Εργαστήριο Τεχνολογίας & Αρχιτεκτονικής Υπολογιστών
Τομέας Υλικού & Αρχιτεκτονικής των Υπολογιστών
Τμήμα Μηχανικών Η/Υ & Πληροφορικής
Πολυτεχνική Σχολή - Πανεπιστήμιο Πατρών
https://tcal.ceid.upatras.gr

Θέματα Διπλωματικών Εργασιών

Ακαδημαϊκό Έτος 2026–2027

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ
1

Εκπαιδευτική Επέκταση του Ripes με Απλό Μηχανισμό Πρόβλεψης Διακλαδώσεων

Educational Extension of Ripes with a Simple Branch Prediction Mechanism

Λέξεις κλειδιά: Ripes · RISC-V · Branch Prediction · Control Hazards

ΠΕΡΙΓΡΑΦΗ / ΑΝΤΙΚΕΙΜΕΝΟ

Ο Ripes είναι ανοικτού κώδικα, γραφικός προσομοιωτής RISC-V που χρησιμοποιείται για την εκπαιδευτική μελέτη της εκτέλεσης εντολών, της διοχέτευσης (pipeline), των κινδύνων (hazards) και της ιεραρχίας μνήμης [1,5]. Το υπάρχον μοντέλο επεξεργαστή πέντε σταδίων αντιμετωπίζει τους κινδύνους ελέγχου (control hazards) χωρίς μηχανισμό πρόβλεψης, με αποτέλεσμα η σχέση μεταξύ πρόβλεψης, λανθασμένης πρόβλεψης (misprediction) και ακύρωσης εντολών της διοχέτευσης (pipeline flush) να μην είναι άμεσα ορατή στους φοιτητές. Η εργασία θα επεκτείνει το μοντέλο με έναν απλό και σαφώς οριοθετημένο μηχανισμό πρόβλεψης διακλαδώσεων, με προτεραιότητα στην εκπαιδευτική ορατότητα της συμπεριφοράς του έναντι της πολυπλοκότητας του ίδιου του predictor. Η βασική υλοποίηση θα περιλαμβάνει τη στατική πολιτική Always Not Taken ως σημείο αναφοράς και έναν δυναμικό predictor ενός bit με μικρό, παραμετροποιήσιμο πίνακα ιστορικού διακλαδώσεων (Branch History Table, BHT) [2,3]. Επειδή μια πρόβλεψη «taken» κατά το στάδιο προσκόμισης εντολών (instruction fetch) προϋποθέτει διαθέσιμη διεύθυνση στόχου πριν αυτή υπολογιστεί στο στάδιο εκτέλεσης, θα υλοποιηθεί και ελάχιστος πίνακας στόχων διακλαδώσεων (Branch Target Buffer, BTB)· ο σχεδιασμός της διεπαφής μεταξύ BHT, BTB και επιλογής του επόμενου μετρητή προγράμματος (program counter, PC) αποτελεί το κρίσιμο σημείο της υλοποίησης. Ο predictor θα ενημερώνεται κατά την επίλυση της διακλάδωσης, ενώ σε λανθασμένη πρόβλεψη θα διορθώνεται ο PC και θα ακυρώνονται οι λανθασμένα προσκομισμένες εντολές. Παράλληλα θα προστεθούν βασικές μετρικές, όπως ακρίβεια πρόβλεψης (prediction accuracy), λανθασμένες προβλέψεις και flushes, καθώς και απλή οπτικοποίηση της κατάστασης του predictor, με λειτουργικό σημείο αναφοράς το QtRvSim [4]. Θα μελετηθεί επίσης η προηγούμενη, μη ενσωματωμένη προσπάθεια υλοποίησης στο επίσημο αποθετήριο [6], ώστε να εντοπιστούν εκ των προτέρων τα σχεδιαστικά ζητήματα που εμπόδισαν την ενσωμάτωσή της. Η επαλήθευση θα γίνει με στοχευμένα προγράμματα RISC-V και θα συνοδευτεί από εκπαιδευτικά παραδείγματα για το Εργαστήριο Αρχιτεκτονικής Υπολογιστών. Στόχος είναι μια τεκμηριωμένη και ελεγμένη υλοποίηση, κατάλληλη για άμεση εργαστηριακή χρήση και, εφόσον πληροί τα πρότυπα κώδικα και ελέγχου του έργου, για υποβολή ως συνεισφορά στο επίσημο αποθετήριο του Ripes. Ως προαιρετική επέκταση, μετά την επαλήθευση του βασικού μηχανισμού, μπορεί να προστεθεί predictor δύο bit με κορεσμένους μετρητές (saturating counters) και να συγκριθεί με την έκδοση ενός bit.

