046280 – עקרונות וכלים באבטחת מחשבים תשפ"ז

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

צורת למידה:

הקורס יועבר במתכונת פרונטלית.

חומר לימוד:

אבטחה הינה דרישה בסיסית בתכן מערכות מחשב מודרניות, החל משרתים, דרך מכשירים ניידים וכלי רכב ועד התקני IOT. קורס זה מספק כלים בסיסיים לתכן וניתוח אבטחה של מערכות מחשב ובכלל.

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) והתקפות ערוצי צד ופתרונות (תזמון מטמון, ערוץ כוח, ריצה ספקולטיבית).

ספרי לימוד:

1. Introduction to computer security - Bishop, Matt
2. Bitcoin and cryptocurrency technologies: a comprehensive introduction - Narayanan, Arvind
3. Cryptography: theory and practice - Stinson, Douglas R
4. Textbook on cybersecurity (as yet, untitled)- Schneider, Fred B

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:

פרופ' חבר איתי אייל
דוא"ל: ittay@technion.ac.il
שעת קבלה: בתיאום במייל.

מתרגלת ובודקת תרגילים:

מרוה מועלם (הכתובת לכל שאלה אדמיניסטרטיבית)
דוא"ל: marwamouallem@campus.technion.ac.il
שעת קבלה: בתיאום במייל.

<u>מרכיבי הציון:</u>

1. <u>בחינה סופית</u>:
   הבחינה מהווה 100% מהציון הסופי בקורס.
   הבחינה תכלול שאלות ברוח תרגילי הבית.

   מועד א': 11/02/27
   מועד ב': 11/03/27

2. <u>עבודות בית + בחני כיתה</u>:
   כ-10 תרגילי בית: תרגיל בית לכל נושא שיתפרסם לאחר שנלמד את הנושא. תרגילי הבית לא ייבדקו.
   בהרצאה / תרגול בשבוע העוקב נקיים בחן קצר (כ-5 דקות) על תרגיל הבית האחרון. כל בחן יעניק 0.5 נקודות בונוס לציון הסופי. ניתן לצבור עד 5 נקודות בונוס.

שימו לב! יש לקבל ציון "עובר" בבחינה על מנת לקבל את הבונוס של הבחנים.