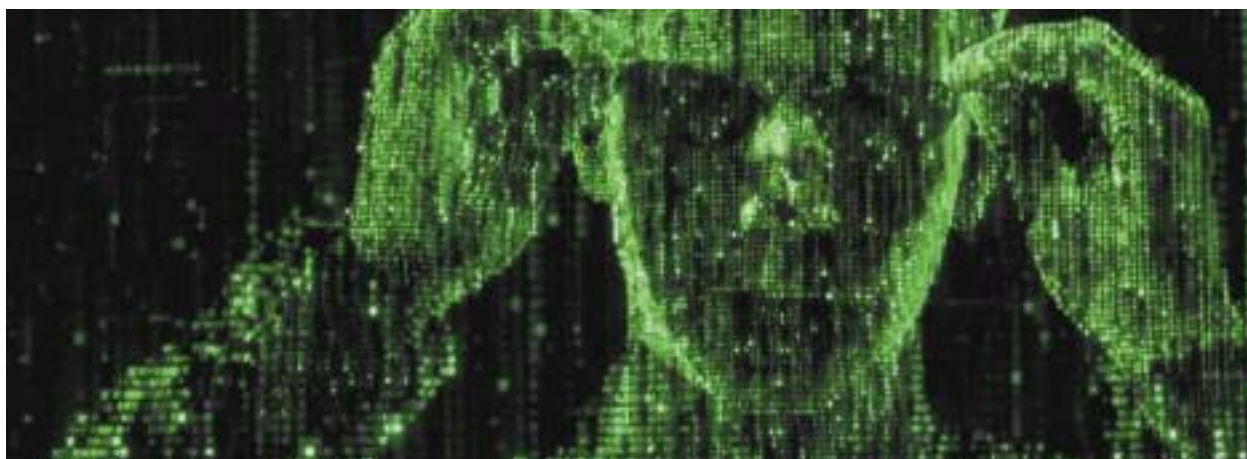


## Αντίστροφη Μηχανική (Reverse Engineering)



**Η** αντίστροφη μηχανική (reverse engineering) είναι η διαδικασία κατά την οποία ένας τεχνολόγος μηχανικός, μηχανικός πληροφορικής και Η/Υ, ηλεκτρονικός μηχανικός ή ηλεκτρολόγος μηχανικός ή και όλοι μαζί αναλαμβάνουν να ανακαλύψουν τις τεχνολογικές αρχές μιας συσκευής, ενός αντικειμένου, ενός λογισμικού ή ενός συστήματος μέσω της ανάλυσης της δομής και της λειτουργίας του.

Ο στόχος είναι να μπορέσει ο μηχανικός να κατανοήσει τον τρόπο με το οποίο το υπό εξέταση αντικείμενο λειτουργεί ώστε να μπορέσει να βρει τρόπους να το αντιγράψει ή να αναπαράγει τη λειτουργικότητά του.

Η χρήση της αντίστροφης μηχανικής μπορεί να είναι απλά η αναπαραγωγή - χωρίς κατανόηση - του πρωτοτύπου ή ένας τρόπος για να μάθει κάποιος ιδιαίτερα μυστικές ή χρήσιμες πληροφορίες μέσα από ένα κλειστό σύστημα.

Για το λόγο αυτό η αντίστροφη μηχανική έχει και τις ρίζες της στην ανάλυση του υλικού για εμπορικούς και στρατιωτικούς σκοπούς.

Τα κίνητρα και οι λόγοι για την ύπαρξη και την χρήση της αντίστροφης μηχανικής μπορεί να είναι οι ακόλουθοι:

### **Διαλειτουργικότητα**

Συχνά γίνεται επειδή η τεκμηρίωση μιας συγκεκριμένης συσκευής έχει χαθεί ή ποτέ δεν γράφτηκε. Ένα κλασικό παράδειγμα είναι τα εγχειρίδια χρήσης για πολύπλοκα ή ακριβά προγράμματα όπως τα λογισμικά σχεδιασμού 3D animation. Εκεί ο μηχανικός με μεθοδολογία καταγράφει τις απαιτήσεις και μετά τον τρόπο χρήσης του προγράμματος μέσα από δοκιμές και επαληθεύσεις των λειτουργιών των προγραμμάτων. Η τεχνική αυτή κατά την οποία ο μηχανικός δεν έχει γνώση της τεχνολογίας, της υποδομής και του κώδικα στο εσωτερικό αλλά καταφέρνει να περιγράψει και να αναλύσει το λογισμικό, λέγεται black box.