ΣΤΟΧΟΙ

1. Μελέτη του μοντέλου επεξεργαστή πέντε σταδίων του Ripes, του υπάρχοντος χειρισμού των control hazards, stalls και flushes, καθώς και της προηγούμενης προσπάθειας υλοποίησης πρόβλεψης στο επίσημο αποθετήριο.
2. Υλοποίηση της στατικής πολιτικής Always Not Taken και δυναμικού predictor ενός bit με παραμετροποιήσιμο BHT και ελάχιστο BTB για την παροχή διεύθυνσης στόχου κατά την προσκόμιση.
3. Ενσωμάτωση της πρόβλεψης στη ροή προσκόμισης εντολών και ορθή ανάκαμψη μετά από misprediction, με διόρθωση του PC και ακύρωση των λανθασμένα προσκομισμένων εντολών.
4. Προσθήκη οπτικοποίησης της κατάστασης του predictor και βασικών μετρικών για prediction accuracy, mispredictions και flushes.
5. Επαλήθευση με στοχευμένα προγράμματα RISC-V, εκπαιδευτικά παραδείγματα για το εργαστήριο και προετοιμασία της υλοποίησης για ενσωμάτωση στο επίσημο αποθετήριο.

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] M. B. Petersen, “Ripes: A Visual Computer Architecture Simulator,” in 2021 ACM/IEEE Workshop on Computer Architecture Education (WCAE), 2021, pp. 1–8, doi: 10.1109/WCAE53984.2021.9707149.

[2] J. E. Smith, “A Study of Branch Prediction Strategies,” in Proc. 8th Annual Symposium on Computer Architecture (ISCA), 1981, pp. 135–148.

[3] D. A. Patterson and J. L. Hennessy, Computer Organization and Design RISC-V Edition: The Hardware/Software Interface, 2nd ed., Morgan Kaufmann, 2020.

[4] J. Dupák, P. Píša, M. Štepanovský and K. Kočí, “QtRVSim – RISC-V Simulator for Computer Architectures Classes,” in embedded world Conference 2022, 2022, pp. 775–778.

[5] M. B. Petersen, Ripes – official source repository, https://github.com/mortbopet/Ripes.

[6] Ripes Project, “Branch prediction processor,” Pull Request #289, https://github.com/mortbopet/Ripes/pull/289.

ΣΧΕΤΙΚΑ ΜΑΘΗΜΑΤΑ

- **Αρχιτεκτονική Υπολογιστών** (CEID_23Y203)
- **Εργαστήριο Αρχιτεκτονικής Υπολογιστών** (CEID_23Y212)
- **Προχωρημένα Θέματα Αρχιτεκτονικής Υπολογιστών** (CEID_NE4617)
- **Αντικειμενοστρεφής Προγραμματισμός** (CEID_23Y106)
- **Προγραμματισμός Συστημάτων** (CEID_25Y401)

ΕΠΙΒΛΕΠΩΝ

Βάιος Παπαϊωάννου, Ε.ΔΙ.Π.

