Hacking with Assembly

Τμήμα μηχανολόγων μηχανικών

21 Νοεμβρίου 2012

Γκανετσίδης Κωνσταντίνος-Ραφαήλ

Επιβλέπων Καθηγητής: Δασυγένης Μηνάς

Διάλεξη 5λεπτών για το μάθημα Αρχιτεκτονικής ΗΥ

Τι είναι;

- Assembly hacking/ASM Hacking

  Τροποποίηση του source code μιας εφαρμογής

- ROM Hacking

  Assembly Hacking στον τομέα του gaming

Απαιτήσεις και δυσκολίες

- Απαιτήσεις
  - Λεπτομερή γνώση γλώσσας Assembly
  - Λεπτομερή γνώση της εσωτερικής λειτουργίας του προγράμματος

- Δυσκολίες
  - Έλλειψη συγκεκριμένου μοτίβου ενεργειών
  - Κάθε σύστημα απαιτεί λεπτομερή γνώση διαφορετικής γλώσσας Assembly
    - » Π.χ. MIPS (N64, PS1, PS2)
      - M68000 (Genesis)
      - Z80 (Game Boy)
      - 65c816 (SNES)
      - 6502 (Atari, NES, PC Engine)

Δυσκολίες(συνέχεια)

- Εύρεση ζητούμενου σημείου κώδικα προς τροποποίηση
  - Πλήθος γραμμών του κώδικα
  - Κρυπτογράφηση του κώδικα από τους Developers για την αποτροπή της τροποποίησης του

- ROM Expansion(σε συγκεκριμενους τομείς του game hacking)
  - Το μέγεθος του ROM Image έιναι καθορισμένο με αποτέλεσμα να μην μπορει θεωρητικά να προσθεθεί επιπλέον περιεχόμενο στο παιχνίδι.
    - Η διαδικασία του ROM Expansion ήταν σχεδόν αδύνατη στην Consola NES και απαιτούσε ιδιαίτερα δύσκολες μετατροπές των mapper.
    - Στην κονσόλα SNES έπρεπε να ξαναγραφούν μεγάλα μέρη του κώδικα ώστε να δημιουρθεί χώρος για τα καινούργια.
    - Στην κονσόλα Gameboy η υπάρχουσα μνήμη ξεπερνούσε εώς και 17 φορές την χρησιμοποιούμενη κατι που καθιστούσε αρκετά έυκολο το ROM Expansion

Γιατί Assemby;

- Έλλειψη του source code
  - Λόγω μη ελεύθερης διανομής του από τους Developers
- Εφικτοί τρόποι ανάκτησης του source code σε γλώσσα assembly
  - Reverse engineering(decompile-modify-compile)
    - Disassemblers: Idapro,Interactive Disassembler etc.
    - Debuggers: OllyDbg,WinDbg,Tseach,Cheat Engine etc.