### **Ανάλυση προϊόντος**

Για να εξετάσει τον τρόπο με τον οποίο ένα προϊόν λειτουργεί, από τι συστατικά αποτελείται, τα έξοδα εκτίμησης και τον εντοπισμό τυχόν παραβίασης των διπλωμάτων ευρεσιτεχνίας. Εάν το προϊόν δεν είναι ιδιοκτησία του μηχανικού τότε η χρήση της τεχνικής του black box είναι συνήθης, αλλιώς η γνώση των πληροφοριών επιτρέπει την χρήση του white box. Το white box είναι δηλαδή η τεχνική κατά την οποία ο μηχανικός κάνει την ανάλυση γνωρίζοντας από μέσα κάθε στοιχείο του συστήματος.

## Έλεγχος ασφάλειας

Η απόκτηση ευαίσθητων δεδομένων από την αποσυναρμολόγηση και την ανάλυση του σχεδιασμού ενός στοιχείου του συστήματος. Εδώ η τεχνική είναι πάντα η black box αλλιώς το σύστημα ασφάλειας δεν είναι ασφαλές.

## Στρατιωτική ή εμπορική κατασκοπία

Η κλοπή ενός πρωτοτύπου του εχθρού και η αποσυναρ-

## Αντίστροφη σχεδίαση του λογισμικού

Ο όρος αντίστροφη μηχανική, όπως αυτός εφαρμόζεται στο λογισμικό σημαίνει διαφορετικά πράγματα για διαφορετικούς ανθρώπους. Γι' αυτό το λόγο υπάρχουν δύο μεγάλες κατηγορίες αντίστροφης μηχανικής λογισμικού.

Στην πρώτη περίπτωση, ο πηγαίος κώδικας είναι ήδη διαθέσιμος μαζί με το λογισμικό (λογισμικό ανοικτού κώδικα), οπότε με μια οποιαδήποτε έρευνα στα ενδότερα του προ-



μολόγηση του ίσως βοηθήσουν στην αντιμετώπιση και την καλύτερη άμυνα.

Επιπλέον μπορεί να συμβάλλει στην αντιμετώπιση με παραγωγή όπλων παρόμοιων του εχθρού. Εδώ η τεχνική ανάλυσης είναι σχεδόν πάντα η black box.

## Απομάκρυνση της προστασίας κατά της αντιγραφής ή την καταστράτηγηση των περιορισμών πρόσβασης

Δημιουργία χωρίς άδεια / μη εγκεκριμένα αντίγραφα. Εδώ η τεχνική ανάλυσης είναι πάντα η black box.

## Ακαδημαϊκοί σκοποί

Να μάθουν από τα λάθη των άλλων ώστε να μην γίνουν τα ίδια λάθη που άλλοι έχουν ήδη κάνει και στη συνέχεια να διορθώσουν τις πρακτικές τους.

