שיטות פורמליות לאימות תוכנה ותכונות אבטחה - 236624

דרישות קדם:
לוגיקה ומבוא לאימות תוכנה או ניסיון בתחום (באישור המרצה).

סילבוס:
בקורס זה נלמד איך להוכיח נכונות של תכניות באמצעות אלגוריתמי בדיקת מודל. הקורס יכלול פן תיאורטי ומעשי, ויתחלק לשני חלקים עיקריים: בחלק א׳ נעסוק בפן התיאורטי של אלגוריתמי הוכחה, ובחלק ב׳ נעסוק ביישומים של אלגוריתמים אלה בעבור אימות של תוכנה ותכונות אבטחה. לדוגמא, נלמד כיצד להוכיח (או להפריך) את עמידותה של תכנית כנגד מתקפות ערוצי-צד (side-channel attacks). כמו כן, ״נלכלך את הידיים״ ונלמד להשתמש בכלים קיימים המיישמים את העקרונות אותם נלמד בקורס.
נושאים שיכוסו במסגרת הקורס:

1. אלגוריתמי SAT ו-SMT, מערכת הוכחה מסוג רזולוציה וכללי היסק.
2. בדיקת מודל חסומה ואינדוקציה.
3. אימות תוכנה: מעבר מקוד ללוגיקה.
4. אלגוריתמי הוכחה מבוססי SAT/SMT (על ידי שימוש באינטרפולציה והכללה אינדוקטיבית).
5. מודלי התקפות סייבר, זליגת מידע ומתקפות side-channel.
6. מידול פורמלי של תכונות אבטחה על ידי הייפר-תכונות.
7. בדיקת מודל עבור הייפר-תוכנות (hyper-properties) ע״י שימוש בהרכבה עצמית.
8. נושאים נוספים (באם יהיה זמן).

דרישות הקורס:

- תרגילי בית תיאורטיים ומעשיים
- מיני-פרויקט
- אין בחינה סופית

קורס צמוד 236346:
הקורס יינתן במקביל לקורס פרויקט באימות תוכנה (236346). מי שמעוניין לקחת את שני הקורסים בצמידות לא יידרש לבצע את מתלת הסיום בקורס (מיני-פרויקט). בנוסף, לאור החפיפה בין חלק מהנושאים, לא יהיה צורך להשתתף בכל ההרצאות של קורס הפרויקט.