**ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ**

**ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ**

**ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ**


## Λαδάκης Ευάγγελος

**Μεταπτυχιακός Φοιτητής**

**Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης**


Επόπτης Μεταπτ. Εργασίας: Καθηγητής, Ε. Μαρκάτος

**Τετάρτη, 14/10/2015, 12:00**

**Αίθουσα B108, Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης**

# " GPU-Disasm: Ένας x86 ανακατασκευαστής βασισμένος στη κάρτα γραφικών"

## ΠΕΡΙΛΗΨΗ


Η στατική ανάλυση και η αποσυμπίληση του δυαδικού κώδικα είναι απαραίτητες λειτουργίες που χρησιμοποιούνται, μεταξύ άλλων, για την ανάλυση κακόβουλου λογισμικού, για τους μηχανισμούς προστασίας προγραμμάτων σε δυαδικό επίπεδο και για τον εντοπισμό και την επιδιόρθωση σφαλμάτων. Η χρήση γρηγορότερων εργαλείων ανάλυσης δυαδικού κώδικα είναι αναγκαία για την εκπόνηση εργασιών, όπως την ανάλυσης πλήθους νέων κακόβουλων λογισμικών τα οποία συγκεντρώνονται κάθε μέρα. Η ανάλυση του δυαδικού κώδικα είναι η κύρια λειτουργικότητα των εργαλείων αυτών, η οποία και δεν έχει λάβει τη πρέπουσα προσοχή από τη σκοπιά της επίδοσης. Σε αυτή την εργασία, παρουσιάζουμε το GPU-Disasm, έναν ανακατασκευαστή υλοποιημένο στη κάρτα γραφικών, για τον x86 κώδικα ο οποίος εκμεταλλεύεται τους επεξεργαστές της κάρτας γραφικών, για να πετύχει αποδοτικότερη ανάλυση εκτελέσιμων προγραμμάτων σε μεγάλη κλίμακα. Περιγράφουμε με λεπτομέρεια τις

διάφορες βελτιώσεις και σχεδιαστικές επιλογές που χρειάστηκαν, για να επιτευχθούν τόσο ο εξο-παραλληλισμός, για την ανακατασκευή πολλαπλών εκτελέσιμων προγραμμάτων, όσο και ο ενδο-παραλληλισμός για την παράλληλη αποκωδικοποίηση των εντολών ενός εκτελέσιμου. Τα αποτελέσματα των πειραμάτων μας από τη σκοπιά της επίδοσης και της κατανάλωσης, δείχνουν ότι το GPU-Disasm είναι δύο φορές πιο γρήγορο από την έκδοση που είναι βασισμένη στον επεξεργαστή, για τη γραμμική ανακατασκευή και 4.4 φορές πιο γρήγορο για την εξαντλητική ανακατασκευή, με συγκρίσιμη κατανάλωση ενέργειας σε σχέση με την υλοποίηση στον επεξεργαστή.


## Ladakis Evangelos

**M.Sc. Thesis**

**Computer Science Department**

**University of Crete**

**Master's Thesis Supervisor: Professor E. Markatos**


**Wednesday, 14/10/2015, 12:00**

**Room B108, Computer Science dept., University of Crete**

**“GPU-Disasm: A GPU based x86 Disassembler”**

### ABSTRACT


Static binary code analysis and reverse engineering are crucial operations for malware analysis, binary level software protections, debugging, and patching, among many other tasks. Faster binary code analysis tools are necessary for tasks such as analyzing the multitude of new malware samples gathered every day. Binary code disassembly is a core functionality of such tools which has not received enough attention from a performance perspective. In this paper we introduce GPU-Disasm, a GPU-based disassembly framework for x86 code that takes advantage of graphics processors to achieve efficient large-scale analysis of binary executables. We describe in detail various optimizations and design decisions for achieving both inter-parallelism, to disassemble multiple binaries in parallel, as well as intra-parallelism, to decode multiple instructions of the same binary in parallel. The results of our experimental evaluation in terms of performance and power consumption demonstrate that GPU-Disasm is twice as fast than a CPU disassembler for linear disassembly and 4.4 times faster for exhaustive disassembly, with power consumption comparable to CPU-only implementations.