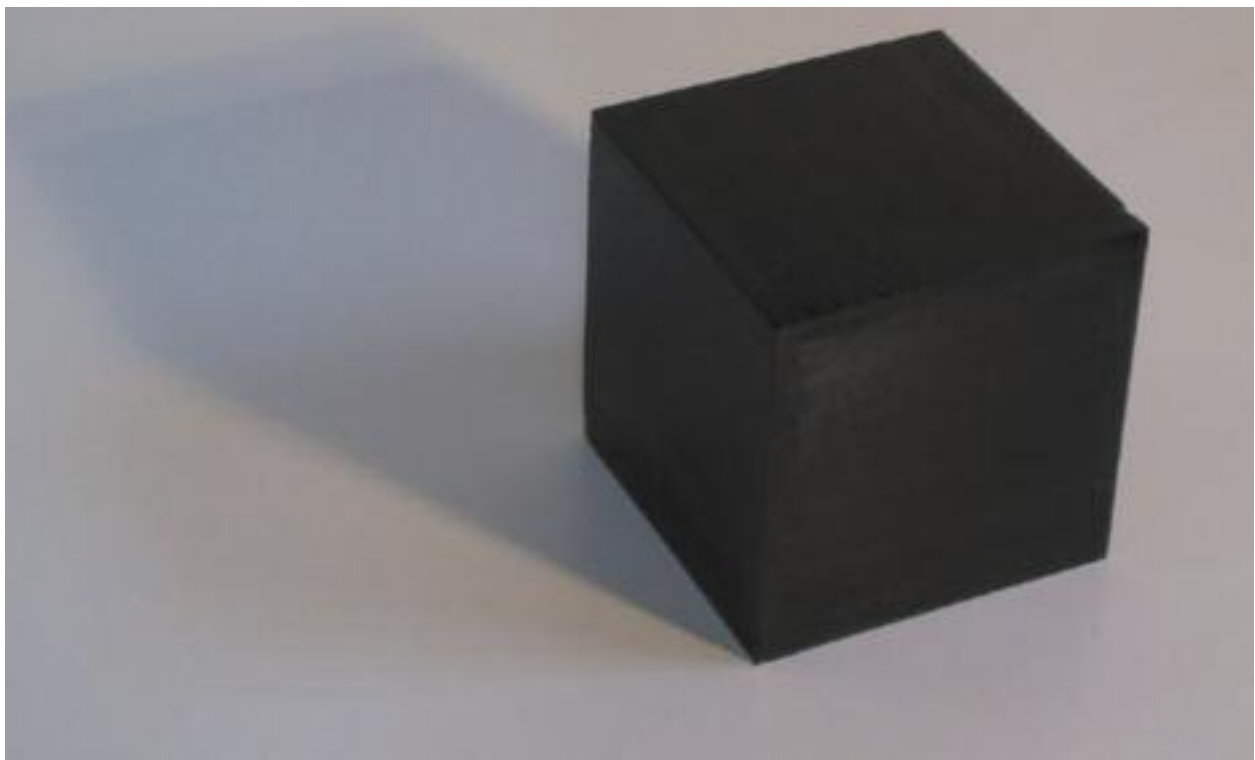
Εδώ η τεχνική ανάλυσης είναι είτε η black box είτε η white box.

γράφματος ανακαλύπτονται οι όποιες πληροφορίες. Στη δεύτερη περίπτωση, δεν υπάρχει πηγαίος κώδικας για το λογισμικό και οι οποιεσδήποτε προσπάθειες για την ανακάλυψη πληροφοριών για το λογισμικό θεωρείται ως αντίστροφη μηχανική. Αυτή η δεύτερη χρήση του όρου είναι που οι περισσότεροι άνθρωποι είναι περισσότερο εξοικειωμένοι. Για την αντίστροφη σχεδίαση του λογισμικού (reverse code engineering) μπορεί να χρησιμοποιηθεί η τεχνική σχεδίασης καθαρού δωματίου (clean room design) για να αποφευχθεί η παραβίαση των πνευματικών δικαιωμάτων.

Το clean room design επίσης γνωστό και ως "Κινέζικο Τοίχος", είναι η μέθοδος της αντιγραφής ενός σχεδίου με αντίστροφη μηχανική και στη συνέχεια η εκ νέου δημιουργία του χωρίς να παραβιάζει κανένα από τα δικαιώματα πνευματικής ιδιοκτησίας και των εμπορικών μυστικών που σχετίζονται με τον αρχικό σχεδιασμό. Ωστόσο, επειδή η ανεξάρτητη εφεύρεση δεν είναι μια άμυνα εναντίον των πατεντών, το

clean room design κατά κανόνα δεν μπορεί να χρησιμοποιηθεί για να παρακάμψει τους περιορισμούς διπλωμάτων ευρεσιτεχνίας.

