אבטחה – 236607 – תרגיל 5

המגיש: שחק בן-כליפה, ת.ז 311242440

הרעיון הכללי

פתרון התרגיל מתבסס על יצירת enclave יחיד שיודע לעבוד באופן מסונכרן עם שני הלקוחות – אליס ובוב. כמובן שאופן הטיפול באליס ובוב שונה (אמנם עובד על פי אותו עקרון אך יש לבצע הפרדה בטיפול לשם שלמות הפתרון) ועל כן בקבצי הקוד של אליס ובוב כל אחד מעביר כפרמטר מזהה ייחודי על מנת לאפשר ל-enclave לדעת בכל עת במי הוא מטפל. הקוד של אליס ובוב נמצא אצל כל אחד בתיקיה הנקראת על שמו ובקובץ הנקרא על שמו – alice.cpp ו-bob.cpp.

ה-enclave שבו שניהם משתמשים ממומש בתיקיה enclave ומופעל על ידי הקבצים compsecEnclave.cpp ו-compsecEnclave.h.

בנוסף ל-enclave (שכמובן מתפקד כ-trusted app) ישנו קוד הממומש גם untrusted app לביצוע פעולות לא מורשות וקריאה לפונקציות המתאימות בכל שלב.

התקשורת בין אליס ובוב מתבצעת על בסיס sockets.

פירוט הפתרון

- ראשית כל, מתבצע האתחול הראשוני ל-enclave ע"י ()initEnclave. אתחול ה-enclave כמובן מתבצע מ-untrusted מאחר ועדיין לא קיים ה-enclave המשמש כ-trusted. האתחול מתבצע בשלושה שלבים, החל מקבלת הטוקן שנשמר מהטרנזאקציה האחרונה, וכלה בקריאה ל-sgx_create_enclave ולבסוף שמירת העדכון לטוקן (אם התעדכן). תהליך האתחול הוא יחסית סטנדרטי ולכן נעזרתי רבות בדוגמאות הקוד המסופקות ע"י Intel עבור SGX. למשל, חלק רב מפונקציית האתחול initEnclave ועוד.

- לאחר מכן, ניצור ערוץ תקשורת בין אליס ובוב ע"י socket המיועד לכך. לשם כך ממומשות ב-untrusted פונקציות יצירת צד שרת וצד לקוח וקריאה וכתיבה לסוקט. במהלך סכימת העבודה, ככלל, נייצג את אליס בתור השרת ואת בוב בתור הלקוח לשם האחידות.

- כעת, נעביר את המידע של המשתמש הקורא ל-enclave. לצורך כך מימשנו פונקציית עזר לקריאה מקבצים. שלב זה מתבצע בשני תתי שלבים – קודם כל קריאת המידע מהקובץ אל untrusted app ע"י ביצוע קוד כרגיל. לאחר מכן, נבצע כתיבה מה-untrusted app אל ה-enclave. בפועל, בשלב זה כל אחד מהמשתמשים מעתיק אל ה-enclave שלו את המידע ולאחר מכן המידע נמחק מה-untrusted app על מנת שלא תתרחש זליגה של המידה לאחר מכן. בשלב זה קיים ב-enclave של כל אחד מהצדדים כל המידע האישי שלו על הלקוחות בשלמותו.

- בהמשך, ה-enclave יצור שני צמדי מפתחות פומבי ופרטי עבור השימוש. המפתחות בכל צד כמובן יאוחסנו ב-enclave עצמו. הצמד הראשון מאותחל על מנת לתקשר עם המשתמש השני ועל כן המפתח הפומבי יוחזר מהפונקציה ויועבר למשתמש האחר והצמד השני מיועד לשם חתימה של המשתמש. לשם יצירת המפתחות נפתח הקשר ע"י sgx_ecc256_open_context ויצירת המפתחות עצמה מתבצעת ע"י קריאה ל-sgx_ecc256_create_key_pair.

- לאחר יצירת המפתחות, נרצה לבצע החלפה שבה כל אחד יעביר לשני את המפתחות הפומביים שלו. נבצע זאת בתתי שלבים כאשר ראשית בוב מעביר לאליס את המפתחות שלו ולאחר מכן אליס

מעבירה לבוב את המפתח שלה. העברות המפתחות מתבצעות על גבי הסוקט שנפתח. לאחר שהתבצעה החלפת מפתחות פומביים, נוצר ביניהם מפתח משותף לפי DH ע"י שימוש בפונקציה sgx_ecc256_create_shared_key.

