ΕΠΛ326: Ασφάλεια Συστημάτων

Πανεπιστήμιο Κύπρου
Τμήμα Πληροφορικής

Microsoft Teams

Άνοιξη
2024

Διδάσκων	Ηλίας Αθανασόπουλος, https://elathan.github.io
Ώρες γραφείου	Τρίτη 12:00-13:00, Τετάρτη 12:00-13:00 (κατόπιν συνεννόησης), ΘΕΕ01 - Β105/Microsoft Teams
Πίστωση	7.5 ECTS

Περιγραφή

Το μάθημα πραγματεύεται θεμελιώδη θέματα ανάλυσης λογισμικού πολλαπλών μορφών και για διαφορετικούς σκοπούς. Πολλές φορές, χρειάζεται να αναλύσουμε λογισμικό για (α) εύρεση λαθών (αποσφαλμάτωση), (β) μέτρηση σημείων καθυστέρησης (profiling), (γ) προσθήκη επιπλέον κώδικα, ο οποίος αλλάζει τη λειτουργικότητα του προγράμματος (π.χ., προσθήκη μιας συγκεκριμένης αμυντικής λειτουργίας). Το μάθημα αναδεικνύει διάφορες τεχνικές για άμεση τροποποίηση της δυαδικής μορφής ενός προγράμματος (ανάλυση και επανεγγραφή), όπως και τον εμπλουτισμό υφιστάμενου κώδικα C/C++ με τη βοήθεια επέκτασης σύγχρονων εργαλειοθηκών μεταγλωττιστών (LLVM). Το μάθημα αξιολογείται με 7.5 μονάδες ECTS. Για την παρακολούθηση του μαθήματος ο φοιτητής καλείται να έχει παρακολουθήσει επιτυχώς τα: *ΕΠΛ211, Θεωρία Υπολογισμού και Πολυπλοκότητα* και *ΕΠΛ232, Προγραμματιστικές Τεχνικές και Εργαλεία*.

Περιεχόμενο

Μια ενδεικτική λίστα με την ύλη του μαθήματος, είναι η ακόλουθη.

- Το πρότυπο ELF για δυαδικά αρχεία στο Unix,
- εργαλεία τα οποία επεξεργάζονται δυαδικά αρχεία στο Unix (επισκόπηση διαφορετικών περιοχών, σύμβολων, βιβλιοθηκών, κ.λπ.),
- ο μηχανισμός με τον οποίο λειτουργούν τα relocations και οι κοινές βιβλιοθήκες στα δυαδικά αρχεία (η χρήση του PLT/GOT),
- η χρήση του ptrace(),
- προ-φόρτωση (preloading) δυαδικών αρχείων,
- οι βιβλιοθήκες χειρισμού δυαδικών αρχείων, libbfd/libelf
- από-συναρμολόγηση (disassembling) δυαδικών αρχείων με τη βοήθεια του Capstone,
- επανεγγραφή δυαδικών αρχείων με προγραμματιστικό τρόπο,
- δυναμική και στατική ανάλυση δυαδικού κώδικα,
- εμπλουτισμός κώδικα C/C++ με τη βοήθεια του LLVM,
- εφαρμογές της ανάλυσης λογισμικού

Διαλέξεις και Εργαστήριο

Η διδασκαλία του μαθήματος αποτελείται από διαλέξεις, και εργαστήρια. Οι φοιτητές παρακαλούνται όπως προσέρχονται στην αίθουσα --είτε αυτή είναι φυσική, είτε εικονική-- των διαλέξεων έγκαιρα. Βασικός στόχος είναι η ενεργή συμμετοχή των φοιτητών μέσω ερωτήσεων, παρουσιάσεων και προγραμματιστικών ασκήσεων.

Στα εργαστήρια του μαθήματος οι φοιτητές θα έχουν την δυνατότητα να υποβοηθούνται στην υλοποίηση των αρχών που διδάσκονται στις διαλέξεις. Τα εργαστήρια θα ανακοινώνονται κατά τη διάρκεια των διαλέξεων.

Πρόγραμμα Διαλέξεων

Οι διαλέξεις θα γίνονται σύμφωνα με το υγειονομικό πρωτοκόλλου του Πανεπιστημίου Κύπρου. Σε περίπτωση που οι διαλέξεις γίνοται δικτυακά, θα χρησιμοποιείται το Microsoft Teams και δεν θα βιντεοσκοπούνται.

Αξιολόγηση

Η επίδοση των φοιτητών θα αξιολογείται συνεχώς με βάση γραπτές εξετάσεις, ασκήσεις διαγνωστικά. Η αναλογία ως προς τον τελικό βαθμό είναι η εξής:

- 50% τελική εξέταση,
- 30% ενδιάμεση εξέταση,
- 20% προγραμματιστικές ασκήσεις

Η παρακολούθηση του μαθήματος θεωρείται επιτυχής εάν ισχύουν όλες οι ακόλουθες συνθήκες:

- όλες οι ασκήσεις έχουν παραδοθεί,
- ο τελικός βαθμός είναι τουλάχιστον 5.

Παραβάσεις

Η αντιγραφή ή η προσπάθεια αντιγραφής μεταξύ φοιτητών σε εξετάσεις ή εργασίες, απαγορεύεται αυστηρά. Οι εργασίες θα ελέγχονται με λογισμικό εντοπισμού αντιγραφής και όλα τα ατυχή περιστατικά θα συνεπάγονται στην αυτόματη αποπομπή των εμπλεκόμενων φοιτητών από την τάξη, τον μηδενισμό του βαθμού τους στις εν λόγω εξετάσεις ή εργασίες και την καταγγελία τους στο συμβούλιο του τμήματος για την εφαρμογή περαιτέρω πειθαρχικών κανόνων.

Βιβλιογραφια

Οι διαλέξεις βασίζονται σε υλικό των παρακάτω εγχειριδίων:

1. Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. Dennis Andriesse. ISBN-10: 1593279124.
2. Τεκμηρίωση LLVM (https://llvm.org/).
3. Δημοσιεύσεις.

Κατά τη διάρκεια των διαλέξεων θα δοθεί επιπλέον υλικό υπό μορφή δημοσιεύσεων, άρθρων, και λογισμικού.