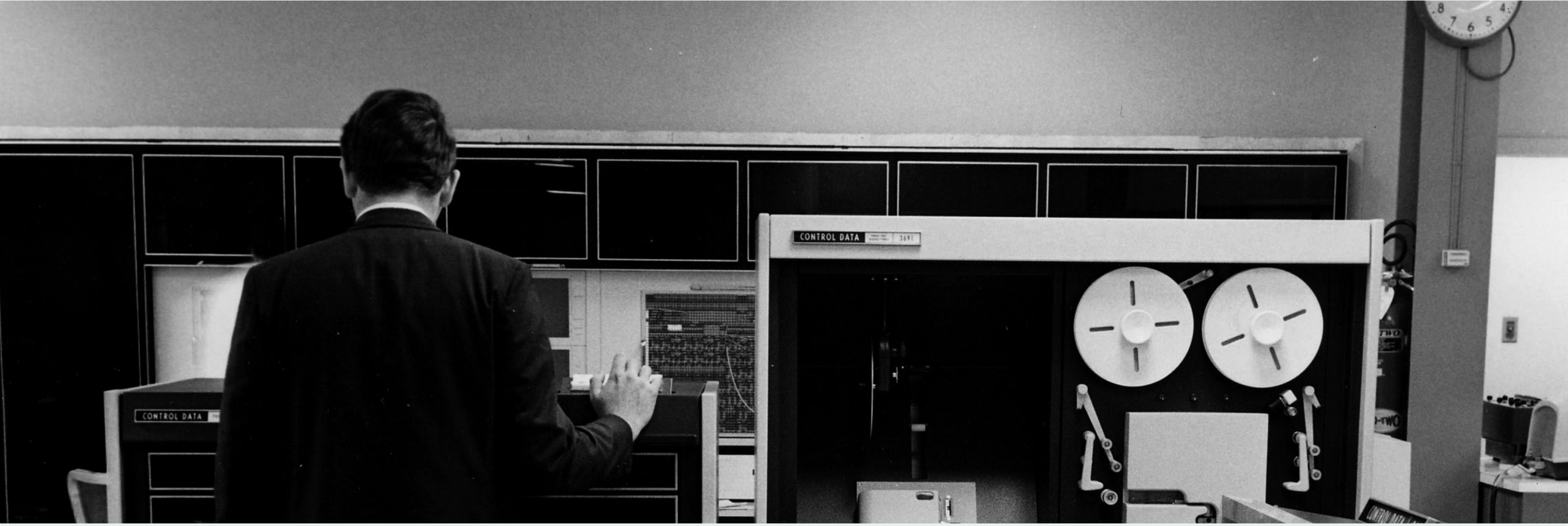

ΞΑΝΑΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ

Κ.Π. Γραμματικάκης
[redacted]@uop.gr

Εισαγωγή

Reverse engineering

Ανάστροφη μηχανική

ή μήπως Αντίστροφη μηχανίκευση;

Η διαδικασία εξαγωγής των σχεδιαστικών αρχών
ενός αντικειμένου, συστήματος ή λογισμικού
μέσω της μελέτης της δομής και της λειτουργίας του.

Σκοπός στην περίπτωση του λογισμικού είναι:

Interfacing – Διασύνδεση με άλλα συστήματα.

Αν το λογισμικό δεν υποστηρίζει επικοινωνία με άλλα συστήματα (είτε hardware, είτε software).

Computer Security – Ασφάλεια λογισμικού/συστήματος.

Ανακάλυψη ευπαθειών χωρίς την ύπαρξη πηγαίου κώδικα, ανάλυση malware.

Bug Fixing – Αποσφαλμάτωση.

Διόρθωση σφαλμάτων χωρίς την ύπαρξη πηγαίου κώδικα, υποστήριξη legacy συστημάτων.

Documentation – Δημιουργία εγγράφων τεκμηρίωσης.

Μπορεί να μην υπάρχει, να έχει καταστραφεί, να είναι ανεπαρκές.

Low level software
Λογισμικό χαμηλού επιπέδου

Source Code
Πηγαίος Κώδικας

Περιέχει εντολές σε γλώσσα υψηλού επιπέδου
(όπως η C, C++, Java, C#), οι οποίες περιγράφουν την λειτουργία και την συμπεριφορά του προγράμματος.

Compiler / Compilation
Μεταγλωττιστής / Μεταγλώττιση

Παράγει κώδικα Assembly
με βάση τις εντολές του Source Code.
Μεταξύ άλλων **κάνει βελτιστοποιήσεις και αλλαγές**
στον κώδικα με σκοπό την καλύτερη χρήση μνήμης,
την καλύτερη ταχύτητα εκτέλεσης, κ.λπ.

Low level software

Λογισμικό χαμηλού επιπέδου

Machine Code

Γλώσσα Μηχανής

Οι εντολές που θα σταλούν στον επεξεργαστή για εκτέλεση.
Αποτελούν **κωδικούς** που αναγνωρίζει ο επεξεργαστής
και μπορεί να εκτελέσει.

Assembly / Assembler

Συμβολική Γλώσσα / Συμβολομεταφραστής

Συμβολική αναπαράσταση των εντολών γλώσσας μηχανής.
Είναι πιο εύκολα κατανοητές από ανθρώπους
σε σχέση με τις “γυμνές” εντολές μηχανής.

Ανάστροφες διαδικασίες

Από το χαμηλό στο υψηλό επίπεδο

Dissasembly

Αποσύμπλιση

Μετατροπή εντολών γλώσσας μηχανής σε assembly.
Κάποιες εντολές assembly έχουν
πολλαπλές αναπαραστάσεις σε γλώσσα μηχανής.

Decompilation

(?)

Ερμηνεία **γλώσσας μηχανής** ή assembly
ως εντολές προγράμματος υψηλού επιπέδου.

Εργαλεία

Υπάρχει επικάλυψη στις λειτουργίες κάθε κατήγορίας.

Disassemblers: Objdump (Open source, Linux), IDA Pro (Proprietary, Cross platform)
Ερμηνεύουν τις εντολές γλώσσας μηχανής σε εντολές assembly, παράγουν γράφους ροής και κλήσεων συναρτήσεων, αναγνωρίζουν κλήσεις σε default APIs, κ.α.

Debuggers: OllyDbg (Shareware, Windows), WinDbg (Commercial, Windows), gdb (Open source, Cross platform), radare2 (Open source, Cross platform)
"Ακολουθούν" την εκτέλεση ενός προγράμματος.
Επιτρέπουν την προβολή/αλλαγή της κατάστασης ενός προγράμματος, κ.α.
Μεγάλη επικάλυψη μεταξύ των interactive debuggers και των disassemblers.

Decompilers: Java Decompiler (Open source, Cross platform), dex2jar, DotPeek (Commercial, Windows), FFDec (Open source, Windows)

Hex editors: radare2 (Open source, Cross platform), HxD