Παραδείγματα

- Always Valid Registration KEY

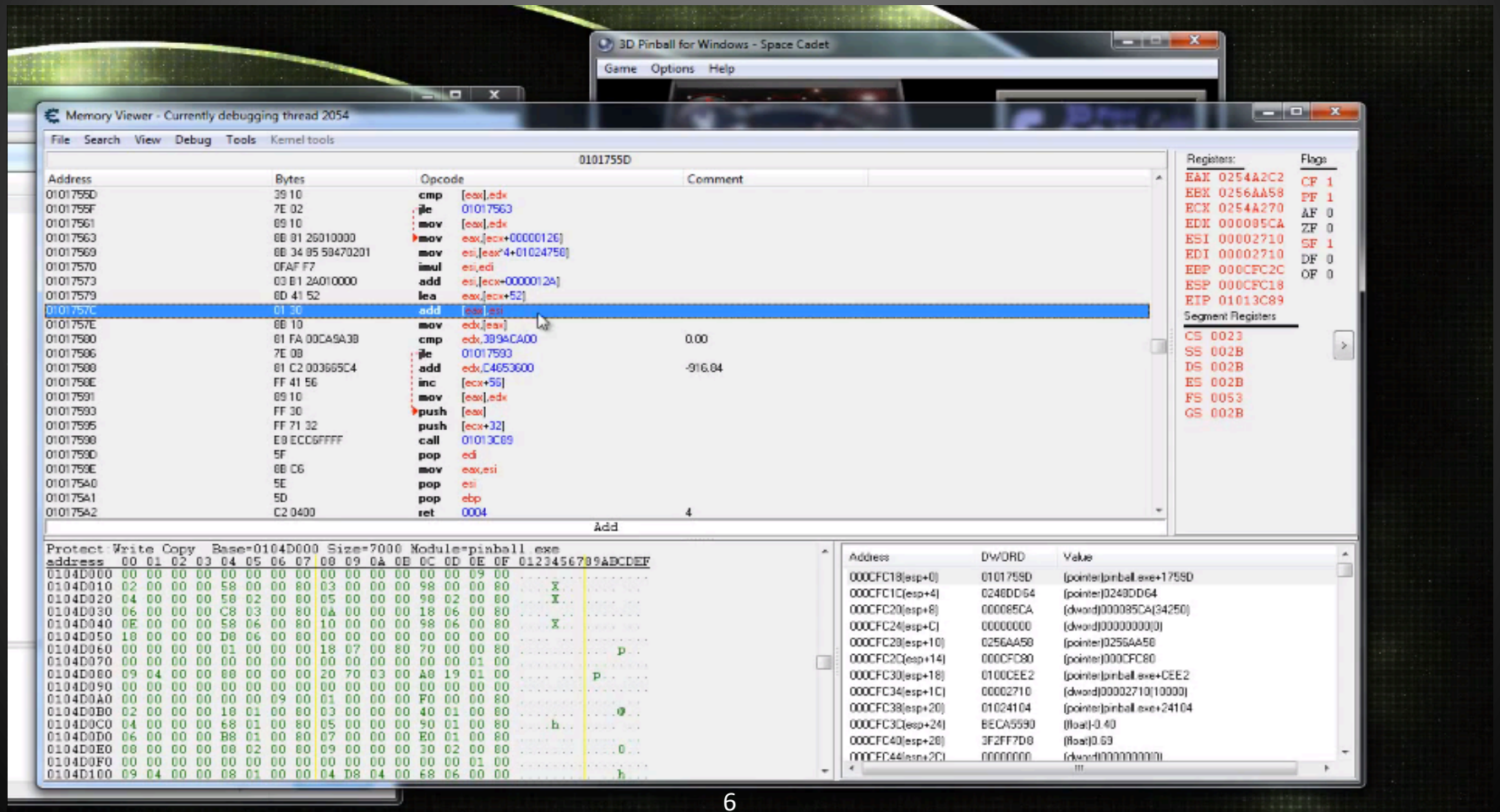
Αλλαγή της εντολής που ελέγχει αν ικανοποιείται η συνθήκη έτσι ώστε να πραγματοποιείται ανεξάρτητα από αυτήν.

