

046280 – עקרונות וכלים באבטחת מחשבים

בעקבות המצב, בסמסטר הקרוב, מספר נושאים יילמדו במתכונת מצומצמת ביחס לסמסטרים קודמים. ניתן להשתמש בהרצאות מוקלטות מהשנה שעברה. יחד עם זאת, שימו לב כי יש נושאים שלא מופיעים בהקלטות.

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, כלי רכב, והתקני 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.

מתרגל ובודק תרגילים:

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



מרכיבי הציון:

1. עבודות בית:

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 או מילואים (בתיאום מראש עם המתרגל האחראי). בשל המצב, היקף תרגילי הבית הוקטן ביחס לסמסטרים קודמים.

תרגיל בית	פרסום*	הגשה*
1	25/01/24	07/02/24
2	08/02/24	21/02/24
3	22/02/24	13/03/24
4	14/03/24	27/03/24

* התאריכים עלולים להשתנות בשל המצב.

2. בחינה סופית:

הבחינה מהווה 70% מהציון הסופי בקורס.

מועד א': יפורסם בקרוב

מועד ב': יפורסם בקרוב

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.