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ

2

Προσαρμόσιμο Σύστημα Ανάκτησης και Συσχέτισης Γνώσης για Ανάλυση Πληροφοριών Κυβερνοαπειλών

Adaptive Knowledge Retrieval and Correlation System for Cyber Threat Intelligence Analysis

Λέξεις κλειδιά: Cyber Threat Intelligence · Ανάκτηση Γνώσης · Μοντέλα Απειλών · MITRE ATT&CK

ΠΕΡΙΓΡΑΦΗ / ΑΝΤΙΚΕΙΜΕΝΟ

Η ανάλυση πληροφοριών κυβερνοαπειλών (Cyber Threat Intelligence, CTI) βασίζεται σε ετερογενείς και συχνά μη δομημένες πηγές, όπως τεχνικές αναφορές περιστατικών, περιγραφές ευπαθειών και αναλύσεις κακόβουλου λογισμικού. Η αξιοποίησή τους δεν απαιτεί μόνο τον εντοπισμό της σχετικής πληροφορίας, αλλά και τη συσχέτισή της με καθιερωμένα μοντέλα γνώσης, ώστε τα ευρήματα να είναι συγκρίσιμα, επαληθεύσιμα και άμεσα αξιοποιήσιμα από έναν αναλυτή. Η εργασία θα σχεδιάσει και θα υλοποιήσει ένα προσαρμόσιμο σύστημα ανάκτησης και συσχέτισης γνώσης, στο οποίο κάθε απάντηση και κάθε συσχέτιση θα ανάγεται ρητά σε ελεγχόμενες πηγές, με έμφαση στην αντιστοίχιση ευρημάτων στις τακτικές και τις τεχνικές του MITRE ATT&CK [2] και, όπου είναι κατάλληλο, στη σύνδεσή τους με τη λειτουργία ανίχνευσης του NIST Cybersecurity Framework [1]. Ως μετρήσιμη εργασία αναφοράς ορίζεται η αντιστοίχιση ελεύθερου κειμένου CTI σε τεχνικές ATT&CK, η οποία επιτρέπει ποσοτική αποτίμηση με ακρίβεια, ανάκληση και F1 έναντι επισημειωμένου συνόλου αναφοράς [7]. Οι επιμέρους τεχνολογικές επιλογές, δηλαδή τα μοντέλα, οι υποδομές αποθήκευσης και οι στρατηγικές ανάκτησης, παραμένουν σκόπιμα ανοικτές και θα καθοριστούν κατά τη διάρκεια της εργασίας· ζητούμενο είναι η αρχιτεκτονική να παραμείνει αρθρωτή, ώστε εναλλακτικές προσεγγίσεις να μπορούν να αντικατασταθούν και να συγκριθούν υπό κοινή μετρική [3–6]. Η βασική εκδοχή θα περιλαμβάνει συλλογή και κανονικοποίηση πηγών, ευρετηρίαση και ανάκτηση, παραγωγή τεκμηριωμένων απαντήσεων και ρητή αναφορά στην πηγή από την οποία προκύπτει κάθε συσχέτιση. Ανάλογα με την πρόοδο και το ενδιαφέρον του φοιτητή ή της φοιτήτριας, η μελέτη μπορεί να επεκταθεί σε πιο δομημένες αναπαραστάσεις της γνώσης και σε συνθετότερες στρατηγικές συσχέτισης μεταξύ οντοτήτων. Ζητούμενο δεν είναι η μέγιστη δυνατή πολυπλοκότητα, αλλά ο τεκμηριωμένος προσδιορισμός των περιπτώσεων στις οποίες μια πιο σύνθετη προσέγγιση βελτιώνει πράγματι το αποτέλεσμα σε σχέση με μια απλούστερη.

