046280 – עקרונות וכלים באבטחת מחשבים

הקורס מנוהל במערכת ה-Moodle. על הסטודנטים לעקוב אחר הפרסומים המופיעים באתר הקורס.

צורת למידה:

הקורס יועבר במתכונת **פרונטלית בלבד**.

חומר לימוד:

אבטחה הינה דרישה בסיסית בתכן מערכות מחשב מודרניות, החל משרתים, דרך מכשירים ניידים, כלי רכב, וכלה בהתקני IOT. קורס זה מספק כלים בסיסיים לתכן וניתוח אבטחה של מערכות מחשב.

הנושאים כוללים: עקרונות (מדיניות, איומים, פגיעויות), כלים קריפטוגרפיים (הגדרות, מפתח סמטרי וציבורי, מערכות קריפטוגרפיות, מנגנון דיפי-הלמן, פונקציות גיבוב), אימות (אדם ומכונה, מפתחות מרובים), הרשאה, פרטיות (אנונימיות, DIFFERENTIAL PRIVACY, באינטרנט), אבטחה עם תורת המשחקים (בלוקצ'יין, הוכחת עבודה, הוכחת השקעה), אבטחת חומרה (סביבות ריצה אמינות, SGX, TRUSTZONE), בעיית ה CONFINEMENT, זרימת מידע, התקפות ערוצי צד ופתרונות (תזמון מטמון, ערוץ כוח, ריצה ספקולטיבית, ROWHAMMER).

ספרי לימוד:

1. Bitcoin and cryptocurrency technologies: a comprehensive introduction - Narayanan, Arvind
2. Cryptography: theory and practice - Stinson, Douglas R
3. Introduction to computer security - Bishop, Matt

בנוסף, ניתן להשתמש בהרצאות מוקלטות מהשנה שעברה. **שימו לב כי יש הבדל בין החומר הנלמד בסמסטרים קודמים לחומר בסמסטר הקרוב**.

תוצאות למידה:

בוגרי הקורס ירכשו את המיומנויות הבאות:

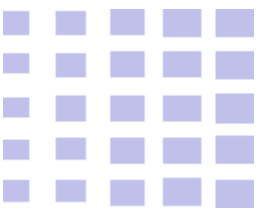
1. ניתוח אבטחה של מערכת מחשב במגוון פרספקטיבות (פגיעויות, אימות, כלים קריפטוגרפיים וכיו"ב).
2. תכן מערכות בטוחות בצורה מובנית (בחירת מודל איום מתאים, מדיניות וכלים).

מרצה:

ד"ר איתי אייל
דוא"ל: ittay@technion.ac.il
שעת קבלה: בתיאום במייל.

מתרגל ובודק תרגילים:

רועי בר-צור (הכתובת לכל שאלה אדמיניסטרטיבית)
דוא"ל: roi.bar-zur@campus.technion.ac.il
שעת קבלה: בתיאום במייל.



<u>מרכיבי הציון</u>:

1. <u>עבודות בית</u>:
ארבעה תרגילי בית. 30% תקף. הגשה בזוגות בלבד. תרגילי הבית יכללו חלק "יבש" וחלק "רטוב". הגשה אלקטרונית בלבד במודל. לא יינתנו דחיות בהגשת תרגילי הבית למעט מקרים חריגים (**בתיאום מראש** עם המתרגל האחראי).

תרגיל בית	פרסום	הגשה
1	15/11/22	29/11/22
2	29/11/22	27/12/22
3	27/12/22	10/01/23
4	10/01/23	24/01/23

2. <u>בחינה סופית</u>:
הבחינה מהווה 70% מהציון הסופי בקורס.

מועד א': 02/02/2023
מועד ב': 02/03/2023

יש לקבל ציון "עובר" גם בבחינה וגם בש"ב על מנת שהציון ישוקלל ע"י 70% בחינה ו-30% ש"ב. אם אחד מהציונים אינו "עובר", הציון הסופי יהיה הנמוך מבין השניים.