מסמך דרישות פרויקט

316295005 דניאלה פרטוק
203839030 עידו אמיתי
204326755 דן בלומנברג

כללי:

Intel SGX הוא רכיב במעבדים חדישים של אינטל המאפשר לקוד ברמת המשתמש להקצות אזורים פרטיים של זיכרון, הנקראים enclaves, המוגנים מפני תהליכים הפועלים ברמות הרשאה גבוהות יותר. אינטל עיצבה את SGX כדי להיות שימושי ליישום חישוב מרחוק מאובטח, גלישה מאובטחת באינטרנט וניהול זכויות דיגיטליות (DRM).
פרויקט זה עוסק בהתגוננות מפני התקפות rootkit באמצעות סביבה מוגנת ע"י Intel SGX במ"ה Linux.
תחילה, ניצור תוכנית הרצה בתוך enclave בסביבת SGX.
לאחר מכן, נתכנן התקפת rootkit שתוכל לשבש את ריצת התוכנית הרצה בenclave, ובכך לחשוף את פגיעותה של המערכת, ואת הפירצות הקיימות ביחס להתקפות מסוג זה.
התקפת הrootkit שבה נתמקד בתחילה תהיה התקפה שמשנה את הsyscall table של מ"ה על מנת להשיג שליטה על המערכת. זאת מכיוון שקריאות מערכת מחייבות מעבר המערכת ל-kernel mode. אנו מעוניינים להראות שלא ניתן לסמוך על הגנת מערכת ההפעלה במצב זה והיא אינה מספקת, ובכך מונעת מ-SGX להבטיח את ההגנה הרצויה.
נתעמק בהכרת הkernel וארכיטקטורת SGX על מנת לתכנן התקפה מתוחכמת שתנצל את חולשות הSGX.
לאחר מכן, נתרכז בכתיבת תכנית נוספת, שתהווה פתרון לפירצת האבטחה ותבטיח הגנה מפני התקפות rootkit מסוג זה ודומות לה תוך שימוש בתכונות מתקדמות שפותחו על ידי אינטל כדוגמת EPCM ו-TCS למעקב אחר זיכרון המטמון וזיכרון ה-RAM ומעקב אחר תהליכונים.
חלק מאתגר נוסף יהיה לבחון את השפעות תכניתנו על שאר ההיבטים האבטחתיים שמציע ה-SGX ולוודא שלא פגענו ביכולתו להגן על התהליך שרץ ב-enclave.

מימוש:

- התקפת rootkit באמצעות c/cpp.
- אימולטור להרצת תוכניות בסביבת SGX למחשבים שאינם נתמכים.
- כתיבת תכנית נוספת שתרוץ ברמת הkernel או הרחבה ל-SGX שתמנע תקיפות מסוג זה ודומותיה.
- בחינה לעומק של יכולות ההגנה והשפעה על היבטים הגנתיים אחרים של תכניתנו על מערכת שמריצה תכניות המוגנות על ידי SGX בזמן אמת.

איש קשר:

מר אסי ברק,
ראש צוות תוכנה, מרכז הסייבר, אוניברסיטת בר אילן.
assaf.barak@biu.ac.il