Στο clean room design η ομάδα σχεδίασης εργάζεται σε ένα περιβάλλον που είναι «καθαρό», ή αποδεδειγμένα δεν έχει “μολυνθεί” από οποιαδήποτε γνώση της ιδιόκτητων τεχνικών που χρησιμοποιούνται από τον ανταγωνιστή. Συνήθως, οι προδιαγραφές στο clean room design γίνονται από κάποιους που έχουν εξετάσει το σύστημα. Οι προδιαγραφές στη συνέχεια εξετάζονται από έναν δικηγόρο για να διασφαλιστεί ότι δεν προστατεύονται από πνευματικά δικαιώματα. Τέλος, οι προδιαγραφές εφαρμόζονται από μια ομάδα που δεν έχει καμία σχέση με την αρχική ομάδα που έγραψαν τις προδιαγραφές. Εδώ η τεχνική ανάλυση είναι είτε η black box είτε η white box.



### **Δυσαιτικές τεχνικές λογισμικού**

Αντίστροφη σχεδίαση του λογισμικού μπορεί να επιτευχθεί με διάφορες μεθόδους.

Οι τρεις κύριες ομάδες της αντίστροφης μηχανικής λογισμικού είναι:

1. Αντίστροφη ανάλυση μέσω της παρατήρησης της ανταλλαγής πληροφοριών.
2. Αποσυναρμολόγηση χρησιμοποιώντας ένα disassembler.
3. Από-μεταγλώττιση χρησιμοποιώντας έναν decompiler.

Εδώ η τεχνική ανάλυση είναι πάντα η black box.

### **Αντίστροφη μηχανική των πρωτοκόλλων**

Με την ανακατασκευή μηνυμάτων τα οποία περιλαμβάνουν ανάλυση του τρόπου που οι εφαρμογές συνεργάζονται κυρίως μέσω services. Εδώ η τεχνική ανάλυσης είναι σχεδόν πάντα η black box.

### **Αντίστροφη μηχανική των ολοκληρωμένων κυκλωμάτων**

Η αντίστροφη μηχανική των CHIP είναι μια επεμβατική και καταστροφική μορφή ανάλυσης αλλά ο επιτιθέμενος είναι δυνατό να αποκαλύψει το πλήρες υλικό και λογισμικό μέρος της συσκευής προς όφελός του. Εδώ η τεχνική ανάλυσης είναι πάντα η black box.

Γενικά η αντίστροφη μηχανική είναι ένα χόμπι για πολλούς ενώ για άλλους όπως οι μεγαλύτερες Κινέζικες εταιρίες είναι ο τρόπος για να βγάλουν στην αγορά προϊόντα που κάνουν παρόμοια πράγματα με άλλα ανταγωνιστικά σε πολύ χαμηλότερες τιμές. Είναι δηλαδή ένας τρόπος να χτυπήσουν την αγορά στο κόστος.

Επειδή όμως όπως αναφέραμε αυτό δεν είναι πάντα θεμιτό

παρακάτω αναφερόμαστε γενικά περί νομιμότητας στις ΗΠΑ και στην ΕΕ.

#### **• Ηνωμένες Πολιτείες Αμερικής**

Στις Ηνωμένες Πολιτείες, ακόμη και αν ένα κατασκεύασμα ή διαδικασία προστατεύεται από το εμπορικό απόρρητο, η αντίστροφη μηχανική το τεχνούργημα ή η διαδικασία συχνά είναι νόμιμη αρκεί να λαμβάνεται νόμιμα.

Ένα κοινό κίνητρο της αντίστροφης μηχανικής είναι να καθοριστεί εάν το προϊόν ενός ανταγωνιστή περιέχει παραβάσεις διπλωμάτων ευρεσιτεχνίας ή παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας.

#### **• Ευρωπαϊκή Ένωση**

Το άρθρο 6 της ευρωπαϊκής οδηγίας του 1991 για τα προγράμματα ηλεκτρονικών υπολογιστών επιτρέπει την αντίστροφη μηχανική για τους σκοπούς της διαλειτουργικότητας αλλά