ΣΤΟΧΟΙ

1. Μελέτη σύγχρονων προσεγγίσεων ανάκτησης και συσχέτισης γνώσης για CTI, καθώς και των μοντέλων γνώσης MITRE ATT&CK και NIST Cybersecurity Framework.
2. Σχεδίαση αρθρωτής ροής συλλογής, κανονικοποίησης, ευρετηρίασης και ανάκτησης ετερογενών πηγών κυβερνοασφάλειας, με δυνατότητα εναλλαγής επιμέρους συνιστωσών.
3. Υλοποίηση μηχανισμού παραγωγής τεκμηριωμένων απαντήσεων, με ρητή αναφορά στην πηγή κάθε συσχέτισης και αντιστοίχιση σε τακτικές και τεχνικές του ATT&CK.
4. Ορισμός επισημειωμένου συνόλου αξιολόγησης και ποσοτική αποτίμηση της ποιότητας ανάκτησης και της ακρίβειας αντιστοίχισης.
5. Συγκριτική αποτίμηση εναλλακτικών στρατηγικών ανάκτησης υπό κοινή μετρική και προσδιορισμός των περιπτώσεων στις οποίες η πιο δομημένη προσέγγιση βελτιώνει την ανάλυση κυβερνοαπειλών.

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] C. Pascoe, S. Quinn and K. Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.

[2] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, "MITRE ATT&CK: Design and Philosophy," The MITRE Corporation, rev. March 2020.

[3] P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, H. Küttler, M. Lewis, W. Yih, T. Rocktäschel, S. Riedel and D. Kiela, "Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks," in Advances in Neural Information Processing Systems (NeurIPS), vol. 33, 2020, pp. 9459–9474.

[4] A. Lekssays, U. Shukla, H. T. Sencar and M. R. Parvez, "TechniqueRAG: Retrieval Augmented Generation for Adversarial Technique Annotation in Cyber Threat Intelligence Text," in Findings of the Association for Computational Linguistics: ACL 2025, 2025, pp. 20913–20926, doi: 10.18653/v1/2025.findings-acl.1076.

[5] X. Yang, R. Zhong, Y. Chen, G. Peng, D. Yao et al., "CTI-Thinker: An LLM-Driven System for CTI Knowledge Graph Construction and Attack Reasoning," Cybersecurity, vol. 9, no. 1, Article 106, 2026, doi: 10.1186/s42400-025-00505-y.

[6] D. Hamzić, F. Skopik, M. Landauer, M. Wurzenberger and A. Rauber, "Beyond RAG for Cyber Threat Intelligence: A Systematic Evaluation of Graph-Based and Agentic Retrieval," arXiv:2604.11419, 2026 (preprint).

[7] Center for Threat-Informed Defense, TRAM – Threat Report ATT&CK Mapper, https://github.com/center-for-threat-informed-defense/tram.

ΣΧΕΤΙΚΑ ΜΑΘΗΜΑΤΑ

- **Κυβερνοασφάλεια** (CEID_NE590)
- **Τεχνητή Νοημοσύνη** (CEID_24Y351)
- **Ανάκτηση Πληροφορίας** (CEID_NE5597)
- **Βάσεις Δεδομένων** (CEID_24Y334)
- **Θεωρία Γραφημάτων και Εφαρμογές** (CEID_23Y202)

ΕΠΙΒΛΕΠΩΝ

Βάιος Παπαϊωάννου, Ε.ΔΙ.Π.

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ

3

Αυτόματη Παραγωγή Εκτελέσιμων Μηχανισμών Αξιολόγησης για Εργαστηριακές Ασκήσεις RISC-V με Ανάκτηση Γνώσης

Knowledge-Grounded Generation of Executable Graders for RISC-V Laboratory Assignments

Λέξεις κλειδιά: RISC-V · Automated Assessment · Retrieval-Augmented Generation · Mutation Testing