JNZ SHORT 00450C56

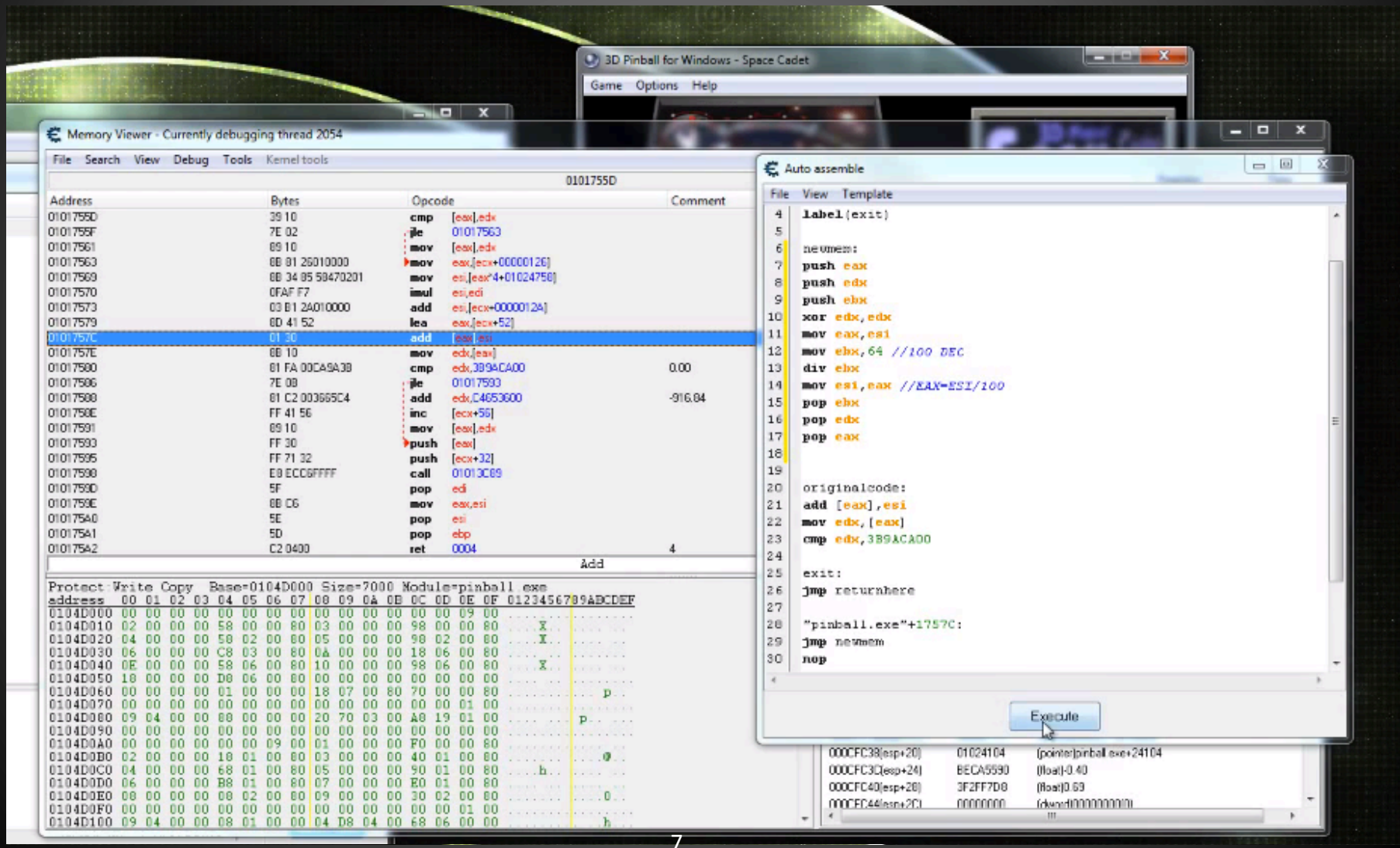
JMP SHORT 00450C56

Παραδείγματα(Code injection)

