**פרוייקט באבטחת מידע**

**236349**

**מנחה:**

אלי קופלביץ

Email : elikop@cs.technion.ac.il

טלפון: 04-8292979

1. **בית חכם מאובטח**

במסגרת פרוייקט הבית החכם מפותחת מערכת לשליטה על מכשירים חשמליים בבית על גבי רשת התקשורת הביתית. השליטה על המכשירים מתבצעת מאפליקציה בטלפון סלולארי המעבירה פקודות לשרת בענן. השרת בענן ייתקשר עם בקר מרכזי בבית.

המטרה במסגרת פרוייקט זה לשלב מגנוני אבטחה קריפטוגרפיים בפרוייקט הבית החכם כדי למנוע השתלטות על מכשירי הבית ע"י גורמים לא רצויים. מנגנוני האבטחה יכילו מספר מנגנונים קריפטוגרפיים כמו הצפנה, חתימה דיגיטלית ועוד.

במסגרת הפרוייקט, הסטודנטים יאפיינו את שיטות האבטחה הנחוצות. יגדירו את אופן המימוש הקריפטוגרפי וייבחרו את השיטות הקריפטוגרפיות תוך התחשבות בשיקולי ביצועים של המעבדים השונים בפרוייקט. לאחר השלמת התכן, יממשו הסטודנטים בפועל, את האבטחה על גבי פלטפורמה שתיבחר ויוודאו שהמימוש נותן מענה לדרישות. מבנה המערכת ופלטפורמת העבודה ייבחנו ויוגדרו בתחילת הפרוייקט, בשיתוף הסטודנטים.

שתי הפלטפורמות שייבחנו עבור הבקר המרכזי בבית הינן מימוש במחשב אישי (PC),

ומימוש בטלויזיה ה"חכמה" של Samsung בפלטפורמת Tizen.

האבטחה תבוצע בשיטה הבאה:

* גישה מרכזית לשליטה על האובייקטים בבית, ע"י התקשרות של הדיירים לבקר מרכזי וביצוע אימות מול הבקר שימומש על הפלטפורמה שתיבחר.
* הבקר המרכזי יאפשר גישה לאחת או יותר מרשימת הפעולות של המערכת ע"י בדיקת הרשאות הגישה.

עבור כל אחת מהפעולות תהיה רשימת דיירים מורשים, שתוגדר ע"י בעל הבית, שיוכל לשנותה מעת לעת, כמו גם את ההרשאות עצמן שיורשו לכל דייר.

הפרוייקט ייבוצע בשיתוף המעבדה לפיתוח תוכנה ומערכות (SSDL) ועם מעבדות נוספות

בפקולטה.

דרישות קדם:

