

תדלוק בטוח

מגישים: יואב אוזן ואלכסנדר סיצ'וב מדעי המחשב



‏ 2022

המרכז האקדמי לב

מרצה : ברק עינב

מדעי המחשב

תוכן עניינים

תוכן עניינים**1**

תאור הפרויקט וניתוחי אבטחה2

תרשים ויזואלי של הפרויקט 3

חלקי הפרויקט4-5

הפעלת הפרויקט וחלוקת העבודה ......................6

**תאור הפרויקט במילים**

כיום ישנם מכונית חשמליות שלוקח זמן רב לתדלק אותם , ולכן התעוררנו למצוא פתרון אבטחה שיאפשר תדלוק בטוח ושמירת נתונים של המתדלק .

היות וזמן התדלוק לוקח עדיין זמן רב. יש צורך בהצפנה ברמה גבוהה של נתוני התשלום וכן יש אפשרות לוודאות שפרטי התשלום אכן שייכים למתדלק לשיפור האבטחה .

לכן יצרנו פרויקט המבקש מהמשתמש את פרטי כרטיס האשראי שלו שומר אותו בסביבה בטוחה ובצורה בטוחה (RSA+TEE) ולאחר שהוא עושה זאת הוא מבצע עוד אבטחה של וידוי ע"י שליחת OTP אל מייל הלקוח .

ורק לאחר האימות של כל זה הוא מתחיל לבצע תדלוק.

לא ידוע לנו לפתרון דומה בנושא היות והמכניות החשמליות עדיין חדשות .

**ניתוחי אבטחה**

ישנם שלושה תהלכים שצריכים אבטחה בפרויקט זה-

1. קבלת הנתונים באופן בטוח.
2. שמירת הנתונים במקום בטוח.
3. העברת הנתונים אל השרת בצורה בטוחה .
4. אימות שאכן מדובר בלקוח ולא באדם זר.

הפרויקט שלנו מטפל בעיקר בסעיפים ב ג וד ואינו מתייחס לסעיף א.

ניתן לטפל בסעיף א ע"י הקלדת נתונים בחלון מאובטח שמערכת ההפעלה אינה יכולה לזהות.

והעברה מיידית לסביבה בטוחה TEE

הכנסת כרטיס באפליקציית HOST

שליחת OTP למייל

לצורך אימות אחרון

ותחילת תדלוק.

שליחת נתונים לשרת לביצוע תשלום ופענוח של RSA שם

כיכ

הכנסה של הOTP בHOST ואימות שלה בשרת.

נ

*חלקי התרשים:*

***SERVER***

***HOST***

הפרויקט בנוי משלושה חלקים –

שרת – שממנו הלקוח מקבל שירות. נכתב בc#

HOST- ובו הלקוח מזין נתונים. נכתב בc#

TEE-אזור בטוח לצורך אבטחה. נכתב בJAVA

**שרת**

מכיל אלגוריתם הצפנה RSA ושולח לhost את הpublic key לצורך הצפנת הנתונים.

מקבל נתונים מוצפנים מן הhost ומפענח אותם.

מייצר OTP ושולח למייל לצורך אימות לקוח .

וכן מקבל OTP שלקוח הזין , ומאמת אותו .

**HOST**

מקבל נתוני תשלום מן הלקוח – כרטיס + ת.ז , ומעביר אותם לTEE

מקבל PUBLIC KEY מן השרת ומעביר אותו אל TEE לצורך הצפנה .

מקבל מTEE נתונים מוצפנים ומעביר לשרת לצורך פענוח.

מקבל OTP מן הלקוח ומעביר לשרת לצורך אימות.

**TEE**

מקבל נתוני תשלום מHOST ושומר אותם בFLASH STORAGE

מקבל PUBLIC KEY מן הhost (שנשלח מן השרת) יוצר הצפנה לנתוני התשלום.

ולסיום מעביר את הנתונים המוצפנים אל השרת דרך הHOST

**איך להפעיל את הפרויקט**

יש להתקין את שלושת החלקים של הפרויקט למחשב ולהריץ את השרת באופן נפרד.

ופרויקט HOST באופן נפרד.

לאחר הרצת השרת ניתן לעבוד עם הHOST.

**חלוקת העבודה**

אלכסנדר לקח פיקוד יותר על ההצפנה ועל אלגוריתם RSA

ויואב יותר עבד עם השרת והOTP .

נתקלנו בקושי רב בסנכרון HOST וTEE בפעולות הצפנה ופיענוח.