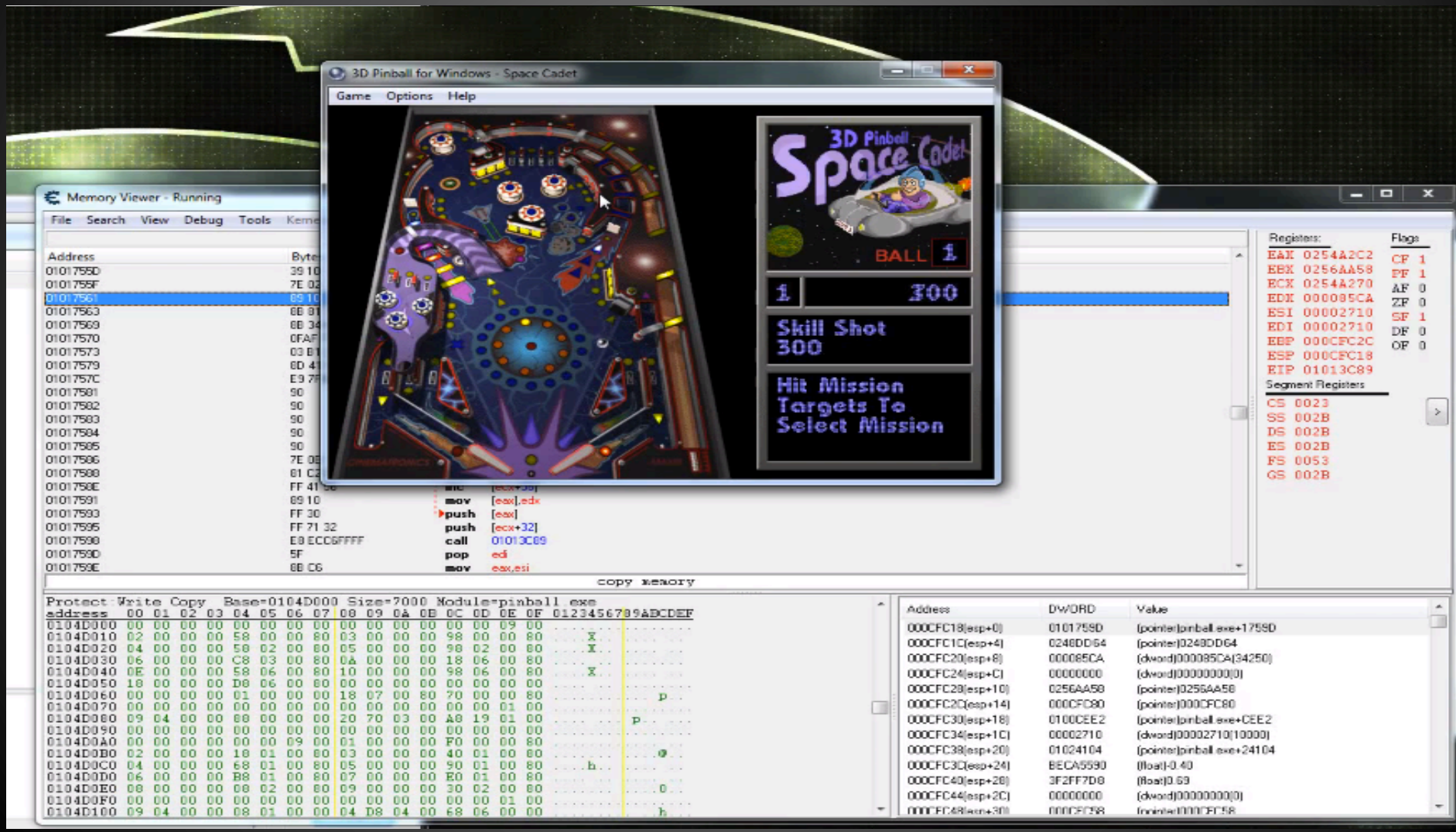
Εύρεση των ζητούμενων εντολών στον κώδικα(εδώ καταμετρηση πόντων/υπολογισμός τελικού σκορ στο παιχνιδι 3D Pinball των Windows).



Εισαγωγή εμβόλιμου κώδικα για την τροποποίηση της καταμέτρησης πόντων.



Αποθήκευση νέου κώδικα και επισκόπηση αποτελεσμάτων



Συμπεράσματα/Μελλοντικές προεκτάσεις

- What a man can do,another man can undo,redo,do better or fail trying

- Η χρήση του Assembly Hacking δύσκολα θα ξεπεραστεί ή θα αντικατασταθεί

Βιβλιογραφια:

- http://www.criticalsecurity.net/index.php/topic/29278-learning-asm-the-hacker-point-of-view/
- http://www.romhacking.net/dictionary/?page=dictionary#term2
- http://romhack.wikia.com/wiki/Assembly_hacking
- http://www.happyhacker.org/indexb.shtml
- http://en.wikipedia.org/wiki/ROM_hacking#ROM_expansion
- http://ffhacktics.com/wiki/ASM_Hacking

Other Links & Guides:

- http://www.securitytube.net/video/208
- http://www.youtube.com/watch?v=Nshy5XMI_FI
- http://dunyainfocom.blogspot.gr/2011/10/reverse-engineering-hacking-tutorial.html