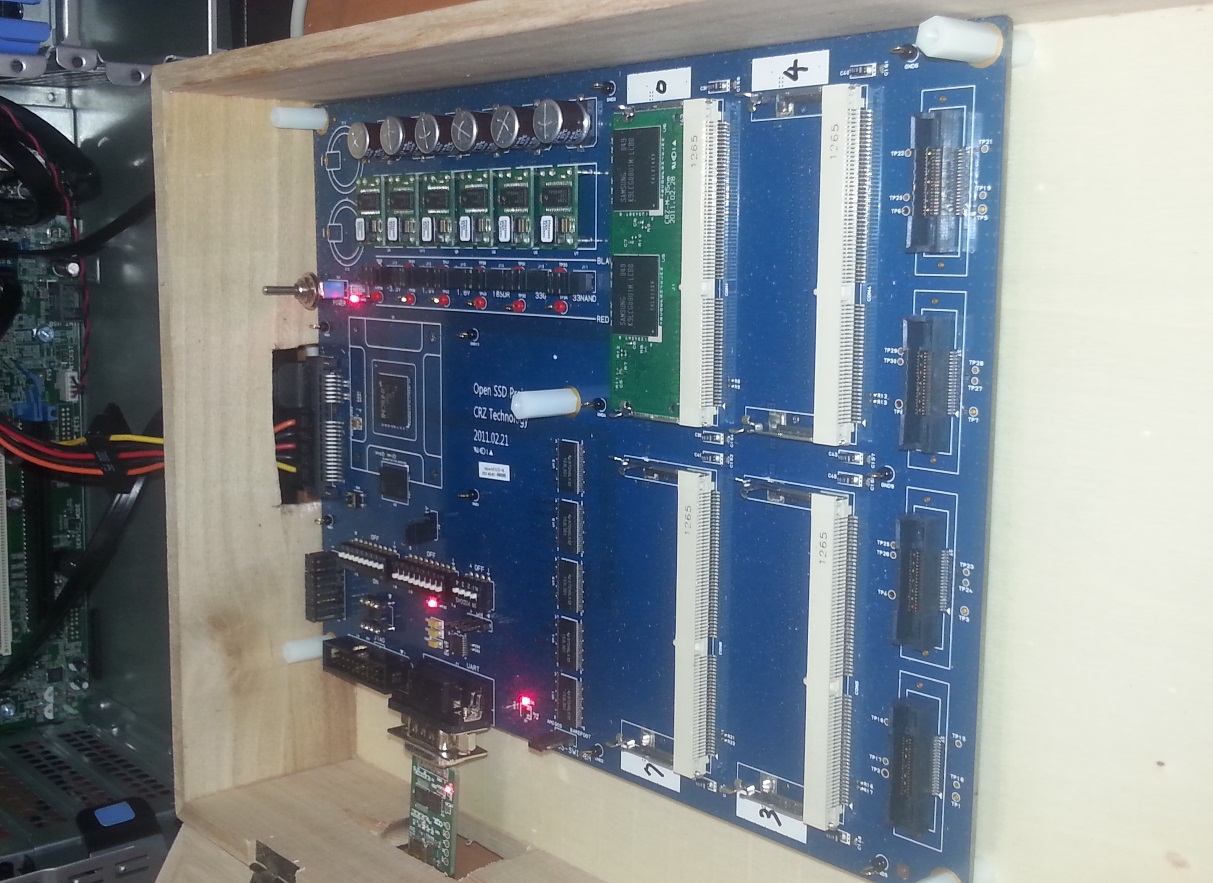
* ידע בתכנות בשפת C.
* הקורס הגנה במערכות מתוכנתות.
* הקורס קריפטולוגיה מודרנית - יתרון, אך לא חובה.

1. **זכרון בטוח**

מטרת הפרוייקט להבטיח שגישה ממחשב לכונן קשיח מסוג SSD (FLASH), תהיה רק למורשים ושהמידע בזכרון לא ישונה ע"י גורמים לא מורשים. בפרוייקט המוצע, יהפוך הזכרון לזכרון בטוח באמצעות שילוב מנגנוני אבטחה קריפטוגרפיים.

במסגרת הפרוייקט יפותח API שייאפשר גישה מאובטחת לאזורי הזכרון השונים, לצורך הגנה על סודיות הנתונים ועל שלמותם.

הגישה לזכרון תהיה גישה ישירה לרכיבי הזכרון או לחילופין תוך שימוש בשרותים של אחת ממערכות ההפעלה הנפוצות (windows או Linux).

בפרוייקט ייעשה שימוש בכרטיס בקר ייעודי של כונן קשיח מסוג SSD הנמצא במעבדה.

במסגרת הפרוייקט, הסטודנטים יגדירו את אופן המימוש, יבחרו את המנגנונים הקריפטוגרפיים המתאימים תוך התאמה לבקר (המותקן בכרטיס הזכרון מסוג ARM 32 bit), יממשו את האבטחה ובסיום המימוש יוודאו את השגת המטרה שהוגדרה.

הפרוייקט הינו פרוייקט משותף למעבדה לסייבר ואבטחת מידע ולמעבדה לזיכרון בלתי נדיף.

דרישות קדם:

* ידע בתכנות בשפת C.
* הקורס הגנה במערכות מתוכנתות.
* הקורס קריפטולוגיה מודרנית - יתרון, אך לא חובה.
* הכרות עם אופני גישה לכונן הקשיח, באמצעות מערכת ההפעלה, תהווה יתרון.