- כעת, קיים מפתח משותף, קיים ערוץ תקשורת וכל אחד מחזיק ב-enclave שלו את המידע הפרטי שלו. אמנם המידע הפרטי אינו מוצפן ב-enclave. לשם ביצוע הצפנה זו, נשתמש בפונקציה sgx_aes_ctr_encrypt. לאחר ביצוע הצפנה, כל צד יחתום על המידע עם המפתח הפרטי שלו המיועד לחתימה ע"י שימוש ב-sgx_ecdsa_sign.

- כעת, מתבצעת החלפה של המידע המסווג בשני תתי שלבים. ראשית אליס שולחת את המידע המוצפן שלה אל בוב ולאחר מכן בוב שולח את המידע המוצפן שלו אל אליס. כל אחד מהצדדים שולח את המידע המוצפן ביחד עם החתימה שלו. המידע הנשלח למעשה הוא רשימת כל הלקוחות שעברה הצפנה.

- כעת, כל אחד מהצדדים מחזיק את המידע המוצפן מהצד השני. שני הצדדים מפענחים את המידע שקיבלו באמצעות sgx_aes_ctr_encrypt לפי המפתח המשותף, מוודאים את החתימה על המידע המוצפן שקיבלו ע"י sgx_ecdsa_verify וכותבים אותו ל-enclave.

- כעת, כל אחד מהצדדים מחזיק ב-enclave שלו את המידע בשלמותו, גם את המידע האישי שלו וגם את המידע של הצד השני וכל המידע עבר פענוח. כל צד כעת מבצע את פעולת חישוב הממוצע בתוך ה-enclave בין הלקוחות החופפים. עם סיום הפעולה כל צד חותם על התוצר והפלט מגיע אל החלק ה-untrusted כאשר הוא מכיל רק את הממוצע של הלקוחות החופפים ולאחר שעבר חפיפה.

- לאחר סיום ביצוע שלבים אלה, למעשה הסתיימה הפעולה הנדרשת. על כן, סוגרים את הסוקט והורסים את ה-enclave ע"י קריאה ל-sgx_destroy_enclave.

ההגנה המסופקת

- ראשית כל, המידע מטפל בסוגיות סודיות המידע הנידונה קודם לכן. למעשה כל משתמש אינו רוצה לחשוף את הנתונים שלו בפני הצד השני אך בכל זאת כל צד צריך גישה למידע של השני. על כן, כל צד מחזיק enclave שיקבל הוא באופן מאובטח את המידע מהצד השני ויעביר למשתמש רק את הממוצע המחושב וכך לכל צד אין בעיה להעביר לצד השני את המידע מאחר וזה נעשה בצורה מאובטחת, מוצפנת וללא גישה למשתמש.
- שנית, מבחינת אותנטיקציה – מאחר ונוצרים מפתחות משותפים התקשורת בין הצדדים מוצפנת היטב וניתנת לפענוח רק על ידי מחזיקי המפתח שללא פרצות אבטחה אלה יהיו רק שניהם. בנוסף, לאחר קבלת נתון הממוצע המידע מגיע חתום ע"י ה-enclave שביצע את החישוב.
- לשם ההכללה, כל מידע העובר בין הצדדים חתום ע"י מפתח. לכן, בעת העברת המידע בין הצדדים כל צד מקבל יכול לוודא שמקור המידע הוא אכן כמצופה.
- כל המידע החיוני מטופל אך ורק בסביבה מבודדת של ה-enclave. מאגר הלקוחות, פרטיהם, כמויות וכל מידע אחר נשמרים אך ורק ב-enclave ואך ורק בצורה מוצפנת (כולל בשלבי התקשורת ביניהם) ועל כן אינו נגיש למשתמש חיצוני ובעצם מסופקת כאן סביבת ריצה מבודדת – isolated execution.

- אם נתייחס למקרה שבו אליס ובוב לא נמצאים על אותה מכונה, הכי שדרך הפעולה שמימשנו לא תעבוד באותו אופן. לשם כך, ניתן להשתמש ב-QE המסופק ע"י אינטל כך שכל צד מבצע תקשורת מולו בביצוע RA וכך נוצרת העברה בטוחה של המידע בין הצדדים.