rasmusen, Eric (2001), Games and Information: An Introduction to Game Theory, 3rd ed. Blackwell, Oxford.

[15] Rothschild M., Stiglitz J. E., (1976), Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information, Quarterly Journal of Economics, Vol. 90, pp. 630-639.

[16] Αδαμοπούλου, Α. Α. (2018). Φυσικές μη κλωνοποιήσιμες συναρτήσεις για τον επακριβή προσδιορισμό συσκευών ασφαλείας.

[17] Βαρουφάκης Γιάνης (2007), Θεωρία Παιγνίων: Η Θεωρία που φιλοδοξεί να ενοποιήσει τις κοινωνικές επιστήμες, Εκδόσεις Gutenberg.

[18] Γιάννης Ρεφανίδης: Σημειώσεις στη Θεωρία Παιγνίων. Πανεπιστήμιο Μακεδονίας Τμήμα Εφαρμοσμένης Πληροφορικής.

[19] Διπλωματική Εργασία: Παραδείγματα στη θεωρία παιγνίων, Κωνσταντίνος Γκραβάς. Εθνικό Μετσόβιο Πολυτεχνίο (2012)

[20] Εμμανουήλ Πετράκης: Σημειώσεις στη Θεωρία Παιγνίων. Τμήμα Οικονομικών Επιστημών Πανεπιστήμιο Κρήτης.

[21] Κατσιάπης, Ε., & Γιάλβαρη, Μ. (2014). Θεωρία παιγνίων και η ελληνική χρεωστική κρίση

[22] M. Osborne, Εισαγωγή στη Θεωρία Παιγνίων, εκδ. Κλειδάριθμος, Αθήνα 2010. Κωδικός Βιβλίου στον ΕΥΔΟΞΟ: 35241.

[23] Μαγείρου, Ευάγγελος Φ. (2012) Παίγνια και αποφάσεις: Μια εισαγωγική προσέγγιση, Αθήνα : Κριτική.

[24] Μάρας, Σ. (2021). Ασφάλεια και προστασία ιδιωτικότητας οικιακών συσκευών που λειτουργούν σε περιβάλλον ΔτΠ.

[25] Μεταπτυχιακή Διατριβή της Βλαχοπούλου Αθανασίας (2010)

[26] Μηλολιδάκης, Κωστής (2009) Θεωρία παιγνίων : Μαθηματικά μοντέλα σύγκρουσης και συνεργασίας, Θεσσαλονίκη: σοφία Α.Ε.

[27] Μπούρα, Β. (2015). Πολιτικές και Μοντέλα Ασφαλείας Πληροφοριακών Συστημάτων.

[28] Νεκτάριος Μ., (2014). Ιδιωτική ασφάλιση και διαχείριση κινδύνων. Εκδόσεις Παπαζήση. Αθήνα.

[29] Ξευγένη, Κ. (2022). Αξιολόγηση της ασφάλειας και της αξιοπιστίας επιταχυντών υλικού σχεδιασμένων με χρήση Σύνθεσης Υψηλού Επιπέδου (Master's thesis, Πανεπιστήμιο Πειραιώς).

[30] Παναγιώτης Χουχούλας: Θεωρία Παιγνίων ΥΕΘΑ/ΕΠΙΤΕΛΕΙΟΥ ΥΠ. 2000

[31] Παναγιωτακόπουλος, Γ. Δ. (2014). Βέλτιστος Σχεδιασμός Κατασκευών με Χρήση Θεωρίας Παιγνίων (Master's thesis).

[32] Πάσσιος, Θ. (2021). Ασφάλεια στο Διαδίκτυο των Πραγμάτων μέσω Φυσικών Μη-Κλωνοποιήσιμων Συναρτήσεων.

[33] Φουσέκης Παναγιώτης (2009), Στοιχεία Θεωρίας Παιγνίων, Πανεπιστημιακές Παραδόσεις, Τμήμα Εκδόσεων ΑΠΘ.

[34] Καμπουρίδης, Π. (2017). Εισαγωγή στη θεωρία παιγνίων και εφαρμογές (Master's thesis, Πανεπιστήμιο Πειραιώς).

[35] Χωραΐτη, Σ. (2013). Θεωρία παιγνίων και προβλήματα βελτιστοποίησης.

[36] D. Bensanko – R. R. Braeutigam, 2009, «Μικροοικονομική», Εκδόσεις Gutenberg, σελίδα 717

[37] Das, T., Eldosouky, A. R., & Sengupta, S. (2020, June). Think smart, play dumb: Analyzing deception in hardware trojan detection using game theory. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.

[38] Kamhoua, C. A., Zhao, H., Rodriguez, M., & Kwiat, K. A. (2016). A game-theoretic approach for testing for hardware trojans. IEEE Transactions on Multi-Scale Computing Systems, 2(3), 199-210.