דו"ח 1 - פרויקט

תיאור ההתקדמות מול התכנון ופערי ביצוע:

עד כה עבדנו על שני השלבים הראשונים לפי פירוט תכנית העבודה.
להלן פירוט ההתקדמות, פערי תכנון מול ביצוע ותכנון ההתמודדות:

שלב א' – יצירת התקפת rootkit:

השלב הקונספטואלי:

- **הכרת ה Linux Kernel לעומקו** - קיבצנו מקורות מידע העוסקים בנושא ולמדנו אותם.
- **תכנון התקפת rootkit שתצליח לרוץ ב- Ring 0 ולהשיג שליטה על טבלת קריאות המערכת ב Kernel על מנת לשנות אותה ולהשיג שליטה על תכנית ה-SGX שתרוץ ב-enclave המוצפן** - תכננו התקפה שתצליח לדרוס את ה-syscall table של מ"ה ותעקוף את מנגון ה- Attestation שמוודא את אמינותו של מקור מידע חיצוני ל-enclave.

פערים בשלב המעשי:

- **כתיבת תכנית ההתקפה בשפת C כך שתשנה את הsyscall table במ"ה Linux** - תוך כדי עבודה גילינו שגרסאות עדכניות של Linux kernel מכילות מנגנוני הגנה מורכבים על מנת למנוע התערבות חיצונית בקבצי המערכת. לבינתיים ההתקפה עובדת על גרסאות ישנות של הקרנל, אך אנו צריכים לגרום לה לעבוד גם עם גרסאות עדכניות יותר, זאת מכיוון שלגרסאות ישנות יותר אין תמיכה ב-SGX. המשך עשייה בליווי וייעוץ מנחה הפרוייקט.
- **הרצת ההתקפה ווידוא יעילותה במצבים שונים.** - לביצוע עתידי.

שלב ב' – תכנון וכתיבת ההתקפה:

השלב הקונספטואלי:

- **הכרת תהליך ה - Attestaion הקריפטוגרפי, התאמת הדרישות לתכניתנו.**
- **הכרת ארכיטקטורת Intel SGX ,רכיביה השונים, דרכי העבודה מול שרתי Intel ועבודה עם ה-API המסופק על ידי אינטל למפתחים** - הורדנו את מסמך הדוקומנטציה לפיתוח ב-SGX מהאתר הרשמי של אינטל המפרט לעומק על הארכיטקטורה, ספריות ה-API ותהליך ה-Attestation. תרגמנו, סיכמנו ולמדנו את חלקי המסמך המהותיים והרלוונטיים לפרויקט שלנו.

השלב המעשי:

- **שימוש באמולטור המדמה הרצת תכניות ב-enclave בסביבת SGX ומעקב אחר ריצת התכנית ב-enclave באמצעות EPCM ו-TCS המשקפים את מצב הזיכרון המטמון והזיכרון ה-RAM על מנת לוודא שההתקפה אכן מצליחה לשבש את ריצת התכנית -** התקנו את האמולטור המאפשר להריץ תכניות SGX במצב סימולציה לצרכי פיתוח, בדיקות והדגמה.
- **יצירת תכנית שתפקידה לרוץ ב-enclave של Intel SGX ולחשוף את פרצת האבטחה של הארכיטקטורה בעת מעבר ל - kernel mode** - כתבנו תכנית בסיסית בשפת CPP שרצה בתוך enclave מוצפן ומקבלת מידע חיצוני לenclave באמצעות מנגנון ה-Attestation. התכנית מדפיסה למסך בזמן אמת מידע על כניסה/יציאה מה-enclave וכמו כן על כמות הזיכרון שהenclave תופס וכמות הזיכרון שנאטמת (אטימה ב-SGX מתייחסת למידע שיישמר על ה-HD תחת הצפנה לשימוש חוזר בהרצות הבאות של הencalve).
- **קבלת מפתח מוצפן ייחודי לתכניתנו משרתי Intel באמצעות מנגנון ה -Attestation** - בוצע במצב סימולציה (מפתח לצרכי פיתוח).

פירוט שעות עבודה:

פגישה עם המנחה – אנחנו נפגשים עם מנחה הפרויקט לפי הצורך שעולה מן הקשיים הנלווים לעשיית השלבים והתמודדות עם נושאים אשר אינם מוכרים ובעלי מידע נרחב. (הפרויקט נעשה במ"ה לינוקס שעבורה הושק ה SGX רק בשנת 2016. מכאן המידע המועט שנמצא ברשת לגבי נושאי הפרויקט).
עבודה עצמאית – לאחר הפגישה, כל אחד מיישם חלק מהמשימות שקבענו לעצמנו ביחד עם המנחה. מספר שעות עבודה שבועיות: כ-10 שעות.

316295005 daniella.fertouk@gmail.com דניאלה פרטוק
203839030 atrap11@gmail.com עידו אמיתי
204326755 dan.blumen1@gmail.com דן בלומנברג