ΠΕΡΙΓΡΑΦΗ / ΑΝΤΙΚΕΙΜΕΝΟ

Η αυτόματη αξιολόγηση προγραμματιστικών ασκήσεων παρέχει άμεση ανατροφοδότηση και μειώνει τον φόρτο διόρθωσης, όμως η κατασκευή αξιόπιστων μηχανισμών αξιολόγησης (graders) παραμένει χειροκίνητη και χρονοβόρα εργασία, καθώς ο διδάσκων πρέπει να μετατρέψει την εκφώνηση σε περιπτώσεις ελέγχου, αναμενόμενα αποτελέσματα και κανόνες ορθότητας [1,2]. Στις ασκήσεις συμβολικής γλώσσας RISC-V η ορθότητα δεν αφορά μόνο την τελική έξοδο, αλλά και την κατάσταση καταχωρητών και μνήμης, τη χρήση της στοίβας, την τήρηση της δυαδικής διεπαφής εφαρμογής (Application Binary Interface, ABI) [3] και περιορισμούς της εκφώνησης, όπως το επιτρεπόμενο υποσύνολο εντολών. Παράλληλα, η απευθείας ανάθεση της βαθμολόγησης σε γλωσσικό μοντέλο εμφανίζει περιορισμένη συμφωνία με ανθρώπινους αξιολογητές και δεν εξασφαλίζει επαναληψιμότητα [4]. Η εργασία θα διερευνήσει υβριδική προσέγγιση, στην οποία το γλωσσικό μοντέλο δεν βαθμολογεί τη λύση αλλά μετατρέπει την εκφώνηση σε δομημένη προδιαγραφή αξιολόγησης, η οποία στη συνέχεια μεταφράζεται σε ντετερμινιστικούς και αναπαραγώγιμους ελέγχους. Σε πρώτο στάδιο θα υλοποιηθεί το εκτελεστικό υπόβαθρο: μηχανισμός που συναρμολογεί και εκτελεί φοιτητικά προγράμματα σε περιβάλλον RISC-V χωρίς γραφική διεπαφή, με χρονικά όρια, απομόνωση και δομημένη καταγραφή της τελικής κατάστασης καταχωρητών, μνήμης και εξόδου· ως υποψήφια υποδομή εξετάζεται, μεταξύ άλλων, ο Ripes [7]. Πάνω σε αυτό θα αναπτυχθεί ο μηχανισμός παραγωγής, όπου η εκφώνηση συνδυάζεται μέσω ανάκτησης-επαυξημένης παραγωγής (Retrieval-Augmented Generation, RAG) [5] με ελεγχόμενες πηγές, όπως η προδιαγραφή της αρχιτεκτονικής, το ABI, οι οδηγίες του εργαστηρίου και ήδη επαληθευμένοι graders, ώστε να παραχθεί προδιαγραφή με εισόδους, αναμενόμενα αποτελέσματα, ελέγχους κατάστασης και συντακτικούς περιορισμούς, επιθεωρήσιμη από τον διδάσκοντα πριν ενεργοποιηθεί. Για την αξιολόγηση, χωρίς εξάρτηση από τη διαθεσιμότητα φοιτητικών δεδομένων, θα κατασκευαστούν συστηματικά μεταλλαγμένες παραλλαγές (mutants) ορθών λύσεων με γνωστά σφάλματα [6], ώστε να μετρηθεί κατά πόσο οι αυτόματα παραγόμενοι graders τις εντοπίζουν. Στόχος είναι ένα εργαλείο άμεσα χρησιμοποιήσιμο στο Εργαστήριο Αρχιτεκτονικής Υπολογιστών και μια τεκμηριωμένη απάντηση στο πόσο αξιόπιστα αυτοματοποιείται η κατασκευή ελέγχων όταν το γλωσσικό μοντέλο περιορίζεται στην παραγωγή προδιαγραφών και όχι στην κρίση. Εκτός πεδίου παραμένουν η αξιολόγηση ποιότητας ή ύφους κώδικα και η παραγωγή τελικού βαθμού.

