



## ΕΠΛ682: Προχωρημένα Θέματα Ασφάλειας

Πανεπιστήμιο Κύπρου,  
Τμήμα Πληροφορικής

<https://piazza.com/>  
<https://www.cs.ucy.ac.cy/courses/EPL682/>

Άνοιξη  
2020

<b>Διδάσκων:</b>	Ηλίας Αθανασόπουλος
<b>Γραφείο:</b>	ΘΕΕ01 Β105
<b>Τηλέφωνο:</b>	2289 2754
<b>E-mail:</b>	<a href="mailto:eliasathan@cs.ucy.ac.cy">eliasathan@cs.ucy.ac.cy</a>
<b>Ώρες γραφείου:</b>	Τρίτη 12:00-14:00
<b>Διαλέξεις:</b>	Πέμπτη, 15:00-18:00 (ΘΕΕ01 147)
<b>Φροντιστήριο:</b>	Πέμπτη, 14:00-15:00 (ΘΕΕ01 147)
<b>Πίστωση:</b>	8 μονάδες ECTS

### ΠΕΡΙΓΡΑΦΗ

Το μάθημα ασχολείται με σύγχρονα και προχωρημένα θέματα ασφάλειας υπολογιστικών συστημάτων. Κατά τη διάρκεια του εξαμήνου θα παρουσιαστούν θέματα εφαρμοσμένης κρυπτογραφίας, ασφάλεια λογισμικού και λειτουργικών συστημάτων (επιθέσεις και άμυνες), ασφάλεια δικτύου, ασφάλεια εφαρμογών παγκόσμιου ιστού, ασφάλεια κινητών εφαρμογών, ανωνυμία και ιδιωτικότητα. Όλα τα θέματα θα παρουσιαστούν μέσα από επιστημονικές δημοσιεύσεις.

Οι φοιτητές θα πρέπει να εκπονήσουν ατομικές παρουσιάσεις δημοσιεύσεων που έχουν επιλεγεί από τον διδάσκοντα. Όλες οι δημοσιεύσεις έχουν κεντρικό θέμα την ασφάλεια υπολογιστικών συστημάτων και έχουν παρουσιαστεί στα κορυφαία συνέδρια του χώρου (IEEE S&P, ACM CCS, Usenix Security, κ.λπ.).

Το μάθημα αξιολογείται με 8 μονάδες ECTS.

### ΔΙΑΛΕΞΕΙΣ ΚΑΙ ΠΑΡΟΥΣΙΑΣΕΙΣ ΔΗΜΟΣΙΕΥΣΕΩΝ

Η διδασκαλία του μαθήματος αποτελείται από διαλέξεις, φροντιστήρια και συζήτηση δημοσιεύσεων. Οι φοιτητές παρακαλούνται όπως προσέρχονται στην αίθουσα των διαλέξεων έγκαιρα. Βασικός στόχος είναι η ενεργή συμμετοχή των φοιτητών μέσω ερωτήσεων και γενικής συζήτησης. Οι φοιτητές καλούνται να προμηθεύονται τις σημειώσεις των διαλέξεων από την ιστοσελίδα του μαθήματος πριν από κάθε διάλεξη.

Ο κάθε φοιτητής θα πρέπει να παρουσιάσει 2 δημοσιεύσεις. Κατόπιν θα πρέπει να κάνει μια εργασία, η οποία περιγράφει το θέμα των δημοσιεύσεων που παρουσίασε. Η εργασία αυτή θα είναι δημόσια και θα μπορεί να χρησιμοποιηθεί για μελέτη από το υπόλοιπο ακροατήριο. Η τελική εξέταση περιλαμβάνει την ύλη που έχει καλύψει ο διδάσκοντας και την ύλη που έχει καλύψει το ακροατήριο.

### ΑΞΙΟΛΟΓΗΣΗ

Η επίδοση των φοιτητών αξιολογείται με βάση γραπτές εξετάσεις, παρουσιάσεις και εργασίες (βασισμένες στις παρουσιάσεις). Η αναλογία ως προς τον τελικό βαθμό είναι η εξής:

- 80% Τελική Εξέταση
- 20% Παρουσίαση Δημοσιεύσεων και Εργασία

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

- η παρουσίαση έχει εκπονηθεί,
- ο βαθμός της τελικής εξέτασης είναι τουλάχιστον 4.5,
- ο τελικός βαθμός είναι τουλάχιστον 5.

Αν ο βαθμός της τελικής εξέτασης είναι μικρότερος από το 4.5 τότε ο τελικός βαθμός θα είναι αυτός της τελικής εξέτασης. Η αντιγραφή ή η προσπάθεια αντιγραφής μεταξύ φοιτητών σε εξετάσεις ή εργασίες, απαγορεύεται αυστηρά.

#### **ΒΙΒΛΙΟΓΡΑΦΙΑ**

Εκτός από τις σημειώσεις διαλέξεων και τις δημοσιεύσεις που θα παρουσιαστούν από το ακροατήριο, για επιπλέον πληροφορίες προτείνονται τα παρακάτω συγγράμματα, τα οποία διατίθενται ελεύθερα:

- Handbook of Applied Cryptography, <http://cacr.uwaterloo.ca/hac/>
- Security Engineering – A Guide to Building Dependable Distributed Systems, <http://www.cl.cam.ac.uk/~rja14/book.html>