ΣΤΟΧΟΙ

1. Σχεδίαση δομημένης και εκτελέσιμης αναπαράστασης που αποτυπώνει τις απαιτήσεις μιας άσκησης RISC-V ως ελέγχους επί της εξόδου, των καταχωρητών, της μνήμης, της στοίβας και του ABI.
2. Υλοποίηση αναπαραγώγιμου μηχανισμού εκτέλεσης φοιτητικών προγραμμάτων σε περιβάλλον RISC-V χωρίς γραφική διεπαφή, με χρονικά όρια, απομόνωση και δομημένη καταγραφή κατάστασης.
3. Ανάπτυξη μηχανισμού ανάκτησης γνώσης από τεχνική τεκμηρίωση, εκπαιδευτικό υλικό και επαληθευμένα παραδείγματα, ώστε η παραγόμενη προδιαγραφή να θεμελιώνεται σε ελεγχόμενες πηγές.
4. Αυτόματη παραγωγή περιπτώσεων ελέγχου και κανόνων αξιολόγησης από την εκφώνηση, με δυνατότητα επιθεώρησης και διόρθωσης από τον διδάσκοντα.
5. Πειραματική σύγκριση αυτόματα και χειροκίνητα παραγόμενων graders με μετρικές κάλυψης απαιτήσεων και ψευδώς θετικών ή αρνητικών αποτελεσμάτων.

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] L. Tavares, B. Lima and A. J. Araújo, "Automatic Test-Based Assessment of Assembly Programs," in Proc. 18th International Conference on Software Technologies (ICSOFT), 2023, pp. 572–579, doi: 10.5220/0012129100003538.

[2] U. Alkafaween, I. Albluwi and P. Denny, "Automating Autograding: Large Language Models as Test Suite Generators for Introductory Programming," Journal of Computer Assisted Learning, vol. 41, no. 1, e13100, 2025, doi: 10.1111/jcal.13100.

[3] K. Cheng and J. Clarke (eds.), RISC-V ABIs Specification, Document Version 1.0, RISC-V International, November 2022, https://docs.riscv.org/reference/abi/v1.0/.

[4] K. Mohamed, M. Yousef, W. Medhat, E. H. Mohamed, G. Khoriba and T. Arafa, "Hands-on Analysis of Using Large Language Models for the Auto Evaluation of Programming Assignments," Information Systems, vol. 128, 102473, 2024, doi: 10.1016/j.is.2024.102473.

[5] Z. Li, Z. Wang, W. Wang, K. Hung, H. Xie and F. L. Wang, "Retrieval-Augmented Generation for Educational Application: A Systematic Survey," Computers and Education: Artificial Intelligence, vol. 8, 100417, 2025, doi: 10.1016/j.caeai.2025.100417.

[6] Y. Jia and M. Harman, "An Analysis and Survey of the Development of Mutation Testing," IEEE Transactions on Software Engineering, vol. 37, no. 5, pp. 649–678, 2011, doi: 10.1109/TSE.2010.62.

[7] M. B. Petersen, "Ripes: A Visual Computer Architecture Simulator," in 2021 ACM/IEEE Workshop on Computer Architecture Education (WCAE), 2021, pp. 1–8, doi: 10.1109/WCAE53984.2021.9707149.

ΣΧΕΤΙΚΑ ΜΑΘΗΜΑΤΑ

- **Αρχιτεκτονική Υπολογιστών** (CEID_23Y203)
- **Εργαστήριο Αρχιτεκτονικής Υπολογιστών** (CEID_23Y212)
- **Προγραμματισμός Συστημάτων** (CEID_25Y401)
- **Τεχνολογία Λογισμικού** (CEID_24Y332)
- **Ποιότητα Λογισμικού** (CEID_NE5577)
- **Τεχνητή Νοημοσύνη** (CEID_24Y351)

ΕΠΙΒΛΕΠΩΝ

Βάιος Παπαϊωάννου, Ε.ΔΙ.Π.